LECON 0 : INTRODUCTION A L'INVESTIGATION NUMERIQUE

Dans ce cours il s'agira de **Forensic** où vous apprendrez à investiguer un incident de sécurité sur Windows. Au travers d'exercices pratiques et d'exploration des différents outils, vous découvrirez l'univers de **l'investigation numérique**, et comment **mener votre investigation**. L'investigation numérique est un **sujet vaste** qui nécessite des années d'apprentissage et de pratique pour comprendre en détail le fonctionnement d'un système d'exploitation, et en extraire les bonnes informations. Ce cours n'a donc pas la prétention d'être exhaustif, mais il a pour but de vous rendre **opérationnel** pour mener une investigation numérique, et de vous fournir les éléments pour **approfondir vos connaissances**. Vous découvrirez donc ce qu'est le **Forensic**, et **comment réaliser une investigation** de base pour répondre à un incident de sécurité. Ce cours est divisé en **5 parties** qui introduiront des concepts de **Forensic** pour vous permettre de réaliser une investigation.

Dans la **Partie 1,** nous allons définir le **Forensic** et quels sont les **objectifs** d'une investigation. Vous découvrirez la **méthodologie** utilisée ainsi que les **outils** qui vous permettront de collecter les données et de les analyser. Enfin, vous apprendrez à réaliser des images (aussi appelées ***dump***) d'un disque dur et de la mémoire RAM.

Dans la **partie 2,** elle sera orientée sur l'analyse de la **mémoire volatile**, ou **mémoire vive** (aussi appelée *RAM*). Nous verrons brièvement comment fonctionne la mémoire vive sur un système Windows, et découvrirons les différents fichiers de mémoires systèmes. Vous apprendrez à utiliser le framework open source **Volatility** pour parser les données présentes dans le dump et extraire les informations pertinentes, telles que la liste des **processus**, ou encore les **connexions réseau**.

Dans la **Partie 3**, vous découvrirez les spécificités du système de fichier **NTFS** utilisé sur les systèmes **Windows**. Vous apprendrez à **extraire les informations** du système pour les analyser, et vous verrez comment réaliser une **chronologie des événements** du système infecté. Vous serez capable de reconnaître les **artefacts** pour l'investigation, c'est-à-dire les éléments importants à prendre en compte. Enfin, vous apprendrez à analyser le registre, les events logs, et comment récupérer les fichiers effacés.

Dans la **partie 4**, vous découvrirez ce qu'est un **vecteur d'infection** et comment ils peuvent être utilisés par un attaquant pour compromettre une machine. Vous apprendrez à analyser un **email**, un **fichier PDF** ou encore un **document Word**.

La rédaction du rapport lors d'un incident de sécurité est capital. Dans la **Partie 5**, vous apprendrez à créer un **rapport d'investigation** en ajoutant les détails de votre analyse, ainsi que le partage des **indicateurs de compromission** (IOC).

1. Windows, première cible des attaques

L'investigation numérique est un domaine vaste et nécessite des années de pratique. Un incident de sécurité peut survenir sur **n'importe quel type de système** : Windows, Linux, Mac, Android, iOS… Il existe

des malwares pour toute ces plateformes. Beaucoup de personne pensent à tort que les **Mac** ne peuvent pas être infectés par un logiciel malveillant**. C'est totalement faux !** Ils sont de plus en plus la cible de pirates.
Il existe toutefois une différence notoire : un malware destiné à infecter un système Windows **ne pourra pas infecter un système MacOS**, et vice-versa. Les systèmes **Windows** sont les **plus répandus en entreprise**, voilà pourquoi ce cours se focalise sur l'investigation sur Windows. Il y a plus de chance que vous soyez confronté à une infection sur un OS Windows que sur Mac, même si ça peut arriver. Par ailleurs, connaître un système tel que celui de Windows en profondeur nécessite du temps, et étant donné que ce cours ne traite pas en profondeur le système Windows, il aurait été difficile de traiter les autres OS.

2. Activité préliminaire

Tout au long de ce cours, vous allez suivre une **méthodologie d'investigation** définie. Pour planter le décor et suivre un fil directeur, vous allez vous mettre dans la peau d'un analyste pour **analyser un système compromis**.

Un utilisateur du **service comptabilité** de votre entreprise a reçu un email contenant une **pièce jointe**. Sans faire attention, l'utilisateur l'a ouverte, pensant qu'elle était légitime. Réalisant son erreur en se rendant compte que l'email émetteur n'était pas légitime, il a directement appelé la direction de la sécurité des systèmes d'information, dont vous faites partie, pour réaliser **l'investigation**. En tant qu'analyste, pour réaliserez un **dump mémoire** ainsi qu'une **copie bit à bit du disque dur**, pour pouvoir collecter un maximum d'informations. Vous réaliserez une analyse du poste infecté et reporterez l'investigation dans votre **rapport**. Vous identifierez les **IOC (Indicateurs de Compromission)** et proposerez des **plans d'action** pour contenir la menace et l'éradiquer. Enfin, vous proposerez des **recommandations** pour améliorer la sécurité de votre entreprise et la prémunir d'attaques similaires. Tout au long de ce cours, il sera question que vous appreniez à faire toutes ces démarches par vous-même.

PARTIE 1 : PREPARER UNE INVESTIGATION NUMERIQUE

LECON 1 : LA NOTION D'INVESTIGATION NUMERIQUE

Dans cette partie, nous allons définir **l'investigation numérique, ou *Forensic***, ainsi que l'intérêt de réaliser une investigation lors d'un incident. Nous aborderons brièvement les **enjeux juridiques**, pour finalement terminer sur la **méthodologie d'investigation**.

1.1. Définition de l'investigation numérique et les objectifs de son utilisation en entreprise

Le terme « **Forensic** » est fortement associé au domaine scientifique et notamment à la **médecine légale**. En informatique, on parle de ***digital Forensic***, c'est-à-dire l'analyse d'un ordinateur pour comprendre les évènements passés et en extraire des conclusions. L'**investigation numérique**, ou *digital* ***Forensic***, consiste à utiliser des techniques spécialisées dans la **recherche**, la **collecte** et **l'analyse de données** issues de supports numériques.

Elle peut également être utilisée dans le cadre **d'enquêtes judiciaires**. Lorsque des supports numériques sont impliqués dans un crime ; c'est notamment le cas lors de perquisitions liées à des actes de cybercriminalité, par exemple. Toutefois, cette investigation devra être réalisée par un **expert judiciaire** et nécessite d'être assermentée, pour que les preuves puissent être recevables. Par ailleurs, la collecte de preuves devra respecter des besoins spécifiques. Par exemple, il faudra utiliser un **bloqueur en écriture** lors de la copie, ou lors de l'accès au disque compromis. Il est également possible de réaliser une investigation numérique en laboratoire, par exemple pour **étudier le fonctionnement d'un logiciel malveillant**. Ainsi, on peut schématiquement diviser l'investigation numérique en trois activités distinctes :

- **L'analyse Forensic judiciaire** : Principalement utilisée dans le cadre d'enquêtes judiciaires, elle a pour but de rechercher toutes les preuves numériques (par exemple lors d'une perquisition), afin de collecter et rassembler un maximum de preuves pouvant incriminer ou innocenter le suspect d'une enquête.
- **L'analyse Forensic en réponse à un incident** : Elle vise à identifier les **conditions** et les **origines** d'une attaque informatique, quelles sont les machines infectées ou encore par quel **vecteur l'attaque** est survenue. Dans le cas d'une réponse à une intrusion, elle joue le rôle de « pompier » et permet d'identifier rapidement les éléments du système d'information compromis, dans le but de combler les failles et d'éradiquer le ou les malwares.
- L'analyse Forensic scientifique : Elle consiste à étudier les mécanismes et les aspects techniques d'un malware ou autre logiciel/matériel malveillant, afin d'identifier les méthodes utilisées par les attaquants pour pénétrer et compromettre un réseau informatique. Les analyses sont souvent réalisées dans un **environnement maîtrisé** (appelé ***sandbox***).

Il existe différents objectifs pour réaliser une investigation numérique. **Dans le cadre de notre cours**, nous nous concentrerons sur l'investigation numérique lors de **la réponse sur incident**.

Les attaquants d'aujourd'hui rivalisent d'ingéniosité pour pirater des entreprises et **voler des informations sensibles**. Il existe tout un tas de menaces et de techniques. Pour pouvoir les contrer efficacement et améliorer la sécurité d'une entreprise, il est nécessaire de comprendre les techniques utilisées

par les attaquants. Lorsqu'une entreprise est compromise en raison d'une attaque informatique, les dégâts peuvent avoir de multiples impacts :

- Sur **l'image de la société**, si l'attaque devient publique ;
- **Opérationnel** direct, en mettant hors service des infrastructures ;
- **Financier**, si des fuites de données ou des versements frauduleux ont été effectué ;
- **Géopolitique** ou **économique**.

En 2017 par exemple, le malware **NotPetya** a impacté plusieurs multinationales en mettant **hors service** des centaines de milliers de machines en l'espace d'une dizaine de minutes. Causant pour certaines d'entre elles plus de **300 millions d'euros** de pertes.

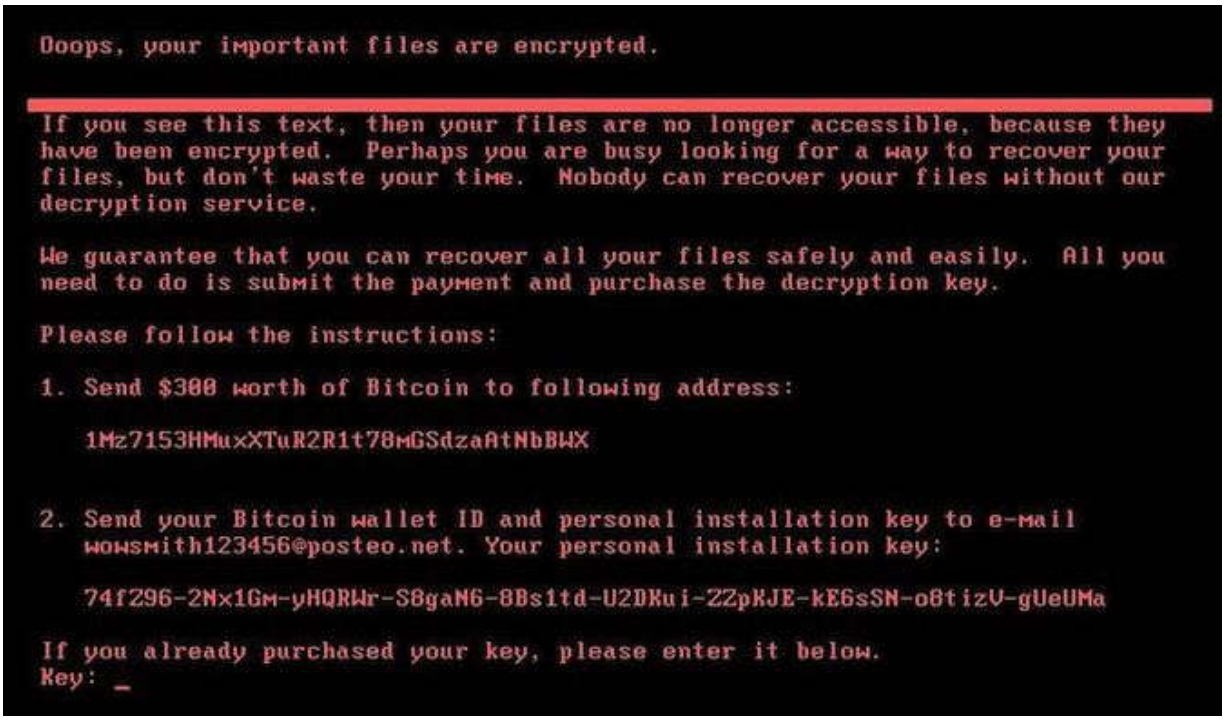

Figure 1.1. Description du message envoyé par le Malware NotPetya

Pour pouvoir comprendre d'où vient une attaque et quel a été le mode opératoire, il est nécessaire de réaliser des **investigations**. Par ailleurs dans certains cas, ces investigations permettront d'obtenir des dommages et intérêts auprès des assurances.

1.2. La Méthodologie d'investigation

Sur le terrain, vous serez parfois amené à travailler dans des situations extrêmement tendues et critiques ; vous devrez alors faire preuve de **sang-froid**. Pour réaliser une investigation, il est nécessaire de suivre une **méthodologie**. Dans certaines situations, l'analyste peut être perçu comme un contrôleur qui est à la recherche d'une personne qui a commis une faute. Ce n'est pas du tout le cas, vous êtes sur les lieux pour réaliser une **analyse factuelle** et en aucun cas vous ne devez apporter un **jugement de valeur**. Par ailleurs, il se peut que vous soyez confronté à des situations où les informations qu'on vous communiquera seront volontairement camouflées ou dissimulées. Ces éléments pourront être mentionnés dans votre rapport. La méthodologie recommandée de suivre et que nous allons appliquer dans ce cours est basée sur **04 étapes** à savoir **:**

- **Étape 1 : Identifiez le contexte et récupérez les informations : L'identification du contexte** est une phase très importante, car elle permet d'**obtenir des informations** liées à l'incident de sécurité. Lors de cette phase, vous devrez rencontrer diverses personnes telles que les personnes de l'IT, les **administrateurs**, les **responsables des machines infectées ou encore le RSSI**. Ceci vous permettra d'orienter vos recherches pour ne pas faire fausse route.
- **Étape 2 : Collectez les supports numériques à analyser :** Vous avez précédemment identifié le **contexte de l'attaque** et également des **machines potentiellement compromises**. La **phase de collecte** va permettre de copier les données pour pouvoir les analyser (copie de la mémoire vive, et copie du disque dur). Vous réaliserez des **hashs** des informations collectées. Cela permettra de réaliser l'analyse sur la copie sans altérer les données originales. Lors d'une analyse **Forensic**, il est primordial de calculer une **empreinte** (hash) qui identifiera le fichier à l'aide d'une **fonction de hachage**. Cette empreinte doit être unique, car elle permet de valider que le fichier n'a pas été **altéré durant l'investigation**. Le calcul des hash permettra ainsi de garantir **l'intégrité** des fichiers analysés. Il existe plusieurs algorithmes de hachage, tels que MD5, SHA1, SHA2, SHA5… À noter que les algorithmes MD5 et SHA1 comportent des faiblesses de collision (c'est-à-dire le même hash pour deux fichiers différents), et sont de moins en moins utilisés.
- **Étape 3 : Analysez les données collectées :** Après avoir collecté les données, il faut maintenant les analyser. C'est la phase la plus technique de l'investigation. Dans cette phase, vous réaliserez la **chronologie** des évènements pour extraire la date et le moment précis de l'incident, ainsi que l'analyse des **artefacts** tels que les processus, le registre et le réseau. Une phase de **triage** sera également réalisée. Nous découperons cette phase en 3 étapes :

1. L'analyse du dump mémoire, c'est-à-dire de la RAM de l'ordinateur — *nous verrons cette étape dans la **partie 2 de ce cours**.*
2. L'analyse du disque dur de l'ordinateur et de tous les fichiers qu'il contient — *nous verrons cette étape dans la **partie 3 de ce cours**.*
3. L'analyse des fichiers identifiés comme suspects ou malveillants — *nous verrons cette étape dans la **partie 4 de ce cours**.*

- **Étape 4 : Corrélation et reporting :** Dans cette phase, vous présenterez dans un **rapport** le résultat de vos analyses. Vous présenterez de manière factuelle les éléments découverts. Vous indiquerez également les **indicateurs de compromission** et les **recommandations** à mettre en place pour améliorer la sécurité de l'entreprise. *Cette étape sera vue dans la **partie 5 de ce cours**.*

Un **indicateur de compromission** est un élément unique et qui permet de caractériser et d'identifier les éléments d'une attaque. Cela peut être : les hash de fichier ou logiciel malveillant ; des adresses IP ; des clés de registre ; des emplacements sur le disque ; une adresse email ; une adresse de portefeuille de cryptomonnaie (pour une rançon, par exemple) ; un mutex.

LECON 2 : CHOIX DES OUTILS CORRESPONDANTS AUX BESOINS DU FORENSIC

L'analyse Forensic nécessite de respecter des bonnes pratiques en utilisant les outils adéquats. Il existe une multitude **d'outils open source, freeware ou propriétaires**, permettant d'analyser des supports numériques. Dans certains cas et notamment lors d'enquêtes judiciaires, il sera également nécessaire d'utiliser du matériel tel que des bloqueurs en écriture lors de la collecte de données. Dans cette leçon, nous allons étudier et parcourir quelques outils qui vous permettront de réaliser une analyse **Forensic**. Nous verrons principalement des outils open source ou gratuits. Toutefois, **notez qu'il n'y a pas de « meilleur outil »**. C'est à vous de vous familiariser avec l'utilisation de ces utilitaires pour en **comprendre les limites** et **adapter les utilisations en fonction des besoins.** Par ailleurs, dans certaines situations, il pourra être nécessaire de développer vos propres **scripts d'analyse**.

2.1. Choisissez l'outil adapté à vos besoins

Pour réaliser une analyse **Forensic** de support numérique, il existe sur le marché des outils reconnus. La société Guidance Software propose une suite d'utilitaires appelée Encase dédiée à l'analyse **Forensic**, en passant de **l'analyse du disque et au tri des données** jusqu'à **l'analyse des fichiers et le déchiffrement des volumes analysés**. Les licences sont payantes et restent relativement chères. Toutefois, ce genre d'outil est largement utilisé par les experts judiciaires ou encore les organismes de police. Il existe également des **outils hardware permettant la collecte de supports numériques** sans altération des données, tels que des bloqueurs en écriture que nous avons évoqués plus haut. Les bloqueurs en écriture sont donc des dispositifs qui permettent de faire **l'acquisition d'une image d'un disque dur en bloquant le mécanisme d'écriture**, mais pas de lecture, dans le but de préserver le contenu. L'utilisation de ce type de dispositif permet de protéger le contenu du disque et **garantit ainsi son intégrité**. La figure 2.1 présente un exemple de bloqueur en écriture, connecté à un disque dur pour copier ses données sans qu'elles soient altérées.

Figure 2.1 : Exemple d'un bloqueur en écriture

Un bloqueur en écriture matériel **s'interpose entre le disque dur (la preuve) et le PC** qui servira à l'acquisition de l'image. Il existe également des bloqueurs en écriture **logiciels**. Il existe également des utilitaires gratuits ou open source qui sont très souvent utilisés lors d'analyses **Forensic**. Le framework The Sleuth Kit permet de réaliser une analyse **Forensic** en passant de la **génération d'une timeline au triage des données** et à **l'analyse des artefacts Windows (registre, email, historique…)**, jusqu'à la génération d'un rapport. Il comporte une interface graphique appelée **Autopsy**.

Les utilitaires NirSoft ou encore la suite Sysinternal de Microsoft sont également utilisés dans l'analyse **Forensic**. Google a également développé son propre framework d'analyse, Google Rapid Response (GRR), qui permet de faire de l'analyse **Forensic** à distance de postes compromis.

Certains projets proposent également des **OS Linux destinés à l'analyse Forensic** et embarquant des outils préinstallés tels que SIFT, Tsurugi, CAINE ou encore DEFT.

Pour l'analyse de la **mémoire vive**, il existe également des frameworks tels que Volatility et Rekall.

Pour la **copie des disques durs et de la RAM**, il est possible d'utiliser le freeware **FTK Imager Lite**.

Nous reviendrons en détail sur ces outils tout au long de ce cours.

2.2. Préparer son environnement d'analyse

Nous allons à présent **préparer notre environnement d'analyse**. Dans ce cours, nous utiliserons **2 machines virtuelles** pour réaliser les investigations. Cela vous permettra d'appréhender des outils sur les différentes plateformes.

1. Une **VM Windows** sur laquelle il faudra installer les outils The Sleuth Kit Autopsy, FTK Imager et Mft2Csv. Il est conseillé de télécharger les différents utilitaires et de les copier dans un répertoire pour les avoir au même endroit. N'hésitez pas non plus à **réaliser un snapshot de vos machines virtuelles** une fois configurées.
2. Une **VM Linux SIFT** que vous pouvez télécharger à cette adresse (puis suivez les instructions d'installation).

Il faut aussi se Méfier de ce que disent les outils ; lors de votre analyse, il peut s'avérer que les résultats des outils que vous utilisez **ne soient pas toujours fiables ou ne soit pas corrects**. Il faudra alors investiguer pourquoi cela ne fonctionne pas correctement, et parfois aller jusqu'à **développer vos propres utilitaires**. Attention, ce n'est pas parce que vous ne trouvez pas de traces d'activité qu'aucune activité n'a eu lieu. Les attaquants utilisent des techniques d'**anti-Forensic** qui permettent de contourner les techniques d'analyse en **masquant leurs traces**, tout en **dissimulant ou en protégeant des données**. Ces techniques **peuvent ralentir votre travail** il s'agit par exemple de la **stéganographie**, qui permet de dissimuler des informations en **masquant un message dans un conteneur anodin**, une photo par exemple, de manière à le rendre invisible pour un individu qui n'est pas concerné par le message, et de le transmettre en toute discrétion. **Le malware Duqu**, par exemple, fut l'un des premiers à utiliser ce genre de techniques pour **exfiltrer des données volées** en les cachant dans des fichiers JPEG.

Certains attaquants vont effacer des données du disque dur ou encore falsifier les **timestamps**. Un attaquant ou un utilisateur malveillant pourra **couvrir ses traces en falsifiant les attributs d'accès aux fichiers.** Les outils comme Timestomp, dont le but est de modifier les attributs des fichiers, sont capables de réécrire les dates d'accès des systèmes de fichiers NTFS (date de création, modification, accès, etc.).
L'investigation **Forensic** nécessite l'analyse et la corrélation de multiples sources. Si vous avez un doute sur un élément, il faudra confirmer ou infirmer via l'analyse d'un autre artefact.

Lorsque vous utilisez un outil d'analyse **Forensic**, assurez-vous de bien comprendre de quoi il s'agit quand vous utilisez un outil. Vérifiez que vous connaissez ses **limites** et sa **fiabilité**. S'il s'agit d'un nouvel outil, renseignez-vous sur **la documentation officielle de l'outil**, mais aussi auprès d'**experts** qui l'ont déjà utilisé, ainsi que sur des sites comparatifs.

LECON 3 : COLLECTEZ LES INFORMATIONS DE BASE POUR L'INVESTIGATION

Dans les leçons précédentes, nous venons de découvrir **les principes et les concepts de l'investigation numérique**. Nous avons également introduit quelques outils utilisés. Dans cette leçon, nous allons à présent passer à la **première phase de l'investigation : la collecte des informations à analyser**.

3.1. Les formats de collecte de données

La phase de **collecte des données**, ou encore **« l'acquisition »**, est la phase qui doit permettre de **copier les données volatiles et non volatiles sur un support externe**, dans le but de réaliser une **analyse approfondie** par la suite. Cette phase est très importante, car elle nécessite de respecter une procédure stricte qui **n'altérera pas les données stockées**. Les données collectées seront stockées dans un container que l'on appelle ***image***. Une image est un **dump brut extrait d'un support numérique**. Il existe plusieurs formats d'image.

- **Les images RAW :** Les images brutes, au format RAW, ne sont pas un format en soi, mais un **bloc de données brutes** reproduites à partir d'une image. Les images brutes ne contiennent aucune métadonnée supplémentaire en dehors des informations sur le fichier image lui-même (nom, taille, horodatage et autres informations).
- **Les formats de Forensic :** Plusieurs problèmes avec les images brutes ont conduit à la création de formats de fichiers pour le **Forensic**. Les formats de **Forensic** comportent des éléments supplémentaires tels que l'horodatage, les hashs des images et d'autres **métadonnées**. Par ailleurs, il peut être nécessaire de compresser ou chiffrer une image acquise. Les formats de **Forensic** facilitent la mise en œuvre de ces fonctionnalités. Vous retrouverez entre autres :
  - **EnCase EWF**, développé par **Guidance Software**, l'une des plus anciennes **entreprises de logiciels de Forensic**. Il utilise le format EWF (*Expert Witness Format*) qui prend en charge les métadonnées, la compression, le chiffrement, le hachage, etc. ;
  - **FTK Smart**, par **AccessData**, est un concurrent direct d'EnCase EWF. Ce **format propriétaire** inclut également les métadonnées, la compression, le chiffrement, le hachage, etc. ;
  - **AFF**, pour *Advanced **Forensic** Format*, a été créé par **Simson Garfinkel** en tant que **format ouvert**. Il comprend toutes les fonctionnalités attendues et inclut également des fonctionnalités de chiffrement et de signature utilisant des certificats X.509 standard.

3.2. Différence entre mémoire volatile et non volatile

La **mémoire non volatile** est issue d'un support numérique qui conserve les données présentes même lorsqu'il n'est pas alimenté électriquement, comme un disque dur ou une clé USB. Ce type de mémoire autorise l'analyse dite à froid, ou post mortem, c'est-à-dire après l'incident et une fois que le système a été éteint.

La **mémoire volatile**, elle, est une mémoire informatique qui a besoin d'alimentation électrique continue pour conserver l'information qui y est enregistrée. Lorsque l'alimentation électrique est interrompue, l'information contenue dans la mémoire volatile est, quasi immédiatement, perdue. Dans notre cas, on parle

de la **RAM**, ou de la **mémoire vive**. Ce type de mémoire doit obligatoirement être enregistré (**dumpé**) sur un support externe à chaud, c'est-à-dire avant extinction de l'ordinateur, sinon tout sera perdu. Sans ça, vous ne pourrez pas l'analyser pour mener votre investigation. La mémoire vive d'un ordinateur peut contenir de nombreuses informations : mots de passe, identifiants, clefs de chiffrement ou encore processus actifs. Elle est donc très utile pour l'analyse Forensic.

3.3. Réalisez un dump mémoire et une copie bit à bit d'un disque dur

Dans le processus de **Forensic**, il faut dans un premier temps **collecter les données qui seront analysées** par la suite. Dans la réalité, il se peut que vous ayez accès à la machine en cours de fonctionnement ; dans ce cas il faudra réaliser dans un premier temps un **dump de la RAM** pour collecter un instantané des processus en cours d'exécution. Cela vous permettra d'identifier un processus malveillant, par exemple. Puis il faudra par la suite réaliser **la copie bit à bit du disque dur**, c'est-à-dire une **copie fidèle de chaque bit du disque**. Cela vous permettra d'accéder à toutes les données du disque pour réaliser l'analyse. Chaque cas est différent, il se peut que les copies soient déjà réalisées, ou alors que l'on vous transmette uniquement le disque dur. C'est à vous de vous adapter à la situation pour réaliser au mieux l'analyse. Dans cette section, nous allons effectuer le **dump du contenu de la RAM et du disque dur**.

3.4. Acquisition de la mémoire volatile

L'acquisition de la mémoire vive intervient généralement lors d'une réponse à incident et **sur un système en fonctionnement**. Lors de l'acquisition, l'analyste **doit éviter au maximum toutes modifications, afin de récupérer une image fidèle du système à analyser**. Il existe une multitude d'outils pour dumper le contenu de la RAM. Nous allons ici utiliser le logiciel free FTK imager, téléchargeable à cette adresse. Libre à vous d'utiliser un autre outil ; par exemple, l'utilitaire free **Dumpit** est une référence dans l'acquisition de la mémoire volatile. Avec le logiciel FTK, il suffit de **cliquer sur l'icône RAM** pour réaliser la capture. Il faudra ensuite préciser le répertoire où le dump sera stocké, puis cliquer sur *Capture Memory* ; il est également possible d'inclure le fichier système **pagefile.sys** à la copie. La copie du dump est ensuite réalisée et stockée dans le répertoire mentionné. Nous réaliserons dans la partie suivante l'analyse de ce dump.

3.5. Acquisition de la mémoire non volatile

Comme pour la mémoire volatile, l'acquisition de la mémoire non volatile est une partie très importante de l'investigation numérique ; elle doit respecter une procédure stricte, afin de ne pas altérer le contenu du support. De nombreux outils ont pour but de copier le contenu d'un disque dur pour l'analyser. **Nous allons ici utiliser le logiciel FTK**. Pour ce faire, il suffit de cliquer sur l'icône **Create Image**, puis sélectionner la source de la copie à réaliser, ici le disque dur **Physical Drive** de notre machine. S'il existe plusieurs disques durs ou des partitions, il faudra sélectionner celui que l'on souhaite copier, puis cliquer sur **Finish**. Il faudra ensuite cliquer sur Add pour sélectionner le **format** de l'image. Ici nous choisirons le format **Raw**, mais vous pouvez utiliser le format que vous désirez. Il faudra ensuite spécifier quelques informations qui permettront d'identifier la preuve collectée. Enfin, il faudra sélectionner le répertoire dans

lequel le disque sera copié. Il faudra stocker cette image **sur un support amovible externe suffisamment grand**. Dans la plupart des cas, les dumps que vous devrez réaliser feront **plusieurs centaines de Go**, il faudra par conséquence utiliser des disques durs externes de **plusieurs téraoctets pour stocker ces données**. Il faudra ensuite cliquer sur **S*tart*** pour réaliser la copie du disque dur. Le temps nécessaire à la copie du disque sera fonction de la taille du disque.

3.6. Calculez l'empreinte (hash) des dumps réalisés

Lors d'une analyse **Forensic**, il est primordial de calculer une empreinte qui identifiera le fichier à l'aide d'une fonction de hachage. Cette empreinte doit être unique, car elle permet de valider que le fichier n'a pas été altèré durant l'investigation. **Le calcul de condensat ou le hachage** permettra ainsi de garantir **l'intégrité des fichiers analysés**. Le calcul de hash s'effectuera directement après l'acquisition des données. Voici les fonctions de hachage les plus utilisées :

- MD5 (*Message Digest*) : hash de 128 bits ;
- SHA1 (*Secure Hash Algorithm*) : hash de 160 bits ;
- SHA224 : hash de 224 bits, communément appelé SHA2 ;
- SHA256 : hash de 256 bits, communément appelé SHA2 ;
- SHA384 : hash de 384 bits ;
- SHA512 : hash de 512 bits.

Sous Linux, il est possible d'utiliser les fonctions de hachage simplement :

```
md5sum memdump.mem
382e0a06865ddcf5aee46aa414fa011b  memdump.mem
sha256sum memdump.mem
e35a660421752b58989ee575566ff42a7c16ed3c9869a69dbce0bc23405d3a7c  memdump.mem
sha512sum memdump.mem
fec5c420fdf5633887e5f2095ed52ea066fded881245d263c13cfc8f2a08990bb62ef62296a6c5c42cfcd1b0e16b33dc9f5d
498fa3695260e3800cbd9d132e7e  memdump.mem
```

Les indicateurs de compromission permettent d'identifier des éléments d'une attaque pour **pouvoir identifier d'autres compromissions**. Nous verrons en détail cette partie dans la dernière leçon.