FORENSICS

M2-SSI

2021 - 2022

LES APPROCHES

- Il existe 3 types d'analyses forensics distinctes :
  - L'analyse à froid (D*ead forensics*) : Elle consiste à analyser un système éteint. Dans ce cas l'ensemble des données du système sera copié et analysé ultérieurement. C'est l'approche la plus complète mais qui nécessite le plus de temps.
  - L'analyse à chaud (*le live forensics*) : Cette analyse consiste à analyser l'état d'un système à un moment T. Dans ce cas, l'enquêteur récupère des informations issues de la mémoire vive (RAM).
  - L'analyse en temps réel : Consiste à capturer et à analyser le trafic réseau.

DEAD FORENSICS VS LIVE FORENSICS

- L'analyse à froid et l'analyse à chaud sont complémentaires. L'analyse à froid consiste à analyser l'ensemble du système et de son contenu (logiciels installés, fichiers présents sur le disque, journaux de logs et d'événements, etc.) ce qui nécessite beaucoup de temps. L'analyse à chaud quant à elle consiste à récupérer l'état de fonctionnement d'un système en cours (fichiers ouverts, processus actifs, connexions réseau établies, etc.).

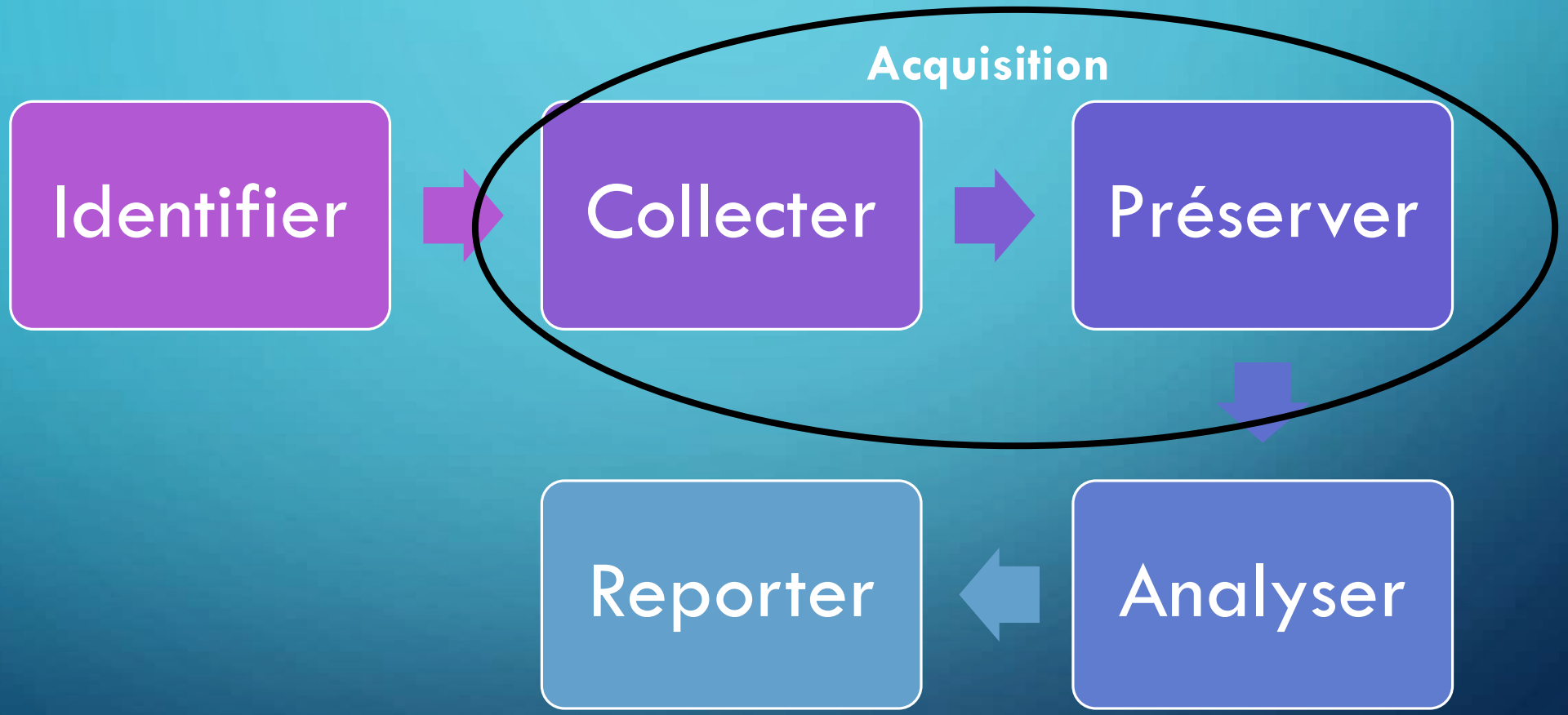
AVANTAGES DU DEAD FORENSICS

- L'analyse à froid (sur un système éteint) consiste à analyser l'ensemble d'un disque dur. Ces opérations prennent beaucoup de temps selon la capacité et le contenu du disque dur à analyser. L'analyse à froid permet de récupérer des informations concerant :
  - Les fichiers supprimés, l'espace libre du disque
  - L'analyse de l'ensemble du système : logiciels installés, ensemble des logs (navigation, fichiers consultés, logiciels, etc), utilisation quotidienne du système
  - Analyse du contenu du disque (fichiers multimédias, bureautiques, événements du système, fichiers exécutables, etc.)
  - La configuration et l'utilisation du système
  - Détection des informations confidentielles (fichiers protégés par mot de passe, conteneurs chiffrés, mots de passe enregistrés)
- L'analyse à froid permet d'aller beaucoup plus en profondeur lors d'une analyse car elle permet d'accéder à l'ensemble des données d'un disque.

AVANTAGES DU LIVE FORENSICS

- Le live forensics consiste à récupérer des informations sur l'état d'un système à un moment T. Cela permet d'étudier un système en cours de fonctionnement et de récupérer :
  - L'état du système (logiciels en cours de fonctionnement, fichiers ouverts/modifiés/utilisés, connexions réseau établies, etc.)
  - Les informations liées à un processus (mots de passe utilisés, sites consultés)
  - La récupération des mots de passe dans la mémoire
- L'avantage de l'analyse à chaud est que bien souvent les informations sont accessibles sans protection en mémoire et que le processus est beaucoup plus rapide que le dead analysis. Parmi les autres avantages du live forensics, nous avons :
  - Rapide
  - Accès physique à l'ordinateur
  - Peu de technique
  - Processus chargés au démarrage
  - Accès à la base de registre
  - Monitoring des actions effectuées (malwares)
  - Processus actifs, partages réseau, écriture sur le disque, fichiers ouverts, connexion réseau
  - Récupération d'informations confidentielles
  - Récupération des mots de passe actifs
  - **Cassage de containers truecrypt**
  - Analyse mémoire vive offline
- Cette analyse est par exemple très utilisée par les analyseurs de malware car elle permet de tracer toutes les actions effectuées par un processus actif.

PROCESSUS D'INVESTIGATION NUMÉRIQUE (FORENSICS)



PHASE 1 : IDENTIFIER

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

SCÈNE DE CRIME NUMÉRIQUE

- Une scène de crime numérique est défini comme :
- L'environnement électronique dans lequel les preuves numériques peuvent potentiellement exister

SCÈNE DE CRIME NUMÉRIQUE

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

- Avant de saisir un article, vérifiez si l'article est susceptibles de contenir des preuves;
- Assurez-vous que les détails de l'endroit où l'article a été trouvé ont été enregistrés, ce qui pourrait aider à hiérarchiser les éléments pour examen à un stade ultérieur;
- Différencier les téléphones mobiles trouvés sur un suspect (susceptible d'être utilisé actuellement) et les téléphones trouvés dans un tiroir (peut ne pas être utilisé actuellement), car ils doivent subir des analyses différentes;

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

- Les preuves peuvent être stockées en ligne, sur les systèmes d'un FAI ou sur les appareils des utilisateurs finaux. Dans certains cas il sera nécessaire d'obtenir certains détails du fournisseur de services pour obtenir ces preuves
- Si tel est le cas, il est préférable de saisir les objets en cours d'utilisation, c'est-à-dire les ordinateurs connectés à Internet.
- Considérez l'environnement comme une scène de crime et abordez-le en utilisant les procédures conventionnelles de scène de crime.
- Des précautions doivent être prises pour minimiser la perturbation de tout élément à proximité.
- "Les yeux d'abord et surtout, les mains après et le moins, et la langue pas du tout"

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

- **Quarantaine:** La première étape à établir est une mise en quarantaine autour de l'équipement suspect pour s'assurer que personne n'a la possibilité de le falsifier.
- Élimine la possibilité que des preuves soient «plantées» ou que l'utilisateur / propriétaire tente d'endommager toute preuve dont il a connaissance.
- **Statut d'enregistrement**: Une fois l'équipement mis en quarantaine, il doit être vérifié pour voir s'il est «allumé».
  - Son statut doit être enregistré aussi complètement que possible à l'aide de croquis, de photographies et de notes détaillées qui décrivent exactement ce qui peut être vu.
  - Il faut résister à la tentation d'utiliser sa propre connaissance des appareils numériques.

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

- Réseaux et communications: la machine est connectée à un appareil de communication tel qu'un port réseau ou un modem.
  - Le conseil général est de déconnecter le système des appareils de communication le plus rapidement possible, souvent avant la fin de l'enregistrement de l'état.
  - Cependant, cela présente certains risques:
    - Peut alerter le suspect et lui donner le temps de détruire les preuves de sa propre implication avant qu'il ne soit identifié.
    - Suppression possible des données.

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

- Alimentation: il est recommandé que tous les systèmes à saisir soient arrêtés dès que possible après leur découverte.
  - Nonobstant le potentiel d'endommagement des périphériques de stockage, il est encore beaucoup plus dangereux d'arrêter les systèmes «proprement» pendant la saisie :
    - L'arrêt du système d'exploitation est un processus logiciel, potentiellement composé de plusieurs programmes.
    - Le processus d'arrêt peut ne pas être le même sur toutes les machines, le processus logiciel d'arrêt peut être modifié à volonté par des utilisateurs avertis

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

- Alors, pourquoi ne pas appuyer sur le bouton de mise hors tension?
  - Dans les systèmes actuels, le bouton d'alimentation est en fait utilisé comme déclencheur pour le processus d'arrêt du système d'exploitation.
  - Appuyer dessus pendant 10 secondes peut tuer complètement le système
    - Que se passe-t-il pendant la période de 10 secondes ?
  - De loin la méthode préférée pour couper l'alimentation directement du système en le déconnectant du secteur. (même ce n'est pas simple comme cela peut paraître).

SCÈNE DE CRIME : PROBLÉMATIQUE DE LA SAISIE

- Éléments supplémentaires: pendant le processus d'acquisition de l'appareil lui-même:
  - Quelqu'un devrait prendre la responsabilité de rassembler les documents associés tels que les cahiers, les documents imprimés, etc.
  - La recherche de notes peut contenir des mots de passe ou d'autres éléments pertinents.
  - L'utilisateur ou le propriétaire doit également être interrogé sur les mots de passe et les systèmes de cryptage à ce moment.

PHASE 1 : IDENTIFIER

SCÈNE DE CRIME : QUE DOIT-ON SAISIR ?

LISTE DES ITEMS À SAISIR

- Unité centrale
- Moniteur, clavier et souris (nécessaires uniquement dans certains cas. En cas de doute, demandez conseil à un expert).
- Leads (encore une fois seulement nécessaire dans certains cas. En cas de doute, demandez l'avis d'un expert).
- Unités d'alimentation.
- Les disques durs externes.
- Dongles - Terme désignant un petit périphérique matériel externe qui se connecte à un ordinateur pour authentifier un logiciel
- Lecteurs externes et autres périphériques externes.

LISTE DES ITEMS À SAISIR

- Modems (certains contiennent des numéros de téléphone).
- Routeurs.
- Caméras digitales.
- Sauvegardez les bandes.
- Cartouches Jaz / Zip.
- CD, DVD.
- Cartes réseau sans fil, cartes PCMCIA.
- Clés USB, cartes mémoire et tous les appareils connectés USB / Firewire.

RECOMMANDATIONS ACPO (ASSOCIATION OF CHIEF POLICE OFFICERS OF ENGLAND)

- Étiquetez toujours les sacs contenant ces articles, pas les articles eux-mêmes.

- Identification attachée
- à l'article lui-même

Identification attachée

au dossier de preuve scellé

PHASE 1 : IDENTIFIER

IDENTIFICATION DES OBJETS

- Les objets ne sont pas toujours ce qu'ils semblent être et doivent être vérifiés de manière approfondie pour voir s'ils peuvent contenir des appareils numériques.

MODÉLISATION DE CAS

MODÉLISATION DE CAS

MODÉLISATION DE CAS

STOCKAGE MOBILE

EN PRATIQUE: MANDAT DE PERQUISITION POUR PREUVE RECEVABLE

- Un mandat de perquisition n'est délivré que si les forces de l'ordre fournissent une preuve suffisante qu'il existe une cause probable qu'un crime a été commis
- Le conseiller juridique doit préciser quels locaux, objets ou personnes seront fouillés
- Les éléments de preuve découverts lors de la perquisition peuvent être saisis

PROCÉDURE RELATIVE À LA CHAINE DE TRAÇABILITÉ

- Le traitement des preuves électroniques doit suivre les trois C de la preuve: soins (Care), Contrôle et Chaîne de traçabilité
- Procédures relatives à la chaîne de traçabilité
  - Tenir un journal des preuves qui montre quand les preuves ont été reçues et saisies, et où elles se trouvent
  - Enregistrer les dates si les articles sont mis à la disposition de quiconque
  - Restreindre l'accès aux preuves
  - Placez le disque dur d'origine dans un casier de preuves
  - Effectuer toutes les analyses sur une copie d'image miroir, jamais sur les données d'origine

FICHE ASSOCIÉE

Case Names			
Case Ref:			
Investigator's Name			
Date		Time	
Item Description:			

Chain of Custody Log				
	Actions	Date Time	Released By: Name	Received By: Name
1				
2				

PHASE 2

ACQUISITION = COLLECTE + PRESERVATION

COLLECTE DE PREUVES

- l'enquêteur doit décider
  - mode d'acquisition
    - Live
    - statique (Dead)
  - comment emballer et prendre des images du matériel collecté
- l'enquêteur doit documenter avec précision et minutie toutes les activités entreprises

LIVE ACQUISITION

- L’enquêteur ignore ce que l’attaquant a fait durant la phase de compromission
- l'enquêteur utilise généralement un ensemble d'outils fiables à partir d'un CD (KNOPPIX-STD, Helix)
- L’acquisition live utilise généralement des scripts pour automatiser le processus d'exécution d'une série d'outils et préserver leur sortie

LIVE ACQUISITION

- bien que généralement pensé dans le contexte d'un serveur en cours d'exécution, la besoin d'acquérir l'état d'un processus actif se fait ressentir au moins dans les deux situations SVT:
  - Logs
  - Equipements actifs tel que les tablettes et les smartphones
- « snapshot forensics » capture une image ponctuelle d’un processus

LIVE ACQUISITION

- L’emballage normalisé est essentiel pour protéger le périphérique sans fil de l'accès au réseau après la saisie et pendant l'analyse

ACQUISITION STATIQUE

- l'ordinateur est généralement éteint afin que ses disque durs puissent être retirés pour le clonage; l'information sur le disque est statique (Dead) et durable
- Bien que les processus et procédures d'acquisition statiques soient développés pour les disques informatiques, ils s'appliquent également aux périphériques de type disque (clés USB, cartes mémoire, lecteurs MP3, etc.)
- l'image forensic du disque ou du périphérique doit inclure les fichiers et répertoires actifs ainsi que les fichiers supprimés et les fragments de fichiers

COMPRENDRE LE FORMAT DE STOCKAGE POUR LES PREUVES NUMÉRIQUES

- Il existe trois formats
  - Format Raw
  - Format propriétaire
  - Advanced Forensics Format (AFF)

FORMAT RAW

- Permet d'écrire des données de flux binaire dans des fichiers
- Avantages
  - Transferts de données rapides
  - Peut ignorer les erreurs de lecture de données mineures sur le lecteur source
    - L'acquisition se poursuit malgré les erreurs
    - Remplit les secteurs manquants avec des zéros dans l'image
    - Hachage par parites
  - La plupart des outils de Forensics peuvent lire le format raw
- Désavantages
  - Nécessite autant de d'espace que le disque ou les données d'origine

FORMAT PROPRIÉTAIRE

- Fonctionnalités offertes
  - Option pour compresser ou ne pas compresser les fichiers image
  - Peut diviser une image en plus petits fichiers segmentés
  - Peut intégrer des métadonnées dans le fichier image
- Désavantages
  - Impossibilité de partager une image entre différents outils
  - Limitation de la taille des fichiers pour chaque volume segmenté

ADVANCED FORENSICS FORMAT

- Développé par le Dr Simson L. Garfinkel de Basis Technology Corporation
  - Fournir des fichiers image compressés ou non
  - Pas de restriction de taille pour les fichiers disque à image
  - réserve de l'espace dans le fichier image ou les fichiers segmentés pour les métadonnées
  - Open source pour plusieurs plates-formes et OS
  - Contrôles de cohérence interne pour l'auto-authentification
- Les extensions de fichier incluent .afd pour les fichiers image segmentés et .afm pour les métadonnées AFF

QUELLE EST LA MEILLEURE MÉTHODE D'ACQUISITION ?

- Quatre méthodes :
  - Bit-stream disk-to-image file
  - Bit-stream disk-to-disk
  - Logical disk-to-disk or disk-to-disk data
  - Sparse data copy of a file or folder

QUELLE EST LA MEILLEURE MÉTHODE D'ACQUISITION ?

- Bit-stream disk-to-image file
  - Méthode la plus courante
  - Peut faire plus d'une copie
  - Les copies sont des réplications bit à bit du lecteur d'origine
  - ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook, jj
- Bit-stream disk-to-disk
  - Lorsque la copie disque vers image n'est pas possible
  - Tenir compte de la configuration de la géométrie du disque
  - EnCase, SafeBack, SnapCopy, dd

QUELLE EST LA MEILLEURE MÉTHODE D'ACQUISITION ?

- Logical acquisition or sparse acquisition
  - Quand le temps est limité
  - L'acquisition logique ne capture que des fichiers spécifiques ayant un interêt particulier pour le cas
  - L'acquisition parcimonieuse recueille également des fragments de données non allouées (supprimées)
  - Pour les grands disques, les serveurs RAID

QUELLE EST LA MEILLEURE MÉTHODE D'ACQUISITION ?

- Lors de la réalisation d'une copie, tenez compte de :
  - Taille du disque source
    - La compression sans perte peut être utile
    - Utilisez des signatures numériques pour la vérification
  - Si vous pouvez conserver le disque

CLONER LE DISQUE DE PREUVE

- Capturez une image précise du système dès possible.
- Avant de créer une image d'une partie du disque, l'origine et la description (fournisseur, modèle et numéro de série) doivent être documentés sous forme écrite et photographique

LE PROCESSUS DE CLÔNAGE

- Le processus général de clônage est :
  - Calculer et enregistrer un hash cryptographique du média suspect
  - Faire une image bit-stream du médias suspecté
  - Calculer et enregistrer le hash de la cible
  - Comparez les hash pour vérifier qu'ils correspondent
  - Emballer le média cible pour le transport

AUTHENTIFIER LES PREUVES

- L'une des principales préoccupations est de pouvoir démontrer que la collection particulière de bits en cours de préparation est vraie et que c'est la copie exacte de l'original
- Une des techniques d'identification d'un élément numérique particulier (collection de bits) est d'utiliser un hash cryptographique
- Lorsque des preuves numériques sont collectées, leur valeur de hash est calculée et enregistrée
- À tout moment ultérieur, la valeur de hachage peut être recalculé pour montrer que l'élément n'a pas été modifié depuis sa collecte

EMBALLAGE POUR LA PROTECTION

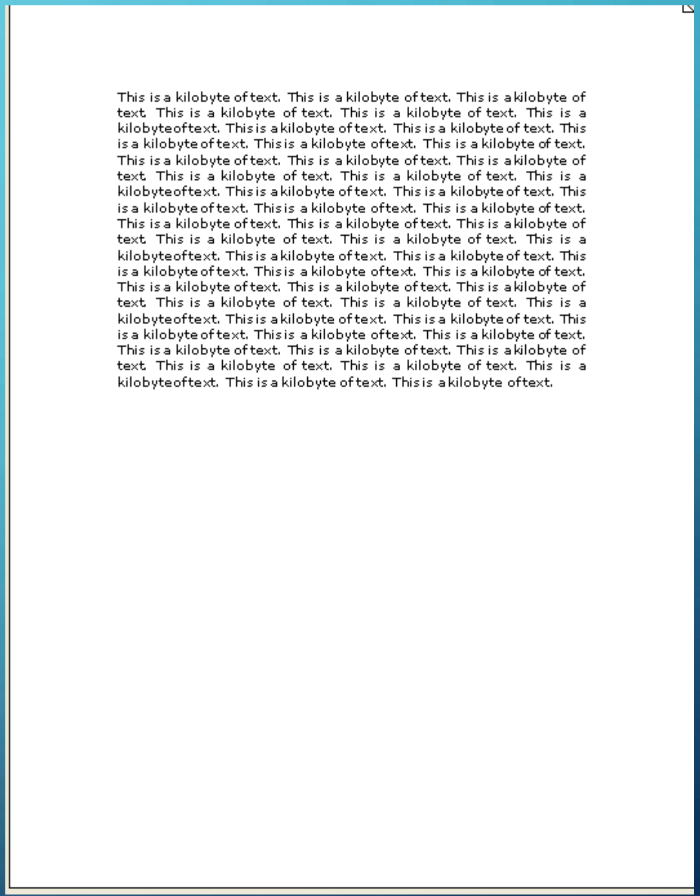
- Utilisation d'emballages spécialement conçus à cet effet facilite une documentation appropriée et le rangement
- L'enveloppe de preuve est pré imprimée avec un formulaire qui permet d'y inscrire les informations pertinentes tel que où, par qui et quand des informations ont été collectées
- Le sceau de preuve est conçu pour un usage unique et est très difficile à enlever sans le casser

PHASE 3

ANALYSE

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- Un octet = un caractère (A)
- Un kilo octet = 1000 charactères

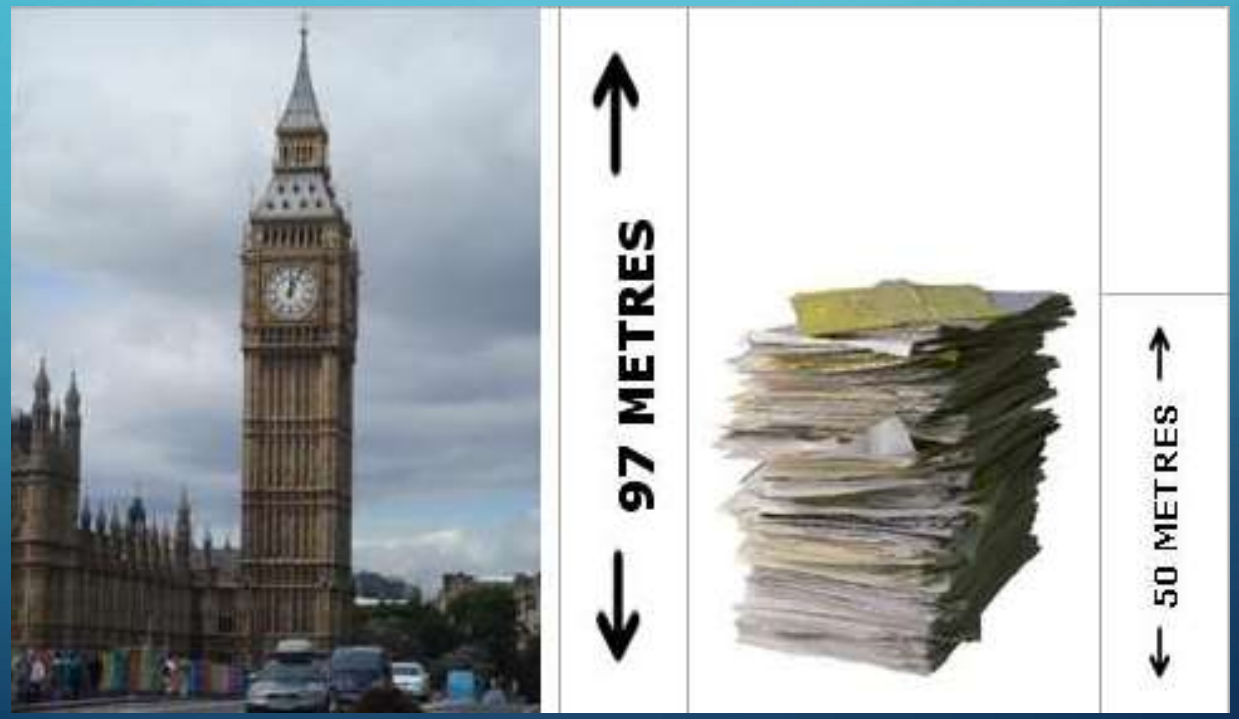

This is a kilobyte of text. This is a kilobyte of text.

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- 1 méga octet = 1 million de caractères ou 500 feuilles de papier

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- 1 giga octet = 1 milliard de caractères soit une pile de papier de 50 m de hauteur



POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- 400 giga octet c'est approximativement une pile de 20 KM de papier ou la moitié de la hauteur du mont Everest

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- Si nous utilisons l'un des disques durs disponibles dans le commerce aujourd'hui, c'est 2 téraoctets, soit 2 trillions de caractères et cela = 2 millions de paquets de papier A4 qui atteindraient ……

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- Une personne peut lire en moyenne et traiter environ 220 mots par minute, soit environ un kilo-octets de données.

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- Par conséquent, la lecture de deux téraoctets de données prendrait en moyenne pour un être humain :
  - 2 * 1000 * 1000 * 1000 minutes
  - Soit 33333333 heures
  - Soit 1388888 jours
  - Ou 3800 ans

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- L'âge du bronze nordique a commencé il y a 3800 ans

POURQUOI LA GESTION DES DONNÉES EST UN CHALLENGE ?

- Hitachi a lancé le premier disque dur de 4 To de classe entreprise en 2012.
- Cela fait 200 km de papier. Trois disques dur pourraient hébergés la totalité de la British Library

ANALYSE DE PREUVES

- La première étape consiste à obtenir des preuves de la zone de stockage et à effectuer une authentification physique
- Une copie des preuves est faite pour analyse et l'original est remis au stockage
- La copie peut ensuite être authentifiée en recalculant son hachage et en le comparant à l'enregistrement écrit
- Les images disque doivent être chargées dans l'outil forensics utilisé par l'organisation
- Implique généralement le traitement de l'image au format utilisé par l'outil et l'exécution d'un prétraitement (restauration de fichiers, gravure de données, etc.)

ANALYSE DE PREUVES

- Deux outils majeurs sont utilisés en analyse forensics :
  - EnCase (logiciel de guidage)
    - Fonctions du menu contextuel
    - Prend en charge les EnScripts
  - Boîte à outils forensics (données d'accès)
    - Prétraitement approfondi des éléments de preuve
    - Organise divers éléments dans un affichage à onglets
- Fonctionnalités largement similaires mais adoptent des approches différentes de la tâche d'analyse

PHASE 4

LE RAPPORT

RÉDACTION D'UN RAPPORT TECHNIQUE FORENSICS

- L'une des principales fonctions de l'analyste forensics est la diffusion du processus forensics au public visé.
- Une excellente enquête peut perdre toute son efficacité et tout son interêt si le rapport qui en résulte est médiocre.
- Un rapport désorganisé et mal rédigé peut en fait entraver tout le dossier

PRÉPARATION DU RAPPORT

- Les informations forensics ont une valeur limitée si elles ne sont pas collectées et rapportées sous une forme utilisable et présentées à ceux qui doivent appliquer les informations.
- Le principal objectif du processus est une manière standard de documenter:
  - pourquoi le système informatique a-t-il été revu?
  - comment les données informatiques ont-elles été revues? Et
  - à quelles conclusions est-il arrivé?

LES OBJECTIFS A ATTEINDRE

- Décrivez avec précision les détails d'un incident
- Être compréhensible pour les décideurs
- Être capable de résister à un d'examen juridique
- Soyez sans ambiguïté afin de ne pas permettre les mauvaises interprétations
- Être facilement référencé
- Contient toutes les informations nécessaires pour expliquer vos conclusions
- Offrir des conclusions, des opinions ou des recommandations valides si nécessaire
- Être créé en temps opportun

ETAPES DE PRÉPARATION D'UN RAPPORT TECHNIQUE

- 1. Collecte des données
- 2. Analyse des résultats
- 3. Présentation et organisation du rapport
- 4. Rédaction du draft
- 5. Révision du draft

ACQUISITION ET DUPLICATION DES DONNÉES

PLANIFICATION D'URGENCE POUR LES ACQUISITIONS D'IMAGES

- Créez une copie de votre fichier image de preuve
- Copiez également la zone hôte protégée du lecteur de disque
  - Pensez à utiliser un outil d'acquisition matériel pouvant accéder au disque au niveau du BIOS
- Soyez prêt à gérer les lecteurs chiffrés
  - Fonctionnalité de chiffrement du disque entier à partir des éditions Windows Vista Ultimate et Enterprise
  - Lecteurs auto-chiffrés éventuellement intégrés avec TPM (Trusted Platform Module)

UTILISER DES OUTILS D'ACQUISITION

- Outils d'acquisition pour Windows
  - ¤ Avantages
    - Facilitez l'acquisition de preuves à partir d'un lecteur suspect
      - Surtout lorsqu'il est utilisé avec des appareils remplaçables à chaud
  - ¤ Inconvénients
    - Doit protéger les données acquises avec un périphérique matériel de blocage en écriture bien testé
    - Les outils ne peuvent pas acquérir de données à partir de la zone protégée d'un disque

DANS LA PRATIQUE : BLOQUEUR D'ECRITURE ET PROTECTION

- Ne mettez jamais un PC sous tension sans disposer d'un logiciel ou de périphériques bloquant l'écriture
- Les dispositifs de blocage d'écriture empêchent toute écriture sur un lecteur, comme cela peut se produire lors de la simple mise sous tension d'un système

PROTECTION EN ÉCRITURE DE WINDOWS XP AVEC DES PÉRIPHÉRIQUES USB

- Fonction de protection en écriture logiciel sur l'USB
  - Bloque toute écriture sur les périphériques USB
- Le lecteur cible doit être connecté à un contrôleur PATA (IDE), SATA ou SCSI interne
- Étapes de mise à jour du registre pour Windows XP SP2
  - Sauvegarder le registre
  - Modifier le registre avec la fonction de protection en écriture
  - Créez deux icônes de bureau pour automatiser la commutation entre l'activation et la désactivation des écritures sur le périphérique USB

ACQUISITION DE DONNÉES AVEC UN CD BOOT LINUX

- Linux peut accéder à un lecteur qui n'est pas monté
  - Accès RAW «brut» sous le système de fichiers
- Les systèmes d'exploitation Windows et Linux plus récents montent et accèdent automatiquement à un lecteur
  - Peut être désactivé sous Linux (la plupart des distributions «forensic» le font automatiquement)
- Forensic Linux Live CD n'accède pas automatiquement aux médias
  - Ce qui réduit le besoin d'un bloqueur d'écriture
- Utilisation des distributions Linux Live CD
  - Forensic Linux Live CD
    - Contient des utilitaires supplémentaires

UTILISATION D'UN CD LINUX BOOTABLE

- Large choix d'outils
- Montage sur un seul CD / DVD bootable
- Certains sont basés sur Klaus Knopper de Knoppix
- Backtrack, Kali Linux
- Penguin Sleuth

ACQUISITION DE DONNÉES AVEC LINUX BOOT CD

- Préparation d'un lecteur cible pour l'acquisition sous Linux
  - La commande fdisk répertorie, crée, supprime et vérifie les partitions sous Linux
  - mke2fs crée un système de fichiers EXT2
- Acquérir des données avec dd sous Linux
  - Commande dd («data dump», «ditto disk», «copy & convert»)
    - Peut lire et écrire à partir d'un périphérique multimédia et d'un fichier de données
    - Crée un fichier au format RAW « brut » que la plupart des outils d'analyse judiciaire informatique peuvent lire

MONTER LA CIBLE

- Nous allons créer une image du disque suspect (sdc) vers un fichier sur le disque cible (sdb)
- Pour écrire dans un fichier, nous devons monter un système de fichiers
  - Soyez très, très sûr d'avoir correctement identifié le lecteur cible. Le montage d'un système de fichiers modifie généralement les données

MONTER UN SYSTÈME DE FICHIER

- Nous créons d'abord un point de montage (/ mnt / target) - le disque sera accessible via ce répertoire
- Nous montons ensuite la partition sur le point de montage

CLONAGE (CRÉATION D'UNE IMAGE)

- Créez un hash pour le périphérique suspect
  - sha256sum
- Créer une image
  - dd –if = <périphérique suspect> of = <chemin de l'image> bs = <Taille du bloc>
- Créez un hash pour l'image

COMMANDE DD : PARAMÈTRE BS

- Le paramètre bs détermine la taille des blocs lus et écrits
- En général, les blocs plus grands sont plus efficaces (16 à 64 Ko)
- Exemple, la création d'image d'un fichier de 20 Go avec un bs de 16 Ko a nécessité 1 426 secondes
- L'augmentation du bs à 32768 a réduit le temps à 1270 secondes

NOM DE PÉRIPHÉRIQUES DANS LINUX

- Linux n'utilise pas de lettres de lecteur
- / dev est le répertoire des fichiers de périphérique
  - Les périphériques sont des fichiers
- / dev / hda est le premier lecteur IDE
- / dev / sda est le premier lecteur SCSI
  - Les périphériques USB / Firewire apparaissent comme SCSI
- / dev / sda1 serait la première partition du premier périphérique SCSI
  - Les partitions primaires sont numérotées de 1 à 4; Les partitions logiques sont numérotées à partir de 5

ACQUISITION DE DONNÉES AVEC UN BOOT CD LINUX

- Acquérir des données avec dd sous Linux
  - Les lacunes de la commande dd
    - Nécessite des compétences en ligne de commande
    - Ne compresse pas les données
  - Commande dd combinée à la commande Split
    - Segmente la sortie en volumes séparés

ACQUISITION DE DONNÉES AVEC UN BOOT CD LINUX

- Acquisition de données avec dcfldd sous Linux
  - Fonctions supplémentaires dcfldd
    - Spécifiez des modèles hexadécimaux ou du texte pour libérer de l'espace disque
    - Consignez les erreurs dans un fichier de sortie pour analyse et examen
    - Utilisez plusieurs options de hachage
    - Reportez-vous à un affichage d'état indiquant la progression de l'acquisition en octets
    - Divisez les acquisitions de données en volumes segmentés avec des extensions numériques
    - Vérifiez les données acquises avec les données originales du disque ou du support

ACQUISITION D'UNE IMAGE AVEC ACCESS DATA FTK IMAGER

- Affiche les disques de preuves et les fichiers disque-à-image
- Effectue des copies disque à image des disques de preuves
  - Au niveau de la partition logique et du disque physique
  - Peut segmenter le fichier image
- Le lecteur de preuves doit avoir un périphérique de blocage en écriture matériel
  - Ou la fonctionalité de registre de protection en écriture USB activée
- FTK Imager ne peut pas faire l'acquisition de manière native de la zone protégée du lecteur

ACQUISITION D'UNE IMAGE AVEC ACCESS DATA FTK IMAGER

- Étapes
- Démarrer sous Windows
- Connecter le disque de preuves à un bloqueur d'écriture
- Connecter le disque cible au bloqueur d'écriture
- Démarrer l'imageur FTK
- Créer une image disque
  - Utiliser l'option Disque physique

VALIDER LES ACQUISITIONS DE DONNÉES

- Aspect le plus critique de la criminalistique (forensics) informatique
- Nécessite l'utilisation d'un utilitaire d'algorithme de hachage
- Techniques de validation
  - MD5 et SHA-1 à SHA-512

MÉTHODE DE VALIDATION LINUX

- Validation des données acquises par dd
  - Vous pouvez utiliser les utilitaires md5sum ou sha1sum
  - Les utilitaires md5sum ou sha1sum doivent être exécutés sur tous les disques et volumes suspects ou volumes segmentés
- Validation des données acquises par dcfldd
  - Utiliser l'option hash pour désigner un algorithme de hachage md5, sha1, sha256, sha384 ou sha512
  - l'option hashlog renvoie les résultats de hachage dans un fichier texte qui peut être stocké avec les fichiers image
  - L'option vf (vérifier le fichier) compare le fichier image au support d'origine

MÉTHODE DE VALIDATION WINDOWS

- Windows n'a pas d'outils d'algorithme de hachage intégrés pour la criminalistique informatique
  - Des utilitaires tiers peuvent être utilisés
- Les programmes de criminalistique informatique du commerce ont également des fonctionnalités de validation intégrées
  - Chaque programme a sa propre technique de validation
- Les fichiers image au format RAW brut ne contiennent pas de métadonnées
  - Une validation manuelle séparée est recommandée pour toutes les acquisitions brutes

CLONAGE DES DISQUES RAID

- Préoccupations
  - Combien de stockage de données est nécessaire?
  - Quel type de RAID est utilisé?
  - Avez-vous le bon outil d'acquisition?
  - L'outil peut-il lire une image RAID copiée de manière légale?
  - L'outil peut-il lire les sauvegardes de données fractionnées de chaque disque RAID?

CLONAGE DES DISQUES RAID

- Fournisseurs proposant des fonctions d'acquisition RAID
  - Technologies Pathways ProDécouvrir
  - Logiciel de guidage EnCase
  - X-Ways Forensics
  - Runtime software
  - Technologies R-Tools
- Parfois, un système RAID est trop volumineux pour une acquisition statique
  - Récupérer uniquement les données pertinentes pour l'enquête avec la méthode d'acquisition parcimonieuse ou logique

UTILISATION DES OUTILS D'ACQUISITION DE RÉSEAU À DISTANCE

- Vous pouvez vous connecter à distance à un ordinateur suspect via une connexion réseau et en copier les données
- Les outils d'acquisition à distance varient en termes de configurations et de capacités
- Désavantages
  - Les vitesses de transfert de données du LAN et les conflits de table de routage peuvent causer des problèmes
  - Obtenir les autorisations nécessaires pour accéder à des sous-réseaux plus sécurisés
  - Un trafic intense peut entraîner des retards et des erreurs

ACQUISITION DISTANTE AVEC ENCASE ENTREPRISE

- Fonctions d'acquisition à distance
  - Acquisition de données à distance des médias d'un ordinateur et des données RAM
  - Intégration avec les outils du système de détection d'intrusion (IDS)
  - Options pour créer une image des données d'un ou plusieurs systèmes
  - Une large gamme de formats de système de fichiers
  - Prise en charge RAID pour le matériel et les logiciels

SYSTÈME DE FICHIER ET DISQUE DUR

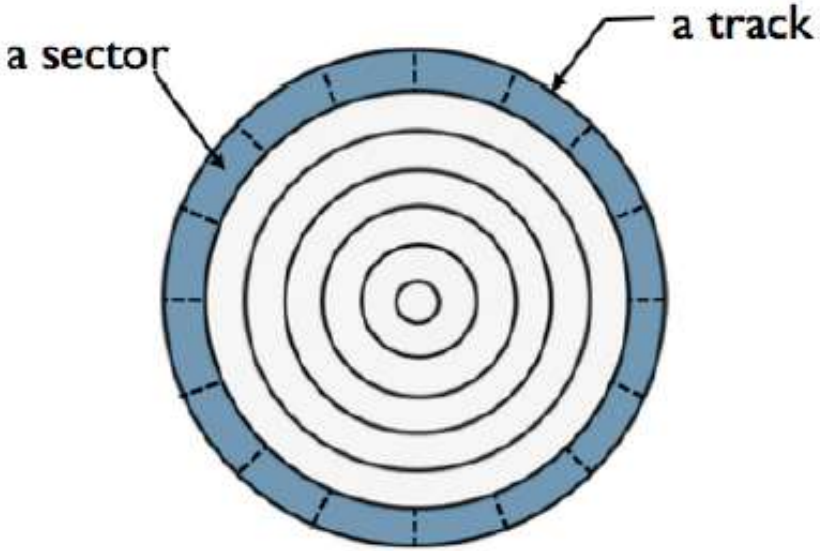
PRÉSENTATION DU LECTEUR DE DISQUE

- Il existe deux types de lecteurs de disque :
  - Disques de stockage fixes
  - Disques de stockage externes
- Peu de lecteurs de stockage amovibles sont :
  - Disquettes
  - Disques compacts
  - Disque numérique polyvalent (DVD)
  - disques ZIP

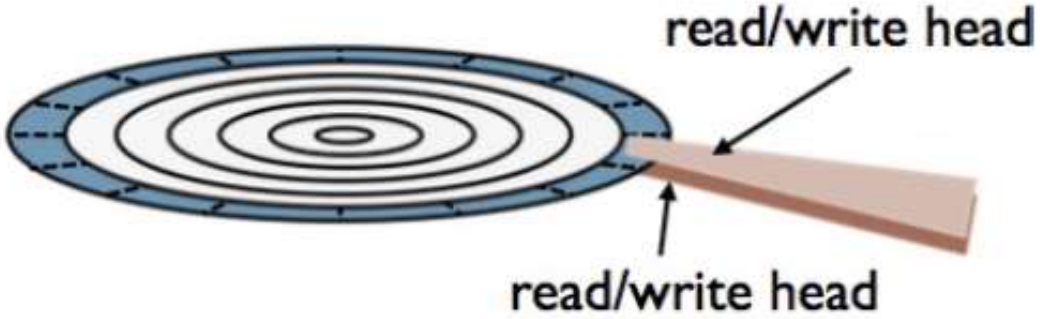
PRÉSENTATION DU LECTEUR DE DISQUE

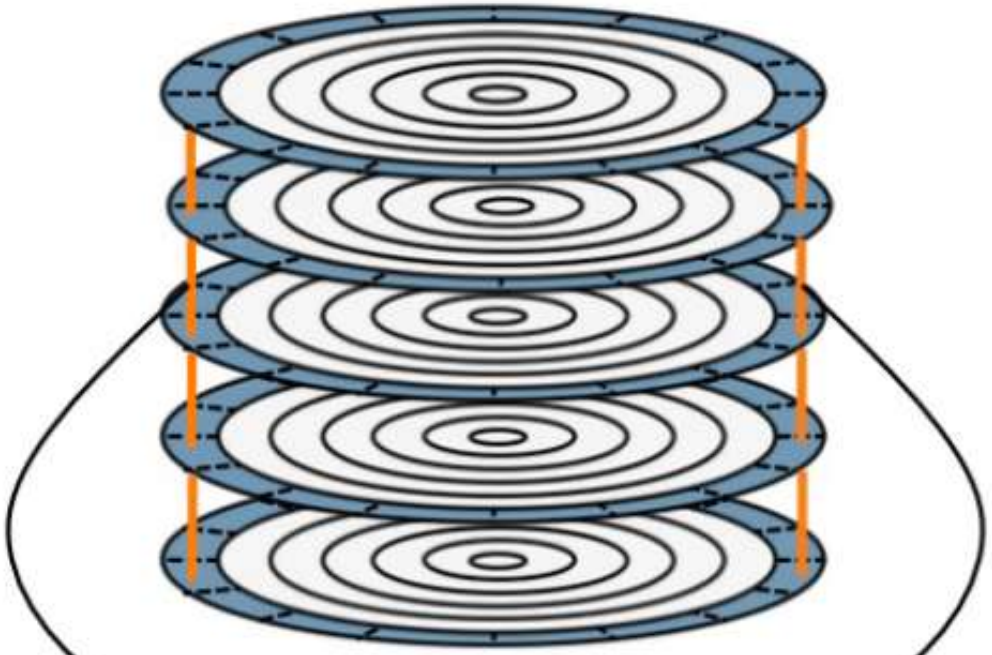
- Les lecteurs de disque conventionnels sont constitués d'un de plusieurs plateaux recouverts de matériau magnétique
- Géométrie du lecteur de disque
  - Tête
  - Pistes
  - Cylindres
  - Secteurs

PRÉSENTATION DU LECTEUR DE DISQUE



one side of a platter





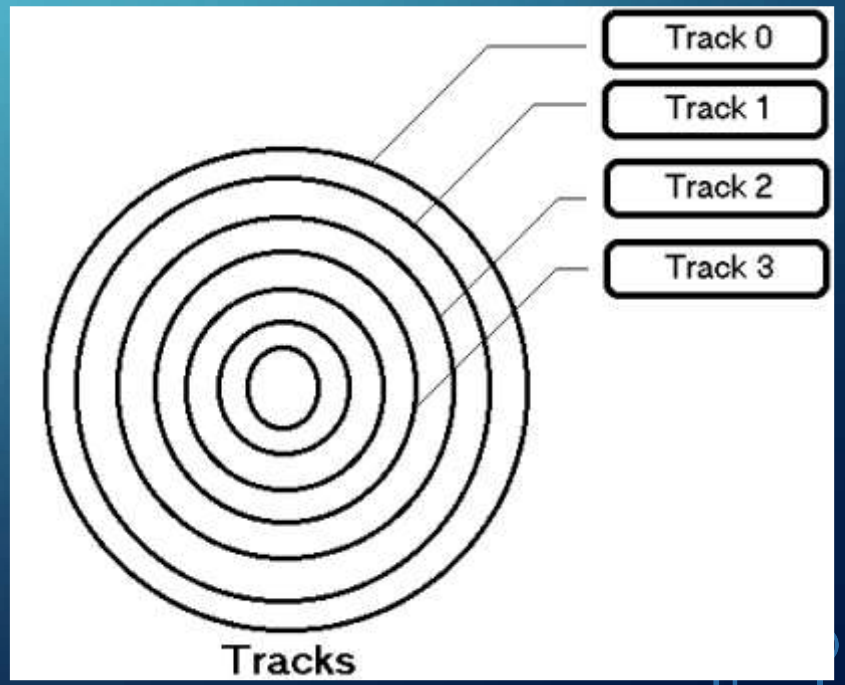
a cylinder
(collection of same tracks)

PLATEAU DE DISQUE

- Un alliage d'aluminium est utilisé pour fabriquer un plateau de disque
- Le verre et la céramique sont utilisés pour les plateaux modernes
- Les données sont écrites des deux côtés d'un plateau de disque dur
- La numérotation se fait des deux côtés

LES PISTES

- Un anneau circulaire sur un côté du plateau
- La tête de lecture peut accéder à cet anneau circulaire dans une position à la fois
- Les pistes sont numérotées pour leur identification, en commençant par 0 au bord extérieur
- Un cylindre se forme lorsque les pistes sont alignées



SECTEUR

- C’est la plus petite unité de stockage physique sur le disque
- Normalement 512 octets de taille
- Les données sont stockées sur le disque en séries contiguës
- Par exemple, si la taille du fichier est de 600 octets, deux secteurs de 512 octets sont alloués au fichier

ADRESSAGE CHS

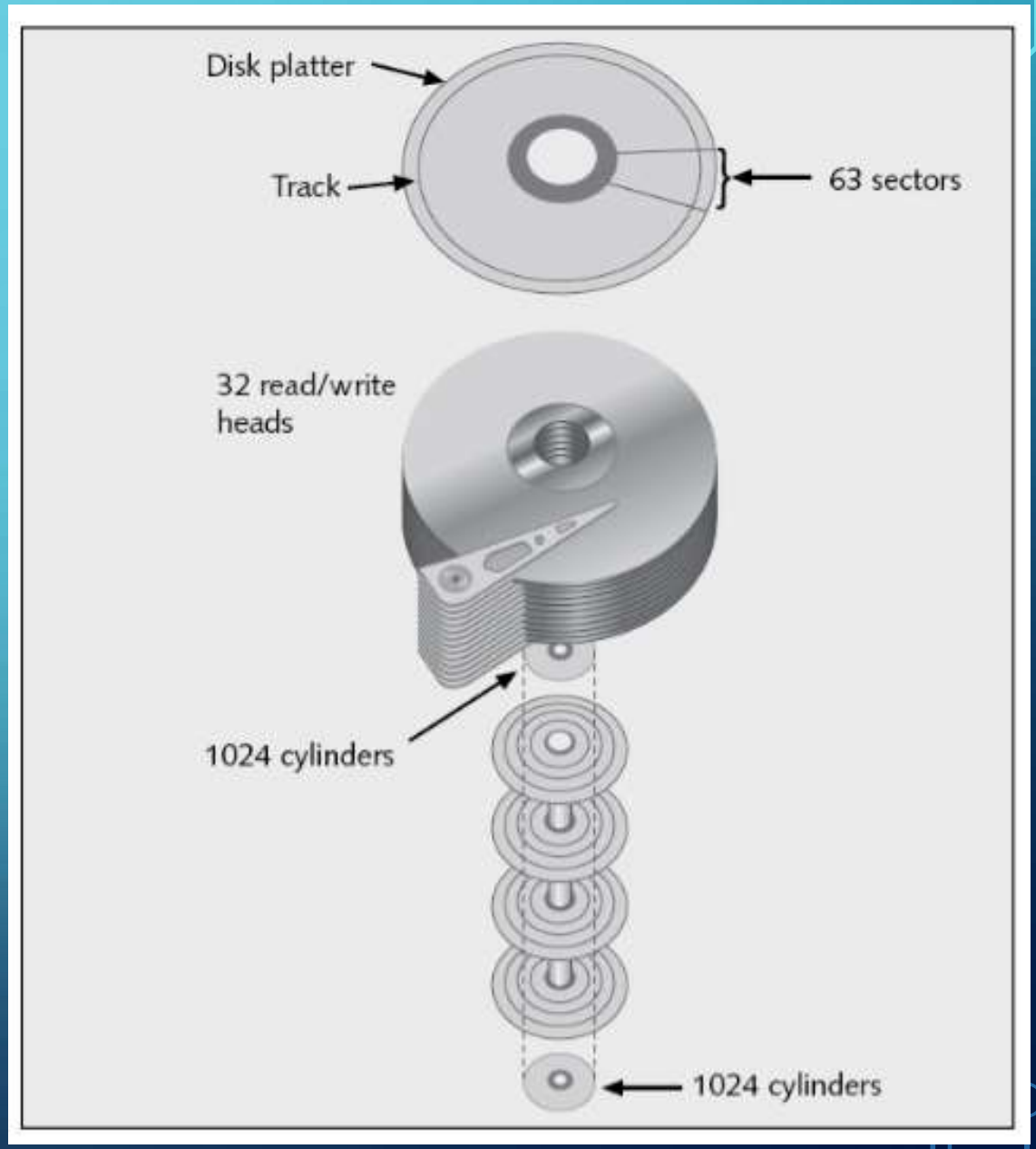
- CHS: Cylindre (Cylinder) – Tête (Head) – Secteur (Sector)
- Adressage CHS: méthode qui fait référence à un secteur du disque
  - La structure physique est généralement très compliquée
  - Un matériel spécial sur le lecteur (contrôleurs de disque) prend en charge le mappage des valeurs CHS à l'emplacement physique
- C’est le seul mode d'adressage possible dans les anciens systèmes

TAILLE DU DISQUE À PARTIR DE CHS

- C = Nombre de cylindres = 1024
- H = Nombre de têtes = 32
- S = Nombre de secteurs par piste = 63
- Nbr total de secteurs = C*H*S

  = 2.064.384
- Taille d'un secteur = 512 octets
- Taille du disque = 2.064.384 * 512

  = 1.056 GO



ADRESSAGE LOGIQUE DE BLOCS (LBA)

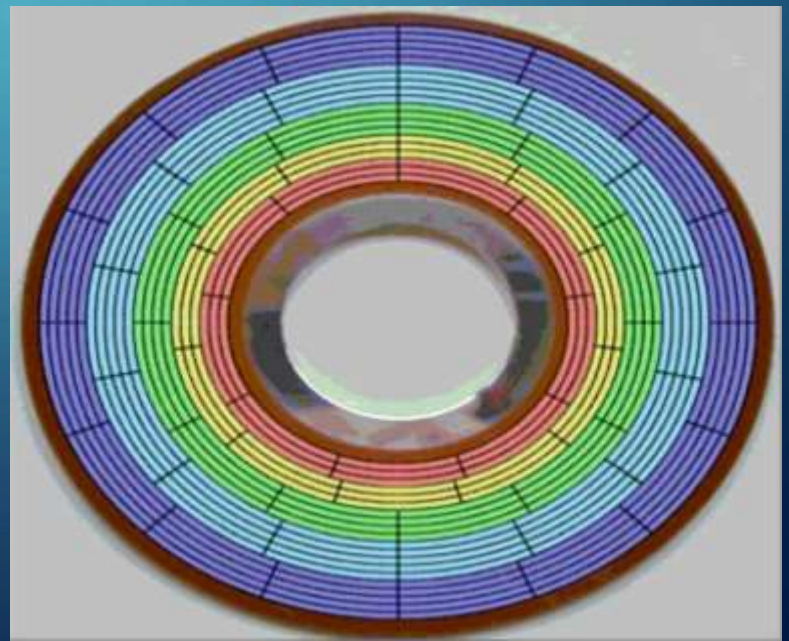
- Alternative à l'utilisation des valeurs C, H et S pour faire référence à un secteur
- Les blocs (généralement des secteurs de 512 octets) sont numérotés de 0 à max LBA
  - C = 0, H = 0, S = 1 est LBA 0
  - C = 0, H = 0, S = 2 est LBA 1
  - C = 0, H = 2, S = 1 est LBA 126 (basé sur la diapositive précédente)
- La fonction d'appel d'interruption BIOS (INT 0x13) 0x08 renvoie les paramètres du lecteur
  - Cylindres totaux, têtes totales, secteurs totaux par piste, secteurs totaux

SECTEURS EXÉDENTAIRES

- Certains systèmes plus anciens nécessitent d'aligner une limite de partition sur un cylindre; qui peut ne pas prendre en considération certains secteurs
  - Bon pour cacher les données

ENREGISTREMENT DE BITS ZONÉ

- Les données sont enregistrées sur le disque dur à l'aide de l'enregistrement de bits zoné
- C'est une méthode d'optimisation physique de l'utilisation d'un disque dur en plaçant plus de secteurs dans les pistes extérieures que dans les pistes intérieures
- Il s'agit de regrouper les pistes par zones
- Exemple :
  - Disque dur avec 20 pistes, 5 zones, dont chacune est représentée avec une couleur différente
  - Zone bleue: 5 pistes, chacune avec 16 secteurs
  - Zone cyan: 5 pistes, chacune avec 14 secteurs
  - Zone verte: 4 pistes, chacune avec 12 secteurs
  - Zone jaune: 3 pistes, chacune avec 11 secteurs
  - Zone rouge: 3 pistes, chacune avec 9 secteurs



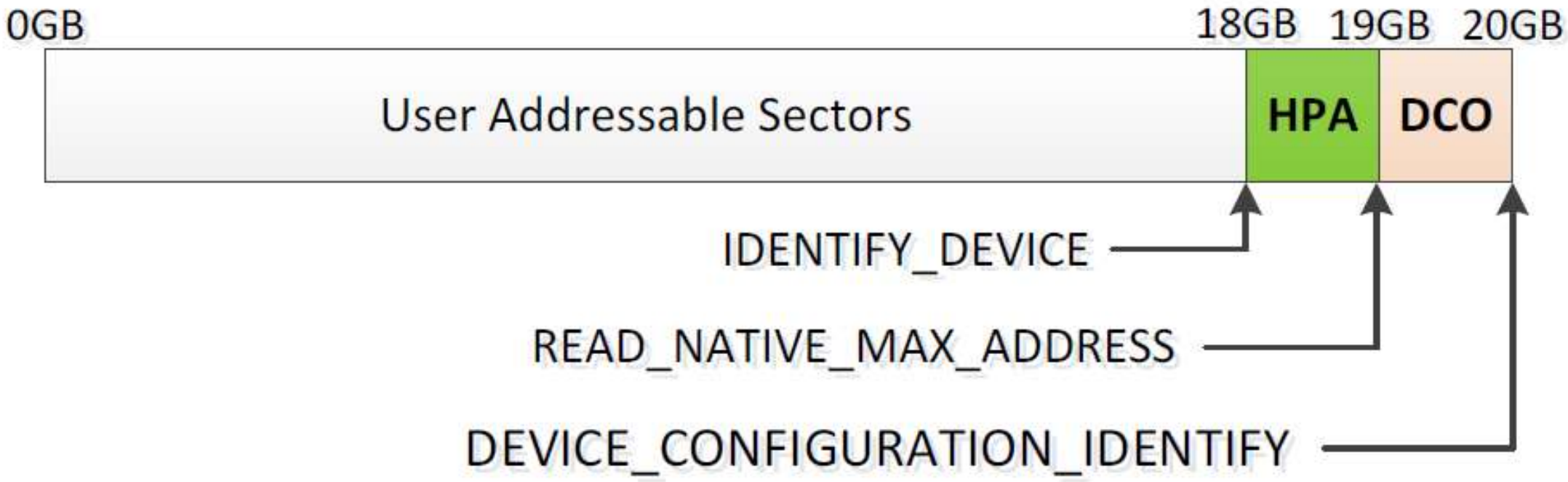
ENREGISTREMENT DE BITS ZONÉ

- Les densités des données sur le lecteur de disque sont de deux types, à savoir :
  - Densité de piste: c'est le nombre de pistes par pouce sur un plateau
  - Densité surfacique: elle est définie comme le nombre de bits par pouce carré sur un plateau
- Exemple
  - 1,2 pouces utilisable pour le stockage avec 22000 pistes
  - Densité des pistes = 22000 / 1,2 = 18333 pistes / pouce
  - Un pouce de piste peut enregistrer 200000 bits
  - Densité linéaire = 200000 bits / pouce
  - Densité surfacique = densité linéaire * densité de la piste
  - = 200000 * 18333 bits / pouce^2
  - = 3666600000 bits / pouce^2

QUELLE EST LA TAILLE D'UN DISQUE

HPA: Host Protected Area (ATA-4)

DCO: Device Configuration Overlay (ATA-6)



Carrier, B. (2005). File System Forensic Analysis, p.38

QUELLE EST LA TAILLE D'UN DISQUE

- Est-ce c’est aussi gros qu'on le dit ?
- La réponse que vous obtenez dépend de la façon dont vous demandez
  - Pour un disque ATA (advanced Technology attachment) , demander avec la commande IDENTIFY_DEVICE exclura HPA et DCO
  - La plupart des systèmes d'exploitation utilisent IDENTIFY_DEVICE ou quelque chose de similaire¨
- Si vous enquêtez sur un délinquant sophistiqué, comparez la taille du lecteur indiquée aux spécifications du fabricant pour le disque
- Si un HPA ou DCO est présent, un logiciel ou un matériel spécialisé peut être nécessaire pour créer une image du disque complet

HDPARM

- est un utilitaire en ligne de commande sur Linux pour visualiser et repérer les paramètres d'un disque IDE
- hdparm –I (Detailed/current information)
- ¨ hdparm –N (HPA) -- Get/set max visible number of sectors (HPA) (VERY DANGEROUS)
- ¨ hdparm --dco-identify (DCO) --- Read/dump device configuration identify data
- ¨ May or may not work depending on drive technology
- **Example**
  - $ hdparm –N /dev/sda
  - /dev/sda:
  - max sectors = 1465149168/1465149168, HPA is disabled
  - $ hdparm –N /dev/sdb
  - /dev/sdb
  - max sectors = 586070255/586072368, HPA is enabled

VOLUMES ET PARTITIONS

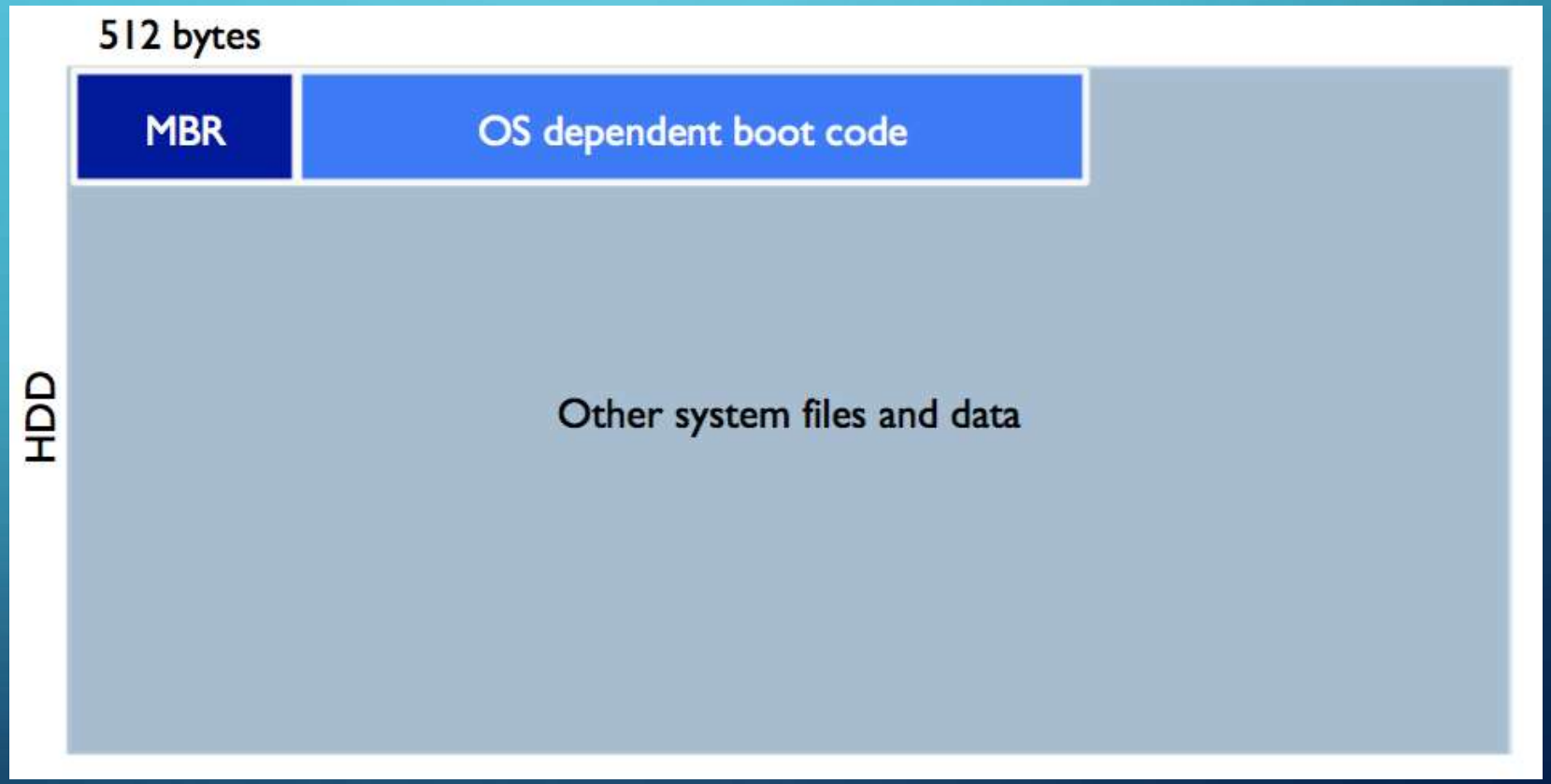
- Un disque peut être divisé en collections de secteurs, formant un lecteur logique
- Une partition est un lecteur logique
  - Partition primaire
  - Partition étendue
- Espace de partition
  - Espace inutilisé entre les partitions
  - Possibilité d'une partition cachée

MASTER BOOT RECORD (MBR)

- Le premier secteur du disque contient un code spécial appelé Master Boot Record (MBR)
  - MBR stocke des informations sur les partitions d'un disque et leurs emplacements, taille et autres éléments importants
  - Le code MBR peut également charger des chargeurs de démarrage complexes pilotés par GUI
- Dans les systèmes multi-partition, le premier secteur d'une partition amorçable est appelé Volume Boot Record (VBR)
  - Contient généralement du code pour charger le système d'exploitation

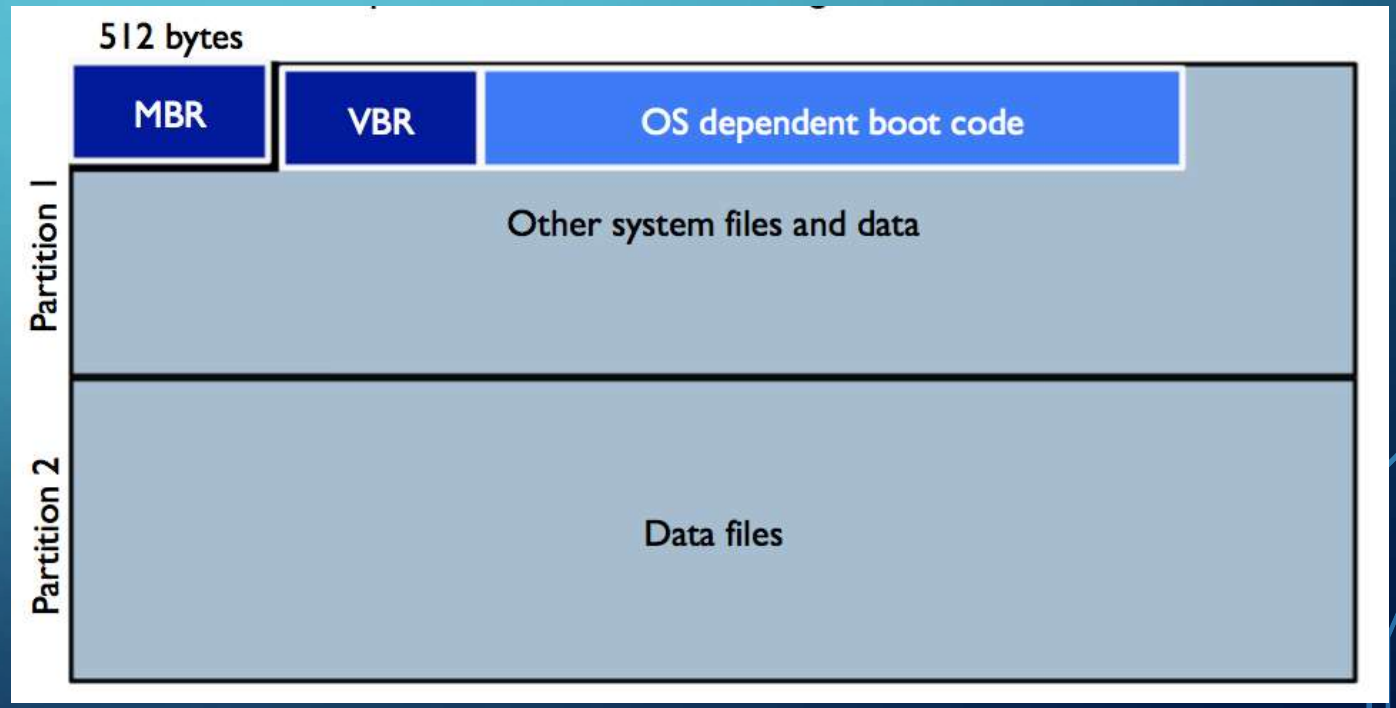
PROCESSUS DE BOOT D'UN OS UNIQUE

- Le BIOS charge le MBR en mémoire et l'exécute
- Le code exécuté sur le MBR charge et exécute le code de démarrage lié au système d'exploitation



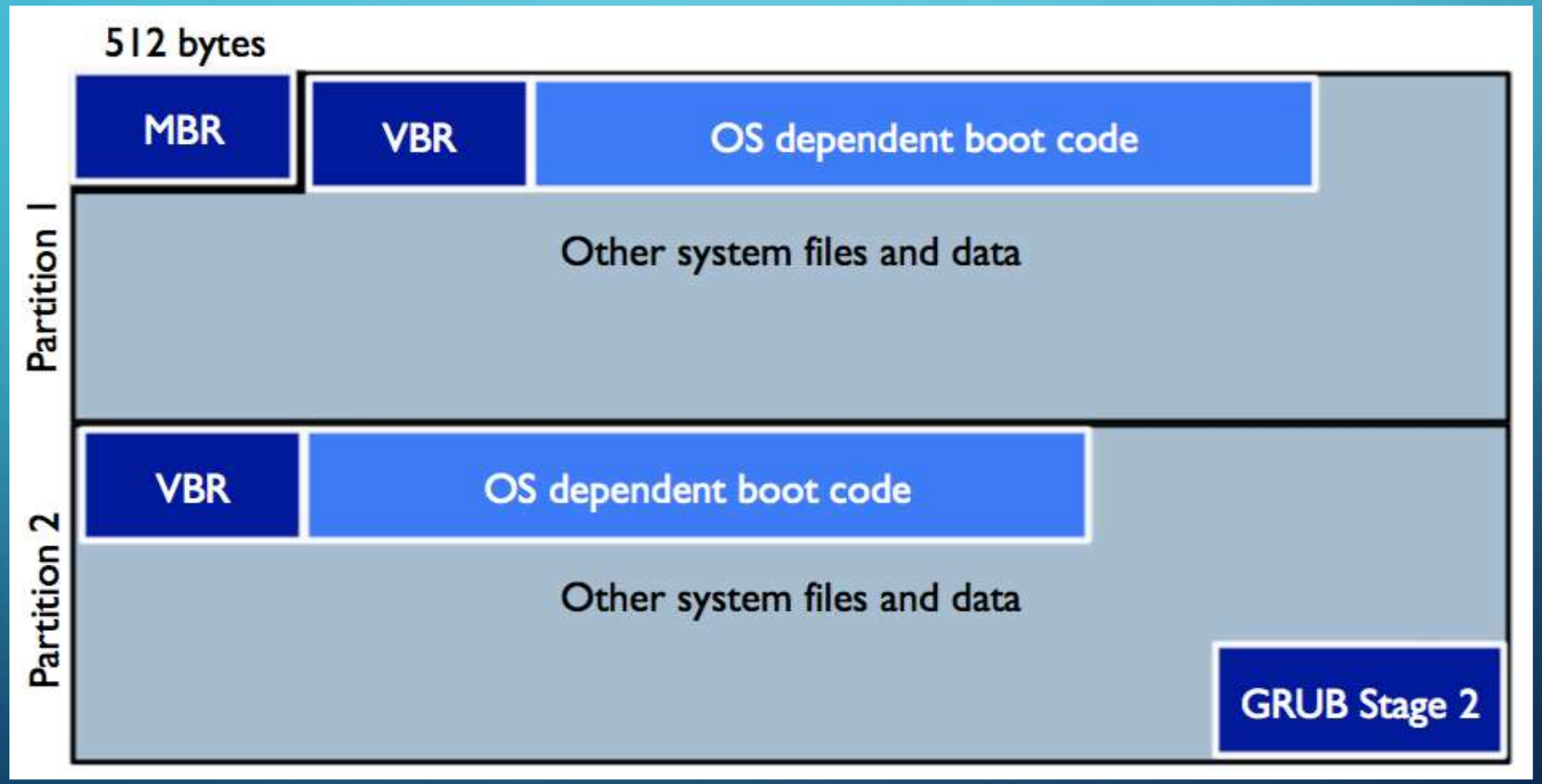
PROCESSUS DE BOOT MULTI PARTITION

- Boot charge le MBR en mémoire et l'exécute
- Le code MBR identifie la partition active
- Le code MBR charge le VBR de la partition active et transfère le contrôle
- L'exécution se déroule comme dans le cas de la méthode OS unique



PROCESSUS DE BOOT MULTI OS AVEC GRUB

- Le code MBR (GRUB) charge le code GRUB Stage 2
- GRUB Stage 2 demande à l'utilisateur de choisir un VBR



PARTITIONS DE DISQUE

- L'utilitaire de l'éditeur de disque peut modifier les informations de la table de partition
  - Pour masquer une partition
- Peut examiner une partition au niveau physique avec un éditeur :
  - Norton DiskEdit, WinHex, HexWorkshop
- Analyser les codes clés hexadécimaux que le système d'exploitation utilise pour identifier et maintenir les partitions

LECTURE DE HEX DUMP

- Les dump hexadécimaux n'ont aucun sens à moins que vous ne sachiez ce que vous lisez
  - La structure des données stockées doit être connue avant de lire un vidage hexadécimal
- Les structures sont généralement spécifiées à l'aide de décalages
  - Un offset spécifie l'emplacement d'une donnée spécifique par rapport à
    - le début du vidage hexadécimal
    - ou le début d'une autre structure
  - Le premier octet d'un vidage hexadécimal est à zéro

EXEMPLE HEX DUMP

- Supposons que nous ayons stocké un caractère (1 octet), suivi d'un entier (4 octets), suivi d'une date (4 octets) dans un fichier

hex dump	4B	CD	34	AB	12	09	0F	DE	07
offset	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8

- Offset 0x0: caractère (1 octet)
  - 0x4B (le caractère K en ASCII)
  - Offset 0x1: entier (4 octets)
    - 0x12AB34CD (les octets CD 34 AB 12 disposés au format little-endian)
  - Offset 0x5: date (4 octets)
    - Mais quelle date est enregistrée? Nous devons connaître la structure!

EXEMPLE HEX DUMP

- Les octets de date sont 09 0F DE 07
  - Si la date était enregistrée comme le nombre de secondes depuis le 1er janvier 1970, alors 0x07DE0F09 serait le 3 mars 1974
- Supposons que la date a été enregistrée au format MM JJ AAAA
  - Offset 0x0 (dans les octets de date): mois MM
    - 0x09 (septembre
  - Offset 0x1: jour JJ
    - 0x0F (15)
  - Offset 0x2: année AAAA
    - DE 07 (= 0x07DE = 2014)

hex dump	4B	CD	34	AB	12	09	0F	DE	07
offset	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8

UN MBR TYPIQUE

- Premiers 440 octets : code du boot loader
  - Instructions pour localiser la partition bootable, charger le premier secteur de cette partition(VBR) et exécutez
- Offset 0x1B8
  - Identificateur de disque - 4 octets
- Offset 0x1BC
  - Nuls
- Offset 0x1BE
  - Table de partition - 16x4 = 64 octets
- Décalage 0x1FE¤
  - Signature du boot record - 2 octets
  - 0xAA55
- Total de 512 octets

TABLE DE PARTITION

- Chaque entrée de 16 octets nous renseigne sur une partition
- Structure
  - Offset 0x0: 0x80 si partition bootable (possède VBR), sinon 0x00
  - Offset 0x1: valeurs CHS du premier secteur
  - Offset 0x4: code du type de partition
  - Offset 0x5: valeurs CHS du dernier secteur
  - Offset 0x8: LBA du premier secteur
  - Offset 0xC: nombre de secteurs dans la partition
- Format littke-endian : les valeurs multi-octets sont stockées dans l'ordre du dernier octet au premier octet

CLUSTERS PERDUS

- Marqué par un système d'exploitation comme utilisé mais non attribué à un fichier
- Les clusters perdus peuvent être réaffectés aux données, ce qui libère de l'espace disque
- L'utilitaire ScanDisk a la capacité d'identifier les clusters perdus dans les systèmes d'exploitation DOS et Windows

MAUVAIS SECTEURS

- Une partie endommagée d'un disque sur laquelle aucune opération de lecture / écriture ne peut être effectuée
- Le formatage d'un disque permet au système d'exploitation d'identifier les secteurs inutilisables et les marque comme défectueux
- Un logiciel spécial est utilisé pour récupérer les données sur un secteur défectueux

COMPRENDRE LE SYSTÈME DE FICHIER

- système de fichiers
  - Comment les fichiers sont-ils organisés sur le disque?
  - Donne à l'OS une feuille de route pour les données sur un disque
- Le type de système de fichiers utilisé par un système d'exploitation détermine la manière dont les données sont stockées sur le disque
- Un système de fichiers est généralement lié à un système d'exploitation
- Lorsque vous devez accéder à l'ordinateur d'un suspect pour acquérir ou inspecter des données
  - Vous devez être familiarisé avec la plate-forme de l’ordinateur

TYPES DE SYSTÈME DE FICHIER

- Systèmes de fichiers sur disque
  - FAT32, exFAT, NTFS, ext2, ext3, ext4, UFS, HFS, ISO 9660,… etc.
- Systèmes de fichiers réseau
  - NFS, AFS, SMB,… etc.
- Systèmes de fichiers de base de données
- Systèmes de fichiers spéciaux
  - GmailFS, ftpfs, procfs,… etc.

SYSTÈMES DE FICHIERS LINUX POPULAIRES

- Ext (système de fichiers étendu)
  - Premier système de fichiers pour le système d'exploitation Linux à surmonter certaines limitations du système de fichiers Minix
  - Remplacement rapide par le deuxième système de fichiers étendu
- Ext2 (deuxième système de fichiers étendu)
  - Système de fichiers standard avec des algorithmes améliorés utilisés sur l'OS Linux depuis plusieurs années
  - Pas un système de fichiers journalisé

SYSTÈMES DE FICHIERS LINUX POPULAIRES

- Ext3 (troisième système de fichiers étendu)
  - Système de fichiers de journalisation utilisé dans le système d'exploitation GNU / Linux
  - Peut être monté et utilisé comme système de fichiers Ext2
  - Peut utiliser des utilitaires de maintenance du système de fichiers (comme fsck) pour maintenir et réparer le système de fichiers Ext2
- Ext4 (quatrième système de fichiers étendu)
  - Journalisation du système de fichiers pour Linux
  - Noyau 2.6.28
  - Extension des limites de stockage

SYSTÈMES DE FICHIERS WINDOWS

- FAT (table d'allocation de fichiers)
  - Système de fichiers 16 bits développé pour MS-DOS
  - Utilisé dans les versions grand public de Microsoft Windows jusqu'à Windows Me
  - Considéré comme relativement simple et est devenu un format populaire pour les périphériques tels que les disquettes, les périphériques USB, les appareils photo numériques, les disques flash
- FAT32
  - Version 32 bits du système de fichiers FAT avec capacité de stockage jusqu'à 2 Go

SYSTÈMES DE FICHIERS WINDOWS

- NTFS (système de fichiers de nouvelle technologie)
  - NTFS a trois versions
    - V1.2 (v4.0) trouvé dans NT 3.51 et NT 4
    - V3.0 (v5.0) trouvé dans Windows 2000
    - V3.1 (v5.1) disponible dans Windows XP et Windows Server 2003, Windows Vista, Windows 7, Windows 10
  - Les nouvelles versions ont ajouté des fonctionnalités supplémentaires telles que les quotas introduits par Windows 2000.
  - En NTFS, tout tel que le nom du fichier, la date de création, les autorisations d'accès et même le contenu est écrit sous forme de métadonnées

EXPLORER LA STRUCTURE DE FICHIERS MICROSOFT

- Dans les structures de fichiers Microsoft, les secteurs sont regroupés pour former des clusters
  - Plus petite unité d'allocation de stockage
    - Le stockage est attribué en multiples de clusters (pas de secteurs)
- La taille du cluster peut varier de 512 octets à 128 Ko (généralement en puissances de 2)
- La combinaison de secteurs en clusters minimise la surcharge d'écriture ou de lecture de fichiers sur un disque

EXPLORER LA STRUCTURE DE FICHIERS MICROSOFT

- Les clusters sont numérotés séquentiellement à partir de 2
  - Le comptage démarre après quelques secteurs initiaux qui contiennent l'enregistrement de démarrage et une base de données de structure de fichiers
- Le système d'exploitation attribue des numéros d'identification à ces clusters, appelés adresses logiques
- Les numéros de secteur sont appelés adresses physiques

CODES DE SYSTÈME DE FICHIERS COMMUNS

Code hexadécimal	Système de fichier
01	DOS 12 bits FAT
04	DOS 16 bits FAT (taille de partitions < 32 MO)
06	DOS 16 bits FAT (taille de partitions > 32 MO)
07	NTFS
0B	DOS 32 bits FAT
83	Linux native
EB	BeOS

Utilisé dans l'entrée de table de partition MBR / VBR

EXAMEN DES DISKS FAT

- Table d'allocation de fichiers (FAT)
  - Base de données de structure de fichiers conçue à l'origine par Microsoft pour les disquettes
  - L'emplacement de FAT sur le disque peut être identifié à partir de l'enregistrement de démarrage d'une partition FAT (début + n ° de secteurs réservés)
- Les informations du répertoire racine dans une base de données FAT commencent après le FAT (plusieurs copies de celui-ci)
  - Contient les noms de fichiers, les noms de répertoires, la date et les horodatages, le numéro de cluster de départ et les attributs de fichier
  - Une entrée (appelée entrée de répertoire) indique un fichier / répertoire
- Versions FAT
  - FAT12, FAT16 et FAT32

EXAMEN DES DISKS FAT

- Les tailles de cluster varient en fonction de la taille du disque dur et du système de fichiers

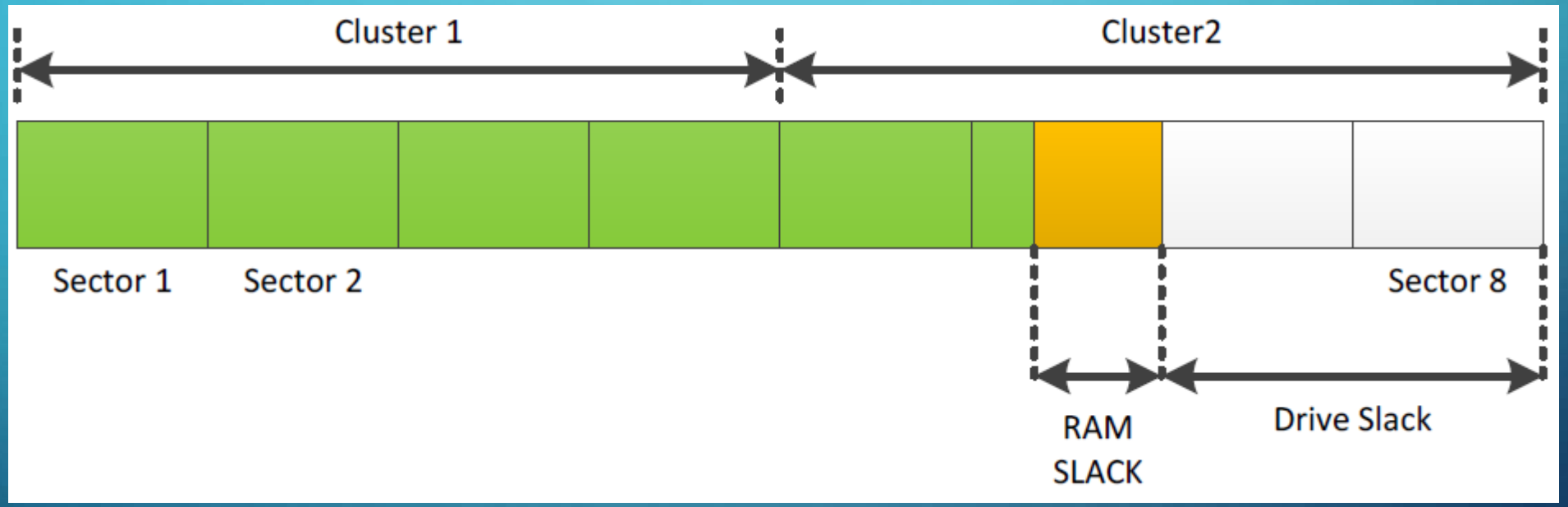
Taille du disque	Nbr de secteurs par cluster	Taille du cluster FAT16
8-32 MO	1	512 O
32-64 MO	2	1 KO
64-128 MO	3	2 KO
128-256 MO	8	4 KO
256-512 MO	16	8 KO
512-1024 MO	32	16 KO
1 – 2 GO	64	32 KO
2 – 4 GO	128	64 KO

- Le cluster 2 commence dans le secteur suivant les entrées du répertoire racine

EXAMEN DES DISKS FAT

- Les systèmes d'exploitation Microsoft allouent de l'espace disque pour les fichiers par clusters
  - Résultats dans File slack
    - Espace inutilisé dans un cluster entre la fin d'un fichier actif et la fin du cluster
  - Le file slack comprend :
    - RAM Slack - zone comprise entre la fin d'un fichier et la fin du secteur
    - Drive Slack : secteurs supplémentaires nécessaires pour remplir un cluster
  - Des données résiduelles peuvent être trouvées dans un stockage non alloué ou dans un espace libre de fichier
    - Les données résiduelles sont des données qui ont été supprimées mais non effacées

DONNÉES RÉSIDUELLES



EXAMEN DES DISKS FAT

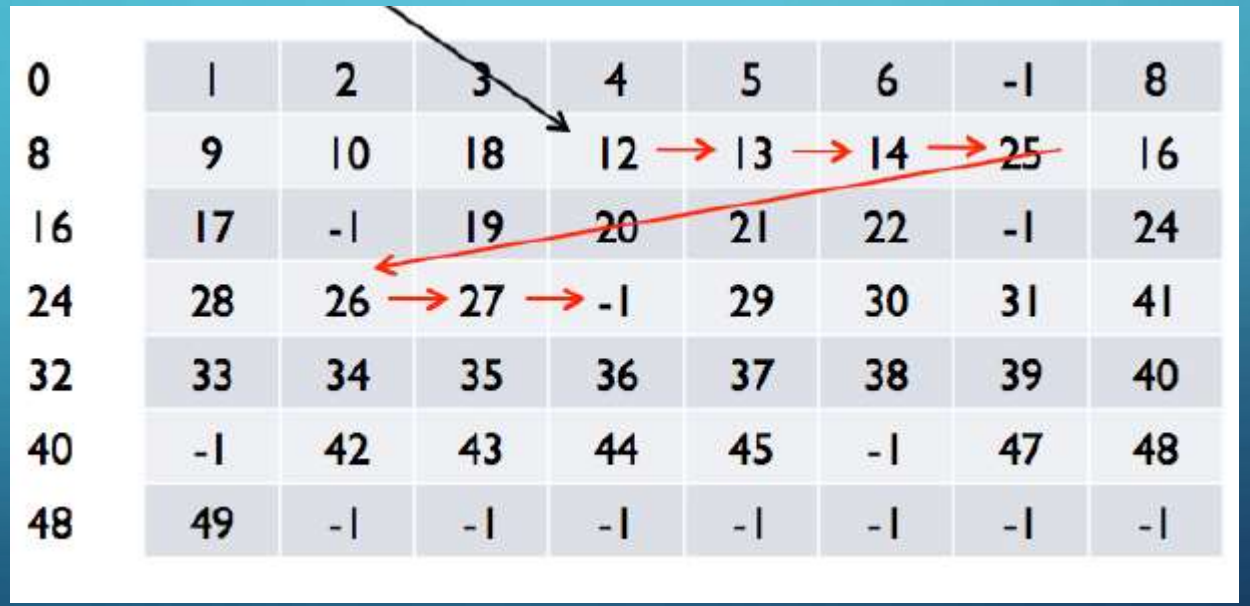
- Lorsque vous manquez d'espace pour un cluster alloué
  - OS alloue un autre cluster pour votre fichier
- À mesure que les fichiers se développent et nécessitent plus d'espace disque, les clusters affectés sont enchaînés
  - La chaîne peut être cassée ou fragmentée

FRAGMENTATION DE FICHIERS

- Lorsque le système d'exploitation stocke des données dans un système de fichiers FAT, il attribue une position de cluster de départ à un fichier
  - Les données du fichier sont écrites dans le premier secteur du premier cluster affecté
- Lorsque ce premier cluster attribué est rempli et manque de place
  - FAT attribue le prochain cluster disponible au fichier
- Si le prochain cluster disponible n'est pas contigu au cluster actuel
  - Le fichier se fragmente
  - FAT permet de relier ces fragments

TABLE D'ALLOCATION DE FICHIERS

- Le système d'exploitation stocke le premier numéro de cluster de chaque fichier dans une entrée de répertoire (contient des métadonnées sur le fichier)
- Les clusters suivants sont recherchés dans la table d'allocation de fichiers



0	1	2	3	4	5	6	-1	8
8	9	10	18	12 →	13 →	14 →	25	16
16	17	-1	19	20	21	22	-1	24
24	28	26 →	27 →	-1	29	30	31	41
32	33	34	35	36	37	38	39	40
40	-1	42	43	44	45	-1	47	48
48	49	-1	-1	-1	-1	-1	-1	-1

SUPPRESSION DES FICHIERS FAT

- Dans les systèmes d'exploitation Microsoft, lorsqu'un fichier est supprimé
  - L'entrée est marquée comme fichier supprimé
    - Avec le caractère 0xE5 (σ) remplaçant la première lettre du nom de fichier
    - La chaîne FAT pour ce fichier est définie sur 0 (clusters inutilisés)
- Les données du fichier restent sur le disque
- La zone du disque où réside le fichier supprimé devient de l'espace disque non alloué
  - Disponible pour recevoir de nouvelles données à partir de fichiers nouvellement créés ou d'autres fichiers nécessitant plus d'espace
  - Les données de l'ancien fichier résident sur cet espace jusqu'à ce qu'elles soient écrasées par le contenu d'un autre fichier

SUPPRESSION DES FICHIERS FAT

- Ces fichiers peuvent être récupérés à l'aide d'outils forensics
- Peu d'outils pouvant être utilisés pour la criminalistique sont
  - WINHEX (X-Ways)
  - Undelete
  - FILE SCAVENGER

EXAMEN DES DISQUES NTFS

- NTFS¨ New Technology File System (NTFS)
  - Introduit avec Windows NT
  - Système de fichiers principal pour Windows Vista et Windows 7
- En NTFS, tout ce qui est écrit sur le disque est considéré comme un fichier
- La taille de cluster par défaut est de 4 Ko (8 secteurs) dans la plupart des disques
  - http://support.microsoft.com/kb/140365

STRUCTURE D'UN DISQUE NTFS

- Le premier secteur est le secteur de démarrage de partition (partition boot sector)
  - Structure similaire à FAT16
  - Offset 0x30: numéro de cluster logique (8 octets) pour le fichier MFT (Master File Table)
- Les 15 secteurs suivants sont réservés
  - Contient le code du bootloader
- Vient ensuite la zone MFT qui contient la table de fichiers maîtres
  - Contient des informations sur chaque fichier du système
  - Au départ, environ 12,5% de l'espace disque lui est réservé
  - Vérifiez toujours le secteur de démarrage pour démarrer le cluster de MFT!

SYSTÈME DE FICHIER NTFS

- MFT contient des informations sur tous les fichiers et dossiers sur le disque
  - Y compris les fichiers système utilisés par l'OS
- Les informations sur un fichier constituent un enregistrement
  - Le MFT n'est rien d'autre qu'une table d'enregistrements
- Les 16 premiers enregistrements sont réservés aux fichiers système
- Les enregistrements dans le MFT sont appelés métadonnées
  - Données sur les données

ENREGISTREMENTS MFT

N° d'enregistrement	Nom de fichier	Description
0	$MFT	Enregistrement de fichier de base
1	$MFTMirr	4 premiers enregistrements de MFT
2	$LogFile	Historique des transactions des fichiers système
3	$Volume	Informations spécifiques au volume
4	$AttrDef	Tableau des noms d'attributs, des numéros et des définitions
5	$	Dossier racine du volume NTFS
6	$Bitmap	Bitmap montrant quels clusters sont utilisés
7	$Boot	Données des secteurs de démarrage
8	$BadClus	Informations sur les mauvais clusters
9	$Secure	Liste de contrôle d'accès
10	$Upcase	Caractère Unicode majuscule
11	$Extend	Extensions facultatives; par exemple, des quotas
12-15		Réservé pour une utilisation future
À partir de 16		Enregistrements du fichier utilisateur

ATTRIBUTS FICHIERS ET MFT

- Dans le NTFS MFT
  - Toutes les métadonnées sur les fichiers et dossiers sont stockées dans des enregistrements séparés de 1024 octets chacun
    - Entier signé à l'offset 0x40 dans le secteur de démarrage (4 octets)
- Chaque enregistrement contient des informations sur le fichier ou le dossier
  - Ces informations sont divisées en champs d'enregistrement contenant des métadonnées
  - Un champ d'enregistrement est également appelé attribut
- Les informations sur les fichiers ou dossiers sont généralement stockées de deux manières dans un enregistrement MFT:
  - Résident: le contenu du fichier tient dans les 1024 octets de l'enregistrement lui-même
  - Non-résident: les données sont stockées en dehors du MFT

ATTRIBUTS FICHIERS ET MFT

- Les fichiers de plus de 512 octets sont stockés en dehors du MFT
  - L'enregistrement MFT fournit les adresses de cluster où le fichier est stocké sur la partition du disque
    - Désigné comme l'exécution des données
- Chaque enregistrement MFT commence par un en-tête l'identifiant comme un attribut résident ou non-résident

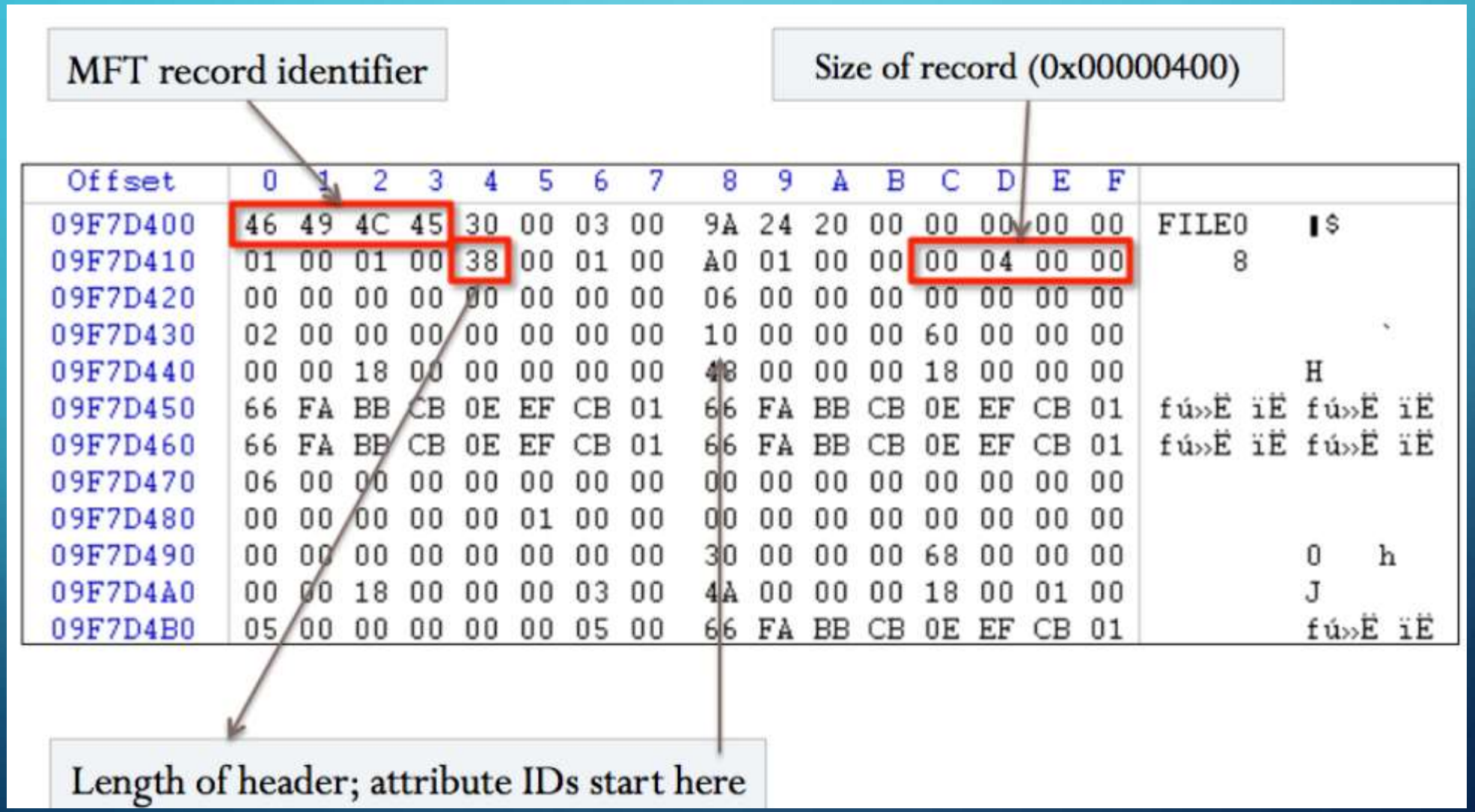
LECTURE DES ENREGISTREMENTS MFT

- Le terme offset signifie l'emplacement par rapport au début de quelque chose
- Les données numériques sont généralement stockées au format little-endian
  - Par exemple si vous regardez par exemple 4 octets de données dans l'éditeur hexadécimal
    - 00 AE 97 02
    - Signifie 0x0297AE00 = 43494912

EN-TÊTE D'ENREGISTREMENT MFT

- Offset 0x00
  - Identifiant: tous les enregistrements MFT commencent par des valeurs hexadécimales 46 49 4C 45 à cet offset
- Offset 0x1C à 0x1F
  - Taille de l'enregistrement MFT; la valeur par défaut est 0x0400 (1024) octets
- Offset 0x14
  - Longueur de l'en-tête: c'est ici que commencent les autres champs d'enregistrement (ID d'attribut)

EN-TÊTE D'ENREGISTREMENT MFT



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
09F7D400	46	49	4C	45	30	00	03	00	9A	24	20	00	00	00	00	00	FILE0 $
09F7D410	01	00	01	00	38	00	01	00	A0	01	00	00	00	04	00	00	8
09F7D420	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00	
09F7D430	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	`
09F7D440	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	H
09F7D450	66	FA	BB	CB	0E	EF	CB	01	66	FA	BB	CB	0E	EF	CB	01	fú»Ë ïË fú»Ë ïË
09F7D460	66	FA	BB	CB	0E	EF	CB	01	66	FA	BB	CB	0E	EF	CB	01	fú»Ë ïË fú»Ë ïË
09F7D470	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
09F7D480	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	
09F7D490	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	0 h
09F7D4A0	00	00	18	00	00	00	03	00	4A	00	00	00	18	00	01	00	J
09F7D4B0	05	00	00	00	00	00	05	00	66	FA	BB	CB	0E	EF	CB	01	fú»Ë ïË

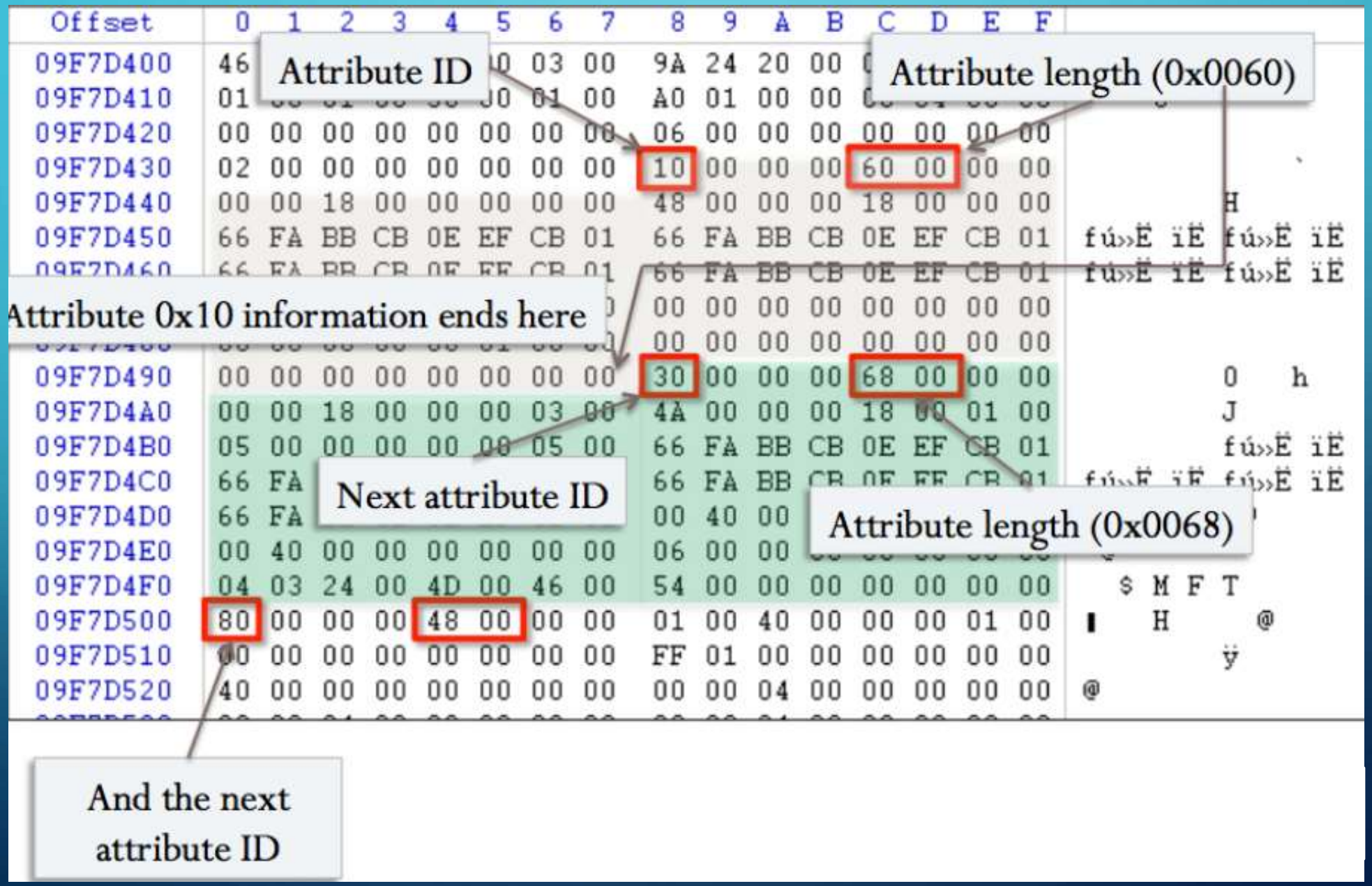
ID D'ATTRIBUTS MFT

- Les informations d'offset ci-dessous sont relatives au point de départ de l'attribut
- Offset 0x00
  - ID d'attribut: vous indique quelles informations suivent
- Offset 0x04 et 0x05
  - Taille de l'attribut depuis le début de l'attribut

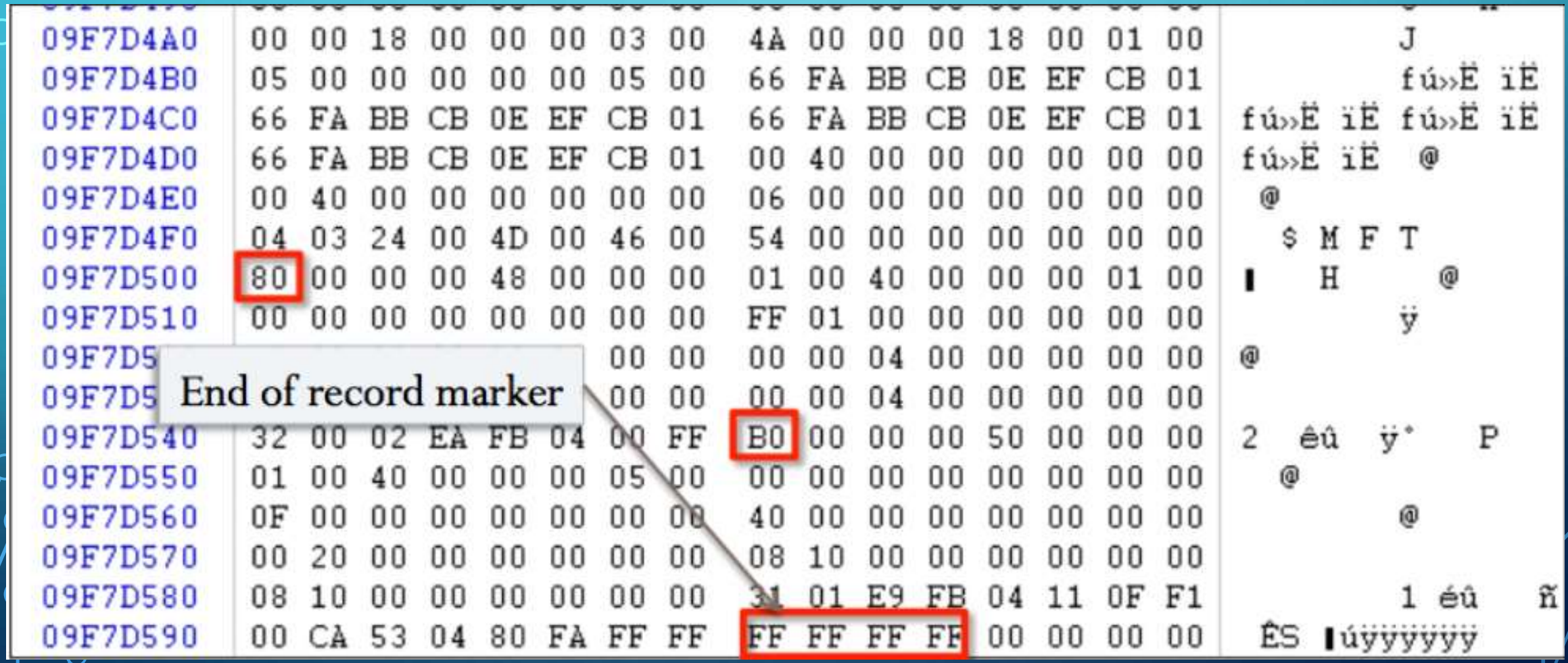
QUELQUES ID D'ATTRIBUTS MFT

- 0x10: informations standard telles que l'heure de création du fichier, l'autorisation, etc.
- 0x20: utilisé lorsque la liste des attributs ne rentre pas dans les 1024 octets de l'enregistrement
- 0x30: nom de fichier
- 0x80: les données de fichier ou les données s'exécutent
- L'idée est de savoir (en lisant des documentations)
  - Ce que signifie un ID d'attribut, et
  - Comment les informations correspondant à cet attribut sont-elles organisées

ID D'ATTRIBUTS MFT



ID D'ATTRIBUTS MFT



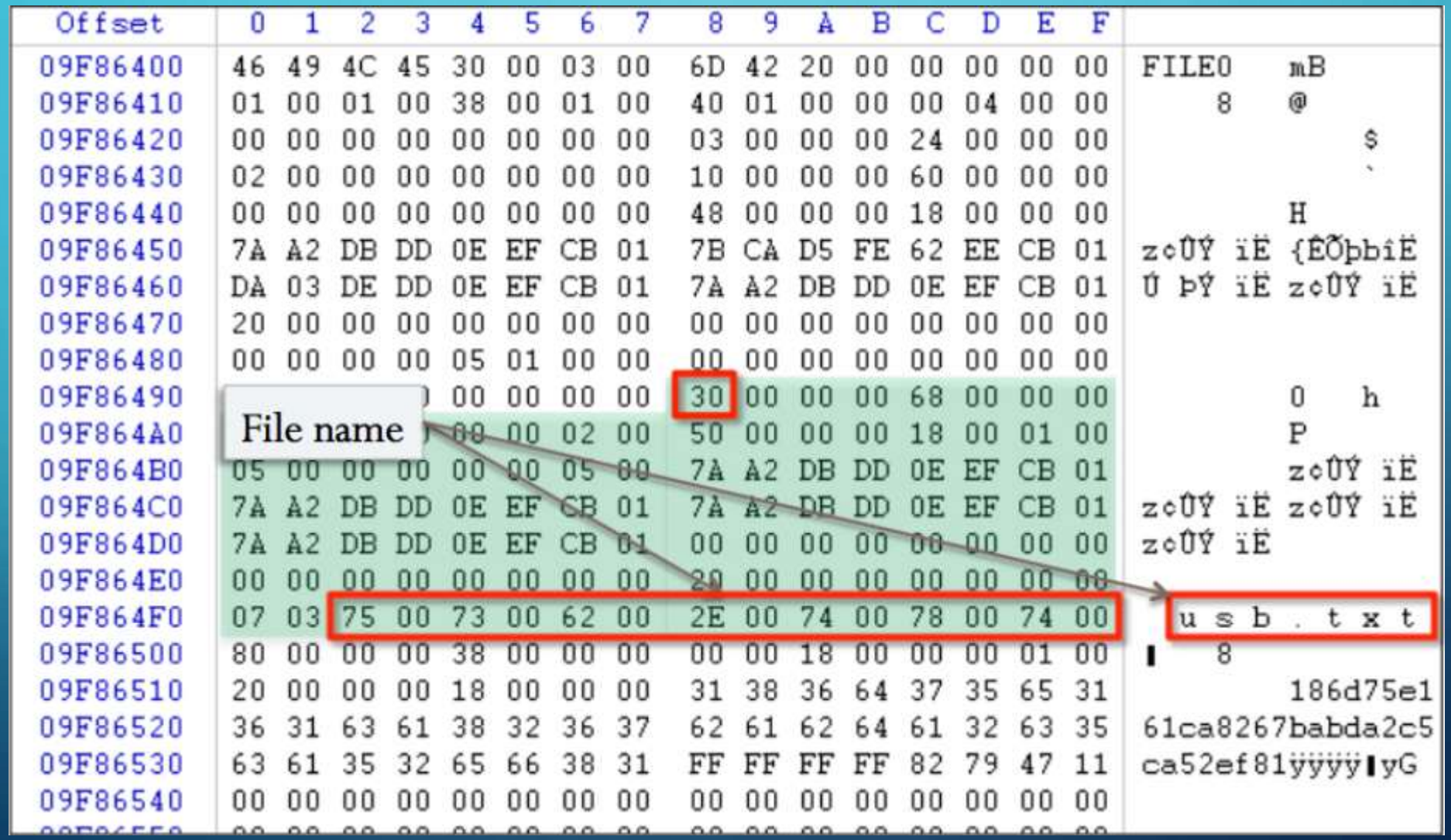
ATTRIBUT 0X10 : INFORMATIONS STANDARDS

- Offset relatif au début des informations d'attribut
- Offset 0x18 à 0x1F
  - la date et l'heure de création du fichier; stocké au format de nom de fichier Win32
- Offset 0x20 à 0x27
  - Date et heure de la dernière modification
- Offset 0x28 à 0x2F
  - Date et heure du dernier accès
- Et il y en a plus!

ATTRIBUT 0X30 : NOM DE FICHIER

- Vous pouvez voir deux instances de cet attribut dans un enregistrement
  - Un pour le nom court du style MS-DOS
  - Un autre pour le nom long
- Offset 0x04 et 0x05
  - Taille de cet attribut (comme dans tous les autres attributs)
- Décalage à partir de 0x5A
  - Le nom
  - Utilisez la taille pour déterminer la quantité à lire à partir d'ici

ATTRIBUT 0X30 : NOM DE FICHIER



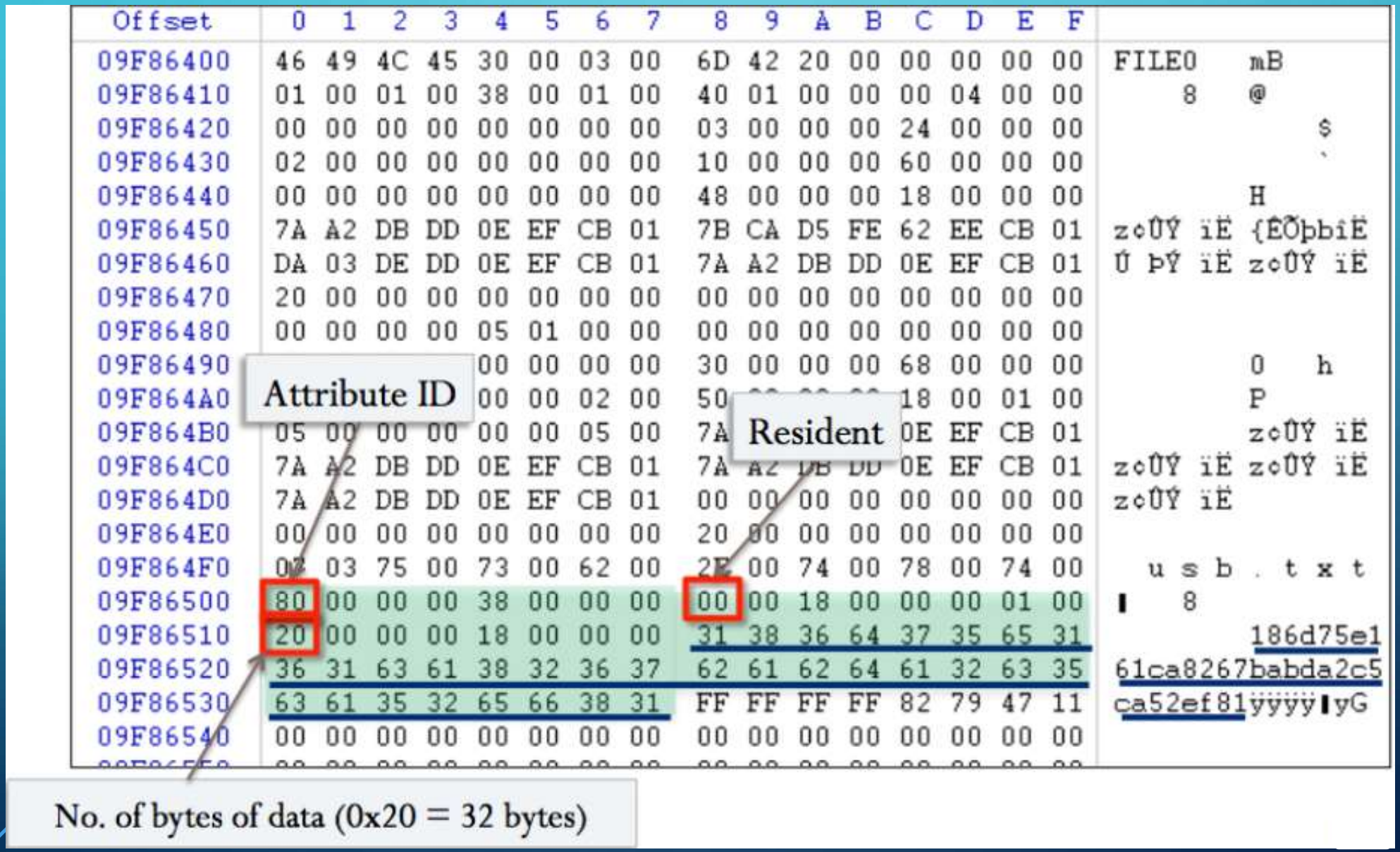
MFT ET NUMÉRO DE CLUSTER

- Lorsqu'un disque est créé en tant que structure de fichiers NTFS
  - Le système d'exploitation attribue des clusters logiques à l'ensemble de la partition de disque
- Ces clusters affectés sont appelés numéros de cluster logiques (LCN)
  - Devenir les adresses qui permettent au MFT de se lier à des fichiers non résidents sur la partition du disque
  - Un numéro de cluster relatif à un autre numéro de cluster est appelé un numéro de cluster virtuel (VCN)

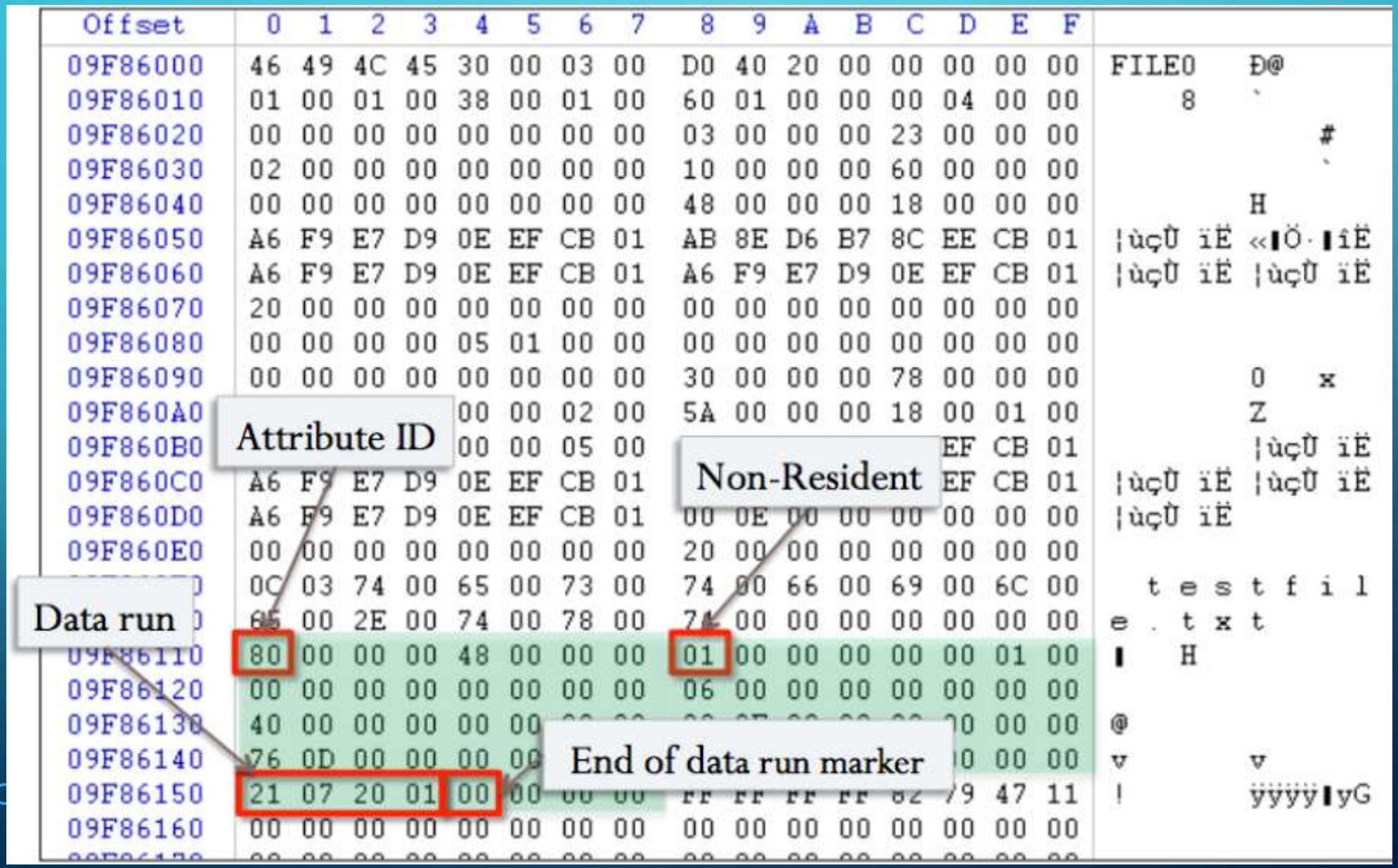
ATTRIBUT 0X80 : DONNÉES

- Décalage 0x08
  - La valeur 0x00 signifie un fichier résident
  - La valeur 0x01 signifie un fichier non résident
- Si dossier résident
  - Offset 0x10: nombre d'octets de données
  - Offset 0x18: début des données
- Si dossier non-résident
  - Offset 0x40: les données s'exécutent
    - Une liste d'adresses de cluster où les données peuvent être trouvées

ATTRIBUT 0X80 : FICHIER RÉSIDENT



ATTRIBUT 0X80 : FICHIER NON RÉSIDENT



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
09F86000	46	49	4C	45	30	00	03	00	D0	40	20	00	00	00	00	00
09F86010	01	00	01	00	38	00	01	00	60	01	00	00	00	04	00	00
09F86020	00	00	00	00	00	00	00	00	03	00	00	00	23	00	00	00
09F86030	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00
09F86040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00
09F86050	A6	F9	E7	D9	0E	EF	CB	01	AB	8E	D6	B7	8C	EE	CB	01
09F86060	A6	F9	E7	D9	0E	EF	CB	01	A6	F9	E7	D9	0E	EF	CB	01
09F86070	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
09F86080	00	00	00	00	05	01	00	00	00	00	00	00	00	00	00	00
09F86090	00	00	00	00	00	00	00	00	30	00	00	00	78	00	00	00
09F860A0					00	00	02	00	5A	00	00	00	18	00	01	00
09F860B0					00	00	05	00						EF	CB	01
09F860C0	A6	F9	E7	D9	0E	EF	CB	01						EF	CB	01
09F860D0	A6	F9	E7	D9	0E	EF	CB	01	00	0E	00	00	00	00	00	00
09F860E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
	0C	03	74	00	65	00	73	00	74	00	66	00	69	00	6C	00
	65	00	2E	00	74	00	78	00	74	00	00	00	00	00	00	00
09F86110	80	00	00	00	48	00	00	00	01	00	00	00	00	00	01	00
09F86120	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00
09F86130	40	00	00	00	00	00									00	00
09F86140	76	0D	00	00	00	00									00	00
09F86150	21	07	20	01	00	00	00	00	FF	FF	FF	FF	82	79	47	11
09F86160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

INTERPRÉTATION DES EXÉCUTIONS DE DONNÉES

- Exécution des données:
  - 32 B1 07 8C 8C 00 22 63 07 95 ED 32 BC 06 3C 36 01 00
- Chaque exécution de données comporte trois composants
  - Premier: indique la longueur des deux autres composants
  - Deuxième: longueur de l'execution
  - Troisième: LCN ou VCN

INTERPRÉTATION DES EXÉCUTIONS DE DONNÉES

- Exécution des données:
  - 32 B1 07 8C 8C 00 22 63 07 95 ED 32 BC 06 3C 36 01 00
- Premier cycle de données: 32 B1 07 8C 8C 00
  - Premier composant: 32
    - Un demi-octet inférieur (0x2 ici) signifie qu'il y a 0x2 octets dans le deuxième composant
    - Un demi-octet supérieur (0x3 ici) signifie qu'il y a 0x3 octets dans le troisième composant
  - Deuxième composante: B1 07, soit 0x07B1 = 1969
  - Troisième composant: 8C 8C 00, soit 0x008C8C = 35980
  - Cela signifie les données résidant dans les grappes contiguës de 1969 à partir de la grappe numéro 35980
    - Par conséquent, le numéro de cluster dans un LCN lors du premier cycle de données
      - Il y a plus de données!

INTERPRÉTATION DES EXÉCUTIONS DE DONNÉES

- Exécution des données:
  - 32 B1 07 8C 8C 00 22 63 07 95 ED 32 BC 06 3C 36 01 00
- Deuxième série de données: 22 63 07 95 ED
  - Le troisième composant est désormais un VCN
    - Aussi, doit être lu comme un entier signé
  - Après avoir lu les données comme indiqué par le premier cycle de données, continuer la lecture à partir
    - Cluster 35980 + (-4715) = 31265 (0xED95 est -4715)
    - Et lisez les clusters 0x0763 (= 1891) de manière contiguë

INTERPRÉTATION DES EXÉCUTIONS DE DONNÉES

- Exécution des données:
  - 32 B1 07 8C 8C 00 22 63 07 95 ED 32 BC 06 3C 36 01 00
- Troisième cycle de données: 32 BC 06 3C 36 01
  - Après avoir lu les données comme indiqué b la deuxième série de données, continuer la lecture
    - Cluster 31265 + (79420) = 110685 (0x01363C est 79420)
    - Et lisez les clusters 0x06BC (= 1724) de manière contiguë
  - Quatrième cycle de données?
    - L'octet suivant est 00, ce qui signifie la fin de l'exécution des données
    - Pour les fichiers très volumineux, les données exécutées elles-mêmes peuvent être stockées en dehors de l'enregistrement MFT!