

Digital Forensics: Case Studies and Investigative Strategies

Ces extraits portent sur la **criminalistique numérique**, en mettant l'accent sur la **méthodologie d'enquête** et l'importance de la **pratique en laboratoire**. L'auteur utilise un premier scénario de **harcèlement au travail** pour illustrer la collecte de preuves via les **journaux réseau**, les courriels et les systèmes d'authentification. Le texte souligne la nécessité pour l'enquêteur de demeurer **impartial**, de documenter rigoureusement la **chaîne de traçabilité** et de respecter les protocoles légaux. Il aborde également les défis techniques comme l'**usurpation d'adresses** et la visibilité limitée des données dans le **cloud**. Enfin, un second scénario introduit l'**analyse forensique des terminaux** pour détecter la suppression intentionnelle de données sensibles.

Quels types de journaux réseau sont essentiels pour identifier un suspect ?

Pour identifier un suspect et attribuer de manière fiable une empreinte numérique lors d'une enquête réseau, plusieurs types de journaux sont essentiels :

- **Les journaux d'authentification centralisée** : La plupart des réseaux d'entreprise s'appuient sur des systèmes centralisés tels que **Active Directory, TACACS+ ou Radius**. Ces journaux sont cruciaux pour relier directement l'activité réseau aux identifiants d'un compte utilisateur précis (par exemple, pour prouver par quel compte une personne s'est authentifiée). Si l'on enquête uniquement sur une machine locale sans authentification centralisée, les journaux risquent de ne pas être fiables.
- **Les journaux de suivi et de serveurs de messagerie** : Obtenus sur des serveurs comme Microsoft Exchange (via des scripts comme Get-MessageTracking), ces journaux consignent l'expéditeur, l'heure, la localisation de la connexion, ainsi que

l'adresse IP de connexion pour les courriels envoyés ou reçus. L'analyse détaillée des **en-têtes de courriels** permet également d'extraire chronologiquement (par ordre inverse) les adresses IP des serveurs SMTP par lesquels le message a transité, révélant ainsi l'adresse IP d'origine du message.

- **Les journaux de pare-feu applicatifs et d'activité utilisateur :** Les équipements réseau de nouvelle génération (tels que Cisco Firepower, Fortinet FortiGate, Checkpoint ou Palo Alto) enregistrent le trafic Internet et l'activité réseau générale. Ils permettent de filtrer et d'analyser le trafic spécifique lié aux applications, comme l'utilisation de **comptes de messagerie chiffrés dans le cloud**, de **messageries instantanées** ou de **réseaux sociaux**.
- **Les journaux de serveurs proxy et de filtres de contenu :** Des outils de filtrage web comme Squid conservent des historiques clairs de l'utilisation du Web. Ces journaux permettent de savoir exactement quand, où et quelles ressources en ligne ont été consultées par les utilisateurs.

L'importance capitale de la corrélation de données

Dans une enquête de criminalistique numérique, l'adresse IP seule ou l'adresse MAC sont insuffisantes pour identifier formellement un suspect, car **les adresses IP peuvent être modifiées et les adresses MAC usurpées**. La défense peut facilement soutenir qu'une adresse IP dynamique appartenait à un autre utilisateur à ce moment-là.

Pour valider l'identité du suspect, l'enquêteur doit **corrélérer plusieurs sources de preuves** :

1. **Croiser l'activité réseau et l'identité personnelle** : Par exemple, l'obtention de journaux web montrant qu'une adresse IP spécifique s'est connectée à un compte de réseau social personnel (dont l'identité est connue) permet de prouver que cette même adresse IP est celle qui a effectué une action suspecte (comme le téléchargement d'un fichier sensible) au même instant.
2. **Établir une chronologie solide** : En combinant les enregistrements de connexion des utilisateurs au pare-feu, les authentifications sur le serveur Active Directory, l'activité de messagerie et les requêtes web, l'enquêteur reconstitue

l'historique complet des événements pour attribuer avec certitude les actions à la partie émettrice.

Simuler le plan d'action du Scénario 1.

1. Phase de Pré-enquête et Cadrage Déontologique

- **Déclaration de conflit d'intérêts** : L'enquêteur doit immédiatement déclarer toute relation personnelle ou professionnelle antérieure avec les employés concernés, identifiés ici comme **Huxley Krepelka** et **Sarah Bleyle**. Si une opinion est déjà formée ou si un conflit d'intérêts existe, l'enquête doit obligatoirement être confiée à un autre organisme.
- **Autorisations formelles et cadre légal** : L'enquêteur doit obtenir une habilitation officielle et écrite de la part d'une personne habilitée pour accéder aux données sensibles (courriels, historiques de navigation web à contenu personnel potentiellement embarrassant) afin de valider la chaîne de traçabilité et de se prémunir de toute responsabilité civile ou pénale.
- **Neutralité de l'enquêteur** : Le rôle de l'enquêteur se limite strictement à **consigner et présenter les faits numériques de manière impartiale**, sans jamais qualifier la culpabilité ni porter de jugement de valeur sur l'existence ou non d'un harcèlement. Si les ressources humaines (RH) demandent d'enquêter uniquement dans le but de prouver la culpabilité, l'enquêteur doit s'y opposer pour éviter tout conflit d'intérêts.
- **Évaluation des risques et imprévus** : Il convient de poser les questions clés de pré-enquête (niveau d'effort, risques d'interruption d'activité, habilitation légale) et de désigner un point de contact au sein de l'organisation pour gérer les situations imprévues, telles que la découverte fortuite d'activités illégales (ex. pornographie infantile ou interactions avec un mineur) qui imposeraient d'alerter immédiatement les autorités.

2. Acquisition et Préparation de l'Examen

- **Collecte des identifiants** : Récupérer les informations d'utilisateur fournies par l'entreprise, y compris les informations d'identification de point de terminaison et les noms de comptes Active Directory.

- **Gestion des accès aux infrastructures** : Solliciter auprès de l'administrateur système (ex. **Steve Stasiukiewicz**) un compte d'accès spécifique en lecture seule pour l'ensemble des plateformes. L'enquêteur doit prendre l'initiative d'extraire lui-même les données non modifiées ou, à défaut d'accès direct, superviser étroitement les manipulations faites par le technicien habilité. Cela évite d'exposer des failles de traçabilité que la défense pourrait exploiter au tribunal.
- **Saisie et traçabilité** : Consigner méticuleusement l'identité de chaque intervenant impliqué dans la collecte de preuves au sein d'un logiciel de gestion de cas et stocker l'ensemble des éléments sur un support physique sécurisé et scellé (comme la clé **USB12345**).

3. Stratégie de Collecte et d'Extraction Réseau

La stratégie consiste à analyser les données ayant transité par les différents points d'intérêt réseau de l'entreprise :

- **Système d'authentification centralisé** : Accéder en priorité au Active Directory (**AD123345** ou systèmes Windows/TACACS+/Radius) pour relier les actions aux comptes de connexion correspondants et démontrer l'intention de l'utilisateur.
- **Analyse de la messagerie d'entreprise** :
 - Cibler les outils de messagerie professionnelle de l'organisation (**EmailTool12345** et **EmailTool54321**).
 - Exécuter des scripts de suivi (comme le script PowerShell Get-MessageTracking si l'entreprise utilise Microsoft Exchange) pour obtenir l'historique complet d'envoi, l'heure, la localisation de la connexion et l'adresse IP associée.
 - Analyser les en-têtes des courriels SMTP dans l'**ordre chronologique inverse** (l'adresse la plus ancienne correspondant à l'adresse IP d'origine de l'e-mail).
 - Vérifier si des signatures numériques ou des certificats de chiffrement d'entreprise ont été apposés afin de garantir l'authenticité de l'expéditeur.
- **Analyse de l'utilisation du Web et des flux applicatifs** :

- Consulter les journaux du serveur proxy Squid ou du filtre de contenu (**ContentFilter12345**) pour obtenir l'historique des connexions internet de Huxley et de Sarah.
- Interroger les pare-feux applicatifs de nouvelle génération (**ApplicationFirewall12345** / Cisco Firepower, Fortinet, Checkpoint, Palo Alto) pour générer des rapports sur l'utilisation d'applications web spécifiques : trafic des réseaux sociaux (ex. Facebook via Context Explorer), messageries cloud personnelles et messagerie instantanée.
- **Exclusion des données de sécurité non pertinentes** : Reporter ou ignorer l'analyse des antivirus et des systèmes de prévention des intrusions (IPS) car l'objectif est de collecter des communications de harcèlement et non de détecter des comportements d'attaque réseau, sauf si un employé affirme qu'un logiciel malveillant a usurpé sa messagerie.

4. Corrélation de Données et Chronologie Forensique

- **Attribution robuste** : Les adresses IP dynamiques pouvant changer et les adresses MAC pouvant être usurpées, l'enquêteur doit croiser plusieurs éléments de preuve.
- **Établissement de la chronologie** : Corréler chronologiquement les données de connexion Active Directory, les historiques d'accès au serveur de messagerie et les journaux du pare-feu applicatif pour reconstituer un historique solide des événements réseau.
- **Preuve d'attribution** : Croiser l'activité de l'adresse IP suspecte avec une connexion simultanée sur la même adresse IP vers un compte personnel (comme un réseau social) pour confirmer de manière indiscutable l'identité de l'expéditeur.

5. Identification des Lacunes et Limitations

- L'investigateur doit explicitement documenter toutes les limitations de l'enquête, notamment l'impossibilité d'accéder aux données hébergées sur le cloud personnel hors du réseau d'entreprise (comme Gmail personnel, applications privées ou réseaux cellulaires tiers).
- Préciser que l'enquête n'a pas inclus l'évaluation des terminaux physiques à ce stade, bien que les conclusions de l'investigation réseau puissent justifier ultérieurement une telle saine auprès des RH.

6. Clôture de l'Enquête et Rapport

- Compilation et numérotation rigoureuse des artefacts découverts (ex. courriels ou logs d'activité Facebook répertoriés) au sein des annexes du rapport d'expertise judiciaire.
- Remise du rapport de synthèse factuel aux RH, se limitant uniquement à l'authentification et l'attribution des communications techniques recensées sans tirer de conclusions personnelles quant à l'existence effective du harcèlement.

Simuler le Scénario 2 : terminaux physiques

Voici la simulation détaillée du plan d'action pour le **Scénario 2** :

Analyse forensique des terminaux physiques (ordinateur portable et téléphones professionnels), élaborée selon les exigences de la criminalistique numérique et les données de vos études de cas.

Ce scénario fait suite à l'enquête réseau. Les indices réseau suggérant que des données d'entreprise hautement confidentielles ont été supprimées et potentiellement exfiltrées vers un concurrent après que l'employée suspecte a été contactée par les RH, vous devez analyser l'ordinateur portable Windows et les deux téléphones saisis (Huxley et Sarah).

Phase 1 : Cadrage légal et Préparation de l'intervention

- **Validation des habilitations et confidentialité** : Confirmer que les deux employés concernés ont formellement signé la clause de renonciation à la confidentialité sur le matériel fourni par l'entreprise avant d'y accéder. Faire valider l'accès par la direction générale ou les propriétaires des actifs informatiques afin d'éviter toute responsabilité civile ou pénale quant au respect de la vie privée.
- **Définition des cibles d'enquête** : Définir précisément avec les RH et le département technique les types de documents qualifiés de « sensibles ». Dans ce cas, l'objectif principal est de cibler des **schémas techniques de nouvelles technologies au format JPEG** (ou d'autres types d'images et archives).

- **Collecte des accès administratifs** : Récupérer auprès du service informatique les identifiants de session et de déchiffrement des appareils Windows et mobiles fournis afin de s'affranchir des difficultés liées au chiffrement de démarrage.

Phase 2 : Préservation et Acquisition Forensique (Clonage et Hachage)

- **Ordinateur Windows (Actif éteint)** :
 - **Ne pas rallumer le système** directement sous Windows afin d'empêcher toute modification de l'état des données et d'assurer une validation conforme des signatures de hachage.
 - Utiliser un **dispositif matériel de blocage en écriture** (Write-Blocker) pour empêcher toute contamination accidentelle.
 - Réaliser un **clonage bit-à-bit (image physique)** du disque dur (ex. avec FTK Imager ou l'utilitaire dd).
 - Calculer et consigner immédiatement la **signature de hachage (MD5/SHA-1)** du clone pour garantir la validité médico-légale de la preuve.
- **Téléphone mobile Android (Samsung exécutant Android 5.x)** :
 - S'il possède une carte mémoire amovible (**microSD**), l'extraire et l'insérer dans un adaptateur SD protégé en écriture pour un clonage direct sur la station d'enquête.
 - Pour la mémoire interne flash, documenter l'état (éteint et réinitialisé d'usine). Utiliser un outil de rootage (comme Kingo Root) puis se connecter via un shell grâce à l'outil **Android Device Bridge (ADB)**.
 - Monter le disque virtuel et créer une **image physique RAW (clone bit-à-bit)** du stockage avec FTK Imager ou DD, puis valider son hachage.
- **Téléphone mobile iPhone (iOS 11+)** :
 - Prendre en compte le fait qu'il est techniquement **impossible de récupérer directement des images sur un terminal iOS moderne réinitialisé d'usine** en raison du chiffrement matériel strict d'Apple.

- La stratégie d'acquisition alternative consiste à chercher l'existence de **sauvegardes iTunes** créées localement sur le disque de l'ordinateur portable Windows de l'utilisateur.

Phase 3 : Extraction et Recherche des Fichiers (Analyse)

- **Sur l'image du disque Windows :**
 - Monter le clone d'enquête sous Kali Linux et utiliser l'outil **Foremost** pour extraire et catégoriser automatiquement l'ensemble des fichiers.
 - Lancer une recherche Windows sur toutes les partitions à l'aide de la commande ciblée `kind:=picture` pour localiser les extensions d'images courantes (JPEG, PNG, GIF, BMP) et de fichiers compressés (ZIP, RAR) pouvant dissimuler des schémas techniques.
 - Exécuter le logiciel de récupération de données **PhotoRec** sur l'image disque Windows pour extraire les images supprimées et reconstituer leurs métadonnées d'origine (date de création, modifications).
 - Analyser le fichier de cache d'images **thumbs.db** (généralement non supprimé par l'utilisateur) situé sous `\Utilisateurs\%nom_utilisateur%\AppData\Local\Microsoft\Windows\Explorer` pour prouver la présence passée et la consultation des fichiers incriminés.
 - Extraire les sauvegardes iTunes non chiffrées identifiées sur le disque dur portable Windows et utiliser l'outil **iPhone Backup Viewer** pour inspecter et visualiser les photos qui y sont stockées.
- **Sur l'image du disque Android :**
 - Utiliser **PhotoRec** (qui prend en charge les systèmes de fichiers Android exFAT, F2FS, JFFS2 et YAFFS2) pour récupérer les photos et schémas supprimés de la mémoire flash.

Phase 4 : Corrélation et Analyse Chronologique

- **Preuve de suppression et d'exfiltration :**
 - Analyser l'historique des e-mails sortants d'**Outlook** sur l'ordinateur Windows de l'utilisateur suspect.

- Vérifier si les fichiers JPEG de schémas techniques récupérés dans le répertoire des fichiers supprimés correspondent à des fichiers cryptés envoyés par courriel vers une **adresse privée externe** appartenant à une **entreprise concurrente**.
- **Chronologie des événements** : Corréler l'historique d'envoi de ces e-mails sortants, les métadonnées de création des fichiers JPEG récupérés et les mises à jour chronologiques du fichier Windows *thumbs.db*.

Phase 5 : Clôture de l'Enquête et Rapport

- **Stockage et sécurité des preuves** : Consigner méticuleusement la chaîne de possession forensique et enregistrer l'ensemble des preuves récupérées sur un support de stockage externe physiquement sécurisé et scellé (ex. disque dur Actif 4301 ou clé USB jointe).
- **Rapport médico-légal final** : Rédiger un rapport de synthèse à l'intention du service des ressources humaines présentant les faits techniques. S'en tenir à l'authentification stricte des artefacts récupérés (images JPEG de schémas d'entreprise chiffrés, traces d'exfiltration et de suppression volontaire) sans formuler de jugement de culpabilité ou d'infraction, tâche qui incombe exclusivement à l'entreprise ou aux autorités.

Simuler le Scénario 3

Voici la simulation détaillée du plan d'action pour le **Scénario 3** :

Investigation de logiciels malveillants, conçu pour analyser un poste de travail anormalement ralenti au sein de votre entreprise.

Contrairement aux deux premiers scénarios, cette investigation s'inscrit dans un contexte de support informatique interne et de réponse aux incidents, sans enjeu légal direct.

Phase 1 : Préparation de l'intervention et Cadrage

- **Prise en charge du ticket d'incident** : Analyser la plainte de l'utilisateur qui signale un ralentissement extrême de sa machine.
- **Autorisations et communication** :

- Vérifier l'habilitation à inspecter et modifier l'ordinateur portable d'entreprise. Si l'appareil appartient à l'entreprise et qu'une charte de confidentialité est signée, l'autorisation technique est de droit, mais il convient de maintenir une communication ouverte avec l'employé.
- Interroger l'employé pour savoir s'il a volontairement installé un outil spécifique ou s'il dispose d'informations sur l'origine du problème, ce qui évite de perdre du temps.
- **Premier diagnostic (Analyse en direct) :**
 - Ouvrir le **Gestionnaire des tâches Windows** sur la machine affectée pour recenser les processus actifs.
 - Identifier **deux processus suspects** consommant anormalement des ressources, puis localiser les fichiers exécutables associés dont la fonction reste inconnue.
 - Soumettre les fichiers à l'antivirus local et au service en ligne **VirusTotal**. Si l'antivirus et VirusTotal ne détectent rien, l'analyse statique et dynamique approfondie est requise.

Phase 2 : Stratégie d'Identification des Fichiers (Analyse Statique)

Les auteurs de logiciels malveillants masquent souvent la nature réelle de leurs exécutables pour tromper l'utilisateur et les outils de sécurité.

L'objectif est d'identifier le vrai type de fichier et la méthode de dissimulation :

- **Vérification de sécurité (Attaquant sophistiqué) :** Si l'on soupçonne une menace ciblée, éviter d'envoyer le fichier complet sur des plateformes publiques comme VirusTotal (car l'attaquant pourrait surveiller la détection de son outil) ; privilégier l'**envoi du hachage** (MD5/SHA-1).
- **Détermination de la signature réelle avec TrIDNET :** Charger les bases de définitions du site *mark0.net* dans l'outil **TrIDNET** pour analyser la structure interne de l'artefact suspect. Dans ce scénario, TrIDNET révèle qu'il s'agit d'une **archive auto-extractible WinRAR (SFX)** dissimulée sous une fausse extension.
- **Analyse du compresseur avec PEiD :** Exécuter l'outil **PEiD** équipé de sa base de signatures userdb.txt. PEiD valide qu'il s'agit bien d'une archive RAR SFX et aide à identifier le compresseur ou

l'encapsulateur (packer) utilisé pour chiffrer ou compacter le malware afin de savoir comment le décompresser.

Phase 3 : Analyse Dynamique en Environnement Isolé (Bac à sable)

- **Préparation du fichier :**
 - Dans l'Explorateur Windows, désactiver l'option *"Masquer les extensions des fichiers dont le type est connu"*.
 - Modifier manuellement l'extension du fichier suspect de **.exe** vers **.rar**.
 - Extraire le contenu de l'archive RAR à l'aide de WinRAR pour isoler l'exécutable malveillant d'origine.
- **Exécution et observation comportementale :**
 - Transférer l'exécutable extrait dans un environnement de test isolé (sandbox), comme **Cuckoo Sandbox** ou **Cisco ThreatGrid**.
 - Utiliser **PE Studio** pour inspecter les métadonnées de l'exécutable décompressé, ses fonctions importées et ses indicateurs suspects.
 - Lancer l'exécution du fichier dans la sandbox pour observer son impact réel (par exemple, la détection d'un rançongiciel comme **Cryptolocker** chiffrant les fichiers et affichant une demande de rançon en Bitcoins).

Phase 4 : Confinement, Enquêtes de Sécurité et Remédiation

- **Alerte et réponse aux incidents :**
 - Contacter immédiatement l'**équipe de réponse aux incidents (CSIRT)** pour lui transmettre les hachages des processus et fichiers malveillants identifiés afin de rechercher d'autres infections sur le réseau.
- **Recherche du vecteur d'infection :**
 - Analyser les journaux du pare-feu applicatif, du filtre de contenu ou du serveur proxy Squid pour comprendre comment l'utilisateur a obtenu le fichier.
 - Vérifier si le téléchargement est lié à l'installation volontaire par l'utilisateur d'un **logiciel potentiellement indésirable (PUP)** utilisé pour contourner la sécurité de l'entreprise (par

exemple, les outils **Hola!VPN** ou **DNS Unlocker** pour regarder des flux vidéo en streaming).

- **Analyse de vulnérabilité** : Utiliser un scanner de vulnérabilités comme **OpenVAS** (ou Nessus / Nexpose) sur la machine pour déterminer si une faille système non corrigée a permis l'exécution ou l'installation furtive du binaire.
- **Remédiation du poste** : Bien qu'une désinfection soit parfois possible, appliquer la politique de sécurité standard de l'entreprise consistant à **formater et réinstaller complètement le système d'exploitation** afin de garantir l'éradication totale de la menace.
- **Suivi** : Documenter l'incident et la méthodologie de remédiation dans l'outil de gestion de tickets de réponse aux incidents (Request Tracker).

Simuler le Scénario 4

1. Phase de Cadrage et de Pré-enquête

- **Validation des autorisations et périmètre légal** : Avant d'accéder aux systèmes du centre de données, l'enquêteur doit s'assurer d'obtenir une **autorisation écrite et officielle** de la direction pour auditer les machines concernées. Les serveurs de démonstration hébergeant parfois des données ou des environnements de clients tiers, il est impératif de bien identifier les segments virtuels autorisés et de s'assurer de ne pas violer la confidentialité d'entités externes.
- **Vérification des conflits d'intérêts** : L'enquêteur doit déclarer formellement n'avoir aucun lien personnel ou professionnel direct avec les ingénieurs ou administrateurs ayant accès au laboratoire de démonstration afin de garantir une impartialité totale, surtout si l'entreprise a déjà une théorie sur l'identité du coupable.
- **Évaluation des risques opérationnels** : Étant donné que les serveurs du laboratoire sont volumineux, coûteux et en exploitation continue, l'interruption de service doit être évitée ou validée par les responsables d'actifs. Un point de contact interne doit être désigné pour encadrer l'intervention en cas d'imprévu technique.

2. Stratégie de Préservation et d'Acquisition (Données Volatiles)

- **Maintien de l'état d'alimentation (Live Acquisition) :** Les serveurs étant allumés et connectés à Internet, **ils ne doivent pas être éteints**. L'extinction détruirait immédiatement le contenu de la mémoire vive (RAM), qui contient pourtant les processus actifs, les connexions réseau en cours et les clés de chiffrement essentielles pour identifier l'activité suspecte.
- **Gestion du risque de compromission à distance :** Puisque les machines sont en ligne, il existe un risque qu'un suspect distant se connecte pour altérer ou supprimer les preuves à la découverte de l'enquête. La décision de déconnecter temporairement les machines du réseau d'entreprise doit être prise conjointement avec les propriétaires d'actifs informatiques après avoir pesé le pour et le contre (perte d'analyse des connexions actives versus risque de sabotage).
- **Création de copies de sécurité (Clonage et Hachage) :**
 - Ne jamais travailler directement sur les serveurs de production originaux afin d'éviter la contamination involontaire des preuves.
 - Réaliser plusieurs copies de sauvegarde (images physiques et de mémoire) avant et après toute modification (comme une déconnexion réseau) afin d'isoler les changements induits par l'intervention.
 - Appliquer un **bloqueur d'écriture matériel** lors de l'analyse des disques durs clonés. Une image de secours non protégée peut être utilisée pour un diagnostic initial rapide des processus, mais la preuve finale devra s'appuyer sur la copie intègre certifiée par hachage.

3. Extraction et Analyse de la Mémoire Vive (RAM)

- **Capture de la mémoire :** Pour extraire l'empreinte de la RAM sans laisser de traces sur les disques durs des serveurs, l'enquêteur utilise des outils d'extraction spécialisés s'exécutant directement depuis une clé USB externe (comme **MoonSols Dumpit.exe**, **Win64dd/Win32dd**, **Winpmem** ou **Memoryze**).
- **Analyse comportementale de la mémoire vive :**
 - **Volatility :** Exécuter l'outil d'analyse forensique de mémoire *Volatility* depuis un support sécurisé pour lister les processus actifs et identifier les plus gourmands en ressources.

- **FireEye Redline / Memoryze** : Utiliser *Redline* ou *Memoryze* (également compatible avec macOS au besoin) pour inspecter l'historique de la mémoire active, recenser les commandes terminales saisies par les utilisateurs et examiner les requêtes réseau effectuées.
 - **Identification des processus inhabituels** : Exporter la consommation de mémoire par application. Si des processus anormaux consomment une grande partie des ressources énergétiques ou du processeur, mener une recherche externe (ex. via un moteur de recherche sécurisé) et croiser ces découvertes avec la liste des logiciels officiellement autorisés par l'entreprise.
4. Constatations Techniques et Attribution (Scénario Bitcoin)
- **Preuve de l'abus de ressources** : L'analyse de la mémoire vive (notamment l'artefact 2343 sur le serveur 4023) révèle qu'un ensemble d'applications non autorisées consomment **environ 80 % de la puissance de calcul** des serveurs référencés 4532 à 4539. Les recherches confirment qu'il s'agit d'un **système de génération de Bitcoins** (cryptomonnaie).
 - **Attribution de l'installation et des accès** : L'examen des journaux d'accès au serveur et des commandes d'exécution identifiées en mémoire permet d'associer deux comptes d'utilisateurs internes spécifiques à ces actions :
 - John.Columbus@company.com
 - Michael.Korten@company.com
 - **Tracé des profits** : Le logiciel de minage exporte les bitcoins générés vers un compte de portefeuille externe qui ne peut pas être identifié directement depuis l'infrastructure interne de l'entreprise.
5. Clôture de l'Enquête, Archivage et Suite Légale
- **Sauvegarde physique des preuves** : Regrouper l'ensemble des journaux d'accès réseau, captures d'écran des processus actifs et images mémoire sur une clé USB sécurisée et scellée, référencée sous le numéro de pièce **USB 38452** (contenant notamment les artefacts 2340, 2341, 4532, 2342).
 - **Rapport de synthèse factuel** : Rédiger un rapport d'expertise forensique final récapitulant la chronologie de l'augmentation d'électricité, la liste des serveurs affectés, les processus de

minage identifiés et l'attribution claire aux deux comptes d'utilisateurs.

- **Suivi administratif et juridique :**
 - Remettre le rapport à la direction pour justifier les mesures RH appropriées (licenciement des employés impliqués).
 - L'entreprise pouvant engager des poursuites judiciaires civiles ou pénales pour récupérer les coûts d'électricité et le temps de travail détourné, l'enquêteur doit se préparer à **témoigner devant les tribunaux** pour valider la chaîne d'intégrité de ses preuves et de ses méthodes d'analyse.

Simuler le Scénario 5

1. Phase de cadrage légal et déontologique (Isoler et s'abstenir de polluer)

- **Contexte de l'incident :** En tant qu'ingénieur réseau situé à la croisée du réseau et de la sécurité, vous êtes désigné comme la personne de référence face à une crise majeure : la direction et les RH vous informent que le FBI a identifié un employé comme membre d'un réseau criminel de blanchiment d'argent via les actifs de l'entreprise. Vous êtes chargé de gérer la situation immédiate.
- **Préservation légale et vie privée :** Puisque des poursuites judiciaires sont hautement probables et que les forces de l'ordre mèneront l'enquête, votre rôle est d'agir en premier intervenant sans compromettre la recevabilité des preuves futures. Vous devez respecter scrupuleusement la vie privée : un bureau individuel ou un ordinateur portable fermé est légalement assimilable à une mallette verrouillée.
- **Principe de prudence maximale :** Les services juridiques et les RH ne maîtrisant pas toujours ces nuances juridiques, la meilleure solution consiste à **isoler et répertorier les éléments de la zone, sans y pénétrer ni manipuler les appareils sans autorisation formelle**. Une intervention technique maladroite ou non autorisée pourrait entraîner l'exclusion des preuves lors du procès. En cas de doute, la consigne est d'entourer la zone de travail de ruban adhésif et d'attendre les instructions des autorités compétentes.

2. Stratégie d'intervention initiale (Délimitation et sécurité physique)

- **Balisage de la scène de crime** : Délimitez physiquement la zone susceptible de contenir des preuves à l'aide de ruban de signalisation, en indiquant clairement que l'accès est strictement interdit. Consignez précisément votre heure d'arrivée et vos observations visuelles.
 - **Contrôle des accès physiques** : Si l'organisation dispose d'agents de sécurité, affectez immédiatement un garde pour surveiller le périmètre et en interdire l'accès aux tiers. Soyez ferme : toute personne traversant la délimitation s'expose à perturber une enquête en cours et devra probablement s'expliquer auprès des autorités.
3. Documentation systématique de la scène (Sans contact physique)
- **Photographie exhaustive** : Utilisez un appareil photo numérique pour photographier l'ensemble de la scène sous tous les angles et documenter l'état visuel de chaque élément consigné.
 - **Croquis détaillé de l'espace de travail** : Réalisez un schéma précis représentant l'agencement physique du bureau, l'emplacement de l'ordinateur piraté (*Hacked PC*), des connexions réseau physiques et des accès. Mesurez les dimensions de l'espace de bureau à l'aide d'un mètre ruban ou estimez-les pour garantir un maximum de détails.
 - **Fiche d'identification des personnes** : Recensez les coordonnées de toute personne d'intérêt ou témoin potentiel, en ajoutant une brève description de leur lien avec l'affaire. **Ne procédez à aucun interrogatoire à ce stade**, l'enquêteur principal des forces de l'ordre s'en chargera.
4. Gestion technique des terminaux et des flux réseau
- **Préservation de l'état d'alimentation** : Ne modifiez jamais l'état électrique des machines (ne pas allumer un système éteint, ne pas éteindre un système allumé) pour ne pas détruire les données volatiles ou altérer la signature de hachage.
 - **Évaluation du risque de modification à distance** :
 - Si le suspect ou ses complices risquent d'altérer ou de supprimer les preuves à distance, la déconnexion réseau ou l'usage d'une cage de Faraday (pour bloquer les connexions sans fil/Bluetooth) doit être envisagée.

- Toutefois, cette décision de bloquer le trafic doit être validée par une personne habilitée ou l'enquêteur principal, car ce dernier souhaitera très probablement collecter d'abord la mémoire vive et les données volatiles actives.
- Si des technologies cloud sont impliquées, le risque d'effacement à distance étant extrême et l'investigation complexe, l'équipe juridique peut vous autoriser à déconnecter les systèmes, mais cette décision se prend strictement au cas par cas.

5. Prélèvement d'indices exceptionnels et chaîne de traçabilité

- **Règle d'or de non-intervention physique** : Dans ce type d'affaires criminelles, il est préférable de ne prélever aucun élément de preuve vous-même.
- **Exception pour risque d'altération immédiate** : Si un appareil d'intérêt se trouve en dehors de la zone sécurisée ou dans un lieu de passage fréquenté (par exemple, un téléphone portable d'intérêt oublié sur une imprimante réseau dans un couloir), vous pouvez l'emballer et l'étiqueter dans un sac antistatique (ou compatible cage de Faraday). Manipulez-le de façon à ne pas introduire d'empreintes digitales supplémentaires.
- **Sécurisation absolue et documentation** : Enregistrez l'objet prélevé dans votre logiciel de gestion de cas et conservez-le dans un conteneur sécurisé sous clé. Ne le laissez jamais dans un lieu public, un tiroir de bureau non verrouillé ou auprès d'un collègue non identifié. Si aucun coffre n'est disponible, maintenez une surveillance humaine de la zone balisée jusqu'au transfert.

6. Clôture de l'intervention et transfert de dossier (Passage de relais)

- **Passage de témoin aux enquêteurs** : Préparez-vous à remettre l'ensemble de vos constatations et pièces à l'équipe responsable de la poursuite de l'enquête dès son arrivée.
- **Contenu du dossier de transfert** :
 - Rapport descriptif détaillé de la scène de crime à votre arrivée (comprenant le rapport écrit, le croquis et les photos de l'espace).
 - Liste complète des personnes d'intérêt identifiées avec leurs coordonnées.

- Tous les éléments saisis d'urgence, emballés, étiquetés, accompagnés de leur journal de chaîne de traçabilité médico-légale.
- Liste des membres de votre équipe d'intervention initiale.
- Coordonnées des agents de sécurité ayant sécurisé la zone.
- Toutes les notes techniques prises concernant les actions préalables à leur arrivée.
- **Fin de votre implication** : Une fois ces documents et preuves transférés sous signature, l'enquête est considérée comme clôturée pour vous et vous n'intervenez plus dans le dossier.

Comment prouver l'intention ?

En criminalistique numérique, prouver l'intention d'un utilisateur derrière une activité suspecte repose sur la capacité de l'enquêteur à lier de manière incontestable une action réseau à une personne physique et à éliminer les explications alternatives, comme une infection virale ou une usurpation d'identité.

Voici les méthodes fondamentales présentées dans vos sources pour démontrer cette intention :

1. S'appuyer sur des systèmes d'authentification centralisés

Pour simplifier la démonstration de l'intention des parties, l'enquêteur doit identifier en premier lieu tout système d'authentification centralisé en place (tels que **Active Directory, TACACS+ ou Radius**). Contrairement aux journaux d'une machine locale qui peuvent être modifiés ou peu fiables, l'authentification centralisée permet de **relier directement les actions réseau observées aux informations de connexion d'un compte utilisateur nominatif et unique**. Une fois cette liaison établie, l'enquêteur peut extraire l'historique de messagerie et d'activité web associé à ce compte pour caractériser l'intention.

2. Écarter l'hypothèse d'une infection par logiciel malveillant

Un suspect peut fréquemment se défendre en affirmant que les actions suspectes ou l'envoi de messages incriminés proviennent d'un logiciel malveillant installé à son insu. Pour prouver le caractère intentionnel, l'enquêteur doit mener des analyses afin de **démontrer soit la présence effective d'un logiciel malveillant (pour valider ou infirmer**

cette ligne de défense), soit que le comportement général de l'utilisateur était très probablement intentionnel et ne correspondait pas à une automatisation malveillante.

3. Corréler l'identité avec des connexions simultanées à des comptes personnels

Sur un réseau, les adresses IP peuvent changer et les adresses MAC peuvent être usurpées, ce qui permet à la défense de soutenir que l'activité suspecte a été réalisée par un autre utilisateur ayant obtenu l'adresse IP à ce moment-là. Pour prouver l'intention et l'attribution, l'enquêteur doit procéder à une **corrélation de données** : si les journaux réseau démontrent qu'une adresse IP s'est connectée à un compte de réseau social personnel appartenant au suspect au même instant précis où cette même adresse IP effectuait une action frauduleuse (comme le téléchargement d'un fichier sensible), **l'identité et l'intention du suspect deviennent extrêmement difficiles à contester.**

4. Exploiter les signatures numériques d'entreprise

La mise en œuvre de signatures numériques gérées de manière centralisée au sein de la messagerie d'entreprise offre une preuve d'attribution technique quasi irréfutable. La signature numérique (composée du nom, de l'adresse courriel, du certificat et de la clé publique de l'utilisateur) fait office de marque numérique unique d'entreprise. Si un courriel litigieux dispose d'une signature valide, **il est très difficile pour l'expéditeur de nier avoir délibérément signé et envoyé le message.**

5. Établir une chronologie cohérente des événements

L'analyse croisée des pare-feu applicatifs (comme Cisco Firepower), des serveurs proxy (comme Squid) et des historiques de messagerie sert à **reconstituer au mieux l'activité temporelle des utilisateurs (quand et où elle s'est produite).** Par exemple, si des données sensibles de l'entreprise sont supprimées volontairement par un employé immédiatement après avoir été contacté par les Ressources Humaines, cette séquence chronologique fournit un indice fort démontrant **l'intention de dissimuler des preuves ou de prendre la fuite pour transmettre ces données à un concurrent.**

Expliquez le risque de logiciel malveillant.

Dans le cadre de la criminalistique numérique et de la sécurité d'entreprise, le risque lié aux logiciels malveillants se manifeste sous plusieurs aspects critiques :

- **L'usurpation d'actions et la contestation de responsabilité :**
Un risque majeur est qu'un suspect utilise la présence (réelle ou supposée) d'un logiciel malveillant pour contester la paternité d'une activité frauduleuse ou de harcèlement. L'utilisateur peut ainsi affirmer que les communications incriminées (comme l'envoi de courriels) ont été générées automatiquement par un programme malveillant installé à son insu.
- **La dissimulation sous forme de logiciels potentiellement indésirables (PUP) :** Les logiciels malveillants se masquent fréquemment derrière des applications d'apparence légitime ou "utiles" installées volontairement par les utilisateurs (comme les outils *Hola!VPN* ou *DNS Unlocker* pour contourner la sécurité d'entreprise ou regarder du streaming). Ces programmes dissimulent des fonctions nuisibles qui s'exécutent en arrière-plan.
- **Le contournement des défenses traditionnelles :** Les solutions de sécurité standard, telles que les antivirus installés sur les postes de travail, échouent parfois à identifier ou à bloquer ces menaces et applications indésirables, les laissant agir librement sur le réseau.
- **La dégradation des performances et la consommation de ressources :** Ces programmes consomment silencieusement les ressources système et réseau, ce qui provoque des ralentissements extrêmes des machines affectées et génère un trafic non autorisé qui s'accapare la bande passante.
- **La propagation latérale au sein du réseau :** Certains logiciels malveillants ont la capacité de se propager d'un système à un autre. L'identification d'une infection isolée sur un poste de travail peut ainsi masquer une menace beaucoup plus large déjà répandue dans l'ensemble de l'organisation.
- **L'encapsulation et le chiffrement (Packing) :** Les auteurs de malwares compressent ou encapsulent souvent leurs fichiers afin de dissimuler leur structure interne. Ils utilisent également de

fausses extensions pour masquer le véritable type de fichier, rendant l'analyse statique et la détection très complexes sans décompression préalable.

- **La réinfection par le biais de vulnérabilités d'image système :**
Si une infection tire parti d'une faille de sécurité présente dans l'image système standard fournie par l'entreprise et déployée sur tous les postes, le simple formatage de l'ordinateur infecté (pratique courante mais insuffisante) ne résout pas le problème. Sans correction de la vulnérabilité à la racine, les systèmes seront réinfectés dès leur remise en service.

Comment décompresser un fichier encapsulé ?

Pour décompresser (ou « déballer ») un fichier encapsulé (*packed*), ce qui est particulièrement fréquent lors de l'analyse de logiciels malveillants dissimulés par leurs auteurs, vous devez suivre une méthodologie rigoureuse en plusieurs étapes :

1. Identifier la méthode de compression (Le Compresseur)

Un fichier encapsulé ne peut pas être analysé en détail tant qu'il n'a pas été décompressé. Pour y parvenir, il est indispensable de connaître la méthode ou l'outil d'encapsulation utilisé. Vous devez utiliser des outils d'analyse statique :

- **TrIDNET** : Cet outil permet d'analyser la structure interne de l'artefact pour identifier son véritable type de fichier (par exemple, s'il s'agit d'une archive auto-extractible dissimulée sous une fausse extension).
- **PEiD** : En l'équipant de sa base de signatures (userdb.txt), PEiD est particulièrement efficace pour détecter si un binaire est compressé et identifier le type exact de compresseur ou d'encapsulateur (*packer*) employé.

2. Isoler le fichier suspect

Toutes les manipulations d'un exécutable suspect doivent impérativement s'effectuer au sein d'un **environnement de test isolé (bac à sable / sandbox)**, comme un laboratoire Cuckoo Sandbox ou Cisco ThreatGrid, afin d'éviter tout risque d'infection accidentelle de vos systèmes de production.

3. Rendre l'extension visible et renommer le fichier

Les fichiers malveillants se font souvent passer pour des exécutables standard (.exe) alors qu'il s'agit d'archives d'encapsulation.

- Dans votre système de test (par exemple Windows), ouvrez les Options des dossiers et **décochez l'option « Masquer les extensions des fichiers dont le type est connu »**.
- Modifiez manuellement l'extension du fichier suspect pour appliquer son extension réelle découverte lors de la première étape (par exemple, **renommez le fichier de .exe en .rar** s'il s'est avéré être une archive RAR).

4. Extraire l'exécutable d'origine

- Utilisez un outil de décompression adapté au format identifié (comme **WinRAR** pour un fichier .rar) pour extraire le contenu de l'archive.
- Une fois l'extraction terminée, vous obtiendrez l'**exécutable malveillant d'origine non compressé**. Celui-ci est désormais prêt à être analysé de manière approfondie, que ce soit par le biais d'un examen statique de ses métadonnées et fonctions importées (avec un outil comme **PE Studio**) ou en observant son comportement dynamique lors de son exécution contrôlée dans le bac à sable.

 **La décompression n'est que la première étape : souhaitez-vous que je vous explique comment mener l'analyse statique de l'exécutable extrait à l'aide de PE Studio pour identifier ses indicateurs de menace ?**

Expliquer PE Studio

PE Studio est un outil gratuit extrêmement populaire et apprécié en criminalistique numérique, disponible au téléchargement sur le site www.winitor.com.

Conçu pour faciliter la tâche des enquêteurs grâce à son **interface graphique conviviale**, il sert de boîte à outils tout-en-un pour effectuer l'**analyse statique initiale d'un fichier suspect** (notamment un binaire ou un exécutable potentiellement malveillant). Sa grande force est de regrouper en une seule interface des fonctionnalités que l'on retrouve

habituellement dispersées dans plusieurs utilitaires distincts comme **TrIDNET** ou **PEiD**.

L'interface de PE Studio extrait et catégorise automatiquement une multitude de métadonnées et d'indicateurs cruciaux sans que l'enquêteur ait besoin d'exécuter le fichier :

1. Métadonnées générales et signatures de hachage

- **Empreintes numériques** : Il calcule instantanément les valeurs de hachage **MD5** et **SHA-1** du fichier, ainsi que l'**imphash** (hachage de la table d'importation, très utile pour identifier et corrélérer des familles de logiciels malveillants apparentées).
- **Entropie** : Il affiche le score d'entropie du fichier, un indicateur clé pour déterminer si le binaire est **chiffré, compressé ou encapsulé**.
- **Informations de compilation** : Il identifie l'architecture cible (ex. 32-bit ou 64-bit) ainsi que la date et l'heure exactes de compilation (*compiler-stamp*), ce qui permet d'établir une chronologie de création du fichier.

2. Structure interne du binaire (Format PE)

- **En-têtes de fichier** : Il décortique les structures de l'exécutable Windows, y compris le *dos-stub*, le *file-header* et l'*optional-header*.
- **Sections du binaire** : Il montre la répartition et les autorisations (lecture, écriture, exécution) des différentes sections du fichier (comme *.text*, *.data* ou *.rsrc*), aidant à repérer des anomalies structurelles typiques des malwares.

3. Analyse comportementale statique

- **Importations (imports)** : PE Studio dresse la liste de toutes les bibliothèques (*libraries*) et des fonctions système (API Windows) que le fichier appelle pour s'exécuter. Par exemple, si un fichier suspect importe des fonctions liées à la manipulation de fichiers, à des connexions réseau ou à l'injection de code, l'enquêteur peut immédiatement suspecter ses intentions.
- **Exportations (exports)** : Il répertorie les fonctions que le fichier met à disposition d'autres programmes ou DLL.
- **Ressources et Manifeste** : Il permet d'analyser les éléments intégrés au fichier (*resources*) et son manifeste Windows (*manifest*), qui gère notamment les privilèges d'exécution et les demandes d'élévation de droits.

4. Indicateurs de suspicion et renseignement sur les menaces

- **Chaînes de caractères (strings)** : Il extrait toutes les chaînes de texte brutes contenues dans le binaire (comme des commandes système, des chemins de fichiers, des adresses IP, des URL ou des messages textuels), ce qui constitue souvent une mine d'or pour comprendre le fonctionnement du programme.
- **Intégration de VirusTotal** : PE Studio interroge la base de données de **VirusTotal**. Pour les attaquants sophistiqués susceptibles de surveiller si leurs fichiers sont détectés sur des plateformes publiques, PE Studio permet d'envoyer uniquement les signatures de hachage sans téléverser le fichier complet, évitant ainsi d'éveiller leurs soupçons tout en obtenant l'analyse de détection des antivirus.
- **Indicateurs de menace** : L'outil met en évidence des alertes automatiques (*indicators*) basées sur des anomalies de structure ou des comportements suspects détectés statiquement, guidant rapidement l'enquêteur vers les éléments les plus critiques.

En résumé, PE Studio est la **première étape indispensable de l'analyse approfondie** d'un exécutable après sa décompression : il permet de dresser une carte d'identité technique extrêmement complète du fichier et de confirmer s'il s'agit d'une menace, le tout en quelques secondes et de manière totalement sécurisée puisqu'il n'y a aucune exécution de code.

⚙️ Maintenant que nous avons vu comment identifier et analyser statiquement un binaire avec PE Studio, aimeriez-vous que nous passions à l'étape suivante en simulant son exécution dynamique et comportementale au sein d'un bac à sable (sandbox) ?

Simuler une sandbox

Étape 1 : Préparation de l'échantillon et initialisation de l'environnement de test

Avant de lancer la simulation, le fichier suspect identifié comme une archive auto-extractible WinRAR masquée est isolé dans notre laboratoire **Cuckoo Sandbox** ou **Cisco ThreatGrid**. Dans les options d'affichage de notre machine Windows de test, l'option « **Masquer les extensions des fichiers dont le type est connu** » est **désactivée**.

L'extension du fichier suspect est ensuite modifiée manuellement de **.exe en .rar** afin de pouvoir en extraire l'exécutable malveillant d'origine prêt pour l'analyse comportementale dynamique.

Étape 2 : Lancement et analyse comportementale dynamique (La Simulation)

Lorsque le binaire extrait est exécuté dans l'environnement virtuel et hermétique de la sandbox, nous observons en temps réel la séquence d'infection suivante :

1. **Exécution et chiffrement silencieux** : Le programme démarre silencieusement en arrière-plan sans comportement visible immédiat pour l'utilisateur afin de ne pas éveiller de soupçons. La sandbox détecte instantanément que le processus accède de manière intensive au disque dur : il commence à parcourir et à chiffrer les fichiers de l'utilisateur (photos, vidéos, documents) situés dans les répertoires clés comme My Documents.
2. **Apparition de l'écran de rançon** : Quelques secondes plus tard, une fenêtre rouge vif intitulée **Cryptolocker-v3** s'ouvre brusquement à l'écran, bloquant l'accès au reste du bureau.
3. **Le message d'extorsion** : Le message affiché en lettres blanches et jaunes indique : « **Your personal files are encrypted!** ». Le logiciel malveillant avertit l'utilisateur que ses fichiers ont été chiffrés à l'aide d'une **clé publique RSA-2048** générée spécifiquement pour son ordinateur et que l'unique copie de la clé privée se trouve sur un serveur secret sur Internet, qui la détruira après un délai de décompte spécifié dans la fenêtre.

Étape 3 : Rapport d'analyse et indicateurs de compromission (Cisco ThreatGrid)

L'environnement d'analyse automatisé de la sandbox capture l'ensemble des modifications système et des flux réseau générés par l'infection :

- **Activité réseau et exfiltration (Réseau Tor)** : La sandbox intercepte des requêtes de communication sortantes via le protocole réseau. La sandbox enregistre les liens d'accès de déchiffrement suivants pointant vers le réseau anonyme Tor :
 - L'adresse Tor directe : **34r6hq26q2h4jkzj.onion**.
 - Le site miroir d'accès web classique :
<https://34r6hq26q2h4jkzj.tor2web.fi>.

- **Adresse de paiement Bitcoin** : La sandbox extrait de l'analyse mémoire l'adresse de portefeuille unique vers laquelle la victime doit envoyer les fonds pour espérer récupérer ses fichiers : **1G8vxA8QoBdbQzuUiyDhcwiakSUKDKNoY**.
- **Traces de persistance et de sabotage** : L'outil de test signale que le logiciel malveillant a modifié les configurations de démarrage de Windows pour se lancer automatiquement à chaque session et qu'il affiche un avertissement de sécurité strict : **toute tentative de modification ou de suppression de ce logiciel entraînera la destruction immédiate de la clé privée** sur le serveur distant.