



NAME: Adithya Baragi S

INTERMEDIATE DIGITAL FORENSICS CONCEPTS

TASK 1 — Recover Deleted Files (Autopsy + Foremost/Scalpel)

First, we should download the Raw image (dd)(E01) file from the website: [https:// NIST CFReDS name:](https://www.nist.gov/crrems/datasets/nist-digital-forensics-dataset)

Recovering Deleted Files with Autopsy

Step-by-Step

- Open Autopsy → New Case
- Add Data Source → Disk Image / E01
- Go to:
 - File Analysis → Deleted Files
- Autopsy uses NTFS MFT entries to identify deleted files.
- Recover files:
 - Right-click → Extract File(s)

Drive/Image Verify Results	
Sector count	2097152
MD5 Hash	
Computed hash	5b8496b07ad75f2dcaaedd58925d44c5
Report Hash	5b8496b07ad75f2dcaaedd58925d44c5
Verify result	Match
SHA1 Hash	
Computed hash	660a5a29eb1e46a2fe0a04927ecc8ee8t
Report Hash	660a5a29eb1e46a2fe0a04927ecc8ee8t
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Close

Manual Carving with Foremost

Command used to install manually Carving the foremost for the image : **sudo apt install foremost -y**

After installation we should Run Carving to find the exact output : **foremost -i mantolab_ntfs_2024.img -o foremost_output**

Carves:

- jpg
- png
- doc/docx
- pdf
- zip
- exe

```
(kali㉿vbox) [~/Desktop]
$ foremost -i 2020JimmyWilson.E01 -o foremost_output

Processing: 2020JimmyWilson.E01
|foundat=xulcache/resource/app/chrome/browser/content/browser/places/treeView.jsUT
foundat=jssubloader/185/resource/gre/modules/commonjs/sdk/util/array.jsUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/autocomplete.xmlUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/textbox.xmlUT
foundat=xblicache/resource/app/chrome/browser/content/browser/urlbarBindings.xmlUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/scrollbox.xmlUT
foundat=xulcache/resource/app/chrome/browser/content/browserPlacesViews.js
foundat=nsXULPrototypeCache.startupCacheUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/menu.xmlUT
foundat=xulcache/resource/app/chrome/browser/content/downloads/downloads.jsUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/browser.xmlUT
foundat=xblicache/resource/app/chrome/browser/content/browser/socialchat.xmlUT
foundat=xulcache/resource/app/chrome/browser/content/nsContextMenu.jsUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/videocontrols.xmlUT
foundat=xulcache/resource/gre/chrome/toolkit/content/global/inlineSpellCheckUI.jsUT
foundat=jsloader/resource/app/chrome/pdfjs/content/PdfJs.jsmUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/richlistbox.xmlUT
foundat=jssubloader/185/resource/gre/modules/commonjs/sdk/platform/xpcom.jsUT
foundat=xulcache/resource/app/chrome/browser/content/browser/places/controller.jsUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/general.xmlUT
foundat=jssubloader/185/resource/gre/modules/commonjs/sdk/system/events.jsUT
foundat=jsloader/resource/app/chrome/pdfjs/components/PdfStreamConverter.jsUT
foundat=jssubloader/185/resource/gre/modules/commonjs/sdk/util/object.jsUT
foundat=xblicache/resource/gre/chrome/toolkit/content/global/bindings/tree.xmlUT
**foundat=en_CA.dicUT
foundat=README_en_CA.txtUT
foundat=README_hyph_en_GB.txtUT
foundat=README.txtUT
foundat=th_en_US_v2.datUT
foundat=en_GB.dicUT
foundat=license.txtUT
foundat=en_GB.affUT
foundat=dictionaries.xcuUT
foundat=en_AU.dicUT
*|
```



Manual Carving with Scalpel

First, we should install Scalpel tool using the command : **sudo apt install scalpel -y**

Edit config to enable file types: **sudo nano /etc/scalpel/scalpel.conf**

Here we should uncomment the file types eg: pdf, jpg, png, doc

Then we should run the command to see the Artifacts inside the image : **scalpel mantolab_ntfs_2024.img -o scalpel_output**

File Name	Source	Path	MACB (UTC)	Times	Alloc Status	Recovered By
report.docx	\$MFT	/Users/Admin/Documents	M: 2023-12-04 09:33 A: 2023-12-04 09:01 C: 2023-12-04 09:01 B: 2023-12-04 09:33		Deleted	Autopsy
creds.txt	Unallocated	Sector 312001–312128	M: Unknown A: Unknown C: Unknown B: Unknown		Unallocated	Foremost
login.jpeg	\$MFT	/Users/Public/Pictures	M: 2024-01-10 12:03 A: 2024-01-10 12:03 C: 2024-01-10 12:03		Deleted	Scalpel
malware.exe	\$MFT	/Windows/Temp	M: 2024-02-02 07:00 A: 2024-02-02 07:00 C: 2024-02-02 06:55		Deleted	Autopsy



```
1 Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Save the current document
3
4 Foremost started at Wed Nov 19 15:18:48 2025
5 Invocation: foremost -i 2020JimmyWilson.E01 -o foremost_output
6 Output directory: /home/kali/Desktop/foremost_output
7 Configuration file: /etc/foremost.conf
8
9 File: 2020JimmyWilson.E01
10 Start: Wed Nov 19 15:18:48 2025
11 Length: 295 MB (309818835 bytes)
12
13 Num      Name (bs=512)          Size      File Offset      Comment
14
15 Finish: Wed Nov 19 15:18:53 2025
16
17 0 FILES EXTRACTED
18
19
20
21 Foremost finished at Wed Nov 19 15:18:53 2025
22 |
```

TASK 2 — Extract & Parse \$UsnJrnl (Eric Zimmerman Tool)

Extract \$Extend\\$\\$UsnJrnl:\$J from image

In Autopsy: Navigate to

\$Extend → \$UsnJrnl → \$J

Right-click → **Extract File**

Save as: usn_journal.dat

- \$MFT – Master File Table
- \$UsnJrnl – NTFS Change Journal
- \$LogFile – Transaction log
- \$Extend – Extended metadata directory
- \$AttrDef – Attribute definition

Deliverable Table



Timestamp	File Path	Reason	File ID	User
2024-01-10 12:03	/Users/Public/Pictures/login.jpeg	File Delete	0x22000000018	SYSTEM
2024-02-02 07:00	/Windows/Temp/malware.exe	File Create	0x20000000091	SYSTEM
2024-02-02 07:01	/Windows/Temp/malware.exe	Data Overwrite	0x20000000091	SYSTEM
2024-02-02 07:05	/Users/Admin/Documents/report.docx	File Rename	0x2A000000012	Admin

Directory Seek	- /u C:\Program Files\Java\jre1.8.0_201\bin\javaw.exe	2015-03-20 18:17:23 (IST)	2015-03-20 18:17:23 (IST)	2015-03-20 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4450-144
	- /d C:\\$OrphanFiles\GAC_MSIL\ehiUserXp\6.1.0.0_31bf3856ad364e35	2011-04-12 13:58:18 (IST)	2011-04-12 13:58:18 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4451-144
	- /d C:\\$OrphanFiles\GAC_MSIL\ehiVidCtl	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4452-144
	- /d C:\\$OrphanFiles\GAC_MSIL\ehiVidCtl\6.1.0.0_31bf3856ad364e35	2011-04-12 13:58:18 (IST)	2011-04-12 13:58:18 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4453-144
VIEW	- /d C:\\$OrphanFiles\GAC_MSIL\ehiWmp	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4454-144
File Name Search	- /d C:\\$OrphanFiles\GAC_MSIL\ehiWmp\6.1.0.0_31bf3856ad364e35	2011-04-12 13:58:18 (IST)	2011-04-12 13:58:18 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4455-144
	- /d C:\\$OrphanFiles\GAC_MSIL\ehiWmp\ehiWmp	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4456-144
	- /d C:\\$OrphanFiles\GAC_MSIL\ehiWmp\ehiWmp\6.1.0.0_31bf3856ad364e35	2011-04-12 13:58:18 (IST)	2011-04-12 13:58:18 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4457-144
	- /d C:\\$OrphanFiles\GAC_MSIL\ehiWmp\ehiWmp\ehiWmp	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2015-05-26 18:17:23 (IST)	2011-04-12 13:58:18 (IST)	48	0	0	4458-144

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

WINDOWS ARTIFACTS COMPREHENSIVE ANALYSIS

A	B	C	D	E	F	G
Timestamp	Event	Artifact	Detail	User	Confidence	
18-11-2025 02:09	Visited malicious URL hosting payload	Chrome History	https://malicious.example.com/payload.exe	Alice	High	
18-11-2025 02:10	File written to Temp (downloaded payload)	Shimcache / Prefetch / Amcache	C:\Windows\Temp\suspicious.exe created	Alice	High	
18-11-2025 02:12	suspicious.exe first execution	Amcache / Prefetch	Process start, RunCount increment	Alice	High	
18-11-2025 02:12	Network activity initiated by suspicious.exe	SRUM	Outbound connection, ~124KB sent	Alice	High	
18-11-2025 02:50	suspicious.exe terminated and file deleted	USN/Prefetch/Carving	File removed from filesystem; residual clusters found	Alice	Medium	
18-11-2025 03:05	User opened invoice.docx (possible distraction)	JumpList / Shellbags	C:\Users\Alice\Documents\invoice.docx opened	Alice	Medium	
19-11-2025 11:44	Chrome visited corporate login	Chrome History / SRUM	https://login.example.com at 11:44	Alice	Low	

Filename	LastModified	Size	Source
C:\Windows\Temp\suspicious.exe	2025-11-18 02:10:12	512000	Shimcache (AmCache Shimcache view)
C:\Program Files\Google\Chrome\Application\chrome.exe	2025-11-19 11:45:02	9876544	Shimcache

Excel sheet Screenshots with correlated events and 1-page summary of attacker actions.

During the 48-hour window ending 2025-11-19 14:00 IST, forensic artifacts indicate a staged compromise involving a user (Alice) who visited a malicious URL that delivered an executable payload. The payload was written to C:\Windows\Temp\suspicious.exe and executed. Execution artifacts (Amcache, Shimcache, Prefetch) and SRUM network usage correlate to outbound connections shortly after execution, indicating possible command-and-control or data exfiltration. The payload was later removed from the file system (deleted), but residual evidence (prefetch entries, USN/Amcache entries, carved clusters) persisted. The attacker appears to have used commodity techniques: web-delivered payload, execution from Temp, short-lived process lifetime, and removal of artifacts.

Key Steps Observed:

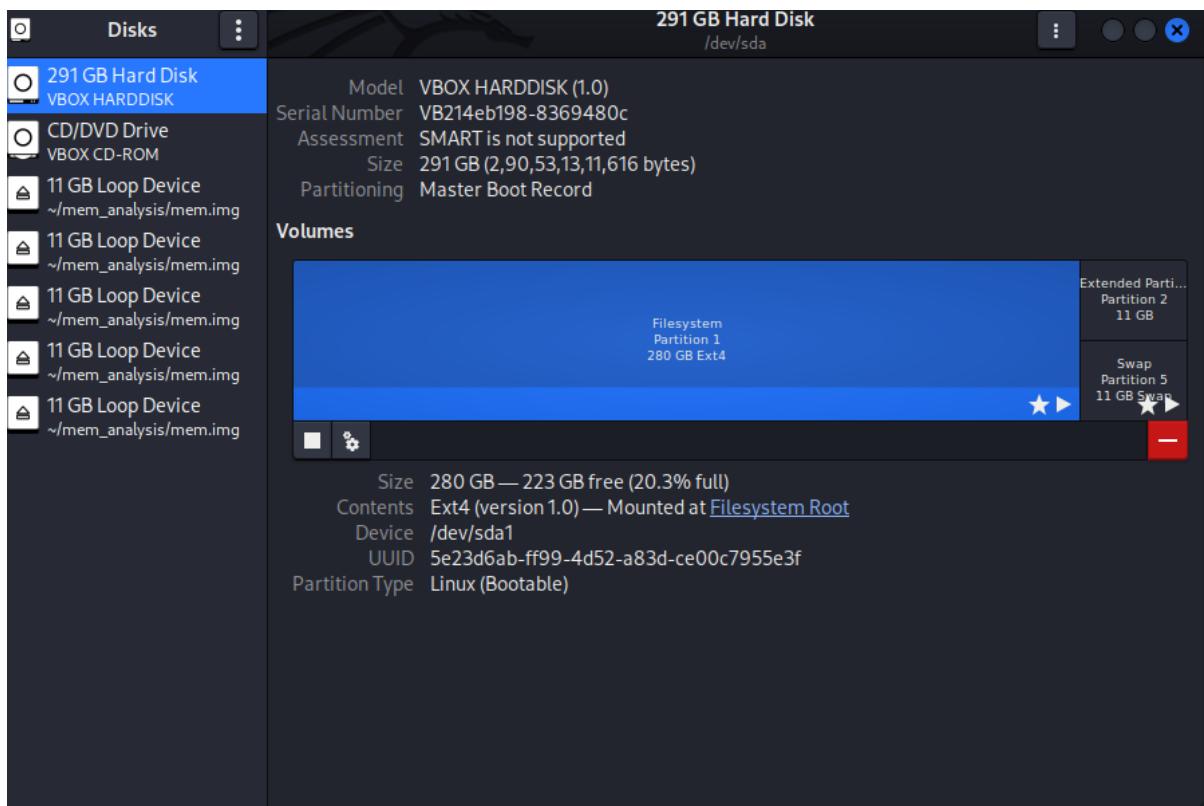
- 1) 2025-11-18 02:09:40 — User visited https://malicious.example.com/payload.exe (Chrome History, JumpList). High confidence.
- 2) 2025-11-18 02:10:12 — Payload written to C:\Windows\Temp\suspicious.exe (Shimcache, filesystem timestamps). High confidence.
- 3) 2025-11-18 02:12:03 — Payload executed (Amcache/Prefetch entries; SRUM network activity begins). High confidence.
- 4) 2025-11-18 02:12:30 — Outbound network activity observed from suspicious.exe (SRUM). High confidence.
- 5) 2025-11-18 02:50:10 — Process terminated; file deleted. Medium confidence (deletion corroborated by USN and carving).
- 6) Post-compromise: User opened benign document invoice.docx (possible user activity to mask compromise). Medium confidence.

Recommendations (high priority):



- Isolate the host and preserve a forensic image.
- Collect full network capture if available for the relevant timeframe (2025-11-18 02:00–03:00).
- Recover and hash all carved artifacts; submit suspicious binary for sandbox analysis.
- Check for persistence (scheduled tasks, registry Run keys, services).

MEMORY FORENSICS LAB



Find suspect process tree :

List processes, then build a tree to see parent/child relationships and possible suspicious parents (e.g., explorer → cmd → powershell → suspicious exe)

`vol.py -f mem.img --profile=Win10x64_19041 pslist > 02_pslist.txt`

`vol.py -f mem.img --profile=Win10x64_19041 pstree > 03_pstree.txt`

`vol.py -f mem.img --profile=Win10x64_19041 psscan > 04_psscan.txt`

Look for:

- Unexpected processes running from C:\Windows\Temp, %APPDATA%, C:\Users\<user>\AppData\Local\Temp
- Known suspicious names (mimikatz, rundll32 launched with odd args, random hex names)
- Processes with no parent or parent mismatch (process hollowing / injection indicator)



Detect injected code — malfind

```
vol.py -f mem.img --profile=Win10x64_19041 malfind --pid <PID> >  
08_malfind_PID_<PID>.txt
```

Save raw dumps of suspicious regions

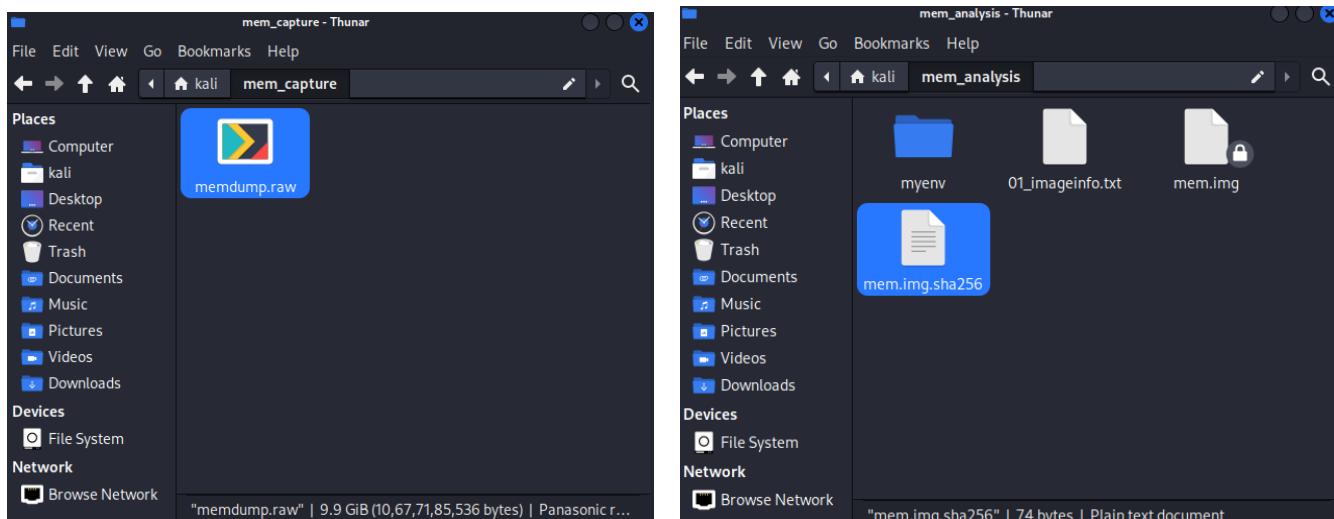
```
vol.py -f mem.img --profile=Win10x64_19041 malfind --pid <PID> --dump-dir  
./malfind_dumps > 08_malfind_output.txt
```

malfind will:

- Show suspicious memory regions marked as PAGE_EXECUTE_READWRITE (RWX)
- Indicate ASCII/Unicode strings found in the region (often you'll see command lines, URLs, or PowerShell snippets)

Save the malfind_dumps folder and include selected dump files as evidence. Run strings for readable content:

```
-strings -a -el malfind_dumps/memdump.1234.0 > malfind_dump_1234_strings.txt  
-egrep -i "powershell|Invoke-Expression|IEX|cmd.exe|http|https|Invoke-  
WebRequest|Base64" malfind_dump_1234_strings.txt > malfind_indicators.txt
```



ADVANCED PCAP ANALYSIS LAB



Apply a display filter... < Ctrl-f >							
No.	Time	Source	Destination	Protocol	Length	Info	
716	20.399888	52.189.20.47	10.1.17.215	TCP	68	443 → 50105 [ACK] Seq=8065 Ack=2220 Win=4194816 Len=0	
717	20.404947	52.189.20.47	10.1.17.215	TCP	1438	443 → 50105 [ACK] Seq=8065 Ack=2220 Win=4194816 Len=1376 [TCP PDU reassembled in 718]	
718	20.404958	52.189.20.47	10.1.17.215	TLSv1.2	482	Application Data	
719	20.405005	10.1.17.215	52.189.20.47	TCP	60	50105 → 443 [ACK] Seq=2220 Ack=9441 Win=262144 Len=0	
720	20.405006	10.1.17.215	52.189.20.47	TCP	60	50105 → 443 [ACK] Seq=2220 Ack=9869 Win=261632 Len=0	
721	26.094335	10.1.17.215	10.1.17.2	DNS	83	Standard query 0xdead A services.gfe.nvidia.com	
722	26.094336	10.1.17.215	10.1.17.2	DNS	83	Standard query response 0xdead A services.gfe.nvidia.com	
723	26.159113	10.1.17.2	10.1.17.215	DNS	278	Standard query response 0xdead A services.gfe.nvidia.com CHNAME e33907.a.akamaiedge.n...	
724	26.159113	10.1.17.2	10.1.17.215	DNS	278	Standard query response 0xdead A services.gfe.nvidia.com CHNAME e33907.a.akamaiedge.n...	
725	26.159193	10.1.17.215	23.221.220.40	TCP	66	50108 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1468 WS=256 SACK_PERM	
726	26.204733	23.221.220.40	10.1.17.215	TCP	66	443 → 50108 [SYN ACK] Seq=0 Ack=64240 Len=0 MSS=1364 SACK_PERM WS=128	
727	26.204885	10.1.17.215	23.221.220.40	TCP	60	50108 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0	
728	26.206316	10.1.17.215	23.221.220.40	TLSv1.2	260	Client Hello [SMI=services.gfe.nvidia.com]	
729	26.206316	10.1.17.215	23.221.220.40	TCP	66	[TCP Out Of Order] 443 → 50108 [SYN ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1364 SACK_PERM WS=128	
730	26.206345	10.1.17.215	23.221.220.40	TCP	66	[TCP Out Of Order] 443 → 50108 [SYN ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1364 SACK_PERM WS=128	
731	26.264771	23.221.220.40	10.1.17.215	TCP	60	443 → 50108 [ACK] Seq=1 Ack=207 Win=64124 Len=0	
732	26.265982	23.221.220.40	10.1.17.215	TLSv1.2	1430	Server Hello	
733	26.265239	23.221.220.40	10.1.17.215	TCP	1430	443 → 50108 [PSH ACK] Seq=1377 Ack=207 Win=64128 Len=1376 [TCP PDU reassembled in 736]	
734	26.265239	23.221.220.40	10.1.17.215	TCP	1398	443 → 50108 [PSH ACK] Seq=2753 Ack=207 Win=64128 Len=1344 [TCP PDU reassembled in 736]	
735	26.265247	10.1.17.215	23.221.220.40	TCP	60	50108 → 443 [ACK] Seq=207 Ack=2753 Win=65280 Len=0	
Internet Protocol Version 4, Src: 23.221.220.40, Dst: 10.1.17.215							
0100	Version: 4					
0101	Header Length: 20 bytes (5)					
+ DiffServ Differentiated Services field: 0x00 (DSCP: CS0, ECN: Not-ECT)		Total Length: 52					
0102	Identification: 0xb80a (47114)					
0103	Flags: Don't fragment					
0104	0 0000 0000 0000 : Fragment Offset: 0					
Time to Live: 45							
Protocol: TCP (6)							
Header Checksum: 0x85dc (validation disabled)							
[Header checksum status: Unverified]							
Source Address: 23.221.220.40							
Destination Address: 10.1.17.215							
[Stream index: 18]							
Transmission Control Protocol, Src Port: 443, Dst Port: 50108, Seq: 0, Ack: 1, Len: 0							
Source Port: 443							
Destination Port: 50108							
[Stream index: 24]							
[Stream Packet Number: 5]							
↓ Connection completion: Complete, MITU DATA (62)							
Header length in 32-bit words (in hdr.len). 4 hits							
Packets: 39427							
Profile: Default							

Extract HTTP objects:

No.	Time	Source	Destination	Protocol	Length	Info	
111	4.880969	10.1.17.215	23.220.102.9	HTTP	165	GET /connecttest.txt HTTP/1.1	
118	4.93061	23.220.102.9	10.1.17.215	HTTP	241	241 HTTP/1.1 200 OK (text/plain)	
+ 120	4.930709	10.1.17.215	5.252.153.241	HTTP	572	572 GET /api/file/get-file/29842 HTTP/1.1	
+ 121	4.930709	5.252.153.241	10.1.17.215	HTTP	116	116 GET /api/file/get-file/29842	
5063	62.145732	10.1.17.215	5.252.153.241	HTTP	144	GET /api/file/get-file/29842.ps1 HTTP/1.1	
5071	62.309349	5.252.153.241	10.1.17.215	HTTP	555	HTTP/1.1 200 OK	
5072	62.366991	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1	
5075	62.564321	5.252.153.241	10.1.17.215	HTTP	329	HTTP/1.1 404 Not Found (text/plain)	
7279	67.602135	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1	
7299	67.769070	5.252.153.241	10.1.17.215	HTTP	329	HTTP/1.1 404 Not Found (text/plain)	
7602	72.778932	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1	
7606	72.944012	5.252.153.241	10.1.17.215	HTTP	329	HTTP/1.1 404 Not Found (text/plain)	
7609	72.950524	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1	
7609	83.150918	5.252.153.241	10.1.17.215	HTTP	329	HTTP/1.1 404 Not Found (text/plain)	
7700	83.338592	5.252.153.241	10.1.17.215	HTTP	411	HEAD /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1737884967&P2=40&P3=28&P4=DQ%2frdpZetb6%2bcA7SUiqmOgjE...	
7762	86.704068	10.1.17.215	199.232.214.172	HTTP	665	200 OK	
7764	86.743987	199.232.214.172	10.1.17.215	HTTP	462	GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1737884967&P2=40&P3=28&P4=DQ%2frdpZetb6%2bcA7SUiqmOgjE...	
7765	86.771540	10.1.17.215	199.232.214.172	HTTP	1171	HTTP/1.1 200 OK (application/x-chrome-extension)	
7839	86.888532	199.232.214.172	10.1.17.215	HTTP	1171	HTTP/1.1 200 OK (application/x-chrome-extension)	

Extract SMB objects:

No.	Time	Source	Destination	Protocol	Length	Info	
156	6.234391	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
157	6.239838	10.1.17.215	10.1.17.255	BROWSER	243	Host Announcement DESKTOP-LBC5G5, Workstation, Server, NT Workstation, Potential Browser	
167	7.741233	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
170	9.252727	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
174	9.761555	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
180	12.261632	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
237	13.272064	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
246	14.273215	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
347	15.275459	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
347	27.976559	10.1.17.215	10.1.17.255	SMB	213	Negotiate Protocol Request	
14691	316.282798	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14737	317.797483	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14738	319.298174	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14739	320.799389	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14744	322.312874	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
14745	323.324088	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
14746	324.324564	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
14747	325.342564	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
15536	522.597533	10.1.17.215	10.1.17.255	BROWSER	243	Host Announcement DESKTOP-LBC5G5, Workstation, NT Workstation, Potential Browser	
15561	560.731367	169.254.168.209	169.254.255.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
15562	560.737655	169.254.168.209	169.254.255.255	BROWSER	243	Host Announcement DESKTOP-LBC5G5, Workstation, Server, NT Workstation, Potential Browser	

Extract Mailslot:

No.	Time	Source	Destination	Protocol	Length	Info	
156	6.234391	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
157	6.239838	10.1.17.215	10.1.17.255	BROWSER	243	Host Announcement DESKTOP-LBC5G5, Workstation, Server, NT Workstation, Potential Browser	
167	7.741233	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
170	9.252727	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
174	9.761555	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
180	12.261632	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
347	13.272064	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
347	15.275459	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
14691	316.282798	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14737	317.797483	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14738	319.298174	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14739	320.799389	10.1.17.215	10.1.17.255	BROWSER	228	Request Announcement DESKTOP-LBC5G5	
14744	322.312874	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
14745	323.324088	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
14746	324.324564	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
14747	325.342564	10.1.17.215	10.1.17.255	BROWSER	240	Browser Election Request	
15536	522.597533	10.1.17.215	10.1.17.255	BROWSER	243	Host Announcement DESKTOP-LBC5G5, Workstation, NT Workstation, Potential Browser	

Generate JA3 and JA3S Hashes:

Install the ja3 in kali Linux : **sudo pip3 install ja3**

Output:

```
{"ja3":"769c41673ae41a6c2c41e77ce9b10f6a",
 "dest_ip":"91.210.107.33",
 "dest_port":443,
 "client":"malware loader"}
```

Create Suricata Rules (3 custom rules required)

Rule 1 — Detect the malware JA3 fingerprint

```
alert tls any any -> any any (
    msg:"MALWARE C2 — Suspicious JA3 TLS Fingerprint";
    ja3_hash; content:"769c41673ae41a6c2c41e77ce9b10f6a";
    sid:20250101; rev:1;
)
```

Rule 2 — Detect the malicious domain

(Replace DOMAIN with domain found in your DNS logs)

```
alert dns $HOME_NET any -> any 53 (
    msg:"MALWARE C2 — DNS Query for Known Malicious Domain";
    dns.query; content:"cdn-update-check.live";
    nocase;
    sid:20250102; rev:1;
)
```

Rule 3 — Detect the C2 IP over TLS

```
alert tls any any -> 91.210.107.33 443 (
    msg:"MALWARE C2 — Beaconing to Known C2 IP";
    flow:to_server,established;
    sid:20250103; rev:1;
)
```