



HAL
open science

Feedback of a Digital Forensics Expert - Part 2

Emmanuel Giguet

► **To cite this version:**

Emmanuel Giguet. Feedback of a Digital Forensics Expert - Part 2. Master. Master 2 Informatique Spécialité Cybersécurité - module Forensique, France. 2023. hal-04454350

HAL Id: hal-04454350

<https://hal.science/hal-04454350>

Submitted on 13 Feb 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Retour d'un expert judiciaire en informatique

Emmanuel Giguët
CNRS Researcher at GREYC Lab

emmanuel.giguët@cnrs.fr

L'investigation numérique

- L'investigation numérique
 - Aussi appelée « analyse forensique » ou « *Digital Forensics* »
 - Analyse systématique et exhaustive de supports numériques à l'aide de matériels et logiciels spécifiques
- Méthode spécifique à l'analyse des traces numériques
 - Analyse qui garantit l'intégrité/la préservation des données
 - Analyse reproductible
- Champs d'applications variés
 - Criminalistique, Police/Justice
 - Assurance, Art, ...



L'expertise judiciaire

- L'expertise judiciaire en informatique
 - Utilise une méthode forensique, des matériels forensiques, des logiciels forensiques
 - Rechercher toute trace d'activités numériques en lien avec une affaire
 - Pour confirmer ou infirmer des dires ou des hypothèses
 - Identifier et mettre en relation des traces pertinentes, vérifier la cohérence
 - Tirer des conclusions
- Spécificité de certaines expertises
 - Le principe du contradictoire
 - Tout élément doit pouvoir être débattu





Réservé
aux abonnés

ENTRETIEN. Gendarme et expert du numérique : la « pédopornographie représente 80 % de mon travail »

Escroquerie par internet, vente de drogues ou de faveurs sexuelles en ligne : à la gendarmerie des Deux-Sèvres, l'adjudant-chef Bortoluzzi passe ses journées à analyser des fichiers numériques pour y dénicher des preuves. À l'occasion du mois d'octobre 2023 dédié à la cybersécurité, Le Courrier de l'Ouest l'a rencontré.

C Le Courrier de l'Ouest
Entretien : Jordan GUERIN-MORIN.

Modifié le 09/10/2023 à 12h24

Publié le 09/10/2023 à 07h38

Abonnez-vous



LIRE PLUS TARD



PARTAGER

Newsletter La
Matinale

Chaque matin, l'actualité du
jour sélectionnée par
Ouest-France



L'adjudant-chef Pascal Bortoluzzi est enquêteur N-Tech à la gendarmerie des Deux-Sèvres, chargé d'analyser des appareils numériques dans le cadre d'affaires criminelles. | CO – JORDAN GUERIN-MORIN

L'expertise au tribunal de commerce et le principe du contradictoire

- Prendre connaissance et comprendre la mission
 - Éventuellement appeler le magistrat
 - Tenter de saisir la pertinence, le bien-fondé avant d'accepter
 - Apprécier l'assistance d'un sapiteur / tenter d'apprécier les délais
- Se préparer à la mission
 - Attendre la consignation = avance sur frais
 - Vérifier si la mission est toujours d'actualité
 - Demander au magistrat les éléments de la procédure
- Prendre contact avec les parties et leur avocat
 - Fixer un premier rendez-vous
 - Demander les pièces jugées nécessaires à considérer et le délai pour les fournir
 - Les obtenir avant le premier rendez-vous
 - Négocier le lieu du rendez-vous
- Respecter le contradictoire
 - Toutes les pièces reçues doivent être portées à la connaissance des autres parties
- Informer par courrier recommandé avec AR la date et lieu du rendez-vous (GPS)
 - Préciser les pièces reçues sur lesquelles vous vous appuyerez, mettre une référence, une pagination
- Faire une relance : avant le rendez-vous, vérifier que les avocats n'ont pas changé
 - Pas de report de dernière minute

L'expertise au tribunal de commerce

- Le jour du rendez-vous : l'habit fait le moine
 - Travailler sa tenue et sa voix
 - Prendre ses documents, son dictaphone, son carnet de notes, ses stylos, ...
 - Arriver le premier, patienter sans accepter de café ou autre
 - Occuper la place centrale, commencer à l'heure
 - Rappeler le rôle de l'expert
- Lancer les débats => écoute active
 - Possibilité d'échanges très vifs
 - Prendre position, écouter les réactions
- Déjeuner seul => consolider les notes
- L'après-midi : reprise des débats
 - Évaluer la nécessité de pièces complémentaires => lettre AR
 - Fixer une éventuelle nouvelle date de réunion
- Produire un pré-rapport, fixer date limite pour recevoir les dires
- Produire le rapport final et le transmettre au magistrat

L'expert judiciaire

- Expert indépendant, assermenté
 - Sur candidature, après examen de recevabilité
 - Missions de la justice/police/gendarmerie : procureur/juge/OPJ
 - Libre d'accepter ou de refuser les missions
 - Libre de mener l'expertise comme souhaité
 - Légalement responsable
- Utilise une méthode et des outils forensiques : acceptabilité
 - Analyse qui garantit l'intégrité des données : conservation de la preuve
 - Analyse systématique et exhaustive
 - Analyse reproductible
- Doit accomplir la mission
 - Rendre un rapport lisible dans un délai correct
 - Répondre aux questions posées



Les types de mission

- 3 grands types de mission (réquisition)
 - Au cours de l'enquête (matériel déjà saisi), à domicile
 - Pendant une perquisition, chez le suspect
 - En garde à vue
- Type de mission détermine le scénario d'analyse
 - Contrainte de temps
 - Reproductible et intégrité
 - Priorisation différente
 - Traitements longs différés



Accomplir la mission :

- Prendre connaissance et comprendre la mission
- Prendre en charge les scellés
 - Vérifier l'intégrité, briser les scellés
- Identifier les matériels et les supports numériques
 - Marque, modèle, numéro de série, capacité
 - Recherche des supports de stockage internes
- Rechercher et extraire toute trace en lien avec l'affaire
 - Ou susceptible d'éclairer l'affaire
- Rédiger un rapport et des conclusions
- Reconstituer les scellés
- Rapporter les scellés



Prise en charge et identification d'un scellé



RF
POLICE

RF

SCELLE N°
VN

P. V. N° 2020 DU 26/11/2020
PIÈCE N°
UNITÉ OU SERVICE SDN ROUBAIX

NATURE DE L'INFRACTION
tenue illégitime d'une
pousin de jeep de hasard
AFFAIRE
c/x 2020/20168

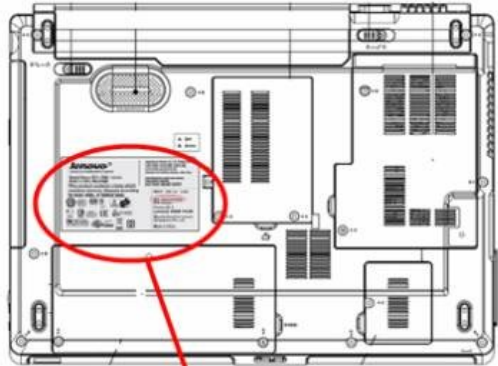
NATURE DE L'OBJET - CONTENU DU SCELLÉ
Scelle' porte -
fermeture établissement

LIEU ET CIRCONSTANCES DE DÉCOUVERTE

LES PERSONNES PRÉSENTES
BR M...
DLC W...
LE PRÉLÈVEUR
LE COMMISSAIRE
POLICE NATIONALE
SÉCURITÉ PUBLIQUE

RF
POLICE NATIONALE
SCELLE
NE PAS OUVRIR
RF

Identification des matériels et supports



EBXXXXXXXX

lenovo™
Lenovo is a trademark of Lenovo

Model Name (型号/ 型号): XXXXX
便携式计算机/ 筆記型電腦

This product contains a lamp which contains mercury; dispose according to local, state, or federal laws.

Apparatus Claims of U.S. Patent Nos. 4,631,603; 4,819,098; 4,907,093; 5,315,448; and 6,516,132 licensed for limited viewing uses only.

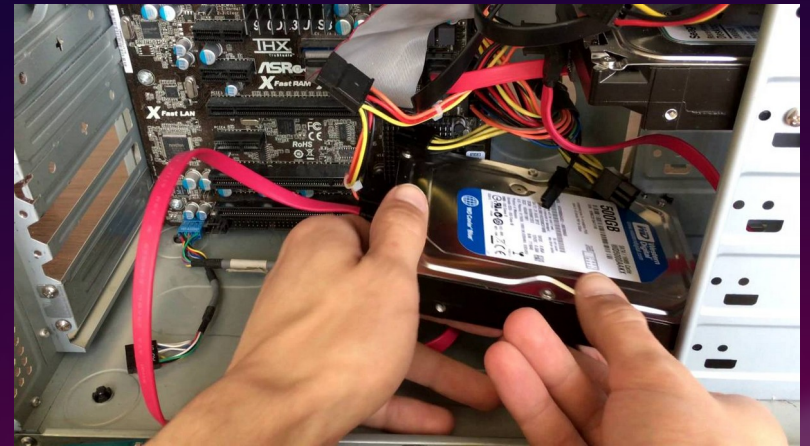
COPYRIGHTED CODE AND PARTS CONTAINED HEREIN.
©COPYRIGHT 2005,2007 LENOVO

INPUT 19V ~ 3.42A

S/N: EBXXXXXXXX

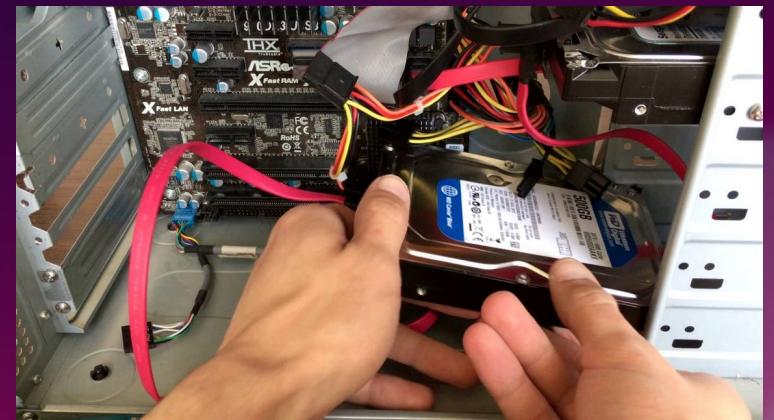
Factory ID: S
Lenovo 3000 Y410
Manufactured for Lenovo (Singapore) Pte, Ltd
Made in China

10 CCC NOM NYCE Z546
PCV AJ46 R33845 CANADA ICES/NMB-003 Class/Class B CE N14608
FC Tested To Comply With FCC Standards FOR HOME OR OFFICE USE LISTED I.T.E. E302338



La boîte à outils de l'expert

- Appareil photo, adaptateurs, câbles, pincés, tournevis, boîtiers, disques, rallonges, ciseaux, cutter, scotch, trombones, aimant...



Matériels d'acquisition

- Bloqueurs, dupliqueurs, tour d'investigation



Acquisition de données sécurisée

- Importance de la méthode
 - Garantir l'intégrité des données : conservation de la preuve
 - S'assurer que l'expertise sera recevable (et reproductible)
 - Travailler dans un environnement protégé, sécurisé, en toute tranquillité : réduire les risques d'erreur de manipulation
- Blocage logiciel des écritures
 - Désactiver l'automount et l'autorun
 - Montage en lecture seule : mount -ro
- Blocage matériel des écritures
 - La sérénité : bloqueur & duplicateur



Acquisition de données sécurisée

- Préserver l'intégrité des données
 - Hash en début d'expertise = Hash en fin d'expertise
- Réaliser une image disque à l'identique : clonage
 - Copie bit à bit avec calcul de hash à la volée : dcfldd, dc3dd
 - Soit avec un bloqueur
 - Soit avec un duplicateur de disque
- Limites à l'utilisation intensive
 - Défaillance technique : Disk stress
 - Les contraintes de temps

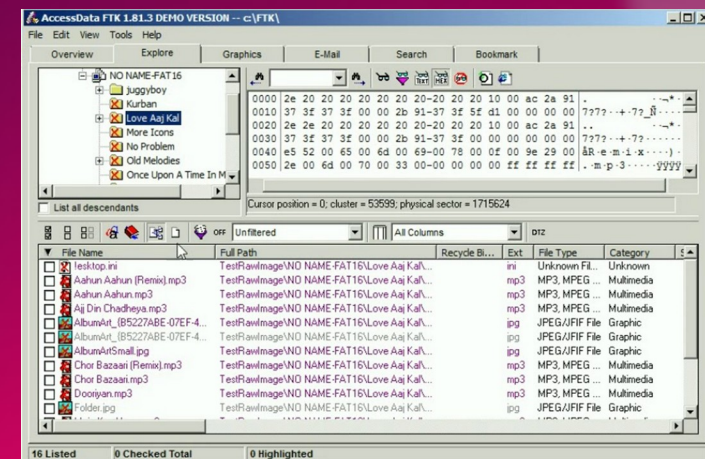


Les champs de l'investigation numérique

- Disk forensics
 - Documents accessibles depuis le système de fichiers : Text & Multimedia Forensics
 - Données accessibles mais à décoder et analyser : Metadonnées de fichiers, Log
- Social Media Forensics : contacts, partages, discussions, interactions
- Web Browser Forensics : sites visités, recherches effectuées, téléchargements
- Ad-hoc app Forensics : Cache et bibliothèque d'applications
- Forensics Data Carving : fichiers effacés, stockés en espace non alloué, fragments de fichier, fragments de données
- Memory forensics
 - Récupération de mots de passe ou de hash de mots de passe
 - Analyse de l'activité non sauvegardée : en cours de consultation, de création
- Cloud forensics and Network forensics
 - Contraintes légales liées aux juridictions et au périmètre de l'expertise
- Contenu chiffré :
 - Difficile à identifier, à différencier de l'aléatoire
 - Recherche d'applications installées, de containers suspects, de noms d'extension
 - Solution préconisée : demander les clés pour le déchiffrementS

L'analyse et l'environnement logiciel

- Les suites logicielles d'investigation numérique :
 - EnCase, FTK, Autopsy, X-Ways, Magnet IEF/Axiom
 - Aide à l'analyse des traces et la recherche de preuves
 - Aide à gérer le cas : ± gestion de projet et éviter les oublis
 - Agrégation de modules spécifiques à certaines traces/logiciels
 - Vers l'automatisation totale ? Risque d'oubli
- Aller au-delà : les outils, protos, et développements spécifiques
 - Extraire des traces de logiciels ou de sites moins populaires
 - Recherche et Veille sur des sites/forums :
Forensics Focus / Github
- Payant, souvent non open-source, non évalué :
 - Risque d'oubli ?



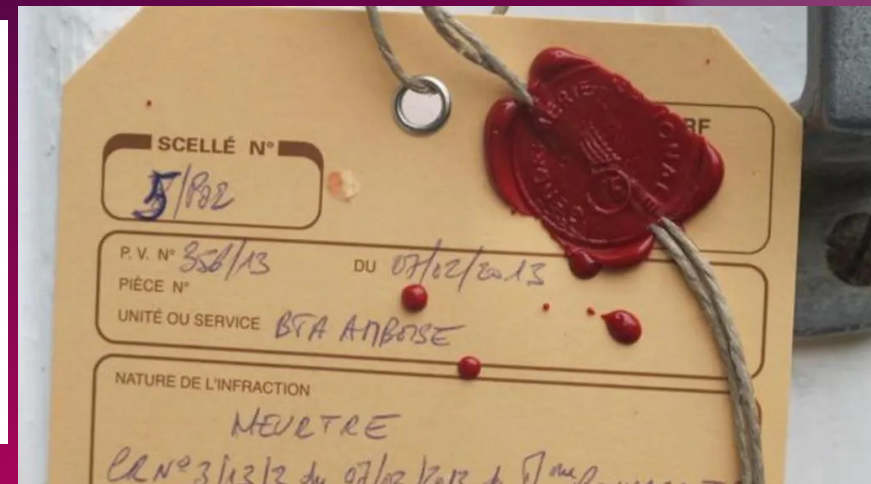
Analyse de traces horodatées

- Une analyse est par essence multi-source :
 - Logs, réseaux sociaux, mails, activité internet, les documents et fichiers multimédias
- Une analyse est souvent cross-device :
 - Stockage externe ou plusieurs ordinateurs saisis
 - Usage simultané de plusieurs matériels : discussion sur téléphone et envoi d'un document par mail depuis l'ordinateur
- Facteur commun : Horodage des contenus = Timestamped content
- Reconstruire la chronologie des événements = timeline
- Problématique : Fiabilité de l'horodage
 - Quelle date ? date d'enregistrement sur le système de fichier, date de création du fichier (métadonnée), date du document (en entête)
 - Modification volontaire, involontaire, pb horloge, de synchro, de fuseaux

Le rapport d'expertise

- Objet : répondre à la mission
- La forme du rapport :
 - Ecriture lisible pour un non expert
 - Met en avant les éléments les plus probants
 - Rester factuel, éviter la sur-interprétation, attention aux certitudes
- Introduction : la mission, les scellés pris en charge, l'environnement technologique de la mission
- Récapitule pour chaque dispositif/support
 - L'identification, le mode d'acquisition, le(s) hash(s) d'intégrité
 - Les analyses effectuées, les résultats obtenus (tableaux, extraits, ...)
 - les éventuelles incohérences détectés ou problèmes rencontrés
- Conclusion : Reprend les principaux résultats obtenus en lien avec la mission
- Peut contenir des annexes numériques

Reconstitution d'un scellé





Digital Forensics Issues

- Towards Forensics Labs ?
 - Coûts initiaux : Matériels (computers, storage devices, write blockers, disk imagers, connectors) et logiciels
 - Coûts récurrents : licence logicielle / frais de maintenance
- Accroître la confiance dans les technologies
 - Need to handle new technologies, usages, software, services, versions
 - Besoin de plus d'évaluation indépendantes et d'outils open-source
- Savoir-faire & Souveraineté
 - Comment adresse le chiffrement natif / Module de sécurité matériel
 - Multiplication des entreprises spécialisées
- Recherche sur des technologies à base d'IA
 - Text : Aller plus loin qu'une recherche par mot-clé ou expression régulière
 - Image/Video : Recherche à partir du contenu & Détection de modification du contenu