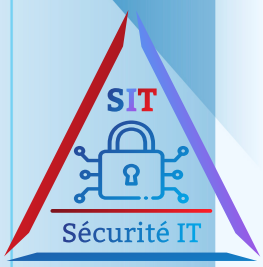

كليـــــة العلـــوم
والتقنيات - مراكش
FACULLTE DES SCIENCES
ET TECHNIQUES - MARRAKECH
MARRAKECH
جامعة القاضي عياض
UNIVERSITÉ CADI AYYAD

Module :Fondamentaux de la sécurité informatique et cyber-droit

Rapport du projet académique

Digital Forensics Investigation

Réalisé par:
ZABRATI Hind

Encadré par:
Mr SADQI Yassine

Table des matières

1 Introduction

Notre monde aujourd'hui devient de plus en plus numérique, oú la technologie est incluse dans tous côté de notre vie quotidienne, ce qui entraine une augmentation et plutôt une multiplication des crimes liées au cyberspace.
Parmi ces crimes on trouve : violation des données, l'espionnage informatique, les fraudes finançières, phishing et les attaques par ransomware. La criminalité a évolué et s'est étendu au monde virtuel. Á cause de ces nouvelles menaces, la criminalistique numérique(Digital Forensics) s'est imposée comme un domaine essentiel, dédié à l'identification, la préservation, l'analyse et la présentation des preuves numériques.
Aujourd'hui, tous ce que nous faisons laisse une trace numérique. À chaque instant, nous utilisons de nombreux appareils électroniques, tels que : téléphones mobiles, ordinateurs portables, tablettes, montres connectées, et bien d'autres qui enregistrent des informations sur notre vie privée et quotidienne. Nos communications, transactions financières et habitudes de navigation sont stockés sur ces appareils et deviennent, sans que nous sont conscient, d'énorme et véritables réservoirs de données personnelles. Cette accumulation de données a créé de nouvelles vulnérabilités, rendant ainsi le numérique une cible pour les cybercriminels, et multiplie aussi les incidents de sécurité et l'exploitation de ces informations.
Le rôle de l'enquêteur en criminalistique numérique est donc devenu plus complexe et plus indispensable que jamais. Les enquêteurs ne sont chargés plus de l'analyse d'un simple ordinateur mais plutôt ils doivent être compétents et capables d'examiner des réseaux énormes, des appareils mobiles complexes, des systèmes embarqués qui contient des milliers de nœuds. Chaque incident de sécurité soit qu'il s'agit d'une exposition de données sensibles, d'un vol de propriété intellectuelle ou d'une attaque ciblée exige une réponse rapide, méthodique et juridiquement solide.
Le rôle du spécialiste en criminalistique numérqiue est essentiel pas seulement pour comprendre et résoudre les crimes liées au cyberspace mais aussi pour aider et soutenir les enquêtes policières, les investigations au sein d'une entreprise et les efforts de sécurité nationale. Ce projet vise à explorer les fondements, les outils, et les applications concrètes de la criminalistique numérique.

2 Définition de la criminalistique numérique

La criminalistique numérique est un domaine de la cybersécurité définie lors du premier atelier de recherche sur la criminalistique numérique (Digital Forensics Research Workshop - DFRWS) en 2001 comme « **l'utilisation de méthodes scientifiquement dérivées et éprouvées pour la préservation, la collecte, la validation, l'identification, l'analyse, l'interprétation, la documentation et la présentation de preuves numériques dérivées de sources numériques dans le but de faciliter ou de faire progresser la reconstitution d'événements jugés criminels, ou d'aider à anticiper des actions non autorisées dont il est démontré qu'elles perturbent des opérations planifiées.** »
Les techniques de criminalistique numérique sont utilisées dans d'autres contextes que celui des enquêtes criminelles, mais les principes et les procédures utilisés restent les mêmes pour n'importe quel contexte ou bien enquête. Ainsi, les sources de preuves demeurent principalement constantes quel que soit le type d'enqête. Les examens de criminalistique numérique utilisent les données générées par l'ordinateur comme une source de preuve. Avant, cela concernait surtout des supports de stockage comme les disques durs ou les CD, mais aujourd'hui, on examine aussi de plus en plus souvent des captures de la mémoire vive des systèmes en fonctionnement.
Généralement, c'est grâce aux principes et procédures de criminalistique numérique que les équipes de réponse aux incidents (Incident Response Team) arrivent à comprendre ce qui s'est passé lors d'une attaque, comme la compromission d'un serveur ou une violation de données. Dans d'autres cas, comme un acte malveillant commis par un employé qui sont appelés pirates malveillants internes, la criminalistique numérique peut fournir des preuves essentielles pour identifier le responsable. Alors, avant d'examiner en détail les outils et les techniques à la disposition des équipes de réponse aux incidents, il est essentiel tout d'abord d'aborder les éléments fondamentaux de la criminalistique numérique. Ces éléments aide de spécifier non seulement un contexte pour des actions spécifiques, mais aussi une méthode pour s'assurer que les preuves recueillies dans le cadre d'une enquête sur un incident ont une utilité.
Les preuves électroniques peuvent être récupérées à partir de diverses sources, notamment les ordinateurs, les appareils mobiles, les dispositifs de stockage à distance, les appareils de l'internet des objets (IoT) et pratiquement tout autre système informatisé.
En bref, la criminalistique numérique est le processus d'investigation des systèmes informatiques, des réseaux et des appareils mobiles afin de recueillir, d'analyser et de présenter des preuves numériques devant un tribunal. Elle joue un rôle majeur non seulement dans la résolution des crimes, mais aussi dans la prévention des failles de sécurité futures et dans le soutien de la responsabilité juridique, organisationnelle et réglementaire.

3 Preuve électronique

3.1 Définition

Une preuve (en science ou en droit) est un fait ou un raisonnement qui démontre, établit, prouve la vérité ou la réalité d'une situation de fait ou de droit.
Les preuves numériques sont définies comme des informations et des données de valeur pour une enquête qui sont stockés, reçus ou transmis par un appareil électronique. Cette

preuve peut être obtenue lorsque des appareils électroniques sont saisis et sécurisés pour examen.

3.2 Les caractéristiques d'une preuve numérique

Les preuves numériques doivent présenter certaines caractéristiques pour être recevables devant un tribunal. Elles doivent être :
Recevables : Les enquêteurs doivent présenter des preuves recevables, c'est-à-dire pertinentes pour l'affaire, qiui justifient la demande du client, et qui peuvent être communiquées de manière impartiales.
Authentiques : Il est très facile de manipuler les preuves numériques. Par conséquent, les enquêteurs doivent fournir des éléments justificatives attestant de l'authenticité des preuves, notamment leur source et leur pertinence pour l'affaire. Si nécessaire, ils doivent également fournir des informations telles que l'auteur ou le mode de transmission des preuves.
Complètes : Les preuves doivent être complètes, c'est-à-dire qu'elles doivent confirmer ou contredire les faits pertinents à la procédure. À défaut, le tribunal risque de rejeter l'affaire pour insuffisance de preuves solides.
Fiables : Les experts judiciaires doivent extraire et traiter les preuves tout en conservant un enregistrement des tâches effectuées tout au long du processus afin de prouver leur fiabilité. Les enquêtes médico-légales doivent être menées uniquement à partir de copies des preuves, car le tribunal doit conserver les preuves originales pour toute référence ultérieure.
Crédibles : Les enquêteurs et les procureurs doivent présenter les preuves de manière claire et compréhensible aux membres du jury. Ils doivent justifier les faits de manière précise et recueillir l'avis d'un professionnel du domaine afin de valider la méthode d'enquête utilisée.

3.3 Types de preuves numériques

Les preuves numériques se présentent sous de nombreuses formes, comme :

1. **Logs :**
   En informatique, un fichier log permet de stocker un historique des événements survenus sur un serveur, un ordinateur ou une application.
   Ils peuvent provenir de :
   - **Systèmes d'exploitation :** Ils enregistrent des événements comme :
     - ◇ Tentatives de connexion (réussies ou échouées)
     - ◇ Fermetures de sessions
     - ◇ Mises à jour ou erreurs système critiques
   - **Bases de données :** Les bases de données génèrent des logs pour :
     - ◇ Les accès aux données ; c'est à dire qui a consulté quoi et quand
     - ◇ Les modifications effectuées sur cette base de données comme : ajout, suppression, mise à jour...
     - ◇ Les tentatives d'accès non autorisées
   - **Réseaux :** Les équipements réseau comme les routeurs, pare-feu, serveurs proxy enregistrent :

- ◇ Les adresses IP utilisées par les utilisateurs
- ◇ Les volumes de données échangés
- ◇ Les connexions entrantes et sortantes

2. **Images et vidéos :**
   Les images et vidéos sont une source de preuve numérique très importante, elles permettent de capturer des événements en temps réel et de documenter visuellement des actions, des lieux ou des individus. Elles incluent :
   - Caméras de surveillance (CCTV) : qui sont des caméras installées dans les des lieux publics qui enregistrent et détectent les mouvements de manière continue.
   - Photos et vidéos prises avec des téléphones ou appareils numériques : ces appareils sont aujourd'hui des outils courants pour capturer des scènes. Les fichiers générés peuvent contenir des métadonnées comme : date et heure de la prise, localisation GPS, modèle de l'appareil utilisé...
3. **Archives :**
   Une archive est une représentation abstraite d'un ensemble d'éléments, qui peuvent être des fichiers, des répertoires et des liens. Les formats d'archives les plus connus sont le format zip, rar, tar, iso et 7z. Elles peuvent contenir :
   - **Documents sensibles** comme des contrats, factures, plans, etc.
   - **Images ou vidéos** qui peuvent être cachées pour dissimuler des preuves.
   - **Codes sources ou bases de données :** qui permettent d'identifier la fonction du logiciel qui est soit bénéfique ou malveillante, de retrouver des commentaires laissés par le développeur qui révèlent parfois son identité ou son intention et ainsi déterminer l'origine et la date de création du malware.
4. **Données actives :**
   Les données actives désignent les fichiers récemment créés ou actuellement utilisés par des logiciels. Elles reflètent les activités immédiates effectuées par l'utilisateur.
   - **Fichiers temporaires :** par exemple lors de la rédaction d'un document Word, les fichiers temporaires servent à prévenir la perte de données en cas de crash. Même s'ils ne soient pas directement visibles, ces fichiers peuvent contenir des informations sensibles.
   - **Fichiers de session :** il existe certains logiciels qui créent des fichiers pour enregistrer l'état d'une session en cours, comme : des éditeurs de texte, logiciels de traitement d'images...
5. **Métadonnées :**
   Une métadonnée est une donnée qui fournit de l'information sur une autre donnée. Elles sont importantes et cruciales en criminalistique numérique car elles fournissent des détails sur la création, la modification et chemin d'utilisation ...
   - **EXIF des photos :** les images prises par des caméras contient des métadonnées EXIF (Exchangeable Image File Format) comme :
     - ◇ La date et l'heure de prise de photo
     - ◇ Les coordonnées GPS
     - ◇ Le modèle de l'appareil utilisé
   - **Métadonnées de documents :** Un fichier Word ou PDF peut contenir :
     - ◇ Le nom de l'auteur

◇ La date de création et modification

En bref, les preuves numériques se présentent sous de nombreuses formes. En connaissant où les chercher et en étant capable de les présenter au tribunal, des preuves solides peuvent renverser la situation juridique et prouver ou réfuter l'implication d'un suspect dans des activités criminelles.
Avec les bons outils et techniques d'investigation numérique, il est possible de récupérer la plupart, voire la totalité, des fichiers, même écrasés, corrompus ou intentionnellement supprimés.

4 Objectifs et rôles de la criminalistique numérique

La criminalistique numérique a pour objectif principal l'extraction des données provenant de preuves électroniques, de les convertir en informations exploitables, et de présenter ces résultats de façon pertinente pour appuyer des procédures judiciaires et ainsi afin de comprendre et prouver un incident numérique ou un crime.
Plusieurs autres objectifs sont visés :

- Extraction et préservation des données issues des systèmes informatiques.
- Identification la source et le lieu de l'incident numérique.
- Détermination des personnes responsables de l'incident.
- Compréhension de la manière dont l'incident a été réalisé, c'est-à-dire savoir les techniques utilisées .
- Quantification des dommages causés par l'incident.
- Préparation des preuves recevables pour les procédures judiciaires.
- Renforcement de la sécurité en identifiant les failles exploitées.

La criminalistique numérique ne se limite pas à la phase judiciaire uniquement. Elle contribue activement à la protection de l'intégrité des systèmes informatiques, en identifiant les failles de sécurité, en détectant les intrusions et en offrant l'aide aux organisations pour renforcer la cybersécurité au sein de leur établissement. Lorsqu'un incident est détecté, elle permet de collecter et de préserver méthodiquement les preuves, afin d'analyser l'étendue de l'attaque et de mesurer les dommages et les dégâts causés.
Ainsi, en retraçant les traces laissées par les cybercriminels, la criminalistique numérique collecte des preuves solides, recevables devant les tribunaux. Ces éléments donnent aux victimes la possibilité de poursuivre les responsables avec des éléments solides, mais aussi de renforcer leurs mesures de prévention.
La criminalistique numérique est devenue un élément clé des stratégies de cybersécurité. Elle joue un rôle essentiel en atténuant les conséquences des cyberattaques et en établissant les fondements juridiques indispensables pour assurer l'application et le respect des lois dans l'espace cyber.

5 Processus d'investigation numérique

Le processus d'investigation numérique définit le flux des preuves numériques liées à un incident, depuis leur identification jusqu'à leur présentation devant la direction ou une autorité judiciaire, comme un tribunal civil ou pénal.

Plusieurs modèles décrivent ce processus, et la plupart suivent une structure similaire. Dans ce rapport, nous adoptons le cadre d'investigation numérique proposé par le DFRWS (Digital Forensic Research Workshop), qui comprend six étapes principales :

1. **"Identification"**
2. **"Préservation"**
3. **"Collecte"**
4. **"Examen"**
5. **"Analyse"**
6. **"Présentation"**

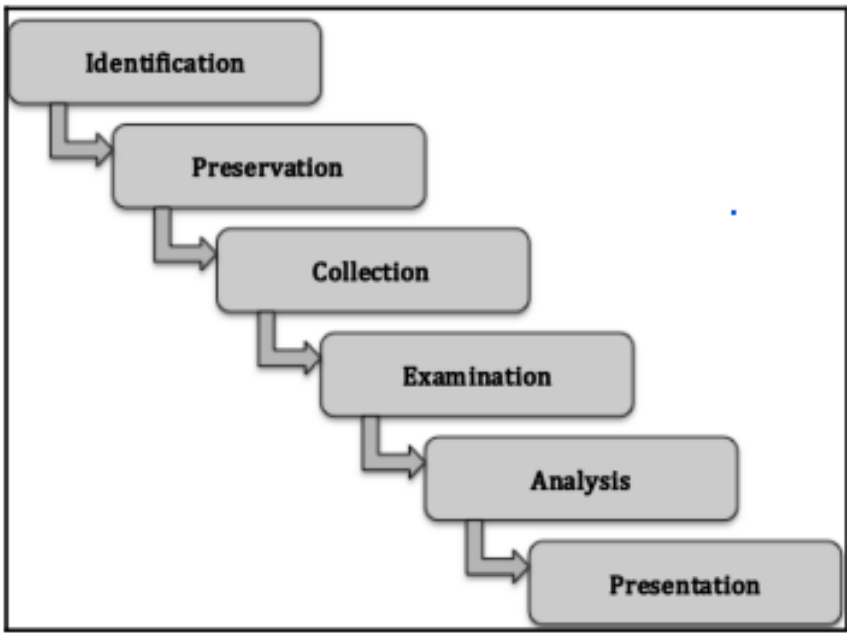

FIGURE 1 – Les etapes du processus d'investigation numérique

5.1 Identification

La phase d'identification présente l'étape initiale et l'une des plus critiques d'une enquête en criminalistique numérique. Elle vise à repérer les incidents potentiels et à identifier les sources de preuves numériques. Cela implique l'identification de divers appareils, notamment les ordinateurs de bureau, les ordinateurs portables, les serveurs, les smartphones, les tablettes et les supports de stockage externes.Cette étape oriente les investigations futures en assurant que rien de pertinent n'est négligé dès le départ.
Dans ce contexte, un concept fondamental en criminalistique est souvent utilisé pour orienter les recherches : le principe d'échange de Locard. Ce principe postule que lorsque deux objets entrent en contact, ils laissent une trace l'un sur l'autre. Par exemple, si vous entrez dans une maison avec de la moquette, la saleté de vos chaussures reste sur la moquette et la moquette laisse des fibres sur les semelles. Ces traces échangées constituent les bases de la science des traces en criminalistique physique. Dans le monde numérique, nous obtenons souvent des traces très similaires lorsque deux systèmes entrent en contact. Par exemple, si une personne consulte un site web, le serveur web ou le pare-feu de l'application web peut enregistrer l'adresse IP de la personne dans un journal de collecte. Le

site web peut également déposer un cookie sur l'ordinateur portable de la personne. T
L'identification d'un incident de sécurité repose sur la surveillance constante de plusieurs sources d'information. Parmi les plus courantes :

- **Journaux système (logs) :** enregistrements des événements système, comme les connexions utilisateur, les erreurs d'application ou les accès non autorisés.
- **Alertes des systèmes de détection d'intrusion (IDS/IPS) :** notifications générées lorsqu'un comportement suspect est détecté sur le réseau ou un hôte.
- **Signalements manuels ou comportements anormaux :** activité inhabituelle observée par un utilisateur ou détectée via des outils d'analyse comportementale ou réseau.

5.2 Préservation

Une fois les preuves identifiées, il est important de les protéger de toute modification ou suppression. Pour les preuves telles que les fichiers journaux, il peut s'avérer nécessaire d'activer des contrôles protégeant ces fichiers contre toute suppression ou modification. Concernant les systèmes hôtes tels que les postes de travail, il peut s'avérer nécessaire d'isoler le système du reste du réseau par des contrôles physiques ou logiques, des contrôles d'accès réseau ou des contrôles de périmètre. Il est également essentiel d'interdire l'accès à un système suspect aux utilisateurs. Cela permet d'éviter toute altération délibérée ou involontaire des preuves. Un autre aspect des mesures de préservation réside dans le recours croissant aux plateformes virtuelles. La préservation de ces systèmes peut être assurée par des systèmes de capture instantanée et une sauvegarde sur un stockage non volatile.

5.3 Collecte

L'étape de collecte est le point de départ du processus d'acquisition des preuves numériques par les experts en criminalistique numérique. Elle consiste à recueillir, de manière rigoureuse et documentée, toutes les données pertinentes identifiées lors de la phase précédente. Lors de l'examen de preuves numériques, il est important de comprendre la nature volatile de certaines d'entre elles. Les preuves volatiles sont celles qui peuvent être perdues lors de la mise hors tension d'un système. Pour les équipements réseau, cela peut inclure les connexions actives ou les données de journal stockées sur l'appareil. Pour les ordinateurs portables et de bureau, les données volatiles incluent la mémoire vive ou le cache du protocole de résolution d'adresse.
Il est impératif que les experts en criminalistique numérique prennent en compte cette volatilité dès le début du processus de collecte de preuves. Des méthodes doivent être employées lorsque les preuves volatiles sont collectées et transférées sur un support non volatile tel qu'un disque dur externe.
Ainsi, le traitement sécurisé et rigoureux des preuves numériques est fondamental. Toute erreur dans la manière dont ces preuves sont acquises ou manipulées peut compromettre leur intégrité, voire les rendre irrecevables dans le cadre d'une procédure judiciaire, qu'elle soit pénale ou civile.
Afin d'assurer que les preuves collectées soient exploitables juridiquement, leur traitement doit respecter des principes stricts :

- **Préservation des preuves originales :** Les experts doivent éviter toute action susceptible de modifier les données initiales. Par exemple, l'accès direct à un système actif doit être évité sauf en cas de nécessité absolue. Certaines opérations peuvent inévitablement altérer des preuves ; dans ce cas, une documentation minutieuse et une justification technique claire permettent de préserver leur valeur probante.
- **Documentation complète :** Un thème récurrent dans les forces de l'ordre est l'expression «si vous ne l'avez pas écrit, cela n'a pas eu lieu». Cela est particulièrement vrai en matière d'investigation numérique. Chaque action doit être documentée d'une manière ou d'une autre, notamment par des notes et des schémas détaillés. Les photographies sont également un moyen de documentation. Une documentation adéquate permet aux enquêteurs de reconstituer la chaîne des événements si l'intégrité des preuves est remise en question.

5.4 Examination

La phase d'examen constitue une étape cruciale où les experts en criminalistique numérique utilisent des outils et des techniques spécialisés pour inspecter minutieusement les preuves collectées. L'objectif est d'identifier, de localiser et d'extraire les données pertinentes sans altérer leur intégrité. Cela peut inclure des éléments comme les fichiers supprimés, les artefacts de navigation, les journaux système, les métadonnées de fichiers, ou encore les traces laissées par un logiciel malveillant.
Par exemple, si une attaque est suspectée d'avoir compromis un poste de travail, les examinateurs peuvent analyser une image mémoire afin d'identifier les processus actifs, les connexions réseau ou les modules suspects chargés en mémoire. Dans d'autres scénarios, comme une compromission de serveur, ils peuvent rechercher des séquences spécifiques dans les fichiers journaux ou reconstituer des sessions SSH à partir de captures réseau (PCAP) pour déterminer les actions d'un attaquant.
Cette phase s'effectue toujours dans le strict respect de la préservation des preuves. Une mauvaise manipulation ou un manque de rigueur peut entraîner la contamination ou la perte d'informations essentielles, rendant les éléments recueillis inadmissibles devant un tribunal. C'est pourquoi des copies bit-à-bit («forensic images») sont généralement examinées à la place des originaux.
Enfin, les résultats issus de cette phase constituent une base essentielle pour l'étape suivante : l'analyse, durant laquelle les données extraites seront corrélées, croisées et interprétées dans le but de reconstituer les faits, comprendre le mode opératoire et, si possible, identifier les auteurs.

5.5 Analyse

La phase d'analyse intervient après l'examen des preuves numériques. Elle consiste à interpréter les données extraites afin de reconstituer les événements liés à l'incident de sécurité. Cette étape est essentielle pour comprendre le déroulement de l'attaque, identifier les vulnérabilités exploitées, les systèmes affectés, et éventuellement les auteurs de l'intrusion.
L'analyste informatique commence par examiner les éléments potentiellement pertinents à la lumière des autres données recueillies, en établissant des corrélations entre elles. Par exemple, si l'analyste informatique découvre qu'un hôte compromis dispose d'une

connexion ouverte à une adresse IP externe, il corrèle cette information avec l'analyse des paquets capturés sur le réseau et il peut isoler le trafic spécifique lié à cette connexion.
Une analyse approfondie peut mettre en évidence l'envoi régulier de signaux par l'hôte vers un serveur de commande et de contrôle (C2), ce qui indique la présence d'un logiciel malveillant. En exploitant et se basant sur des bases de données de renseignement sur les menaces (threat intelligence), il devient alors possible d'identifier la nature du serveur C2, le type de logiciel malveillant utilisé. Ces informations permettent ensuite à l'analyste de retracer le vecteur d'attaque initial.
Cette phase s'appuie sur une approche méthodique guidée et orientée par les indices déjà collectées et exige une expertise avancée afin de convertir des données brutes en informations pertinentes et admissibles sur le plan juridique.

5.6 Présentation

La phase de présentation constitue l'aboutissement du processus d'investigation numérique. Elle vise à communiquer les résultats de manière claire, concise et impartiale. Dans la grande majorité des cas, l'expert est tenu de rédiger un rapport écrit détaillé, retraçant l'ensemble des actions menées et mettant en évidence les données clés recueillies tout au long de l'enquête.
Ce rapport doit être rigoureux, complet et dénué de tout parti pris ou interprétation personnelle. Il s'inscrit généralement dans le cadre d'une enquête plus large sur un incident de sécurité, et joue un rôle crucial dans la détermination de sa cause profonde ainsi que dans la formulation de recommandations.
Un autre aspect fondamental de cette phase concerne la participation de l'expert à une procédure judiciaire, qu'elle soit pénale ou civile. Si l'enquête identifie un suspect ou une entité responsable, l'expert peut être amené à témoigner devant un tribunal. Dans ce contexte, il doit présenter les faits et ses conclusions avec la même objectivité que dans son rapport écrit.
Selon la juridiction et le niveau d'expertise reconnu, l'expert peut être limité à une simple présentation factuelle ou, au contraire, autorisé à exprimer des opinions fondées sur son expérience. Les experts qualifiés et reconnus comme témoins experts peuvent ainsi émettre des avis techniques destinés à éclairer le juge ou les jurés.

Le processus d'investigation numérique repose sur six étapes clès qui assurent l'intégrité, la fiabilité et la recevabilité juridique des preuves numériques. En appliquant et respectant méthodiquement les phases d'identification, de préservation, de collecte, d'examen, d'analyse et de présentation, les spécialistes peuvent retracer les événements d'un incident, en comprendre les causes et, si nécessaire, identifier les responsables. Ce cadre structuré est essentiel non seulement pour les enquêtes internes en cybersécurité, mais aussi pour les procédures judiciaires, où chaque intervention doit être rigoureusement justifiée, documentée et défendable.

6 Branches de la criminalistique numérique

La criminalistique numérique est un vaste domaine englobant diverses sous-disciplines, chacune axée sur un aspect spécifique de la collecte et de l'analyse des preuves numériques. Voici les principales branches de la criminalistique numérique :

6.1 Criminalistique réseau

6.1.1 Définition

La criminalistique réseau est une branche essentielle de la criminalistique numérique qui se concentre sur la surveillance et l'analyse du trafic réseau afin de collecter des informations, de recueillir des preuves juridiques ou de détecter des intrusions. Ce processus implique la collecte de données en temps réel ou de journaux stockés à partir de divers périphériques réseau, tels que des routeurs, des pare-feu et des systèmes de détection d'intrusion (IDS).
Contrairement à d'autres domaines de la criminalistique numérique, les investigations réseau traitent des informations volatiles et dynamiques, car le trafic réseau est transmis puis perdu. L'interception du trafic se produit généralement au niveau des paquets, où les données sont soit stockées pour une analyse ultérieure, soit filtrées en temps réel. Les professionnels de la sécurité utilisent régulièrement des outils d'investigation réseau non seulement pour condamner les attaquants, mais aussi pour comprendre comment ils ont accédé au réseau et pour sécuriser les vulnérabilités exploitées. L'investigation réseau contribue aux enquêtes post-incident afin de déterminer comment les infractions ont été commises et d'identifier les responsables.
Deux systèmes sont couramment utilisés pour collecter les données réseau : une méthode de force brute « catch it as you can» et une méthode plus intelligente «stop look listen».

- **"Catch-it-as-you-can" :** Cette approche consiste à capturer tous les paquets transitant par un point de trafic donné et à les enregistrer sur le stockage, puis à les analyser par lots. Cette approche nécessite un espace de stockage important.
- **"Stop, look and listen" :** Cette approche consiste à analyser chaque paquet de manière rudimentaire en mémoire, et seules certaines informations sont enregistrées pour une analyse ultérieure. Cette approche nécessite un processeur plus rapide pour gérer le trafic entrant.

6.1.2 Composants clés de la criminalistique réseau

La criminalistique réseau est une discipline complexe et multidimensionnelle qui repose sur plusieurs éléments essentiels :

- **Capture et analyse de paquets :** Les paquets sont les unités de base du trafic réseau. Les outils d'investigation réseau capturent ces paquets pour analyser les données transmises sur un réseau. Les informations contenues dans les en-têtes de paquets peuvent révéler les adresses source et de destination, les horodatages et les types de protocoles, autant d'éléments essentiels pour enquêter sur les incidents de sécurité.
- **Analyse des fichiers logs :** Les fichiers logs des routeurs, des pare-feu, des systèmes IDS/IPS et des serveurs fournissent des informations précieuses sur les événements réseau. Les logs réseau enregistrent l'activité, comme les tentatives de connexion, les connexions des utilisateurs et les transferts de données. L'analyse de ces fichiers permet de reconstituer les événements avant, pendant et après une attaque.
- **Analyse des flux de trafic :** Plutôt que de se concentrer sur des paquets individuels, l'analyse des flux de trafic examine les schémas globaux du trafic réseau. Ce type d'analyse est utile pour identifier les anomalies, telles que les pics de trafic inhabituels ou les connexions à des adresses IP externes suspectes.

- **Analyse des protocoles :** Différents types de trafic utilisent divers protocoles de communication, tels que HTTP, FTP et DNS. En analysant ces protocoles, les enquêteurs peuvent déterminer le type de données transférées et la manière dont les attaquants ont pu exploiter les vulnérabilités du protocole.
- **Corrélation des données :** L'investigation réseau implique également la corrélation de données provenant de sources multiples pour dresser un tableau complet d'un incident. En combinant les captures de paquets, les journaux et les données de flux, les enquêteurs peuvent reconstituer l'intégralité de la chaîne d'événements ayant conduit à une faille de sécurité.

6.1.3 Sources de preuves dans la criminalistique réseau

Dans toute enquête d'investigation réseau, les preuves sont essentielles pour établir des conclusions. L'investigation réseau repose sur différentes sources de preuves permettant de tracer et de reconstruire les cyberincidents.
Les sources de preuves les plus courantes sont :

1. **Trafic réseau :**
   La preuve la plus directe est le trafic réseau lui-même. En capturant les paquets sur le réseau, les professionnels peuvent voir de manière précise quelles données ont été envoyées et reçues. Les captures de paquets fournissent des informations détaillées sur la communication entre les appareils, permettant aux analystes d'identifier la source du trafic malveillant.
2. **Logs des pare-feu et des routeurs :**
   Les pare-feu et les routeurs agissent comme des gardiens du trafic réseau, ce qui rend leurs fivhiers logs précieux pour une enquête forensique. Ces dispositifs enregistrent des informations sur l'ensemble du trafic qui les traverse, y compris les connexions autorisées et bloquées. Les fichiers logs des pare-feu, en particulier, peuvent révéler les tentatives de violation, les adresses IP des attaquants et les schémas de trafic inhabituels.
3. **Logs du système de détection d'intrusion (IDS) :**
   Les logs IDS contiennent des données sur les activités potentiellement malveillantes détectées sur le réseau. Un IDS peut générer des alertes lorsqu'il identifie des comportements suspects, tels que des tentatives d'exploitation de vulnérabilités ou des accès non autorisés. Ces journaux aident les enquêteurs à déterminer l'heure et la nature d'une attaque, ce qui les rend essentiels pour la surveillance en temps réel et l'analyse post-événement.
4. **Logs des applications :**
   Les applications exécutées sur le réseau, telles que les serveurs web, les bases de données et les systèmes de messagerie, génèrent des logs contenant des informations précieuses pour l'analyse forensique du réseau. Par exemple, les logs de serveur web peuvent révéler les requêtes HTTP adressées au serveur, notamment l'adresse IP source, la méthode de requête et les ressources consultées. Ces logs sont utiles pour enquêter sur les attaques web, telles que les injections SQL ou les scripts intersites (XSS).

La criminalistique réseau joue un rôle clé dans la cybersécurité en permettant aux organisations d'identifier et de répondre aux incidents de sécurité. Grâce à l'analyse du

trafic réseau, des fichiers logs et d'autres sources de données, elle facilite la détection des cyberattaques et des vulnérabilités. Malgré des défis comme le volume de données et le chiffrement, il y a des outils spécialisés qui permettent d'y faire face. La maîtrise des sources de preuves, telles que les captures de paquets et les requêtes DNS, est essentielle pour renforcer la sécurité.

6.2 Criminalistique des appareils mobiles

6.2.1 Définition

L'investigation numérique sur appareils mobiles est une branche de la criminalistique numérique qui vise à récupérer des preuves ou des données numériques à partir d'un appareil mobile dans des conditions rigoureuses. L'expression «appareil mobile» désigne généralement les téléphones portables ; cependant, elle peut également désigner tout appareil numérique doté d'une mémoire interne et de capacités de communication, notamment les assistants numériques personnels (PDA), les GPS et les tablettes. En suivant une méthodologie stricte, les experts peuvent extraire les informations sans les altérer, garantissant ainsi leur recevabilité devant les tribunaux ou d'autres instances juridiques.
Contrairement à l'analyse forensique traditionnelle des ordinateurs, l'analyse des appareils mobiles doit prendre en compte la diversité des dispositifs, leurs systèmes de communication intégrés (par exemple GSM) et leurs mécanismes de stockage propriétaires. La conception des téléphones évolue constamment avec les avancées technologiques, ce qui impose une adaptation continue des méthodes d'investigation.
Le besoin d'investigation des appareils mobiles est devenu croissant pour plusieurs raisons, parmi lesquelles :

- **Utilisation massive des téléphones portables :** Les appareils mobiles sont utilisés largement par les utilisateurs, pour stocker des informations personnelles (photos, messages, contacts) et professionnelles (e-mails, documents d'entreprise, accès aux systèmes internes).
- **Multiplication des transactions en ligne :** De nombreux achats, paiements, transferts bancaires et échanges commerciaux passent désormais par des applications mobiles, rendant les téléphones des sources précieuses de preuves en cas de fraude ou de vol.
- **Géolocalisation et traçabilité :** Les appareils mobiles enregistrent en permanence des données de localisation. Cela permet aux enquêteurs de situer un suspect ou une victime à un endroit précis à un moment donné, renforçant les éléments de preuve.
- **Internet des Objets (IoT) :** Les téléphones mobiles servent souvent de hubs pour d'autres appareils connectés (montres intelligentes, caméras, voitures connectées), créant ainsi un écosystème élargi de preuves numériques.

6.2.2 Les preuves numériques issues des appareils mobiles

Les appareils mobiles modernes, notamment les téléphones, fournissent une diversité d'informations utiles. Ces données deviennent de plus en plus imprévisibles, et une analyse forensique en temps réel est donc toujours nécessaire avant de pouvoir utiliser des approches forensiques automatisées de manière isolée. Selon l'état de fonctionnement de

l'appareil, des données techniques supplémentaires peuvent être obtenues via le réseau. Voici quelques exemples de données qu'on peut trouver sur les appareils mobiles :

Types de preuves mobile
Historique des appels émis, reçus et manqués
Répertoire téléphonique ou listes de contacts
Contenu des SMS, MMS et messages via applications
Photos, audios, vidéos, fichiers et parfois messages vocaux
Historique de navigation Internet, cookies, contenus, informations analytiques, historique des recherches
Entrées du calendrier, listes de tâches, sonneries, notes, mémos
Documents, fichiers de présentation, feuilles de calcul et autres données créées par l'utilisateur
Mots de passe, codes de verrouillage, identifiants de comptes utilisateurs
Données de géolocalisation historiques, informations de connexion Wi-Fi, données de localisation via antennes relais
Données issues des différentes applications installées
Données supprimées correspondant à tous les types mentionnés
Fichiers système, messages d'erreur, journaux d'utilisation.

TABLE 1 – Types de preuves extraites des appareils mobiles

6.2.3 Types d'acquisition de données

L'extraction de données consiste à récupérer des données depuis un smartphone ou tout autre appareil. Différentes techniques sont donc utilisées pour extraire les données des appareils mobiles, chacune adaptée à des situations particulières :

1. **Acquisition manuelle :**
   L'acquisition manuelle consiste à examiner un appareil mobile via son interface utilisateur, en explorant normalement et en prenant des photos de l'écran. L'avantage de cette approche est ce qu'elle ne nécessite pas d'outils spécialisés. Ses inconvénients sont que seules les données visibles par le système d'exploitation peuvent être récupérées et elle prend du temps.
2. **Acquisition logique :**
   L'acquisition logique consiste à copier bit par bit des objets de stockage logique présents sur l'appareil. Elle présente l'avantage de simplifier l'extraction et l'organisation des structures de données système. L'extraction logique acquiert les informations de l'appareil via l'interface de programmation d'application du fabricant d'origine pour synchroniser le contenu du téléphone avec un ordinateur personnel.
3. **Acquisition du système de fichiers :**
   L'acquisition du système de fichiers consiste à extraire les données accessibles via l'interface de synchronisation d'un appareil. Bien que l'extraction logique ne supprime pas d'informations, certaines plateformes comme iOS et Android marquent simplement les données supprimées comme disponibles pour un écrasement ultérieur. Cela permet parfois de récupérer ces informations. Cette méthode est utile pour analyser la structure des fichiers, l'historique de navigation et l'utilisation des applications à l'aide d'outils informatiques légaux traditionnels.

4. **Acquisition physique :**
   L'acquisition physique implique une copie bit à bit de l'intégralité d'une mémoire physique ; c'est donc la méthode la plus proche de l'examen d'un ordinateur personnel. Elle présente l'avantage de permettre l'examen des fichiers supprimés et des données restantes. L'extraction physique acquiert les informations de l'appareil par accès direct aux mémoires flash.

   Cette opération est généralement plus difficile à réaliser, car le fabricant d'origine de l'appareil doit le protéger contre toute lecture arbitraire de la mémoire.
5. **Acquisition par force brute :**
   L'acquisition par force brute utilise des essais et des erreurs pour créer la bonne combinaison de mot de passe ou de code PIN afin d'authentifier l'accès à l'appareil mobile. Malgré son temps considérable, elle reste l'une des meilleures méthodes à utiliser si le professionnel de la criminalistique ne parvient pas à obtenir le code d'accès. Avec les logiciels et le matériel actuels, il est devenu assez facile de casser le chiffrement du fichier de mots de passe d'un appareil mobile pour obtenir le code d'accès.

6.3 Criminalistique des supports de stockage

6.3.1 Définition

La criminalistique des supports de stockage(Disk Forensics) est une branche de la criminalistique numérique qui a pour objectif l'examination des supports de stockage tels que les disques durs, clés USB, CD, DVD et autres périphériques. Elle permet d'extraire des données, notamment les fichiers supprimés, les espaces non alloués et les métadonnées, afin de retrouver des informations cruciales. Ce processus aide à identifier des traces numériques laissées après des opérations de suppression ou de formatage et peut être essentiel dans les enquêtes judiciaires ou la récupération de données perdues.
L'objectif principal de l'analyse forensique des supports de stockage est d'identifier et de collecter des preuves liées à des crimes ou incidents informatiques. Elle implique l'examen systématique des supports de stockage numériques afin de récupérer, d'analyser et d'interpréter des données susceptibles d'être pertinentes pour une enquête judiciaire ou interne à une organisation. Cette approche contribue à la compréhension des incidents numériques et à la mise en lumière d'éléments clés pour la résolution des affaires.

6.3.2 Utilisation de la criminalistique des supports de stockage

La criminalistique des supports de stockage est principalement utilisée dans les situations suivantes :

- **Inaccessibilité de l'état actif du système :** Lorsque le système n'est plus en fonctionnement, par exemple après une coupure de courant, un sabotage, ou une cyberattaque, il devient nécessaire d'analyser directement les supports physiques pour retrouver les données.
- **Investigation d'activités passées :** Cette approche permet de retracer des activités anciennes, comme la récupération de fichiers supprimés, la reconstruction de l'historique de navigation Internet, ou l'analyse de journaux d'événements effacés.

- **Enquêtes judiciaires (Law Enforcement) :** Dans les procédures pénales, l'analyse des disques est utilisée pour recueillir des preuves numériques tout en respectant la chaîne de conservation des preuves (chain of custody), afin d'assurer leur validité devant un tribunal.

Grâce à l'analyse minutieuse des supports, les enquêteurs peuvent ainsi reconstituer des faits, détecter des comportements suspects et attribuer des actions à des utilisateurs spécifiques. Différentes méthodes et outils spécialisés sont employés pour mener à bien ces investigations.

6.3.3 Données récupérables

L'analyse forensique des supports de stockage permet de récupérer différentes catégories de données, souvent ignorées par les utilisateurs ou considérées comme définitivement supprimées. Même s'elles sont invisibles à l'utilisateur final, ces informations peuvent représenter des preuves cruciales et importantes dans les investigations numériques. On distingue principalement :

- **Les fichiers supprimés :** Ils ne sont pas instantanément effacés du support de stockage. Lorsqu'un fichier est supprimé sur un système de fichiers, seule son entrée dans la table d'allocation est mise à jour pour indiquer que l'espace est disponible. Tant que cet espace n'est pas réécrit par de nouvelles données, il reste possible de récupérer les fichiers à l'aide d'outils spécialisés, permettant ainsi de restaurer des documents effacés volontairement ou perdus accidentellement.
- **Les espaces non alloués (unallocated space) :** Il s'agit des zones du disque dur qui ne sont pas associées à aucun fichier actif. Ces zones peuvent contenir des fragments de fichiers anciens, y compris ceux issus d'une précédente installation du système, de fichiers temporairement créés par des applications, ou de documents partiellement supprimés. L'analyse de ces espaces permet de découvrir des éléments autrement inaccessibles à travers l'explorateur de fichiers classique.
- **Les métadonnées :** Elles sont associées à chaque fichier ou dossier. Celles-ci contiennent des informations essentielles telles que : la date de création, de modification et d'accès, les autorisations d'utilisation, ainsi que l'identité de l'utilisateur ou du système ayant effectué ces actions. Elles jouent un rôle clé dans l'analyse des comportements numériques en permettant de détecter des activités inhabituelles, comme la création de fichiers à des heures inhabituelles ou l'utilisation de comptes non autorisés, tout en facilitant la reconstitution d'une chronologie des événements.
- **Les journaux du système de fichiers et fichiers temporaires :** Certains systèmes de fichiers maintiennent des journaux internes (logs) pour assurer l'intégrité des opérations. Ces journaux peuvent contenir des informations précieuses sur les activités du système, comme la copie, le déplacement ou la suppression de fichiers. De plus, de nombreux programmes créent des fichiers temporaires ou des caches, qui peuvent rester stockés même après la fermeture ou la suppression de l'application. Ces artefacts sont souvent riches en informations, notamment dans les cas d'utilisation d'applications web, de traitements de texte ou de logiciels de messagerie.

6.3.4 Types de supports analysés

L'analyse forensique des supports de stockage s'applique à divers dispositifs numériques, chacun ayant ses particularités techniques et ses propres défis. Les types de supports les plus couramment examinés incluent :

- **Disques durs (HDD) et disques SSD :** Ces supports de stockage internes ou externes contiennent généralement une grande quantité de données, y compris des fichiers d'utilisateur, des systèmes d'exploitation, et des journaux système. Les SSD, en particulier, posent des défis supplémentaires en raison de leurs mécanismes de gestion de la mémoire.
- **Clés USB et disques durs externes :** Très utilisés pour le transfert de données, ils peuvent contenir des fichiers personnels, professionnels ou malveillants. Leur portabilité les rend souvent associés à des cas d'exfiltration de données.
- **Cartes mémoire (SD, microSD) :** Utilisées principalement dans les smartphones, appareils photo ou drones, elles peuvent contenir des images, vidéos, documents et autres données sensibles.
- **CD/DVD :** Bien que moins courants aujourd'hui, ces supports sont encore rencontrés dans les enquêtes portant sur de vieux équipements. Ils offrent une bonne stabilité des données mais sont en lecture seule.
- **Disques virtuels :** Utilisés dans des environnements virtualisés, ces disques peuvent contenir des systèmes complets. Leur analyse nécessite des outils spécialisés pour accéder à leur contenu de manière forensique.
- **Autres supports amovibles :** Cela inclut les lecteurs MP3, les anciens lecteurs ZIP, ou tout autre périphérique pouvant contenir de la mémoire flash ou magnétique exploitable.

Chaque type de support requiert des techniques et des outils d'acquisition adaptés, tout en respectant les principes de préservation de l'intégrité des preuves numériques.

6.4 Criminalistique du Cloud

6.4.1 Définition

L'informatique « en nuage » (cloud, en anglais) est une déclinaison récente des systèmes distribués. Il s'agit de l'exploitation de serveurs distants par l'intermédiaire d'un réseau, Internet. Ces serveurs sont loués à la demande à des fournisseurs externes selon l'utilisation (pay per use) ou forfaitairement.
La criminalistique du cloud est une branche de l'investigation numérique qui s'intéresse à l'identification, la collecte, la préservation, l'analyse et la présentation des preuves numériques provenant d'environnements cloud comme : Amazon Web Services, Microsoft Azure, Google Cloud, etc. L'investigation forensique dans le cloud désigne les enquêtes axées sur les crimes impliquant principalement le cloud. Il peut s'agir de violations de données ou d'usurpations d'identité. Grâce à l'investigation forensique dans le cloud, le propriétaire bénéficie d'une protection et peut mieux préserver les preuves. Sans stratégie d'investigation forensique dans le cloud, le propriétaire risque de ne pas avoir accès à toutes les données ou preuves présentes dans le cloud, surtout si elles sont hébergées hors site ou par un tiers.

L'informatique en nuage (cloud computing) est une déclinaison récente des systèmes distribués. Elle s'agit de l'exploitation des serveurs distants via l'intermédiaire d'un réseau Internet, loués à la demande auprès de fournisseurs externes (comme Amazon Web Services, Microsoft Azure ou Google Cloud), soit en mode pay-per-use (paiement à l'usage), soit selon un forfait.
La criminalistique du cloud est une branche de l'investigation numérique qui vise l'identification, la collecte, la préservation, l'analyse et la présentation de preuves numériques issues d'environnements cloud.
Elle est utilisée lors d'enquêtes portant sur :

- des violations de données,
- des vols d'identité,
- ou d'autres actes criminels où les ressources cloud sont impliquées.

Grâce à l'investigation forensique du cloud, les propriétaires de données peuvent bénéficier d'une protection renforcée et d'une meilleure préservation des preuves. En l'absence de stratégie adaptée, il devient difficile, voire impossible, d'accéder à l'ensemble des données critiques, surtout lorsque : les données sont hébergées hors site ou lorsqu'elles sont gérées par des tiers situés dans d'autres juridictions.

6.4.2 Localisation des preuves numériques selon le type du service cloud :

- **SaaS (Software-as-a-Service) :** est une forme de cloud computing qui permet de fournir une application cloud, avec ses plateformes et son infrastructure sous-jacentes, aux utilisateurs finaux via un navigateur Internet. Cette solution est particulièrement adaptée aux grandes entreprises, aux petites structures ou aux particuliers qui :
  - ne souhaitent pas acheter ou entretenir une infrastructure, des plateformes et des logiciels sur site ;
  - préfèrent une gestion plus simple des coûts par les coûts d'exploitation, plutôt que par les dépenses d'investissement ;
- **PaaS (Platform as a service)** s'agit d'un modèle de cloud computing dans lequel un système d'exploitation (SE) est installé sur un serveur cloud. Les utilisateurs peuvent ensuite installer leurs propres applications, paramètres et outils dans l'environnement cloud. Le fournisseur de cloud gère uniquement le matériel pour les clients, qui sont responsables de l'administration système et du support applicatif. Il est principalement destiné aux développeurs ou aux entreprises de développement, où :
  - l'entité cliente maintient les applications proprement dites ;
  - le fournisseur cloud maintient la plate-forme d'exécution de ces applications : le matériel du ou des serveurs, les logiciels de base et l'infrastructure.
- **IaaS (Infrastructure as a service)**IaaS — est un modèle de cloud computing dans lequel les clients peuvent louer du matériel, tel que des serveurs et des postes de travail, et installer les systèmes d'exploitation et les applications dont ils ont besoin. L'IaaS peut s'avérer utile lorsque les clients n'ont pas les moyens d'acheter du matériel ou de payer un prestataire pour sa maintenance, mais peuvent se permettre de le louer. De plus, ce niveau de service facilite l'ajout de matériel pendant les

périodes de pointe, comme la période des impôts ou les périodes comptables de fin d'année, puis la réduction des besoins en matériel lorsqu'il n'est pas nécessaire pendant les périodes creuses. Il est destiné aux entreprises où :

— l'entreprise gère le Middleware des serveurs, et surtout les logiciels applicatifs (exécutables, paramétrages, l'intégration SOA, les bases de données) ;

— le fournisseur cloud gère le matériel serveur, les couches de virtualisation, le stockage, les réseaux.

Niveau de service	**Localisation des preuves numériques**
SaaS (Software as a Service)	Les données et les logiciels sont stockés sur l'infrastructure du fournisseur de service. Les preuves sont principalement accessibles via un navigateur sur un ordinateur de bureau, un ordinateur portable, une tablette ou un smartphone. Exemples de SaaS : Google Drive, Microsoft 365, Dropbox. Les journaux d'accès et les historiques de modification peuvent être récupérés.
PaaS (Platform as a Service)	Les données peuvent être localisées sur un ordinateur de bureau ou un serveur. Elles peuvent aussi être stockées sur le réseau interne d'une entreprise ou sur l'infrastructure du fournisseur externe. Exemples de PaaS : Google App Engine, Microsoft Azure App Services. Les preuves comprennent les configurations d'applications, les logs d'exécution, et les bases de données hébergées.
IaaS (Infrastructure as a Service)	Les preuves se trouvent habituellement sur des serveurs ou ordinateurs de bureau. L'infrastructure physique (machines virtuelles, stockage, réseaux) peut appartenir soit à l'entreprise, soit au fournisseur cloud. Exemples d'IaaS : Amazon EC2, Microsoft Azure Virtual Machines. Les données clés sont : instantanés (snapshots), volumes de disques virtuels, et journaux réseau.

TABLE 2 – Localisation des preuves numériques selon le modèle de service cloud

6.4.3 Les avantages et les défis du criminalistique du cloud

Parmi les avantages de l'investigation forensique dans le cloud, on trouve :

- **Efficacité des investigations :** L'investigation forensique dans le cloud permet aux enquêteurs de recueillir efficacement des preuves auprès de différents fournisseurs de services cloud (FSC) sans accéder physiquement au matériel ou à l'infrastructure. Cela accélère les investigations et réduit les temps d'arrêt associés aux méthodes d'investigation forensique traditionnelles.
- **Accessibilité mondiale :** L'investigation forensique dans le cloud permet aux enquêteurs d'accéder aux données stockées dans le cloud depuis n'importe quel endroit disposant d'une connexion Internet. Cette accessibilité mondiale facilite la collaboration entre les équipes d'investigation forensique réparties géographiquement, améliorant ainsi l'efficacité des investigations.

- **Évolutivité :** Les environnements cloud offrent une évolutivité permettant aux enquêteurs forensiques de traiter efficacement d'importants volumes de données. Grâce à l'allocation dynamique des ressources par les services cloud en fonction de la demande, les enquêteurs peuvent adapter leurs outils et processus d'investigation forensique à la gestion de volumes de données croissants sans investissement initial important.
- **Préservation des preuves :** L'investigation forensique dans le cloud garantit la préservation des preuves numériques de manière rigoureuse. En suivant les protocoles et procédures établis, les enquêteurs peuvent garantir l'intégrité et la recevabilité des preuves, essentielles aux procédures judiciaires.
- **Conformité réglementaire :** De nombreuses organisations sont tenues de se conformer aux réglementations et normes sectorielles régissant la sécurité et la confidentialité des données. L'investigation numérique dans le cloud aide les organisations à démontrer leur conformité en fournissant des preuves des incidents de sécurité, des failles de données et des mesures prises pour atténuer les risques.

Cependant, cette approche n'est pas sans défis :

- **Sécurité et confidentialité des données :** Un des principaux défis du cloud computing réside dans la protection des données sensibles. Les utilisateurs du cloud confient leurs données aux fournisseurs tiers, qui peuvent ne pas disposer des mesures adéquates pour les protéger contre les accès non autorisés, les violations ou les fuites. Les utilisateurs du cloud sont également confrontés à des risques de conformité.
- **Visibilité et contrôle réduits :** Les utilisateurs du cloud peuvent ne pas avoir une vision complète de la gestion, de la configuration ou de l'optimisation de leurs ressources cloud par leurs fournisseurs. Ils peuvent également avoir une capacité limitée à personnaliser ou à modifier leurs services cloud en fonction de leurs besoins ou préférences spécifiques.
- **Complexité technique :** Une compréhension complète de toutes les technologies peut s'avérer impossible, notamment compte tenu de l'échelle, de la complexité et de l'opacité délibérée des systèmes contemporains ; cependant, cette compréhension est nécessaire pour pouvoir exercer une influence sur ces systèmes et garantir leur sécurité.
- **Migration vers le cloud :** De plus, la migration vers le cloud représente un défi majeur. Ce processus implique le transfert de données, d'applications ou de charges de travail d'un environnement cloud à un autre, ou d'une infrastructure sur site vers le cloud. La migration vers le cloud peut s'avérer complexe, longue et coûteuse, notamment en cas de problèmes de compatibilité entre différentes plateformes ou architectures cloud. Mal planifiée et exécutée, elle peut entraîner des temps d'arrêt, une baisse des performances, voire des pertes de données.

7 Outils et techniques utilisés dans la criminalistique numérique

7.1 Outils utilisés dans la criminalistique numérique

Les outils d'investigation numérique sont des outils matériels et logiciels permettant de récupérer et de préserver des preuves numériques. Les forces de l'ordre peuvent les utiliser pour collecter et préserver des preuves numériques et étayer ou réfuter des hypothèses devant les tribunaux. Cependant, les outils d'investigation sont constamment développés, mis à jour, corrigés, révisés et abandonnés. Il est donc important de consulter régulièrement les sites web des fournisseurs pour découvrir les nouvelles fonctionnalités et améliorations. Ces améliorations pourraient résoudre un problème complexe que vous rencontrez lors d'une enquête.
Avant d'acheter un outil d'investigation, déterminez s'il peut vous faire gagner du temps lors des enquêtes et si ce gain de temps affecte la fiabilité des données récupérées. De nombreux outils avancés basés sur une interface utilisateur graphique peuvent être exigeants, nécessitant souvent des machines dotées de RAM et de processeurs importants. Les enquêteurs doivent également se méfier des surcharges système causées par des processus d'arrière-plan, tels que les antivirus, qui peuvent interférer avec les applications d'investigation.
De plus, lors de la recherche et de l'évaluation de matériels et de logiciels d'investigation numérique, il est recommandé de privilégier les outils open source, qui offrent parfois un support technique communautaire ou professionnel. L'objectif est d'obtenir le meilleur rapport qualité-prix tout en bénéficiant d'un maximum de fonctionnalités. Différents aspects et critères doivent être pris en compte lors de l'évaluation et du choix des outils :

- Sur quel système d'exploitation l'outil d'investigation fonctionne-t-il ?
- Est-il polyvalent ? Par exemple, fonctionne-t-il sous Windows, Linux et macOS ?
- Peut-il analyser plusieurs systèmes de fichiers, tels que FAT, NTFS et Ext4 ?
- Un langage de script peut-il être utilisé pour automatiser les fonctions et tâches répétitives ?
- Est-il intuitif et bien documenté, ou nécessite-t-il une formation spécialisée de la part du fournisseur ?

Ces critères permettent de sélectionner des outils qui répondent non seulement aux besoins des investigations, mais aussi aux normes de fiabilité, de répétabilité et de défense juridique de l'investigation.

7.1.1 Wireshark

Wireshark est un outil puissant d'analyse du trafic réseau, couramment utilisé dans les enquêtes numériques. En installant Wireshark sur un disque dur portable, les enquêteurs peuvent effectuer une analyse forensique en temps réel, ce qui facilite la réponse aux incidents et la concentration sur les tâches importantes.
Cet outil permet aux enquêteurs de comprendre rapidement la situation actuelle, de stopper l'attaque et de collecter des preuves et des informations pour éviter de tels incidents. Wireshark est un analyseur de trafic et de protocole réseau gratuit et open source qui

permet aux utilisateurs de capturer et de dépanner le trafic réseau.
Wireshark est un outil riche en fonctionnalités, parmi eux on trouve :

- **Affichage de l'heure des paquets :** Cette fonctionnalité permet de choisir le format d'affichage de l'heure pour chaque paquet capturé. L'analyste peut opter pour l'heure depuis le 1er janvier 1970, depuis le début de la capture, ou encore afficher la date et l'heure du jour. Cette dernière option est particulièrement utile pour corréler les événements réseau avec les journaux système ou d'autres sources de preuve. Wireshark permet également d'utiliser l'heure UTC, ce qui est pertinent dans des environnements où l'heure locale diffère ou dans les grandes infrastructures multi-fuseaux horaires.
- **Résolution de noms :** Wireshark peut résoudre les adresses IP en noms d'hôtes grâce à la résolution DNS. Cela permet à l'analyste de mieux comprendre la destination du trafic en affichant par exemple google.com plutôt qu'une simple adresse IP. Cette fonction est utile pour identifier rapidement les connexions vers des domaines suspects ou inconnus, surtout dans les cas d'attaques utilisant des C2 (Command and Control).
- **Coloration des paquets :** Pour faciliter la lecture visuelle, Wireshark applique automatiquement une coloration des lignes de la capture en fonction des types de paquets (ex : vert pour TCP, bleu pour DNS, noir pour les erreurs). Cela permet à l'analyste de repérer d'un coup d'œil les anomalies, erreurs ou types de trafic spécifiques, sans devoir lire chaque ligne en détail.
- **Filtres d'affichage :** L'une des fonctionnalités les plus puissantes de Wireshark est la possibilité de filtrer les paquets affichés selon des critères très précis (adresses IP, ports, protocoles, contenu, etc.). Par exemple, l'analyste peut afficher uniquement le trafic HTTP ou les paquets provenant d'une adresse IP donnée. Ces filtres permettent d'isoler rapidement les éléments pertinents d'une capture volumineuse, accélérant l'analyse.
- **Identification de l'hôte local :** Lors de l'analyse d'une capture, notamment dans des environnements individuels, Wireshark permet d'identifier facilement l'hôte concerné (nom, adresse IP, adresse MAC). Cela est souvent visible dès les premiers paquets DHCP ou ARP de la capture. Cette identification est utile pour distinguer l'activité du système analysé de celle des autres machines présentes sur le réseau.

On utilise WiresHark pour :

- **La détection d'un accès non autorisé :** En effectuant une analyse des adresses IP sources et les ports utilisés, l'analyste peut repérer des connexions suspectes ou non autorisées. Wireshark facilite l'identification des tentatives d'intrusion en mettant en évidence des comportements inhabituels, comme des connexions répétées depuis des adresses inconnues.
- **L'exfiltration de données sensibles :** Lorsqu'une fuite de données est suspectée, Wireshark permet d'analyser le trafic sortant afin d'identifier si des fichiers ont été transmis vers l'extérieur du réseau. Grâce aux filtres d'affichage, il est possible de cibler uniquement les transferts via des protocoles comme FTP, HTTP ou SMTP.
- **Analyse d'une attaque par déni de service (DoS) :** En cas de ralentissement ou d'indisponibilité de services, Wireshark aide à détecter un afflux anormal de paquets (souvent ICMP, UDP ou SYN flood). Les statistiques et les visualisations de débit dans Wireshark permettent de quantifier et qualifier l'attaque.

En résumé, Wireshark est un outil puissant utilisé principalement lorsque le trafic réseau est capturé en temps réel ou lorsqu'on dispose de fichiers de capture réseau préalablement enregistrés (au format .pcap ou .pcapng). Ces fichiers peuvent provenir de systèmes de surveillance réseau tels qu'un IDS (par exemple Snort ou Suricata), d'un pare-feu ou routeur configuré pour enregistrer le trafic, ou encore d'un port miroir sur un commutateur. En l'absence de capture active ou de fichiers existants, Wireshark devient inutile car il ne permet pas d'analyser des données passées non enregistrées. Dans ce cas, l'enquêteur se tourne vers d'autres sources de preuves comme les journaux système, les caches DNS ou navigateur, les fichiers de mémoire vive ou encore les artefacts stockés sur disque. Ainsi, l'utilisation de Wireshark dépend directement de l'existence de données réseau disponibles à analyser.

7.1.2 FTK Imager

FTK Imager est un outil d'imagerie et d'analyse forensique conçu pour acquérir, créer des images forensiques et effectuer une analyse détaillée de divers types de supports numériques. Il offre aux enquêteurs une interface conviviale, des fonctionnalités étendues et une compatibilité avec différents systèmes d'exploitation, ce qui en fait un outil essentiel pour les professionnels du domaine.

- **Acquisition de données**
  L'une des principales fonctions de FTK Imager est d'acquérir des données à partir de différents types d'appareils et de supports, tels que les disques durs, les cartes mémoire, les clés USB, les disques optiques et les téléphones portables. FTK Imager peut créer des images forensiques des données, copies exactes des données originales, utilisables à des fins d'analyse et de vérification. FTK Imager prend en charge différents formats d'image, tels que E01, DD, SMART et AFF. Vous pouvez également créer des images logiques, qui sont des sous-ensembles de données basés sur certains critères, tels que le type de fichier, la date ou les mots-clés.
- **Prévisualisation des données**
  Une autre fonctionnalité utile de FTK Imager est la prévisualisation des données avant leur acquisition. Cela vous permet de gagner du temps et de l'argent en sélectionnant uniquement les données pertinentes pour votre investigation. FTK Imager peut afficher le contenu des fichiers et des dossiers, ainsi que les métadonnées telles que les noms, les tailles, les dates et les hachages des fichiers. Vous pouvez également visualiser la structure du système de fichiers, les partitions et l'espace non alloué d'un périphérique. FTK Imager peut également prévisualiser les données des fichiers chiffrés ou compressés, ainsi que celles des systèmes actifs ou des vidages mémoire.
- **Analyse des données**
  FTK Imager peut également vous aider à analyser les données après leur acquisition. Vous pouvez utiliser FTK Imager pour monter des images forensiques sur des disques en lecture seule, ce qui vous permet d'accéder aux données et de les examiner sans les modifier. Vous pouvez également utiliser FTK Imager pour exporter des données d'images forensiques vers d'autres formats, tels que CSV, HTML ou XML. FTK Imager peut également effectuer des recherches et des filtres de base sur les données, par exemple par nom de fichier, extension, hachage ou mot-clé. FTK Imager peut également générer des rapports et des journaux sur le processus d'acquisition et d'analyse des données, utiles à des fins de documentation et de vérification.

- **Récupération de données**
  FTK Imager peut également vous aider à récupérer des données cachées, supprimées ou corrompues. Il peut identifier et récupérer des données provenant de divers systèmes de fichiers, tels que FAT, NTFS, HFS, EXT et UFS. Il peut également récupérer des données provenant de l'espace non alloué, de l'espace libre et des secteurs défectueux d'un appareil. Il peut également récupérer des données à partir de fichiers chiffrés ou compressés, ainsi que de matrices RAID ou de machines virtuelles.
- **Comparaison de données**
  FTK Imager peut également vous aider à comparer des données provenant de différentes sources ou images, ce qui peut s'avérer utile pour identifier des similitudes ou des différences. FTK Imager compare les données à l'aide de hachages, qui sont des identifiants uniques des données. FTK Imager peut générer et vérifier les hachages de fichiers, dossiers, partitions ou images à l'aide de divers algorithmes, tels que MD5, SHA1, SHA256 ou SHA512. Vous pouvez également utiliser FTK Imager pour comparer les hachages de données provenant de différentes sources ou images et identifier les correspondances ou les incohérences.
- **Intégration des données**
  FTK Imager peut également vous aider à intégrer des données provenant de différentes sources ou images, ce qui peut s'avérer utile pour créer une vue complète et cohérente des données. FTK Imager peut importer et exporter des données provenant d'autres outils d'investigation, tels qu'EnCase, X-Ways, Cellebrite ou Magnet. Vous pouvez également utiliser FTK Imager pour ajouter des données provenant de différentes sources ou images à un seul dossier, qui peut être ouvert et analysé par FTK, le logiciel d'investigation phare d'AccessData. FTK Imager permet également de créer des dossiers portables, des fichiers autonomes et exécutables, partageables et consultables par d'autres utilisateurs sans installer FTK Imager.

En résumé, FTK Imager est un outil essentiel pour les enquêteurs en criminalistique numérique. Ses capacités d'imagerie robustes, ses fonctions d'analyse complètes et sa simplicité d'utilisation en font une solution incontournable pour l'acquisition, l'examen et la validation de preuves numériques. Qu'il s'agisse d'acquérir des images, d'analyser des fichiers, d'extraire des métadonnées ou d'analyser des données de mémoire volatile, FTK Imager fournit aux enquêteurs les outils nécessaires pour découvrir des preuves essentielles et soutenir le processus d'enquête.

7.1.3 Autopsy

Autopsy est un outil d'investigation numérique open source et multiplateforme offrant un large éventail de fonctionnalités pour aider les enquêteurs à récupérer et analyser des preuves numériques. Initialement développé par Brian Carrier, il a depuis été largement adopté par la communauté de l'investigation numérique grâce à sa polyvalence, sa fiabilité et son rapport coût-efficacité. Autopsy est disponible pour Windows, macOS et Linux, ce qui le rend accessible à un large éventail d'utilisateurs.
Voici quelques fonctionnalités essentielles qui font d'Autopsy une bien meilleure plateforme pour effectuer des processus d'investigation numérique :

- **Interface conviviale :** L'interface d'Autopsy est intuitive et facilite l'installation. Elle guide les utilisateurs à chaque étape de leur première utilisation. L'accès et

l'utilisation de l'outil sont faciles, que ce soit pour leur travail professionnel ou personnel.

- **Résultats rapides :** Autopsy permet aux utilisateurs d'obtenir leurs résultats plus rapidement. Elle prend en charge l'utilisation parallèle de plusieurs activités et s'exécute en arrière-plan. L'optimisation complète du disque peut prendre quelques heures, ce qui vous permet de vaquer à vos autres activités pendant ce temps.
- **Analyse des systèmes de fichiers :** Autopsy prend en charge l'analyse de divers systèmes de fichiers, notamment NTFS, FAT, exFAT, HFS+, Ext2/3/4 et UFS. Cette polyvalence permet aux enquêteurs d'examiner des preuves provenant d'une large gamme de supports de stockage, tels que les disques durs, les clés USB, les stockages embarqués de drones et les cartes mémoire. Lors de l'ingestion des données, nous pouvons sélectionner les modules d'ingestion à utiliser, ou les sélectionner tous.
- **Recherche par mots-clés :** Autopsy recherche automatiquement des mots-clés en fonction des modules d'ingestion et permet aux enquêteurs de rechercher des mots-clés ou des schémas spécifiques dans les fichiers et l'espace libre. Cette fonctionnalité est précieuse pour localiser des preuves cruciales dissimulées dans une grande quantité de données. Il suffit de sélectionner la fenêtre principale et de saisir le mot-clé recherché.
- **Analyse chronologique :** Autopsy offre une vue chronologique qui aide les enquêteurs à reconstituer les événements et les activités en analysant les horodatages des fichiers, notamment les heures de création, de modification et d'accès. Cette fonctionnalité est particulièrement utile pour le traitement des artefacts vidéo ; ces éléments peuvent être essentiels pour établir la séquence des événements d'une affaire.
- **Analyse des registres :** L'outil prend en charge l'examen des registres Windows, permettant aux enquêteurs de découvrir des informations importantes sur les activités d'un suspect, les logiciels installés et les configurations système. L'efficacité de l'analyse du registre est extrêmement utile pour traquer les logiciels malveillants.
- **Analyse des artefacts Web :** Autopsy peut analyser les artefacts des navigateurs Web, tels que l'historique de navigation, les cookies et les téléchargements. Ceci est essentiel pour suivre les activités en ligne et identifier les traces numériques potentielles laissées par les acteurs malveillants. Autopsy peut révéler ces traces avec une grande précision et une intelligence organisationnelle.
- **Analyse des e-mails :** Autopsy prend en charge l'analyse des e-mails et des pièces jointes, permettant ainsi de retracer les schémas de communication et de recueillir des preuves à partir des comptes de messagerie. Même si le destinataire a supprimé des e-mails ou les comptes qui y étaient associés, Autopsy peut toujours les détecter, ainsi que les messages.
- **File Craving :**

  Autopsy intègre des fonctionnalités d'extraction de fichiers, lui permettant de récupérer des fichiers supprimés ou endommagés, même lorsque les métadonnées du système de fichiers sont manquantes ou corrompues. C'est sans doute l'une des fonctionnalités les plus intéressantes, car les personnes malveillantes suppriment souvent des données en pensant que cela masquera leurs activités.

- **Rapports et Exportation :** Autopsy génère des rapports détaillés utilisables dans des procédures judiciaires. Ces rapports offrent un aperçu clair des conclusions, facilitant ainsi la présentation des preuves par les enquêteurs ou les équipes juridiques chargées de présenter les conclusions.

Dans le monde de la criminalistique numérique, Autopsy s'impose comme une boîte à outils précieuse permettant aux enquêteurs d'extraire, d'analyser et d'interpréter efficacement les preuves numériques. Sa diversité de fonctionnalités, sa compatibilité avec diverses plateformes et son caractère open source en font une ressource fiable et accessible pour les professionnels de la criminalistique numérique du monde entier.

7.1.4 Volatility

Volatility est un framework open source d'analyse forensique avancée de la mémoire. Son principal outil est le script Python Volatility, qui utilise de nombreux plugins pour analyser les images mémoire. Volatility peut donc être exécuté sur tout système d'exploitation prenant en charge Python. De plus, Volatility peut être utilisé sur les fichiers images mémoire de la plupart des systèmes d'exploitation courants, notamment Windows (de Windows XP à Windows Server 2016), macOS et les distributions Linux courantes. Plusieurs plugins sont disponibles pour Volatility, et d'autres sont en cours de développement. Pour examiner la mémoire système, plusieurs plugins seront examinés afin de garantir que l'analyste dispose de suffisamment d'informations pour mener une analyse appropriée. Il est toutefois recommandé, avant d'utiliser Volatility, de s'assurer que le logiciel est à jour et d'explorer les nouveaux plugins afin de déterminer leur applicabilité à l'enquête sur l'incident en cours.
Parmi les fonctionnalités de ce framework ; on trouve :

- **Analyse de la mémoire :** Volatility est spécialisé dans l'analyse de la mémoire volatile (RAM) des systèmes, permettant aux enquêteurs d'extraire des informations précieuses des processus en cours d'exécution, des connexions réseau, etc.
- **Open source :** Grâce à son open source, Volatility est librement accessible et personnalisable, ce qui encourage la collaboration et le développement au sein de la communauté.
- **Support multiplateforme :** Compatible avec plusieurs plateformes et systèmes d'exploitation, il est polyvalent pour l'analyse des vidages mémoire provenant de sources diverses.
- **Architecture de plugins :** L'infrastructure de plugins de Volatility permet le développement d'outils d'analyse personnalisés pour des besoins d'enquête spécifiques.
- **Large gamme d'artefacts :** Il donne accès à un large éventail d'artefacts mémoire, notamment les détails des processus, les connexions réseau, les descripteurs de fichiers et les données de registre.
- **Analyse des logiciels malveillants :** Volatility est souvent utilisé pour détecter et analyser les logiciels malveillants en examinant l'état de la mémoire pour détecter toute activité suspecte ou malveillante.
- **Réponse aux incidents :** Cet outil aide les intervenants en cas d'incident à comprendre l'étendue et l'impact des failles de sécurité en examinant la mémoire volatile.

- **Support communautaire :** Une communauté dynamique contribue aux plugins, à la documentation et à l'expertise, garantissant ainsi une amélioration et un support continus.
- **Chronologie forensique :** Volatility permet aux utilisateurs de créer une chronologie de l'activité du système, facilitant ainsi la reconstitution des événements et des séquences.
- **Automatisation et scripts :** Volatility prend en charge l'automatisation par scripts, ce qui optimise le traitement de grands ensembles de données ou de tâches répétitives.
- **Rapports forensiques :** Volatility peut générer des rapports complets résumant les résultats de l'analyse de la mémoire à des fins d'enquête.
  L'ensemble de ces fonctionnalités fait de Volatility un outil puissant et essentiel dans le domaine de la forensique numérique et de la réponse aux incidents.

En résumé, Volatility est un outil incontournable de l'analyse forensique de la mémoire, offrant une visibilité sur l'état volatile des systèmes informatiques. Qu'il s'agisse d'enquêter sur les menaces persistantes avancées (APT), d'analyser les logiciels malveillants ou de mener des investigations forensiques, Volatility permet aux professionnels de la cybersécurité de révéler des informations cruciales cachées dans la mémoire. En maîtrisant Volatility, les analystes peuvent améliorer leur capacité à réagir aux incidents, à détecter les activités malveillantes et à sécuriser leurs systèmes contre les menaces sophistiquées.

7.1.5 Andiller

Andriller est un utilitaire logiciel doté d'une collection d'outils d'analyse forensique pour smartphones. Il effectue une acquisition non destructive, en lecture seule et en toute sécurité, à partir d'appareils Android. Il offre des fonctionnalités telles qu'un puissant piratage d'écran de verrouillage pour détecter les motifs, codes PIN ou mots de passe, ainsi que des décodeurs personnalisés pour les données d'applications issues de bases de données Android (certains systèmes Apple iOS et Windows) afin de décoder les communications. L'extraction et les décodeurs produisent des rapports aux formats HTML et Excel.
Andriller propose de nombreuses fonctionnalités dédiées à l'analyse forensique Android, notamment :

- Extraction et décodage automatisés des données
- Extraction des données des appareils non rootés via la sauvegarde Android (versions Android 4.x, prise en charge variée/limitée)
- Extraction des données avec les autorisations root
- Analyse et décodage des données pour la structure des dossiers, les fichiers Tarball (à partir des sauvegardes Android) et la sauvegarde Android (fichiers backup.ab)
- Sélection de décodeurs de bases de données individuels pour les applications Android
- Déchiffrement des bases de données WhatsApp archivées chiffrées (de .crypt à .crypt12, fichier de clé requis)
- Cracking de l'écran de verrouillage pour le schéma, le code PIN et le mot de passe
- Décompression des fichiers de sauvegarde Android

Grâce à sa spécialisation sur Android et son approche open source, Andriller s'impose comme un outil incontournable dans le domaine de la criminalistique mobile. Il permet aux enquêteurs de réaliser des extractions de données efficaces, tout en respectant les principes fondamentaux de la forensique, notamment la non-altération des preuves. Sa capacité à contourner les écrans de verrouillage, à décoder les bases de données d'applications populaires (comme WhatsApp), et à générer des rapports exploitables en fait un choix privilégié lors d'enquêtes impliquant des appareils mobiles. Andriller s'inscrit ainsi dans une démarche professionnelle rigoureuse, offrant flexibilité, transparence et performance dans l'analyse des smartphones Android, même dans les contextes les plus sensibles.

7.1.6 CAINE Linux

CAINE est une plateforme d'investigation forensique open source professionnelle qui intègre des outils logiciels sous forme de modules ainsi que de puissants scripts dans un environnement d'interface graphique. Son environnement opérationnel a été conçu dans le but de fournir aux professionnels de l'investigation forensique tous les outils nécessaires à la réalisation du processus d'investigation forensique numérique (préservation, collecte, examen et analyse).
CAINE est une distribution Linux active, elle peut donc être démarrée à partir d'un support amovible (clé USB) ou d'un disque optique et s'exécuter en mémoire.Elle peut également être installée sur un système physique ou virtuel. En mode actif, CAINE peut fonctionner sur des objets de stockage de données sans avoir à démarrer un système d'exploitation compatible. La dernière version 11.0 peut démarrer sur UEFI/UEFI+Secure et Legacy BIOS, ce qui permet à CAINE d'être utilisé sur des systèmes d'information qui démarrent des systèmes d'exploitation plus anciens (par exemple, Windows NT) et des plateformes plus récentes (Linux, Windows 10).
CAINE Linux propose une variété d'outils logiciels pour l'analyse de la mémoire, des bases de données, du réseau et l'analyse forensique. L'analyse des systèmes de fichiers tels que FAT/ExFAT, NTFS, Ext2, Ext3, HFS et ISO 9660 est possible en ligne de commande ou via une interface graphique. CAINE Linux prend également en charge l'imagerie disque aux formats RAW (dd) et Expert Witness/Advanced. Les images disque peuvent être obtenues à l'aide des outils intégrés à CAINE ou d'outils tiers comme EnCase ou Forensic Tool Kit.
Contrairement à des outils autonomes tels que FTK Imager ou Volatility, CAINE se présente comme une suite intégrée prête à l'emploi, simplifiant l'environnement de travail de l'enquêteur.

Voici quelques outils inclus dans CAINE Linux :

- Autopsy (Autopsy est simplement l'interface graphique de The Sleuth Kit.)
- The Sleuth Kit : Cet outil en ligne de commande open source permet l'inspection forensique des systèmes de fichiers et des volumes de disque.
- Wireshark
- PhotoRec
- Fsstat : Cet outil affiche les statistiques du système de fichiers d'une image ou d'un objet de stockage.
- RegRipper : Cet outil open source, écrit en Perl, extrait et analyse des informations telles que les clés, les valeurs, les données, etc. de la base de données du Registre pour les analyser.

- Tinfoleak : Cet outil open source permet de collecter des analyses détaillées des données Twitter.

Grâce à son caractère open source, sa modularité, et son large éventail d'outils intégrés, CAINE Linux s'impose comme une solution incontournable dans le domaine de l'investigation numérique. Elle offre aux professionnels une plateforme fiable et prête à l'emploi, adaptée aussi bien aux environnements opérationnels complexes qu'aux interventions en urgence.

7.2 Techniques de la criminalistique numérique

L'investigation numérique utilise diverses techniques et outils pour examiner les appareils compromis. Ces techniques permettent de découvrir des informations cachées, d'analyser l'activité numérique, de détecter des anomalies et de récupérer des fichiers supprimés. Voici quelques techniques couramment utilisées en investigation numérique.

7.2.1 Stéganographie inversée

La Stéganographie s'agit d'une technique utilisée par les cybercriminels pour dissimuler des données dans des fichiers numériques, des communications ou des flux de données. La stéganographie inversée examine le hachage des données d'un fichier particulier. Les informations cachées dans un fichier numérique ou une image peuvent ne pas paraître suspectes à l'examen. En revanche, le hachage sous-jacent, ou la chaîne de données qui représente l'image, est altéré par des informations dissimulées. Pour contrer ce phénomène, les enquêteurs en informatique légale peuvent vérifier et comparer les valeurs de hachage du fichier original et du fichier modifié. Même si les deux fichiers semblent similaires à première vue, les valeurs de hachage diffèrent. Il existe différents types de stéganographie, notamment la stéganographie textuelle, la stéganographie d'image, la stéganographie vidéo, la stéganographie audio et la stéganographie réseau.

7.2.2 Analyse stochastique

L'analyse stochastique est une méthode ou une technique d'analyse forensique informatique permettant d'analyser et de reconstituer une activité numérique ne produisant pas d'artefacts numériques. Un artefact numérique peut être défini comme une modification involontaire de données provoquée par des opérations numériques. Par exemple, les fichiers texte peuvent être considérés comme des artefacts numériques pouvant contenir des indices liés à une cybercriminalité, comme le vol de données, modifiant les propriétés des fichiers. L'utilisation de l'analyse stochastique forensique permet d'enquêter sur les violations de données causées par des menaces internes, qui pourraient ne pas laisser de preuves numériques derrière les artefacts numériques. L'analyse stochastique forensique peut faciliter cette enquête.

7.2.3 Analyse en temps réel

L'analyse en temps réel est une méthode utilisée pour examiner les ordinateurs ou les appareils en fonctionnement. Elle s'effectue au sein du système d'exploitation à l'aide de divers outils d'analyse et d'administration système pour extraire les informations de

l'appareil ou de l'ordinateur. L'utilisation d'outils système pour localiser, examiner et récupérer les données volatiles, généralement stockées dans la mémoire vive ou le cache, fait partie du processus d'analyse en temps réel. Les données collectées proviennent des logiciels installés, des informations matérielles, etc. Les laboratoires d'analyse et les experts sont généralement tenus de conserver l'ordinateur examiné tout au long de l'analyse afin de préserver la chaîne de possession des preuves admissibles devant le tribunal.

7.2.4 Analyse croisée (CDA- Cross Drive Analysis))

L'analyse croisée, également appelée détection d'anomalies, est une technique qui aide les enquêteurs à identifier les similitudes afin de fournir le contexte de l'enquête. Ces similitudes servent de base à l'identification des événements suspects. Elle intègre généralement la corrélation et le recoupement de données sur plusieurs disques informatiques, ce qui permet de localiser, d'analyser et de conserver toute information similaire à la procédure d'enquête, comme les adresses e-mail, les numéros de sécurité sociale, les identifiants de messages, etc.

7.2.5 Récupération de fichiers supprimés

Cette technique, également appelée «sculpture de fichiers» ou «sculpture de données», est utilisée en criminalistique numérique pour récupérer des fichiers supprimés. Elle commence par l'analyse de la mémoire et du système informatique à la recherche de fragments d'informations partiellement effacés à un endroit, mais laissant des traces dans une autre zone de l'appareil examiné. Les informations supprimées peuvent être récupérées à l'aide d'outils d'investigation tels que Wise Data Recovery et CrashPlan.

En conclusion, les techniques d'investigation numérique constituent le cœur de l'analyse forensique. Elles permettent de déceler des activités malveillantes, de restaurer des données cruciales, et de garantir l'intégrité des preuves. Qu'il s'agisse de repérer des données cachées, de reconstruire des événements invisibles ou de récupérer des fichiers supprimés, chacune de ces méthodes contribue à établir la vérité numérique. Leur maîtrise est essentielle pour mener des enquêtes rigoureuses, fiables et juridiquement recevables.

8 Analyse de disque avec Autopsy (Lab TryHackMe)

Afin de pratiquer ce que j'ai appris tout au long de ce rapport, j'ai réalisé le lab "Autopsy : Disk Analysis" proposé sur la plateforme TryHackMe. Ce laboratoire pratique m'a permis de me familiariser avec l'outil Autopsy, utilisé pour l'analyse forensique de systèmes de fichiers.
Le lab consistait à examiner une image disque contenant plusieurs artefacts numériques (fichiers supprimés, historiques de navigation, documents, etc.) afin de reconstituer les activités des utilisateurs.
J'ai enregistré une vidéo durant la période oú j'ai fait le lab pour documenter ma démarche et garder une trace de l'ensemble des manipulations effectuées. Ainsi, ce lab m'a permis d'acquérir des compétences essentielles en analyse forensique :

- Utilisation d'un outil professionnel Autopsy
- Analyse de systèmes de fichiers et récupération de données supprimées,
- Interprétation de traces numériques pertinentes dans un cadre d'enquête.
- Naviguation dans la structure du système de fichiers à l'aide d'Autopsy

Ce lab pratique m'a permis de renfonrcer ma compréhension des concepts clés de la criminalistique numérique et m'a permis d'acquérir des bases solides pour aborder des analyses forensiques plus complexes à l'avenir.

9 Conclusion

Ce rapport m'a permis d'explorer en profondeur le domaine de la criminalistique numérique, un pilier essentiel de la cybersécurité moderne. De la compréhension des preuves électroniques jusqu'à les outils avancés utilisés dans ce domaine comme Wireshark, FTK Imager ou Autopsy, cchaque section a souligné l'importance d'une méthodologie rigoureuse et d'une approche scientifique dans l'investigation des incidents numériques. J'ai abordé les techniques utilisées pour identifier, collecter, préserver et présenter les preuves de manière juridiquement recevable, ainsi que les principales branches spécialisées telles que les réseaux, les appareils mobiles, le stockage et le cloud.
Dans un contexte où les cyberattaques deviennent plus fréquentes et sophistiquées, la criminalistique numérique permet non seulement de répondre efficacement aux incidents, mais aussi de renforcer la prévention et la résilience organisationnelle. Son rôle est essentiel et crucial pour assurer la traçabilité des actes malveillants, garantir la responsabilité légale et faciliter la mise en place de mesures correctives.
Ce travail m'a permis d'enrichir et d'approfondir mes connaissances pratiques et théoriques, de mieux comprendre les outils et techniques utilisés par les professionnels du domaine, et de prendre en conscience l'importance de la précision, de la documentation et de l'intégrité dans chaque étape de l'investigation. La criminalistique numérique n'est pas seulement un domaine technique ; c'est aussi une discipline exigeante, au service de la justice et de la vérité dans l'univers numérique.

10 Références

1. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, Christopher K. Steuart and Robert S. Wilson
2. Digital Forensics and Incident Response by Gerard Johansen
3. Handbook of Digital Forensics and Investigation edited by Eoghan Casey
4. Digital Forensics with Open Source Tools – Cory Altheide & Harlan Carvey
5. https ://www.e-spincorp.com/master-network-forensics-tools-techniques-best-practices-cybersecurity/
6. https ://eforensicsmag.com/autopsy-the-digital-forensics-toolkit/
7. https ://medium.com/infosecmatrix/ftk-imager-a-comprehensive-guide-to-forensic-imaging-and-analysis-2023-4eca04272614
8. https ://medium.com/@careertechnologymiraroad/volatility-978e32316616
9. https ://systemweakness.com/android-forensics-with-andriller-on-kali-linux-a770591331b1
10. https ://www.geeksforgeeks.org/caine-forensic-environment/
11. https ://en.wikipedia.org/wiki/CAINE_Linux
12. https ://www.geeksforgeeks.org/techniques-of-cyber-forensics/
13. https ://eclipseforensics.com/forensic-techniques-for-recovering-deleted-data-from-digital-devices/
14. https ://www.sentinelone.com/cybersecurity-101/cybersecurity/digital-forensics/
15. https ://cyfor.co.uk/the-role-of-digital-forensics-in-cybersecurity-incident-response/
16. https ://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools
17. https ://www.proofpoint.com/fr/threat-reference/digital-forensics
18. https ://www.servicenow.com/fr/products/legal-service-delivery/what-is-digital-forensics.html
19. https ://en.wikipedia.org/wiki/Cloud_computing
20. https ://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene
21. https ://zimperium.com/glossary/mobile-device-forensics
22. https ://translate.google.com/
23. Dans le cadre de ce projet l'intelligence artificielle générative, en particulier ChatGPT, a été utilisée pour :
    - Reformuler et structurer certaines sections théoriques du rapport.
    - Expliquer des concepts complexes
    - Fournir des suggestions de plans, de transitions logiques entre les parties
    - Accompagner l'élaboration de la partie pratique, notamment dans l'installation, le choix de l'image disque...
    - Génération d'illustrations à inclure dans le rapport et la présentation pour appuyer visuellement les explications.
    - Résumés clairs et structurés des grandes parties du projet pour inclure dans la présentation

L'IA a donc été utilisée comme un assistant intelligent, pour gagner du temps, améliorer la qualité de l'écriture, et faciliter la compréhension de notions techniques

24. https ://tryhackme.com/room/autopsy2ze0
25. Pour le lab pratique j'ai utilisé cette vidéo pour m'aider : https ://www.youtube.com/watch ?v=6xkPjqY5Pd8&t=17s
26. Lien de la présentation : https ://www.canva.com/design/DAGlrMCOkuc/HVpdamFiO7rymAKhMaZd-A/edit ?utm_content=DAGlrMCOkuc&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton