

COMPUTER FORENSICS

Analyse approfondie d'images de clé USB et disque dur avec : FTK Imager, Autopsy, Registry Explorer et OSForensics

Travail réalisé par :

EL HANAFI Maha

TP1 : l'analyse forensique d'une clé USB-----	3
Acquisition d'une image USB -----	3
La création d'une image de la clé USB en utilisant FTK imager -----	4
L'analyse de la Clé USB avec l'outil Autopsy -----	10
TP 2 : Analyse de bases de registre-----	14
Etape 1 : C'est l'étape de l'exportation des ruches en utilisant FTK Imager -----	14
Etape 2 : Importation des ruches en utilisant Registry Explorer -----	15
Etape 3 : analyse des registres -----	17
Cas 1 : Analyse approfondie d'une image de disque (cas réel : win10 UIR) Avec Autopsy -----	19
Cas 2 : Analyse approfondie d'une image de disque (cas réel : win10 UIR) Avec OSForensics-----	24
Conclusion : -----	39

Objectif : L'objectif de ce rapport c'est de faire une analyse approfondie d'une image créer en utilisant des outils de l'analyse forensique.

TP1 : l'analyse forensique d'une clé USB

Acquisition d'une image USB

1. FTK imager
2. Image USB
3. dc3dd

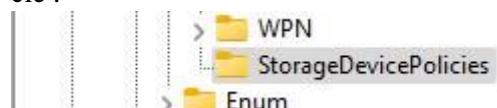
Etape 0 : Installation des outils : FTK imager, Autopsy

Etape 1 : création d'un WriteBlocker software Objectifs :

- Éviter d'une personne ne soit écrite sur la clé USB préserve toutes les données de la clé •
- Éviter la corruption de la clé.

Les étapes pour créer un WriteBlocker : réaliser un WriteBlocker logiciel pour bloquer l'accès à clé USB c'est-à-dire on aura seulement le droit de la lecture.

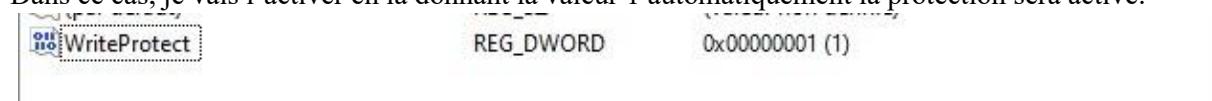
Sur Windows, Allons à la base de registre (tапant dans la barre de recherche éditeur de Registre), cherchons SYSTEM, CurrentControlSet, control, au niveau de ce chemin on va créer une nouvelle clé :



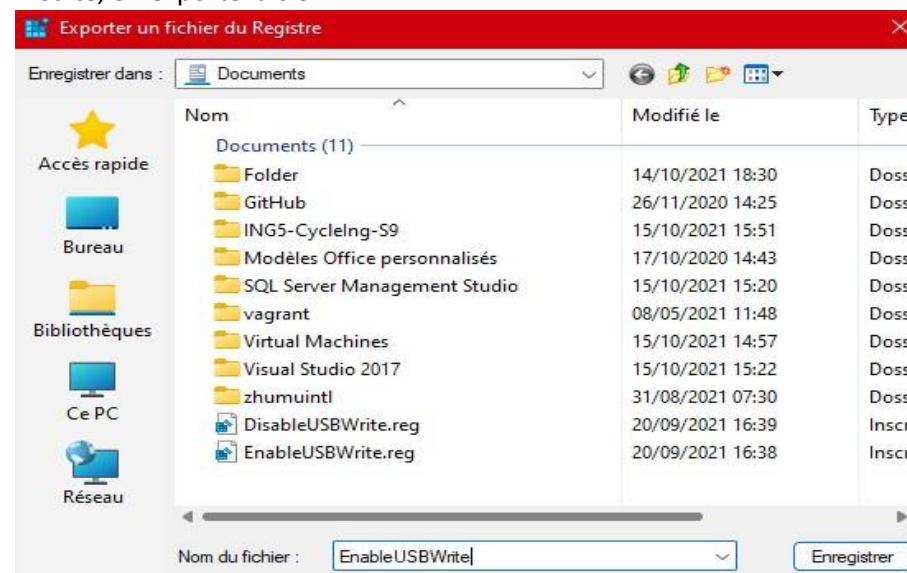
Au niveau de chemin on va créer une nouvelle clé de type DWORD (32 bits) : « WriteProtect », comme la Screenshot ci-dessous le montre, la protection n'est pas active (la valeur c'est 0)

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\StorageDevicePolicies			
	Nom	Type	Données
> Srp > SrpExtensionConfig > StillImage > Storage > StorageManagement	(par défaut) WriteProtect	REG_SZ REG_DWORD	(valeur non définie) 0x00000000 (0)

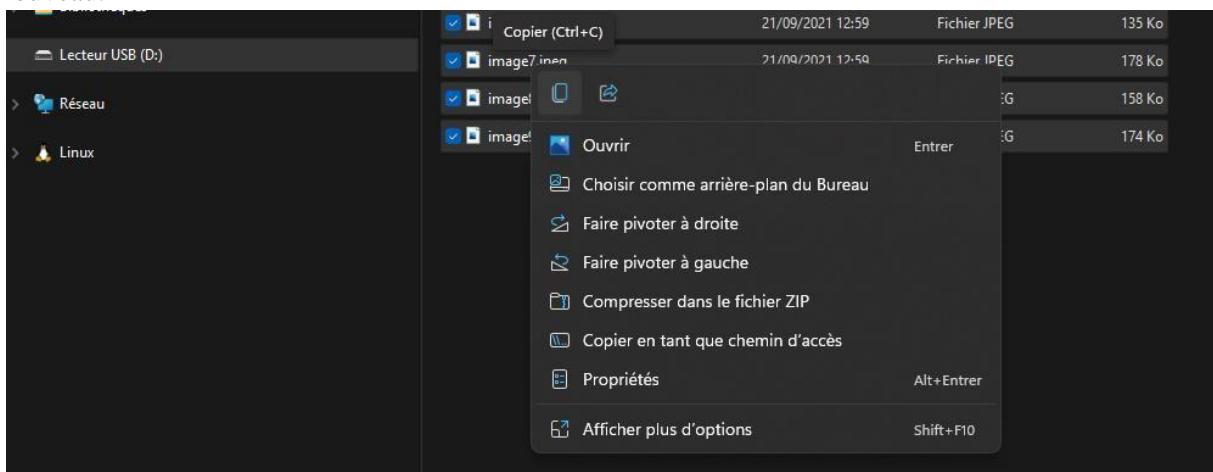
Dans ce cas, je vais l'activer en la donnant la valeur 1 automatiquement la protection sera active.



Ensuite, on exporte la clé



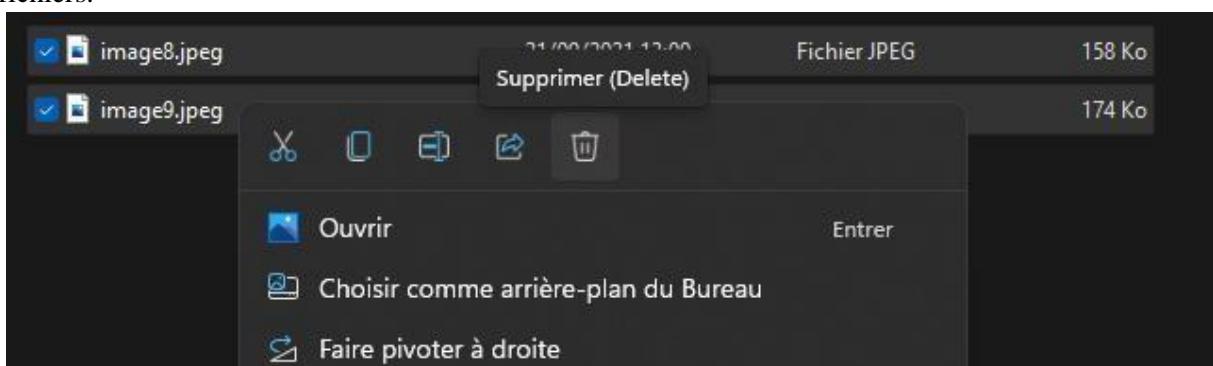
-On branche une clé USB et on vérifie les droits d'accès : comme la Screenshot ci-dessous le montre, je ne peux ni supprimer les fichiers sélectionnés ni créer un nouveau.



-Ensuite si je clique sur « DisableUsbWrite » sa valeur est 0, c'est-à-dire je désactive la protection et j'aurai l'accès à la clé USB du coup je peux modifier ou supprimer le contenu de cette clé.



-Après que je branche la clé USB, comme le Screenshot ci-dessous le montre, je peux supprimer les fichiers.

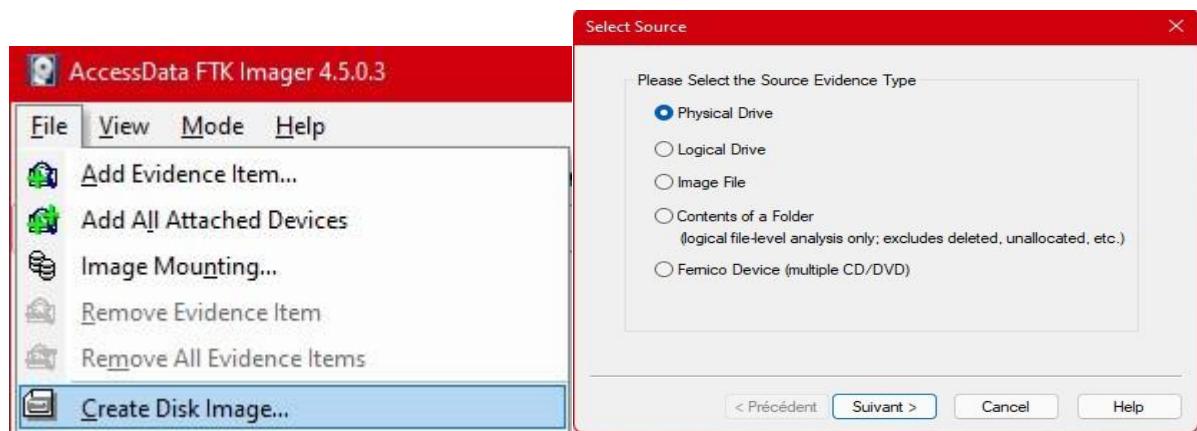


La création d'une image de la clé USB en utilisant FTK imager

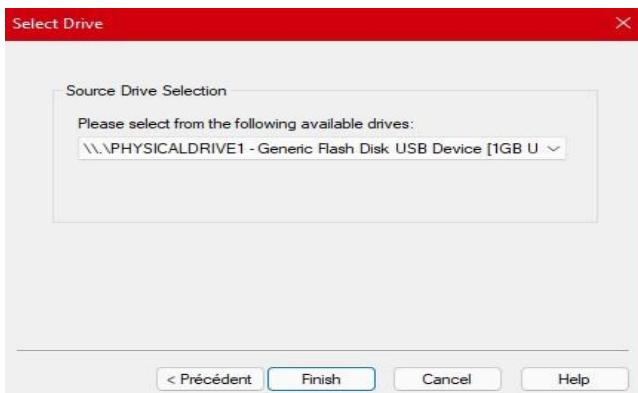
FTK Imager est un outil d'aperçu et d'imagerie de données utilisé pour acquérir des données (preuves) d'une manière solide sur le plan médico-légal en créant des copies de données sans apporter de modifications aux preuves originales. Après avoir créé une image des données, utilisez Forensics Toolkit pour effectuer un examen médico-légal approfondi et créer un rapport de vos conclusions.

Dans cette étape, nous allons utiliser **FTK imager**. Ce dernier est un outil d'acquisition d'images. Il est possible de faire une image d'un disque dur, d'une clé USB etc. avant d'en récupérer les données.

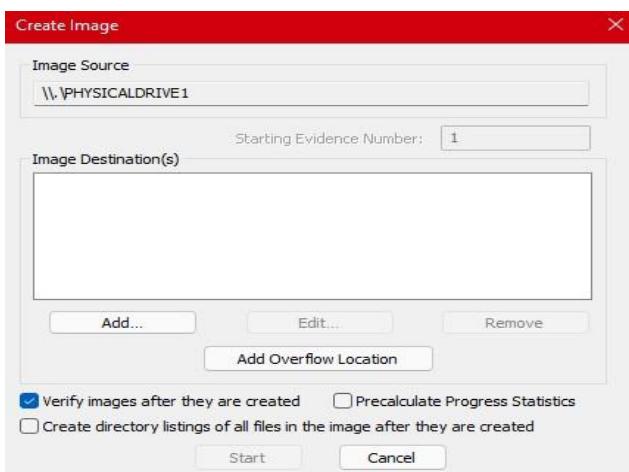
❾ Voici les étapes qui montrent la création d'une image de clé USB :



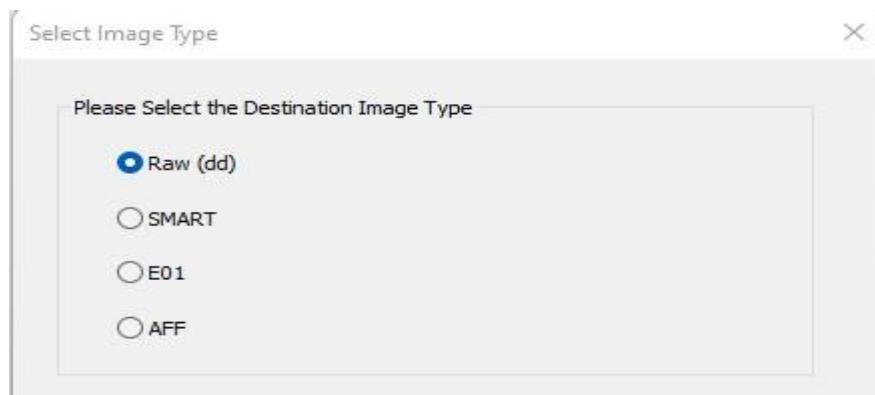
-Après on sélectionne la clé USB :



-Ensuite, on choisit la destination (l'image de clé USB sera enregistrer où exactement ?)



-On choisit le type d'image qu'on veut : nous allons choisir le type Raw (dd) :



-Les informations sur l'enquête en cours :

Evidence Item Information

Case Number:	1
Evidence Number:	1
Unique Description:	enquête 1
Examiner:	Maha
Notes:	UIR

< Précédent Suivant > Cancel Help

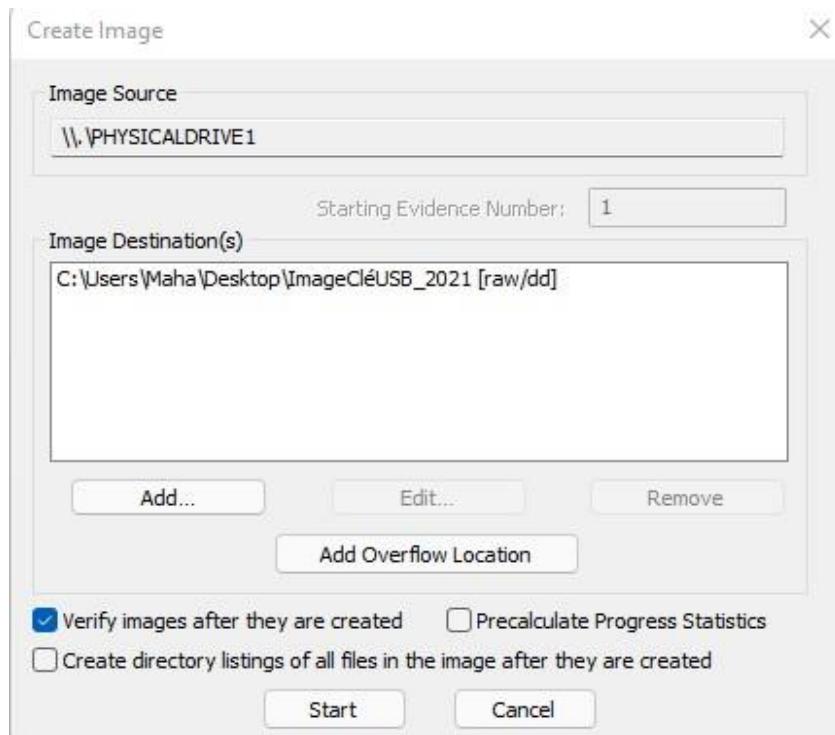
-Ensuite, on sélectionne le chemin où on va enregistrer l'image :

Select Image Destination

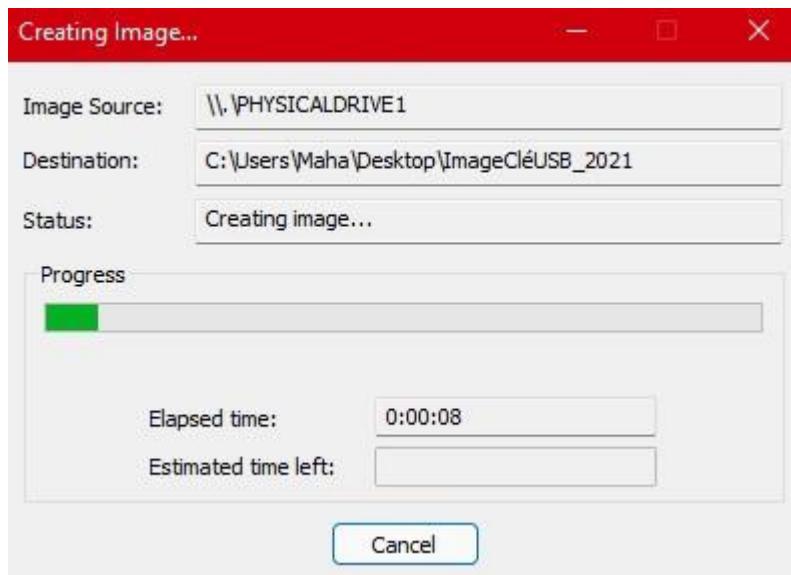
Image Destination Folder	C:\Users\Maha\Desktop	Browse
Image Filename (Excluding Extension)	ImageCléUSB_2021	
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment	1500	
Compression (0=None, 1=Fastest, ..., 9=Smallest)	0	
Use AD Encryption <input type="checkbox"/>		

< Précédent Finish Cancel Help

-Enfin on démarre :



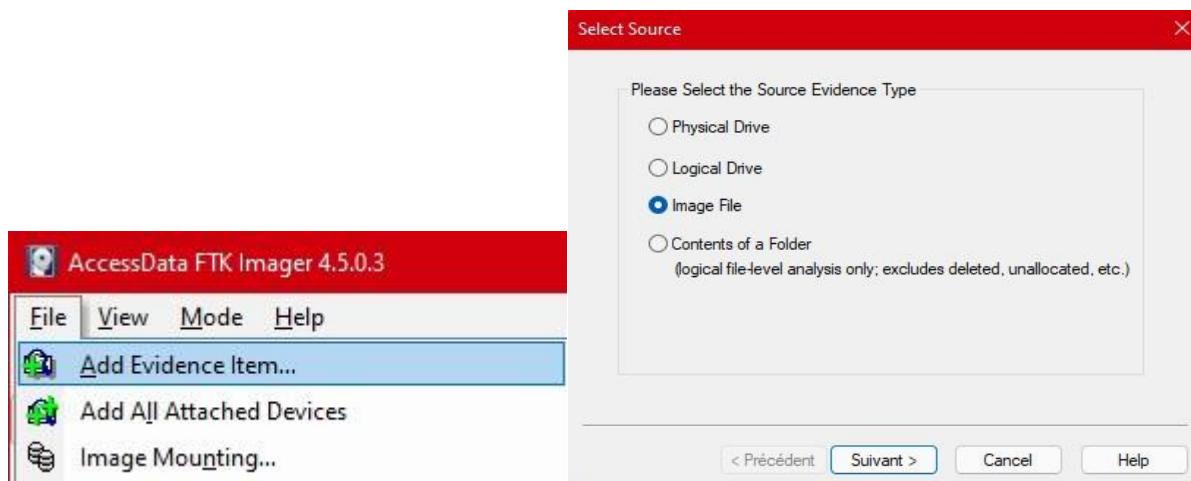
-Comme le Screenshot ci-dessous le montre, il est entrain de copier le contenu (clonage bit à bit) de la clé USB et de le mettre dans un fichier appelé ImageCléUSB_2021 et il va l'enregistrer dans le bureau



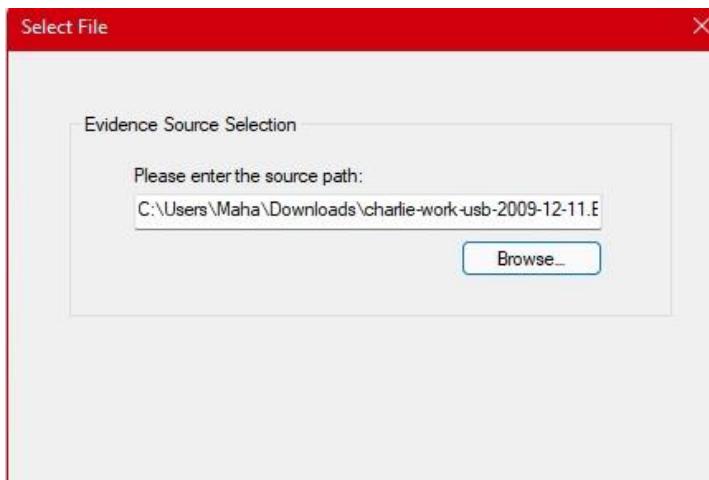
-Et voilà l'image a été créée dans le bureau :



➊Une fois la création de l'image est terminée, nous maintenant l'analyser :



-Ensuite, On va sélectionner une image :



-On va maintenant l'arborescence de la partition de la clé USB, ce qui nous intéresse c'est la Partition 1 :

Name	Size	Type	Date Modified
00000240 F6 00 00 00 01 00 00 00-02 BD 3E CE FE 3E CE B0 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 00000250 00 00 00 00 00 00 00 00-00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 00000260 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E 00000270 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu-Aa*Ui-r-ü 00000280 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC U*u-A-u-éY-i 00000290 18 69 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 h-H-ö-i 000002A0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 OB 00 75 DB A3 -A-X-rä- uÜ 000002B0 0F 00 C1 2E 0F 00 04 1E-SA 33 DB B9 00 20 2B C8 -A- z3Ü+ +E 000002C0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fy- Áy- è 000002D0 4B 00 2B C5 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K-Ewi- ,í fñAu- 000002E0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f-GTCPAu- ü- r- 000002F0 68 07 BB 16 68 70 0E 16-69 09 00 66 53 66 53 66 h->hp-h- f\$Stf 00000300 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U- h- fa- i 3A; 00000310 28 10 B9 D8 0F F3 F3 AA-E9 5F 01 90 90 66 60 1E (-10 6ü*é- -f- 00000320 06 66 A1 11 00 63 03 06-1C 00 1F 66 60 00 00 fí- f- -fh- 00000330 00 66 50 06 53 63 01 00-65 10 00 B4 42 8A 16 0E fB Sh-h- B- 00000340 00 16 1F 88 F4 C3 13 66-59 SB SA 66 52 66 59 1F -öí fñ[ZYfY- 00000350 0F 82 16 00 66 F6 06 11-00 03 16 0F 00 8E C2 FF -fy- Áy 00000360 0E 16 00 75 BC 07 1F 66-61 C3 A0 F8 01 E8 09 00 -ü- fñA- ö- è- 00000370 A0 FB 01 E8 03 04 F4 EB-FD B4 01 8B F0 AC 3C 00 ü- è- ö-ý- -ö- <- 00000380 74 09 B4 0E BB 07 00 CD-10 EB F2 C3 08 OA 41 20 t- > i éöA- A 00000390 64 69 73 6B 20 72 65 61-64 20 65 72 72 6F 72 20 disk read error 000003a0 6F 63 63 75 72 72 65 64-00 0D OA 42 4F 4F 54 4D occurred--BOOT			

Ceci c'est juste un exemple théorique : le Screenshot on voit les courriels envoyés et reçus :

Name	Size	Type	Date Modified
other	1	Directory	10/12/2009 22:39:09
\$130	36	NTFS Index Allocation	10/12/2009 22:27:55
Charlie_2009-11-16_1102_Received.txt	1	Regular File	03/12/2009 21:19:12
Charlie_2009-11-16_1102_Received.txt.FileSlack	4	File Slack	
Charlie_2009-11-16_1122_Received.txt	1	Regular File	03/12/2009 21:19:27
Charlie_2009-11-16_1122_Received.txt.FileSlack	4	File Slack	
Charlie_2009-11-16_1151_Sent.txt	1	Regular File	04/12/2009 21:44:29
Charlie_2009-11-16_1326_Sent.txt	1	Regular File	04/12/2009 21:45:00
Charlie_2009-11-16_1338_Received.txt	1	Regular File	03/12/2009 21:19:43
Charlie_2009-11-16_1338_Received.txt.FileSlack	4	File Slack	
Charlie_2009-11-16_1433_Received.txt	1	Regular File	03/12/2009 21:19:55
Charlie_2009-11-16_1553_Received.txt	1	Regular File	03/12/2009 21:20:10
Charlie_2009-11-16_1559_Sent.txt	1	Regular File	04/12/2009 21:45:14
Charlie_2009-11-17_0845_Received.txt	1	Regular File	03/12/2009 21:20:26
Charlie_2009-11-17_0845_Received.txt.FileSlack	4	File Slack	
Charlie_2009-11-17_1030_Received.txt	2	Regular File	03/12/2009 21:20:37
Charlie_2009-11-17_1030_Received.txt.FileSlack	3	File Slack	
Charlie_2009-11-17_1033_Received.txt	1	Regular File	03/12/2009 21:21:40
Charlie_2009-11-17_1033_Received.txt.FileSlack	4	File Slack	
Charlie_2009-11-17_1039_Received.txt	1	Regular File	03/12/2009 21:21:08
Charlie_2009-11-17_1039_Received.txt.FileSlack	4	File Slack	
Charlie_2009-11-17_1040_Received.txt	1	Regular File	03/12/2009 21:21:22
Charlie_2009-11-17_1040_Received.txt	1	Regular File	03/12/2009 21:21:22

```

Subject:
Re: New email address
From:
Alix Pery <alix.pery@yahoo.com>
Date:
Mon, 16 Nov 2009 13:38:51 -0800 (PST)
To:
Charlie <charlie@m57.biz>

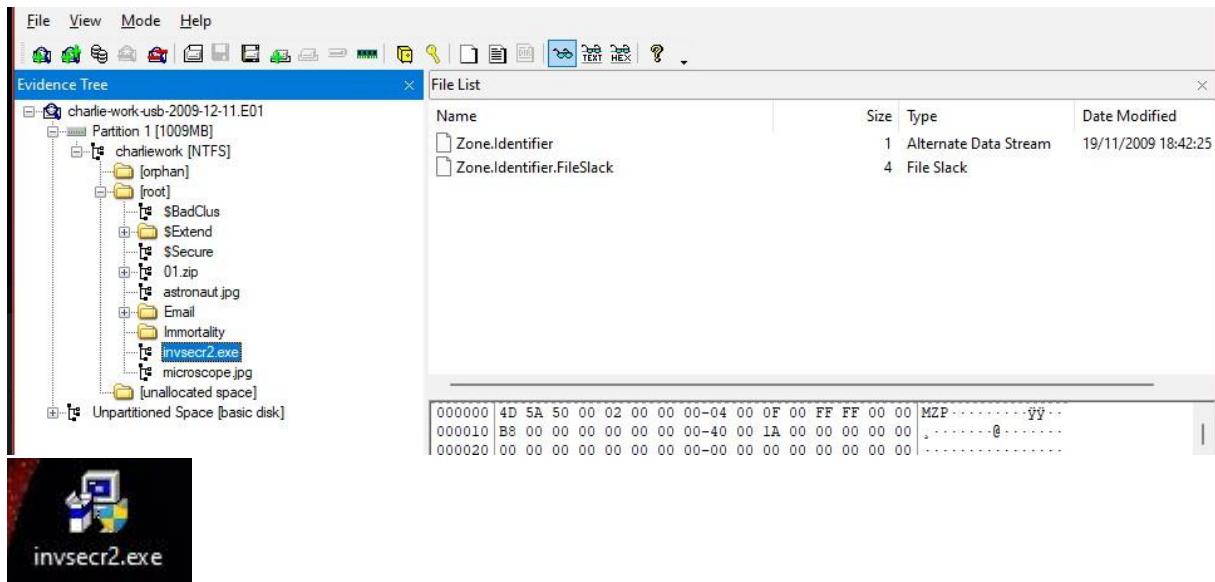
Great! Congrats on the new job!

From: Charlie <charlie@m57.biz>
To: alix.pery@yahoo.com; rubinfritz31@mail.com
Sent: Mon, November 16, 2009 1:26:16 PM
Subject: New email address

Hey everybody. I started working at the new company today. It's pretty slow going so far, w
Charlie

```

Aussi, je peux exporter ce fichier (un fichier exécutable) pour l'analyser

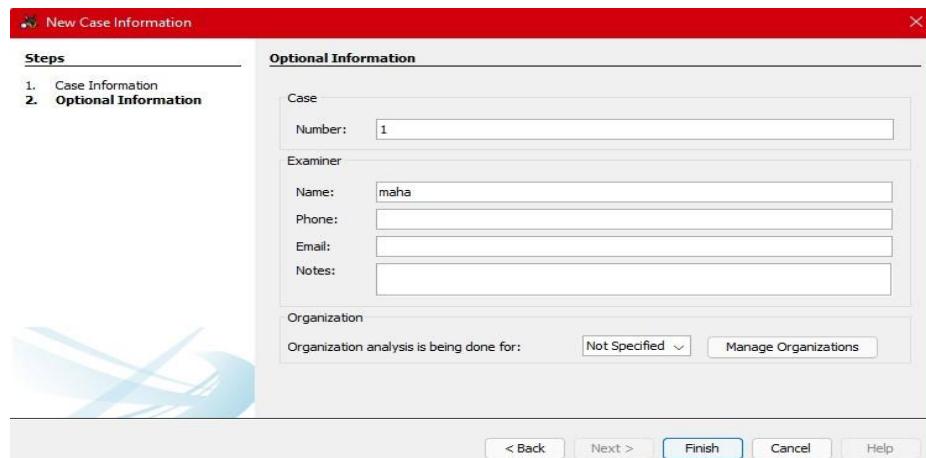


L'analyse de la Clé USB avec l'outil Autopsy

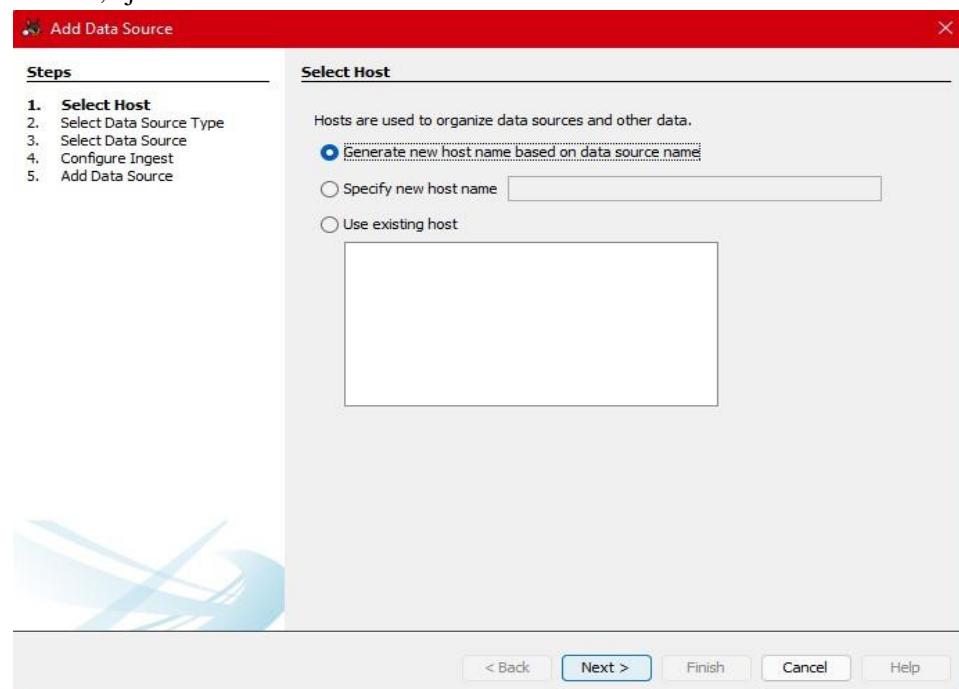
Autopsy est un outil de criminalistique numérique open source développée par Basis Technology, publié pour la première fois en 2000. C'est un outil gratuit à utiliser et assez efficace pour l'enquête sur le disque dur avec des fonctionnalités telles que les cas multi-utilisateurs, l'analyse chronologique, l'analyse du registre, la recherche par mot-clé, l'analyse des courriels, la lecture multimédia, l'analyse EXIF, la détection de fichiers malveillants et bien plus encore. [Source](#) -Créer une case :



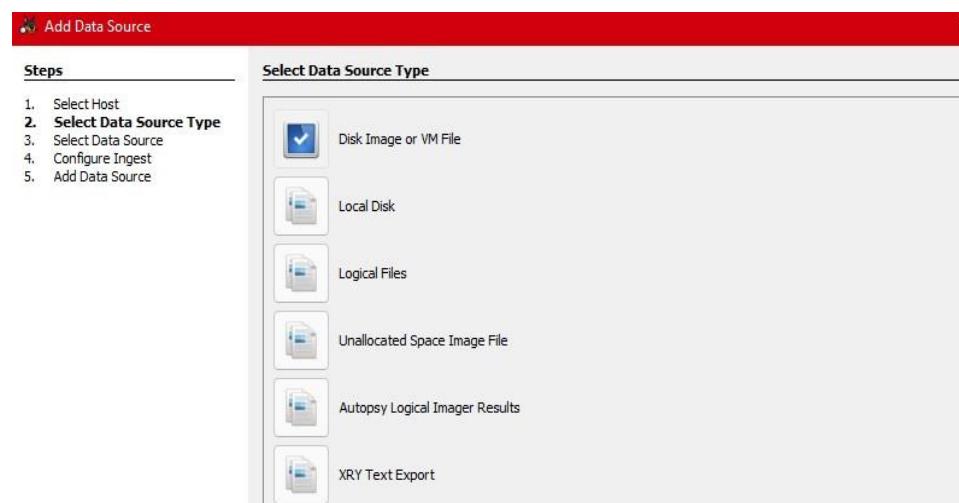
Les informations sur l'enquêteur :



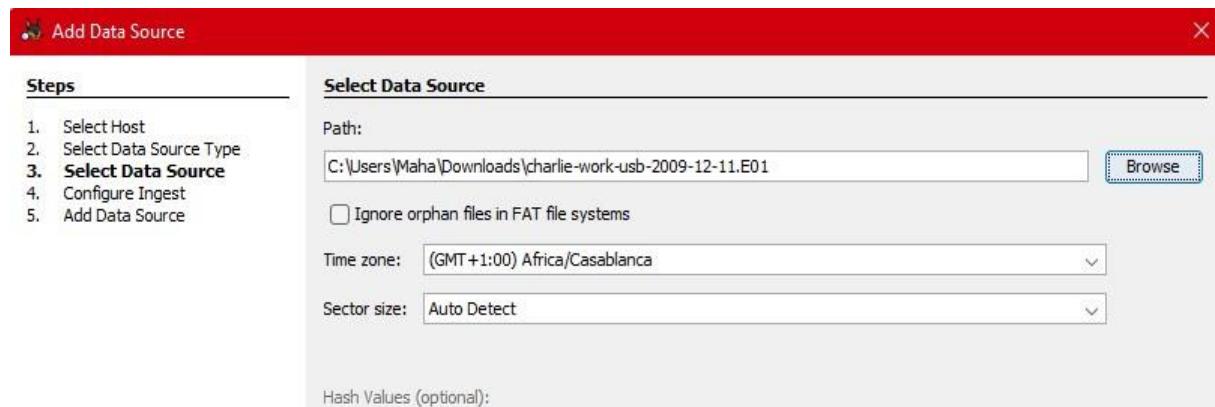
-Ensuite, ajouter la source des données :



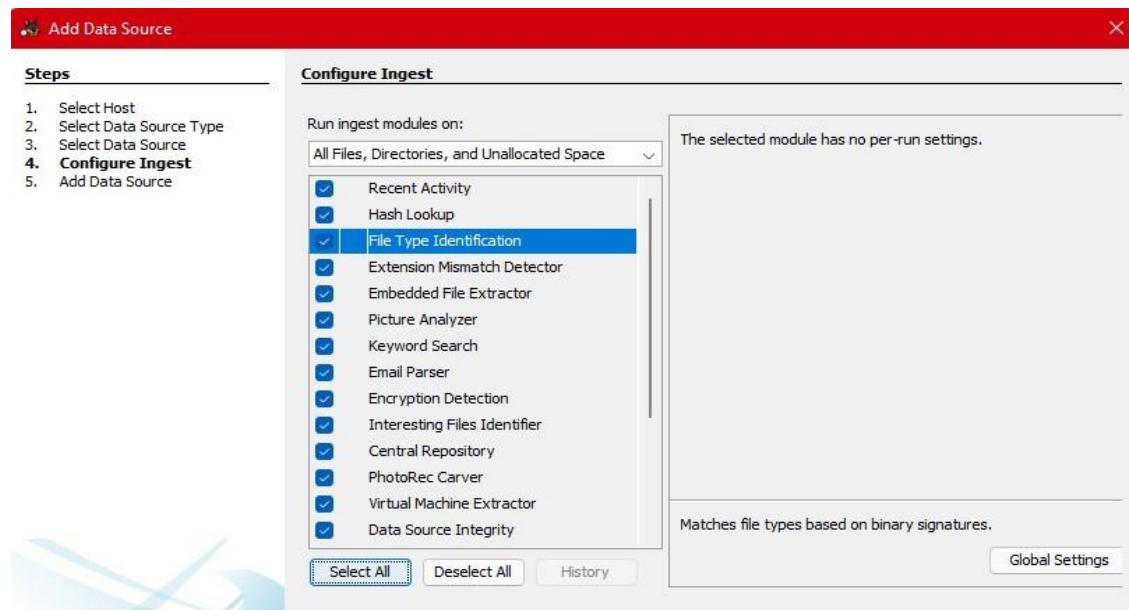
-Choisir le type de la source de données : ici on va choisir image de disque :



On sélectionne maintenant la source de données :



-Autopsy affiche la configuration et les modules qui va activer pour rechercher des informations spécifiques : Par exemple, il va chercher l'activité récente, à identifier le type des fichiers selon le besoin etc..



Résultat : comme la figure ci-dessous le montre, File views nous donne un aperçu de tous les fichiers que Autopsy a trouvé par catégories.

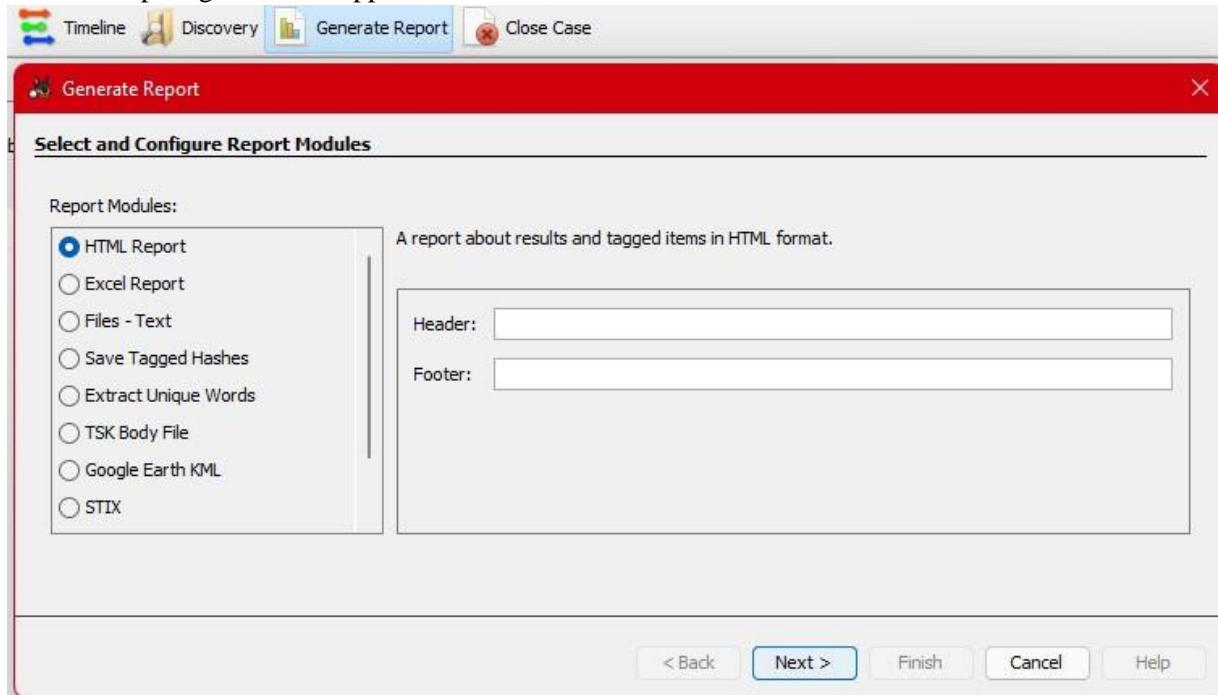
-Il a trouvé par exemple 10 images, il a regroupé toutes les images en extensions par rapport au FTK imager Autopsy donne plus d'information par catégories. Il nous donne aussi plus de détails sous forme d'un tableau, ces informations concernant la date de création, de modification et même les images supprimées. Tous ces détails peuvent nous aider et faciliter l'analyse d'un disque.

-On voit aussi qu'il a trouvé 4 fichiers compressés :

-Ici les fichiers supprimés :

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D)	Flags(M)	Known	Location
Charlie_2009-11-20_1303_Sent.txt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/img_charlie-work-usb-2009-12-11.E01/vol_
Charlie_2009-12-02_1305_Received_Part 1.2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0			unknown	/img_charlie-work-usb-2009-12-11.E01/vol_

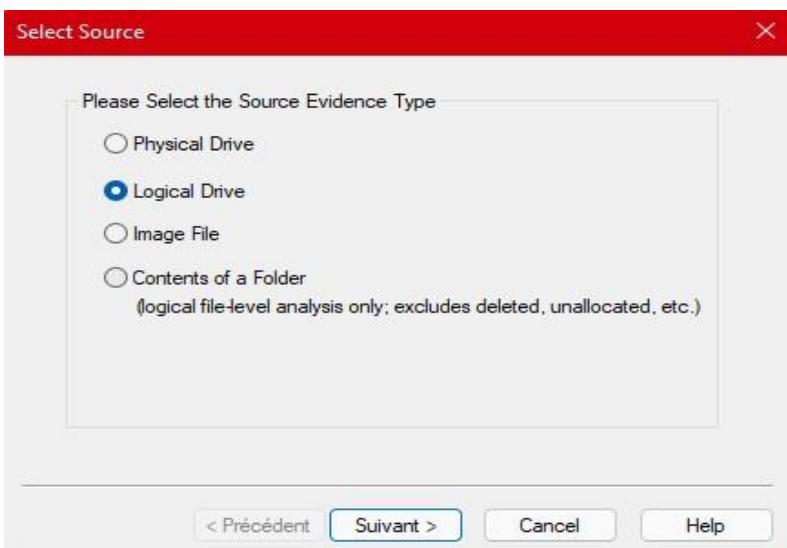
-Ensuite on peut générer un rapport soit en HTML ou Excel etc..



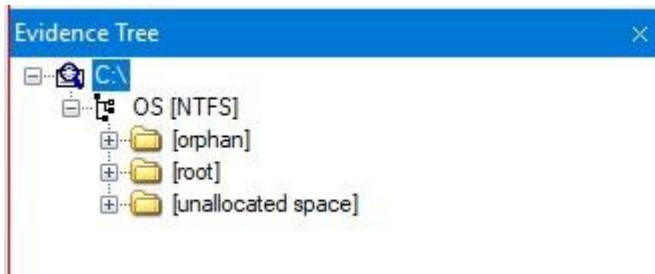
TP 2 : Analyse de bases de registre

Etape 1 : C'est l'étape de l'exportation des ruches en utilisant FTK Imager

-On crée une preuve en suivant les étapes : File → Add and Evidence → on sélectionne le type de la source de la preuve



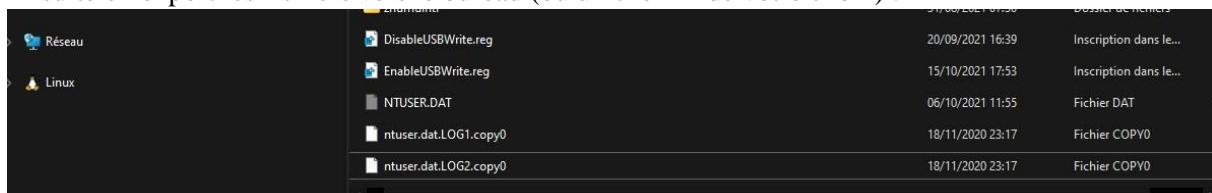
-Ici la preuve représente une partition C:\ :



-Maintenant on cherche les fichiers *NTUSER.DAT*, *ntuser.dat.LOG1*, *ntuser.dat.LOG2* : en suivant le chemin suivant : C:/ → root → Users → 'utilisateur normal'

Path	File/Folder	Type	Creation Date	Last Modified Date
C:\Users\All Users	\$130	NFS Index All...	27/10/2021 22:49:05	
C:\Users\Default	-1.14-windows.xml	Regular File	04/08/2021 13:55:11	
C:\Users\Default User	-1.14-windows.xml.FileSlack	File Slack		
C:\Users\Maha	.gitconfig	Regular File	11/10/2020 09:19:13	
C:\Users\Maha\.android	.packettracer	Regular File	26/07/2021 21:18:38	
C:\Users\Maha\.config	client.py	Regular File	20/03/2021 10:52:20	
C:\Users\Maha\icesoft	NTUSER.DAT	Regular File	30/10/2021 20:26:16	
C:\Users\Maha\idlerc	NTUSER.DAT.FileSlack	File Slack		
C:\Users\Maha\lemmix	ntuser.dat.LOG1	Regular File	12/10/2021 00:14:49	
C:\Users\Maha\m2	ntuser.dat.LOG1.FileSlack	File Slack		
C:\Users\Maha\p2	ntuser.dat.LOG2	Regular File	12/10/2021 00:14:49	
C:\Users\Maha\pylint.d	ntuser.dat.LOG2.FileSlack	File Slack		
C:\Users\Maha\ssh	NTUSER.DAT[1c2b59c5-c5f5-11eb-bacb-...]	Regular File	23/10/2021 11:49:11	
C:\Users\Maha\swt	NTUSER.DAT[1c2b59c5-c5f5-11eb-bacb-...]	Regular File	23/10/2021 11:49:11	
C:\Users\Maha\tooling	NTUSER.DAT[1c2b59c5-c5f5-11eb-bacb-...]	Regular File	23/10/2021 11:49:11	
C:\Users\Maha\vagrant	NTUSER.DAT[1c2b59c5-c5f5-11eb-bacb-...]	Regular File	23/10/2021 11:49:11	
C:\Users\Maha\.vagrant.d	NTUSER.DAT[1c2b59c5-c5f5-11eb-bacb-...]	Regular File	23/10/2021 11:49:11	
C:\Users\Maha\VirtualBox	NTUSER.DAT[1c2b59c6-c5f5-11eb-bacb-...]	Regular File	23/10/2021 11:49:11	
C:\Users\Maha\.vscode	NTUSER.DAT[1c2b59c6-c5f5-11eb-bacb-...]	Regular File	12/10/2021 00:14:49	
C:\Users\Maha\3D Objects	NTUSER.DAT[1c2b59c6-c5f5-11eb-bacb-...]	Regular File	12/10/2021 00:14:49	
C:\Users\Maha\Application Data	NTUSER.DAT[1c2b59c6-c5f5-11eb-bacb-...]	Regular File	12/10/2021 00:14:49	
C:\Users\Maha\Cisco Packet Tracer 7.3.1	ntuser.ini	Regular File	12/10/2021 00:37:11	
C:\Users\Maha\Contacts	NTUSER~2.LOG	INDX Entry		
C:\Users\Maha\Cookies	test.txt	Regular File	01/04/2021 13:57:05	
C:\Users\Maha\Desktop	test.txt.FileSlack	File Slack		

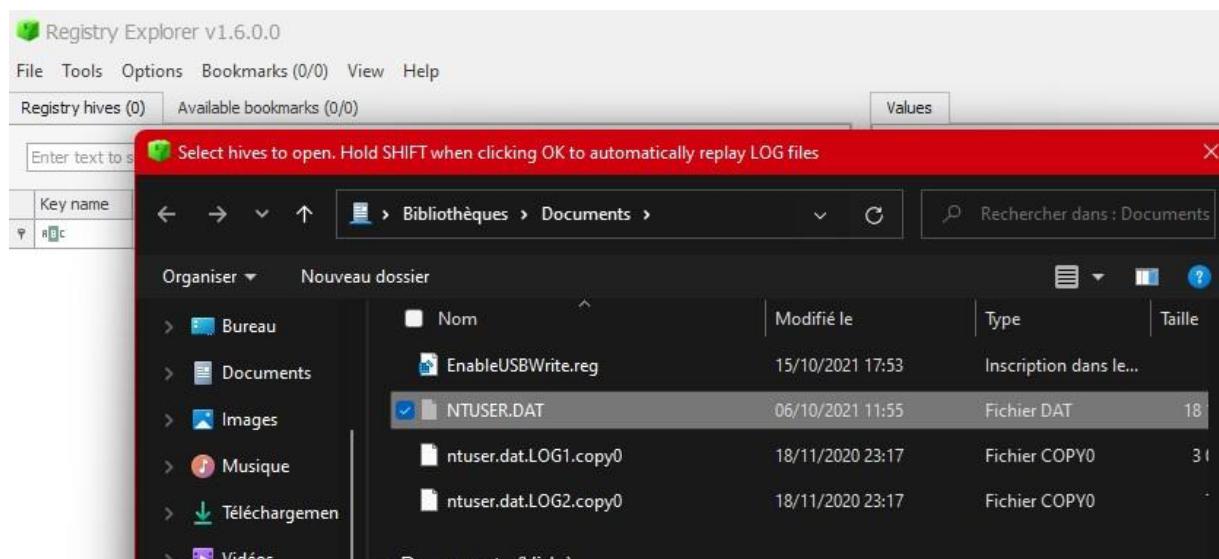
-Ensuite on export les fichiers vers le bureau (ou un chemin de votre choix) :



Etape 2 : Importation des ruches en utilisant Registry Explorer

Registry Explorer est un outil dont l'objectif est de remplacer l'éditeur du registre proposé par Windows. On appréciera notamment le gestionnaire de signets, l'import/export de données, l'historique complet, la sauvegarde automatique des manipulations effectuées ou encore la recherche performante intégrée.

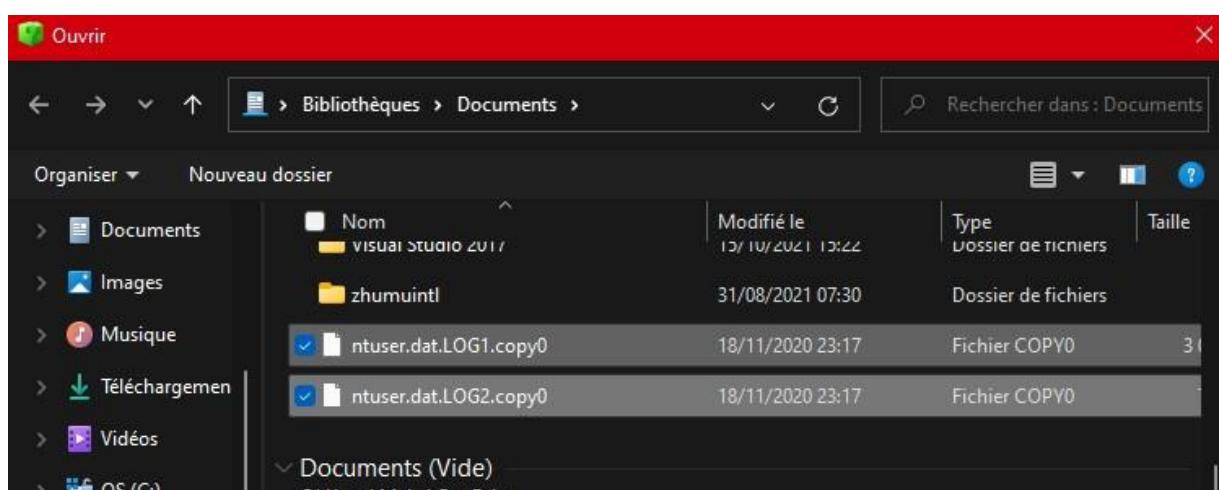
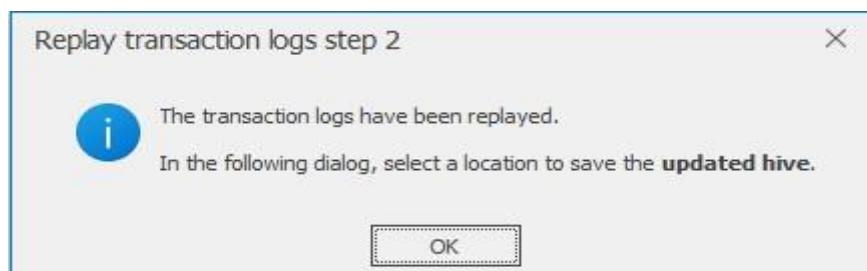
Dans cette étape, on importe les ruches qu'on a exporté dans la première étape. On clique sur File → Load hive et on sélectionne le fichier NTUSER.DAT



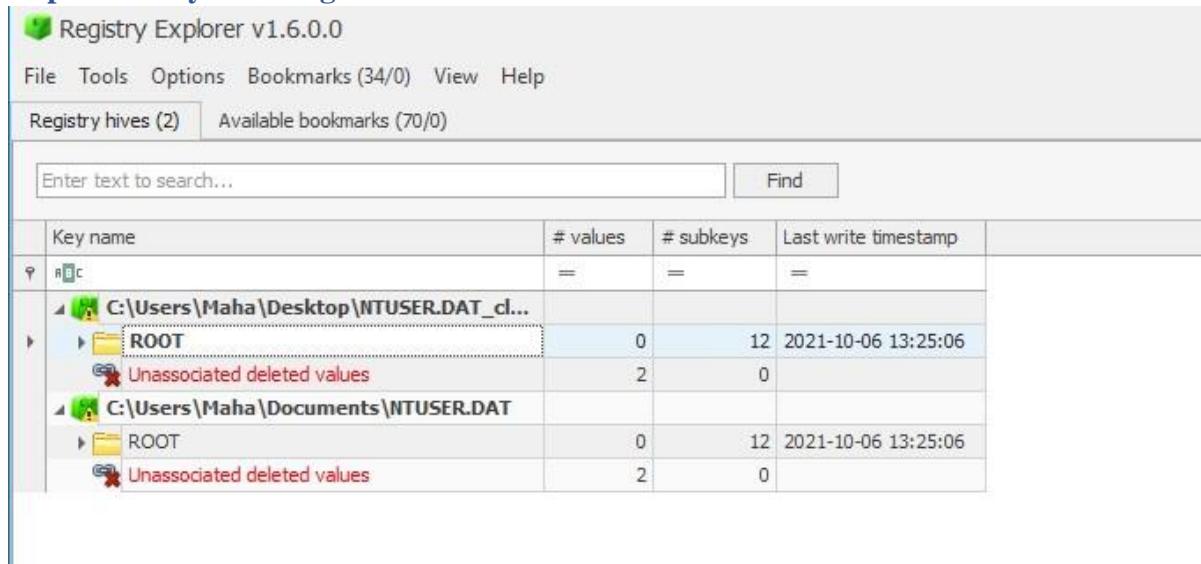
-On clique sur Yes :



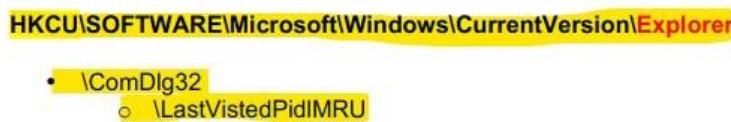
-On clique sur ok puis on importe les fichiers ntuser.dat.LOG1 et ntuser.dat.LOG2 :



Etape 3 : analyse des registres

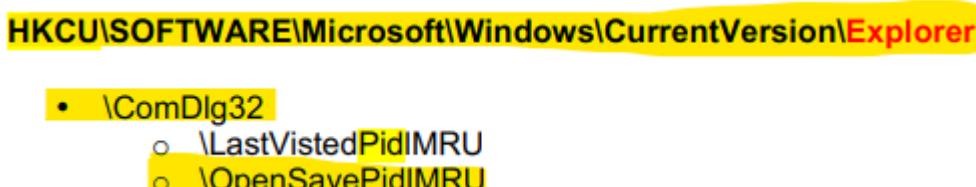


-On analyse les derniers PID les plus utilisés récemment :



Value Name	Hru Position	Executable	Absolute Path	Opened On
7	--	vmsware.exe	My Computer\Documents\Virtual Machines\Windows 10	2021-10-06 08:05:41
1	1	Pokernot.exe	My Computer\Desktop	
0	2	chrome.exe	My Computer\Desktop\Documents\Scholar	
22	3	brave.exe	My Computer\Desktop\Documents\Scholar	
2	4	microsoft.exe	My Computer\Desktop	
5	5	WhatsApp.exe	My Computer\Desktop	
10	6	{02352944-117B-45A3-B927-65C3EE08F8A8}	My Computer\C:\Users\Maha\Desktop\Stage 2ème Année cycle Ing	
15	7	{0F2C0D07-74F8-4766-B2F-89F9EA36726A}	My Computer\Documents	
18	8	Code.exe	My Computer\Desktop\poker_terraform-master	
17	9	SnippingTool.exe	My Computer\Pictures\Saved Pictures	
16	10	opera.exe	My Computer\Downloads	
14	11	Program Checker X.exe	My Computer\Desktop	
15	12	... (remaining 13 items)		

-On analyse les fichiers ouverts ou enregistrés récemment par une application via la boîte dialogue du Shell Windows :



Registry hives (2) Available bookmarks (70/0)				Values ComDig32\OpenSavePidIMRU					
				Drag a column header here to group by that column					
Key name	# values	# subkeys	Last write timestamp	Extension	Value Name	Mru Position	Absolute Path	Opened On	
C:\Users\Haha\Desktop\...	=	=	1601-01-01 00:00:00		10	=	=	=	
C:\Users\Haha\Documents...			1601-01-01 00:00:00		1	3	My Computer\Documents\Virtual Machines\Windows 10\Windows 10.vmx	2021-10-06 08:05:41	
Accounts	1	2	2021-09-26 15:15:45		2		My Computer\Virtual Machines\Windows 10\Windows 10.vmx	2020-12-28 14:40:54	
Applets	0	3	2021-02-27 08:42:59		3		My Computer\Virtual Machines\Windows 10\Windows 10.vmx	2020-12-28 14:40:54	
ComDig32	0	5	2021-03-18 16:40:18		4		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 21:06:43	
CDSaveIMRU	48	0	2021-06-08 08:05:41		5		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 20:54:49	
FirstFolder	8	0	2021-01-01 12:52:47		6		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 20:54:49	
LastVistedPidIMRU	26	0	2021-06-08 08:05:41		7		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 21:06:43	
LastVistedPidIMRU	3	0	2021-06-20 15:39:30		8		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 21:06:43	
OpenSavePidIMRU	0	45	2021-06-08 08:05:41		9		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 21:06:43	
RecentConversion	0	0	2021-09-26 18:07:36		10		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 21:06:43	
Conversion	0	0	2021-09-26 18:07:36		11		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-01 21:06:43	
Conversion	0	83	2021-04-08 10:19:02		12		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2021-04-23 11:27:40	
Conversion	0	17	2021-09-26 13:14:52		13		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2021-03-06 05:30:31	
Environment	10	0	2021-07-08 15:05:45		14		My Computer\Program Files\Apache Software Foundation\apache-tomcat-9.0.40\bin\catalina.bat	2020-12-27 22:37:55	

-On analyse la liste des fichiers récemment consultés :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

- \ComDig32
 - \LastVistedPidIMRU
 - \OpenSavePidIMRU
- \RecentDocs

Registry Explorer v1.6.0.0				Values Recent documents						
				Drag a column header here to group by that column						
Key name	# values	# subkeys	Last write timestamp	Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Las...
RecentDocs	0	0	2021-08-01 12:15:40	c	windowsupdate	ms-settings-win downdatewin	nsettingshome (17).lnk	3		
RecentDocs	81	0	2021-02-12 01:56:40	lnk	?LinkID=864206	https://go.microsoft.com/fwlink/?LinkID=864206.lnk		70		
RecentDocs	114	0	2021-02-12 01:56:40	lnk	edit?&source=Toast&&Temp orary=true&&sh aredAccess=T oken=E5E3E11-7B7E-481E Token=E5E3E-B4AC-3770E2 11-7B7E-481E 21DFB5&sec ondarySharedA ccessToken=898F3162-315B AccessToken=451B-B4C7-6768DF84AD39 6768DF84AD39 9.lnk	ms-screensket credit&source =Toast&&Temp orary=true&&sh aredAccess=T oken=E5E3E11-7B7E-481E Token=E5E3E-B4AC-3770E2 11-7B7E-481E 21DFB5&sec ondarySharedA ccessToken=898F3162-315B AccessToken=451B-B4C7-6768DF84AD39 6768DF84AD39 9.lnk		71		
RecentDocs	75	0	2021-09-14 13:08:00	lnk	feed?oid=wini taskbar	microsoft-edg https://www.msn.com/fr-xl-	feed?oid=wini taskbar.lnk	72		
RecentDocs	147	0	2021-10-06 14:00:00	lnk	settings?oid=wini taskbar	microsoft-edg https://www.msn.com/fr-xl-	settings?oid=wini taskbar.lnk	73		

-On analyse la liste des programmes exécutés récemment :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

- \ComDig32
 - \LastVistedPidIMRU
 - \OpenSavePidIMRU
- \RecentDocs
- \RunMRU

Registry Explorer v1.6.0.0				Values RunMRU			
				Drag a column header here to group by that column			
Key name	# values	# subkeys	Last write timestamp	Value Name	Mru Position	Executable	Opened On
App Paths	0	2	2021-09-27 15:20:00				
Uninstall	0	9	2021-10-01 21:59:00				
OneDrive	5	3	2021-09-14 13:08:00				
PrinterPorts	5	0	2021-10-06 13:25:00				
RecentDocs	151	99	2021-10-06 14:00:00				
Run	6	0	2021-09-16 10:41:00				
RunMRU	0	0	2020-11-18 22:17:00				
RunOnce	0	0	2021-10-06 13:25:00				

-On analyse les derniers chemins tapés ou insérés dans la barre de chemin de l'Explorateur de fichiers :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

- \ComDlg32
 - \LastVisitedPidIMRU
 - \OpenSavePidIMRU
- \RecentDocs
- \RunMRU
- \TypedPaths

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
url1	RegSz	C:\Users\Maha\...	35-00	<input type="checkbox"/>	<input type="checkbox"/>
url2	RegSz	C:\Users\Maha\...	67-00-5C-...	<input type="checkbox"/>	<input type="checkbox"/>
url3	RegSz	C:\...	72-00-6F-...	<input type="checkbox"/>	<input type="checkbox"/>
url4	RegSz	C:\Users\Maha\...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
url5	RegSz	C:\ProgramData	00-00-62-...	<input type="checkbox"/>	<input type="checkbox"/>

-On analyse les programmes exécutés :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Value Name	Value Type	Data	V...	Is Delete...	Data Record Real...
OneDrive	RegSz	"C:\...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
com.squirrel.Teams	RegSz	C:\...\ 0...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lync	RegSz	"C:\...\ 0...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Discord	RegSz	C:\...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MicrosoftEdgeAutoLaunch_F732A456E572DA499E7C83FC74A2250C	RegSz	"C:\...\ 0...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Opera GX Browser Assistant	RegSz	C:\...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cas 1 : Analyse approfondie d'une image de disque (cas réel : win10 UIR) Avec Autopsy

Dans cette étape nous allons faire une analyse forensique d'un cas réel en utilisant l'outil Autopsy : une image de disque dur externe.

Création d'une case :

New Case Information

Steps		Case Information
1. Case Information 2. Optional Information		Case Name: DiskWin10 Base Directory: C:\Users\Maha\Desktop <input type="button" value="Browse"/> Case Type: <input checked="" type="radio"/> Single-User <input type="radio"/> Multi-User Case data will be stored in the following directory: C:\Users\Maha\Desktop\DiskWin10

New Case Information

Steps		Optional Information
1. Case Information 2. Optional Information		Case Number: DiskImage01 Examiner Name: maha Phone: Email: Notes: Organization Organization analysis is being done for: Not Specified <input type="button" value="Manage Organizations"/>

Add Data Source

Steps		Select Host
1. Select Host 2. Select Data Source Type 3. Select Data Source 4. Configure Ingest 5. Add Data Source		Hosts are used to organize data sources and other data. <input checked="" type="radio"/> Generate new host name based on data source name <input type="radio"/> Specify new host name <input type="text"/> <input type="radio"/> Use existing host <input type="text"/>

Add Data Source

Steps	
1.	Select Host
2.	Select Data Source Type
3.	Select Data Source
4.	Configure Ingest
5.	Add Data Source

Select Data Source Type

- Disk Image or VM File
- Local Disk

Add Data Source

Steps	
1.	Select Host
2.	Select Data Source Type
3.	Select Data Source
4.	Configure Ingest
5.	Add Data Source

Select Data Source

Path: C:\Users\Maha\Desktop\Windows10.img

Ignore orphan files in FAT file systems

Time zone: (GMT+1:00) Africa/Casablanca

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Add Data Source

Steps	
1.	Select Host
2.	Select Data Source Type
3.	Select Data Source
4.	Configure Ingest
5.	Add Data Source

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

The selected module has no per-run settings.

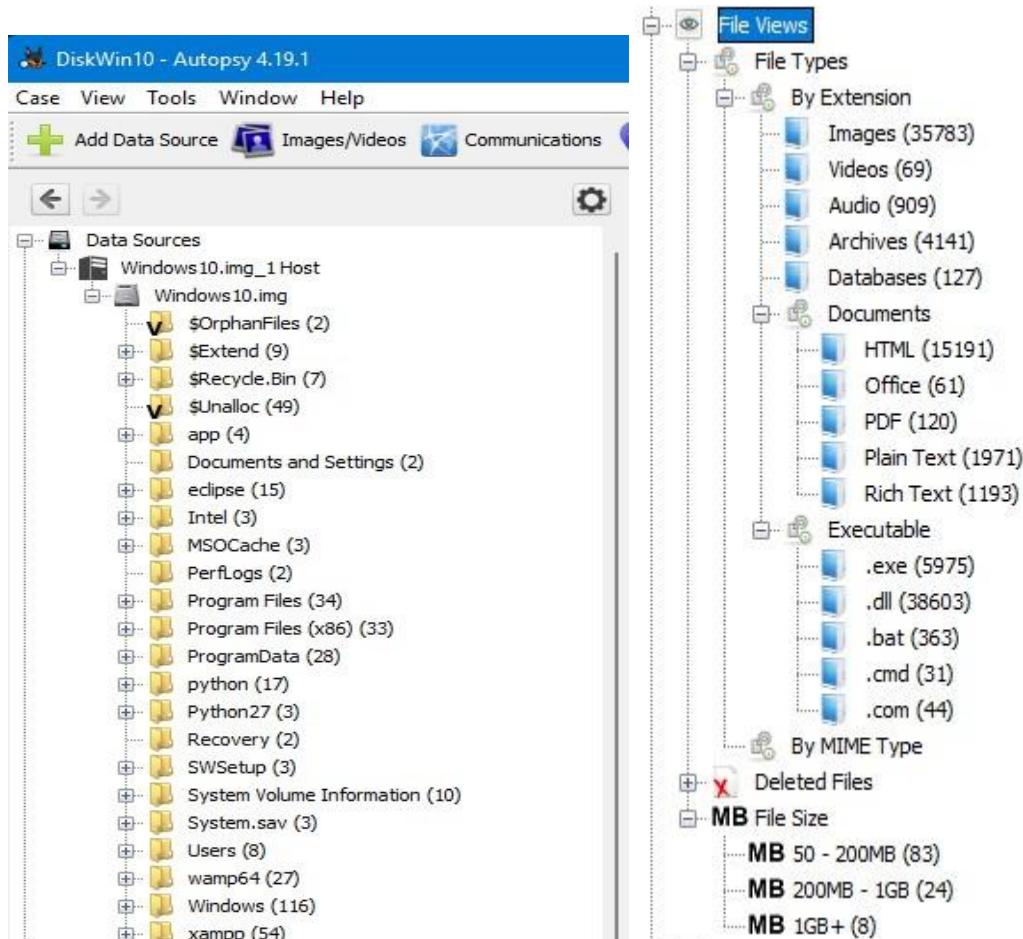
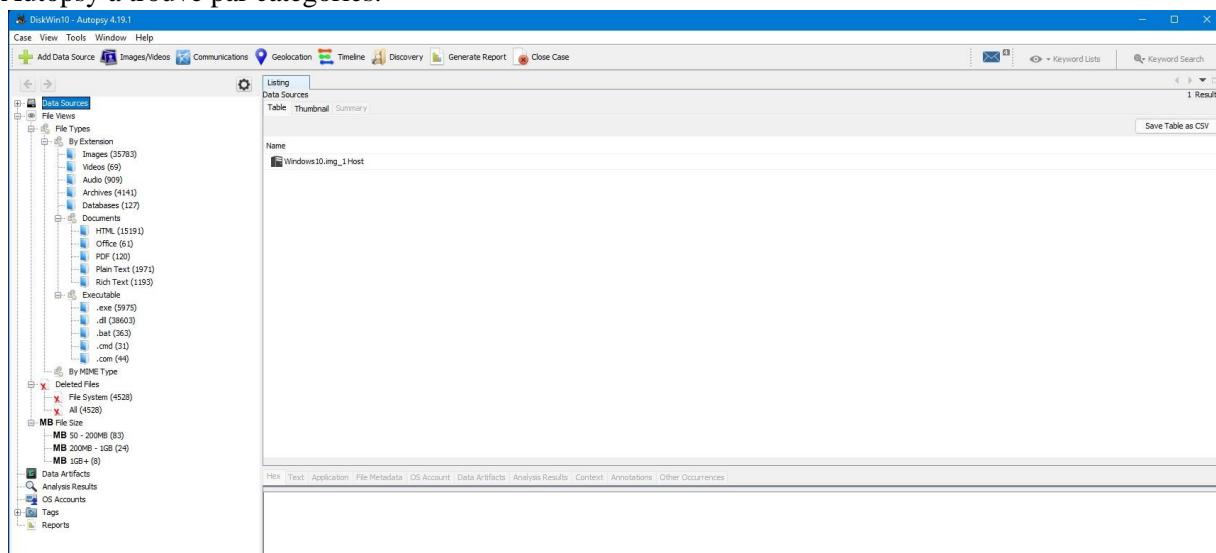
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity

Select All Deselect All History Global Settings

Uses iLEAPP to analyze logical acquisitions of iOS devices.

< Back Next > Finish Cancel Help

Comme les figures ci-dessous le montre, File views nous donne un aperçu de tous les fichiers que Autopsy a trouvé par catégories.



La liste des fichiers supprimés :

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
x MicrosoftOffice365Win64.xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x hwrcommuin.dat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x PhotosMedTitle.scale-125.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x AlarmsSplashScreen.contrast-block_scale-125.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x GetStartedMedTitle.scale-200.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x GetStartedMedTitle.scale-256_contrast-black.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x GetStartedApplist.targetsize_24_contrast-black.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x GetStartedApplist.targetsize_36_alfForm-unplated_contrast-black.				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x GetStartedApplist.targetsize_48_alfForm-unplated.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x Applist.applarge_72_alfForm-unplated.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x Applist.applarge_125.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x Applist.targetsize_60_alfForm-unplated_contrast-black.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x Applist.targetsize_64_contrast-black.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x LargeFile.scale-100_contrast-black.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x SmallFile.scale-200_contrast-black.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m
x Applist.targetsize_256_alfForm-unplated_contrast-white.png				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/m

Exemple d'un fichier supprimé avec plus d'information :

x SmallFile.scale-200_contrast-black.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/img_Window
x Applist.targetsize_256_alfForm-unplated_contrast-white			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/img_Window
x Applist.targetsize_48_contrast-white.png			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown	/img_Window

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Metadata

Name: /img_Windows10.img/Program Files/Microsoft.HEIFImageExtension_1.0.13472.0_x64_8wekyb3d8bbwe/Assets/contrast-black/SmallTitle.scale-200_contrast-black.png

Type: File System

MDME Type: application/octet-stream

Size: 0

File Name Allocation: Unallocated

Metadata Allocation:

Modified: 0000-00-00 00:00:00

Accessed: 0000-00-00 00:00:00

Created: 0000-00-00 00:00:00

Changed: 0000-00-00 00:00:00

MD5: Not calculated

SHA-256: Not calculated

Hash Lookup Results: UNKNOWN

Internal ID: 173011

From the Sleuth Kit istat Tool:

No Data

La liste des exécutables :

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
setup.exe				2019-12-01 01:55:40 WET	2020-01-09 09:42:56 WET	2021-10-27 12:38:43 WET	2019-12-03 01:55:40 WET	46826	Allocated	Allocated	unknown	/img_Windows10
msiClientInstaller.exe				2019-06-05 12:59:36 WET	2020-01-09 12:02:47 WET	2020-02-05 13:25:23 WET	2020-01-09 12:03:03 WET	14599960	Allocated	Allocated	unknown	/img_Windows10
SetupChiset.exe				2020-01-09 12:01:32 WET	2020-01-22 15:42:05 WET	2021-10-27 12:38:44 WET	2020-01-09 12:01:32 WET	2179216	Allocated	Allocated	unknown	/img_Windows10
VC_redist.x64.exe				2020-01-21 08:09:12 WET	2020-01-22 15:42:35 WET	2021-10-27 12:38:49 WET	2020-01-21 08:10:44 WET	654632	Allocated	Allocated	unknown	/img_Windows10
setup.exe				2019-06-05 12:02:47 WET	2020-01-09 12:02:43 WET	2020-02-05 13:25:23 WET	2020-01-09 12:03:04 WET	89544680	Allocated	Allocated	unknown	/img_Windows10
ConfigSecurePolicy.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2020-01-09 11:42:48 WET	2020-01-09 11:42:48 WET	309776	Allocated	Allocated	unknown	/img_Windows10
McPinRun.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2021-10-27 12:28:28 WET	2020-01-09 11:42:48 WET	156642	Allocated	Allocated	unknown	/img_Windows10
McPinRun.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2021-10-27 12:28:28 WET	2020-01-09 11:42:48 WET	469646	Allocated	Allocated	unknown	/img_Windows10
McPinRun.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2021-10-27 12:28:28 WET	2020-01-09 11:42:48 WET	233015	Allocated	Allocated	unknown	/img_Windows10
McPinRun.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2021-10-27 12:17:59 WET	2020-01-09 11:42:48 WET	103376	Allocated	Allocated	unknown	/img_Windows10
McPinRun.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2021-10-27 12:17:59 WET	2020-01-09 11:42:48 WET	61454	Allocated	Allocated	unknown	/img_Windows10
NsDriver.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2021-10-27 12:18:27 WET	2020-01-09 11:42:48 WET	3206472	Allocated	Allocated	unknown	/img_Windows10
NsDriver.exe				2020-01-09 11:42:48 WET	2020-02-18 07:11:11 WET	2021-10-27 12:18:27 WET	2020-01-09 11:42:48 WET	1929428	Allocated	Allocated	unknown	/img_Windows10
opdf.exe				2021-02-16 15:26:22 WET	2021-10-27 12:25:53 WET	2021-10-27 12:25:53 WET	2021-02-17 12:25:53 WET	170976	Allocated	Allocated	unknown	/img_Windows10

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Exemple d'un programme python qui est installé dans ce disque : cette analyse des ce types de fichiers nous permet de détecter s'il y a un processus malveillant installé

				2021-02-16 15:27:08 WET	2021-10-27 12:25:58 WET	2021-10-27 12:25:58 WET	2021-10-27 12:25:58 WET	97944	Allocated	Allocated	unknown	/img_Windows10.	
	python.exe				2021-02-16 15:27:08 WET	2021-10-27 12:25:58 WET	2021-10-27 12:25:58 WET	2021-10-27 12:25:58 WET	96408	Allocated	Allocated	unknown	/img_Windows10.
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences													
Page:	1	of	6	Page	Go to Page:	1	Jump to Offset		Launch in HxD				
0x000000000: 4D 5A 00 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....													
0x00000010: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....													
0x00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00													
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00													
0x00000040: 0E 1F BA 00 00 B4 09 CD 21 BB 01 4C CD 21 64 E8!..L..Th													
0x00000050: 69 73 20 70 72 EF 67 72 61 ED 20 63 61 E6 EF EF is program canno													
0x00000060: 74 20 E2 65 20 72 75 EE 20 E9 EE 20 44 F8 53 20 t be run in DOS													
0x00000070: E9 EF E4 65 2E 0D 0A 20 00 00 00 00 00 00 mode...\$.....													
0x00000080: 7A FF 7D 60 3E 9E 13 33 3E 9E 13 33 3E 9E 13 33 z.~>..3>..3													
0x00000090: 37 B6 80 33 34 98 13 33 00 C0 12 32 3C 98 13 33 7..34..3..2<..3													
0x000000A0: 00 C0 10 32 3F 98 13 33 00 C0 16 32 2C 98 13 3327..3..2..3													
0x000000B0: 05 CO 17 32 33 98 13 33 AC CO 12 32 3D 98 13 3323..3..2=..3													
0x000000C0: 1C FF 12 32 3C 98 13 33 3E 9E 12 33 10 98 13 3324..3..3..3													
0x000000D0: AC CO 1B 32 3F 98 13 33 AC CO EC 33 3F 98 13 3327..3..3?..3													
0x000000E0: AC CO 11 32 3F 98 13 33 52 E9 E8 68 3E 98 13 3327..3Rich>..3													
0x000000F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00-----													
0x00000100: 50 45 00 4C 01 06 00 98 BB BB SA 00 00 00 00 PE..L..Z....													
0x00000110: 00 00 00 00 E0 02 01 00 01 00 00 00 00 00 00 00-----													
0x00000120: 00 00 01 00 00 00 00 00 93 12 00 00 00 10 00 00 P.....-----													

Aussi, on peut analyser les fichiers enregistrés au niveau du fichier d'un utilisateur normal :

Listing /img_Windows10.img/Users/UIR-B2/Documents												
Table Thumbnail Summary												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2021-10-27 12:26:24 WET	2021-10-27 12:27:12 WET	2020-01-09 09:33:07 WET	56	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
[parent folder]				2021-10-27 12:22:22 WET	2021-10-27 12:27:35 WET	2020-01-09 09:33:06 WET	360	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
ArcGIS 10.7.1				2020-02-13 07:20:33 WET	2020-02-13 07:30:32 WET	2020-02-13 07:30:32 WET	144	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
My Pictures				2020-01-09 09:33:07 WET	2020-01-09 09:33:07 WET	2020-01-09 09:33:07 WET	48	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
My Videos				2020-01-09 09:33:07 WET	2020-01-09 09:33:07 WET	2020-01-09 09:33:07 WET	48	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
PassMark				2021-10-27 12:26:41 WET	2021-10-27 12:26:41 WET	2021-10-27 12:26:41 WET	256	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
desktop.ini				2020-01-20 16:32:42 WET	2020-01-20 16:32:42 WET	2020-01-20 16:32:42 WET	402	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
Sauvegarde EasyBCD (2020-01-09).bcd				2020-01-09 15:05:27 WET	2020-01-09 15:05:27 WET	2020-01-09 15:05:27 WET	32768	Allocated	Allocated	unknown	/img_Windows10.img/Users/U	
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences												
Page: 1	of	1	Pages:	Go to Page:	1	Jump to Offset		Launch in HxD				

La liste des logiciels installées :

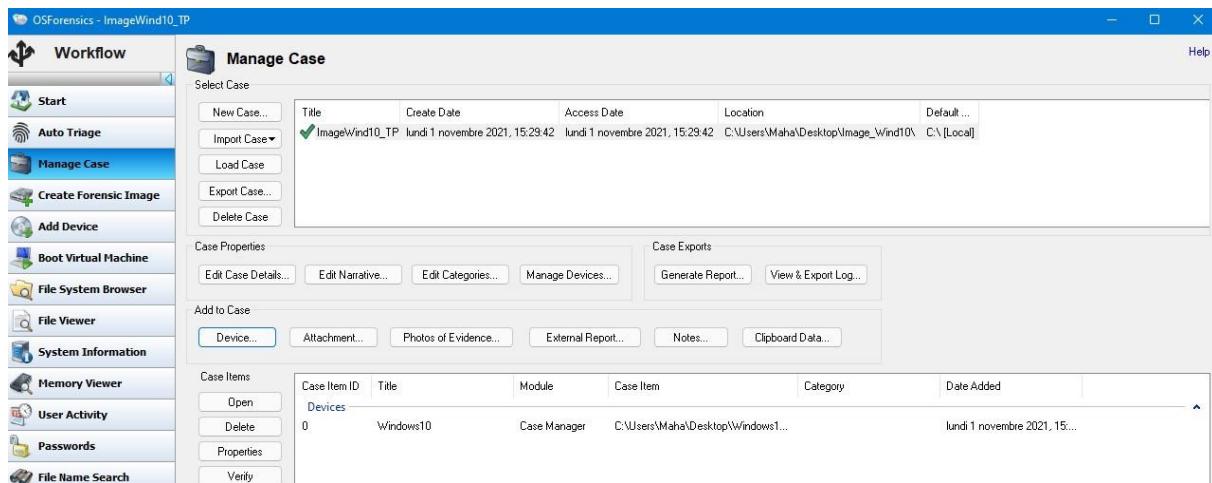
Listing /img_Windows10.img/Program Files												
Table Thumbnail Summary												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Microsoft Office				2020-01-23 14:44:40 WET	2021-10-27 12:27:10 WET	2020-01-09 12:55:11 WET	240	Allocated	Allocated	unknown	/img_Windows10.i	
Microsoft SQL Server				2020-01-09 12:57:08 WET	2020-01-09 12:57:08 WET	2020-01-09 12:57:07 WET	136	Allocated	Allocated	unknown	/img_Windows10.i	
Microsoft .NET				2020-01-09 12:57:22 WET	2020-01-09 12:37:46 WET	2020-01-09 12:37:46 WET	152	Allocated	Allocated	unknown	/img_Windows10.i	
ModifiableWindowsApps				2019-03-19 05:52:44 WET	2020-01-09 18:16:51 WET	2020-02-18 07:45:39 WET	48	Allocated	Allocated	unknown	/img_Windows10.i	
Mozilla Firefox				2020-01-22 16:09:32 WET	2020-01-27 12:37:46 WET	2020-01-09 09:47:53 WET	56	Allocated	Allocated	unknown	/img_Windows10.i	
MSBuild				2020-01-09 09:28:31 WET	2020-01-27 12:37:46 WET	2020-01-09 09:28:31 WET	256	Allocated	Allocated	unknown	/img_Windows10.i	
Notepad++				2020-01-22 15:26:51 WET	2020-01-27 12:37:46 WET	2020-01-22 15:26:51 WET	56	Allocated	Allocated	unknown	/img_Windows10.i	
Oracle				2020-01-22 16:37:14 WET	2020-10-27 12:21:50 WET	2020-01-21 08:08:09 WET	464	Allocated	Allocated	unknown	/img_Windows10.i	
OSForensics				2021-10-27 12:26:15 WET	2021-10-27 12:26:15 WET	2021-10-27 12:28:12 WET	200	Allocated	Allocated	unknown	/img_Windows10.i	
Realtek				2020-01-09 09:43:39 WET	2020-01-09 09:43:39 WET	2020-01-09 09:43:39 WET	144	Allocated	Allocated	unknown	/img_Windows10.i	
Reference Assemblies				2020-01-09 09:28:31 WET	2020-10-27 12:17:50 WET	2020-01-09 09:28:31 WET	256	Allocated	Allocated	unknown	/img_Windows10.i	
Sublime Text 3				2020-01-22 15:28:34 WET	2020-01-22 15:28:34 WET	2020-10-27 12:37:47 WET	56	Allocated	Allocated	unknown	/img_Windows10.i	
Uninstall Information				2020-01-09 09:20:24 WET	2020-01-09 09:20:24 WET	2020-10-27 12:37:47 WET	48	Allocated	Allocated	unknown	/img_Windows10.i	
Windows Defender				2020-01-09 13:11:46 WET	2020-10-27 12:18:00 WET	2019-03-19 05:52:44 WET	56	Allocated	Allocated	unknown	/img_Windows10.i	
Windows Defender Advanced Threat Protection				2020-01-15 14:10:07 WET	2020-01-15 14:10:07 WET	2020-02-18 07:45:46 WET	2019-03-19 07:22:01 WET	56	Allocated	Allocated	unknown	/img_Windows10.i
Windows Mail				2019-03-19 05:52:50 WET	2020-01-09 18:16:51 WET	2020-02-18 07:45:46 WET	2019-03-19 05:52:44 WET	352	Allocated	Allocated	unknown	/img_Windows10.i
Windows Media Player				2020-01-09 13:11:46 WET	2020-01-09 13:11:46 WET	2019-03-19 07:45:46 WET	56	Allocated	Allocated	unknown	/img_Windows10.i	
Windows Multimedia Platform				2019-03-19 07:22:01 WET	2020-01-09 18:16:51 WET	2020-02-18 07:45:47 WET	2019-03-19 07:22:01 WET	152	Allocated	Allocated	unknown	/img_Windows10.i
Windows NT				2019-03-19 06:02:05 WET	2020-01-09 18:16:51 WET	2020-02-18 07:45:47 WET	2019-03-19 05:52:44 WET	480	Allocated	Allocated	unknown	/img_Windows10.i
Windows Photo Viewer				2020-01-09 13:11:46 WET	2020-01-09 13:11:46 WET	2020-02-18 07:45:47 WET	2019-03-19 07:22:01 WET	56	Allocated	Allocated	unknown	/img_Windows10.i
Windows Portable Devices				2019-03-19 07:22:01 WET	2020-01-09 18:16:51 WET	2020-02-18 07:45:47 WET	2019-03-19 07:22:01 WET	152	Allocated	Allocated	unknown	/img_Windows10.i
Windows Security				2019-03-19 05:52:44 WET	2020-01-09 18:16:51 WET	2020-02-18 07:45:47 WET	2019-03-19 05:52:44 WET	152	Allocated	Allocated	unknown	/img_Windows10.i
Windows Sidebar				2019-03-19 05:52:44 WET	2020-01-09 18:16:51 WET	2020-02-18 07:45:47 WET	2019-03-19 05:52:44 WET	256	Allocated	Allocated	unknown	/img_Windows10.i
WindowsApps				2020-01-09 13:01:02 WET	2020-01-09 13:01:02 WET	2021-10-27 12:27:03 WET	2019-03-19 05:52:44 WET	288	Allocated	Allocated	unknown	/img_Windows10.i
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences												
Page: 1	of	1	Pages:	Go to Page:	1	Jump to Offset		Launch in HxD				

Cas 2 : Analyse approfondie d'une image de disque (cas réel : win10 UIR) Avec OSForensics

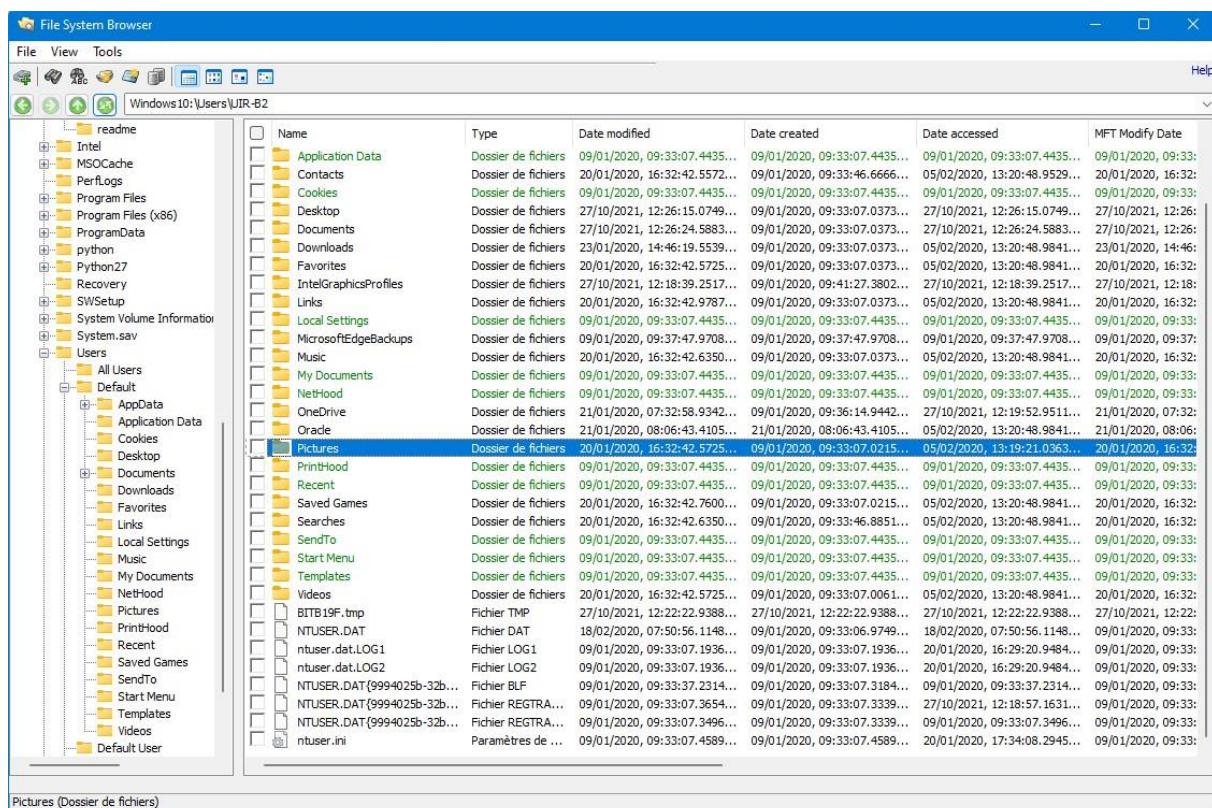
Dans cette étape nous allons analyser la même image de disque avec OSforensics.

OSForensics fournit l'un des moyens les plus rapides et les plus puissants de localiser des fichiers sur un ordinateur Windows. OSForensics Extrayez les données médico-légales des ordinateurs, plus rapidement et plus facilement que jamais. Découvrez tout ce qui se cache à l'intérieur d'un PC.

Création d'une case et on ajoute l'image de disque dur externe :

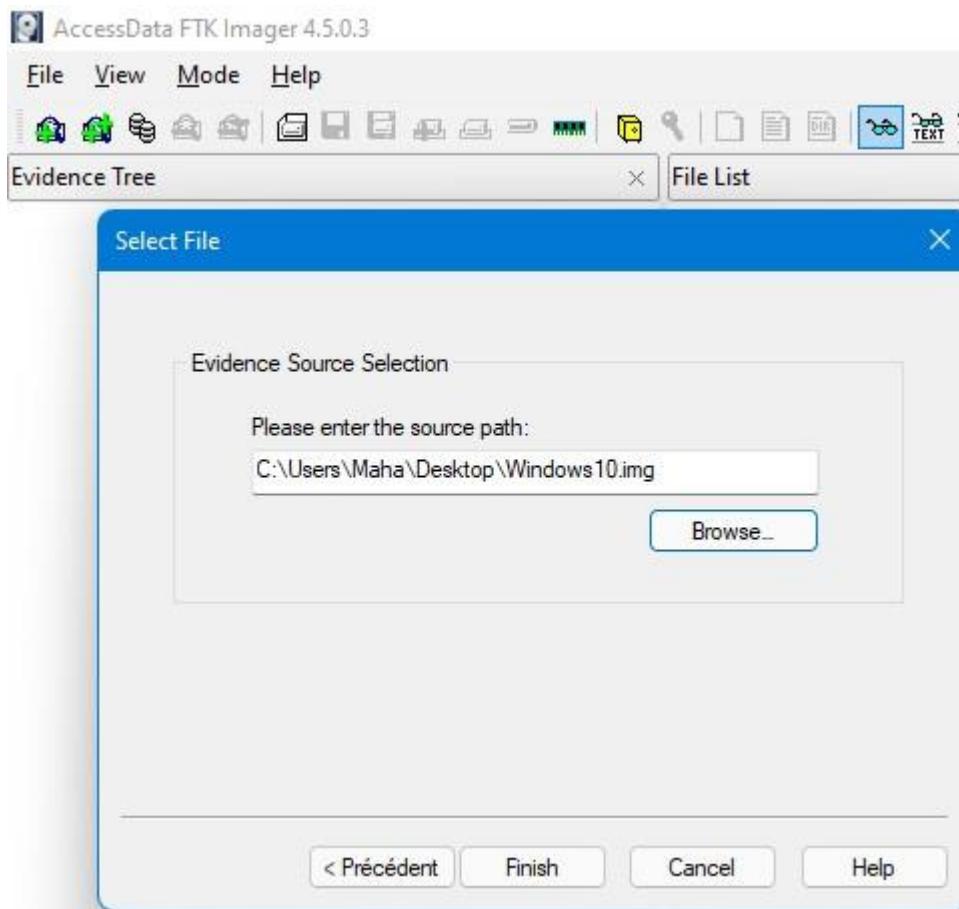


Après on scanne les fichiers systèmes :



On remarque les trois fichiers NTUSER.DAT, ntuser.dat.LOG1, ntuser.dat.LOG2 , on peut utiliser Registry Explorer pour analyser la base de registre de ce système comme on a déjà fait dans les parties précédentes.

On utilise FTK Imager pour l'exportation des ruches

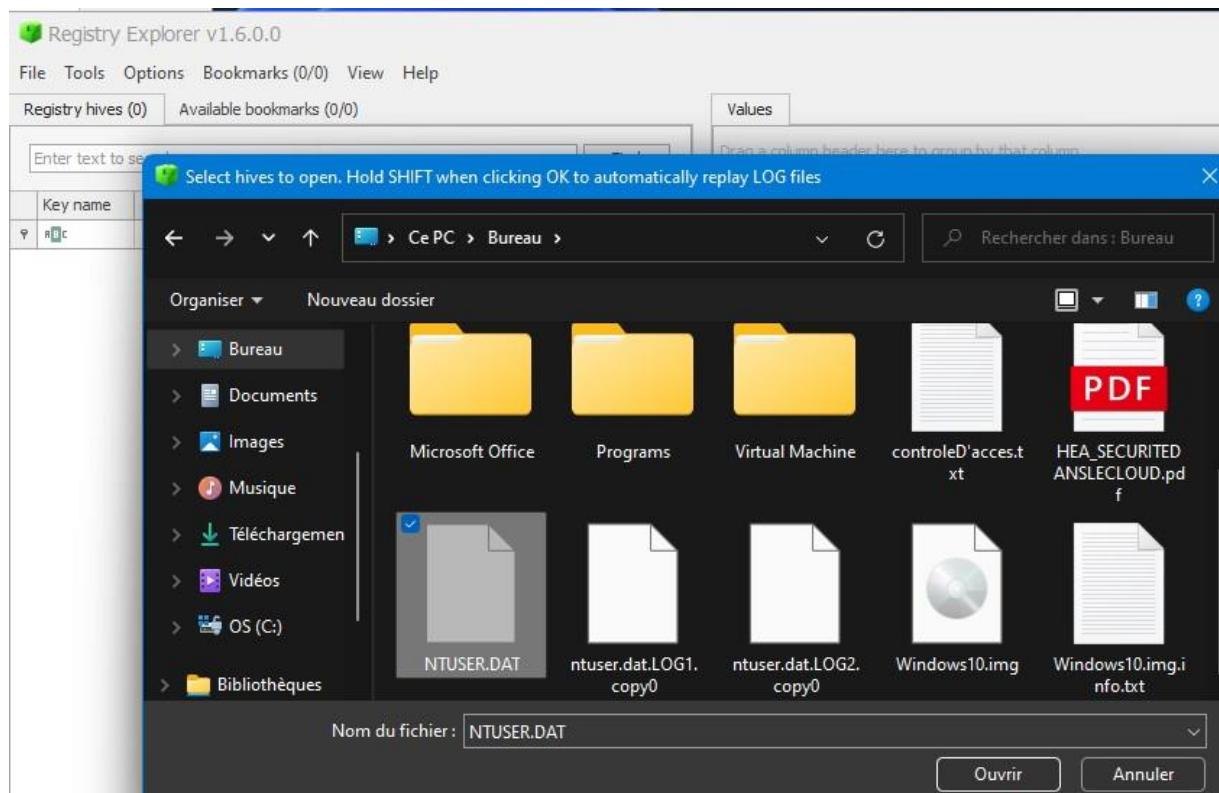


On exporte :

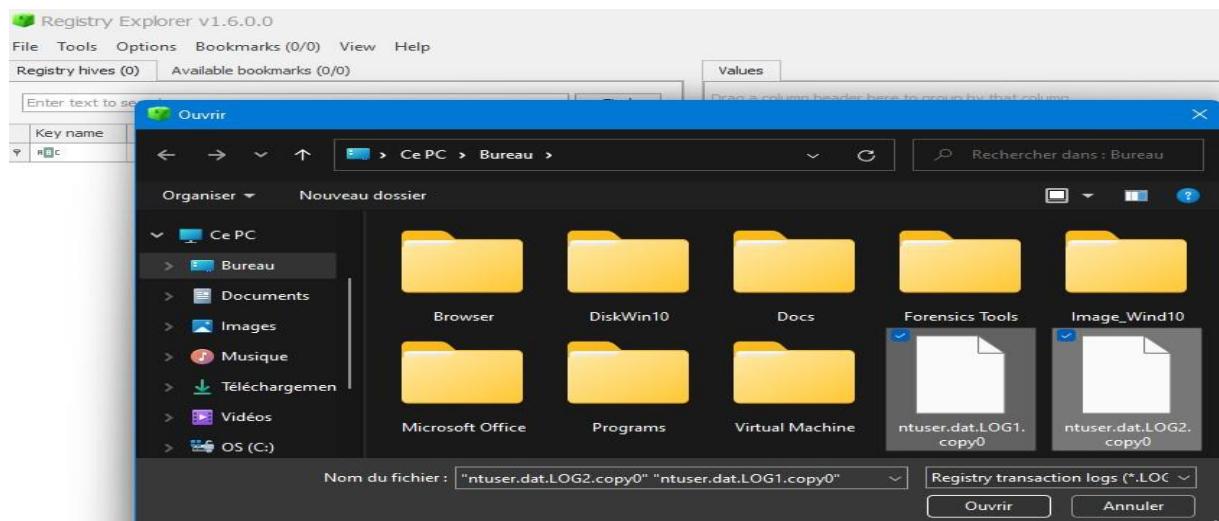
\$TxF_DATA	1	NTFS Logged ...	27/10/2021 11:22:22
BITB19F.tmp	0	Regular File	27/10/2021 11:22:22
NTUSER.DAT	2 048	Regular File	18/02/2020 06:50:56
NTUSER.DAT.FileSlack	200	File Slack	
ntuse	496	Regular File	09/01/2020 08:33:07
ntuse	100	File Slack	
ntuse	680	Regular File	09/01/2020 08:33:07
NTUS		\$130 INDX Entry	



Dans Registry Explorer : importation des ruches



Importe ntuser.dat.LOG1 et ntuser.dat.LOG2 :



Registry Explorer v1.6.0.0				
File Tools Options Bookmarks (27/0) View Help				
Registry hives (2)		Available bookmarks (54/0)		
Enter text to search...				Find
Key name	# values	# subkeys	Last write timestamp	
?	=	=	=	
↻ C:\Users\Maha\Desktop\N...			1601-01-01 00:00:00	
Accounts	1	1	2021-10-27 11:27:34	
Applets	0	1	2020-01-09 08:35:13	
CD Burning	2	2	2020-01-09 08:35:14	
ComDlg32	0	4	2020-01-22 15:16:38	
CurrentVersion	0	63	2020-01-22 15:37:13	
CurrentVersion	0	15	2020-01-10 06:48:54	
Environment	4	0	2020-01-22 14:43:02	
FeatureUsage	1	5	2020-01-09 08:41:31	
FileExts	0	219	2021-10-27 11:27:34	
FileHistory	0	1	2020-01-09 08:33:07	
FTP	1	0	2020-01-20 15:32:42	
History	1	0	2020-01-09 08:33:40	
Internet Settings	12	11	2020-01-09 14:54:54	
Main	35	2	2020-01-23 13:00:07	
MountPoints2	0	12	2021-10-27 11:25:13	

Analyse des registres d'image de disque win10 :

Registry Explorer v1.6.0.0				
File Tools Options Bookmarks (27/0) View Help				
Registry hives (2)		Available bookmarks (54/0)		
Enter text to search...				Find
Key name	# values	# subkeys	Last write timestamp	
?	=	=	=	
↻ C:\Users\Maha\Desktop\N...			1601-01-01 00:00:00	
Accounts	1	1	2021-10-27 11:27:34	
Applets	0	1	2020-01-09 08:35:13	
CD Burning	2	2	2020-01-09 08:35:14	
ComDlg32	0	4	2020-01-22 15:16:38	
CurrentVersion	0	63	2020-01-22 15:37:13	
CurrentVersion	0	15	2020-01-10 06:48:54	
Environment	4	0	2020-01-22 14:43:02	
FeatureUsage	1	5	2020-01-09 08:41:31	
FileExts	0	219	2021-10-27 11:27:34	
FileHistory	0	1	2020-01-09 08:33:07	
FTP	1	0	2020-01-20 15:32:42	
History	1	0	2020-01-09 08:33:40	
Internet Settings	12	11	2020-01-09 14:54:54	
Main	35	2	2020-01-23 13:00:07	
MountPoints2	0	12	2021-10-27 11:25:13	

-Analysons les derniers PID les plus utilisés récemment :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Values [ComDlg32 LastVisitedPidlMRU]				
	Value Name	Mru Position	Executable	Absolute Path
0	=	=	chrome.exe	My Computer\Desktop
				2020-01-22 15:03:49

-Analysons les fichiers ouverts ou enregistrés récemment par une application via la boîte de dialogue du shell Windows :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

Values [ComDlg32 OpenSavePidlMRU]				
	Extension	Value Name	Mru Position	Absolute Path
0	*.c	=	=	=
2				0 G:\image\Windows10.img
0	cpp	0		0 SansNom1.cpp
0	img	0		0 G:\image\Windows10.img
0	py	0		0 My Computer\Desktop\get-pip.py
1	*	1		1 SansNom1.cpp
0	=	0		2 My Computer\Desktop\get-pip.py

Dans OSForensics:

-Scan User activity

The screenshot shows the OSForensics interface for Windows 10. The left sidebar contains a navigation menu with options like Workflow, Start, Auto Triage, Manage Case, Create Forensic Image, Add Device, Boot Virtual Machine, File System Browser, File Viewer, System Information, Memory Viewer, User Activity (which is selected and highlighted in blue), Passwords, File Name Search, Deleted Files Search, Mismatch Files Search, Program Artifacts, ThumbCache Viewer, Registry Viewer, Raw Disk Viewer, Email Viewer, Create Index, Search Index, Signatures, and Analyze Shadow Copies.

The main area is titled "User Activity" and displays a summary of user activity. A modal dialog box titled "User Activity - Summary" is open, showing a list of activity types and their counts: Most Recently Used: 95, Installed Programs: 799, Autorun Commands: 4, Clipboard: 0, Event Logs: 1434, UserAssist: 139, Jump Lists: 46, Shellbags: 53, Windows 10 Timeline: 236, BAM/DAM: 20, Downloads: 72, Browser History: 70, Website Logins: 1, Form History: 11, Bookmarks: 7, USB: 30, Mounted Volumes: 5. The total items listed are 3022.

The main table lists activity details for user UIR-B2, sorted by time (descending). The columns include Item, Activity Type, User, Time, Time Source, and Flags. Key entries include:

- Most Recently Used [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Installed Programs [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Autorun Commands [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Clipboard [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Event Logs [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- UserAssist [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Jump Lists [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Shellbags [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Windows 10 Timeline [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- BAM/DAM [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Downloads [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Browser History [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Website Logins [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Form History [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Bookmarks [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- USB [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Mounted Volumes [Image] UIR-B2 27/10/2021, 12:27:34 Date Last Accessed
- Total Items: 3022

-La liste des programmes et fichiers les plus utilisés par utilisateur UIRB2 :

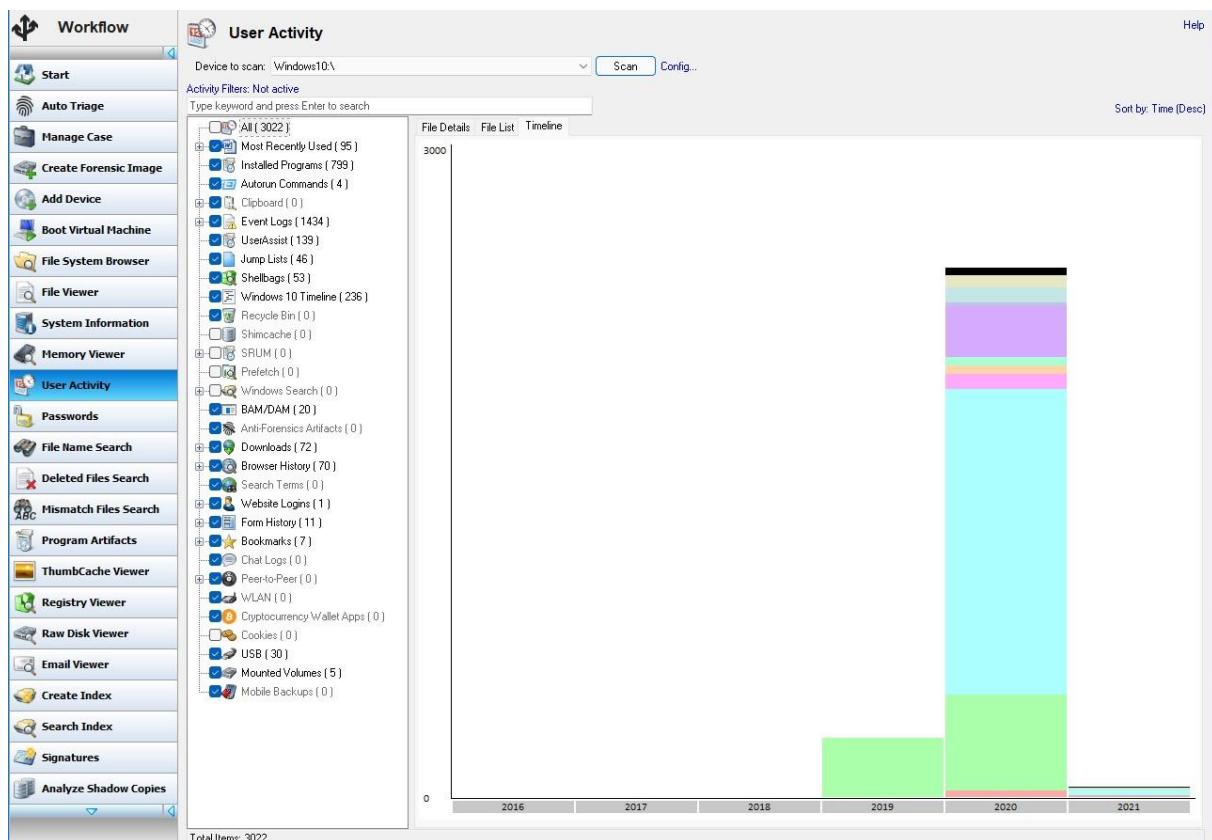
The screenshot shows the OSForensics interface for Windows 10. The left sidebar contains a navigation menu with options like Workflow, Start, Auto Triage, Manage Case, Create Forensic Image, Add Device, Boot Virtual Machine, File System Browser, File Viewer, System Information, Memory Viewer, User Activity (which is selected and highlighted in blue), Passwords, File Name Search, Deleted Files Search, Mismatch Files Search, Program Artifacts, ThumbCache Viewer, Registry Viewer, Raw Disk Viewer, Email Viewer, Create Index, Search Index, Signatures, and Analyze Shadow Copies.

The main area is titled "User Activity" and displays a summary of user activity. A modal dialog box titled "User Activity - Summary" is open, showing a list of activity types and their counts: Most Recently Used: 95, Installed Programs: 799, Autorun Commands: 4, Clipboard: 0, Event Logs: 1434, UserAssist: 139, Jump Lists: 46, Shellbags: 53, Windows 10 Timeline: 236, BAM/DAM: 20, Downloads: 72, Browser History: 70, Website Logins: 1, Form History: 11, Bookmarks: 7, USB: 30, Mounted Volumes: 5. The total items listed are 3022.

The main table lists activity details for user UIR-B2, sorted by time (descending). The columns include Item, Category, Path, Date Last Accessed, Window, Evidence Location, and Flags. Key entries include:

- Most Recently Used [Recent Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- Installed Programs [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\AppData\Roa...
- Autorun Commands [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- Clipboard [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\AppData\Roa...
- Event Logs [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- UserAssist [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- Jump Lists [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- Shellbags [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- Windows 10 Timeline [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- BAM/DAM [Link (Shortcut) Files] UIR-B2 27/10/2021, 12:27:34 Windows10\Users\UIR-B2\NTUSER.DAT...
- Downloads [Link (Shortcut) Files] UIR-B2 23/01/2020, 14:42:04 Windows10\Users\UIR-B2\AppData\Roa...
- Browser History [Link (Shortcut) Files] UIR-B2 23/01/2020, 14:42:04 Windows10\Users\UIR-B2\AppData\Roa...
- Website Logins [Link (Shortcut) Files] UIR-B2 23/01/2020, 14:42:04 Windows10\Users\UIR-B2\AppData\Roa...
- Form History [Recent Files] UIR-B2 23/01/2020, 14:42:04 Windows10\Users\UIR-B2\AppData\Roa...
- Bookmarks [Recent Files] UIR-B2 23/01/2020, 14:42:04 Windows10\Users\UIR-B2\AppData\Roa...
- USB [Recent Files] UIR-B2 23/01/2020, 14:42:04 Windows10\Users\UIR-B2\AppData\Roa...
- Mounted Volumes [Recent Files] UIR-B2 23/01/2020, 14:42:04 Windows10\Users\UIR-B2\AppData\Roa...
- Total Items: 3022

-Le temps d'utilisation :



-La liste des fichiers log :

User Activity							Help				
Device to scan: Windows10\		Scan	Config...								
Activity Filters: Active (Match Any)		log									
log											
Item	Activity Type	User	Time	Time Source	Flags						
Driver Installation Comp...	Event Logs		27/10/2021, 12:25:13	Event Time							
Driver Installation Comp...	Event Logs		27/10/2021, 12:25:13	Event Time							
Installing/Updating De...	Event Logs		27/10/2021, 12:25:13	Event Time							
Driver Installation Comp...	Event Logs		27/10/2021, 12:25:13	Event Time							
Service Addition Proces...	Event Logs		27/10/2021, 12:25:12	Event Time							
Installing/Updating De...	Event Logs		27/10/2021, 12:25:12	Event Time							
Driver Installation Comp...	Event Logs		27/10/2021, 12:25:12	Event Time							
Service Addition Proces...	Event Logs		27/10/2021, 12:25:12	Event Time							
Installing/Updating De...	Event Logs		27/10/2021, 12:25:11	Event Time							
Completed Processing Us...	Event Logs		27/10/2021, 12:18:25	Event Time							
Received User Logon ...	Event Logs		27/10/2021, 12:18:24	Event Time							
Successful Logon	Event Logs	UIR-B2	27/10/2021, 12:18:23	Event Time							
Successful Logon	Event Logs	UIR-B2	27/10/2021, 12:18:23	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:18:23	Event Time							
Successful Logoff	Event Logs	OracleVsvWiredORCL	27/10/2021, 12:18:07	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:17:59	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:17:59	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:17:59	Event Time							
System Uptime	Event Logs		27/10/2021, 12:17:52	Event Time							
Event Log Service Star...	Event Logs		27/10/2021, 12:17:52	Event Time							
Successful Logon	Event Logs	DWM-1	27/10/2021, 12:17:50	Event Time							
Successful Logon	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:17:50	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:17:50	Event Time							
Successful Logon	Event Logs	UMFD-1	27/10/2021, 12:17:49	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:17:49	Event Time							
Successful Logon	Event Logs	UMFD-0	27/10/2021, 12:17:49	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	27/10/2021, 12:17:49	Event Time							
Successful Logon	Event Logs	Système	27/10/2021, 12:17:49	Event Time							
Device Connected/Dis...	Event Logs		27/10/2021, 12:17:17	Event Time							
Windows Update Succ...	Event Logs		27/10/2021, 12:17:16	Event Time							
Operating System Start...	Event Logs		27/10/2021, 12:17:16	Event Time							
Operating System Shut...	Event Logs		18/02/2020, 07:51:13	Event Time							
Event Log Service Star...	Event Logs		18/02/2020, 07:50:57	Event Time							
Finished Processing Us...	Event Logs		18/02/2020, 07:50:56	Event Time							
Received User Logoff ...	Event Logs		18/02/2020, 07:50:55	Event Time							
User Initiated Logoff	Event Logs		18/02/2020, 07:50:55	Event Time							
Process Initiated Power...	Event Logs		18/02/2020, 07:50:50	Event Time							
Service Start Type Cha...	Event Logs		18/02/2020, 07:44:19	Event Time							
Service Start Type Cha...	Event Logs		18/02/2020, 07:35:35	Event Time							
Service Start Type Cha...	Event Logs		18/02/2020, 07:35:34	Event Time							
Service Start Type Cha...	Event Logs		18/02/2020, 07:26:40	Event Time							
Failed Logon Attempts	Event Logs	UIR-B2	18/02/2020, 07:26:25	Event Time							
Finished Processing Us...	Event Logs		18/02/2020, 07:16:12	Event Time							
Received User Logon ...	Event Logs		18/02/2020, 07:16:12	Event Time							
Successful Logon	Event Logs	UIR-B2	18/02/2020, 07:16:11	Event Time							
Successful Logon	Event Logs	UIR-B2	18/02/2020, 07:16:11	Event Time							
Logon Attempted Using...	Event Logs	DESKTOP-D6N10MM\$	18/02/2020, 07:16:11	Event Time							
Successful Logon	Event Logs	OracleVsvWiredORCL	18/02/2020, 07:15:52	Event Time							

Aucun réseau Wifi enregistré trouvé, cela indique que cette machine ne se connecte pas à un réseau Wifi

The screenshot shows the 'User Activity' interface with the following details:

- Device to scan:** Windows10\
- Activity Filters:** Active (Match Any)
- File Details:** File List, Timeline
- Sort by:** Time (Desc)
- Log Types:**
 - All (3022)
 - Most Recently Used (9)
 - Installed Programs (799)
 - Autorun Commands (4)
 - Clipboard (0)
 - Event Logs (1434)
 - UserAssist (139)
 - Jump Lists (46)
 - Shellbags (53)
 - Windows 10 Timeline (2)
 - Recycle Bin (0)
 - Shimcache (0)
 - SRUM (0)
 - Prefetch (0)
 - Windows Search (0)
 - BAM/DAM (20)
 - Anti-Forensics Artifacts (2)
 - Downloads (72)
 - Browser History (70)
 - Search Terms (0)
 - Website Logins (1)
 - Form History (11)
 - Bookmarks (7)
 - Chat Logs (0)
 - Peer-to-Peer (0)
 - WLAN (0)
 - Cryptocurrency Wallet (0)
 - Cookies (0)
 - USB (30)
 - Mounted Volumes (5)
 - Mobile Backups (0)

La liste d'historique Web :

The screenshot shows the 'User Activity' interface with the following details:

- Device to scan:** Windows10\
- Activity Filters:** Active (Match Any)
- File Details:** File List, Timeline
- Sort by:** Time (Desc)
- Log Types:**
 - All (3022)
 - Most Recently Used (9)
 - Installed Programs (799)
 - Autorun Commands (4)
 - Clipboard (0)
 - Event Logs (1434)
 - UserAssist (139)
 - Jump Lists (46)
 - Shellbags (53)
 - Windows 10 Timeline (2)
 - Recycle Bin (0)
 - Shimcache (0)
 - SRUM (0)
 - Prefetch (0)
 - Windows Search (0)
 - BAM/DAM (20)
 - Anti-Forensics Artifacts (2)
 - Downloads (72)
 - Browser History (70)
 - Search Terms (0)
 - Website Logins (1)
 - Form History (11)
 - Bookmarks (7)
 - Chat Logs (0)
 - Peer-to-Peer (0)
 - WLAN (0)
 - Cryptocurrency Wallet (0)
 - Cookies (0)
 - USB (30)
 - Mounted Volumes (5)
 - Mobile Backups (0)

Title	URL	Date Last Accessed	Visit Count	Browser	Username	Profile
file:///G:/image/Windo...	file:///G:/image/Windoo...	27/10/2021, 12:27:34	1	Internet Explorer	UIR-B2	
file:///G:/	file:///G:/	27/10/2021, 12:26:38	1	Internet Explorer	UIR-B2	
file:///G:/image	file:///G:/image	27/10/2021, 12:26:38	0	Internet Explorer	UIR-B2	
ms-gamingoverlay://sta...	ms-gamingoverlay://startu...	27/10/2021, 12:19:53	0	Internet Explorer	UIR-B2	
https://get.adobe.com...	https://get.adobe.com/rh...	09/01/2020, 09:53:47	1	Microsoft Edge	UIR-B2	
https://get.adobe.com...	https://get.adobe.com/rh...	09/01/2020, 09:53:47	1	Internet Explorer	UIR-B2	
https://get.adobe.com/	https://get.adobe.com/	09/01/2020, 09:53:26	0	Internet Explorer	UIR-B2	
https://get.adobe.com/	https://get.adobe.com/	09/01/2020, 09:53:26	0	Microsoft Edge	UIR-B2	
https://get.adobe.com/	https://get.adobe.com/rh...	09/01/2020, 09:52:16	1	Microsoft Edge	UIR-B2	
https://get.adobe.com/	https://get.adobe.com/rh...	09/01/2020, 09:52:16	1	Internet Explorer	UIR-B2	
Firefox Politique de co...	https://www.mozilla.org/f...	09/01/2020, 09:48:15	1	Firefox	UIR-B2	
https://www.mozilla.or...	https://www.mozilla.org/p...	09/01/2020, 09:48:14	1	Firefox	UIR-B2	bni9bx8d.default-releas...
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:49	2	Internet Explorer	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:49	2	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:48	0	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:48	0	Internet Explorer	UIR-B2	
https://dl.google.com/...	https://dl.google.com/ta...	09/01/2020, 09:37:41	1	Microsoft Edge	UIR-B2	
https://dl.google.com/...	https://dl.google.com/ta...	09/01/2020, 09:37:41	1	Internet Explorer	UIR-B2	
https://dl.google.com/...	https://dl.google.com/ta...	09/01/2020, 09:37:41	0	Internet Explorer	UIR-B2	
https://dl.google.com/...	https://dl.google.com/ta...	09/01/2020, 09:37:41	0	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	0	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	0	Internet Explorer	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	1	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	1	Internet Explorer	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	1	Internet Explorer	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	1	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	1	Internet Explorer	UIR-B2	
https://www.google.co...	https://www.google.co/v...	09/01/2020, 09:37:38	1	Microsoft Edge	UIR-B2	
about://	about://	09/01/2020, 09:37:37	0	Internet Explorer	UIR-B2	
about://	about://	09/01/2020, 09:37:37	0	Internet Explorer	UIR-B2	
about://	about://	09/01/2020, 09:37:37	0	Microsoft Edge	UIR-B2	
about://	about://	09/01/2020, 09:37:37	0	Internet Explorer	UIR-B2	
https://www.google.co...	https://www.google.co.ma...	09/01/2020, 09:37:35	1	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co.ma...	09/01/2020, 09:37:35	2	Internet Explorer	UIR-B2	
https://www.google.co...	https://www.google.co.ma...	09/01/2020, 09:37:35	2	Microsoft Edge	UIR-B2	
https://www.google.co...	https://www.google.co.ma...	09/01/2020, 09:37:35	n	Microsoft Edge	UIR-B2	

-Exemple d'un fichiers log que j'ai consulté pour avoir lus d'information :

Event Log Viewer

Select Event Logs

Drive: Windows10:\ Scan Drive Scan Folder

Filtering (showing 342 of 342 events)

Presets: -- Defaults -- Quick Filter Apply Advanced Filter

Timeline Filter: Off

Level	Date and Time	Source	Event ID	Task Category	User
Information-4	27/10/2021, 12:18:25	Microsoft-Windows-User P...	2	None	S-:
Information-4	27/10/2021, 12:18:25	Microsoft-Windows-User P...	5	None	S-:
Information-4	27/10/2021, 12:18:24	Microsoft-Windows-User P...	67	None	S-:
Information-4	27/10/2021, 12:18:24	Microsoft-Windows-User P...	5	None	S-:
Information-4	27/10/2021, 12:18:24	Microsoft-Windows-User P...	1	None	S-:
Information-4	27/10/2021, 12:18:01	Microsoft-Windows-User P...	5	None	S-:
Information-4	27/10/2021, 12:18:01	Microsoft-Windows-User P...	5	None	S-:
Information-4	27/10/2021, 12:18:01	Microsoft-Windows-User P...	5	None	S-:

General Details

Session: 1

Traitement de la notification d'ouverture de session utilisateur terminé pour la session 1.

Log Name: Microsoft-Windows-User Profile Service OpCode: Informations

Source: Microsoft-Windows-User Profiles Service Logged: 27/10/2021, 12:18:25

Event ID: 2 Task Category: None

Level: Information Keywords:

User: S-1-5-21-2158224076-766019520-3378 Computer: DESKTOP-D6N10MM

-Consulter un fichier History de Google chrome

File System Browser

File View Tools

Windows 10:\Users\UIR-B2\AppData\Local\Google\Chrome\User Data\Default

Name	Type	Date modified	Date created	Date accessed	MFT Modify Date
001316.ldb	Microsoft Access	23/01/2020, 14:46:03.5464...	23/01/2020, 14:46:03.5455...	23/01/2020, 14:46:03.5464...	23/01/2020, 14:46:
Cookies	Fichier	23/01/2020, 14:46:06.3421...	09/01/2020, 09:38:26.2018...	05/02/2020, 13:21:53.2919...	23/01/2020, 14:46:
Cookies-journal	Fichier	23/01/2020, 14:46:06.8883...	09/01/2020, 09:38:26.2018...	23/01/2020, 14:46:06.8883...	23/01/2020, 14:46:
CURRENT	Fichier	23/01/2020, 14:46:03.4993...	09/01/2020, 09:39:03.5132...	23/01/2020, 14:46:03.4993...	23/01/2020, 14:46:
Current Session	Fichier	05/02/2020, 13:22:09.7588...	09/01/2020, 09:38:25.5196...	05/02/2020, 13:22:09.7588...	05/02/2020, 13:22:
Current Tabs	Fichier	05/02/2020, 13:22:09.7588...	09/01/2020, 09:38:23.3111...	05/02/2020, 13:22:09.7588...	05/02/2020, 13:22:
DownloadMetadata	Fichier	23/01/2020, 14:42:03.6680...	09/01/2020, 09:39:11.9983...	23/01/2020, 14:42:03.6680...	23/01/2020, 14:42:
Favicons	Fichier	23/01/2020, 14:46:07.6048...	09/01/2020, 09:38:24.5113...	05/02/2020, 13:21:51.4379...	23/01/2020, 14:46:
Favicons-journal	Fichier	23/01/2020, 14:46:07.5961...	09/01/2020, 09:38:24.5123...	23/01/2020, 14:46:07.5961...	23/01/2020, 14:46:
Google Profile.ico	Icone	09/01/2020, 09:38:24.6808...	09/01/2020, 09:38:24.6808...	09/01/2020, 15:04:03.1326...	09/01/2020, 09:38:
heavy_ad_intervention_opt...	Data Base File	09/01/2020, 09:38:29.1797...	09/01/2020, 09:38:28.8371...	05/02/2020, 13:22:11.3054...	09/01/2020, 09:38:
heavy_ad_intervention_opt...	Fichier DB-JOU...	09/01/2020, 09:38:29.2124...	09/01/2020, 09:38:28.8371...	09/01/2020, 09:38:29.2124...	09/01/2020, 09:38:
History	Fichier	23/01/2020, 14:46:08.0812...	09/01/2020, 09:38:23.0123...	05/02/2020, 13:21:51.4379...	23/01/2020, 14:46:
LocalStorage Cache	Fichier	23/01/2020, 14:46:08.0812...	09/01/2020, 09:38:23.0123...	05/02/2020, 13:21:51.4379...	23/01/2020, 14:46:

SQLite Database Browser

SQLite Database File: Windows10:\Users\UIR-B2\AppData\Local\Google\Chrome\User Data\Default\History

Table List

Table Contents

id	chain_index	url
1	0	https://get.videolan.org/vlc/3.0.8/win32/vlc-3.0.8-win...
1	1	https://ftp.ml.tecnico.ulisboa.pt/pub/videolan/vlc/3.0...
2	0	https://www.win-rar.com/postdownload.html?&=10
2	1	https://www.win-rar.com/fileadmin/winrar-versions/win...
3	0	https://get.adobe.com/fr/reader/download/?installer=...
3	1	https://adownload.adobe.com/bin/live/readerdc_fr...
4	0	https://www.mozilla.org/fr/firefox/all/#product=desktop...
4	1	https://download.mozilla.org/?product=firefox-latest-ssl...
5	0	https://download-installer.cdn.mozilla.net/pub/firefox/r...
14	0	https://www49.zippypshare.com/d/F0im3hX3/46250/m...
6	0	https://www114.zippypshare.com/d/1kjEpMf/21445/m...
7	0	https://www94.zippypshare.com/d/fYtdlYnR/41471/m...

Search Table Clear Search << < 1 to 100 of 110 > >>

Table Information

Column ID	Name	Type	Not Null
0	id	INTEGER	1
1	chain_index	INTEGER	1
2	...	LONGVARCHAR	1

Add DB to Case

-Passwords: les mots de passe qui sont enregistrés dans la machine

-Les fichiers supprimés :

-Les informations sur le système :

-Sur la carte réseau :

Network Info (Registry)

Date: mardi 2 novembre 2021, 11:07:29

Registry File: Windows10:\Windows\System32\Config\SYSTEM
Key Location: ControlSet001\services\Tcpip\Parameters\Interfaces
Timezone: +1:00

Network GUID	{b419bc18-32b8-11ea-8dea-806e6f6e6963}
Network Name	
IP (using DHCP)	(No)
Network GUID	{b86fb20-32f6-4ab4-a779-b58fbca656c5}
Network Name	Ethernet
IP (using DHCP)	(No)
Network GUID	{d655a026-f976-435c-b04d-24a7434bf345}
Network Name	VirtualBox Host-Only Network
IP (using DHCP)	(No)
Network GUID	{fc33b7c6-e146-40d4-bf4b-e115b0eea9e4}
Network Name	Ethernet (Kernel Debugger)
IP (using DHCP)	(Yes)
DHCP Server	
DHCP Name Server	
Lease Obtained	mercredi 22 janvier 2020, 15:17:34
Lease Expires	mercredi 22 janvier 2020, 15:17:34

-Sur les comptes utilisateurs :

User Info (Registry)

Date: mardi 2 novembre 2021, 11:07:29

Registry File: Windows10:\Windows\System32\Config\SAM
Key Location: SAM\Domains\Account\Users
Using Timezone: +1:00

Username [ID]	Administrator [500]
Full Name	
Description	Built-in account for administering the computer/domain
Password Hint	
Account Created	N/A
Last Login	Never
Password Reset	Never
Password Fail Date	N/A
Password Fail Count	0 (reset after correct login)
Login Count	0
Notes	*Password never expires*
Username [ID]	Guest [501]
Full Name	
Description	Built-in account for guest access to the computer/domain
Password Hint	
Account Created	jeudi 9 janvier 2020, 09:26:32 (can be inaccurate if registry permissions have been updated)
Last Login	Never
Password Reset	Never
Password Fail Date	N/A
Password Fail Count	0 (reset after correct login)
Login Count	0
Notes	*Password never expires*

Username [ID]	UIR-B2 [1001]
Full Name	UIR-B2-DEV
Description	
Password Hint	
Account Created	jeudi 9 janvier 2020, 09:26:32 (can be inaccurate if registry permissions have been updated)
Last Login	mercredi 27 octobre 2021, 12:18:23
Password Reset	lundi 13 janvier 2020, 11:12:54
Password Fail Date	lundi 13 janvier 2020, 10:23:44
Password Fail Count	0 (reset after correct login)
Login Count	50
Notes	*Password never expires*

-Sur le temps d'arrêt de la machine :

Shutdown Time (Registry)

Date: mardi 2 novembre 2021, 11:07:29

Registry File: Windows10:\Windows\System32\Config\SYSTEM

Key Location: ControlSet001\Control\Windows

Last shutdown time:	mardi 18 février 2020, 07:51:12
---------------------	---------------------------------

Sur le système d'exploitation installé :

Windows Info (Registry)

Date: mardi 2 novembre 2021, 11:07:29

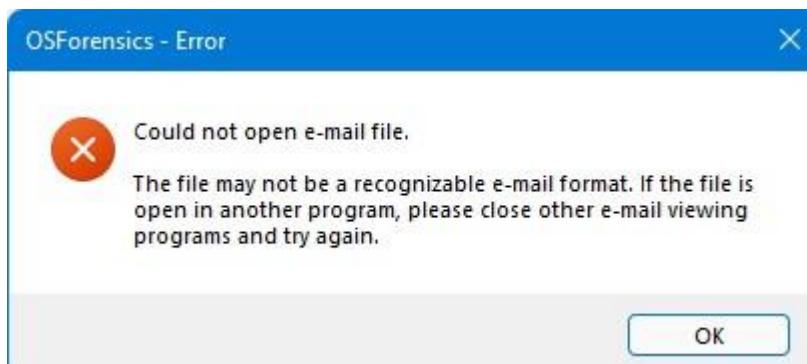
Registry File: Windows10:\Windows\System32\Config\SOFTWARE

Key Location: Microsoft\Windows NT\CurrentVersion

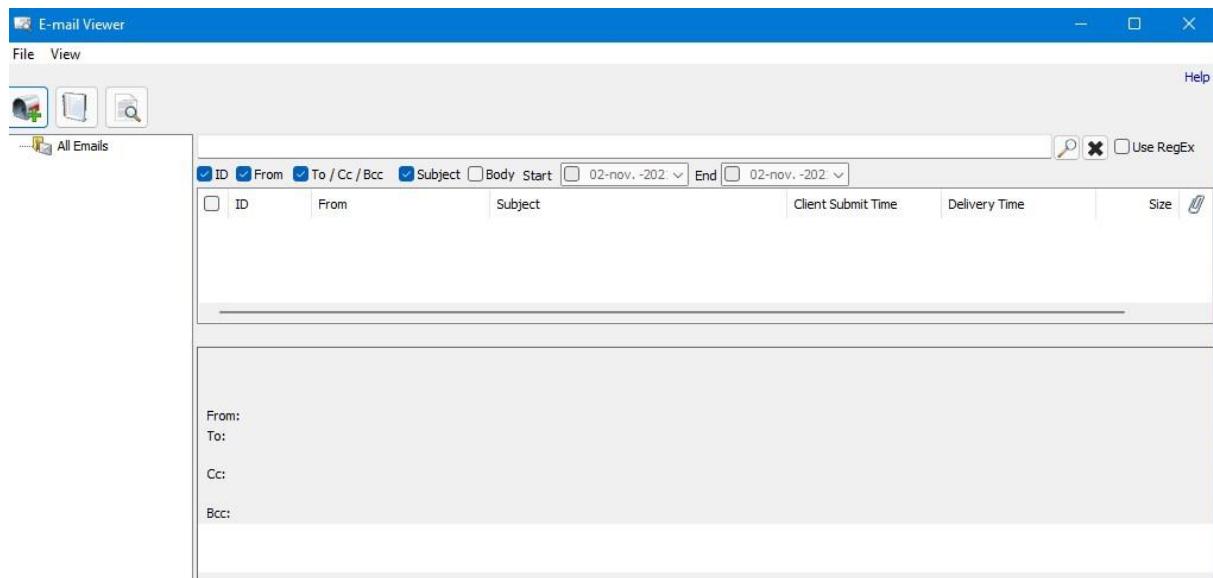
Timezone: +1:00

Install path	C:\Windows
Build string	18362.19h1_release.190318-1202
Extended build string	18362.1.amd64fre.19h1_release.190318-1202
Build number	18362
Install date	jeudi 9 janvier 2020, 09:29:10
ProductName	Windows 10 Pro
Version	1903
ProductId	00331-10000-00001-AA734
DigitalProductId	W269N-WFGWX-YVC9B-4J6C9-T83GX
RegisteredOwner	UIR-B2
RegisteredOrganization	

Pour les emails : je ne peux pas avoir un aperçu sur les emails, une erreur s'affiche lors de consulter email viewer :



Aucun courriel trouvé :



Les fichiers hachés :

The screenshot shows the "File Hashing" application interface. The title bar says "File Hashing". Below it is a navigation bar with tabs: "Hash Sets" (selected), "Verify/Create Hash", and "Hash Set Management". Under "Hash Sets", there are buttons for "New DB...", "Make DB Active", "New Set...", "Quick Set...", and "Import CSV Set...". On the right, there is a "Search Hash Sets:" field with arrows for navigation. The main pane displays a hierarchical tree view of hash sets. The tree includes categories like "Cryptocurrency", "Example", "NSRL" (with sub-categories "Web Browser", "Web Utility", and "zip"), "Keyloggers" (with sub-categories "PassMark" and "Keylogger" containing numerous entries), "P2P" (with sub-categories "PassMark" and "P2P" containing entries like "P2PBitComet", "P2PBitLord", etc.), and "VPN" (with sub-categories "PassMark" and "VPN" containing entries like "VPNBetternet", "VPNLexpress", etc.). Each entry in the tree provides information such as the file name, author, and language.

Conclusion :

Une analyse forensique fait suite à un incident, on utilise le forensique pour analyser les malwares c'est-à-dire surveiller un PC pour détecter des actions malveillantes, ou bien récupérer des preuves numériques. Il existe plusieurs domaines de forensique : forensique réseau qui se limitent à analyser la connexion réseau, etc.

Les différentes approches pour faire une analyse forensique :

Dans ce rapport on a fait de types d'approches, la première c'est analyse à chaud (live Forensics) on a utilisé Registry Explorer pour analyser la base de registre et étudier l'état du système qui allumé

La deuxième c'est l'analyse à froid (Dead Forensics) on a analysé à l'aide des outils OSforensics, Autopsy un système éteint, on a copié un ensemble de données d'une machine réel.