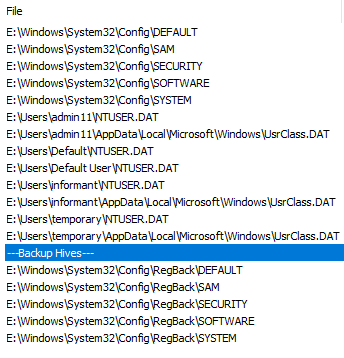
**Windows**



# Security

A check

# Software

Clients

Classes

Microsoft/Windows NT/CurrentVersion : OS Infos

Microsoft/Windows :

# System

CurrentControlSet/Control : Info sur les configurations du pc

# NTUser.DAT

Configuration utilisateur windows

Software :

# AppData/Local

Email, infos users sur des applications

Fichier de cache, paramètres locaux

Données non partagées



# AppData/Roaming

Données « itinérantes » : infos pouvant être synchronisées entre différents ordinateurs

Quick launch : Détermine les applications utilisées

# Technique pour trouver des infos

Recherche :

* Registry windows « terme à trouve”

OSForensics Register Viewer : Parcourir les registres (clic droit add report, info page html)

* Report très intéressant pour convertir les données et afficher toutes les données d’un même dossier

Autopsy : Afficher les bdd facilement, les infos pertinantes

Magic number : <https://www.filesignatures.net/index.php?page=search>

Infos sur les registres : Getadmx.com

# Notes du cours

1.le moyen : quels outils ont permis au cybercrime d’avoir lieu

2.l’opportunité : quels faiblesses ont permis au cybercriminel de commettre le cybercrime

3.la motivation : la raison qui a poussé l’auteur-ricedu cybercrime à le faire

**Authentification :**

lsass.exe (Local Security Authority Subsystem) est un [exécutable](https://fr.wikipedia.org/wiki/Ex%C3%A9cutable) qui est nécessaire pour le bon fonctionnement de [Windows](https://fr.wikipedia.org/wiki/Microsoft_Windows).

Il assure l'identification des utilisateurs (utilisateurs du [domaine](https://fr.wikipedia.org/wiki/Domaine_(informatique)#Le_concept_de_Domaine_chez_Microsoft) ou utilisateurs locaux). Pour [Windows 2000](https://fr.wikipedia.org/wiki/Windows_2000) et les versions postérieures, les utilisateurs du domaine sont identifiés d'après les informations de l'annuaire [Active Directory](https://fr.wikipedia.org/wiki/Active_Directory). Les utilisateurs locaux sont identifiés d'après les informations de la [SAM](https://fr.wikipedia.org/wiki/Security_Account_Manager).

## Collecte

Identifier les données

* Compressées ou non compressées ?
* En direct ou hôte éteint ?

Identifier les paramètres de l’acquisition

* Une partie ou le disque complet ?

Collecte des informations du BIOS

* Particulièrement l’horodatage (stocké dans le RTC/CMOS)

Prenez des photos, plein de photos !

* De l’environnement (l’espace autour)
* Des objets (dommages, rayures, traces)
* Des câbles

Ajouter des étiquettes distinctives pour éviter les doublons

Mémoire vive :

* dump mémoire %WINDIR%\MEMORY.DMP (contient toutes les données présentes en mémoire avant le plantage.)
  + La pile en mémoire: contient les objets et variables créés par un processus.
  + Pile d’exécution (i.e. "callstack") de tous les "threads": on peut savoir précisemment les fonctions qui étaient exécutées au moment du "dump"
  + Blocs de l’environnement des "threads": contient des informations sur les "threads" en cours d’exécution de façon à en connaître l’état et le thread ID.
  + Code assembleur: dans le pire des cas, on peut avoir à lire le code assembleur. Cette solution est généralement trop fastidieuse et trop couteuse. Toutefois en rapprochant le "dump" des fichiers de symboles “PDB”, on peut avoir les piles d’appels par rapport au code source, ce qui est plus facile pour déboguer.
  + Information sur les modules: le processus charge souvent plusieurs assemblies. Le "dump" permet d’avoir des informations sur les dépendances qui ont été chargées notamment la version des assemblies.
* Le fichier hibernation %SystemDrive%\hiberfile.sys
* Le fichier page %SystemDrive%\pagefile.sys (lié à la mémoire virtuelle de votre ordinateur. Il intervient quand vous n’avez plus d’espace disponible en réserve.)

Slack Space: espace libre dans le cluster

* La données précédemment stockée dans le secteur n’était pas écrasée
* Des fragments de fichiers peuvent être trouvés dans les clusters alloués

Remarque : Linux écrase tout l’espace libre avec des octets

## Analyse de malware

Chiffré :

* Un clé par infection
* Déchiffreur constant qui peut être utilisé pour la detection

Polymorphe :

* Créer des décrypteurs distincs
* Insertion de codes mort
* Corps constant qui peut être utilisé pour la détection

Métamorphe :

* Capable de reconnaitre, d’analyser et de muter son propre corps

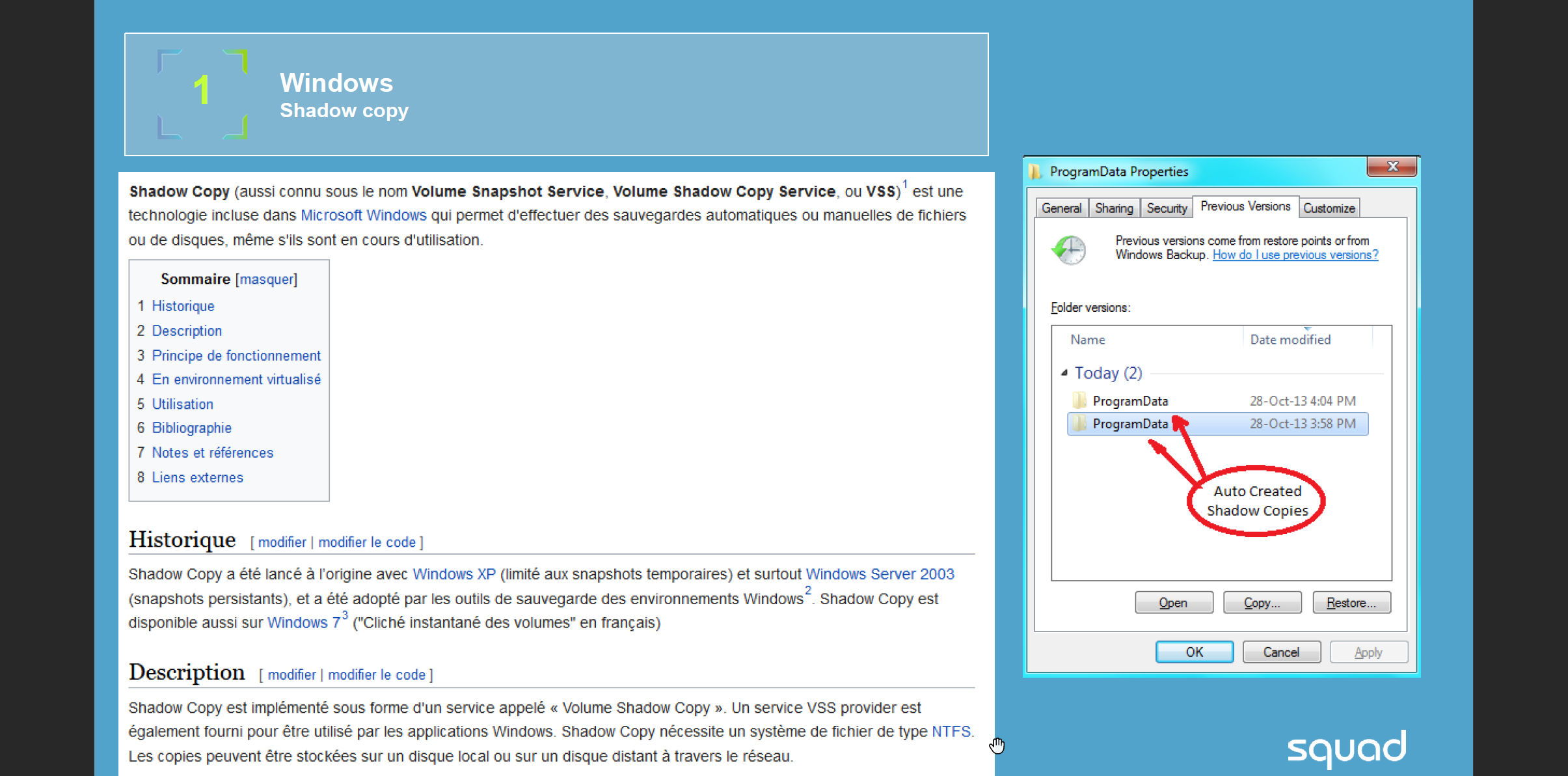
## Windows

Lors de la suppression d’un fichier, Windows se contente de modifier l’index.

BitLocker(permet de chiffrer ces données, une fonctionnalité de protection des données intégrée au système d’exploitation, qui s’attaque aux menaces que constituent le vol ou l’exposition de données provenant des ordinateurs perdus, volés ou mis hors service de façon inappropriée.) :

* Transparent operation mode : Pas authentification lors de la phase pré boot
* User authentication mode : Requiert à l’utilisateur de s’identifier
* USB-Key

Shadow copy permet d’effectuer des sauvegardes automatiques ou manuelles de fichiers ou de disques, même s’ils sont en cours d’utilisation.



## MAC

HFS (Hierarchical file system) :

* Local domain
* System domain
* User domain

## Linux



Fichier .bash\_history est très utile pour comprendre ce qu’il s’est passé.

## Réseau

Wireshark : Clique droit exporter objet « http » pour récupérer les fichiers échangés en clair.

Cyber Kill Chain :

* Reconnaissance : Recherches, identification des cibles
* Weaponization : Préparer les malwares etc
* Delivery : Transmettre l’arme à la cible
* Exploitation : Activation du code malicieux
* Installation : Mise en place d’une backdoor
* Command & control : Communiquer à distance avec l’arme
* Actions on objctive : L’attaquant cherche à réaliser son objectif

## Terminaux mobiles

Grandes richesses d’informations.

Comme tous ces équipements n’ont pas forcément d’outils inforensique associés, l’investigateur-rice doit toujours tester l’outil inforensique qu’il utilise avant son utilisation dans le cadre de l’investigation.

Utiliser une cage de faraday à la perquisition.

Analyse statique :

* Secrets codés en dur
* Cryptographie utilisé
* Les hôtes distants avec qui ça communique
* Les certificats
* La détection d’une action en root ou qui essaie de modifier le système du smartphone
* Les accès au système de fichier ou aux bases de données
* Les interceptions de schémas d’URL

## Conseils

Garder la trace de vos actions pour exclure/expliquer les preuves liés à vos actions durant l’acquisition.

Préserver au mieux l’intégrité de la mémoire (write blocker)

Il n’y a pas de solution idéale. Il est recommandé de favoriser la collecte en direct machine allumée.

# Cas d’usage

## Investigation en ligne

Des outils de hacking ont été détectés par l’antivirus sur un poste utilisateur. L’utilisateur a remonté qu’il n’était pas au courant. Pourtant les outils étant dans son répertoire de téléchargement, c’est très anormal que ça a été fait à son insu. Afin de gagner du temps au lieu de lancer une longue investigation, l’utilisateur a été appelé au téléphone et après lui avoir expliqué qu’il était préférable qu’il nous dise la vérité plutôt que l’investigation nous indique que c’est bien lui qui a téléchargé ces outils. Il a fini par avouer que c’était bien lui. Nous avons pu ainsi gagner du temps et simplement le réprimander afin qu’il ne renouvelle pas l’expérience.

* Faire pression sur l’utilisateur

Une utilisatrice nous a remonté des mouvements de souris étranges, un peu comme si quelqu’un avait pris le contrôle de son PC. Après une première analyse, rien de suspect n’était présent dans les traces de la machine. Après une longue conversation avec l’utilisatrice, en prenant le temps de lui expliquer qu’il est rare qu’un utilisateur se rende compte qu’il s’est fait piraté dans les attaques actuelles, nous avons fini par comprendre que l’utilisatrice avait des craintes côté personnel à cause de son ex-conjoint. Comme elle n’a pas accès à des informations sensibles pour le client, nous avons clos l’investigation en lui indiquant de nous recontacter si ça se reproduit. C’était probablement la touche Alt ou Ctrl qui était bloqué et a affiché des choses inhabituelles.

* Les attaques sont invisibles pour l’utilisateur

Le PC portable professionnel d’un utilisateur a été infecté par un rançongiciel durant le confinement. Il n’avait pas effectué de backup car la sauvegarde automatique n’est pas active pour les personnes en télétravail. Il n’y avait pas d’outils de déchiffrement proposés pour ce malware. Heureusement, une partie du code du malware a été retrouvée sur GitHub, dont sa clé en dur qui était présente dans une ancienne version, ce qui a permis de déchiffrer les fichiers.

* Vérifier si le code du rançongiciel existe, trouver une potentielle clé

Un smartphone est infecté par une application malveillante qui est complexe à analyser car elle a obfusqué son code. Une ancienne version de l’application a été trouvé sur un site stockant des applications Android. Cette ancienne version n’était pas obfusquée, ainsi l’analyse du code malveillant de l’application actuelle a été simplifiée.

* Vérifier s’il exite une ancienne version de l’app

## Photo et vidéo

Un client recherche une taupe en son sein qui alimente un blog d’un avocat anglais diffusant des scandales à son sujet. La première vague de l’investigation sur les postes des suspectés ne donne rien alors le périmètre est élargi et les tablettes professionnelles sont également analysés. Une vidéo effacée est retrouvée sur une tablette où l’on voit une personnalité politique filmé en douce durant une réunion. Il n’a pas été prouvé que cet employé avait un lien avec l’affaire mais il a été licencié pour non-respect du règlement intérieur.

* Elargir le périmètre au maximum : pc, tablettes, portables, etc

Une investigation sur une intrusion numérique indique qu’il y a des connexions non-identifiées depuis une des caméras de surveillance vers des serveurs en interne. L’analyse des caméras de surveillance a permis d’identifier qu’une faille est présente sur celles-ci qui permet de prendre la main en tant que root sans besoin d’être identifié. Le prix d’une analyse inforensique de la centaine de caméra étant trop élevé, il a été décidé de mettre à jour les caméras sans avoir pu identifier l’attaquant qui a utilisé les caméras comme rebond.

* Patcher les failles, si l’analyse est trop cher ou l’attaque sans conséquence c’est ok de ne pas la faire

## Windows

Suite à un incident, une société est sollicité pour établir un diagnostic puis une autre pour une opération d’éviction.

* Faire évaluer les résultats pour un professionnel

Man in the middle.

## Linux

Vulnérabilité sur un serveur apache.

* Comment détecter l’exploitation de cette vulnérabilité ?

1.En observant l’horodate des requêtes POST sur cette URI (mais on n’a pas le contenu de la requête POST dans les logs)

2.En observant un nombre anormal de requête vers cette URI

3.En lisant le fichier .bash\_history(s’il existe) de l’utilisateur faisant tourner le service

Il est également possible d’obtenir les informations suivantes :

4.L’adresse IP source de la requête d’exploitation est disponible dans les logs du serveur web

5.L’écoute du trafic réseau depuis cette machine ou l’analyse des sockets ouvertes peut permettre d’identifier si un flux C&C est en cours vers l’attaquant

6.L’analyse des logs du pare-feu du serveur peut permettre d’identifier la première connexion vers l’attaquant

7.La liste des fichiers modifiés ces derniers jours et la consultation de leurs contenus peut donner des indices sur le déroulement de la post-exploitation

## Réseau

Une connexion sur un site malveillant a été détectée par une sonde chez une filiale du client. Après analyse du JavaScript offusqué, il s’avérait que le site d’un important vendeur d’électroménager était compromis et redirigeait sur des sites malveillants. Le propriétaire du site a été informé.

* Informer le propriétaire

Un scan interne est détecté, c’est-à-dire qu’une machine du client semble scanner un serveur du client. L’investigation a permis de confirmer que ce n’était pas un scan malveillant mais que c’était un produit utilisé par le client qui effectue un balayage réseau lors de son exécution.

Une alerte du SIEM a sonné concernant un scan du compte sa sur SQL. L’investigation a permis de comprendre que c’était un faux-positif lié à une sauvegarde d’un fichier de journalisation des connexions SQL qui est passé sur le même port TCP que les connexions SQL. Ainsi, les nombreuses connexions vues en peu de temps étaient en fait le contenu du fichier de journalisation lors de son transit.

Une alerte a été remontée par l’IDS local sur un serveur. Après analyse, c’était un faux-positif car elle concernait une application non-présente sur le serveur. Cependant cela nous a fait découvrir que ce serveur présentait des services en frontal sur Internet alors que le client l’ignorait. Un scan de vulnérabilité a été demandé et a révélé des vulnérabilités potentielles. Une investigation dans les logs du serveur a permis de valider qu’aucun attaquant n’a exploité ces vulnérabilités.

* Réaliser une investigation. En fonction des résultats, patcher les failles

Un callback vers un site malveillant a été détecté par une sonde. L’analyse des traces forensique remontées par un outil en interne a permis de trouver le processus initiant cette connexion. Le programme malveillant était lancé au démarrage et consistait à lancer un script autoIT offusqué qu’il a fallu analyser à la main car il avait des mécanismes de détection de machine virtuelle. Le malware a été envoyé à une compagnie d’antivirus.

* Envoyer le malware à une compagnie d’anti virus pour l’analyser

## Terminaux mobiles

Un outil de hacking a été détecté sur un poste d’un utilisateur qui n’a pas de numéro de téléphone dans l’annuaire. L’utilisateur ne répondant pas aux mails, j’ai appelé un par un les gens du même service que lui pour finir par trouver quelqu’un connaissant cet utilisateur et pouvant nous fournir son numéro de téléphone. Il s’avérait en fait que l’utilisateur n’était pas du tout IT-friendlyet que le poste était partagé par plusieurs personnes. A l’aide d’un rapport issu du SIEM, les autres utilisateurs de ce poste ont été retrouvés et avertis.

* Faire attention aux personnes qui utilisent le même ordinateur

Une application smartphone basée sur le volontariat permet aux employé-esdu client de déclarer s’ils ont le Covid-19 afin d’identifier et prévenir les personnes qui étaient dans le bâtiment en même temps. De nombreux évènements se sont retrouvés injectés et après analyse il s’avérait que la décompilation de l’application permettait de comprendre rapidement que l’authentifiant était basé sur le numéro de badge qu’il était facile de brute-forcer.

* Utiliser un fort niveau de hash pour l’authentifiant ou des données plus compliquées

## Megacorp

### Road Map

Localiser le document (effacé ?) :

* Acquisition : Disque dur acquis avec une clé USB bootable
* Montage de l’image
* Constatation simple :
  + Répertoire perso
  + Recycle-bin
  + Find
* Autopsy : permet de connaître les fichiers supprimés

Trace du document trouvé (Est-ce vraiment le bon ? .lnk != .xlxs) :

* Grep : trouver un lien avec le document (trace avec edge)
* MRU (Most recently used) : liste des fichiers utilisés récemment (présent dans NTUSER.DAT)
  + Leads.xlxs a été ouvert récemment
* Cache de microsoft egde : fichier webcacheV01.dat stocke la plupart de la navigation internet
  + Check si le fichier/bdd est corrumpu
  + Recherche du fichier .htm en lien avec leads
* Heure entre l’ouverture du document et l’accès à l’intranet concorde

Technical\_plan ?

* Récupérer les images effacées : Thumbchache viewer
* Vérification du volume D
  + .lnk sont crées quand une appli ouvre un fichier, Peuvent contenir le path du fichier
  + Vérification pour le document leads
  + Récupération du maximum d’informations en lien avec la clé (nom, numéro de série, code vendeur, code produit, horodatage, etc)

Explorer la clé usb :

* Trouver des infos intéressantes :
  + Dmesg (mémoire tampon de message du noyau)
  + Lsusb -D (affiche USB buses and devices that are attached to them)
* File carving : réassemble les documents depuis des fragments

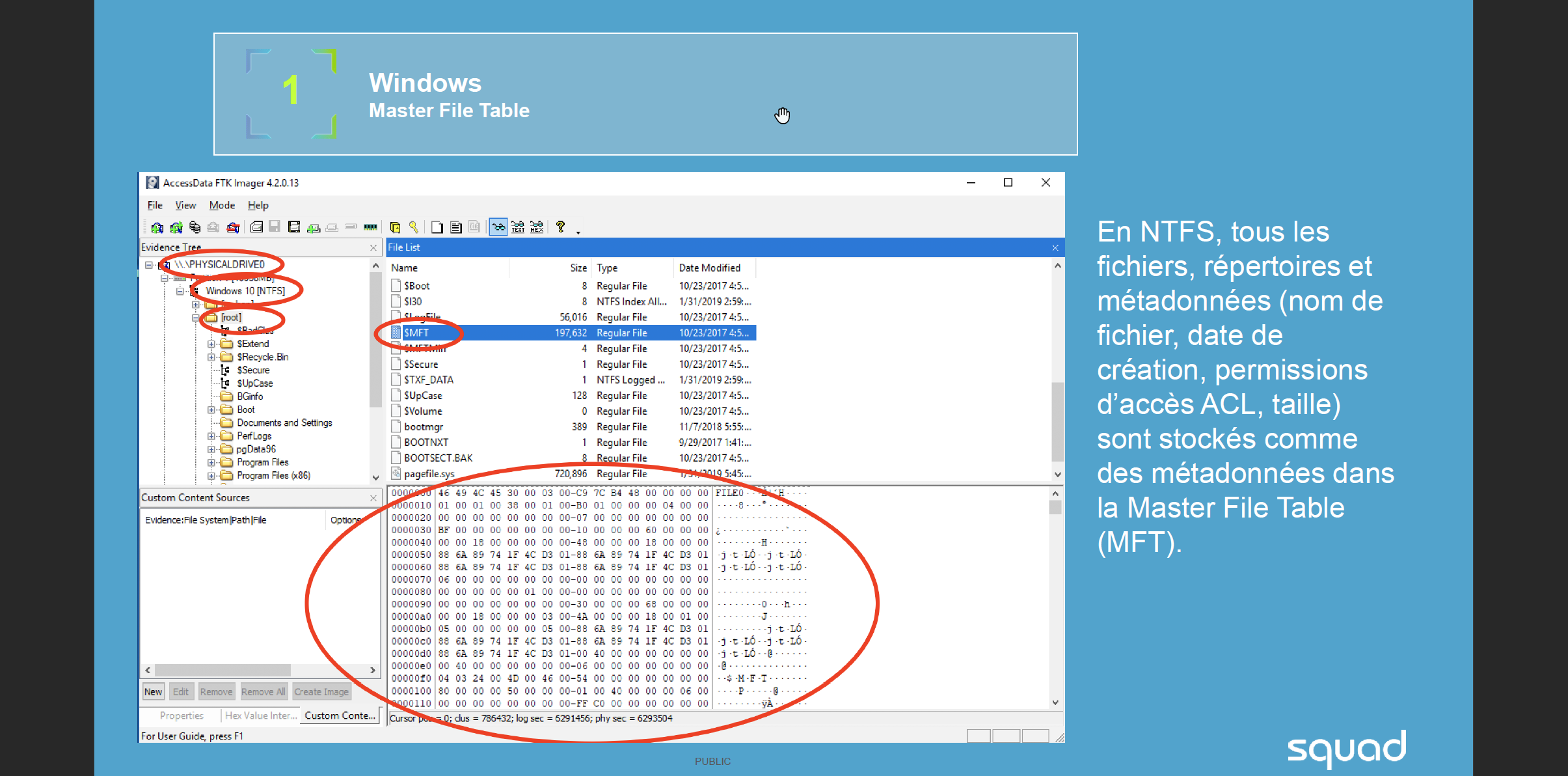
Vérifier l’identité de la personne :

* Logs windows (.evt ou .evtx) : script evtx\_dump.py
* Check les events d’authentification
* Traces wifi (registre software, networklist/profiles)

### A retenir

Il y a plusieurs façons de restaurer un fichier effacé :

* Explorer la MFT (Master file table = chaque fichier est enregistré avec certains infos : nom, taille, etc)



* Faire une recherche avec la méthode de file carving.
* Pour les images uniquement : regarder dans «Thumbs.db» ou «Thumbcache»

Il y a plusieurs façons de trouver des traces d’utilisation de fichiers

* Regarder dans Internet Explorer le fichier «Index.dat» («Webcache» pour Edge)
* Regarder dans la base de registre pour le MRU (Most RecentlyUsed)
* Faire un grep sur le nom de fichier…

## Evaluer le niveau de sécurité d’un client

Si [www.xxx](http://www.xxx), on peut attaquer les sous réseau AAAA.www.xxx

Reconnaissances :

* Comprendre la cible
* Identifier les points d’entrées
* Identifier les communications clefs

Attaque :

* Sqlmap : injection sql

Exploitation :

* Trouver des vulnérabilités exploitables
* Exploitation et post-exploitation si validé par le client

Reverse shell : Un reverse shell consiste à configurer le shell pour s'exécuter (en général en mode silencieux, sans avertir l'utilisateur de l'ordinateur) en acceptant en entrée des commandes qu'il va lui-même récupérer depuis un système distant et en redirigeant sa sortie vers ce même système ; par ce moyen, l'opérateur du système distant est en mesure d'utiliser l'ordinateur local comme s'il était présent physiquement à ses commandes

Post-Exploitation :

* Récupérer des identifiants et mots de passe réutilisables
* Elévation de privilège
* Utilisation de la machine compromise comme rebond pour entrer plus profondément dans le réseau