

INTRODUCTION À LA FORENSICS



HackInTn x hayb

14/05/24



SOMMAIRE

1. Quésaco ?
2. Un peu de théorie ...
3. ... mais surtout beaucoup de pratique
4. Annexes



1. QUÉSACO ?

- « Forensics » = médecin légiste 🤪
- « Investigation numérique » in french 😊
- Analyse de disques durs, de la mémoire vive, du réseau, ...
- Surtout un **mindset** ! Se mettre dans la tête des attaquants ...



2.UN PEU DE THÉORIE ...

- **Analyse de disques durs - Windows**

Disque 0 De base 953,85 Go En ligne			
	100 Mo Sain (Partition du système EFI)	(C:) 952,99 Go NTFS Sain (Démarrer, Fichier d'échange, Image mémoire après incident, Partition de données de base)	781 Mo Sain (Partition de récupération)

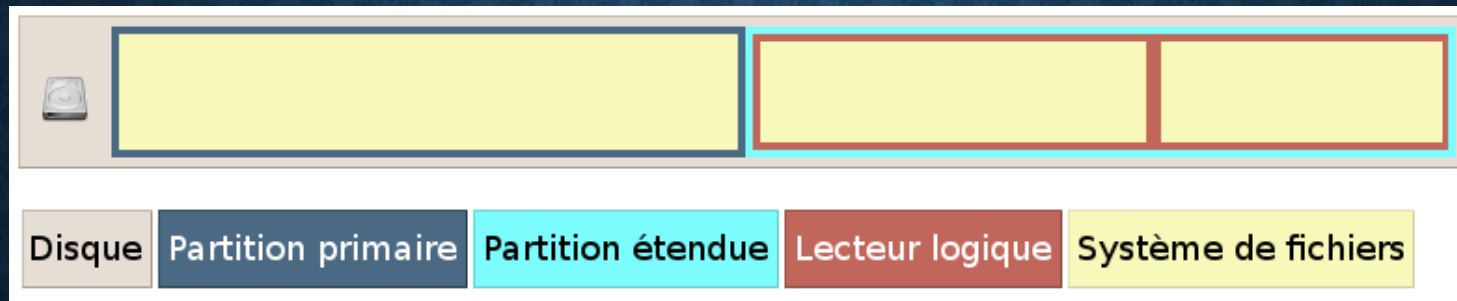
1.EFI (Extensible Firmware Interface) : logiciel qui remplace le BIOS (Basic Input/Output System), charge le système d'exploitation à partir du disque dur, généralement formatée en FAT32.

2.NTFS (New Technology File System) : système de fichiers utilisé par Windows.

3.Partition de récupération : partition spéciale sur le disque dur qui contient les fichiers nécessaires pour récupérer ou réinstaller le système d'exploitation en cas de défaillance.

2.UN PEU DE THÉORIE ...

- **Analyse de disques durs - Linux**



Le système de fichiers par défaut est **ext4**.

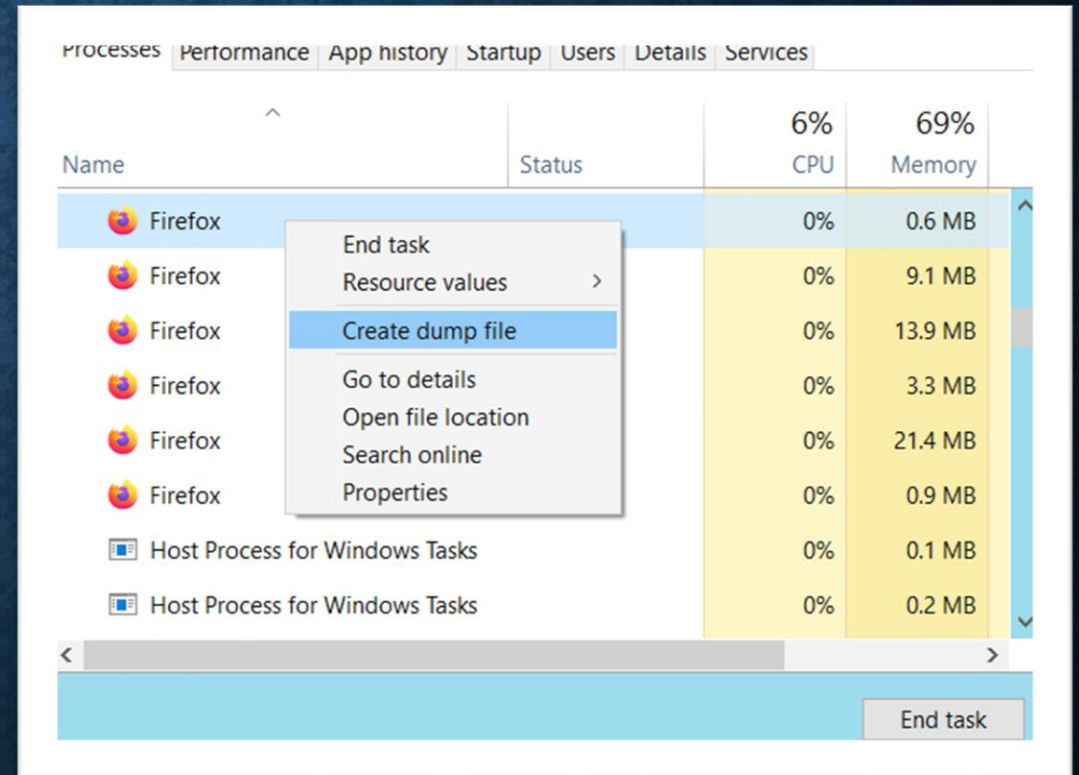
- **Partitions primaires / principales** : type de partition le plus utilisé, permet de stocker des données en MBR
- **Partition étendue** : utilisé pour dépasser la limite des 4 partitions principales.

Puis la partition de démarrage des disques GPT (GUID Partition Table) :

- **Partitions EFI** : partition de démarrage pour les disques GPT sur les PC UEFI, formatée en FAT32 et stocke le firmware EFI.

2.UN PEU DE THÉORIE ...

- **Analyse de mémoire vive**
- Les fichiers de *dump* (en .dmp) contiennent une *photographie* des informations de bas niveau associées à l'application qui a planté.
- liste des programmes en cours d'exécution, état des registres et de la pile du microprocesseur, un listing en hexa. du contenu de la mémoire allouée à l'application.



2.UN PEU DE THÉORIE ...

tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

> Ethernet II, Src: Globalsec_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21

> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

▼ Domain Name System (response)

[Request In: 348]

[Time: 0.034338000 seconds]

Transaction ID: 0x2188

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 9

Additional RRs: 9

▼ Queries

> cdn-0.nflximg.com: type A, class IN

> Answers

> Authoritative nameservers

0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5.... ?!....

0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6cc dn-0.nfl

0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com

0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73). ".images

0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg

0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et../...

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

2.UN PEU DE THÉORIE ...

Analyse réseau - notions intéressantes :

HTTPS/HTTP : protocole de communication client/serveur pour le web, chiffré ou non

TCP : protocole de contrôle de transmission (handshaking puis échange des paquets numérotés et vérification à chaque fois)

UDP : protocole de datagramme utilisateur, pas d'échange permanent, envoie de paquets non numérotés à la machine de destination, mais sans la prévenir. Il n'y a pas de conversation.

SSH : Secure Shell - programme informatique et un protocole de communication sécurisé. Impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés.

2.UN PEU DE THÉORIE ...

Analyse réseau - notions intéressantes :

SSL/TLS : Sécurité de la couche de transport, protocoles de sécurisation des échanges par Internet. La *TLS* (ou *SSL*) fonctionne suivant un mode client-serveur.

- l'authentification du serveur ;
- la confidentialité des données échangées (ou session chiffrée) ;
- l'intégrité des données échangées ;

FTP : protocole de transfert de fichier, destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

DNS : Système de nom de domaine, service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements.

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'outils sous Linux

```
(kali㉿kali)-[~/Documents/challenge]
$ ls
boule-1.pdf  boule-2.pdf  image.img

(kali㉿kali)-[~/Documents/challenge]
$ file image.img
image.img: DOS/MBR boot sector

(kali㉿kali)-[~/Documents/challenge]
$ strings image.img | head
ZRR=
`lf
\\f1
GRUB
Geom
Hard Disk
Read
Error
EFI PART
hHML
```

```
(kali㉿kali)-[~/Documents/challenge]
$ fdisk -l image.img
Disk image.img: 6 GiB, 6442450944 bytes, 12582912 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 3249E840-24CF-40DC-BDC8-FD95544D3951

Device            Start      End  Sectors  Size Type
image.img1         2048     18431    16384    8M BIOS boot
image.img2        18432  11552767  11534336  5.5G Linux root (x86-64)
image.img3       11552768  12582878   1030111  503M Linux filesystem
```


3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'outils sous Linux

```
(kali㉿kali)-[~/Documents/challenge]
$ mmls image.img
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors
```

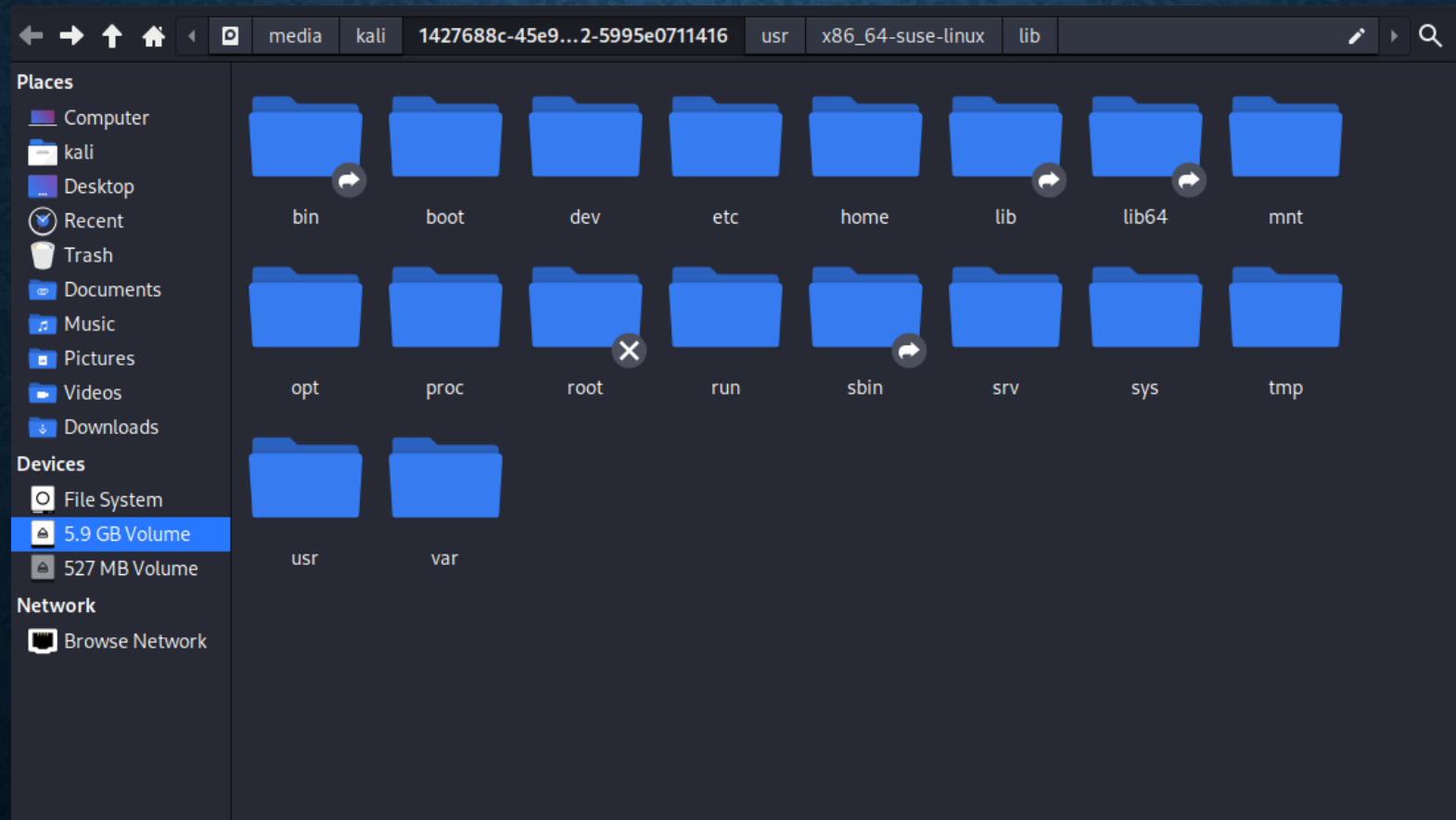
	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Safety Table
001:	———	0000000000	0000002047	0000002048	Unallocated
002:	Meta	0000000001	0000000001	0000000001	GPT Header
003:	Meta	0000000002	0000000033	0000000032	Partition Table
004:	000	0000002048	0000018431	0000016384	
005:	001	0000018432	0011552767	0011534336	
006:	002	0011552768	0012582878	0001030111	
007:	———	0012582879	0012582911	0000000033	Unallocated

```
(kali㉿kali)-[~/Documents/challenge]
$ sudo losetup -fP image.img
```

```
sudo mount /dev/sdb1 /mnt/media
```

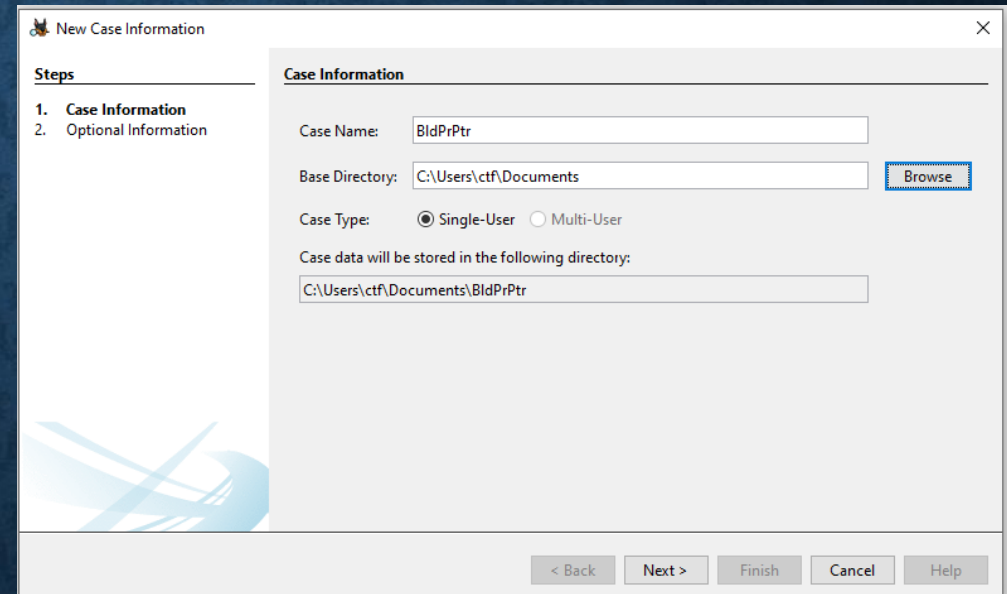
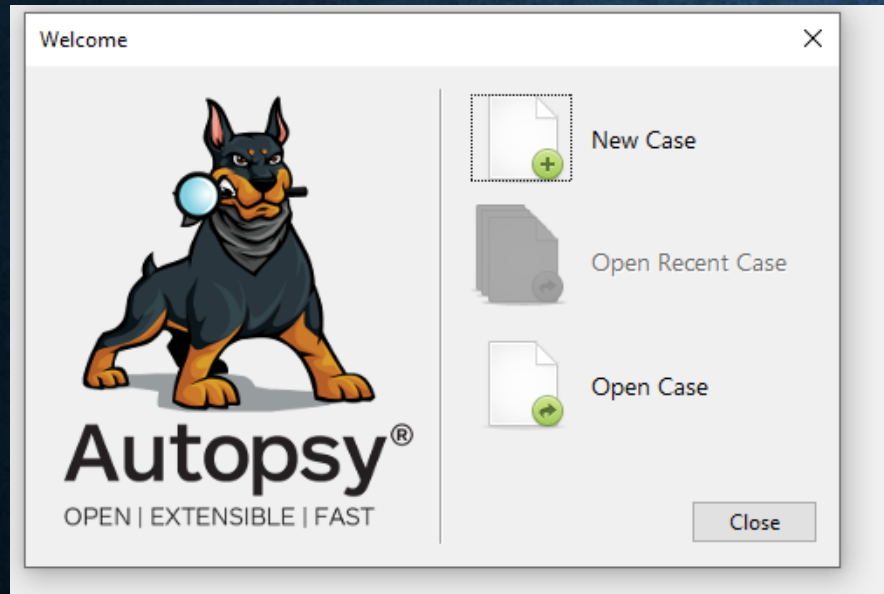
3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'outils sous Linux



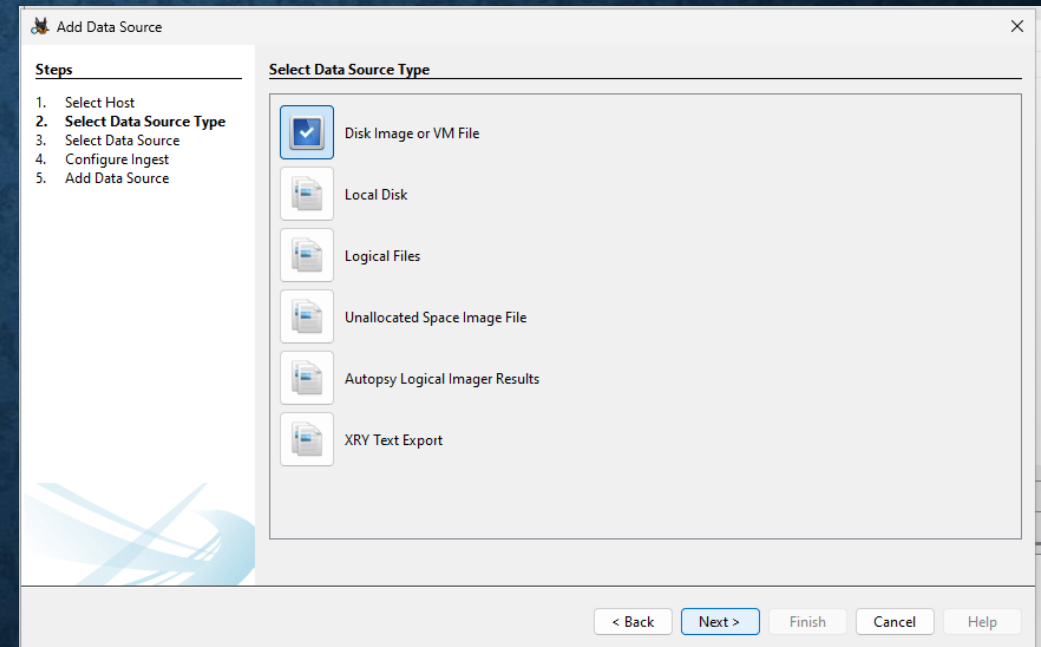
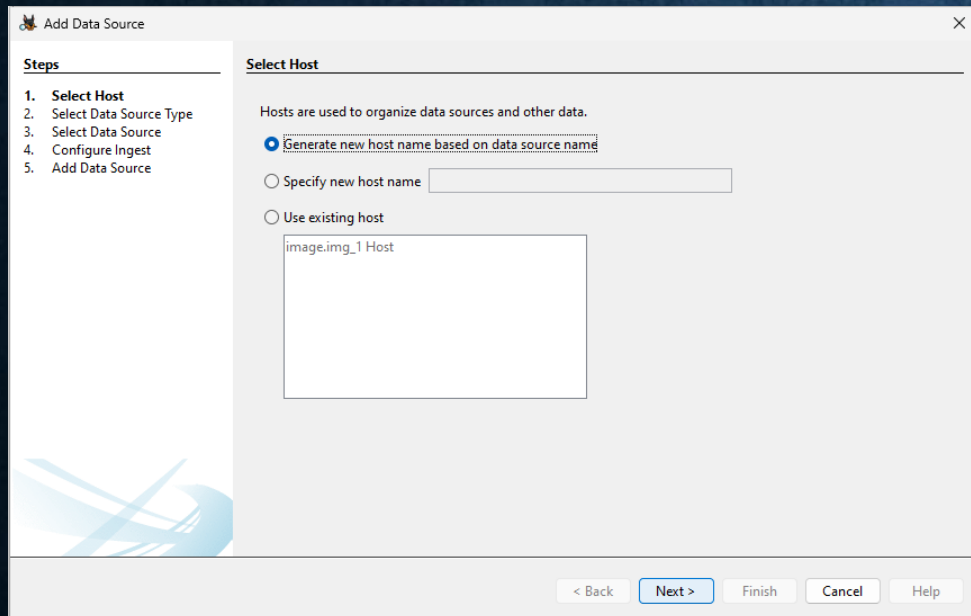
3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'Autopsy



3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'Autopsy



3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'Autopsy

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\User\Documents\boulevard_pointer\image.img Browse

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

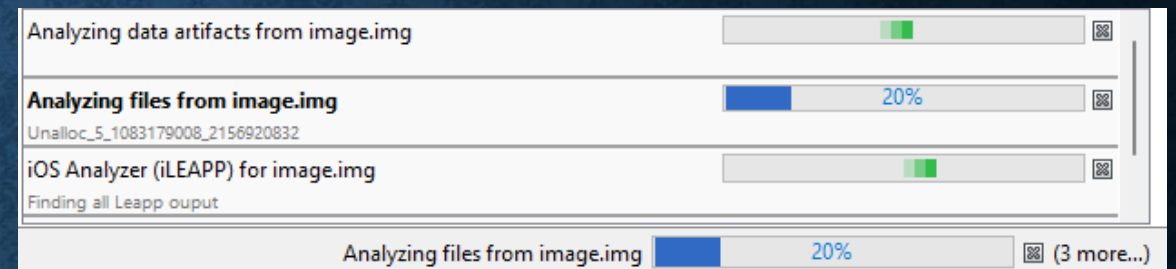
MD5:

SHA-1:

SHA-256:

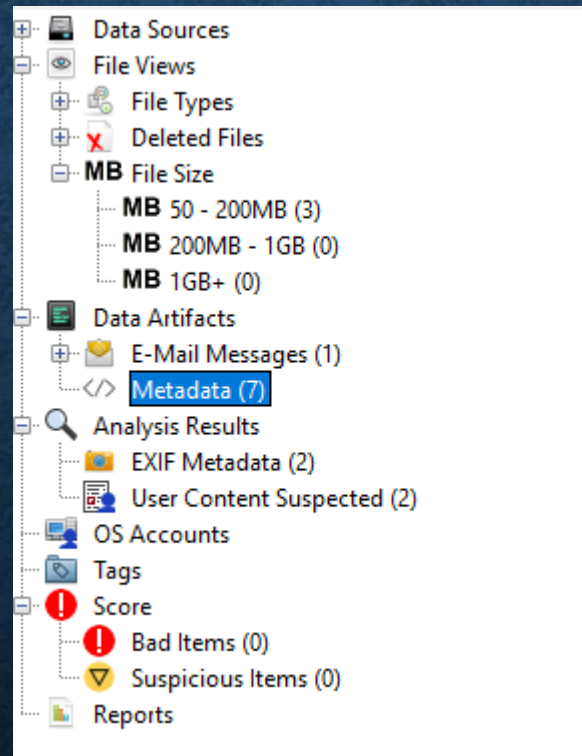
NOTE: These values will not be validated when the data source is added.

< Back Next > Finish Cancel Help



3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'Autopsy




3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE


- Démonstration d'une analyse disque à l'aide d'Autopsy

Source Name	S	C	O	Version	Date Created	Owner	Date Modified	Data Source	S	C	O
</> f1861416_GhostscriptDocumentation.pdf				1.5	2024-03-06 08:58:13 PST	Artifex	2024-03-06 08:58:13 PST	image.img			
</> f1848424.pdf				1.5	2021-04-01 20:53:56 PDT		2021-04-01 20:53:56 PDT	image.img			
</> f1394392.h						Jesse Glick <jglick@cloudbees.com>		image.img			
</> f0833448.pdf				1.5	2024-03-07 14:06:13 PST		2024-03-07 14:06:13 PST	image.img			
</> f0834184.pdf				1.5	2018-01-20 17:43:25 PST			image.img			
</> f0832680_AppArmorTechnicalDocumentation.pdf				1.5	2024-02-02 22:13:05 PST	Andreas Gruenbacher and Seth Arnold	2024-02-02 22:13:05 PST	image.img			
</> f1783544.pdf				1.7	2024-04-30 17:01:17 PDT			image.img			

Data Content

HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

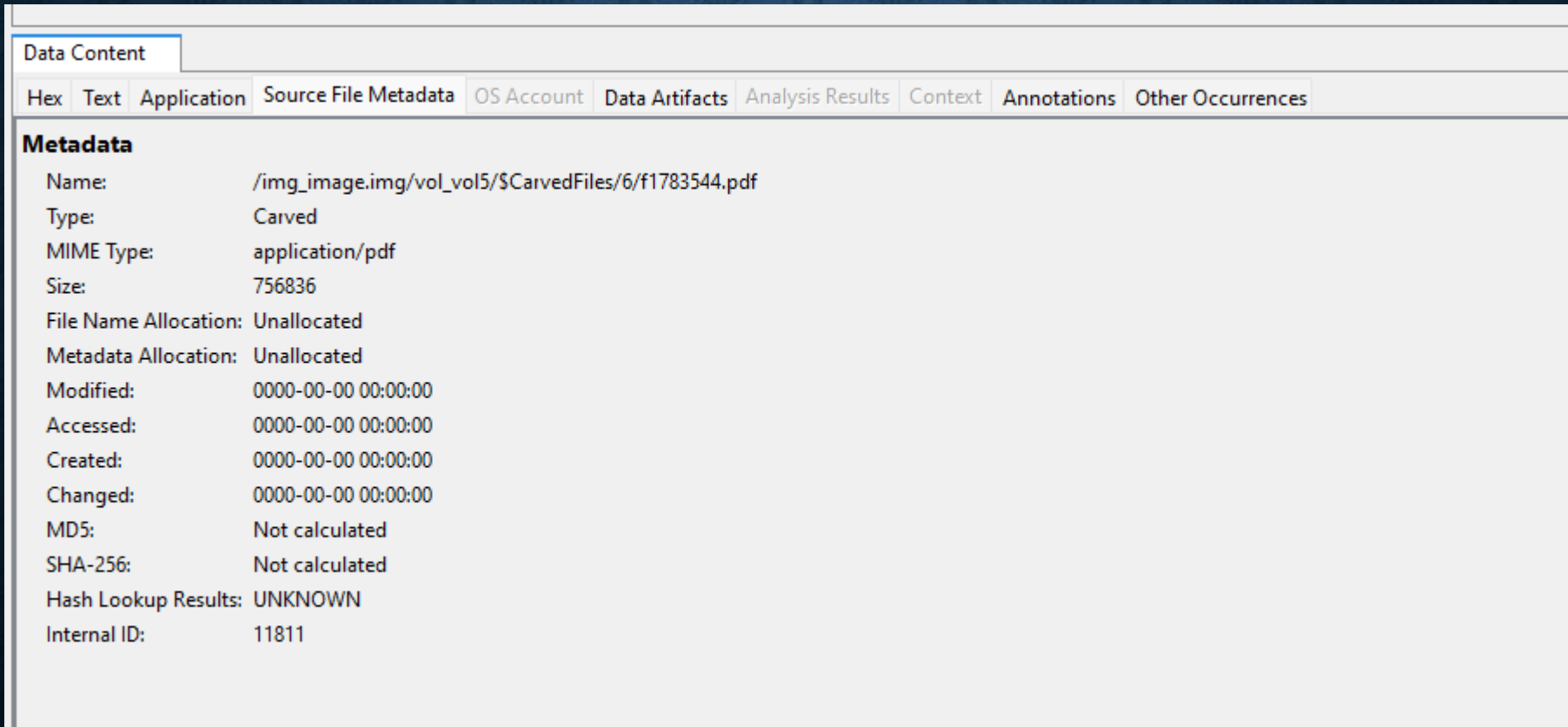



[Source](#)

404CTF{ bi 1_j oué_br 4vo_c_l e_f l 4g}

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'Autopsy



The screenshot shows the Autopsy interface with the 'Data Content' tab selected. The 'Source File Metadata' sub-tab is active, displaying the following metadata for a file:

Metadata	
Name:	/img_image.img/vol_vol5/\$CarvedFiles/6/f1783544.pdf
Type:	Carved
MIME Type:	application/pdf
Size:	756836
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
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:	11811

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse disque à l'aide d'Autopsy

Data Content	
Hex	Text
Application	Source File Metadata
OS Account	Data Artifacts
Analysis Results	Context
Annotations	Other Occurrences
Result: 1 of 1 Result < >	
Type	Value
Version	1.7
Date Created	2024-04-30 17:01:17 PDT
Source File Path	/img_image.img/vol_vol5/\$CarvedFiles/6/f1783544.pdf
Artifact ID	-9223372036854775796

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse de dump mémoire à l'aide de Volatility

```
(kali@Hugo)~[~/Documents/volatility3-develop]
$ python3 vol.py -f MEMORY.DMP isfinfo
Volatility 3 Framework 2.7.0
Progress: 100.00          PDB scanning finished
URI      Valid  Number of base_types  Number of types  Number of symbols  Number of enums  Identifying information
file:///home/kali/Documents/volatility3-develop/volatility3/symbols/windows/tcpip.pdb/ABB23D00EE7E4165B6AFF66F2DF02EB2-2
.json.xz  True (cached)  0      0      7313    0      b'tcpip.pdb|ABB23D00EE7E4165B6AFF66F2DF02EB2|2'
file:///home/kali/Documents/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb/3844DBB920174967BE7AA4A2C20430FA-2
.json.xz  True (cached)  14     880    18644   114    b'ntkrnlmp.pdb|3844DBB920174967BE7AA4A2C20430FA|2'
file:///home/kali/Documents/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb/039281E5F80D4711858194C121C9D89
D-1.json.xz  True (cached)  14    1436   33723   230    b'ntkrnlmp.pdb|039281E5F80D4711858194C121C9D89D|1'
file:///home/kali/Documents/volatility3-develop/volatility3/symbols/windows/tcpip.pdb/6E867CA47AABC85F750E8B1B5FBFC274-1
.json.xz  True (cached)  0      0      8811    0      b'tcpip.pdb|6E867CA47AABC85F750E8B1B5FBFC274|1'
file:///home/kali/Documents/volatility3-develop/volatility3/symbols/windows/ntkrnlmp.pdb/E2BA44E0E506968538EA272B1E5030C
5-1.json.xz  True (cached)  16    1652   39959   293    b'ntkrnlmp.pdb|E2BA44E0E506968538EA272B1E5030C5|1'
file:///home/kali/Documents/volatility3-develop/volatility3/symbols/windows/ntkrpamp.pdb/5B308B4ED6464159B87117C711E7340
C-2.json.xz  True (cached)  15     870   18517   110    b'ntkrpamp.pdb|5B308B4ED6464159B87117C711E7340C|2'
```


3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse de dump mémoire à l'aide de Volatility

```
(kali㉿Hugo)-[~/Documents/volatility3-develop]
$ python3 vol.py -h
Volatility 3 Framework 2.7.0
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS]
                  [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config]
                  [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--offline]
                  [--filters FILTERS] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
                  plugin ...

An open-source memory forensics framework

options:
  -h, --help                Show this help message and exit, for specific plugin options use 'volatility <pluginname>
                             --help'
  -c CONFIG, --config CONFIG
                             Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                             Enables parallelism (defaults to off if no argument given)
  -e EXTEND, --extend EXTEND
                             Extend the configuration with a new (or changed) setting
  -p PLUGIN_DIRS, --plugin-dirs PLUGIN_DIRS
                             Semi-colon separated list of paths to find plugins
  -s SYMBOL_DIRS, --symbol-dirs SYMBOL_DIRS
```

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse de dump mémoire à l'aide de Volatility

```
windows.bigpools.BigPools
    List big page pools.
windows.cachedump.Cachedump
    Dumps lsa secrets from memory
windows.callbacks.Callbacks
    Lists kernel callbacks and notification routines.
windows.cmdline.CmdLine
    Lists process command line arguments.
windows.crashinfo.Crashinfo
    Lists the information from a Windows crash dump.
windows.devicetree.DeviceTree
    Listing tree based on drivers and attached devices in a particular windows memory image.
windows.dlllist.DllList
    Lists the loaded modules in a particular windows memory image.
windows.driverirp.DriverIrp
    List IRPs for drivers in a particular windows memory image.
windows.drivermodule.DriverModule
    Determines if any loaded drivers were hidden by a rootkit
windows.driverscan.DriverScan
    Scans for drivers present in a particular windows memory image.
windows.dumpfiles.DumpFiles
    Dumps cached file contents from Windows memory samples.
```


3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse de dump mémoire à l'aide de Volatility

```
(kali@Hugo) [~/Documents/volatility3-develop]
$ python3 vol.py -f MEMORY.DMP windows.psscan
Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
32	4096	S	0xf198f08	3538995	-	-	True	2010-11-21 03:22:32.000000	N/A	Disabled
33554432		84547187215129	*****	0x56714fe6		4294967295	520101376	-	True	2004-03-02 02:42:27.0
00000	1600	02-10 05:15:02.000000		Disabled						
107163729068032	11599872		1.7600.16385_en	0x66100c9a		530579456	-	-	True	2000-08-06 23:42:37.000000
	1759-10-09 02:23:21.000000		Disabled							
215504284424960	214804749124424	UH♦♦ H♦♦H♦M(♦♦♦	0x73ee7d83		4258431208	-	-	True	2017-03-18 15:55:00.000000	
	1620-05-14 00:22:43.000000		Disabled							
26818077787940	13958912151092	*	0x79555561		2885681314	-	-	True	2000-09-03 17:55:06.000000	4669-
05-22 13:14:41.000000		Disabled								
2568	2492	taskmgr.exe	0x7de2db30	7	124	1	False	2024-03-09 12:05:33.000000	N/A	Disabled
2040	444	mscorsvw.exe	0x7e25db30	8	84	0	True	2024-03-09 11:49:52.000000	N/A	Disabled
988	360	conhost.exe	0x7e25e1d0	2	38	1	False	2024-03-09 11:49:15.000000	N/A	Disabled
396	1320	multireader.ex	0x7e2601d0	2	57	1	False	2024-03-09 11:54:50.000000	N/A	Disabled
1680	1320	cmd.exe	0x7e262060	1	19	1	False	2024-03-09 11:49:15.000000	N/A	Disabled
1956	444	sppsvc.exe	0x7e27f4f0	5	151	0	False	2024-03-09 11:47:59.000000	N/A	Disabled
1804	1320	cGFzdGViaW4uY2	0x7e2de800	8	258	1	False	2024-03-09 11:54:49.000000	N/A	Disabled
1536	444	spoolsv.exe	0x7e33fb30	13	254	0	False	2024-03-09 11:56:05.000000	N/A	Disabled
1272	1320	iexplore.exe	0x7e383b30	11	381	1	True	2024-03-09 11:55:44.000000	N/A	Disabled

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse de dump mémoire à l'aide de Volatility

```
(kali@Hugo)-[~/Documents/volatility3-develop]
$ python3 vol.py -f MEMORY.DMP windows.cmdline
Volatility 3 Framework 2.7.0
Progress: 100.00          PDB scanning finished
PID      Process Args
4        System Required memory at 0x20 is not valid (process exited?)
224      smss.exe      \SystemRoot\System32\smss.exe
296      csrss.exe      %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,
erDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitiali
MaxRequestThreads=16
348      wininit.exe    wininit.exe
804      cmd.exe      "C:\Windows\system32\cmd.exe"
1868     conhost.exe    \??\C:\Windows\system32\conhost.exe
1644     notepad.exe    "C:\Windows\system32\notepad.exe" C:\Users\joe\Desktop\schedule.txt
1804     cGFzdGViaW4uY2 "C:\temp\cGFzdGViaW4uY29tL3lBYTFhS2l1.exe"
896      multireader.ex "C:\temp\multireader.exe"
1272     iexplore.exe    "C:\Program Files (x86)\Internet Explorer\iexplore.exe"
```


3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse de dump mémoire à l'aide de Volatility

Recipe	Input
<p>From Base64</p> <p>Alphabet A-Za-z0-9+/=</p> <p><input checked="" type="checkbox"/> Remove non-alphabet chars</p> <p><input type="checkbox"/> Strict mode</p>	<p>cGFzdGViaW4uY29tL3lBYTFhS211</p>
	<p>REC 28 1 28</p> <p>Output</p> <p>pastebin.com/yAa1aKiu</p>

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse réseau à l'aide de Wireshark
- Statistics > Protocol Hierarchy

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	8494	100.0	7332846	331 k	0	0	0	8494
Ethernet	100.0	8494	1.7	122242	5,534	0	0	0	8494
Logical-Link Control	1.0	88	0.0	3344	151	0	0	0	88
Spanning Tree Protocol	1.0	88	0.0	3080	139	88	3080	139	88
Internet Protocol Version 6	0.2	18	0.0	720	32	0	0	0	18
User Datagram Protocol	0.1	11	0.0	88	3	0	0	0	11
Multicast Domain Name System	0.1	10	0.0	422	19	10	422	19	10
Link-local Multicast Name Resolution	0.0	1	0.0	23	1	1	23	1	1
Internet Control Message Protocol v6	0.1	7	0.0	196	8	7	196	8	7
Internet Protocol Version 4	98.7	8383	2.3	167688	7,591	0	0	0	8383
User Datagram Protocol	4.2	353	0.0	2824	127	0	0	0	353
Simple Service Discovery Protocol	0.2	20	0.0	3500	158	20	3500	158	20
QUIC IETF	1.7	144	0.6	47020	2,128	144	39029	1,767	151
Multicast Domain Name System	0.1	10	0.0	422	19	10	422	19	10
Link-local Multicast Name Resolution	0.0	1	0.0	23	1	1	23	1	1
Dynamic Host Configuration Protocol	0.0	2	0.0	600	27	2	600	27	2
Domain Name System	2.1	176	0.2	11780	533	176	11780	533	176
Transmission Control Protocol	94.5	8023	95.2	6977203	315 k	4442	3515739	159 k	8023
Transport Layer Security	41.6	3533	93.3	6844329	309 k	3533	5939651	268 k	3657
Hypertext Transfer Protocol	0.5	40	1.2	86012	3,894	29	2309	104	40
Line-based text data	0.0	1	0.0	207	9	1	207	9	1
HTML Form URL Encoded	0.1	9	0.5	38664	1,750	9	38664	1,750	9
Data	0.0	1	0.6	42109	1,906	1	42109	1,906	1
Data	0.1	8	0.0	8	0	8	8	0	8
Internet Group Management Protocol	0.1	7	0.0	112	5	7	112	5	7
Address Resolution Protocol	0.1	5	0.0	194	8	5	194	8	5

No display filter.

× Close Copy Protocols Help

3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse réseau à l'aide de Wireshark
- Statistics > Conversations

Wireshark - Conversations - dart.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

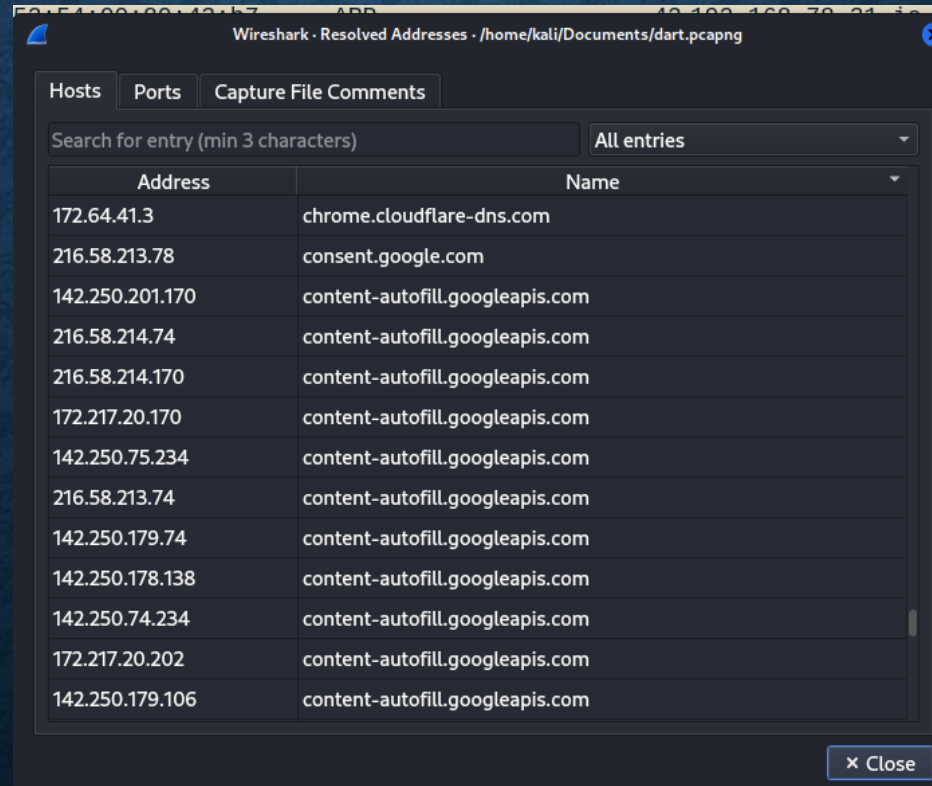
Follow Stream...

Graph...

Ethernet · 11	IPv4 · 41	IPv6 · 3	TCP · 72	UDP · 104							
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
52:54:00:80:43:b7	52:54:00:ef:1f:74	8,347	7 MB	6,286	7 MB	2,061	317 kB	0.000000	176.7017	317 kbps	14 kbps
52:54:00:a6:0a:e8	52:54:00:ef:1f:74	2	126 bytes	1	60 bytes	1	66 bytes	33.089199	0.0007		
52:54:00:ef:1f:74	01:00:5e:00:00:16	7	378 bytes	7	378 bytes	0	0 bytes	146.159915	1.8156	1,665 bits/s	0 bits/s
52:54:00:ef:1f:74	01:00:5e:00:00:fb	10	842 bytes	10	842 bytes	0	0 bytes	31.961829	115.7916	58 bits/s	0 bits/s
52:54:00:ef:1f:74	01:00:5e:00:00:fc	1	65 bytes	1	65 bytes	0	0 bytes	147.801958	0.0000		
52:54:00:ef:1f:74	01:00:5e:7f:ff:fa	20	4 kB	20	4 kB	0	0 bytes	41.092793	123.0355	282 bits/s	0 bits/s
52:54:00:ef:1f:74	33:33:00:00:00:16	7	630 bytes	7	630 bytes	0	0 bytes	146.158845	1.8170	2,773 bits/s	0 bits/s
52:54:00:ef:1f:74	33:33:00:00:00:fb	10	1 kB	10	1 kB	0	0 bytes	31.962978	115.8251	71 bits/s	0 bits/s
52:54:00:ef:1f:74	33:33:00:01:00:03	1	85 bytes	1	85 bytes	0	0 bytes	147.791970	0.0000		
52:54:00:ef:1f:74	ff:ff:ff:ff:ff:ff	1	42 bytes	1	42 bytes	0	0 bytes	33.088203	0.0000		
fe:54:00:ef:1f:74	01:80:c2:00:00:00	88	5 kB	88	5 kB	0	0 bytes	1.531172	173.9485	242 bits/s	0 bits/s

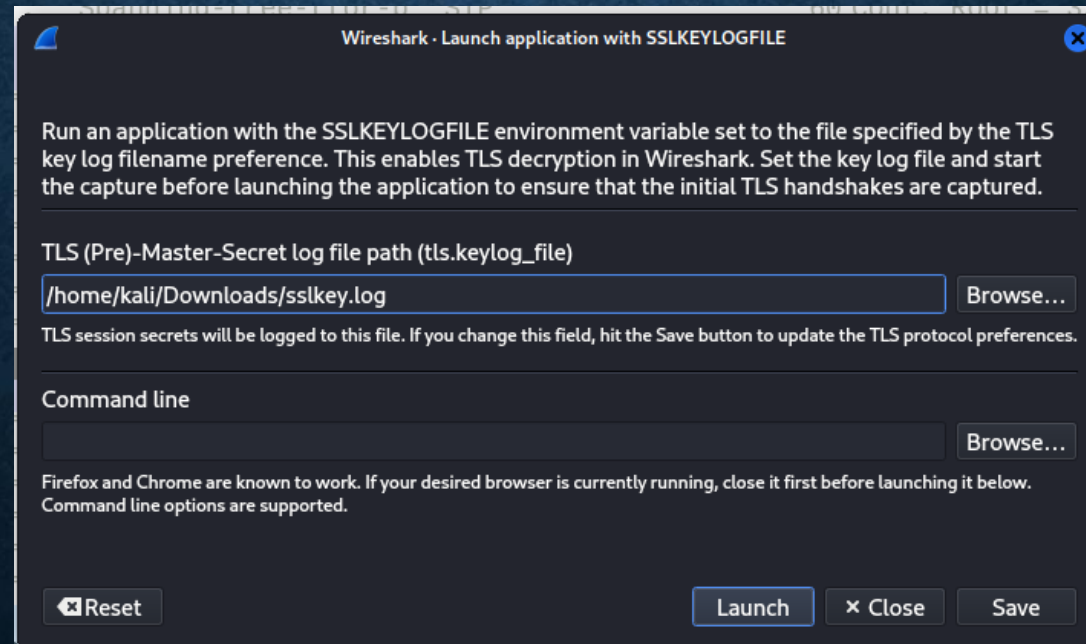
3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse réseau à l'aide de Wireshark
- Statistics > Resolved Addresses



3. ... MAIS SURTOUT BEAUCOUP DE PRATIQUE

- Démonstration d'une analyse réseau à l'aide de Wireshark
- Exportation de tous les fichiers trouvés :
File > Export Objects > HTTP / FTP / ...
- Ajout clés SSL :





MERCI À VOUS !

Hackin'TN

4. ANNEXES

- Installation des outils mentionnés :
 - <https://www.autopsy.com/download/>
 - <https://github.com/volatilityfoundation/volatility3>
- Vidéos explicatives très complètes :
 - Sur volatility: https://youtu.be/2S_pi9qnIo8?list=PL_TfKyL-HEyF1JkgkdMA--HfIFLY2Htnc
 - Sur autopsy: https://youtu.be/o6boK9dG-Lc?list=PL_TfKyL-HEyF1JkgkdMA--HfIFLY2Htnc