Forensic

m2iformation.fr

Sommaire Partie 1

Méthodologie d'investigation

La **méthodologie d'investigation légale** dans le domaine de l'informatique forensique consiste en une série de procédures structurées et standardisées pour collecter, analyser et présenter des données provenant de systèmes informatiques, de manière à ce que ces informations soient reconnues comme des preuves valides dans un cadre juridique.

1. Audit préalable :

- Avant de commencer une enquête, il est essentiel de réaliser un audit préalable pour comprendre l'environnement et les systèmes impliqués. Cela inclut l'évaluation des mesures de sécurité existantes, la cartographie du réseau, et la détermination des rôles et des accès des utilisateurs impliqués.

2. Enregistrements des preuves (Chain of Custody) :

- La "Chain of Custody" (chaîne de conservation) est essentielle pour maintenir l'intégrité des preuves. Elle documente la collecte, le transport, la conservation, et la manipulation des preuves pour prouver qu'elles n'ont pas été altérées ou compromises. Chaque interaction avec la preuve doit être enregistrée.

3. Collecte des preuves :

- La collecte des preuves doit être effectuée de manière méthodique pour s'assurer que les données ne sont pas corrompues ou modifiées pendant le processus. Cela comprend l'utilisation de techniques telles que l'imagerie disque en mode lecture seule et la collecte de données volatiles.

Méthodologie d'investigation

4. Matériels d'investigation :

- Le matériel d'investigation inclut des dispositifs spécialisés comme les write blockers qui permettent de copier des informations d'un disque dur sans écrire de données dessus, préservant ainsi l'état original des données.

5. Logiciels d'investigation :

- Les logiciels d'investigation comprennent des outils comme EnCase, FTK, ou Autopsy, qui aident à analyser les disques durs, récupérer des fichiers supprimés, et examiner les fichiers système et les logs.

6. Protection de la collecte :

- Protéger les données collectées est crucial pour prévenir toute altération. Cela inclut des mesures de sécurité physiques et numériques, telles que le chiffrement des données et la sécurisation des lieux où les données et les matériels sont stockés.

7. Calculs des empreintes de fichiers :

- Les empreintes de fichiers, ou hash, sont utilisées pour vérifier l'intégrité des données. Si le fichier est modifié, même légèrement, l'empreinte sera différente.

8. Rédaction du rapport :

- Le rapport d'investigation doit documenter minutieusement tous les processus et découvertes de l'enquête. Il doit être compréhensible pour les non-experts, tout en incluant les détails techniques nécessaires pour les procédures judiciaires. Le rapport doit également inclure un résumé des preuves, la méthode de collecte, les analyses effectuées, et les conclusions.

Dead Forensic (Forensique à froid)

La dead forensic se réfère à l'analyse des systèmes qui ne sont pas en fonctionnement actif. Cette méthode est traditionnellement utilisée pour examiner des dispositifs après qu'ils ont été éteints, ce qui permet une approche plus minutieuse sans le risque de modifier les données par des opérations en cours.

Caractéristiques principales :

- **Analyse hors ligne** : L'analyse se fait sur des systèmes éteints ou sur des images disque qui ont été préalablement créées à partir de systèmes opérationnels.
- **Préservation des données** : Comme le système est éteint, les données ne sont pas sujettes à des modifications dues à des processus système ou à des activités d'utilisateur, ce qui peut aider à préserver l'intégrité des preuves.
- **Enquête approfondie** : Permet une analyse détaillée des disques durs, des mémoires de stockage, et d'autres supports sans le risque d'interférence par des processus ou des connexions réseau actives.
- **Utilisation d'outils forensiques standard** : Des outils comme EnCase, FTK (Forensic Toolkit), et Autopsy sont typiquement utilisés pour réaliser une analyse post-mortem.

Exemples d'utilisation de la Dead Forensic

1. **Enquête criminelle** : Après la saisie d'un ordinateur lors d'une perquisition, les enquêteurs créeront une image forensique du disque dur pour une analyse approfondie sans risquer de modifier les données.
2. **Analyse de malwares** : L'examen d'un système infecté par un malware peut être effectué en toute sécurité sur une image du disque dur, permettant aux analystes de déterminer comment le malware a pénétré le système et quelles modifications il a apportées.
3. **Récupération de données** : La récupération de fichiers supprimés ou endommagés est souvent réalisée via une analyse post-mortem, en utilisant des outils spécialisés pour fouiller profondément dans les structures de données du disque.

Forensic Windows

L'investigation forensique sur les systèmes Windows implique l'analyse détaillée de divers aspects du système d'exploitation, des systèmes de fichiers aux artefacts laissés par les applications.

1. Analyse des systèmes de fichiers: Les systèmes de fichiers structurent la manière dont les données sont stockées et récupérées sur un disque.

1. **FAT (File Allocation Table) / exFAT (Extended File Allocation Table)** :
   - **FAT** est l'un des plus anciens systèmes de fichiers, simple mais moins efficace avec de grands volumes ou fichiers. **exFAT** est une version modernisée de FAT avec de meilleures performances et prise en charge de fichiers plus grands. Un exemple d'analyse pourrait être la récupération de fichiers supprimés en scannant la table d'allocation pour des entrées non liées à des fichiers actifs.
2. **NTFS (New Technology File System)** :
   - **NTFS** supporte des fonctionnalités avancées comme les permissions, la journalisation pour la récupération, et les liens symboliques. Les métadonnées pour chaque fichier sont stockées dans le Master File Table (MFT) qui peut être analysé pour récupérer des informations sur chaque fichier, y compris les heures de création, de modification et d'accès, même après suppression.
3. **Timeline (MFT)** :
   - La timeline MFT permet de construire une chronologie d'activité sur le disque en examinant les horodatages stockés dans la MFT.

Forensic Windows

2. Artefacts Système: Les artefacts système fournissent des données sur l'utilisation et l'activité du système

1. **EVTX (Windows XML Event Log)** :
   - Les fichiers EVTX sont des journaux d'événements Windows qui enregistrent des actions telles que les démarrages de session et les erreurs système. Analyser ces fichiers peut aider à identifier des comportements suspects, comme des échecs de connexion répétés.
2. **Analyse de la base de registre** :
   - Le registre Windows contient des configurations et des paramètres qui influencent le fonctionnement du système. L'analyse de la base de registre peut révéler des programmes configurés pour démarrer automatiquement, des traces de logiciels malveillants, et les dernières applications utilisées.
3. **Analyse VSC (Volume Shadow Copies)** :
   - Les copies d'ombre sont des instantanés automatiques du système de fichiers. Analyser ces copies peut permettre de récupérer des fichiers ou des configurations système d'états précédents, même si ceux-ci ont été modifiés ou supprimés dans le système actuel.

FTK Imager

FTK Imager est un outil populaire de forensique numérique utilisé pour l'acquisition et l'analyse d'images de disques.

1. Installation et Configuration

FTK Imager est disponible gratuitement. Vous pouvez le télécharger depuis le site web d'AccessData. Après le téléchargement, installez le logiciel en suivant les instructions. Une fois installé, vous pouvez lancer le programme.

2. Création d'une Image Disque

1. **Démarrer une Nouvelle Acquisition**
2. **Sélection de la Source**
3. **Configuration de l'Image**
4. **Vérification**
5. **Création de l'Image**

2. Exploration d'Images et de Disques

1. **Ajouter une Image ou un Disque**
2. **Navigation dans l'Arborescence des Fichiers**
3. **Visualisation et Exportation de Fichiers**

FTK Imager

3. Analyse Forensique

- **Analyse de Méta-données** : Examinez les méta-données des fichiers, y compris les horodatages de création, modification et dernier accès.
- **Récupération de Fichiers Supprimés** : Tentez de récupérer des fichiers supprimés si l'espace qu'ils occupaient n'a pas été réécrit.
- **Utilisation de Hash Sets** : Comparez les hash de fichiers à des bases de données connues pour identifier des fichiers connus ou suspects.

4. Exportation de Rapports

- **Génération de Rapports** : Créez des rapports détaillés de vos découvertes pour documentation ou preuve légale.

Exercice : Analyse et Récupération Forensique avec FTK Imager

1. **Préparation** :
    - Placez plusieurs types de fichiers sur la clé USB et supprimez volontairement certains fichiers pour tester la récupération de données.
2. **Création de l'Image du Disque**
3. **Analyse de l'Image**
4. **Récupération de Fichiers Supprimés**

Challenge CyberDefenders Injector

Le serveur web d'une entreprise a été compromis via leur site internet. Notre équipe est arrivée juste à temps pour prendre une image forensique du système en fonctionnement et de sa mémoire pour une analyse approfondie.
En tant qu'analyste SOC, vous êtes chargé de monter l'image pour déterminer comment le système a été compromis et les actions/commandes exécutées par l'attaquant.

1. Quel est le nom de l'ordinateur ?
2. Quel est le fuseau horaire de la machine compromise ?
3. Quel est le numéro de build du système d'exploitation ?
4. Combien d'utilisateurs sont présents sur la machine compromise ?
5. Quel est le paquet de serveur web installé sur la machine ?
6. Quel est le nom de l'application web vulnérable installée sur le serveur web ?
7. Quel est le nom de l'application web vulnérable installée sur le serveur web ?

Challenge CyberDefenders Injector

8. Quel est l'agent utilisateur utilisé dans les requêtes HTTP envoyées par l'outil d'attaque par injection SQL ?
9. L'attaquant a lu plusieurs fichiers via une vulnérabilité LFI. L'un d'eux est lié à la configuration réseau. Quel est le nom du fichier ?
10. Quand l'attaquant a-t-il créé le premier utilisateur ?
11. L'attaquant a lu plusieurs fichiers à travers une vulnérabilité LFI. L'un d'eux est lié à la configuration réseau. Quel est le nom du fichier ?

Autopsy

Autopsy est un outil d'analyse forensique numérique open-source qui est largement utilisé pour les investigations informatiques. Il permet d'effectuer une analyse approfondie de divers supports numériques comme des disques durs, des clés USB, et des images de systèmes de fichiers.

1. **Interface Utilisateur** :
   - Autopsy offre une interface graphique utilisateur (GUI) qui guide les utilisateurs à travers le processus d'ajout de sources de données, l'analyse de ces données, et l'examen des résultats.
   - La navigation est basée sur des onglets qui séparent les différentes phases et aspects de l'analyse, rendant le processus structuré et facile à suivre.
2. **Ajout de sources de données** :
   - Autopsy peut analyser des images de disques, des répliques de mémoire, et même des disques en direct. Les utilisateurs peuvent ajouter ces sources via l'interface en sélectionnant le type de source et en naviguant vers l'emplacement du fichier ou du dispositif.

Autopsy

3. **Modules d'analyse** :
   - Autopsy utilise des modules pour traiter les données. Ces modules peuvent être configurés pour exécuter des tâches spécifiques comme la récupération de fichiers supprimés, l'extraction de méta-données, l'analyse de la chronologie des événements, et plus encore.
   - Les modules sont divisés en types tels que les modules de type de fichier, les modules d'analyse de contenu, et les modules de rapport.
4. **Visualisation des résultats** :
   - Les résultats de l'analyse sont présentés sous forme de vues qui peuvent inclure des vues de type de fichier, des chronologies, et des vues de données géolocalisées.
   - Autopsy permet également de rechercher des mots-clés et d'utiliser des filtres pour affiner les résultats.

Autopsy - Options et Configuration

- **Gestion des cas** : Autopsy permet de créer des "cas", qui sont des dossiers contenant toutes les données et configurations pour une enquête spécifique. Chaque cas peut contenir une ou plusieurs sources de données.
- **Modules personnalisés** : Les utilisateurs peuvent ajouter des modules personnalisés pour étendre les fonctionnalités d'Autopsy. Ces modules peuvent être développés en Java ou Python.
- **Configuration des modules** : Chaque module peut être configuré individuellement pour cibler des types de données spécifiques ou pour répondre à des besoins d'enquête particuliers.

Cas d'Utilisation

- **Enquêtes sur les intrusions informatiques** : Utiliser Autopsy pour analyser les disques d'ordinateurs compromis afin de découvrir comment les attaquants ont pénétré le système, quelles données ont été consultées ou exfiltrées, et quelles traces ils ont laissées derrière eux.
- **Récupération de données** : Utiliser Autopsy pour récupérer des fichiers supprimés ou pour extraire des données depuis des appareils endommagés ou formatés.
- **Analyse de dispositifs mobiles** : Bien qu'Autopsy soit principalement conçu pour les systèmes de fichiers de PC, il peut également être utilisé pour analyser des dispositifs mobiles avec des modules adaptés.

Exercice Autopsy

Utilisation de l'image du corpus numérique (Voir : https://downloads.digitalcorpora.org/corpora/drives/nps-2009-ubnist1) :

1. Téléchargez l'image au format prioritaire ubnist1.gen0.E01
2. Utilisez l'outil d'analyse médico-légale Autopsy pour analyser l'image.
   Répondez aux questions suivantes.
3. Remplissez le Tableau 1 ci-dessous.

Exercice Autopsy

Tableau : Valeurs de hachage récupérées

N°	Nom de l'élément de preuve	Type d'élément de preuve	MD5	SHA-256
A	Preuve principale	ubnist1.gen0.E01		
B	debian.jpg	Image/photo		
C	debian-dpkg@lists.debian.org	Email		
D	Packages.gz	Archive		
E	isolinux.cfg	Fichier supprimé		

4. À quoi peuvent servir les valeurs de hachage MD5 et SHA-256 obtenues dans le Tableau 1 devant un tribunal ?

Exercice Autopsy

5. Combien de fichiers chiffrés avez-vous récupérés ?
   - Nom(s) du ou des fichiers chiffrés : .....
   - Valeurs de hachage du ou des fichiers chiffrés : .....
   - Date de la dernière modification du ou des fichiers chiffrés : .....
   - Pouvez-vous considérer le ou les fichiers chiffrés comme suspect(s) ? .....
     - Si oui, indiquez la raison : .....
   - Indiquez une manière de lire le contenu réel du ou des fichiers chiffrés : .....
6. Utilisez la fonctionnalité d'analyse de la chronologie de l'outil Autopsy pour générer un rapport instantané pour ce dispositif de preuve.
   Combien d'applications avez-vous récupérées à partir du dispositif de preuve ?
7. En vous basant sur la fonctionnalité de géolocalisation de l'outil Autopsy, pouvez-vous montrer le lieu où ce dispositif a été utilisé pour la dernière fois ?
8. Combien de détails de cartes de crédit sont susceptibles d'être présents dans ce dispositif de preuve ?
9. Générez le rapport final complet pour cette affaire.

Challenge 2 AfricanFalls Blue Team Lab

https://cyberdefenders.org/blueteam-ctf-challenges/africanfalls/

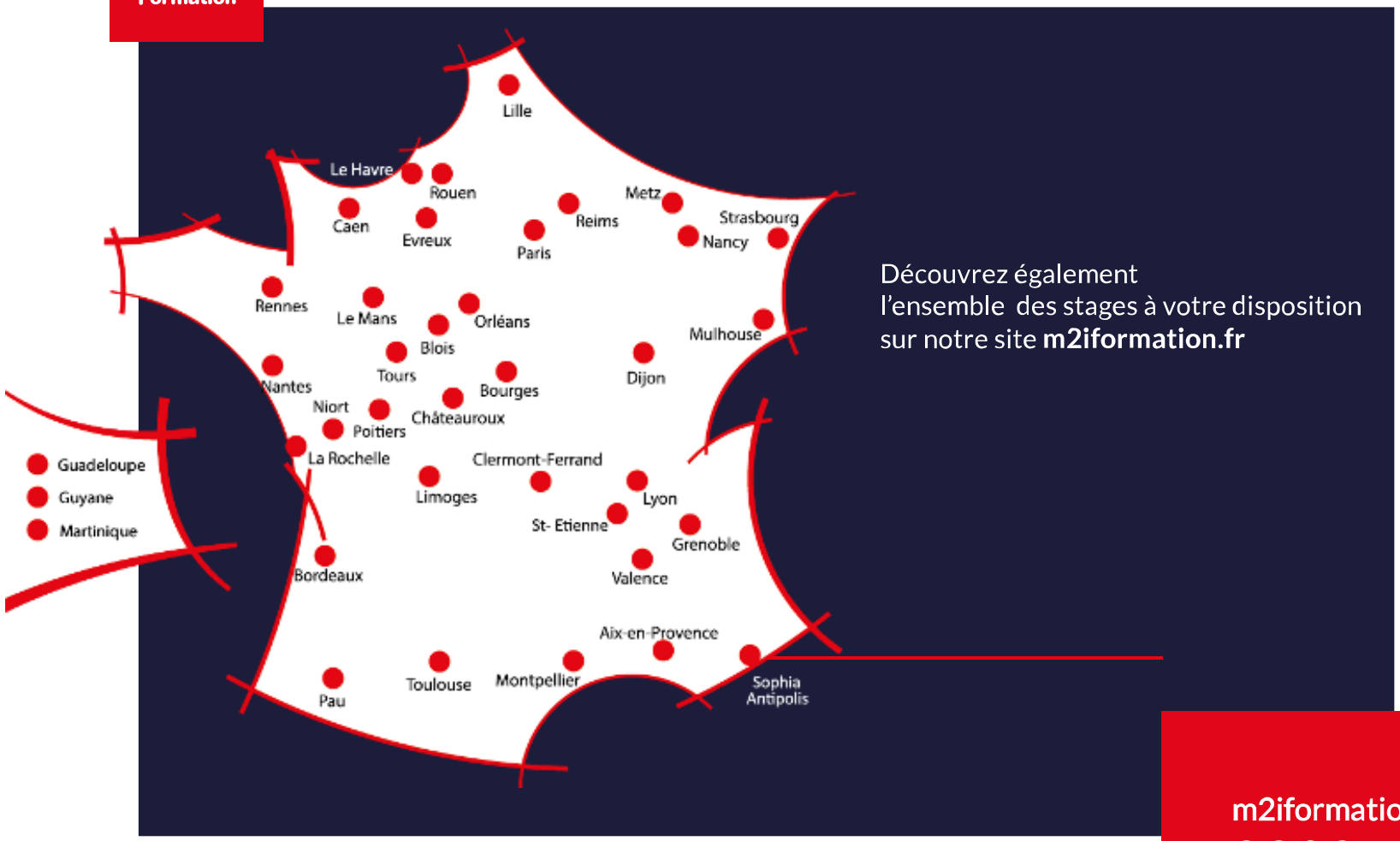
John Doe a été accusé de mener des activités illégales. Une image disque de son ordinateur portable a été prise. Votre tâche en tant qu'analyste SOC est d'analyser l'image et de comprendre ce qui s'est passé sous le capot.

1. Quelle est la valeur de hachage MD5 du disque suspect ?
2. Quelle phrase le suspect a-t-il recherchée le 29 avril 2021 à 18:17:38 UTC ? (trois mots, deux espaces entre eux)
3. Quelle est l'adresse IPv4 du serveur FTP auquel le suspect s'est connecté ?
4. Quelle date et quelle heure une liste de mots de passe a-t-elle été supprimée en UTC ? (AAAA-MM-JJ HH:MM:SS UTC)
5. Combien de fois le navigateur Tor a-t-il été utilisé sur l'ordinateur du suspect ? (nombre uniquement)
6. Quelle est l'adresse e-mail du suspect ?
7. Quel est le nom de domaine pleinement qualifié (FQDN) que le suspect a scanné ?
8. Dans quel pays la photo "20210429_152043.jpg" aurait-elle été prise ?
9. Quel est le nom du dossier parent où se trouvait la photo "20210429_151535.jpg" avant que le suspect ne la copie dans le dossier "contact" sur son bureau ?
10. Quel est le mot de passe de connexion Windows de l'utilisateur « John Doe » ?

UTOPIOS®
TRANSFORMATION DIGITALE INTELLIGENTE

Merci pour votre attention

Des questions ?



Découvrez également
l'ensemble des stages à votre disposition
sur notre site **m2iformation.fr**

m2iformation.fr