



4e Rendez-vous 4n6s

26 Mai 2020

Cyril Texier Ministère de l'Intérieur

Jean-Philippe Noat Sr Directeur du training international chez Cellebrite

Format des rendez-vous

- Votre rendez-vous d'échange
- Proposer les sujets qui vous intéressent
- Poser des questions techniques, si toutes ne peuvent être répondues elles le seront lors du prochain rendez-vous.
- Faites vous plaisir et échangez
- Mettre l'humain au coeur de la technique
- N'hésitez pas à présenter un sujet si vous le souhaitez



Que faire en cas de pépin ?

En cas de perturbation technique :

mon portable +33 6 08 98 08 94

Pour toute question sur le thème (et les thèmes à venir)

jean-philippe.noat@cellebrite.com

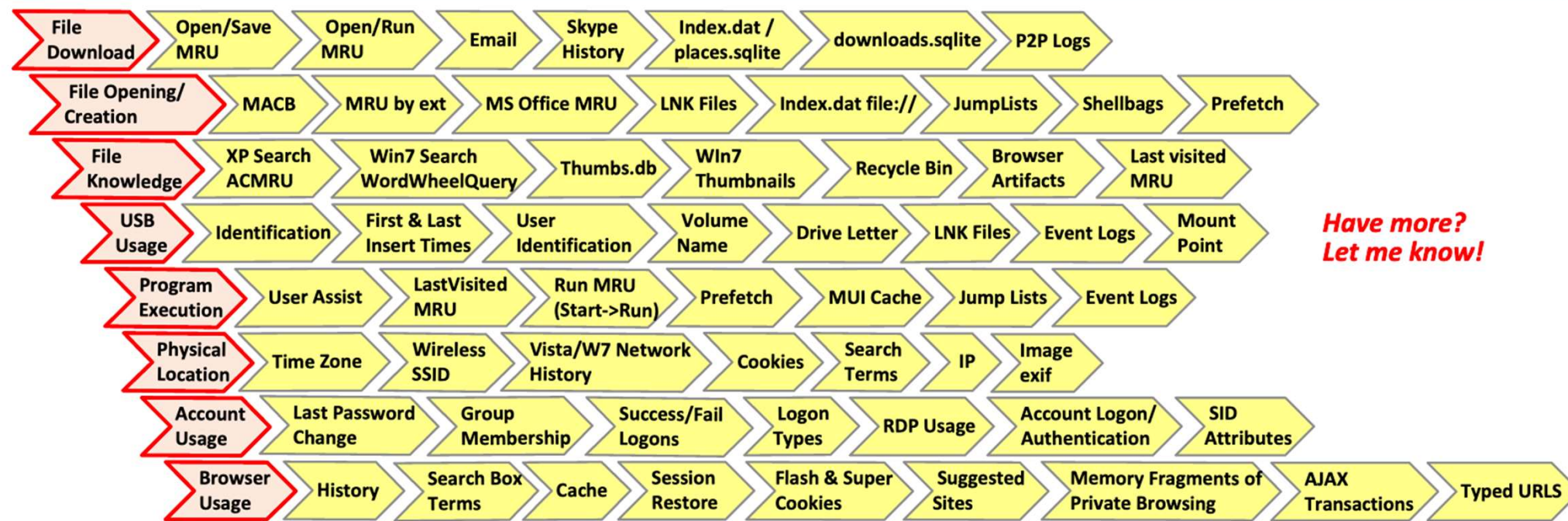
Rdv cet après-midi :

<https://www.cellebrite.com/fr/webinaires/pa-7-33-les-nouveautes/>

Le Graal de l'investigateur cyber : Le Timeline

- Mal supporté par les outils jusqu'à présent
- X-Ways (impossible d'être exhaustif)
- IEF/Axiom (dates erronées, voir les éléments effacés)
- Encase : peu ou pas d'option de tri exhaustive
- Impossible à faire à chaud (réponse sur incident)
- Des outils existent en ligne de commande :
log2timeline / plaso mais installation délicate et les
nouveaux artifacts ne sont pas supportés

Quels événements prendre en compte



Installation Plaso / Log2timeline

<https://plaso.readthedocs.io/en/latest/sourceuser/Users-Guide.html#installing-the-packaged-release>

Disponible uniquement en version Docker /
Ubuntu / Mac / Fedora



Installation

<https://plaso.readthedocs.io/en/latest/sourceuser/MacOS-Source-Release.html>

N'a jamais fonctionné correctement pour moi

La solution : <https://tsurugi-linux.org/>



Log2Timeline

SINGLE OR SPLIT IMAGE (2 options):

```
# mount_ewf.py image.E01 /mnt/ewf  
or  
# ewfmount image.E01 /mnt/ewf/
```

Not
Needed
For 7-A

```
# mount -t ntfs -o ro,loop,show_sys_files,streams_interface=windows,  
offset=#### /mnt/ewf/<image> /mnt/windows_mount/
```

MOUNT TO MOUNT POINT

SINGLE IMAGE

```
# mount -t ntfs -o ro,loop,show_sys_files,streams_interface=windows,offset=#### image.dd /mnt/windows_mount/
```


Etapes de creation du supertimeline

Log2timeline

Outil ligne de commande pour extraire les événements de fichiers individuels ou de répertoires (points de montage). Log2timeline crée un fichier plaso qui doit être ensuite analysé avec les outils pinfo ou psort

Pinfo

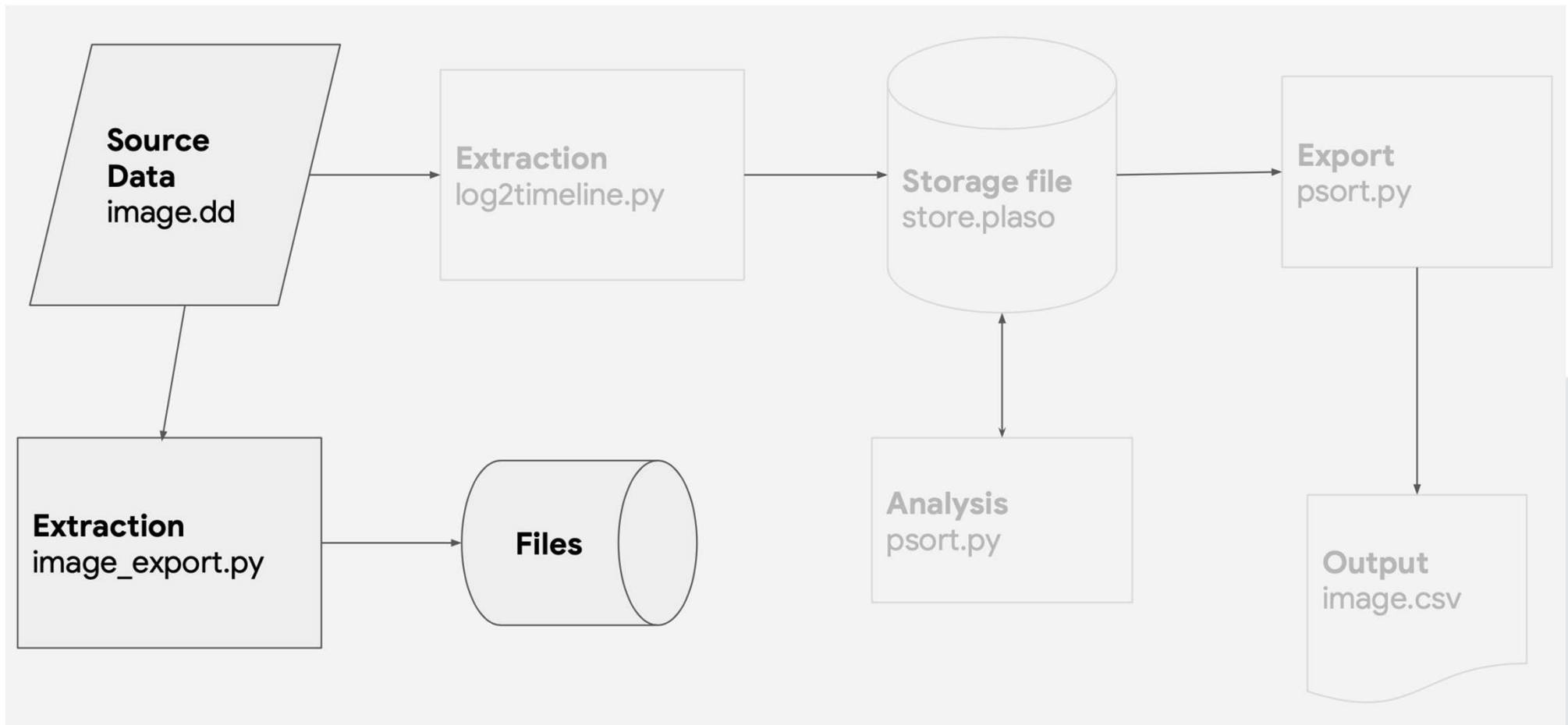
Information à d'un fichier plaso

Psort outil pour post processer un fichier plaso (filtres, tris, analyses automatique)

Psteal (le tout en un)

```
psteal.py --source ~/cases/greendale/registrar.dd -o l2tcsv -w /tmp/registrar.csv
```

Etapes de création du supertimeline



Visualisation des résultats : timesketch

Outil open source

Analyse de timeline et ingestion de données en provenance de Plaso

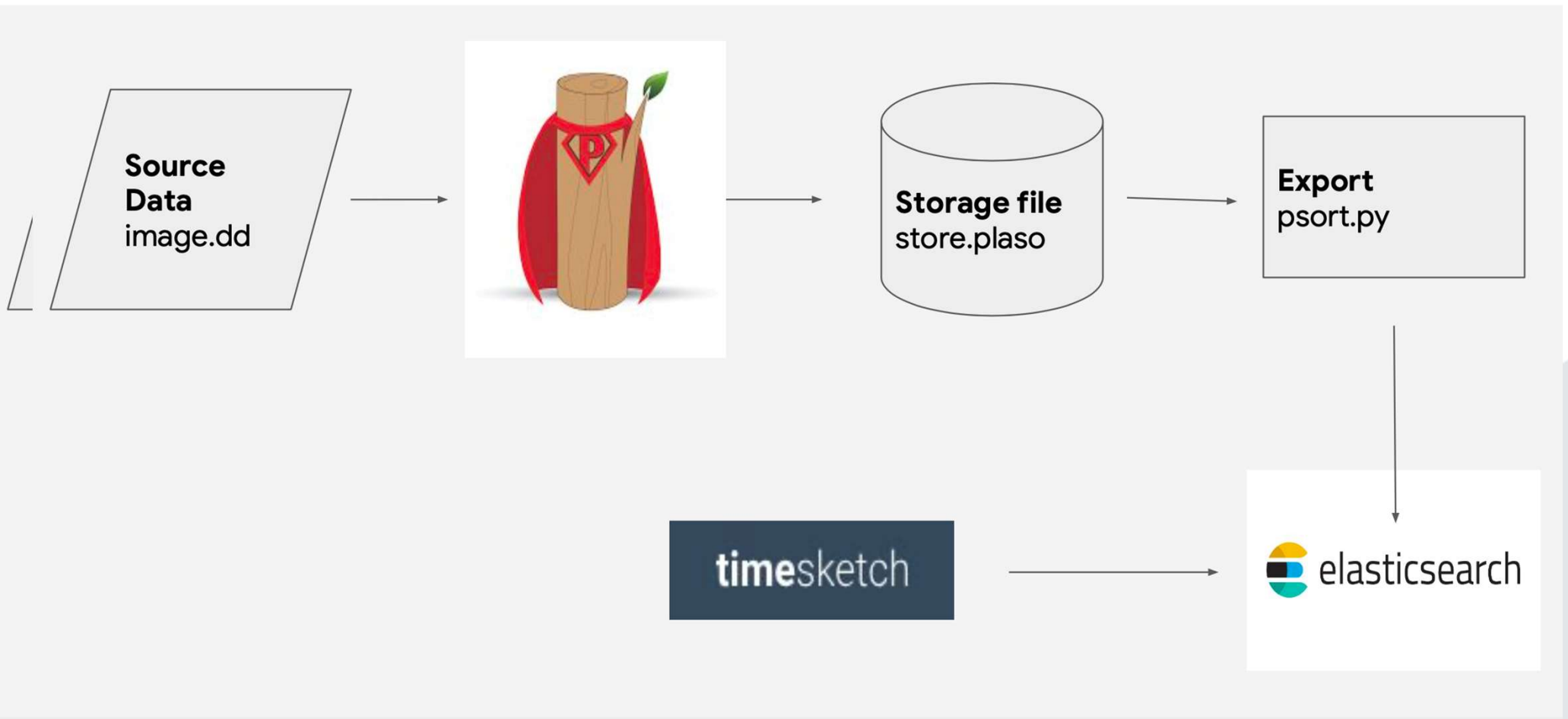
Basé sur une interface web

Partage d'information entre utilisateurs

Annotation et partage des découvertes

Basé sur Elastic Search

Analyse du supertimeline : Timesketch



The Greendale incident

Search

Filters Starred Save view Choose view

Enable all Disable all

dc2

student-pc1

student-pc2

10 events (0.029s)

2014-09-16T19:19:20+00:00	[Content Modification Time] [1149 / 0x0000047d] Record Number: 297376 Event Level: 4 Source Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager Computer Name: student-pc1.ad.greendale.edu Strings: [u'ad\\pelton_da', u'', u'192.168.56.101']	student-pc1
2014-09-16T19:23:50+00:00	[Content Modification Time] [21 / 0x00000015] Record Number: 49 Event Level: 4 Source Name: Microsoft-Windows-TerminalServices-LocalSessionManager Computer Name: student-pc1.ad.greendale.edu Strings: [u'AD\\pelton_da', u'1', u'192.168.56.101']	student-pc1
2014-09-16T19:25:01+00:00	[Content Modification Time] [1149 / 0x0000047d] Record Number: 299229 Event Level: 4 Source Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager Computer Name: student-pc1.ad.greendale.edu Strings: [u'root', u'', u'192.168.56.101']	student-pc1
2014-09-16T19:28:18+00:00	[Content Modification Time] [\\Software\\Microsoft\\Internet Explorer\\TypedURLs] url1: http://192.168.56.101/explooder.exe	student-pc1
2014-09-16T19:28:21+00:00	[mtime] OS:/media/disk/Windows/Temp/explooder.exe	student-pc2
2014-09-16T19:28:21+00:00	[File Last Modification Time] [\\ControlSet001\\Control\\Session Manager\\AppCompatCache] Cached entry: 23 Path: \\?? \\C:\\Users\\pelton_da\\Downloads\\exploder.exe	student-pc1
2014-09-16T19:28:21+00:00	[File Last Modification Time] [\\ControlSet001\\Control\\Session Manager\\AppCompatCache] Cached entry: 19 Path: \\??C:\\windows\\temp\\exploder.exe	student-pc2
2014-09-16T19:42:35+00:00	[Content Modification Time] [24 / 0x00000018] Record Number: 55 Event Level: 4 Source Name: Microsoft-Windows-TerminalServices-LocalSessionManager Computer Name: student-pc1.ad.greendale.edu Strings: [u'AD\\pelton_da', u'1', u'192.168.56.101']	student-pc1
2014-09-16T20:43:00+00:00	[Last Time Executed] Application: C:\\windows\\temp\\exploder.exe Scheduled by: SYSTEM Run Iteration: ONCE	student-pc2
2014-09-17T20:42:00+00:00	[Scheduled To Start] Application: C:\\windows\\temp\\exploder.exe Scheduled by: SYSTEM Run Iteration: ONCE	student-pc2

ANALYSE A CHAUD D'UN WINDOWS 10 POUR RECUPERER UN TIMELINE

Présentation des outils utilisés

Présentation de Powershell

Utilité de connaître quelque commandes Powershell

Démonstrations en local

Cas particulier dans une infrastructure de type Active Directory

Powershell

Langage de script apparu pour la première en 2005 en version bêta.

2006 devient une MAJ non obligatoire de Windows Vista.

Disponible de base dans toutes les versions de Windows depuis W8.

Successeur des interfaces en ligne de commande DOS/Windows

Compatible avec toutes les versions de windows supportant la version 2 de .NET

Pourquoi utiliser Powershell ?

Il peut arriver que dans le cadre d'une réponse sur incident vous soyez amené à effectuer une première analyse à chaud et que vous ne puissiez pas:

- utiliser de clef usb (ports bloqués, risque d'infection virale trop important),
- arrêter la machine à auditer (risque de perte des signes de compromission, etc...)

Avantage :

- Le lancement de powershell n'inscrit qu'un seul évènement dans le journal de windows.
- Tout le système est accessible depuis powershell. (journaux, extraction de données etc)
- Exportation aisée du résultat des recherches

Commandes Utiles 1/2

#Get-Winevent

##Afficher les événements

#Lister les événements classiques :

Get-eventlog -list

#Lister tous les événements :

Get-winevent -listlog * | select logname

#Lister les événements de sécurité dans les 100 dernières entrées

get-eventlog -new 100 -Logname Security

#"Lister les événements de sécurité dans les 100 dernières entrées (ouverture de session : 4624, fermeture de session 4634) pour un utilisateur (guillaume, syntaxe simple mais peu précise)

get-eventlog -new 100 -Logname Security -InstanceId 4624,4634 -Message "*cyril*" | fl TimeWritten,entrytype,eventid,message

#Même commande mais autre syntaxe, en utilisant le splatting :

```
$params = @{ new= 100  
             logname= "security"  
             instanceid = 4624,4634  
             message = "*cyril*" }
```

get-eventlog @params | fl TimeWritten,entrytype,eventid,message

#Afficher un événement spécifique via id (index) :

Get-eventlog -logname system -Index 227211 | fl

Commandes Utiles 2/2

```
#Afficher les événements datant de 2 jours maximum
$jours=(Get-Date).AddDays(-2)
Get-Eventlog -LogName "security" | Where-Object {$_.TimeGenerated -ge $jours} | Format-Table TimeCreated, LogName, Level, Id, ProviderName, Message
#ou
Get-WinEvent -LogName "security" | Where-Object {$_.TimeCreated -ge $jours} | Format-Table TimeCreated, LogName, Level, Id, ProviderName, Message

##Exporter et importer
#Exporter les événements :
Get-EventLog System | Export-CliXml "c:\temp\eventsystem.clixml"

#Vous pouvez ensuite travailler sur l'élément exporté :
$systemlogs = Import-CliXml "c:\temp\eventsystem.clixml"
$systemlogs | fl TimeWritten,entrytype,eventid,message

#Vous pouvez aussi exporter les événements avec la commande suivante :
wevtutil epl System "c:\temp\eventsystem.evtx"
#Et utiliser le fichier dans powershell de la manière suivante
Get-winevent -path "c:\temp\eventsystem.evtx"
```

Démonstration en live

Script Powershell utilisé :

```
#on récupère le nom de la machine :  
[system.environment]::MachineName
```

```
#on recupère l'utilisateur courant :  
[Environment]::UserName
```

```
#on recupère l'heure système
```

```
#On recupere les informations du bios  
Get-CimInstance -ClassName Win32_BIOS
```

```
$Date = (Get-Date).AddDays(-2)
```

```
Get-WinEvent application | Where-Object {$_.TimeCreated -ge $Date} | Format-Table TimeCreated, LogName, Level, Id, ProviderName, Message
```

Démonstration de l'outil « ORC » de l'ANSSI :

Sources : <https://www.ssi.gouv.fr/actualite/decouvrez-dfir-orc-un-outil-de-collecte-libre-pour-lanalyse-forensique/>

Cas particulier d'un environnement de type industriel (AD)

La particularité de cet environnement est que généralement les journaux d'évènements sont déportés sur un serveur distant afin de décharger la machine

Il faudra alors pour pouvoir utiliser powershell téléchargé certains modules spécifique à l'Active Directory.

Dans ce cas de figure, il y a un outil gratuit fournit par l'ANSSI appelé « ADTimeline3 » qui permet d'extraire toutes les informations nécessaires et d'en avoir une exploitation aisée via SPLUNK.

Site : <https://github.com/ANSSI-FR/ADTimeline>

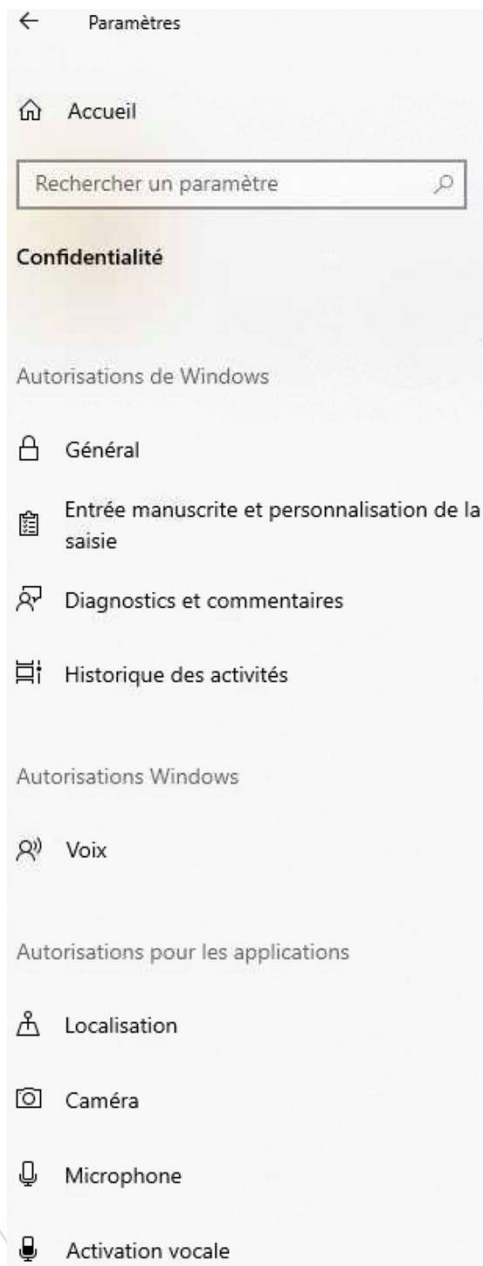
ANALYSE A FROID D'UN WINDOWS 10 POUR EFFECTUER UN TIMELINE

Windows 10 et le Timeline

- Nouvelle fonctionnalité introduite depuis la 1803
- Intégrée dans “Connected Device Platform Service”
- Service Windows pour interconnecter Windows / PC et Smartphones
- Le service fonctionne avec un compte Microsoft Azur ou un compte Active Directory mais le timeline lui peut fonctionner quelque soit le compte

Windows 10 et le Timeline

- Enregistrement de l'activité Utilisateur des 30 derniers jours
- Pas de documentation exhaustive sur ce qui est capturé
- Au depart c'est toute la navigation Web qui est capture (Edge, mais aussi les applications associées, Photos, News, Sport, Weather etc...)
- Possibilité de pousser la timeline sur le cloud
- Paramétré par l'Utilisateur ou poussé par une GPO



Historique des activités

Revenez à ce que vous faisiez sur votre appareil en stockant l'historique de vos activités, y compris les informations sur les sites web que vous visitez et la façon dont vous utilisez les applications et les services.

☒ Enregistrer l'historique de mes activités sur cet appareil

Revenez à ce que vous faisiez, même si vous changez d'appareil, en envoyant à Microsoft l'historique de vos activités, y compris les informations sur les sites web que vous visitez et sur l'utilisation des applications et des services.

☒ Envoyer l'historique de mes activités à Microsoft

Consultez [En savoir plus](#) et la [Déclaration de confidentialité](#) pour découvrir comment les produits et services Microsoft utilisent ces données pour personnaliser des expériences, tout en respectant votre vie privée.

Afficher les activités de ces comptes

Il s'agit de vos comptes sur cet appareil. Désactivez-les pour masquer leurs activités de votre chronologie.



jpnoat@uriel-expert.com



Activé

Effacer l'historique des activités

Effacer l'historique pour jpnoat@uriel-expert.com

Windows 10 et le Timeline à froid

2 min. ago						
Name	Description	Path	Size	Created	Modified	Record changed
.. = Local (115 125)	existing, already viewed	\Users\jpnoa\AppData	4,9 GB	19/12/2019 19:20:01	23/05/2020 10:18:27	23/05/2020 10:18:27
. = ConnectedDevicesPlatform (8)	existing	\Users\jpnoa\AppData\Local	5,1 MB	19/12/2019 19:22:21	19/12/2019 22:08:19	19/12/2019 22:08:19
8fa27725ac0c0315 (3)	existing	\Users\jpnoa\AppData\Local\ConnectedDevicesPlatform	5,1 MB	19/12/2019 19:22:25	19/12/2019 19:22:25	19/12/2019 19:22:25
8fa27725ac0c0315.cdp	existing, already viewed	\Users\jpnoa\AppData\Local\ConnectedDevicesPlatform	1,5 KB	19/12/2019 19:22:25	22/05/2020 14:47:56	22/05/2020 14:47:56
8fa27725ac0c0315.cdpresource	existing, already viewed	\Users\jpnoa\AppData\Local\ConnectedDevicesPlatform	54 B	19/12/2019 22:08:19	22/05/2020 14:47:56	22/05/2020 14:47:56
CDPGlobalSettings.cdp	existing, already viewed	\Users\jpnoa:				19/05/2020 10:17:49
Connected Devices Platform certificates.sst	existing	\Users\jpnoa:				19/12/2019 19:22:25
L.jpnoa.cdpresource	existing	\Users\jpnoa:				19/12/2019 19:22:21

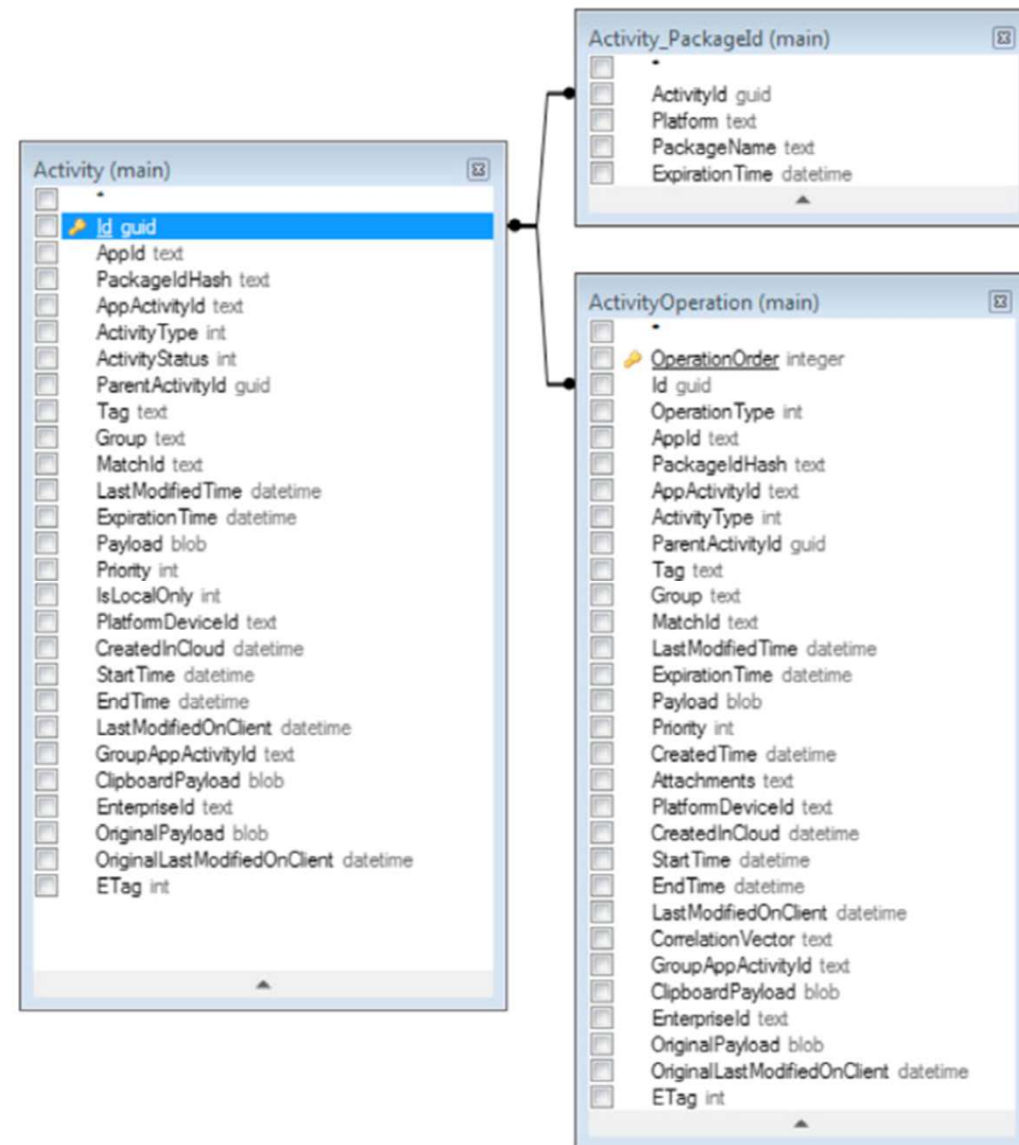
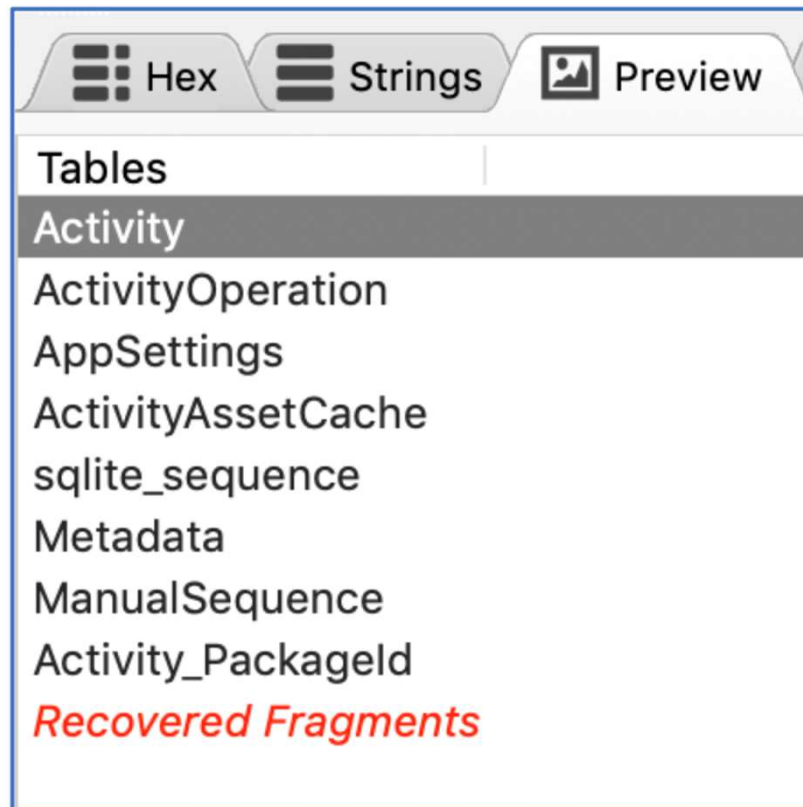
```
{
  "AFSEnvironment" : 0,
  "AFSUrl" : "https://activity.windows.com",
  "AccountSettings" : [],
  "ActivityStoreInfo" : [
    {
      "active" : true,
      "activityStoreId" : "0DED15FC-531F-6814-89E4-227ADF6C4804",
      "stableUserId" : "8fa27725ac0c0315"
    }
  ],
  "AfcDefaultUser" : "undefined",
  "AfcPrivacySettings" : {
    "ActivityFeed" : 0,
    "CloudSync" : 0,
    "PublishUserActivity" : 0,
    "UploadUserActivity" : 0
  },
  "AfsConnectivityEnabled" : true,
  "AfsPostInitializeSyncWaitMs" : 10000,
  "AfsSyncFrequencyMs" : 86400000
}
```

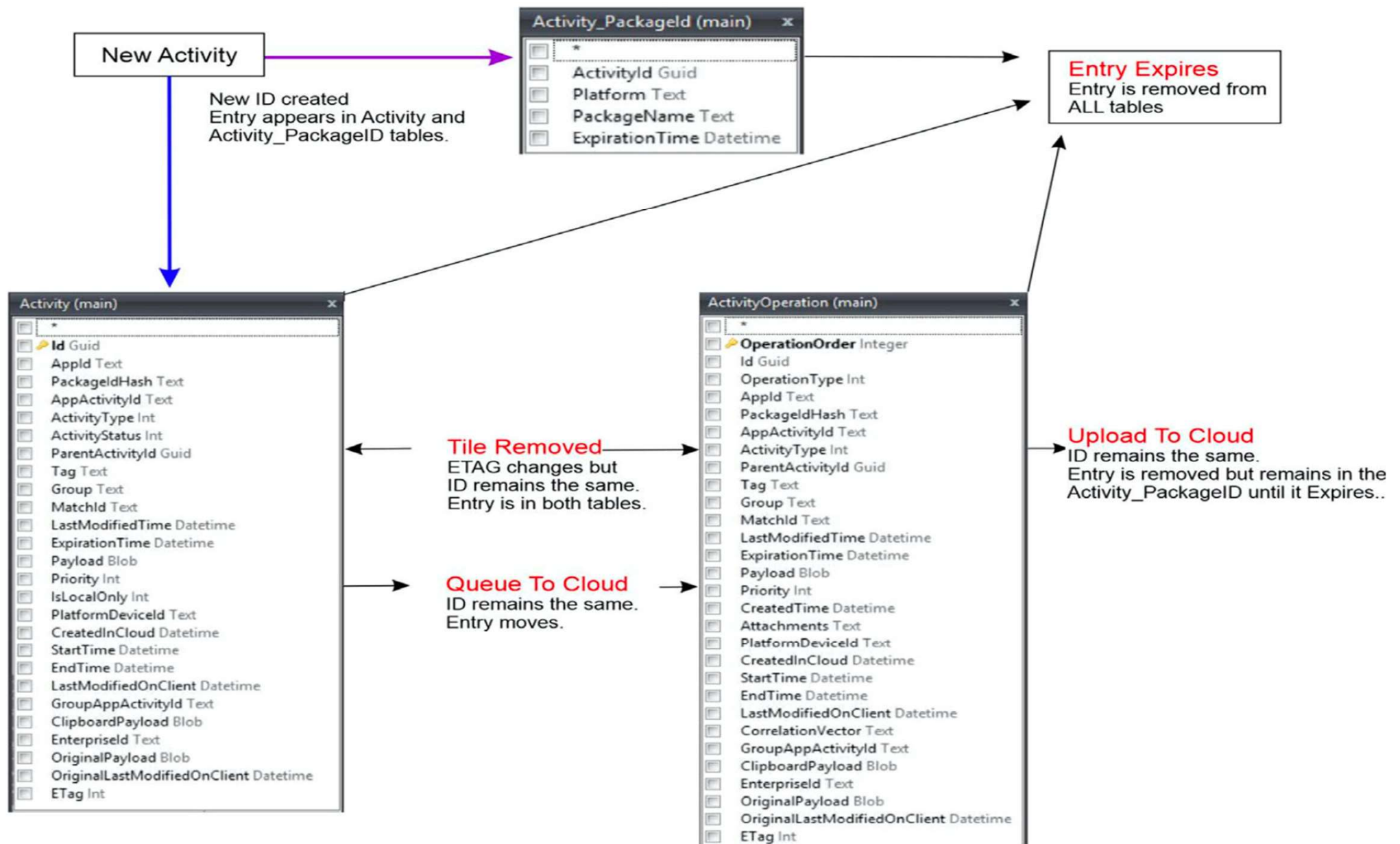
%USER%/Appdata/Local/Connected...

Windows 10 et le Timeline à froid

\Users\jpnoa\AppData\Local\ConnectedDevicesPlatform\8fa27725ac0c0315	
<input type="checkbox"/> Name▲	<input type="checkbox"/> Description
<input checked="" type="checkbox"/> .. = ConnectedDevicesPlatform (8)	existing, already viewed
<input type="checkbox"/> . = 8fa27725ac0c0315 (3)	existing
<input checked="" type="checkbox"/> ActivitiesCache.db	existing, already viewed
<input type="checkbox"/> ActivitiesCache.db-shm	existing
<input checked="" type="checkbox"/> ActivitiesCache.db-wal	existing, already viewed

Structure interne des tables





Explication de certains champs de table

- <https://github.com/kacos2000/WindowsTimeline/blob/master/WindowsTimeline.sql>
- Exemple activity type (2 notification, 3 sauvegarde mobile, 5, démarrage application, 6 focus sur l'application, 10 clipboard, 16 activité copier / coller), 11, 12 et 15 applis système

Références

<https://www.youtube.com/watch?v=-vsXFrOZOtc>

<https://www.blackbagtech.com/blog/exploring-the-windows-activity-timeline-part-1-the-high-points/>

<https://github.com/kacos2000/WindowsTimeline/blob/master/README.md>

<https://github.com/kacos2000/Win10/blob/master/README.md>

https://digital-forensics.sans.org/media/log2timeline_cheatsheet.pdf

<https://readthedocs.org/projects/plaso/downloads/pdf/latest/>

[https://digital-forensics.sans.org/summit-](https://digital-forensics.sans.org/summit-archives/dfirprague14/Collaborative_Timeline_Analysis_in_Large_Incidents_Johan_Berggren.pdf)

[archives/dfirprague14/Collaborative_Timeline_Analysis_in_Large_Incidents_Johan_Berggren.pdf](https://digital-forensics.sans.org/summit-archives/dfirprague14/Collaborative_Timeline_Analysis_in_Large_Incidents_Johan_Berggren.pdf)

Les prochains rendez-vous...

26 mai : <https://www.cellebrite.com/fr/webinaires/pa-7-33-les-nouveautes/>

30 juin avec Sarah Edwards et Heather Mahalik investigation sur Mac (suite)

<https://us02web.zoom.us/meeting/register/tZAlf-uqqT8tE9TCoz1zvGv3s23RZjf59iHo>

9 juin sur l'investigation sur Mac (Introduction)

<https://us02web.zoom.us/meeting/register/tZYtd-GrpzMrG9X9tbFV5btkpqZpQK348zYX>

Pas de Rdv les 16 et 23 juin du fait d'obligations professionnelles (cours à donner)



La parole est à vous !