Criminalistique informatique : exploration et enjeux

La criminalistique informatique, également appelée « *inforensique* » ou « *digital forensics* », est une discipline moderne qui joue un rôle crucial dans la lutte contre la cybercriminalité.

Inspirée par des méthodes similaires à celles utilisées dans la médecine légale, cette science numérique se concentre sur l'analyse et la collecte de preuves électroniques afin de contribuer à la recherche dans les enquêtes judiciaires, d'auteurs de crime ou de délit.

Sa base repose sur l'axiome cher au Professeur Edmond LOCARD, selon lequel 'tout contact laisse des traces[1].

Cette approche méthodologique guidant en permanence l'orientation du travail des investigateurs, ces derniers s'efforcent de rassembler et de présenter en justice tous les éléments matériels de preuves tangibles en mesure d'établir la participation d'un délinquant à la commission d'une infraction ou sa présence sur une scène de crime ou de délit.

I. Le champ d'application de la criminalistique informatique :

Le champ d'application de la criminalistique numérique est vaste et englobe une multitude de supports numériques et électroniques : ainsi,
- les ordinateurs
- les téléphones GSM
- les disques durs divers et tablettes numériques
- les mémoires USB
- les cartes à mémoire
- les G.P.S.
- les drones
- l'électronique embarquée des véhicules
- les réseaux informatiques.

II. Les trois principales branches de la criminalistique informatique :

Dès l'aube des années 1990 et l'essor exponentiel des technologies numériques dans notre quotidien, la criminalistique informatique a largement élargi son champ d'application devenant une branche à part entière de la criminalistique dans l'enquête judiciaire.

Aujourd'hui, elle se divise en trois principales branches que sont :

a) L'analyse des ordinateurs ou *computer forensic* :
Cette branche se concentre sur l'analyse approfondie des ordinateurs et des supports numériques voisins incluant : ainsi,

- l'examen des fichiers protégés et non protégés des disques durs et supports de mémoire
- la récupération des données effacées
- l'analyse des horodatages et signatures
- l'étude du contenu des mémoires (y compris la mémoire vive)
- l'inspection de la base de registre
- l'examen des activités de navigation et de l'usage du courrier électronique
- la détection de logiciels de retro-Ingénierie ou anti-forensique.

b) L'analyse des appareils téléphoniques ou phone forensic :
Les investigateurs s'intéressent à l'examen des traces propres à la téléphonie, telles que :
- les répertoires de contacts
- les journaux d'appels (entrants, sortants, manqués)
- les messages électroniques (SMS, MMS)
- la messagerie instantanée
- les fichiers multimédias (images, sons, vidéos) et de bureutique (doc, xls, pdf)
- les données de géolocalisation des appareils aussi bien GPS que GSM.

c) L'analyse des réseaux ou *network forensics* :
Cette dernière branche se concentre sur la surveillance des flux de données sur les réseaux, l'extraction de clés de chiffrement et la collecte d'informations stockées dans le cloud.

- la surveillance et l'analyse des flux sur les réseaux
- la réponse aux incidents
- la collecte synchronisée en divers points du réseau
- la récupération de données supprimées, de clés de chiffrement et de données stockés dans le cloud
- l'analyse des traces rémanentes.

III. Les outils utilisés en criminalistique informatique :

Afin de préserver l'intégrité des preuves numériques, les investigateurs utilisent divers outils spécialisés pour :

Préserver l'intégrité des preuves :
- Bloqueur en écriture : dispositif électronique qui permet la lecture des informations tout en empêchant toute modification du support original.
- Outils de duplication : des logiciels permettant d'imager les supports ou des malettes dédiées pour créer des copies exactes des supports numériques (malettes logicube, copieurs Tableau TD.1)

Analyser les supports :
- Logiciels forensique spécialisés tels que *Encase*, *FTK*, *Forensic Explorer*, *X- Ways Forensics* ou le plus connu *Autopsy*.
- Outils complémentaires : logiciels pour l'analyse de la navigation Web, du courriel, de la messagerie instantanée, des ruches du registre ou de reconstruction de données.

1 - Edmond LOCARD (1877-1966) est la figure majeure dans l'histoire de la criminalistique, il est considéré comme le fondateur de la police scientifique moderne. Il a étudié le droit et la médecine et a exercé les professions de médecin, de juriste dont celle de criminologue et de professeur. En 1910, il a fondé à Lyon le premier laboratoire de police scientifique au monde et révolutionné les enquêtes criminelles en introduisant une démarche scientifique rigoureuse.

Analyse de la téléphonie :
• Malettes spécifiques des marques *CELLEBRITE*, *XRY* ou logiciels dédiés comme *Oxygène Forensic Détective* ou *Magnet Automate*.

Analyse des réseaux :
• Techniques de *netmonitoring* du réseau GSM.
• Logiciels dédiés à l'analyse et la surveillance des réseaux informatiques comme *Exegol*, *KALI Linux*, ou *Wireshark*.

Conclusions :

La criminalistique informatique est une discipline indispensable dans la résolution des crimes et délits liés aux technologies numériques, en particulier dans le contexte actuel marqué par la croissance exponentielle de différents vecteurs d'information.

En combinant expertise technique pointue, rigueur méthodologique et usage d'une panoplie d'outils spécialisés afin de préserver, analyser et présenter des preuves numériques de manière légalement recevable, les experts inforensiques apportent des réponses cruciales dans la résolution des nombreuses affaires judiciaires souvent complexes.

Leur travail permet non seulement de traduire les criminels en justice, mais aussi de renforcer la confiance dans les systèmes numériques et leur sécurité.

Enfin avec l'évolution constante des technologies, ce domaine continue de se développer et de s'adapter afin de relever les nouveaux défis de la criminalité comme les *DeepFake*, les *ransomawares* ou l'arrivée de l'I.A. et de l'informatique quantique.

Un travail efficace en matière de criminalité informatique ne se conçoit que dans un cadre juridique interdisciplinaire. ***EUROLAW FRANCE CYBER*** offre celui-ci car il est le lieu de la rencontre de spécialistes cyber (avocats, commissaires de justice, spécialistes de la propriété intellectuelle/industrielle) et d'experts judiciaires indépendants qui préparent en amont d'un dépôt de plainte pénale un dossier technique complet.

Ces travaux permettront aux services régaliens d'enquête (gendarmerie ou police) de compléter celui-ci par les outils performants *cyberntech* dont dispose l'État et permettre ainsi la transmission d'un dossier le plus complet possible au procureur de la République ou au magistrat instructeur.

Jean-Pierre PASSEMARD,
membre d'EUROLAW FRANCE CYBER
expert près la Cour d'Appel d'AIX EN PROVENCE, membre du groupe de travailcyber droit et expertise cyber