TP1 : Découverte des artefacts Windows- Corrigé

1 Identification

1.1 : Dans la ruche SYSTEM, récupérez le nom de l'ordinateur.

HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName : MARCEL-PC

1.2 : Déterminer également si la machine appartient à un domaine et si oui, lequel (SYSTEM\CurrentControlSet\Services\TcpIp\Parameters).

RegistryExplorer Bookmark : Services

La valeur Domain n'a pas de valeur : Aucun domaine.

1.3 : Toujours dans la clef Tcpip, profitez-en pour relever l'adresse IP de la machine lors de sa dernière connexion, l'adresse de sa passerelle par défaut et de son serveur DNS

RegistryExplorer Bookmark : Services

IP : 192.168.1.123 / Gateway : 192.168.1.203 / DNS : 192.168.1.198

1.4 : Dans la ruche SOFTWARE cette fois, trouvez la version complète du système (vous aurez besoin de deux valeurs).

RegistryExplorer Bookmark : CurrentVersion

HKLM\SOFTWARE\Mirosoft\Windows NT\CurrentVersion[ProductName] : Windows 10 Home / [DisplayVersion] : 22H2

1.5 : Profitez-en pour relever également la date d'installation (dans un format lisible par un humain).

HKLM\SOFTWARE\Mirosoft\Windows NT\CurrentVersion[InstallDate] : 1704456688

HKLM\SOFTWARE\Mirosoft\Windows NT\CurrentVersion[InstallTime] : 133489302882920370

Le premier est un timestamp Unix, le second un timestamp Windows. On peut les convertir en date avec, par exemple, Cyberchef : https://gchq.github.io/CyberChef/#recipe=Windows_Filetime_to_UNIX_Timestamp('Seconds%20(s)','Decimal')From_UNIX_Timestamp('Seconds%20(s)')

Soit Fri Jan 05 2024 12:11:28.

1.6 : En parlant de date, revenez dans SYSTEM, sous CurrentControlSet\Control, et identifiez la timezone du système (par rapport à UTC).

HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation.

Timezone = UTC – Bias, soit UTC – (-60), soit UTC+1

1.7 : Prenez connaissance de la SAM et listez les comptes locaux présents sur le système.

SAM\Domains\Account\Users\Names :

- Administrateur
- Default Account
- Filip
- Invité
- Marcel
- WDAGUtilityAccount

1.8 : Quand les comptes de Filip et Marcel ont-il été créés ? De quand date leur dernière connexion au système ?

Marcel : créé le 2024-01-05 12:09:58, dernière connexion le 2024-01-12 11:46:50

Filip : créé le 2024-01-12 09:16:37, dernière connexion le 2024-01-12 11:23:24

2. Authentification

2.1 En utilisant l'outil de votre choix, parsez ou ouvrez le fichier Security.evtx. Filtrez uniquement les événements 4624. Combien y en a-t-il ?

EvtxeCmd, extx_dump, plaso, ou autre donne le même résultat : 638 événements 4624.

```
forensics@forensics:~/Forensics/TP1/Marcel-PC/Evtx$ evtx_parse Security.evtx | rg 'event_id":4624' | wc
    638    1891  559528
```

2.2 A quoi correspondent ces événements ? Expliquez la différence entre le SubjectUserName et le TargetUserName.

Les événements 4624 enregistrent les authentifications réussies sur le système. Le SubjectUserName est le compte réalisant l'authentification, le TargetUserName est le compte avec lequel il s'authentifie (le compte cible, celui dont les droits et privilèges seront appliqués).

2.3 Quel utilisateur s'est authentifié le 5 janvier à 12:11:47 ? Notez le type d'authentification réalisée et expliquez à quoi il correspond.

Marcel. Type 2 : ouverture de session interactive (l'utilisateur s'est connecté manuellement).

```
forensics@forensics:~/Forensics/TP1/Marcel-PC/Evtx$ evtx_parse Security.evtx | rg 'time":"2024-01-05T12:11:47.*event_id":4624' |jq
-c '[.event_data.TargetUserName, .event_data.LogonType]'
["Marcel",2]
["Marcel",2]
```

2.4 Combien de fois et à quelle heure s'est authentifié l'utilisateur Filip ? Notez à chaque fois le type de connexion.

Trois fois :

Date	Type
2024-01-12T09:23:44	2
2024-01-12T11:06:47	2
2024-01-12T11:23:24	2

```
forensics@forensics:~/Forensics/TP1/Marcel-PC/Evtx$ evtx_parse Security.evtx |jq -c '[.time, .event_id, .event_data.TargetUserName,
 .event_data.LogonType]' | rg '4624.*Filip'
["2024-01-12T09:23:44.324006Z",4624,"Filip",2]
["2024-01-12T11:06:47.484913Z",4624,"Filip",2]
["2024-01-12T11:23:24.972600Z",4624,"Filip",2]
```

2.5 Parsez ou ouvrez le fichier `Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx`. Filtrez les événements pour ne garder que les ID 21, 24 et 25. A quoi correspondent-ils ?

- 21 : Ouverture de session RDP
- 24 : Fermeture de session RDP
- 25 : Reconnexion à une session existante

2.6 Relevez les timestamps des événements 21 qui concernent Filip ; sont-ils cohérents avec votre réponse en 2.4 ?

Oui, parfois à une seconde près :

Date
2024-01-12T09:23:45
2024-01-12T11:06:47
2024-01-12T11:23:25

```
forensics@forensics:~/Forensics/TP1/Marcel-PC/Evtx$ evtx_parse Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.
evtx |jq -c '[.time, .event_id, .user_data.User]' | rg '21.*Filip'
["2024-01-12T09:23:45.157754Z",21,"MARCEL-PC\\Filip"]
["2024-01-12T11:06:47.734323Z",21,"MARCEL-PC\\Filip"]
["2024-01-12T11:23:25.463702Z",21,"MARCEL-PC\\Filip"]
```

2.7 D'après la documentation qu'on peut trouver en ligne, que signifie le champ Address ? Quelle est sa valeur pour les événements associés à Filip ?

Il s'agit de l'adresse source de la connexion RDP. La valeur est LOCAL pour les trois événements.

```
forensics@forensics:~/Forensics/TP1/Marcel-PC/Evtx$ evtx_parse Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.
evtx |jq -c '[.time, .event_id, .user_data.User, .user_data.Address]' | rg '21.*Filip'
["2024-01-12T09:23:45.157754Z",21,"MARCEL-PC\\Filip","LOCAL"]
["2024-01-12T11:06:47.734323Z",21,"MARCEL-PC\\Filip","LOCAL"]
["2024-01-12T11:23:25.463702Z",21,"MARCEL-PC\\Filip","LOCAL"]
```

2.8 A votre avis, que peut-on en déduire concernant les authentifications de Filip ?

Ce sont des authentifications locales, et non des authentifications via RDP.

2.9 En analysant les événements 21, 25 et 24 du même journal, établissez les heures de début et de fin de la dernière session de Filip.

Début	Fin
2024-01-12T11:23:25	2024-01-12T11:46:45

```
forensics@forensics:~/Forensics/TP1/Marcel-PC/Evtx$ evtx_parse Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.
evtx |jq -c '[.time, .event_id, .user_data.User]' | rg ',2[154].*Filip' | tail -n 2 |jsonl
["2024-01-12T11:23:25.463702Z",21,"MARCEL-PC\\Filip"]
["2024-01-12T11:46:45.249428Z",24,"MARCEL-PC\\Filip"]
```

3. Artefacts de navigation

3.1 Malheureusement, il semble que le répertoire de la collecte contenant les profils Firefox ne contient pas l'historique de navigation de Filip. Néanmoins, les données du cache du navigateur sont bien présentes et peuvent fournir des informations. En vous aidant des résultats de plaso, trouvez l'URL relative à la société de Filip qu'il a consulté, et l'heure à laquelle il s'y est connecté.

On liste dans un premier temps les types de fichiers, ce qui correspond aux colonnes 3 et 4 de la timeline :

```
forensics@forensics:~/Forensics/TP1$ cut -d',' -f3,4 Marcel.csv |sort -ur
WEBHIST,Firefox Cache
source,source_long
REG,Winlogon Registry Key
REG,UserAssist Registry Key
REG,User Account Information Registry Key
REG,USBStor Registry Key
```

On peut maintenant plus facilement faire notre recherche en ciblant le WEBHIST. On cherche une URL en lien avec ECORP :

```
forensics@forensics:~/Forensics/TP1$ rg -iN 'Last Visited.*WEBHIST.*ecorp' Marcel.csv
2024-01-12T09:26:30.000000+00:00,Last Visited Time,WEBHIST,Firefox Cache,Fetched 2 time(s) "~predictor-origin :http://netscaler.ecorp.com/",firefox_cache2,OS:/home/qbrs2968/Work/ESGI/TP1/Marcel-Desktop/Firefox/Profiles/ce8duxqs.default-release/cache2/entries/75B875F52F7E8A0C1B04BF32125D2A4E8F7A4486,-
2024-01-12T09:26:30.000000+00:00,Last Visited Time,WEBHIST,Firefox Cache,Fetched 1 time(s) [HTTP/1.1 200 OK] GET "O^partitionKey=%28http%2Cecorp.com%29 :http://netscaler.ecorp.com/web_images/bg.png",firefox_cache2,OS:/home/qbrs2968/Work/ESGI/TP1/Marcel-Desktop/Firefox/Profiles/ce8duxqs.default-release/cache2/entries/79DB04DDED021D795395D218E0D8C7C6030B18A1,-
2024-01-12T09:26:30.000000+00:00,Last Visited Time,WEBHIST,Firefox Cache,Fetched 1 time(s) [HTTP/1.1 200 OK] GET "O^partitionKey=%28http%2Cecorp.com%29 :http://netscaler.ecorp.com/web_images/icon.png",firefox_cache2,OS:/home/qbrs2968/Work/ESGI/TP1/Marcel-Desktop/Firefox/Profiles/ce8duxqs.default-release/cache2/entries/B00413E18B40F36030126752A2339C5F2AF0DD84,-
```

https://netscaler.ecorp.com, à 2024-01-12T09:26:30

3.2 L'URL est assez évocatrice. A votre avis, de quel service s'agit-il et pourquoi Filip s'y serait connecté ?

Filip s'est connecté au VPN SSL de son entreprise pour accéder au réseau local de cette dernière.

4. Activités liées aux fichiers

4.1 En utilisant ShellBagsExplorer ou en analysant la sortie plaso, retrouver les entrées ShellBags de Filip présentes dans les bases de registre NTUSER.DAT et UsrClass.dat. Quelle est l'adresse du partage réseau que Filip a visité à 9h29 ? Est-il raisonnable de penser que cette adresse ne fait pas partie du réseau local de Filip ?

Adresse : 10.1.0.5. D'après la réponse à la question 1.4, le réseau local de Filip semble plutôt être 192.168.1.0/24. Il est donc raisonnable de penser que cette adresse n'en fait pas partie (sans compter qu'il est plutôt rare de trouver une adresse en 10.X.X.X chez un particulier).

4.2 Un répertoire lié à une application semble avoir été consulté à plusieurs reprise. Quel est son nom complet ?

Adobe Photoshop 2024 v25.2.0.196

4.3 Dans RegistryExplorer, ouvrez la base NTUSER.DAT et consultez les entrées RecentDocs (`SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`). Une archive semble avoir été ouverte : laquelle, et à quelle heure ?

Adobe Photoshop 2024 v25.2.0.196.zip, à 2024-01-12 11:36:53

4.4 En analysant la $MFT, retrouver l'heure à laquelle cette archive a été déposée sur le système, et son chemin complet.

On regarde le timestamp de création et l'attribut FILENAME pour être bien sûr de la date de création :

```
forensics@forensics:~/Forensics/TP1/Marcel-PC/FileSystem$ rg 'Adobe Photoshop 2024 v25.2.0.196.zip' MFT.csv
1076283:2024-01-12T10:07:36Z,4674420736,..c.,,0,0,109937-128-1,"/Users/Filip/Desktop/Adobe Photoshop 2024 v25.2.0.196.zip"
1237215:2024-01-12T10:57:29Z,4674420736,...b,,0,0,109937-128-1,"/Users/Filip/Desktop/Adobe Photoshop 2024 v25.2.0.196.zip"
1237216:2024-01-12T10:57:29Z,4674420736,macb,,0,0,109937-48-2,"/Users/Filip/Desktop/Adobe Photoshop 2024 v25.2.0.196.zip ($FILE_NAM
E)"
1307319:2024-01-12T11:36:53Z,4674420736,ma..,,0,0,109937-128-1,"/Users/Filip/Desktop/Adobe Photoshop 2024 v25.2.0.196.zip"
```

2024-01-12T10:57:29 - C:\Users\Filip\Desktop\Adobe Photoshop 2024 v25.2.0.196.zip

4.5 Un binaire suspect est présent dans cette archive. Retrouver son chemin et l'heure à laquelle il a été extrait de l'archive.

Plusieurs possibilités. On peut chercher les exécutables créés après l'apparition de l'archive, ou simplement se dire que le répertoire extrait a probablement le même nom que l'archive.

```
forensics@forensics:~/Forensics/TP1$ rg -N '2024-01-12T.*Adobe.*\.exe' Marcel-PC/FileSystem/MFT.csv | less
```

Après analyse, on peut identifier les fichiers suivants (on ne garde que le FILE_NAME puisqu'on veut des dates de création):

```
forensics@forensics:~/Forensics/TP1$ rg -N '2024-01-12T.*Adobe.*Crack\.exe.*FILE_NAME' Marcel-PC/FileSystem/MFT.csv
2024-01-12T11:08:24Z,0,macb,,0,0,141168-48-2,"/$Recycle.Bin/S-1-5-21-1602562492-3974572016-3261653425-1001/$RDIO5MA.196/Adobe Photo
shop 2024 v25.2.0.196/Crack.exe ($FILE_NAME)"
2024-01-12T11:10:40Z,0,macb,,0,0,309263-48-2,"/Users/Filip/Desktop/Adobe Photoshop 2024 v25.2.0.196/Adobe Photoshop 2024 v25.2.0.19
6/Crack.exe ($FILE_NAME)"
2024-01-12T11:37:01Z,0,macb,,0,0,93590-48-2,"/Users/Filip/Desktop/Adobe Photoshop 2024 v25.2.0.196/Crack.exe ($FILE_NAME)"
```

4.6 Ce binaire a pu être récupéré sur le PC, et son SHA256 est le suivant : `94fca89e71f396bf1fd8f97ab027d6f64d443f6e3b8bc6ff259604401f78416b`. De quel type de binaire s'agit-il ?

D'après Virus Total et Malware Bazaar, il s'agit d'un variant de RedlineStealer, un infostealer (malware dédié à la récupération de mots de passe et de donnés sensibles).

https://www.virustotal.com/gui/file/94fca89e71f396bf1fd8f97ab027d6f64d443f6e3b8bc6ff259604401f78416b

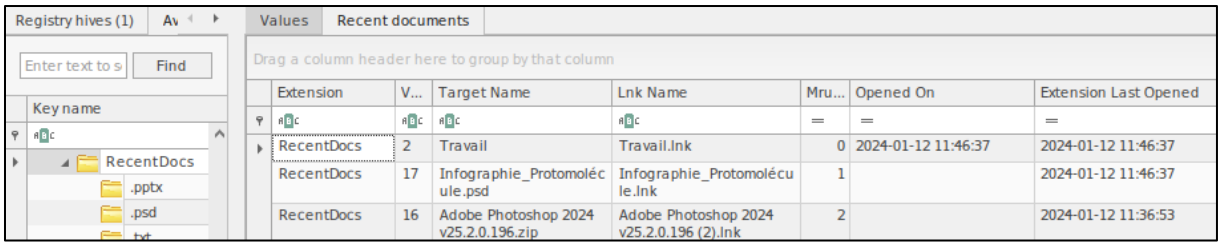
4.7 En analysant les entrées UserAssist, lister les dates d'exécution de ce binaire par Filip.

En allant regarder les UserAssist dans RegistryExplorer ou dans la timeline, on trouve :

Date	Binaire
2024-01-12T11:36:40	C:\Users\Filip\Desktop\Adobe Photoshop 2024 v25.2.0.196\Adobe Photoshop 2024 v25.2.0.196\Crack.exe
2024-01-12T11:40:16	C:\Users\Filip\Desktop\Adobe Photoshop 2024 v25.2.0.196\Crack.exe

4.8 Intéressez-vous à la clef RecentDocs de NTUSER.DAT. Quel fichier a été ouvert avec l'application installée par Filip peu après l'exécution du malware ?

D'après les entrées RecentDocs associées à l'extension `.psd`, il s'agit d'un fichier nommé Infographie_Protomolécule.psd.



4.9 D'après ces informations, pensez-vous que la compromission du poste par Filip était volontaire ? Quelles informations importantes et concernant la société de Filip ont potentiellement été récupérées par le malware ?

Visiblement non, Filip a simplement voulu installer une version crackée de Photoshop pour travailler. En revanche, puisque Filip s'est connecté au site netscaler.ecorp.com, il est possible que les identifiants de connexion de Filip aient été dérobées.

Bonus

Trouvez (et prouvez !) comment l'archive a été déposée sur le PC, en donnant un maximum d'informations (timestamps et données précises utiles à une investigation).

Déposée par la clef USB SanDisk Cruzer Blade insérée vers 10h56.

En corrélant :

- Les ShellBags
- Les clefs Mountpoints2 de NTUSER.DAT
- Les événements 142 de Microsoft-Windows-Ntfs

On peut prouver que la clef SanDisk a bien été branchée avant l'apparition de l'archive sur le système, et qu'elle contenait un répertoire portant le même nom. Elle est donc vraisemblablement le moyen par lequel l'archive a été déposée sur le système.

Retrouver le contenu du fichier README.txt qui était dans l'archive malveillante.

Le fichier est un fichier résident de la $MFT. Son contenu est donc facilement accessible dans son attribut $DATA. Aidez vous du TP3 pour la démarche précise.