Université Panthéon-Assas

Université Panthéon-Assas

Ecole doctorale sciences économiques et de gestion, sciences de l'information et de la communication (455)

Thèse de doctorat en Informatique
soutenue le 30 juin 2015

Validation des logiciels d'expertise judiciaire de preuves informatiques

*Thèse de Doctorat / juin 2015

Université Panthéon-Assas

Elina NIKOOAZM
Sous la direction de Monsieur le professeur David NACCACHE, Professeur à l'université Paris II – Panthéon - Assas

Rapporteurs :

Jean Jacques QUISQUATER, Professeur à l'Université Catholique de Louvain
Assia TRIA, Docteur HDR, EDSIS, Ingénieur de recherche, CEA

Membres du jury :
Jean DONIO, Professeur émérite à l'université de Paris II
David BILLARD, Professeur à l'Université des Sciences Appliquées de Genève
Jean Phillipe NOAT, Expert international en cybercriminalité, Instructeur Encase et Cellebrite

Avertissement

La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

Je souhaite exprimer ma gratitude au Professeur David Naccache pour avoir dirigé mes recherches et m'avoir permis la réalisation de ce travail.

J'adresse mon profond respect et ma reconnaissance à Monsieur Jean Donio pour sa confiance et son soutien permanent.

Mes sincères remerciements s'adressent aux membres du jury qui m'ont fait l'honneur de juger mon travail.
Je tiens à remercier tout particulièrement Jean Philippe Noat pour ses encouragements, sa générosité et sa grande disponibilité.

Je tiens également à remercier M. Bill Thompson, directeur du centre de formation Guidance Software en Angleterre pour l'intérêt qu'il a porté à ce travail et pour ses précieux conseils.

Un grand merci à Nathalie, Isabelle, Olivia et Marie-Laure pour leur soutien et leur présence tout au long de ces années de recherche.

Je remercie mon époux pour sa patience et son soutien inconditionnel et sans lequel ce projet n'aurait pas pu aboutir.

Mes affectueuses pensées vont aussi à mes parents pour leur amour et leur soutien.

Je dédie cette thèse à mon fils, mon plus grand bonheur.

Résumé :

Dans les affaires judiciaires, les juges confrontés à des questions d'ordre techniques en matière informatique, recourent à des experts qui mettent leur savoir faire au service de la justice.

Régulièrement mandatés par les tribunaux, ils ont pour mission d'éclairer le juge en apportant des éléments de preuve utiles à l'enquête.

Ils recherchent dans les scellés informatiques les éléments relatifs aux faits incriminés en préservant l'intégrité des données et évitant toute altération des supports originaux.

Les éléments de preuve ainsi recueillis sont analysés par l'expert qui déposera ses conclusions au magistrat sous forme d'un rapport d'expertise.

les investigations techniques sont effectuées à l'aide des outils très sophistiqués qui permettent de prendre connaissance des informations présentes, effacées, cachées ou chiffrées dans les supports numériques examinés.

Ce qui requiert une parfaite maîtrise du matériel déployé et une identification claire des bonnes pratiques de la discipline.

Ce projet de recherches vise à mettre en exergue les défis techniques aux quels sont confrontés les experts, la complexité des outils utilisés dans le cadre des investigations techniques et l'importance de la mise en place des tests de validation qui permettent de connaître les capacités et limites de chaque outil.

Descripteurs :

Expertise Judiciaire en Informatique, Investigation technique, Preuves numérique, Validation, outils d'analyse de preuves.

Title and Abstract:

Validation of digital forensic software used in courts

In criminal cases, judges confronted with questions of technical order in computer technology, designate expert witnesses who put their expertise at the service of justice.

Duly appointed by the courts, they help the judge by providing evidence relevant to the investigation.

They search the suspect's seized digital devices for elements of computer related crime, while preserving the integrity of the data and avoiding any alteration of the original media.

The evidence thus collected is analyzed by a digital forensic expert who will document their findings to the judge in a report.

Technical investigations are conducted by using powerful and sophisticated tools to find the current files and recover deleted, hidden or encrypted data from the digital media device examined.

This requires perfect control of the utilized equipment and a clear identification of the methods used during the analysis.

This research project aims to highlight the technical challenges which experts face, the complexity of digital forensic tools used for technical investigations, and the importance of their validation to understand the capabilities and limitations of each tool.

Keywords :

Digital Forensic, Technical Investigation, Digital Evidence, validation, Digital forensic tools.

Principales abréviations

ADFM	Abstract Digital Forensic Model,
AF	Advanced Format,
BHO	Browser Helper Object,
CART	Computer Analysis and Response Team,
CEDH	Convention Européenne des Droits de l'Homme,
CFTL	Comité Français des Tests Logiciels,
CFTT	Computer Forensics Tool Testing,
CFFTPM	Cyber Forensic Field Triage Process Model,
C.P.P	Code de Procédure Pénale,
DCO	Device Configuration Overlay,
DELV	Distributed Environment for Large-scale investigations,
DEX	Digital Evidence Exchange,
DFRWS	Digital Forensic Research Workshop,
DFTT	Digital Forensics Tool Testing,
DFXML	Digital Forensic XML,
EDIP	Enhanced Digital Investigation Process Model,
ENFSI	European Network of Forensic Science Institutes,
FBI	Federal Bureau of Investigation,
FS-TST	Forensic Software Testing Support Tools,
HPA	Host Protected Area,
IACIS	International Association of Computer Investigative Specialists,
IDEMA	International Disk drive Equipment and Materials Association,
IDIP	Integrated Digital Investigation Model,

IOCE International Organization on Computer Evidence,

ISTQB International Software Testing Qualifications Board,

LERTI Laboratoire d'Expertise et de Recherche de Traces Informatiques,

NIJ Institut national de la justice,

NIST National Institute of Standards and Technology,

SSD Solid State Drive,

SWGDE Scientific Working Group on Digital Evidence,

Sommaire

Introduction générale: Contexte scientifique et problématique _____ 13

I Méthodes et pratiques de l'expertise judiciaire en Informtaique _____ 16

1. Introduction _____ 16

2. Concept de sciences criminologiques et expertise judiciaire en Informatique____ 17

2.1. Terminologies et historique _____ 17

2.1.1 Sciences Criminologiques _____ 17

2.1.2 Sciences Criminalistiques _____ 18

2.1.3 Expertise Judiciaire en Informatique _____ 19

2.2. L'apport de McKemmish _____ 21

2.2.1 Identification de la preuve numérique _____ 21

2.2.2 Préservation de la preuve numérique _____ 21

2.2.3 Analyse de la preuve numérique _____ 22

2.2.3 Présentation de la preuve numérique _____ 22

2.3. Définition proposée par DRFWS _____ 23

3. Standardisation et processus d'analyse judiciaire de preuves informatiques ____ 24

3.1. Tentatives de standardisation au niveau européen et international _____ 25

3.1.1 Equipe d'analyse informatique et d'intervention (CART) _____ 25

3.1.2 Organisation internationale dans le domaine de la preuve numérique (IOCE) _____ 26

3.1.3 Le groupe de travail scientifique sur les preuves numériques (SWGDE) _____ 26

3.1.4 Institut national de la justice (NIJ)_____ 27

3.1.5 Réseau européen des Instituts de Police scientifique (ENFSI) _____ 27

3.2. Guides de bonnes pratiques dans l'analyse de preuve numérique_____ 28

3.3. Modèles associés à l'expertise judiciaire en informatique _____ 29

3.3.1 Les modèles de McKemmish et DFRWS _____ 29

3.3.2 Modèle abstrait de l'investigation numérique (ADFM) _____ 30

3.3.3 Processus d'investigation numérique intégré (IDIP) _____ 30

3.3.4 Modèle du processus d'investigation numérique renforcé (EDIP) _____ 31

3.3.5 Modèle de processus de triage dans le domaine de l'investigation numérique (CFFTPM) _____ 31

3.3.6 Modèle de maturité DF-C²M² _____ 30

4. Techniques d'investigation numérique _____ 34

4.1. Analyse post-mortem en laboratoire_____ 34

4.2. Détection d'intrusion et analyse de réseaux _____ 48

4.2.1 Principe de "l'échange de Locard" et son application dans le domaine de l'investigation numérique _____ 38

4.2.2Analyse de "Malwares" _____ 38

4.3. Nouvelles techniques d'analyse de preuve _____ 39
4.3.1 Analyse dite "Live Forensic" _____ 40
4.3.2 Analyse de preuves et émulation de disque dur _____ 42
4.3.3 Examen des machines virtuelles _____ 45
4.4. Complexité liée au Cloud Computing _____ 45

II Etat de l'art sur les technologies d'investigation numérique _____ 47

2. Introduction _____ 47

2. Méthode scientifique et validation des outils d'analyses informatiques _____ 48
2.1. Admissibilité de la preuve et processus scientifique devant la justice américaine _____ 48
2.1.1 L'arrêt "FRYE v United States _____ 48
2.1.2 Les règles fédérales en matière de preuves (FRE) _____ 49
2.1.3 "Le standard DAUBERT" _____ 49
2.2. les outils d'investigation de nouvelles générations _____ 52
2.2.1 Panorama des technologies d'investigations _____ 52
2.2.2 Principaux logiciels à code source libre _____ 54
2.2.3 Principaux outils de licences propriétaires _____ 55
2.3.Limitation des outils d'expertise en informatique _____ 57
3.2.1 Techniques de camouflage dites "anti-forensic" _____ 57
3.2.2 Prototype DELV (Environnement numérique pour une investigation à grande échelle) _____ 58
2.4. Utilisation du langage XML dans le domaine de l'expertise judiciaire _____ 59
2.4.1 Le prototype XIRAF et la technologie XML _____ 59
2.4.2 DEX(Digital Evidence Exchange) _____ 60
2.4.3 DFXML "Investigation numérique XML" _____ 61

3. Principales fonctionnalités des technologies d'analyse de preuves informatiques 63
3.1. Acquisition physique des données _____ 63
3.1.1 Copie physique de disques durs _____ 63
3.1.2 Différents formats d'acquisition d'images _____ 66
3.2. Vérification de l'intégrité des données _____ 68
3.2.1 Calcul d'empreinte numérique ou la valeur de "HASH" _____ 68
3.2.2 Comparaisons des empreintes numériques des fichiers _____ 69
3.2.3 Identification par analyse de signature _____ 70
3.3. Analyse et extraction des données _____ 71
3.3.1 Techniques de récupération des données supprimées sur un système Windows _____ 71
3.3.1.1 Récupération des partitions effacées sur un disque dur _____ 71
3.3.1.2 Récupération de fichiers effacés sur un disque dur _____ 72
3.3.1.3 Récupération de fichiers basée sur la technique du "Carving" _____ 74
3.3.2 Analyse du registre _____ 74

3.3.3 Récuération de la messagerie et recherche des traces sur Internet_____ 79

III Evaluation et perspective de certification des logiciels d'investigation numérique **_____ 83**

1. Introduction _____ 83

2. Tests de logiciels _____ 87

2.1. Concepts de "validation" et "vérification" _____ 87

2.1.1 La "vérification" des logiciels _____ 88

2.1.2 La "validation" des logiciels _____ 88

2.2. Méthodes de tests logiciels "boîtes noires" et "boîtes blanches" _____ 89

2.2.1 Méthodes de tests "boîte noire" _____ 89

2.2.2 Méthodes de tests "boîte blanche" ou tests structurels_____ 91

2.3. Importance de la mise en œuvre des tests de "validation" de logiciels d'analyse de preuve numérique _____ 91

3. Les normes internationales et les enjeux de la certification dans le domaine de l'expertise en informatique _____ 93

3.1. Exigences de qualité appliquées à l'expertise_____ 94

3.1.1 La norme ISO 9001 _____ 94

3.1.2 La norme AFNOR NFX 50-110 "prescriptions générales de compétence pour5 une expertise" _____ 95

3.1.3 La norme internationale ISO/CEI 17025 _____ 95

3.2. Exigences de la sécurité de l'information et gestion d'incidents _____ 97

3.2.1 La norme ISO 27002 (anciennement ISO: CEI 17799) _____ 97

3.2.2 La norme internationale ISO 27001 intitulée "Technologies de l'information-Techniques de sécurité-Systèmes de gestion de sécurité de l'information- Exigences" ____ 97

3.3. Exigences liées au respect de la méthodologie et de l'intégrité de la preuve durant les phases d'investigation numérique _____ 97

4. Tests et travaux de recherches _____ 99

4.1. Travaux de l'Institut National des Normes et de la Technologie _____ 99

4.2. Recommandations générales du groupe de travail sur l'investigation numérique _____ 101

4.3. Validation par des organes indépendants _____ 103

4.3.1 Travaux de Brian Carrier _____ 103

4.3.2 Travaux de SLAY et BECKETT _____ 103

4.3.3 Travaux de BYERS et SHAHMEHRI _____ 107

4.3.4 Travaux de CUSACK et LIANG _____ 109

IV Expérimentations et proposition d'une méthodologie d'évaluation des outils d'analyse judiciaire de preuve numérique ____ **110**

1. Introduction ____ **110**

2. Etude de la structure géométrique des disques durs classiques et des nouveaux formats de disques ____ **111**

2.1. La technologie magnétique et les méthodes d'accès aux zones dissimulées des disques durs ____ 111
2.1.1 La capacité des disques durs magnétiques ____ 112
2.1.2 Techniques de dissimulations utilisées par les constructeurs ____ 113
2.1.3 Copie physique des secteurs cachés d'un disque dur et la question du respect de l'intégrité du support original ____ 116
2.2. Problématique de l'expertise des disques durs au format avancé (AF) ____ 119
2.2.1 Encase version 6.18.1 ____ 121
2.2.2 Encase version 7.06 ____ 122
2.3. La complexité de la recherche de preuves sur les supports SSD ____ 123
2.3.1 Description de l'architecture des disques SSD et leurs caractéristiques techniques ____ 124
2.3.2 Présentation des fonctions avancées des SSD ____ 126
2.3.2.1 Algorithmes de gestion de l'usure ____ 126
2.3.2.2 Algorithme de "Garbage Collector" ____ 127
2.3.2.3 La commande TRIM ____ 128
2.3.3 Recommandations techniques de recherches de preuves sur les supports SSD ____ 129

3. Evaluation des fonctions de récupération de données supprimées du logiciel Encase Forensic ____ **131**

3.1. Introduction ____ 131
3.1.1 Objectifs des tests ____ 131
3.1.2 Documents de références (conformité à la documentation d'utilisation) ____ 134
3.1.3 Terminologies et glossaires ____ 135
3.2. Présentation du plan de test détaillé ____ 136
3.2.1 Description de l'environnement de tests ____ 137
3.2.2 Configurations matérielles des tests ____ 137
3.2.3 Outils de tests utilisés ____ 138
3.2.4 Description de la méthodologie ____ 138
3.2.5 Exigences générales ____ 140
3.2.6 Cas de tests ____ 140
3.2.6.1 Encase Law Enforcement version 6.18.1 ____ 145
3.2.6.1.1 Cas de test CT-01-V6 ____ 145
3.2.6.1.2 Cas de test CT-02-V6 ____ 146
3.2.6.1.3 Cas de test CT-03-V6 ____ 147
3.2.6.1.4 Cas de test CT-04-V6 ____ 148
3.2.6.1.5 Cas de test CT-05-V6 ____ 148

3.2.6.1.6 Cas de test CT-06-V6 _____ 149
3.2.6.1.7 Cas de test CT-07-V6 _____ 150
3.2.6.1.8 Cas de test CT-08-V6 _____ 151
3.2.6.2 Encase version 7.06 _____ 152
3.3. Résultats expérimentaux et observations _____ 154
3.3.1 Rapports de tests _____ 154
3.3.1.1 Rapports de tests Encase version 6.18.1 _____ 154
3.3.1.1.1 Cas de test CT-01-V6 _____ 154
3.3.1.1.2 Cas de test CT-02-V6 _____ 157
3.3.1.1.3 Cas de test CT-03-V6 _____ 159
3.3.1.1.4 Cas de test CT-04-V6 _____ 162
3.3.1.1.5 Cas de test CT-05-V6 _____ 165
3.3.1.1.6 Cas de test CT-06-V6 _____ 166
3.3.1.1.7 Cas de test CT-07-V6 _____ 168
3.3.1.1.8 Cas de test CT-08-V6 _____ 171
3.3.1.2 Rapports de tests Encase version 7.06 _____ 173
3.3.1.2.1 Cas de test CT-01-V7 _____ 173
3.3.1.2.2 Cas de test CT-02- V7 _____ 176
3.3.1.2.3 Cas de test CT-03- V7 _____ 178
3.3.1.2.4 Cas de test CT-04- V7 _____ 181
3.3.1.2.5 Cas de test CT-05- V7 _____ 183
3.3.1.2.6 Cas de test CT-06- V7 _____ 186
3.3.1.2.7 Cas de test CT-07-V7 _____ 188
3.3.1.2.8 Cas de test CT-08-V7 _____ 190
3.3.2 Synthèse des résultats obtenus _____ 193
3.3.2.1 Encase version 6.18.1 _____ 194
3.3.2.2 Encase version 7.06 _____ 211
3.4. Conclusions et perspectives _____ 226

Bibliographie _____ ***229***

Index _____ ***232***

Table des annexes _____ ***235***

Introduction générale :
Contexte scientifique et problématique

Il n'y a pratiquement plus d'informations qui transitent dans le monde sans qu'un support informatique ne soit utilisé.
En 2000, des travaux réalisés par l'Université de Californie montrent que 93% des flux de données échangés dans les entreprises sont partagés sous forme numérique[1].

Il y a une vingtaine d'années, les supports de stockages informatiques ne dépassaient pas quelques mégaoctets alors qu'aujourd'hui la capacité des disques durs dépasse le « Téraoctet » tant pour les particuliers que pour les entreprises.
En avril 2014, selon une étude menée par le cabinet IDC auprès de deux cents entreprises, les volumes d'informations générées par les appareils connectés représentent quatre « Zettaoctet »[2] et on estime qu'ils atteindront plusieurs « Yottaoctets » dans dix ans.

Ces évolutions technologiques ont également une incidence sur les méthodes d'analyses et d'investigations techniques.
Lorsque la réalisation d'un crime ou un délit implique l'utilisation de supports numériques, l'informatique constitue le moyen de preuve principal mis à la disposition de la justice.

Le magistrat saisi d'une affaire judiciaire peut désigner le spécialiste de son choix dans une ordonnance de commission d'experts.
A la suite de placement sous scellés des pièces à conviction par les enquêteurs, l'expert nommé prendra possession des supports.
A ce titre, il utilise des moyens techniques pour rechercher des traces informatiques en rapport avec les faits incriminés et met ses compétences au service de la justice.

[1] « The five Organizational Stages of Digital Preservation », Anne R. Kenny & Nancy Y. McGovern.

Avec l'émergence de nouvelles technologies et le besoin d'outils sophistiqués pour l'analyse des supports numériques, l'expertise judiciaire en informatique a connu un essor rapide ces dernières années.

De plus en plus de logiciels et matériels coûteux sont déployés par les spécialistes pour accomplir leur mission et assister la justice.

Dans le cadre d'une expertise réalisée en rapport avec une enquête criminelle, les professionnels du monde judiciaire accordent une grande importance au respect de l'intégrité de la preuve et à l'exactitude des résultats produits devant la justice.

Bien que des guides de bonnes pratiques soient proposés par les compagnies d'experts et membres de la profession, aucune réglementation n'encadre spécifiquement la conduite d'une expertise informatique alors même que le respect absolu de certaines règles est essentiel.

Les logiciels d'analyse de preuves de nouvelles générations, deviennent de plus en plus complexes et conduisent les spécialistes à s'interroger sur leur fiabilité et performance.

Il faut comprendre le fonctionnement de l'outil informatique et tester ses différentes fonctionnalités afin de connaître ses capacités et limites avant toute utilisation dans le cadre d'une expertise pénale.

La validation des technologies utilisées dans un cadre judiciaire constitue l'une des problématiques identifiées par les experts, mais les travaux dans ce domaine restent isolés. Cela constituerait pourtant la garantie d'une procédure juste et équitable nécessaire pour l'équilibre et le respect des droits des parties.

Le procès équitable est un fondement de la démocratie et figure dans l'article 6-1 de la Convention européenne des droits de l'homme et du citoyen.

La complexité des expérimentations ainsi que le manque de temps et de moyens rendent cette tâche ardue et ne permettent pas de définir des méthodologies normées.

Cette question, difficile à régler, a pourtant suscité beaucoup d'intérêt de la part des praticiens et au sein de la communauté scientifique.

Elle est soulevée dans certains pays, principalement aux Etats-Unis où la procédure

---

[2] « The digital Universe of opportunities », IDC, Avril 2014.

est très encadrée dans ce domaine depuis la décision "DAUBERT"[3] rendue par la Cour suprême des Etats Unis en 1993, qui identifie les différents critères d'admissibilité de la preuve scientifique devant les juridictions.

En France, l'utilisation des logiciels d'expertise dans un cadre judiciaire n'est soumise ni à des exigences de tests, ni au respect de règles particulières.
En l'absence d'un référentiel unique conçu pour la discipline, certains praticiens se tournent vers des normes du type ISO dont la mise en œuvre s'avère compliquée et coûteuse.

Nos travaux de recherche ont pour objectif de mener des expérimentations sur un programme dédié à l'investigation technique et de proposer une méthodologie d'évaluation qui serait applicable à tous les logiciels utilisés dans le cadre de l'expertise informatique.
Avant de procéder aux tests, nous soulignerons l'état de l'art dans la discipline et l'importance de la bonne compréhension des différentes technologies existantes, leurs différences, leurs complexités et le fait qu'elles peuvent avoir une incidence sur le comportement des programmes d'analyse de preuves judiciaires.

Puis, nous ferons un travail de comparaison entre deux versions différentes du même programme afin d'observer leurs comportements en mettant en évidence les possibilités techniques offertes par ces outils.
Nous analyserons les limites de ces logiciels, notamment celles inhérentes aux technologies utilisées dans les supports informatiques et ce qui les différencie.

Enfin, nous validerons les résultats des expérimentations et ferons un parallèle entre les résultats attendus et ceux obtenus à partir de plusieurs tests.

[3] Court suprême des Etats-Unis, « Daubert V.Merrell Dow Pharmaceuticals, 509 US.579 (1993).

Première partie: METHODES ET PRATIQUES DE L'EXPERTISE JUDICIAIRE EN INFORMATIQUE

Chapitre 1 - Introduction

L'expertise judiciaire en informatique est une discipline relativement récente qui se situe entre la technique et le droit.
Elle permet aux spécialistes de rechercher toutes informations, présentes ou effacées, sur un support de stockage, à l'aide des technologies de dernières générations, constituant un moyen de preuve dans le cadre d'une enquête en cours.

A l'instar des spécialistes de la police scientifique dans les domaines tels que la balistique ou les empreintes digitales, qui prennent beaucoup de précautions afin de recueillir les preuves sur une scène de crime, les experts informatiques prennent toutes les mesures adéquates pour ne laisser aucune trace de leur passage sur le matériel examiné.

Le déroulement de l'expertise et les preuves produites devant la justice doivent intervenir dans le respect total des principes fondamentaux régis par le Code de Procédure Pénale (articles 156 à 169 du C.P.P).

L'admissibilité de la preuve devant les juridictions, nécessite le respect de l'ensemble de ces règles et l'expert commis est tenu de prendre en considération ces dispositions afin que les preuves présentées devant la justice soient irréfutables.

Se rapprochant de la police technique et scientifique, l'expertise judiciaire en informatique commence à devenir une discipline indépendante en pleine expansion qui requiert la maîtrise de différentes techniques d'analyses de preuves numériques.

Chapitre 2 - Concepts de « sciences criminologiques » et « Expertise judiciaire en Informatique»

2.1 Terminologies et historique

Contrairement à l'expertise judiciaire en informatique, née au vingtième siècle, les sciences criminologiques et criminalistiques mettant la science au profit de l'enquête, sont apparues quelques siècles auparavant.

2.1.1 « Sciences criminologiques »

Raymond Gassin décrit le concept de « *sciences criminologiques* » comme « *la science qui étudie les facteurs et les processus de l'action criminelle et qui détermine, à partir de la connaissance de ces facteurs et de ces processus, les stratégies et les techniques les meilleures pour contenir et si possible réduire ce mal social* »[4].

Bien que les origines de la criminologie restent incertaines, les juristes situent la genèse de la discipline entre le dix-septième et dix-huitième siècle.
Elle consistait à l'étude du comportement et de la personnalité des criminels afin de caractériser la dangerosité des individus et préconiser à leur encontre des sanctions répressives.

C'est à cette période qu'apparaissent également la notion de la prévention du crime et le principe de la « *légalité des délits et des peines* », énoncé par l'article 8 de la déclaration des droits de l'homme et du citoyen.

[4] Raymond GASSIN, *Criminologie*, Précis Dalloz, 6ème éd. 2007.

2.1.2 « Sciences criminalistiques »

Les « *sciences criminalistiques* » constituent l'ensemble des techniques appliquées à l'investigation criminelle, permettant d'aider la justice à rechercher la preuve d'un crime, identifier son auteur et déterminer son mode opératoire.
Elle regroupe des domaines comme la police technique, la police scientifique, la toxicologie et la médecine légale.
Discipline complémentaire et souvent confondue avec la criminologie, elle est apparue à la fin du dix-neuvième siècle.

En France, Alphonse Bertillon et Edmond Locard, sont les deux figures emblématiques de la criminalistique.

Les travaux d'autres grands scientifiques ont également apporté une importante contribution en mettant la science à la disposition de la justice.
Francis Galton, scientifique anglais, publie en 1850 un ouvrage relatif à ses travaux sur les empreintes digitales.
Selon lui, il y a seulement une chance sur soixante quatre milliards pour que deux personnes puissent posséder des empreintes identiques[5].
Alphonse Bertillon, connu comme le père de la police scientifique, contribue aux travaux et techniques d'identifications des personnes.
Il est le fondateur de l'anthropométrie et de la fiche signalétique.
En 1902, il réussit à identifier un criminel grâce à ses empreintes digitales.
Edmond Locard, pionnier dans le domaine de la médecine légale, a crée en 1910 le premier laboratoire français de police technique à Lyon.
Il a été à l'origine des grands fondements de la police scientifique et son héritage est précieux dans l'expertise judiciaire actuelle.

Leone Lattes, spécialiste en médecine légale, crée en 1915, le test d'identification des groupes sanguins et en fait usage dans une affaire judiciaire.
Calvin Goddard, expert en balistique, a identifié en 1929, les armes qui ont servi lors du « *massacre de la Saint Valentin* ».

[5] « Des empreintes digitales aux empreintes génétiques, à la recherche de la preuve indiscutable », Nicole Le Douarin.

Cette découverte a permis aux enquêteurs d'arrêter l'un des criminels.
Albert Sherman Osborn est un pionnier et le premier américain expert en écritures et Hans Gustav Adolf Gross (1847-1915), magistrat autrichien, préconise l'utilisation de la science dans les investigations criminelles et crée le concept de la «*criminalistique*».

2.1.3 « Expertise Judiciaire en Informatique »

L'expertise judiciaire en Informatique est une discipline récente et différente des autres domaines techniques et scientifiques.
Pour la première fois, tout ce qui est criminel va être mémorisé sur des supports numériques et la recherche puis l'extraction des éléments de preuves interviennent au moyen d'outils spécialisés.

Dans le cadre d'une procédure judiciaire, le juge demande à un expert de porter une appréciation technique sur les faits afin de l'éclairer sur les questions spécifiques.
Le juge pourra s'appuyer sur cet avis pour fonder sa décision.

Pour confier une mission d'expertise judiciaire à un spécialiste de l'informatique, le magistrat a la liberté de désigner toute personne de son choix qu'il estime techniquement compétente.
Cette disposition est expressément prévue par l'article 157 du Code de Procédure Pénale qui dispose :
«*Les experts sont choisis parmi les personnes physiques ou morales qui figurent sur la liste nationale dressée par la Cour de Cassation ou sur une des listes dressées par les Cours d'Appel dans les conditions prévues par la loi n°71-498 du 29 juin 1971 relative aux experts judiciaires. A titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes* ».
Le terme « *Computer Forensic* » ou « *Digital Forensics* » est utilisé par les anglo-saxons pour désigner l'expertise en informatique.
En français ce vocable est souvent traduit de l'anglais par la terminologie « *analyse inforensique*».

Le mot « *Forensic* » qui vient du latin « *forensi* » signifie « *forum* » et fait référence au lieu où se tenaient les débats ou les procès durant l'Antiquité.

Le laboratoire d'analyse technique LERTI, dans son « *glossaire de l'informatique légale* »[6], fait une distinction entre les terminologies « *Investigation numérique légale*» ou « *Informatique légale* » pour désigner l'expertise judiciaire en informatique et « l'*investigation numérique* » à laquelle il attribue une portée plus large et extra-judiciaire.

Pour notre part, nous retiendrons indifféremment les terminologies "recherche de preuves informatiques", "recherche de preuves numériques" ou "investigation informatique ou technique".

Il n'est pas aisé de dater précisément les origines de cette discipline mais la plupart des spécialistes s'accordent à dire qu'elle est née aux Etats-Unis, il y a une trentaine d'années, lorsque les enquêteurs ont constaté que les ordinateurs étaient utilisés pour perpétrer des actions criminelles.

En 1984, le FBI a crée l'entité CART (équipe d'analyse informatique et d'intervention)[7] qui avait pour mission d'analyser et récupérer des données sur des ordinateurs.
En 1990, Michael R. Anderson, pionnier dans le domaine de l'investigation technique, a cofondé l'union internationale des spécialistes d'investigation en Informatique (IACIS)[8] à Portland en Oregon, réunissant un groupe de spécialistes dans la discipline.
C'est lui qui a mis en place les premières formations relatives à la récupération de la preuve informatique sur les ordinateurs.

[6] www.lerti.fr/web/documents_public.php, « glossaire de l'informatique légale.pdf », page 4.
[7] « A Brief history of the FBI », www.fbi.gov
[8] IACIS (International Association of Computer Investigative Specialists).

2.2 L'apport de McKemmish:

Rodney MCKEMMISH, dans un article publié en 1999, intitulé « *what is Forensic Computing?* » définit la recherche de preuves informatiques comme un « *processus qui permet d'identifier, préserver, analyser et présenter la preuve numérique afin qu'elle puisse être légalement acceptée*»[9].

Son apport est très important car tous les autres auteurs se sont inspirés de cette définition pour décrire la discipline.
Selon MCKEMMISH, le processus d'analyse de preuves numériques est constitué de quatre phases majeures :

2.2.1 Identification de la preuve numérique

L' « *identification* » de la preuve constitue la première é&tape du processus d'investigation.
Dans un premier temps, tout support numérique susceptible de contenir des indices ou des éléments probants doit être identifié .
Cela sera déterminant dans le choix de l'outil adéquat pour analyser les supports incriminés.

2.2.2 Préservation de la preuve numérique

Cette seconde phase est particulièrement importante car elle consiste à préserver l'authenticité et l'intégrité des supports originaux.
Si l'un des éléments de preuve recueillis est altéré, il risque d'être irrecevable devant les tribunaux.
Il arrive toutefois que dans certaines circonstances des modifications soient apportées au support original, afin d'accéder aux données.
Un tel changement doit être documenté et expliqué dans le rapport d'expertise.

[9] Rodney McKemmish, « What is Forensic Computing ? », Australian Institute of Criminolgy- n°118 ;

2.2.3 Analyse de la preuve numérique

L'extraction et l'analyse des données constituent la troisième phase du processus d'investigation.
Cela signifie que les données numériques doivent être recueillies sous une forme intelligible et exploitable.

2.2.4 Présentation de la preuve numérique

La dernière phase est la présentation, au magistrat, de la preuve numérique, sous forme d'un rapport d'expertise.
L'admissibilité des éléments de preuve devant les tribunaux, requiert le respect de quatre conditions:

a) Une manipulation minimale des supports originaux :
La règle d'or en matière d'expertise en Informatique consiste à préserver l'intégrité de la preuve numérique.

b) La justification de chaque modification apportée pendant la phase d'analyse :
Toute modification apportée au support original, doit être justifiée par l'expert dans son rapport qui doit également expliquer que cela n'aura aucune incidence sur la nature même de la preuve.

c) Le respect des bonnes pratiques :
Les techniques utilisées doivent respecter l'état de l'art et les règles applicables en matière de collecte de preuves.

d) L'expert doit remplir sa mission sans surestimer son niveau de compétence :
Il est impératif d'avoir conscience des limites de sa propre connaissance.
L'expert doit maîtriser les technologies utilisées et apporter des explications claires sur la fiabilité des techniques employées ayant permis de produire la preuve devant la justice.

2.3 Définition proposée par « DFRWS »

En août 2001, le premier groupe de travail DFRWS, regroupant une communauté d'experts, s'est réuni aux Etats-Unis dont l'objectif était de partager les connaissances et faire évoluer la recherche dans le domaine de l'investigation numérique.

Les travaux de ce groupe ont contribué à la proposition d'une nouvelle définition du terme anglais « *digital forensic* » :
Il s'agit de l'« *utilisation des méthodes scientifiquement prouvées pour la préservation, collecte, validation, identification, analyse, interprétation, documentation et présentation de la preuve numérique provenant de supports informatiques dans l'objectif de faciliter ou de contribuer à la compréhension des faits incriminés ou à la prévention des actions illicites* »[10].
Cette définition souligne plusieurs points importants :
Les techniques utilisées pour analyser la preuve, correspondent à des « *méthodes scientifiquement prouvées* ».

De plus, la définition proposée est plus complète que celle suggérée par McKemmish en 1999, puisqu'elle distingue huit phases dans le processus d'investigation.

Enfin, elle met en évidence l'apport important de l'analyse et l'exploitation des supports numériques car les informations retrouvées pourront contribuer à la manifestation de la vérité ou à empêcher qu'une infraction soit commise.

Ces travaux ont également été l'occasion de débats relatifs à la mise en place de standards ou de bonnes pratiques dans le domaine de l'analyse judiciaire des preuves informatiques.

[10] Dfrws Technical Report, « A road Map for Digital Forensic Research », 7-8 Août 2001

Chapitre 3 - Standardisation et processus d'analyse judiciaire de preuves informatiques

Depuis la genèse de l'expertise judiciaire en informatique, trois grandes phases peuvent été identifiées :

La première période se caractérise par la constatation de l'absence de procédures et d'outils adaptés pour les enquêtes relevant de la criminalité informatique et un vide juridique sur les questions liées à la collecte de preuves numériques.

La seconde phase apparaît vers la fin des années quatre-vingt lorsque des entités comme le CART ont été autorisées à intervenir dans les enquêtes de cybercriminalité aux Etats-Unis.
C'est durant cette période que des outils spécialisés ont été développés et la preuve numérique est encadrée sur le plan légal.

La dernière phase concerne l'état actuel de la technologie, marquée par l'apparition d'outils sophistiqués de dernière génération.
Aujourd'hui, l'informatique judiciaire est considérée comme une discipline scientifique permettant la collecte des données en temps réel, le développement d'outils performants et l'application de protocoles structurés.
Par ailleurs, le domaine de l'investigation numérique intéresse de plus en plus les entreprises notamment pour les audits de sécurité des systèmes d'information.

Il est très important de développer des procédures constantes et standardisées pour établir une cohérence entre les normes juridiques et techniques.
Dans un article[11] relatif à l'harmonisation des procédures d'analyse de preuves informatiques, les auteurs proposent un modèle qui prend en considération les deux dimensions juridiques et techniques de la discipline.

[11] « Standardization of Computer Forensic Protocols and Procedures ». REIS Marcello Abdalla Dos & Paulo Licio de Geus

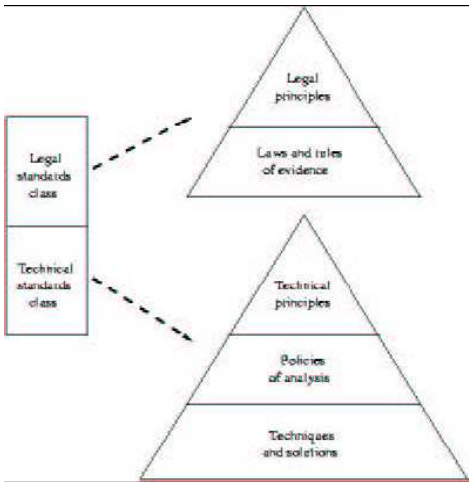


Figure1- Modèle de standardisation- Source[12]

Dans ce modèle, l'aspect légal est relatif aux dispositions juridiques régissant notamment les règles de l'admissibilité de la preuve devant les tribunaux.

La dimension technique concerne toutes les règles de procédure permettant la collecte et l'analyse de la preuve dans le respect de l'intégrité des données du support d'origine.

Depuis plusieurs années, des groupes de travail tentent d'harmoniser les pratiques expertales dans le domaine de l'informatique mais à ce jour, il n'y a pas d'harmonisation des règles de la discipline.

3.1 Tentatives de standardisation au niveau européen et International

Les principaux travaux dans le sens d'une harmonisation ou de standardisation des règles de procédures sont proposés par quelques groupes de recherches.

3.1.1 « Equipe d'analyse informatique et d'intervention » (CART):

Avec la recrudescence de la criminalité informatique, le laboratoire du FBI et des services de police aux Etats-Unis, ont commencé à développer dès 1984, un programme pour examiner la preuve informatique.

Afin de répondre à une demande croissante des professionnels de l'investigation, le FBI a crée une équipe de spécialistes intervenant dans l'analyse de la preuve numérique.

Depuis sa création, cette organisation a développé des formations sur les techniques d'analyses et de recherches sur des supports numériques avec le respect de l'intégrité des données.

3.1.2 «Organisation internationale dans le domaine de la preuve numérique» (IOCE):

Cette organisation a été fondée en 1995[13] dans le but de mettre en place un forum d'échanges au niveau international entre différents services de police spécialisés, dans le domaine de la criminalité informatique et la recherche de preuves numériques. En 1999, lors de la conférence internationale sur les crimes de haute technologie et d'investigation numérique, elle a réuni un groupe de travail qui a adopté des règles de procédures standardisées en matière de récupération des données informatiques.

3.1.3 « Le groupe de travail scientifique sur les preuves numériques » (SWGDE):

Il a pour mission de rassembler différentes organisations et agences gouvernementales intervenant dans le domaine d'investigation technique.

Initialement baptisé « *groupe de travail technique sur les preuves numériques*» (TWGDE), son nom a été remplacé en 1999 par le « *groupe de travail scientifique sur les preuves numériques*».[14]

Il contribue à l'élaboration des méthodes et des guides de bonnes pratiques pour la récupération, la préservation et l'analyse des preuves numériques sur différents types de supports informatiques et multimédia (audio, imagerie, dispositifs électronique).

---

[12] REIS Marcello Abdalla Dos & Paulo Licio de Geus, « *Standardization of Computer Forensic Protocols and Procedures*», 14 novembre 2001, page 4.

[13] www.fbi.gov

[14] « An historical perspective of digital evidence : A forensic scientist's view» , Carrie Morgan Whitcomb. International Journal of Digital Evidence.

Ce groupe de travail a publié de nombreux documents sur les meilleures pratiques de l'expertise judiciaire en informatique.
Ce sont des lignes directrices générales ayant pour objectif de guider les experts et enquêteurs dans l'analyse de la preuve numérique et la mise en place de standards dans la discipline.

3.1.4« Institut National de la Justice» (NIJ):

L'Institut National de la Justice est un organisme américain de recherches et développement des technologies au profit de la justice pénale.
A travers son centre de criminalité lié aux technologies numériques, il travaille en partenariat avec d'autres organisations afin de mettre en place des standards dans le domaine de la recherche de preuves informatiques.
Ces standards concernent le processus d'analyse, le type de matériel utilisé en laboratoires et les procédures légales à respecter durant toute la phase d'investigation.

3.1.5 « Réseau européen des instituts de police scientifique » (ENFSI):

Crée depuis 1995, il s'agit d'un réseau d'échanges, de coopération et de projets communs entre les laboratoires de police scientifique des Etats membres européens.
En 2003, ce réseau a constitué un groupe de travail qui a publié un guide de bonnes pratiques dans le domaine de l'investigation technique de supports informatiques[15].
Ce document a pour objectif d'exposer les principes de base dans la discipline et de proposer un standard aux experts de la police scientifique dans l'accomplissement de leur mission d'expertise en Informatique.

[15] « Guidelines for the best practice in the forensic examination of digital technology »,

3.2 Guides de bonnes pratiques dans l'analyse de preuve numérique

Un standard est un référentiel, un ensemble de recommandations et recueils de bonnes pratiques qui a pour objectif d'harmoniser les pratiques d'une discipline.
En matière de recherche de preuves numériques, de nombreux textes étrangers servent de guides de bonnes pratiques et de cadres pour les experts au niveau européen et américain.
En France, nous ne disposons toujours pas de documents de référence servant de base à l'ensemble de la profession.

Au Royaume-Uni, le document de référence en matière d'investigations numérique, est le « *Guide de bonnes pratiques pour l'analyse de la preuve numérique* »[16] dont experts et enquêteurs suivent minutieusement les recommandations.
En 2007, ce document a été établi par l'association des chefs de police au Royaume Uni (ACPO), organisme indépendant qui coordonne les services de police d'Angleterre, du Pays de Galles et d'Irlande du Nord.

Bien qu'il n'ait pas un caractère juridique, c'est un document auquel on peut faire référence devant la justice.
Ce texte met l'accent sur la fragilité de la preuve numérique qui peut facilement être altérée par toute manipulation impropre.
Il propose une méthodologie permettant de garantir le respect de l'authenticité de la preuve et met en exergue les principes suivants essentiels à la conduite d'une investigation technique:
"1.Aucune intervention ne devrait altérer la preuve,
2.Toute modification apportée à un support original, doit être faite par une personne compétente qui sera tenue de documenter son action et les conséquences sur la preuve,
3.Une copie du support original devra être réalisée et préservée,
4.L'officier en charge de l'enquête à l'obligation de veiller à l'application de la loi et l'ensemble de ces principes".

Aux Etats-Unis, de nombreux guides ont été publiés par différents organismes notamment les travaux effectués par le « *groupe de travail scientifique sur les*

[16] www.acpo.police.uk

preuves numériques» et surtout un guide de bonnes pratiques en matière de l'expertise en informatique.[17]

3.3 Modèles associés à l'expertise judiciaire en informatique

Depuis plusieurs années, des modèles associés à l'analyse des supports informatiques sont proposés par les spécialistes de la profession dans le but d'harmoniser les pratiques expertales de la discipline[18].

Cela consiste à organiser le processus de la collecte et l'analyse de la preuve numérique en plusieurs phases.

La méthodologie adoptée aura une incidence directe sur les résultats produits. Le choix d'un modèle inapproprié ou l'oubli d'une étape pourrait avoir pour conséquence des résultats d'analyses incomplets et de compromettre la recevabilité de la preuve devant les juridictions.

3.3.1 Les modèles McKemmish et DFRWS

Le premier modèle servant de référence à tous les auteurs est celui proposé par McKemmish qui distingue quatre phases dans le processus de la recherche de preuves informatiques :

- Identification,
- Préservation,
- Analyse,
- Présentation.

En 2001, le groupe de travail DFRWS propose un modèle plus complet constitué de sept étapes intégrant trois nouvelles phases de "collecte", "d'examen" et de "décision".

[17] SWGDE Best practices for Computer Forensics, V3-0- 14-09-2013.
[18] YUSOFF Yunus, Roslan Ismail and Zainuddin Hassan, « *Commun phases of computer forensics investigation models* ».

3.3.2 "*Modèle abstrait de l'investigation numérique (ADFM)*":

En 2002, un nouveau modèle inspiré de celui de DRFWS, intègre les trois phases supplémentaires de « la préparation », « la stratégie d'approche » et la « restitution des preuves »[19].

Ainsi neuf étapes sont identifiées dans le processus d'investigation :

- Identification
- Préparation
- Stratégie d'approche
- Préservation
- Collecte des données
- Examen
- Analyse
- Présentation
- Restitution des preuves

3.3.3 " *Processus d'investigation numérique intégré*" *(IDIP)*

En 2003, le modèle présenté par Brian Carrier et Eugene Spafford[20] avait pour ambition de combiner tous les modèles d'investigation existants en un modèle unique. Le nouveau concept « *d'analyse d'une scène de crime numérique*» est alors introduit faisant référence à un environnement virtuel dans lequel des traces d'un crime informatique ou d'un incident existant sont laissés.

Les auteurs proposent un modèle complexe en cinq catégories :

- « *Phase de préparation* » : vérifier que les enquêteurs et leurs équipements sont prêts,
- « *Phase d'intervention* »: permettre de prendre les mesures adéquates pour intervenir,
- « *Phase d'analyse sur la scène de crime* » : collecter toutes les preuves physiques et les préserver,
- « *Phase d'analyse de la scène de crime numérique*» : Analyser la preuve

[19] Modèle proposé par Mark Reith, Clint Carr et Gregg H. Gunsch.
[20] CARRIER Brian D., Eugene H. Spafford, «*An Event-Based Digital Forensic Investigation Framework* »;

numérique,

- « *Phase de présentation des résultats*» : Présenter les résultats d'analyse et d'examen de la preuve en justice ou à toute autorité saisie.

3.3.4 " *Modèle du processus d'investigation numérique renfonrcé* " (EDIP)

Venansius Baryamureeba et Florence Tushabe soutiennent que le modèle de Brian Carrier manque de précisions et dans la pratique, il ne serait pas facilement utilisable.

En 2004, ils proposent alors un nouveau modèle s'inspirant de celui de Brian Carrier mais ils modifient deux des cinq étapes précédentes:

Ils remplacent la « *Phase d'analyse sur la scène de crime* » par une phase qu'ils qualifient de « *retraçage* » qui consiste à retracer la source d'une attaque.

Pour éviter toute confusion, la catégorie « *Phase d'analyse de la scène de crime numérique* » est également supprimée.

3.3.5 "*Modèle de processus de triage dans le domaine de l'investigation numérique*" (CFFTPM)

Le modèle CFFTPM, présenté lors de la conférence « *Investigation numérique, sécurité et droit* »[21], est fondé sur un processus d'identification et d'analyse immédiate du matériel informatique lors des perquisitions.

Dans certains types de dossiers comme ceux relatifs au terrorisme ou à la pédopornographie pour lesquels il faut rechercher rapidement la preuve, une analyse urgente des supports sur site est alors privilégiée.

Les experts doivent rechercher immédiatement tout élément susceptible d'intéresser l'enquête en cours et l'approche classique d'un examen à postériori n'est plus envisageable.

Le modèle CFFTPM, composé de six étapes intègre ainsi cette notion d'urgence :

[21] Marcus K.Rogers, James Goldman, Rick Mislan, Timothy Wedge, « *Computer Forensics Field Triage Process Model*».

- **Planification :** C'est la phase préliminaire qui permettra à l'expert de définir une stratégie afin de prendre les mesures adéquates pour la recherche de preuves numériques.
- **Triage :** Après avoir préservé l'authenticité de la preuve, il faut classer l'ordre d'importance et de priorité des éléments à traiter. Les informations pertinentes et les données volatiles sont analysées en premier.

  Cette phase préliminaire de triage constitue une étape majeure dans le processus d'investigation.
- **Profil utilisateur :** Il s'agit de chercher un lien entre la personne mise en cause et l'utilisateur du matériel informatique examiné.

  Durant cette phase, les profils utilisateurs, les traces d'activités et accès aux supports informatiques sont identifiés.
- **Chronologie :** Une recherche sur les fichiers en fonction de leurs dates de modification, d'accès ou de création peut également s'avérer utile.
- **Internet :** Il s'agit de rechercher les traces d'information liées aux connexions Internet comme les traces de navigation web, E-mail ou messageries instantanées.

  Eléments de preuves spécifiques à chaque dossier : Les méthodes de recherches varient en fonction de chaque type de dossier et doivent être adaptées en fonction de chaque mission.

Ainsi dans une affaire relative à la pédophilie, les recherches sont davantage portées sur l'examen des fichiers audio, photographiques ou vidéos alors que les investigations en matière de délinquances financières, sont plus centrées sur des documents, fichiers scannés, courriels, etc.

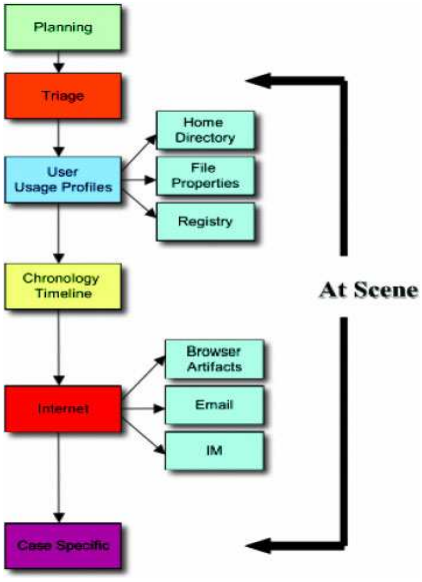


Figure2- Phases CFFTPM – source[22]

3.3.6 Modèle de maturité DF-C²M²

Dans tous les modèles proposés, l'accent est toujours mis sur les différentes phases d'investigations et non sur l'évaluation de la maturité de chaque processus.

Des chercheurs proposent alors un modèle[23] de maturation pouvant servir de référence et destiné à évaluer les pratiques pour atteindre un niveau attendu.

Le modèle DF-C²M², utilisé dans de nombreuses industries notamment dans le domaine du génie logiciel, a été proposé par Awais Rashid et Ebrahim Hamad Al-Hanaei[1], chercheurs à l'université de Lancaster en Angleterre, pour être transposé à la recherche de preuves numériques.

L'objectif principal étant de constituer une structure permettant de développer la performance avec une approche de management de processus.

Un audit de l'infrastructure et identification des améliorations, contribueraient à atteindre le niveau de maturité espéré.

Ce modèle comporte six niveaux de maturité allant de niveau 0 à 5, le niveau 0 constituant le niveau le plus bas qui correspond à l'absence de méthode formelle.

L'activité dépend de l'effort individuel et il n'y a pas de traçabilité.

---

[22] ROGERS Marcus K., James Goldman, Rick Mislan, Timothy Wedge, « *Computer Forensics Field Triage Process Model*», Conference on Digital Forensics, Security and Law, 2006.

[23] DF-C²M² : "*a capability maturity model for digital forensics organizations*"- 2014 IEEE Security and privacy Workshops.

Le niveau 5 montre que l'organisme améliore en permanence son processus de développement et les différents objectifs sont régulièrement atteints.
Il s'agit d'un modèle intéressant qui repose sur des bonnes pratiques mais il ne constitue pas un référentiel unique en la matière et c'est ce qui constitue sa faiblesse.

Chapitre 4 - Techniques d'investigation numérique

L'analyse judiciaire de la preuve informatique a connu un développement majeur au cours de ces dernières années.
Les supports numériques étant très fréquemment utilisés pour commettre des actions criminelles, les magistrats instructeurs sollicitent les spécialistes pour rechercher des informations utiles à la manifestation de la vérité dans le cadre d'une enquête.

Les litiges concernent des domaines très variés et cette recherche de preuves peut viser tous types d'infractions pénales comme le piratage informatique, la délinquance financière, les attaques réseaux avec notamment des problèmes d'intrusions en Entreprise, la pédophilie, les homicides, trafic du stupéfiant, le terrorisme, etc.

La preuve numérique est par nature fragile et le caractère modifiable des données exige le respect d'une procédure rigoureuse pour leur préservation.
Il faut recourir à une méthodologie bien définie garantissant le respect de l'intégrité de la preuve collectée.
Pour réaliser leurs missions d'expertises, les spécialistes devront non seulement maîtriser les techniques traditionnelles de recherches de preuves, ils devront également connaître les nouvelles techniques d'analyses.

4.1 Analyse post-mortem en laboratoire

Lorsqu'un expert prend connaissance d'une mission d'expertise en informatique ordonnée par la justice, il prend possession des scellés, les brise et commence alors les opérations d'expertise.

L'évolution très rapide des technologies informatiques et l'émergence de nouveaux supports, la diversité des systèmes d'exploitation, l'augmentation de la capacité de stockage des supports numériques, l'impossibilité de maîtriser tous les environnements et les technologies d'investigation, constituent autant de facteurs conduisant à la complexification des techniques de recherches sur les supports numériques dans un cadre judiciaire.
A toutes ces causes, il faut également ajouter différentes méthodes de camouflage des données dites « anti-forensic » qui rendent cette tâche encore plus compliquée.

D'où l'importance de la mise en place d'une procédure bien documentée.
Cette traçabilité garantit à la justice le respect d'une méthode de travail rigoureuse et démontre que l'intégrité de la preuve a été préservée et n'a subi aucune altération pendant les différents processus d'expertise.
La notion de «*chain of custody* » qui constitue un principe très important dans la procédure pénale américaine, portant sur les procédures relatives à l'admissibilité de la preuve devant la justice, en est une parfaite illustration.

Plusieurs traductions de cette terminologie sont proposées en français, on parle de « *rapport de garde* », de « *chaîne de traçabilité* » ou encore de « *chaîne de responsabilité* ».
Nous retiendrons la notion de « *traçabilité de la preuve* » qui nous paraît plus adéquate.
Aux Etats-Unis, l'Institut National de la Justice (NIJ), organisme de recherche, du développement et d'évaluation rattaché au ministère de la justice, définit cette notion comme un « *processus utilisé pour maintenir et documenter la traçabilité de la preuve* ».
Il s'agit d'un suivi de tous les éléments recueillis par les enquêteurs jusqu'à leur présentation devant les tribunaux.
Un procès-verbal établi lors de la réception du matériel informatique à des fins d'expertise, décrit de manière détaillée toutes les étapes de la procédure et les opérations réalisées.
C'est une transparence sur les méthodes de travail qui comporte des descriptions très détaillées des personnes, des lieux, des scellés et tout l'historique des opérations d'expertise.

En France, la pratique de l'expertise en informatique n'est pas très encadrée et notre procédure ne prévoit pas cette règle de traçabilité.
Des guides de bonnes pratiques sont mises en places par les Compagnies d'Experts mais aucune réglementation en la matière exige le respect de ces principes.
Chaque expert reste maître de ses pratiques et de sa propre procédure durant tout le processus d'investigation.
Le respect de plusieurs étapes dans chaque procédure d'investigation informatique reste néanmoins primordial :

- Protéger les supports informatiques avec un dispositif de blocage en écriture des données :

Tous les supports informatiques doivent être préservés avec une solution logicielle ou matérielle de blocage en écriture des données du type « Tableau Forensic » ou « FastBloc SE » pour Encase V7.
Cela empêche l'altération du support original et toute éventuelle attaque par un virus ou processus malicieux.
Cette règle connaît des aménagements notamment dans le cadre d'analyse de mémoires volatiles des ordinateurs.

- Procéder à des copies physiques des données :

Afin de préserver l'intégrité des supports originaux, il faut toujours réaliser une copie bit-à-bit (identique à l'original) du support examiné et mener les investigations sur des copies de travail.

- vérifier l'intégrité des données en produisant les algorithmes MD5 et SHA-1

C'est le calcul de l'empreinte numérique ou le HASH. Après la réalisation de la copie bit-à-bit du support numérique, les données recueillies doivent être contrôlées pour établir la conformité des données copiées par rapport aux données d'origine.
Si on fait une analogie entre l'algorithme MD5 et les empreintes digitales, il y a une chance sur soixante quatre milliards, selon Galton ou une chance sur cent billion, billion selon Osterburg, pour que deux individus aient les mêmes empreintes.
Mais il existe une chance sur trois cent quarante et un décillions pour que deux fichiers différents puissent obtenir la même empreinte.

- Analyse et recherche de preuves sur un ordinateur fonctionnant sous Windows :

Le tableau ci-dessous reprend les importantes étapes d'analyses et de recherches. Cette liste n'est pas exhaustive, les recherches sont surtout ciblées par la nature de l'affaire et sont conditionnées par rapport aux informations utiles à l'enquête:

Illustration de différentes phases d'analyses et de recherches un ordinateur fonctionnant sous Windows
Analyse des dates de fichiers (MAC times)/Fuseaux horaires
Identification des systèmes de fichiers (FAT, NTFS, EXFAT...), systèmes d'exploitation, informations relatives au disque dur et sessions d'utilisateurs
Identification des virus et malwares
Analyse de signatures de fichiers
Analyse des « empreintes numériques » (techniques de hachage et comparaison avec une base de signatures)
Analyse du Registre
Analyse des fichiers logs
Recherche de mots de passe
Recherche d'utilisation de logiciels d'effacement/ Stéganographie
Recherche de fichiers, volumes cryptés et cachés (techniques de décryptage : attaque par dictionnaire, force brute…)
Récupération des fichiers effacés sur la totalité des secteurs (espaces non alloués, file slacks », fichiers swap et hibernation), « *Data Carving* »
Récupération de partitions effacées
Recherche par mots clés (recherches avancées GREP)
Recherche cache Internet/ historique
Récupération de courriers électroniques
Analyse des traces de messageries instantanées
Analyses d'informations relatives aux réseaux sociaux
Recherche de fichiers multimédia, programmes spécifiques…
Analyses traces adresses IP
Recherches ciblées en fonction de la nature de l'affaire notamment numéros de carte de crédit.

4.2 Détection d'intrusions et analyse de réseaux

4.2.1 Principe de "*l'échange de Locard*" et son application dans le domaine de l'investigation numérique

L'un des principes fondateurs de la police scientifique est le principe de « *l'échange de Locard* » c'est-à-dire l'étude des traces laissées par un criminel.
En 1919, Edmond Locard, médecin légiste, fondateur du premier laboratoire français de la police technique, expose la notion de transfert sur une scène de crime.

Il considère qu'un malfaiteur laisse toujours des traces de son passage comme des empreintes ou des fibres de vêtements sur les lieux d'une infraction.
De même, il emporte avec lui des traces d'ADN, de fibres ou tout élément constituant la preuve de sa présence sur un lieu du crime.

Ce même principe peut également s'appliquer dans le domaine de l'investigation numérique[24] et plus particulièrement pour permettre d'identifier les attaques informatiques comme une fraude à la carte bancaire ou une usurpation d'identité sur Internet.
Dans ces exemples, même si le pirate n'est pas physiquement présent sur les lieux de l'infraction et opère à distance, les machines sont connectées sur le réseau.
Les informations sont échangées entre elles et des traces de données y sont laissées.
Lorsqu'on intervient sur un système actif, même de façon virtuelle, des modifications y sont immédiatement apportées et des traces de données sont laissées.

4.2.2 Analyse de « Malwares » :

Les intrusions et les attaques concernent des méthodes utilisées par des pirates informatiques[25] pour accéder aux informations d'un système de manière illégale ou de prendre le contrôle d'un appareil à distance.
Ils utilisent des vulnérabilités d'un système ou exploitent une faille de sécurité d'une

[24] « Windows Forensic Analysis », Harlan Carvey, Syngress
[25] « *The Art of Intrusion* », Kevin Mitnick

application pour dérober des informations.
Les Botnets maveillants, Rootkits, injections SQL ou dépassement de tampon constituent les principaux types d'attaque réseaux.
Kevin MITNICK, le hacker informatique le plus célèbre accusé de piratages à plusieurs reprises et poursuivi par la justice, a notamment réussi de pénétrer les réseaux informatiques du Pentagone.

Les experts doivent être familiarisés avec les différentes techniques utilisées par les pirates.
La création d'une table de hachage est une méthode qui permet de faire une comparaison entre les empreintes numériques de certains fichiers afin de détecter la présence des programmes malveillants sur un système compromis et remontrer la piste de l'attaque.

4.3 Nouvelles techniques d'analyse de preuves

Aujourd'hui dans de nombreuses situations, les procédures traditionnelles de l'expertise en informatique qui consistent à débrancher l'alimentation d'un ordinateur et extraire le disque dur avant toute analyse, ne peuvent plus être systématiquement applicables.
Lors d'interventions en Entreprise, le fait d'arrêter les serveurs en fonctionnement, peut avoir des conséquences désastreuses et de paralyser l'activité de toute la structure. Il est quasiment impossible de mettre sous scellés les machines pour procéder à une analyse ultérieure des supports.

De nouvelles approches de recherches et d'investigations sont proposées qui consistent à intervenir sur les appareils directement pour capturer la mémoire à l'aide d'outils adaptés.

4.3.1 Analyse dite « Live Forensic »

La collecte des données volatiles sur les systèmes en fonctionnement, appelé « *Live Forensic* », constitue aujourd'hui une nouvelle approche technique permettant d'analyser les systèmes vivants et de récupérer les données encore présentes dans la mémoire de l'appareil.

Cette technique permet de recueillir les informations qui ne sont pas sauvegardées sur les disques durs et seront définitivement perdues une fois que l'ordinateur est débranché.

Il s'agit de capturer des éléments de preuves éphémères qui tendent à disparaître.

En effet, certaines données ne sont disponibles que pendant le temps où le système est en fonctionnement et seulement pour une durée limitée.

Cela peut concerner de nombreuses informations comme les mots de passes, clés de chiffrement, fichiers ou processus en cours d'utilisation, connexions réseaux actives, clients de messagerie, accès au service de Cloud.

Les logiciels malveillants et les Rootkits laissent également des traces dans la mémoire vive et ne sont pas enregistrés sur les supports magnétiques.

Lors de la mise hors tension de la machine, toutes ces informations peuvent être perdues.

De plus lorsqu'un disque dur, une partition ou un fichier utilise un programme de chiffrement, tant que l'ordinateur est allumé, les informations seront disponibles en texte clair.

Dès l'instant où la machine est arrêtée, la clé du chiffrement sera nécessaire pour déchiffrer le contenu de ces éléments.

La réalisation d'une capture de la mémoire peut ainsi constituer un moyen de preuves essentiel et utile dans le cadre d'une investigation technique.

Cependant, lorsqu'on intervient directement sur un système en fonctionnement, il est impossible de ne pas introduire des données additionnelles et de ne pas laisser de traces. Du fait de leur grande fragilité, les preuves sont souvent être détruites par inadvertance.

Certaines informations sont plus volatiles que d'autres avec une durée de vie limitée, c'est la raison pour laquelle celles-ci doivent être recueillies en premier.

Lors de la collecte de preuves, il est donc important d'adopter une approche

méthodique afin d'identifier l'ordre de volatilité des données pour chaque système.
Généralement, les données sont collectées dans l'ordre suivant :

- Contenu de la mémoire vive (RAM) :

De nombreux utilitaires tels que « MoonSols Windows Memory Toolkit» ou « *Magnet RAM Capture* » permettent de capturer la mémoire vive.

- Connexions réseaux actives :

L'invite de commande réseau netstat –an permet de connaître les connexions TCP et UDP et de lister les ports actifs.
Elle permet de détecter les communications par socket non autorisées ainsi que les programmes malveillants.

- Les processus en cours d'exécution :

Ils pourront fournir des informations sur la présence de programmes suspects notamment à l'aide de l'utilitaire « userdump.exe ».

- Contenu du disque :

Il faut obtenir la liste des fichiers ouverts avec un programme comme « psfile.exe », inclus dans la suite « PsTools ».

Une parfaite méthode de copie consisterait à capturer la mémoire volatile sans passer par le système d'exploitation.
Dans le cas d'un système basé sur Windows, des malware pourraient notamment cibler un fichier bibliothèque[26] couramment utilisé par une application.
Des solutions étaient proposées pour copier le contenu de la mémoire vive en utilisant une carte d'extension matérielle PCI.
Brian Carrier et Joe Grand avaient développé la solution « Tribble »[27], carte PCI qui s'insérait dans un PC avant toutes intrusions. Komoku CoPilot, une autre carte au format PCI permettait également de contrôler le système d'exploitation depuis une unité indépendante à l'abri de toutes modifications.

[26] Notamment le « Trojan.Dropper.UAJ » qui cible le fichier bibliothèque (comres.dll) couramment utilisé par un certain nombre d'applications.

Mais ces solutions ont montré leurs faiblesses dans le passé et ne se sont pas avérées très efficaces.

Le programme Encase dans sa version « Enterprise » permet de capturer et de collecter des données de n'importe quel système à travers le réseau sans interrompre l'activité.
Il permet d'obtenir de nombreuses informations sur les serveurs en faisant une analyse sur le système en fonctionnement.
Il apporte une sécurité durant l'analyse des serveurs en identifiant les utilisateurs, évitant ainsi tout accès non autorisé au système.
De plus, tous les fichiers de preuves bénéficient d'un chiffrement AES-128 octets.
La validité de ce logiciel a été approuvée a de nombreuses reprises par les juridictions américaines.
La décision de référence est celle de la Cour fédérale dans l'affaire « *Positive Software Solutions Inc. v. New Century Mortgage »,* 2003 WL 21000002 (N.D.Tex. 2003).
En l'espèce, le plaignant avait contesté la procédure de la capture d'image des serveurs en fonctionnement laquelle n'a pas été désapprouvé par la Cour de justice.
A travers cette décision, les juges ont implicitement accepté l'utilisation du programme Encase Enterprise et la méthode d'acquisition d'images dite « live forensic ».

4.3.2 Analyse de preuves et émulation de disque dur :

Les techniques d'émulation de disques durs utilisées dans le domaine de l'investigation numérique constituent une approche plus récente d'analyse de preuves. La démarche consiste à recréer virtuellement l'environnement de la machine analysée et à démarrer le système d'exploitation sans y apporter de modifications.

Le recours à cette technologie présente également d'autres intérêts notamment afin d'exécuter des programmes tierces ou de procéder à une détection de virus ou malwares.
Les deux modules « *Virtual File System* » et « *Physical Disk Emulator* » du logiciel Encase® permettent de réaliser cette tâche. Modules payants dans la version six du

[27] « A Hardware based memory acquisition procedure for digital investigations".

programme, ils sont intégrés à celui-ci dans sa version sept.

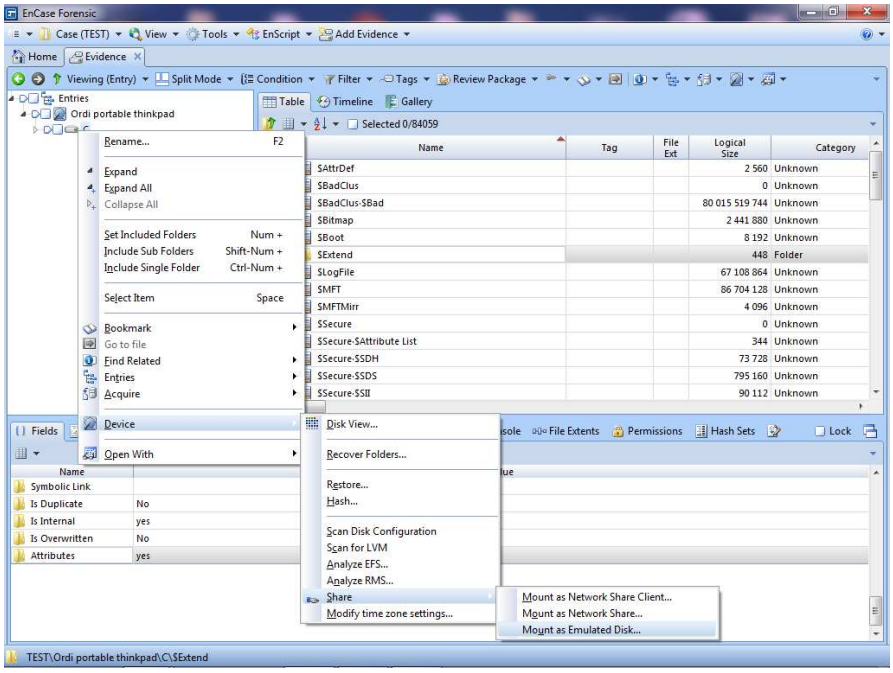


Figure3- Le module « *Physical Disk Emulator* dans Encase® version 7.06

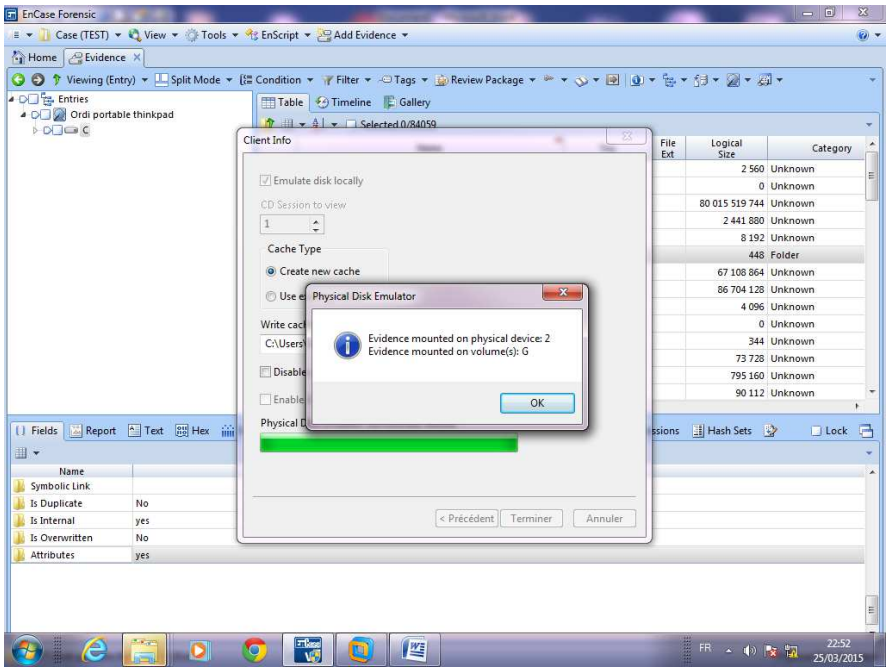


Figure4- Création d'une machine virtuelle à partir de l'image disque - Encase version 7.06

Une utilisation conjointe du logiciel Encase® et le programme VMWARE permet de créer une machine virtuelle à partir de l'image du disque.

A la différence du module d'émulateur de disque, celui du « VFS » permet d'accéder aux fichiers effacés et aux espaces non-alloués du disque dur à l'extérieur du logiciel Encase. Le support numérique est représenté en partage réseau dans l'explorateur Windows.

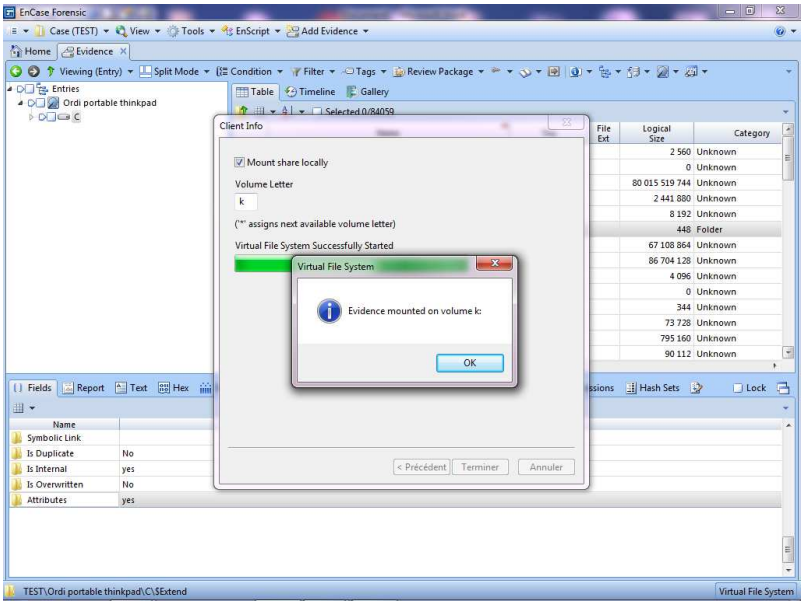


Figure5- Le module « *Virtual File System* » dans Encase version 7.06

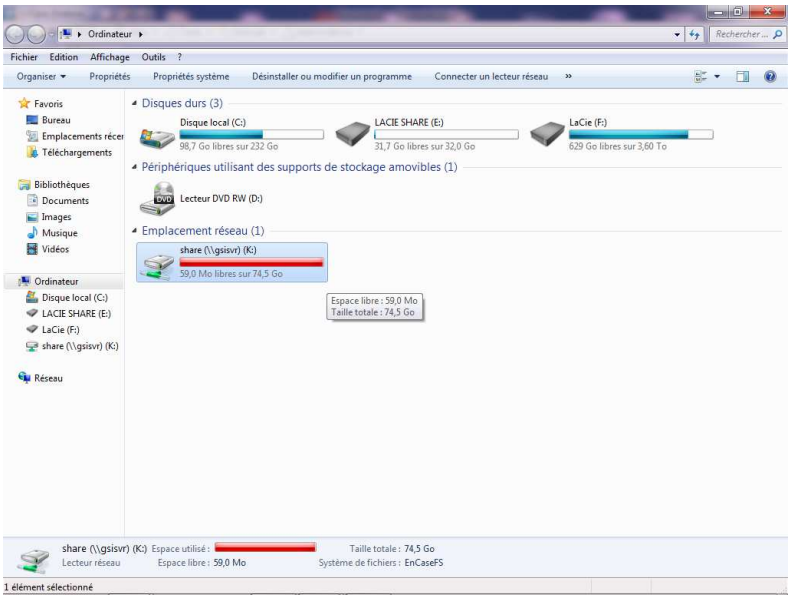


Figure6- Disque dur présenté en partage réseau dans l'explorateur Windows

4.3.3 Examen des machines virtuelles :

L'un des défis en matière d'expertise concerne la problématique de la recherche et de l'analyse des traces laissées lors de l'utilisation de machines virtuelles.

La virtualisation permet de faire cohabiter plusieurs systèmes sur la même machine d'accueil en utilisant les ressources de l'hôte.

A titre d'exemple, le logiciel VMware, sauvegarde les fichiers avec des extensions comme « vmdk », « vmsd », « nvram »...

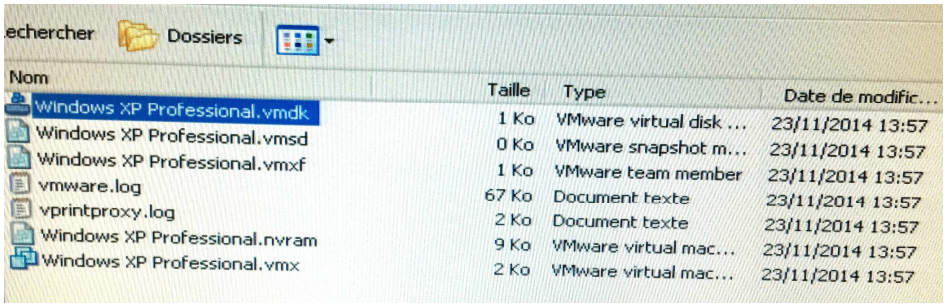


Figure7- Aperçu des fichiers sauvegardés par le logiciel VMware sur Windows

L'ensemble des techniques utilisées pour l'analyse de disques durs ne peut être appliqué à l'expertise des machines virtuelles.

Du fait de l'utilisation des disques virtuels, la collecte des données doit intervenir sur le système en fonctionnement.

Cette méthode consisterait à réaliser un instantané de la machine virtuelle pour la sauvegarder à un moment précis.

Le logiciel Encase permet notamment d'utiliser cette technique dans le cadre de l'analyse de la preuve informatique.

Il est ainsi possible de procéder à la conversion des fichiers portant l'extension « *VMDK* » au format dd.

4.4 Complexité liée au « Cloud Computing »

Le terme « *Cloud Computing* » ou « *l'Informatique en nuages* », vise une externalisation de l'infrastructure informatique.

Le service de l'informatique en nuage permet de stocker et d'accéder aux données sur des serveurs distants pour créer des services accessibles en ligne.

L'analyse du « *Cloud* » représente un défi technique et juridique pour les experts.
La difficulté majeure dans le processus d'investigation réside dans le fait que les enquêteurs n'ont pas le contrôle physique des médias ni du réseau sur lequel il transite.

De plus, les règles de territorialité rendent les perquisitions plus compliquées notamment lorsque les données sont stockées dans un pays tiers.
Seules les données disponibles sur le territoire national peuvent être perquisitionnées.

Des questions juridiques relatives à l'application de la loi applicable ou le respect des règles de la vie privée sont alors soulevées.

L'« *Institut National des Normes et de la Technologie*» a constitué un groupe de travail et a publié un document en juin 2014 mettant en évidence les différents défis posés par l'investigation de l'informatique en nuage[28].

[28] « *Nist Cloud Computing Forensic Science Challenges* », june 2014, Draft NISTIR 8006

Deuxième partie: ETAT DE L'ART SUR LES TECHNOLOGIES D'INVESTIGATION NUMERIQUE

Chapitre 1 - Introduction

Le droit et la science relèvent de deux disciplines bien différentes mais sont souvent complémentaires.
Depuis plusieurs siècles, la science en matière de la preuve occupe une place prépondérante dans le déroulement du procès.

L'expertise scientifique peut apporter des réponses là où le droit reste impuissant.
Le juge a recours à l'expert pour l'éclairer sur des questions d'ordre techniques et minimiser les incertitudes.

C'est l'émergence de la notion de la vérité « *technique* » apportée par l'expert dont l'avis est dans la majorité des cas suivi par le juge.

Le technicien a l'obligation de respecter les règles déontologiques et devra répondre aux exigences d'impartialité, d'indépendance intellectuelle et de clarté d' analyse.

C'est la jurisprudence américaine[29] qui a posé les critères de recevabilité de la preuve scientifique devant les juridictions.

[29] « *L'expert scientifique et les critères : Regards sur le droit Américain et sa philosophie des sciences implicite* »., Mathias Girel

Chapitre 2 - Méthode scientifique et validation des outils d'analyses informatiques

Les jurisprudences « *FRYE* » et « *DAUBERT* » ont constitué une étape importante dans la définition de la preuve scientifique et son admissibilité devant la justice pénale américaine.
Le champ d'application de ces deux décisions a également été étendu au domaine de la recherche de preuve numérique.

2.1 Admissibilité de la preuve et processus scientifique devant la justice américaine

2.1.1 L'arrêt « Frye v United States »[30]

Au dix-neuvième siècle, la nomination d'un expert par le juge était seulement fondée sur la réussite professionnelle du spécialiste dans l'exercice de sa fonction.
A cette époque, le choix de l'expert était laissé à l'appréciation discrétionnaire du juge.
De même, le magistrat jugeait arbitrairement de la qualité de l'expertise produite et il suffisait qu'il considère que l'expert était compétent pour que le moyen de preuve utilisé dans le cadre de l'expertise devienne recevable devant les tribunaux.

En 1923, l'arrêt FRYE marque un tournant important en posant le critère de « *l'acceptation générale* ».
L'admissibilité de la preuve scientifique devant les juridictions est désormais basée sur une opinion généralement admise.
En l'espèce, un expert a tenté d'établir, dans une affaire criminelle, que le prévenu accusé du meurtre d'un médecin n'avait pas menti.
Pour étayer son analyse, il a utilisé un instrument mesurant la tension artérielle pendant l'interrogatoire.
Mais son expertise a été déclarée irrecevable car l'appareil de détecteur de mensonge

n'a pas été retenu comme moyen de preuve par le tribunal.
L'appareil de mesure de tension artérielle ne correspondait pas au savoir généralement partagé par la communauté scientifique.
Ainsi, le témoignage de l'expert ne devient recevable que s'il s'appuie sur des études techniques reconnues par les spécialistes de la discipline.

2.1.2 « Les règles fédérales en matière de preuves (FRE) »

En 1975, l'exigence par les tribunaux du critère de « *l'acceptation générale* » disparaît avec la codification des règles de preuves Il s'agit des règles de recevabilité de l'expertise scientifique devant les tribunaux fédéraux américains dont l'une des règles importantes, est relative au témoignage des experts.
L'article 702 des règles fédérales en matière de preuve dispose que « *si la connaissance scientifique, technique ou toute autre connaissance spécialisée aide le jury à la compréhension de preuves ou pour déterminer un fait litigieux, un témoin qualifié d'expert de par ses connaissances, sa compétence, son expérience et sa formation peut témoigner en émettant une opinion ou sous une autre forme[…]*».
Selon cet article, lorsqu'un spécialiste est désigné comme « *expert* » par la justice, il doit pouvoir justifier ses connaissances et qualifications professionnelles en rapport avec son domaine d'expertise.
Mais les choses évoluent en 1993 et de nouveaux critères de recevabilité de preuves sont posés.

2.1.3 "Le Standard DAUBERT"[31]

La célèbre décision de la Cour Suprême des Etats-Unis, "*Daubert v. Merrell Dow Pharmaceuticals, Inc. (509 U.S. 579 (28 juin 1993)"* a posé les jalons de la jurisprudence actuelle en matière de la preuve scientifique.
Avec cette décision, le juge a défini quatre conditions d'admissibilité d'une expertise scientifique devant les tribunaux.

---

[30] « FRYE v, United States », 293F, 1013 (D,C, Cir 1923),
[31] « La recherche de la vérité par le savoir scientifique », Annarita M. Busbee,

Pour évaluer la fiabilité du témoignage d'un expert, le juge devra ainsi vérifier que:

1. la méthode avancée a été expérimentée,
2. les travaux sont évalués par les pairs et ont fait l'objet de publications,
3. le taux d'erreurs et la marge d'incertitude de la méthode sont faibles,
4. la théorie est acceptée par la communauté scientifique et fait l'objet d'un consensus.

En l'espèce, la cour suprême devait se prononcer sur une expertise relative à la toxicité d'un produit pharmaceutique et son lien avec une anomalie congénitale.
Les parents d'un enfant ont saisi la justice pour faire établir un lien de causalité entre le médicament "Bendectin", consommé pendant la grossesse de la mère et la malformation de son enfant à la naissance.

Depuis cette jurisprudence, les connaissances scientifiques d'un expert nommé dans un cadre judiciaire, sont appréciées au regard des quatre critères posés par le « *test DAUBERT* ».

En 1999, la Cour Suprême était de nouveau saisie pour déterminer si la jurisprudence "*DAUBERT*" pouvait également s'appliquer aux avis d'autres experts techniques. Dans l'arrêt « *Kumho Tire Co. v. Carmichael* », la Cour Suprême a étendu l'application des critères définis par la décision "DAUBERT" aux témoins experts non-scientifiques.
En l'espèce, un ingénieur expert avait démontré qu'un pneu défectueux a été à l'origine d'un accident de la route.
Les juridictions de première et deuxième instances n'avaient pas retenu l'avis de l'expert en soutenant que le « test DAUBERT » ne s'appliquait pas à un domaine non-scientifique. La décision de la Cour d'Appel a été rejetée par la Cour Suprême.

Les critères de la jurisprudence "DAUBERT" sont également exigés des experts dans le cadre de la recherche de preuves numériques.
Dans le domaine de l'expertise judiciaire en Informatique, les experts recourent aux différents logiciels et matériels spécialisés pour collecter la preuve avant de la produire en justice.

Pour apprécier la validité d'une telle preuve, la justice américaine exige que les critères de la jurisprudence "DUBERT" soient réunis.

Prenons l'exemple du programme « Encase® » de la société Guidance Software, leader international dans le domaine d'investigation numérique.
Avec trente cinq mille licences vendues, il est le logiciel le plus utilisé à travers le monde.
La justice américaine a eu l'occasion de statuer, à plusieurs reprises, sur la recevabilité du programme Encase®.
Elle a estimé que ce logiciel rencontre bien tous les critères exigés par la jurisprudence "DAUBERT" et les preuves collectées par le programme sont admissibles devant les tribunaux.
Afin de démontrer que les conditions d'admissibilité sont bien remplies, la société éditrice du logiciel a invoqué les éléments suivants qui ont été approuvés par les juges américains :

- Le logiciel Encase® est accessible au public et peut facilement être testé par ses utilisateurs, ce qui n'est pas le cas des outils fonctionnant en lignes de commandes lesquels ne sont pas connus de tous et ne peuvent être testés que par ceux qui sont familiers avec ces processus.

- De nombreux articles publiés par les spécialistes de la sécurité de l'information et l'investigation numérique donnent un retour d'expérience favorable à l'utilisation du programme Encase®.
  Cette disposition renforce le critère « *de travaux évalués par les pairs* » défini par la jurisprudence DAUBERT.

- Tous les logiciels connaissent des bogues mais les différents tests et l'utilisation extensive du programme Encase® révèlent que, contrairement à d'autres logiciels d'expertise judiciaire en Informatique, celui-ci ne contient pas un taux d'erreurs élevé (Affaire Rodriguez).

- La société Guidance software forme plus de cinq mille personnes par an et plus de trente mille utilisateurs sont titulaires de la licence du logiciel Encase®. Le critère de « *l'opinion généralement acceptée* » exigé par la jurisprudence FRYE /DAUBERT est donc satisfait.

L'adoption généralisée du logiciel Encase® par la communauté des experts et l'usage étendu du programme constituent ainsi des facteurs importants de son authenticité.

2.2 Les outils d'investigation de nouvelles générations

2.2.1 Panorama des technologies d'investigations

La démocratisation des ordinateurs personnels dans les années 1980 a été accompagnée par la nécessité d'utiliser des technologies nouvelles pour combattre la criminalité informatique.
A l'époque, il n'existait pas d'outils spécialisés pour la recherche de preuves.
Les méthodes d'investigation étaient assez basiques et des programmes comme la suite « Norton », « PC Tools » ou « Mace Utilities» étaient utilisés.
Les premières analyses de preuves sur les ordinateurs se faisaient également sans recours à un dispositif de blocage en écriture.
Une copie logique du support original était réalisée et l'exploitation se faisait manuellement à l'aide de gestionnaires de fichiers sous DOS comme les programmes "XTree Gold" et "Norton Commander".
Or, s'agissant seulement de copies logiques, les recherches excluaient la récupération des données au niveau des fichiers effacés, des espaces non-alloués ou des « file slacks» du support examiné.

C'est la raison pour laquelle les experts privilégiaient d'examiner directement les supports originaux plutôt que de travailler sur des copies partielles. C'est également l'époque de l'apparition des premiers dispositifs de blocage en écriture.
Ce n'est qu'à la fin des années 1980 que les méthodes d'analyse ont changé en permettant la réalisation des copies intégrales de supports originaux.

Le premier logiciel d'expertise « IMDUMP » a été crée en 1989 par Michael WHITE[32].
Le programme « SafeBack » connu comme référence en tant que logiciel de copie d'images physiques est sorti l'année suivante.
D'autres utilitaires d'analyse de disquettes comme « Anadisk », « Teledisk » et « CopyQM » ont également été distribués.

Depuis cette période, beaucoup de recherches ont été menées et de nombreux outils ont été développés à travers le monde.
Aujourd'hui, l'émergence des technologies nouvelles et l'utilisation massive de Smartphones, ordinateurs ou tablettes créé le besoin de recourir à des outils sophistiqués capables d'extraire et de récupérer de plus en plus de données et preuves numériques.

Depuis ces dernières années, de nombreux logiciels de nouvelle génération ont fait leur apparition et proposent une multitude de fonctionnalités pour l'analyse des supports numériques.

Aujourd'hui, ces technologies d'investigations sont classées en plusieurs catégories :

- Bloqueurs en écriture (logicielles et matérielles),
- Duplicateurs de copies bit-à-bit pour disques durs et supports amovibles (logiciels et matériels),
- Outils d'analyse de preuves multi-supports (Encase® Forensic, FTK®…),
- Logiciels de cassage et récupération de mots de passe,
- Recherche de traces sur internet (Netanalysis), Analyse et récupération de courriels et archives de messagerie (IEF),
- Outils d'analyse de téléphones portables, tablettes, GPS…(UFED, MPE+, XRY…),
- Logiciel d'analyse réseaux (Encase® Enterprise, AD Enterprise, …),
- Outils de collectes des données volatiles (Encase® portable),

[32] « Computer and intrusion forensics »

Les logiciels propriétaires représentent un investissement financier important.
Ainsi, une licence de logiciel coûte en moyenne trois mille euros auxquels s'ajoutent les frais de renouvellement annuel, estimés à environ mille euros chaque année.
Par leur complexité, la majorité de ces programmes nécessitent également le suivi des formations techniques très onéreuses.
Certains experts se retournent alors vers des logiciels à code source libres fonctionnant sous Linux qui ne sont pas toujours à la pointe de la technologie.

2.2.2 Principaux logiciels à code source libre

A l'opposé des logiciels de licence propriétaires, les logiciels libres dits « Open Sources » permettent aux utilisateurs d'accéder au code source du programme. La liste suivante recense les logiciels plus couramment utilisés par les spécialistes:

- **The Sleuthkit Kit (TSK):** Il s'agit d'une version modifiée de Coroner's Toolkit lequel ne gérait pas les systèmes NTFS, FAT ou EXT3. [33]
  C'est un ensemble d'outils open source développé par Brian CARRIER fonctionnant en ligne de commande Unix.
  "Sleuth Kit" contient un ensemble d'outils fonctionnant en ligne de commande sous Linux permettant d'examiner différents systèmes de fichiers NTFS, FAT, EXT2/3, HFS, etc.
  L'outil "Autopsy" utilisé en complément constitue l'interface graphique Web de SleuthKit.
- **HELIX 3 Pro**: Outil développé par la société e-fence, il regroupe plusieurs logiciels spécialisés dans le domaine d'expertise en Informatique.
- **DFF (Digital Forensic Framework),** logiciel open source français, multiplateforme développé par la société Arxsys[34], écrit en langages Python et C++. Il combine une interface utilisateur avec une architecture modulaire et multiplateforme pour linux et Windows.

[33] Développé par Dan Farmer et Wietse Venema, analyse d'une machine compromise du système Unix.

La problématique identifiée par l'utilisation de ces logiciels dans un carde judiciaire concerne principalement la question de l'admissibilité de la preuve devant les tribunaux et l'application des critères énoncés par la jurisprudence américaine "DAUBERT".

Aux Etats-Unis, ce sont les logiciels commerciaux qui sont surtout reconnus devant les juridictions.

Les experts qui ont recours à l'ensemble des outils open source dans le cadre leurs analyses s'interrogent alors sur leur recevabilité devant les tribunaux.

Brian Carrier, un des spécialistes prônant le recours aux logiciels « open source», met en évidence dans un article[35] qu'un logiciel libre peut également satisfaire les conditions définies par le « *standard DAUBERT* ».

Or, la démonstration de la fiabilité et de la reconnaissance de ces outils doivent se manifester à travers différentes publications dans les revues spécialisées et des tests de validation organisés par des organismes officiels.

2.2.3 Principaux outils de licences propriétaires

Aujourd'hui, de nombreux outils proposent d'analyser et de rechercher la preuve sur les supports informatiques.
Parmi les programmes le plus couramment utilisés peuvent être cités « X-Ways Forensics » ou les logiciels complémentaires aux outils d'investigation comme « Internet Evidence Finder® » (IEF) et « Belkasoft Evidence Center Ultimate ».

Mais deux logiciels constituent la référence à travers le monde.
Le programme « Encase® » de la société Guidance Software et le logiciel « FTK® » (Forensic Toolkit®) sont les outils le plus largement utilisés par la communauté de l'investigation numérique.

---

[34] Il a remporté le prix de l'innovation des assises de la sécurité 2010, décerné pour la première fois à un logiciel libre.
[35] « Open source digital ForensicsTools », Brian Carrier,

- EnCase® Forenisc

Le programme EnCase® Forenisc, a été originairement développé sur les spécifications des Services de Police américains.

L'ancêtre du logiciel Encase® est le programme « *Expert Witness»,* première plateforme d'analyse et de recherches de preuves pour Macintosh qui a été conçu par la société ASR DATA en 1992.[36]

En 1997, Guidance Software a développé Encase® et l'a commercialisé sous le nom « *Expert Witness for windows».*

Jusqu'en 1998, cette première version du programme fonctionnait sur Windows 95/NT[37].

A la suite d'une procédure d'arbitrage entre les deux sociétés en 1999, la société Guidance Software a abandonné le programme « *Expert Witness for windows »* et l'a remplacé par Encase®.

Aujourd'hui, le logiciel Encase® propose une gamme de produits destinée aux différents domaines de la cyber-sécurité, l'E-discovery, l'Entreprise, l'investigation numérique et la récupération des données sur le réseau.

La version six du programme Encase® Forensic qui disponible depuis 2007 est encore utilisée par les experts.

Le logiciel propose de nombreuses fonctionnalités de recherches et d'analyses de données et a souvent été critiqué pour la complexité de sa plateforme.

Le langage du script intégré au programme permet de rajouter des modules complémentaires personnalisables.

Il utilise les langages Java et C++ qui requièrent une connaissance de la programmation.

Une bonne compréhension de l'ensemble de ces fonctionnalités nécessite également des formations de prises en mains du logiciel.

[36] « Computer Evidence, Collection and Preservation », page 230.
[37] « Auditing information systems », page 274

Depuis 2011, la commercialisation de la version sept a complètement remodelé le programme et son interface utilisateur qui propose de nouvelles fonctionnalités.

Contrairement au programme Encase®, le logiciel FTK est présenté comme un outil intuitif et plus facile d'utilisation par rapport à son concurrent.

- Forensic Toolkit® (FTK)

A l'instar du logiciel Encase®, le programme FTK®, représente un standard en matière d'analyses de preuves numériques.
C'est un outil d'investigation global qui permet de réaliser une analyse complète sur un support informatique.
Il dispose notamment des modules de récupérations de mots de passe et déchiffrement de fichiers cryptés.
En cas de bogues au niveau de l'interface du programme, les recherches pourront continuer et le travail d'analyse ne sera pas perdu.

2. 3 Limitation des outils d'expertise en informatique

3.2.1 Techniques de camouflage dites « Anti-forensic »

Les différentes techniques dites « *anti-forensics* » visent les méthodes qui permettent de camoufler, détruire ou modifier les traces laissées sur les supports numériques.

L'ensemble de ces procédés a pour objectif d'entraver la recherche des moyens de preuves informatiques.

Selon les auteurs Liu et Brown quatre raisons principales incitent les personnes à recourir à ce genre de techniques : [38] Ainsi, ces actions sont perpétrées dans le but de supprimer certaines traces sur les supports, d'empêcher la collecte d'informations, d'augmenter la charge de travail des experts ou encore de jeter le discrédit sur la valeur probante d'un rapport d'expertise.

[38]"Bleeding-Edge Anti-Forensics", Liu and Brown (2006).

Ces méthodes sont également être utiles pour les experts à les sensibiliser sur les différentes possibilités techniques en mettant en exergue les limites des outils d'analyses de preuves informatiques.
En effet, lors des conférences internationales comme le « Black Hat » les spécialistes de la sécurité informatique ont pu démontrer que les technologies d'investigations peuvent représenter des failles et d'être dupées par différentes méthodes comme l'altération des dates de fichiers ou la modifications des signatures numériques.

L'exploitation des vulnérabilités de certains outils d'analyse de preuves numériques telles que les versions antérieures du logiciel Encase® (versions 6.2 et 6.5) ont notamment été mises en évidence dans le passé.
Avant de procéder à une recherche de preuves sur un support informatique, il faut toujours envisager la possibilité le mis en cause ait pu recourir à l'une des techniques de camouflages comme le Chiffrement des volumes ou fichiers, la Stéganographie, la présence de Rootkits ou l'effacement définitif des données.

3.2.2 Prototype DELV (Environnement numérique pour une investigation à grande échelle)

Les évolutions technologiques et l'augmentation de la capacité des supports informatiques font apparaître les limites des outils d'investigation numériques.
Aujourd'hui, les disques durs examinés disposent en moyenne d'une capacité de stockage de 1To, les recherches et la récupération de données deviennent de plus en plus longues sur ces supports.
Les bogues et les erreurs logicielles sont également des facteurs qui rendent le travail d'investigation plus compliqué.
A titre d'exemple, le logiciel Encase® dans sa version 6 rencontre souvent des bogues en présence de gros volumes de fichiers décompressés comme les fichiers au format "PST".
Il en est de même lorsque les archives de messageries au format "DBX" sont exportées, leur nom d'origine est modifié par le logiciel.
Les nouvelles mises à jour corrigent souvent les bogues logicielles mais les problèmes rencontrés ne peuvent pas toujours être solutionnés dans l'immédiat.

En 2004, Roussev et Richard[39] avaient fait la démonstration du prototype "DELV" et son potentiel en utilisant un petit cluster Beowulf avec huit nœuds, un serveur de fichiers et un système de commandes reliés par un réseau Ethernet de grande vitesse.

A l'époque, ses performances étaient comparées à celles du logiciel FTK®.
Des recherches par mots clés étaient lancées et, à chaque reprise, DELV apparaissait beaucoup plus rapide que FTK®.
Ces résultats montraient que même une configuration de petite taille permettrait d'atteindre des performances supérieures par rapport à celles qui étaient attendues.

2. 4 Utilisation du langage XML dans le domaine d'expertise judiciaire

2.4.1 Le prototype XIRAF et la technologie XML

Le prototype XIRAF a été présenté lors du groupe de travail DRFWS réuni en 2006.
Les auteurs[40] ont décrit une nouvelle approche d'analyses de supports informatiques ayant recours au schéma XML, conçu pour faciliter l'échange et la standardisation des données dans la recherche de preuves numériques.

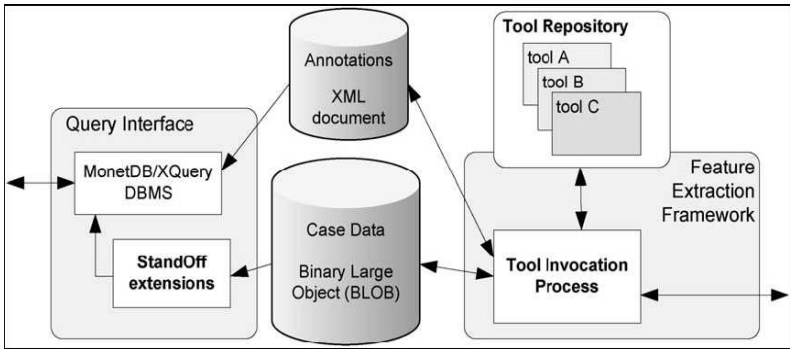
Le modèle basé sur la norme XML était utilisé pour l'indexation et la recherche d'informations durant le processus d'investigation.
La diversité des outils d'analyse de preuves numériques avait introduit le problème de formats utilisés par ces logiciels.
Il n'y avait pas d'interopérabilité entre les outils et les différents formats, la plupart d'entre eux utilisait un format spécifique.

L'objectif était de mettre en place une méthode uniforme de langage de recherches qui serait compatible avec les outils d'analyses de preuves numériques.

[39]Roussev & Richard,"*Breaking the Performance Wall: The Case for Distributed Digital Forensics*."

L'interface de recherche XIRAF permettait de combiner les outils d'investigation pour convertir et générer des résultats au format XML.
Après l'indexation dans une base de données, il permettait de lancer des requêtes et de générer des résultats en XML.

Interface de recherche



Interface de sortie

Figure 8- Architecture XIRAF- source[41]

Les auteurs mettaient l'accent sur la séparation des deux phases d'extraction et d'analyse des informations collectées.
Ils soulignaient également l'importance de générer un format de fichier standard XML pour tous les outils d'investigation.

3.4.2 DEX (Digital Evidence Exchange)

Lors du groupe de travail DRFWS en 2009, Brian Neil Levine et Marc Liberatore ont introduit un format de preuve numérique indépendant qui permettrait aux experts d'échanger et de comparer leurs résultats de recherches indépendamment de l'outil d'analyse de preuve utilisé.
Les versions étaient exécutées en parallèles avec des entrées identiques et les sorties étaient comparées entre elles.

---

[40] Présenté par Alink, Bhoedjang, Boncz et de Vries
[41] « XIRAF -*XML-based indexing and querying for digital Forensics* », 2006

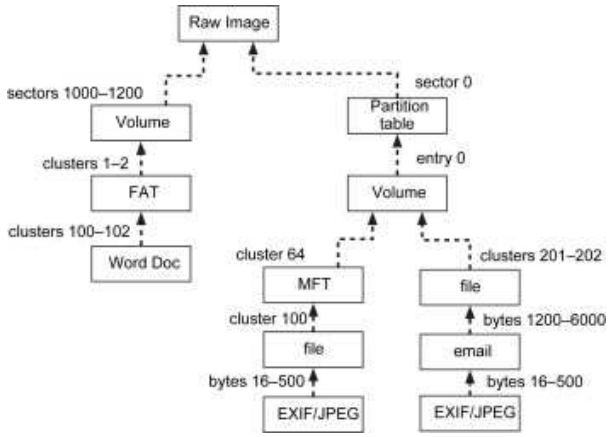


Figure9- Diagramme de la description DEX de la preuve numérique- source[42]

Cette technique permettait de détecter les erreurs ou de faire valider un outil.
Une comparaison entre les programmes constituant un moyen de garantir leur fiabilité.

3.4.3 DFXML « investigation numérique XML »

Les précédents efforts visant à développer un format unique pour les outils d'investigation n'ayant pas abouti le format DFXML a alors été présenté par Simon Garfinkel.

Il a été conçu pour apporter les éléments suivants :

- Métadonnées avec des informations sur le support original,
- Informations détaillées sur le logiciel d'expertise utilisé,
- Données concernant l'ordinateur sur lequel le programme a été lancé,
- Détails relatives aux informations extraites des supports examinés,
- Valeur de hachage de la séquence d'octets,
- Informations relatives au système d'exploitation.

Basé sur le langage XML, le format DFXML offrait un partage structuré d'informations pour améliorer l'interopérabilité entre différents outils.

Dans le cadre d'échanges d'informations sur un même dossier, il était plus pratique de partager des fichiers au format XML plutôt que d'échanger des images physiques des disques.
Des programmes comme « Photorec » et « md5deep » étaient modifiés pour être compatibles avec fichiers DFXML.

[42] « *DEX: Digital evidence provenance supporting reproducibility and comparison* »

Chapitre 3 - Principales fonctionnalités des technologies d'analyse de preuves informatiques

3.1 Acquisition physique des données

Les duplicateurs de supports informatiques permettent de réaliser une copie exacte des supports de stockages afin d'éviter tout risque d'altération ou d'erreurs de manipulation des données.
Cette fonctionnalité de copie physique ou logique du support examiné est également prévue par les outils muti-suppports d'analyses de preuves numériques.
La réalisation d'une image physique permet de copier la totalité du contenu d'un support, secteur par secteur, sur un autre support cible tandis qu'une copie logique permet seulement de copier les informations présentes sur les support de stockage.
Les fichiers effacés et les espaces non alloués seront ainsi exclus de la copie.

3.1.1 Copie physique de disques durs

Avant de rechercher et d'analyser la preuve informatique, un certain nombre de règles de bonnes pratiques doivent être observée parmi lesquelles figurent la copie bit-à-bit du support original et l'utilisation d'un dispositif de blocage en écriture.
Un système de protection en écriture logiciel ou matériel permet de préserver les données et garantir leur intégrité.
Aujourd'hui, des solutions complètes de blocage en écritures existent sur le marché de l'investigation numérique.
Des protections matérielles du type « Tableau Forensic» ou logicielles comme le « FastBloc », directement intégré dans la version sept du logiciel Encase® Forensic, sont largement utilisées par les professionnels de l'investigation.
Par ailleurs, si le support original est copié sur un autre support identique, celui-ci doit être « stérilisé ».
Dans l'hypothèse de la copie physique d'un disque dur original sur un second disque dur, l'utilisation d'un support neuf est fortement préconisée.

Afin d'éviter la présence accidentelle des données antérieures, il est recommandé de procéder au préalable à un effacement permanent du support.
Plusieurs normes d'effacements et de réecritures des données informatiques sont prévues au niveau international.
De nombreuses d'interrogations subsistent sur le type d'outils et le nombre de passages nécessaires pour garantir un effacement complet des sonnées.
En 1996 Peter Gutmann, chercheur à l'université d'Auckland, a publié une étude suggérant une méthode de réécriture jusqu'à trente-cinq passages sur les secteurs d'un disque dur.
Parmi différentes normes d'effacement permanent d'un support informatique, la norme DoD 5220.22-M est celle recommandée par le Département de la Défense Américain prévoyant trois cycles de réecritures des données[43].

3.1.1.1 Copies physiques sous MS-DOS :

Il arrive encore que dans certaines situations, les copies physiques soient réalisées dans l'environnement MS-DOS.
Cela consiste à créer une disquette de démarrage « in*forensique* » comme « *Encase*® *pour DOS* » et à redémarrer l'ordinateur pour cloner un disque dur source vers un autre disque dur cible sans apporter de modifications au support original.
La réalisation d'une copie sous DOS nécessite une bonne connaissance du processus de démarrage du système d'exploitation pour empêcher de manipuler par inadvertance le support original.

Cette technique est notamment efficace pour détecter les zones cachées « HPA » et « DCO » sur un disque dur.
Un autre cas de figure consiste à retirer le disque dur original de l'ordinateur et le connecter à la machine de l'expert pour faire une copie sur un disque dur cible.
Cette méthode classique a longtemps été utilisée pour éviter de redémarrer directement sur la machine saisie.
Aujourd'hui, d'autres méthodes d'acquisitions plus adaptées aux technologies actuelles, sont proposées par les outils d'analyse de preuves numériques.

3.1.1.2 Copie avec la mise en réseau de deux ordinateurs :

Une autre technique consiste à connecter deux ordinateurs à l'aide d'un câble Ethernet croisé à travers le réseau et à réaliser une copie bit-à-bit du support de stockage avec une distribution linux tel que "LinEn" pour Encase®.
Les machines communiqueront entre elles par une adresse IP qui leur sera attribuée.
Cette méthode peut notamment être utilisée dans le cas de copies de disques assemblés selon la technologie RAID.

3.1.1.3 Copie du disque dur en mode maître/esclave :

Cette procédure consiste à retirer le disque dur original d'un ordinateur pour le placer dans une machine destinée aux investigations en déterminant le mode d'accès aux disques par le BIOS en maître ou en esclave.
Généralement, ce type de copies était réalisé dans l'environnement MS-DOS mais aujourd'hui avec l'évolution constante de la capacité de stockage des disques durs, cette méthode s'avère très lente.
Les praticiens recommandent plutôt l'utilisation d'un CD-ROM de démarrage sous Linux.
Cette technique comporte tout de même ses faiblesses avec un risque de confusion entre les deux supports de stockage.
C'est la raison pour laquelle il est important de bien différencier le disque original de celui qui sert de copie.

Une dernière méthode consiste à retirer le disque dur original et le connecter à la machine de l'expert à l'aide d'un dispositif de blocage en écriture qui s'intercale entre l'ordinateur et le support examiné.
Cette démarche permettra de préserver l'intégrité des données et de réaliser une duplication sur un support de même taille ou de capacité supérieure.

[43] «Computer Forensics Jumpstarts», 2011

3.1.2 Différents formats d'acquisition d'images

Pour créer une copie exacte d'un support informatique, les logiciels d'analyses de preuves numériques utilisent différents formats de fichiers .

Les copies physiques des données étaient généralement réalisées au format RAW (image DD), compatible avec la plupart des outils d'investigation.
L'inconvénients de ce type de format était principalement lié à la taille des fichiers non compressés et au fait qu'ils ne contenaient aucune métadonnée ou d'informations relatives à la copie.
Afin de pallier à ces carences, les spécialistes ont préféré de privilégier l'utilisation d'un « *fichier image*».

En 2006, Simon Garfinkel présente un fichier conteneur au format AFF (format avancé d'analyse numérique), format de fichier Open Source constituant ainsi une alternative aux formats propriétaires de copies d'images.

Le format le plus populaire étant celui du logiciel ENCASE® qui est reconnu par la plupart des technologies d'investigations comme FTK®, X-Ways Forensic ou SMART.

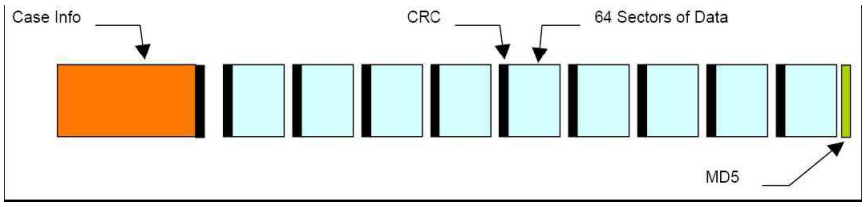


Figure10. Format Encase « E01»- source[44]

Il est basé sur le format initialement utilisé par le programme « Expert Witness » de la société ASR Data.
Dans la version six et les versions antérieures du logiciel Encase®, les copies sont réalisées aux formats E01/L01 (Encase® six et versions antérieures).
Les nouveaux formats de fichiers Ex01/Lx01 sont activés par défaut dans la version sept du programme[45].

[44]«*Advanced forensic format: An open, extensible format for disk imaging*»,GARFINKEL.
[45] VANDEVEN Sally, "Forensic images: for your viewing pleasure", 15 septembre 2014.

Une compression BZIP est utilisée dans cette dernière version qui permet de réduire la taille du « *fichier image* » et offre la possibilité d'utiliser un chiffrement AES-256 bits.

Les « *fichiers images* » crées par Encase® représentent une copie fidèle respectant l'intégrité du support original et contiennent également des informations complémentaires relatives à l'opération de la copie.

Un fichier Encase® est constitué de trois éléments :

1. Entête de fichier : elle peut contenir différentes informations comme le numéro de dossier, la date de la copie, la version du logiciel...
   Le contrôle de redondance cyclique intervient sur l'entête de fichier,
2. Blocs de données : le « *fichier image* » est divisé par défaut en plusieurs segments de 640 Mo dont la taille reste configurable.
3. Intégrité des fichiers : il s'agit de vérifier l'intégrité des données en faisant un contrôle de redondance cyclique pour chaque bloc de 64 secteurs et en calculant la valeur HASH.
   Certaines critiques contestent la validation MD5 en invoquant l'existence d'un risque de collisions. Cette double vérification réalisée par Encase® permet d'éviter un éventuel risque de « collisions», c'est-à-dire des données qui posséderaient la même valeur MD5.

Par ailleurs, les deux fonctions de hachage MD5 et SHA-1 sont prises en charge par le programme Encase®.

La totalité des blocs de données est vérifiée par le MD5 (128 bits) qui exige plus de calculs et de ressources qu'un contrôle de redondance cyclique.

Depuis la version six, le SHA-1 produisant des résultats de 160 bits a été également introduit dans le logiciel.

Les erreurs de calcul ou les fichiers corrompus sont automatiquement signalés par le logiciel:

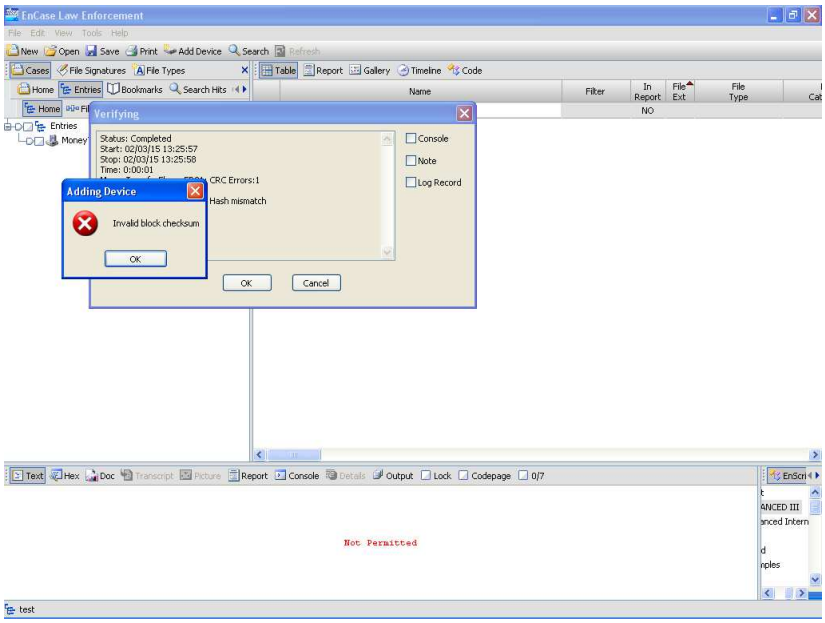


Figure11- Illustration d'un fichier de preuve contenant des erreurs, les valeurs HAH ne correspondent pas- "Encase version 6.18.1"

Le processus de vérification généré par Encase® à la suite de la copie d'une image, contrôle l'intégrité de la copie et non celle du support original.
Le résultat produisant des algorithmes MD5 et SHA-1 concerne le fichier image.

3.2 Vérification de l'intégrité des données

3.2.1 Calcul d'empreinte numérique ou la valeur de « Hash »

Après l'utilisation d'un dispositif de blocage en écriture et la réalisation d'une copie du support examiné, leurs empreintes numériques sont contrôlées pour établir la conformité des données copiées par rapport aux données d'origine.

Les algorithmes MD5 des deux supports informatiques devront être identiques.
Dans l'hypothèse où les données sont modifiées, l'empreinte numérique change et les valeurs de HASH sont différentes.

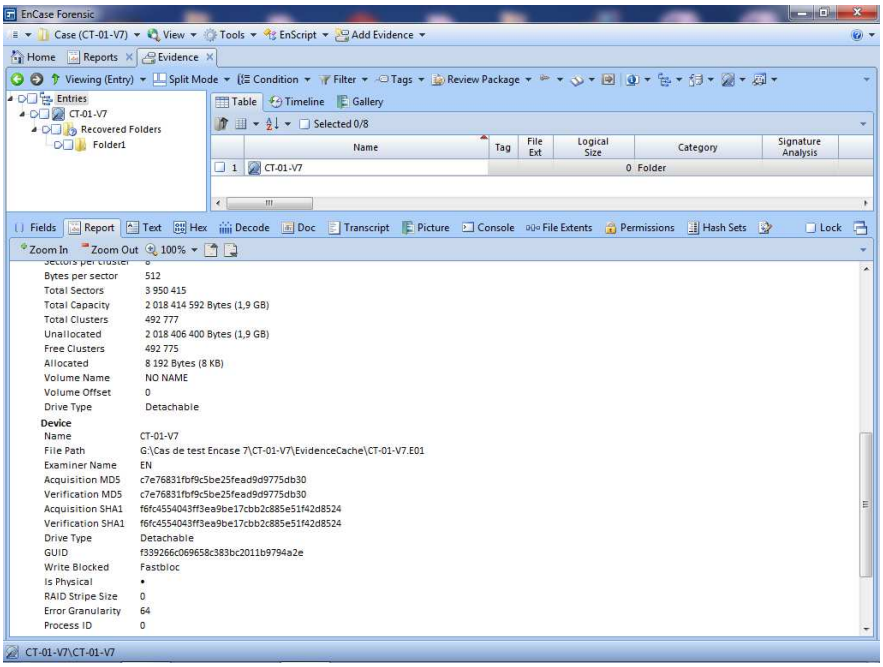


Figure12- Modèle d'un rapport de vérification MD5/SHA-1 par le logiciel Encase® version 7

3.2.2 Comparaison des empreintes numériques des fichiers

Plusieurs techniques de comparaisons entre les empreintes numériques des fichiers permettent de confirmer leur intégrité.

L'une d'entre elles consiste à utiliser la base de données de la « *National Software Reference Library* » (NSRL), mise à la disposition des enquêteurs par l'Institut National des Normes et de la Technologie.

Cette ressource fournit une collection de valeurs de hachage MD5 et SHA-1 des logiciels connus et des informations complémentaires relatives aux fichiers.

La création d'une table de hachage permet de faire une comparaison entre les empreintes numériques des fichiers.

Une analyse réalisée à partir de cette base de données permet de filtrer plus rapidement les fichiers et d'éliminer tous ceux qui ne sont pas utiles à l'enquête.

Grâce à cette méthode, toute modification de fichiers par un virus ou par une utilisation illégale est identifiée.

L'utilisation de l'outil «ssdeep» permet également de trouver deux fichiers similaires même s'ils ne sont pas identiques au niveau binaire.

Le programme permet d'associer deux fichiers lorsque l'un d'entre eux est une version tronquée de l'autre, c'est la technique dite « *fuzzy hashing* ».
Avec cette méthode il n'est cependant pas possible de récupérer des fichiers fragmentés sur des supports reformatés ou repartitionnés.
Lorsqu'un fichier ne possède ni d'entête ni fin de fichier reconnaissable, un calcul basé sur la taille du secteur ou celle du cluster, de l'anglais « *block-based hash analysis* » permet de calculer des valeurs de hachage pour chaque bloc de fichier fragmenté.

3.2.3 Identification par analyse de signature

Une comparaison entre la signature numérique d'un fichier et son extension permet de déterminer son format.
Cette technique est efficace pour retrouver des fichiers dont les extensions sont volontairement modifiées notamment dans le but de masquer des activités criminelles.
Les fichiers sont standardisés par la norme ISO et ITU-T, la plupart d'entre eux étant reconnaissable par l'analyse d'une suite d'octets se trouvant en début de chaque fichier.

A titre d'illustration, un fichier au format « BMP » commence par les caractères "BM" codés en ASCII et la signature hexadécimale "0x424D".

Au contraire un fichier du type « TXT » contenant du texte au format ASCII, n'a pas de signature et peut seulement être identifié par son extension.
Ce type de fichiers peut être à l'origine des résultats faux-positifs générés par les outils d'expertise.

3.3 Analyse et extraction des données

Pour rechercher des informations en lien avec une infraction ou un litige, différentes techniques sont déployées. Elles permettent de récupérer des données effacées, de reconstituer les fichiers fragmentés, d'analyser le registre, d'exploiter l'historique de connexions internet, d'analyser la messageries électroniques, etc.

Ce travail d'analyse et d'extraction des données requiert une bonne connaissance de la structure du système de fichiers ainsi que du système d'exploitation que contiennent les support numériques.

3.3.1 Techniques de récupération de données supprimées sur un Système Windows

Les technologies d'investigations utilisent plusieurs méthodes de recherches afin de récupérer les données effacées sur un support informatique.

3.3.1.1 Récupération de partitions effacées sur un disque dur :

L'une des techniques de récupération des données concerne la recherche de partitions supprimées.
Le secteur de démarrage ou le "MBR", situé au premier secteur physique d'un disque dur contient la table des quatre partitions principales d'un disque dur à l'octet 446.
La zone des messages d'erreurs, le code exécutable lancé par le BIOS et les signatures hexadécimales 0x55-0xAA occupent les octets 510 et 511.

Lorsqu'une partition est effacée, le système d'exploitation remplace les seize octets de celles-ci par des valeurs zéros.
Or, les données resteront intactes jusqu'à la création d'une nouvelle partition ou leur suppression par un programme d'effacement permanent.

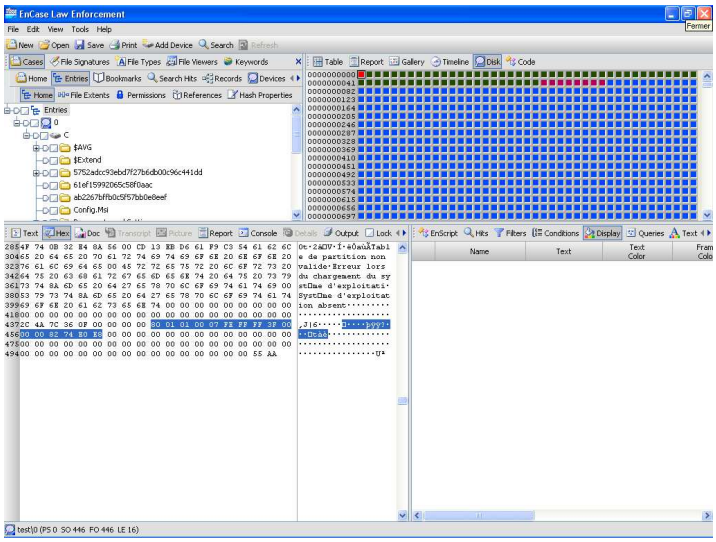


Figure13- Partition du type NTFS- Copie écran « Encase® Forensic version6»

La figure ci-dessus illustre un disque dur constitué d'une seule partition primaire du type NTFS (07). Le secteur de démarrage principal contient une signature de quatre octets attribuée au disque et insérée dans le MBR, pour indiquer que celui-ci a été utilisé par le système Windows.
Cette signature est comprise entre les octets 440 et 443, sous Windows sept elle est précédée par des valeurs hexadécimales 62 7A 99.

Le VBR, le premier secteur de la partition, contient une série d'informations importantes sur la taille, le nombre de secteurs et la référence OEM du système d'exploitation.
Le dernier secteur du volume contient également une copie de sauvegarde du VBR.
Si la table des partitions est effacée, une recherche par mots clés permettra de la récupérer dans les zones non utilisées du disque dur.

3.3.1.2 Récupération de fichiers effacés sur un disque dur :

Lorsqu'une partition est formatée avec un système de fichiers NTFS, plusieurs fichiers systèmes sont crées dans le répertoire racine du volume.
Les dates de création et de modification de ces entrées sont identiques et correspondent à la date du formatage de la partition en NTFS.

Le fichier système le plus important est la table de fichiers maître, connu sous le nom

de $MFT qui répertorie tous les fichiers sauvegardés sur le disque dur.
Chaque entrée porte l'entête [FILE0], disposant d'une taille de 1024 octets et contient une série d'informations relatives au fichier associé.
Il s'agit de son nom complet, le nom court, sa taille, les dates de création, de modification ou d'accès, la liste des blocs contenant le fichier, etc.

Un fichier de petite taille, comme un fichier au format texte est directement enregistré dans la MFT. On parle alors de fichiers "résidents" dont les tailles logique et physique seront identiques.

Lorsque la taille d'un fichier est trop grande pour être sauvegardée dans la MFT, il devient alors "non-résident".
Le contenu de l'attribut est écrit sur le disque et un pointeur vers cette zone est crée dans l'entrée de la MFT.

Sous Windows, lorsqu'un fichier est placé dans la corbeille par l'utilisateur, son entrée dans la MFT est supprimée et son nom remplacé par la lettre D.
Le nom du fichier sera ensuite suivi de la lettre assignée au volume sur lequel il était enregistré et d'un numéro d'index commençant par "1".
Dans les versions antérieures à Windows Vista, les informations concernant un fichier supprimé étaient stockées dans le fichier « INFO2 » dans la corbeille.
Il contenait le nom original du fichier supprimé, son emplacement sur le disque, la date et l'heure d'effacement ainsi que son numéro d'index.

Depuis Windows Vista, le nom de la corbeille a été remplacé par "$Recycle.Bin" et les informations contenues dans le fichier "INFO2" sont désormais enregistrées dans un fichier d'index dont le nom commence par les lettres "$I".

Sur un système de fichier FAT, lorsqu'un fichier est supprimé, la première lettre de l'entrée est remplacée par le caractère "E5" en hexadécimal pour indiquer au système que la place qu'il occupait sur le disque est à nouveau disponible.

3.3.1.3 Récupération de fichiers basée sur la technique du « Carving » :

Les techniques classiques de récupération des données permettant d'utiliser les informations contenues dans un système de fichier diffèrent de celles pratiquées pour le « Carving ».
Lorsqu'un fichier effacé n'est plus référencé dans la table d'allocation, sa récupération devient plus complexe.
La technique du « Carving » consiste à reconstituer un fichier enprocédant à une recherche par signature du début et de la fin de fichier.
A titre d'illustration, un fichier au format « JPEG » débute toujours par les valeurs hexadécimales sur deux octets « FF D8 » et se termine par le marqueur « FF D9», l'image se trouve entre l'entête et la fin de fichier.

Une recherche par mots clés du type « *GREP* » dans les espaces non alloués du support examiné permettra d'identifier ces valeurs et de reconstruire l'image.
Dans le cas des fichiers fragmentés, des méthodes plus sophistiquées de « Carving » sont utilisées et d'autres informations sont prises en considération.

Pour la récupération de données effacées, l'une des zones importantes à examiner reste le « slack ». C'est l'espace qui sépare la fin logique d'un fichier de sa fin physique.
Des données qui occupaient précédemment cet espace mais qui n'ont pas été réécrites, sont susceptibles d'être récupérées.
Ainsi, des fragments de fichiers sont susceptibles d'être reconstitués.

3.3.2 Analyse du registre

La base de registre, apparue avec la version de Windows 95, a remplacé les différents fichiers textes linéaires sous DOS (config.sys, autoexec.bat) et les fichiers INI (win.ini, system.ini) qui contenaient les informations relatives à la configuration du système.
Cette base de données centrale conserve les paramètres du système d'exploitation.
Les versions ultérieures de Windows apportant quelques innovations, utilisent ce même modèle de registre.

Pour la recherche de preuves informatiques, les deux clés "*HKEY_LOCAL_MACHINE"* et "*HKEY_USERS"* sont fondamentales.

Une analyse approfondie du registre peut apporter des informations importantes sur l'utilisateur ainsi que les programmes utilisés.

- Algorithme « ROT13 » :

La clé « *User Assist* » gérant les programmes récemment utilisés dans Windows utilise un chiffrement de ROT13.

C'est un algorithme simple que Jules césar utilisait pour chiffrer certains messages.

Il n'y a pas d'informations officielles relatives au chiffrement de cette clé dans la base de connaissance de Microsoft .

Une méthode de recherches consisterait à décoder cet algorithme pour obtenir des informations sur les programmes, leur utilisation ou leur date d'accès par l'utilisateur.

L'examen des points de restauration du « system volume information» ou du fichier « gvzrqngr.pcy » (timedate.cpl) permettent également de déterminer si la date et l'heure du système ont été manipulées.

- Périphérique USB :

Dès la connexion d'un périphérique USB à un ordinateur, des entrées sont crées dans la base de registre sous la clé *SYSTEM\CurrentControlSet\Enum\USBSTOR*.

L'analyse des traces laissées dans le registre permet d'identifier des informations sur le support, la marque, le numéro de série, la dernière fois où le support a été utilisé ou bien la lettre assignée au volume lorsqu'il a été connecté à la machine :

NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{GUID}
SOFTWARE\Microsoft\Windows Portable Devices\Devices (sous Windows sept)

- La détermination du fuseau horaire :

Avant de débuter l'expertise d'un ordinateur, il est important de déterminer la date et l'heure de l'appareil.

Cette information doit être vérifiée dans le BIOS et dans le registre de Windows sous les clés suivantes :

- HKLM\SOFTWARE\Microsoft\windowsNT\CurrentVersion\TimeZones
- HKLM\SYSTEM\Microsoft\CurrentControlSet\Control\TimeZoneInformation

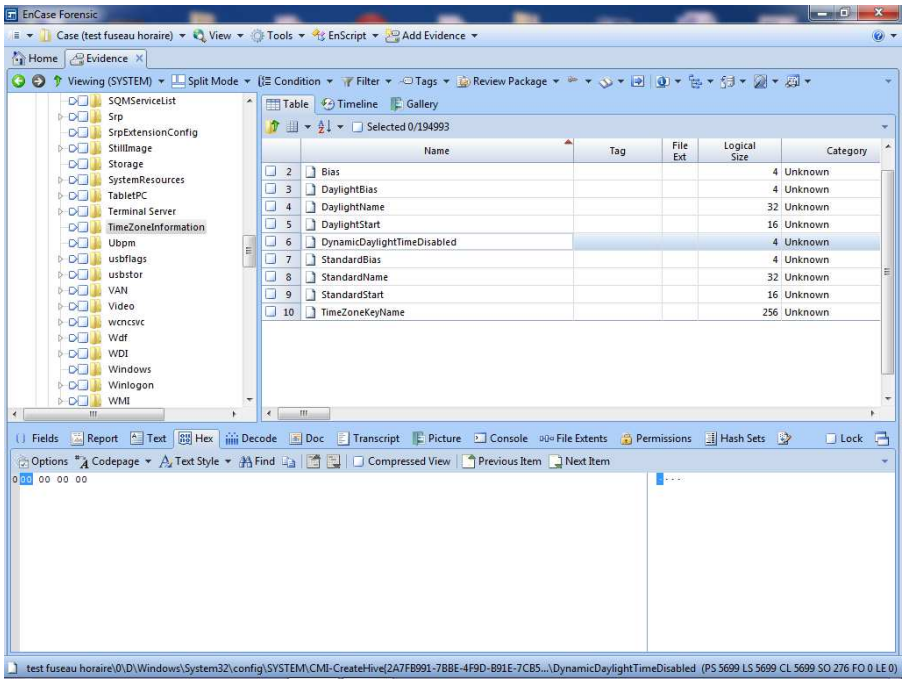


Figure14- La clé "TimeZoneInformation", Encase version 7.06

La valeur « TimeZoneKeyName » contient le fuseau horaire de l'appareil.

Dans l'exemple illustré par la figure 15, le programme Encase version 7.06 affiche le fuseau horaire de « Romance Standard Time » qui correspond à l'heure normale d'Europe centrale (GMT+01:00, Bruxelles, Copenhague, Madrid, Paris) :

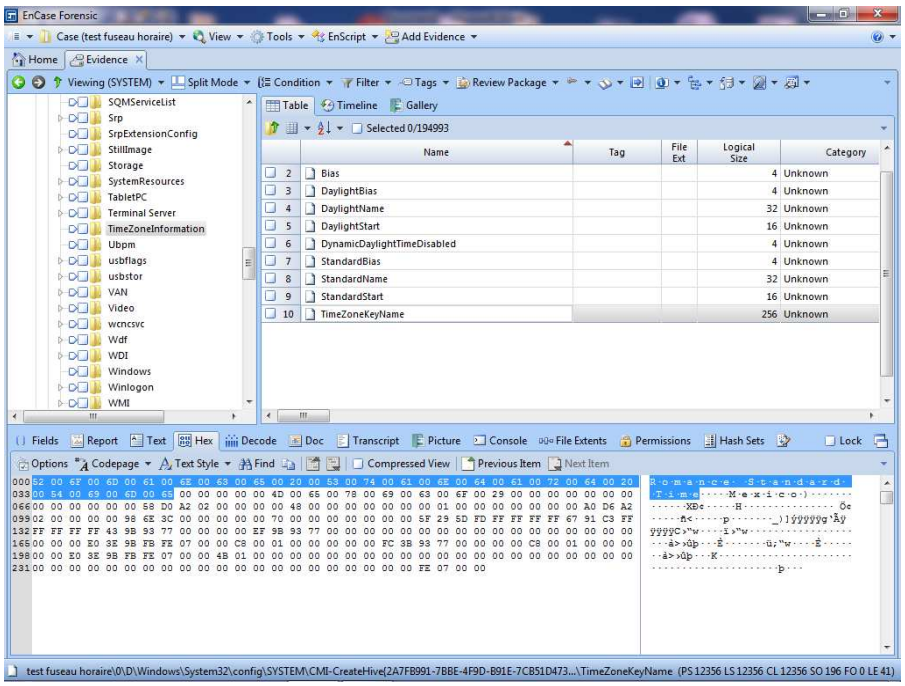


Figure15- Indication du fuseau horaire dans Encase version 7.06

Le logiciel Encase permet également de localiser la clé « CurrentControlSet » et de

déterminer la date et l'heure de Windows soit manuellement soit à l'aide d'une recherche automatisée:

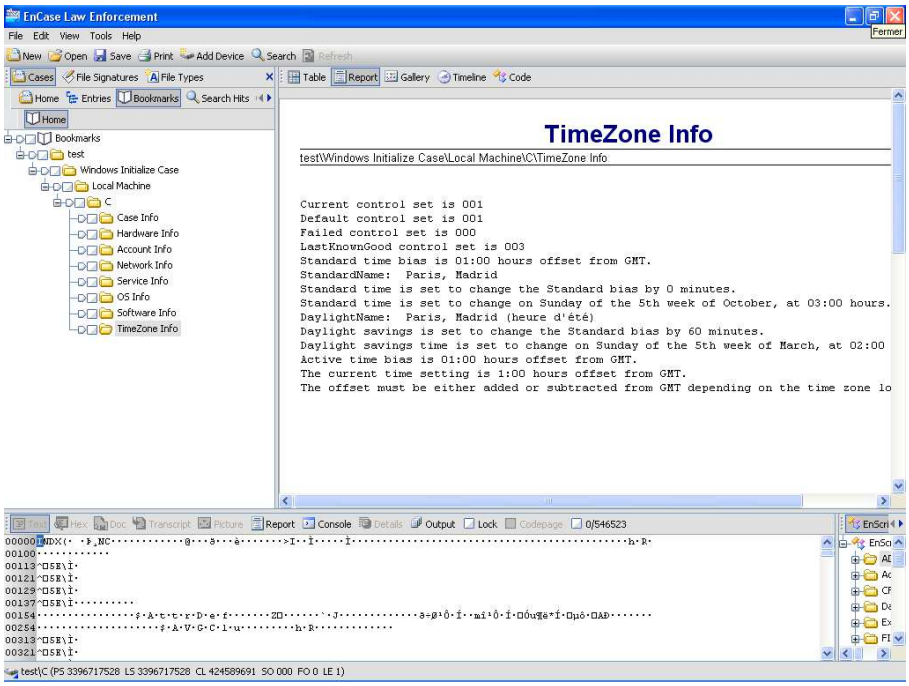


Figure16- Recherche automatisée du Fuseau horaire, Encase version 6.18.1

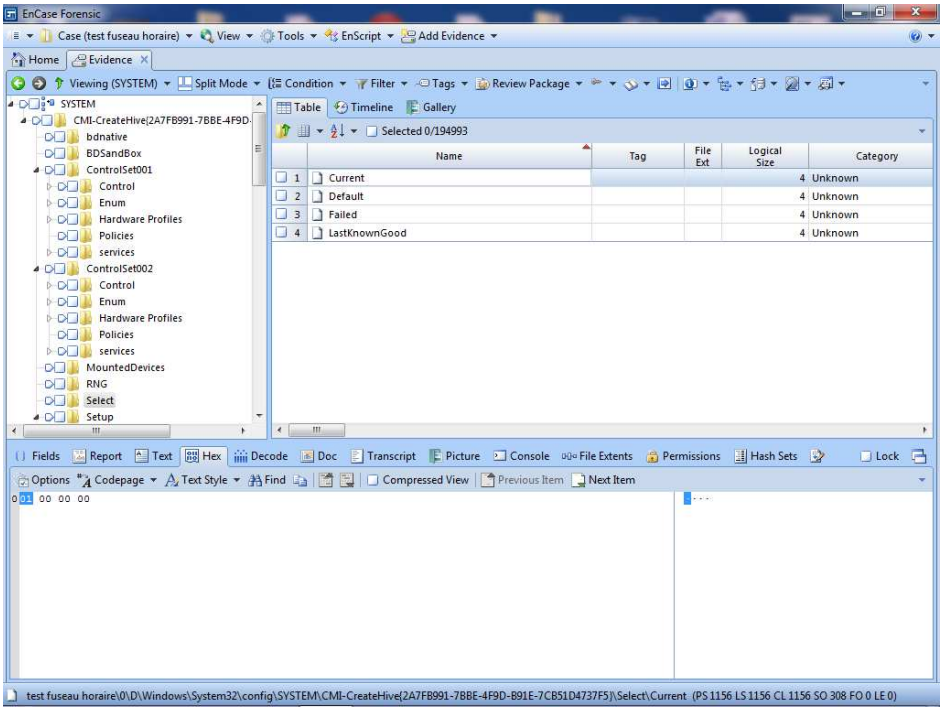


Figure17- Recherche manuelle du fuseau horaire dans le registre- Encase version 7.06

Lorsque le fuseau horaire du disque dur examiné est différent de celui de la machine de l'expert, le programme Encase permet de modifier la date et l'heure du système

afin d'éviter toute confusion sur l'interprétation de différentes données :

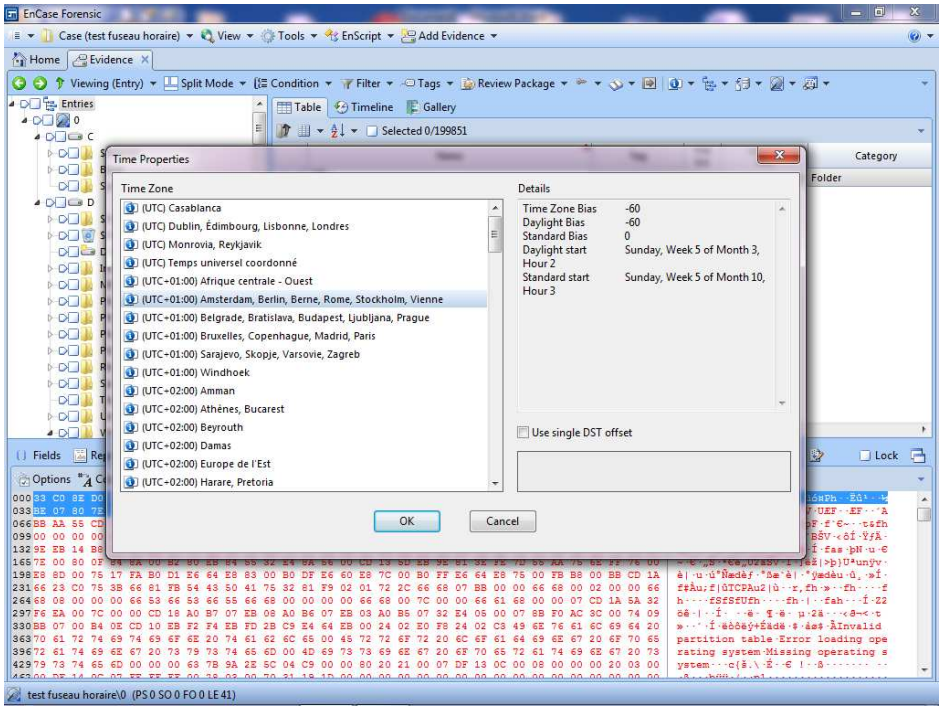


Figure18- Modification du fuseau horaire- Encase version 7.06

Dès lors que les informations relatives au fuseau horaire seront déterminées, les recherches sur le support pourront commencer.

- La date des sites internet consultés:

Depuis la sortie de Windows 8 et la version 10 de l'Internet Explorer, l'examen de la clé« TypedURLsTime » est important car elle indique la date des derniers sites visités par l'utilisateur.

Cette information est enregistrée dans le registre sous la clé « ntuser.dat\Software\Microsoft\Internet Explorer\ TypedURLsTime ».

Elle permet de mettre en évidence la dernière date de connexion aux différents sites visités, la plus récente sera référencée avec la valeur « url1 ».

Le registre constitue ainsi une ressource importante dans la recherche et l'analyse de preuves informatiques.

D'autres clés permettent aussi d'apporter des informations précieuses sur les activités de l'utilisateur, le réseau ainsi que les applications installées sur la machine.

L'analyse du registre permet également d'identifier des informations relatives aux traces laissées par les navigateurs web comme l'historique de connexions internet, les cookies, les mots de passes enregistrés dans le navigateur, etc.

3.3.3 Récupération de la messagerie et recherche des traces sur Internet

- Internet Explorer :

Dans les versions antérieures du navigateur « Internet Explorer », l'historique de connexions Web était enregistré dans un fichier intitulé « index.dat » qui conservait la trace de toutes les activités quotidiennes et hebdomadaires de l'utilisateur comme les pages web visitées ou les documents consultés.

Avant la version de Windows Vista, ces informations étaient sauvegardées dans le répertoire « *Application Data* ».

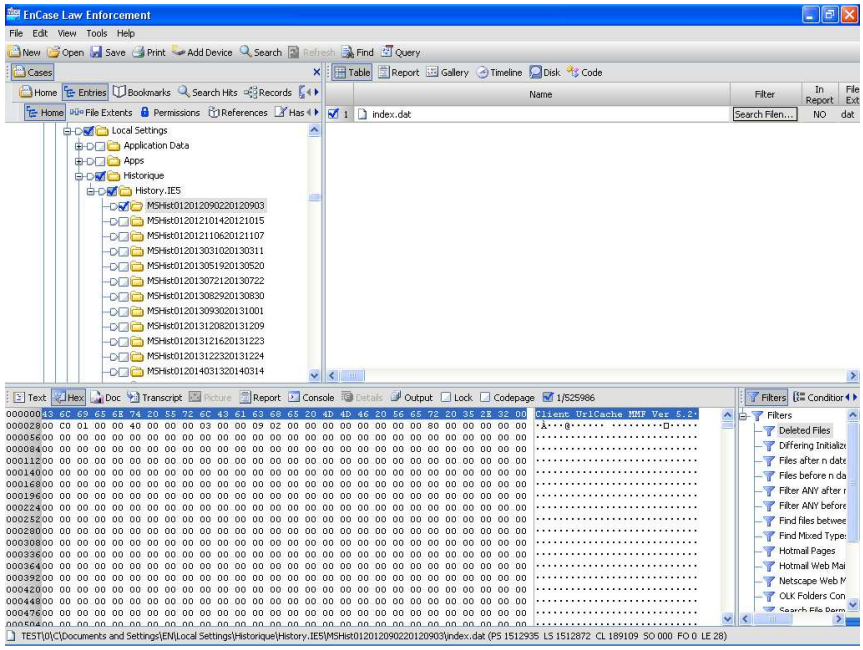


Figure 19- Fichier INDEX.DAT sous Windows XP- copie écran logiciel « Encase® Forensic V6»

Cet ancien fichier « index.dat », utilisé dans les versions 1 à 9 d'Internet Explorer, était composé d'une entête de fichier de 28 octets :

Représentation hexadécimale de l'en-tête du fichier INDEX.DAT	43 6c 69 65 6e 74 20 55 72 6c 43 61 63 68 65 20 4d 4d 46 20 56 65 72 20 35 2e 32 00
Caractères en ASCII	Client UrlCache MMF Ver 5.2

Windows Vista a remplacé le répertoire « *Application Data* » par « AppData » et les informations relatives aux navigateurs Web comme les fichiers historiques, le cache ou les cookies sont désormais enregistrés dans le sous répertoire « Local ».

Depuis la version 10 du navigateur, ces informations se trouvent dans un nouveau fichier intitulé «WebcacheV*.dat»[46] qui se trouve sous le chemin Users\%user%\AppData\Local\Microsoft\Windows\WebCache.

Il remplace le fichier « index.dat » et son analyse peut apporter des informations précieuses.

Afin de sauvegarder les métadonnées, cette version utilise le format de base de données ESE ou JetBlue qui est déjà utilisé par plusieurs applications de Microsoft comme « Windows Mail », « Active Directory », « Windows Search » ou encore « Exchange ».

Avec l'apparition de Windows 8, les traces laissées par les applications de la nouvelle interface metro sont à rechercher dans les répertoires « INetCache », « INetCookies », et « INetHistory ».

Les programmes tels que Encase ou FTK ne permettent pas d'exploiter le contenu de ces fichiers et les utilitaires comme «ESEDatabaseView» de Nirsoft ou «Internet Evidence Finder» de Magnet Forensics peuvent extraire les données.

De même l'outil «esentutl.exe» développé par Microsoft permet de nettoyer et de réparer les bases ESE.

Crées par Microsoft pour ajouter des fonctionnalités additionnelles à Internet Explorer sous forme de fichier DLL, des modules complémentaires tels que les « *Browser Helper Object* » (BHO) sont souvent utilisés par les programmes malveillants.

Rarement détectés par les pare-feu et les antivirus, ils compromettent le navigateur et effectuent des actions à l'insu de l'utilisateur.

Un examen minutieux du registre permet de localiser la présence de tels utilitaires :

\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
\SOFTWARE\Classes\CLSID{GUID}\InprocServer32

[46]« Internet Explorer 10 et 11, un nouveau format de données pour de nouveaux défis», Jean Philippe NOAT, Bruno VALENTIN.

- Archives de messagerie :

Afin de récupérer le contenu des messages électroniques sauvegardés, il faut d'abord extraire les données d'archive et de procéder ensuite à une analyse de courriels par différentes techniques de recherches par mots clés.

Les fichiers de sauvegarde des logiciels de messageries tels que « Microsoft Outlook », « Outlook Express » (remplacé par Windows live mail), « Exchange » et « Lotus » sont enregistrés aux formats PST, DBX, MBOX et NSF.

Prenons l'exemple du fichier de dossiers personnels (PST)[47] de Microsoft Outlook utilisant le protocole MAPI qui peut être très volumineux.
Depuis la version de Microsoft Outlook 2010 sa taille peut même atteindre 50 Go.

Les spécifications techniques de ces fichiers sont rendus publics par la société Microsoft. Les données composant un fichier au format "PST" sont consignées dans le tableau ci-dessous :

Propriété	Description
PR_SENDER_NAME	Le nom de l'expéditeur du message
PR_DISPLAY_TO	La liste des premiers destinataires
PR_DISPLAY_CC	La liste de tous les destinataires du message
PR_SUBJECT	L'objet du message
PR_PRIORITY	La priorité du message
PR_TRANSPORT_MESSAGE_HEADERS	Les informations spécifiques sur les enveloppes des messages transmis
PR_BODY	Le message
PR_ATTACH_FILENAME	Le nom du fichier joint et son extension
PR_ATTACH_LONG_FILENAME	Le nom complet de la pièce jointe et son extension
PR_MESSAGE_SIZE	La taille en octets du message
PR_CREATION_TIME	La date de création du message
PR_LAST_MODIFICATION_TIME	La date de modification de l'objet ou du contenu du message

[47] De l'anglais "*personal storage table*".

PR_MESSAGE_DELIVERY_TIME	La date de la réception du message
PR_CONTAINER_CLASS	Une chaîne de caractères décrivant le type du fichier
PR_MESSAGE_ CLASS	Une chaîne de caractères identifiant la classe de message de l'expéditeur
PR_DISPLAY_NAME	Le nom du profil MAPI
PR_CLIENT_SUBMIT_TIME	La date de l'envoi du message

Troisième partie : EVALUATION ET PERSPECTIVE DE CERTIFICATION DES LOGICIELS D'INVESTIGATION NUMERIQUE

Chapitre 1 - Introduction

Les tests font partie intégrante du cycle de développement logiciel et visent à s'assurer que le système est conforme aux spécifications.

D'après la norme 610.12-1990 de l'Institut des ingénieurs électriciens et électroniciens (IEEE)[48]: "*Le test est l'exécution ou l'évaluation d'un système ou d'un composant par des moyens automatiques ou manuels, pour vérifier qu'il répond à ses spécifications ou identifier les différences entre les résultats attendus et les résultats observés*".

Le « *zéro défaut* » n'existe pas en matière de logiciel et l'impossibilité d'identifier des anomalies n'implique pas nécessairement l'absence de défauts[49].

Avec la complexité des logiciels, les taux d'erreurs sont également susceptibles d'augmenter.

Les erreurs de programmation ne sont pas sans dangers, elles peuvent avoir des conséquences désastreuses et influer notamment sur la sécurité d'un dispositif.

En 1996, lors du lancement de la fusée Ariane5, celle-ci se brise et explose en raison de l'utilisation sur Ariane5 du logiciel de correction latéral Ariane4 (32 bits) lequel n'avait pas fait l'objet de tests de validation préalables.

Dans une procédure judiciaire, le juge peut solliciter un expert pour l'éclairer sur des questions d'ordre techniques ne relevant pas de sa compétence.

Dans l'exercice de sa mission et pour contribuer à la manifestation de la vérité, le spécialiste recourt aux logiciels et matériels labellisés « investigation numérique ».

Le magistrat en charge de l'enquête s'appuie sur les conclusions techniques de l'expert pour rendre sa décision.

[48] Institute of Electrical and electronics Engineers.

L'issue d'une décision judiciaire pourrait dépendre de ces analyses techniques car la justice se fie à l'expérience et à la compétence de l'expert.
En France, contrairement au système accusatoire des pays anglo-saxons, il n'y a aucune prescription ou exigences en matière de validation d'outils d'investigation technique.
Les experts doivent mettre en place leurs propres procédures de validation ou tests de logiciels.
Ces programmes nécessitent d'être testés avant d'être utilisés dans le cadre d'une expertise judiciaire.
La constatation d'erreurs dans un programme informatique peut compromettre la fiabilité des résultats produits devant la justice.
Si l'expert dépose des conclusions erronées que les magistrats suivent, cela conduirait à des erreurs judiciaires.

Aux Etats-Unis en 2011, dans l'affaire très médiatisée « *State of Florida Vs Casey Anthony* » qui a passionné l'Amérique pendant un mois, les constatations des experts fondées sur un logiciel d'expertise judiciaire se sont avérées être inexactes.
Le programme comportait des erreurs et a été par la suite corrigé par l'éditeur.

Il s'agissait du procès d'une jeune femme qui était accusée du meurtre de sa fille de deux ans après l'avoir endormie avec du chloroforme.
Les données produites lors de ce procès ont joué un rôle prépondérant.
Les conclusions de l'expert en Informatique qui avait analysé l'ordinateur saisi au domicile du prévenu montraient que l'historique de connexion internet, récupérée parmi les espaces non alloués du disque dur, comportaient des traces de recherches par mots clés du mot « *chloroforme* » à de nombreuses reprises.

Ces résultats étayaient ainsi la thèse de la préméditation soutenue par l'accusation.
Les informations étaient identifiées par le programme « Cacheback » souvent utilisé par les Services de Police aux Etats-Unis, qui permet de reconstruire l'historique de navigations web.

---

[49] « *Economics of Software Verification* », Gerald J. HOLZMANN, page 1.

Selon ce logiciel, le mis en examen avait recherché le mot « *chloroforme* » à quatre vingt quatre reprises alors que les résultats produits par l'autre programme d'analyse de preuves « NetAnalysis » montraient au contraire une seule recherche de ce mot.

Dans le domaine de l'expertise judiciaire, les méthodes de collecte et d'analyses des données sont bien documentées par la communauté des experts et de nombreux recueils de bonnes pratiques sont proposés.

Mais peu d'informations concernant la capacité et le degré de fiabilité et de précision des programmes utilisés dans le cadre des investigations numériques sont disponibles. Il n'existe aucun référentiel dans la discipline permettant de comparer les résultats générés par différents logiciels d'expertise en Informatique.

Les outils les plus connus comme Forensic ToolKit (FTK®) ou Encase® sont largement utilisés au niveau international.
Mais toutes leurs fonctionnalités ne sont pas connues ou testées par des spécialistes.
Il en est de même pour beaucoup d'autres logiciels dont les résultats ne sont pas toujours vérifiés par les experts.
Les logiciels d'expertise de nouvelles générations proposent une multitude de fonctionnalités.
A titre d'exemple, le logiciel Encase® offre la possibilité d'écrire des scripts personnalisés qui seront ensuite intégrés au programme.

Comment peut-on s'assurer que chaque composant d'un logiciel fonctionne correctement?

Gerald J. HOLZMANN propose une étude dans laquelle il démontre que plus un outil est complexe et contient de fonctionnalités, plus le risque de défauts dans le logiciel est grand. Cette affirmation est illustrée par le schéma ci-dessous:

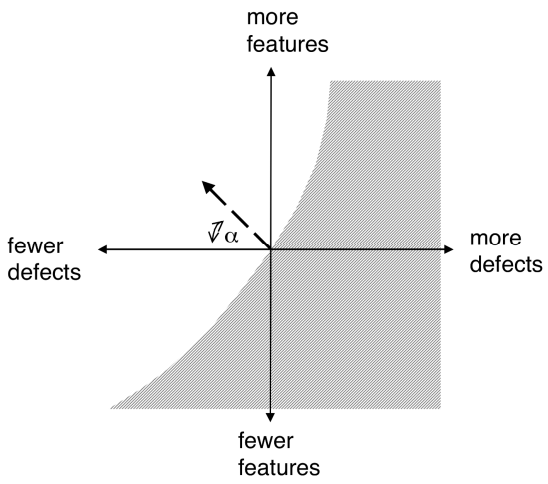


Figure20- Source « *Economics of Software Verification* »[50]

Selon l'auteur, l'ajout de nouvelles fonctionnalités dans un logiciel est attractif pour les utilisateurs mais il doit également correspondre aux exigences de qualité et de fiabilité attendues.

Si le nombre de défauts dans le logiciel croît, cela entraînera une diminution de la satisfaction de l'utilisateur.

La diminution du nombre de fonctionnalités n'est pas non plus une solution adéquate, sauf si elle est compensée par un gain considérable de fiabilité.

Sur le schéma ci-dessus, la partie grise sélectionnée représente la zone à éviter et la flèche en pointillés sur la partie gauche du schéma indique une trajectoire optimale du développement combinant l'augmentation des fonctionnalités et une diminution de la densité des défauts résiduels.

La meilleure stratégie étant de combiner ces deux valeurs afin de rester le plus éloigné de la zone sélectionnée.

Ce principe peut également être applicable au domaine de l'investigation numérique et plus précisément à celui des outils d'analyse de preuves lesquels deviennent de plus en plus complexes et sophistiqués.

Ces logiciels proposent aujourd'hui une multitude de fonctionnalités qui sont mises à jour régulièrement nécessitant une veille périodique et une adaptation constante des procédures de tests.

[50] HOLZMANN Gerald J. « *Economics of Software Verification* ».

Chapitre 2 – Tests logiciels

En matière de génie logiciel, les tests de validation et de vérification sont des activités normées et régies par le référentiel international proposé par le « *Comité international de qualification du test logiciel*» (l'ISTQB).
En France, depuis 2005, celui-ci est représenté par le « *Comité Français des tests Logiciels* » (CFTL)[51].

2.1 Concepts de «validation» et «vérification»

La qualité d'un logiciel dépend de plusieurs critères comme la "maintenabilité", la "robustesse", "l'efficacité" et "l'utilisabilité".
Les concepts de « *validation* » et de « *vérification* » de logiciels sont des méthodes techniques déployées pour maîtriser la qualité du produit et garantir la fiabilité des processus de tests réalisés.

Un test de logiciel fait partie intégrante de son processus de développement, il doit être mené à différents niveaux du cycle et se prépare dès la phase de spécifications.
La mise en place de tests de logiciel permet de réduire le taux d'erreurs et de trouver des anomalies ou défauts cachés au sein d'un programme.

Le cycle de vie de logiciel repose sur plusieurs modèles. Le cycle de développement en V propose une approche traditionnelle qui s'appuie sur plusieurs phases et les tests sont réalisés à différents niveaux de chaque étape de conception.
Le glossaire CFTL/ISTQB des termes utilisés en tests de logiciels définit le modèle en « V » comme « *une structure décrivant les activités du cycle de développement logiciel, depuis la spécification des exigences jusqu'à la maintenance.*
Le modèle en V illustre comment les activités de tests peuvent être intégrées dans chaque phase du cycle de développement».

[51] Wwww.cftl.fr

Les concepts de « vérification » et de validation » de logiciels, définis par la norme ISO 9000, constituent deux fonctions complémentaires essentielles à la garantie des exigences de qualité et de conformité d'un produit.
Le processus de « validation » et « vérification » doit être appliqué à chaque étape du développement afin de garantir que le programme ne présente pas de défauts.

2.1.1 La vérification des logiciels

La vérification d'un logiciel consiste à s'assurer que le logiciel est bien construit.
Selon la norme IEEE 1012-1998, la vérification est décrite comme le « *processus d'évaluation d'un système ou d'un composant pour déterminer si les produits logiciels issus d'une phase du cycle de développement sont conformes aux spécifications établies lors des phases précédentes* ».

La norme ISO 9000 définit la vérification comme la « *confirmation par l'examen et la fourniture de preuves objectives que des exigences spécifiées ont été remplies*».
Il s'agit des tests de fiabilité, de précision et la confirmation que le produit répond bien aux besoins définis par les clients.

2.1.2 La validation des logiciels

Elle permet de s'assurer qu'on a construit le bon produit.
Selon la norme ISO 9000, la validation est la « *confirmation par l'examen et la fourniture de preuves objectives que les exigences, pour un usage ou une application voulue, ont été remplies*».

La validation est le procédé d'évaluation qui permet de déterminer si le logiciel satisfait aux exigences de spécification.
C'est l'assurance d'un certain niveau de confiance dans le programme.

Dans la décision de principe qui sert de référence en matière de recevabilité de la preuve scientifique devant la justice, "*Daubert v. Merrell Dow Pharmaceuticals, Inc. (509 U.S. 579 (28 juin 1993)",* la cour suprême américaine considère que la partie qui produit une

preuve scientifique doit en établir la validité sous peine de la voir exclue par la juridiction.
Cela implique que pour être recevables devant la justice, les technologies utilisées dans le cadre de la recherche de preuve informatique doivent préalablement être testées et validées.
Un test consiste à exécuter un programme pour vérifier que les résultats correspondent bien à ceux qui sont attendus et pour détecter des anomalies ou des erreurs.

2.2 Méthodes de tests logiciels « boîtes noires » et « boîtes blanches »

Parmi les différentes techniques de conception de tests, on peut distinguer la méthode usuelle dite de « boîte noire », basée sur les spécifications et celle de la « boîte blanche », basée sur une étude de la structure.

2.2.1 Méthode de test "boîte noire"

Dans ce type de tests, la structure interne du programme est inconnue de l'utilisateur et les tests sont construits à partir des exigences définies.
Cette méthode peut être utilisée pour détecter des erreurs et des omissions, cela peut concerner un composant ou un module.
Les évaluations permettent d'examiner le comportement extérieur du logiciel, les résultats de sortie sont prévus en fonction des valeurs définies en entrée.
Dans l'hypothèse où les sorties ne correspondent pas aux résultats attendus, cela signifie que le programme présente une anomalie.
Ce modèle a déjà été appliqué à des tests de validation des logiciels d'analyse de preuves numériques.
En 2006, les auteurs WILSDON et SLAY ont proposé un modèle basé sur la technique de test « boîte noire »[52].
Ils soulignaient que les tests implémentés aux Etats-Unis par l'Institut National des Normes et de la Technologie et le groupe de travail scientifique sur les preuves

numériques sont trop longs à réaliser et s'avèrent inadaptés à l'évolution rapide des technologies d'investigation.
Leurs travaux prévoyaient un processus de test de vérification en six étapes :

- Acquisition du logiciel :

Avant de commencer les tests, la première phase consiste à procéder à une acquisition des données et vérifier leur intégrité.

- Choix des fonctions à tester :

Les différentes fonctions proposées par le logiciel doivent être identifiées et il convient de déterminer avec clarté celles qui seront testées.

- Mise en place des cas et scenarii de tests :

Dès lors que toutes les fonctions de l'application sont identifiées, les cas de tests sont préparés. Ces tests interviennent sur les outils de licence propriétaire dont le code source reste secret.

- Définition d'un périmètre d'évaluation des résultats:

Il s'agit de définir un périmètre d'évaluation des résultats de tests.
Si l'une des fonctions testées ne réunit pas les critères attendus, les résultats ne pourront pas être validés.

- Exécution et évaluation des tests :

L'ensemble des processus de tests seront documentés dans le respect des dispositions définies par la norme ISO 17025-2005.

Les résultats de tests seront comparés aux exigences définies à l'avance et seront évalués par rapport au périmètre d'acceptation prévu dans la phase précédente.

[52] «Validation of Forensic computing software utilizing Black Box testing techniques», T. Wilsdon & J. Slay.

- Evaluation des résultats générés :

A l'issue des tests, les résultats devront être partagés avec la communauté d'experts qui donnera ainsi son avis sur les travaux.

2.2.2 Méthode de test "boîte blanche" ou test structurel

Les tests "boîte blanche" visent à analyser un programme informatique dont on connaît bien le fonctionnement interne en utilisant sa structure interne c'est-à-dire le code source du programme.
Chaque instruction et chaque chemin est exécuté au moins une fois.
Cette méthode est généralement utilisée pour détecter des erreurs de programmation dans des logiciels libres pour lesquels le code source est connu du public, elle ne peut pas être appliquée aux tests de logiciels propriétaires qui ne communiquent pas cette information.

2.3 Importance de la mise en œuvre des tests de validations de logiciels d'analyse de preuve numérique

Dans un cadre judiciaire, lorsqu'un magistrat chargé de l'instruction d'un dossier, rencontre une question d'ordre technique qui ne relève pas de sa compétence, il peut faire appel à un expert de son choix.
Ces spécialistes recourent à de nombreux outils logiciels afin de conduire les recherches sur le contenu des supports et analyser la preuve informatique.
Les logiciels d'analyses de recherche de preuve pouvant être utilisés par les experts dans des affaires pénales dont les enjeux sont considérables pour les accusés, il est donc important que la preuve apportée par l'expert soit fiable.
« *L'expert dit sa vérité scientifique comme l'enquêteur a dit sa vérité policière et pour le juge qui les a choisis et leur faut confiance, ces vérités deviennent la vérité* »[53].

Une erreur d'appréciation de l'expert pourrait conduire à des conclusions infondées et impacter la procédure.

Des conclusions erronées pourraient notamment avoir pour conséquence la prononciation, à tort, d'une peine privative de liberté à l'égard de la personne accusée.

Les spécialistes ont tenté d'appliquer certaines normes au domaine de l'investigation numérique mais celles-ci ne sont pas complètement adaptées à la discipline.
Aucune obligation d'évaluation des logiciels d'analyse de preuve n'est prévue pour les praticiens et les tests restent isolés.

En pratique, les experts manquent de moyens et ne peuvent pas toujours tester les outils qu'ils utilisent dans un cadre judiciaire.
Il est très difficile d'identifier tous les défauts affectant un programme mais les tests de validation permettent de réduire les risques d'imprécisions ou d'erreurs.
Il est donc important de définir une stratégie de tests et de mettre en place un plan de test détaillé pour contrôler les résultats et les exigences attendus par l'outil.

S'agissant des logiciels de licences propriétaires, dans la mesure où leurs codes sources sont tenus secrets par les éditeurs, les seuls tests proposés sont ceux effectués en interne par les éditeurs de ces programmes sans que les détails ne puissent être communiqués.

Les deux éditeurs des deux logiciels « Encase® Forensic » et «Forensic Toolkit» (FTK) fournissent régulièrement des documents attestant que leurs outils respectent les principes énoncés par la jurisprudence DAUBERT et les conditions de recevabilité de la preuve scientifique devant les juridictions.
La société AccessData, éditrice du programme FTK, quant à elle, soutient que son logiciel fait_régulièrement l'objet d'évaluations par les développeurs de la société, les agences gouvernementales et les enquêteurs spécialisés dans le domaine de l'investigation[54].

Pourtant, les résultats des tests effectués par l'Institut National des Normes et de la Technologie en 2008, sur la fonction d'acquisition des données du programme « Forensic Toolkit », montrent plusieurs catégories d'erreurs.

---

[53] LECLERC, op.cit, page 271
[54] « *The Rules of Digital Evidence and AccessData Technology* », Accesdata.

Il en est de même pour le logiciel « Encase® Forensic ».
Ainsi, sans la définition d'une stratégie de tests adéquate, il n'est pas possible de connaître les capacités et les limites de ces technologies qui assistent les experts dans l'analyse et la recherche de preuve informatique.

Chapitre 3 - Les normes internationales et les enjeux de la certification dans le domaine de l'expertise en informatique

L'expertise judiciaire en informatique est une discipline entre l'informatique et la justice qui permet de produire des éléments de preuve en justice.

Les laboratoires d'investigation technique jouent ainsi un rôle prépondérant dans notre système judiciaire.

Pour répondre aux exigences de qualité et de confiance, les praticiens ressentent le besoin de recourir à des certifications accordées par un organisme tierce et s'orientent de plus en plus vers une norme internationale du type ISO.

La certification est une procédure par laquelle une tierce partie atteste qu'un produit ou un service est bien conforme aux exigences définies dans un référentiel ou une norme.
Plusieurs types de certifications existent et ils constituent un gage de qualité, de confiance et de sécurité des produits ou services.

Différents dispositifs relatifs à la certification des personnes, des pratiques de l'expertise ou des systèmes de management s'appliquent au domaine de l'expertise.
C'est la reconnaissance par un organisme indépendant que les exigences d'une norme sont bien appliquées.
Elle peut constituer un gage de fiabilité, de compétence et peut être une réponse aux exigences de qualité.
Contrairement à certaines disciplines, il n'existe pas d'obligation légale de certification dans le domaine de l'expertise technique.

Certaines normes ISO sont appliquées au domaine d'investigation numérique sans pour autant être initialement prévues pour cette discipline.

L'objectif des normes est d'harmoniser les procédures et les utiliser comme directives.

« *La normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux* ».[55]

Il existe bien une normalisation des pratiques de l'expert en général mais il n'y a pas de certification ou de procédures de validation pour les outils d'analyse de preuves numériques. De plus, les dispositifs de certification actuels restent insuffisants pour ce domaine.

En raison des enjeux importants liés à l'utilisation de ces outils dans un cadre judiciaire, certains spécialistes font état de l'importance d'une procédure de validation de ces technologies[56] et s'interrogent sur une nouvelle modalité de certification en soulignant l'exigence de la mise en place de standards dans la discipline.

Aujourd'hui, il apparaît presque impossible de mener une investigation technique sans recourir à des logiciels sophistiqués, en se reposant uniquement sur le savoir faire du praticien.

La quantité très importante de données à analyser sur les supports informatiques nécessite de se faire aider par des outils automatisés.

Mais les conclusions d'un expert dépendent souvent des résultats générés et la fiabilité des outils utilisés.

3.1 Exigences de qualité appliquées à l'expertise

3.1.1 La norme ISO 9001

La norme ISO 9001 est un référentiel qui vise la certification et la reconnaissance de la conformité du système qualité.

Lorsqu'un organisme d'expertise est certifié ISO 9001, il s'agit de garantir un système de management de la qualité dans un organisme pratiquant des activités d'expertise.

---

[55] Igalens, J. Penan H. la normalisation, PUF- Que sais-je, 1994

[56] Reust 2006, Meyers & Rogers 2004.

Mais cette certification ne satisfait pas pour autant les exigences techniques de la conduite d'expertise.

3.1.2 La norme AFNOR NFX 50-110 « prescriptions générales de compétence pour une expertise »

La norme NFX 50-110 sur la qualité en expertise a été élaborée par AFNOR en 1999.
Elle permet d'établir des règles transverses applicables à différents secteurs d'activité, garantissant la qualité de la conduite expertale en général.
Sa version actuelle date de 2003 et elle concerne la certification des pratiques et la conduite d'une expertise.

3.1.3 La norme internationale ISO/CEI 17025

Cette norme est le référentiel utilisé lors des audits d'accréditation des « *exigences générales concernant la compétence des laboratoires d'étalonnages et d'essai*».
En France le COFRAC, reconnu comme instance nationale, accrédite les laboratoires d'essai et d'analyses selon cette norme.
Elle garantit que les pratiques mises en place par toute organisation qui procède à des essais, produisent des résultats précis et fiables.

L'accréditation ISO/IEC17025 prévoit des procédures d'inspections régulières pour s'assurer que les exigences prévues par la norme sont bien respectées.

Un laboratoire accrédité par cette norme répond également aux exigences de qualité du système de management déjà prévues par la norme ISO 9001.

Les laboratoires tentent ainsi d'obtenir l'accréditation ISO 17025 qui leur fournira un standard pour valider et pour garantir la fiabilité des résultats pendant le processus d'analyse de la preuve numérique.

Selon la norme 17025, la validation apparaît comme *« un équilibre entre les coûts, les risques et les possibilités techniques* » (clause 5.4.5.3- note 3).

En effet, en raison du coût élevé des recherches, du manque de temps ou de ressources, les travaux sur la validation des technologies d'investigations restent limités et il n'existe toujours pas de standards dans ce domaine.

L'une des difficultés constituant un frein à une demande d'accréditation est liée à son coût élevé, comprenant plusieurs types de dépenses comme des frais relatifs à la mise en place du système qualité, des redevances annuelles, des frais d'audit ou d'étalonnage annuel des équipements du laboratoire.

Le coût moyen d'une demande d'accréditation auprès de COFRAC est de l'ordre de 5000 € la première année et de 1000€ pour chaque renouvellement.
Cette procédure risque également d'être longue en fonction de la complexité du domaine.

La technologie connaît une évolution très rapide et il est difficile de mettre en place des procédures pour tester et valider tous les outils utilisés dans le domaine de l'investigation numérique.
La grande diversité de ces technologies d'analyses de preuve et les mises à jour régulières des logiciels rendent cette tâche d'autant plus compliquée.

La mise en place d'une méthodologie de tests nécessiterait alors des ressources techniques et financières importantes.

Les laboratoires d'analyses sont tenus de prouver la fiabilité de leurs résultats.
Ils peuvent obtenir un agrément pour démontrer qu'ils sont en conformité avec la norme ISO 17025, ce qui constitue une garantie du respect des normes et des méthodes déployées.

Aux Etats-Unis, depuis avril 2003, c'est le Comité d'accréditation des laboratoires de la société américaine des directeurs de laboratoires médico-légaux[57] qui a compétence pour accorder une accréditation en matière d'analyse vidéo, image, son ainsi que l'expertise des moyens de preuve informatique.

3.2 Exigences de la sécurité de l'information et la gestion d'incidents

3.2.1 La norme ISO 27002 (anciennement ISO : CEI 17799)

La norme ISO17799 créée en décembre 2000, est relative à la sécurité de l'information. Traitant de la « *gouvernance des systèmes d'information* », elle définit les principes directeurs de la gestion de la sécurité de l'information au sein d'un organisme pour élaborer les référentiels de sécurité.
Cette norme peut être associée aux bonnes pratiques et recommandations dans le domaine de l'investigation numérique.

3.2.2 ISO 27001 norme internationale intitulée « Technologies de l'information-Techniques de sécurité-Systèmes de gestion de sécurité de l'informations-Exigences »

Publiée en 2005, cette norme porte sur la gestion de la sécurité de l'information.
C'est la mise en place des mesures de sécurité pour garantir la protection des biens d'un organisme.

3.3 Exigences liées au respect de la méthodologie et l'intégrité de la preuve durant les phases d'investigation numérique

Quelques normes internationales proposent une harmonisation des méthodes de recherche et analyse de preuves numériques devant les juridictions.

Une nouvelle norme ISO/CEI 27037 intitulée « *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et*

---

[57] « ASCLD/LAB ».

la préservation de preuves numériques », publiée en octobre 2012, donne des lignes directrices concernant les différentes phases d'une investigation technique.

Les preuves informatiques sont par nature « *fragiles* », la fiabilité et la crédibilité de la preuve devant les juridictions dépendent du respect d'une méthodologie garantissant l'intégrité de la preuve des supports examinés[58].

La certification des pratiques d'experts ne permet pas de résoudre la problématique d'évaluation des technologies d'investigation.

La mise en place d'une procédure de validation des outils d'analyse de preuves numériques, nécessite de procéder à un inventaire détaillé de toutes les fonctionnalités et les exigences attendues par chaque logiciel.
Pour cela, il faut définir des protocoles de tests, en énumérant les différentes étapes, le matériel utilisé ainsi que les scenarii de tests.
Il est important de déterminer la fréquence à laquelle ces tests sont effectués, notamment à chaque nouvelle mise à jour de logiciel.

Les technologies utilisées au cours des investigations techniques sont en général très complexes.
Tester chaque nouvelle fonctionnalité ou chaque nouvelle version du logiciel peut s'avérer compliqué et laborieux.

Bien qu'il soit très important que chaque expert puisse vérifier par lui-même les limites et les capacités de ses outils, il est matériellement impossible qu'un seul expert puisse tester la totalité des modules disponibles par ses propres moyens et il est difficile de trouver un référentiel ou un modèle spécialisé dans le domaine de l'expertise en informatique.

La mise en place d'un groupe de travail permettra de générer une grille d'audit et de livrer un référentiel d'analyse pour garantir la fiabilité des outils utilisés.
L'objectif étant d'accompagner les experts dans la mise en place de leurs propres protocoles de tests, à partir d'un cadre et de méthodes déjà définies et validées.

Chapitre 4 - Tests et travaux de recherches

Aux Etats-Unis, l'Institut National des Normes et de la Technologie et le groupe de travail scientifique sur les preuves numériques, en organisant une série de tests de validation d'outils, ont tenté de proposer une méthodologie de validation des logiciels pour compenser l'absence d'harmonisation et de référentiels.
Cependant, ces expérimentations ne sont pas exhaustives et restent trop générales.

Les professionnels s'appuient souvent sur les tests de validation réalisés en interne par les éditeurs de logiciels.

S'agissant souvent de logiciels propriétaires dont la structure interne reste inconnue, les résultats des tests de validation ne sont pas communiqués au public.
Pour des raisons de compétitivité et celles relatives à la propriété intellectuelle, les expérimentations sont directement effectuées par les éditeurs de logiciels, réticents à publier le code source de leur programme.
Ils restent les seuls à réaliser de telles expérimentations car le comportement et la structure interne du système sont seulement connus par le testeur.

Ainsi, il sera impossible pour d'autres personnes de vérifier le bon fonctionnement d'un outil avec précision sans accès au code source.
La seule option envisageable est la mise en place de tests indépendants qui permettront de garantir l'exactitude des résultats produits par les logiciels d'analyse de preuves informatiques.

4.1 Travaux de l'Institut National des Normes et de la Technologie

L'Institut National des Normes et de la Technologie, basé aux Etats-Unis, réalise des tests de validation des outils d'analyse de preuve informatique avec son projet commun de « *tests des outils d'investigation numérique* » (CFTT).

---

[58] Maslina Daud, rédactrice de projet pour ISO/CEI 27037.

Pour garantir la validité et l'admissibilité de la preuve numérique, les résultats des tests doivent être fondés sur deux critères de "répétabilité" et "reproductibilité"[59]:

- « *La Répétabilité*» :

Un praticien qui réalise des tests en laboratoire doit obtenir les mêmes résultats en utilisant le même support et le même matériel.

- « *La Reproductibilité* » :

En appliquant la même méthodologie de tests sur le même support informatique, deux spécialistes travaillant dans différents laboratoires doivent obtenir des résultats identiques.

En 2001, l'Institut National des Normes et de la Technologie recensait approximativement cent cinquante outils utilisés par les professionnels du domaine de l'investigation informatique[60].
Le programme de tests CFTT est un projet commun entre trois organisations américaines, l'Institut National de la Justice, le Département de la Justice ainsi que l'Institut National des Normes et de la Technologie.
Son objectif est de mettre en place des méthodologies de tests afin de garantir la fiabilité des technologies d'investigations utilisées.
Ces outils sont classés en différentes catégories et des méthodes de tests sont développées pour chacune d'entre elles :

- Bloqueurs en écriture logiciels: Les tests sont réalisés entre 2004- 2008 différentes versions du RCMP-HDL[61], PDBLOCK[62] versions 2.00 et 2.10,

- Bloqueurs en écriture matériels: Plusieurs modèles de bloqueur Tableau Forensic et WiebeTech ont été testés entre 2006 et 2009 (De même pour FastBloc, ICS ImageMasster DriveLock, etc),

[59] "*General test methodology for computer forensic tools* », NIST 2001, page 4.
[60] Cftt.nist.gov/project_overview.htm
[61] Royal Canadian Mounted Police Hard-Disk Write Lock.
[62] Physical Drive Blocker.

- Analyses de téléphones mobiles: Les tests sont réalisés entre 2008 et 2015 sur plusieurs modèles et différentes versions de technologies d'analyse de téléphone portable : UFED Physical Analyser V3.9.6.7 XRY 6.10.1, Encase® Smartphone Examiner V7.10.00.103, Device seizure V5.0, Lantern V2.3, MPE+…

- Logiciels et matériels de copies Bit-à-Bit : Les tests sont menés entre 2002 et 2014: Tableau TD3 Forensic Imager 1.3.0, X-Ways Forensics 16.2 SR-5, ImageMasster Solo-4 Forensic, (safeback 2.18, Encase® 6.5, Encase® linen 5.05, FTK® imager 2.9.0, Logicube Forensic 2.43, Tableau Imager (TIM) version 1.1, Tableau TD1 Forensic duplicator,

Afin de réaliser des tests sur les technologies d'acquisitions physiques, l'Institut National des Normes et de la Technologie, dans le cadre du projet CFTT, a développé la suite logicielle FS-TST, composée d'une série d'utilitaires.
Ces programmes sont regroupés en quatre catégories et permettent de préparer, comparer, documenter les résultats et paramétrer les supports de test[63].

4.2 Recommandations générales du groupe de travail sur l'investigation numérique

Le groupe de travail scientifique sur les preuves numériques, a mis en place des lignes directrices pour la réalisation des tests de validation des technologies d'investigation informatiques.
Ces recommandations prévoient la définition de stratégies, de méthodologies et de mise en place des scénarii de tests.
Selon ce groupe de travail[64], dès la sortie d'une nouvelle version ou de mises à jour logiciel une procédure d'évaluation s'avère nécessaire.
La validation a pour objectif de déterminer si les outils d'analyse de preuves sont adaptés aux exigences attendues.

[63] « *FS-TST: Forensic Software Testing Support Tools* », Requirements, Design Notes and User Manual, NIST 2005.
[64] « *SWGDE recommended guidelines for validation testing* », version 2.0-septembre 2014.

Avant de commencer les tests, la première étape consiste à définir un ensemble de critères dans un plan de test, comme les objectifs, les exigences générales de vérification et les cas de tests.
Des scenarii de tests devront ensuite être préparés et les résultats seront reproduits dans un rapport de test.
Si des anomalies sont détectées, les causes doivent être identifiées et de nouveaux tests seront réalisés.

Le statut de réussite ou d'échec pour l'ensemble des tests est documenté.
L'une des métriques les plus connues en matière de validation de logiciels est relative à l'évaluation de la marge d'erreur de l'outil.
Dans la jurisprudence américaine, selon la décision "DAUBERT", l'analyse du « *pourcentage d'erreur et de la marge d'incertitude de la méthode* » constitue l'une des conditions de recevabilité de la preuve scientifique devant la justice américaine.

Concernant les technologies d'investigation, deux types d'erreurs[65] statistiques sont pris en compte :
- Le « *faux-positif* » : lorsqu'un outil identifie à tort un résultat positif alors qu'il est en réalité négatif.
- Un « *faux-négatif* » : lorsque l'outil ne parvient pas à détecter un résultat existant.

Si un test de logiciel échoue, il faut impérativement identifier l'erreur.
Mais l'existence d'une erreur ne discrédite pas l'outil, une certaine marge d'erreur est généralement acceptable.
Dans un document publié en 2008[66], le Groupe de travail scientifique sur les preuves numériques souligne que dans le domaine de l'investigation numérique, contrairement aux sciences criminalistiques, la notion de « *faux-positifs* » est inexistante.
Cependant, les résultats générés par les logiciels d'analyse de preuve numérique peuvent contredire cette affirmation, qui peut s'avérer erronée dans certaines circonstances.

[65] « If error rate is such a simple concept, why don't I have one for my forensic tool yet », J.R Lyle
[66] « *SWGDE standards and controls position paper* », version 1.0- 30 Janvier 2008.

Les programmes n'étant pas infaillibles, il peut arriver qu'un outil trouve des résultats faux-positifs.

A titre d'illustration, les recherches par analyse de signatures, la Stéganographie, l'analyse de programmes malveillants, les fichiers identifiés comme « *Orphan's files* » sur le logiciel FTK ou « *Lost files* » sur le programme Encase® sont autant de situations dans les quelles de tels résultats peuvent être rencontrés.

Un autre exemple peut être rencontré lors des analyses de signatures de fichiers.

Lorsqu'une telle analyse est effectuée par le logiciel Encase®, si l'en-tête d'un fichier au format « *txt* », contient la signature « *%PDF* », le résultat de l'analyse de signature présentera ce fichier comme un « **[Alias]* », indiquant que le document a une signature « * *Adobe PDF* ».

Cela montre que l'en-tête du fichier est connue dans la base de signatures mais pas son extension.

4.3 Validation par des organes indépendants

L'un des moyens d'évaluer la performance d'un logiciel d'expertise et de connaître ses capacités consiste à réaliser des tests indépendants et comparer les résultats générés par différents outils.

4.3.1 Travaux de Brian CARRIER

Brian Carrier, chercheur indépendant, a développé un programme intitulé « *évaluation des outils d'investigation numérique* » (DFTT) ayant pour objectif de mettre à la disposition du public plusieurs cas de tests.

Bien qu'il s'agisse d'une initiative intéressante, les tests mis en ligne sont anciens et insuffisants pour répondre à une demande croissante des technologies d'investigation.

4.3.2 Travaux de SLAY et BECKETT

Les travaux réalisés par Jill SLAY et Jason BECKETT en 2007 sont inspirés du modèle d'analyse CFSAP, développé par MOHAY dans lequel quatre critères

d'identification, de préservation, d'analyse et de présentation de la preuve numérique sont combinés avec les trois phases de « *sécurisation de la preuve numérique* », « *d'analyse* » et de « *présentation des données* » :

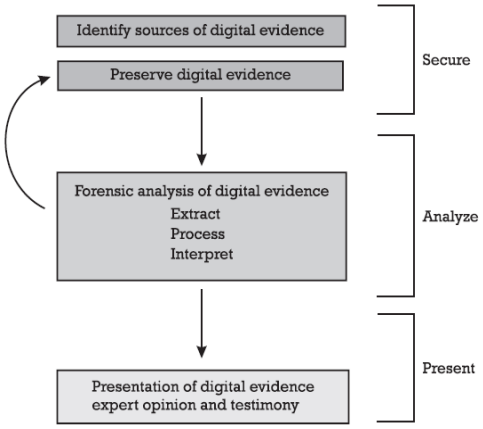


Figure 3.1 The CFSAP model.

Figure21- Le modèle CFSAP- Source[67]

SLAY et BECKETT ont mis l'accent sur deux concepts essentiels dans la recherche de preuve numérique que sont la « *préservation* » et « l'*analyse* » des données.
Pour chacune de ces phases, les auteurs ont identifié différentes sous-catégories :

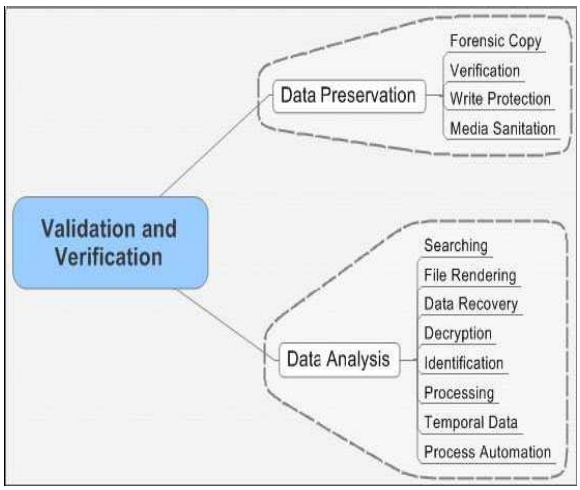


Figure22- Modèle de validation et vérification- source[68]

L'intérêt de cette méthode réside dans le fait qu'elle teste séparément chaque module présent dans un outil d'investigation technique.

[67] "computer and Intrusion forensics », MOHAY, page 129.

SLAY et BECKETT estiment qu'il faut préciser les spécifications d'une fonction et développer un ensemble de références dans lequel chaque cas de tests correspond à une fonction.

A titre d'exemple, la fonction de « *recherche par mots clés*» dans un logiciel d'expertise permet de retrouver sur le support examiné toutes les données contenant le mot clé choisi.

Avant de configurer une recherche par mots clés, plusieurs paramètres devront être pris en considération:

- Une recherche sur des lettres en majuscules ou en minuscules peut éventuellement avoir une incidence sur le résultat,
- Le mot clé recherché peut se trouver sur différents fragments du disque,
- Le mot clé peut être suivi ou précédé d'autres caractères ou de signes,
- Il peut se trouver à l'intérieur d'un fichier compressé,
- Le mot clé peut se trouver dans les métadonnées d'un fichier,
- Il peut être identifié parmi les fichiers effacés ou dans l'espace non-alloué du support informatique.

Pour évaluer la fonction de recherches d'un logiciel d'analyse de preuves, SLAY et BECKETT proposent un modèle en identifiant seize exigences[69]:

---

[68] « *Digital Forensics : validation and verification in a Dynamic work environment*», J.SALY & J. BECKETT.

[69] "Validation and verification of computer forensic software tools- searching function", Yinghua Guo, Jill Slay, Jason Beckett, S19.

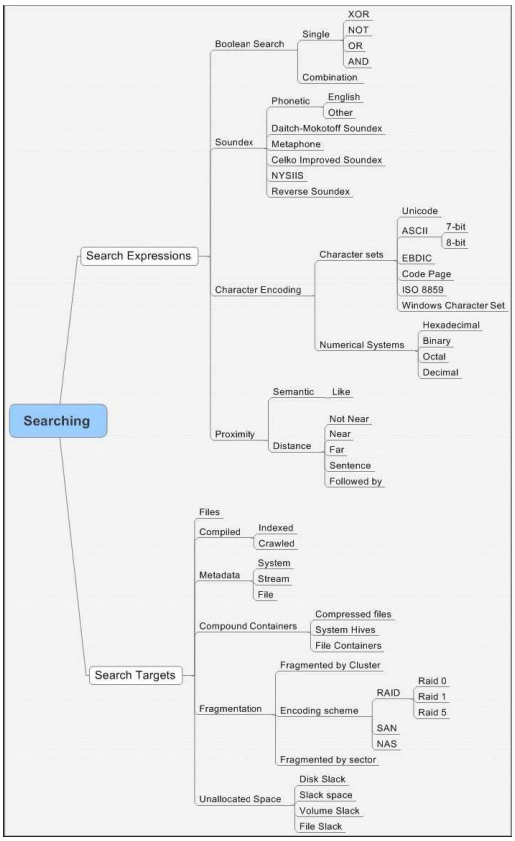


Figure23- Cartographie d'une fonction de recherche - source[70]

1. L'outil doit fonctionner au moins sur un système d'exploitation,
2. Il doit permettre à l'utilisateur de réaliser des recherches sur le fichier image du support original ou sur une copie physique du support numérique,
3. Le logiciel d'expertise doit mener les recherches sur différentes plateformes,
4. L'outil doit faire les recherches sur chaque système de fichiers,
5. L'outil doit permettre de procéder à une recherche par mots clés en texte intégral ou par indexation,
6. Le logiciel doit identifier les mots clés dans un fichier compressé,
7. Le logiciel doit retrouver les mots clés dans un fichier compressé sur l'espace non-alloué du support examiné,
8. L'outil doit être en mesure d'identifier le fichier recherché dans une zone non-accessible du support examiné,
9. Il doit identifier l'information recherchée dans les métadonnées,
10. L'outil doit trouver l'information par une recherche dite « Soundex » dans un fichier compressé,

11. L'outil doit retrouver l'information par une recherche « Soundex » dans un fichier compressé sur l'espace non-alloué du support examiné,
12. Le logiciel doit pouvoir trouver des informations en réalisant une recherche booléenne dans un fichier compressé,
13. L'outil doit identifier des données en faisant une recherche de proximité sur un fichier compressé,
14. Le logiciel doit retrouver des informations en réalisant une recherche booléenne sur les métadonnées,
15. L'outil doit récupérer des informations en réalisant une recherche de proximité dans les métadonnées,
16. L'outil doit pouvoir filtrer les fichiers en fonction de leurs attributs.

4.3.3 Travaux de BYERS et SHAHMEHRI

David Byers et le professeur Nahid Shahmehri de l'université de Linköping en Suède, ont mené une série d'expérimentations sur les logiciels Encase® version 6.8 et LinEn version 6.01 afin de tester les fonctions d'acquisitions d'images physiques.
Leurs travaux ont été réalisés entre 2007 et 2008 et la méthodologie proposée correspond à une approche systémique.

[70] « *Digital Forensics : validation and verification in a Dynamic work environment*», J.SALY & J. BECKETT.

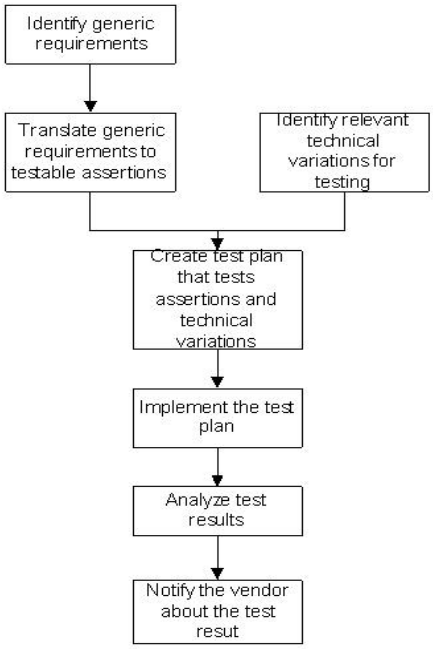


Figure24- Méthodologie de test de logiciel d'acquisition de données- source[71]

La méthodologie proposée est très proche de celle du projet américain de « *tests des outils d'investigation numérique* » de l'Institut National des Normes et de la Technologie.

Leur objectif est de déterminer si les logiciels d'acquisitions de données répondent bien aux exigences préalablement définies et produisent des résultats précis :

Les résultats des évaluations apportent les constats suivants sur les deux outils testés[72] :

- « *EnCase® 6.8 ne détecte pas les secteurs dissimulés et ne peut pas faire l'image physique des secteurs cachés* »,
- « *EnCase® 6.8 ne gère pas les disques avec plus de 25 partitions »,*
- *« EnCase® 6.8 rencontre des problèmes pour faire une image physique des partitions séparément avec une table de partition corrompue »*,
- « *LinEn 6.01 fonctionne uniquement en mode BIOS et non pas en mode ATA. Les secteurs cachés ne sont pas copiés en mode BIOS* ».

Il est regrettable que cette évaluation ne soit pas été réactualisée.

[71] « *Comparing the performance of three digital forensic tools* », Cusack & Liang.
[72] « *Disk imaging evaluation : Encase 6.8/LinEn 6.1 », Byers & Shahmehri*

4.3.4 Travaux de CUSACK et LIANG

En 2011, Brian CUSACK et James LIANG ont réalisés des tests de comparaison entre trois logiciels d'acquisition de données à l'université technologique d'Auckland en Nouvelle Zélande, tout en respectant les exigences de l'Institut National des Normes et de la Technologie.
Les tests ont été réalisés sur les logiciels « FTK® Imager » Version 2.9.0, « Helix3 Pro » et « AIR» Version 2.0.0.[73].

Les résultats des tests ont permis de mettre en évidence les limites de chaque outil. Aucun d'entre eux n'a été en mesure de réaliser une copie des secteurs cachés du disque dur.
CUSACK et LIANG ont souligné l'importance pour les praticiens de connaître les limitations de chaque outil et de les tester avant leur utilisation dans le cadre des expertises en informatique.

[73] « *Comparing the performance of three digital forensic tools* », Cusack & Liang.

Quatrième partie : EXPERIMENTATIONS ET PROPOSITION D'UNE METHODOLOGIE D'EVALUATION DES OUTILS D'ANALYSE JUDICIAIRE DE PREUVE NUMERIQUE

Chapitre 1 – Introduction

«*Un outil fiable est celui dont on comprend ce qu'il fait, comment il est fait, quels sont ses défauts et quels sont les résultats attendus* »[74].

L'évaluation d'un outil consiste à s'assurer qu'il exécute correctement les fonctionnalités attendues. Elle permet également de définir ses capacités et d'identifier ses limites.

En France, les tests de validation des logiciels d'analyse de preuves informatiques sont restreints.

En l'absence d'instances officielles permettant de conduire ce type d'évaluations, il est nécessaire de mettre en place une procédure claire pour réaliser des tests indépendants sur ces outils.

Le comportement de chaque outil doit également être étudié en fonction du type de technologie utilisée.

Avec l'apparition de nouveaux supports, les techniques de recherches et d'investigations évoluent et peuvent présenter certaines limites.

Il est donc important de mettre en évidence les outils adaptés pour tel ou tel type d'analyse.

Nous proposons une méthodologie d'évaluation d'outils d'analyse de preuves numériques. La procédure est applicable aux différents modules des logiciels d'expertise.

[74] *Chris Pogue (présentation SANS 2010 "Forensics & incident response summit").*

Cette approche d'évaluation prend en considération plusieurs éléments :
Une première phase consiste à comprendre la structure géométrique des supports magnétiques et disques électroniques.
Cela permettra d'identifier leur complexité et les difficultés rencontrées lors de leur analyse.
Des précisions sur le concept de « *l'intégrité des données* », principe essentiel dans la conduite d'une investigation technique, seront apportées.
Le plan de test va ensuite permettre d'évaluer le module de récupération des données effacées du logiciel « Encase® Forensic » version 6.18.1 et version 7.06.

Chapitre 2 – Etude de la structure géométrique des disques durs classiques et des nouveaux formats de disques

L'apparition de nouveaux types de mémoires de masse a complexifié le paysage de l'investigation numérique.
Les méthodes traditionnelles d'analyse de preuves sur ces supports paraissant inadaptées. La compréhension de leur géométrie et l'identification de leur différence avec les disques durs magnétiques permettent de prendre les dispositions adéquates dans le cadre de l'expertise de ces nouveaux formats de disques.

2.1 La technologie magnétique et les méthodes d'accès aux zones dissimulées des disques durs

Le « *RAMAC 305* » est le premier ordinateur équipé d'un disque dur référencé « *IBM 350* » qui a été commercialisé en septembre 1956 par IBM[75].
Les disques durs classiques existant sous leur forme actuelle ont été mis sur le marché en mars 1973.
Il s'agissait du disque « *IBM 3340* », baptisé « *Winchester* », qui contenait deux disques dont chacun avait une capacité de stockage de 30Mo.

[75] www.03.ibm.com

Depuis, ces supports informatiques continuent d'évoluer et nécessitent de grandes capacités de stockage.
Pour procéder à une recherche de preuve sur ces supports, il est primordial de comprendre le technologie magnétique, le système des fichiers et la gestion des données.

2.1.1 La capacité des disques durs magnétiques

Les disques durs magnétiques sont constitués de plateaux tournant autour d'un axe ainsi que de têtes de lectures et d'écritures qui enregistrent les données sur des cylindres en système binaire. Leur vitesse de rotation varie entre 4 800 et 15 000 tours.

Ces supports disposent de deux méthodes d'adressage pour localiser les secteurs sur le disque. Il s'agit des schémas « *CHS* » utilisant les trois coordonnées « *cylindre-tête-secteur* » et « *LBA* » qui est une recherche par numéro de secteur.

Cette méthode d'accès aux données est très importante, notamment dans les hypothèses de calcul de la capacité de stockage, de la détection des zones dissimulées et de la réalisation d'une copie de tous les secteurs d'un disque dur.
Sous Windows, la capacité affichée d'un support magnétique est toujours inférieure à celle référencée par l'étiquetage du constructeur.
Les méthodes de calcul des capacités de stockage des disques durs diffèrent entre les fabricants de disques durs, qui calculent en base décimale, et le système d'exploitation, qui compte en base binaire.
Les deux systèmes sont utilisés conjointement, ce qui est souvent source de confusions.
Prenons l'exemple d'un disque dur dont le fabricant affiche une mémoire de 500 Go, il ne dispose en réalité que d'une capacité de stockage de 465,6 Go.

A part ces différences de calcul, il faut aussi tenir compte de l'affichage d'informations erronées par Windows concernant l'espace disponible ou la mémoire utilisée sur le support de stockage.

En effet, pour calculer l'espace utilisé sur un disque, l'explorateur Windows ne prend pas en compte certains fichiers comme le « *Volume Shadow* » contenant les points de restaurations systèmes.

2.1.2 Techniques de dissimulation par les constructeurs

Plusieurs techniques permettent de dissimuler des données sur un disque dur telles que le chiffrement, la Stéganographie, la manipulation d'extensions ou d'en-têtes de fichiers, etc.

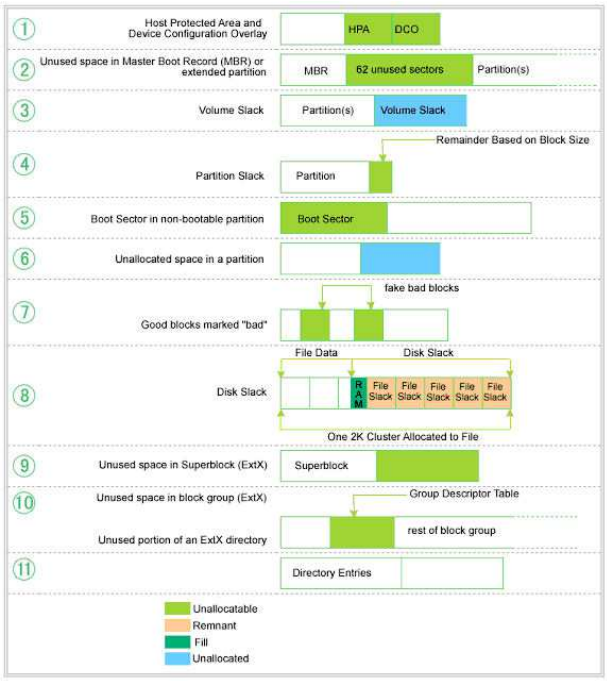


Figure25- Différentes techniques de dissimulation des données- source[76]

D'autres méthodes consistent à rendre une partie du disque dur inaccessible.
les constructeurs de disques communiquent très peu d'informations sur les fonctionnalités cachées des « zones constructeurs »[77] dites « *Service Area* », « *HPA* » ou « *DCO* »[78].
L'utilisation de ces zones pourrait également permettre à un utilisateur de dissimuler certaines données.

[76] *"Data Hiding Tactics for Windows and Unix File Systems", Hal Berghel, David Hoelzer et Michael Sthultz.*
[77] « *Indiscrétions et zones constructeurs des disques durs* », Laurent DUPUY, SSTIC,
[78] « *Hidden disk areas : HPA and DCO* », 2006.

- **La zone dite « *Service Area* »**:

Des spécialistes en sécurité ont découvert une nouvelle technique qui permet de dissimuler des données sans qu'elles ne puissent être détectées dans une zone du disque dur dite « service area » [79].

La plupart des outils d'investigation ne donnent pas accès à cette zone protégée du disque dur.

Des outils de récupération de données avancées comme le PC-3000 UDMA des laboratoires ACE, utilisant les commandes constructeurs, permettent d'accéder à cette partie du disque dur.

Cet espace caché du disque dur contient des informations sur l'état du support, le microcode, le numéro de série, les secteurs défectueux rencontrés en usine et ceux découverts après l'utilisation du support de stockage.

- **La zone dite « *HPA* »** :

La zone « *HPA* » introduite avec le standard ATA-4 est une zone protégée du disque dur par le constructeur.

Invisible par le BIOS et le système d'exploitation, elle permet aux fabricants de sauvegarder des données de récupération et de sécurité.

Elle peut être modifiée par l'intermédiaire d'utilitaires faisant appel aux commandes utilisées par les fabricants de disques durs.

Les trois commandes ATA « IDENTIFY DEVICE», « SET MAX ADDRESS» et « READ NATIVE MAX ADDRESS» permettent d'accéder à cette zone cachée du support.

Cette zone peut également être créée par un utilisateur malveillant afin de cacher des données ou pour introduire des malwares dans le but d'obtenir un accès non-autorisé à l'ordinateur d'un tiers.

Dans le cas de dissimulation d'un « *Rootkit* » dans cette zone du disque dur, celui-ci sera indétectable par un antivirus de la victime.

La zone «HPA», surtout prévue par le constructeur, peut être préinstallée sur le disque dur d'un ordinateur.
Elle est notamment présente sur les ordinateurs portables de la marque IBM « Thinkpad » et contient les outils de diagnostic, de sauvegarde, et les fichiers de restauration du système d'exploitation[80].
De même, sur les disques du fabricant Samsung, l'application « *Samsung Recovery Plus*», permet de restaurer le système en cas de problème à partir de la partition cachée du disque [81].

Les programmes qui ouvrent l'accès à cette zone interviennent pendant le démarrage du système.
Le BIOS démarre le système via cette zone afin de résoudre les problèmes de démarrage et de récupération de système.

La zone « *HPA* » est seulement accessible par la technologie « *BEER* », qui réside dans l'en-tête du « *HPA* » et sur le dernier secteur du disque dur.

Tous les outils d'investigation numérique ne permettent pas de détecter la zone « *HPA* ».
Contrairement au logiciel Encase® qui détecte le HPA, le programme FTK Imager ne permet pas de réaliser une copie de la zone « *HPA* » du disque dur.
Du point de vue de l'expertise technique, il est important de détecter cette zone pour la copier par l'intermédiaire des commandes ATA.
Un disque en mode « *HPA* » peut être détecté par une comparaison entre les résultats du nombre total de secteurs d'un disque dur, affichés par les commandes constructeurs et le nombre de secteurs accessible à l'utilisateur.
La constatation d'un écart entre ces deux valeurs peut s'expliquer par la présence d'une zone cachée.
Cette protection peut être supprimée de façon temporaire ou de manière définitive, mais dans ce dernier cas des modifications sont apportées dans la « *zone constructeur* » du disque dur.

---

[79] « *Hiding data in hard drive's service areas*», Ariel Berkman, 2013.
[80] « *IBM Hidden Protected Area* », 2003.

- **La zone « *DCO* »**:

Introduite avec la norme ATA-6, la zone « *DCO* » permet de configurer un disque avec les mêmes caractéristiques qu'un disque dur de capacité inférieure.
A l'instar de la zone « *HPA* », la « *DCO* » est également créée à la fin du disque dur. Inaccessible par le BIOS, un simple formatage ne suffit pas à supprimer cet espace.
Plusieurs méthodes permettent de faire une acquisition des supports et accéder aux zones cachées.
L'utilisation du logiciel « LinEn », appelé également « Linux Encase® », permet de détecter ces zones protégées « *HPA* » et « *DCO* ». Pour cela, il est important d'utiliser une version récente du logiciel inclus dans le programme « Encase® ».

2.1.3 Copie physique des secteurs cachés d'un disque dur et la question du respect de l'intégrité du support original

Dans le cadre des investigations judiciaires, tous les outils utilisés pour faire des acquisitions d'images de disques durs n'ont pas la capacité de détecter et de copier la zone protégée du disque dur dite « *HPA* ».
Bien que des logiciels comme « *Prodiscover* », « *X-ways Replica* » ou « *Snapback* » disposent tous de cette fonctionnalité avancée, à contrario, le logiciel FTK ne peut pas accéder à cette zone.
Pour réaliser un clone avec le logiciel FTK, il faut au préalable recourir à un autre outil que « *FTK Imager* » pour supprimer la zone protégée du disque dur.

Le logiciel Encase® prévoit cette option depuis la version cinq du programme.
Toutefois, si une image disque contenant une zone « *DCO* » est créée avec un autre logiciel d'investigation, le logiciel Encase® ne sera pas en mesure de la détecter.

Dans les versions 6.18 et 7 du programme, lorsque la protection « *DCO* » est activée ou si les protections « *DCO* » et « *HPA* » sont conjointement configurées, elles doivent être définitivement supprimées avant la réalisation de toute copie de disque dur.

---

[81] www.samsung.com

Dans la version Encase® 7, le bloqueur en écriture "FastBloc SE", détecte ces deux protections sur les disques durs lorsqu'elles sont activées dans le programme.

L'utilisation de certains dispositifs de blocage en écriture peut toutefois empêcher Encase® de les détecter.
Le résultat des tests réalisés aux Etats-Unis en 2009 par l'Institut National de la Justice sur le logiciel Encase® version 6.5 montraient que certains bloqueurs en écriture tel que « FastBloc FE » ne détectaient pas les zones protégées.
Cela empêchait le logiciel Encase® de copier les secteurs cachés du disque dur[82].

Des problèmes d'incompatibilités entre certaines technologies d'investigation et des disques durs peuvent également survenir.
A titre d'illustration, le duplicateur TD1 de marque « Tableau » présente des limitations avec certains disques durs[83].
Cette incompatibilité empêche le duplicateur de supprimer la protection « *HPA* » et « *DCO* ».

Dans le cas de l'utilisation du bloqueur en écriture de marque « Tableau » lors de l'acquisition de l'espace « *HPA* » et « *DCO* », le pilote de l'appareil devra être mis à jour pour que les deux protections puissent être détectées.

Lorsqu' une copie physique du disque dur est réalisée avec le bloqueur en écriture de marque « Tableau » et le logiciel Encase®, si une zone « *DCO* » est détectée, le bloqueur proposera à l'utilisateur de la supprimer définitivement.
Si cette option est activée, elle entraînera une modification du contrôleur de disque.

[82] « Tests results for digital data acquisition tool: Encase 6.5», NIJ, 2009
[83] Selon les tests réalisés par « tableau », le disque dur Samsung MCBQE32G8MPP 32Go micro-SATA pose des problèmes d'incompatibilité.

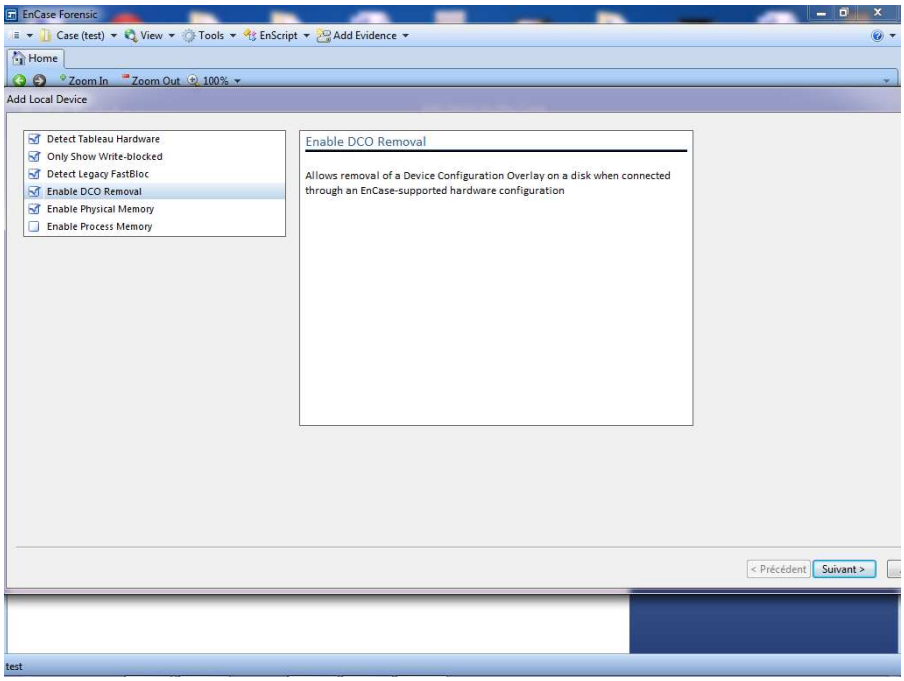


Figure 26 - Activation de la suppression de la protection DCO, logiciel Encase® V7

Même si cette modification n'a aucune incidence sur le contenu du disque dur, il s'agit néanmoins d'une altération du disque original.
Il est important que cette information soit mentionnée dans le rapport d'expertise.
En effet, le respect de l'intégrité des données d'un support original constitue un principe élémentaire en matière d'investigation numérique.

Il est important de garantir que l'outil n'apporte aucune altération au support original et respecte ainsi son authenticité.
Cependant, l'évolution technologique et l'apparition de nouveaux supports révolutionnant le monde de l'expertise nécessitent de définir de nouvelles procédures en matière d'analyse de supports numériques.
L'expert est tenu de documenter ces éléments, mettant en exergue que le changement apporté est nécessaire et n'entraîne pas une altération du support.

2.2 Problématique de l'expertise des disques au format avancé (AF)

En 2009, les fabricants membres de L'IDEMA ont décidé d'introduire sur le marché un nouveau format de disques durs, remplaçant progressivement la taille des secteurs de 512 octets par les secteurs physiques de 4096 octets.

Ils considèrent que le format antérieur des disques durs, utilisé pendant plus de trente ans constitue un frein à l'amélioration de leur capacité de stockage et à l'optimisation de la correction d'erreurs sur ces supports.

Ce nouveau format regroupe huit secteurs de 512 octets en un seul secteur de 4 096 octets, appelé « *secteur de 4K* ».
Les secteurs élargis permettent d'augmenter l'efficacité du stockage sur les plateaux et offrent de meilleurs performances pour les corrections d'erreurs pendant le processus de lecture et d'écriture.
Certains constructeurs de disques durs comme WESTERN DIGITAL estiment cette augmentation de capacités entre 7% et 11%[84].
En attendant l'application de cette nouvelle norme par l'ensemble du marché, les constructeurs ont préparé la transition vers les secteurs élargis avec la technique de l'émulation de secteurs de 512 octets.

Deux types de disques durs au format avancé doivent être distingués:
Les supports qui sont nativement conçus pour les secteurs 4K, et ceux qui utilisent une technologie transitoire de l'émulation 512 qui facilite la communication entre les anciens systèmes et les nouveaux formats de disques à secteurs 4K.
Certains d'entre eux sont néanmoins susceptibles de poser des problèmes de performance ou d'alignements entre le système de fichier et les disques à secteur 4K.

Sur les disques durs au format avancé, la partition commence au début d'un secteur de 4K alors que sur les systèmes anciens comme Windows XP la première partition commence à partir du secteur 63.
Les systèmes d'exploitation anciens créent des partitions en supportant la taille standard

[84] « *Exploring WD's Advanced Format HD Technology* », 2010, www.hothardware.com

des secteurs 512 octets et sont incompatibles avec le nouveau format de secteur physique à 4Ko.
Des utilitaires spécifiques d'alignement de secteurs 4K sont proposés par les fabricants qui permettent de résoudre des problèmes de communications avec le système d'exploitation afin d'identifier le type de formatage utilisé.

Dans l'environnement Windows, la gestion des secteurs de ces formats de disques durs varie en fonction des versions du système d'exploitation.
Des mises à jour logiciels pour la compatibilité de Windows sept et Windows Server 2008 peuvent être installées lorsque les pilotes de stockage ne prennent pas en charge la taille des secteur 4Ko.

Ce nouveau format peut susciter des interrogations relatives à la recherche de preuves et l'utilisation des logiciels d'investigation numérique.
A cette effet, nous avons tenté d'analyser un disque dur externe de marque Iomega composé d'un disque dur du type SATA 2,5'' de marque SAMSUNG 1To, modèle HM100UI avec le numéro de série : S2GHJ9EB319278.

Le disque dur externe a été connecté à un ordinateur fonctionnant sur le système d'exploitation Microsoft Windows XP Professionnel service Pack3.
Il est réparti en deux partitions:
- Une partition NTFS avec une capacité de stockage de 930 Go dont 886 Go sont utilisés,
- Une partition CDFS système (lecteur CD virtuel) avec une capacité de stockage de 81,1 Mo qui contient le logiciel de chiffrement « *IomegaEncryptionSetup.exe* ».

Le disque dur SATA, extrait du boîtier externe, a été ensuite connecté au bloqueur en écriture Tableau T35E avec l'interface SATA/IDE.
Nous avons tenté de monter la partition afin de réaliser une copie intégrale du support original et naviguer dans le contenu de l'image.
Pour analyser ce disque dur, les logiciels « *Encase*® version 6.18.1 et version® 7.06 ont été utilisés.

2.2.1 Encase® version 6.18.1

Le logiciel Encase® n'a pas pu reconnaître le disque dur. Il a rencontré un bogue et a cessé immédiatement de fonctionner.

La même expérience a été renouvelée sur un autre ordinateur de test fonctionnant sous Windows 7 Professionnel.
De même que sous Windows XP, Encase® a cessé de fonctionner et Windows a subitement fermé le programme.

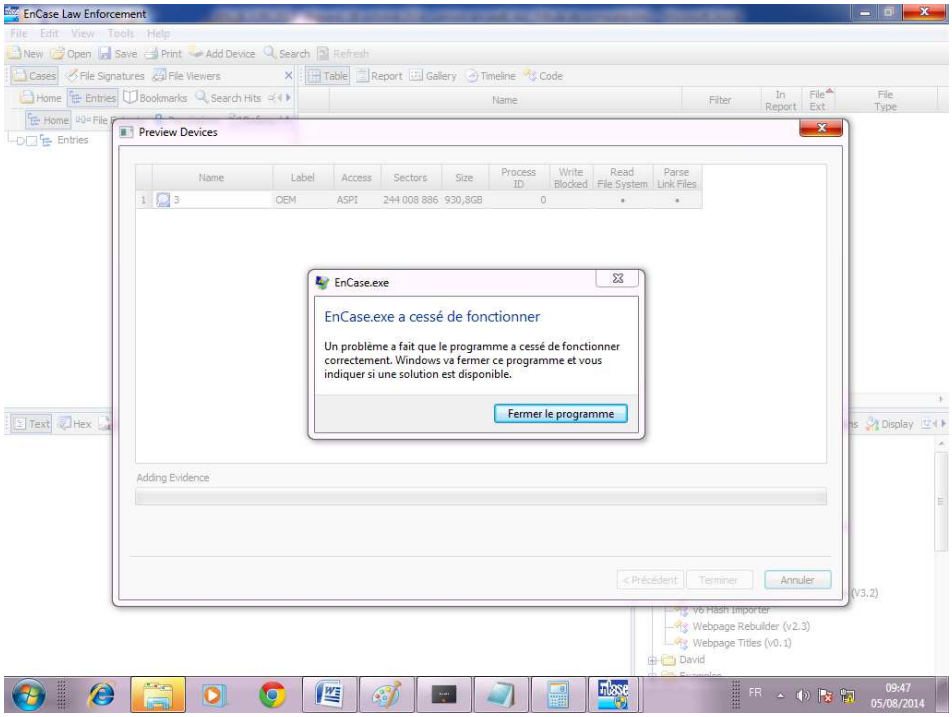


Figure27- capture d'écran du message d'erreur dans Encase® V6

Sur des systèmes anciens comme le Windows XP, le disque dur n'est reconnu ni dans l'explorateur Windows ni dans la gestion des disques.
Il apparaît alors comme une partition inconnue et non initialisée.
Il semble qu'en raison des problèmes d'alignement entre les secteurs physiques et logiques, Windows ne peut pas montrer la partition dans son explorateur.

2.2.2 Encase® version 7.06

Contrairement à la version six du logiciel Encase®, les disques durs au format avancé sont pris en charge par la version sept du programme.

Après avoir connecté le disque dur de test a un ordinateur fonctionnant sous Windows sept, une copie du support a été réalisée avec la version sept du programme Encase®.

Il a été protégé en écriture avec le logiciel FastBloc SE, faisant partie intégrante d'Encase®.

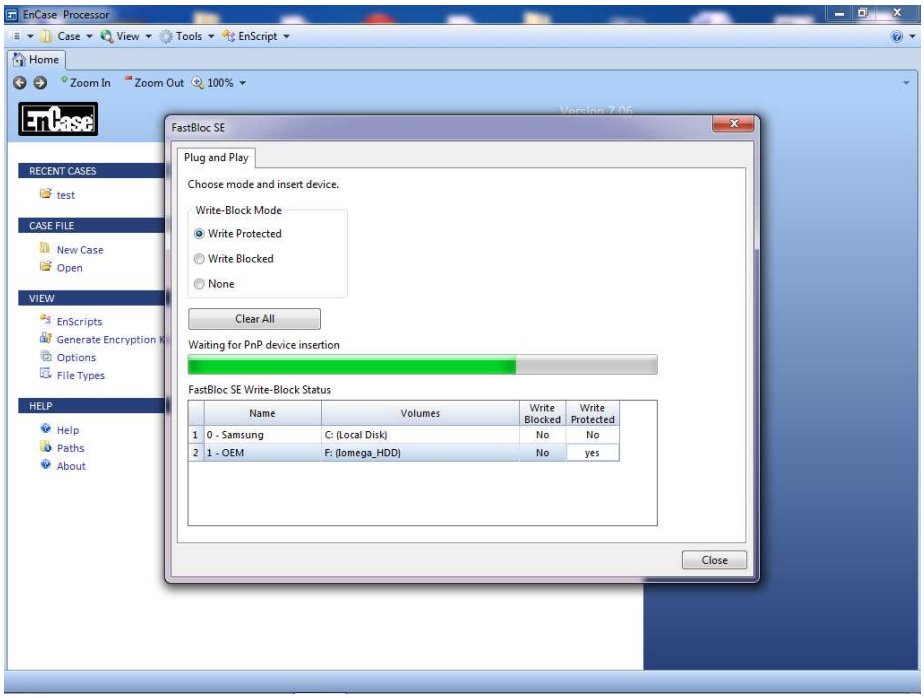


Figure 28- Bloqueur en écriture FastBloc SE, Encase® V7

Après avoir essayé de visionner le disque dur depuis l'interface Encase®, le logiciel a montré son contenu sans aucune difficulté et aucun bogue.

La version sept du programme bien compatible avec les disques durs au format avancé, permet également de déterminer si un disque est au format 4K.

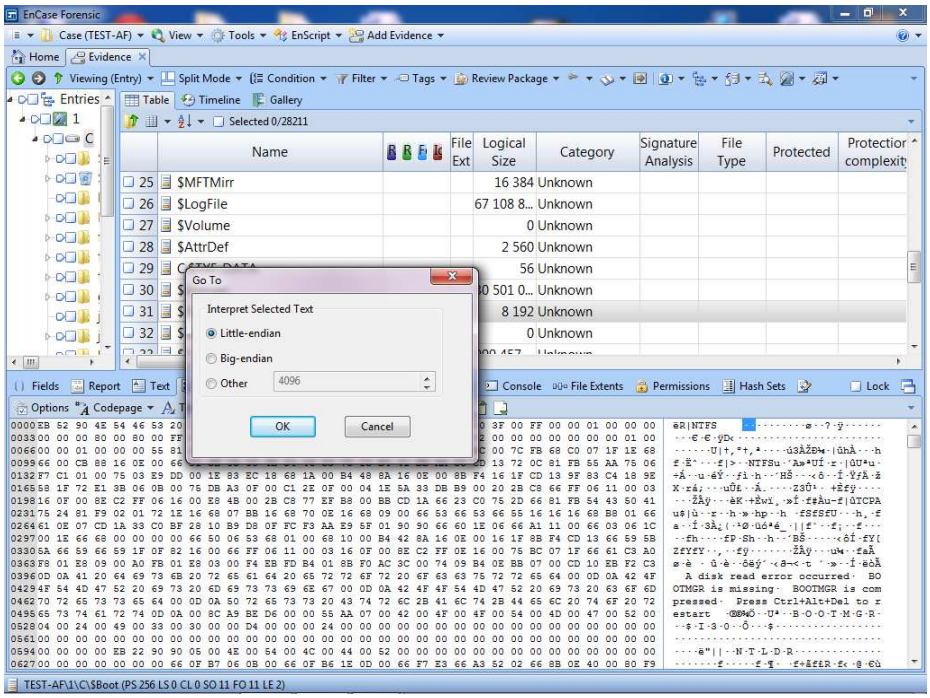


Figure 29- Aperçu du secteur 4K, Encase® V7

2.3 La complexité de la recherche de preuve sur les supports SSD

Les disques SSD révolutionnent le monde informatique et plus particulièrement le domaine de l'expertise judiciaire pour lequel l'analyse et la recherche de preuves nécessitent la mise en place de nouvelles techniques d'investigations.
Cette technologie sophistiquée est totalement différente de celle utilisée jusqu'ici pour les disques durs magnétiques.

La conception classique d'écritures et d'effacements des données se trouve complètement bouleversée[85] et les techniques traditionnelles d'analyse et de recherches de preuves deviennent inadaptées pour ces nouveaux supports.

« *L'âge d'or de la récupération et de l'analyse des données effacées touche ainsi à sa fin* »[86].

[85] « *Solid State Drives : The begining of the end for current practice in digital forensic recovery ?* », Graeme B.Bell and Richard Boddington, 3 novembre 2010.

Pour la mise en place d'une procédure d'analyses des supports SSD, les_praticiens doivent avoir une bonne connaissance des technologies utilisées et prendre en considération les spécificités techniques de ce type de matériels.

2.3.1 Description de l'architecture des disques SSD et leurs caractéristiques techniques

Le terme anglais « *Solid State* » fait référence aux composants électroniques à semi-conducteurs, inspirés des circuits électroniques utilisés par les récepteurs radio dans les années cinquante.

Ces Supports de stockages sont plus rapides et plus résistants que les disques durs classiques. Ils sont de plus en plus répandus dans les ordinateurs individuels et se démocratisent.

Selon Gartner, le marché des disques SSD a atteint près de 11 milliards de dollars en 2013, les cinq premiers fournisseurs étant respectivement Samsung, Intel, Sandisk, Micron Technology et Toshiba.

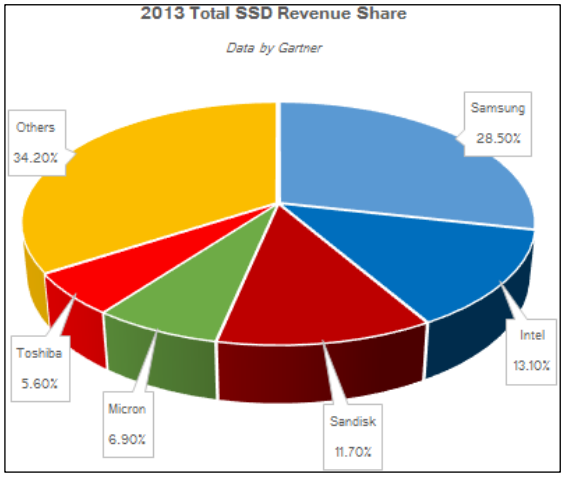


Figure 30- Schéma publié par Gartner- source[87]

L'utilisation d'une technologie totalement différente de celle des disques durs classiques rend l'analyse ainsi que l'extraction des données plus complexes et soulève des interrogations majeures sur la processus technique.

---

[87] www.kitguru.net, « « *Samsung remains the world's largest maker of SSDs-Gartner* », Anton Shilov, 4 juillet 2014.

Entièrement électroniques, ces nouveaux supports n'intègrent aucune pièce mécanique mobile. Ils ne disposent pas de tête de lecture ni de plateaux en rotation et l'accès aux données est plus rapide.
Ils sont plus performants, consomment moins d'énergie et sont résistants aux chocs.
Mais en raison du nombre limité de cycles d'écritures et d'effacements leur longévité est plus courte.
Composés de mémoire flash NAND développée par Toshiba en 1989, les supports SSD utilisent les trois types de puces mémoires SLC « *Single Level Cell* », MLC « *Multiple Level Cell* » ou TLC « *Triple Level Cell* ».

Dans les mémoires du type MLC chaque cellule peut stocker plusieurs bits de données. Les mémoires flash NAND du type SLC, quant à elles, stockent un bit par cellule et chacune fonctionne à deux niveaux de tensions[88].
Elles sont plus rapides et disposent des performances élevées en cycles de lectures et d'écritures.

Avec la technologie Flash, les cycles d'effacements et d'écritures sont complètement différents sur les SSD car une cellule de mémoire flash NAND ne peut pas être réecrite. Elle nécessite que les données soient d'abord effacées avant d'être écrites à un nombre limité de cycles.

Les unités d'adressages physiques utilisées par les contrôleurs de disque sont les pages et les blocs.

L'unité de base pour l'écriture des données est la "page" répartie en zone de données et zone de service etsa taille est généralement comprise entre 1 Ko et 4 Ko.
La mémoire flash NAND ne peut pas écraser les données existantes dans une page, la moindre écriture nécessite un effacement complet du bloc de données avant d'écrire une nouvelle valeur.
Il est difficile de connaître l'emplacement d'écriture d'un fichier sur ce type de disques.

[88] « *Pourquoi les disques SSD sont des solutions révolutionnaire* », livre blanc sur les disque ssd samsung.

2.3.2 Présentation des fonctions avancées des SSD

Lors de la mise sous tension du support SSD les données sont réorganisées.
Intégrés dans les SSD modernes, les algorithmes sophistiqués de la « *gestion de l'usure* » et du « *Garbage Collector* » rendent la récupération des données très difficiles.
La commande « *TRIM* » compatible également avec certains systèmes d'exploitation complique la reconstitution des données sur ce type de supports de stockage.

2.3.2.1 Algorithmes de gestion de l'usure:

Un disque SSD utilise des algorithmes de gestion de l'usure implémentés par les constructeurs, dans le but de limiter l'usure de la mémoire flash et d'augmenter la durée de vie du support.
Cette technique permet de répartir le nombre d'écritures et d'effacements sur la totalité de la mémoire.
En effet, une utilisation fréquente des mêmes cellules risquerait de les rendre inutilisables.
Ce processus de gestion des données consiste à minimiser l'usure en diminuant le nombre d'effacements de chaque bloc. Il permet de s'assurer que chaque cellule contient des données de manière uniforme.

Pour éviter que les écritures interviennent toujours sur les mêmes blocs, le contrôleur va répertorier leur nombre et déterminer leur fréquence d'utilisation.
Avant l'effacement d'un bloc de données, son contenu doit être lu dans une mémoire temporaire et les informations vont prioritairement être écrites sur les blocs les moins utilisés.
Ce mécanisme qui contribue à la longévité des disques SSD, représente néanmoins un frein pour la récupération des données supprimées.

La technique dite d'«*Over-Provisioning*» permet également de redimensionner l'espace non-alloué de la mémoire et d'augmenter la durée de vie des SSD.
Ainsi, une partie de la capacité du disque peut être réservée au niveau du contrôleur par le fabricant ou être allouée par l'utilisateur en effaçant l'espace préalablement prédéfini.

La fonction de nettoyage du disque utilise l'Overprovisioning pour gérer les blocs contenant des données invalides.
Ce processus profite des périodes de faible activité du disque pour redimensionner les partitions.. L'intérêt étant de garder un espace disponible en mémoire et d'ajuster la quantité d'espace non-alloué réservée sur un disque.

2.3.2.2 Algorithme de « Garbage Collector » :

Depuis plusieurs années, les spécialistes soutiennent que les supports SSD autodétruisent définitivement la preuve informatique.
Le terme anglais "*Garbage Collector*" traduit en français par les expressions « *ramasse-miettes* » ou « *algorithme de nettoyage de la mémoire* » est un mécanisme incorporé dans certains contrôleurs de disques SSD dont le rôle consiste à identifier les blocs de mémoires non-utilisés pour rendre l'espace de stockage accessible.
C'est une tâche automatisée, exécutée en arrière-plan des disques permettant de détecter les pages à effacer pour libérer des blocs.
Ce procédé, assez proche des programmes de défragmentation, intervient en arrière plan pour réorganiser les données au sein de la mémoire Flash. Il profite de ses périodes de moindre activité pour accélérer la vitesse d'écritures et d'optimiser l'espace libre du disque.

Sur un disque dur magnétique, un fichier effacé n'est pas réellement supprimé, le système de fichier indique seulement que son emplacement est disponible.
Sur un disque SSD, dès l'instant où le fichier est effacé, le « *Garbage Collector* » procède à un effacement permanent du fichier destiné à être supprimé.
Le bloc contenant l'ancien fichier sera entièrement effacé et devient disponible par le processus de "*Grabage Collector*".

De nombreux auteurs font état de la perte des données sur un SSD même pendant la copie physique du support.
Ils constatent que le fait de connecter un SSD à un dispositif de blocage en écriture peut représenter un risque d'altération des données durant le processus d'acquisition.

D'autres spécialistes ont tendance aujourd'hui à soutenir le contraire de ces affirmations[89].
De interrogations sont alors soulevées concernant la préservation de la preuve durant la phase d'acquisition des données.

Ces affirmations doivent néanmoins être nuancées en ce sens que tous les supports SSD n'ont pas un comportement similaire et cela peut dépendre particulièrement du modèle ou du contrôleur de disque utilisé[90].
La configuration de la commande « *TRIM* » renforce également ce processus d'effacement fragilisant ainsi la préservation des données.

2.3.2.3 La commande TRIM :

Il s'agit d'une commande ATA créée afin d'augmenter la vitesse en écriture et d'améliorer les performances des supports SSD.
La « *TRIM* » est envoyée au contrôleur de disque par le système d'exploitation qui lui permet d'indiquer quels sont les blocs de données inutilisés et si le disque peut procéder à leur effacement.
Sur les disques SSD, la table d'allocation n'étant pas synchronisée avec le système de fichier, il est donc difficile de connaître l'emplacement d'écriture sur le support.
La commande « *TRIM* » permet au SSD de mettre à jour sa table et connaître les cellules vides.
Elle permet au système d'exploitation de prévenir le SSD lorsqu'une plage de mémoire est effacée et c'est le « *Garbage Collector* » qui procédera à la suppression des données.
Mais la « TRIM » ne fonctionne que si elle est supportée par le système d'exploitation et les pilotes du contrôleur de la carte mère doivent également être compatibles.
Les interfaces SATA et eSATA supportent la commande tandis que les connexions USB, LAN ou FireWire ne sont pas compatibles.
Sous Windows, les versions antérieures à Windows Sept ne supportent pas

[89] "La récupération de données sur SSD: un défi", Thomas Souvignet, Matthieu Regnery, mars 2013.
[90] "Recovering Evidence from SSD Drives in 2014...", Belkasoft, 23 novembre 2014.

nativement la « *TRIM* ».
Les systèmes de fichiers formatés sous NTFS sont compatibles avec cette technologie tandis que les systèmes FAT ne la supportent pas.
Linux reconnaît toutefois cette commande même sur les volumes formatés en FAT.

Tous les SSD ne détruisent pas la preuve numérique. Il faut faire une distinction entre les supports récents disposant de la fonction de « Garbage Collection » et ceux qui en sont dépourvus qui n'effacent pas les données de façon automatique.

2.3.3 Recommandations techniques de recherche de preuves sur les supports SSD

A l'heure actuelle, il n'existe pas de standards relatifs à la gestion des données sur les supports SSD et le fonctionnement de l'algorithme de « *Garbage Collector*» dépend des paramètres mis en place par chaque fabricant.

La récupération des données sur ces supports représente un vrai défi pour les spécialistes[91] et les méthodes d'investigation dépendent de leurs caractéristiques techniques.
La procédure traditionnelle d'acquisition physique des disques durs et les moyens d'investigations classiques semblent dépassés.
La proposition d'une nouvelle procédure d'analyse de ces disques s'avère nécessaire.

La recherche de preuves sur les SSD, suscite de nombreuses interrogations liées notamment à la préservation de l'intégrité de la preuve qui constituant un principe fondamental et un élément indispensable à l'expertise en informatique dont le non-respect risque de rendre la preuve irrecevable devant la justice.

Le problème des disques SSD est qu'il est difficile de garantir avec certitude la préservation des données durant une analyse post mortem ou sur un « système vivant ».
Dans certains cas, l'utilisation d'un dispositif de protection des données semble être inefficace.

De plus, les résultats de l'empreinte numérique du support original pourrait ne pas être identiques à celui de la copie.
Afin d'adopter une méthodologie adaptée, il est primordial de maîtriser des concepts de la gestion de l'usure, de l'algorithme de recyclage de mémoire ou encore la commande « TRIM ».
Une bonne connaissance du mode de fonctionnement de ces supports et les technologies implémentées, permet de prendre les précautions nécessaires avant de procéder à leur analyse.

Trois générations de disques SSD peuvent être distinguées:
Les premiers supports n'intégraient pas encore la fonction de « *Garbage Collector* »,
En 2012, les disques dits de « *seconde génération* » ont tous été équipés de cette technologie et reconnaissaient la commande TRIM,
Enfin, les disques de dernière génération sont équipés de ces nouvelles technologies présentant néanmoins des particularités par rapport à leurs aînés.
Pour l'analyse post-mortem de ces support, certaines précautions doivent être prises en compte.
Il est important de réaliser une copie sur un support magnétique vierge ayant fait l'objet d'un effacement permanent ou de faire une acquisition dans un format compressé comme un fichier image au format « E0 » utilisé par le logiciel Encase®.

La copie physique permet ainsi de figer le contenu du support. Pour des questions de procédures, il peut également être conseillé de placer la copie sous scellé.

---

[91] « *les disques durs SSD un défi pour l'expert informatique* », Jean-louis Courteaud, Jean-François Tyrode.

Chapitre 3 Evaluation des fonctions de récupération de données supprimées du logiciel Encase® Forensic

3.1 Introduction

3.1.1 Objectifs des tests

Les enjeux fondamentaux de l'expertise pénale et l'importance de la discipline requièrent un professionnalisme sans faille.
Pour mener leur mission d'expertises, les experts de justice procèdent à l'exploitation des supports informatiques, en recourant à des outils et des logiciels spécialisés qui leur garantissent le respect de l'intégrité des données examinées.
Face au développement et à la complexité des logiciels d'analyse judiciaire de preuves informatiques, les capacités et les limites de chaque outil doivent être identifiées par les experts avant toute utilisation dans un cadre judiciaire.
Afin de réaliser une telle évaluation, il est important de mettre en place une méthodologie rigoureuse.

Les outils d'analyses disposent de nombreuses fonctionnalités, souvent automatisées, et la difficulté principale consiste à tester chaque module ainsi que chaque nouvelle version du logiciel.
Ce qui nécessite des ressources importantes très difficiles à mettre en place par des petites structures ou de petits laboratoires.

Faute de temps et de moyens, ces tests restent donc isolés et sont rarement menés par l'ensemble de la profession.
Par ailleurs, en France nous ne disposons pas d'instances ou de laboratoires officiels recourant à des évaluations des outils d'investigations qui communiqueraient leurs résultats d'analyses.

Parmi les outils d'investigation techniques, deux logiciels se démarquent en se positionnant comme références dans l'industrie de la recherche de preuve numérique à travers le monde :

Il s'agit du logiciel « Forensic Toolkit (FTK®) » de la société AccessData et le programme « Encase® Forensic », édité par la société Guidance Software, leader également sur le marché mondial de l'investigation.

Les logiciels « Encase® » et « FTK® » sont les outils les plus utilisés par les experts, les enquêteurs ainsi que les entités gouvernementales.
Ils sont reconnus par les juridictions et répondent aux critères de recevabilité et de validation devant les tribunaux.

S'agissant de deux outils complémentaires, ils disposent d'une variété de fonctions ayant chacune leurs forces et faiblesses.

Parmi leurs caractéristiques, le logiciel FTK® ne permet pas de créer un réseau local pour faire une acquisition physique de disques durs par un câble Ethernet croisé.
Ce qui pourrait être pénalisant dans les situations où l'on ne peut pas recourir à un bloqueur en écriture de disques durs.
De même, à l'issue de la réalisation de la copie d'un disque dur, FTK génère automatiquement un rapport complet d'acquisition des données, tandis que dans le cas du programme Encase®, celui-ci est créé manuellement par l'expert.

Le programme Encase® dispose d'une multitude d'options de personnalisation, notamment la fonction du script qui permet d'effectuer des recherches plus avancées qui ne fait pas partie des capacités d'analyses proposées par le logiciel FTK.
Pour certains types d'analyses, une utilisation conjointe des deux outils peut s'avérer essentielle.
Il appartient alors à l'expert de connaître les capacités de chaque logiciel en identifiant leurs forces et faiblesses et d'en faire un usage adapté.
Nous avons choisi de pratiquer différents tests sur les versions six et sept du logiciel Encase® Forensic.

La diversité des modules disponibles dans ces logiciels rend l'évaluation de chaque fonctionnalité assez complexe.

Dans le cadre du présent projet de recherche, , les tests se limiteront aux modules de la récupération de données effacées.

Notre objectif est de soumettre à une série de tests ces différents modules du logiciel Encase® Forensic version 6.18.1 et version 7.06.
Bien qu'ancienne, la version six du logiciel serait encore utilisé par certains spécialistes.
Il apparaît ainsi opportun de comparer les résultats obtenus par les deux versions du logiciel afin d'évaluer la capacité d'analyse de ces deux outils, tout en mettant en évidence leurs différences.

Ces tests ne sont pas exhaustifs, la méthodologie proposée pourra être complétée et servir de modèle pour la mise en place d'autres catégories de tests qui seront exécutés sur différents modules des outils d'investigation technique.

Afin de mener à bien notre projet, nous avons acquis les licences des versions six et sept du logiciel Encase® ainsi que les mises à jours annuelles imposées par l'éditeur.
Le choix du logiciel Encase® s'explique par sa large utilisation dans le cadre de l'entreprise et par la communauté d'investigation numérique .

La version sept du logiciel nécessitant un nouvel investissement ainsi que des formations de prise en main, il y a encore des experts qui utilisent la version six.
La nouvelle version intègre des fonctionnalités telles que l'analyse de Smartphones et tablettes et dispose de nouveaux modules tels que "*Encase® Forensic Imager*" et "*Process Evidence*" qui rendent les recherches plus aisées.

La rapidité des recherches et d'exploitation des données constitue aujourd'hui un facteur primordial pour l'analyse d'une quantité importante d'informations.
La version sept permet de procéder au traitement de l'information rapidement et offre la possibilité de continuer à travailler simultanément pendant que les recherches sont lancées sur la machine.
Le moteur d'indexation du logiciel offre une indexation complète des données mais nécessite que le logiciel soit installé sur une machine performante.

3.1.2 Documents de référence (conformité à la documentation d'utilisation)

Le tableau ci-dessous reproduit la liste des documents disponibles pour l'activité de tests :

Documents	Version	Observations
Manuel d'utilisateur Encase®	7.06	Les configurations logicielles et matérielles exigées sont détaillées dans ce document : Pour une meilleure performance, il est recommandé d'installer le logiciel sur un système fonctionnant sous Windows7 (64-bit).
Manuel d'utilisateur "EnCase®_Forensic_Imager"	7.06	-
Encase® Processor	2-2012	Les configurations recommandées: -RAM : 16 Go, -Prévoir 3 supports de stockage : ✓ 1er disque : contient le système d'exploitation, ✓ 2ème disque : La preuve, ✓ 3ème disque : Le cache -CPU : Quad-Core i7, -Système d'exploitation : Windows 7 (64-bit) ou Windows Server 2K8 R2 (64-bit).
Manuel d'utilisateur Encase® version 6.18	6.18	-
Manuel Encase® version 6.12 "Modules Manuals"	6.12	-

3.1.3 Terminologie et glossaire

La terminologie se conforme aux documents suivants :

- « IEEE 610.12:1990 : *Glossaire normalisé IEEE de la terminologie de génie logiciel* »,
- « IEEE 829:1998 : *Standard de l'IEEE pour la documentation de test logiciel* »,
- « *Le Glossaire CFTL/ISTQB des termes utilisés en tests de logiciels*, décembre 2007 ».

Les concepts et termes suivants ont été définis par ces textes avec comme objectif la mise en place d'un standard international de tests servant de documents de référence:

- ✓ **Cas de test** : « *Un ensemble de valeurs d'entrée, de pré-conditions d'exécution, de résultats attendus et de post-conditions d'exécution, développées pour un objectif ou une condition de tests particulier, tel qu'exécuter un chemin particulier d'un programme ou vérifier le respect d'une exigence spécifique* » (norme IEEE 610.12:1990),

- ✓ **Exigence : «** *Une condition ou capacité requise par un utilisateur pour résoudre un problème ou atteindre un objectif qui doit être tenu ou possédé par un système ou composant pour satisfaire à un contrat, standard, spécification ou autre document imposé formellement* » (norme IEEE 610.12:1990),

- ✓ **Plan de tests : «** *Un document décrivant l'étendue, l'approche, les ressources et le planning des activités de test prévues. Il identifie entre autres les éléments et caractéristiques à tester, qui fera chaque tâche, le degré d'indépendance des testeurs, l'environnement de test, les techniques de conception des tests et les techniques de mesure des tests à utiliser, et tout risque nécessitant des plans de contingence. C'est un document reprenant les processus de planification des tests* » (IEEE 829:1998),

- ✓ **Rapport d'évaluation des tests : «** *un document produit à la fin du processus de tests et récapitulant les activités et les résultats de tests. Il contient aussi une évaluation du processus de tests et des leçons apprises*»,

- ✓ **Rapport de synthèse de tests :** « *un document synthétisant les activités et résultats de tests. Il contient aussi une évaluation des articles de tests correspondants par rapport aux critères de sortie* » (IEEE 829:1998),

- ✓ **Résultat attendu : «** *le comportement prédit par les spécifications, ou par d'autres sources, du composant ou système, dans des conditions spécifiées*»,

- ✓ **Technique de conception de tests boîte noire : «** *Procédure documentée pour élaborer et sélectionner des cas de tests basés sur une analyse des spécifications, soit fonctionnelles soit non-fonctionnelles, d'un composant ou système sans faire référence à ses structures internes*»,

- ✓ **Test :** « *Un ensemble d'un ou plusieurs cas de tests* » (IEEE 829:1998).

3.2 Présentation du plan de test détaillé

Le présent plan de test a pour objectif d'identifier toutes les informations relatives au projet et les modules de logiciels devant être évalués.
Il permet d'établir une liste des exigences minimales de tests et de définir en détail les procédures d'évaluation.
La stratégie de test et les ressources nécessaires sont également identifiées.
Avant de procéder à une évaluation des outils, nous avons mis en place une plateforme dédiée en respectant différentes étapes et une méthodologie rigoureuse.

Le programme Encase® étant un logiciel de licence propriétaire, ses codes sources ne sont pas communiqués aux utilisateurs, des tests sur les composants internes de cet outil sont ainsi exclus.

3.2.1 Description de l'environnement de tests

Les tests sont effectués avec le logiciel Encase® version 6.18.1 et Encase® version 7.06.

A cet effet, pour la réalisation de ce projet, différents types de supports informatiques ont été préparés.

Le tableau ci-dessous reprend les informations relatives à ces supports :

#	Type	Marque/Modèle	Numéro de série	Capacité de Stockage
1	Clé USB	CELLEBRITE	-	2Go
2	Clé USB	CELLEBRITE	-	2Go
3	Disque dur interne SATA 3,5"	MAXTOR DiamondMax21	9RY3J29S	250Go
4	Carte mémoire SDHC	SANDISK	-	4Go
5	Carte mémoire Compact Flash	SANDISK	-	8Go
6	Disque dur SSD	SAMSUNG 840Evo	S1DBNSAF834070B	250Go
7	Disque dur SSD	KINGSTON	-	60Go
8	Disque dur SSD	SANDISK	143906400721	64Go

3.2.2 Configurations matérielles des tests

Pour la préparation de la machine de tests, nous avons respecté les configurations recommandées par Guidance Software, l'éditeur du logiciel Encase® :

- **Processeur (CPU) :** Intel Core i7-3770K à 3,50 GHz
- **Mémoire vive (RAM):** 32 Go
- **Stockage :** Samsung SSD 840 series,
- **Capacité de stockage :** 250 Go
- **OS :** Windows 7 Professionnel 64 bits
- **Sauvegarde des résultats de tests :** Disque dur externe Lacie Porsche design 4 To,
- **Interface pour acquisition de disques :** USB 2.0 et 3.0,

3.2.3 Outils de tests utilisés

-Bloqueur en écriture « Tableau Forensic T35E » interfaces IDE/SATA,
-Bloqueur en écriture de carte mémoire « Adonics Forensic »,
-Bloqueur en écriture « Tableau Forensic T8 » interface USB,
-Bloqueur en écriture «FastBloc SE» intégré au logiciel Encase® version 7.06,
-Installation du fichier « encase_examiner_(x64)_70602.exe » : Logiciel Encase ®Version 7.06 (64 bits),
-Installation du fichier exécutable «Encase_forensic_imager»_Version 7.06 (64 bits),
-Licence Encase® sous forme de Dongle,
-Licence complémentaire pour Encase® V7 Processor (pour l'acquisition et le Processing de la preuve),
-Installation du fichier exécutable du logiciel Encase® Version 6.18.1,
-Lecteur de carte mémoire Transcend,
-Station d'accueil Icy Dock pour disques durs SATA et IDE 2,5/3,5'',
-Duplicateur « *Image Masster Solo-4 Forensic* ».

3.2.4 Description de la méthodologie

Les tests ont pour objectifs de vérifier les capacités et la fonction de récupération des données effacées du logiciel Encase® Forensic dans ses deux versions 6.18.1 et 7.06.

La mise en place d'une plateforme de tests nécessite un investissement financier et représente un coût important.

Elle nécessite la préparation d'une machine de tests, achat de licences, acquisition de mises à jour annuels des logiciels, achats de différents supports informatiques, bloqueurs en écritures, etc.

A travers les supports numériques choisis, notre analyse tend également à identifier les limites du programme Encase® dans la recherche et la récupération de données effacées.
Toutes les informations relatives aux tests seront référencées dans une table.

Les exigences définies dans le cadre du présent projet, ont été identifiées au regard des informations fournies par le manuel d'utilisateur de ces logiciels.
Les différentes étapes de tests seront décrites en détail et seront illustrées par des captures d'écran du support analysé.

Ces tests sont menés de manière indépendante sans aucune assistance et nos propres moyens matériels et techniques ont été déployés pour la réalisation du présent projet.

A cet effet, les licences de logiciels et leurs mises à jour ont été payés à l'éditeur.
Les deux outils ont été testés en respectant les spécifications techniques définies par Guidance Software, l'éditeur du logiciel Encase®.

Après la préparation des supports de tests, nous avons utilisé un dispositif de blocage en écriture permettant de préserver l'intégrité des données originales.
Concernant les tests menés avec la version six du logiciel, nous avons utilisé des bloqueurs en écriture matériels.
Avant de réaliser ces tests, tous ces bloqueurs ont été testés afin de s'assurer qu'ils protègent bien les supports en écriture.
Pour ce qui est des tests réalisés sur la version sept du programme Encase®, nous avons eu recours à la solution "FastBloc SE" intégrée dans le logiciel lui-même.
De la même façon, nous avons d'abord contrôlé le bon fonctionnement de ce logiciel avec d'autres supports avant de procéder à nos évaluations.
Nous avons ensuite réalisé une copie bit-à bit de chaque support original au format compressé « E0 ».

3.2.5 Exigences générales

Dans le cadre de ce projet de recherches, nous avons défini certains critères et les éléments suivants ont été retenus comme exigences générales de tests :

Exigences	Description
E-1	Identifier les informations relatives au support de stockage
E-2	Récupérer tous types de fichiers supprimés
E-3	Localiser le fichier supprimé
E-4	Récupérer des données supprimées présentes dans la corbeille
E-5	Récupérer des données dans les espaces non-alloués
E-6	Récupérer des fragments de fichiers
E-7	Indiquer le chemin original du fichier effacé
E-8	Récupérer de données par analyse de signature

Parmi ces exigences, la recherche d'informations relatives à la date et l'heure des fichiers constituant souvent un élément prépondérant dans l'analyse de la preuve numérique, n'a pas été prise en compte.

La question de l'horodatage n'a pas été intégrée à nos travaux de recherches car elle constitue un sujet complexe nécessitant de faire l'objet d'études détaillées.
Elle présente d'autant plus d'intérêt notamment dans les hypothèses de l'utilisation de logiciels de manipulation des dates de fichiers.

3.2.6 Cas de tests

Les tests sont opérés sur deux clés USB, un disque dur SATA, trois supports SSD, une carte mémoire SDHC et une carte compact flash supportant les systèmes de fichiers NTFS et FAT.

Cent vingt et un fichiers (898 Mo) aux divers formats ont été sélectionnés et par la suite copiés sur chaque support destiné aux tests.

Selon les cas, soit ces fichiers ont été supprimés soit les supports ont fait l'objet de formatage.

La liste de l'ensemble de ces documents a été répertoriée dans le tableau ci-dessous:

#	Nom du fichier	Extension	Type
1	Vidéo000.3gp	3gp	Vidéo
2	Car.avi	Avi	Vidéo
3	Train.avi	avi	Vidéo
4	Windows2000Events.csv	csv	Fichier texte
5	page.doc	doc	Document Word
6	batterie lithium.doc	doc	Document Word
7	processeurs.doc	doc	Document Word
8	demande remboursement .doc	doc	Document Word
9	styles_these-numerique_Word[1].doc	doc	Document Word
10	contract mobiledit.doc	doc	Document Word
11	Report- acquisition MD5.doc	doc	Document Word
12	exonération taxe habitation.doc	doc	Document Word
13	coldboot attack.doc	doc	Document Word
14	RENT.doc	doc	Document Word
15	classement RAM.doc	doc	Document Word
16	MovingNT4.doc	doc	Document Word
17	Cast your vote for CEIC locations.eml	eml	MS Outlook Express Mail
18	LIVE WEBINAR_ Reducing Digital Case Load.eml	eml	MS Outlook Express Mail
19	Your new issue of Real eDiscovery magazine is available now.eml	eml	MS Outlook Express Mail
20	UFED Training in UK.eml	eml	MS Outlook Express Mail
21	FW_ What will they think of next.eml	eml	MS Outlook Express Mail
22	Fwd_ EnCase(R) Portable version 2.2 has been released.eml	eml	MS Outlook Express Mail
23	CEIC 2011 Agenda Now Online.eml	eml	MS Outlook Express Mail
24	CEIC 2011- Practical resources for success.eml	eml	MS Outlook Express Mail
25	UFED Physical Analyzer Trial.eml	eml	MS Outlook Express Mail
26	SafeBootInstaller.exe	exe	Fichier exécutable
27	ef_portable_setup_231_english.exe	exe	Fichier exécutable

28	TrueImage11_s_en.exe	exe	Fichier exécutable
29	setup_2.0.exe	exe	Fichier exécutable
30	vlc-2.0.3-win32.exe	exe	Fichier exécutable
31	PGPInstaller.exe	exe	Fichier exécutable
32	UFED Movie.exe	exe	Fichier exécutable
33	SviViewer.exe	exe	Fichier exécutable
34	Chapter07_Services.flv	flv	vidéo
35	Chapter02_Kit Contents.flv	flv	vidéo
36	ts_ipad_takeapart_700[1].flv	flv	vidéo
37	Chapter09_About Cellebrite.flv	flv	vidéo
38	Chapter01_Introduction.flv	flv	vidéo
39	IMG_5413.jpg	jpg	Photo
40	winter.jpg	jpg	Photo
41	CIMG8645.JPG	JPG	Photo
42	492455main_image_1790_1600-1200.jpg	jpg	Photo
43	IMG_0469.jpg	jpg	Photo
44	CIMG8636.JPG	JPG	Photo
45	IMG_0002.jpg	jpg	Photo
46	IMG_5346.jpg	jpg	Photo
47	IMG_0045.jpg	jpg	Photo
48	IMG_0047.jpg	jpg	Photo
49	IMG_0053.jpg	jpg	Photo
50	IMG_0074.jpg	jpg	Photo
51	the-big-bang-experiment.jpg	jpg	Photo
52	IMG_0102.jpg	jpg	Photo
53	IMG_0110.jpg	jpg	Photo
54	IMG_0118.JPG	JPG	Photo
55	IMG_0119.jpg	jpg	Photo
56	IMG_0160.jpg	jpg	Photo
57	IMG_0287.jpg	jpg	Photo
58	IMG_0294.jpg	jpg	Photo
59	IMG_0298.jpg	jpg	Photo
60	IMG_0417.JPG	JPG	Photo
61	IMG_4091.jpg	jpg	Photo

62	IMG_0823.jpg	jpg	Photo
63	IMG_0863.jpg	jpg	Photo
64	IMG_0867.jpg	jpg	Photo
65	IMG_0870.jpg	jpg	Photo
66	IMG_0938.jpg	jpg	Photo
67	IMG_0972.jpg	jpg	Photo
68	IMG_0979.jpg	jpg	Photo
69	IMG_0980.jpg	jpg	Photo
70	IMG_0983.jpg	jpg	Photo
71	IMG_1105.jpg	jpg	Photo
72	IMG_1450.jpg	jpg	Photo
73	IMG_1505.jpg	jpg	Photo
74	IMG_4090.jpg	jpg	Photo
75	13Robin Thicke Lost Without You.mp3	mp3	MPEG-1 Audio
76	schiller - feel you.mp3	mp3	MPEG-1 Audio
77	Duffy-Mercy.mp3	mp3	MPEG-1 Audio
78	Concerto De Aranjuez paco de lucia[1].mp3	mp3	MPEG-1 Audio
79	Vargo-The Moment Original Mix.mp3	mp3	MPEG-1 Audio
80	Bille Davis Nights in white satin.mp3	mp3	MPEG-1 Audio
81	01 Marcello_Earl Adagio[1].mp3	mp3	MPEG-1 Audio
82	Albinoni adagio.mp3	mp3	MPEG-1 Audio
83	Acker Bilk - Autumn Leaves.mp3	mp3	MPEG-1 Audio
84	Stan GetzThe girl fromIpanama[1].mp3	mp3	MPEG-1 Audio
85	nina simone - Piste 02.mp3	mp3	MPEG-1 Audio
86	HTC Touch Commercial.mp4	mp4	Vidéo
87	VIDEO0016.mp4	mp4	Vidéo
88	VIDEO0017.mp4	mp4	Vidéo
89	VIDEO0015.mp4	mp4	Vidéo
90	iPad_User_Guide.pdf	pdf	Adobe PDF
91	Le devis préalable en expertise judiciaire pénale.pdf	pdf	Adobe PDF
92	Cellebrite Family Products.pdf	pdf	Adobe PDF
93	La Police Nationale et la criminalité informatique.pdf	pdf	Adobe PDF

94	release note-march-2-ROW-s.pdf	pdf	Adobe PDF
95	Difficultés rencontrées par les experts.pdf	pdf	Adobe PDF
96	Cellebrite UFED Brochure FRENCH.pdf	pdf	Adobe PDF
97	CNEJITA-ACTES-COLLOQUE13042010-A5-V5.1.pdf	pdf	Adobe PDF
98	UFED Physical Pro Brochure ENGLISH.pdf	pdf	Adobe PDF
99	economics for software verification.pdf	pdf	Adobe PDF
100	CCF181120119_00000.pdf	pdf	Adobe PDF
101	IMG_0093.PNG	PNG	Fichier Graphique
102	IMG_0033.PNG	PNG	Fichier Graphique
103	UFED Presentation09.pps	pps	MS Powerpoint
104	Auscert_2006_-_Defeating_Live_Windows_Forensics_DB_v1.8.ppt	ppt	MS Powerpoint
105	live-forensics.ppt	ppt	MS Powerpoint
106	custom TS.txt	txt	Texte
107	Cea.mobile.nokia.com01.txt	txt	Texte
108	Global keywords.txt	txt	Texte
109	C.google.com01.txt	txt	Texte
110	wcmd.txt	txt	Texte
111	HTC Touch Presentation.wmv	wmv	Windows Media Video (WMV)
112	UFED Logical v1170 Phones supported(2)(1).xls	xls	MS Excel
113	06 juin 2010.xlsx	xlsx	MS Excel
114	03 mars 2010.xlsx	xlsx	MS Excel
115	02 fevrier 2010.xlsx	xlsx	MS Excel
116	EnCase_Portable_v21_User_Guide.zip	zip	Fichier compressé
117	encase_portable_v22_release_notes.zip	zip	Fichier compressé
118	EnScriptProgramsV6_3UserManual.zip	zip	Fichier compressé
119	Exif_Reader_3.0.zip	zip	Fichier compressé
120	microsoft-cofee-112.zip	zip	Fichier compressé
121	EF_User_Manual.zip	zip	Fichier compressé

3.2.6.1 Encase® Law Enforcement version 6.18.1

Avant de préparer les supports de tests, nous avons procédé à leur effacement complet avec les outils "*Wipe Drive*" du logiciel Encase® ou « *Image Masster Solo-4* Forensic ».

Pour tous les cas de tests, une deuxième copie des supports a été réalisée et les résultats des algorithmes MD5 ont été comparés et vérifiés.

La recherche de fichiers effacés a été effectuée à partir de l'image du support réalisée au format "E0". Tous les résultats obtenus sont commentés dans un tableau au point 3.3.

3.2.6.1.1 Cas de test CT-01-V6 :

Le premier cas de test consiste à analyser le contenu d'une clé USB de marque "CELLEBRITE" disposant d'une capacité de stockage de 2Go.
Avant de commencer les essais, le support a été connecté à l'ordinateur afin de procéder à son effacement complet avec l'outil "*Wipe Drive*" du logiciel Encase®.

Nous avons ensuite réalisé un formatage rapide de la clé au format FAT32.
Les fichiers sélectionnés pour les tests ont été copiés sur le support et la clé USB a été formatée, les données figurant sur la clé ont ainsi été supprimées.

Avant la création d'une image complète du support, nous avons relevé les informations affichées dans l'explorateur Windows et dans le gestionnaire de disques, relatives à la capacité de stockage du support :

Capacité affichée sur l'étiquette de la clé USB	Capacité affichée dans l'explorateur Windows	Capacité affichée dans le gestionnaire des disques
2Go	1,87Go	1,88Go

Nous avons connecté la clé USB au bloqueur en écriture de marque Tableau modèle « *T8 Forensic USB Bridge* ». Avec le programme « Encase® Forensic » version 6.18.1, une copie bit-à-bit du support original a été réalisée au format de fichier "E0".

A l'issue de la copie, l'intégrité des données a été vérifiée par le logiciel qui a calculé l'empreinte numérique du fichier et produit l'algorithme MD5.
Le rapport généré par le logiciel Encase® est reproduit dans les résultats de tests.
La recherche de fichiers effacés a été effectuée à partir de l'image au format "E0" et les résultats obtenus sont commentés dans un tableau au point 3.3.

3.2.6.1.2 Cas de test CT-02-V6 :

Le support objet de la présente recherche correspond à une clé USB de marque "CELLEBRITE" avec une capacité de stockage de 2Go.
Après avoir connecté la clé à l'ordinateur de test, nous avons procédé à un effacement complet du support avec l'outil "Wipe Drive" du logiciel Encase®.

Un formatage rapide de la clé USB a été réalisée au format FAT32 et les cent vingt et un fichiers testés ont été copiés sur le support.
Après le formatage, les fichiers tests ont été copiés sur le support et ont été tous effacés en même temps.

Nous avons identifié la capacité de stockage du support telle que définie dans l'explorateur Windows et dans le gestionnaire de disques:

Capacité affichée sur l'étiquette de la clé USB	Capacité affichée dans l'explorateur Windows	Capacité de stockage affichée dans le gestionnaire des disques
2Go	1,87Go	1,88Go

La clé USB a été connectée au Bloqueur en écriture Tableau, modèle « *T8 Forensic USB Bridge* » et une copie exacte du support a été créée au format "E0" avec le logiciel Encase® Forensic Version 6.18.1.
L'algorithme MD5 a été contrôlé et le rapport généré par le logiciel Encase® est reproduit dans les résultats de tests.

3.2.6.1.3 Cas de test CT-03-V6 :

Le présent cas de test permet de rechercher des fichiers effacés sur un disque dur du type SATA 2,5".
Les informations suivantes sont relevées sur l'étiquette du fabricant :
-Marque : MAXTOR
-Modèle : DiamondMax21- STM32350310AS
-Numéro de série : 9RY3J29S
-Capacité de stockage: 250 Go

Bien qu'il s'agisse d'un support vierge, nous avons complètement effacé son contenu à l'aide du module "*wipe*" du duplicateur « *Image Masster Solo-4 Forensic* ».
Le disque dur a été connecté à la machine de test via le port USB de la Station d'accueil « Icy Dock pour disques durs SATA et IDE 2,5/3,5 ».

Nous avons procédé à un formatage rapide du disque dur et à la création d'une partition NTFS.
Tous les fichiers testés ont été copiés sur le support magnétique et ont été ensuite placés dans la corbeille.

Avant de réaliser une acquisition physique du support, nous avons noté la capacité du disque dur affichée dans Windows :

Capacité affichée sur l'étiquette du disque dur	Capacité affichée dans l'explorateur Windows	Capacité affichée dans le gestionnaire des disques
250 Go	232 Go	232,88Go

Afin de créer une copie bit-à-bit du support original, le disque dur a été déconnecté de l'ordinateur et puis branché au dispositif de blocage en écriture « *Tableau Forensic T35E interfaces IDE/SATA* », le protégeant contre toute altération des données.
Nous avons calculé l'empreinte numérique du disque dur et les algorithmes MD5 ont été contrôlés et vérifiés.

3.2.6.1.4 Cas de test CT-04-V6 :

Le support objet du présent test correspond à une carte mémoire SDHC de marque SanDisk avec une capacité de stockage de 4Go.

Capacité affichée sur l'étiquette de la carte SD	Capacité affichée dans l'explorateur Windows	Capacité reportée dans le gestionnaire des disques
4 Go	3,68 Go	3,69Go

Il a été connecté à l'ordinateur de test via un lecteur de cartes mémoires de marque Transcend. Son contenu a été complètement effacé avec le logiciel Encase® et a été par la suite formaté au format FAT32.

Nous avons copié cent vingt et un fichiers choisis pour les tests sur le support et les avons tous supprimés.
Après avoir déconnecté la carte SD de l'ordinateur, elle a été insérée dans le lecteur de carte mémoire et connectée au bloqueur en écriture Tableau « *T8 Forensic USB Bridge* ».
Une image du support a été réalisée avec le logiciel Encase® qui a calculé l'empreinte numérique, les résultats ont été comparés avec la création d'une deuxième copie. .

3.2.6.1.5 Cas de test CT-05-V6 :

Il s'agit d'une carte mémoire Compact Flash Ultra de marque SanDisk avec une capacité de stockage de 8Go.

Capacité affichée sur l'étiquette de la carte mémoire	Capacité affichée dans l'explorateur Windows	Capacité reportée dans le gestionnaire des disques
8Go	7,44 Go	7,45Go

Elle a été connectée à l'ordinateur via le lecteur de carte mémoire Transcend.
Nous avons copié tous les fichiers tests et avons par la suite formaté le support.

La mémoire flash a été insérée dans le bloqueur en écriture « *Adonics Forensic* » afin de réaliser une copie exacte du support.

Cependant, dès que le programme Encase® s'est exécuté, il a rencontré un bogue en affichant un temps de copie supérieure à 12h00.
Après plusieurs tentatives, nous avons inséré la carte mémoire dans le lecteur Transcend et l'avons connectée au bloqueur en écriture Tableau "T8 Forensic USB Bridge" qui ne l'a pas reconnue.
Cette expérience a été renouvelée à plusieurs reprises sans succès.
Nous avons alors copié le support sans utiliser un dispositif de blocage en écriture.

3.2.6.1.6 Cas de test CT-06-V6 :

le présent cas de test porte sur un support SSD et les informations suivantes ont été identifiées sur l'étiquette du support :
-Marque : SAMSUNG 840 EVO
-Modèle : MZ- 7TE250
-Numéro de série : S1DBNSAF834070B
-Capacité de stockage: 250 Go

Capacité affichée sur l'étiquette du disque SSD	Capacité affichée dans l'explorateur Windows	Capacité reportée dans le gestionnaire des disques
250 Go	232 Go	232,88 Go

Le support est fourni avec l'utilitaire de gestion « *Samsung Magician* », conçu pour fonctionner avec les SSD de marque Samsung. Il propose différentes fonctionnalités comme le paramétrage de « l'Overprovisioning » qui augmente la performance et la durée de vie des SSD.

Avant de débuter les tests, nous avons désactivé la commande TRIM qui est activée par défaut sur Windows sept.

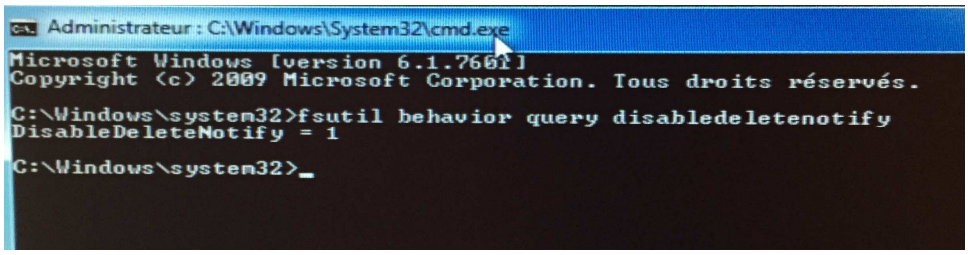


Figure 31- Désactivation de la commande TRIM

Les fichiers choisis pour les tests ont été copiés sur le support SSD puis ont été supprimé.

Différentes études montrent que le comportement d'un SSD dépend principalement du contrôleur et du type de technologie utilisé par le fabricant de celui-ci.
Afin de déterminer les spécificités techniques de ces supports, des expérimentations approfondies doivent permettre d'identifier différents modèles de disques et de comparer leurs résultats.
Nos évaluations restent toutefois limitées à trois modèles récents de SSD vierges qui n'ont jamais été utilisés auparavant.

3.2.6.1.7 Cas de test CT-07-V6 :

Le second SSD objet du présent test est de marque KINGSTON, ,disposant d'une capacité de stockage de 60 Go.
Le support est connecté à l'ordinateur de test par le port USB de la Station d'accueil « Icy Dock pour disques durs SATA et IDE 2,5/3,5».

Nous avons relevé les informations suivantes relatives à la capacité du disque dur :

Capacité affichée sur l'étiquette du disque SSD	Capacité affichée dans l'explorateur Windows	Capacité reportée dans le gestionnaire des disques
60 Go	55,8 Go	55,9 Go

Au préalable, la commande TRIM a été désactivée et tous les fichiers tests ont été copiés sur le support. Ils ont ensuite été tous effacés par un formatage rapide avec Windows.
Enfin, une acquisition physique du support original a été effectuée avec le logiciel Encase®.
Pour cela, le disque dur a été déconnecté de l'ordinateur et puis branché au dispositif de blocage en écriture « *Tableau Forensic T35E interfaces IDE/SATA* » le protégeant contre toute altération des données.
L'empreinte numérique du disque dur et les algorithmes MD5 ont été contrôlés par le logiciel.
Les résultats de la deuxième copie ont été comparés et l'intégrité du support a été vérifiée.

3.2.6.1.8 Cas de test CT-08-V6 :

Le dernier support de test correspond à un disque SSD de marque SANDISK avec une capacité de stockage de 64 Go, portant le numéro de série 143906400721.

Le SSD a été connecté à l'ordinateur de test par le port USB de la Station d'accueil « Icy Dock pour disques durs SATA et IDE 2,5/3,5 ».

Après un formatage rapide de la partition au format NTFS, nous avons relevé les informations suivantes relatives à la capacité du disque dur :

Capacité affichée sur l'étiquette du disque SSD	Capacité affichée dans l'explorateur Windows	Capacité reportée dans le gestionnaire des disques
64 Go	58,6 Go	58,69 Go

Nous avons vérifié que la commande TRIM est bien active.

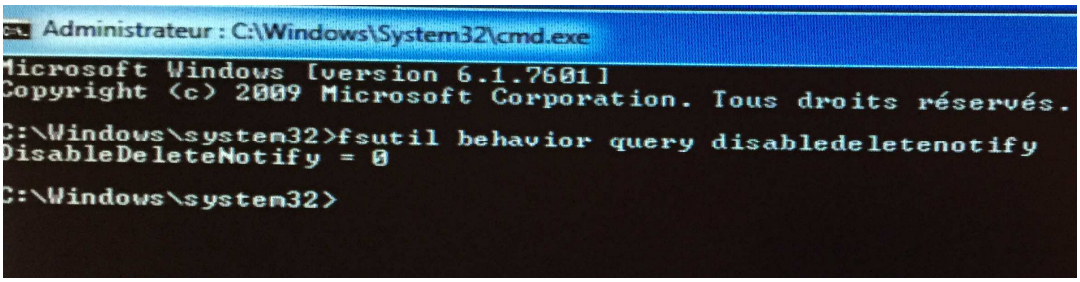


Figure 32- Activation de la commande TRIM

Cent vingt et un fichiers ont été copiés sur le support et ont été par la suite effacés. Nous avons connecté le disque dur au bloqueur en écriture « *Tableau Forensic T35E interfaces IDE/SATA* », le protégeant contre toute altération des données.

Une copie du SSD a été réalisée avec le logiciel Encase® et son empreinte numérique et les algorithmes MD5 ont été contrôlés par le logiciel.

3.2.6.2 Encase® version 7.06

La recherche de fichiers effacés a été effectuée à partir de l'image du support réalisée au format "E0". Tous les résultats obtenus sont commentés dans un tableau au point 3.3.

Nous avons réalisé les tests sur les mêmes supports que ceux utilisés pour l'évaluation du logiciel Encase® version 6.

Avant de connecter chaque support à la machine de tests, nous avons activé le blocage en écriture "FastBloc SE", fonction intégrée dans Encase® version 7.

Afin de nous assurer du bon fonctionnement du dispositif de protection en écriture, des tests séparés ont été réalisés sur d'autres supports et les valeurs HASH ont été comparées.

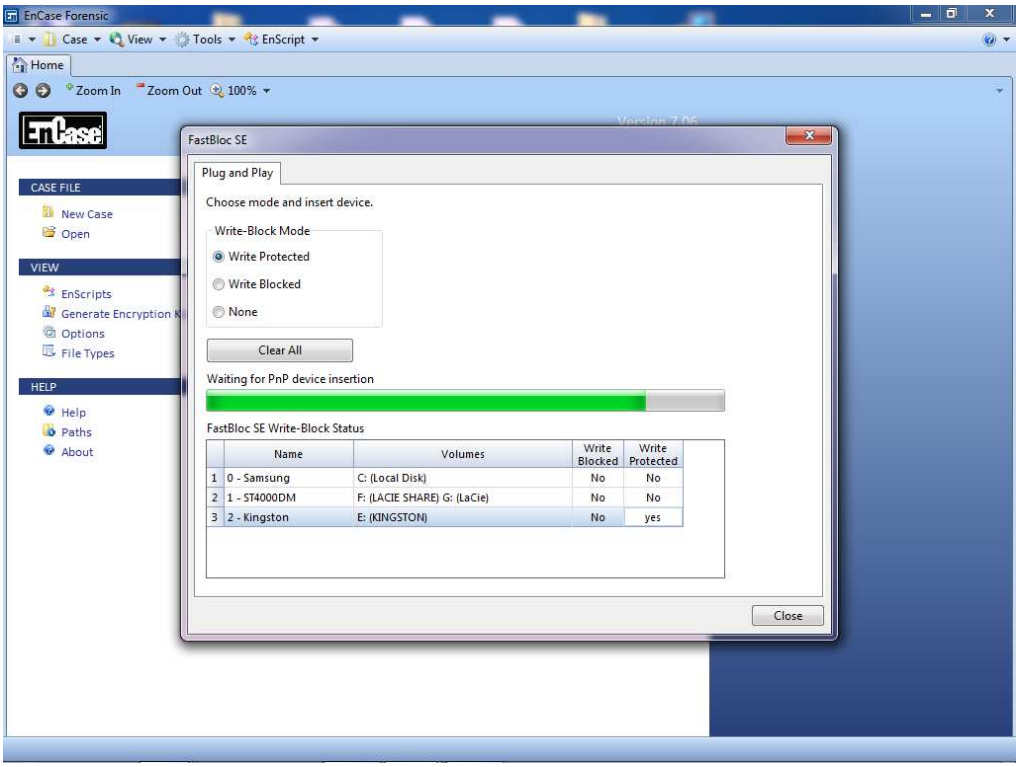


Figure33 - : copie écran "FastBloc SE"- Encase® version 7.06

Pour l'évaluation du programme Encase® version 7.06, nous avons crée les cas de tests CT-01-V7 à CT-08-V7.

Pour chaque support de tests, nous avons réalisé une acquisition physique avec la version sept du logiciel.
Les résultats détaillés sont reproduits au point 3.3 de la présente expérimentation.

Selon les spécifications de la société Guidance Software, la version sept du logiciel Encase® permet de restituer les images des supports informatiques sous quatre formats physiques et logiques (.EX01), (.LX01), (.E01) et (.L01). Les nouveaux formats permettent également d'utiliser un chiffrement AES-256.
Pour nos cas de tests, toutes les images ont été réalisées au format classique (.E01).

3.3 Résultats expérimentaux et observations

3.3.1 Rapports de tests

Les tests exécutés identifient le comportement général de l'outil et permettent de mettre en place une méthodologie pour évaluer d'autres modules du programme Encase® ou d'autres logiciels d'analyse de preuves informatiques.

La difficulté principale d'évaluation du programme Encase® est liée à sa complexité et au fait qu'il est composé de nombreux modules.

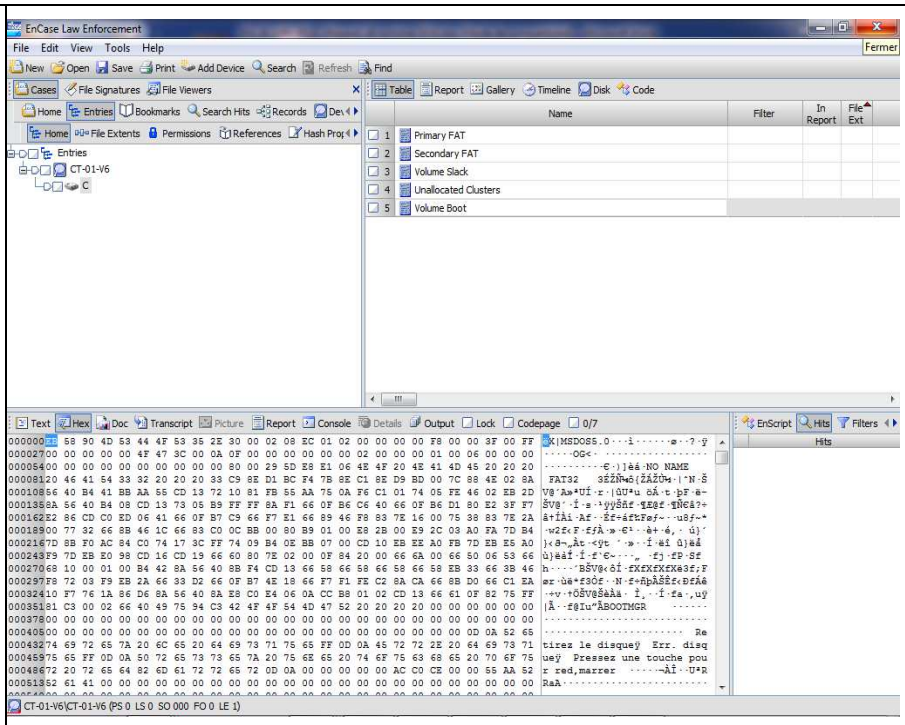
En effet, la fonction de "scripts" permet de personnaliser les recherches et de créer de nouveaux petits programmes qui seront intégrés dans le logiciel.

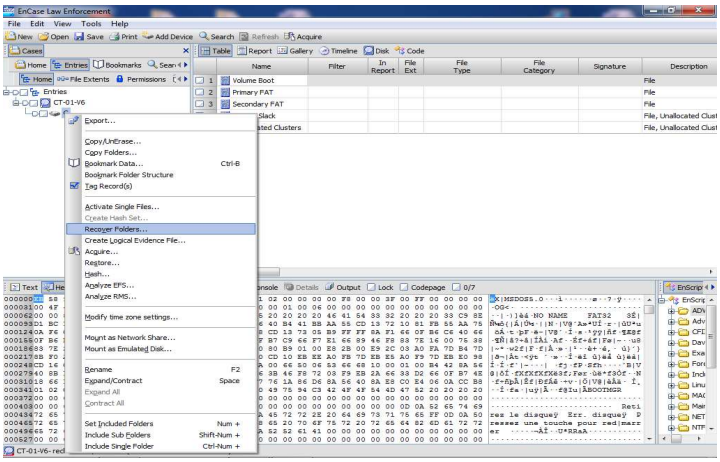
Or, peu d'informations sont communiquées par l'éditeur concernant le fonctionnement de ces scripts.
Ces différents scripts n'ont pas été intégrés dans les présents cas de tests.

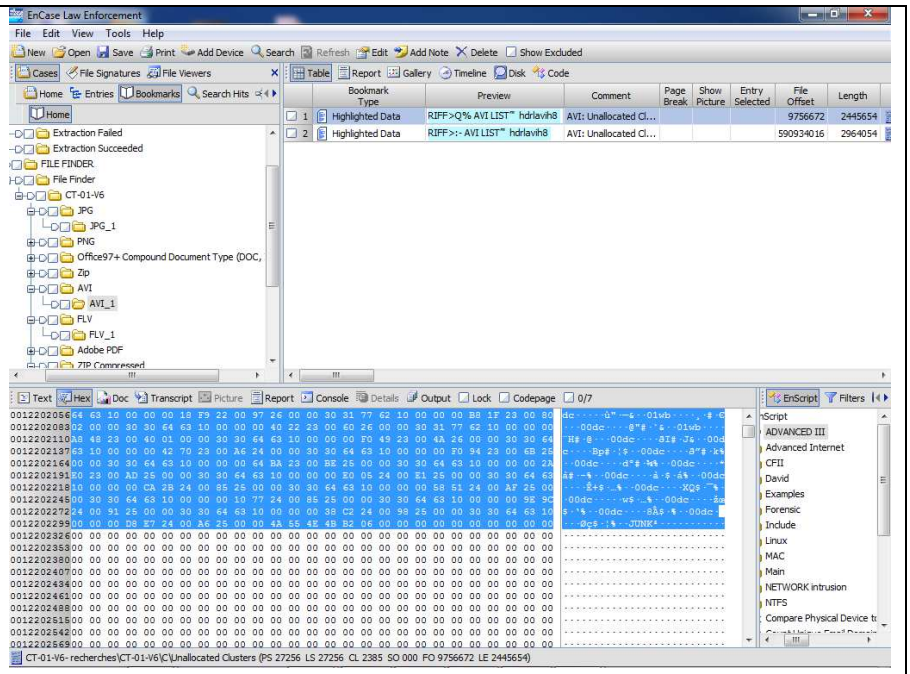
3.3.2.1 Rapports de tests Encase® version 6.18.1

3.3.2.1.1 Cas de test CT-01-V6

Référence du cas de test: CT-01-V6	
Outil testé	**Encase® Forensic version 6.18.1**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une clé USB suite à un formatage rapide de celle-ci.

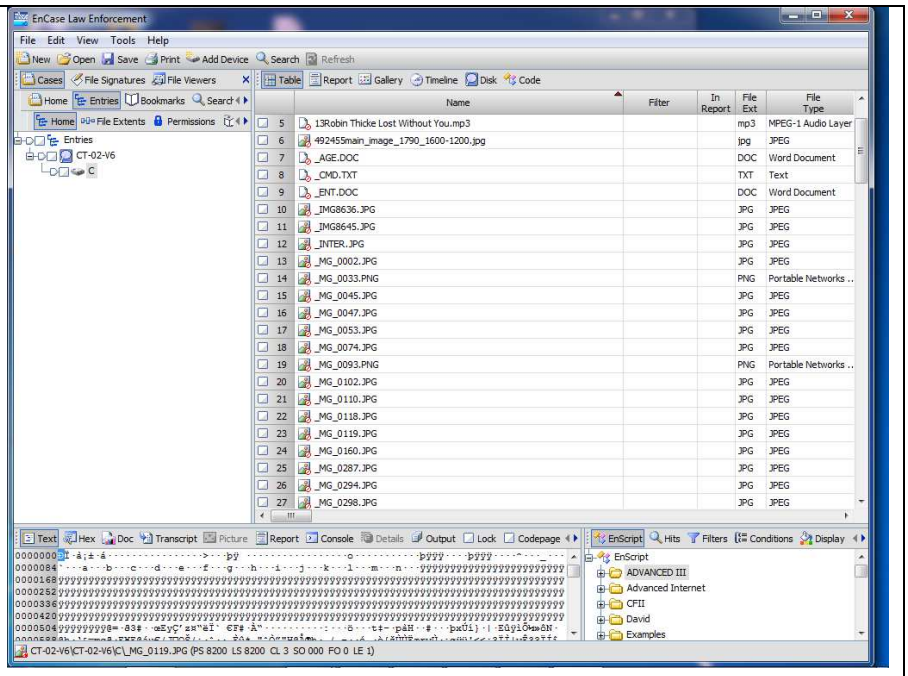
Capture d'écran de la clé USB formatée dans Encase® V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase® Version 6.18.1 Version du système d'exploitation: Windows 7 Dispositif de blocage en écriture: Tableau  Date de la copie du support: 21/11/13 23:12:52
Informations relatives au support examiné:	Système de fichiers: FAT32 Numéro de série: 0909040700255 Capacité : 2 022 612 480 octets (1,9Go) Nombre de secteurs: 3 950 415 Signature disque 20646973 Partitions Valide

Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: c7e76831fbf9c5be25fead9d9775db30 Vérification MD5: c7e76831fbf9c5be25fead9d9775db30 GUID: 181f077813004f4699269db901accaa4
Détail des résultats obtenus: Détection d'anomalies:	*Le logiciel Encase, via le module "*Recover folders*", permet de récupérer des informations effacées sur toute la partition FAT et de chercher dans les espaces non-alloués du support les répertoires effacés. Elle reconstitue la structure de répertoires, des fichiers ainsi que leur arborescence.  Dans le cas de la présente expérimentation, cette recherche n'a généré aucun résultat. *La recherche de fichiers effacés a été effectuée par une analyse de l'en-tête de fichiers dans les espaces non-alloués du support amovible. Nous avons préparé une liste de signatures parmi les quelles figurent notamment les formats suivants: -"JPG": \xFF\xD8\xFF[\xFE\xE0\xDB\xC4\xE1\xEE], -"PNG": \x89\x50\x4E\x47 -"Windows média": \x30\x26\xB2\x75\x8E\x66\xCF\x11 Avec cette méthode, il a été possible d'identifier le contenu des fichiers et de les reconstruire. Le schéma ci-dessous illustre la reconstruction d'un fichier vidéo au format Avi :

3.3.2.1.2 Cas de test CT-02-V6

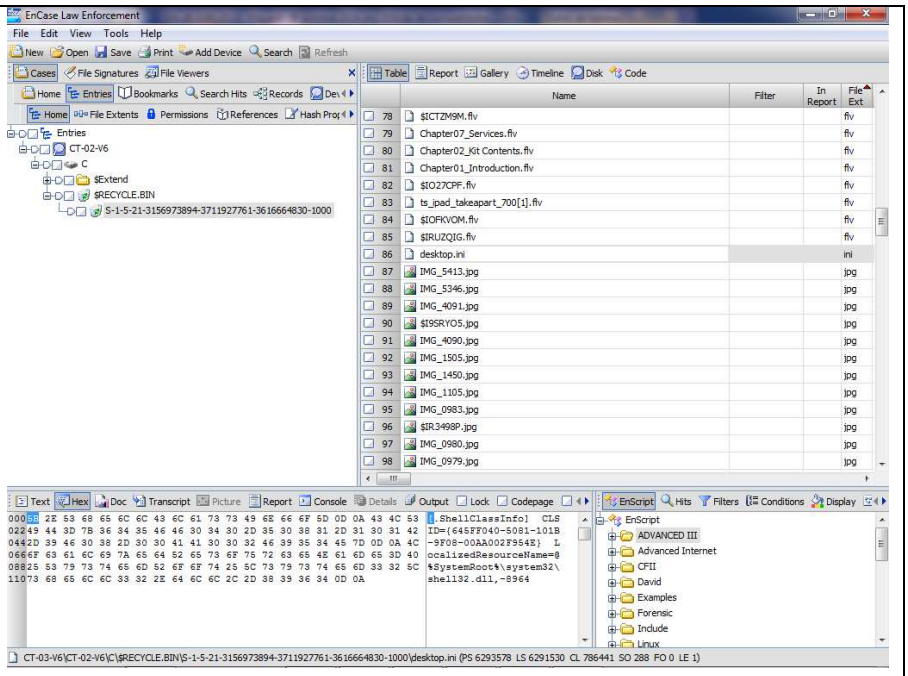
Référence Cas de test: CT-02-V6	
Outil testé	**Encase Forensic version 6.18.1**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une clé USB suite à la suppression de tous les fichiers du support.

Capture d'écran de la clé USB avec les fichiers effacés dans Encase V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 6.18.1 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: Tableau  Date de la copie du support: 22/11/13 01:01:43
Informations relatives au support examiné:	Système de fichiers: FAT32 Numéro de série: 10081851030154 Capacité : 2 021 654 528 octets (1,9Go) Nombre de secteurs: 3 948 544 Signature disque 20646973 Partitions Valide

<table>
<tr><td>Calcul de l'intégrité des données:</td><td>Intégrité Vérifiée, 0 Erreur
Acquisition MD5: 301c9bb11ae65a82237aaa33c56d98b9
Vérification MD5: 301c9bb11ae65a82237aaa33c56d98b9
GUID: 1a148e403721c5469e87798991446600</td></tr>
<tr><td>Observations:</td><td>Sur un système de fichier du type FAT, lorsqu'un fichier est effacé, la première lettre de l’entrée est remplacée par le caractère E5 en hexadécimal (hex\xE5).
Cela indique au système que la place qu’il occupe sur le disque est à nouveau disponible.
Par défaut, le symbole "_" est utilisé par Encase pour distinguer ces fichiers mais l'utilisateur peut le modifier.</td></tr>
<tr><td>Détail des résultats obtenus:</td><td>*Le logiciel Encase et Windows n'affichent pas la même capacité de stockage pour le support analysé:
<table>
<tr><th>Capacité affichée par le constructeur</th><th>Capacité par l'explorateur Windows</th><th>Capacité par le gestionnaire des disques</th><th>Capacité par Encase</th></tr>
<tr><td>2Go</td><td>1,87Go</td><td>1,88Go</td><td>1,9Go</td></tr>
</table>
*Les fichiers supprimés s'affichent avec leurs noms d'origines. Certains d’entre eux sont endommagés et certains ne nécessitent pas de recherches complémentaires, ils sont directement récupérables depuis l'interface du programme.</td></tr>
</table>

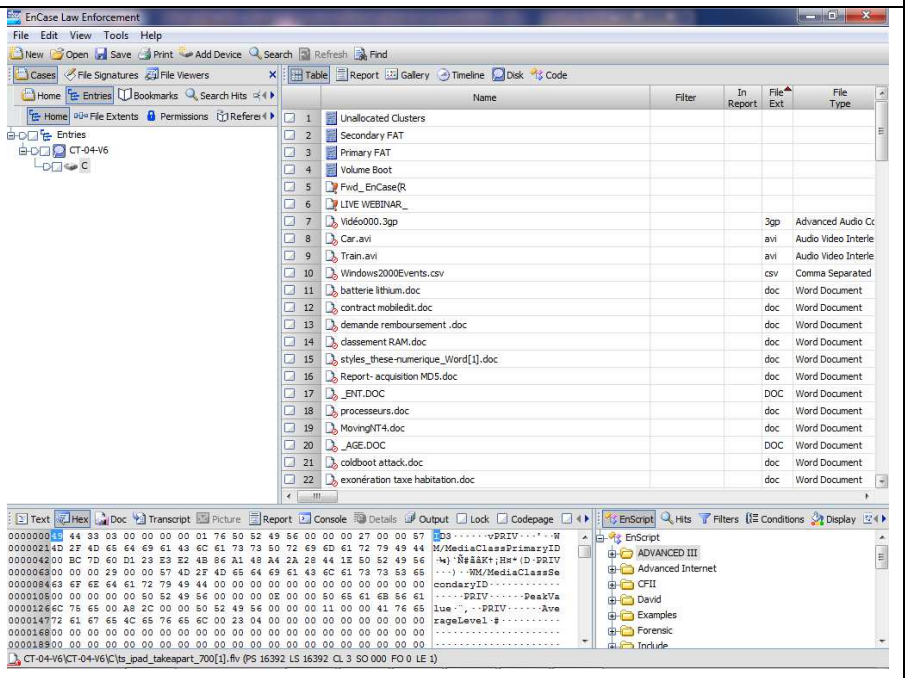
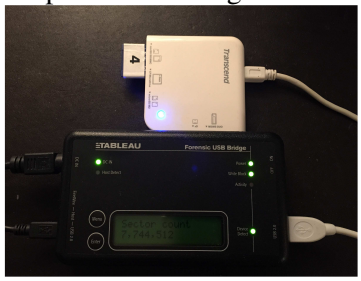
3.3.2.1.3 Cas de test CT-03-V6

Référence Cas de test: CT-03-V6	
Outil testé	**Encase Forensic version 6.18.1**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur un disque dur interne du type SATA suite à la suppression de tous les fichiers du support.

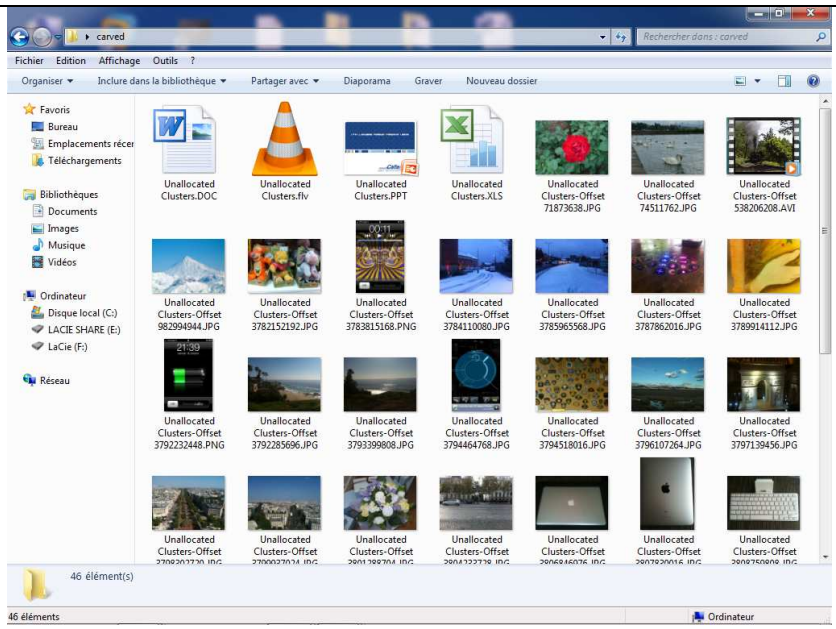
Capture d'écran des fichiers effacés dans Encase® V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase® Version 6.18.1 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: Tableau  Date de la copie du support: 17/12/13 15:19:56
Informations relatives au support examiné:	Système de fichiers: NTFS Marque: Maxtor S Modèle: TM3250310AS Numéro de série: 9RY3J29S Capacité : 250 059 350 016 (232,9Go) Nombre de secteurs: 488 397 168

	Signature disque FB6B1998 Partitions Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: aff92bb0630733ac3397c581ce71ab36 Vérification MD5: aff92bb0630733ac3397c581ce71ab36 GUID 60f1a84b1c0ecb4da58f99b38b4f8305
Détail des résultats obtenus:	Encase® répertorie au total 252 fichiers dans la corbeille : *On identifie très aisément cent vingt et un fichiers supprimés. Ils sont restés intacts et récupérables avec la fonction « *Copy/UnErase* » du programme. *Les noms de fichiers n'ont pas été altérés. *Le logiciel affiche également cent vingt et un fichiers d'index dont le nom commence par les lettres $I. Ils sont associés aux fichiers d'origines par le logiciel (liste ci-dessous non- exhaustive) : -$I00TWOX.eml = ·U·F·E·D· ·T·r·a·i·n·i·n·g· ·i·n· ·U·K·.·e·m·l -$I0G8QDG.doc= p·a·g·e·.·d·o·c -$I0L9OPJ.pdf= r·e·l·e·a·s·e· ·n·o·t·e·-·m·a·r·c·h·-·2·-·R·O·W -$I0NOHDC.eml= U·F·E·D· ·P·h·y·s·i·c·a·l· ·A·n·a·l·y·z·e·r· ·T·r·i·a·l·.·e·m·l· -$I14HD7I.exe= S·v·i·V·i·e·w·e·r·.·e·x·e· Depuis la version de Windows Vista, le nom de la corbeille a été remplacé par "$Recycle.Bin" et les informations contenues dans le fichier "INFO2" sont désormais enregistrées dans un fichier d'index dont le nom commence par les lettres $I. *Encase® met également en évidence neuf fichiers « métadonnées » "OECustomProperty" associés aux Emails qui contiennent des informations relatives à l'expéditeur, le destinataire, l'objet, la date… *Le fichier « desktop.ini », généré par Windows se trouve également présent dans la corbeille.

3.3.2.1.4 Cas de test CT-04-V6

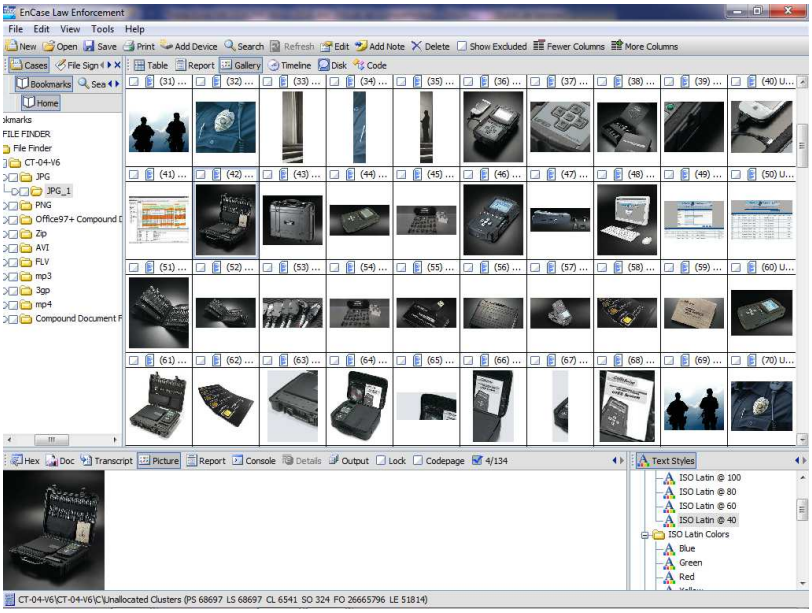
Référence Cas de test: CT-04-V6	
Outil testé	**Encase Forensic version 6.18.1**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une carte mémoire SDHC suite à la suppression de tous les fichiers du support.
Capture d'écran de la carte SD avec les fichiers effacés dans Encase V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 6.18.1 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: Tableau  Date de la copie du support: 18/12/13 09:45:41

Informations relatives au support examiné:	Système de fichiers: FAT32 Numéro de série: 058F63626376 Capacité : 3 965 190 144 octets (3,7Go) Nombre de secteurs: 7 744 512 Signature disque 20646973 Partitions Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: e33a7af5d4c1b9e6ede5d84931895c9d Vérification MD5: e33a7af5d4c1b9e6ede5d84931895c9d GUID 54884ea8c2dc854192622adfe4cb5dcb
Détail des résultats obtenus:	*Le module "*Recover folders*" qui permet de récupérer les données supprimées ne reconstitue aucune donnée effacée. *Sur son interface, le programme Encase® liste 128 fichiers: -118 fichiers effacés, -2 fichiers irrécupérables, -7 fichiers associés aux clusters invalides. Pour certains d'entre eux, leur première lettre est remplacée par le symbole "_". *Une partie des fichiers reste inexploitable et ne peut être exportée par des techniques classiques de récupération de données. Les résultats d'analyses par signatures de fichiers montrent que les entêtes ne correspondent pas aux extensions analysées ("*! Bad signature*"). *La méthode traditionnelle étant ainsi inefficace, une recherche sur les espaces non-alloués par la technique du "*carving*" a été effectuée : Il s'agit d'une reconstitution de fichiers par une analyse de signatures du début et fin de fichiers : Les recherches sont menées sur les types de fichiers suivants : [.doc, xls, png, jpg, eml, mp3, mp4, avi, flv, zip, 3gp, pps].

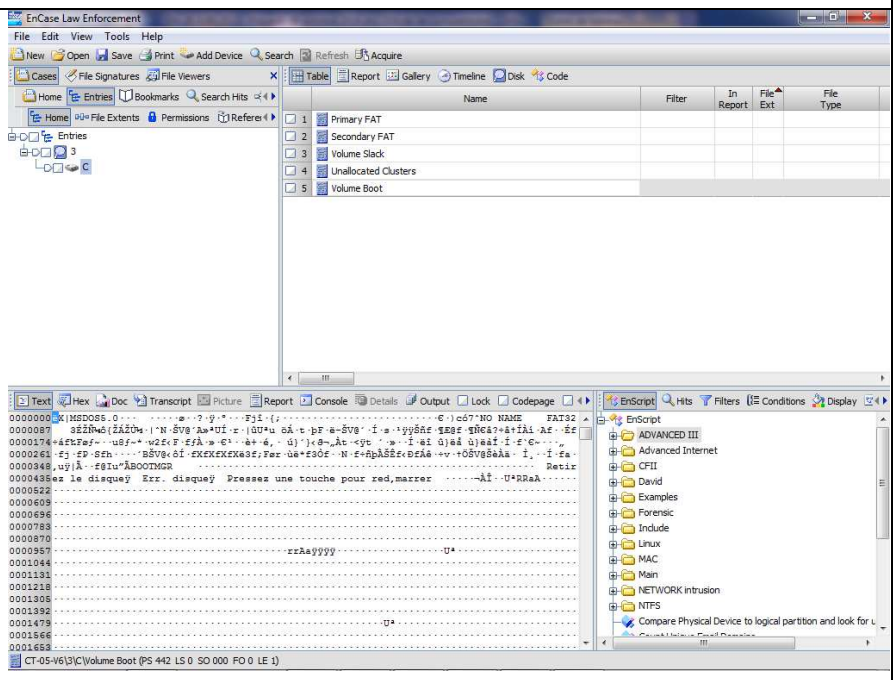


Dans la version six du programme Encase, le module "File Finder" permet de procéder automatiquement à cette recherche en choisissant le type de fichier recherché.
Pour certains formats comme le "mp4", "3gp", "mp3", "pdf",etc, les informations relatives à l'en-tête et la fin de fichiers doivent être rajoutées manuellement dans le logiciel sans lesquelles ils ne peuvent pas être récupérés.

*Concernant les fichiers images, le logiciel recherche toutes les photos disponibles y compris celles qui font partie intégrante d'un document "*Pdf*" ou "*Word*".



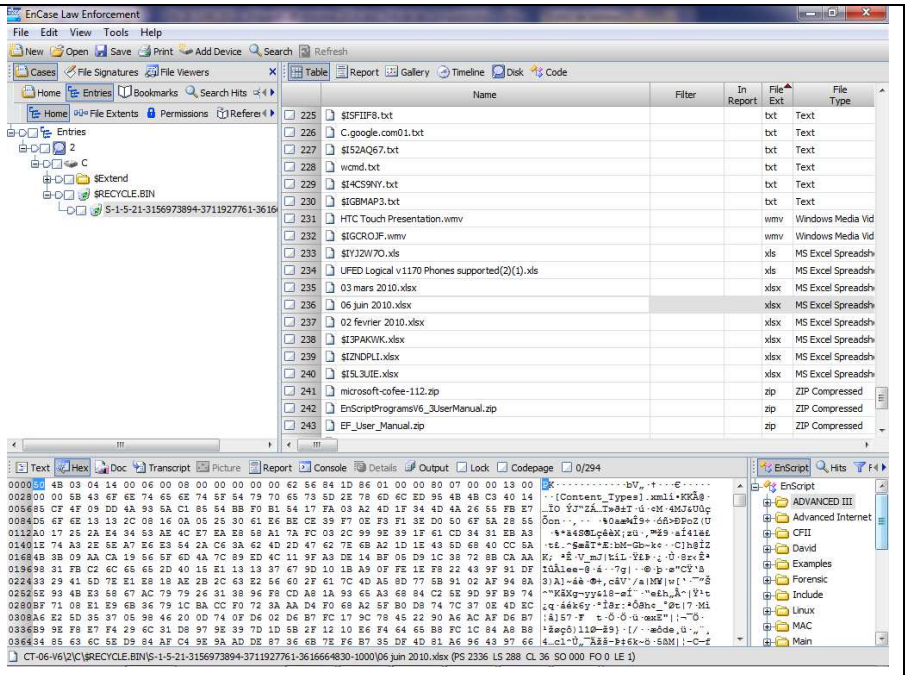
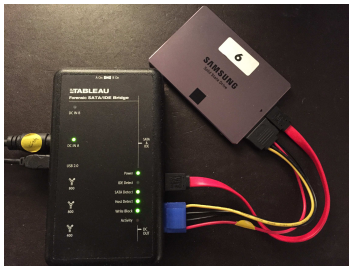
3.3.2.1.5 Cas de test CT-05-V6

Référence Cas de test: CT-05-V6	
Outil testé	**Encase Forensic version 6.18.1**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une carte mémoire Compact Flash suite au formatage du support.
Capture d'écran de la carte compact Flash dans Encase V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 6.18.1 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: **Non** Date de la copie du support: 18/12/13 09:45:41
Informations relatives au support examiné:	Système de fichiers: FAT32 Capacité : 8 000 110 592 octets (7,5GB) Nombre de secteurs: 15 625 216 Signature disque - Partitions Valide

Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: f517b2b94dfd0cb2443359f6b992e1c6 Vérification MD5: f517b2b94dfd0cb2443359f6b992e1c6 GUID fc1053d1e0584542be33f8ba6347f786
Détail des résultats obtenus:	*Le volume a été formaté et le logiciel n'affiche aucun fichier effacé. *Le module "*Recover folders*" qui permet de récupérer des données effacées, ne retrouve aucune information. *Afin de reconstituer les fichiers, la méthode du "*Carving*" a été utilisée recherchant les types de fichiers suivants: [.doc, xls, png, jpg, eml, mp3, mp4, avi, flv, zip, 3gp, pps]. -Concernant les fichiers compressés au format "zip", ils ont tous été récupérés. ENCASE® a recensé 120 fichiers au format zip, un tri a été nécessaire pour éliminer les informations non-exploitables. Lorsque les recherches sont menées sur les espaces non-alloués d'un support, des résultats faux-positifs peuvent être générés. -Pour ce qui est des fichiers images, au total, 324 fichiers ont pu être reconstitués par Encase®. Il s'agit principalement des photos insérées dans les documents. -Pour les fichiers au format mp4 et 3gp, les fichiers ne sont pas récupérés da façon automatique, les informations concernant les en-têtes et les fins de fichiers doivent être recherchées manuellement. -Il en est de même pour les fichiers mp3 pour lesquels, un tri s'avère nécessaire pour les résultats faux-positifs générés par le logiciel.

3.3.2.1.6 Cas de test CT-06-V6

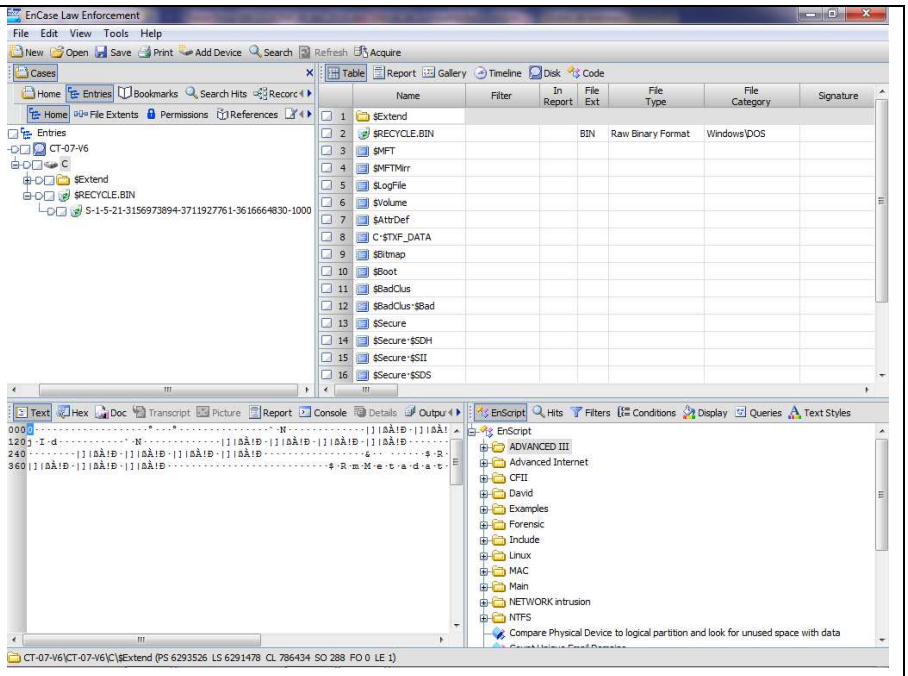
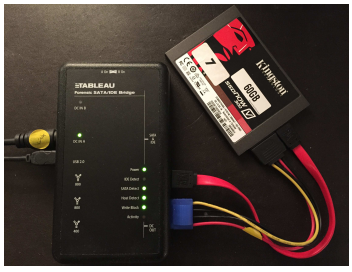
Référence Cas de test: CT-06-V6	
Outil testé	**Encase Forensic version 6.18.1**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur un SSD suite à la suppression des fichiers du support.

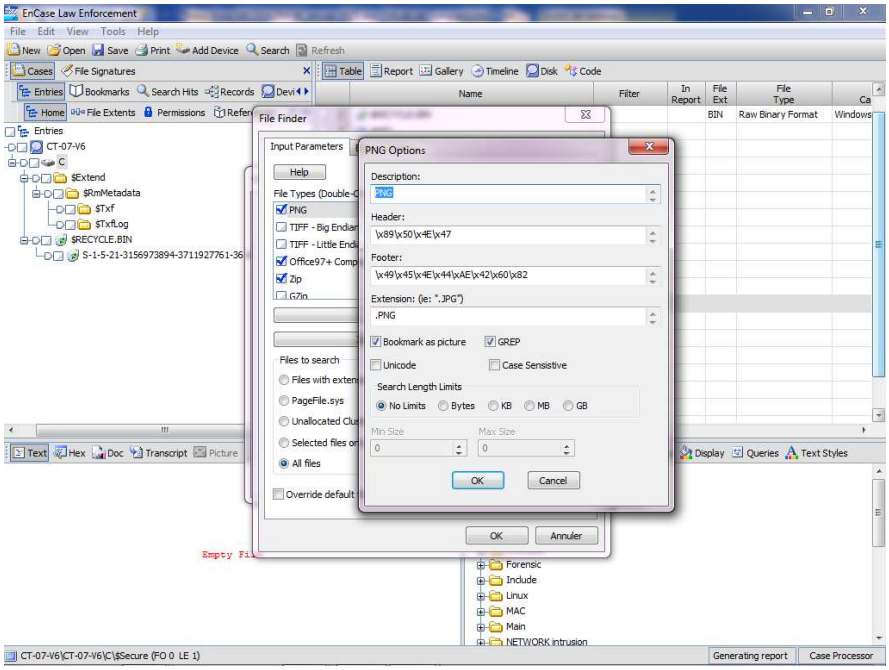
Capture d'écran du SSD dans Encase V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 6.18.1 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: Tableau  Date de la copie du support: 19/02/14 11:44:06
Informations relatives au support examiné:	Système de fichiers: NTFS Marque: Samsung Modèle: SSD 840 EVO 250G Numéro de série: S1DBNSAF834070B Capacité : 250 059 350 016 octets (232,9GB) Nombre de secteurs: 488 397 168 Signature disque 643A47F8 Partitions Valide

Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: a140c44911462fc549e9f2207e95845c Vérification MD5: a140c44911462fc549e9f2207e95845c
Observations :	*Après avoir réalisé la copie du SSD, nous avons fait une deuxième copie du support et avons calculé les empreintes numériques pour comparer les résultats. Aucune divergence entre les deux copies n'a été relevée, les algorithmes MD5 restent identiques dans les deux cas de testés.
Détail des résultats obtenus:	Au total, Encase® répertorie 252 fichiers dans la corbeille : *Tous les fichiers tests supprimés restent intacts et sont récupérables via la fonction « Copy/UnErase » permettant de les exporter directement depuis l'interface du logiciel. Les noms des fichiers n'ont subi aucune modification. *Le logiciel affiche également 121 fichiers d'index dont le nom commence par les lettres $I et sont associés aux fichiers d'origines. * 9 fichiers métadonnées "OECustomProperty" sont également associés aux courriels. Ils contiennent des informations relatives notamment à l'expéditeur ou destinataire... *Fichier « desktop.ini » généré par Windows est aussi présent dans la corbeille.

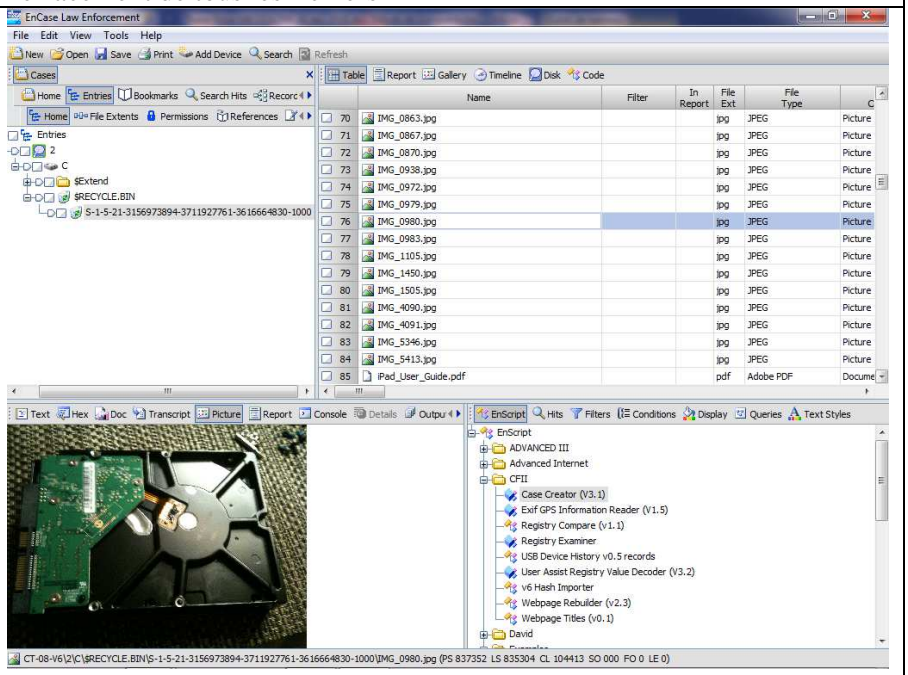
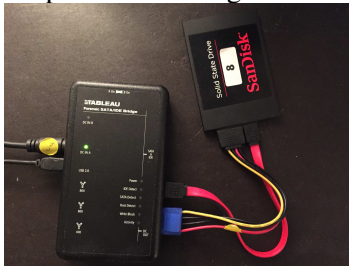
3.3.2.1.7 Cas de test CT-07-V6

Référence Cas de test: CT-07-V6	
Outil testé	**Encase Forensic version 6.18.1**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur un SSD suite à un formatage du support

Capture d'écran du SSD dans Encase V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 6.18.1 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: Tableau  Date de la copie du support: 27/12/14 12:40:09
Informations relatives au support examiné:	Système de fichiers: NTFS Marque: KINGSTON Modèle: SV300S37A 60G Numéro de série: 50026B7749039E49 60 022 480 896 octets (55,9GB) Nombre de secteurs: 117 231 408 Signature disque: 5BD4AA2D Partitions: Valide

Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: 2bfcbfe7ef924a5f338c78ea2742876f Vérification MD5: 2bfcbfe7ef924a5f338c78ea2742876f GUID 835442b2859da940b30d807c75ba99a4
Observations	Après avoir réalisé la copie du SSD, nous avons réalisé une deuxième copie du support et calculé l'empreinte numérique du disque afin de comparer les deux résultats. Nous avons constaté aucune divergence entre les deux copies, les algorithmes MD5 restent identiques dans les deux cas de figures.
Détail des résultats obtenus:	*Le module "*recover folders*" ne récupère aucune donnée effacée. *Afin de reconstituer les fichiers, la méthode du "*Carving*" a été utilisée pour rechercher les types de fichiers suivants: [.doc, xls, png, jpg, eml, mp3, mp4, avi, flv, zip, 3gp, pps].  Les fichiers compressés au format "zip", les images, vidéos aux formats "flv" et "Avi" ont tous été reconstitués. Mais de nombreux résultats ont été retrouvés nécessitant un tri pour éliminer les informations non-exploitables. Concernant les photographies retrouvées, certaines d'entre elles sont normalement insérées dans les fichiers tels que Word de Microsoft. Dans l'hypothèse d'un formatage de support et de recherches au niveau des espaces non-alloués, il est difficile de faire une distinction entre les images insérées dans un fichier et les fichiers photos.

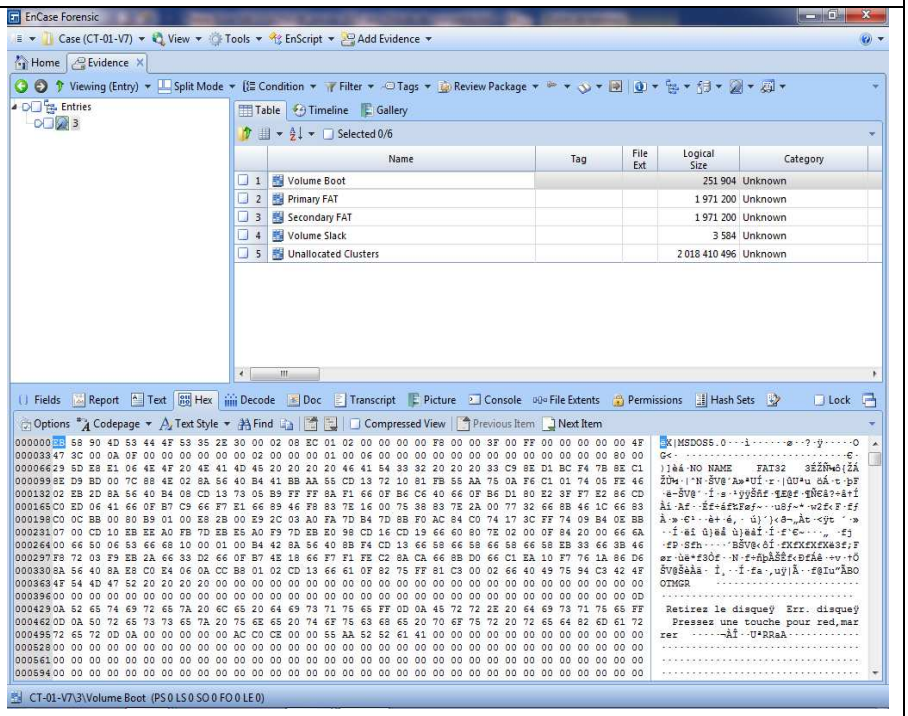
3.3.2.1.8 Cas de test CT-08-V6

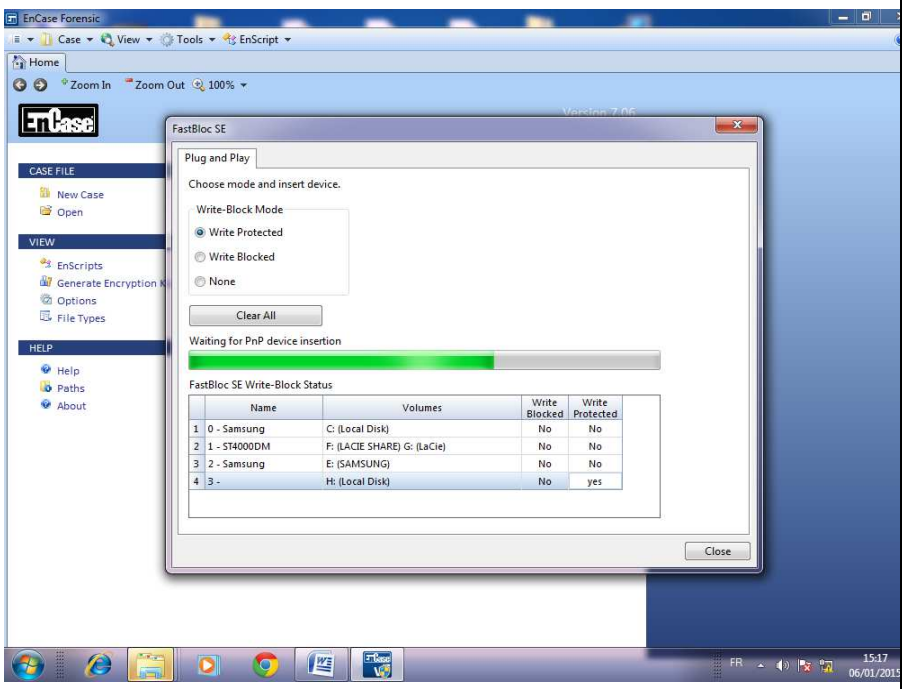
Référence Cas de test: CT-08-V6	
Outil testé	**Encase Forensic version 6.18.1**
Description du cas de test:	Recherche cent vingt et un fichiers effacés sur un disque dur SSD suite à l'effacement de tous les fichiers
Capture d'écran du disque SSD dans Encase V6.18.1	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 6.18.1 Version du système d'exploitation Windows 7 Dispositif de blocage en écriture: Tableau  Date de la copie du support: 03/01/15 13:44:36

Informations relatives au support examiné:	Système de fichiers: NTFS Marque: SanDisk Modèle: SDSSDP064G Numéro de série: 143906400721 63 023 063 040 Bytes (58,7GB) Nombre de secteurs: 123 091 920 Signature disque: 9C943B84 Partitions: Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: 4764d6b7d9a5d271c5a35aae44f2de0a Vérification MD5: 4764d6b7d9a5d271c5a35aae44f2de0a GUID 87beb13e11f63e46bb9c1a87795a6d7f
Observations	Nous avons réalisé une deuxième copie du support et avons calculé son empreinte numérique afin de la comparer avec celle de la première copie. Aucune divergence entre les deux copies n'a été relevée, les algorithmes MD5 restent identiques dans les deux cas de figures.
Détail des résultats obtenus:	L'interface du logiciel Encase affiche au total 252 fichiers placés dans la corbeille: *121 fichiers supprimés sont restés intacts et restent aisément récupérables via la commande "Copy/UnErase" du programme. Le nom des fichiers n'a pas subi d'altération. *Le logiciel affiche également 121 autres fichiers d'index dont le nom a été modifié et commence par la lettre $I. Le logiciel les associe à leurs fichiers d'origines. *9 fichiers “OECustomProperty” contiennent des métadonnées des courriels qui leurs sont associés. Il s'agit notamment des informations relatives à l'objet ou courriers électroniques des expéditeurs et destinataires. *1 fichier « desktop.ini » généré par Windows est aussi présent dans la corbeille.

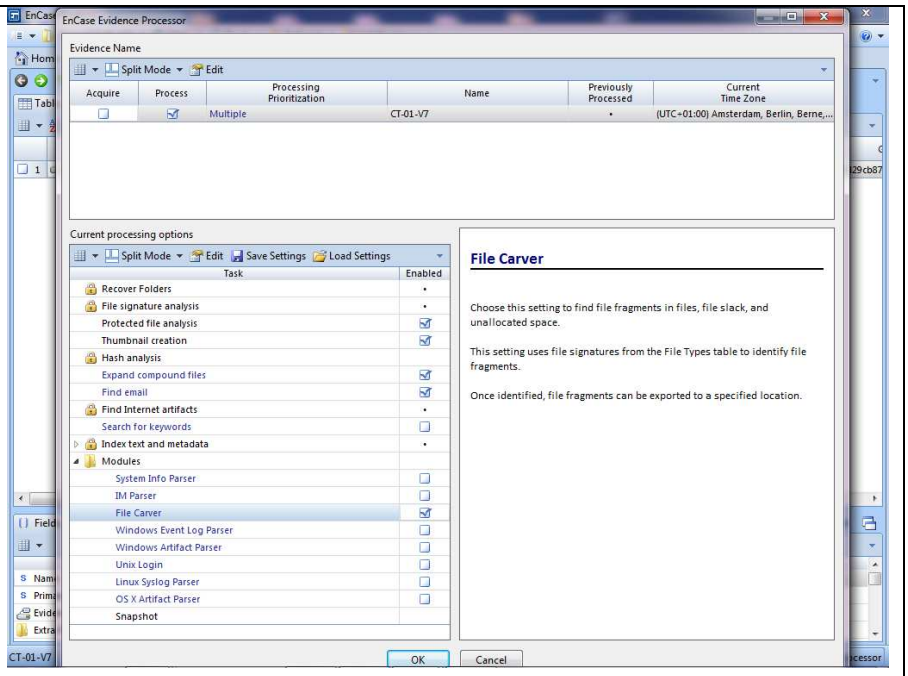
3.3.2.2 Rapports de tests Encase® version 7.06

3.3.2.2.1 Cas de test CT-01-V7

Référence Cas de test: CT-01-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une clé USB suite à un formatage rapide de celle-ci.
Capture d'écran de la clé USB formatée dans Encase version 7.06	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.

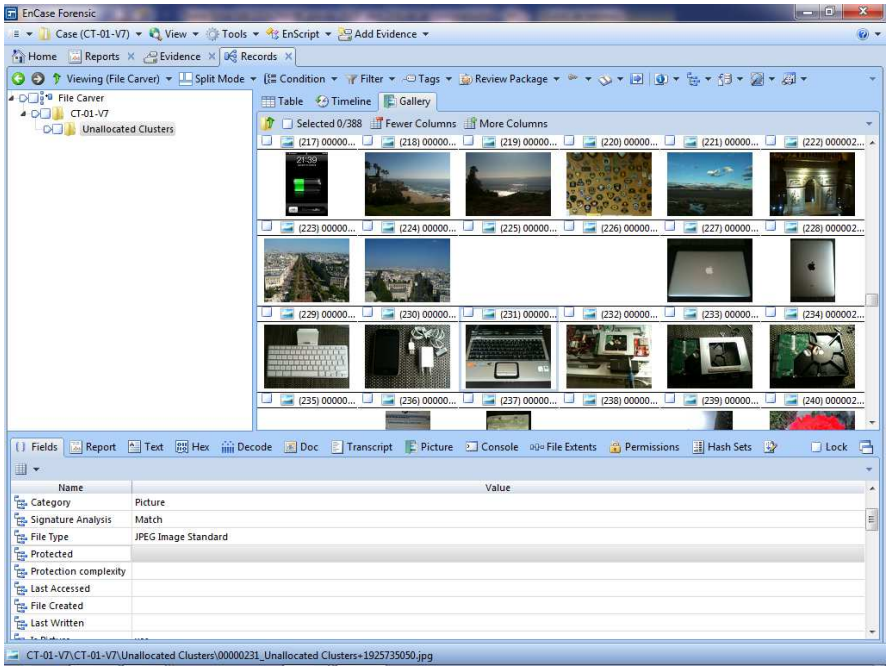
Informations sur la machine et matériels de tests	EnCase Version 7.06 Versiondu système d'exploitation :Windows 7 Dispositif de blocage en écriture: "F²astBloc SE"  Date de la copie du support: 06/01/15 15:31:08
Informations relatives au support examiné:	Système de fichiers: FAT32 Capacité : 2 022 612 480 octets (1,9GB) Nombre de secteurs: 3 950 415 Signature disque 20646973 Partitions Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: c7e76831fbf9c5be25fead9d9775db30 Vérification MD5: c7e76831fbf9c5be25fead9d9775db30 Acquisition SHA1: F6FC4554043FF3EA9BE17CBB2C885E51F42D8524
	*La commande "*Recover folders*" n'apporte aucun résultat. *Nous avons procédé à une analyse de "Carving" dans les espaces non-alloués du support afin de rechercher différents types de fichiers [.doc, xls, png, jpg, eml, mp3, mp4, avi, flv, zip, 3gp, pps] :

Détail des résultats obtenus:



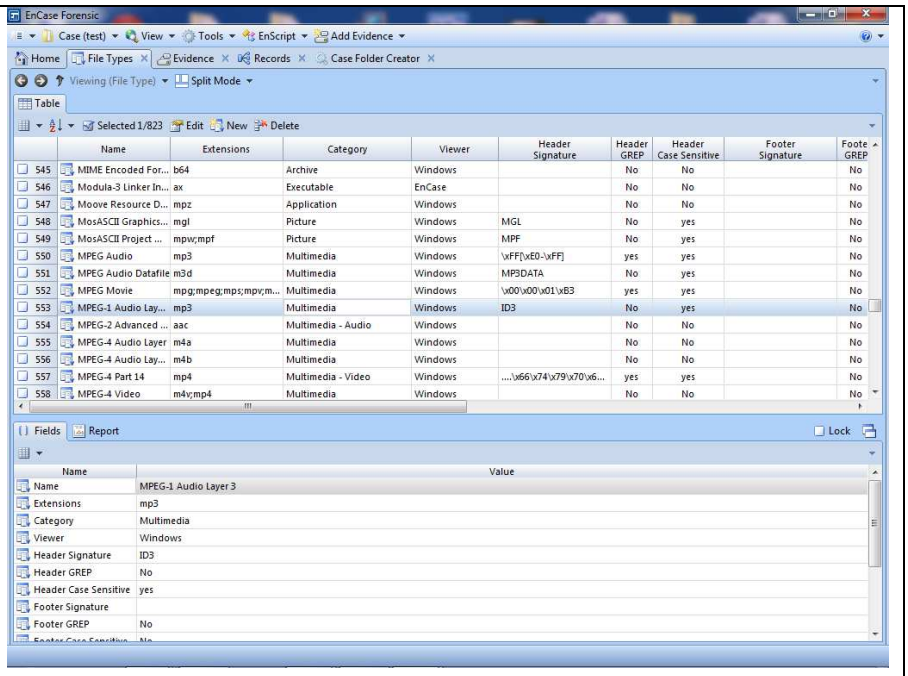
Ces recherches ont permis de récupérer un nombre important de fichiers.

La copie écran ci-dessous illustre des résultats d'images reconstitués.

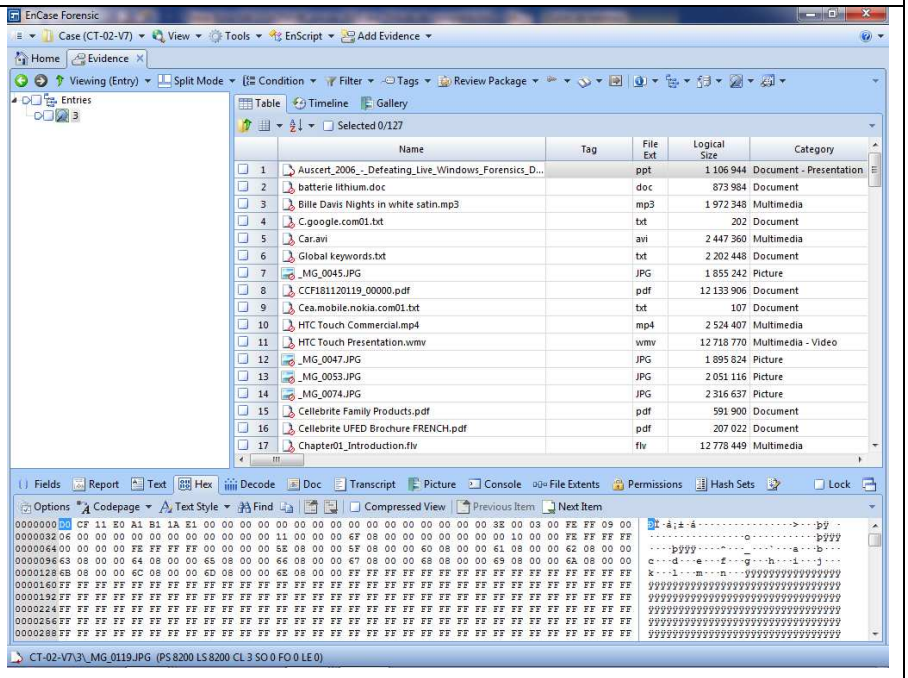


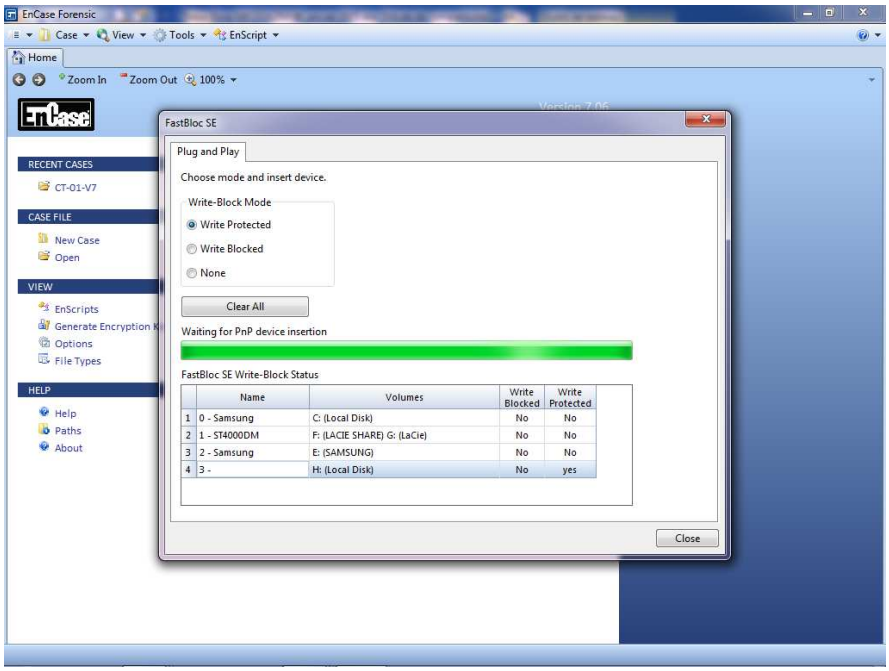
-Certains types de fichiers comme ceux au format mp4 et 3gp, n'ont pas été tous récupérés directement par le module automatisé du carving.

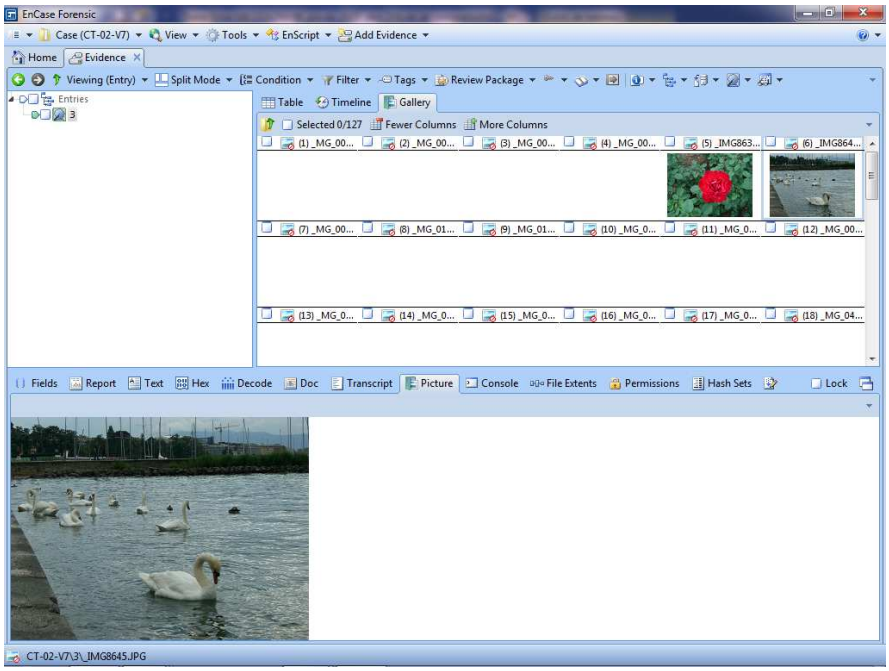
Pour trouver ces fichiers vidéos, nous avons procédé à une analyse manuelle en rentrant les informations relatives à l'en-tête et la fin de fichiers.

3.3.2.2.2 Cas de test CT-02-V7

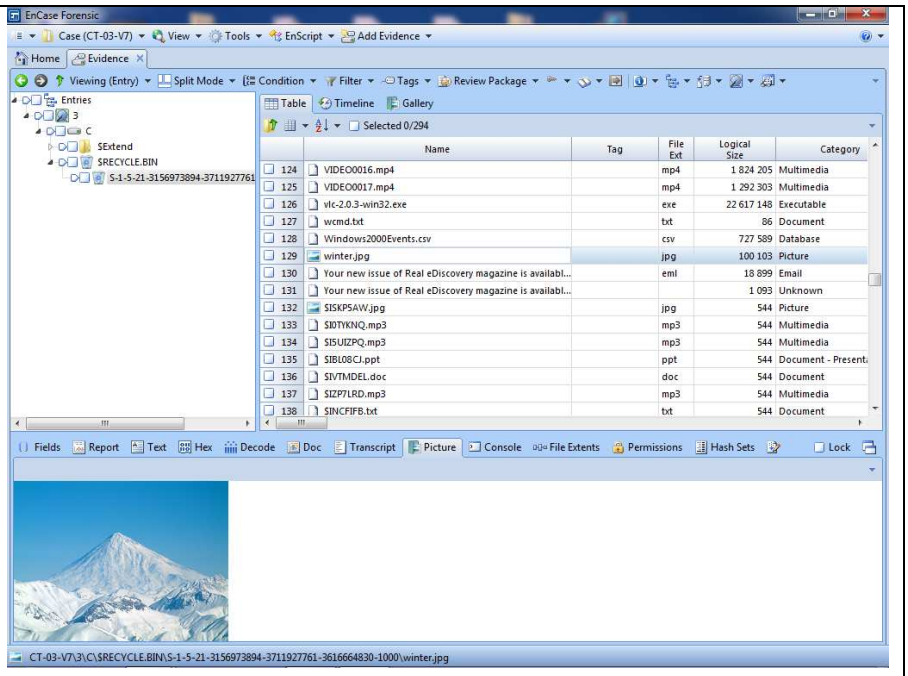
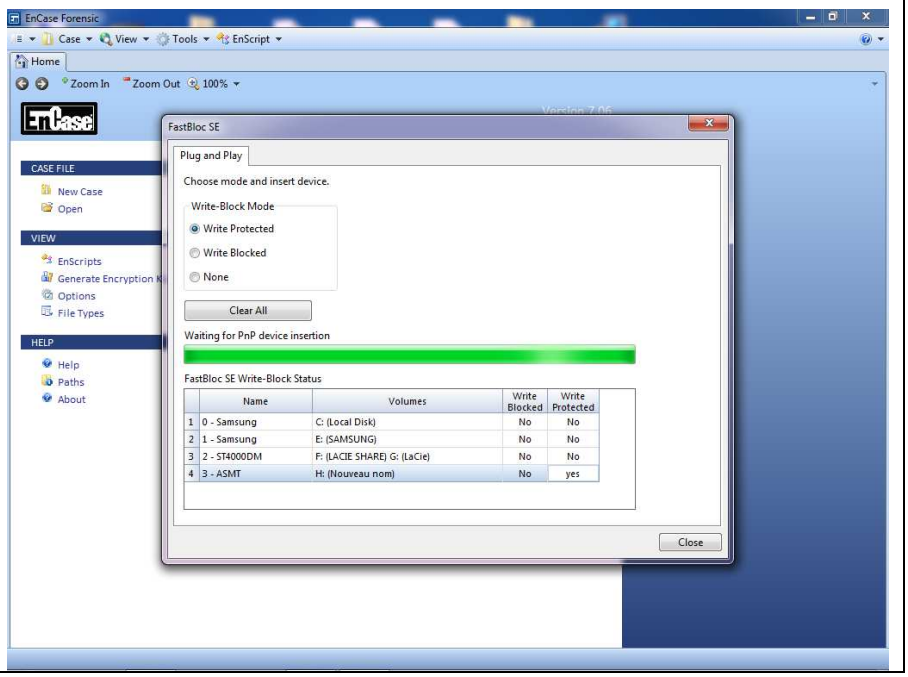
Référence Cas de test: CT-02-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une clé USB suite à la suppression de tous les fichiers du support.
Capture d'écran de la clé USB avec les fichiers effacés dans Encase version 7.06	

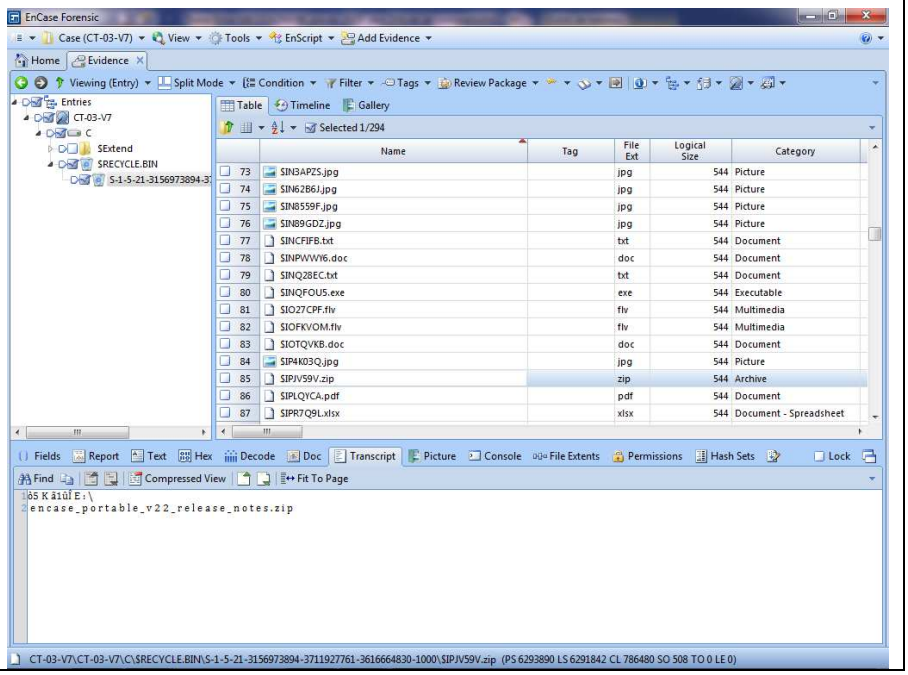
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 7.06 Version système d'exploitation : Windows 7 Dispositif de blocage en écriture: "FastBloc SE"  Date de la copie du support : 06/01/15 16:21:35
Informations relatives au support examiné:	Système de fichiers: FAT32 Capacité : 2 021 654 528 octets (1,9GB) Nombre de secteurs: 3 948 544 Signature disque 20646973 Partitions Valide
Calcul de l'intégrité des données:	Intégrité : vérifiée, 0 Erreur Acquisition MD5: 301C9BB11AE65A82237AAA33C56D98B9 Vérification MD5: 301C9BB11AE65A82237AAA33C56D98B9 Acquisition SHA1: 12E68E89270D77621551F257D22E95CF146621D8

Observations:	*Tous les fichiers effacés sont référencés par Encase et leur nom reste intact. Pour certains d'entre eux, la première lettre est remplacée par le symbole "_". Mais la majorité des fichiers semble altérée. A titre d'illustration, parmi tous les fichiers au format images, seulement deux fichiers ne sont pas endommagés:  *La commande "*Recover folders*" ne permet de récupérer aucun fichier. *La majorité des fichiers sont corrompus mais certains fichiers ne nécessitent pas de recherches complémentaires car ils sont directement récupérables à partir de l'interface du programme.

3.3.2.2.3 Cas de test CT-03-V7

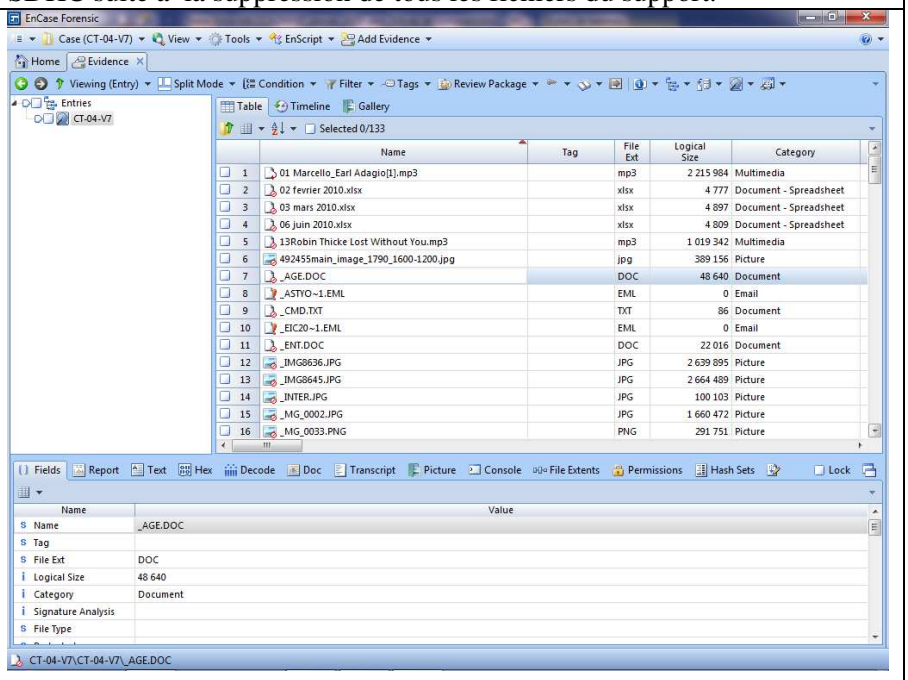
Référence Cas de test: CT-03-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur un disque dur interne du type SATA suite à la suppression de tous les fichiers du support.

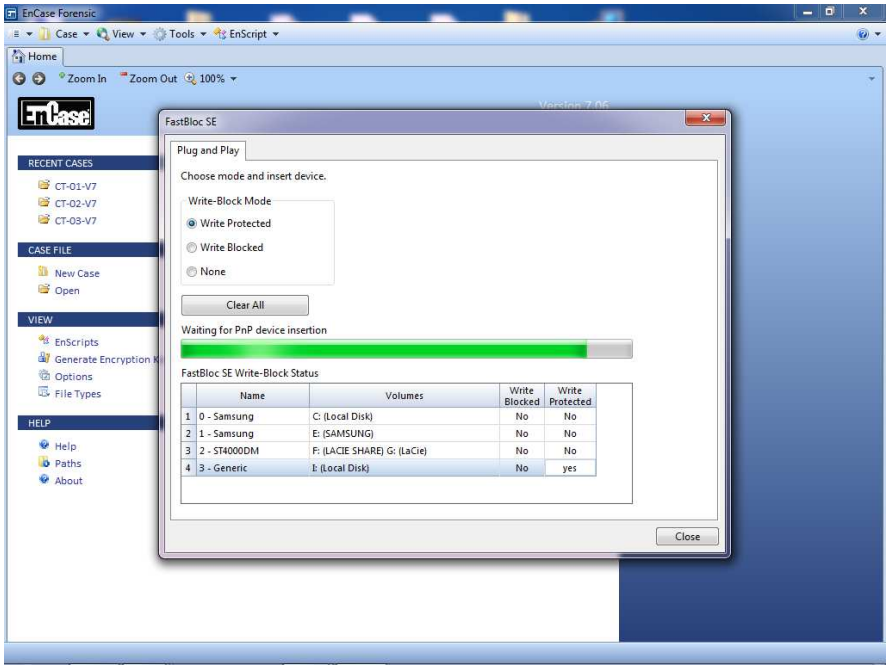
Capture d'écran du disque dur interne SATA avec les fichiers effacés dans Encase V7.06	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase version 7.06 Version du système d'exploitation Windows 7 Dispositif de blocage en écriture: "FastBloc SE" 

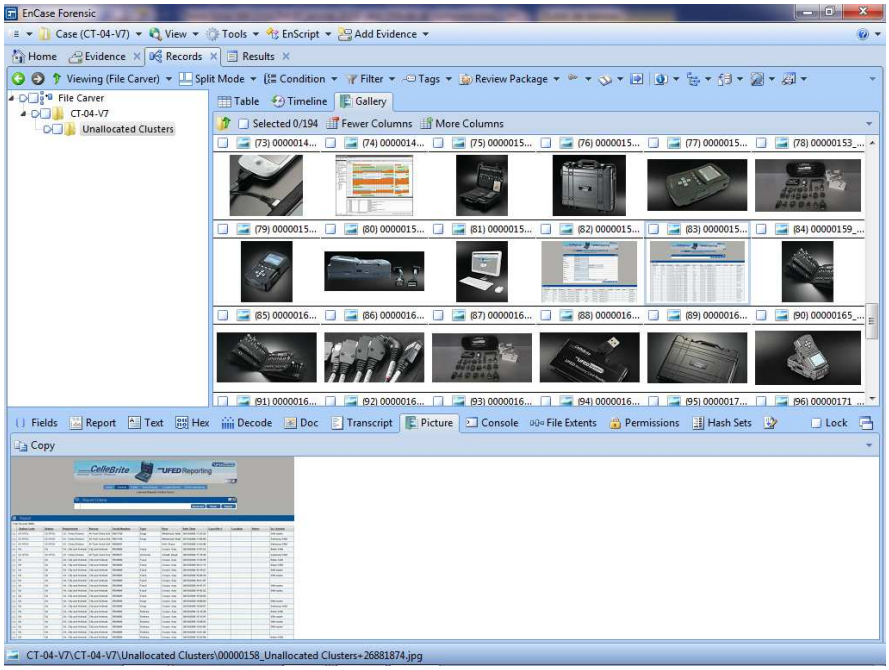
	Date de la copie du support: 07/01/15 17:54:16
Informations relatives au support examiné:	Système de fichiers: NTFS Capacité : 250 059 350 016 (232,9GB) Nombre de secteurs: 488 392 704 Signature disque FB6B1998 Partitions Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: AFF92BB0630733AC3397C581CE71AB36 Vérification MD5: AFF92BB0630733AC3397C581CE71AB36 Acquisition SHA1: 68BC887CA84630A68E8E025ED8183B04074224F8
Détail des résultats obtenus:	Encase® répertorie au total 252 fichiers dans la corbeille: On y retrouve la totalité des fichiers effacés ainsi que des fichiers d'Index et des métadonnées associées aux E-mails : * 121 fichiers supprimés sont directement récupérables depuis l'interface du logiciel avec la fonction « *Copy/UnErase* ». Le nom des fichiers n'a pas subi d'altération. * 121 fichiers d'index dont le nom commence par la lettre $I : Le logiciel les associe aux fichiers d'origines (liste ci-dessous non exhaustive): - $ILO5NED.zip = E x i f _ R e a d e r _ 3 . 0 . z i p -$IN3APZS.jpg = I M G _ 0 1 6 0 . j p g 

	* 9 fichiers métadonnées “OECustomProperty” sont associés aux Emails avec des informations relatives à l’expéditeur ou le destinataire… *Fichier « desktop.ini » généré par Windows se trouve également présent dans la corbeille.

3.3.2.2.3 Cas de test CT-04-V7

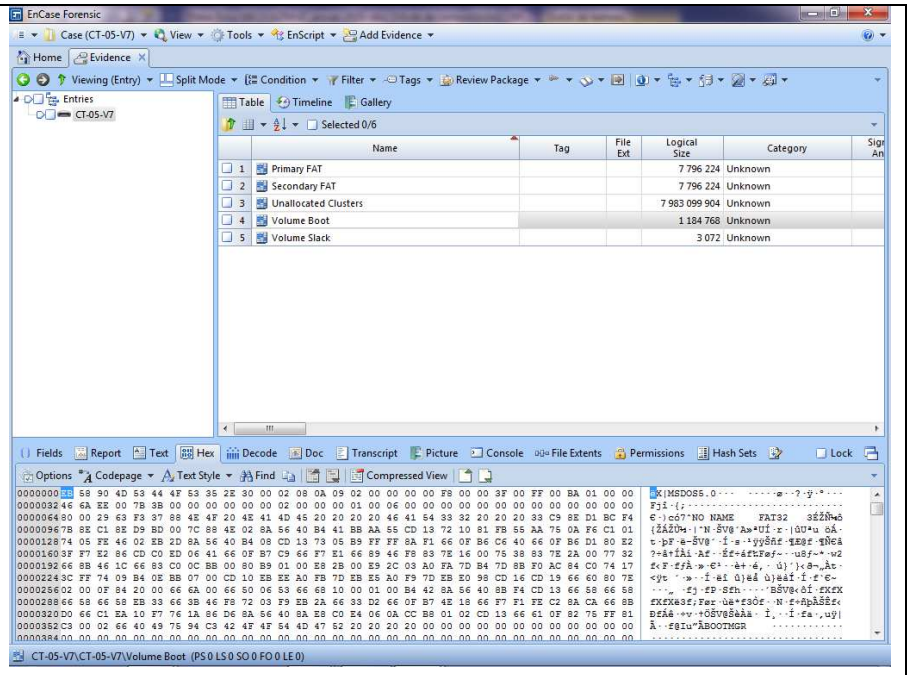
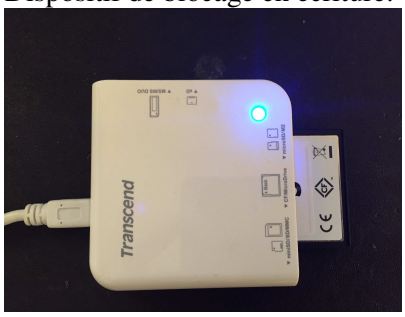
Référence Cas de test: CT-04-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une carte mémoire SDHC suite à la suppression de tous les fichiers du support.
Capture d'écran de la carte SD avec les fichiers effacés dans Encase V 7.06	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase version 7.06

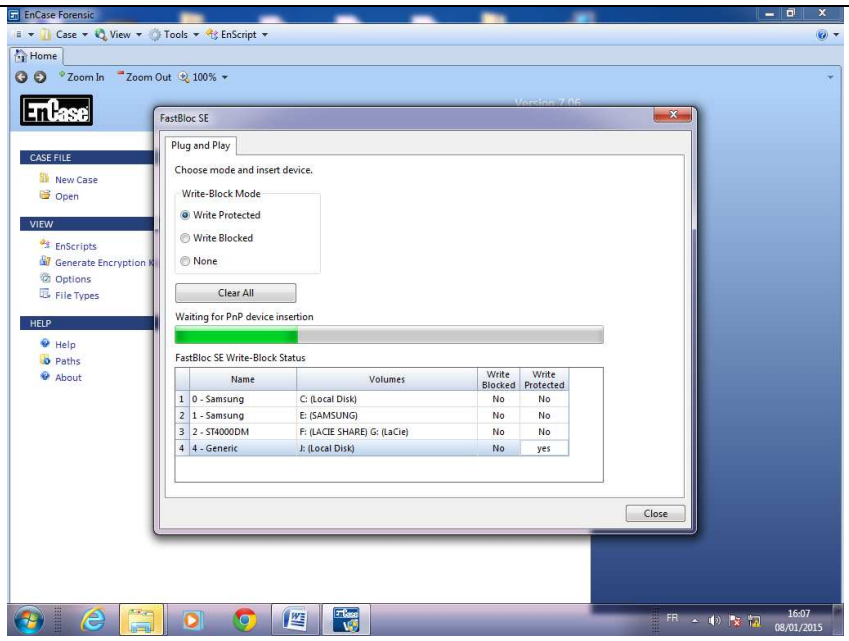
	Version système d'exploitation Windows 7 Dispositif de blocage en écriture: "FastBloc SE"  Date de la copie du support : 07/01/15 21:49:21
Informations relatives au support examiné:	Système de fichiers: FAT32 Numéro de série: A815-8EF4 Capacité : 3 965 190 144 octets (3,7GB) Nombre de secteurs: 7 744 512 Signature disque 20646973 Partitions Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: e33a7af5d4c1b9e6ede5d84931895c9d Vérification MD5: e33a7af5d4c1b9e6ede5d84931895c9d Acquisition SHA1: 8b820ae6a463d9ce0cf2b457b2436d6c3f9c92db Vérification SHA1: 8b820ae6a463d9ce0cf2b457b2436d6c3f9c92db
Détail des résultats obtenus:	*Le logiciel répertorie au total 128 fichiers : 118 fichiers effacés, 2 fichiers irrécupérables et 7 fichiers associés aux clusters invalides. Les noms des fichiers n'ont pas été altérés mais pour certains d'entre eux, la première lettre est remplacée par le symbole "_". * 95 fichiers sont corrompus et leur contenu n'est pas exploitable. La méthode traditionnelle de la récupération des données étant inefficace, une recherche avec le module "File Carver" a été effectuée afin de reconstituer différents formats de fichiers [.doc, xls, png, jpg, eml, mp3, mp4, avi, flv, zip, 3gp, pps].

	Cette technique permet de récupérer les informations en procédant à une analyse de signature sur les espaces non alloués du support :  -Certains fichiers ont pu être entièrement reconstruits mais leur nom d'origine n'a pas été récupéré. *Concernant la recherche d'images, le logiciel retrouve toutes les images disponibles y compris celles qui sont initialement insérées dans un document du type "Pdf" ou "Word". *Parmi les fichiers aux formats "3gp" et "mp4", beaucoup de résultats sont générés mais seulement deux fichiers ont été correctement reconstitués.

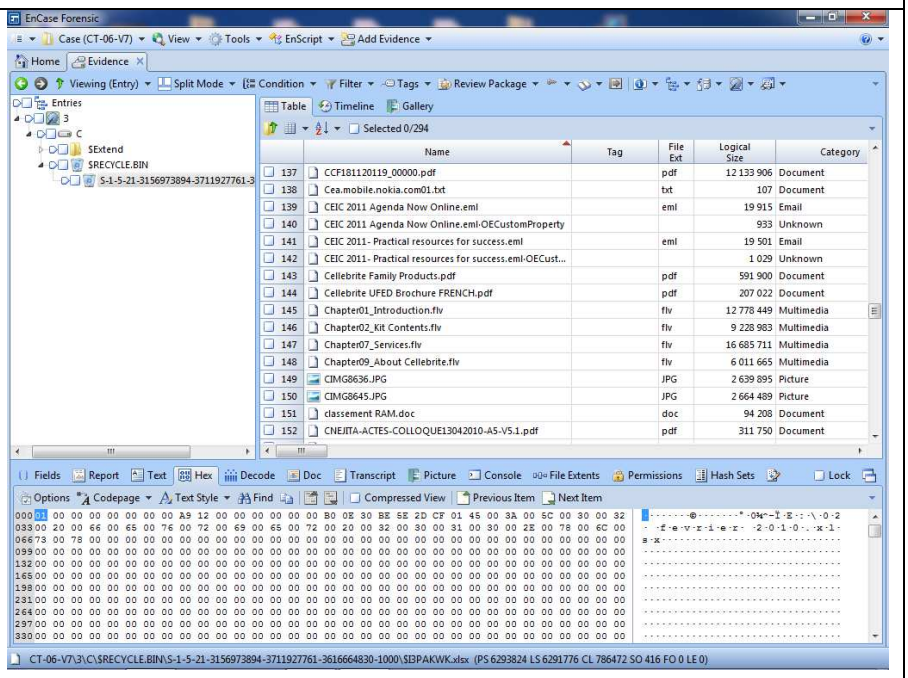
3.3.2.2.3 Cas de test CT-05-V7

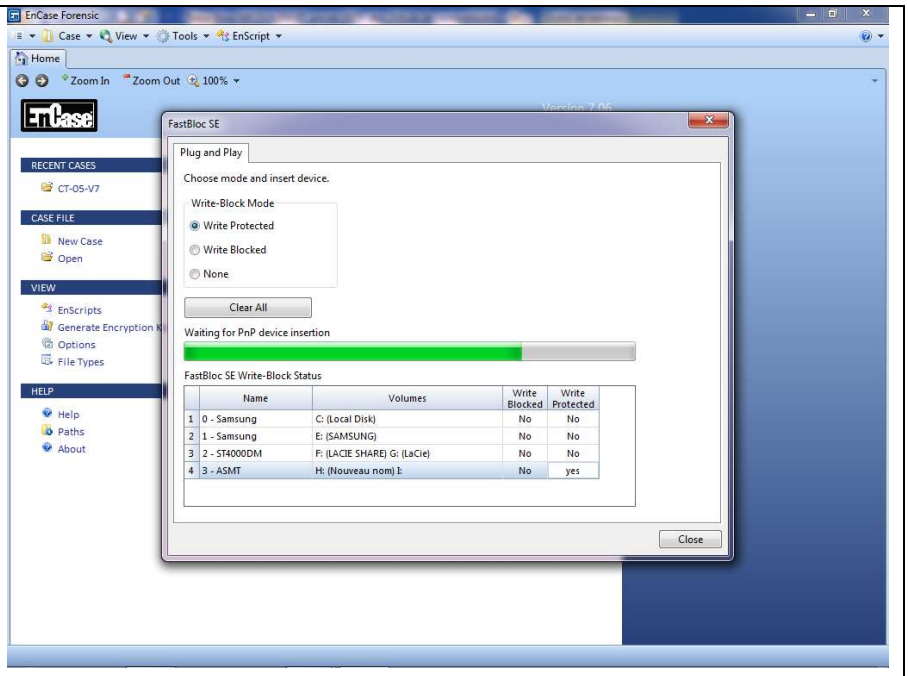
Référence Cas de test: CT-05-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur une carte mémoire Compact Flash suite au formatage du support.

Capture d'écran de la carte compact Flash dans Encase V7.06	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 7.06 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: "FastBloc SE"  Date de la copie du support: 08/01/15 16:16:12

	
Informations relatives au support examiné:	Système de fichiers: FAT32 Capacité : 8 000 110 592 (7,5GB) Nombre de secteurs: 15 625 216 Signature disque - Partitions Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: f517b2b94dfd0cb2443359f6b992e1c6 Vérification MD5: f517b2b94dfd0cb2443359f6b992e1c6 Acquisition SHA1: e82fee76c3bca96068387a09585dffeaf3db4dfa Vérification SHA1: e82fee76c3bca96068387a09585dffeaf3db4dfa
Détail des résultats obtenus:	*Le volume étant formaté, l'interface du logiciel n'affiche aucun fichier. *La fonction "*Recover folders*" ne permet de trouver aucune information. *Nous avons réalisé une recherche au niveau des espaces non-alloués en utilisant le module "*file carver*" afin de récupérer les différents types de fichiers recherchés: [.doc, xls, png, jpg, eml, mp3, mp4, avi, flv, zip, 3gp, pps]. -En ce qui concerne les fichiers compressés au format "zip", le logiciel ENCASE® a récupéré l'ensemble des fichiers effacés mais le programme a identifié un nombre important de fichiers dont un grand nombre est inexploitable. Un grand tri a été réalisé afin de retrouver les fichiers recherchés. -Il en est de même pour les fichiers " images". De nombreux fichiers ont pu être reconstitués par Encase®, il s'agit principalement de photos insérées à l'intérieur des documents.

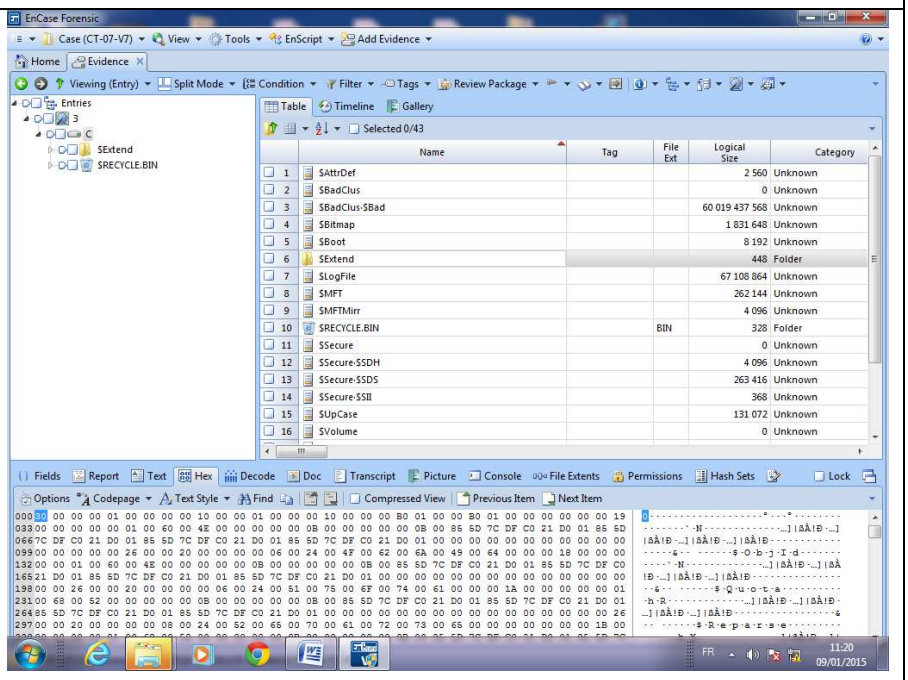
3.3.2.2.6 Cas de test CT-06-V7

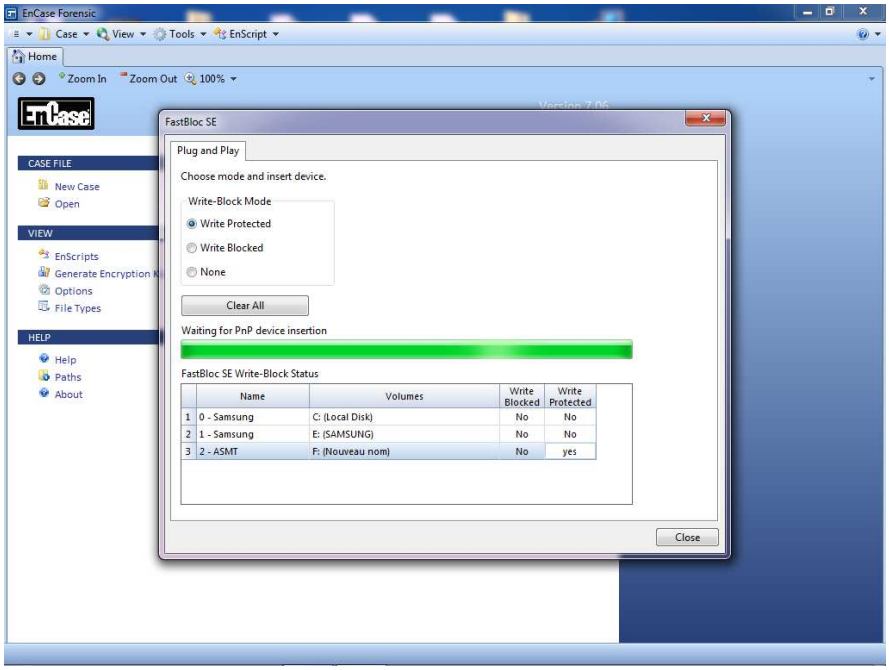
Référence Cas de test: CT-06-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur un SSD suite à la suppression des fichiers du support.
Capture d'écran du disque SSD dans Encase V7.06	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 7.06 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: "FastBloc SE"

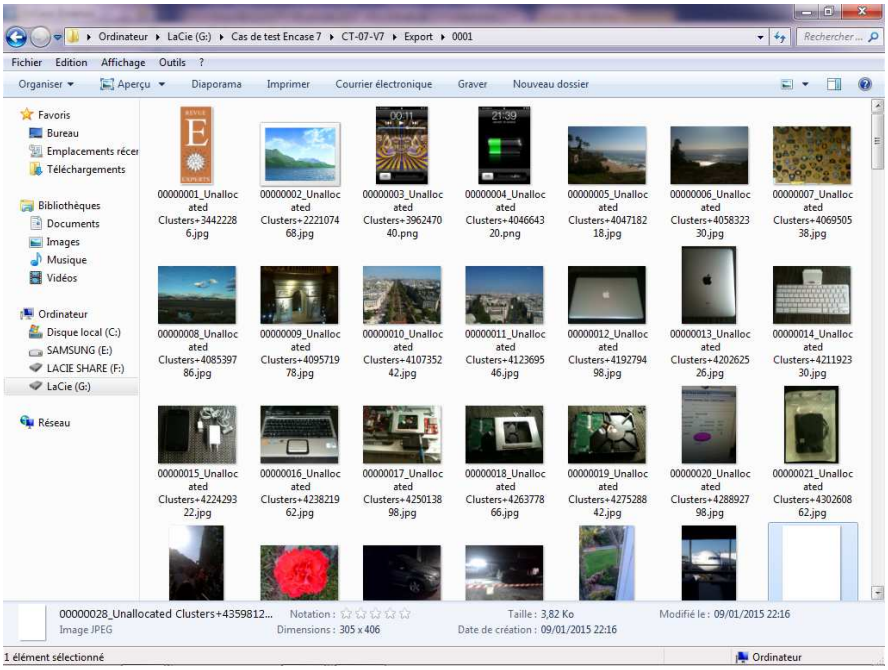
	 Date de la copie du support: 08/01/15 20:41:31
Informations relatives au support examiné:	Système de fichiers: NTFS Capacité : 250 059 350 016 octets (232,9GB) Nombre de secteurs: 488 397 168 Signature disque 643A47F8 Partitions Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: a140c44911462fc549e9f2207e95845c Verification MD5: a140c44911462fc549e9f2207e95845c Acquisition SHA1: A1813F8CFF370C5D54201352FB0523A83343CC11
Observations	*Après avoir réalisé une copie du support SSD, nous avons fait une deuxième copie du support. Les empreintes numériques des deux supports ont ensuite été comparées. Aucune différence entre les deux copies n'a été constatée, les algorithmes MD5 restent identiques dans les deux cas de figures.
	Encase® répertorie au total 252 fichiers dans la corbeille : *L'ensemble des fichiers supprimés sont directement récupérables depuis l'interface du logiciel et aucune recherche ne s'avère nécessaire. Les noms des fichiers n'ont subi aucune altération. La fonction « *Copy/UnErase* » du programme permet d'exporter aisément la totalité des fichiers. *Le logiciel affiche également 121 fichiers d'index dont le nom

Détail des résultats obtenus:	commence par les lettres $I et sont associés aux fichiers d'origines. Depuis la version de Windows Vista, le nom de la corbeille a été remplacé par "$Recycle.Bin" et les informations contenues dans le fichier "INFO2" sont désormais enregistrées dans un fichier d'index dont le nom commence par les lettres $I. *9 fichiers du type métadonnées "OECustomProperty" sont associés aux courriers électroniques et contiennent des informations relatives à l'expéditeur ou au destinataire des courriels. *Nous n'avons identifié aucune différence entre les valeurs HASH.

3.3.2.2.7 Cas de test CT-07-V7

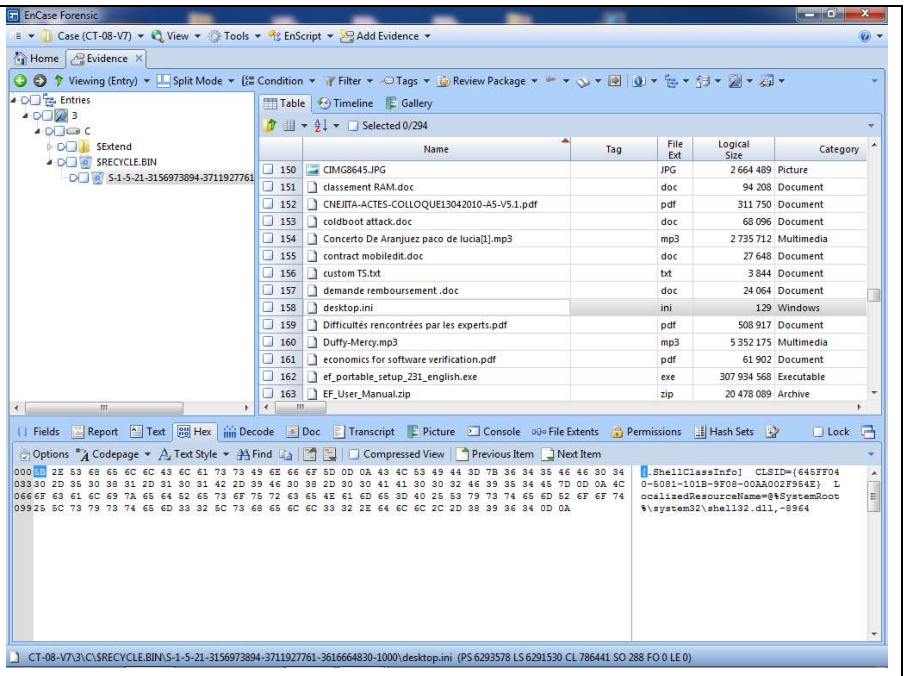
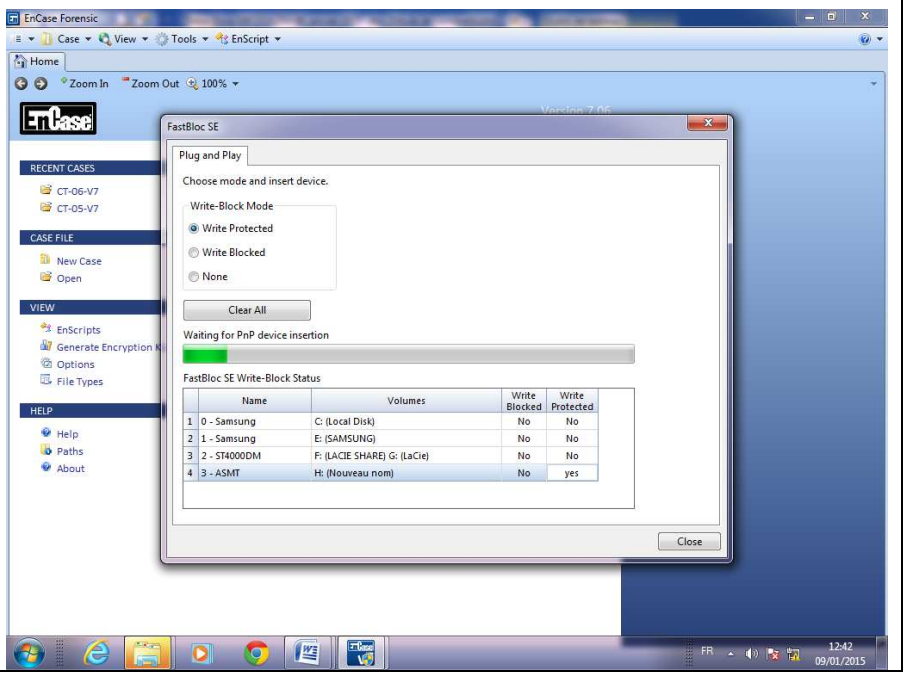
Référence Cas de test: CT-07-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche de cent vingt et un fichiers effacés sur un SSD suite au formatage du support
Capture d'écran du disque SSD dans Encase V7.06	

Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 7.06 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: "FastBloc SE"  Date de la copie du support: 09/01/15 12:04:04
Informations relatives au support examiné:	Système de fichiers: NTFS 60 022 480 896 octets (55,9GB) Nombre de secteurs: 117 231 408 Signature disque: 5BD4AA2D Partitions: Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: 2bfcbfe7ef924a5f338c78ea2742876f Vérification MD5: 2bfcbfe7ef924a5f338c78ea2742876f Acquisition SHA1: EEFD520BEAB6CD6600B82D6C24FF52F3F9725414
Observations	Après avoir fait une acquisition physique du SSD, nous avons réalisé une deuxième copie du support.

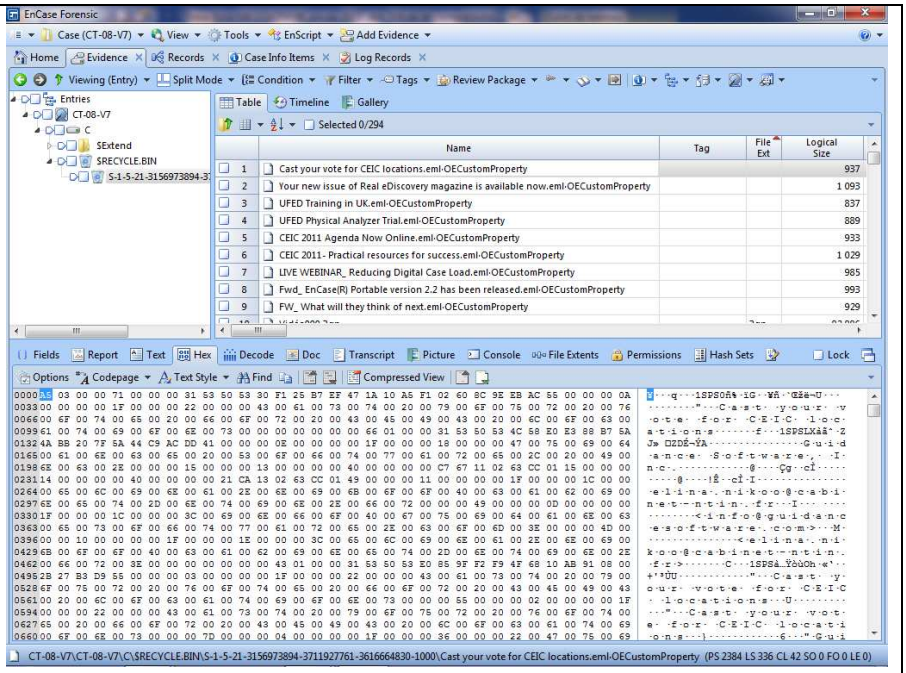
	Aucune différence de résultat n'a été constatée entre les deux copies, les algorithmes MD5 sont identiques dans les deux cas de tests.
Détail des résultats obtenus:	*La fonction "*recover folders*" ne trouve aucune donnée effacée. *Le module "*file carver* " a permis de récupérer différents types de fichiers dans les espaces non alloués du support : [.doc, xls, png, jpg, eml, mp3, mp4, avi, flv, zip, 3gp, pps]. Tous les fichiers "zip", images et vidéos aux formats "flv" et "Avi" ont été reconstitués. Les noms d'origines des fichiers récupérés dans les espaces non alloués du support ont été altérés. 

3.3.2.2.8 Cas de test CT-08-V7

Référence Cas de test: CT-08-V7	
Outil testé	**Encase Forensic version 7.06**
Description du cas de test:	Recherche cent vingt et un fichiers effacés sur un SSD suite à l'effacement de tous les fichiers

Capture d'écran du disque SSD dans Encase V7.06	
Exigences générales testées	E-1.Identifie les informations relatives au support de stockage, E-2.Récupère tous types de fichiers supprimés, E-3.Localise les fichiers supprimés, E-4.Récupère les données supprimées présentes dans la corbeille, E-5.Récupère dans les espaces non-alloués, E-6.Indique le chemin original du fichier effacé, E-7.Récupère des données par analyse de signature.
Informations sur la machine et matériels de tests	EnCase Version 7.06 Version du système d'exploitation : Windows 7 Dispositif de blocage en écriture: "FastBloc SE" 

	Date de la copie du support: 09/01/15 13:32:13
Informations relatives au support examiné:	Système de fichiers: NTFS 63 023 063 040 octets (58,7GB) Nombre de secteurs: 123 091 920 Signature disque: 9C943B84 Partitions: Valide
Calcul de l'intégrité des données:	Intégrité : Vérifiée, 0 Erreur Acquisition MD5: 4764d6b7d9a5d271c5a35aae44f2de0a Vérification MD5: 4764d6b7d9a5d271c5a35aae44f2de0a Acquisition SHA1: 5C3B2C9DEA9B246EE522AF40A2C7FB4BD33B6ADF
Observations	Deux copies du support ont été réalisées et leurs empreintes numériques ont été comparées. Aucune différence entre les deux copies n'a été constatée, les algorithmes MD5 restent identiques dans les deux cas de tests. Cette situation peut s'expliquer par le fait que le support SSD ne contient que très peu d'informations. De plus, à l'issue de la suppression des fichiers, il n'y a pas eu de réecritures de données.En général, les pertes des données arrivent plus aisément sur les disques dont les cellules sont fréquemment utilisées.
Détail des résultats obtenus:	Le logiciel Encase répertorie au total 252 fichiers placés dans la corbeille: * 121 fichiers supprimés sont facilement récupérables avec la commande "*Copy/UnErase*" du programme. Le nom des fichiers n'a pas été modifié. *Le logiciel affiche également 121 autres fichiers d'index dont les noms ont été modifiés et commencent par la lettre $I. *9 fichiers “OECustomProperty” contiennent des métadonnées en lien avec les messages électroniques qui leurs sont associés. Ces informations concernent notamment l'expéditeur ou le destinataire du message:



*1 fichier « desktop.ini » généré par Windows est également présent dans la corbeille.

3.3.2 Synthèse des résultats obtenus par les deux versions du logiciel Encase

Les tests ont été menés sur huit supports informatiques composés de deux clés USB, un disque dur interne SATA, une carte mémoire SD, une carte mémoire compact flash et trois supports SSD.

Les recherches ont porté sur cent vingt et un fichiers supprimés avec dix-neuf extensions différentes :

Formats de fichiers recherchés	Nombre de fichiers recherchés
3gp	1
avi	2
csv	1
doc	12
eml	9
exe	8
flv	5

jpg	36
mp3	11
mp4	4
pdf	11
png	2
pps	1
ppt	2
txt	5
wmv	1
xls	1
xlsx	3
zip	6

3.3.2.1 Encase Version 6.18.1

Cas de test : CT-01-V6
Support examiné : Clé USB CELLEBRITE

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. <u>Identifie les informations relatives au support de stockage</u> :

Le programme a listé **de nombreuses** informations relatives notamment au système de fichiers la capacité, le nombre de secteurs et la signature du support amovible.

E-2. <u>Récupère tous types de fichiers supprimés</u>:

Nos tests ont porté sur dix-neuf formats de fichiers différents.
Dans le cas d'un formatage, les données doivent êtres recherchées dans les espaces non-alloués du support notamment avec la technique de « Carving » qui permet d'analyser l'entête et la fin d'un fichier.
Certains types de fichiers comme les formats « txt » ou « csv » ne disposent pas d'en-têtes.
Dans une telle hypothèse à moins de disposer des mots clés ou d'informations sur le contenu des données, il n'est pas possible de récupérer le document recherché.

E-3. <u>Localise les fichiers supprimés:</u>

Les fichiers sont identifiés par leur offset, à titre d'illustration :
❖ Les en-têtes de courriers électroniques sont identifiées aux Offsets suivants :

918221188, 918241668, 918262148, 918283559, 918328891, 918345135, 918357065, 918373441, 918385028,

❖ Les entêtes des fichiers "pdf" se trouvent aux Offsets 12206080, 78442496, 882896896, 1957208064, 1957871616.

E-4. Récupère les données supprimées présentes dans la corbeille:

Cette exigence s'applique uniquement dans le cas des disques durs.

E-5. Récupère dans les espaces non-alloués:

Le support a fait l'objet d'un formatage. En l'absence de répertoire racine, les recherches sont menées dans les espaces non-alloués du support examiné. Différents types de recherches sont possibles mais les résultats doivent souvent faire l'objet d'un tri minutieux.

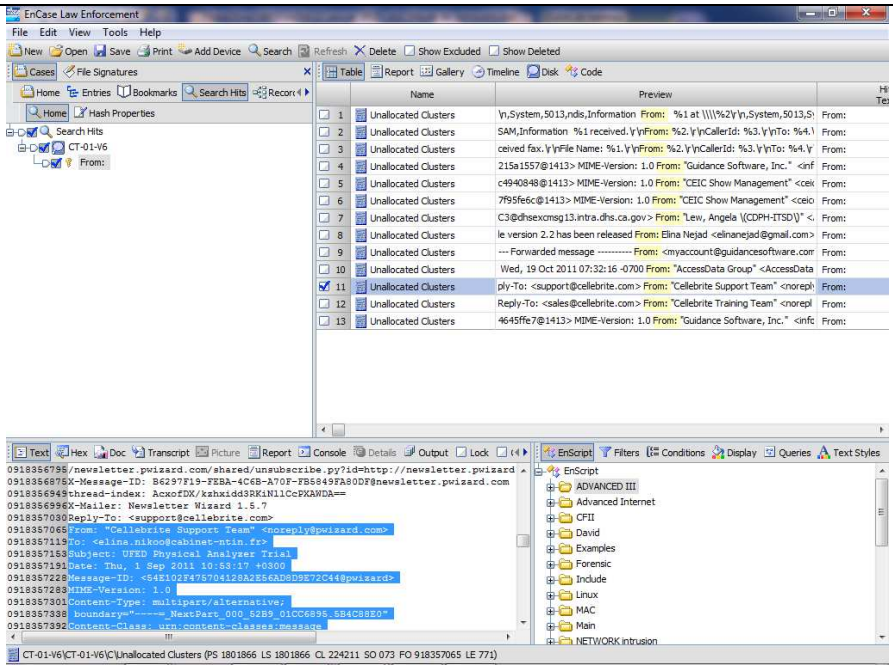
E-6. Indique le chemin original du fichier effacé:

La clé USB ayant été formatée, le chemin d'accès au répertoire racine n'existe plus.

E-7. Récupère des données par analyse de signature:

La recherche par analyse de signature permet de reconstituer un nombre important de données : Pour mener cette recherche, certains types de fichiers sont automatiquement prédéfinis par le logiciel comme les formats "BMP", "JPG", "GIF", "PNG"….
Pour d'autres formats comme les fichiers « EML » ou « PDF », les informations relatives au "carving" doivent être manuellement insérées dans le programme :

❖ Tous les courriers électroniques au format "eml" ont pu être récupérés Mais les résultats ont du être extraits manuellement :



-Cinq fichiers "pdf" sur onze ont été entièrement récupérés.
Pour les fichiers "pdf", les informations relatives au "Carving" sont manuellement insérées dans le module de recherche du logiciel Encase.

Cas de test : CT-02-V6
Support examiné : Clé USB CELLEBRITE

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. <u>Identifie les informations relatives au support de stockage</u> :

Le logiciel Encase récupère différentes informations comme la capacité du support, le nombre de secteurs, numéro de série, version OEM ou le système de fichier.

E-2. <u>Récupère tous types de fichiers supprimés</u>:

Les recherches ont porté sur cent-vingt et un fichiers qui portent dix-neuf extensions différentes.
Le nom de la majorité des fichiers n'a pas subi d'altérations.

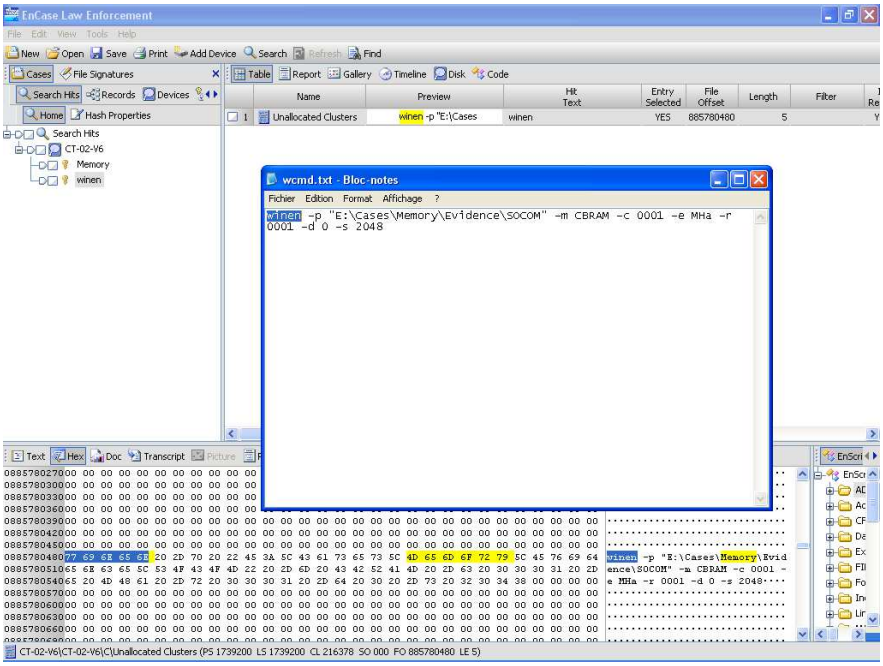
Les fichiers restés intacts avec leur nom d'origine sont directement identifiables depuis l'interface du programme.

Pour d'autres fichiers, leur premier caractère est remplacé par un le symbole "_", c'est une indication par le programme Encase qu'il s'agit de fichiers effacés.

A titre d'exemple, un fichier intitulé « wcmd.txt » a été corrompu et son nom remplacé par « _CMD.TXT ».

Afin de récupérer le fichier original, une recherche par mots clés avec les termes

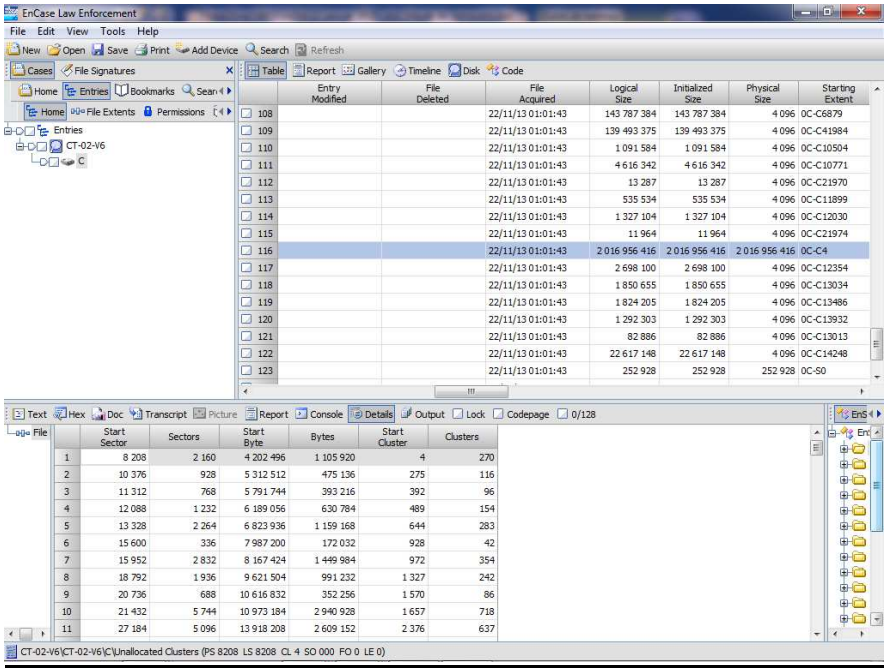
« *Memory* » et « *winen* », contenus dans ce fichier, a permis de le reconstituer mais sans trouver aucune indication sur le format du fichier :



E-3. Localise les fichiers supprimés:

Les informations relatives au nom des fichiers et leur chemin sont produites par le logiciel.

Des données concernant les clusters et début et fin de secteurs occupés par les fichiers permettent également de les localiser:

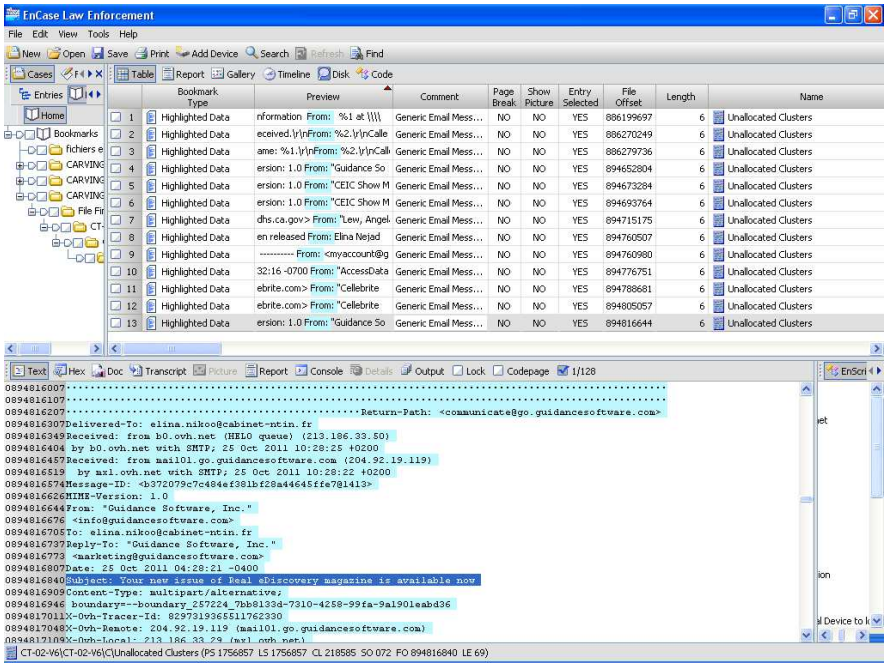


E-4. Récupère les données supprimées présentes dans la corbeille:

Cette exigence ne concerne pas le présent support testé.

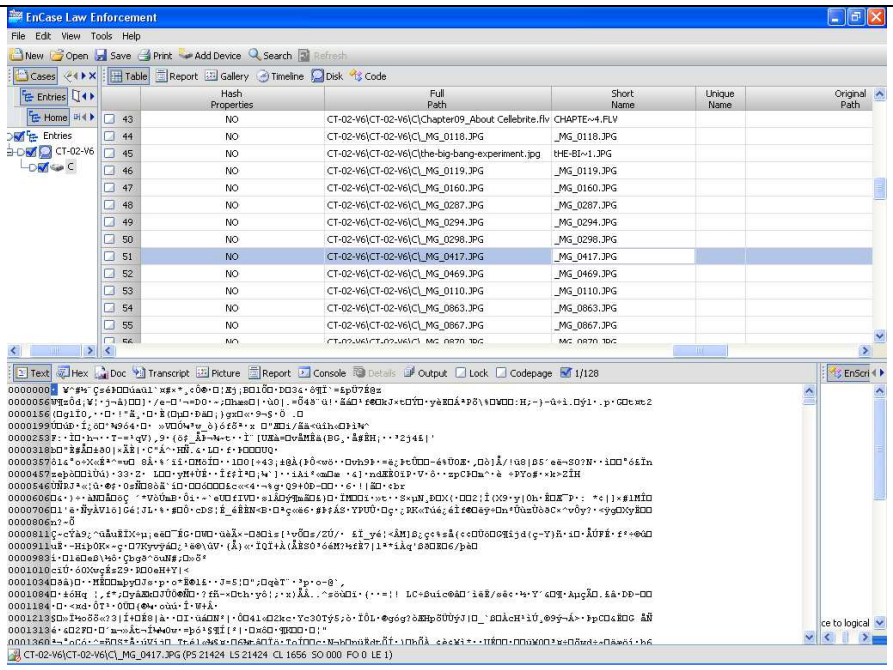
E-5. <u>Récupère dans les espaces non-alloués:</u>

Quatre vingt quatorze fichiers parmi ceux listés par le logiciel sont corrompus et ne peuvent pas s'ouvrir.
Pour la reconstitution d'autres fichiers, les recherches ont été menées dans les espaces non-alloués du support.
La totalité des fichiers n'a pas été reconstituée mais différents formats ont été récupérés :



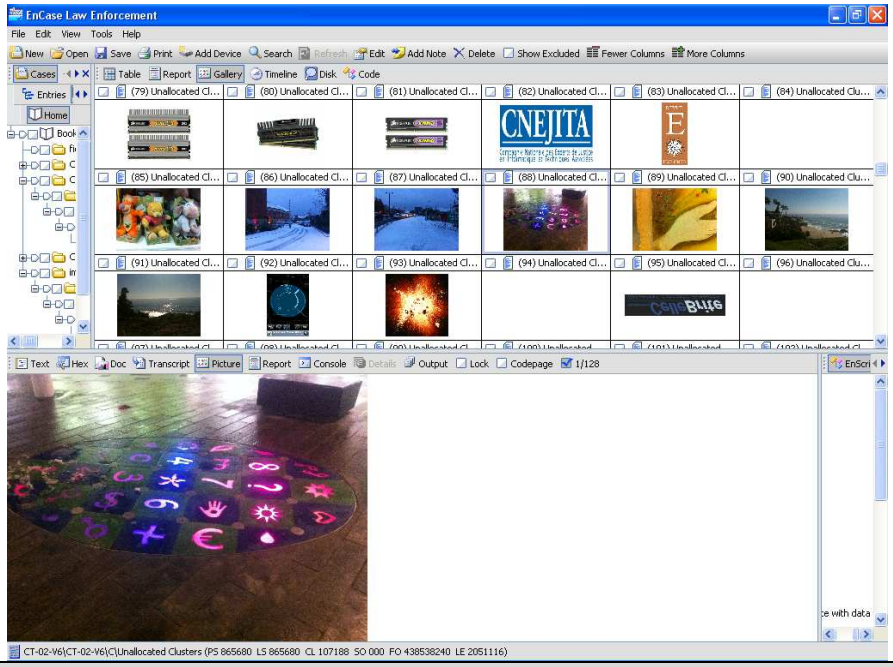
E-6. <u>Indique le chemin original du fichier effacé</u>:

Le programme n'indique pas le chemin original des fichiers effacés mais il contient des informations sur l'emplacement et le nom actuel de chaque fichier:



E-7. Récupère des données par analyse de signature:

La recherche par analyse de signature permet de récupérer de nombreuses données parmi les espaces non-alloués du support examiné.
Le recours à cette technique a permis de retrouver de nombreux fichiers aux formats « mp3 », « images » ou autres:



Cas de test : CT-03-V6
Support examiné : Disque dur SATA MAXTOR

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Le logiciel fournit des informations relatives à la marque, le modèle, le numéro de série, la signature, le nombre total de secteurs et la capacité du disque dur.

E-2. Récupère tous types de fichiers supprimés:

Tous les formats de fichiers supprimés sur le support informatique ont été récupérés par Encase.

E-3. Localise les fichiers supprimés:

Le programme contient des informations détaillées relatives à l'emplacement de chaque fichier.
A titre d'illustration, pour un fichier intitulé « *Difficultés rencontrées par les experts.pdf* », Encase répertorie les informations suivantes:

Début secteur	*Secteurs*	*Début octet*	*Octets*	*Début cluster*	*Clusters*
6 275 920	1 000	3 213 271 040	512 000	784 234	125

E-4. Récupère les données supprimées présentes dans la corbeille:

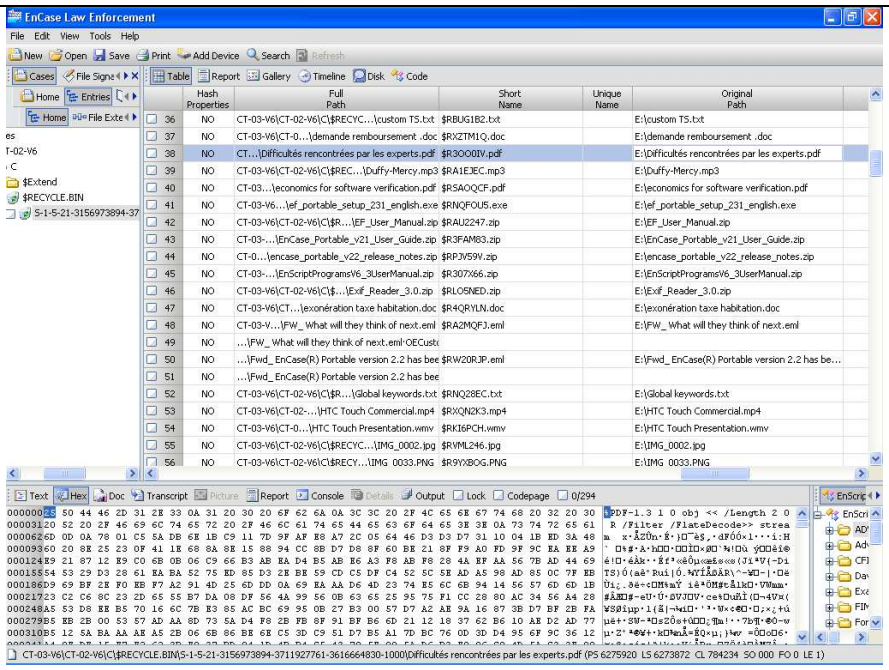
Cent vingt-et-un fichiers supprimés sont récupérés dans la corbeille.

E-5. Récupère dans les espaces non-alloués:

Tous les fichiers supprimés étant récupérés dans la corbeille, il n'a pas été utile de mener une recherche au niveau des espaces non-alloués du disque dur.

E-6. Indique le chemin original du fichier effacé:

L'emplacement original de chaque fichier est identifié par le programme Encase :



E-7. Récupère des données par analyse de signature:

Tous les fichiers étant récupérables, cette analyse ne s'est pas avérée pertinente.

Cas de test : CT-04-V6

Support examiné : Carte mémoire SDHC

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Encase identifie différentes informations relatives au support de stockage (modèle, numéro de série, capacité, nombre de secteurs…).

E-2. Récupère tous types de fichiers supprimés:

Le logiciel répertorie la totalité des fichiers effacés avec leur nom d'origine.
Quatre vingt cinq fichiers sont corrompus.
Le module "Recover Folders" ne permet pas de reconstituer des fichiers effacés.
Différents types de fichiers sont reconstitués par le carving.

E-3. Localise les fichiers supprimés:

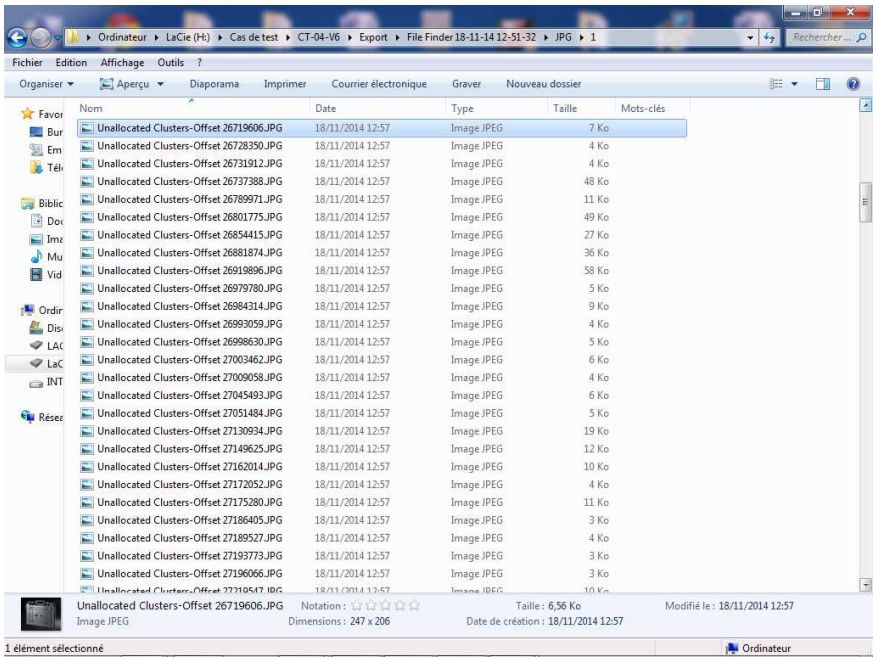
Le Logiciel fournit des informations concernant les fichiers référencés.

E-4. Récupère les données supprimées présentes dans la corbeille:

Cette exigence ne s'applique pas au présent cas de test.

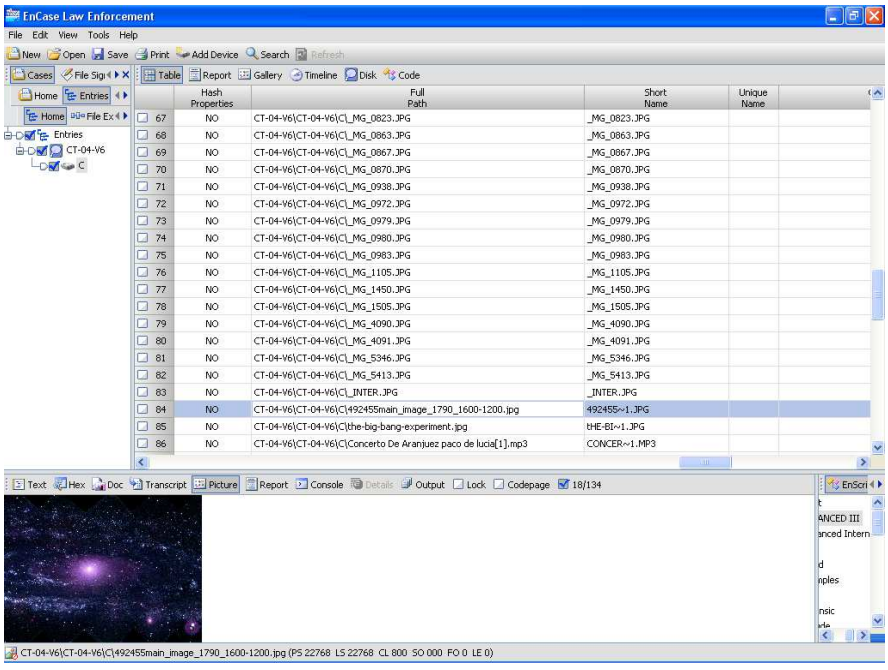
E-5. Récupère dans les espaces non-alloués:

Des recherches au niveau des espaces non-alloués ont permis de récupérer un certain nombre de fichiers.
Le nom des fichiers exportés automatiquement par le logiciel est remplacé par celui de "unallocated clusters" suivi de son numéro d'offset:



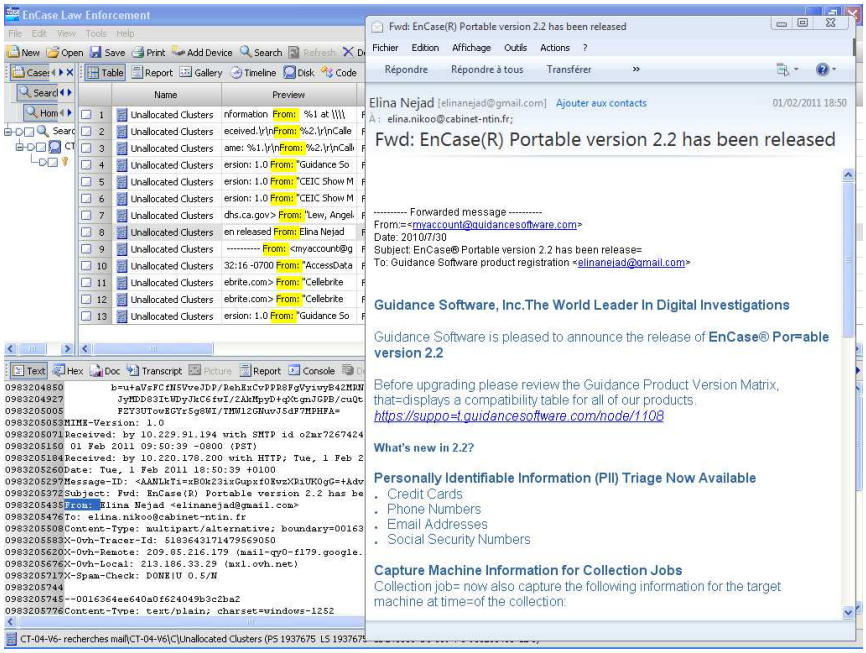
E-6. Indique le chemin original du fichier effacé:

Le chemin original des fichiers n'est pas indiqué par le programme Encase.
Il répertorie l'emplacement et le nom actuel de chaque fichier :



E-7. Récupère des données par analyse de signature:

Des recherches par une analyse de signature ont permis de reconstituer plusieurs types de fichiers.
Le nom de ces fichiers n'a pas été récupéré mais leur contenu a été entièrement reconstitué.



Cas de test : CT-05-V6
Support examiné : Carte mémoire compact Flash

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Les informations suivantes sont identifiées par Encase : modèle, numéro de série, capacité du support, nombre de secteurs, cluster, système de fichier…

E-2. Récupère tous types de fichiers supprimés:

Le support original a fait l'objet d'un formatage, la recherche classique de fichiers effacés ne permet de récupérer aucun fichier.

Des recherches plus approfondies sont nécessaires pour reconstituer différents types de fichiers. Pour cela, des informations doivent être insérées manuellement dans le logiciel afin de trouver les données effacées.
Les résultats devront par la suite être triés.

E-3. Localise les fichiers supprimés:

Chaque fichier récupéré est localisé avec son numéro « offset ».
A titre d'exemple, un fichier audio au format « mp3 » est identifié avec les informations suivantes :

«Unallocated Clusters
File offset:894172627
Length: 19188
MD5 Hash:076111E8D1B1609F299933D72DE3F0FD».

E-4. Récupère les données supprimées présentes dans la corbeille:

Cette exigence ne s'applique pas au présent cas de test.

E-5. Récupère dans les espaces non-alloués:

La totalité des données est récupérée dans les espaces non-alloués du support.

E-6. Indique le chemin original du fichier effacé:

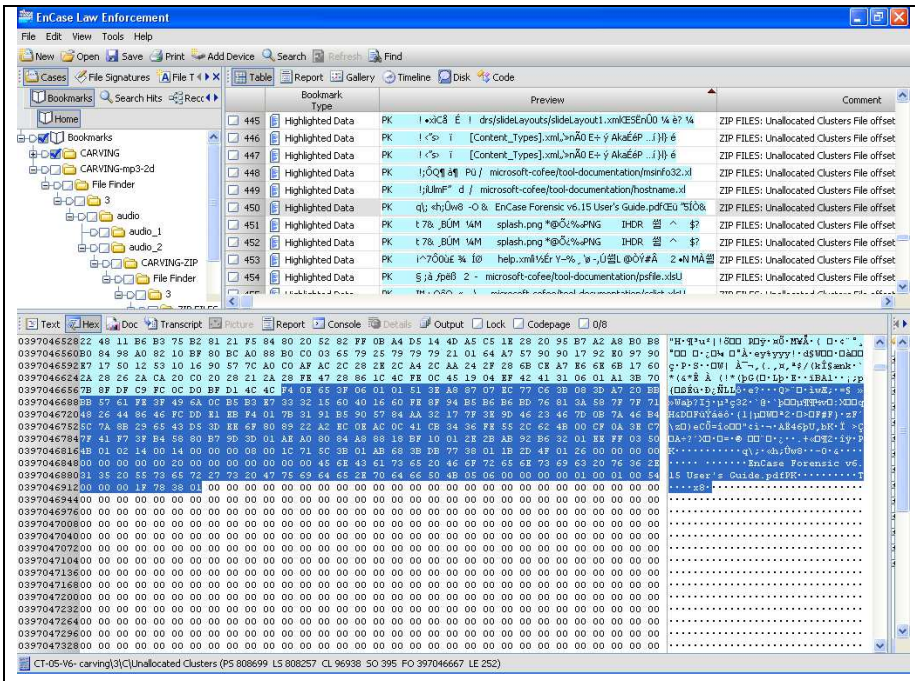
Le chemin original n'existe plus et le logiciel ne peut fournir aucune information à ce sujet.

E-7. Récupère des données par analyse de signature:

Les recherches de fichiers effacés sont réalisés par une analyse de signature dans les espaces non-alloués du support informatique.

Dix-neuf différents formats de fichiers ont été recherchés, pour certains formats comme les fichiers multimédia, les informations relatives aux en-têtes et fin de fichiers sont entrées manuellement.

Des résultats faux-positifs ont nécessité un tri minutieux des fichiers afin de récupérer les données exploitables.



Cas de test : CT-06-V6
Support examiné : Disque SSD SAMSUNG

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. <u>Identifie les informations relatives au support de stockage</u> :

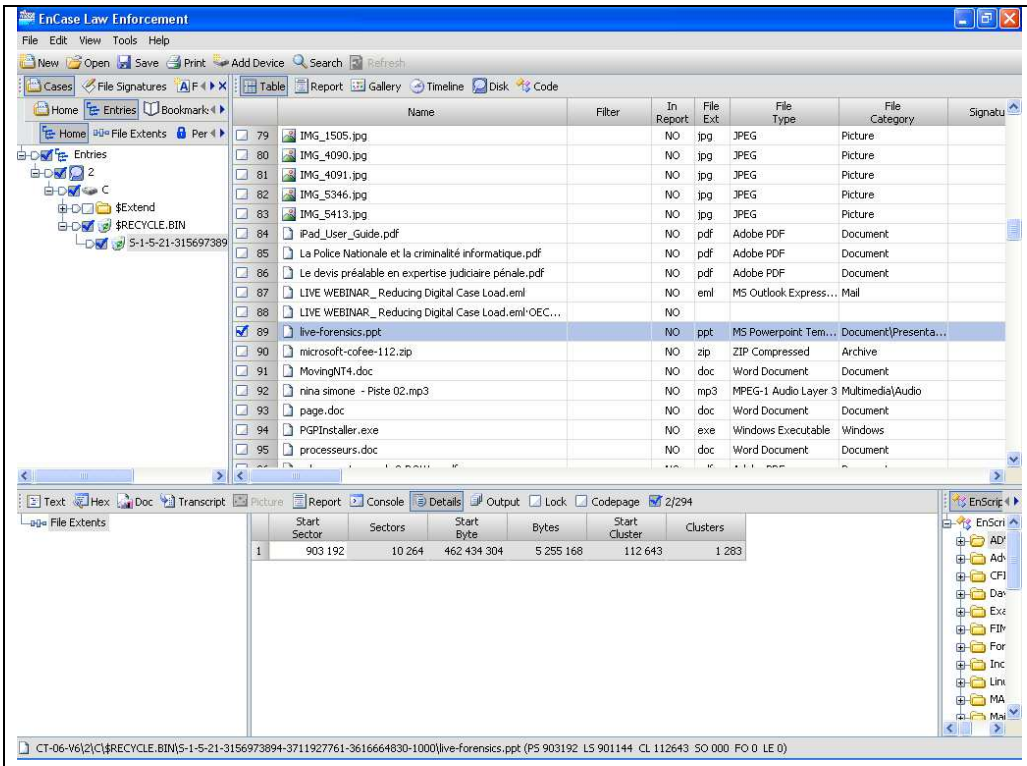
Encase affiche de nombreuses informations relatives notamment à la marque, le modèle, l'intégrité et la date de copie du disque dur (liste non-exhaustive).

E-2. <u>Récupère tous types de fichiers supprimés</u>:

Dix-neuf différents formats de fichiers ont été récupérés par le logiciel.

E-3. <u>Localise les fichiers supprimés:</u>

Le programme répertoire des informations détaillées concernant l'emplacement de chaque fichier.
A titre d'exemple, pour un fichier intitulé « live-forensics.ppt», le programme Encase affiche les informations relatives aux secteurs et clusters qui permettent de le localiser sur le support :



E-4. <u>Récupère les données supprimées présentes dans la corbeille</u>:

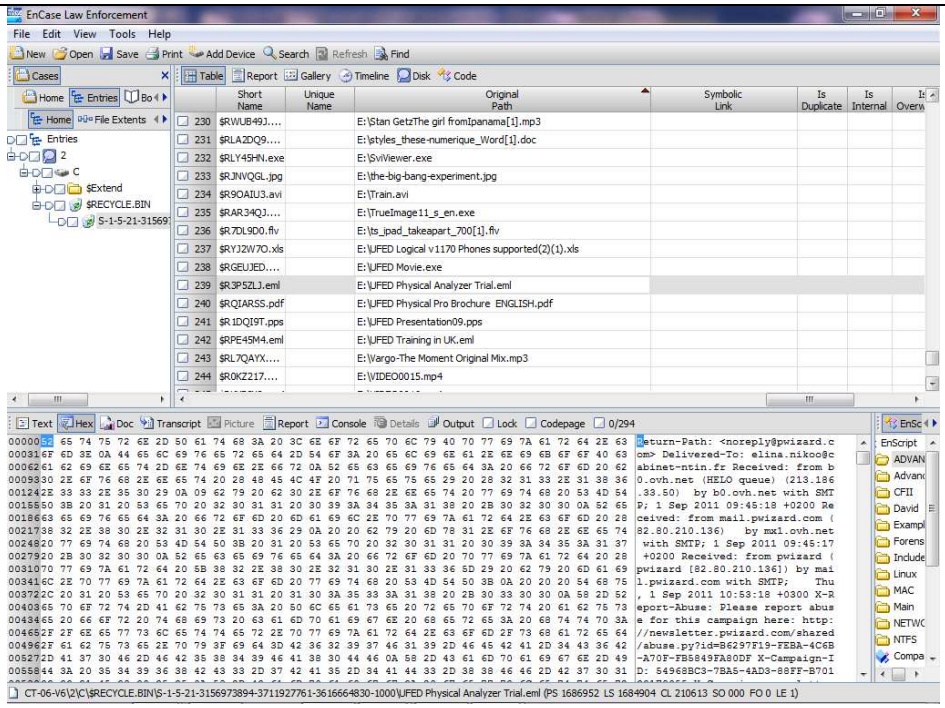
Tous les fichiers supprimés sont récupérés dans la corbeille.

E-5. <u>Récupère dans les espaces non-alloués:</u>

Tous les fichiers supprimés ont été récupéré dans la corbeille.
Il n'a pas été nécessaire de rechercher au niveau des espaces non-alloués du disque dur.

E-6. <u>Indique le chemin original du fichier effacé</u>:

Le programme identifie le chemin original de chaque fichier :



E-7. Récupère des données par analyse de signature:

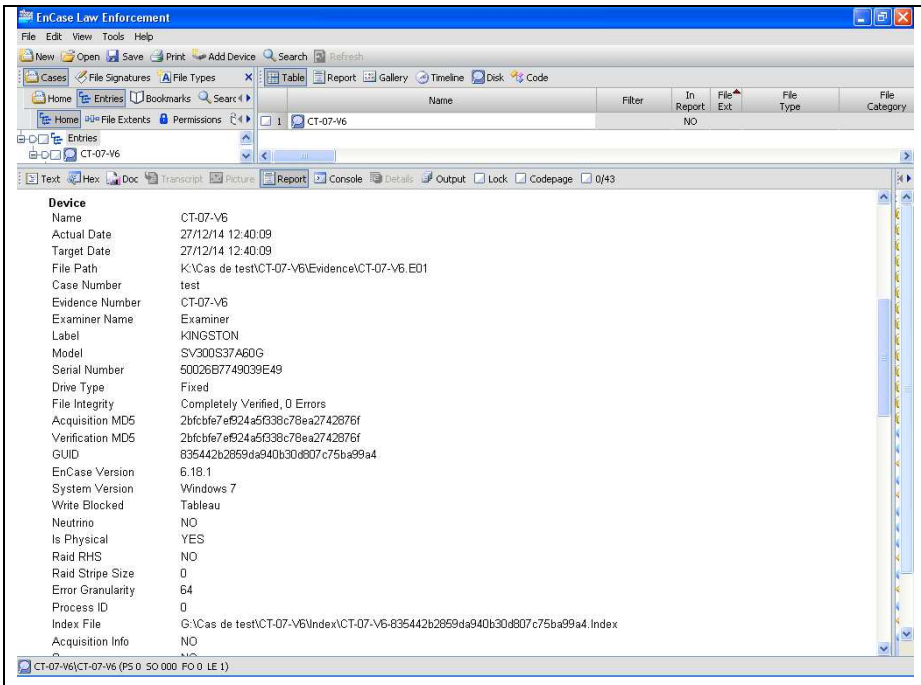
Toutes les données effacées ayant été retrouvées, il n'a pas été opportun de procéder à une analyse par signature.

Cas de test : CT-07-V6
Support examiné : Disque SSD KINGSTON

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Les informations relatives au support sont identifiées par le logiciel.

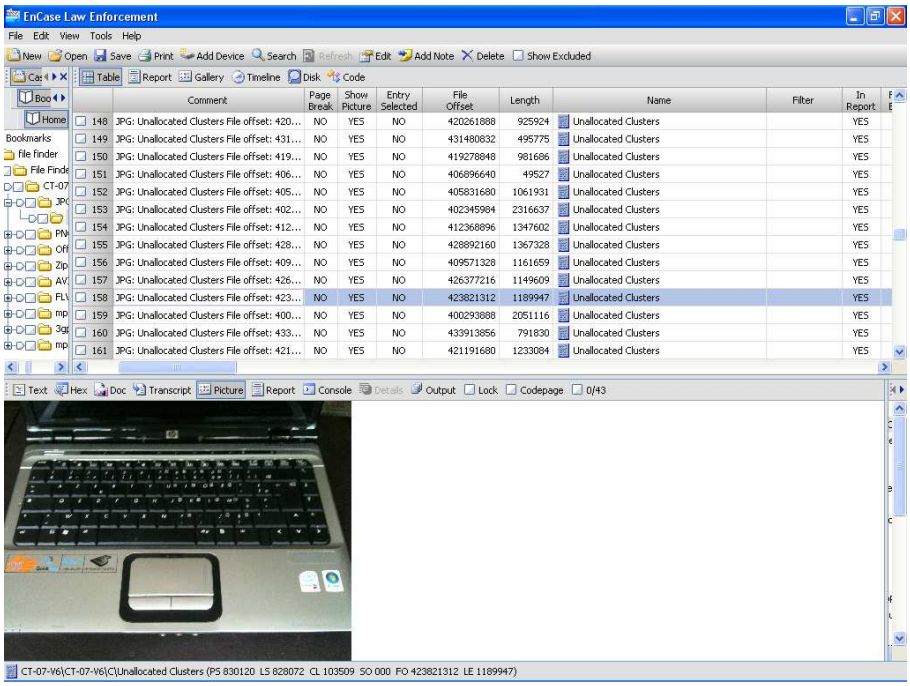


E-2. Récupère tous types de fichiers supprimés:

Le SSD ayant fait l'objet d'un formatage, les méthodes classiques de récupération de données ne permettent pas de reconstituer l'ensemble des fichiers.
Dans une telle situation, des recherches dans les espaces non-alloués du support permettront de reconstituer les fichiers.

E-3. Localise les fichiers supprimés:

Les fichiers effacés sont identifiés par leur « *Offset* » dans les espaces non-alloués du SSD.



E-4. Récupère les données supprimées présentes dans la corbeille:

Les données supprimées ne se trouvent pas dans la corbeille.
Le support a été formaté et les répertoires racines n'existent plus.
Les fichiers devront être recherchés dans les espaces non-alloués du support.

E-5. Récupère dans les espaces non-alloués:

La recherche dans les espaces non-alloués du support a permis de reconstituer de nombreux fichiers effacés.

E-6. Indique le chemin original du fichier effacé:

Il n'y a aucune indication relative à l'emplacement original des fichiers.
Ils sont tous récupérés dans les espaces non-alloués.

E-7. Récupère des données par analyse de signature:

Toutes les données récupérées sont issues d'une recherche par analyse de signature. Le programme Encase dispose d'un module automatisé qui permet de récupérer certains formats de fichiers.
Pour ceux qui ne sont pas prévus par le logiciel, les informations peuvent être rentrées manuellement pour rechercher et exporter les données.

Cas de test : CT-08-V6
Support examiné : Disque SSD SANDISK

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Encase affiche notamment les informations relatives à la marque, le modèle, , l'intégrité et la date de copie du support SSD (liste non-exhaustive).

E-2. Récupère tous types de fichiers supprimés:

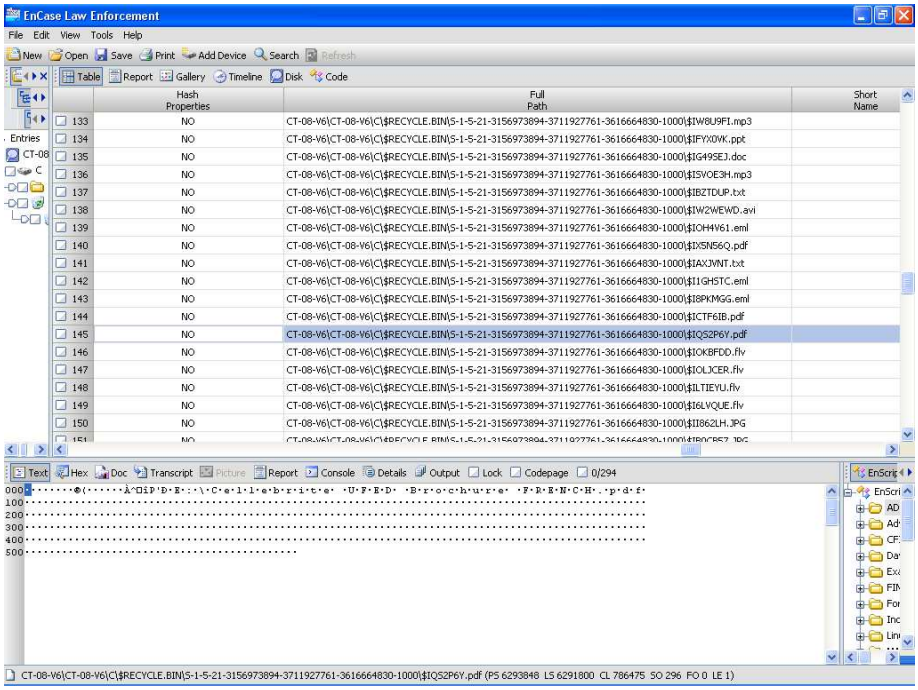
Tous les fichiers supprimés ont été récupérés par le logiciel Encase.

E-3. Localise les fichiers supprimés:

Le logiciel répertoire des informations détaillées sur l'emplacement de chaque fichier.

E-4. Récupère les données supprimées présentes dans la corbeille:

Tous les fichiers supprimés sont récupérés dans la corbeille.
Chaque fichier index $I identifié dans la corbeille indique le nom du fichier d'origine :



E-5. Récupère dans les espaces non-alloués:

Tous les fichiers effacés ont été récupérés dans la corbeille.
Il n'y a pas été utile de rechercher au niveau des espaces non-alloués du SSD.

E-6. Indique le chemin original du fichier effacé:

Le chemin original de chaque fichier est identifié par le programme Encase.

E-7. Récupère des données par analyse de signature:

Il n'a pas été nécessaire de procéder à cette recherche.

3.3.2.1 Encase Version 7.06

Cas de test : CT-01-V7
Support examiné : Clé USB CELLEBRITE

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

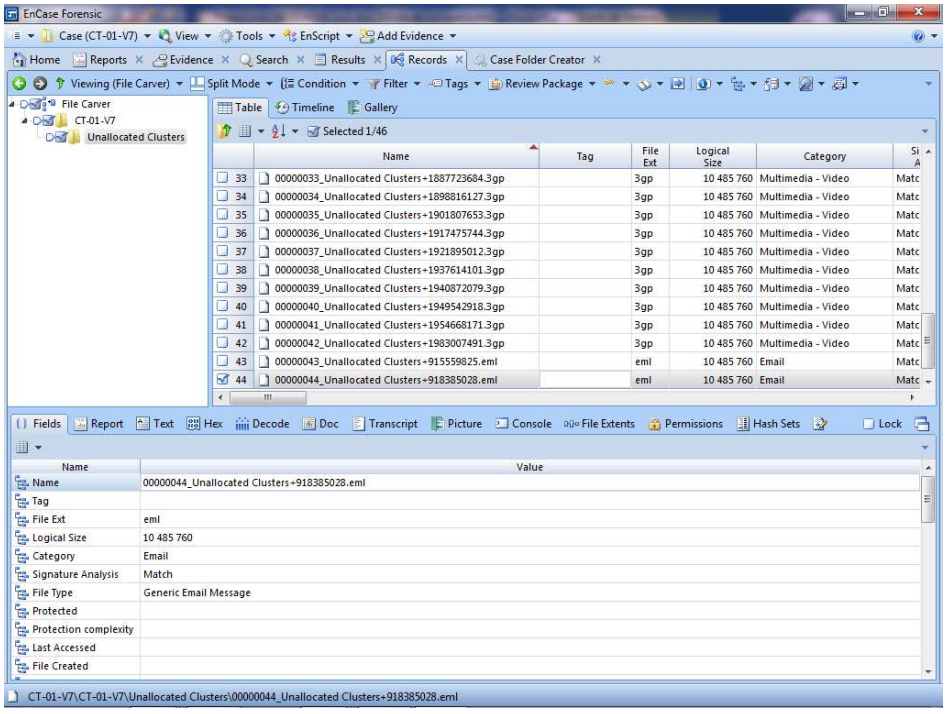
Encase affiche des informations relatives notamment au modèle, nombre de secteurs, l'intégrité et la date de copie du support.

E-2. Récupère tous types de fichiers supprimés:

Le module "Recover folders" ne permet de reconstituer aucun fichier effacé.
Le support ayant fait l'objet d'un formatage, une recherche plus avancée des fichiers effacés est réalisée pour les récupérer dans les espaces non-alloués du support examiné.

E-3. Localise les fichiers supprimés:

La seule information relative aux fichiers reconstitués concerne leur numéro d'offset:



E-4. Récupère les données supprimées présentes dans la corbeille:

Cette exigence ne s'applique pas au présent cas de test.

E-5. Récupère dans les espaces non-alloués:

Le support de stockage, ayant fait l'objet de formatage, toutes les recherches sont effectuées parmi les espaces non-alloués.

E-6. Indique le chemin original du fichier effacé:

Le logiciel n'affiche pas d'informations concernant le chemin original du fichier.

E-7. Récupère des données par analyse de signature:

Les recherches réalisées par analyse de signature permettent de reconstituer de nombreuses données effacées.
Le module automatique "file carver" permet de rechercher tous types de fichiers effacés.
Il est également possible de personnaliser les recherches en rentrant manuellement des informations relatives à l'en-tête et la fin de fichier.

Cas de test : CT-02-V7
Support examiné : Clé USB CELLEBRITE

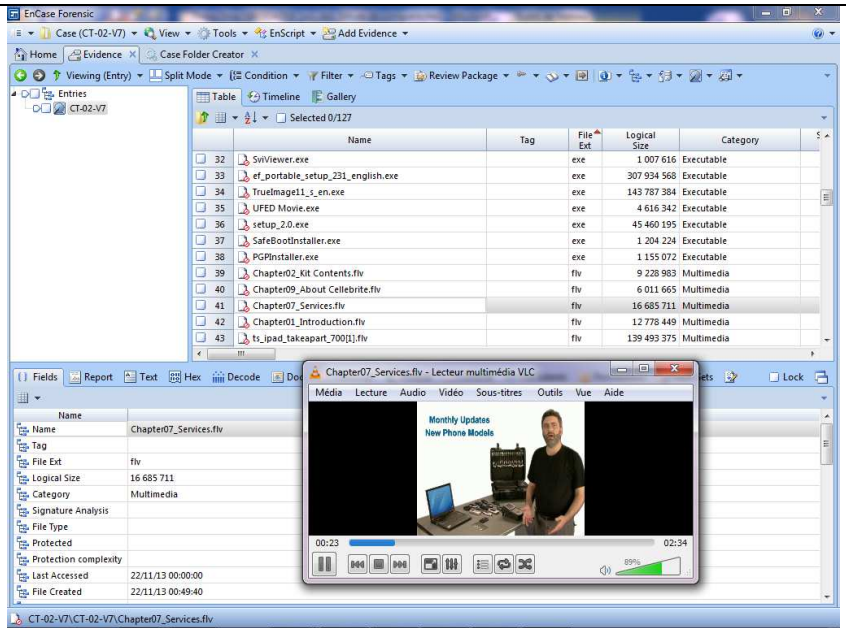
Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Des informations relatives au modèle, nombre de secteurs du support, l'intégrité et la date de copie sont relevées.

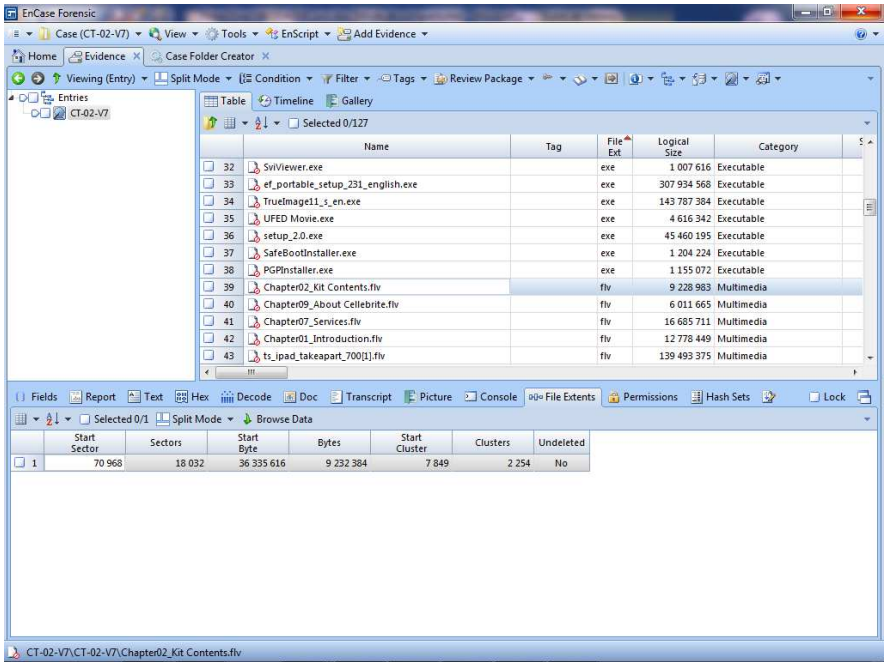
E-2. Récupère tous types de fichiers supprimés:

Le logiciel affiche le nom original des fichiers et certains d'entre eux sont récupérés directement depuis l'interface du programme Encase:



E-3. Localise les fichiers supprimés:

Des informations relatives aux secteurs et cluster de fichiers permettent de les localiser:



E-4. Récupère les données supprimées présentes dans la corbeille:

Cette exigence ne s'applique pas au présent cas de test.

E-5. Récupère dans les espaces non-alloués:

De nombreux fichiers récupérés sont corrompus, une recherche parmi les espaces non-alloués a permis de reconstituer des données.

E-6. Indique le chemin original du fichier effacé:

Le logiciel ne communique pas d'informations concernant le chemin original du fichier.

E-7. Récupère des données par analyse de signature:

Les recherches réalisées par analyse de signature permettent de reconstituer de nombreuses données effacées.

Cas de test : CT-03-V7
Support examiné : Disque dur SATA MAXTOR

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

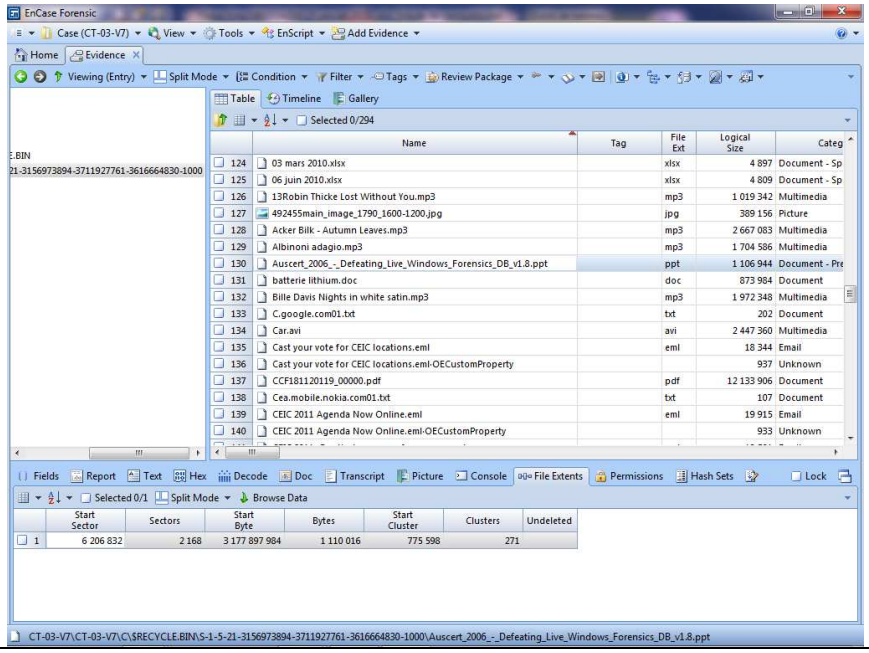
Encase affiche des informations relatives notamment au modèle, nombre de secteurs du support, l'intégrité et la date de copie.

E-2. Récupère tous types de fichiers supprimés:

Tous les fichiers effacés sont récupérés.

E-3. Localise les fichiers supprimés:

De nombreuses informations fournies par le logiciel permettent d'identifier chaque fichier:



E-4. Récupère les données supprimées présentes dans la corbeille:

Les données effacées sont récupérées depuis la corbeille.

E-5. Récupère dans les espaces non-alloués:

Il n'a pas été nécessaire de rechercher des données dans les espaces non-alloués du disque dur.

E-6. Indique le chemin original du fichier effacé:

Le chemin original de chaque fichier est bien mis en évidence par Encase:
A titre d'exemple, l'emplacement du fichier intitulé "CNEJITA-ACTES-COLLOQUE13042010-A5-V5.1.pdf" est présenté par le logiciel de la façon suivante :
"CT-03-V7\CT-03-V7\C\$RECYCLE.BIN\S-1-5-21-3156973894-3711927761-3616664830-1000\CNEJITA-ACTES-COLLOQUE13042010-A5-V5.1.pdf"

E-7. Récupère des données par analyse de signature:

Toutes les données ont été aisément récupérées, il n'a pas été utile de procéder à une analyse par signature de fichiers.

Cas de test : CT-04-V7
Support examiné : Carte mémoire SDHC

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Le programme affiche certaines informations relatives au support de stockage (modèle, capacité, nombre de secteurs…).

E-2. Récupère tous types de fichiers supprimés:

Tous les fichiers effacés sont répertoriés avec leurs noms d'origine. De nombreux fichiers sont corrompus et ne peuvent pas s'ouvrir.

E-3. Localise les fichiers supprimés:

Le Logiciel fournit des informations relatives à l'emplacement de chaque fichier.

E-4. Récupère les données supprimées présentes dans la corbeille:

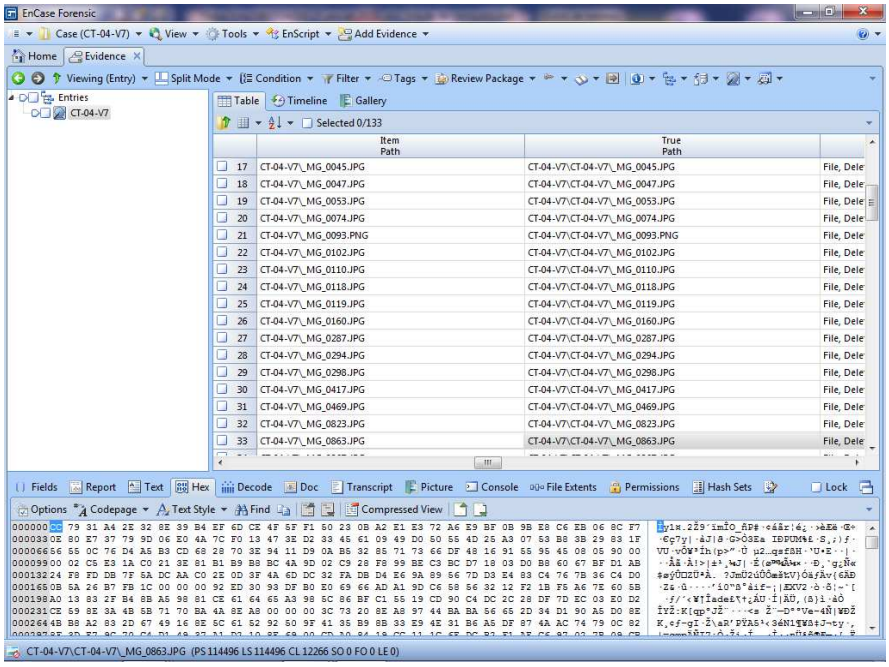
Cette exigence ne s'applique pas au présent cas de test.

E-5. Récupère dans les espaces non-alloués:

Des recherches au niveau des espaces non-alloués ont permis de récupérer un certain nombre de fichiers, mais dans ce cas leur nom d'origine ne peut pas être reconstitué.

E-6. Indique le chemin original du fichier effacé:

Le chemin fourni par le logiciel Encase pour chaque fichier concerne son emplacement après l'effacement :



E-7. Récupère des données par analyse de signature:

La recherche par analyse de signature a permis de récupérer certaines données.

Cas de test : CT-05-V7
Support examiné : Carte mémoire compact flash

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Le logiciel apporte des informations sur la capacité, les secteurs ou le système de fichier utilisé par le support.

E-2. Récupère tous types de fichiers supprimés:

Le volume a été formaté et aucun fichier effacé n'a été récupéré par la méthode classique de récupération des données.

E-3. Localise les fichiers supprimés:

Les fichiers effacés sont localisés avec leur « offset ». Le répertoire racine étant supprimé, aucune autre information sur le chemin du fichier n'est disponible.

E-4. Récupère les données supprimées présentes dans la corbeille:

Cette exigence ne s'applique pas au présent cas de test.

E-5. Récupère dans les espaces non-alloués:

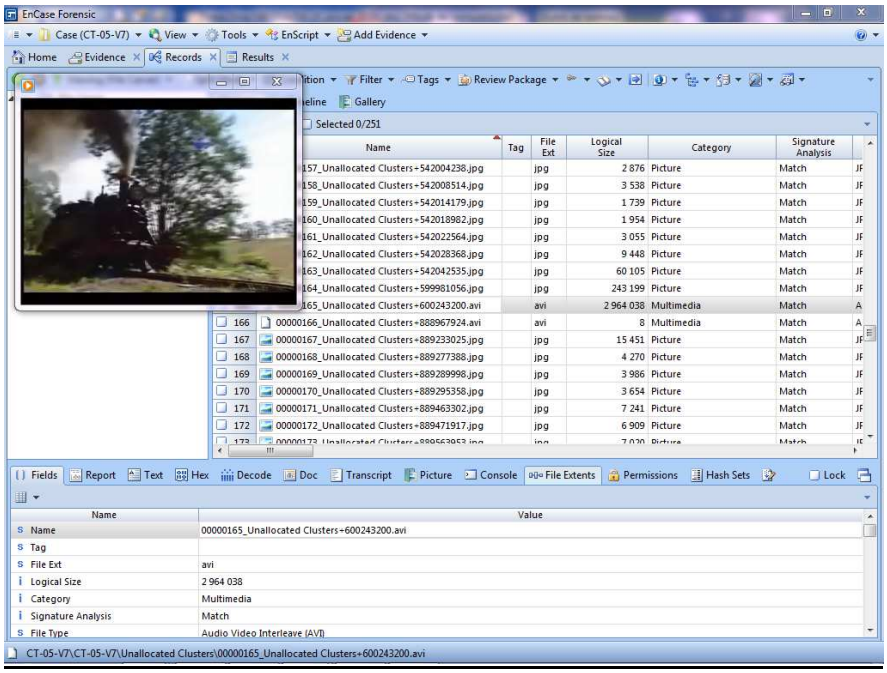
Tous les fichiers reconstitués on été récupérés en en effectuant une recherche dans les espaces non-alloués du support de stockage.

E-6. Indique le chemin original du fichier effacé:

Le programme ne fournit aucune information concernant le chemin original des fichiers.

E-7. Récupère des données par analyse de signature:

Le module "carving" configuré dans le logiciel a permis de retrouver des données. Différents types de fichiers sont répertoriés et les recherches sont automatiquement réalisées:



Cas de test : CT-06-V7
Support examiné : SSD SAMSUNG

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

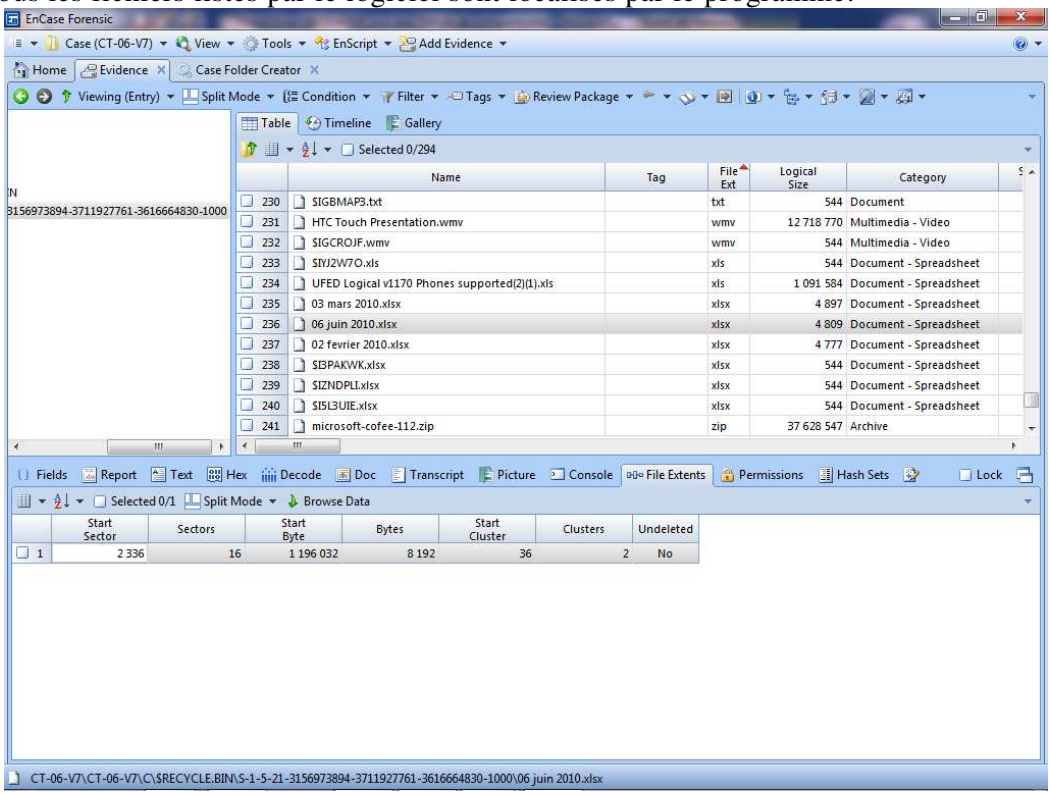
De nombreuses informations relatives au support de stockage sont identifiées.

E-2. Récupère tous types de fichiers supprimés:

Tous les fichiers qui ont été effacés du support sont récupérés par le logiciel Encase.

E-3. Localise les fichiers supprimés:

Tous les fichiers listés par le logiciel sont localisés par le programme:



E-4. Récupère les données supprimées présentes dans la corbeille:

Les fichiers effacés ont été récupérés dans la corbeille.
Encase répertorie la liste de tous les fichiers ainsi que leurs index $I qui les associent aux fichiers d'origine.

E-5. Récupère dans les espaces non-alloués:

Nous n'avons pas effectué de recherches dans les espaces non-alloués du support.

E-6. Indique le chemin original du fichier effacé:

Le chemin original n'est pas indiqué par le logiciel, il renvoie vers l'emplacement des données après leur effacement.

E-7. Récupère des données par analyse de signature:

Aucune recherche par analyse de signature n'a été réalisée pour reconstituer des données.

Cas de test : CT-07-V7
Support examiné : Disque SSD KINGSTON

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Le programme donne plusieurs informations relatives au support et notamment sa taille ou le nombre de secteurs:

ID	Type	Début du secteur	Nombre total de secteurs	Taille
07	NTFS	2 048	117 225 472	55,9 GB

E-2. Récupère tous types de fichiers supprimés:

La totalité des fichiers effacés n'a pas été récupérée.

E-3. Localise les fichiers supprimés:

Les fichiers récupérés ne sont pas localisés. Ils sont reconstitués à partir des espaces non-alloués du support, cela signifie que leur répertoire racine n'existe plus et il est difficile de trouver leur emplacement.

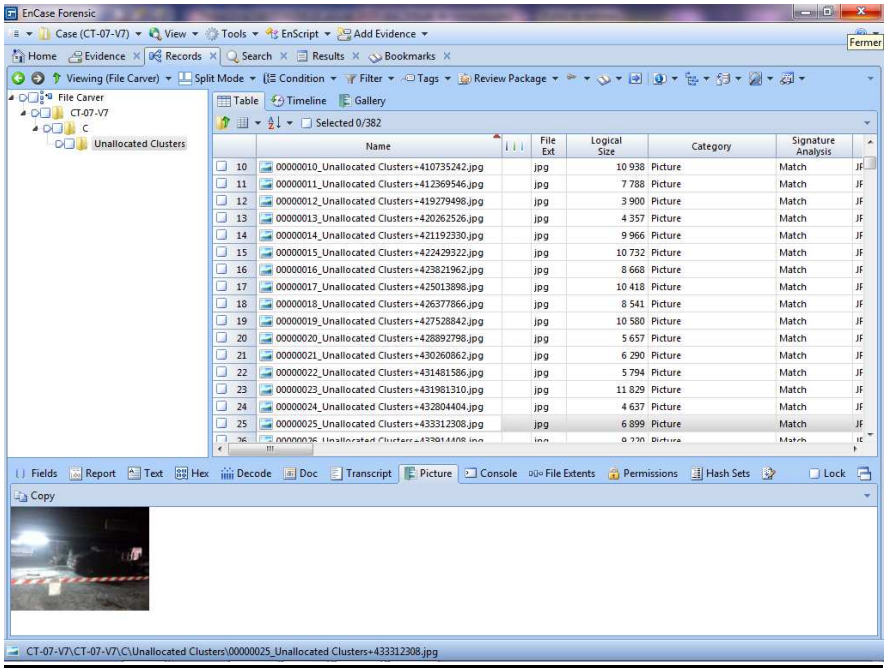
E-4. Récupère les données supprimées présentes dans la corbeille:

Les données supprimées ne se trouvent pas dans la Corbeille.

E-5. Récupère dans les espaces non-alloués:

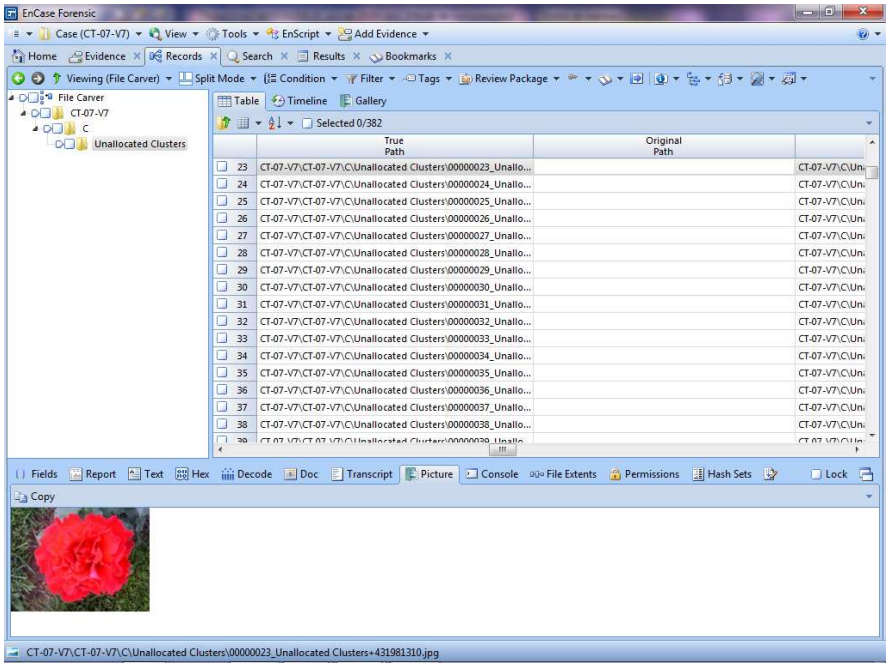
Toutes les données effacées ne sont pas récupérées mais de nombreux fichiers sont reconstitués à partir des espaces non-alloués.

Le nom des ces fichiers est remplacé par "Unallocated Clusters":



E-6. Indique le chemin original du fichier effacé:

L'emplacement original du fichier n'est pas du tout identifié par le programme:



E-7. Récupère des données par analyse de signature:

Les fichiers sont reconstitués grâce à une analyse d'en-tête de fichiers.
La technique du "carving" permet de retrouver plus aisément les fichiers effacés.

Cas de test : CT-08-V7
Support examiné : Disque SSD SANDISK

Résultats obtenus par rapport aux exigences définies dans le plan de tests

E-1. Identifie les informations relatives au support de stockage :

Encase donne de nombreuses informations sur le volume comme la capacité, nombre de secteurs ainsi que le format de partition.

E-2. Récupère tous types de fichiers supprimés:

Tous les fichiers supprimés sont récupérés.

E-3. Localise les fichiers supprimés:

Le logiciel identifie l'emplacement de chaque fichier.

E-4. Récupère les données supprimées présentes dans la corbeille:

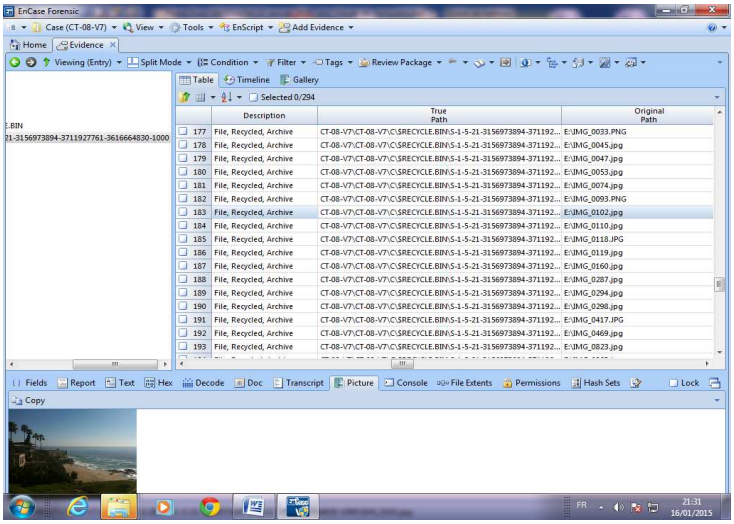
Toutes les données effacées sont récupérées dans la corbeille.

E-5. Récupère dans les espaces non-alloués:

Aucune recherche parmi les espaces non-alloués du SSD n'a été effectuée.

E-6. Indique le chemin original du fichier effacé:

Encase répertorie non seulement le chemin original du fichier effacé, il identifie également le chemin des fichiers après leur effacement:



E-7. Récupère des données par analyse de signature:

Nous n'avons procédé à aucune recherche par analyse de signature.

Concernant les présents cas de tests, le format et le nombre de tous les fichiers effacés étaient connus à l'avance.

Dans le contexte d'une expertise technique et dans la majorité des cas, l'expert ignore cette information et ne dispose que des indications d'ordre générales.

La difficulté principale consiste alors à cibler les recherches afin de retrouver des données pertinentes.

Une bonne connaissance de l'outil permet d'éviter toutes confusions ou erreurs d'analyses.

Pour l'analyse de courriels, certaines incohérences peuvent être relevées en rapport avec l'heure d'envoi des messages électroniques qui s'expliquent par la problématique du fuseau horaire.

Prenons l'exemple d'un courriel fichier faisant partie de nos cas de tests, intitulé "*FW_ What will they think of next.eml*", envoyé le 17 février 2010 à 19h44 par l'application « Windows Live Mail » :

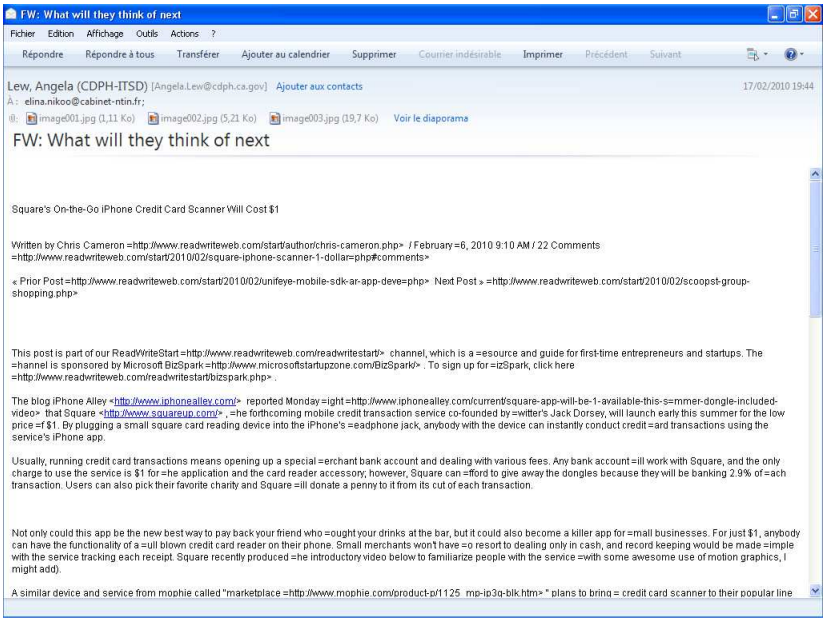


Figure 34- Aperçu du courriel dans Windows Live Mail

Le même message visionné dans le logiciel Encase, est daté du 17 février 2010 à 10h44 (-0800), l'heure correspond à celle du Pacifique (Etats-Unis et Canada) :

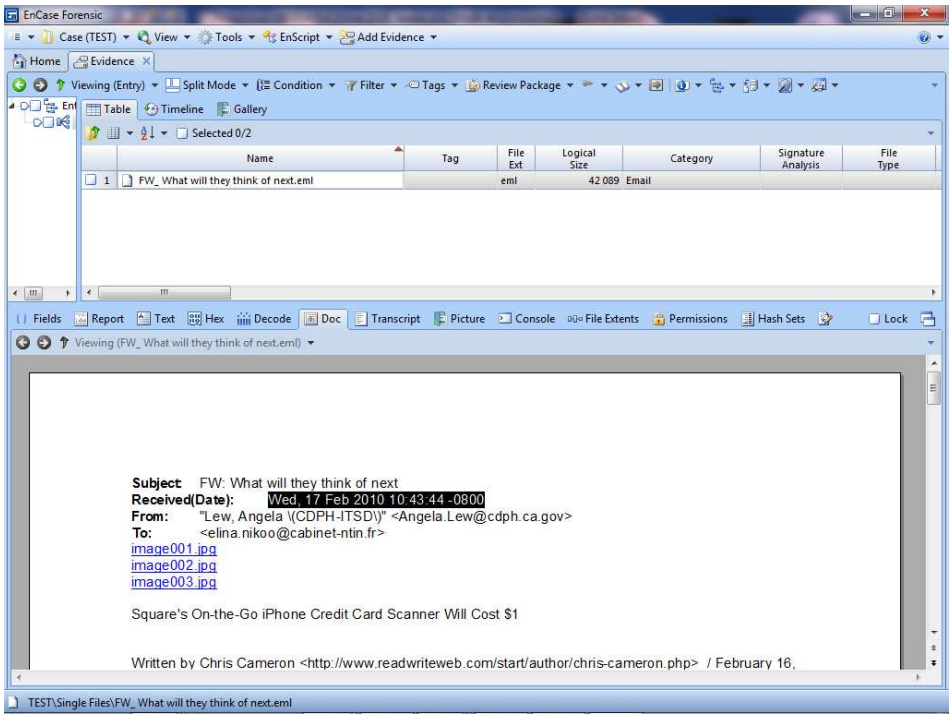


Figure 35- Aperçu du courriel dans Encase V7

Una analyse manuelle du contenu du message permet de déterminer l'heure à la quelle le message a été transmis. L'heure indiquée correspond à 18h44 UTC.

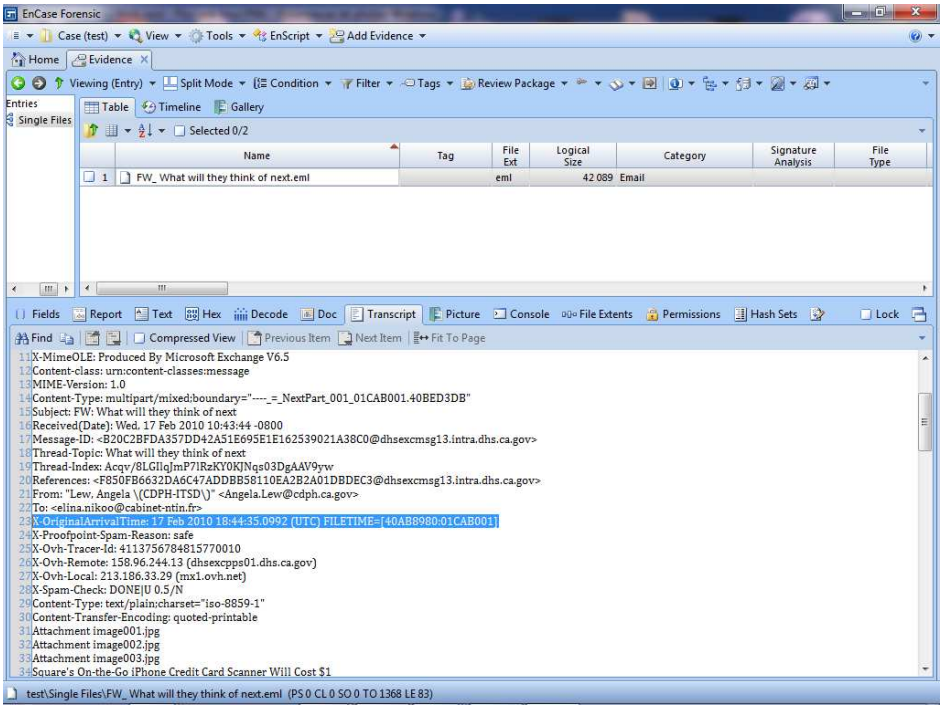


Figure 36- Analyse de l'entête du courriel dans Encase V7

Le programme DCODE permet de convertir les valeurs hexadécimales et vérifier les dates et heures trouvées par les logiciels d'investigation.

Dans l'exemple susmentionné, le message est envoyé le 17 février à 19h44 en fuseau horaire (UTC+1).

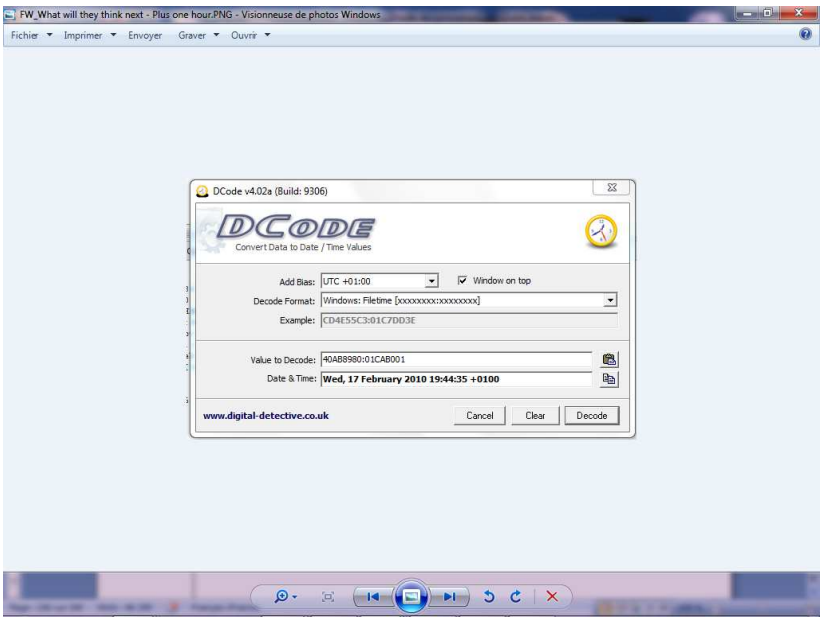


Figure 37- Conversion d'une valeur hexadécimale en date et heure par l'utilitaire DCODE

Le changement de fuseau horaire n'a aucune incidence sur les volumes formatés en FAT car ils enregistrent les dates en heure locale. Il en va différemment pour les systèmes NTFS qui retiennent le format de l'heure UTC.

Avant chaque analyse de disques durs avec un système de fichier NTFS, la vérification du fuseau horaire constitue une étape essentielle dans l'analyse de preuve car un matériel saisi peut être configuré à un fuseau horaire différent de l'heure locale.

La prise en compte des règles relatives au changement d'heure d'été peut également avoir des conséquences importantes.

Depuis 2007, pour les appareils configurés à l'heure normale du Pacifique, le passage à l'heure d'été intervient la deuxième semaine du mois de mars.

Le programme Encase permet de procéder à cet ajustement manuellement notamment pour les appareils anciens qui ne prennent pas en compte cette modification.

Un autre point important en rapport avec l'horodatage concerne les paramètres du logiciel Encase. Contrairement à la version sept, dans la version six du logiciel, par défaut le format de date est configuré sur le système américain.

A titre d'illustration, pour un fichier image intitulé « *IMG_0870.jpg* » dont la date de modification correspond à 11 juin 2011, ENCASE répertoriera la date du 06 novembre 2011 :

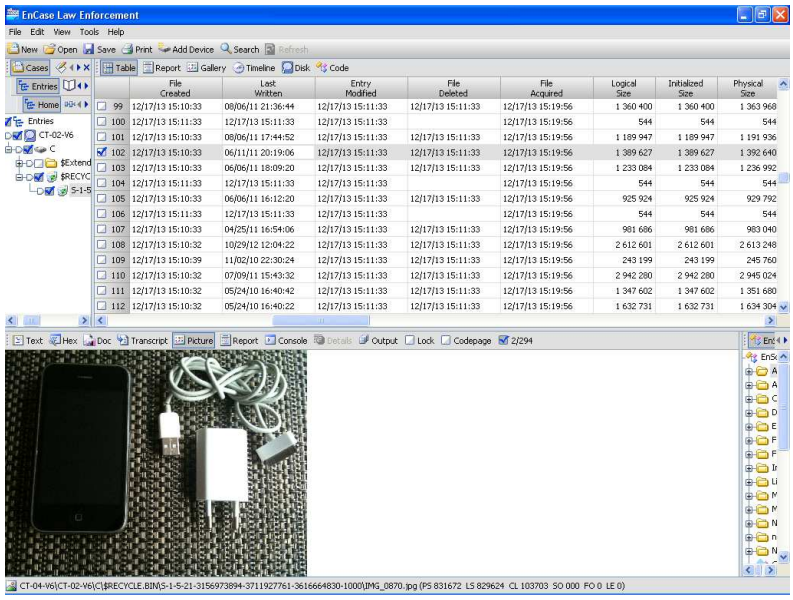


Figure 38- Affichage des dates et heures dans Encase V6

Une telle erreur d'interprétation pourrait prêter à confusion en faussant l'analyse et faire l'objet de contestations ultérieures.

3.4 Conclusions et perspectives

L'expertise en informatique se caractérise par sa place prépondérante dans la recherche de preuves et connaît des enjeux importants.
L'utilisation inappropriée ou l'absence de maîtrise des outils dans le domaine de la criminalistique peut avoir des conséquences désastreuses et induire la justice en erreur.
Ces dernières années, les méthodes d'investigation ont dû s'adapter à la notion de "Big Data" et à la complexité d'analyse du volume important d'informations.
Ainsi, les expertises ne se limitent plus à l'analyse d'un ou deux ordinateurs mais impliquent aujourd'hui plusieurs dizaines de supports et des infrastructures complexes tournées vers l'entreprise.
Pour faire face à une demande croissante de travailler dans l'urgence en recherchant les éléments de preuves sur des volumes importants de données, les praticiens ont de plus en plus recours à des outils automatisés.

Les experts ont tendance à se fier aux résultats produits par de tels programmes sans pour autant en maîtriser les fonctionnalités, ni même avoir suivi de formations certifiantes.
Si l'automatisation des outils doit accompagner l'expert dans ses recherches, elle n'a en revanche pas vocation à remplacer son savoir faire.
Un outil n'est jamais infaillible et le monde judiciaire devra être sensibilisé au danger que peut représenter une telle confiance.

Il convient de rappeler que, dans le cadre des expertises judiciaires, un expert peut être cité à comparaître devant la justice concernant ses travaux.
Son témoignage technique doit alors démontrer qu'il dispose de connaissances approfondies des outils utilisés et des différentes fonctionnalités pour la réalisation des opérations d'expertise.

La France souffre d'un sérieux retard dans le suivi des formations par les professionnels de l'investigation alors que ce sujet devrait se trouver au cœur des préoccupations des spécialistes.

Il permettrait en effet de leur accorder de la crédibilité et d'apporter les compétences nécessaires à l'accomplissement de leur mission.

Des formations sont régulièrement organisées par les éditeurs de logiciels comme la société Guidance Software ou AccesData pour préparer des certificats EnCE (Encase) et ACE (FTK).
Or, à l'heure actuelle, bien que plus de deux mille personnes soient titulaires du certificat EnCE dans le monde, seulement trois personnes sont certifiées en France et deux à Monaco.

Les bonnes pratiques sont enrichies par l'usage, mais la discipline souffre d'un manque de cadres ou de références.

Une autre difficulté est liée également aux règles de déontologie prévoyant que l'expert inscrit sur une liste officielle n'est pas considéré comme exerçant une profession mais comme réalisant une activité dans le cadre de sa mission.
Or, cette position déontologique nous place devant un paradoxe: alors que l'évolution permanente de la technologie et la nature très spécialisée de l'investigation technique requièrent une pratique régulière, qui ne peut se faire que dans le cadre d'une profession à temps plein, la professionnalisation de la pratique de l'expertise n'est pas reconnue.

La connaissance approfondie des outils passe également par la connaissance des capacités et des limites de ces programmes, pour une meilleure prise en compte de leurs spécificités techniques.

Il ressort de nos recherches qu'il est important de maîtriser de nombreux concepts clés et la phase de validation d'outils, bien qu'absente de notre procédure, sera ainsi sécurisante pour le juge.
L'approche traditionnelle de l'expertise a également évolué avec l’arrivée des nouveaux types de supports de stockages numériques.

En soumettant les outils aux tests, le risque de passer à côté des éléments importants serait diminué.
Bien qu'une évaluation ne soit jamais totalement exhaustive, le besoin de validation constituera une garantie d'efficacité et de confiance.
A travers les cas de tests réalisés, nous avons mis en évidence l'importance de la compréhension de l'outil et le fait que certaines incohérences ou erreurs dans les résultats pourraient conduire à des conclusions erronées.
Une comparaison des résultats de plusieurs outils permet de maîtriser les possibilités techniques de chaque programme.

Cependant, les travaux demeurent isolés et les référentiels de validation utilisés par des entités gouvernementales restent confidentiels et ne sont jamais publiés.

La création d'une communauté d'experts qui procéderait aux tests et dont les résultats seraient partagés avec d'autres confrères pourrait avoir un impact important sur le processus de validation.
En plus de permettre une diminution des coûts, une telle mutualisation des moyens constituerait le référentiel commun qui, aujourd'hui, fait défaut et serait une évolution dans la pratique de l'expertise judiciaire en informatique.

Bibliographie

Al-HANAEI Ebrahim Hamad, Awais Rachid, DF-C²M²: «*a capability maturity model for digital forensics organizations*»,- 2014 IEEE Security and privacy Workshops.W.

ALINK, R.A.F. Bhoedjang, P.A. de Vries, « XIRAF-*XML-based indexing and querying for digital Forensics* », digital investigation Elsevier, 2006.

BELL Graeme B, BODDINGTON Richard, «*Solid State Drives: The beginning of the end for current practice in digital forensic recovery?*», JDFLS, volume 5, Number3, 2010.

BERGHEL Hal, HOELZER David, STHULTZ Michael, «*Data Hiding Tactics for Windows and Unix File Systems*»,, advanced in computers, vol 74, 2008 Elsevier Inc.

BERKMAN Ariel, « *Hiding data in hard drive's service areas*», recover information technologies LTD, February 14, 2013.

BROWN Christopher L.T., « *Computer Evidence, Collection and Preservation* », second edition, Charles River Media, Course technology CENGAGE Learning, 2010.

BUSBEE Annarita M., Noelle A. Abastillas, Owen Gleaton Egan Jones & Sweeney, LLP, « *La recherche de la vérité par le savoir scientifique: Comment éliminer la mauvaise science de la bonne avec le test Daubert* ».

BYERS David, SHAHMEHRI Nahid, « *Disk imaging evaluation : Encase 6.8/LinEn 6.1* », Linköping University, department of computer and Information science, october 2008.

CARRIER Brian D., Eugene H. Spafford, «*An Event-Based Digital Forensic Investigation Framework* », CERIAS, Purdue University.

CARRIER Brian, « *Open source digital Forensics Tools, the legal Argument* ».

CARVEY Harlan, « *Windows Forensic Analysis* », Syngress Publishing, 2009.

CHAMPLAIN Jack J., « *Auditing information systems* », seconde edition, John Wiley & Sons, 2003.

COURTEAUD Jean-Louis, TYRODE Jean-François, « *Les disques durs SSD un défi pour l'expert informatique* », Revue Experts n°88, 2010, pp.36 à 39.

CUSACK, B. & LIANG, J. « *Comparing the performance of three digital forensic tools* », Journal of applied computing and information technology, ISSN 2230-4398, Volume 15, Issue 1, 2011.

DUPUY Laurent, « *Indiscrétions et zones constructeurs des disques durs* », actes du symposium SSTIC07.

GARFINKEL, Simson L., David J. Malan, Karl-Alexander Dubec, Christopher C. Stevens, and Cecile Pham. 2006. «*Advanced forensic format: An open, extensible format for disk imaging*». In Advances in Digital Forensics II: FIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, January 29-February 1, 2006, ed. Martin Olivier and Sujeet Shenoi, 17-31. New York: Springer.

GUBANOV Yuri, AFONIN oleg, « *Why SSD Drives destroy court evidence, and what can be done about it* », Q3 2012: state of the art in SSD forensics, Belkasoft Ltd.

GUBANOV Yuri, AFONIN oleg, « *Recovering Evidence from SSD drives in 2014: understanding TRIM, Garbage Collection and Exclusions*», Belkasoft, 23 Septembre 2014.

GUO Yinghua, SLAY Jill, BECKETT Jason, «*Validation and verification of computer forensic software tools- searching function*», Defense and systems institute, university of south Australia- Elsevier, Science direct, Digital investigation 6 (2009) S12-S22

GUPTA, Mayank R, HOESCHELE Michael D, ROGERS Marcus K, « *Hidden disk areas : HPA and DCO* », Purdue University, International Journal of Digitan Evidence, Fall 2006, Volume 5, Issue1.

HOLZMANN Gerald J. « *Economics of Software Verification* », Bell Laboratories, Murray Hill NJ.

LE DOUARIN Nicole, « *Des empreintes digitales aux empreintes génétiques, à la recherche de la preuve indiscutable* », Académie des sciences, séance solennelle 23 novembre 2004, science et justice.

LEVINE Brian Neil, Marc Liberatore, « *DEX: Digital evidence provenance supporting reproducibility and comparison*», digital investigation Elsevier, 2009

LIU and Brown (2006), «*Bleeding-Edge Anti-Forensics*», Infosec world conference and Expo, MIS training institute.

LYLE James R. « *If error rate is such a simple concept, why don't I have one for my forensic tool yet* », Digital Investigation 7 (2010) SI35-SI39, Elsevier.

MOHAY George, ANDERSON Alison, COLLIE Byron, DE VEL Olivier, McKEMMISH Rodney, «*Computer and Intrusion forensics*», 2003, Artech House.

NOAT Jean-Philippe, VALENTIN Bruno, « *Internet Explorer 10 et 11, un nouveau format de données pour de nouveaux défis* », Uriel Expert.

REIS Marcello Abdalla Dos & Paulo Licio de Geus, « *Standardization of Computer Forensic Protocols and Procedures*», 14 novembre 2001, page 4.

ROGERS Marcus K., James Goldman, Rick Mislan, Timothy Wedge, « *Computer Forensics Field Triage Process Model*», Conference on Digital Forensics, Security and Law, 2006.

ROSE Kiristina, ROBINSON LAURIE. O, HOLDER JR Eric H. « *Test results for digital data acquisition tool: Encase 6.5"* », NIJ special Report, September 2009.

ROUSSEV, V., Richard, G. «*Breaking the Performance Wall: The Case for Distributed Digital Forensics*». In Proceedings of the 2004, Digital Forensics Research Workshop (DFRWS). Aug 2004, Baltimore,MD.

SLAY Jill, BECKETT Jason, « *Digital Forensics : validation and verification in a Dynamic work environment*», proceedings of the 40th Hawaii International Conference on System Sciences-2007.

SOLOMON Michael G., K Rudolph, Ed Tittel, Neil Broom, Diane Barrett, «*Computer Forensics Jumpstarts*», Wiley Publishing, 2011.

SOUVIGNET Thomas, REGNERY Matthieu, « *La récupération de données sur SSD: un défi?* », Misc n°066, mars 2013.

VANDEVEN Sally, «*Forensic images: for your viewing pleasure*», GIAC (GCFA), gold certification, SANS Institute Infosec Reading Room, 15 september 2014,

WILSDON Tom & SLAY Jill, «*Validation of Forensic computing software utilizing Black Box testing techniques*», 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

YUSOFF Yunus, Roslan Ismail and Zainuddin Hassan, « *Commun phases of computer forensics investigation models* », International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No3, June 2011.

Index

algorithme, 36, 75, 127, 129, 130, 146
analyse de signature, 70, 103, 140, 155, 158, 160, 162, 163, 165, 167, 169, 171, 173, 177, 179, 181, 184, 186, 189, 191, 194, 196, 200, 201, 203, 205, 207, 209, 211, 212, 214, 215, 216, 218, 219, 221
Anti-forensic, 35, 57
bloqueur en écriture, 117, 120, 127, 145, 148, 149, 152
boîte noire, 89, 136
Carving, 37, 74, 163, 166, 170, 174, 194, 216, 219
Cas de test, 135, 140, 145, 146, 147, 148, 149, 150, 151, 154, 157, 159, 162, 165, 166, 168, 171, 173, 176, 178, 181, 183, 186, 188, 190, 194, 196, 199, 201, 203, 205, 207, 209, 211, 212, 214, 215, 216, 218, 219, 221
copie bit-à-bit, 36, 63, 65, 145, 147
copie physique, 63, 117
Copie physique, 63, 64
Daubert, 15, 48, 49, 50, 51, 52, 55, 88, 92, 102, 229
DCO, 6, 64, 113, 116, 117, 230
DFRWS, 6, 23, 29, 231
disque dur, 37, 63, 64, 65, 71, 72, 73, 84, 109, 111, 112, 113, 114, 115, 116, 117, 120, 121, 127, 130, 132, 137, 138, 140, 147, 149, 150, 151, 152, 159, 171, 178, 179, 193, 199, 200, 205, 207, 209, 214, 218
Disque dur, 137, 138, 199, 214
E01, 66, 153
effacé, 74, 127, 140, 147, 148, 155, 158, 159, 160, 162, 165, 166, 167, 169, 171, 173, 177, 179, 181, 184, 186, 189, 191, 194, 196, 200, 201, 203, 205, 207, 209, 211, 212, 214, 215, 216, 218, 219, 221
Encase, 11, 51, 52, 53, 55, 56, 57, 58, 63, 64, 65, 66, 67, 69, 72, 79, 85, 92, 93, 101, 103, 107, 108, 111, 115, 116, 117, 120, 121, 130, 131, 132, 133, 134, 136, 137, 138, 139, 145, 146, 148, 149, 151, 152, 153, 154, 155, 157, 158, 159, 160, 161, 162, 165, 166, 167, 168, 169, 171, 172, 173, 176, 178, 179, 180, 181, 183, 184,

185, 186, 187, 188, 190, 191, 192, 193, 194, 196, 200, 201, 203, 205, 207, 209, 211, 214, 215, 218, 221, 222, 224, 225, 229, 231
espaces non-alloués, 52, 140, 155, 156, 158, 160, 162, 163, 165, 167, 169, 171, 173, 174, 177, 179, 181, 184, 186, 189, 191, 194, 196, 200, 201, 203, 205, 207, 209, 211, 212, 214, 215, 216, 218, 219, 221
expertise judiciaire, 8, 9, 14, 15, 16, 17, 18, 19, 20, 24, 27, 29, 34, 50, 51, 59, 84, 85, 93, 123, 143, 228
expertise pénale, 131
FastBloc, 63, 100, 117, 138, 139, 152, 153, 174, 177, 179, 181, 184, 186, 189, 191
FAT, 54, 73, 128, 140, 156, 159
Forensic, 6, 19, 20, 21, 23, 24, 38, 40, 46, 53, 54, 55, 56, 57, 63, 72, 79, 85, 90, 92, 100, 101, 111, 131, 132, 133, 134, 138, 145, 146, 147, 148, 149, 151, 152, 154, 157, 159, 162, 165, 166, 168, 171, 173, 176, 178, 181, 183, 186, 188, 190, 229, 230, 231
Frye, 48, 49, 52
FTK, 53, 55, 57, 59, 66, 85, 92, 101, 103, 109, 115, 116, 132
Garbage Collector, 126, 127, 128, 129, 130
gestion de l'usure, 126, 130
HASH, 36, 67, 68, 129, 152, 187
HPA, 6, 64, 113, 114, 115, 116, 117, 230
Institut national des normes et de la technologie, 10, 46, 69, 92, 99, 100
intégrité, 9, 10, 14, 21, 22, 25, 26, 32, 34, 35, 36, 65, 68, 69, 90, 97, 98, 111, 116, 118, 129, 131, 139, 146, 156, 159, 161, 163, 166, 168, 170, 172, 174, 177, 180, 182, 185, 187, 189, 192, 205, 209, 211, 212, 214
Investigation numérique, 8, 9, 10, 20, 23, 24, 26, 29, 30, 31, 34, 38, 51, 55, 56, 58, 61, 63, 83, 86, 92, 94, 96, 97, 99, 101, 102, 103, 108, 111, 115, 118, 120, 133
ISO, 15, 70, 88, 90, 93, 94, 95, 96, 97, 99
logiciel, 11, 33, 51, 52, 53, 54, 55, 56, 57, 58, 59, 61, 63, 66, 67, 69, 79, 83, 84, 85, 86, 87, 88, 89, 90, 92, 93, 98, 102, 103, 105, 106, 107, 108, 111, 115, 116, 117, 120, 121, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 145, 146, 148, 151, 152, 153, 154, 159, 161, 163, 166, 168, 172, 180, 182, 185, 187, 192, 193, 194, 196, 200, 201, 203, 205, 207, 209, 211, 212, 214, 216, 218, 221, 222, 225
MBR, 71

MCKEMMISH, 8, 21, 23, 29
MD5, 36, 67, 68, 69, 141, 146, 147, 151, 152, 156, 159, 161, 163, 166, 168, 170, 172, 174, 177, 180, 182, 185, 187, 189, 192, 203
norme, 59, 64, 70, 83, 88, 90, 93, 94, 95, 96, 97, 116, 119, 135
NTFS, 54, 72, 120, 128, 140, 147, 151, 160, 167, 169, 172, 180, 187, 189, 192, 219, 224
outil, 14, 21, 54, 57, 61, 64, 69, 85, 92, 99, 102, 103, 104, 106, 107, 110, 116, 118, 131, 136, 145, 146, 154, 222, 228
Overprovisioning, 127, 149
Plan de Test, 11, 92, 102, 111, 136, 194, 196, 199, 201, 203, 205, 207, 209, 211, 212, 214, 215, 216, 218, 219, 221
preuve, 1, 8, 9, 10, 11, 13, 14, 15, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 37, 38, 39, 40, 47, 48, 49, 50, 51, 52, 53, 55, 56, 57, 58, 59, 60, 61, 63, 64, 66, 75, 78, 85, 86, 88, 89, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 104, 105, 110, 111, 120, 123, 127, 128, 129, 131, 134, 138, 140, 154, 230
programme, 15, 25, 41, 51, 52, 53, 54, 55, 56, 57, 61, 66, 70, 71, 84, 85, 87, 88, 89, 91, 92, 100, 103, 115, 116, 121, 132, 135, 136, 139, 145, 149, 153, 154, 159, 172, 178, 185, 187, 192, 194, 196, 200, 201, 205, 207, 209, 216, 218, 219, 224, 225, 228
récupération de données, 11, 56, 71, 74, 111, 126, 129, 131, 133, 138, 139, 163, 182, 207
SATA, 117, 120, 128, 137, 138, 140, 147, 150, 151, 152, 159, 178, 179, 193, 199, 214
SHA-1, 36, 69
support original, 28, 36, 52, 61, 63, 64, 116, 118, 120, 129, 139, 145, 147, 151, 203
supprimé, 31, 72, 73, 115, 127, 140
TRIM, 126, 128, 130, 149, 151
validation, 9, 10, 14, 15, 23, 48, 55, 84, 87, 88, 89, 92, 94, 95, 96, 98, 99, 101, 104, 105, 107, 110, 132, 228, 231
Windows, 38, 41, 54, 56, 72, 73, 74, 75, 79, 80, 81, 112, 113, 119, 120, 121, 128, 134, 138, 144, 145, 146, 147, 148, 149, 150, 151, 155, 156, 158, 159, 160, 161, 162, 165, 167, 168, 169, 171, 172, 174, 177, 179, 180, 181, 184, 186, 187, 189, 191, 192, 222, 229

Table des annexes

Annexe 1 Encase® Version 6.18.1 Release Notes 236

Annexe 2 Encase® Version 7.6 Release Notes 240

ANNEXE I

Encase® Version 6.18.1 Release Notes

EnCase® Version 6.18.1 Release Notes

May 11, 2011

EnCase Version 6.18.1

Thank you for using Guidance Software products.

The *Release Notes* for this version of EnCase contain enhanced features, known issues, and items fixed. Before you install the upgrade, we recommend that you read these *Release Notes* to better understand the changes we have made.

Items Fixed

40762: Windows 7 machines with Intel core i7 series processors using 4GB of RAM were reported locking up while acquiring physical memory. This issue has been fixed and memory acquisition using the Examiner, a servlet, or WinEn now works correctly with this machine configuration.

EnCase Version 6 Guidance Product Version Matrix

The Guidance Product Version Matrix (GPVM) displays a version-to-version compatibility table for all of our products. For information about EnCase compatibility with our other products, see the GPVM at: https://support.guidancesoftware.com/node/1108.

FDCC Compliance

Guidance Software's EnCase product has been validated as FDCC compliant using these versions of NIST VHD images:

- 1/5/10 (for XP)
- 10/19/09 (for Vista)

EnCase was tested using Retina Network Security Scanner, which is an NIST validated FDCC scanner (http://nvd.nist.gov/fdcc/download_fdcc.cfm).

Support

Technical assistance is available online at http://www.guidancesoftware.com/technical-support.htm. From this page you can register for and access the Guidance Software **Support Portal**, an invaluable resource providing product-specific technical forums, an extensive knowledge base, a bug tracking database and an Online Submission Form for your questions.

Technical Support

Telephone technical support is available 24 hours a day, excluding weekends and holidays. All technical support calls are automatically routed to the open US or UK office: 10 PM Sunday – 7 PM Friday, US Pacific time (6 AM Monday – 3 AM Saturday, UK time).

US Office hours: Monday–Thursday 5 AM–10 PM Pacific time, Friday 5 AM–7 PM Pacific time

Ph: (626) 229-9191, Option 4
Fax: (626) 229-9199

215 North Marengo Avenue, Suite 250
Pasadena, CA 91101

UK Office hours: Monday–Friday 6 AM–4 PM UK time

Ph: +44 (0) 175-355-2252, Option 4
Fax: +44 (0) 175-355-2232

Thames Central, 5th Floor
Hatfield Road
Slough, Berkshire UK SL1 1QE

Telephone technical support is also available at the following numbers:

Germany: 0-800-181-4625
China: 10-800-130-0976
Australia: 1-800-750-639
Hong Kong: 800-96-4635
New Zealand: 0-800-45-0523
Japan: 00-531-13-0890

Customer Service

Please direct service questions to the Guidance Software Customer Service Department:

Monday–Friday 7 AM–5 PM Pacific time
Phone: (626) 229-9191, press 5
Fax: (626) 229-9199
Email: customerservice@guidancesoftware.com

215 North Marengo Avenue, Suite 250
Pasadena, CA 91101

You can access our Customer Service Request Form online at http://www.encaseenterprise.com/support/cs_requestform.aspx.

ANNEXE II

Encase® Version 7.6 Release Notes

EnCase® Version 7.06
Release Notes

February 21, 2013

EnCase Version 7.06

Thank you for using Guidance Software products.

The *Release Notes* for this version of EnCase contain important information regarding your EnCase application. Before you install, we recommend that you read the *Release Notes* to better understand the changes we have made.

New Product

EnCase Forensic Imager

EnCase Forensic Imager is a new product that lets you create EnCase evidence files or EnCase logical evidence files. It is similar in look and feel to EnCase, but it does not contain processing, review, or analysis functionality. EnCase Forensic Imager is available for free and does not require an EnCase license to operate. For more information, see the *EnCase Forensic Imager User's Guide*.

New Features

Support for Macintosh Logical Volumes

EnCase Enterprise now supports logical volumes for Macintosh systems. This feature functions in the same way as EnCase handles Windows logical volumes. When connecting to systems via servlets, the servlet interacts with the operating system to address the volume. Macintosh logical volumes can include single disks, RAIDs, and encrypted volumes.

Enhanced Macintosh Artifacts Support

Enhanced Macintosh artifacts support in EnCase Version 7.06 includes:

- Displaying all HFS+ file system compressed files as uncompressed
- Support for directories' hard links
- Support for Finder information and extended file attributes
- Displaying security Access Control Lists (ACLs)

For details, see the *EnCase Version 7.06 User's Guide*.

Enhanced Support for Macintosh OS X and Installer

EnCase now supports Mac OS X 10.8. This update includes an enhanced Mac installer that supports launchd, a unified, open-source service management framework for starting, stopping and managing daemons, applications, processes, and scripts.

Enhanced Support for Macintosh Servlets

EnCase now code-signs Macintosh servlets. To use this feature, you must reinstall both the servlet and the driver. This requires uninstalling the old driver and servlet and installing the new Installer.pkg, which includes the new servlet and drivers.

Formerly, when using Macintosh servlets, OS X would display a confirmation dialog. With code-signed servlets, this message does not appear.

Support for Macintosh Trash Items

EnCase now supports Trash items for Mac OS X, including support for multiple types of trash and tracking multiple items with the same filename.

Enhanced Windows Support

EnCase now provides support for:

- Parsing Windows 7 AutomaticDestinations, CustomDestinations (jump lists) and their link files.
- Parsing Windows 7 thumbs.db.
- Parsing .lnk file for IDList structures.
- Parsing support for Windows 8 artifacts:
  - Registry parsing
  - System information parsing
  - Thumbs.db parsing
- Servlet for Windows 8 and Windows Server 2012.
- Windows 8 BitLocker encryption.

Updated Documentation for McAfee ePolicy Orchestrator Integration

Documentation for McAfee ePolicy Orchestrator (ePO) is updated with instructions and screenshots for Version 4.6.

Credant Cached Authorization Credentials

EnCase now caches Credant authorization credentials for forensic administrators. Once a forensic administrator enters credentials, EnCase caches the credentials, and there is no prompt to enter them again within a given EnCase session.

Direct Network Preview

Now for the first time EnCase Forensic and Enterprise users can securely preview a live computer over a network. Direct Network Preview provides the ability to create servlets and installers that you can run and connect to without using a SAFE.

This functionality is split into two parts:

- Creating Servlets. The steps for this process are accessed by selecting **Create Direct Servlet** from the **Tools** menu.
- Adding Direct Network Preview Devices. The steps for this process are accessed by selecting **Add Network Preview** > **Add Direct Network Preview** from the **Add Evidence** menu.

For details, see the *EnCase Version 7.06 User's Guide*.

Automatic Windows Firewall Configuration

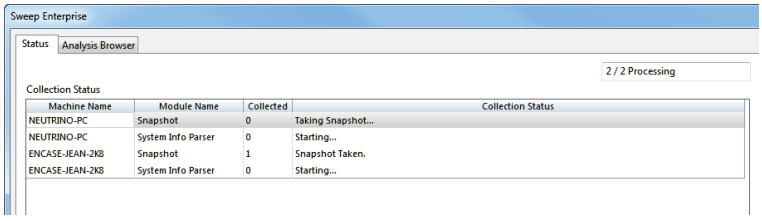
By default, the Windows Firewall does not have exceptions configured for SAFE and servlet. This can result in Windows interactively prompting you to allow incoming connections.

Now when these services run for the first time, they configure the Windows Firewall by adding necessary exceptions. This happens automatically, and no user intervention is required.

Sweep Enterprise Parallel Processing

Sweep Enterprise now has the ability to sweep multiple targets in parallel, significantly improving performance.

In this example, you can see in the **Status** tab that Sweep Enterprise is scanning two machines and four modules in parallel, instead of serially:



Note: Sweep Enterprise runs up to five threads in parallel (if the connections are available in the SAFE).

Enhanced Documentation Support for Reports and ROC

The *EnCase Version 7.06 User's Guide* now includes full documentation of EnCase Report Object Code (ROC) and includes enhanced documentation of all aspects of EnCase report creation.

Snapshot Reports Display Additional Information

Snapshot reports now contain new columns which display information from the DLL Report, Process Report, and information from open ports. New columns displayed include Instance Name, Children Processes, Open Ports, and DLL Counts.

Enhanced Support for Android OS and Device Acquisition

EnCase supports logical and physical acquisition of devices, including phones and tablets, running Android OS Version 4, Ice Cream Sandwich, as well as Version 4.1-2, Jelly Bean.

EnCase now analyzes Android physical evidence files (E01) and produces logical evidence files (L01) containing common smartphone categories: contacts, messages, call logs, and calendars. The result is a byte for byte copy of the device data partition and a navigable file/folder hierarchy. However users must manually discover, research, and export high level logical data (for example, contacts, messages, call logs, and calendars).

Android Backup

EnCase Version 7.06 also provides support for acquiring Android backup data.

Android Backup is used in two features:

1. Android backup file support:

   EnCase 7.06 supports parsing of Android Backup (*.ab) files. This is used when these files are either created manually by the user from an examined device or found as evidence on a machine. To use this feature select **Evidence** > **Backup Files** > **Android Backup**. If the backup is encrypted, EnCase decrypts it if you supply the password.

2. Acquisition of an Android device using the backup functionality:

   This feature is available only for devices running Android OS versions 4 and above (Ice Cream Sandwich and Jelly Bean). This is an alternative method for logical acquisition and complements the existing Android logical acquisition. It is accessible via the Android OS 4.x option in the **Devices** section of the smartphone acquisition dialog. It uses a slightly different acquisition method. After starting the acquisition, on the device screen you are prompted to press **OK** to start the backup process.

Enhanced Support for Tablets

EnCase Version 7.06 provides support for these tablets:

- Google Nexus 7
- Acer Iconia Tab A500
- Samsung Galaxy Tab 2
- Kindle Fire HD (support for Lightspeed browser artifacts and social media)

File Type Updates

EnCase now supports additional file types for devices running the Android operating system. The new file types are shown in the table below.

Name	Extension(s)	Category
Android Application Package	apk	Archive
Android Dalvik Executable	dex, odex, deodex	Executable
SQLite Write-Ahead Log	db-wal, sqlite-wal	Database
SQLite Shared Memory File	shm	Database

The following are renamed file types:

Old	New	Extension
HP-UX Archive	Unix Archive	a
HP_UX Object File	ELF (Executable and Linkable Format)	o
HP_UX Object File	Unix Object File	01

Smartphone Reports Data Can Be Exported for Use by Microsoft Excel

Data displayed in smartphone reports, in Summary view only, can be exported as comma separated value files (.csv), and used by Microsoft Excel.

Enhanced Support for Symantec Endpoint Encryption

EnCase now supports Symantec Endpoint Encryption Version 8.2. As with all Symantec Endpoint Encryption versions, EnCase works with user and admin credentials.

Enhanced Oracle Outside In Support

EnCase now uses Oracle Outside In Version 8.4.

Items Fixed

Acquisition/Add Device/Preview/File System

40896: EnCase records display Mobile Data for phone logical evidence files (LEFs), Internet for Internet LEFs, and Email for Email LEFs.

50423: EnCase no longer detects FastBloc when the **Detect Legacy FastBloc** checkbox is cleared.

52894: Secure Storage correctly lists the items associated with a disk, and does not repeat disks in its listing.

53272: When viewing the evidence information for a newly acquired device, the EnCase Version column now displays the correct version number.

59934 and 60095: EnCase no longer crashes when trying to recreate an undocked view from a previous session.

60484: EnCase now releases the hold on a device after acquisition through the Evidence Processor, and the device can be safely ejected.

60536: When performing a physical acquisition, EnCase now prompts you to create an output path if the specified path does not exist.

61796: The EnCase search engine has been optimized to make better use of available information. EnCase now finds Registry keywords that it previously failed to locate.

61846: When acquiring a device using the SHA1 or the MD5 and SHA1 verification hash option, and a LEF is created subsequent to that acquisition, a warning dialog now appears if the hash type is blank.

61856: BlackBerry Torch text messages containing the non-ASCII character ‘é’ are reported correctly.

61857: EnCase functions as designed when performing Smartphone acquisition of BlackBerry devices.

61935: When acquiring evidence, **Examiner Name** is now a required field.

Bookmarks

60202: Transcript bookmarks within unallocated cluster search hits now display correctly.

61338 and 61483: The Next/Previous function now works as expected when viewing the **Transcript** tab of Bookmarks.

61343: Tags in bookmarks now update without requiring any additional user action.

61898: After bookmarking MS Office 2007, 2010, and 2013 files in evidence, for display in reports, clicking the hyperlink for each file functions correctly. Office does not state the file is corrupt.

Case Analyzer

51459: In Case Analyzer, content refreshes as expected when browsing from tab to tab.

51478: $Logfile views no longer display internal database columns.

62639: Records parsed from wtmp no longer show a reversed IP address.

Doc/Transcript

29506: Doc view displays Word 4.x text with even spacing.

37177: Now partially generated transcripts display in the UI and are added to the index when run via the Evidence Processor.

37315: An .eml file now displays correctly in Doc view.

49022: A PDF in an evidence file now displays correctly in the **Doc** tab.

Email

42442: When you mouse over the email body of a LEF, tool tips appear as expected.

47516: Japanese PST is no longer garbled.

Encoding/Text Styles/Fonts

60241: Focus on any highlighted data is now maintained when switching between Text view and Hex view.

EnScript

33893: WebServiceClass::RequestClass now returns correct data.

44225: When using an unusual EnScript syntax, the compiler no longer shows an object leak when there is actually no leak.

49546: Example DatabaseClass EnScript no longer causes an error.

51977: The IPFieldClass now displays the IPv6 (loopback) address correctly.

61634: Now when multiple bookmarks on the same item are created by EnScript, the correct number of objects displays in Bookmarks view.

61770: When you mount a nested .zip file, TruePath, when accessed via EnScript, now points back to the root device.

Evidence Files

62952: When an encrypted .Ex01 file is used, the password for the file is no longer stored in Secure Storage.

Evidence Processor

50668: The Evidence Processor System Info parser returns account profile paths as expected.

53151: When you set the date format to mm/dd/yyyy, the last logon date for accounts collected in the System Info Parser is now correct.

61734: EnCase no longer crashes after acquiring a new device and processing it.

62464: EnCase no longer crashes when processing evidence containing a recovered Chrome cache file.

62469: EnCase no longer crashes if the Verification thread completes while a popup menu displays.

Export Files/Folders

49561: When creating a review package, if you exceed a certain number of files (around 2,000), the export no longer becomes slower.

50378: When you use a LEF from a phone acquisition and select the **Add link to File** option to export the file, the file is now exported correctly.

General

50296: Item Path information is now consistent in all appropriate tabs.

51103: An EnScript option was added to allow EnCase to set the date properly for any DST mode.

52036: During a raw keyword search, the progress bar is no longer truncated by performing a refresh function.

62042: EnCase now can specify a time of 00:00 when using a foreign 24 hour system time format.

Hashing/Hash Sets

60133: Hashkeeper data now imports correctly into EnCase.

61873: Hash sets now correctly display in the Manage Hash Library window.

Index/Query Index

51643: After indexing multiple pieces of evidence in a case, when you enter a query, aggregate results display instead of results for the last index only.

60244: Index search highlights are corrected for words containing diacritical markings.

60320: When searching for foreign characters with accents (for example, é), EnCase now returns the correct results in the Table pane.

60652: When using the nw/ or the npre/ operators, the word on the left size of the operator is the only word required to be present for the search to return a hit.

60832: A proximity index search no longer returns results for the first two words only.

61375: EnCase now returns the correct number of hits when using `or` logic.

Internet

48824: When running a condition on Internet artifacts, the **Report** tab in the View pane now displays content correctly.

60098: Default view for Internet records lists correct Internet fields.

LinEn

48949: EnCase no longer crashes when attempting to create a LinEn boot disk.

Records

50625: When performing a reverse sort on records, the reverse sort is no longer slow and takes the same amount of time as a regular sort.

Report

46997: EnCase no longer displays an error message for margin values that are within range.

59803: EnCase no longer crashes when viewing the **Console** tab in an environment where Windows folder redirection is used to map the Users Profile to a network share.

60776: After inserting the evidence table into a report template, partition information is included as expected in main reports.

61972: A bookmark of transcript text now displays correctly in the Examination report.

62058: The DLL Report view displays a DLL name for every row.

SAFE

61111: NAS configuration now accepts `localhost` as a server address.

Sweep Enterprise

46674: The Report Zoom menu now works correctly and displays the right percentage.

51116: Blue checking **Views** in the Analysis Browser now adds all views to a report.

61447: The Deleted view no longer contains the same files as the Collected Files view.

UI/Controls/Configuration

50322: You can move or copy items in the File Types view.

50514: A review package now opens when the filename uses a single quote, and there is no JavaScript error in the .hta file.

53162: In the Search view **Index** tab, if you enter an index expression and output to PDF File, the PDF is no longer blank.

60471 and 61396: When viewing sectors, Disk view now populates the sector position column if focused on a sector outside the volume.

60574: Menu items no longer disappear when switching tabs in an undocked pane.

61270: The keyboard shortcut **Ctrl+U** now performs an Autofit All.

Users/Roles/Permissions

61853: When selecting an Active Domain user to associate with a SAFE user, the **Select User or Group** > **Locations** dialog now displays child domains.

Virtual File System

61033: After mounting a folder as a network share and trying to browse to a file that is in a deeply nested folder, ending VFS no longer causes a crash on 32-bit Windows machines.

Known Limitations

62196: EnCase returns empty records when the Sweep Enterprise Snapshot module takes more than ten minutes to run on a machine. This causes EnCase to time out, and fails to return any Snapshot data for that machine. When this happens you can reboot the machine that returns these empty records and rerun Sweep Enterprise with the Snapshot module on.

Note: The Sweep UI does not tell you which targets return no data. To get that information, you must query the Sweep.sqlite database using a query of this form: (Select B.Target From Snapshot as A, _TargetRuns as B Where A._TargetRuns_Key = B.ID and A.Name = ‘’)

The Sweep database is stored in the Case folder, under EnScript/Sweep Enterprise.

Found in Version 7.05

51723: 32-bit x86 Evidence Processor generates an error and does not complete successfully. Workaround: Guidance Software strongly recommends that you install 64-bit EnCase.

Found in Version 7.04

43707: When acquiring email data from Acer tablets, only some Gmail messages from the inbox are able to be parsed. Gmail messages in drafts and other folders are not captured in the .L01 file. This is due to a change in how Gmail caches information. In addition, the default Acer email application does not provide read access to its data, so no email messages from the default email application can be acquired.

Found in Version 7.03

46686: Email messages for Blackberry phones are shown in a Smartphone Report only if they are in Plain Text.

45813: Index hits with large numbers of characters that wrap over line breaks do not display in the Review tab.

Guidance Software Product Compatibility Tables

The Support Portal contains a list of version-to-version compatibility tables for all Guidance Software products at ***https://support.guidancesoftware.com/matrix***.

Encryption Support

EnCase now supports the following encryption products.

Vendor	Product	Supported Versions	64-bit Support
Check Point	Check Point Full Disk Encryption (formerly Pointsec PC)	6.3.1 up to 7.4	Yes
Credant	Mobile Guardian	5.2.1, 5.3, 5.4.1, 5.4.2, 6.1 through 6.8, 7.3	No
GuardianEdge	Encryption Plus/Anywhere	7 and 8	No
GuardianEdge	Hard Disk Encryption	9.1.5, 9.2.2 , 9.3.0, 9.4.0, 9.5.0, 9.5.1	Yes
McAfee	EndPoint Encryption (formerly SafeBoot)	4, 5, 6 (for Windows and Macintosh computers)	Yes (for Versions 4 and 5)
Microsoft	BitLocker and BitLocker To Go	Vista, 7, Server 2008	Yes
Sophos	SafeGuard Easy and Enterprise (formerly Utimaco)	4.5, 5.5, 5.6	Yes (only for SafeGuard Easy, not for Enterprise)
Symantec	PGP Whole Disk Encryption	9.8, 9.9, 10, 10.1, 10.2	Yes
Symantec	Endpoint Encryption	7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.0.7, 7.0.8, 8.0, 8.2	Yes
WinMagic	SecureDoc Full Disk Encryption	4.5, 4.6	No

USGCB Compliance

EnCase has been validated as USGCB compliant using the following version of NIST VHD images:

10/14/11 (for Windows 7 only)

EnCase was tested using Retina Network Security Scanner, which is an NIST validated USGCB scanner (***http://usgcb.nist.gov/usgcb/microsoft_content.html***).

Support

Technical assistance is available online at ***http://www.guidancesoftware.com/technical-support.htm***. From this page you can register for and access the Guidance Software **Support Portal**, an invaluable resource providing product-specific technical forums, an extensive knowledge base, a bug tracking database, and an Online Submission Form for your questions.

Technical Support

Guidance Software offers several technical support options, including:

- Live Chat
- Support Request Form
- Email
- Telephone

Customer Service

Please direct service questions to the Guidance Software Customer Service Department:

Monday–Friday 7 AM–5 PM Pacific time
Phone: (626) 229-9191, press 5
Fax: (626) 229-9199
Email: ***customerservice@guidancesoftware.com***

215 North Marengo Avenue, Suite 250
Pasadena, CA 91101

You can access our Customer Service Request Form online at ***http://www.guidancesoftware.com/CustomerServiceRequest.aspx***.