RÉSUMÉ THÉORIQUE – FILIÈRE INFRASTRUCTURE DIGITALE

Option Cybersécurité

M205 Méthodes d'investigation numérique

150 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

Introduction à l'investigation numérique

Dans ce module, vous allez :

- Définition de la recherche numérique et de ses objectifs
- Définition de la cybercriminalité et des sources de cybercriminalité
- Catégories de la recherche numérique
- Utilisateurs de recherche numérique
- Types d'investigations
- Préparation à la recherche numérique
- Types de preuves numériques
- Localisation des preuves électroniques
- Processus d'examen

90 heures

CHAPITRE 1

Qu'est-ce que l'investigation numérique ?

Ce que vous allez apprendre dans ce chapitre :

- Les définitions et les concepts de l'investigation numérique, tels que la collecte de preuves numériques, l'analyse de données numériques et la présentation de preuves numériques en justice.

Définition de l’investigation numérique

La cybercriminalité est en augmentation constante, et la cyber-investigation est devenue une branche importante de la sécurité numérique. La cyber-investigation, ou l’investigation numérique, est une discipline de la science médico-légale qui utilise une compréhension scientifique pour acquérir, évaluer, enregistrer et présenter des preuves numériques liées à des crimes informatiques en justice. L'objectif principal est de déterminer ce qui s'est passé, quand cela s'est produit, et qui en est responsable. Les investigations peuvent inclure des ordinateurs personnels, des téléphones portables, des périphériques de réseau, des caméras, des tablettes, des enregistreurs vidéo numériques, des objets connectés, ainsi que des supports de stockage tels que des clés USB, des CD/DVD, des cartes SD et des bandes, parmi d'autres systèmes et appareils numériques qui peuvent envoyer, recevoir et stocker des données numériques.

Les attaques informatiques, telles que les violations de données, les attaques de phishing, les rançongiciels, les attaques par déni de service (DoS) et les injections SQL, sont autant d'exemples de cyberattaques sur des systèmes numériques qui peuvent être investigués en utilisant la forensique numérique. Les cyber-espionnages, les attaques adverses qui compromettent des comptes et des services, l'accès non autorisé aux systèmes et aux réseaux, ou d'autres cyber-attaques connexes qui causent un préjudice commercial ou de réputation, sont également inclus dans cette catégorie. Une investigation en forensique informatique nécessite le respect de certaines directives qui peuvent résister à l'interrogatoire croisé en justice. Cela comprend la collecte de données (statiques et volatiles) de manière forensiquement fiable, l'évaluation des données à l'aide d'outils de forensique approuvés par la cour, la recherche dans les données pour localiser des preuves, et enfin, la présentation des conclusions à la cour dans un rapport officiel. Si ces procédures ne sont pas suivies correctement, il y a un risque de dommage ou de suppression des preuves numériques, les rendant ainsi inadmissibles en cour.

L’investigation numérique est une profession relativement nouvelle dans le domaine de la cybersécurité, qui devient de plus en plus importante à mesure que le nombre de crimes et d'actions illégales dans le cyberespace augmente. Comparée aux sciences médico-légales traditionnelles (tests sanguins, profilage ADN ou empreintes digitales), la forensique numérique est une science jeune; le fait qu'elle interagit avec des changements rapides dans l'écosystème informatique qui nous entoure et touche à d'autres domaines (tels que le processus judiciaire, l'application de la loi, le conseil en gestion, la technologie de l'information et la portée sans frontières d'Internet), en fait un domaine difficile qui nécessite un développement constant.

Les objectifs de l'investigation numérique

L'objectif principal de l'investigation numérique est d'enquêter sur les crimes commis à l'aide de systèmes informatiques qui stockent et traitent des données numériques et d'extraire des preuves numériques forensiques à présenter en cour. Ceci est réalisé de la manière suivante à l'aide de l'investigation numérique. Localiser et préserver les preuves légales sur les dispositifs informatiques d'une manière acceptable en cour de justice. Suivre les méthodes technologiques approuvées par la cour pour préserver et récupérer les preuves. Attribuer la responsabilité d'une activité à la personne qui l'a initiée. Déterminer les violations de données à l'intérieur d'une entreprise. Identifier l'étendue de tout dommage qui pourrait résulter d'une violation de données. Compiler les résultats dans un rapport formel qui peut être soumis en cour. Fournir des preuves d'expert en cour en tant que guide.

La définition du CyberCrime

Le cybercrime désigne toute activité illégale effectuée sur un ordinateur ou via un réseau informatique, tel que l'internet. Selon le Département de la Justice des États-Unis, le cybercrime est défini comme tout comportement illégal effectué contre ou avec l'utilisation d'un ordinateur ou d'un réseau informatique. La motivation fondamentale du cybercrime est le gain financier (par exemple : la propagation de logiciels malveillants pour voler des codes d'accès à des comptes bancaires). Cependant, différentes motivations poussent une partie importante du cybercrime, notamment la perturbation de services (par exemple, les attaques DDoS pour fermer les services d'une organisation cible), le vol de données confidentielles (par exemple, les données des consommateurs et les informations médicales), l'espionnage cybernétique (les secrets commerciaux et militaires) ou l'échange illégal de matériel protégé par le droit d'auteur.

Les sources de cybercriminalité.

Les menaces internes et les attaques externes sont les deux principales sources de cybercriminalité.

- Les menaces internes: En raison de la difficulté à les détecter, elles représentent le risque cybernétique le plus important qui pèse sur les entreprises aujourd'hui. Les employés, ou d'autres personnes travaillant au sein de l'entreprise cible, tels que d'anciens employés, des contractuels tiers ou des associés commerciaux, ayant un accès autorisé aux systèmes informatiques de l'organisation cible et/ou des informations sur ses procédures et défenses de cybersécurité, commettent des attaques internes. Cela est illustré par l'espionnage économique.
- Les attaques externes: Ces tentatives sont généralement menées par des hackers expérimentés opérant depuis l'extérieur de l'entreprise cible. Ce sont les types d'attaques les plus courants contre les organisations dans le monde entier. Un hacker malveillant peut tenter d'entrer dans les réseaux de l'entreprise cible depuis un autre pays pour obtenir un accès illicite. Pour faciliter leur accès illégal, les attaquants externes peuvent obtenir des informations sur les systèmes de sécurité de la société cible auprès d'un insider (membre du personnel mécontent).

Les ordinateurs dans les cybercrimes

Les ordinateurs sont impliqués dans les cybercrimes de trois manières différentes selon leur utilisation dans la commission d'un crime.

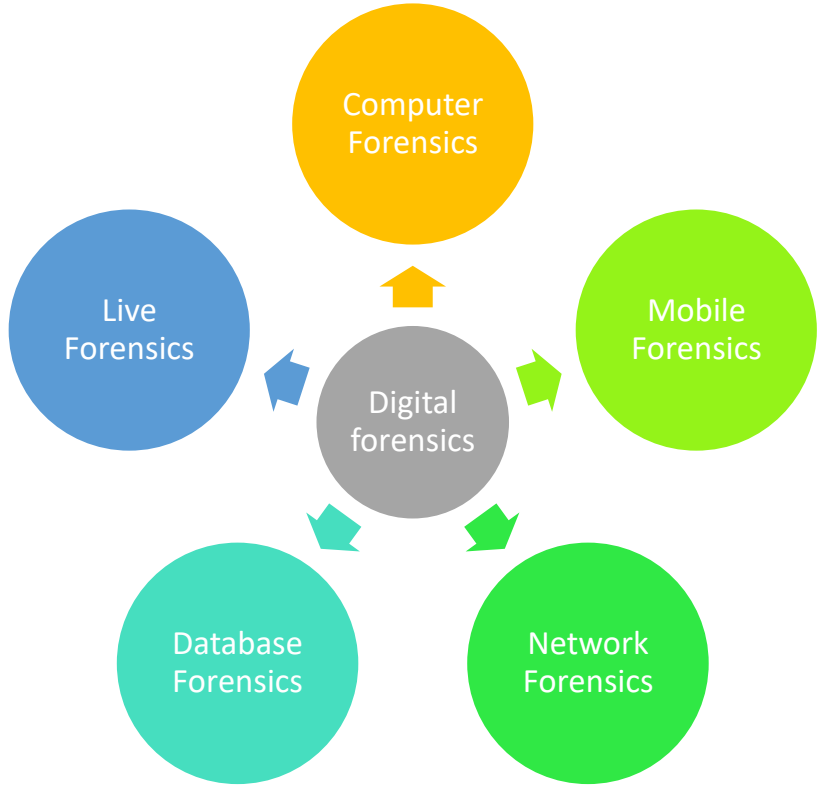
- Premièrement, l'ordinateur peut être utilisé comme une arme pour commettre un crime, comme dans le cas des attaques par déni de service (DoS) ou la distribution de rançongiciels.
- Deuxièmement, un crime peut être commis contre un dispositif informatique, comme lors de l'obtention illégale d'accès à un ordinateur cible.
- Troisièmement, l'ordinateur peut être utilisé pour aider à la commission d'un crime, par exemple en stockant des données incriminantes ou en communiquant avec d'autres criminels en ligne.

Par exemple, certaines cyberattaques peuvent endommager ou détruire le système d'exploitation, vous obligeant à le réinstaller. Un autre type peut essayer de voler vos mots de passe et vos informations de connexion. D'autres attaques, en revanche, peuvent ne pas endommager complètement votre ordinateur, mais elles suivront vos activités en ligne et compromettront votre vie privée. Les

Catégories d'investigation numérique

L'investigation numérique peut être classée en fonction de la source des preuves numériques obtenues. La collection d'artefacts numériques présents sur le dispositif informatique cible, qui peuvent être utilisés comme preuve devant les tribunaux, est appelée preuve numérique, comme présenté dans la figure ci-dessous:

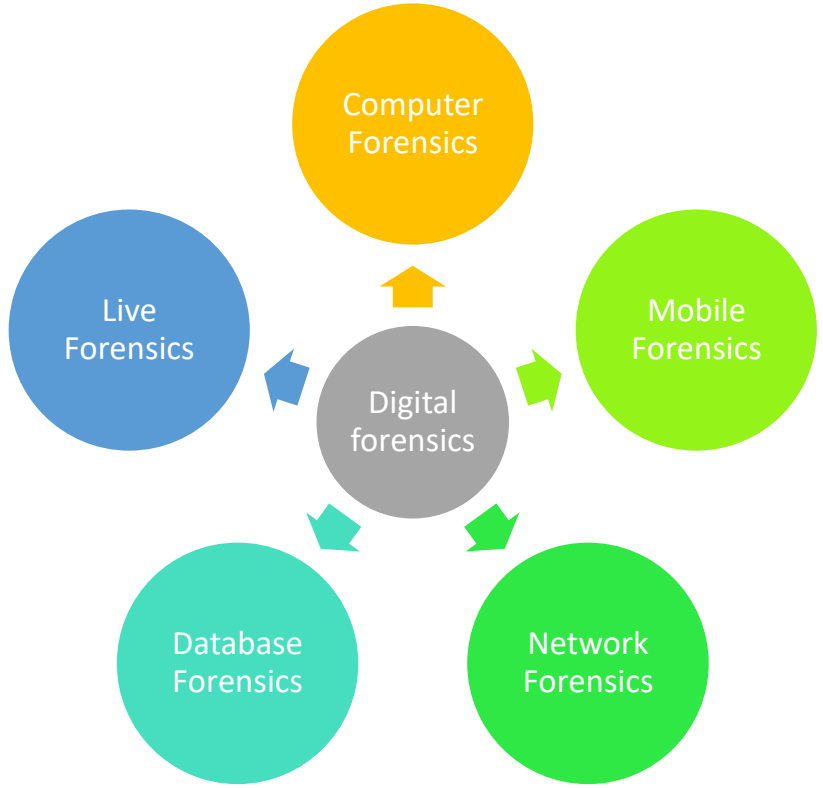
- **Investigation numérique sur les ordinateurs:** Il s'agit du type le plus courant d'investigation numérique; elle consiste à enquêter sur les preuves numériques sur les ordinateurs portables, les ordinateurs de bureau et les dispositifs de stockage tels que les clés USB, les cartes SD, la mémoire système (RAM), les systèmes d'exploitation et les journaux d'application. L'objectif principal de ce type d'enquête est de récupérer les données supprimées du stockage du dispositif cible et de les examiner à la recherche de preuves incriminantes ou disculpatoires.
- **Investigation numérique sur les appareils mobiles** : est une sous-catégorie de l'investigation numérique qui se spécialise dans la collecte de données à partir de dispositifs mobiles. Un dispositif mobile est tout appareil informatique (tel que des téléphones, des smartphones, des tablettes et des appareils portables tels que les montres intelligentes) qui peut passer des appels téléphoniques via des réseaux de communication traditionnels. Ces gadgets sont généralement conscients de leur géolocalisation, ce qui signifie qu'ils ont un GPS ou un autre système de positionnement par satellite intégré. En raison de l'utilisation extensive de la technologie mobile chez les clients du monde entier, l'investigation numérique sur les appareils mobiles remplacera bientôt les méthodes existantes d'investigation numérique.



PARTIE 1

Catégories d'investigation numérique

- **L'investigation réseau** :Ce domaine de l'investigation numérique consiste à surveiller et analyser le trafic réseau afin d'extraire des preuves, telles que l'origine d'une intrusion sur le réseau, ou pour identifier des intrusions. Le flux de données via les réseaux peut être collecté en masse en temps réel et stocké pour une analyse ultérieure. Alternativement, il peut être examiné en temps réel avec la possibilité de conserver des morceaux choisis d'événements pertinents pour une étude ultérieure (cette option nécessite moins d'espace de stockage). Contrairement à d'autres types d'investigation numérique, la forensique réseau se concentre uniquement sur les données en direct volatiles.
- **Forensique de base de données:** L'analyse des données et des informations contenues dans les bases de données telles que Microsoft SQL Server, Oracle, MySQL, et autres est appelée forensique de base de données. La forensique de base de données examine qui a accès à une base de données et quelles actions sont entreprises pour détecter un comportement malveillant.
- **Analyse de données de la criminalistique numérique**: Cette analyse est capable d'examiner les données d'entreprise pour prévenir et identifier les fraudes financières criminelles. Pour identifier et prévenir l'utilisation abusive des ressources de l'entreprise, elle recherche des motifs pertinents, combine les actifs de données et les compare aux résultats antérieurs l'analyse des courriels, l'analyse des espaces de stockage cloud, l'analyse des applications spécifiques telles que les navigateurs Web, l'analyse des systèmes de fichiers (FAT, NTFS ou EXT), l'analyse matérielle, l'analyse multimédia (texte, image, audio ou vidéo) et l'analyse en direct de la mémoire volatile ou de la RAM sont toutes des sous-branches de types principaux déjà mentionnés



Les types d'investigation numérique

En fonction de l'organisme chargé de lancer l'enquête, les investigations numériques peuvent être divisées en deux catégories :

- Les enquêtes publiques
- Les enquêtes du secteur privé.

Les enquêtes criminelles sont traitées selon les directives légales établies par les autorités compétentes. Les organismes chargés de l'application des lois participent aux enquêtes publiques, qui sont menées en vertu de la législation nationale ou étatique. Les trois phases principales de ces enquêtes sont la plainte, l'enquête et la poursuite.

Les enquêtes privées sont couramment menées par des entreprises pour enquêter sur les violations de politiques, les problèmes juridiques, les licenciements abusifs ou la divulgation d'informations confidentielles telles que l'espionnage industriel. Comme il revient à chaque entreprise de déterminer ses propres règles, il n'existe pas de réglementation fixe pour mener de telles enquêtes. Néanmoins, de nombreuses entreprises mettent déjà en place des normes internes strictes pour enquêter sur les crimes numériques. Ces procédures sont similaires aux enquêtes publiques sur les crimes, dans la mesure où certains cas peuvent être présentés devant un tribunal et finalement transformés en poursuites pénales officielles.

Les entreprises peuvent réduire leur responsabilité liée à la criminalité informatique en développant une politique claire, facile à lire et à comprendre pour leurs employés. Une telle politique peut également aider les enquêtes numériques à progresser plus facilement et avec moins de temps d'arrêt pour l'entreprise si elles sont nécessaires. La règle la plus importante que tous les employés doivent signer est la politique d'utilisation de l'ordinateur. Cette politique décrit comment les employés peuvent utiliser les réseaux informatiques et les systèmes informatiques de l'entreprise et les met en garde contre les conséquences juridiques en cas de non-respect des directives.

Les types d'investigation numérique

En fonction de l'organisme chargé de lancer l'enquête, les investigations numériques peuvent être divisées en deux catégories :

- Les enquêtes publiques
- Les enquêtes du secteur privé.

Les enquêtes criminelles sont traitées selon les directives légales établies par les autorités compétentes. Les organismes chargés de l'application des lois participent aux enquêtes publiques, qui sont menées en vertu de la législation nationale ou étatique. Les trois phases principales de ces enquêtes sont la plainte, l'enquête et la poursuite.

Les enquêtes privées sont couramment menées par des entreprises pour enquêter sur les violations de politiques, les problèmes juridiques, les licenciements abusifs ou la divulgation d'informations confidentielles telles que l'espionnage industriel. Comme il revient à chaque entreprise de déterminer ses propres règles, il n'existe pas de réglementation fixe pour mener de telles enquêtes. Néanmoins, de nombreuses entreprises mettent déjà en place des normes internes strictes pour enquêter sur les crimes numériques. Ces procédures sont similaires aux enquêtes publiques sur les crimes, dans la mesure où certains cas peuvent être présentés devant un tribunal et finalement transformés en poursuites pénales officielles.

Les entreprises peuvent réduire leur responsabilité liée à la criminalité informatique en développant une politique claire, facile à lire et à comprendre pour leurs employés. Une telle politique peut également aider les enquêtes numériques à progresser plus facilement et avec moins de temps d'arrêt pour l'entreprise si elles sont nécessaires. La règle la plus importante que tous les employés doivent signer est la politique d'utilisation de l'ordinateur. Cette politique décrit comment les employés peuvent utiliser les réseaux informatiques et les systèmes informatiques de l'entreprise et les met en garde contre les conséquences juridiques en cas de non-respect des directives.

Préparation à l'investigation numérique

La préparation en vue d'une investigation numérique fait référence à la capacité d'une organisation à acquérir, conserver, sécuriser et analyser des preuves numériques de manière forensiquement valide. Pour réduire les coûts, la procédure doit se dérouler sans interférer avec les opérations existantes. La mise en place d'une planification de préparation à l'investigation numérique dans les entreprises offre de nombreux avantages, qui sont énumérés ci-dessous :

- Pour les cas nécessitant des preuves numériques, une réponse rapide est requise. Lorsqu'une violation de données ou une fuite d'informations se produit, la mise en place d'une politique claire d'e-discovery peut permettre aux entreprises de réagir rapidement et d'obtenir des preuves numériques de manière forensiquement valide.
- Les réglementations gouvernementales doivent être respectées ; les procédures fédérales américaines ont élaboré un ensemble de lignes directrices pour les parties impliquées dans des litiges juridiques sur la manière d'obtenir et de gérer des preuves numériques afin qu'elles puissent être utilisées en justice. Si l'affaire arrive devant les tribunaux, la préparation forensique réduira le coût de la collecte de preuves numériques et conduira probablement à une résolution plus rapide.
- Amélioration des défenses de sécurité de l'entreprise. La surveillance de l'utilisation des ordinateurs peut permettre de détecter des malwares dangereux, tels que des ransomwares, avant que l'infection ne se propage à l'ensemble du réseau de l'organisation. En utilisant une préparation forensique, une organisation sera bien préparée à gérer les incidents de sécurité internes et externes et sera en mesure d'identifier rapidement une attaque avant qu'elle ne se propage dans son infrastructure IT.
- Réduction du nombre d'attaques internes. Comme mentionné précédemment, les menaces internes telles que les employés malveillants sont plus dangereuses que les attaques externes ; la présence d'un plan de préparation forensique dans une organisation incitera les employés malveillants à craindre d'être découverts s'ils se livrent à un comportement illégal.
- Amélioration de la posture de sécurité de l'organisation. La stratégie de préparation forensique d'une entreprise la distinguera en tant que défenseur puissant contre les cyberattaques. Les clients seront plus enclins à faire affaire avec cette organisation car leurs données seront conservées de manière privée et sécurisée. Les investisseurs se sentiront également en sécurité en sachant que leur argent est protégé et qu'il y a une probabilité minimale que des attaques réussies contre cette organisation entraînent une perte d'argent.

Les types des preuves numériques

Les deux types de preuves numériques les plus courants sont les données créées par l'utilisateur et les données créées par la machine.

- Les données créées par l'utilisateur sont tout ce qui est créé par une personne (humaine) à l'aide d'un dispositif numérique. Les métadonnées sont des données incluses dans des fichiers créés par un utilisateur d'ordinateur ; les métadonnées peuvent être créées par l'utilisateur d'ordinateur de manière intentionnelle (par exemple : nom de l'auteur et adresse e-mail), ou elles peuvent être générées automatiquement par le logiciel qui a créé le fichier, telles que le modèle/type d'appareil photo utilisé pour prendre la photo, la date et l'heure de prise de la photo, les coordonnées GPS de la photo et sa résolution. Les métadonnées doivent être examinées attentivement dans toute enquête, car elles peuvent contenir des informations importantes sur le sujet étudié. Elles comprennent, entre autres, les éléments suivants :
  - Les sauvegardes précédentes (y compris les sauvegardes stockées dans le cloud et les sauvegardes hors ligne telles que les CD/DVD et les bandes)
  - Les détails du compte (nom d'utilisateur, photo et mot de passe)
  - Les messages électroniques et leurs pièces jointes (à la fois les e-mails en ligne et les e-mails clients tels que Outlook)
  - Les fichiers audio et vidéo
  - Le carnet d'adresses et le calendrier
  - Les enregistrements de la webcam (photos et vidéos numériques)
  - Les fichiers de contenu (par exemple, des documents MS Office, des conversations de messagerie instantanée, des favoris), des feuilles de calcul, des bases de données et tout autre texte stocké numériquement
  - Les fichiers cachés et chiffrés (y compris les dossiers compressés) créés par l'utilisateur d'ordinateur.

Les types des preuves numériques

- Toute donnée générée automatiquement par un appareil numérique est considérée comme des données créées par la machine/réseau. Cela inclut, entre autres choses
  - Les fichiers de configuration et les pistes d'audit, y compris celles des prestataires de services tiers (par exemple, les fournisseurs de services Internet (FAI) conservent souvent les journaux d'historique de compte et de navigation de leurs clients)
  - Les journaux sur l'ordinateur sous Windows OS contiennent les journaux suivants : journaux d'application, de sécurité, de configuration, de système, d'événements avancés, d'applications et de services
  - Les informations du navigateur (historique de navigation, cookies et historique de téléchargement)
  - Les informations du navigateur (historique de navigation, cookies et historique de téléchargement)
  - En plus des adresses IP associées à un réseau LAN et des paramètres de diffusion, les dispositifs ont des adresses de protocole Internet (IP) et MAC.
  - L'historique de messagerie instantanée et la liste de contacts (Skype et WhatsApp) (à partir d'appareils avec une capacité GPS)
  - L'historique des applications et de Windows (par exemple, un fichier récemment ouvert dans MS Office)
  - L'historique de suivi GPS
  - Les fichiers système cachés et classiques, les fichiers temporaires, les fichiers du spouleur d'impression
  - Les machines virtuelles
  - Les enregistrements vidéo de surveillance
  - …,etc.

Par conséquent, les preuves numériques peuvent être définies comme tout fichier ou donnée/métadonnée qui est fourni dans un format numérique (binaire) et qui pourrait être utilisé dans un procès.

Les emplacements des preuves électroniques

Les preuves numériques se trouvent fréquemment sur les disques durs, mais à mesure que la technologie informatique progresse, les preuves numériques sont de plus en plus découvertes dans pratiquement tous les dispositifs numériques. Voici une liste des types d'appareils les plus courants qui doivent être examinés pour trouver des preuves numériques :

- Systèmes : ordinateurs de bureau, ordinateurs portables, tablettes, serveurs et systèmes RAID
- Appareils réseau : concentrateurs, commutateurs, modems, routeurs et points d'accès sans fil
- Appareils de domotique et objets connectés à Internet : climatiseurs et réfrigérateurs intelligents
- DVR et systèmes de surveillance
- Lecteurs MP3
- Appareils GPS
- Smartphones
- PDA
- Consoles de jeux - Xbox, PlayStation
- Appareils photo numériques
- Cartes à puce
- Pagers
- Enregistreurs vocaux numériques

La chaîne de conservation de la preuve (Chain of Custody)

La chaîne de conservation de la preuve est nécessaire pour toute enquête de cybercriminalité. Une chaîne de conservation appropriée doit détailler comment la preuve numérique a été découverte, collectée, transportée, analysée, stockée et conservée par les différentes parties impliquées dans l'enquête. L'objectif ultime est de protéger l'intégrité de la preuve numérique en retrouvant tous ceux qui ont eu contact avec elle depuis sa collecte jusqu'à sa présentation devant un tribunal. Si nous ne comprenons pas qui a eu contact avec la preuve à tout moment au cours de l'enquête, la chaîne de conservation sera compromise et la preuve obtenue sera inutilisable devant un tribunal. Pour maintenir une chaîne de conservation appropriée acceptée par un tribunal, un registre d'audit de toutes les preuves numériques acquises qui suit les mouvements et les détenteurs de preuves numériques doit être conservé en tout temps. Si la chaîne de conservation est valide, les enquêteurs seront en mesure de répondre aux questions posées devant un tribunal :

- Quelle est la définition de la preuve numérique ? (Par exemple, décrire la preuve numérique qui a été obtenue.)
- Où avez-vous trouvé la preuve numérique ? (Par exemple, un ordinateur, une tablette ou un téléphone portable ; en outre, l'état de l'appareil informatique lors de l'acquisition de la preuve numérique - ALLUMÉ ou ÉTEINT ?)
- Comment la preuve numérique est-elle apparue ? (Par exemple, les outils employés ; vous devez également indiquer les procédures effectuées pour protéger l'intégrité de la preuve tout au long de la phase d'acquisition.)
- Quelles méthodes ont été utilisées pour transférer, préserver et manipuler la preuve numérique ?
- Quelles méthodes ont été utilisées pour évaluer la preuve numérique ? (Par exemple, tous les outils et procédures utilisés.)
- Quand, par qui et dans quel but la preuve numérique a-t-elle été consultée ?
- Quel a été le rôle de la preuve numérique dans l'enquête ? Chaque mouvement de données numériques doit être enregistré pour qu'un enquêteur puisse s'assurer que les données en question n'ont pas été altérées et qu'aucune preuve externe n'a été insérée pour tromper l'enquêteur pendant l'enquête.

Processus d'examen

Processus d'examen Bien qu'il n'existe pas de méthode ou de procédure universellement acceptée pour effectuer des enquêtes de cybercriminalité, plusieurs approches sont disponibles, avec des étapes ou des phases variables. Cependant, toutes les stratégies divisent le travail en quatre phases principales.

- Recherche et saisie
- Acquisition
- Analyse Collecte d'informations et
- rapport

Seizure (la saisie)

Pendant ce processus, la preuve matérielle (appareil numérique) sera confisquée et livrée avec soin au laboratoire de la police scientifique. Tout type d'appareil informatique peut être utilisé comme preuve, y compris un ordinateur portable, une tablette, un téléphone, un disque dur externe, une clé USB, un appareil portable (par exemple, une montre connectée) ou même un ordinateur de bureau. Vous aurez besoin de l'autorisation des autorités compétentes pour confisquer l'appareil du suspect (par exemple, un mandat judiciaire). Lorsque des experts professionnels arrivent sur les lieux du crime, l'appareil numérique de l'accusé doit être examiné pour s'assurer que la preuve numérique a été capturée et conservée correctement. Si l'ordinateur suspect était encore allumé, nous devrions essayer de récupérer autant de mémoire volatile que possible. Il était autrefois courant de débrancher l'ordinateur et de le placer dans un boîtier anti-statique. Cependant, les approches modernes en matière de police scientifique comprennent la nécessité de récupérer la mémoire volatile pendant que l'appareil est encore opérationnel. Dans la RAM, on peut trouver des journaux de discussion, des clés cryptographiques, des contenus du presse-papiers, des données non chiffrées et des informations sur les processus système. Étant donné que l'application utilisée pour extraire le contenu de la RAM peut créer des modifications mineures aux fichiers du système d'exploitation cible, à la RAM et au disque dur, la collecte de la RAM doit être notée dans le rapport final d'enquête ainsi que l'outil utilisé.

Acquisition (Acquisition)

Si la machine était encore opérationnelle, cette étape portait sur les dispositifs de stockage secondaires tels que les SSD, les clés USB, les bandes et la mémoire RAM volatile. À cette étape, un spécialiste de la criminalistique informatique dupliquera le disque dur suspect pour créer une image complète du disque dur confisqué (également appelée image bit à bit). Les examinateurs utilisent fréquemment des duplicateurs matériels ou des outils d'imagerie logiciels tels que la commande DD de Linux pour dupliquer des CD. Gardez à l'esprit que le disque dur suspect doit être protégé en écriture pour éviter toute altération de l'original lors de la copie des preuves. Si la machine suspecte était encore en marche, la RAM doit être collectée pour prendre en compte divers scénarios.

Analyse

Cette étape examine le contenu du fichier image de la preuve acquise en utilisant une gamme d'outils pour rechercher des indices utiles à l'intérieur de l'image. Volatility, EnCase, Sleuth Kit et Forensic Toolkit sont des exemples d'outils spécialisés qui peuvent récupérer des données supprimées, cachées et chiffrées, ainsi que des journaux de conversation de messagerie, l'historique du navigateur Web, des fichiers et des e-mails supprimés. L'outil de criminalistique utilise l'analyse de signature de hachage à cette étape pour localiser des fichiers remarquables ou exclure ceux qui sont connus. Le contenu des fichiers d'image obtenus est haché et comparé à des listes précompilées telles que l'ensemble de données de référence de la Bibliothèque nationale de référence logicielle. La bibliothèque collecte des logiciels provenant de nombreuses sources et convertit les profils de fichiers du logiciel en un RDS de données. Les outils de criminalistique peuvent rechercher à l'intérieur du fichier photo acquis à l'aide de termes ou de phrases de recherche par mot-clé. Cela accélérera considérablement l'enquête et aidera les enquêteurs à découvrir rapidement des informations pertinentes.

Rapport

Dans cette phase, l'expert crée un rapport structuré présentant ses conclusions. Ce type de rapport est généralement créé pour des audiences non techniques (comme des juges, des avocats et des jurés). Lors de la préparation du rapport, il convient de prendre en compte le style d'écriture, la terminologie et la présentation des informations. Les preuves doivent être incluses dans le rapport, idéalement sous forme numérique. Les éléments suivants devraient figurer dans le contenu général du rapport d'expertise :

- Un résumé des conclusions les plus importantes.
- Une description des outils (matériels et logiciels) utilisés tout au long du processus d'enquête, ainsi que leurs fonctions et versions de logiciel.
- La méthode par laquelle la preuve numérique a été obtenue.
- Une description de la preuve numérique (contenu des images) ainsi que les objets intéressants découverts à l'intérieur (par exemple, historique de navigation sur Internet, historique des e-mails, analyse du registre USB et fichiers supprimés trouvés).
- Lorsque cela est possible, utilisez des captures d'écran pour clarifier les procédures impliquées dans l'analyse de la preuve numérique pour le lecteur.
- Explication des termes techniques utilisés dans le rapport, tels que "espace disque non alloué" et "zone protégée de l'hôte", afin que les personnes non techniques puissent les comprendre.
- Le disque dur original du suspect, ainsi que des copies numériques (images), doivent être fournis à la cour avec le rapport.

Conclusion

Ce chapitre a défini la science informatique légale et l'a différenciée des autres domaines de la cybersécurité. Le concept de la preuve numérique a été brièvement examiné, ainsi que les nombreux types de preuves numériques et où nous pouvons les trouver dans les appareils électroniques. Bien qu'il n'existe pas de protocole universellement accepté pour mener des enquêtes en science informatique légale, nous avons décrit les étapes essentielles de chaque enquête numérique ainsi que les responsabilités qui doivent être remplies à chaque étape. De nombreuses tentatives ont été faites pour normaliser les normes et les procédures de la science informatique légale par la publication de recommandations par des organismes gouvernementaux reconnus, dont les plus remarquables sont celles produites dans les tribunaux. Les experts en science informatique légale sont nécessaires dans pratiquement tous les secteurs, allant des ONG aux agences gouvernementales en passant par les entreprises et les sociétés privées. La demande pour les spécialistes de la science informatique légale devrait augmenter dans les années à venir à mesure que de plus en plus d'organisations déplacent leur travail vers la sphère numérique. Dans le prochain chapitre, nous passerons en revue les concepts technologiques clés que tout spécialiste en science informatique légale ou en cybersécurité devrait connaître avant de commencer son enquête.

Quiz?

1. L'informatique légale est également connue sous le nom de :
    a. Science légale numérique
    b. Flux de criminalité informatique
    c. Science légale informatique
    d. Enquêtes informatiques légales
2. L'informatique légale peut également être utilisée dans des procédures civiles.
    a. Vrai
    b. Faux
    c. Peut être oui ou non
    d. Impossible à dire
3. Vous devez tenir trois types d'enregistrements en informatique légale, lequel de ceux-ci n'est pas un enregistrement ?
    a. Chaîne de garde
    b. Documentation de la scène de crime
    c. Recherche de la scène de crime
    d. Documentation des actions

Quiz?

4. Les données volatiles résident dans:
    a. Registres
    b. Cache
    c. RAM
    d. Tous les trois
5. Les enquêteurs en informatique légale doivent satisfaire à...
    a. Contribuer à la société et aux êtres humains
    b. Éviter de nuire à autrui
    c. Être honnête et digne de confiance
    d. Tous les trois
6. Les preuves numériques sont utilisées pour établir un lien crédible entre...
    a. L'attaquant et la victime et la scène de crime
    b. L'attaquant et l'information
    c. Soit A soit B
    d. Les deux A et B

Quiz?

7. La preuve et la démonstration qui peuvent être obtenues à partir de la source électronique s'appellent...
    a. Preuve numérique
    b. Preuve explicable
    c. Soit A soit B
    d. Les deux A et B
8. Les preuves numériques doivent suivre les exigences de la...
    a. Règle de la preuve idéale
    b. Règle de la meilleure preuve
    c. Règle de l'échange
    d. Tous les trois
9. Un faux positif peut être défini comme...
    a. Une alerte qui indique une activité néfaste sur un système qui, après inspection approfondie, s'avère représenter un trafic ou un comportement de réseau légitime
    b. Une alerte qui indique une activité néfaste sur un système qui, après inspection approfondie, s'avère être réellement une activité néfaste
    c. L'absence d'une alerte pour une activité néfaste
    d. Tous les trois

Quiz?

10. Une définition valide de preuve numérique est :

a. Aucune des réponses ci-dessous
b. Données stockées ou transmises à l'aide d'un ordinateur
c. Données numériques ayant une valeur probante
d. Toute preuve numérique sur un ordinateur Réponses

Réponses

1. c
2. a
3. c
4. d
5. d
6. a
7. a
8. d
9. a
10. c

CHAPITRE 2

Concepts, Techniques, Essentiels

Ce que vous allez apprendre dans ce chapitre :

- Nous allons explorer dans cette partie comment un système représente les données, ainsi que les systèmes de numérotation typiques et la stratégie d'encodage principale utilisée par les machines pour générer du texte lisible par les humains. Commençons par le système de numérotation standard.

Introduction

Entreprendre une enquête en informatique légale exige une compréhension approfondie de certains concepts technologiques fondamentaux de l'informatique. Pour découvrir et gérer les preuves numériques, il est nécessaire de comprendre comment les informations sont stockées dans les ordinateurs, la théorie des nombres, la construction des fichiers numériques et les nombreux types d'unités de stockage et leurs différences. Ces sujets fondamentaux seront abordés dans ce chapitre. Les ordinateurs stockent, traitent et présentent les données numériques d'une certaine manière, comme expliqué dans ce chapitre.

Décimal (Base-10)

Le système décimal, qui utilise 10 chiffres ou symboles (0, 1, 2, 3, 4, 5, 6, 7, 8 et 9) pour représenter ses valeurs, est le système de numérotation le plus couramment utilisé que nous utilisons tous les jours lors de nos calculs arithmétiques (par exemple, 17 + 71 = 88). La valeur qu'un nombre représente est déterminée par sa position dans le système décimal, où chaque chiffre est multiplié par la puissance de 10 correspondant à l'emplacement de ce chiffre. Prenons par exemple le nombre décimal 7 564. Ce nombre peut être interprété comme suit :

$$7\,654 = 7\,000 + 600 + 50 + 4$$

Une compréhension du système de numérotation décimal est essentielle, car les autres systèmes de numérotation suivent des règles similaires.

Binaire

Les données sont stockées sous forme binaire sur les ordinateurs, ce qui est le système numérique de base 2 représenté par des 1 et des 0. Le langage informatique, binaire, suit les mêmes règles qu'un système décimal. Le binaire, en revanche, contient deux symboles (0 et 1) et multiplie par la puissance de deux, contrairement au décimal, qui a 10 symboles et multiplie par la puissance de 10. Chaque 1 OU 0 dans un ordinateur est appelé un bit (ou chiffre binaire), et l'ensemble de huit bits est appelé un octet. Le bit le plus significatif est le bit d'ordre supérieur, qui est placé dans le bit le plus à gauche et a la plus grande valeur significative (MSB). En revanche, le bit le moins significatif est positionné dans le bit le plus à droite et a la valeur de bits la plus faible (LSB). Le tableau ci-dessous identifie les valeurs de bits en fonction de leur position pour les nombres binaires.

MSB	Binary Digit							LSB
2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
256	128	64	32	16	8	4	2	1

Par exemple, le nombre binaire 110011001 peut être converti en décimal comme 409, comme calculé dans le tableau suivant:

Binary								
1	1	0	0	1	1	0	0	1
Decimal								
1×2^8	1×2^7	0×2^6	0×2^5	1×2^4	1×2^3	0×2^2	0×2^1	1×2^0
256	128	0	0	16	8	0	0	1
= 256+128+0+0+16+8+0+0+1								
= 409								

Les données sont stockées dans les systèmes informatiques sous forme binaire, y compris les documents Microsoft Word, les photographies numériques, les vidéos, les feuilles Excel, les tweets et publications sur les réseaux sociaux, les e-mails, ainsi que tout ce qui est créé et stocké sur les systèmes informatiques.

Hexadécimal (Base-64)

La seule différence majeure entre Base64 et hexadécimal est la façon dont les octets sont représentés. Base16 est également appelé "hex". L'hexadécimal nécessite deux caractères pour chaque octet, tandis que Base64 en nécessite quatre pour chaque trois octets, le rendant plus efficace que l'hexadécimal. Un fichier de 100 Ko nécessitera 200 Ko pour être encodé en hexadécimal ou 133 Ko en Base64, en supposant que vous utilisez UTF-8 pour encoder le texte XML. Bien sûr, il est possible que vous n'ayez aucun intérêt pour l'efficacité de l'espace; dans de nombreuses situations, cela n'aura pas d'importance. Si c'est le cas, Base64 est sans aucun doute supérieur à cet égard. (Des alternatives existent qui sont encore plus efficaces, mais elles sont moins répandues.) Voici une phrase courante utilisée en informatique distribuée "Many hands help with a task". La citation est représentée lorsqu'elle est encodée en Base64 comme la séquence d'octets suivante de caractères ASCII à 8 bits remplis: "TWFueSBoYW5kcyBtYWtlIGxpZ2h0Ihdvcmsu" (les sauts de ligne et les espaces blancs peuvent être inclus n'importe où, mais ils doivent être ignorés lors du décodage).

Character encoding schema

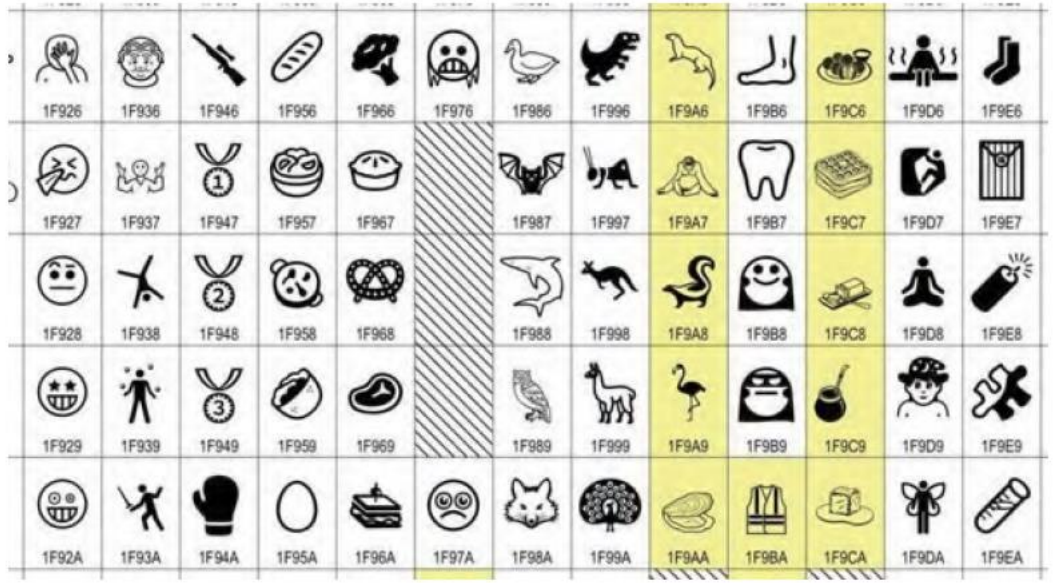
Comment les 1 et les 0 peuvent-ils apparaître à l'écran sous forme de lettres comme A, B, ou X, Y, X, alors que tout dans les ordinateurs est représenté par des 0 ou des 1 ? Pour transformer des nombres binaires en texte significatif que l'on peut lire, les ordinateurs utilisent des schémas de codage de caractères comme le contenu de l'alphabet et les textes affichés sur votre écran lorsque la version PDF de ce livre est ouverte sur l'écran de l'ordinateur). Il existe deux principaux schémas de codage utilisés par les ordinateurs pour représenter le texte :

- ASCII, ou le code américain standard pour l'échange d'informations (https://ascii.cl), a été créé il y a de nombreuses années et est toujours pris en charge par presque tous les éditeurs de texte aujourd'hui. Parce qu'il ne comporte que sept bits ou 128 valeurs, ASCII a une capacité limitée à représenter toutes les lettres de toutes les langues du monde, ainsi que la ponctuation et les autres symboles spéciaux d'autres langues. ASCII amélioré est une autre forme étendue d'ASCII qui fournit 256 caractères ; cependant, il ne prend toujours pas en charge toutes les langues du monde.

PARTIE 1

Character encoding schema

Le consortium Unicode (https://unicode.org) a inventé l'encodage Unicode, qui est une stratégie de codage de caractères largement utilisée et qui attribue un numéro unique à chaque caractère de chaque langue dans le monde entier. Les principaux systèmes d'exploitation, plates-formes logicielles, appareils portables et applications en ligne prennent tous en charge Unicode. UTF-8, UTF-16 et UTF-32 sont les trois types d'Unicode.



UNICODE VER 12

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

ASCII TABLE

Carving de fichiers / File Craving

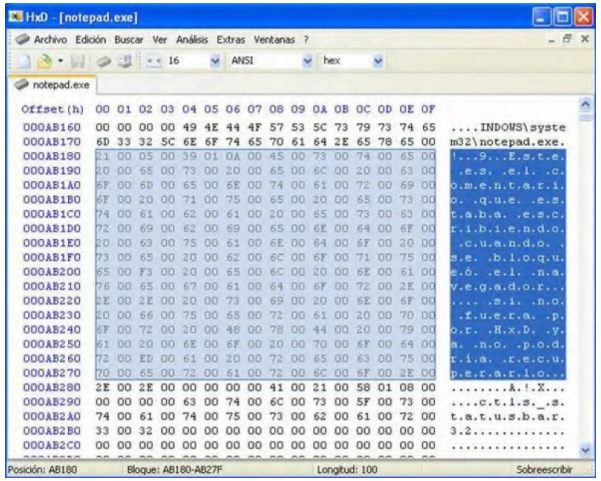
En informatique légale, comprendre comment les ordinateurs stockent et représentent les données est essentiel ; par exemple, un analyste peut avoir besoin de récupérer et d'ouvrir un fichier à partir de l'espace disque non alloué sur le disque dur cible ou à partir d'un ensemble de données brut sans utiliser le logiciel qui a produit le fichier (par exemple, MS Word). Cette méthode est appelée "file carving", et elle peut être utilisée pour récupérer des fichiers perdus et des fragments de fichiers à partir de disques durs effacés ou endommagés. Pour effectuer le "file carving", nous devons d'abord comprendre comment séparer un fichier de sa signature. Le "file carving" est le plus souvent utilisé pour récupérer des fichiers de l'espace non alloué d'un disque car il s'agit d'une méthode d'informatique légale qui récupère des fichiers uniquement sur la base de leur structure et de leur contenu, sans utiliser de métadonnées de système de fichiers correspondantes. L'espace non alloué est la partie du disque qui, selon l'architecture du système de fichiers, comme la table de fichiers, ne contient plus aucune information de fichier. Tout le disque peut être affecté si les structures du système de fichiers sont brisées ou absentes. En termes simples, de nombreux systèmes de fichiers ne suppriment pas complètement les données lorsqu'ils les effacent. Au lieu de cela, ils suppriment simplement les informations de localisation. En scannant les octets bruts du disque et en les remettant ensemble, un processus appelé "file carving" reconstruit les fichiers. Cela se fait souvent en examinant l'en-tête et le pied de page d'un fichier, qui sont respectivement les premiers et les derniers octets.

Lorsque les entrées de répertoire sont endommagées ou manquantes, le "file carving" est une technique fantastique pour récupérer des fichiers et des morceaux de fichiers. Les professionnels de l'informatique légale utilisent cette méthode, en particulier, pour récupérer des preuves dans des situations criminelles. Les agents de la force publique utilisent fréquemment des techniques de "carving" pour extraire plus de photos à partir des disques durs des suspects dans des cas spécifiques de pornographie infantile. Les disques durs et les dispositifs de stockage portables saisis par les Navy Seals américains lors de leur raid sur le campus d'Osama Ben Laden servent d'autre exemple. Les professionnels de l'informatique légale ont utilisé des techniques de "file carving" pour extraire chaque morceau d'information de ce support.

Structure de fichier

Chaque type de fichier possède son propre schéma d'encodage qui spécifie la façon dont les informations sont stockées, et un fichier numérique est constitué d'une série de bits. Le nom de ce schéma est "format de fichier". Le format de fichier peut être soit open source (comme PNG, un format d'image raster ISO/CEI) soit propriétaire (comme Adobe Photoshop) (comme le format de fichier audio **Windows Media [WMA]).** De nombreux formats de fichiers multimédias courants peuvent contenir plusieurs types de contenus, comme c'est le cas avec certains formats de fichiers. Par exemple, le format OGG peut contenir de la vidéo, de la musique, du texte et des métadonnées dans un seul conteneur. Les extensions de fichier permettent d'identifier les types de fichiers, selon les chercheurs. L'extension DOCX ou DOC est utilisée pour les fichiers MS Word, tandis que l'extension XLSX ou XLS est utilisée pour les fichiers MS Excel. Cependant, en tant qu'investigateurs en informatique légale, nous ne pouvons pas nous fier uniquement à l'extension de fichier pour déterminer le type de fichier car elle peut être modifiée en n'importe quoi (par exemple, un fichier MS Word peut être modifié en fichier DLL ou PNG pour dissimuler sa véritable identité).

La signature de fichier (en-tête) peut être vérifiée pour établir le type de stratégie de détection. Les 20 premiers octets de la plupart des fichiers numériques contiennent une signature; vous pouvez vérifier cette signature en ouvrant le fichier en question dans le Bloc-notes de Windows ou un autre éditeur de texte comme Notepad++. Pour analyser un fichier texte ou un document, changez l'extension en, par exemple, JPG et analysez ensuite les 20 premiers octets du fichier JPG dans un éditeur hexadécimal (voir la figure 2.3). HexEditor révélera la signature de fichier d'origine comme étant éditable dans **Notepad.exe**.



Il existe de nombreux éditeurs hexadécimaux gratuits; voici quelques-uns couramment utilisés :

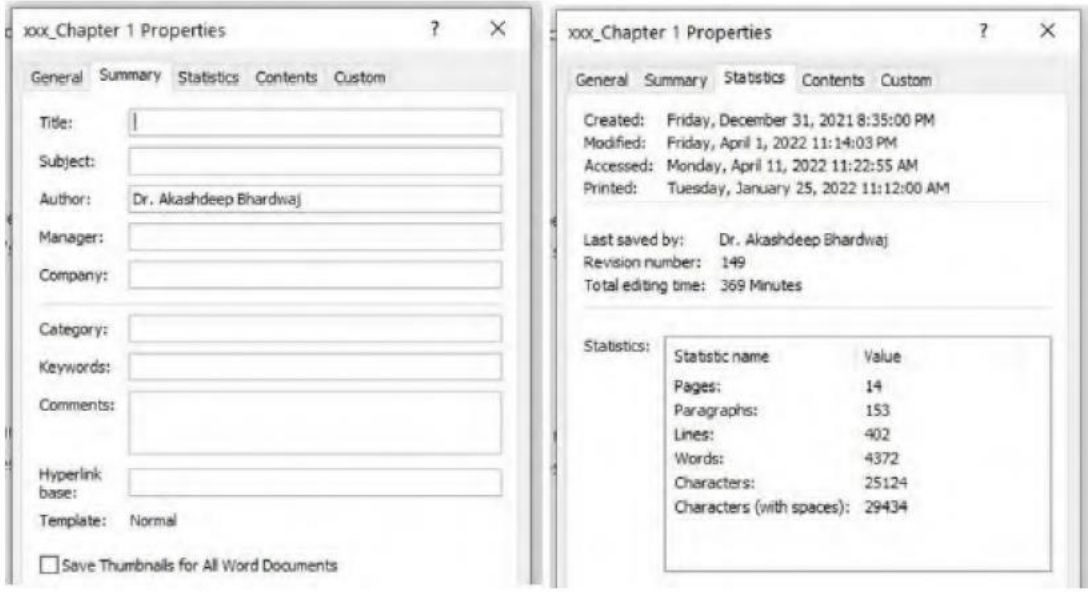
- wxHexEditor (www.wxhexeditor.org/home.php)
- Free Hex Editor Neo (www.hhdsoftware.com/free-hex-editor)
- PSPad (www.pspad.com/en)

PARTIE 1

Métadonnées de fichiers numériques

Les métadonnées sont des informations à propos de l'information. Les métadonnées sont liées à presque tous les formats de fichiers numériques. Bien qu'elles soient fréquemment incluses dans le même fichier, certains formats de fichiers enregistrent leurs informations dans un fichier distinct. Les métadonnées contiennent des informations sur le fichier auquel elles sont liées. Le nom de l'auteur, le nom de l'organisation, le nom de l'ordinateur, la date/heure de création et les commentaires sont des exemples d'informations que l'on peut trouver dans les fichiers MS Word. Les métadonnées peuvent être très utiles dans de nombreuses circonstances en matière de cybercriminalité. Nous pouvons, par exemple, retracer les auteurs de fichiers en utilisant les informations qui leur sont associées. Nous pouvons également rechercher des informations utiles dans les métadonnées du fichier (la plupart des systèmes d'exploitation offrent actuellement la possibilité de rechercher dans les informations de métadonnées de fichier), et la plupart des suites de cybercriminalité prennent en charge la recherche dans les métadonnées des images acquises lors des enquêtes.

Sous le système d'exploitation Windows, nous pouvons modifier les métadonnées de nombreux types de fichiers numériques sans avoir besoin de programmes tiers. Par exemple, nous pouvons mettre à jour les informations de métadonnées d'un fichier MS Office en faisant un clic droit dessus et en sélectionnant "**fichier | Propriétés** " dans le menu qui apparaît (voir la figure ci-dessous) pour déterminer l'auteur du fichier et les statistiques telles que la date/heure de création, de modification, d'accès et même d'impression. Les statistiques révèlent également le nombre de pages, de paragraphes, de lignes, de mots et de caractères au total avec et sans espaces.



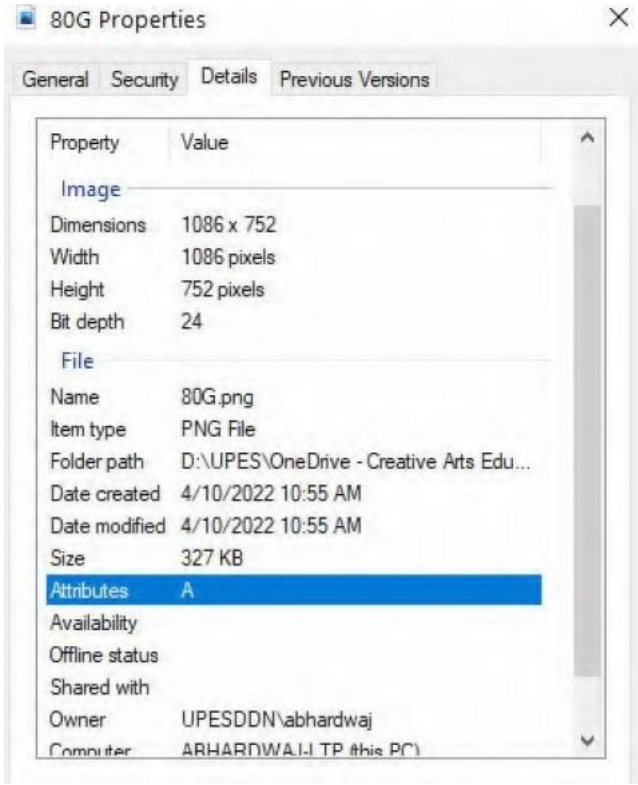
PARTIE 1

Métadonnées de fichiers numériques -Suite

Métadonnées d'un fichier image contient des données forensiques cruciales telles que l'horodatage de la prise de vue et les coordonnées GPS de l'endroit où elle a été prise (si autorisées sur l'appareil de capture), ainsi que les spécifications et les réglages de l'appareil photo (voir la figure 2.5). Les informations de métadonnées d'image peuvent être consultées sur Windows de manière similaire aux fichiers MS Office.

Plusieurs outils gratuits peuvent également afficher et modifier les informations de métadonnées des fichiers numériques, comme suit:

- ExifTool de Phil Harvey (www.sno.phy.queensu.ca/~phil/exiftool). Permet de lire, écrire et modifier les méta-informations pour une grande variété de fichiers numériques (la plupart des formats d'image).
- Exif Pilot (www.colorpilot.com/exif.html). Éditeur et visualiseur de métadonnées d'images.
- GIMP (www.gimp.org). Éditeur d'image ; peut manipuler/visualiser les métadonnées des fichiers d'images.
- Pdf Metadata Editor (http://broken-by.me/pdf-metadataeditor). Pour les fichiers PDF.
- Mp3tag (www.mp3tag.de/en). Pour les fichiers audio.
- XnView (www.xnview.com/en/). Affiche/modifie les métadonnées d'images.
- MediaInfo (https://mediaarea.net/en/MediaInfo). Visionneur/éditeur de métadonnées pour les fichiers vidéo et audio.

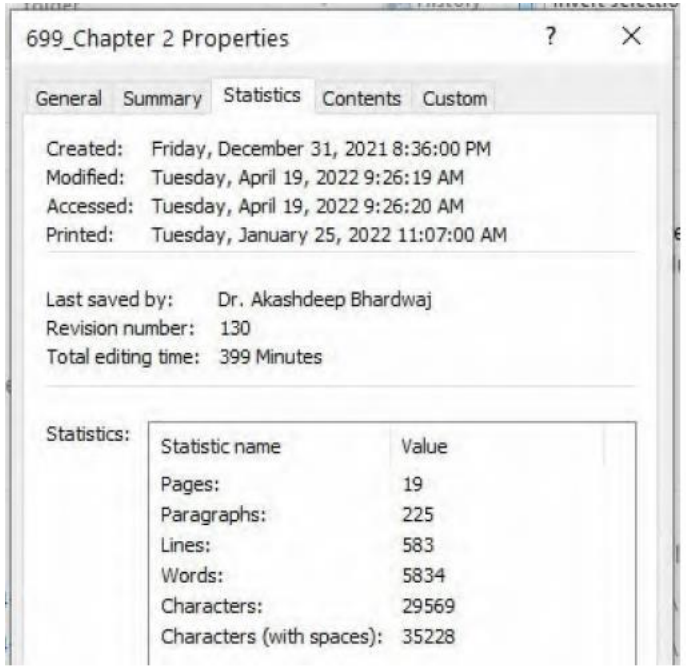


PARTIE 1

Décodage des horodatages

Pour les versions de Microsoft Office 2010 à 2016, allez à l'onglet **Fichier | Propriétés** pour obtenir les informations de métadonnées telles qu'illustrées dans la figure ci-dessous. Le panneau Propriétés apparaîtra sur le côté droit ; en cliquant sur le bouton **Propriétés** et en choisissant **Propriétés avancées**, vous pouvez examiner les métadonnées du document. Du point de vue de la cybercriminalité, l'analyse des métadonnées est essentielle pour toute enquête, car elle peut révéler une mine d'informations sur l'affaire en cours. Certains utilisateurs (par exemple, les criminels) peuvent tenter de modifier les métadonnées du fichier pour effacer les preuves et tromper les enquêteurs. Les spécialistes en informatique légale sont chargés de détecter de telles manipulations et d'essayer de les révéler devant le tribunal. La plupart des logiciels de cybercriminalité permettent l'extraction massive et la recherche de métadonnées de fichiers.

Les fichiers numériques contiennent une variété d'informations, dont la plus importante est la métadonnée d'horodatage, qui est utilisée pour indiquer différents événements de date/heure liés au fichier d'intérêt, tels que la dernière date/heure d'accès, la dernière mise à jour et la date de création. Au cours des enquêtes, nous pouvons rencontrer une date/heure encodée de manière spécifique que nous devons décoder (par exemple, les données de date/heure dans le registre Windows qui sont enregistrées au format binaire et doivent être converties en ASCII) à partir de https://www.digital-detective.net/digital-forensic-software/free-tools/

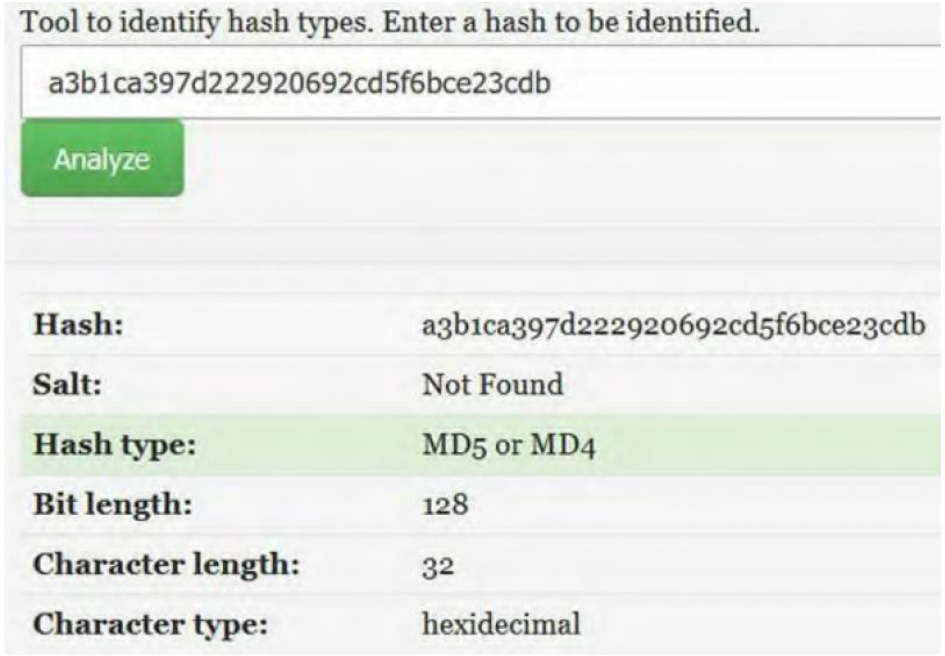


PARTIE 1

Décodage des horodatages

L'analyse de hachage Le hachage est un concept important en cyber criminalistique; en fait, vous devez calculer la valeur de hachage de chaque preuve numérique que vous obtenez tout au long de votre enquête (qu'il s'agisse d'une image de disque dur ou d'un simple fichier) pour vérifier que les données acquises (c'est-à-dire la preuve numérique) n'ont pas été altérées. Le hachage fonctionne en convertissant un fichier numérique (entrée) en une valeur de chaîne fixe (sortie); la valeur de hachage résultante est unique et ne peut pas être créée à l'aide d'un autre fichier ou d'une autre donnée. Un outil de génération de hachage peut être utilisé pour déterminer la valeur de hachage de n'importe quel fichier numérique ou morceau de données. MD5 et SHA-256 sont deux des algorithmes de hachage cryptographique les plus connus.

Le hachage, appelé empreinte numérique, est utilisé dans les enquêtes de cyber criminalistique la première fois pour déterminer l'image de cyber criminalistique acquise avant même que l'analyse ne commence (pour créer des copies identiques de l'image de cyber criminalistique acquise), puis la deuxième fois après l'enquête pour vérifier l'intégrité des données et du traitement de cyber criminalistique présenté dans la figure suivante.



PARTIE 1

Calcul du hachage de fichier

Les capacités de hachage sont incluses dans toutes les suites de forensique numérique. Cependant, vous pouvez utiliser une application tierce ou l'outil de hachage intégré dans le système d'exploitation Windows.

- Méthode 1: Utiliser un outil tiers
  - **Febooti Hash et CRC:** Utilisez cet outil tiers (www.febooti.com), installez ce programme sur votre PC Windows, puis cliquez avec le bouton droit sur le fichier dont vous souhaitez calculer le hachage, sélectionnez Propriétés, puis l'onglet Hash/CRC.
  - **HashMyFile**: (http://www.nirsoft.net/utils/hashmyfiles.html) est un programme portable qui affiche les valeurs de hachage de fichiers et de répertoires choisis à l'aide de différentes techniques de hachage (par exemple, MD5, SHA 256).
- Méthode 2: Utiliser la fonction de hachage intégrée dans Windows
  - Lorsque vous utilisez PowerShell pour calculer le hachage d'un fichier, Windows utilise par défaut l'algorithme SHA256. Cependant, vous pouvez spécifier la fonction de hachage cryptographique à utiliser en ajoutant le paramètre de l'algorithme après le chemin du fichier suivi de l'une des fonctions de hachage cryptographiques suivantes (SHA1, SHA256, SHA384, SHA512 et MD5)

Calcul du hachage de fichier

Les capacités de hachage sont incluses dans toutes les suites de forensique numérique. Cependant, vous pouvez utiliser une application tierce ou l'outil de hachage intégré dans le système d'exploitation Windows.

- Méthode 1: Utiliser un outil tiers
  - **Febooti Hash et CRC:** Utilisez cet outil tiers (www.febooti.com), installez ce programme sur votre PC Windows, puis cliquez avec le bouton droit sur le fichier dont vous souhaitez calculer le hachage, sélectionnez Propriétés, puis l'onglet Hash/CRC.
  - **HashMyFile**: (http://www.nirsoft.net/utils/hashmyfiles.html) est un programme portable qui affiche les valeurs de hachage de fichiers et de répertoires choisis à l'aide de différentes techniques de hachage (par exemple, MD5, SHA 256).
- Méthode 2: Utiliser la fonction de hachage intégrée dans Windows
  - Lorsque vous utilisez PowerShell pour calculer le hachage d'un fichier, Windows utilise par défaut l'algorithme SHA256. Cependant, vous pouvez spécifier la fonction de hachage cryptographique à utiliser en ajoutant le paramètre de l'algorithme après le chemin du fichier suivi de l'une des fonctions de hachage cryptographiques suivantes (SHA1, SHA256, SHA384, SHA512 et MD5)

Mémoire système

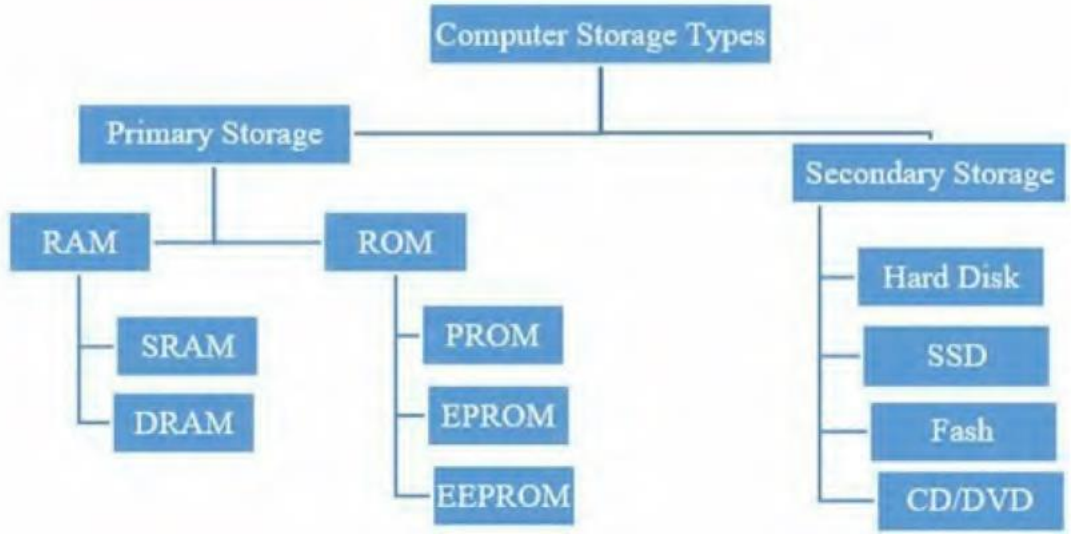
La mémoire fait référence à la composante physique d'un ordinateur qui stocke des données pour une utilisation immédiate ou ultérieure. Selon la durée pendant laquelle les informations sont conservées, nous pouvons distinguer deux types principaux.

- Mémoire volatile : Stocke des données pendant une période limitée ; en fait, il a besoin d'électricité pour conserver les données, mais lorsqu'on éteint l'alimentation, il perd rapidement son contenu. La RAM est un exemple de mémoire volatile.
- Mémoire non volatile : Même si l'alimentation est coupée, la mémoire non volatile peut conserver les données pendant une longue période. C'est le plus souvent utilisé pour le stockage à long terme. Les disques durs d'ordinateur, la mémoire flash et la ROM sont des exemples de ce type de mémoire (mémoire en lecture seule).

Types de stockage de mémoire informatique

Le stockage de mémoire informatique est divisé en deux catégories principales :

- Le stockage primaire
- Le stockage secondaire



Stockage primaire

Cette forme de stockage, souvent appelée stockage principal ou stockage système, contient une mémoire volatile qui perd les données lorsque l'alimentation est coupée. Le stockage primaire est utilisé pour stocker temporairement des données et des programmes, et il a une capacité de stockage plus petite et des opérations de lecture/écriture plus rapides que le stockage secondaire. Il est également plus coûteux. La RAM et le cache sont les deux types de mémoire de stockage primaire que l'on trouve dans les ordinateurs (mémoire CPU)

La mémoire vive (RAM - Random Access Memory) est le composant le plus crucial de tout dispositif informatique; la mémoire volatile stocke les informations dont le système a besoin pour traiter immédiatement ou dans le futur. C'est une mémoire haute vitesse par rapport aux médias de stockage secondaires. Par exemple, lorsque vous exécutez un navigateur Web, il se chargera dans la RAM. La RAM contient une pléthore de données en termes de l'informatique forensique, telles que les applications exécutables, les sessions réseau, l'historique du navigateur Web, les discussions de messagerie instantanée, les mots de passe, les photographies, les fichiers décryptés, et ainsi de suite. Dans toute enquête en informatique forensique impliquant une machine en marche, la capture d'une image RAM devient essentielle. La RAM est divisée en deux types :

- La mémoire vive dynamique (DRAM) est le premier type de mémoire où "dynamique" fait référence au fait que pour conserver ses données, cette mémoire doit être mise à jour chaque seconde. La DRAM est le type de mémoire primaire le plus courant que l'on trouve dans les PC, les stations de travail, les serveurs et les smartphones. La DRAM (DDR2, DDR3, DDR4, où DDR signifie Double Data Rate) car elle est synchronisée avec la vitesse d'horloge du microprocesseur.
- La mémoire vive statique à accès aléatoire (SRAM) est utilisée dans les mémoires CPU (Cache CPU) et est extrêmement rapide (plus rapide que la DRAM) car elle ne nécessite pas de rafraîchissement constant (d'où le terme "statique"). La SRAM est plus coûteuse et consomme plus d'énergie que la DRAM. Les deux formes de RAM sont volatiles, ce qui signifie qu'elles perdront leur contenu si l'alimentation est coupée.

Stockage primaire

Cette forme de stockage, souvent appelée stockage principal ou stockage système, contient une mémoire volatile qui perd les données lorsque l'alimentation est coupée. Le stockage primaire est utilisé pour stocker temporairement des données et des programmes, et il a une capacité de stockage plus petite et des opérations de lecture/écriture plus rapides que le stockage secondaire. Il est également plus coûteux. La RAM et le cache sont les deux types de mémoire de stockage primaire que l'on trouve dans les ordinateurs (mémoire CPU)

La mémoire vive (RAM - Random Access Memory) est le composant le plus crucial de tout dispositif informatique; la mémoire volatile stocke les informations dont le système a besoin pour traiter immédiatement ou dans le futur. C'est une mémoire haute vitesse par rapport aux médias de stockage secondaires. Par exemple, lorsque vous exécutez un navigateur Web, il se chargera dans la RAM. La RAM contient une pléthore de données en termes de l'informatique forensique, telles que les applications exécutables, les sessions réseau, l'historique du navigateur Web, les discussions de messagerie instantanée, les mots de passe, les photographies, les fichiers décryptés, et ainsi de suite. Dans toute enquête en informatique forensique impliquant une machine en marche, la capture d'une image RAM devient essentielle. La RAM est divisée en deux types :

- La mémoire vive dynamique (DRAM) est le premier type de mémoire où "dynamique" fait référence au fait que pour conserver ses données, cette mémoire doit être mise à jour chaque seconde. La DRAM est le type de mémoire primaire le plus courant que l'on trouve dans les PC, les stations de travail, les serveurs et les smartphones. La DRAM (DDR2, DDR3, DDR4, où DDR signifie Double Data Rate) car elle est synchronisée avec la vitesse d'horloge du microprocesseur.
- La mémoire vive statique à accès aléatoire (SRAM) est utilisée dans les mémoires CPU (Cache CPU) et est extrêmement rapide (plus rapide que la DRAM) car elle ne nécessite pas de rafraîchissement constant (d'où le terme "statique"). La SRAM est plus coûteuse et consomme plus d'énergie que la DRAM. Les deux formes de RAM sont volatiles, ce qui signifie qu'elles perdront leur contenu si l'alimentation est coupée.

Stockage primaire

La Mémoire Morte (ROM, Read Only Memory en anglais) est utilisée uniquement pour les opérations de lecture ; comme son nom l'indique, elle ne supporte pas les opérations d'écriture. Cette mémoire est non volatile car elle conserve les informations qu'elle contient même lorsque l'alimentation est coupée. Ce type de mémoire est utilisé pour stocker les programmes de firmware (logiciel stocké sur des dispositifs matériels tels que la carte mère d'un ordinateur et la carte graphique qui fournit des instructions sur le fonctionnement de ce périphérique) dans les ordinateurs et de nombreux autres appareils numériques. La modification des données dans la ROM est difficile et nécessite l'utilisation d'applications spéciales. Il existe trois types différents de ROM :

- ROM programmable (PROM)
- ROM programmable effaçable (EPROM)
- ROM programmable effaçable électriquement (EEPROM)

Stockage secondaire

Le stockage secondaire est une mémoire non volatile à long terme. Sans le stockage secondaire, tous les programmes et les données seraient perdus dès que l'ordinateur est éteint. Il existe trois types principaux de stockage secondaire dans un système informatique : les dispositifs de stockage à semi-conducteurs, tels que les clés USB

1. **Le stockage de sauvegarde**

Le stockage externe ou la mémoire auxiliaire sont d'autres termes pour le stockage secondaire. Il s'agit d'un type de mémoire non volatile qui conserve son contenu, qu'il y ait du courant ou non. Il est utilisé pour conserver des données pendant une longue période. Le stockage secondaire est plus lent que le stockage primaire, tel que la RAM, mais il est beaucoup moins cher. Les exemples suivants illustrent le stockage secondaire.

2. **HDD**

Dans un ordinateur, le disque dur (HDD) est la destination de stockage permanente (non volatile) primaire pour les données. Il stocke des données à l'aide de la technologie de stockage magnétique pour une utilisation ultérieure. Les HDD sont une technologie bien établie qui est utilisée depuis 1960 lorsqu'ils sont devenus les dispositifs de stockage primaire et secondaire pour divers systèmes informatiques tels que les ordinateurs de bureau, les serveurs et les ordinateurs portables. Tout enquêteur judiciaire numérique a probablement déjà traité avec un disque dur, et cette technologie est prévue pour être disponible pendant longtemps. Il existe deux types de disques durs : fixes (internes) et externes. Le premier (fixe) est intégré à l'ordinateur, tandis que le disque dur externe peut être connecté à l'aide d'un câble USB ou eSATA pour étendre le stockage. Les données sont stockées sur des plateaux dans les disques durs (HDD). Un plateau est un disque métallique rond composé d'aluminium, de verre ou de céramique qui est recouvert d'une substance magnétique et peut stocker des données sur les deux faces (surfaces supérieure et inférieure). Un disque dur peut avoir plusieurs plateaux ; cependant, les disques durs grand public d'une capacité inférieure à 500 Go n'en auront qu'un seul. En fonction de la taille physique, de la capacité, du fabricant et du modèle d'un disque dur grand public à grande capacité, le nombre de plateaux peut varier de un à cinq. Un plateau est divisé en plusieurs pistes. Sur chaque plateau, les pistes créent un anneau complet. Chacune de ces pistes est subdivisée en un nombre égal de secteurs. Une partition est un segment du disque qui est séparé du reste du disque (unité de stockage logique). Comme nous le savons tous, un disque dur peut avoir de nombreuses partitions. Le partitionnement de disque est utilisé pour traiter un seul disque dur physique comme s'il était plusieurs disques.

Stockage secondaire

Le stockage secondaire est une mémoire non volatile à long terme. Sans le stockage secondaire, tous les programmes et les données seraient perdus dès que l'ordinateur est éteint. Il existe trois types principaux de stockage secondaire dans un système informatique : les dispositifs de stockage à semi-conducteurs, tels que les clés USB

1. **Le stockage de sauvegarde**

Le stockage externe ou la mémoire auxiliaire sont d'autres termes pour le stockage secondaire. Il s'agit d'un type de mémoire non volatile qui conserve son contenu, qu'il y ait du courant ou non. Il est utilisé pour conserver des données pendant une longue période. Le stockage secondaire est plus lent que le stockage primaire, tel que la RAM, mais il est beaucoup moins cher. Les exemples suivants illustrent le stockage secondaire.

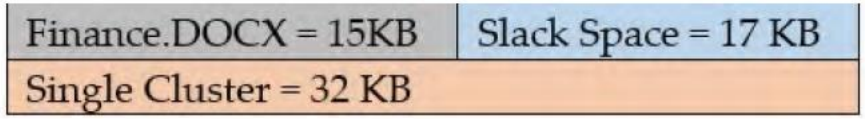
2. **HDD**

Dans un ordinateur, le disque dur (HDD) est la destination de stockage permanente (non volatile) primaire pour les données. Il stocke des données à l'aide de la technologie de stockage magnétique pour une utilisation ultérieure. Les HDD sont une technologie bien établie qui est utilisée depuis 1960 lorsqu'ils sont devenus les dispositifs de stockage primaire et secondaire pour divers systèmes informatiques tels que les ordinateurs de bureau, les serveurs et les ordinateurs portables. Tout enquêteur judiciaire numérique a probablement déjà traité avec un disque dur, et cette technologie est prévue pour être disponible pendant longtemps. Il existe deux types de disques durs : fixes (internes) et externes. Le premier (fixe) est intégré à l'ordinateur, tandis que le disque dur externe peut être connecté à l'aide d'un câble USB ou eSATA pour étendre le stockage. Les données sont stockées sur des plateaux dans les disques durs (HDD). Un plateau est un disque métallique rond composé d'aluminium, de verre ou de céramique qui est recouvert d'une substance magnétique et peut stocker des données sur les deux faces (surfaces supérieure et inférieure). Un disque dur peut avoir plusieurs plateaux ; cependant, les disques durs grand public d'une capacité inférieure à 500 Go n'en auront qu'un seul. En fonction de la taille physique, de la capacité, du fabricant et du modèle d'un disque dur grand public à grande capacité, le nombre de plateaux peut varier de un à cinq. Un plateau est divisé en plusieurs pistes. Sur chaque plateau, les pistes créent un anneau complet. Chacune de ces pistes est subdivisée en un nombre égal de secteurs. Une partition est un segment du disque qui est séparé du reste du disque (unité de stockage logique). Comme nous le savons tous, un disque dur peut avoir de nombreuses partitions. Le partitionnement de disque est utilisé pour traiter un seul disque dur physique comme s'il était plusieurs disques.

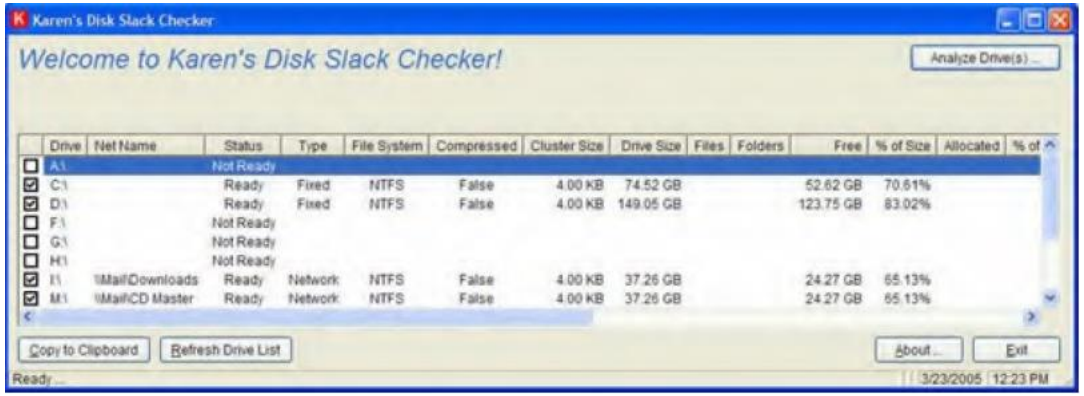
Stockage secondaire - suite

3. Stockage sur disque dur

Chaque plateau, comme précédemment mentionné, contient des milliers de pistes, chacune étant divisée en secteurs. Le nombre de secteurs sur chaque piste du plateau est le même. Des millions de secteurs peuvent être stockés sur un disque dur. Chaque secteur a une capacité de stockage standard de 512 octets, mais les nouveaux systèmes de fichiers peuvent contenir jusqu'à 4 Ko. Tous les systèmes de fichiers Windows organisent les disques durs en clusters en fonction de la taille du cluster (un cluster est composé de plusieurs secteurs). La taille du cluster est la plus petite quantité d'espace disque qu'un fichier peut occuper. La taille des clusters varie de 4 à 64 secteurs, en fonction du système de fichiers utilisé et de la taille de la partition. Avec ces paramètres par défaut, un seul cluster peut stocker jusqu'à 64 Ko de données. À tout moment, chaque cluster ne peut contenir les données que d'un seul fichier. Par conséquent, un fichier texte de 11 Ko occupera un cluster (en supposant que la taille du cluster est de 32 Ko) ; l'espace de stockage restant (21 Ko) restera inutilisé et est appelé espace libre (voir figure suivante). L'espace libre peut être utilisé pour stocker des données potentiellement compromettantes, ou il peut simplement contenir des fichiers résiduels recyclés qui peuvent être restaurés à des fins de preuve.



Le Disk Slack Checker (outil disponible sur www.karenware.com/powertools/ptslack) est un outil qui permet de calculer l'espace non-utilisé présent sur un disque dur, tel qu'illustré dans la figure 2.10. Les plateaux d'un disque dur tournent à une vitesse élevée pour permettre à d'autres parties d'écrire et de lire des données sur les plateaux. Par conséquent, ce type de disque est également connu sous le nom de disque dur mécanique. Un disque SSD (solid-state drive) est un type de disque dur moderne qui stocke les données en utilisant de la mémoire flash NAND (non volatile), et c'est de cela que nous parlerons dans la prochaine section.



PARTIE 1

Stockage secondaire - suite

4. SSD

Les SSD (Solid-State Drives) peuvent être considérés comme la version moderne des disques durs. Les SSD n'ont pas de pièces mobiles (plateaux) et stockent les données dans une série de cellules de mémoire flash NAND ou de micro-puces, similaire à la mémoire flash (NAND est composé d'un ensemble de transistors similaires à ceux utilisés dans la RAM; cependant, ce type de transistor n'a pas besoin d'être régulièrement rafraîchi pour conserver ses données, ce qui en fait un type de mémoire non volatile). Pour déterminer comment stocker, récupérer et mettre en cache les données, le SSD utilise un contrôleur (qui est un processeur intégré). Comparé à un disque dur traditionnel (10), les SSD consomment moins d'énergie et ont des vitesses plus rapides en raison de l'absence de pièces mécaniques en mouvement. Les SSD avaient un inconvénient majeur au début, qui était leur nombre limité de cycles d'écriture; cependant, à mesure que la technologie progresse, les fabricants de SSD travaillent à résoudre ce problème en développant des algorithmes plus efficaces qui répartissent les données uniformément sur toutes les cellules SSD, permettant à toutes les cellules SSD de vivre plus longtemps sans problèmes. Les SSD deviennent de plus en plus populaires dans les ordinateurs portables et les stations de travail de gamme moyenne et haut de gamme, et à mesure que la technologie avance quotidiennement, nous pouvons nous attendre à voir les prix des SSD baisser.

Les unités SSD ont encore une faible capacité par rapport aux disques durs, ce qui pose problème. Les problèmes de prix et de capacité seront presque certainement résolus bientôt, nous pouvons donc nous attendre à voir ce type de disque dur dans la plupart des ordinateurs portables et des stations de travail, ainsi que dans les serveurs. Cela présentera sans aucun doute un défi pour les enquêteurs en informatique judiciaire, car la récupération de données supprimées à partir de SSD est extrêmement difficile, voire impossible dans de nombreux cas.

Data Measurement	Size
1 Bit	1 or 0
1 Byte	8 Bits
1 Kilobyte (1 KB)	1,024 Bytes
1 Megabyte (1 MB)	1,024 KB
1 Gigabyte (1 GB)	1,024 MB
1 Terabytes (1 TB)	1,024 GB
1 Petabyte (1 PB)	1,024 TB
1 Exabyte (1EB)	1,024 PB
1 Zettabyte (1 ZB)	1,024 TB

Stockage secondaire - suite

4. DCO et HPA

Le fabricant de disques durs crée une zone réservée qui n'est pas accessible par l'utilisateur, le système d'exploitation ou le BIOS. Ce dossier contient généralement des utilitaires de support de disque dur (tels que des programmes de diagnostic et de récupération) ainsi que les fichiers de secteur d'amorçage de l'OS installé. L'overlay de configuration du périphérique (DCO) est une zone réservée sur un disque dur qui n'est pas pris en charge par tous les fabricants de disques durs; il est situé après la partition HPA à la fin du disque. Les deux zones HPA et DCO peuvent coexister sur le même disque dur, mais DCO doit être créé en premier. En termes de cyber forensique, les zones DCO et HPA survivront à un formatage complet du disque, ce qui en fait un endroit idéal pour les auteurs d'infractions potentiels pour cacher des données compromettantes. De nombreux logiciels de cyber forensique peuvent accéder et créer une image de ces zones sur un disque dur, et la plupart des outils d'acquisition de matériel peuvent également créer une image de ces zones. Vérifiez toujours les capacités de l'outil de cyber forensique que vous souhaitez utiliser.

5. Considérations pour la récupération de données

La récupération de données à partir d'un SSD est plus difficile que la récupération de données à partir d'un HDD, et parfois impossible. Lorsque vous supprimez un fichier sur un HDD, par exemple, les données dans le fichier ne sont pas immédiatement supprimées; au lieu de cela, le disque dur ne supprime que le pointeur vers le fichier, marquant son espace sur le disque comme libre. Ce n'est que lorsque le système d'exploitation a besoin d'écrire de nouvelles données à son emplacement que les données du fichier en question sont supprimées. Lorsqu'un utilisateur supprime un fichier, par exemple, le SSD utilisera la commande **TRIM**, qui fonctionne pour supprimer instantanément un fichier donné, laissant son emplacement libre pour qu'un autre fichier l'occupe. La commande **TRIM** est mise en œuvre différemment par chaque type de système d'exploitation: certains systèmes d'exploitation l'exécutent immédiatement après que l'utilisateur supprime un fichier, tandis que d'autres l'exécutent à intervalles réguliers.

Stockage secondaire - suite

6. NFS

Le formatage d'un volume avec NTFS entraîne la création de plusieurs fichiers de métadonnées (voir la figure 2.11), notamment la table des fichiers principaux ($MFT), $Bitmap, $LogFile et d'autres, qui contiennent des informations sur tous les fichiers et dossiers sur le volume NTFS.

Chaque fichier dans le système de fichiers NTFS est composé de nombreux flux de données : le flux principal (qui n'a pas de nom) contient les données qu'un utilisateur voit lorsqu'il ouvre un fichier. Le flux de données alternatif est l'autre flux (ADS). Les examinateurs de la forensique numérique doivent rechercher les flux de données de tous les fichiers stockés sur une partition NTFS, car ils peuvent contenir des données cachées. Pour savoir comment un délinquant peut créer un fichier ADS et cacher des données secrètes, voire un logiciel malveillant, ainsi que pour savoir comment un enquêteur peut détecter manuellement de tels fichiers et utiliser divers outils tiers pour le faire.

- Créer, ouvrir, détecter et supprimer des ADS : https://www.minitool.com/partition-disk/alternate-datastreams.html
- Identifier les fichiers cachés avec ADS : https://www.minitool.com/partition-disk/alternate-datastreams.html
- Extraire des ADS avec Linux : https://tmairi.github.io/posts/extracting-alternate-data-streams-with-linux/

7. FAT

Le système de fichiers de la table **d'allocation des fichiers (FAT**) est l'un des plus anciens encore utilisés et est disponible en quatre versions : FAT12, FAT16, FAT32 et FATX. Toutes les versions précédentes de Windows de Microsoft, y compris Windows NT, utilisaient FAT comme système de fichiers par défaut. FAT est plus portable que NTFS car il peut être utilisé sur une variété de périphériques tels que les appareils photo numériques, les cartes SD, les smartphones, les clés USB et les dispositifs intégrés. Contrairement à NTFS, qui ne peut être lu que par le système d'exploitation Windows, les dispositifs de stockage formatés avec FAT peuvent être lus sur plusieurs plates-formes. De nombreuses fonctionnalités de NTFS surpassent FAT, notamment la prise en charge de fichiers de grande taille et la fonctionnalité de chiffrement de fichiers. Microsoft utilise NTFS pour installer ses versions modernes de Windows OS, telles que Windows 8 et 10, ainsi que les nouvelles éditions du serveur.

Stockage secondaire - suite

8. Environnement informatique

Votre choix de méthode pour collecter des preuves numériques sera fortement influencé par votre environnement informatique. Dans les années à venir, nous pouvons nous attendre à une transition significative des architectures informatiques centralisées vers des architectures informatiques non centralisées ou distribuées à mesure que la technologie progresse et que les vitesses Internet augmentent. Les environnements informatiques les plus courants sont les suivants :

- **Environnement de calcul personnel** : c'est probablement le plus courant de nos jours. Tous les programmes sont installés localement et s'exécutent sur la même machine dans cet environnement. Les données sont également enregistrées sur le disque dur local de la machine. Les environnements de calcul personnel comprennent les ordinateurs portables, les ordinateurs de bureau, les imprimantes, les tablettes et même les smartphones. Étant donné que l'emplacement des preuves est lié uniquement à l'appareil concerné, cet environnement est le plus facile à gérer si un appareil personnel devient une partie d'une enquête criminelle.
- **Environnement de calcul client-serveur** : il y a deux machines dans cet environnement : un client (par exemple, un ordinateur personnel, un ordinateur portable ou une tablette) et un serveur. Le client utilise une connexion HTTP pour demander des données au serveur, et le serveur répond avec des données. Le serveur de messagerie électronique que vous utilisez pour recevoir vos e-mails est un exemple d'un tel environnement.
- **Environnement de calcul distribué** : les applications sont installées et s'exécutent sur plusieurs ordinateurs dans cet environnement, permettant à une application de diviser ses fonctions en plusieurs composants, chacun s'exécutant sur son propre ordinateur. Dans ce type d'environnement, le stockage des données est également distribué, et les clients et autres applications doivent communiquer avec des serveurs distants via des réseaux pour accéder aux données ou exécuter des programmes. Dans un tel environnement, la collecte de preuves numériques est difficile car les données privées des utilisateurs et les journaux peuvent être dispersés sur plusieurs serveurs distants, qui peuvent être situés dans différentes régions géographiques et sous différentes juridictions. Dans de tels environnements, le volume de données (et de journaux) à examiner est également un problème, car le volume peut être énorme dans de nombreux cas.

Stockage secondaire - suite

8. Cloud Computing

Le Cloud Computing est un modèle technologique moderne qui permet à un prestataire de services de fournir divers services informatiques aux utilisateurs via Internet, en raison de la croissance explosive d'Internet et des communications en ligne. Par exemple, au lieu d'acheter un disque dur externe pour stocker vos données de sauvegarde, vous pouvez les stocker moyennant des frais modiques chez un fournisseur de Cloud. Le fournisseur de Cloud sera chargé de la gestion des données utilisateur dans le Cloud (par exemple, la création de copies de sauvegarde et la protection de ces données contre les logiciels malveillants et les cyberattaques). Le Cloud Computing n'est pas seulement destiné au stockage des données utilisateur, il est également utilisé par les entreprises pour réduire les coûts de l'infrastructure informatique. Au lieu d'acheter une licence logicielle pour chaque utilisateur individuellement, une entreprise peut utiliser un service de Cloud Computing qui fournit les applications nécessaires (comme la suite MS Office) pour son travail. Lorsque l'on utilise des logiciels coûteux tels que SQL Server et Windows Server OS, le coût semble être plus élevé ; cependant, payer pour ces logiciels sur une base d'utilisation dans le Cloud est plus rentable que de les installer sur site. Comme nous le verrons ci-dessous, les entreprises utilisent différents modèles de Cloud Computing.

- Logiciel en tant que service (SaaS):

Dans ce modèle, un utilisateur achète un compte de Cloud Computing, puis choisit les applications qu'il souhaite installer. Au lieu d'utiliser ces applications sur une machine locale, un utilisateur effectue son travail sur un serveur distant (Cloud). Google Apps for Education et Microsoft Office 365 sont deux exemples de tels services.

- Plateforme en tant que service (PaaS):

Ce modèle est populaire parmi les sociétés de développement de logiciels/Web, dans lequel un client - par exemple, une société de développement Web - paie pour un compte auprès d'un fournisseur de services Cloud qui fournit un environnement personnalisé en fonction des besoins du client (par exemple, pour installer les outils de développement Web nécessaires, préparer l'environnement de développement et de test, etc.). Cela permet à un client de commencer à travailler rapidement et à faible coût.

Stockage secondaire - suite

8. Cloud Computing

➢ Infrastructure en tant que service (IaaS):

Dans ce modèle, un fournisseur de cloud loue le matériel requis par le client (serveur physique et matériel de centre de données) via Internet. Le client achète et installe les applications et les systèmes d'exploitation nécessaires, puis les configure pour répondre aux exigences de l'entreprise. Les entreprises d'hébergement Web et les entreprises utilisent généralement ce service pour le stockage de données, la sauvegarde et la récupération en dehors de leurs bureaux. Ce qui nous intéresse dans cette discussion, c'est de savoir comment les services de cloud computing vont rendre plus difficile pour les forces de l'ordre d'enquêter sur les affaires criminelles. Par exemple, si un citoyen britannique est soupçonné dans une affaire criminelle et que ses données sont téléchargées sur un fournisseur de stockage en nuage à Singapour, la police britannique peut-elle obliger le fournisseur singapourien à remettre une copie des données utilisateur ?

9. Les versions de Windows

En tant qu'investigateur en informatique judiciaire, il est important de savoir comment collecter les informations actuelles sur les systèmes d'exploitation Windows afin d'être conscient des différences entre les versions lors des phases d'acquisition et d'analyse. Pour déterminer la version Windows actuelle sur un ordinateur exécutant Windows 8 ou une version ultérieure, suivez ces étapes :

➢ Appuyez et maintenez la touche Windows tout en maintenant également la touche R.

➢ Dans la zone de recherche, tapez "winver" et appuyez sur Entrée.

➢ Vous devriez voir la version Windows et le numéro de build (voir la figure 2.12).

PARTIE 1

Stockage secondaire - suite

10. Adresse de protocole internet (IP)

Au cours de vos enquêtes, vous rencontrerez probablement des informations qui nécessitent une compréhension du schéma d'adressage utilisé sur internet et de nombreux réseaux privés. Ainsi, la connaissance du protocole IP est essentielle pour tout enquêteur numérique. Dans cette section, nous aborderons le concept d'une adresse IP et la manière dont les dispositifs informatiques se connectent à internet.

Lorsqu'un dispositif informatique est connecté à un réseau IP, une adresse IP est attribuée à ce dernier afin de l'identifier de manière unique. Comme une adresse IP est similaire à une empreinte digitale, aucun deux dispositifs sur le même réseau IP ne peuvent avoir la même adresse IP. IP est souvent utilisé conjointement avec le protocole de contrôle de transmission (TCP), qui permet à un dispositif informatique d'établir une connexion virtuelle entre une destination et une source afin d'échanger des données. Les deux schémas d'adressage IP couramment utilisés sont l'IP version 4 et l'IP version 6. Le protocole IP v4 est le plus largement utilisé sur la planète ; il est actuellement utilisé par la majorité des services en ligne. L'IP v4 utilise un schéma d'adressage de 32 bits et peut contenir jusqu'à 4,3 milliards d'adresses ; cependant, en raison de la croissance rapide d'internet et du nombre croissant de dispositifs IoT, ce nombre est limité et risque bientôt d'être épuisé. Par conséquent, un autre standard connu sous le nom d'IP v6 a été développé, qui peut accueillir plus de 7,9 x 10^28 fois plus d'adresses que l'IP v4. Il existe deux types d'adresses IP : publiques et privées.

- **Adresses IP publiques** : Ces dernières sont attribuées par votre fournisseur de services internet (ISP) et permettent un accès internet direct. Chaque adresse IP est unique. Par exemple, un serveur de messagerie électronique nécessite une adresse IP publique unique à l'échelle mondiale.
  - **Adresses IP statiques :** Cette adresse, comme votre numéro de téléphone, est fixe et restera identique tant que l'ISP la réservera pour vous.
  - **Adresses IP dynamiques :** Ces dernières changent avec le temps. Elles sont attribuées automatiquement aux abonnés par l'ISP à l'aide d'un protocole appelé Dynamic Host Configuration Protocol (DHCP) chaque fois qu'ils se connectent à internet.
- **Adresses IP privées** (également connues sous le nom d'adresses IP locales) : Il s'agit d'une adresse IP non orientée vers internet pour les dispositifs généralement situés derrière un routeur. Tous les dispositifs existant dans un réseau fermé (par exemple, les réseaux domestiques ou scolaires) utiliseront des adresses IP privées. Ces adresses sont généralement attribuées automatiquement à l'aide du DHCP du routeur.

Conclusion

Dans ce chapitre, nous avons abordé des concepts techniques importants sur les ordinateurs qui doivent être bien compris par tout examinateur de la cybercriminalité. Nous avons décrit comment les ordinateurs stockent et représentent les données numériquement, la structure de fichiers du système d'exploitation et ses types, ainsi que les algorithmes de hachage et comment nous pouvons les utiliser pour vérifier l'authenticité de n'importe quelle pièce de données numériques. Dans le prochain chapitre, nous discuterons de la façon dont la cybercriminalité numérique fonctionne avec les dispositifs des utilisateurs et enquêterons sur les disques système, les disques durs et les systèmes de fichiers.

CHAPITRE 3

Disques durs et systèmes de fichiers

Ce que vous allez apprendre dans ce chapitre :

- Nous allons explorer dans cette partie, comment un système représente les données, ainsi que les systèmes de numérotation courants et la stratégie d'encodage principale utilisée par les machines pour générer du texte lisible par l'homme. Commençons par le système de numérotation standard..

Introduction

Mener une enquête de cybercriminalité exige une compréhension approfondie de certains des concepts technologiques fondamentaux de l'informatique. Pour découvrir et gérer les preuves numériques, il est nécessaire de comprendre comment l'information est stockée dans les ordinateurs, la théorie des nombres, comment les fichiers numériques sont construits et les différents types d'unités de stockage et leurs différences. Ces sujets fondamentaux seront couverts dans ce chapitre. Les ordinateurs stockent, traitent et affichent les données numériques d'une certaine manière, comme expliqué dans ce chapitre.

Disques durs et systèmes de fichiers

Les enquêtes en informatique judiciaire deviennent de plus en plus importantes avec l'augmentation des crimes impliquant des ordinateurs et internet. Des outils ont été créés pour aider les experts en informatique judiciaire à enquêter correctement sur les crimes numériques. Pour les services de renseignement, les services de police et les groupes militaires d'aujourd'hui, l'informatique judiciaire est un domaine de recherche en évolution et important. À mesure que de plus en plus de données sont stockées numériquement, la capacité d'évaluer et de filtrer ces données pour obtenir des preuves significatives est devenue de plus en plus complexe. Les informations obtenues par l'informatique judiciaire sont utilisées pour analyser et évaluer des données numériques en tant que preuves. La criminalistique numérique est un domaine relativement récent. L'utilisation de l'examen informatique judiciaire s'est avérée bénéfique dans un large éventail de processus judiciaires, et la zone d'analyse informatique judiciaire a connu une croissance rapide ces dernières années. La criminalistique numérique est utilisée pour examiner non seulement les crimes informatiques tels que la pénétration de réseau, la fabrication de données et la distribution non autorisée de matériel via des services numériques, mais aussi les crimes dans lesquels les preuves sont stockées dans tout support électronique sur tout dispositif numérique. L'espace de stockage en constante expansion des supports tels que les disques durs aggrave l'utilisation et la collecte de preuves numériques. Des technologies avancées de compression et de duplication de données sont largement utilisées dans les principales applications de stockage d'entreprise, indiquant que le développement rapide de la capacité de stockage ne se limite pas au domaine de la criminalistique.

Les disques durs et les systèmes de fichiers sont les principales sources de stockage de données; par conséquent, les comprendre est essentiel lors de l'enquête sur une infraction informatique. Pour éviter d'être détectées, les personnes suppriment souvent leurs traces après avoir commis un crime en utilisant un ordinateur. Lors de l'enquête sur une infraction informatique, la récupération de données supprimées à partir de disques durs et l'étude des systèmes de fichiers sont essentielles. Un système de fichiers, également appelé gestion de fichiers ou FS, est une méthode de contrôle de la façon dont et où les données sont stockées sur un disque de stockage. C'est un composant de stockage logique qui contient des fichiers qui sont divisés en groupes appelés répertoires.

Disques durs et systèmes de fichiers

Il s'agit d'un concept spécifique lié à l'utilisateur et à l'ordinateur, qui gère les opérations internes d'un disque. Les répertoires peuvent contenir des fichiers et des dossiers supplémentaires. Bien que Windows prenne en charge une variété de systèmes de fichiers, NTFS est le plus populaire dans le monde actuel. Il serait impossible d'avoir deux fichiers avec le même nom, ainsi que de supprimer des programmes installés et de récupérer des fichiers spécifiques sans gestion de fichiers. Les fichiers seraient également désorganisés sans structure de fichier. Parce que les fichiers sont gérés fréquemment dans une hiérarchie, le système de fichiers permet à l'utilisateur de visualiser un fichier dans le répertoire courant.

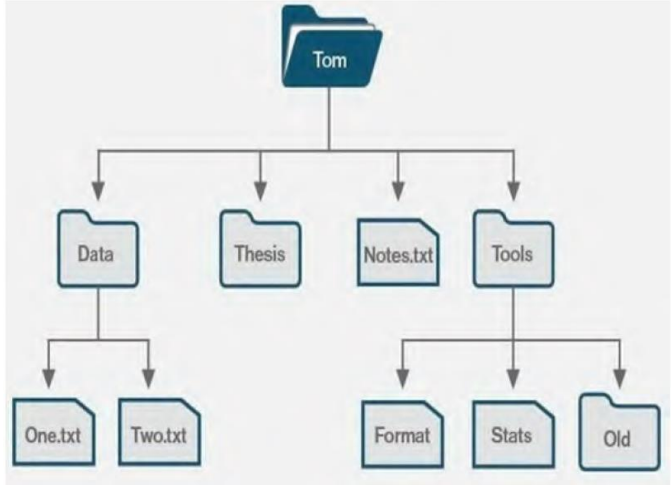
Indépendamment du type d'utilisation, un disque (par exemple, un disque dur) a un système de fichiers. Il inclut également des informations sur la taille du fichier, le nom du fichier, l'emplacement du fichier, les informations de fragmentation et où les données de disque sont stockées, ainsi que la façon dont un utilisateur ou une application peut accéder aux données. Le système de fichiers est responsable des métadonnées, de la dénomination des fichiers, de la gestion du stockage et de la gestion des répertoires/dossiers. Le système de fichiers est la technique de stockage et d'accès aux contenus de fichiers, tels que les données et les applications, en ligne. Les détails techniques de haut niveau des systèmes de fichiers sont abordés dans cet article, ainsi que des sujets connexes, tels que le cache de disque, le système de fichiers connecté au noyau et les API de niveau utilisateur qui exploitent les capacités du système de fichiers. Cela vous apprendra tout ce que vous devez savoir sur le fonctionnement général d'un système de fichiers. Le système de fichiers est la partie la plus importante du système d'exploitation. Il crée, manipule, stocke et récupère les données. Un système de fichiers est, à son niveau le plus élémentaire, une méthode de gestion de données sur un support de stockage secondaire. Il y a plusieurs niveaux en dessous et au-dessus du système de fichiers.

Les documents sont enregistrés dans des secteurs sur un dispositif de stockage et les données sont stockées dans des blocs, qui sont des groupes de secteurs. Le système de fichiers détermine la taille et l'emplacement des fichiers, ainsi que les secteurs prêts à être utilisés. Les systèmes de fichiers FAT et NTFS se trouvent dans une variété de systèmes d'exploitation autres que Windows. Cependant, les produits d'Apple (tels que iOS et macOS) utilisent HFS+ comme système d'exploitation, qui est compatible avec une large gamme de systèmes de fichiers.

Systèmes de fichiers

Systèmes de fichiers Lorsqu'on parle de partitions, le terme "système de fichiers" est parfois utilisé. Par exemple, "Deux systèmes de fichiers sont disponibles sur le disque dur" ne signifie pas nécessairement que le disque est partitionné en deux systèmes de fichiers, NTFS et FAT. Cela signifie plutôt qu'il existe deux partitions distinctes sur le même disque physique.

La plupart des applications avec lesquelles vous interagissez nécessitent un système de fichiers pour fonctionner ; par conséquent, chaque partition doit en avoir un. De plus, comme les programmes dépendent du système de fichiers, si un programme est conçu pour macOS, vous ne pourrez pas l'utiliser sur Windows. Voici quelques exemples de systèmes de fichiers :



- **FAT :** File Allocation Table (FAT) est un système de fichiers conçu spécifiquement pour les disques durs. Il signifie table d'allocation de fichiers et a été introduit pour la première fois en 1977. Il est utilisé pour chaque accès de cluster à la table d'allocation de fichiers et utilise 12 ou 16 bits (FAT). Il aide les systèmes d'exploitation Microsoft à gérer les fichiers sur les disques durs et d'autres systèmes informatiques. On le trouve également couramment dans des dispositifs tels que les appareils photo numériques, la mémoire flash et d'autres dispositifs portables, où il est utilisé pour stocker des informations de fichiers. Il aide également à prolonger la durée de vie d'un disque dur en réduisant l'usure de celui-ci. Les versions ultérieures de Microsoft Windows, telles que Windows XP, Vista, 7 et 10, n'utilisent plus FAT au profit de NTFS. Les différents types de FAT sont FAT8, FAT12, FAT32 et FAT16 (pour table d'allocation de fichiers).
- **GFS** : Global File System (GFS) a été développé pour la première fois à l'Université du Minnesota et permet à plusieurs ordinateurs de travailler ensemble comme une seule machine. Toutefois, Red Hat est maintenant responsable de son entretien. Lorsque deux ordinateurs ou plus sont séparés par une grande distance physique et ne peuvent pas s'envoyer des fichiers directement, un système de fichiers GFS leur permet de partager un groupe de fichiers directement. Avec l'aide d'un système de fichiers global, un ordinateur peut organiser son E/S pour préserver les systèmes de fichiers.

Systèmes de fichiers

- **Système de fichiers hiérarchique (HFS)** : c'est le système de fichiers qu'un ordinateur Macintosh utilise pour créer un répertoire lorsqu'un disque dur est formaté. Sa fonction principale est d'organiser et de stocker des fichiers sur un disque dur Macintosh. Depuis la sortie d'OS X, Apple ne peut plus prendre en charge l'écriture sur des disques HFS ou leur formatage. De plus, comme HFS est un format Macintosh, les ordinateurs Windows ne reconnaissent pas les lecteurs formatés en HFS. Les disques durs Windows sont formatés en utilisant les systèmes de fichiers WIN32 ou NTFS.
- **Le système de fichiers NTFS** (New Technology File System): stocke et récupère des fichiers sur le système d'exploitation Windows NT, ainsi que sur d'autres versions de Windows telles que Windows 2000, Windows XP, Windows 7 et Windows 10. Il offre des méthodes de récupération de fichiers et de protection de données plus performantes que les systèmes de fichiers FAT et HPFS, ainsi que plusieurs améliorations en termes d'extensibilité, de sécurité et de performances.
- **UDF :** est un système de fichiers qui signifie Universal Disk Format. Il a été créé en 1995 par l'association Optical Storage Technology Association (OSTA) pour garantir la cohérence des données sur plusieurs supports optiques. Il fonctionne avec des CD-ROM et des DVD-ROM, et est compatible avec tous les principaux systèmes d'exploitation. Il est maintenant utilisé dans le processus d'écriture de paquets pour les CD-R et les CD-RW.

FAT32 est un système de fichiers plus ancien qui est moins efficace que NTFS et possède un ensemble de fonctionnalités plus restreint, mais il est plus compatible avec d'autres systèmes d'exploitation. Bien que exFAT soit une alternative contemporaine à FAT32, et qu'il soit pris en charge par plus de dispositifs et de systèmes d'exploitation que NTFS, il n'est pas aussi largement utilisé que FAT32. Par défaut, Windows utilise NTFS, un système de fichiers contemporain. Le système de fichiers NTFS est installé lorsque vous installez Windows. Vous ne rencontrerez aucune contrainte de taille de fichier ou de partition avec NTFS car elles sont censées être si grandes. Bien qu'il ait fait ses débuts avec Windows NT, NTFS est arrivé pour la première fois dans les systèmes Windows grand public avec Windows XP. Le système de fichiers FAT32 est le plus ancien des trois systèmes de fichiers pris en charge par Windows. Il a été introduit pour la première fois dans Windows 95 pour remplacer le système de fichiers FAT16 utilisé dans MS-DOS et Windows 3. L'âge du système de fichiers FAT32 offre à la fois des avantages et des inconvénients. FAT32 a un avantage important en ce qu'il est la norme de facto en raison de son âge. Les clés USB achetées sont fréquemment formatées en FAT32 pour une compatibilité optimale avec les PC actuels, mais aussi avec d'autres appareils tels que les consoles de jeux et tout ce qui possède un port USB.

Systèmes de fichiers

Le système de fichiers exFAT a été lancé pour la première fois en 2006 et a ensuite été introduit dans les versions précédentes de Windows avec les mises à niveau de Windows XP et Vista. exFAT est un système de fichiers léger similaire à FAT32 qui est destiné aux clés USB, mais sans la fonctionnalité et les coûts supplémentaires de NTFS et les contraintes de FAT32. Comme NTFS, exFAT offre des restrictions de taille de fichier et de partition très importantes, vous permettant de stocker des données considérablement plus grandes que la limite de 4 Go de FAT32. Les disques durs internes doivent utiliser NTFS, tandis que les périphériques de stockage amovibles doivent utiliser exFAT. Si exFAT n'est pas pris en charge sur le périphérique, vous devrez utiliser FAT32 et vous devrez peut-être formater le disque externe en FAT32. Tout fichier numérique est enregistré sur un support de stockage de taille donnée. En réalité, chaque unité de stockage est un endroit linéaire pour la lecture ou la lecture des données numériques des livres. Chaque octet de données sur celui-ci a une adresse qui fait référence à son décalage à partir du début du stockage. Une grille de cellules numérotées peut être utilisée pour représenter le stockage. Tout objet enregistré dans le stockage reçoit son propre ensemble de cellules.

Les systèmes de fichiers de disques/tapes, les systèmes de fichiers de réseau et les systèmes de fichiers spécialisés sont les trois types de systèmes de fichiers.

- **Les systèmes de fichiers de disques:** Un système de fichiers de disque utilise la capacité des supports de stockage de disque à résoudre les données de manière aléatoire en un court laps de temps. D'autres facteurs à prendre en compte comprennent la vitesse à laquelle les données sont accessibles après la demande initiale, ainsi que la possibilité de rechercher des preuves supplémentaires. Cela permet à plusieurs utilisateurs (ou applications) de récupérer des données différentes sur le disque, quel que soit le placement séquentiel des données.
- **Système de fichiers flash**: prend en compte les capacités, les performances et les limites des dispositifs de mémoire flash. Un système de fichiers de disque peut souvent être utilisé comme support de stockage sous-jacent pour un dispositif de mémoire flash, mais il est préférable d'utiliser un système de fichiers spécialement conçu pour un dispositif flash.

Systèmes de fichiers

- **Le système de fichiers de bande** est un système de fichiers et un format de bande pour stocker des fichiers auto-descriptifs sur bande. Les bandes magnétiques sont des supports de stockage séquentiels qui prennent beaucoup plus de temps pour récupérer des données aléatoires que les disques, ce qui rend la construction et la maintenance d'un système de fichiers généraliste difficile. Dans un système de fichiers de disque, il y a généralement un répertoire principal de fichiers et une carte des zones de données utilisées et libres. Toutes les modifications, ajouts ou suppressions de fichiers nécessitent une mise à jour du répertoire et des cartes utilisées/libres. Cette approche fonctionne bien pour les disques car l'accès aléatoire aux zones de données se mesure en millisecondes. Pour dérouler et enrouler potentiellement des bobines de matériel extrêmement longues, la bande nécessite un mouvement linéaire. Le déplacement de la tête de lecture/écriture d'une extrémité de la bande à l'autre peut prendre de quelques secondes à plusieurs minutes.
- **Les systèmes de fichiers de base de données :** La notion de système de fichiers de système de données est une autre approche pour la gestion de fichiers. Les fichiers sont reconnus par leurs attributs, tels que le type de fichier, le sujet, l'auteur ou d'autres informations riches, au lieu d'une gestion organisée de manière hiérarchique ou en conjonction avec celle-ci. IBM DB2 pour I (anciennement connu sous les noms de DB2/400 et DB2 pour i5/OS) est un système de fichiers de base de données qui s'exécute sur les systèmes IBM Power et fait partie de l'OS IBM I basé sur des objets (anciennement connu sous les noms de OS/400 et i5/OS). Il a un magasin à un seul niveau.
- **Les systèmes de fichiers transactionnels** : Certaines applications ont besoin de mises à jour "tout en une fois" pour de nombreux fichiers. Une installation de logiciel, par exemple, peut créer des binaires de programme, des modules et des données de configuration. L'application peut devenir inopérante si l'installation de logiciel échoue. Si un outil système crucial, tel que la ligne de commande, est mis à niveau pendant l'installation, l'ensemble du système peut devenir inutile. La promesse d'isolation, qui spécifie que les activités à l'intérieur d'une transaction restent cachées des autres processus sur l'ordinateur jusqu'à ce que la transaction soit confirmée et que les opérations conflictuelles sur le réseau soient correctement sérialisées avec la transaction, est introduite par le traitement de transaction. Les transactions offrent également la garantie d'atomicité, assurant que les activités à l'intérieur d'une transaction sont soit entièrement engagées, soit que l'opération peut être annulée, avec des résultats incomplets étant rejetés par le système.

Systèmes de fichiers

- **Le système de fichiers de réseau** est un dispositif de stockage qui fonctionne comme un client pour une interface d'accès à des fichiers distants, offrant un accès aux fichiers sur un serveur. Les programmes utilisant des interfaces locales peuvent facilement créer, maintenir et accéder à des structures de dossiers hiérarchiques dans des systèmes distants connectés en réseau.
- **Le système de fichiers de disque partagé** est un système dans lequel un certain nombre d'appareils connectés (généralement des serveurs) ont tous des connexions au même sous-système de disque externe (généralement un SAN) (généralement un SAN). Le système de fichiers adjudique l'accès à ce sous-système, éliminant les collisions d'écriture. Des exemples comprennent GFS2 de Red Hat, GPFS d'IBM, SFS de DataPlow, CXFS de SGI et StorNext de Quantum Corporation.

➢ **Systèmes de fichiers spéciaux** : Un système de fichiers personnalisé affiche des aspects non fichiers d'un système d'exploitation sous forme de fichiers afin qu'ils puissent être traités à l'aide d'API de système de fichiers. Cela est généralement fait dans les systèmes d'exploitation de type Unix, bien que les périphériques se voient également attribuer des noms de fichiers dans plusieurs systèmes d'exploitation non de type Unix.

➢ **Système de fichiers minimal** : La fin des années 1970 a vu l'émergence de l'ordinateur personnel. Les dispositifs de disque et de bande magnétique numérique étaient trop coûteux pour les amateurs. Un dispositif de stockage de données de base abordable a été conçu qui utilisait une cassette audio standard. Lorsque le système avait besoin d'écrire des données, l'utilisateur était invité à appuyer sur "ENREGISTRER" sur l'enregistreur à cassette, puis sur "RETOUR" sur le clavier pour indiquer à l'ordinateur que l'enregistreur à cassette était en train d'enregistrer. Le système a écrit un son pour établir une synchronisation temporelle, puis a modulé des bruits qui codent un préambule, les données, une somme de contrôle et un suffixe. Lorsque le système avait besoin de lire des données, l'utilisateur était invité à appuyer sur "LECTURE" sur l'enregistreur à cassette.

➢ **Système de fichiers plat** : Il n'y a pas de sous-répertoires dans un système de fichiers plat. En raison de la capacité de données limitée disponible lors de l'introduction initiale du support de disquette, cette forme de système de fichiers était appropriée. Les ordinateurs CP/M utilisaient un système de fichiers plat, dans lequel les fichiers étaient alloués à l'une des 16 régions utilisateur, et les opérations de fichiers générales étaient limitées à travailler sur un seul groupe au lieu de tous. Ces zones utilisateur étaient simplement des propriétés uniques associées aux fichiers; par conséquent, aucune attribution explicite n'était nécessaire pour chacune de ces zones, et les fichiers pouvaient être ajoutés à des groupes tant qu'il y avait encore de l'espace de stockage disponible sur le disque

Systèmes de fichiers

Le système de fichiers physique, qui est la troisième couche, est responsable du tampon et de la gestion de la mémoire. Il est concerné par le fonctionnement physique du périphérique de stockage et traite les blocs physiques qui sont en cours de lecture ou d'écriture, comme présenté dans la figure. Cette couche interagit également avec les pilotes de canal et de périphérique pour piloter le périphérique de stockage.

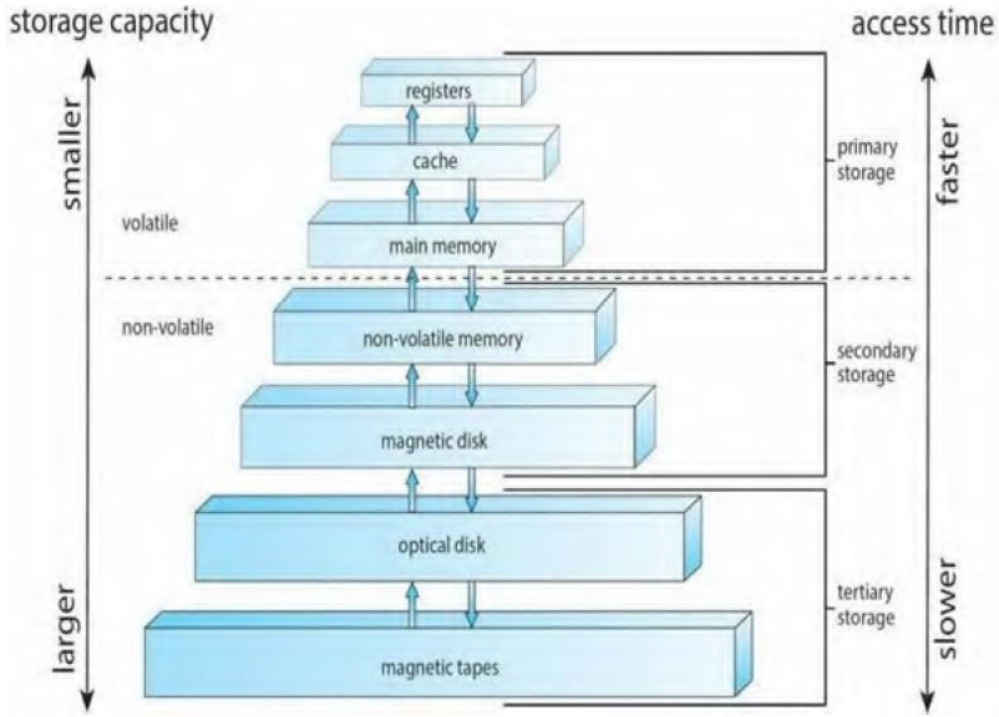
La capacité de mémoire et le coût sont inversément proportionnels à la vitesse dans la hiérarchie de la mémoire. Les dispositifs sont regroupés du plus rapide au plus lent ou du registre à la mémoire tertiaire dans ce diagramme. À l'intérieur du processeur, il y a des registres. Ils ont le temps d'accès le plus rapide car ils sont à l'intérieur du processeur. Les registres sont les plus coûteux et ont la plus petite capacité de stockage, généralement mesurée en kilo-octets. Des bascules sont utilisées pour les implémenter. La mémoire cache est utilisée pour stocker les parties du programme auxquelles le CPU accède souvent. Elle est coûteuse et plus petite en taille, généralement mesurée en mégaoctets, et elle est réalisée en utilisant de la RAM statique. Par l'intermédiaire d'un processeur d'E/S, elle interagit directement avec le CPU et les autres dispositifs de mémoire. La figure 3.3 montre la hiérarchie de la mémoire de stockage. La mémoire principale est moins coûteuse que la mémoire cache et a une capacité de stockage plus importante, généralement mesurée en gigaoctets. La RAM dynamique est utilisée pour implémenter cette mémoire.

File Type	Usual extension	Function
Executable	exe, com, bin or none	ready-to-run machine-language program
Object	obj, o	complied, machine language, not linked
Source code	c, p, pas, 177, asm, a	source code in various languages
Batch	bat, sh	commands to the command interpreter
Text	txt, doc	textual data documents
Word processor	wp, tex, rrf, etc.	various word-processor formats
Library	lib, a	libraries of routines
Print or view	ps, dvi, gif, pdf	ASCII or binary file
Archive	arc, zip, tar, gz	related files grouped into one file, sometimes compressed.

Systèmes de fichiers

Au niveau 3, des dispositifs de stockage secondaires tels que des disques magnétiques sont présents. Ils sont utilisés pour stocker des données de sauvegarde. Ils sont moins chers que la mémoire principale et ont une capacité plus grande de quelques To. Au niveau 4, des systèmes de stockage tertiaires tels que des bandes magnétiques sont présents. Ils sont les moins chers et les plus grands en taille et sont utilisés pour stocker des données amovibles (1-20 To). La hiérarchie de la mémoire est le processus d'organisation de plusieurs types de stockage sur un ordinateur en fonction de la vitesse d'accès. Les registres du CPU, qui sont les plus rapides à lire et à écrire, constituent la mémoire la plus performante en haut de la hiérarchie.

La mémoire cache vient ensuite, suivie de la mémoire DRAM traditionnelle, et enfin, du stockage sur disque avec différents niveaux de performance, tels que les SSD, les disques optiques et magnétiques. Pour combler ou éliminer l'écart de performance entre le CPU et la mémoire, les concepteurs matériels dépendent de plus en plus de la mémoire en haut de la hiérarchie de la mémoire. Cela est accompli en créant des hiérarchies de cache plus grandes (que les processeurs peuvent atteindre considérablement plus rapidement), en minimisant le besoin de mémoire principale plus lente.



MEMORY HIERARCHY OF STORAGE

PARTIE 1

Disque dur

Malgré la croissance explosive des appareils tels que les smartphones et les PDA ces derniers jours, le disque dur reste un sujet courant d'analyse forensique informatique. La conception de base du disque dur est restée essentiellement inchangée depuis son lancement ; cependant, des révisions apportées aux éléments individuels ont entraîné des augmentations significatives de la vitesse, de la capacité et de la fiabilité. Les quatre composants clés de la structure interne d'un disque dur conventionnel sont brièvement détaillés comme suit. Le plateau de disque, le bras de tête, le châssis et l'actionneur de tête sont les quatre composants. Le châssis est la partie du disque dur qui sert de fondation et de support pratique. Les plateaux sont des disques circulaires placés sur un pôle central appelé broche et empilés les uns sur les autres. Les plateaux ont un revêtement de chaque côté qui leur permet de conserver des informations de manière magnétique. Les pistes sont des cercles concentriques qui contiennent des données sur les côtés supérieur et inférieur du disque.

Lorsqu'un disque est allumé et que des données doivent être lues ou écrites, les plateaux tournent à une vitesse très rapide, permettant au bras d'actionnement et à ses composants accompagnants de lire la région appropriée du disque. Un petit dispositif appelé tête de lecture/écriture doit être situé juste au-dessus de la surface du plateau pour lire ou écrire des données sur ou à partir d'un disque, c'est-à-dire sur ou à partir d'un plateau. La tête de lecture/écriture est couplée à un "curseur de tête", qui est lui-même attaché au bras de tête, afin de le positionner avec précision. Le nombre de plateaux contrôle le nombre de bras de tête dans un disque dur, chaque bras étant utilisé pour placer une tête de lecture/écriture sur le côté opposé d'un plateau. Un bras d'actionneur, un ensemble d'actionneurs ou un ensemble de têtes est une structure qui relie les bras de tête. L'ensemble pivote sur un axe qui permet aux têtes de lecture/écriture de se déplacer autour de la surface du plateau afin de les positionner correctement sur les plateaux. Ce mouvement, associé à la rotation du plateau, permet aux têtes d'être correctement positionnées.

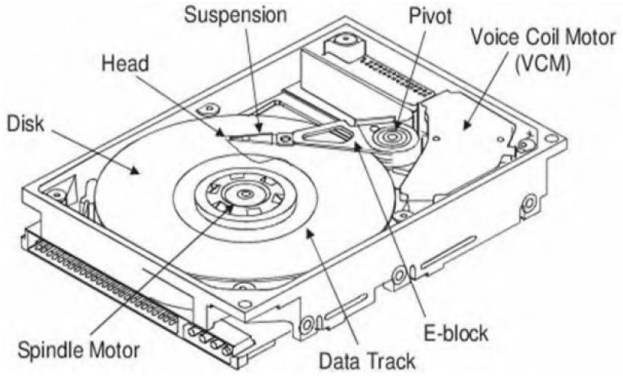
Un disque dur, tel qu'illustré dans la figure 3.4, est un dispositif scellé qui se compose d'une pile de plateaux. Les disques durs peuvent être installés horizontalement ou verticalement. Dans cet exemple, le disque dur est positionné horizontalement. Au-dessus et en dessous de chaque disque, des têtes de lecture/écriture magnétiques sont positionnées. Les têtes de disque se déplacent vers l'intérieur vers le centre des plateaux et vers l'extérieur vers les bords lorsqu'elles tournent. De cette manière, les têtes de disque peuvent accéder à toute la surface de chaque plateau. Les données sont stockées sur un disque dur dans des bandes minces et concentriques. Une tête de disque dans une position donnée peut lire ou écrire une piste, qui est une bague circulaire ou une bande. Sur un disque dur de 3,5 pouces, il peut y avoir plus d'un millier de pistes. Les secteurs sont des sections individuelles de chaque piste. L'unité de stockage physique la plus petite sur un disque est un secteur, qui est généralement toujours de 512 octets (0,5 Ko)

Disque dur - Suite

Le texte parle de la nomenclature de cylindre/tête/secteur utilisée dans la construction des anciens disques durs (c'est-à-dire avant Windows 95). Lorsque toutes les têtes de lecture du disque sont dans la même position, un cylindre est produit. Les pistes créent un cylindre lorsqu'elles sont empilées les unes sur les autres. Cette approche est progressivement abandonnée avec les disques durs contemporains. Tous les nouveaux disques utilisent un facteur de traduction pour rendre leur disposition matérielle réelle continue, car c'est ainsi que les systèmes d'exploitation à partir de Windows 95 aiment fonctionner. Les pistes sont des structures conceptuelles plutôt que physiques aux yeux du système d'exploitation de l'ordinateur, et elles sont créées lors du formatage de bas niveau du disque. Les plateaux dans la pile tournent à la même vitesse, mais la tête de lecture lit à partir d'une surface plus lente près du centre du disque que des bords extérieurs du disque. Les pistes situées sur la périphérie du disque sont moins densément remplies de données que les pistes situées au centre du disque pour compenser cette différence physique.

En raison de la densité de données variable, le même nombre d'informations peut être lu en même temps à partir de n'importe quelle position de la tête de lecture. Un plan typique est utilisé pour remplir l'espace disque avec des données. Le système d'exploitation n'a pas accès à un côté d'un plateau d'un ensemble de disques, qui est réservé aux informations de positionnement de piste de matériel. Par conséquent, les données peuvent être stockées sur trois côtés d'un ensemble de disques à deux plateaux. Lors de l'assemblage en usine, des données sont enregistrées sur le disque. Ces données sont lues par le contrôleur de disque système, qui place ensuite les têtes de lecture dans la situation de secteur correcte.

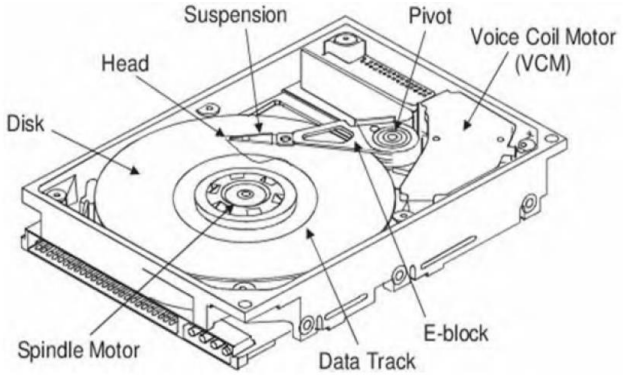
Étant donné que 512 est une puissance de deux, un secteur, qui est la plus petite unité de stockage physique sur le disque, fait presque toujours 512 octets. Étant donné que les langages informatiques les plus fondamentaux ont seulement deux états - allumé et éteint - le nombre 2 est utilisé. Les informations de positionnement de la piste d'usine sont utilisées pour marquer chaque secteur du disque.



PARTIE 1

Disque dur - Suite

L'identité de secteur écrit des données dans la région juste avant le contenu du secteur, et elle indique l'adresse de début du secteur. Une série continue, ou toutes les données stockées séquentiellement de bout en bout dans une seule phrase, est la meilleure approche pour stocker un fichier sur un disque. Un ou plusieurs secteurs successifs peuvent former un groupe. Le nombre de secteurs est toujours divisible par deux. Un groupe peut être aussi petit qu'un secteur ou aussi grand que huit secteurs. Le seul nombre impair de secteurs qui peut constituer un groupe est 1. Ce ne pourrait pas être cinq secteurs ou un nombre pair qui n'est pas divisible par deux. Ce ne serait pas dix secteurs, mais plutôt huit ou seize. Les groupes sont ainsi nommés parce que l'espace est réservé pour les données. Cette technique empêche l'écrasement des données enregistrées. Si le fichier est ultérieurement étendu à une taille de 1600 octets, deux groupes supplémentaires sont alloués, permettant à l'ensemble du fichier d'être stocké dans quatre ordinateurs domestiques d'aujourd'hui qui utilisent des disques qui tournent à une vitesse constante. Les pistes à l'extrémité du disque sont moins densément remplies de données que celles vers le cœur du disque. En conséquence, même si la vitesse de la surface du disque est plus rapide sur les pistes positionnées plus loin du centre du disque, une quantité fixe de données peut être lue dans une durée constante. Les disques modernes réservent un côté d'un plateau pour les données de positionnement de la piste, qui sont enregistrées sur le disque lors de la fabrication du disque aux groupes d'usine. Le système d'exploitation n'y a pas accès. Lorsque les têtes se déplacent vers un autre point sur le disque, le contrôleur de disque utilise ces données pour affiner les emplacements de tête. Lorsqu'un site dispose d'informations sur l'emplacement de la piste, il ne peut pas être utilisé pour les données. En conséquence, un ensemble de disques avec deux plateaux a trois côtés disponibles pour les données.



PARTIE 1

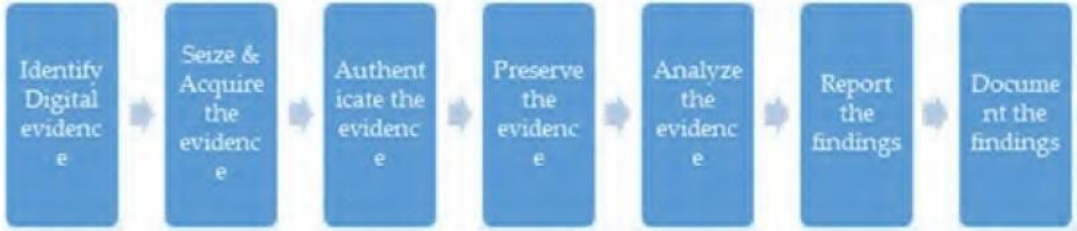
La forensique de disque dur

La forensique de disque dur est le processus d'extraction de données exploitables à partir du stockage informatique afin de l'utiliser comme preuve dans des affaires criminelles. La procédure nécessite souvent de récupérer et recréer du matériel qui a été effacé ou détruit. De plus, les ordinateurs personnels des criminels et des fraudeurs peuvent inclure des éléments de preuve cruciaux qui pourraient mener à une résolution rapide d'une affaire criminelle et à une punition.

Texial dispose d'un laboratoire de forensique cybernétique de pointe et utilise certains des meilleurs et des plus brillants experts de l'industrie. Nous nous spécialisons dans la récupération de données forensiques à partir de disques durs physiquement détruits par des criminels pour cacher leurs traces, quelle que soit leur dissimulation ou leur suppression. Il existe plusieurs avantages à la forensique de disque dur. Voici quelques-uns des plus importants :

- Les informations des disques durs sont recherchées et extraites.
- Les données corrompues du stockage informatique sont récupérées et reconstruites.
- La récupération de données à partir de disques durs cachés ou cryptés est effectuée. Les hackers en profitent.

L'étude de la récupération de preuves forensiques à partir de supports de stockage numérique tels que les disques durs, les clés USB, les périphériques Firewire, les CD, les DVD, les disques flash et les disquettes est connue sous le nom de forensique de disque dur.



PARTIE 1

La forensique de disque dur

La forensique de disque dur est le processus d'extraction de données exploitables à partir du stockage informatique afin de l'utiliser comme preuve dans des affaires criminelles. La procédure nécessite souvent de récupérer et recréer du matériel qui a été effacé ou détruit. De plus, les ordinateurs personnels des criminels et des fraudeurs peuvent inclure des éléments de preuve cruciaux qui pourraient mener à une résolution rapide d'une affaire criminelle et à une punition.

Texial dispose d'un laboratoire de forensique cybernétique de pointe et utilise certains des meilleurs et des plus brillants experts de l'industrie. Nous nous spécialisons dans la récupération de données forensiques à partir de disques durs physiquement détruits par des criminels pour cacher leurs traces, quelle que soit leur dissimulation ou leur suppression. Il existe plusieurs avantages à la forensique de disque dur. Voici quelques-uns des plus importants :

- Les informations des disques durs sont recherchées et extraites.
- Les données corrompues du stockage informatique sont récupérées et reconstruites.
- La récupération de données à partir de disques durs cachés ou cryptés est effectuée. Les hackers en profitent.

L'étude de la récupération de preuves forensiques à partir de supports de stockage numérique tels que les disques durs, les clés USB, les périphériques Firewire, les CD, les DVD, les disques flash et les disquettes est connue sous le nom de forensique de disque dur.

La première phase est également connue sous le nom de phase de reconnaissance, au cours de laquelle nos experts en cybersécurité rassemblent autant d'informations que possible sur la cible avant de lancer une attaque. L'identification des dispositifs de stockage sur le lieu du crime, tels que les disques durs avec interfaces IDE/SATA/SCSI, les CD, les DVD, les disquettes, les téléphones portables, les assistants personnels, les cartes flash, les cartes SIM, les disques USB/Firewire, les bandes magnétiques, les disques Zip, les disques Jazz, et ainsi de suite, est la première étape de la forensique de disques. Ce sont quelques-unes des sources de preuves numériques. La prochaine étape consiste à saisir les supports de stockage pour acquérir des preuves numériques. Cette étape est effectuée sur le lieu du crime. En utilisant un programme de cyber forensique approprié, la valeur de hachage des supports de stockage à saisir est calculée à cette phase. Une valeur de hachage est une signature unique créée par un algorithme de hachage statistique qui est basé sur le contenu du support de stockage. Une fois que la valeur de hachage est calculée, le support de stockage est emballé de manière sécurisée et récupéré pour un traitement ultérieur. Cette phase est également connue sous le nom de phase de reconnaissance, au cours de laquelle nos experts en cybersécurité rassemblent autant d'informations que possible sur la cible avant de lancer une attaque.

La forensique de disque dur

"Ne travaillez jamais sur des preuves originales" est l'une des lois cardinales de la Cyber Forensics. Pour garantir que ce critère est respecté, une réplique identique de la preuve originale doit être générée pour l'analyse et la collecte de preuves numériques. Le processus de création de cette copie précise, dans lequel le support de stockage source est protégé en écriture et la copie en flux de bits est utilisée pour vérifier que toutes les données sont transférées vers le support de destination, est appelé acquisition. Dans la plupart des cas, le support source est acquis dans un laboratoire de Cyber Forensics.

u laboratoire de Cyber Forensics, l'authenticité des preuves est vérifiée. Les valeurs de hachage des supports source et de destination sont vérifiées pour confirmer qu'elles sont identiques, garantissant que le contenu du support de destination est une réplique identique de celui du support source. Les preuves électroniques peuvent être altérées ou manipulées sans laisser de trace. Les preuves réelles doivent être stockées dans un endroit sûr, à l'abri des sources électromagnétiques et de radiation, une fois qu'elles ont été acquises et authentifiées. Une autre copie de l'image doit être réalisée et conservée sur un support approprié ou dans un système de stockage de masse fiable. Les médias optiques peuvent être utilisés comme support de stockage de masse. Ils sont fiables, rapides, ont une longue durée de vie et peuvent être réutilisés.

Dans le processus de Cyber Forensics, il est crucial de vérifier les preuves avant de commencer l'analyse. Cette vérification est effectuée au laboratoire de Cyber Forensics avant de commencer une analyse. La valeur de hachage des preuves est calculée et comparée à celle obtenue lors de l'acquisition. S'il n'y a pas de différence entre les deux valeurs, l'essence des preuves est la même. S'il y a une différence, le contenu des preuves a été altéré. Les résultats de la vérification doivent être documentés avec précision. Le rapport d'analyse de cas devrait refléter le type d'examen demandé par un tribunal ou un organisme d'enquête. Il devrait inclure les informations suivantes : la nature de l'affaire, l'examen demandé, les objets physiques et les valeurs de hachage, les résultats de la vérification des preuves, l'analyse effectuée et les preuves numériques obtenues, les observations de l'examinateur et la conclusion. Les personnes non techniques devraient être en mesure de comprendre le rapport s'il est présenté dans un langage simple et détaillé.

Analyse des fichiers de registre

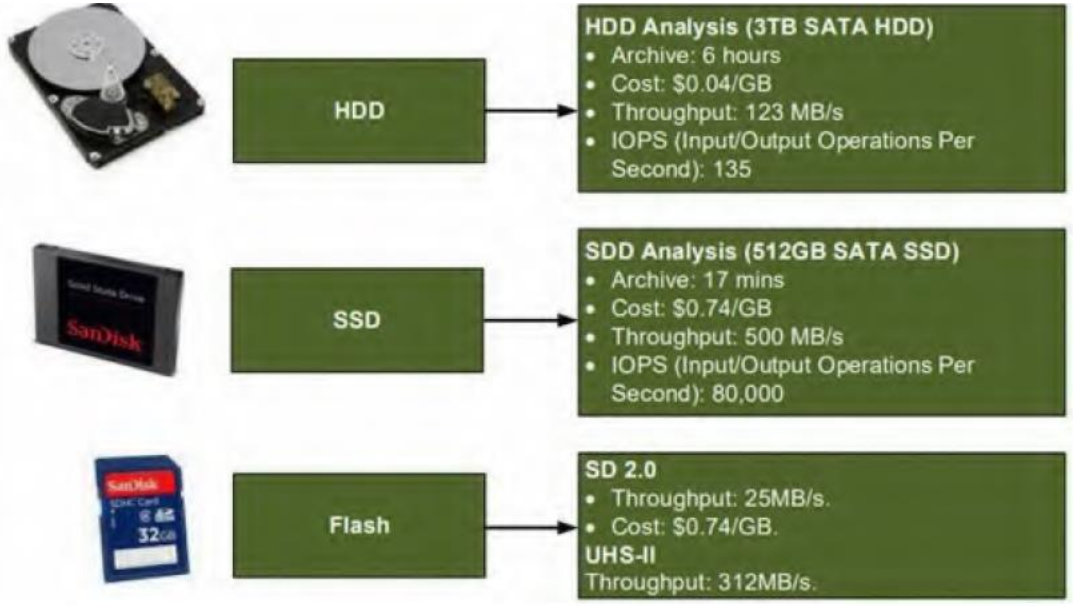
Étant donné que la plupart des utilisateurs ignorent la fonction du système, ils laissent des traces de leurs activités sur celui-ci, en particulier dans le registre. L'analyse de ces données fournit à l'investigateur une connaissance préliminaire de l'environnement du système ainsi qu'une orientation pour les enquêtes futures. L'extraction de preuves essentielles est extrêmement difficile et chronophage en raison de la structure complexe du registre. Ce package automatisera le travail d'examen du registre de Windows 7 pour les enquêteurs en forensics afin de résoudre ces défis. Cela améliorera l'analyse standard du registre en donnant aux enquêteurs un avantage dans l'analyse forensique en cachant les informations non pertinentes et en mettant en évidence les informations cruciales du registre, ainsi qu'en réduisant le temps nécessaire à l'analyse du registre de Windows. RegAlyzer est un outil de navigation et d'édition de registre. Il a été conçu pour combler plusieurs lacunes de l'outil regedit précédent, telles que le support de types de valeurs inhabituels, la recherche par motif, les signets améliorés et l'affichage des fichiers .reg dans la mise en page familière, ainsi qu'une vue d'historique. RegAlyzer 2, qui est maintenant en version bêta, aura une interface à onglets multiples, des interprétations de valeurs, des noms permanents pour les variables et des instantanés de ruche pour suivre les changements.

Faire plusieurs copies du matériel qui sera utilisé ultérieurement dans l'analyse forensique d'un décès est crucial. Ce module facilite la procédure d'acquisition en permettant la création de copies/images brutes de disques durs et de clés USB qui pourront être utilisées pour l'enquête forensique ultérieurement. Étant donné que la fonctionnalité des flux de données alternatifs du système de fichiers NTFS permet aux personnes de masquer des données dans le système de fichiers, les enquêteurs forensiques doivent garder cela à l'esprit lorsqu'ils enquêtent sur des ordinateurs Windows utilisant le système de fichiers NTFS. Les flux de données alternatifs dans les fichiers supprimés sont tout aussi importants, bien qu'ils puissent être ignorés car les professionnels forensiques ne sont pas familiarisés avec eux. Ce module aide à la découverte de données cachées dans des flux de données alternatifs à différents emplacements, tels que des fichiers, des dossiers et des partitions, ainsi que des données contenues dans des flux de données alternatifs de fichiers supprimés.

En forensique informatique, les données enregistrées dans les fichiers sont la source principale de preuves. Ces fichiers sur le disque sont gérés via le système de fichiers. Un auteur peut effacer des preuves d'un disque dur en supprimant les fichiers relatifs aux preuves. Il est crucial pour les enquêteurs forensiques de récupérer des preuves qui ont été effacées par le défendeur.

Analyse des fichiers de registre

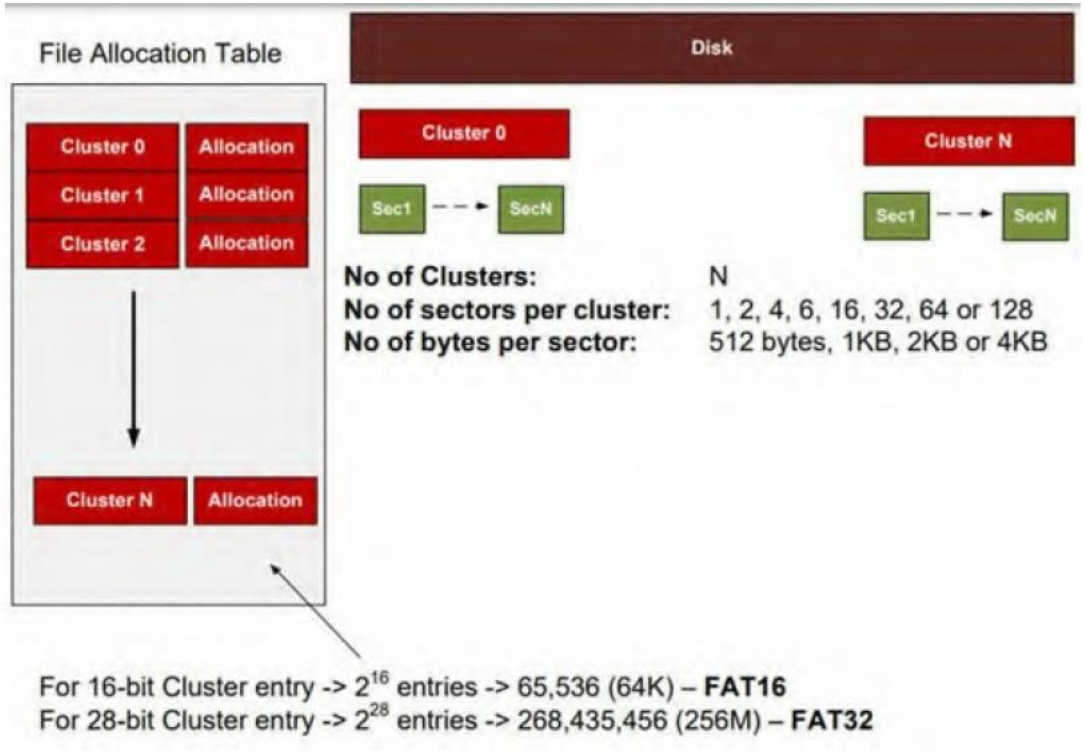
Ce composant aide les enquêteurs forensiques à récupérer des fichiers supprimés à partir de disques durs formatés en NTFS et de clés USB, et à analyser le moment où le système informatique est allumé et la personne qui est connectée à ce moment peut révéler des informations importantes qui peuvent être liées à d'autres preuves. Par exemple, sur un système de fichiers NTFS, l'heure de suppression du fichier peut être reliée à la personne qui était connectée à ce moment-là pour déterminer qui a supprimé les fichiers. En fournissant une chronologie des événements de connexion et de déconnexion de l'utilisateur, ce module aide les enquêteurs forensiques à analyser le comportement de l'utilisateur sur l'ordinateur. La figure ci-dessous montre la comparaison des disques durs, des disques SSD et de la mémoire flash.



Analyse des fichiers de registre

La figure suivante affiche la structure de la table d'allocation de fichiers.

Dans l'environnement actuel, la forensique informatique est nécessaire en raison de la prévalence de la cybercriminalité. Étant donné que Windows 7 est un système d'exploitation largement utilisé, les enquêtes forensiques devraient se concentrer sur ses artefacts, tels que le registre, les fichiers journaux et le système de fichiers NTFS. Les outils aident dans le processus d'analyse ; par conséquent, il est nécessaire de développer des outils pour aider dans les enquêtes forensiques. Ainsi, nous avons suggéré et créé un programme pour l'enquête forensique de Windows 7. Notre projet aidera les enquêteurs forensiques à entreprendre des enquêtes forensiques informatiques des fichiers du registre et du système NTFS de Windows 7 sur des machines Windows 7 en économisant du temps et de l'argent. Faire plusieurs copies de matériel qui seront utilisées ultérieurement dans l'analyse forensique est essentiel. Ce composant aide dans le processus d'acquisition en permettant la création de copies/ images brutes de disques durs et de clés USB qui peuvent être utilisées pour une enquête forensique ultérieure. Étant donné que la fonctionnalité des flux de données alternatifs du système de fichiers NTFS permet aux utilisateurs de masquer des données dans les fichiers système, les enquêteurs forensiques doivent en tenir compte lors de l'investigation des PC Windows utilisant le système de fichiers NTFS. Les flux de données alternatifs dans les fichiers supprimés sont tout aussi importants, bien qu'ils puissent être ignorés car les professionnels forensiques ne sont pas familiers avec eux.



PARTIE 1

Analyse des fichiers de registre

En matière de forensique numérique, le contenu stocké dans les fichiers est la principale preuve. Ces fichiers sur le disque dur sont gérés via le système de fichiers. Un auteur peut effacer une preuve à partir d'un disque dur en supprimant les fichiers liés à la preuve. Il est essentiel que les enquêteurs forensiques récupèrent les preuves qui ont été effacées par l'auteur. Ce composant aide les enquêteurs forensiques à récupérer des fichiers supprimés à partir de disques durs formatés en NTFS et de clés USB et à analyser le moment où l'ordinateur est allumé, et la personne qui s'est connectée à ce moment-là pourrait révéler des données cruciales qui peuvent être liées à d'autres preuves. Par exemple, sur un système de fichiers NTFS, l'heure de suppression du fichier peut être reliée à la personne qui était connectée à ce moment-là pour déterminer qui a supprimé les fichiers. En fournissant une chronologie des événements de connexion et de déconnexion de l'utilisateur, ce composant aide les enquêteurs forensiques à analyser le comportement de l'utilisateur sur l'ordinateur. Dans la société actuelle, où les données sont l'aspect le plus crucial de la vie humaine, il est essentiel de comprendre comment les données peuvent être perdues et si elles peuvent être récupérées. Le concept de récupération de données est présenté dans la première partie, suivi d'une discussion sur la raison pour laquelle c'est nécessaire. Ensuite, nous discuterons des procédures de récupération de données et des obstacles. Les entreprises dépendent de plus en plus des ordinateurs pour interagir avec des documents internes et externes, et le stockage numérique est de plus en plus important. La plupart des efforts se sont concentrés sur des problèmes connus tels que les infections et les vulnérabilités.

Chaque fois que les données ne peuvent pas être accessibles normalement, une récupération de données est effectuée. Cela peut être causé par des dommages physiques ou logiques aux fichiers système, les empêchant d'être installés par le système hôte. Les dommages logiques ou physiques au mécanisme de fichier pour l'empêcher d'être installé par le système hôte peuvent nécessiter une récupération. La perte de données peut se produire en raison d'erreurs physiques et logiques, ainsi que de l'écrasement de données. Et il existe plusieurs approches pour chacune de ces trois exigences. Des problèmes internes ou externes ont causé la perte ou les dommages de données. La souffrance a été aggravée par l'augmentation de la hâte et du rythme de vie, ce qui a entraîné la suppression involontaire de données utiles importantes. Cela ne montre qu'un côté de l'importance de la récupération de données; l'autre aspect est l'importance médico-légale de la récupération de données. La distinction que les besoins médico-légaux ont est que les données ne peuvent pas être supprimées par erreur ici, mais cela crée également une distinction dans la méthode de récupération car la récupération sera difficile dans ce cas car la suppression a été faite dans le but que les données ne soient jamais récupérées. De nombreuses défaillances peuvent entraîner des dommages physiques. Les disques durs peuvent échouer pour diverses raisons, telles que des collisions de tête de lecture ou des ruptures de bande.

Analyse des fichiers de registre

Les dommages physiques entraînent toujours une perte de données, et dans certains cas, les structures logiques du système de fichiers sont également brisées. Récupération de données à partir de disques durs physiquement endommagés : la plupart des dommages physiques ne peuvent pas être réparés par les utilisateurs finaux. Les virus, la mise en forme, la mauvaise partition, la mauvaise duplication, l'opération incorrecte, la suppression du réseau et les pannes de courant pendant la procédure sont toutes des causes logicielles possibles. Les erreurs de manipulation, les erreurs de lecture, l'impossibilité de trouver ou d'ouvrir le fichier, les rapports de partition absente, non formatée, la perte de mot de passe et les caractères problématiques sont les symptômes les plus courants. Les disques durs actuels des ordinateurs stockent une variété de données, comprenant les applications du système d'exploitation et les données utilisateur enregistrées dans des fichiers. Les disques contiennent également les informations de métadonnées du système d'exploitation, y compris les répertoires, les caractéristiques de fichier et les tables d'allocation, ainsi qu'une sauvegarde pour la mémoire virtuelle. Les façons les plus courantes de nuire aux disques durs sont les suivantes :

- Endommager physiquement le disque, le rendant inutilisable.
- Démagnétiser le disque pour rendre aléatoires les domaines magnétiques, ce qui laissera très probablement le disque inopérant.
- Effacer les données sur l'appareil afin qu'elles ne puissent pas être récupérées.
- Selon Anthony Verducci, il existe trois façons de supprimer des fichiers :
- La méthode de suppression des fichiers individuels (les fichiers individuels sont supprimés, mais le logiciel reste intact).
- L'approche de l'effacement complet du disque (le disque entier est effacé de façon permanente mais reste utilisable).
- La technique de l'outil de puissance (les données ont disparu, le disque dur est inutilisable).

Chaque périphérique de stockage électronique (espace utilisé) contient des fichiers et de l'espace libre. Chaque fois que l'ordinateur est utilisé, les informations des fichiers dans l'espace utilisé peuvent être modifiées, et les données précédemment supprimées dans l'espace libre peuvent être écrasées. Les personnes ayant des compétences de bas niveau suppriment des documents à l'aide d'instructions de suppression ou d'effacement. Les criminels experts, en revanche, suivent la destruction en écrasant les données afin qu'elles ne puissent pas être récupérées. Ils utilisent une méthode consistant à remplir chaque bloc accessible avec des octets ASCII NUL pour écraser un disque dur.

conclusion

Dans ce chapitre, nous avons abordé d'importants concepts techniques concernant les ordinateurs qui doivent être bien compris par tout enquêteur en forensic numérique. Nous avons décrit comment les ordinateurs stockent et représentent les données de manière numérique, le concept de la structure de fichiers du système d'exploitation et ses types, ainsi que les algorithmes de hachage et comment nous pouvons les utiliser pour vérifier l'authenticité de toute donnée numérique. Dans le prochain chapitre, nous discuterons de la mise en place d'un laboratoire d'investigation en forensic numérique professionnel, des outils, logiciels et matériels nécessaires au minimum requis.

PARTIE 2

ACQUISITION DE PREUVES NUMÉRIQUES

Dans ce module, vous allez :

- Nous commençons par discuter des différents formats de fichiers que les images forensiques utilisent pour stocker des données. Les images forensiques peuvent être dans différents formats de fichiers, certains sont open source et d'autres sont propriétaires de l'entreprise qui a développé le logiciel forensique utilisé pour créer l'image. Ceux répertoriés ci-dessous sont les plus couramment utilisés dans le domaine

60 heures

ACQUISITION DE PREUVES NUMÉRIQUES

Ce que vous allez apprendre dans ce chapitre :

- Nous commençons par discuter des différents formats de fichiers que les images forensiques utilisent pour stocker des données. Les images forensiques peuvent être dans différents formats de fichiers, certains sont open source et d'autres sont propriétaires de l'entreprise qui a développé le logiciel forensique utilisé pour créer l'image. Ceux répertoriés ci-dessous sont les plus couramment utilisés dans le domaine

Introduction

Le travail principal d'un enquêteur en forensic informatique consiste à collecter et analyser des images provenant d'ordinateurs. En résumé, une image forensique est une capture statique de tout ou partie des données stockées sur la mémoire secondaire d'un ordinateur (par exemple, un disque dur ou un SSD), sur un périphérique de stockage externe (par exemple, une clé USB, un disque dur externe ou une bande magnétique) ou sur la RAM (lors de l'acquisition en direct de systèmes en cours d'exécution). Cette image peut être considérée comme un conteneur de données, permettant de stocker des fichiers individuels ou l'ensemble des fichiers de disque/vivre en mémoire dans un seul fichier image. Les preuves numériques doivent être récupérées et analysées afin d'identifier des indications d'incidents de sécurité, de fraudes et d'autres pratiques illégales ciblant les systèmes d'information qui seront contenues dans une image forensique. N'oubliez pas que les images forensiques peuvent être utilisées en justice, les outils et techniques utilisés pour les acquérir et les analyser doivent donc être légaux.

Les formats RAW

Le format Raw est le format de fichier le plus couramment utilisé ; c'est une copie bit à bit des données brutes du disque et peut être utilisé pour imager l'ensemble du disque ou une seule partition. La capacité à ignorer les erreurs de lecture mineures du disque source et sa rapidité sont deux des principaux avantages du format de fichier Raw. Bien que le format Raw ne puisse pas stocker de métadonnées, certaines applications le font dans un fichier séparé (par exemple, la valeur de hachage du fichier image, le numéro de série du disque, etc.). Le format Raw est le format de fichier par défaut pour la sortie générée par la célèbre commande Linux/UNIX dd, et il est pris en charge par la plupart des logiciels de forensic informatique. 001, dd, dmg, raw et img ne sont que quelques exemples de la structure de nommage (extensions) pour le format Raw. Le principal inconvénient du format Raw est qu'il nécessite la même quantité d'espace de stockage que le disque source car les données en format Raw ne peuvent pas être compressées, ce qui peut poser un problème lors de l'achat de grands disques durs.

Le format de forensic informatique avancé (Advanced Forensic Format – AFF)

Le format de forensic informatique avancé (AFF) est un format de fichier extensible open-source pour les images de forensic informatique qui peut être intégré librement dans d'autres programmes open-source et propriétaires. Les algorithmes de compression Zlib et LZMA sont tous deux pris en charge par AFF. Vous pouvez également diviser le fichier image de forensic en plusieurs fichiers une fois qu'il a été créé. AFF (à partir de AFF V2.0) prend en charge le chiffrement de l'image de disque, vous permettant de protéger par mot de passe votre image acquise. AFF permet de stocker une large gamme d'informations de métadonnées dans le fichier image lui-même, réduisant ainsi la quantité de travail et permettant à un seul fichier de contenir toutes les informations relatives à l'image de forensic acquise (par exemple, un fichier de métadonnées peut contenir la chaîne de preuve ou le journal d'audit). AFF4 est la version la plus récente, et AFF3 et AFFLIBv3 ne sont plus pris en charge et ne devraient pas être utilisés dans de nouveaux projets. Sleuthkit, Autopsy, OSFMount, X-mount, FTK Imager et FTK sont tous des logiciels de forensic informatique qui fonctionnent avec les versions plus récentes de AFF. Pour les fichiers image segmentés, AFF utilise l'extension .afd, tandis que les métadonnées AFF sont enregistrées sous forme de fichier .afm.

EnCase : Transferts d'expert témoin

Il s'agit d'un format de fichier propriétaire développé par Guidance Software (maintenant OpenText) pour leur produit populaire "EnCase Forensic", largement utilisé par les forces de l'ordre dans le cadre d'enquêtes criminelles dans le monde entier. Ce format de fichier peut être utilisé pour stocker diverses preuves numériques ; il est compressible et consultable, et l'image qu'il produit peut être divisée en plusieurs fichiers. Les métadonnées peuvent être associées au même fichier image ; cependant, comparé au format de fichier AFF, la quantité et le type de métadonnées sont limités.

EnCase divise l'image résultante en morceaux de 640 Mo lors de la capture de disques durs. Les extensions de fichier changeront en fonction du numéro de morceau en raison de cette division des données d'image forensique (par exemple, l'extension du premier morceau est ".e01", l'extension du deuxième morceau est ".e02", et ainsi de suite).

D’autre formats des fichiers

D'autres formats de fichiers d'image forensique sont des formats propriétaires utilisés par certaines suites de forensique informatique et sont moins couramment utilisés (tels que Safeback de NTI, ILook Imager et ProDiscover).

Validation des fichiers d'image forensique

La validation garantit que les fichiers d'image forensique acquis sont identiques à la source à 100 % et n'ont pas été altérés au cours du processus d'acquisition. Dans l'industrie de la forensique informatique, le hachage est la norme acceptée pour valider les images forensiques acquises. La valeur de hachage du fichier d'image résultant est considérée comme une empreinte électronique. La plupart des logiciels de forensique informatique génèrent une valeur de hachage des données capturées lorsqu'ils ont terminé, mais vous pouvez calculer la valeur de hachage de n'importe quelle donnée à l'aide d'outils tiers ou de l'utilitaire standard, qui est disponible dans les versions modernes de Windows via PowerShell.

Acquisition de la mémoire vive en direct

L'acquisition en direct est devenue un élément essentiel de tout type d'enquête numérique, bien qu'elle n'ait reçu que peu d'attention jusqu'à récemment. De nombreux types d'artefacts numériques, par exemple, n'existent que dans la RAM, sans qu'aucune trace de leur existence ne soit écrite sur le disque dur. Lorsqu'un appareil est éteint ou redémarré, les données qu'il contient sont considérées comme volatiles. Veuillez noter que ces informations seront écrasées lors de l'utilisation d'un ordinateur (par exemple, lors de la fermeture d'une application spécifique sur un PC, l'espace de données réservé disparaîtra de la RAM, permettant à d'autres applications d'utiliser son espace pour fonctionner) et seront complètement perdues lors de l'arrêt du système. Des outils logiciels spécialisés (et, dans certains cas, matériels) sont nécessaires pour capturer une mémoire vive en direct. Étant donné que la RAM ne stocke pas les données de la même manière que les disques durs, l'analyse du contenu d'une image forensique de données volatiles nécessite également un logiciel spécialisé.

En raison de ces deux facteurs, la capture et l'analyse de la mémoire volatile sont plus difficiles que l'acquisition traditionnelle des disques durs. Par exemple, les dispositifs de mise en réseau tels que les routeurs et les commutateurs peuvent stocker des données volatiles dans leurs journaux. Le dumping est le processus d'extraction de données de la mémoire volatile, et la méthode pour le faire varie en fonction du système d'exploitation. Seuls les ordinateurs exécutant le système d'exploitation Windows sont discutés dans ce cours.

Les informations qui peuvent être trouvées dans la RAM comprennent les éléments suivants :

- Clés de chiffrement
- Processus en cours d'exécution
- Commandes de console qui ont été exécutées
- Éléments dans le presse-papiers
- Données provenant d'un réseau
- Contenus de fichiers image et texte
- Fichiers supprimés
- Journaux de navigation sur le web
- Clés du registre qui sont ouvertes et actives
- Mots de passe pour les comptes Web (par exemple, e-mail, médias sociaux et stockage en nuage)
- Messagerie instantanée
- Informations d'exploit
- Rootkits et malwares Trojan
- Preuves d'activité qui ne sont généralement pas enregistrées sur le disque dur local

La mémoire virtuelle (SWAP)

Le fichier **Pagefile.sys** (également appelé mémoire virtuelle) est un fichier Windows qui compense la capacité limitée de la RAM. Son emplacement par défaut est C:>**pagefile.sys**. Le fichier de pagination de mémoire virtuelle initiale dans Windows est normalement défini sur la quantité de RAM installée, mais un utilisateur ou un administrateur système peut généralement en modifier la taille. Lorsque la RAM de votre machine commence à se remplir, cette fonctionnalité permet à Windows d'utiliser l'espace du disque dur comme mémoire. Pour libérer de l'espace pour plus de données, des parties des fichiers de la RAM sont déplacées dans la mémoire virtuelle. Le système d'exploitation ne peut plus traiter directement les fichiers qui ont été envoyés à la mémoire virtuelle. Par conséquent, il devra envoyer plus de fichiers à la mémoire virtuelle pour libérer de l'espace afin de récupérer les fichiers qu'il souhaite traiter à partir de la mémoire virtuelle et les remettre dans la RAM. L'utilisateur n'est pas conscient de ce processus, appelé échange ou pagination. L'acquisition de la mémoire virtuelle est une partie critique du processus de la criminalistique numérique, car elle peut contenir des informations précieuses telles que les mots de passe utilisateur, les clés de chiffrement, l'activité du navigateur Web et d'autres artefacts importants transférés depuis la RAM. La mémoire virtuelle peut être acquise par certains outils de capture de la RAM en plus de la RAM elle-même, par exemple, FTK Imager.

Difficultés liées à l'acquisition de la RAM en Forensic

Les examinateurs en Forensic rencontrent souvent des difficultés lors de l'acquisition de la mémoire vive. Voici quelques points à prendre en compte lors d'une acquisition en direct.

Windows verrouillé : il est préférable de procéder à un arrêt forcé si l'on tombe sur un ordinateur en cours d'exécution mais verrouillé par un écran de connexion. Cependant, certains experts soutiennent que l'utilisation de certains outils/techniques permet d'éviter de perdre le contenu de la RAM et de contourner la page de connexion de Windows sans avoir à redémarrer. Pour accéder à la mémoire vive et aux disques chiffrés sans mot de passe, utilisez les accessoires matériels CaptureGUARD et Phantom Probe (www.windowsscope.com). Pour se connecter au système, utilisez une attaque d'accès direct à la mémoire (DMA) pour extraire le mot de passe de la RAM.

Difficultés liées à l'acquisition de la RAM en Forensic

Il convient de garder à l'esprit que l'utilisation de telles techniques laisse des traces dans la RAM et peut ne pas réussir dans certains cas. Il est donc important de réaliser une évaluation des risques pour déterminer si l'acquisition en direct de la mémoire vive est utile et, en cas de doute, de consulter un expert en la matière.

Le DMA est une méthode informatique qui permet à certains composants matériels d'interagir directement avec la mémoire physique (RAM) de l'ordinateur et de transférer des données vers et depuis celle-ci sans passer d'abord par le CPU de l'ordinateur. Cette méthode est utilisée pour réduire le temps de traitement et augmenter le débit de l'ordinateur en transférant les données directement de la RAM au CPU sans avoir à les traiter d'abord. Les experts en Forensic peuvent utiliser cette technique pour accéder aux données sensibles sur une machine cible, en contournant toutes les mécanismes de sécurité du système d'exploitation ainsi que tout écran de verrouillage ou logiciel antivirus.

Imaginez la situation suivante ➔ un examinateur en informatique légale connecte son appareil (une station de travail d'investigation mobile) à l'ordinateur suspect et utilise un logiciel de craquage spécial pour rechercher dans la RAM de l'ordinateur suspect des artefacts intéressants tels que des clés cryptographiques, des mots de passe ou des fichiers déchiffrés. L'ordinateur suspect doit avoir des ports compatibles DMA pour que cette méthode fonctionne. FireWire, Thunderbolt, PCMCIA, PCI, PCI-X et PCI Express sont tous des exemples de ces types de ports. La fonctionnalité DMA n'est pas disponible sur les ports USB.

Les privilèges administratives

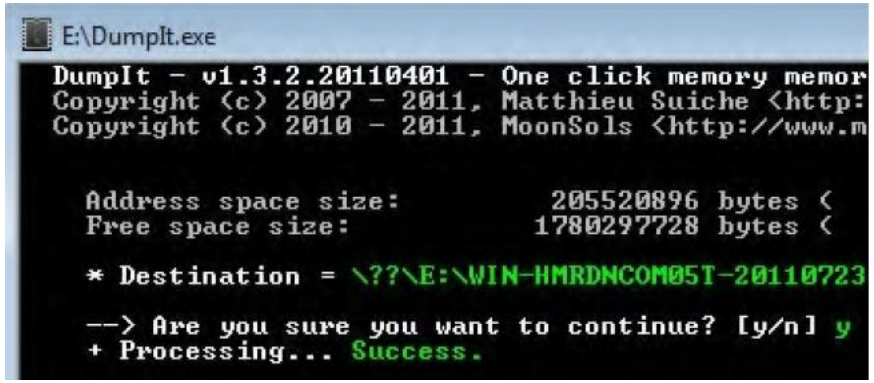
Pour fonctionner, la majorité des outils logiciels de capture de RAM nécessitent des privilèges administratifs. Si vous vous retrouvez devant un ordinateur en cours d'exécution avec des autorisations d'utilisateur limitées (par exemple, un compte utilisateur), vous pouvez acquérir la RAM avec un outil d'acquisition matérielle (qui nécessite l'installation d'un petit pilote sur la machine cible) ou une attaque DMA. Sur la machine suspecte, l'outil de capture qui a été utilisé pour obtenir la RAM laissera des traces. Certaines données peuvent être écrasées lors de l'acquisition de la mémoire en direct, malgré les affirmations des fournisseurs de logiciels d'investigation informatique selon lesquelles leurs outils laissent une empreinte minimale sur le système acquis. Pour fonctionner, les outils d'acquisition matérielle nécessiteront également l'installation d'un petit pilote sur la machine cible. Afin d'éviter que vos preuves ne soient inadmissibles devant un tribunal, ces modifications doivent être bien documentées dans le rapport final de l'enquête. Toute machine Windows soumise à une acquisition en direct sera généralement modifiée de la manière suivante : Modifications du registre Entrées dans la mémoire (écrasement des données en RAM) Il est possible d'écrire une petite quantité de données sur un disque dur Les tribunaux sont généralement indulgents en ce qui concerne les petites empreintes laissées par les outils de capture de RAM ; cependant, assurez-vous de documenter chaque interaction avec l'ordinateur suspect lors de la capture de la RAM dans votre rapport final, et utilisez des outils légalement acceptables pour le faire.

La création de copies de RAM peut être effectuée à l'aide de divers outils d'imagerie, tels que DumpIt, un petit outil portable permettant d'acquérir la RAM sur les ordinateurs Windows (32 ou 64 bits) de la manière suivante :

- Pour accéder à la section de téléchargement, rendez-vous sur le lien **https://my.comae.io/login** et inscrivez-vous pour obtenir un compte gratuit.
- Placez l'outil sur une clé USB (si vous prévoyez de l'exécuter à partir de celle-ci) ; veillez à ce que cette clé USB soit suffisamment grande pour contenir la RAM de l'ordinateur cible, car elle contiendra le fichier que vous allez créer. Par exemple, si vous souhaitez enregistrer une RAM de 8 Go, votre clé USB devrait avoir une capacité de 9 Go d'espace libre.
- Pour utiliser DumpIt, double-cliquez dessus et saisissez "y" pour confirmer que vous souhaitez copier la RAM de l'ordinateur cible sous Windows (figure dans le next slide). Le fichier RAM capturé sera stocké au même emplacement que DumpIt.
- Il est important de noter que l'image capturée est plus grande que la taille de la RAM (dans ce cas, nous capturons un PC avec 8 Go de RAM ; la taille de l'image est d'environ 8,269 Go).

Les privilèges administratives

Après avoir terminé l'acquisition, DumpIt crée deux fichiers : un fichier DMP contenant l'image de la RAM et un fichier JSON contenant des informations techniques importantes sur la machine capturée, telles que les informations sur la machine, le type d'architecture, le nom de la machine, la mémoire physique, le nom d'utilisateur, la version du système d'exploitation et les informations sur le service.



RAM with the DumpIt tool

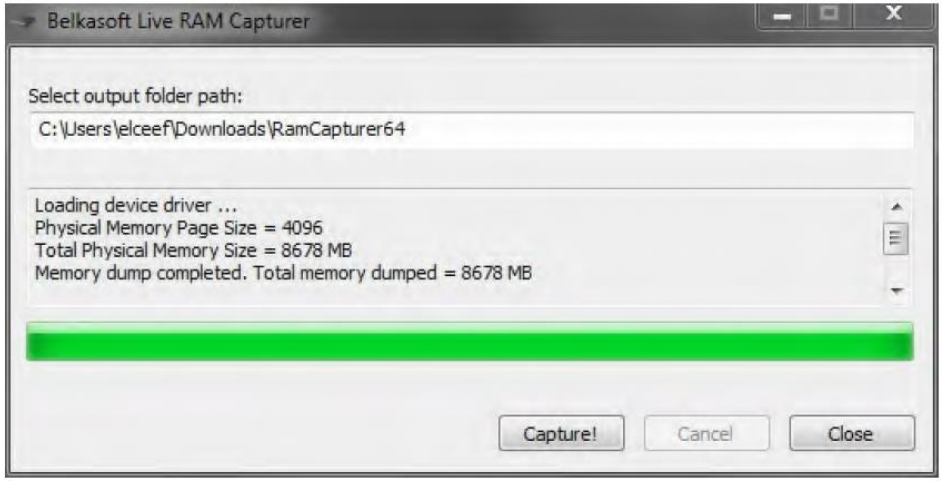
PARTIE 2

Capturateur de RAM en direct

Après avoir terminé l'acquisition, DumpIt crée deux fichiers : un fichier DMP contenant l'image de la RAM et un fichier JSON contenant des informations techniques importantes sur la machine capturée, telles que les informations sur la machine, le type d'architecture, le nom de la machine, la mémoire physique, le nom d'utilisateur, la version du système d'exploitation et les informations sur le service.

Belkasoft est le deuxième outil que nous utiliserons pour capturer la RAM. Il s'agit d'un petit outil gratuit qui s'exécute à partir d'une clé USB et peut capturer l'intégralité du contenu de la RAM, même si le système est protégé par un système anti-débogage ou anti-dumping actif. Afin de réduire au maximum l'empreinte de l'outil, des versions distinctes en 32 bits et 64 bits sont disponibles. Toutes les versions et éditions de Windows, y compris XP, Vista, Windows 7, 8, 10, 2003 et Server 2008, sont prises en charge par Belkasoft Live RAM Capturer. Suivez ces étapes pour utiliser cet outil :

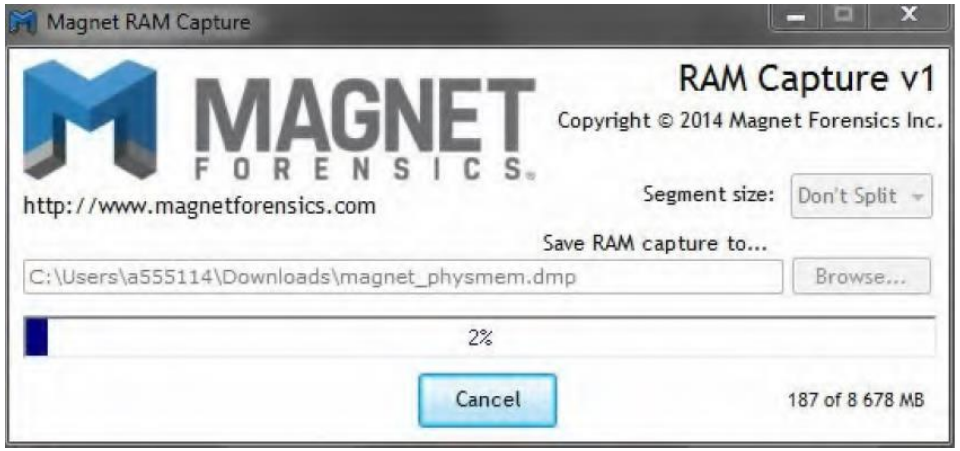
- Rendez-vous sur **https://belkasoft.com/ram-capturer** pour obtenir l'outil (vous devrez d'abord remplir un formulaire d'inscription simple pour accéder à la section de téléchargement).
- Placez l'outil sur une clé USB ayant une capacité de stockage supérieure à celle de la RAM de l'ordinateur cible.
- Sur l'ordinateur où vous souhaitez capturer la RAM, exécutez le programme et cliquez sur le bouton "Capture" (figure 5.2).



Belkasoft to capture RAM

La capture de RAM Magnet

Magnet est un outil de capture de RAM portable qui prétend avoir une empreinte minimale sur la machine cible et prend en charge presque toutes les versions du système d'exploitation Windows, y compris Windows XP, Vista, 7, 8, 10, 2003, 2008 et 2012 (32 et 64 bits). Il est facile d'utiliser cet outil ; rendez-vous sur **www.magnetforensics.com/free-toolmagnet-ram-capture/** et remplissez un court formulaire pour obtenir le lien de téléchargement. Placez l'outil sur votre clé USB et connectez-la à la machine cible ; ensuite, exécutez l'outil et choisissez où vous souhaitez enregistrer l'image de la RAM résultante. Enfin, appuyez sur le bouton Démarrer pour commencer l'enregistrement.



Magnet RAM capture

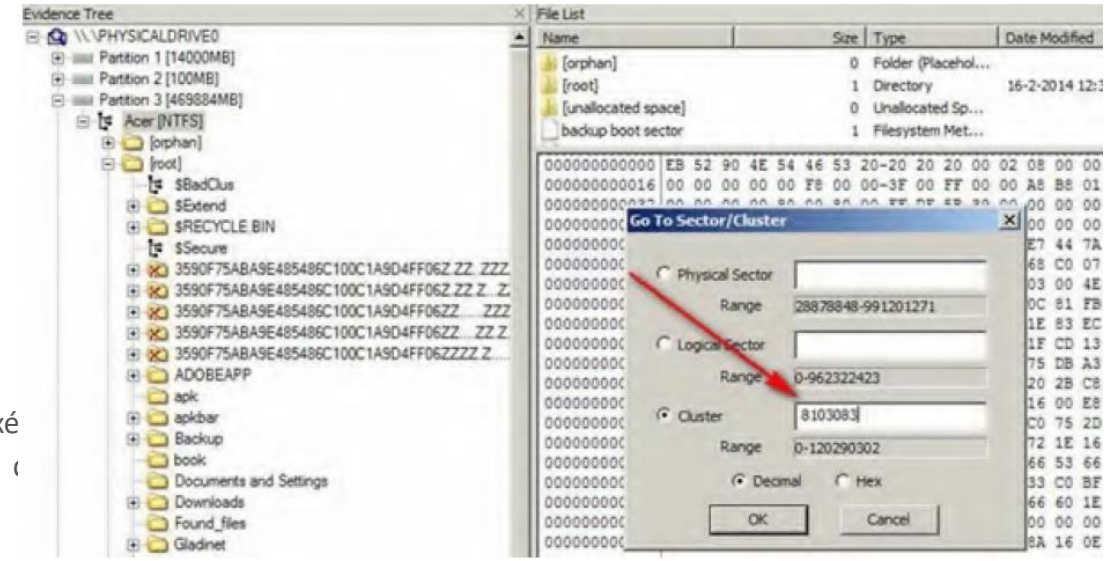
FTK imager

FTK Imager est un outil de prévisualisation et d'imagerie de données permettant de créer des images forensiques des données d'un ordinateur cible sans altérer les preuves originales. Vous pouvez créer des images forensiques de disques durs locaux, de disquettes, de disques Zip, de CD, de DVD, de dossiers entiers ou de fichiers individuels à partir de différents emplacements dans les supports avec cet outil, comme présenté dans la figure suivante.

FTK Imager peut également être utilisé pour d'autres tâches que l'acquisition d'images, notamment les suivantes :

- Installation d'une image en lecture seule.
- Examen du contenu des images forensiques.
- Exportation de fichiers et de dossiers à partir des images forensiques.
- Obtention du registre Windows.
- Récupération de fichiers supprimés.

Cet outil peut être installé localement sur la machine où il sera utilisé, ou il peut être exé option est préférée lors de l'analyse forensique en direct sur des systèmes en cours portable (comme une clé USB) avant de commencer à l'utiliser :



FTK Imager for RAM capturing

PARTIE 2

L'acquisition de mémoire non volatile

La mémoire non volatile désigne tout support de stockage capable de conserver des données même après une coupure de courant prolongée. Les disques durs et les mémoires flash sont deux des types les plus courants (lecteurs flash). Les images des disques durs constituent l'élément le plus important de toute enquête judiciaire informatique, car elles contiennent la majorité des données susceptibles de contenir des éléments de preuve à charge ou à décharge. FTK Imager, Pro Discover, EnCase et X-WaysForensics ne sont que quelques-uns des outils qui peuvent être utilisés pour acquérir des images de disques durs dans le système d'exploitation Windows. Avant de connecter le disque dur suspect à votre station de travail, assurez-vous qu'il est protégé en écriture. De nombreux enquêteurs préfèrent démarrer à partir d'un CD/DVD en utilisant une distribution forensique Linux comme CAINE **(www.caine-live.net)** ou DEFT **(www.deftlinux.net),** qui est préconfigurée pour bloquer le démontage automatique, et attacher ensuite un disque suspect sans risque de manipulation de données provenant de sources externes.

Acquisition d'un disque dur

Au cours d'une enquête, vous pouvez utiliser diverses méthodes d'acquisition statique. Vous devez prendre en compte les critères suivants avant de déterminer laquelle utiliser :

- La taille du disque source (suspect). (L'obtention de disques durs de grande capacité nécessite d'énormes unités de stockage pour contenir l'image forensique créée, ce qui peut prendre plus de temps lors du traitement.)
- Le délai dans lequel l'acquisition sera effectuée (si le temps est limité, vous ne pouvez pas passer des heures à acquérir l'intégralité des disques durs de l'ordinateur ou des ordinateurs suspects).
- Est-il possible d'apporter le support numérique douteux (par exemple, un disque dur) au laboratoire avec vous, ou l'acquisition doit-elle être effectuée sur place ?
- Est-il possible d'arrêter la machine cible pour obtenir les données de son disque dur, ou est-ce impossible en raison de divers facteurs (par exemple, l'arrêt d'un serveur de messagerie électronique pourrait entraîner une perte d'exploitation importante) ?

Vous pouvez choisir la stratégie d'acquisition qui convient le mieux au scénario en tenant compte de ces variables et d'autres. Les trois méthodes les plus courantes pour obtenir des photographies judiciaires sont les suivantes.

Acquisition de ressources physiques

Cette méthode permet de créer un clone bit par bit/secteur par secteur d'un disque dur, également connu sous le nom d'image de flux binaire. Cette approche permet également de capturer les métadonnées du système de fichiers, les fichiers supprimés, les fragments de fichiers supprimés et l'espace non alloué. À moins que la compression ne soit utilisée pendant le processus d'acquisition, l'image résultante sera une reproduction complète de la source (une copie exacte). Par exemple, si nous réalisons une image judiciaire d'un disque dur de 500 Go, l'image résultante sera exactement de 500 Go. Tout programme d'expertise informatique peut lire des images de flux binaire et, comme nous l'avons indiqué précédemment, vous devez connecter le disque dur du suspect à un bloqueur d'écriture matériel afin que le poste d'expertise utilisé pour acquérir l'image n'écrive pas de données sur le disque dur du suspect au cours du processus d'acquisition.

En fonction de l'endroit où les données acquises sont stockées, on peut distinguer deux types d'acquisition physique :

- **Conversion d'un disque à flux binaire en fichier image** : Les données capturées sont sauvegardées sous forme de fichier image. C'est l'approche d'investigation la plus fréquemment utilisée. Elle permet de faire une copie identique, bit pour bit, du disque source et de l'enregistrer sous forme de fichier image. Le principal avantage de cette procédure est qu'elle permet de faire de nombreuses copies d'un disque douteux tout en conservant le support original intact.
- **Flux de bits de disque à disque** : Dans cette méthode, les données sont copiées (bit par bit) du disque source vers un disque plus récent ayant une capacité de stockage identique ou légèrement supérieure. Bien que cette méthode ne soit généralement pas utilisée, elle est néanmoins nécessaire dans certaines situations, par exemple lors de l'achat d'un ancien disque dur. Certains logiciels de criminalistique informatique (par exemple, EnCase et X-Ways forensics) peuvent modifier la forme du nouveau disque dur (de destination) de manière à ce que les données collectées se trouvent au même endroit que le disque source (suspect).

Acquisition logique

Cette approche ne fait que capturer un sous-ensemble de données actives. Lorsque nous parlons de "données actives", nous parlons des informations qui se trouvent devant nous lorsque nous utilisons un ordinateur. Cette méthode ne permet pas de capturer l'espace non alloué, les données du système de fichiers, les fichiers supprimés ou partiellement effacés, les données cachées ou tout l'espace inutilisé. Si vous capturez logiquement un disque de 500 Go avec seulement 100 Go de données actives, vous n'obtiendrez qu'une image de 100 Go. Lorsque le disque cible (suspect) est trop volumineux (par exemple, stockage RAID) et que le secouriste n'a pas le temps d'effectuer une acquisition (physique) d'un volume complet sur place, l'acquisition logique est une option viable. Elle est également possible si l'on souhaite obtenir un ou plusieurs fichiers spécifiques de manière ciblée (par exemple, acquérir des fichiers de courrier électronique uniquement à partir de la machine cible ou capturer tous les fichiers photo présents sur un disque suspect). Dans le cadre de certains types d'actions civiles, une acquisition logique peut être la seule option possible (e-discovery). Il est également possible d'utiliser des termes de recherche pour trouver un mot-clé spécifique ou une combinaison de mots-clés parmi de vastes ensembles de données et de n'obtenir ensuite que les résultats.

Acquisition de données éparses

Cette méthode est similaire à l'acquisition logique en ce sens qu'elle ne capture que des fichiers spécifiques liés à l'enquête ; toutefois, les données supprimées et leurs fragments sont également capturés au cours du processus de capture dans le cadre de l'acquisition éparse. Cette méthode est fréquemment utilisée lors de l'exécution d'une acquisition statique sur des systèmes RAID ou lorsque le suspect n'est pas suffisamment expérimenté pour déployer des mesures anti-forensiques avancées. Maintenant que nous connaissons les différentes méthodes d'acquisition de disques durs, il est temps de commencer à rassembler des images de disques durs. De nombreux types de logiciels permettent de réaliser l'acquisition de disques durs ; cependant, nous ne pourrons pas tous les couvrir dans ce livre, c'est pourquoi nous utiliserons FTK Imager, qui est un programme gratuit et fiable.

Acquisition de réseaux

La criminalité électronique, qui implique l'utilisation d'ordinateurs en réseau, est en augmentation. En travaillant sur des affaires criminelles impliquant l'utilisation de réseaux informatiques en tant qu'expert en criminalistique, vous pouvez vous attendre à être confronté aux défis suivants.

- Dans la plupart des cas, vous devrez collecter et analyser une grande quantité de données (par exemple, les acquisitions de réseaux redondants de disques indépendants [RAID], qui impliquent deux disques durs ou plus).
- Étant donné que les preuves peuvent être dispersées sur plusieurs types de dispositifs dans le réseau cible, une expertise technologique sera nécessaire.
- Les entreprises imposeront des défis organisationnels qui nécessiteront une enquête ; par exemple, vous ne pouvez pas mettre fin à un service spécifique parce qu'il est essentiel au succès de l'entreprise.
- La multiplicité des juridictions peut créer des difficultés ; par exemple, il est arrivé qu'un serveur de stockage soit situé en Europe, mais que l'enquête - ou la violation - soit menée à New York. Quelles mesures juridiques allez-vous prendre ? D'autres problèmes juridiques se posent lorsque plusieurs juridictions imposent des normes différentes en matière de protection de la vie privée ; par exemple, des informations privées (concernant des clients, des partenaires ou des travailleurs) peuvent être exposées à l'examinateur lors d'une violation de réseau, et ces données peuvent être protégées par des réglementations différentes en matière de protection de la vie privée.

Les limites des outils de forensics

Certains logiciels de collecte de données criminalistiques ne sont pas en mesure de copier ou d'accéder aux données dans HPA et DCO, alors que ces deux emplacements peuvent contenir des informations accablantes qui doivent être obtenues pour être examinées. Vérifiez toujours la documentation de l'outil d'acquisition pour voir s'il possède cette fonction ; si ce n'est pas le cas, il est préférable d'utiliser un outil d'acquisition matériel.

Conclusion

La capture d'une image de la mémoire d'un ordinateur est l'objectif principal de toute enquête de police scientifique numérique. L'approche la plus répandue pour obtenir des images numériques est l'image en flux continu, qui consiste à copier toutes les données du disque suspect, y compris les fichiers supprimés, les fragments de fichiers supprimés et l'espace non alloué, dans un fichier d'image judiciaire qui peut être évalué ultérieurement à la recherche de preuves numériques. On peut distinguer deux types d'acquisitions d'images ou d'expertises :

- Capture de la mémoire vive et d'autres données volatiles, telles que les informations réseau de l'acquisition en direct.
- Acquisition statique de la mémoire non volatile (HDD, SSD et supports de stockage numériques).

Pour préserver l'intégrité des images forensiques collectées, une valeur de hachage est utilisée pour s'assurer qu'elles sont 100% similaires à la source et qu'elles n'ont pas été modifiées au cours du processus de collecte. C'est toujours une bonne pratique que de créer plusieurs copies du fichier image ; de cette façon, vous garderez le support original intact tout en ayant plusieurs images avec lesquelles travailler en cas de problème (par exemple, l'image est modifiée par erreur) au cours du processus d'analyse. Dans ce chapitre, nous avons abordé l'utilisation de différents outils pour capturer la mémoire vive et les diverses considérations et difficultés qui en découlent. Nous avons également passé en revue diverses méthodes d'acquisition de disques durs et l'utilisation deFTK Imager pour capturer un disque dur. Dans le chapitre suivant, nous analyserons le processus après avoir obtenu un disque dur et une image de RAM douteux.

PARTIE 3

Investigation du système Windows

Dans ce module, vous allez :

Investigation du système Windows

Ce que vous allez apprendre dans ce chapitre :

Une analyse en détail les éléments suivants :

- Outils d'analyse de la chronologie
- Gravure de données
- Analyse du registre Windows
- Analyse légale des périphériques USB
- Informations sur le registre de l'imprimante
- Identification du format de fichier
- Analyse des vignettes Windows
- Criminalistique de Windows 10
- Base de données de la zone de notification
- Criminalistique de Cortana

OFPPT
La Voie de l'Avenir

WEBFORCE
BE THE CHANGE

Introduction

Le processus de conduite ou d'exécution d'enquêtes judiciaires sur les ordinateurs fonctionnant sous les systèmes d'exploitation Windows est connu sous le nom de criminalistique Windows. Ce chapitre traite de la réponse aux incidents, de la récupération et de l'audit des technologies Windows utilisées pour mener des activités criminelles. Les enquêteurs doivent comprendre parfaitement les systèmes d'exploitation Microsoft Windows pour mener à bien des enquêtes criminalistiques aussi complexes. La plupart des systèmes stockent temporairement des données sur la session en cours dans le registre, la mémoire cache et la mémoire vive. Lorsque l'utilisateur éteint l'ordinateur, ces données sont facilement perdues, tout comme les informations relatives à la session, et les enquêteurs doivent donc les récupérer dès que possible. Ce chapitre explique ce que sont les données volatiles, pourquoi elles sont importantes et comment les extraire.

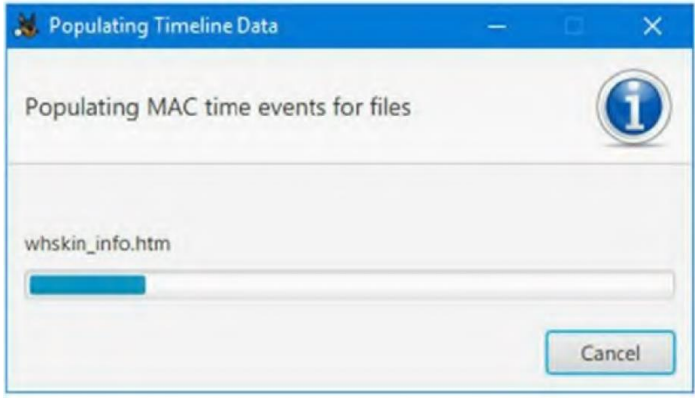
Outils d'analyse chronologique

La plupart des enquêtes de criminalistique numérique comprennent une analyse de la chronologie, car elle fournit une perspective complète de la séquence des événements qui se sont produits sur le système dans l'ordre et permet de répondre à une question clé dans toute enquête : quand une action donnée s'est-elle produite ? Les enquêteurs peuvent gagner du temps en limitant la quantité de données à étudier dans un laps de temps donné, par exemple à la suite d'un incident, grâce à l'analyse chronologique. Lors de l'analyse des occurrences de logiciels malveillants, l'analyse de la chronologie est essentielle pour déterminer quand l'état d'un système a changé à la suite d'une attaque de logiciels malveillants. L'interface de chronologie d'Autopsie regroupe les anomalies distinctes découvertes dans les images forensiques données en fonction de leurs horodatages.

Chaque fichier de l'image forensique est associé à un horodatage. Les propriétés temporelles d'un fichier comprennent la date de sa création, de sa modification et de son accès. N'oubliez pas que les propriétés temporelles "Modifié" et "Créé" des fichiers sont traitées différemment par chaque système d'exploitation. Par exemple, les heures de création et de modification des fichiers sous Windows indiquent les changements de contenu, alors que sous UNIX, les attributs de l'heure de création ne sont pas stockés, et un fichier est considéré comme modifié lorsque ses métadonnées sont modifiées, que le contenu du fichier ait changé ou non.

L'analyse de la chronologie est utile pour divers types d'enquêtes, pour générer une chronologie des événements, et est souvent utilisée pour fournir des réponses sur l'utilisation de l'ordinateur et les événements qui se sont produits avant ou après un événement donné. Autopsie contient une interface de chronologie avancée, comme l'illustre la figure suivant.

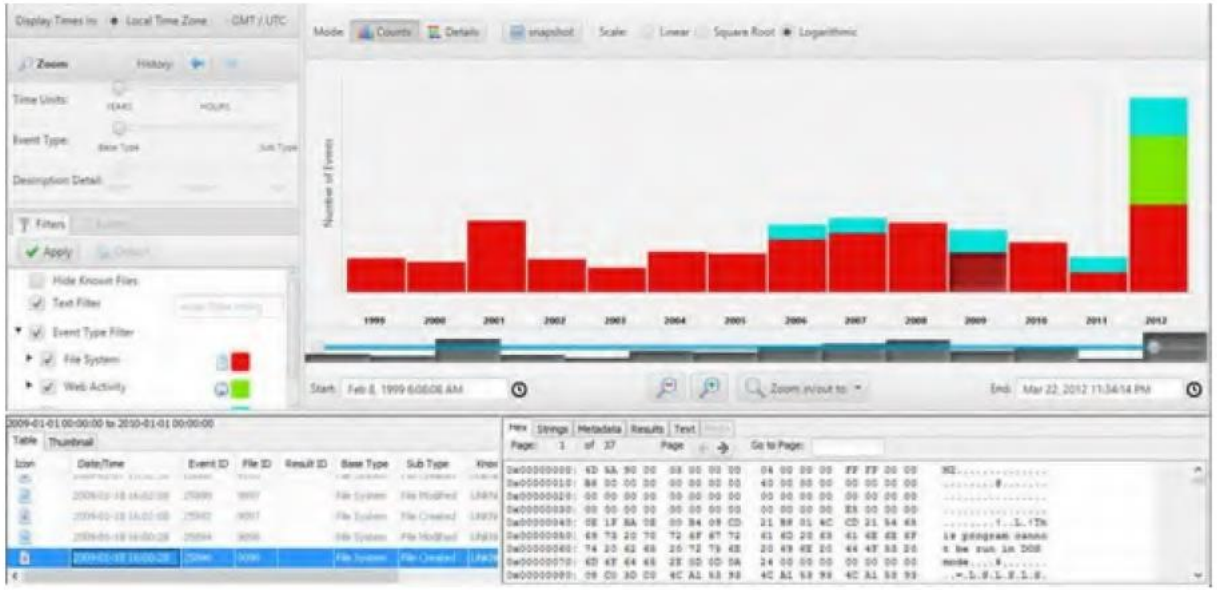
1. Lancez Autopsy pour générer et construire un nouveau cas ou lancez un cas existant.
2. Cliquez sur le menu Outils | Ligne de temps.
3. En fonction de la taille de l'image médico-légale, Autopsy peut prendre un certain temps pour remplir les données de la ligne de temps.



Outils d'analyse chronologique

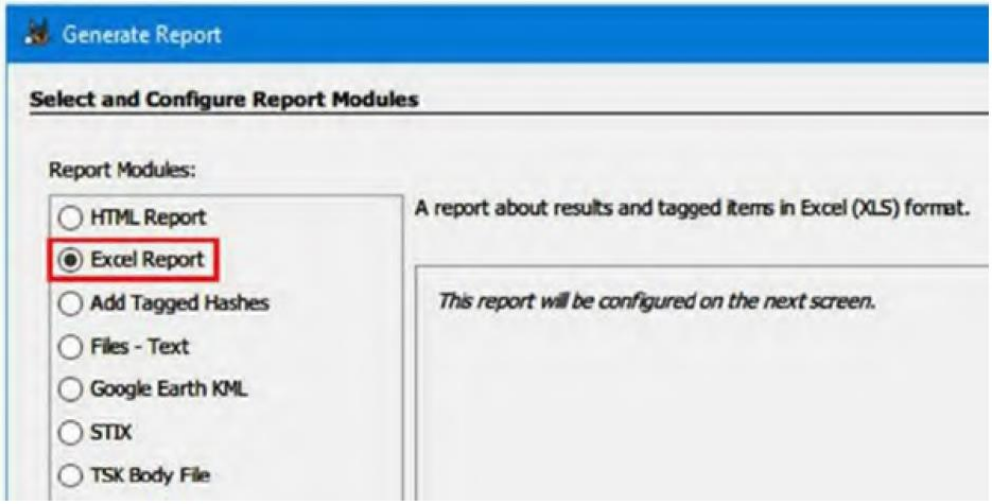
Après la finalisation du processus d'alimentation des données de la ligne de temps, Autopsy peut fournir des données dans trois modes d'affichage :

- Mode pour les diagrammes à barres (comptes) : Comme le montre la figure ci-dessous, ce mode fournit moins d'informations et est destiné à répondre aux demandes concernant le nombre de modifications de données survenues au cours d'une période donnée. Autopsie permet aux enquêteurs de la police scientifique d'inspecter le contenu du fichier d'images de la police scientifique à l'aide d'une variété d'applications de visualisation.
- Mode détail : Ce mode fournit des informations sur les événements et les présente à l'aide d'une méthode de regroupement unique en regroupant les mêmes fichiers d'événement dans un dossier et en affichant les URL appartenant à un domaine comme un seul événement.
- Mode liste : Similaire au mode détail, mais affiche les résultats dans une liste ordonnée chronologiquement.



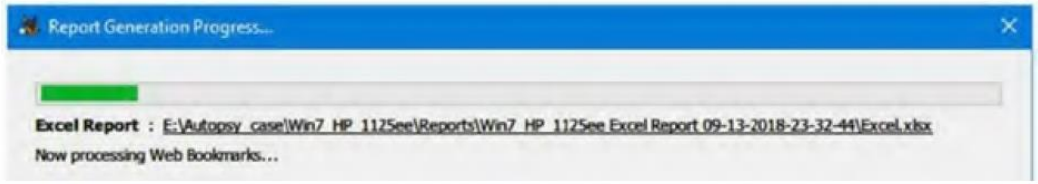
Outils d'analyse chronologique

Autopsie vous permet de créer un rapport au format texte, Excel, HTML et autres formats de fichiers, y compris les horodatages de chaque fichier de l'image judiciaire que vous avez fournie. Cette capacité offre la possibilité d'utiliser ces données dans des applications autres que l'outil Autopsie. Pour générer le rapport sur la chronologie, il suffit de cliquer sur le menu Outils → sélectionner l'assistant Générer un rapport. Cela permet de sélectionner différents modules de format de rapport, comme illustré dans la figure suivante.



Select report format

La figureci-dessous affiche le rapport Excel sélectionné afin que nous puissions vérifier les données à l'aide de Microsoft Excel ou d'autres alternatives telles que Apache OpenOffice. Cliquez sur Next, et nous pouvons configurer deux options pour les résultats Tagged (Étiqueté) ou All Results (Tous les résultats). Ici, une fois que nous avons sélectionné tous les résultats, Autopsy commence à générer le rapport. Une fois le processus de génération du rapport terminé, Autopsy affiche un lien permettant d'accéder au rapport généré, comme le montre la figure 7.5.



Report generation progress window

Autopsy-generated report

Récupération de fichiers

Dans toute forme d'investigation numérique, l'analyse des fichiers supprimés est une tâche essentielle. Les bons enquêteurs en criminalistique numérique doivent comprendre les titres et les emplacements des fichiers dans Windows, même après leur suppression, et analyser les fichiers (par exemple, en obtenant les métadonnées des fichiers supprimés pour faciliter l'enquête criminelle). Dans cette partie, nous passerons en revue plusieurs outils et procédures permettant de récupérer des documents essentiels et des fragments de fichiers qui peuvent contribuer à l'enquête sur le problème en question.

Suppression de fichiers

Le médecin légiste n'a pas besoin d'intervenir lorsqu'il utilise Autopsie pour récupérer des fichiers supprimés. Une Autopsie récupère les données de l'espace non alloué de la source de données fournie, qui est affiché sous les vues Fichiers supprimés dans le volet Explorateur de données. PhotoRec est un utilitaire gratuit, autonome et open-source qui permet de récupérer des données et des fichiers à partir d'une variété de périphériques numériques, y compris les cartes USB, HDD et externes, ainsi que les cartes SD des smartphones, les CD-ROM ou les appareils photo numériques. PhotoRec peut être utilisé conjointement avec TestDisk, une autre application libre spécialisée dans la récupération de partitions manquantes et/ou la réparation de disques non amorçables afin qu'ils puissent être redémarrés. Une démonstration détaillée de l'utilisation de TestDisk.

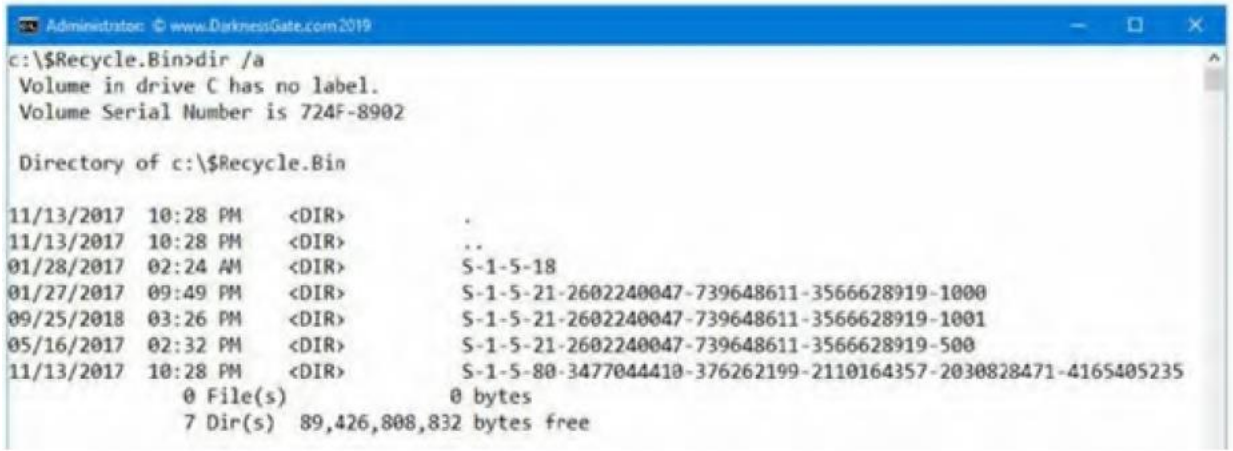
Investigation de la corbeille

La corbeille du système d'exploitation Windows a été introduite initialement dans Windows 95 ; elle contient les fichiers qui ont été supprimés par les utilisateurs mais qui restent sur le système. Lorsqu'un utilisateur supprime un fichier (en appuyant sur la touche de suppression conventionnelle après avoir sélectionné le fichier cible OU en sélectionnant un fichier, en cliquant dessus avec le bouton droit de la souris et en sélectionnant l'option "Supprimer" du menu contextuel), Windows envoie le fichier concerné dans la corbeille plutôt que de l'effacer définitivement. Il s'agit du comportement par défaut de Windows ; toutefois, un utilisateur peut modifier les paramètres de la corbeille pour supprimer les fichiers de manière permanente plutôt que de les déplacer vers la corbeille. Peu d'utilisateurs maintiennent la touche Majuscule enfoncée lorsqu'ils suppriment des fichiers ; cette option supprime définitivement les données et les fichiers au lieu de les déplacer vers la corbeille.

Dans la pratique, peu de personnes suppriment définitivement les fichiers recyclés (ou même le savent) ; par conséquent, la corbeille peut stocker des artefacts recyclés vitaux, qui sont considérés comme des sources précieuses de preuves numériques. Lorsqu'un utilisateur supprime un fichier, Windows l'envoie automatiquement dans la corbeille. Le nom et l'emplacement des fichiers de la corbeille varient selon les versions de Windows. Les fichiers supprimés sous le système de fichiers FAT de Windows XP sont enregistrés dans le dossier C:\Recycler du lecteur C :. Ce dossier contient également un autre fichier important intitulé INFO2 en tant que fichier caché. Pour les afficher, activez l'option Afficher les fichiers cachés, y compris les fichiers C:\ OS. Le dossier Recycler contient quelques dossiers nommés en fonction de l'identification de sécurité de l'utilisateur (SID) ; si un système compte de nombreux utilisateurs, chacun d'entre eux aura son propre dossier contenant les éléments supprimés appartenant à ce compte d'utilisateur. Dans le dossier de la corbeille de recyclage de chaque utilisateur se trouve un autre fichier essentiel, appelé INFO2, qui contient un index de tous les fichiers que l'utilisateur a précédemment supprimés. Il contient également des informations sur chaque fichier supprimé, telles que son emplacement d'origine, sa taille et la date et l'heure de sa suppression. Vista et les versions ultérieures de Windows (7 à 10) ont modifié la corbeille, les éléments supprimés et le dossier principal.

Investigation de la corbeille

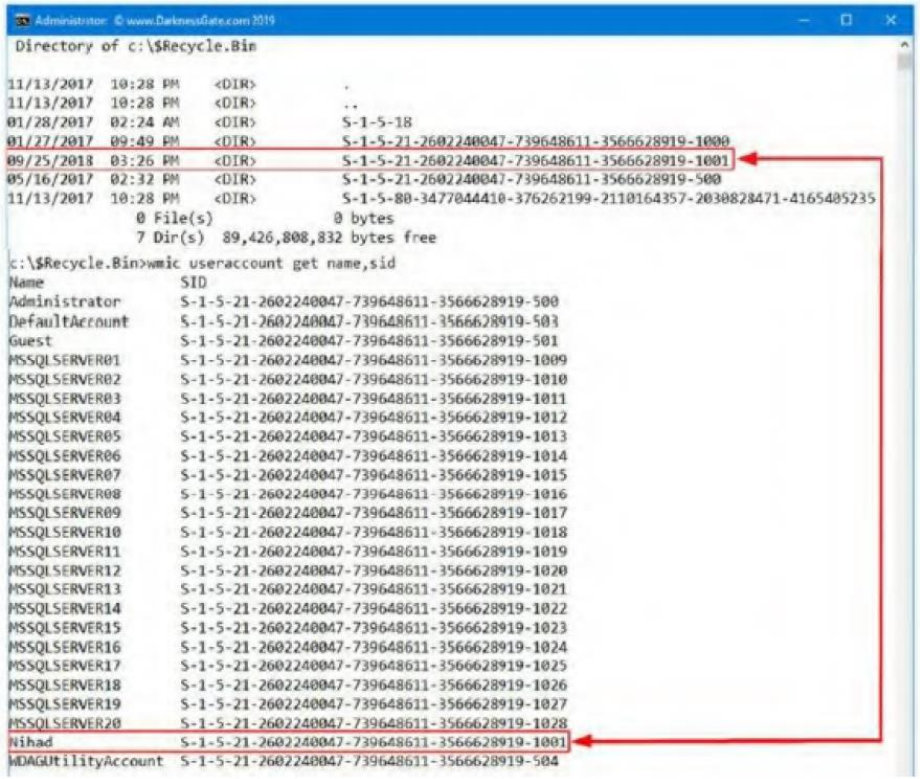
Les fichiers supprimés, par exemple, sont enregistrés dans un dossier appelé $Recycle.Bin, qui comporte un sous-répertoire pour chaque utilisateur du système, nommé d'après l'IDS de l'utilisateur en question. Lorsqu'un fichier est supprimé dans les versions récentes du système d'exploitation Windows, il est déplacé vers la corbeille en tant que premier fichier, y compris le contenu du fichier recyclé commençant par "$R", et l'autre fichier contenant les métadonnées du fichier supprimé commençant par "$I". Il n'est donc plus nécessaire d'utiliser le fichierINFO2 des versions antérieures de Windows, qui servait à recycler les métadonnées d'un fichier. En ce qui concerne la quantité de données supprimées que la corbeille de Windows peut contenir, sa capacité de stockage est limitée. Dans Windows XP, la corbeille est configurée par défaut pour contenir 10 % du disque dur ; si elle atteint sa pleine capacité, elle mettra à la poubelle les anciennes données afin de créer un espace pour les nouvelles données supprimées. Dans les versions récentes de Windows, telles que Vista et les versions ultérieures, la taille par défaut est de 10 % des 40 premiers Go d'espace de stockage et de 5 % de l'espace de stockage restant au-delà de 40 Go. Essayons de supprimer un fichier et de l'analyser avec Windows 10 et un programme gratuit appelé $I Parse. Ouvrez une invite de commande et changez le répertoire de travail en dossier $Recycle.Bin sur le disque C : à l'aide de la commande CD. En utilisant la commande DIR et le commutateur /a, vous pouvez afficher le contenu d'un dossier (pour afficher les fichiers système cachés). La figure suivante illustre ces instructions.



View $Recycle.Bin contents

Investigation de la corbeille

La corbeille est divisée en quatre sous-dossiers, chacun correspondant à l'IDS de la personne qui a supprimé le fichier. Lorsque le fichier est supprimé, il est envoyé pour la première fois dans la corbeille, puis un sous-dossier est également créé. La commande "wmic useraccount get name, sid" permet de connaître le nom du compte utilisateur propriétaire d'un sous-répertoire SID donné. Cela permet de connaître tous les comptes utilisateurs de la machine cible et de déterminer quel sous-répertoire SID de la corbeille correspond à l'utilisateur, comme le montre la figure suivante.

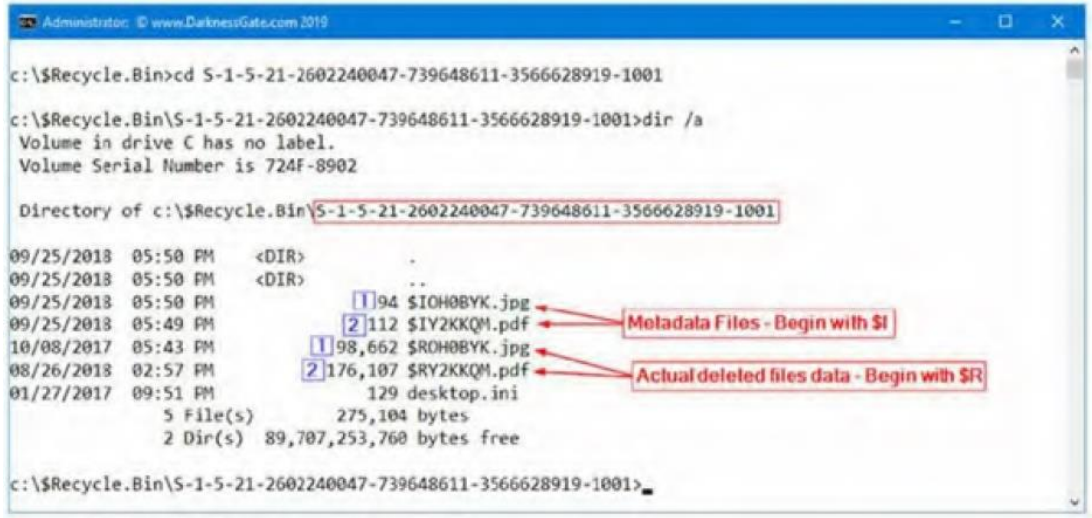


Determine owner of specific SID subfolder inside $Recycle.Bin

PARTIE 3

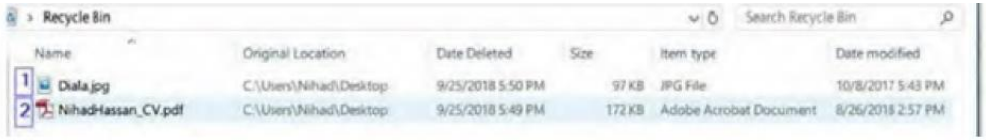
Investigation de la corbeille

Nous pouvons utiliser la commande change directory (CD) pour accéder à la corbeille de recyclage du compte cible une fois que nous savons à quel compte il appartient. Pour afficher le contenu d'un répertoire, utilisez la commande DIR avec le commutateur /a, comme illustré sur la figure suivante.

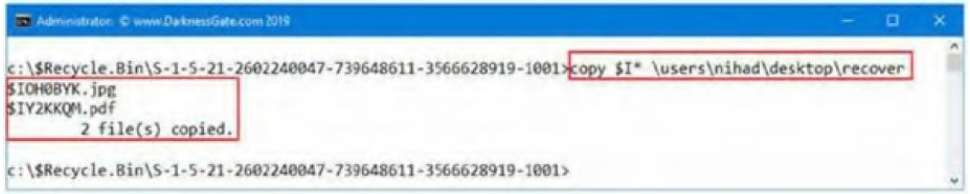


Determine owner of specific SID subfolder inside $Recycle.Bin

La figure précédente affiche la corbeille cible qui contient quatre fichiers - il s'agit des fichiers supprimés présentés dans la figure ci-dessous. Comme indiqué précédemment, chaque fichier supprimé contient deux fichiers différents dans la corbeille : le fichier de métadonnées et le contenu réel du fichier supprimé, qui peuvent être récupérés.

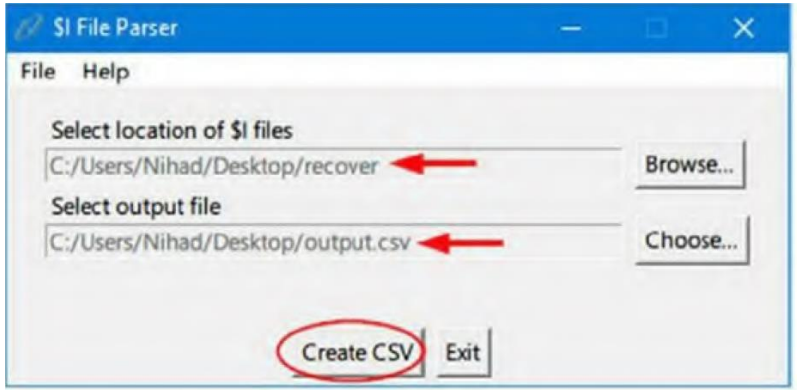


Regardons les métadonnées du fichier supprimé, également connu sous le nom de fichiers d'index (commençant par $I), dans la corbeille de Windows Vista, puis extrayons son contenu à l'aide d'un programme gratuit appelé $I Parse (s'il est zippé). Pour utiliser cet utilitaire, vous devez d'abord extraire le fichier de métadonnées du fichier recyclé. Pour ce faire, ouvrez une fenêtre de commande et tapez ce qui suit (voir figure 7.11) : $I* \users\ desktop\recover est copié, et l'outil $I Parse est exécuté à partir du menu File (Fichier). Sélectionnez le dossier des fichiers de métadonnées dans la liste des options.



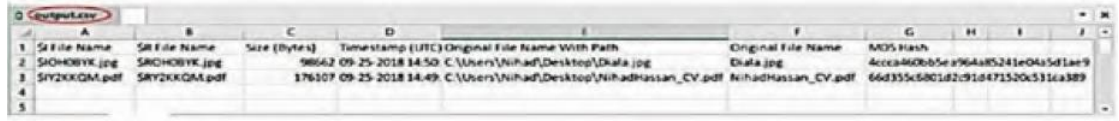
Investigation de la corbeille

Sélectionnez l'emplacement du fichier CSV de sortie, qui contiendra les résultats analysés du menu du code du programme, en cliquant sur le bouton Choose:



Parse metadata files in the target directory

Enfin, cliquez sur Créer CSV lorsque tous les fichiers ont été analysés, une fenêtre de réussite s'affiche et vous avez terminé. Ouvrez maintenant le fichier de sortie (Output.csv) pour voir une liste de tous les noms de fichiers recyclés dans la corbeille cible, ainsi que les informations de métadonnées pour la date/heure de suppression, le chemin d'origine et la taille du fichier, comme le montre la figure:



Output.csv displays recycled files' metadata files

"Rifiuti2" peut être utilisé pour extraire des informations des fichiers metadataINFO2 recyclés dans Windows XP (et les versions supérieures du système d'exploitation Windows).

PARTIE 3

Data carving (Découpage des données)

Le découpage des données est utilisé dans les enquêtes judiciaires numériques dans le cadre d'une récupération de données sophistiquée pour extraire des fichiers spécifiques à l'aide des informations du pied de page et de l'en-tête du fichier. Ces informations sont recueillies à partir de l'espace non alloué (données brutes) sans utiliser de structure MFT ou de système de fichiers. Lorsque le système de fichiers qui était à l'origine responsable de l'organisation de ces fichiers sur le disque dur est absent ou corrompu, la sculpture de données peut être la seule méthode pour récupérer des artefacts vitaux et des fichiers de preuve à partir de fragments de fichiers dans le cadre d'une enquête criminelle. Lorsqu'il s'agit d'extraire un ou plusieurs fichiers d'un flux de trafic réseau enregistré, la sculpture de données est également nécessaire. La sculpture de données est une méthode de criminalistique numérique plus avancée qui sort du cadre de cet ouvrage. Les enquêteurs experts en criminalistique peuvent toutefois utiliser des techniques de découpage de données pour extraire (récupérer) des données organisées, et donc un fichier, comme un document ou une photo, à partir de données non structurées ou brutes. Bien que le découpage de fichiers puisse être effectué à l'aide d'un simple éditeur Hex, certains outils peuvent aider les enquêteurs, tels que Foremost, Scalpel, Jpegcarver et Forensics wiki.

Action du compte d'utilisateur associé.

Un PC Windows suspect peut contenir de nombreux comptes, par exemple un pour Nihad, un autre pour Rita et encore un autre pour Susan. Le SID est un numéro unique qui différencie chaque compte sur un PC Windows. Un expert en criminalistique numérique peut utiliser ce SID pour déterminer quel compte d'utilisateur a effectué quelle activité ou quand un certain compte d'utilisateur a provoqué un événement spécifique.

Analyse du registre Windows

Le registre est le cœur du système d'exploitation Windows ; il stocke des informations vitales dont le système d'exploitation et les applications installées ont besoin pour fonctionner. Presque toutes les actions effectuées par un utilisateur de Windows sont enregistrées dans le registre d'une manière ou d'une autre, ce qui fait du registre une riche source de preuves qui peut être incroyablement utile dans toute enquête judiciaire numérique.

Architecture du registre Windows

Le registre est une base de données hiérarchique qui contient les préférences de l'utilisateur et l'historique de l'utilisation des ordinateurs et des programmes, ainsi que les paramètres de configuration de Windows pour les applications logicielles, les systèmes d'exploitation et le matériel. Les données du registre sont organisées sous forme d'arbre, chaque nœud de l'arbre étant appelé clé. Outre les valeurs de données, une clé peut inclure d'autres clés (sous-clés), comme le montre la figure suivante:

Registry hive	Supporting files
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

Windows registry structure

Architecture du registre Windows

Le registre de Windows comporte cinq dossiers racine ou ruches. Lorsque vous utilisez l'éditeur de registre pour la première fois, les premiers dossiers apparaissent sur le côté gauche de l'écran et toutes les autres entrées sont réduites. En ce qui concerne la durabilité des données, les répertoires racine sont divisés en deux catégories : les répertoires volatils et les répertoires non volatils. Les clés non volatiles HKEY LOCAL MACHINE et HKEY USERS sont sauvegardées sur le disque dur ; en revanche, les autres ruches sont volatiles et doivent être collectées lorsque le système est en cours d'exécution pour obtenir des informations pertinentes. Le registre de Windows peut être examiné par les enquêteurs en criminalistique numérique à l'aide du registre contenu dans une image de criminalistique. Par conséquent, l'outil de criminalistique informatique sera utilisé pour explorer les données du registre de la même manière que l'explorateur de fichiers de Windows. Deuxièmement, l'analyse en direct permet d'accéder au registre à l'aide de l'éditeur de registre de Windows, comme vous le feriez sur n'importe quelle autre machine.

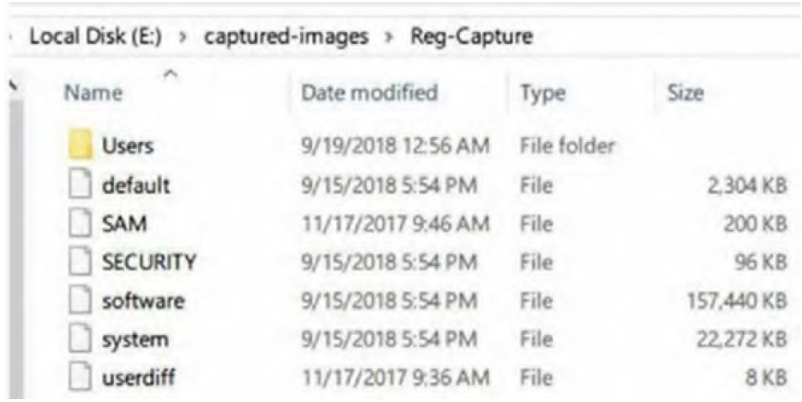
Il est essentiel de savoir où se trouvent les fichiers de registre si nous étudions le registre Windows à l'aide d'une image judiciaire enregistrée. Les ruches de registre sont stockées dans le dossier Windows | System32 | Config, donc si votre système d'exploitation est installé sur le disque C :, vous trouverez vos fichiers de registre dans le dossier C:\NWindows |System32 | Config. Vous trouverez de nombreux fichiers dans ce dossier (un pour chaque répertoire de stockage racine et quelques fichiers de soutien pour chacun d'entre eux, à l'exception du répertoire de stockage HKEYCURRENT USER, qui est placé dans votre dossier de profil). Un éditeur de registre est inclus dans Windows, permettant à tout utilisateur disposant de privilèges d'administrateur de visualiser, de modifier et de sauvegarder le registre.

Acquisition du registre de Windows

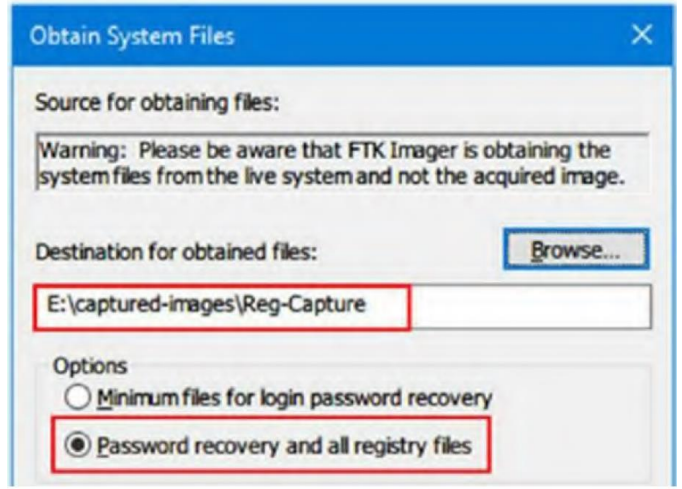
Lors de l'obtention du lecteur système de la machine cible ou de l'acquisition d'un disque dur complet, les outils d'investigation informatique acquièrent les données du registre Windows. Vous pouvez également supprimer uniquement les fichiers de registre d'un système en cours d'exécution et les enregistrer séparément pour une étude ultérieure (c'est ce que l'on appelle une image de registre). Pour acquérir le registre de la machine Windows cible à l'aide de FTK Imager, vous devez d'abord télécharger AccessData FTK Imager sur une clé USB. Attachez le périphérique USB contenant FTK Imager à l'ordinateur compromis, lancez FTK Image, puis naviguez dans le menu File pour acquérir Protected Files.

La figure ci-dessous illustre la nouvelle boîte de dialogue ; sélectionnez l'emplacement où vous souhaitez stocker les fichiers récupérés, et cochez l'option Récupération du mot de passe et de tous les fichiers de registre avant de cliquer sur OK. La progression de l'exportation des fichiers de registre est affichée dans une fenêtre de progression, qui disparaît à la fin sans afficher de message de réussite.

Pour visualiser les fichiers générés, naviguez jusqu'au répertoire où vous avez stocké vos fichiers de registre ; vous devriez voir cinq fichiers et un dossier.



Registry forensic image captured with AccessData FTK Imager



FTK Imager to acquire target Windows registry database

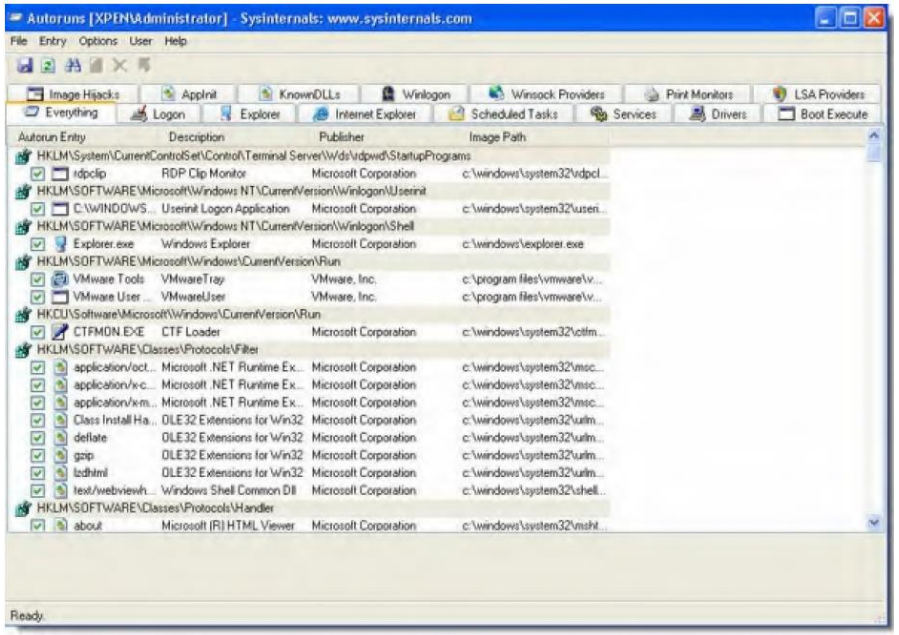
Le registre de la machine cible ayant été exporté, nous pouvons maintenant procéder à une évaluation plus poussée à l'aide de divers outils de criminalistique.

PARTIE 3

Examen du registre

À partir de l'image forensique recueillie, la plupart des applications d'informatique légale peuvent explorer le registre de Windows. D'autres outils se concentrent uniquement sur l'étude des données du registre Windows. Dans cette partie, nous supposerons que nous avons démarré avec une image criminelle suspecte afin d'exécuter différentes analyses criminelles sur celle-ci. Le cas échéant, plusieurs outils spécialisés dans la recherche de sections spécifiques du registre seront également fournis. Cette fonctionnalité est importante pour les logiciels antivirus, qui doivent d'abord s'exécuter pour bloquer tout logiciel dangereux avant que Windows ne puisse démarrer complètement. Les logiciels malveillants, tels que les enregistreurs de frappe et les réseaux de zombies, peuvent créer des entrées dans le registre Windows pour s'exécuter automatiquement au démarrage du système d'exploitation, comme l'illustre la figure suiavnte.

Dans de nombreuses circonstances, la recherche de programmes de démarrage peut contribuer à la police scientifique ; par exemple, un logiciel malveillant peut prendre le contrôle d'un système suspect et l'utiliser pour exécuter des attaques par déni de service à l'insu de son propriétaire. même si son ordinateur a été utilisé pour commettre un délit, un suspect peut se montrer très ouvert à l'égard des autorités lorsqu'un tel élément est sondé.

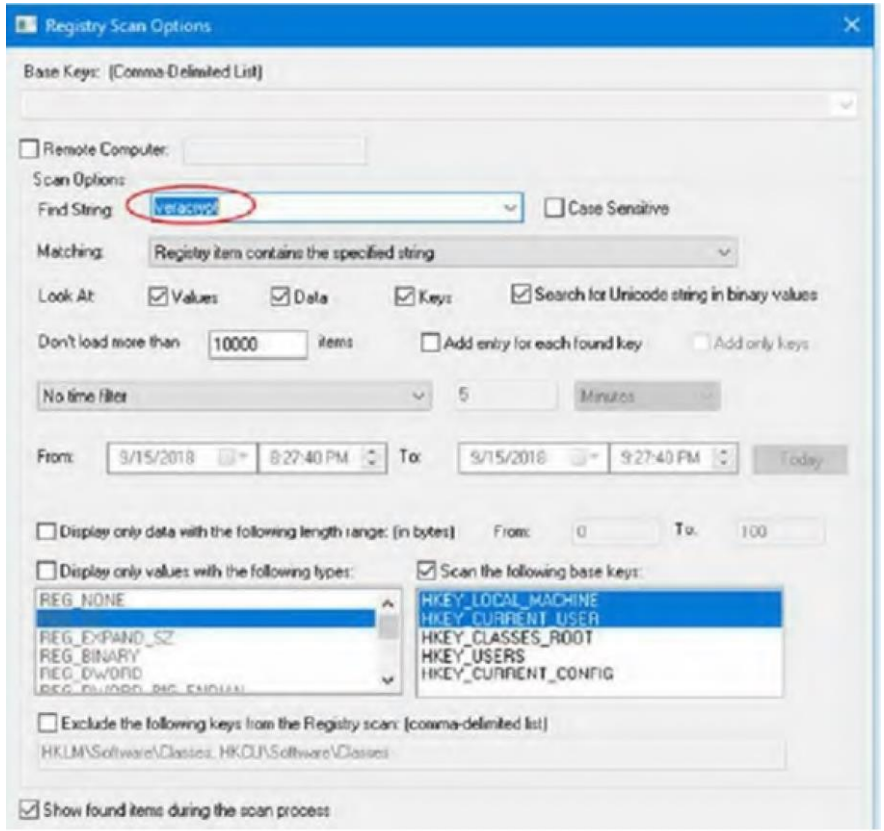


Autorun from Sysinternals

PARTIE 3

Les clés de programme du registre Windows.

Les enquêteurs judiciaires peuvent tirer un grand profit de la connaissance des programmes actuellement ou précédemment installés sur le système suspect. Par exemple, la présence d'applications de stéganographie et de cryptage ou les restes d'un tel outil indiquent que le système suspect peut contenir des données dissimulées ou être simplement utilisé pour exécuter un tel programme. Les emplacements suivants du registre de Windows conservent la trace de toutes les applications installées. Nous pouvons utiliser des outils automatisés pour rechercher un programme installé dans le registre de Windows ou pour rechercher des informations perdues comme des morceaux de programmes installés, des applications qui ont été laissées derrière, ou tout autre élément de données qui peut être caché dans le registre de Windows. RegScanner est un programme simple offert par Nirsoft qui recherche le registre de Windows sur la base de critères de recherche spécifiés fournis par l'utilisateur. Les résultats de la recherche sont affichés dans une liste, et l'utilisateur peut sélectionner n'importe quel élément de la liste pour ouvrir RegEdit et afficher la valeur correspondante. Nous pouvons également enregistrer les valeurs de registre contenues dans le fichier a.reg. Après l'exécution de ce programme, une fenêtre d'options de recherche s'affiche, dans laquelle vous pouvez saisir vos critères de recherche et spécifier certains paramètres de recherche (voir figure 7.18).



Registry scan options by RegScanner

Les clés de programme du registre Windows.

Tous les programmes ne nécessitent pas l'installation d'une entrée de registre avant d'être utilisés ; par exemple, les applications portables n'ont pas besoin d'être installées sur Windows pour s'exécuter, comme les applications exécutées à partir de clés USB. Il est possible d'examiner le registre pour vérifier si des périphériques USB ont déjà été connectés afin d'évaluer les possibilités d'exécution d'applications portables à partir d'un PC douteux. Un autre moyen de savoir si des PortableApps sont exécutées est de regarder dans le dossier Windows Prefetch. Il s'agit des fichiers temporaires stockés dans le dossier Système sous le nom de prefetch. Le Prefetch est une fonction de gestion de la mémoire. Le journal des applications fréquemment exécutées sur votre machine est stocké dans le dossier prefetch. Le journal est crypté au format Hash afin que personne ne puisse facilement décrypter les données de l'application.

Investigation des périphériques USB

Tous les périphériques USB précédemment connectés, leurs délais de connexion et le compte d'utilisateur qui les a installés sont enregistrés dans l'historique de Windows. Des informations techniques importantes concernant chaque périphérique USB connecté sont également stockées dans le registre de Windows, notamment l'ID du fournisseur, l'ID du produit, la révision et le numéro de série. Windows utilise cinq clés de registre pour conserver les informations relatives à l'historique du périphérique USB, chacune contenant une information distincte sur le périphérique connecté. Le registre de Windows est une base de données hiérarchique dans laquelle les informations sont présentées sur plusieurs niveaux (jusqu'à six). Les clés de ruche se trouvent au premier niveau.Il existe cinq clés de ruche, dont chacune commence par "HKEY_" et dont le nom est HKEY_CLASSES_ROOT, HKEY_CURRENT_USER,HKEY_LOCAL_MACHINE, HKEY_USERS et HKEY_CURRENT_CONFIG.Les enquêteurs seront en mesure de voir comment un délinquant a utilisé des dispositifs détachables, tels qu'une clé USB, pour mener/faciliter ses actions après avoir combiné ces informations. Vous pouvez télécharger un utilitaire gratuit appeléUSBDeview de Nirsoft pour automatiser le processus de découverte d'informations sur les dispositifs connectés à l'USB actuels et antérieurs. Cet outil peut exécuter toutes les opérations que nous venons de réaliser manuellement. De nombreuses informations (par exemple, le nom/la description du périphérique, le type de périphérique, le numéro de série et bien plus encore) sur chaque périphérique USB connecté s'afficheront après l'exécution de cet utilitaire sur la machine cible. La date de la dernière connexion/déconnexion reflète la première fois que le périphérique a été connecté au système. Lorsque le même périphérique est réinséré plusieurs fois, la date n'est pas mise à jour. La "Date de création" indique la date de la dernière connexion du même périphérique au système.

Malheureusement, tous les types de périphériques USB, tels que les périphériques USB qui utilisent le protocole de transfert de médias (MTP) pour se connecter aux PC, ne laissent pas de traces dans le registre Windows, comme nous l'avons montré. Le protocole MTP est utilisé par les appareils fonctionnant sous les nouvelles versions du système d'exploitation Android, ainsi que par les téléphones Windows et les Blackberry ; ce protocole ne laisse pas de traces dans le registre Windows lorsqu'un appareil USB est connecté à un PC Windows. Ce protocole ne laisse pas de traces dans le registre de Windows lorsqu'un périphérique USB est connecté à un PC Windows, ce qui nécessite l'utilisation d'un instrument spécialisé pour rechercher de tels objets. USB Detective (https://usbdetective.com) peut détecter les périphériques USB qui se connectent à Windows via le protocole MTP. Il dispose également d'outils avancés pour analyser en profondeur les périphériques USB liés, tels que la construction de lignes temporelles de chaque connexion/déconnexion unique et d'horodatages de suppression pour chaque périphérique ; cependant, pour accéder à toutes ces fonctions, vous devez passer à l'édition professionnelle premium. En résumé, cette partie, l'obtention de traces à partir d'un périphérique USB connecté via une connexion MTP, nécessite un traitement spécifique ; vérifiez dans le manuel de votre logiciel d'investigation informatique l'existence d'une telle fonction.

Liste des fichiers les plus récemment utilisés.

Lorsque vous ouvrez un fichier à l'aide de l'explorateur de fichiers de Windows, d'une boîte de dialogue standard d'ouverture/enregistrement ou d'une invite de commande MS-DOS sur le registre, Windows conserve la trace des fichiers les plus récemment accédés. De nombreuses applications Windows, y compris les fichiers MS Office récemment ouverts et les sites web récemment visités, disposent de listes des fichiers les plus récemment utilisés (MRU) ; ces applications répertorient les fichiers les plus récemment accédés.

Analyse du réseau.

Lorsqu'un utilisateur de Windows connecte son ordinateur à l'internet ou à un intranet, Windows enregistre la connexion dans le registre. La connaissance de la connexion réseau est cruciale à des fins judiciaires ; par exemple, le registre détaille toutes les cartes réseau qui ont été utilisées sur le système suspect, qu'elles soient intégrées ou externes (par exemple, via un port USB). Le registre indique également le profil de la connexion sans fil (nom, adresse IP, masque de sous-réseau et DHCP), ainsi que la date à laquelle la connexion a été établie et la dernière fois qu'elle a été utilisée.

Windows shutdown time

Sous la valeur ShutdownTime de l'entrée de registre HKEY LOCALMACHINE\SYSTEM\Current\ControlSet\Control\Windows, Windows enregistre la date du dernier arrêt de la machine. La valeur d'arrêt est enregistrée sous la forme d'une valeur binaire écrite au format Little Endian ; utilisez l'outilDCode de Digital Detective pour la décoder dans un format lisible. Pour utiliser cet outil, il faut d'abord extraire la valeur binaire de la clé cible, puis la saisir dans l'application DCode à l'aide des choix, comme le montre la figure 7.19.

Decode Windows shutdown time

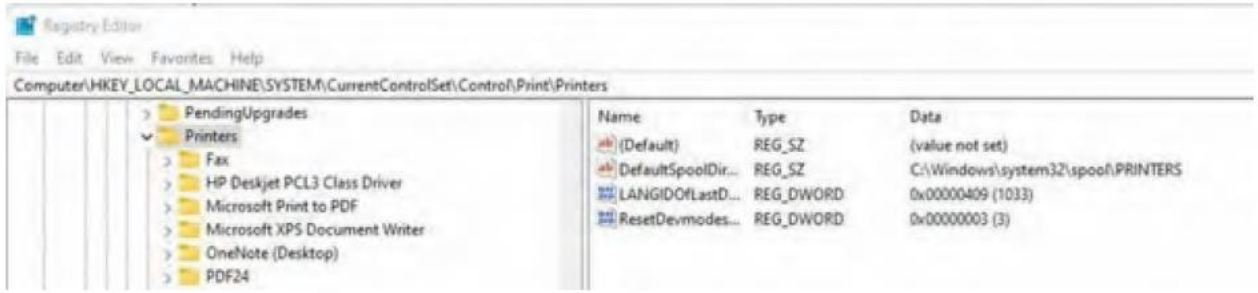
PARTIE 3

UserAssist forensics

UserAssist conserve la trace de toutes les applications exécutables récemment ouvertes, ainsi que la fréquence d'utilisation (nombre d'exécutions) de chacune d'entre elles. Les informations de la clé de registre UserAssist se trouvent à l'emplacement suivant : HKEY CURRENTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist.Le schéma de codage ROT-13 est utilisé pour coder les informations stockées dans les clés UserAssist. Pour décoder ces données, utilisez UserAssist-View, un programme Nirsoft qui peut afficher les données stockées dans un format compréhensible.

Informations sur le registre des imprimantes.

Par exemple, pour vérifier les propriétés des imprimantes actuellement installées sur le système cible, accédez à HKEY LOCALMACHINESYSTEM\Current\ControlSet\Control\Printers\Nom de l'imprimante dans le registre Windows (voir figure 7.20).

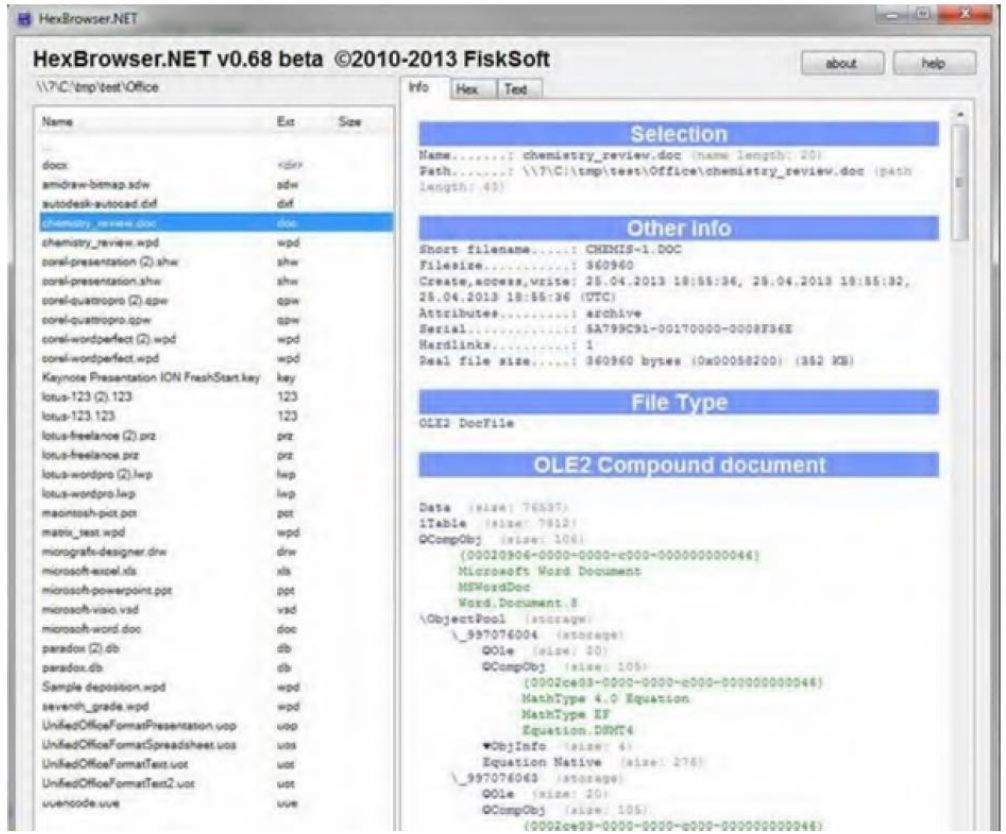


View installed printer properties

Identification du format de fichier

L'analyse de la signature est une procédure qui consiste à comparer les en-têtes et les extensions de fichiers à une base de données connue d'en-têtes et d'extensions de fichiers afin de déterminer s'il y a eu tentative de dissimulation du type de fichier original (en changeant l'extension du fichier par quelque chose d'autre pour le dissimuler aux yeux des enquêteurs). Comme nous le savons tous, chaque fichier sous Windows possède sa signature, qui est normalement contenue dans les 20 premiers octets. En inspectant un fichier à l'aide du Bloc-notes ou d'un éditeur hexadécimal, il est possible de déterminer sa signature originale. En étudiant manuellement la signature d'un fichier, nous pouvons déterminer son type. Nous pouvons utiliser HexBrowser, un programme gratuit, pour automatiser cette procédure. HexBrowser est un programme Windows capable de détecter et d'afficher des informations détaillées sur plus de 1 000 types de fichiers différents, comme le montre la figure suivante.

Dans ce cas, HexBrowser a été utilisé pour explorer un fichier avec une extension DLL, et il a été révélé que le type de fichier original était MS Word 2016. L'Autopsie peut détecter des erreurs d'extension de fichier ; pour utiliser cette capacité, vous devez d'abord activer le module "Détecteur d'erreurs d'extension". En naviguant dans le menu Outils et en sélectionnant Choix de non-concordance d'extension de fichier, vous pouvez personnaliser davantage vos options de recherche de non-concordance de fichier. Vous pouvez ajouter ou supprimer des extensions en fonction des exigences de votre cas, et les résultats sont affichés dans l'arborescence des résultats sous Extension Mismatch Detected (incompatibilité d'extension détectée).



HexBrowser discovers original formats

PARTIE 3

Windows thumbnail forensics

Lorsqu'un utilisateur choisit d'afficher les fichiers sous forme de vignettes, Windows enregistre les vignettes des fichiers graphiques (JPEG, BMP, GIF, PNG et TIFF), de certains types de documents (DOCX, PPTX et PDF) et des fichiers vidéo dans le fichier cache des vignettes thumbs.db pour un affichage ultérieur. L'examen de cette fonction peut révéler des fichiers antérieurs (par exemple, des photos) qui se trouvaient sur un système même après que l'utilisateur les a effacés, car les vignettes d'image peuvent persister dans thumbs.db. Les aperçus des vignettes sont stockés dans un emplacement central dans les versions modernes de Windows (Vista+). Le cache est conservé sous la forme d'une succession de fichiers portant le nom habituel thumb cache xxx.db (XXX fait référence à sa taille), ainsi que d'un fichier d'index permettant de trouver les vignettes dans chaque base de données, dans%userprofile%\AppData\Local\Microsoft\Windows\Explorer. Thumbs Viewer est un utilitaire portable qui extrait les vignettes des fichiers de base de données Thumbs.db, ehthumbs.db, ehthumbs vista.db, Image.db, Video.db, TVThumb.db, et musicThumb.db sont disponibles sur toutes les versions du système d'exploitation Windows. Il peut être téléchargé à l'adresse suivante : https://thumbsviewer.github.io. Si vous avez besoin d'accéder aux fichiers thumb cache *.db, essayez Thumbcache Viewer (https://thumbcacheviewer.github.io), un outil du même créateur qui vous permet d'extraire des images miniatures des fichiers de base de données thumb cache *.db et icon cache *.db trouvés dans WindowsVista, 7, 8, 8.1, et 10. Dans Windows Vista et les versions ultérieures, les caches de vignettes se trouvent normalement dans Users<USERNAME>\AppData\Local\Microsoft\Windows\Explorer.

Windows 10 forensics.

Le navigateur Edge, les applications Windows 10, Cortana (l'assistant numérique à commande vocale de Microsoft), et bien d'autres nouvelles fonctionnalités et applications sont à la disposition des utilisateurs de Windows 10. La plus importante a été l'introduction de la plateforme de programme universelle (UAP), qui permet à la même application de fonctionner sur différentes plateformes, y compris les ordinateurs portables, les ordinateurs de bureau, les appareils IoT, les tablettes, les smartphones, et plus encore. Windows 10 s'accompagne d'une multitude de nouvelles fonctionnalités. Dans cette section, nous allons nous pencher sur deux d'entre elles : Base de données de la zone de notification Cortana forensics

Base de données de la zone de notification

Cette nouvelle fonctionnalité a fait ses débuts avec Windows 8 et est désormais disponible dans les versions 10 et 11 de Windows. Tout programme capable de générer une notification dans le systray l'enregistre dans une base de données centralisée. Sous le nom de wpndatabase.db, la base de données de la zone de notification est située dans le dossierC:\NUsers\NUserName\NAppData\NLocal\NMicrosoft\NWindows\NNNotifications. La base de données des notifications stocke divers types de notifications que les utilisateurs de Windows voient dans le coin inférieur droit de l'écran, notamment des messages contextuels provenant de diverses parties du système d'exploitation (par exemple, sauvegarde et restauration), des alertes de courrier électronique et des messages liés à des applications spécifiques telles que les téléchargements Torrent, entre autres choses. Les notifications Windows ont une importance médico-légale car elles peuvent montrer des comportements antérieurs de l'utilisateur sur la machine cible.

Cortana forensics

Cortana est un assistant personnel qui répond aux commandes vocales, à l'instar de Siri d'Apple. Cortana a d'abord été lancée dans Windows Phone 8.1, puis a migré vers le bureau Windows avec la sortie de Windows 10. Son principal objectif est d'offrir aux utilisateurs de Windows 10 une expérience personnalisée en leur proposant des suggestions de recherche, en se souvenant d'événements, en envoyant des courriels au nom de l'utilisateur (s'il est correctement configuré), en naviguant sur Internet et en surveillant la météo, entre autres fonctions utiles. Cortana fonctionne en accumulant des connaissances. En termes de criminalistique numérique, outre les données de géolocalisation (longitude et latitude des rappels basés sur la localisation) et les recherches en ligne, Cortana peut révéler une pléthore d'informations sur l'activité antérieure d'un utilisateur sur le système cible. Bien que Cortana fournisse de nombreuses informations utiles, elle n'est pas toujours activée sur les appareils Windows, car cet outil a la réputation de porter atteinte à la vie privée, et de nombreux utilisateurs de Windows l'ont déjà désactivée pour des raisons de confidentialité. Cortana enregistre les informations relatives à son travail dans une base de données **ESE (extensible storage engine)** à l'adresse :

```
\Users\<UserName>\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\D\IndexedDB.edb
\Users\<UserName>\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\
```

Base de données de la zone de notification

Le fichier CortanaCoreDb.dat contient des informations importantes sur les données de géolocalisation de l'utilisateur, ainsi que sur les rappels émis par l'utilisateur et sur le lieu et le moment où ils ont été effectués. N'oubliez pas que Cortana a accès à un grand nombre d'informations personnelles sur ses utilisateurs ; néanmoins, il semble que Microsoft ait déplacé un grand nombre d'interactions de Cortana dans le nuage Microsoft. Les artefacts liés à Cortana se trouvent également dans les dossiers des machines locales à l'adresse suivante :

\Users\<User>\AppData\Local\Packages\Microsoft.Windows.Cortana_1234\LocalState\LocalRecorder\

Ce dossier contient des enregistrements de commandes vocales (fichiers audio WAV) envoyées à Cortana par un utilisateur afin d'exécuter une tâche. Toutes les suites d'investigation informatique ne peuvent pas décoder la base de données Cortana ; lisez toujours les instructions ou vérifiez les fonctionnalités de l'outil avant de l'acheter. EnCase, par exemple, propose un script qui décode les mots de recherche de Cortana à partir des fichiers IndexedDB.edb fournis par l'utilisateur.

Conclusion

Windows stocke une grande quantité de données sur ses utilisateurs, que l'on appelle artefacts dans le domaine de la criminalistique informatique. Ces données peuvent être dispersées dans le système à de nombreux endroits. Peu de gens savent que les artefacts du programme qui a été exécuté, ainsi que les clés USB qui ont été attachées à un PC Windows depuis son installation, sont sauvegardés à plusieurs endroits dans Windows. Il en va de même pour les fichiers supprimés : la corbeille enregistre des informations sur chaque fichier supprimé et sur le compte qui l'a supprimé. Même si les données ont été supprimées volontairement ou simplement écrasées, des copies des fichiers et dossiers supprimés, formatés, modifiés, endommagés ou perdus peuvent toujours être trouvées sur le système cible à de nombreux endroits.

Le chapitre suivant traite de l'investigation des navigateurs Web pour résoudre l'affaire en question. Le courrier électronique joue également un rôle essentiel dans les communications de l'ère numérique, et il convient de comprendre comment analyser les messages électroniques pour trouver des indices.

PARTIE 4

Web Browser and E-mail Forensics

Dans ce module, vous allez :

Web Browser and E-mail Forensics

Ce que vous allez apprendre dans ce chapitre :

- Dans ce chapitre, nous verrons comment rechercher dans divers navigateurs Web des indices intéressants susceptibles de nous aider à résoudre l'affaire en cours dans les communications numériques d'aujourd'hui ; comment examiner les schémas de navigation des utilisateurs à la recherche d'indices et de données cachées dans les navigateurs Web. Par exemple, si nous examinons les navigateurs Web du suspect et que nous découvrons son historique de navigation, des mots de passe enregistrés ou qu'il télécharge ou recherche du matériel sur la stéganographie et les outils de cryptage, il s'agit d'une forte indication que l'utilisateur peut utiliser ces tactiques pour dissimuler des informations sensibles.

OFPPT
La Voie de l'Avenir

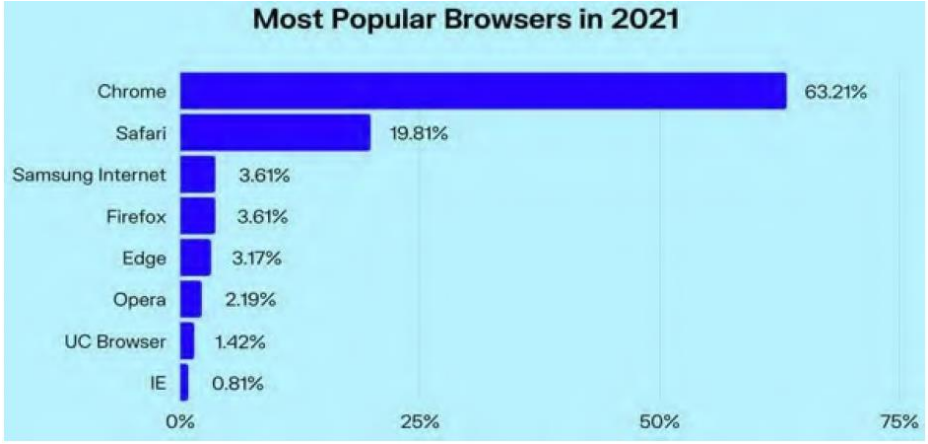
WEBFORCE
BE THE CHANGE

Introduction

Les applications Internet déjà déployées sur Windows peuvent fournir des informations utiles sur les activités informatiques antérieures de l'utilisateur. Un navigateur Web, par exemple, est la méthode par défaut pour accéder à l'internet, et les criminels l'utilisent pour perpétrer des délits liés à l'internet ou pour cibler d'autres personnes en ligne. Les navigateurs Web sont utilisés par les utilisateurs d'Internet pour socialiser, faire des achats en ligne, envoyer des courriels et surfer sur le Web, entre autres choses. L'analyse des artefacts du navigateur Web est un aspect important de toute enquête judiciaire informatique, car elle peut aider à localiser la source de la violation des comportements antérieurs de l'utilisateur dans de nombreuses circonstances.

Web browser forensics

Google Chrome, Safari, Samsung Internet, Firefox, Edge, Opera, UCBrowser et Internet Explorer de Microsoft détenaient la majorité des parts de marché des navigateurs Web à la fin de 2021. (Voir figure ci-dessous). En toile de fond, ce chapitre se concentre sur l'analyse d'artefacts provenant de trois navigateurs Web principaux : Google Chrome, Mozilla Firefox et Microsoft Edge, à l'aide de diverses techniques de criminalistique numérique.



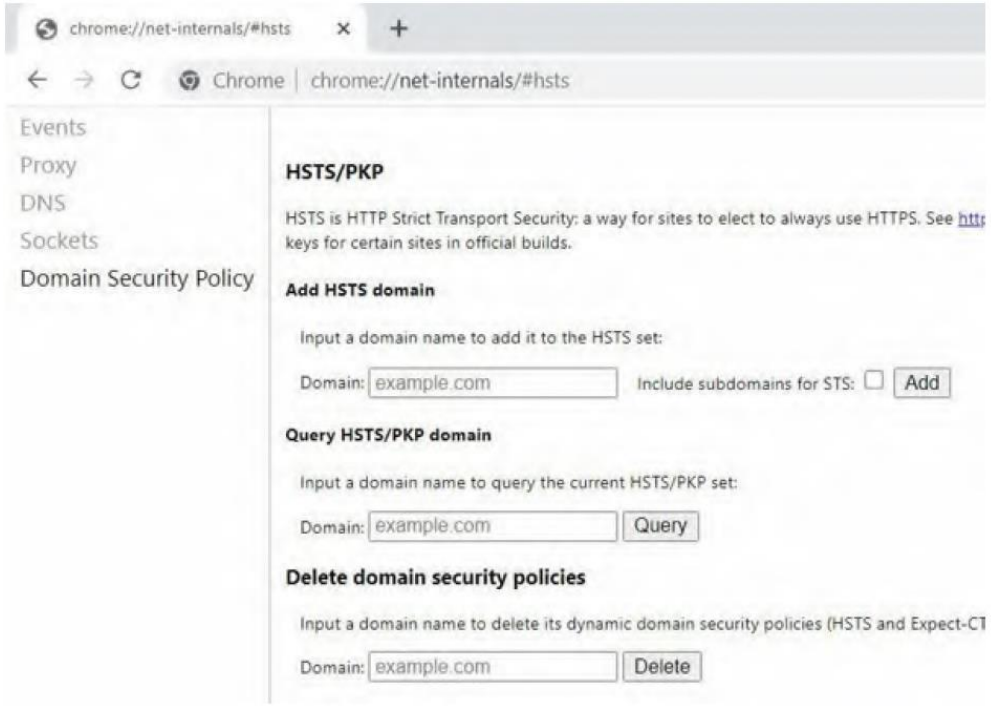
Popular Web browsers in 2021

En 2022, la part de marché varie légèrement entre les principaux concurrents, à savoir Chrome et Safari, tandis que les autres restent stables, comme le montre la figure suivante.

Web browser market share 2022

Google chrome browser forensics

La plupart des enquêteurs en criminalistique numérique rencontrent Google Chrome au cours de l'un de leurs examens, car il s'agit du navigateur Web le plus rapide et le plus largement utilisé sur les ordinateurs de bureau et les ordinateurs portables de nos jours. Google Chrome est basé surChromium, un projet de navigateur open-source développé par Google. Étant donné que le projet Chrome n'a pas encore été publié en tant que navigateur distinct, nous pouvons désigner Google Chrome [4] comme la version publique du projet. Vivaldi (https://vivaldi.com), le navigateur Yandex (https://browser.yandex.com), Centbrowser (www.centbrowser.com) et le navigateur Opera (www.opera.com), pour n'en citer que quelques-uns, sont tous basés sur le projet Chromium. La plupart des navigateurs Web basés sur le projet Chromium stockent les données de la même manière ; cela permet aux experts d'utiliser les mêmes techniques d'investigation que celles utilisées pour enquêter sur Google Chrome pour enquêter sur ces navigateurs, ce qui fait de l'enquête sur Google Chrome un modèle standard pour enquêter sur la plupart des navigateurs Web basés sur le projet Chromium. Chrome (créé par Google Inc.) utilise des bases de données SQLite pour stocker ses paramètres de configuration et les informations privées de l'utilisateur, tout comme les autres navigateurs web. Comme ces bases de données sont des fichiers sans extension, vous n'aurez aucune difficulté à les ouvrir à l'aide du navigateur SQLite. Pour le vérifier, allez dans le dossier de profil de Google Chrome et assurez-vous que l'option "Tous les fichiers (*)" est sélectionnée, où vous pouvez voir les événements, le proxy, le DNS, les sockets et la stratégie de sécurité du domaine, comme le montre la figure ci-après.

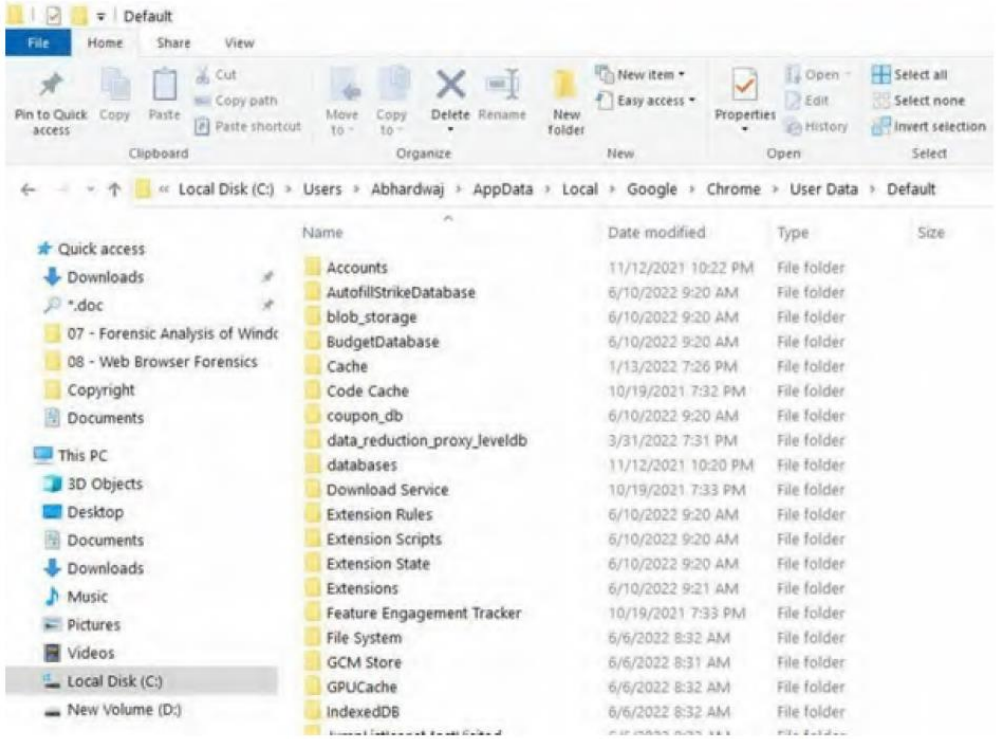


Google Chrome internals

Google chrome browser forensics

Les paramètres de configuration, les programmes, les signets et les extensions de Google Chrome sont tous stockés dans le profil. Google Chrome peut avoir de nombreux profils ; cependant, comme le montre la figure ci-après, il existe un profil par défaut qui peut être situé sous:

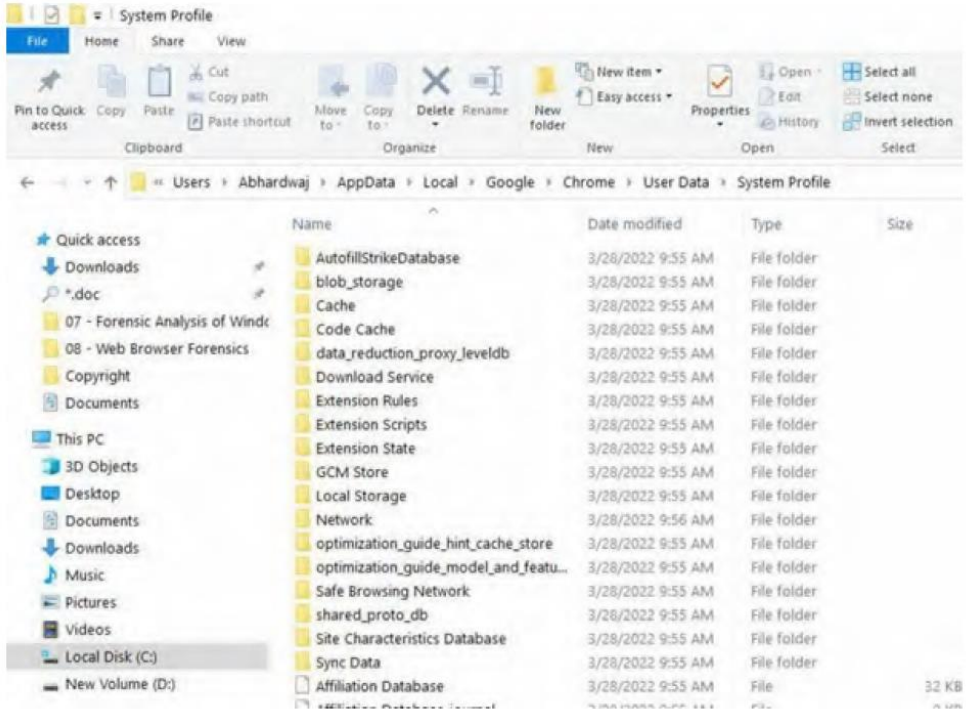
C:\NUsers\N<Nom d'utilisateur>\NAppData\NLocal\NGoogle\NChrome\NUserData\NDefault.



Google Chrome user data

Google chrome browser forensics

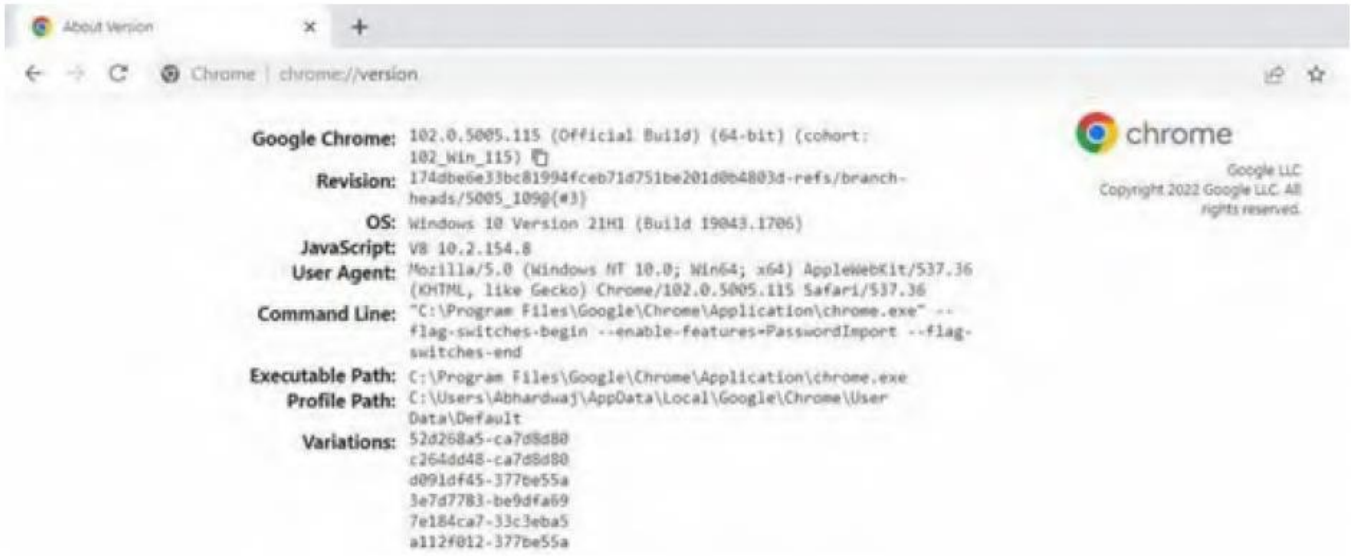
Si vous avez plusieurs profils dans Google Chrome, chacun d'entre eux aura son propre dossier contenant les paramètres du navigateur et les données privées (mots de passe, historique de navigation, signets, etc. Google Chrome n'attribue pas de nom aux profils supplémentaires en fonction de l'identifiant de l'utilisateur, mais leur donne un nom générique (par exemple, Profil système ou Profil 1, Profil 2, etc.) Les profils Chrome supplémentaires se trouvent dans le répertoireUsers\NUserName\AppData\Local\Google\Chrome\User Data\SystemProfile, comme le montre la figure ci-après. Ensuite, dans la fenêtre qui s'affiche, recherchez "Profile Path". Maintenant que nous savons comment y accéder, nous allons examiner les fichiers stockés dans le dossier du (des) profil(s) GoogleChrome.



Chrome system profile location

Google chrome browser forensics

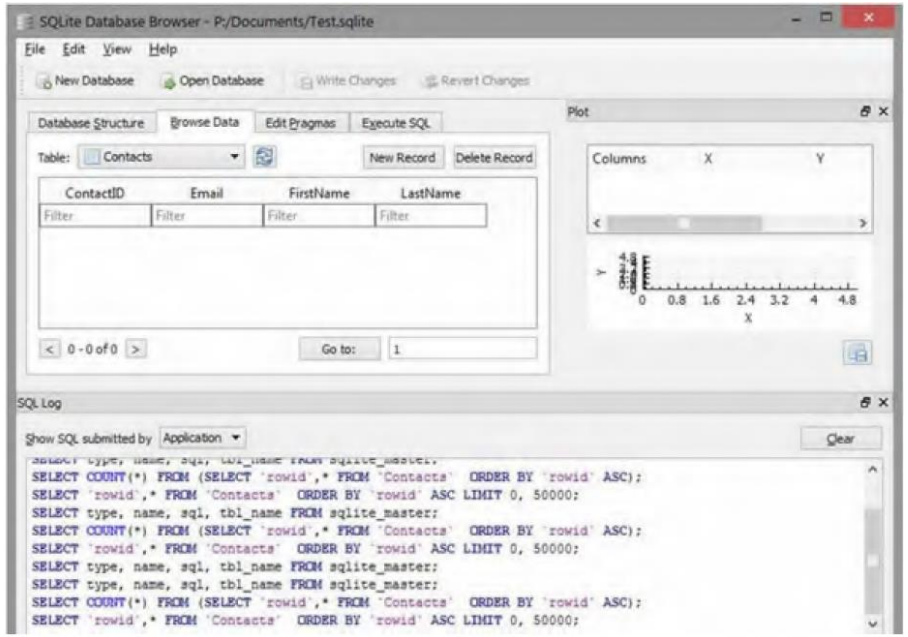
Pour trouver l'emplacement du dossier d'un profil Google Chrome (voir figure 8.6), démarrez une fenêtre Chrome avec le nom/image du profil dans le coin supérieur de la fenêtre du navigateur, puis tapez chrome:/version dans la barre d'adresse du navigateur.



Chrome version

Google chrome browser forensics

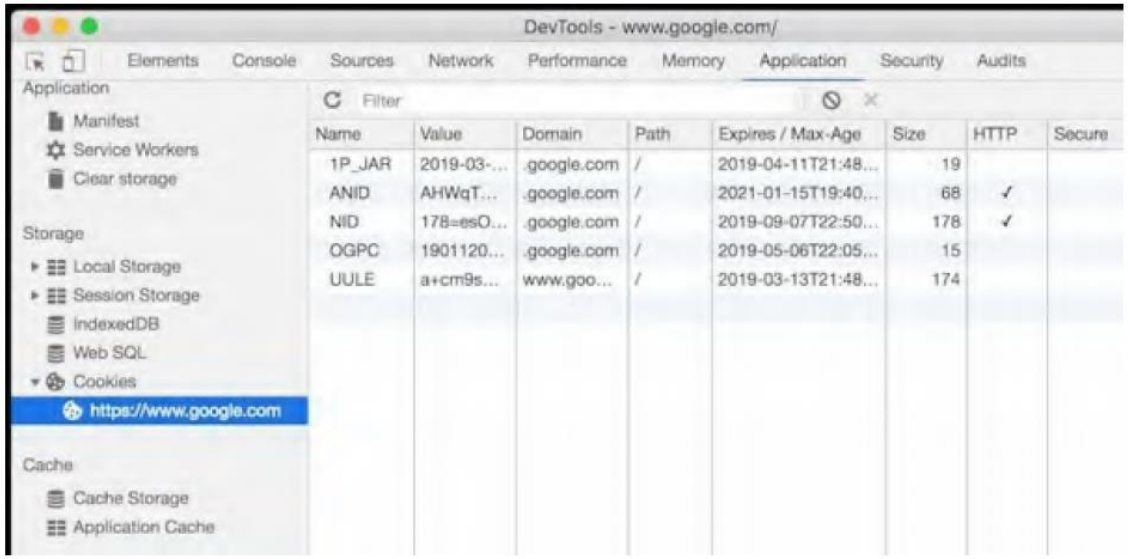
Le fichier de la base de données Historique est placé sous le profil de l'utilisateur de Chrome et stocke l'historique de navigation de l'utilisateur, les téléchargements, les mots-clés et les termes de recherche. Comme le montre la figure 8.7, ce fichier peut être inspecté à l'aide de DB Browser forSQLite. Allez dans le tableau Téléchargements sous l'onglet Parcourir les données pour découvrir quand un fichier spécifique a été téléchargé et une foule d'autres informations sur l'historique des téléchargements. DB Browser for SQLite utilise les horodateurs de Google Chrome pour afficher les informations temporelles (également connu sous le nom de format Webkit, qui indique le nombre de microsecondes écoulées depuis 00:00:00 UTC le 7 janvier 1971). Utilisez l'outil DCode pour le convertir dans un format lisible. ChromeHistoryView est un programme Nirsoft qui révèle l'historique de Chrome. Cet utilitaire lit le fichier "History" du navigateur Google Chrome et peut être téléchargé depuis www.nirsoft.net/utils/chromehistoryview.html.



SQLite portable visual schema

Google chrome browser forensics

Lorsque vous utilisez l'internet, les cookies sont des fichiers texte qui contiennent de petites informations, telles qu'un nom d'utilisateur et un mot de passe, afin d'identifier votre ordinateur. Les cookies HTTP sont un type particulier de cookies utilisés pour identifier des utilisateurs spécifiques et améliorer la navigation sur le web. Le serveur crée des données dans un cookie dès que vous vous connectez. Un identifiant propre à vous et à votre ordinateur est utilisé pour identifier ces données. Votre ordinateur et le serveur du réseau échangent des cookies, et lorsqu'ils le font, le serveur lit l'ID et sait quelles données vous fournir exactement. Google Chrome enregistre les informations relatives aux cookies dans le fichier Cookies sous le profil de l'utilisateur de Chrome ; nous pouvons inspecter le contenu du fichier Cookies avec DB Browser for SQLite, tout comme nous l'avons fait avec le fichier Historique précédemment, pour obtenir des informations détaillées sur les cookies Chrome stockés, comme le montre la figure ci-dessous.



View saved cookies

PARTIE 4

Top sites et raccourcis

Ce fichier de base de données contient une liste des sites web les plus fréquentés par Google Chrome. Les informations sont enregistrées dans la base de données des vignettes, qui comporte deux tableaux : méta et vignettes. Cette base de données est chargée d'alimenter la fonction d'autocomplétion de Google Chrome lors de la saisie de raccourcis (par exemple, un mot-clé de recherche dans la barre d'adresse et les formulaires Web). Ce fichier comporte deux tables : Meta et Omni box shortcuts. Le texte de la saisie semi-automatique et les URL sont stockés dans le second tableau.

Données de connexion

Ce fichier de base de données comporte trois tables : login, meta et stats. Pour de nombreux sites en ligne, la base de données "login" stocke les noms d'utilisateur et les mots de passe (souvent cryptés), ainsi que d'autres informations associées. Tous les noms d'utilisateur et mots de passe (en texte clair) stockés par le navigateur Web Google Chrome peuvent être révélés à l'aide d'un outil portable de Nirsoft. Chromecast, tel qu'illustré à la figure8.9, peut être téléchargé à partir de www.nirsoft.net/utils/chromepass.html.

ChromePass reveals all passwords stored by Google Chrome

Web data

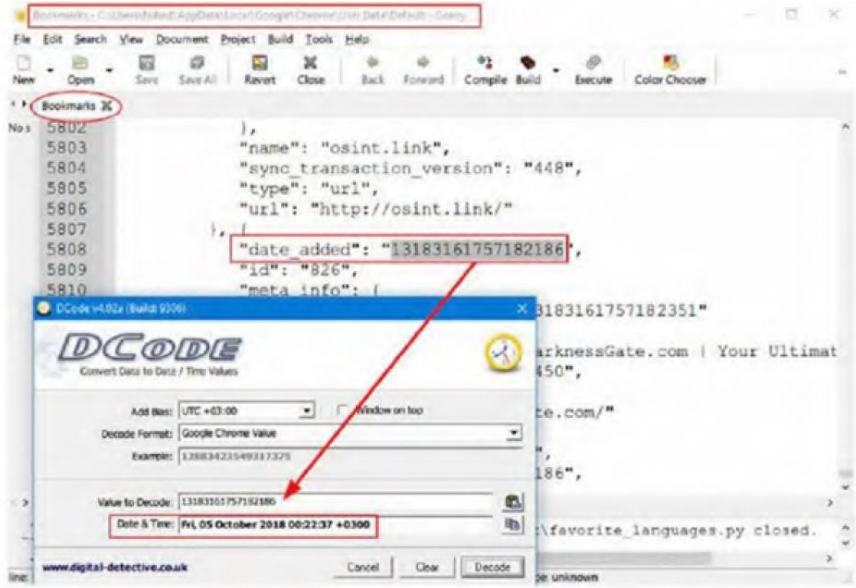
Cette fonction enregistre les identifiants de connexion des utilisateurs (sans les mots de passe, car Chrome a déplacé les mots de passe de connexion dans un fichier distinct appelé "Données de connexion" dans les versions plus récentes de Google Chrome) de sorte que la prochaine fois que l'utilisateur remplira un formulaire de connexion, recherchera des mots-clés, etc., Google Chrome proposera de compléter automatiquement les suggestions au fur et à mesure de la saisie.

Bookmarks

Un signet de navigateur (parfois appelé "favori") est une URL qu'un utilisateur enregistre pour y accéder ultérieurement. Dans Google Chrome, le fichier "Base de données des signets" stocke les signets actuels de l'utilisateur. Nous pouvons ouvrir ce fichier dans le Bloc-notes de Windows pour voir ce qu'il contient. Nous pouvons utiliser l'outil DCode pour transformer la valeur "date ajoutée" dans un format lisible afin de vérifier la date et l'heure auxquelles un signet spécifique a été ajouté à Chrome ; nous l'avons déjà fait à plusieurs reprises, comme le montre la figure suivante.

Bookmarks.bak

Ce fichier de base de données contient des sauvegardes récentes des signets de Chrome ; veuillez noter que ce fichier sera réécrit régulièrement à chaque lancement de Google Chrome. Ce fichier est important pour la police scientifique, car si un suspect supprime certains signets avant de fermer son navigateur Chrome, nous pouvons localiser le(s) signet(s) supprimé(s) dans ce fichier. Pour éviter d'écraser ce fichier, nous ne devons pas lancer Google Chrome tant que nous n'en avons pas sauvegardé une copie dans un endroit sûr.



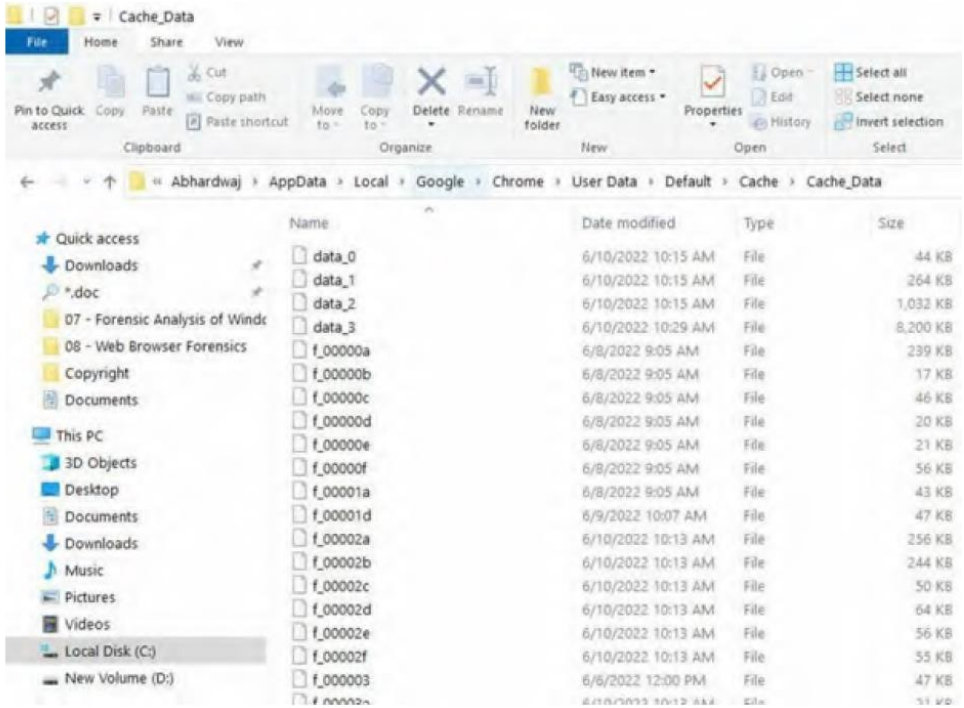
Analyzing Google Chrome “Bookmarks”

PARTIE 4

Dossier cache

Ce dossier stocke les contenus statiques fréquemment consultés, tels que les images et les parties de fichiers HTML, de sorte que la prochaine fois qu'un utilisateur visite le même site Web, le navigateur le charge plus rapidement parce que des parties du contenu sont chargées à partir d'un dossier de cache local plutôt que de le télécharger à partir du serveur d'origine du site Web. En utilisant ChromeCacheView de Nirsoft (www.nirsoft.net/utils/chromecacheview.html), nous pouvons automatiser la procédure d'extraction de la mémoire cache de Google Chrome. Ce programme examine le contenu du dossier cache du navigateur Google Chrome, comme le montre la figure ci-après, qui est situé dansUsers\UserName\AppData\Local\Google\Chrome\UserData\default\Cache.

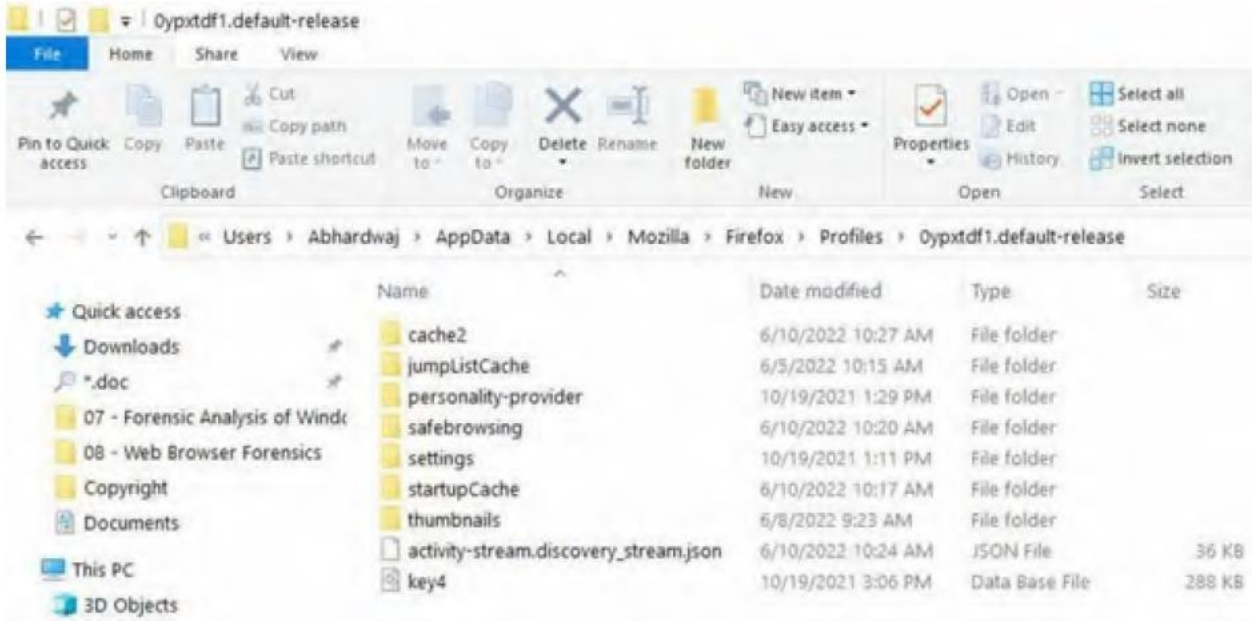
Comme nous l'avons vu, Google Chrome stocke un grand nombre d'informations personnelles sur son utilisateur. L'étude de tous ces artefacts peut aider les examinateurs à établir une chronologie complète des activités en ligne d'un utilisateur et à comprendre ses intentions ou ses intérêts en analysant son historique de navigation.



View Google Chrome cache contents

Mozilla Firefox Browser Forensics

Firefox est un navigateur Web gratuit et open-source créé par Mozilla, et c'est l'un des navigateurs les plus utilisés sur la planète. Firefox n'utilise pas le registre Windows comme le fait Internet Explorer ; au lieu de cela, Firefox conserve son historique Web, son historique de téléchargement et ses signets dans le fichier de base de donnéesplaces.sqlite. Ce fichier se trouve dans votre dossier de profil Firefox. En cliquant sur la touche Windows et en allant dans %APPDATA%\Mozilla\Firefox\Profils, comme illustré dans la figure ci-dessous, vous pouvez aller dans votre profil. Votre profil Firefox s'affiche comme un dossier dans les résultats de la recherche ; cliquez dessus pour y accéder. Vous pouvez également accéder au dossier du profil Firefox en appuyant sur la touche Windows + R, puis en tapant ce qui suit dans la fenêtre d'exécution : %APPDATA%. Cliquez sur OK → La fenêtre de l'explorateur Windows apparaît → Allez à Mozilla → Firefox → Profils



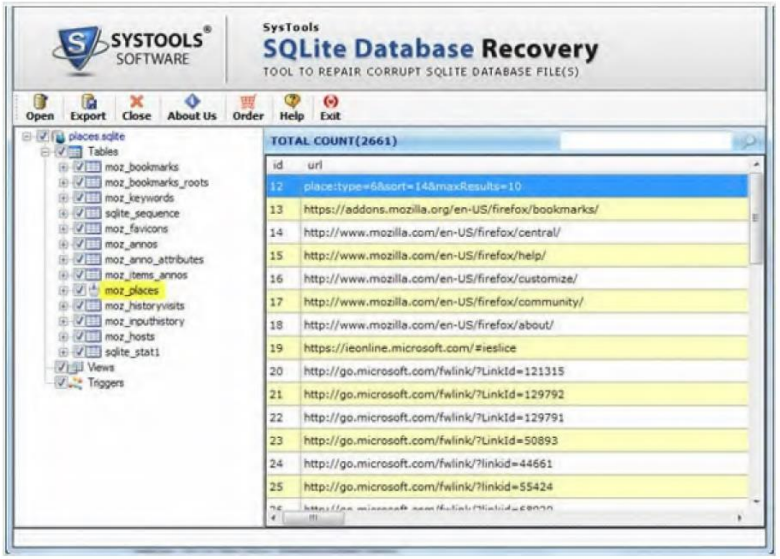
Firefox browser folders

PARTIE 4

Mozilla Firefox Browser Forensics

Pour réaliser des enquêtes de Firefox, nous pouvons obtenir des informations à partir du cache du navigateur Mozilla Firefox, situé dans le dossier de profil, plus précisément dans le dossier cache. Les informations du cache contiennent des informations sur les habitudes de navigation de l'utilisateur, les signets et d'autres informations pertinentes. Comme nous nous concentrons sur les enquêtes sur le navigateur Web Firefox, passons brièvement en revue quelques fichiers pertinents et présentons quelques outils pour nous aider à automatiser notre recherche.

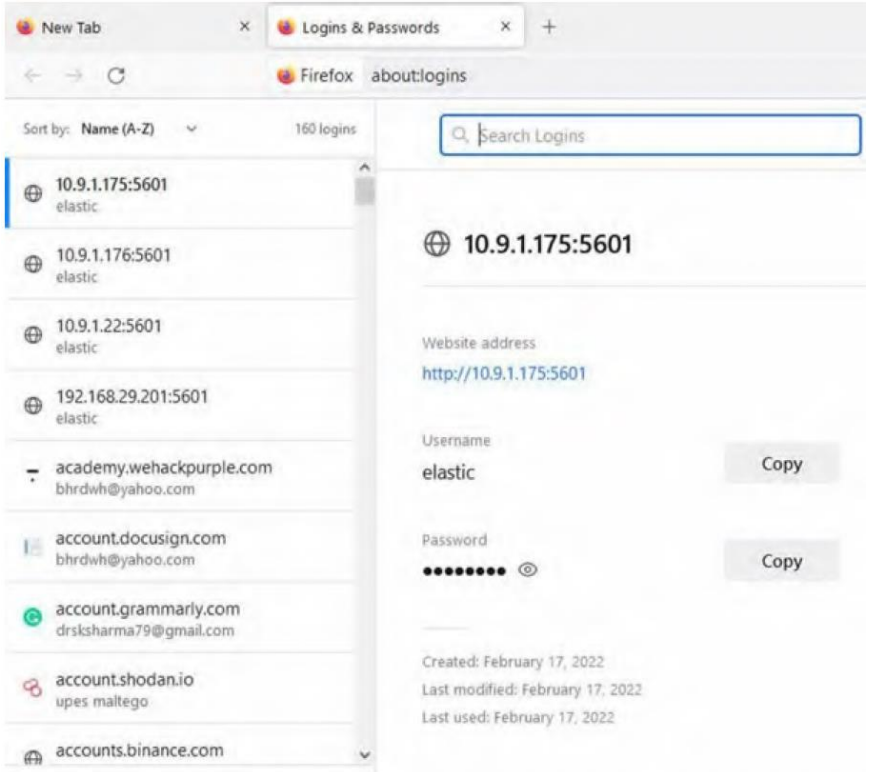
- Les signets, les sites Web visités et l'historique des téléchargements sont tous stockés dans le fichier places.sqlite. L'application DB Browser for SQLite peut être utilisée pour obtenir des informations à partir de la base de données places.sqlite. Nous pouvons utiliser cet outil pour afficher les tables cibles de la base de données SQLite et leur contenu, comme nous l'avons fait précédemment. Le fichier places.sqlite est utilisé par Firefox pour conserver l'intégralité de l'historique des sites visités dans un profil utilisateur. Comme le montre la figure ci-dessous, le fichier places.sqlite est un fichier de base de données SQLite qui peut être inspecté à l'aide de l'outil d'enquête sur les bases de données SQLite.



Place.Sqlite tables and contents

Mozilla Firefox Browser Forensics

- Cookies.sqlite : Stocke les cookies laissés par les sites Web visités précédemment (les cookies sont souvent utilisés pour enregistrer les noms d'utilisateur et les mots de passe de connexion des sites Web précédemment visités, ainsi que pour conserver les préférences des sites Web). Les outils suivants peuvent être utilisés pour récupérer des informations à partir du fichier de base de données cookies.sqlite :
    - MZCookiesView (www.nirsoft.net/utils/mzcv.html) : Affiche tous les cookies stockés dans un fichier de cookies Firefox ; vous pouvez également exporter les résultats dans un fichier texte, XML ou HTML.
    - DB Browser for SQLite.
- formhistory.sqlite : Stocke les mots-clés de recherche utilisés dans la barre de recherche Firefox, et vos recherches sont saisies dans les formulaires Web.
- Key4.db et logins.json : Firefox conserve vos mots de passe à cet emplacement (le fichier de base de données de clés était autrefois connu sous le nom de key3.db ; à partir de la version 58 de Firefox, le nom a été changé en Key4.db, mais le fichier logins.json, qui contient les mots de passe sous forme chiffrée, reste inchangé). Pour afficher tous les noms d'utilisateur et mots de passe conservés par Firefox, utilisez PasswordFox, qui peut être téléchargé depuis www.nirsoft.net/utils/passwordfox.html. Si vous exécutez cette application sur le système cible, elle vous montrera les mots de passe pour le profil Firefox actuel ; si vous souhaitez voir les mots de passe, consultez la figure suivante.



Firefox passwords

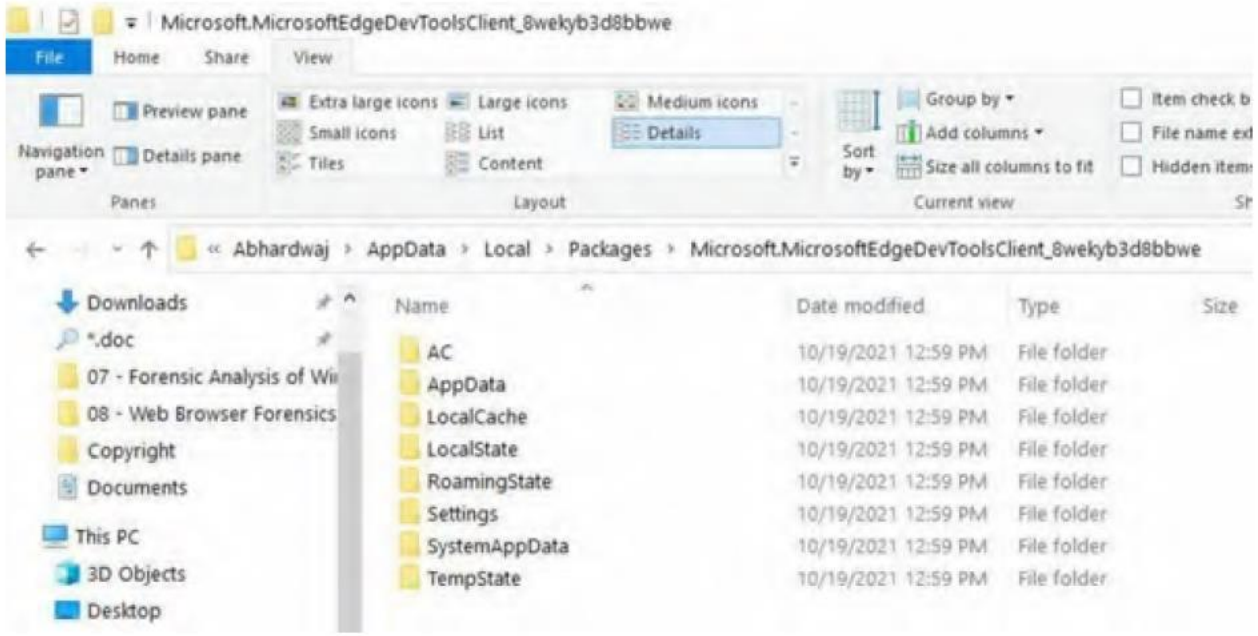
Mozilla Firefox Browser Forensics

- permissions.sqlite : Stocke les permissions Firefox pour des sites Web individuels. Par exemple, lorsque vous autorisez un site Web spécifique à afficher des pop-ups, Firefox enregistre cette permission dans ce fichier. Il en va de même lors de l'installation d'une extension à partir d'un site Web particulier.
- search.json.mozlz4 : Contient les moteurs de recherche installés par l'utilisateur.
- prefs.js : Stocke les préférences de Firefox.
- addons.json : Affiche les extensions installées sur Firefox.
- Extension-data [Dossier] : Contient les données générées par les extensions installées (add-ons).

Microsoft Edge browser forensics

Microsoft Edge (nom de code Spartan) est le nouveau navigateur par défaut [6] de Windows 10 qui remplace Internet Explorer. Il s'agit d'un navigateur Web léger qui interagit avec la fonction Cortana de Windows 10, permettant aux utilisateurs d'effectuer de nombreuses activités (telles que l'ouverture de pages Web et la réalisation de recherches en ligne) par simple commande vocale. On peut s'attendre à ce que de plus en plus de consommateurs utilisent Microsoft Edge au lieu d'IE à l'avenir ; il est donc essentiel de comprendre où ce navigateur enregistre ses données pour notre travail de criminalistique. Les paramètres de configuration du navigateur Edge sont stockés dans une base de données ESE, qui peut être trouvée via Utilisateurs. La Figure ci-après illustre :

Microsoft.MicrosoftEdgexxxx\AC\MicrosoftEdge\UserDefault\DataStore\



PARTIE 4

Microsoft Edge browser forensics

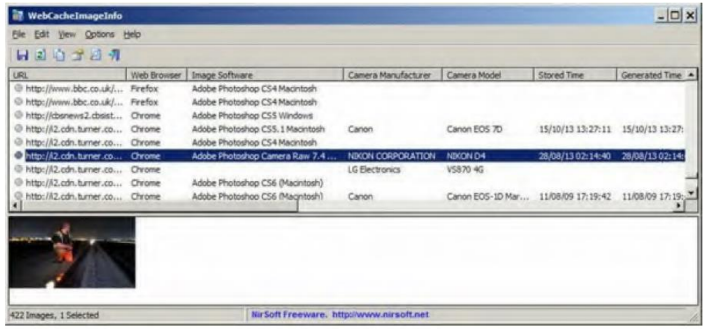
Les enquêteurs peuvent utiliser ESEDatabaseView de Nirsoft (www.nirsoft.net/utils/ese_databaseview.html) pour afficher les données de la base de données Spartan.edb.

- Le contenu du cache de Microsoft Edge est stocké dans le chemin suivant : \Utilisateurs <NomUtilisateur>\AppData\Local\Packages\Microsoft.MicrosoftEdge_*****\AC#!001\
- Microsoft Edge stocke son historique de navigation au même emplacement (dans le même fichier de base de données) où les versions 10 et 11 d'Internet Explorer stockent leurs données : \Utilisateurs <NomUtilisateur>\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- La dernière session de navigation de Microsoft Edge est stockée à l'emplacement suivant : \Utilisateurs <NomUtilisateur>\AppData\Local\Packages\Microsoft.MicrosoftEdge_****\AC\MicrosoftEdge\
- Une analyse approfondie des artefacts d'Edge peut révéler des informations forensiques précieuses. Comme nous l'avons déjà vu, les informations précieuses se trouvent dans les bases de données Edge nommées spartan.edb et WebCacheV01.dat, ainsi que dans divers emplacements à l'intérieur de son dossier principal, situé à : \Utilisateurs <NomUtilisateur>\AppData\Local\Packages\Microsoft.MicrosoftEdge_*****

Autres outils d'enquête sur les navigateurs Web

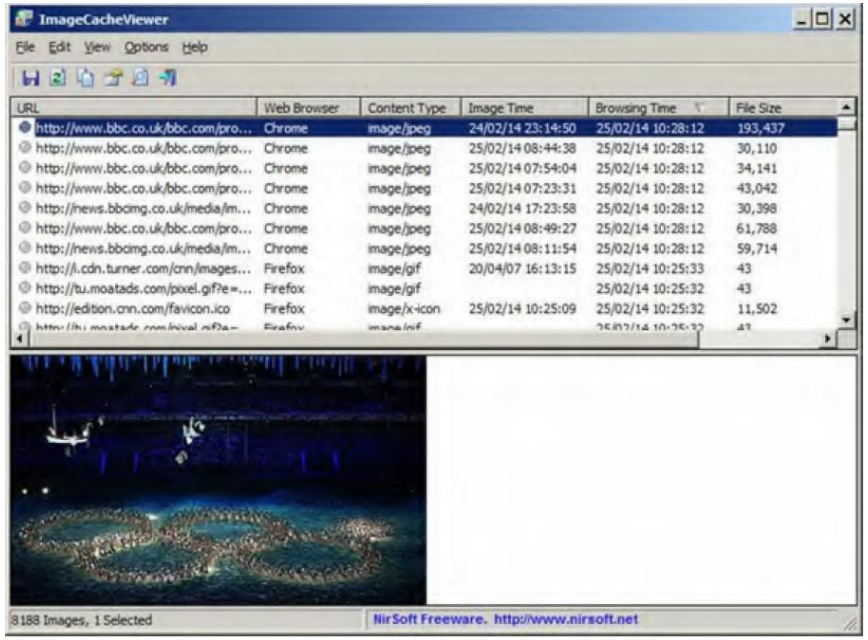
Il existe d'autres outils généraux pour enquêter sur les artefacts des navigateurs Web, principalement provenant de Nirsoft.

- WebCacheImageInfo peut trouver et répertorier toutes les images JPEG avec des métadonnées EXIF enregistrées dans les dossiers de cache d'Internet Explorer, Firefox et Google Chrome. Comme le montre la figure ci-dessous, les métadonnées EXIF contiennent des informations critiques sur les photos JPG, telles que le type d'appareil photo utilisé pour prendre la photo et la date et l'heure de production de l'image. Rendez-vous sur www.nirsoft.net/utils/web cache image info.html pour obtenir cet utilitaire.



WebCacheImageInfo

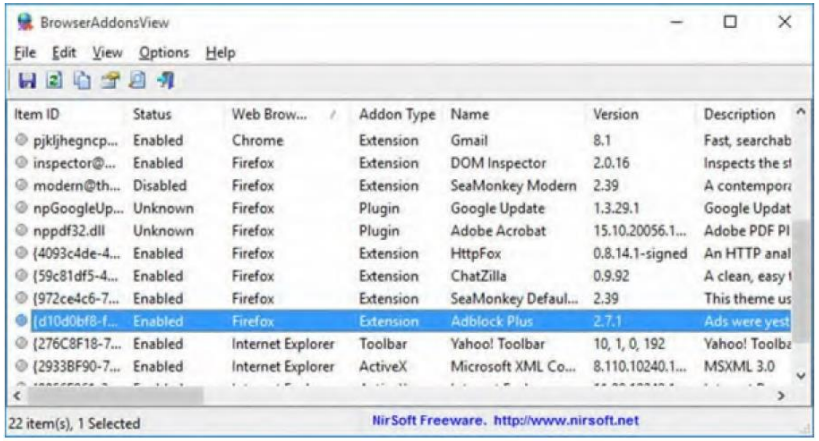
- ImageCacheViewer examine tous les principaux dossiers de cache des navigateurs (IE, Firefox et Google Chrome) et affiche toutes les images découvertes à l'intérieur, comme le montre la figure dans le slide suivante. Téléchargez cet outil depuis www.nirsoft.net/utils/image cache viewer.html.



ImageCacheViewer displays all cached images

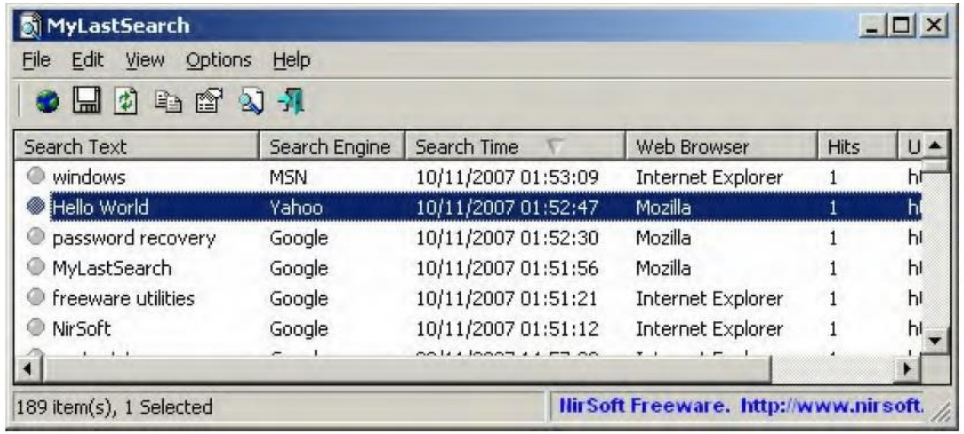
Autres outils d'enquête sur les navigateurs Web

- Toutes les extensions installées sur tous les principaux navigateurs Web sont affichées dans BrowserAddonsView (Chrome, Firefox et IE) . Si Firefox et Chrome ont plusieurs profils, l'outil peut afficher les extensions pour tous les profils, comme le montre la figure à coté. Cet outil peut être télécharger depuis www.nirsoft.net/utils/web_browser_addons_view.html.



BrowserAddonsView displays Web browser add-ons/plugins

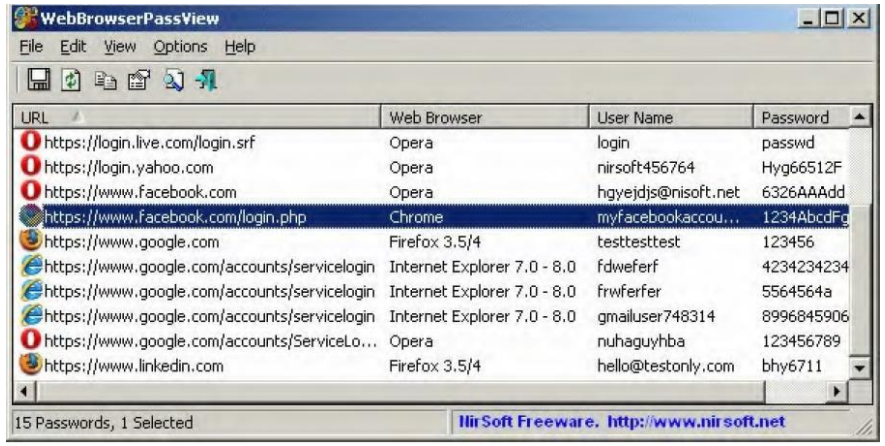
- Comme le montre la figure suivante, MyLastSearch vérifie l'historique en ligne dans tous les principaux navigateurs (Chrome, Firefox et Internet Explorer), ainsi que le dossier de cache, afin d'obtenir toutes les recherches effectuées précédemment. Cet outil est utile pour déterminer ce que recherche un suspect à un moment donné et quel moteur de recherche est utilisé. Il peut être obtenu depuis www.nirsoft.net/utils/my_last_search.html.



MyLastSearch displaying cache and history of Web browser

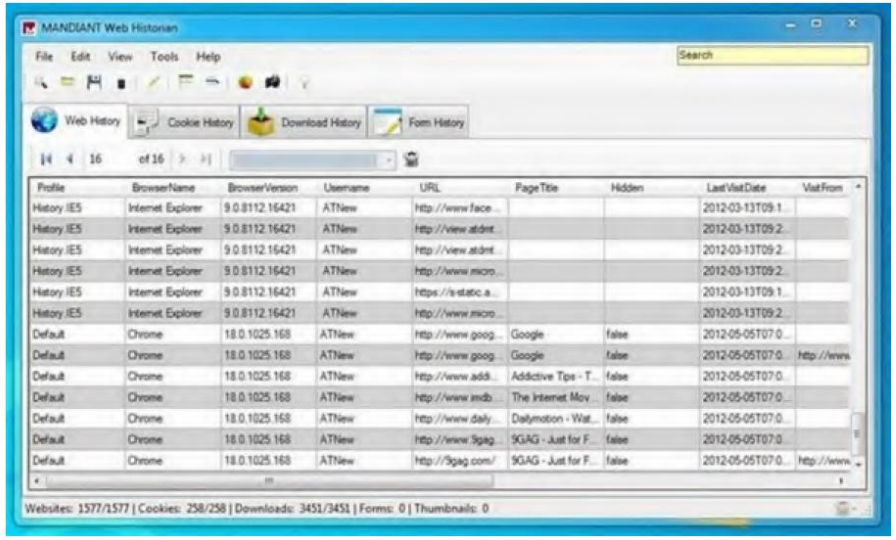
Autres outils d'enquête sur les navigateurs Web

- Comme le montre la figure suivante, WebBrowserPassView est une application de récupération de mots de passe qui affiche les mots de passe enregistrés dans Internet Explorer (versions 4.0 à 11.0), Mozilla Firefox (toutes les versions), Google Chrome, Safari et Opera. Cet outil peut être téléchargé depuis www.nirsoft.net/utils/web_browser_password.html.



MyLastSearch displaying

- Web Historian est un excellent outil d'extension pour le navigateur Google Chrome qui permet de visualiser l'historique de navigation Web. Il affiche des cercles graphiques représentant le nombre de jours où un site Web a été visité (en fonction de l'ordre chronologique de vos visites sur les sites Web) ainsi que les termes de recherche par mots-clés, comme le montre la figure suivante. Il affiche également les heures de navigation les plus actives de la journée et les jours de la semaine. Vous pouvez l'installer à partir de www.webhistorian.org.



Web Historian

PARTIE 4

Conclusion

Dans ce chapitre, nous avons discuté de la façon d'enquêter sur les navigateurs Web les plus utilisés, à savoir Google Chrome, Firefox et IE/Edge, pour trouver des artefacts forensiques. Notre approche dans ce chapitre était basée sur l'analyse manuelle, en plus de l'utilisation de quelques outils simples et gratuits pouvant aider les enquêteurs dans leur travail forensique sur les navigateurs Web. Dans le prochain chapitre, nous aborderons l'enquête sur les e-mails et les crimes liés aux e-mails.

OFPPT
La Voie de l'Avenir

WEBFORCE
BE THE CHANGE

PARTIE 5

Dans ce module, vous allez :

Ce que vous allez apprendre dans ce chapitre :

OFPPT
La Voie de l'Avenir

WEBFORCE
BE THE CHANGE

PARTIE 5

Ex : Modèle tableau Partie 1

Fichier	Table Début	Fin
A	0	3
B	4	6
C	7	12
D	13	29
E	18	35
F	30	38

	Serveur
Fonctionnalité	Les systèmes serveurs traitent les demandes des clients pour divers services.
Configuration	Les systèmes de serveurs ont une configuration plus complexe et sophistiquée.
Mode de Connexion	Ils prennent en charge la connexion simultanée de plusieurs utilisateurs.
Tâches exécutées	Les tâches complexes telles que l'analyse des données, le stockage et le traitement de grands ensembles de données ainsi que la satisfaction des demandes des clients sont courantes pour les systèmes de serveurs.
Power Off	L'arrêt des serveurs peut avoir de graves répercussions. Ils ne sont généralement jamais éteints.

Ex : Idée de SmartArt (Pour changer la forme, allez dans insertion, puis SmartArt)

Un langage de script (également appelé script) est une série de commandes qui peuvent être exécutées sans compilation.

Tous les langages de script sont des langages de programmation, mais tous les langages de programmation ne sont pas des langages de script.

Les langages de script utilisent un programme appelé interpréteur pour traduire les commandes.

Ex : Modèle Remarque Partie 1

Remarques

- Les chaînes sont écrites entre guillemets simples ou doubles.
- Les nombres sont écrits sans guillemets.

Ex : Modèle tableau Partie 2

Méthode	Description
length	C'est un entier qui indique la taille de la chaîne de caractères.
charAt()	Méthode qui permet d'accéder à un caractère isolé d'une chaîne.
substring(x,y)	Méthode qui renvoie un string partiel situé entre la position x et la position y-1.
toLowerCase()	Transforme toutes les lettres en minuscules.
toUpperCase()	Transforme toutes les lettres en Majuscules.

Ex : Idée SmartArt

Un serveur web

- Un serveur web sert à rendre accessibles des pages web sur internet via le protocole HTTP.
- Un serveur web répond par défaut sur le port 80.
- Pour qu'un site Web soit accessible à tout moment, le serveur Web sur lequel il est hébergé doit être connecté à Internet en permanence

Ex : Modèle Remarque Partie 2

Remarques

- Une méthode est une propriété dont la valeur est une fonction. Son rôle est de définir un comportement (action) pour l'objet
- On peut utiliser var au lieu de const

Ex : Modèle tableau Partie 3

Fonctionnalité	Syntaxe
Déplacer fichier1 dans le répertoire /tmp	mv fichier1 /tmp
Déplace le répertoire TEST dans le répertoire /tmp	mv TEST /tmp
Supprimer des fichiers	rm fichier1 fichier2
Supprimer un répertoire vide	rmdir rep

Ex : Idée SmartArt

Ex : Modèle Remarque Partie 3

Remarque

- Re-exécuter ce code en supprimant l'espace entre l'élément « div » et la balise « h1 »

Ex : Modèle tableau Partie 4

Sélecteur	Description
:disabled	Sélectionner les éléments désactivés
:invalid	Sélectionner les éléments don’t la valeur est invalide
:optional	Sélectionner les éléments d'entrée sans attribut "requis" spécifié
:required	Sélectionner les éléments d'entrée avec l'attribut "requis" spécifié
:valid	Sélectionner les éléments d'entrée avec des valeurs valides

Ex : Idée SmartArt

1

Écouteur d'événement (Event Listner) :

L'écouteur d'événement est un objet qui attend qu’un certain événement se produise (un clic, un mouvement de souris, etc.)

2

Gestionnaire d'événements :

le gestionnaire d'événements correspond généralement une fonction appelée suite à la production de l’événement.

Ex : Modèle Remarque Partie 4

Remarques

- Les événements **keydown** et **keypress** sont déclenchés avant toute modification apportée à la zone de texte.
- L'événement **keyup** se déclenche après que les modifications soient été apportées à la zone de texte.

Ex : Modèle tableau Partie 5

Propriété	Description
onreadystatechange	Définit une fonction à appeler lorsque la propriété **readyState** change
readyState	Contient le statut de XMLHttpRequest
responseText	Renvoie les données de réponse sous forme de chaîne
responseXML	Renvoie les données de réponse sous forme de données XML
status	Renvoie le numéro d'état d'une requête 200: "OK" 403: "Forbidden" 404: "Not Found"
statusText	Renvoie le texte d'état (par exemple "OK" ou "Not Found")

Ex : Idée SmartArt

Ex : Modèle Remarque Partie 5

Remarque

- Si aucun élément n'est trouvé par le sélecteur alors la requête Ajax ne sera pas envoyée

Couleurs de la Charte Graphique à utiliser par l'expert