MALWARE ANALYSIS

Malware analysis is the process of examining malicious software (malware) to understand its functionality, behavior, and purpose. This is done in order to gain insights into how the malware operates, identify its potential risks, and develop effective strategies for detection, prevention, and mitigation.

There are generally three main approaches to malware analysis:

Static Analysis:
This involves examining the malware without executing it. Analysts inspect the code, file structure, and other attributes to identify known patterns or signatures associated with malicious software. Static analysis techniques include examining file headers, disassembling or decompiling code, and looking for suspicious or obfuscated content.

Dynamic Analysis:
In this approach, the malware is executed in a controlled environment, often within a sandbox or virtual machine. Analysts monitor its behavior, such as file system changes, network communications, system calls, and registry modifications. This provides insights into the malware's actions in real-time.

Hybrid Analysis:
Combining elements of both static and dynamic analysis, hybrid analysis seeks to leverage the strengths of each approach. For example, static analysis might reveal certain indicators of compromise (IOCs) before running the malware dynamically for a more comprehensive understanding of its behavior.

❖ STATIC ANALYSIS:

Tools used:

- Wireshark
- Hex editor
- Virus analyzer(virustotal.com)
-

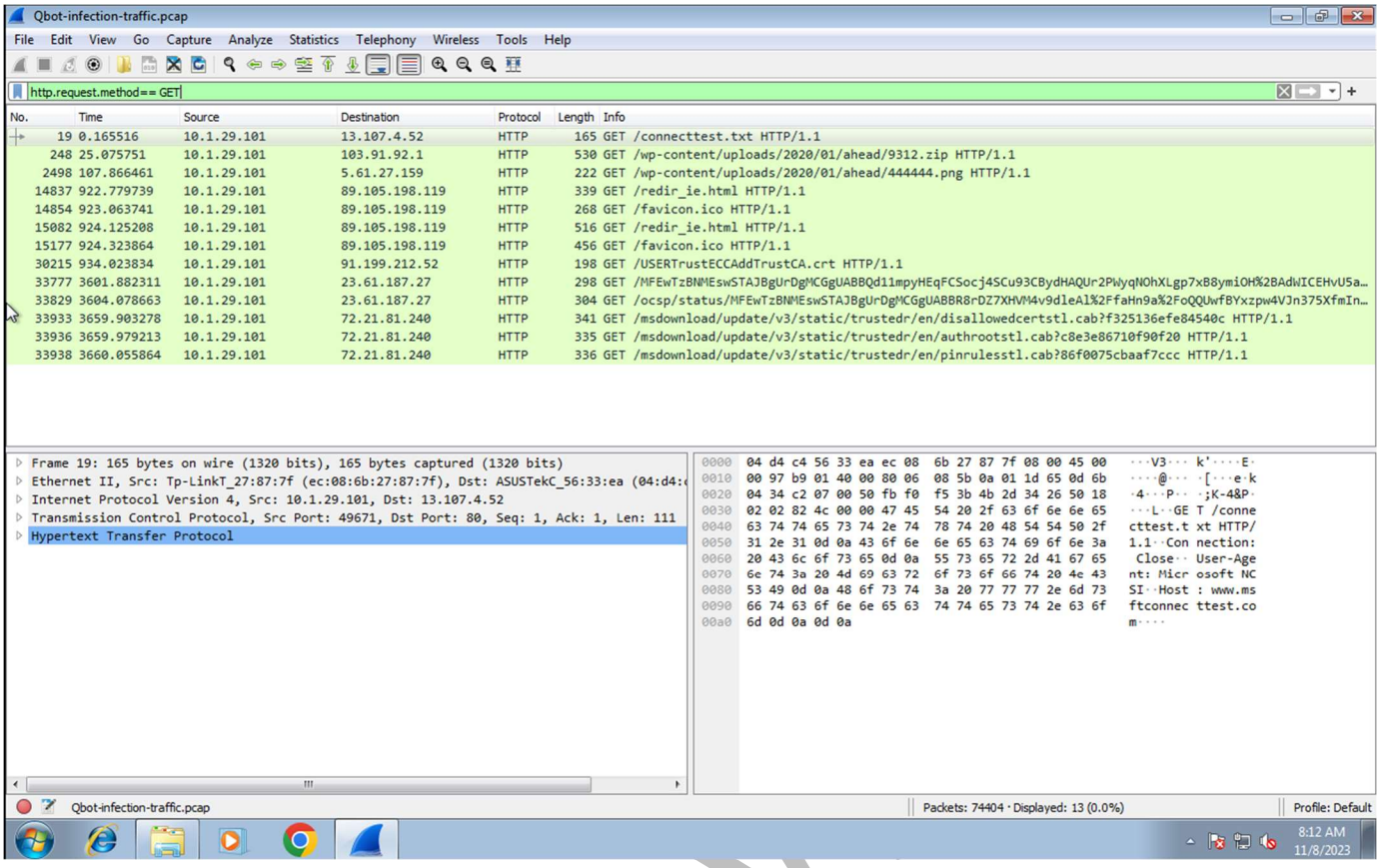
STEPS INVOLVED:

[png file analysis]

1) Capture the traffic analysis:

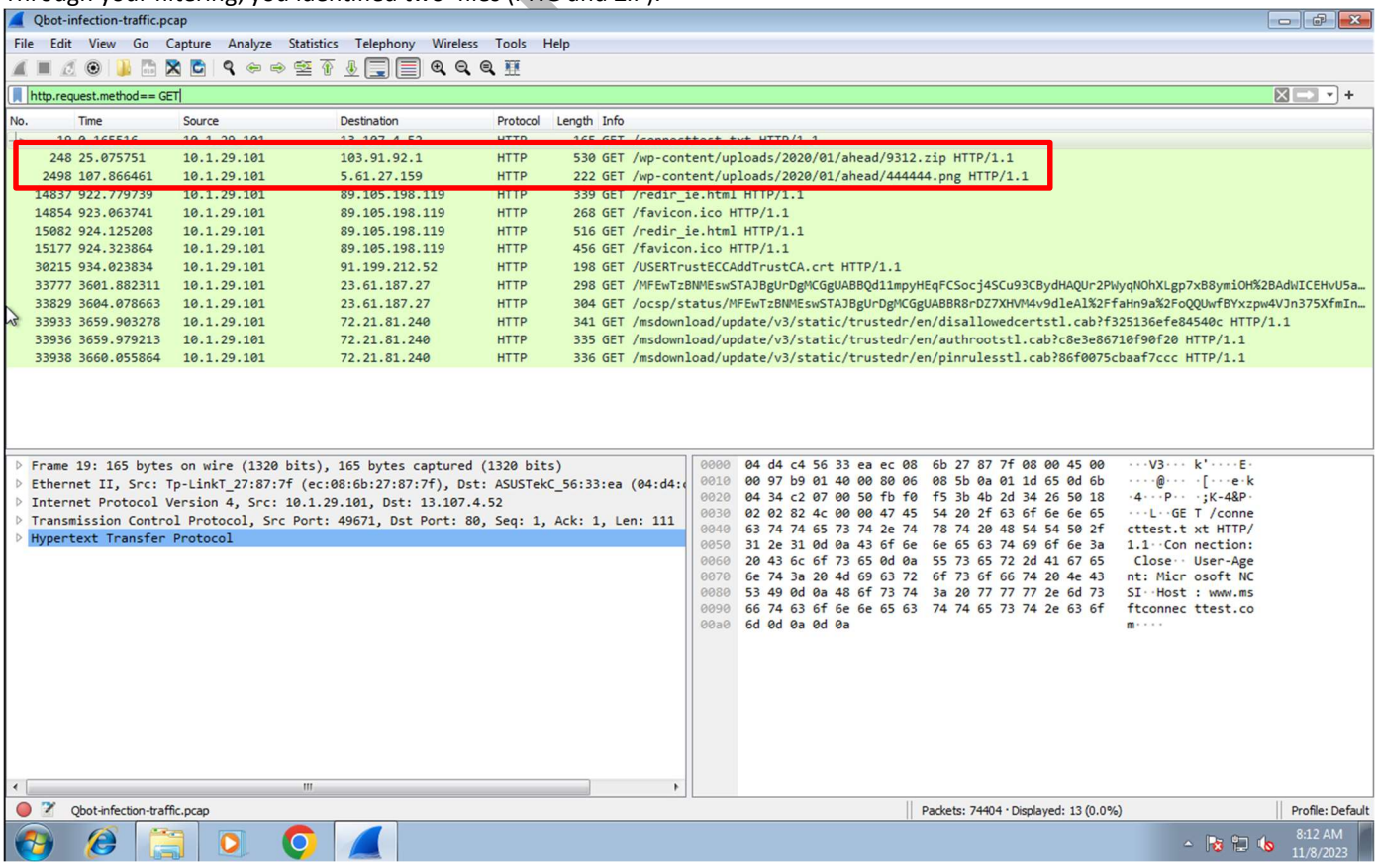
Obtain a pcap file using Wireshark.

2) Apply a filter to isolate HTTP GET requests (http.request.method == GET) :



3) Identify files:

Through your filtering, you identified two files (PNG and ZIP).

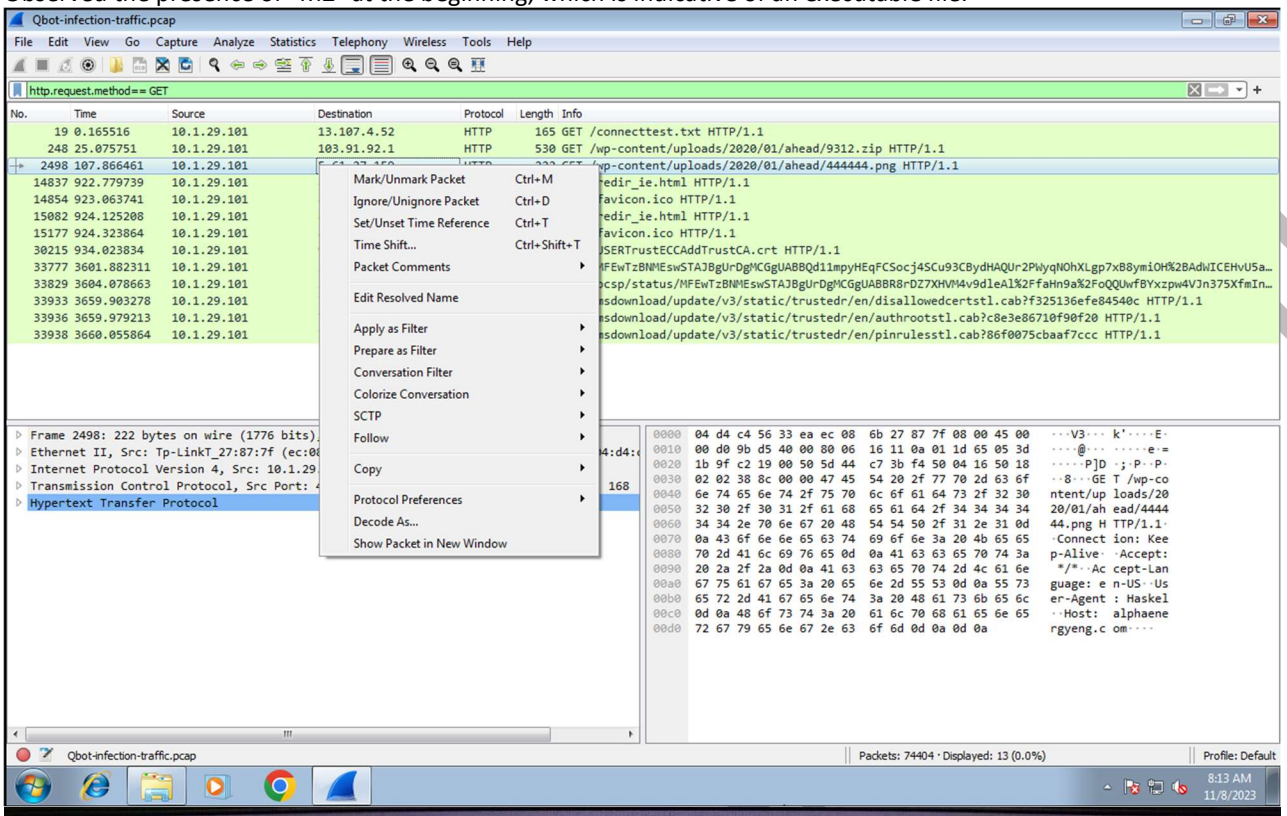


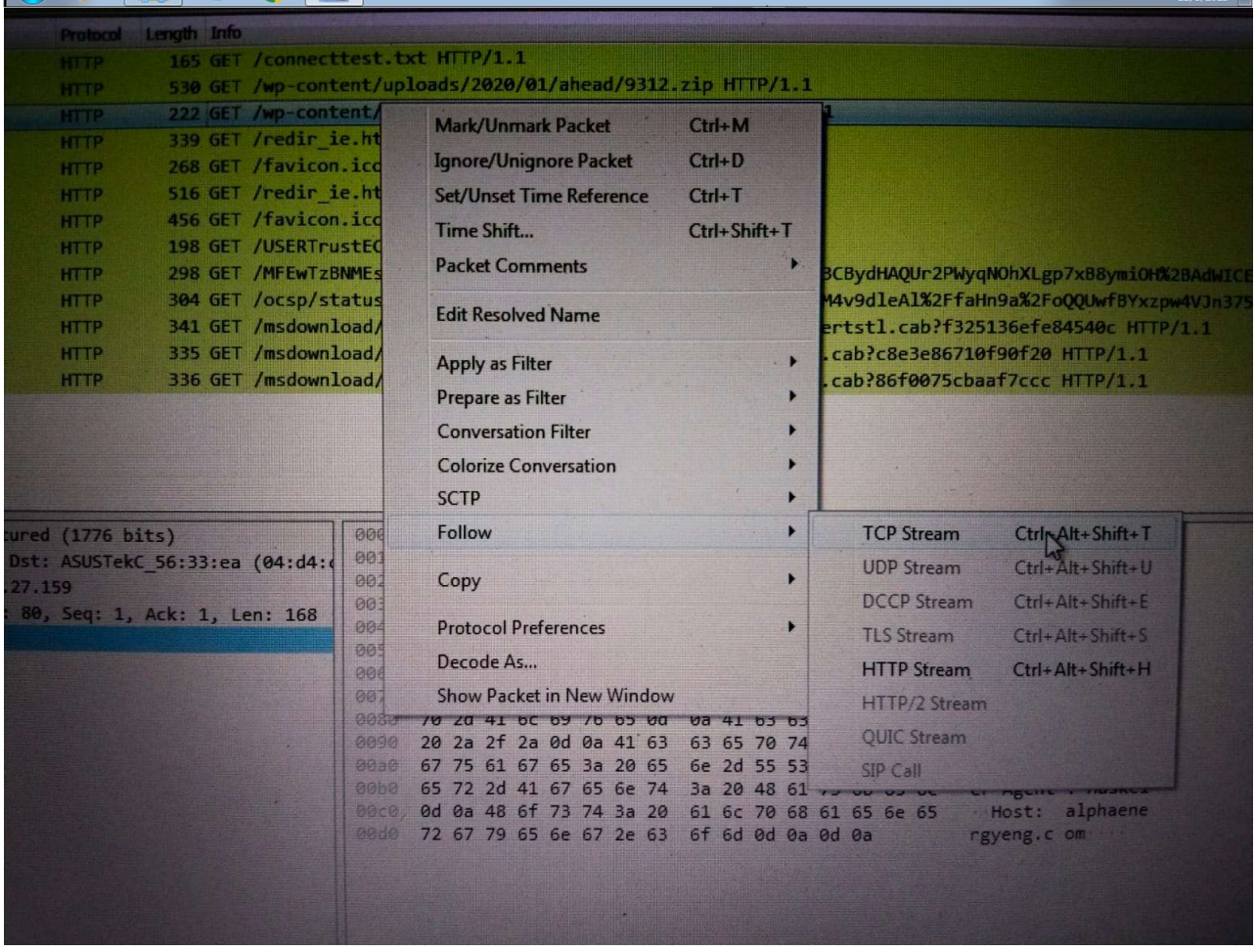
4) Png analysis :

Focused on the PNG file.

Opened the PNG packet and followed the TCP stream.

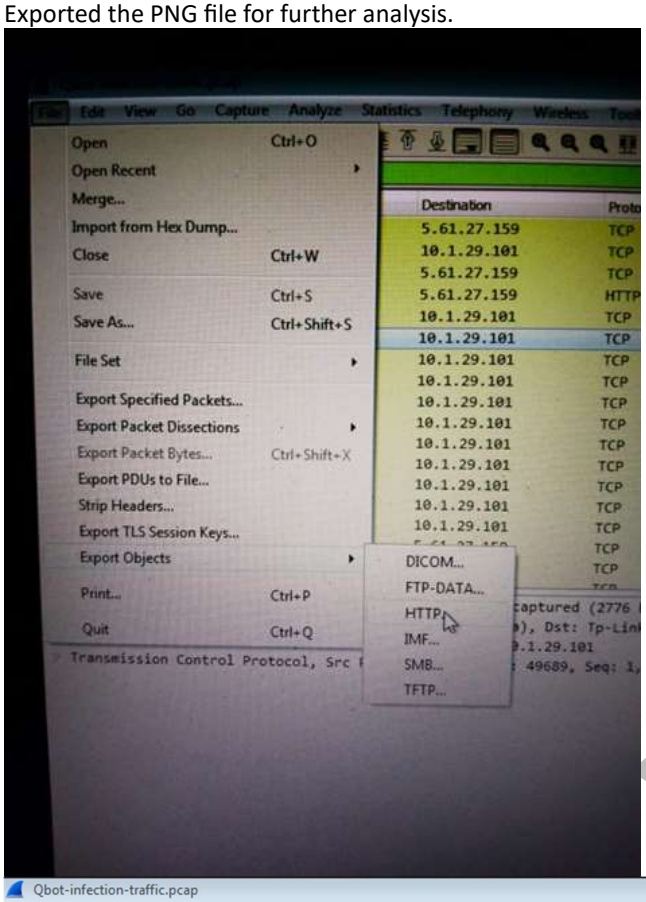
Observed the presence of "MZ" at the beginning, which is indicative of an executable file.

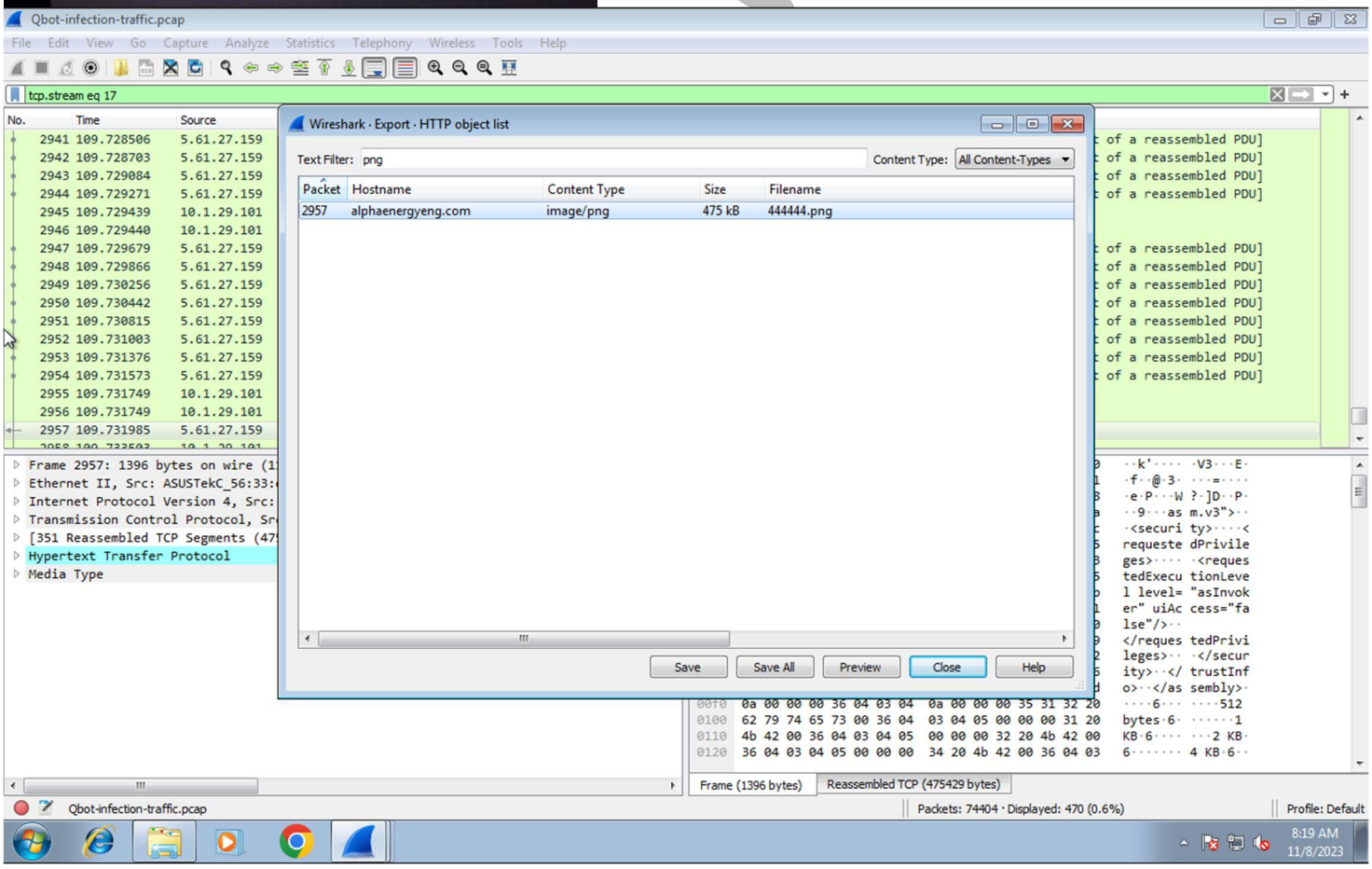


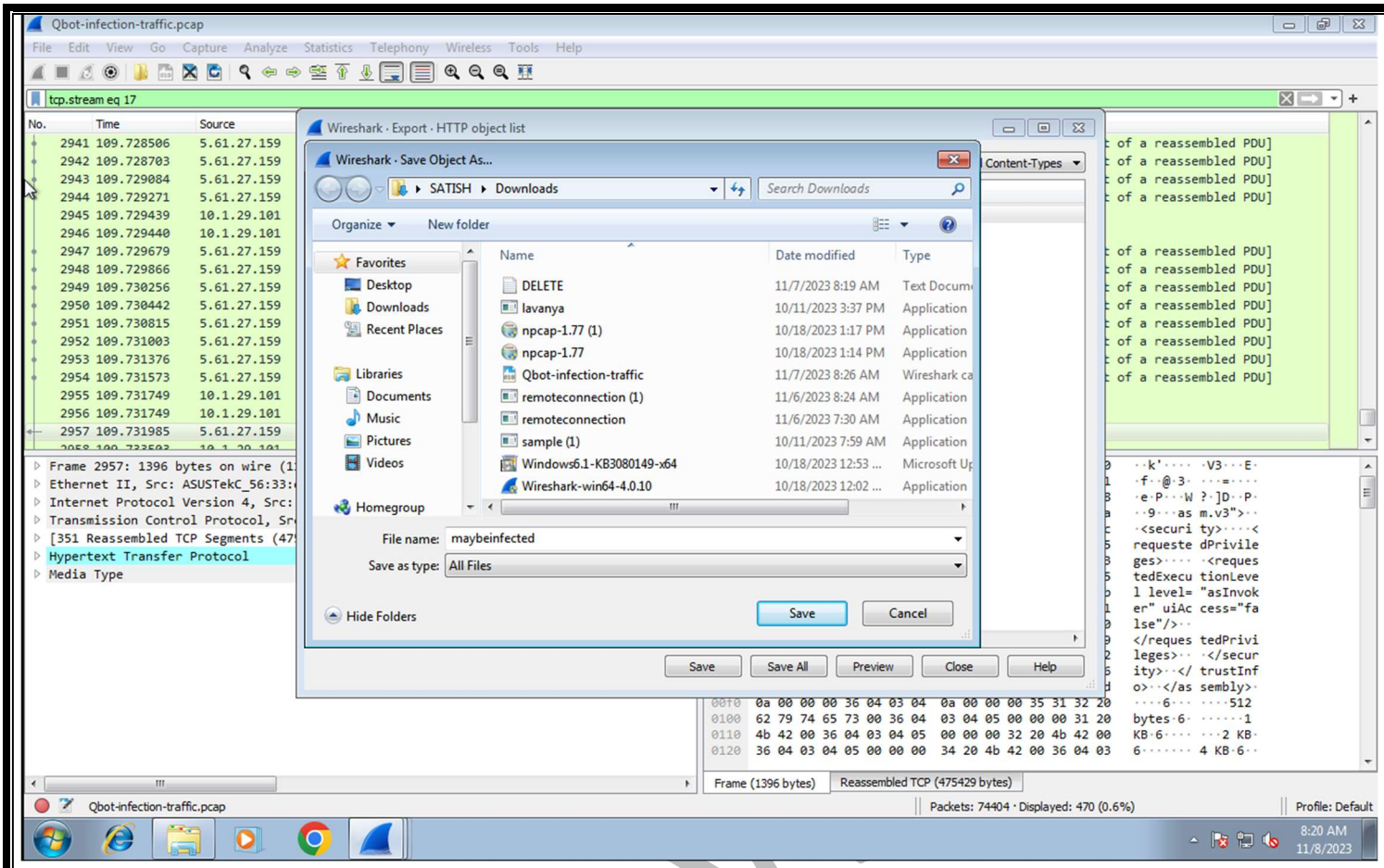


5) Exported objects :

Navigate to the File menu in Wireshark.
Selected "Export Objects" and then "HTTP."
Exported the PNG file for further analysis.

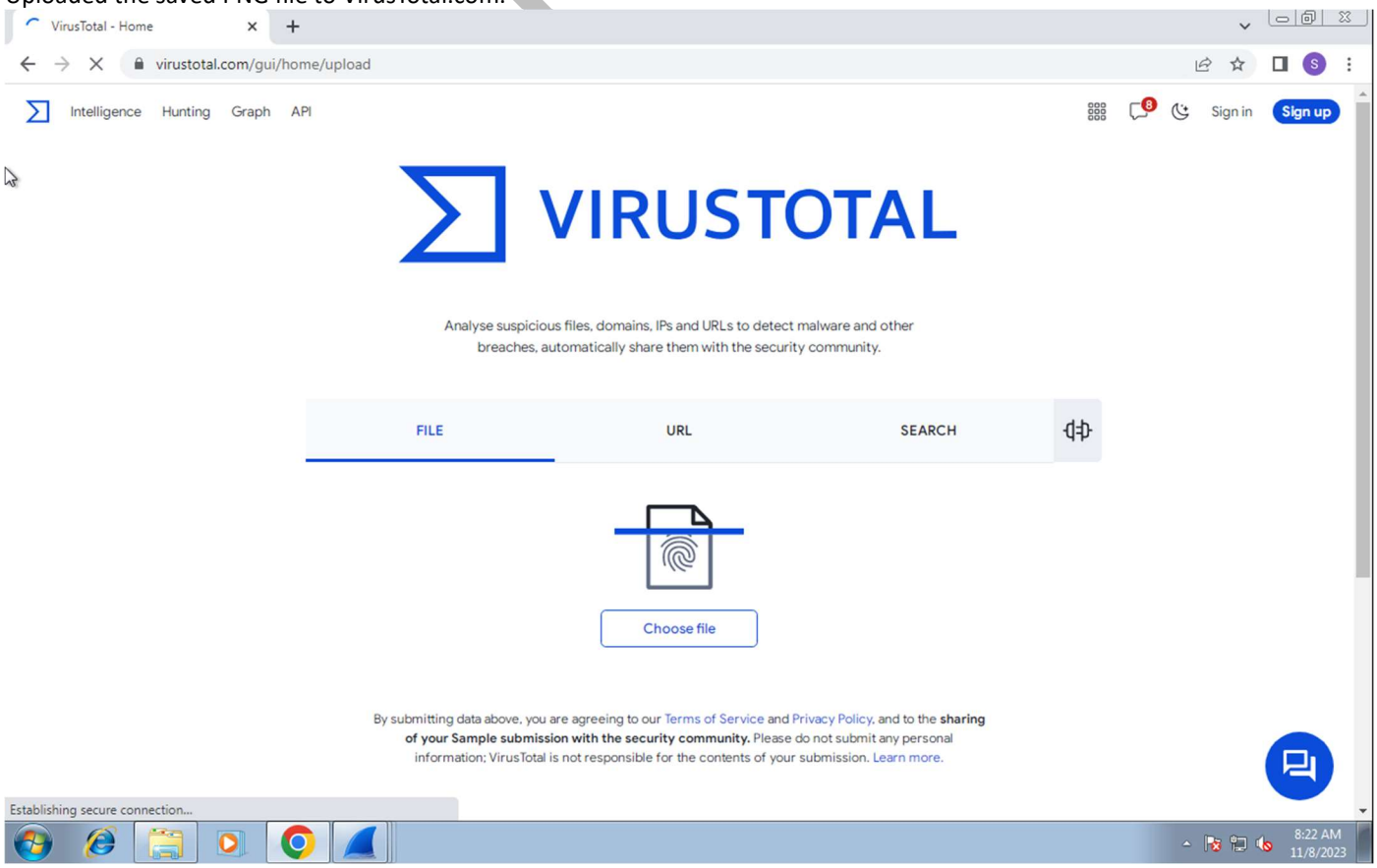


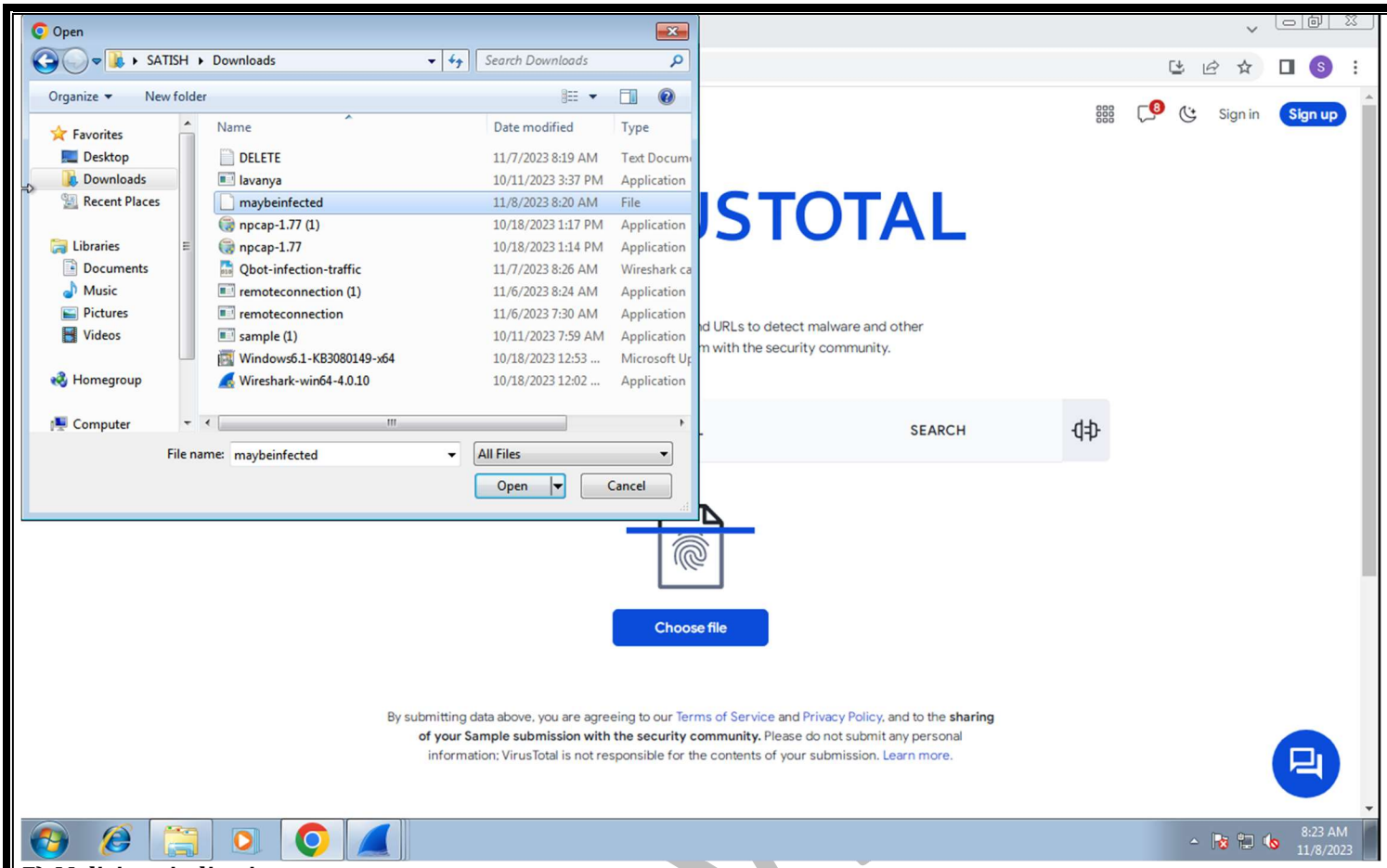




6) Virustotal scan:

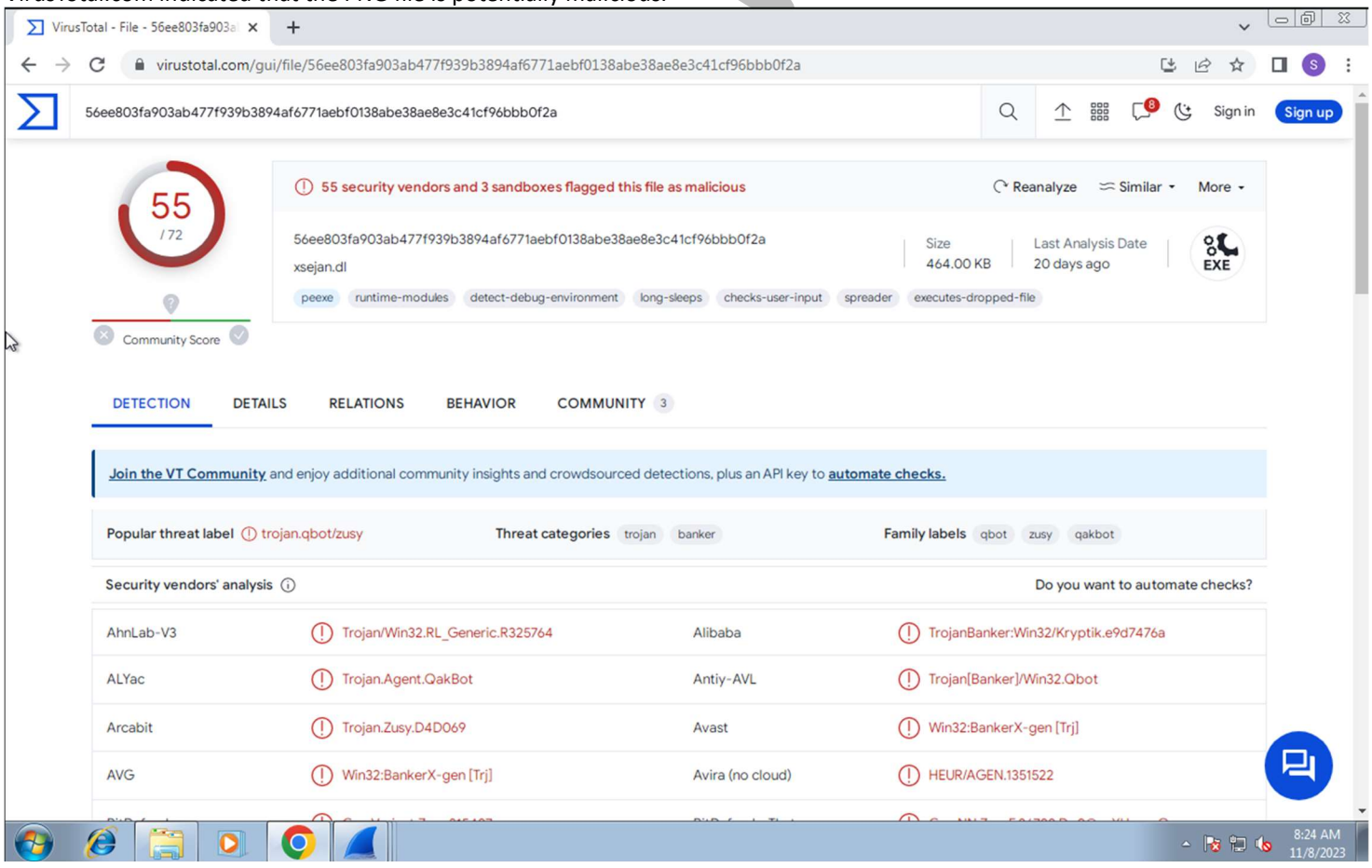
Uploaded the saved PNG file to VirusTotal.com.





7) Malicious indication:

VirusTotal.com indicated that the PNG file is potentially malicious.

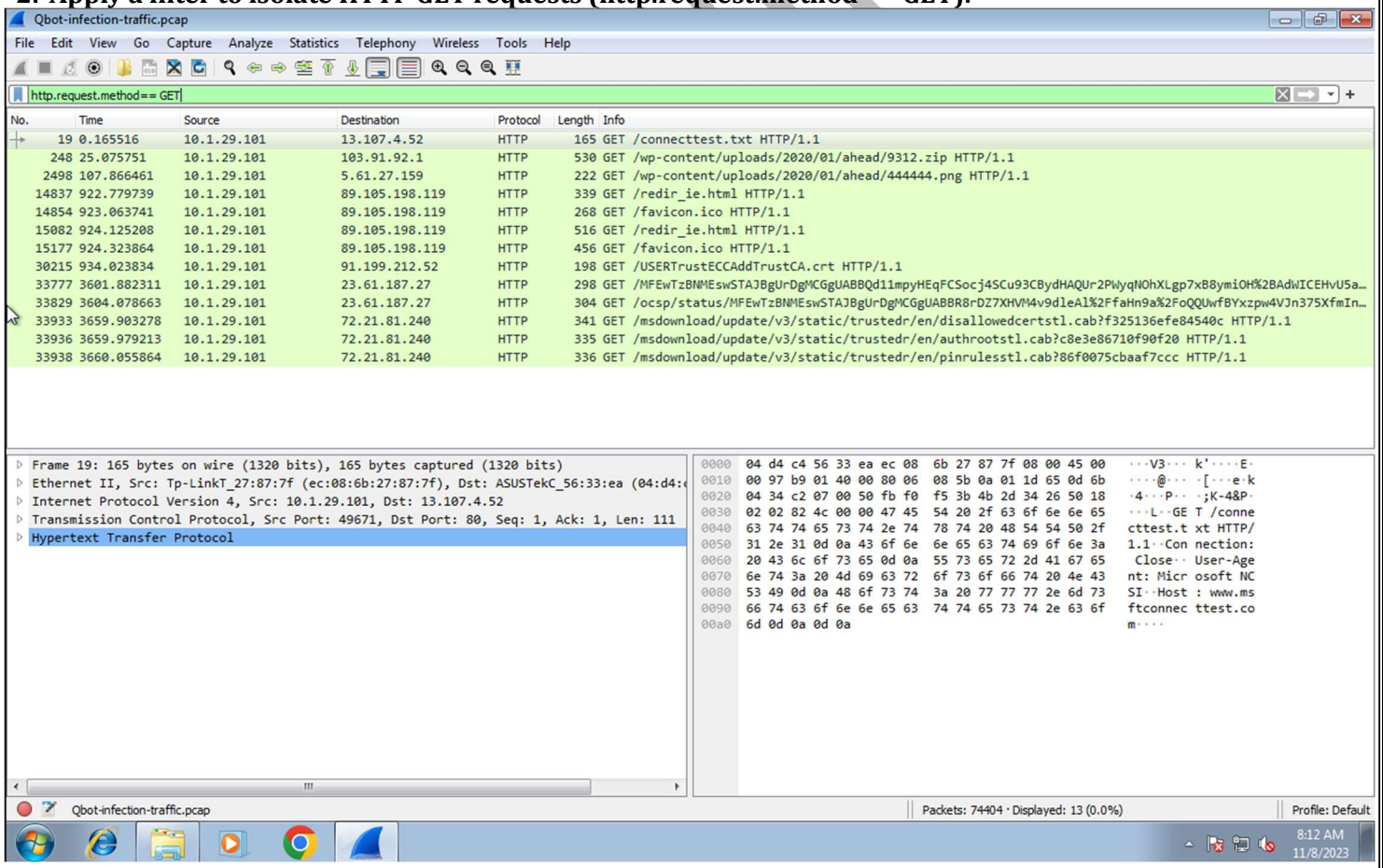


[zip file analysis]

1. Capture and Filter Traffic:

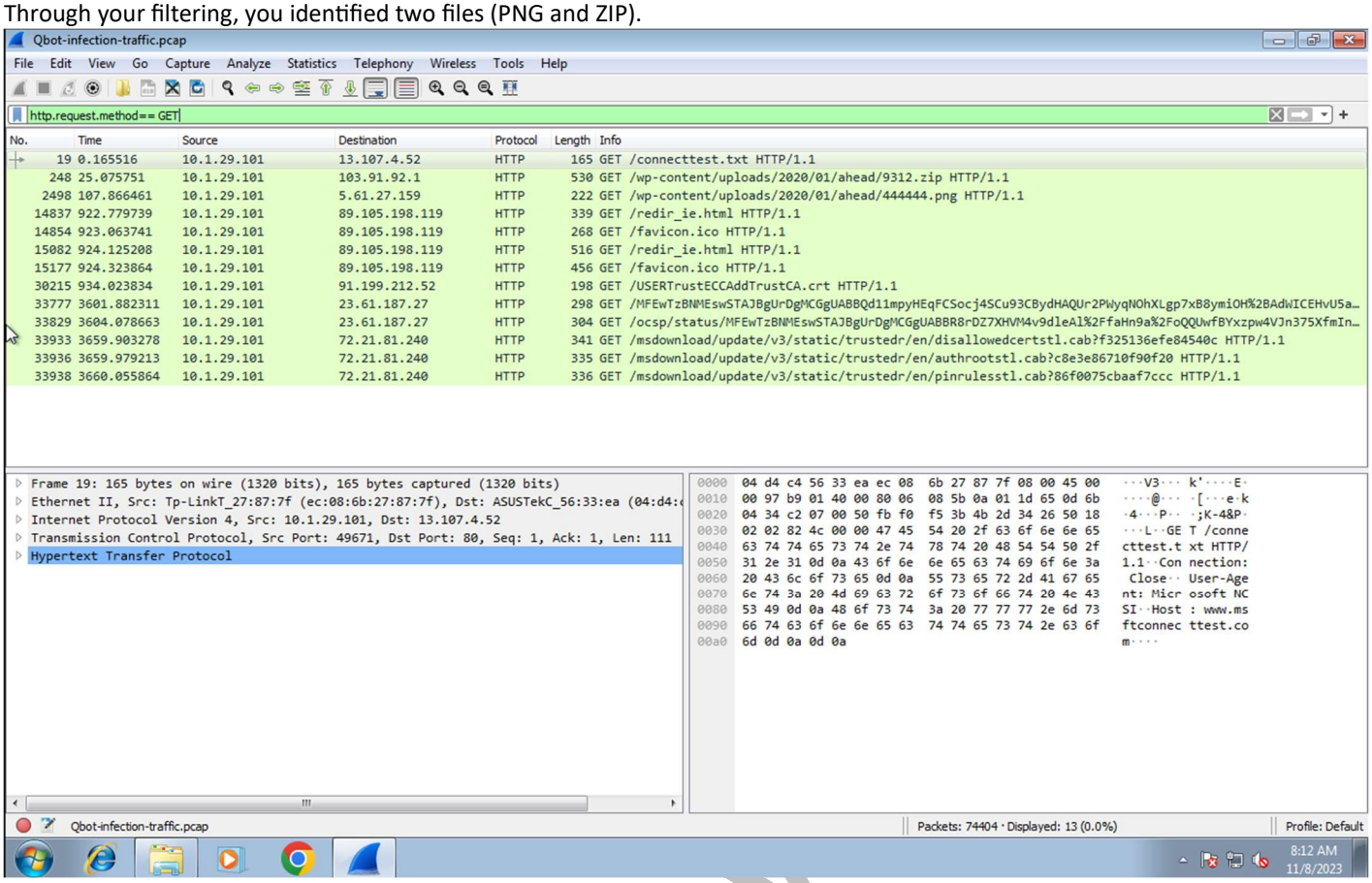
Obtain a pcap file using Wireshark.

2. Apply a filter to isolate HTTP GET requests (http.request.method == GET).



3. Identify files:

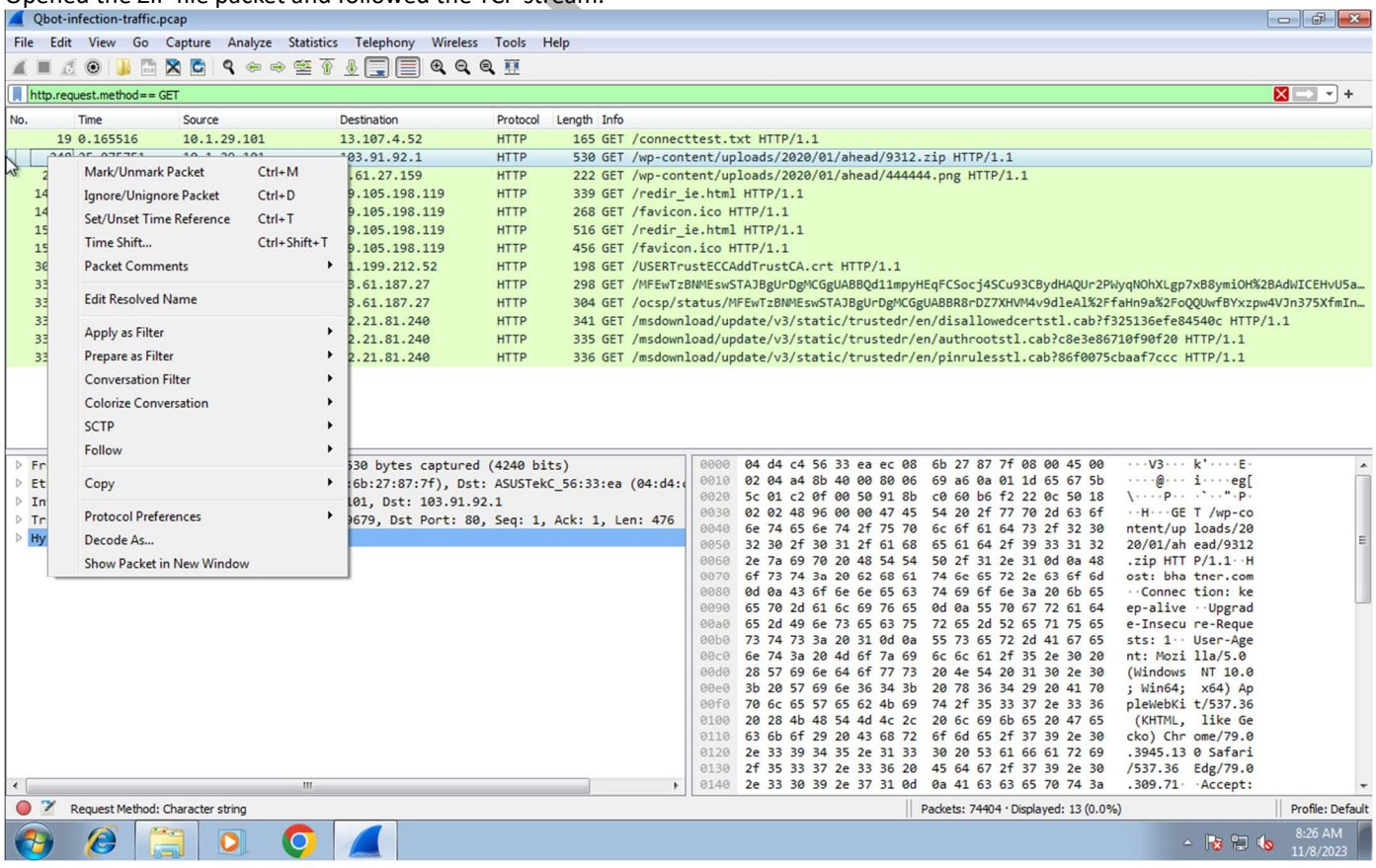
Through your filtering, you identified two files (PNG and ZIP).

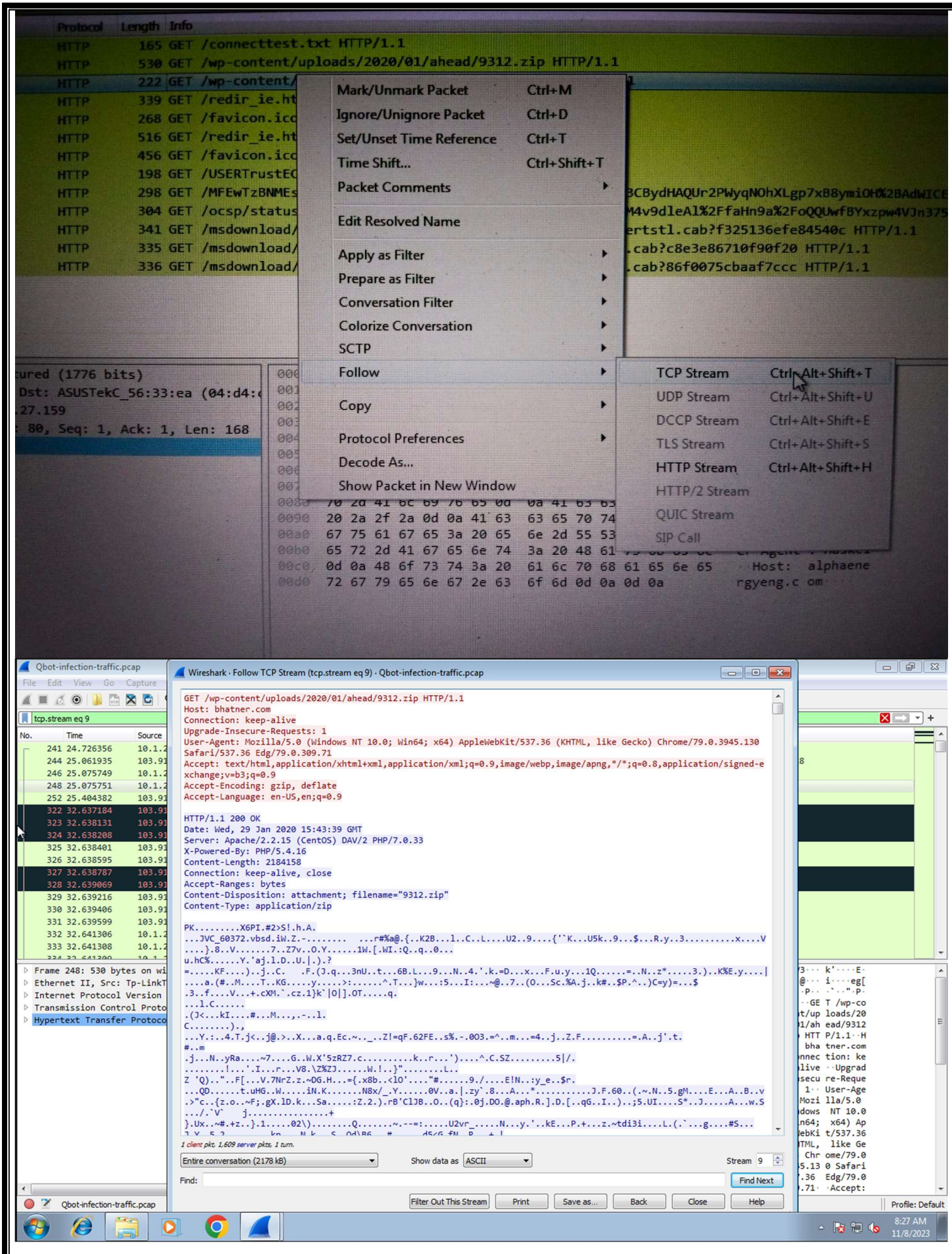


4. ZIP File Analysis:

Focused on the ZIP file.

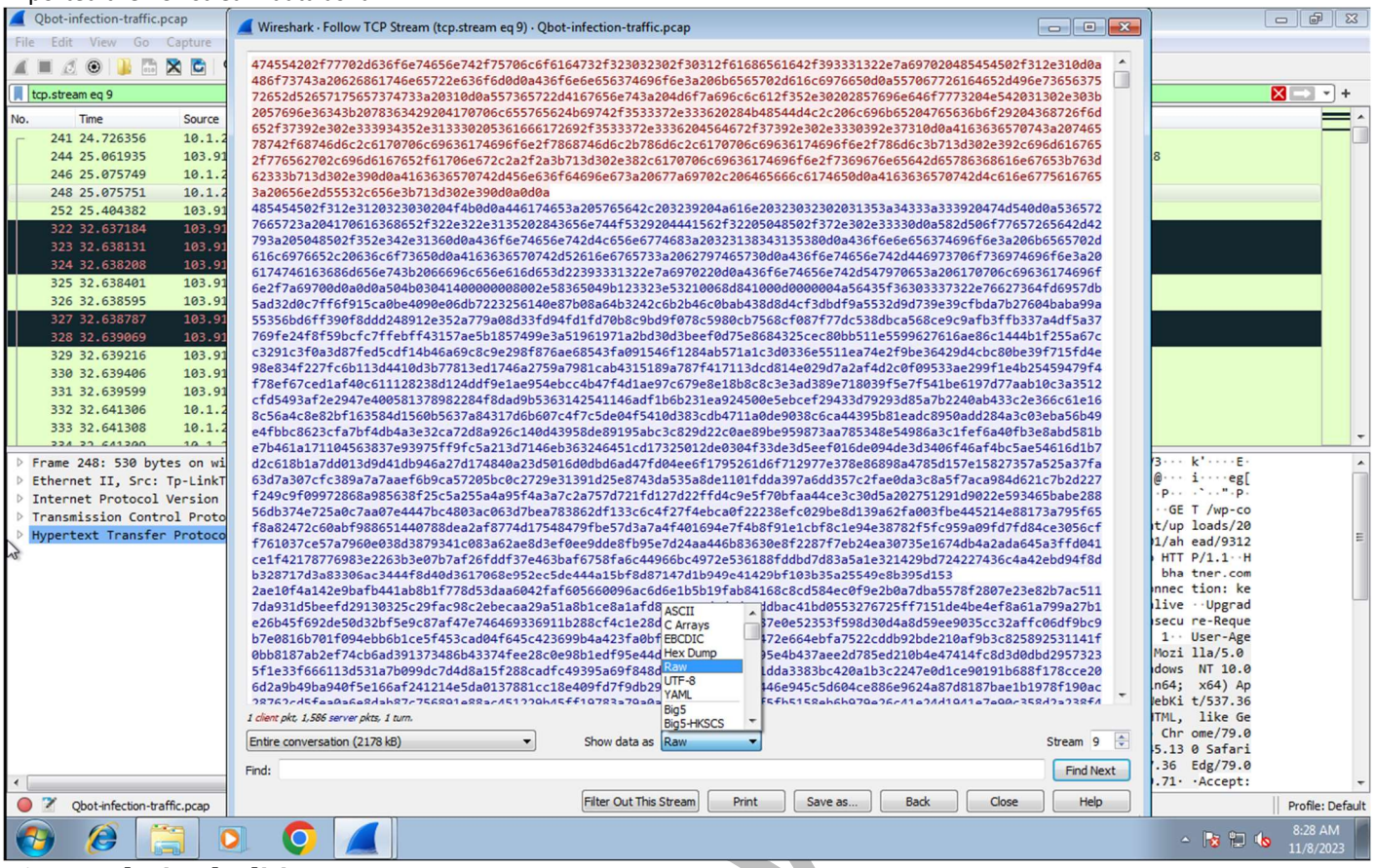
Opened the ZIP file packet and followed the TCP stream.




Protocol Length Info
HTTP 165 GET /connecttest.txt HTTP/1.1
HTTP 530 GET /wp-content/uploads/2020/01/ahead/9312.zip HTTP/1.1
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call
Qbot-infection-traffic.pcap
Wireshark · Follow TCP Stream (tcp.stream eq 9) · Qbot-infection-traffic.pcap
GET /wp-content/uploads/2020/01/ahead/9312.zip HTTP/1.1
Host: bhatner.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 Edg/79.0.309.71
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
HTTP/1.1 200 OK
Date: Wed, 29 Jan 2020 15:43:39 GMT
Server: Apache/2.2.15 (CentOS) DAV/2 PHP/7.0.33
X-Powered-By: PHP/5.4.16
Content-Length: 2184158
Connection: keep-alive, close
Accept-Ranges: bytes
Content-Disposition: attachment; filename="9312.zip"
Content-Type: application/zip
Entire conversation (2178 kB)
Show data as ASCII
Stream 9
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

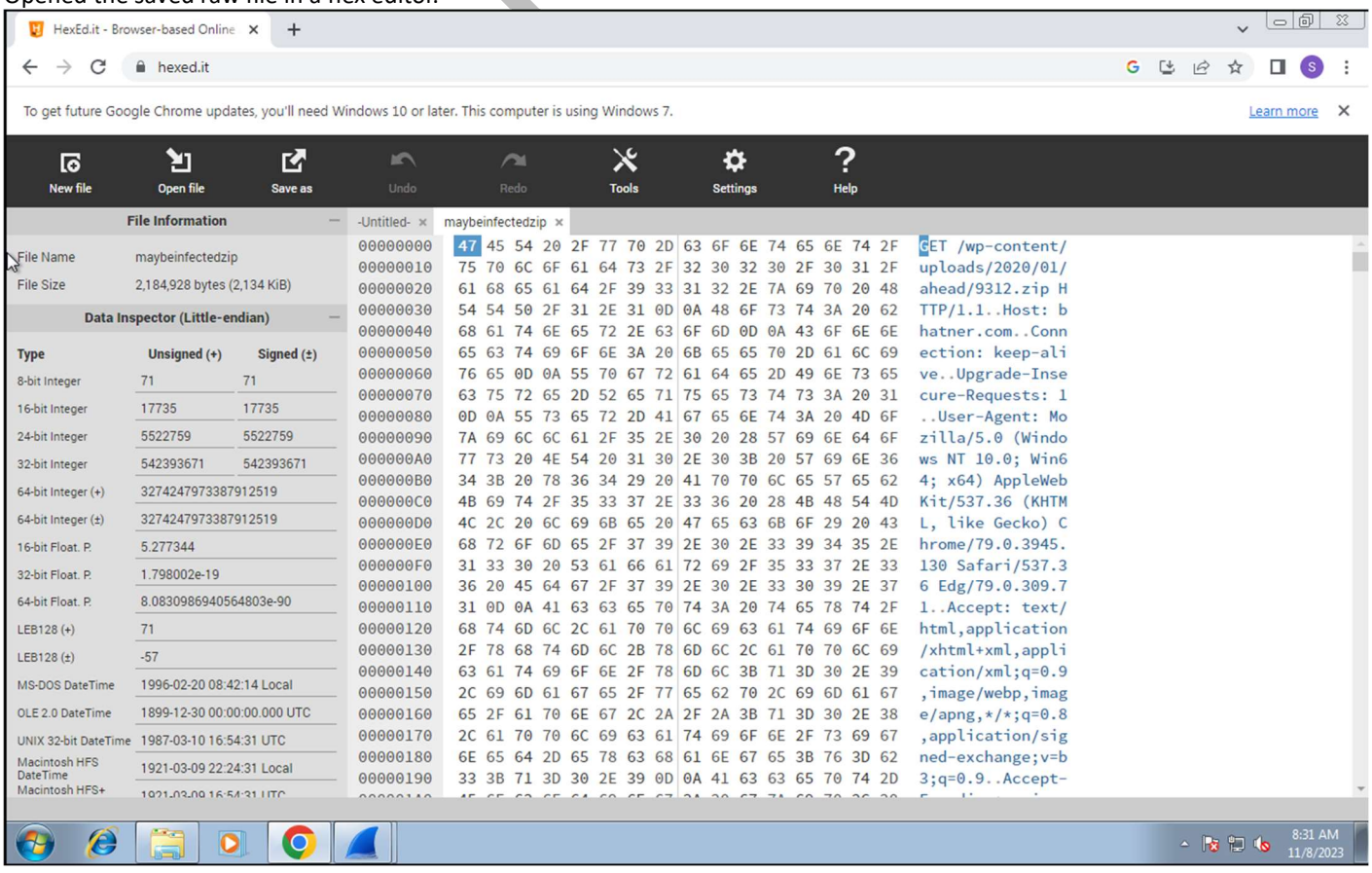
5. Save TCP Stream as Raw:

Exported the TCP stream data as raw.



6. Hexadecimal Editing:

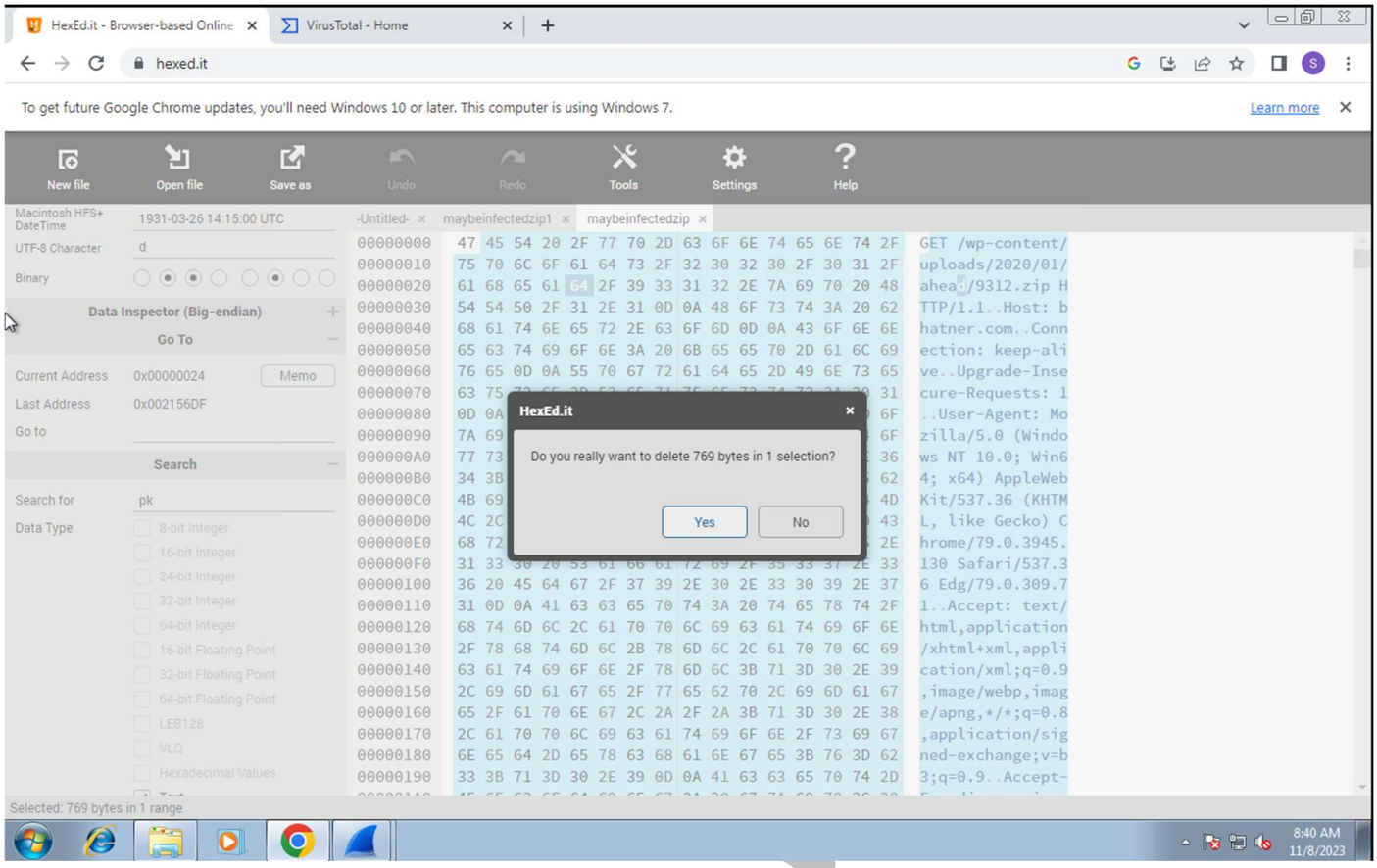
Opened the saved raw file in a hex editor.

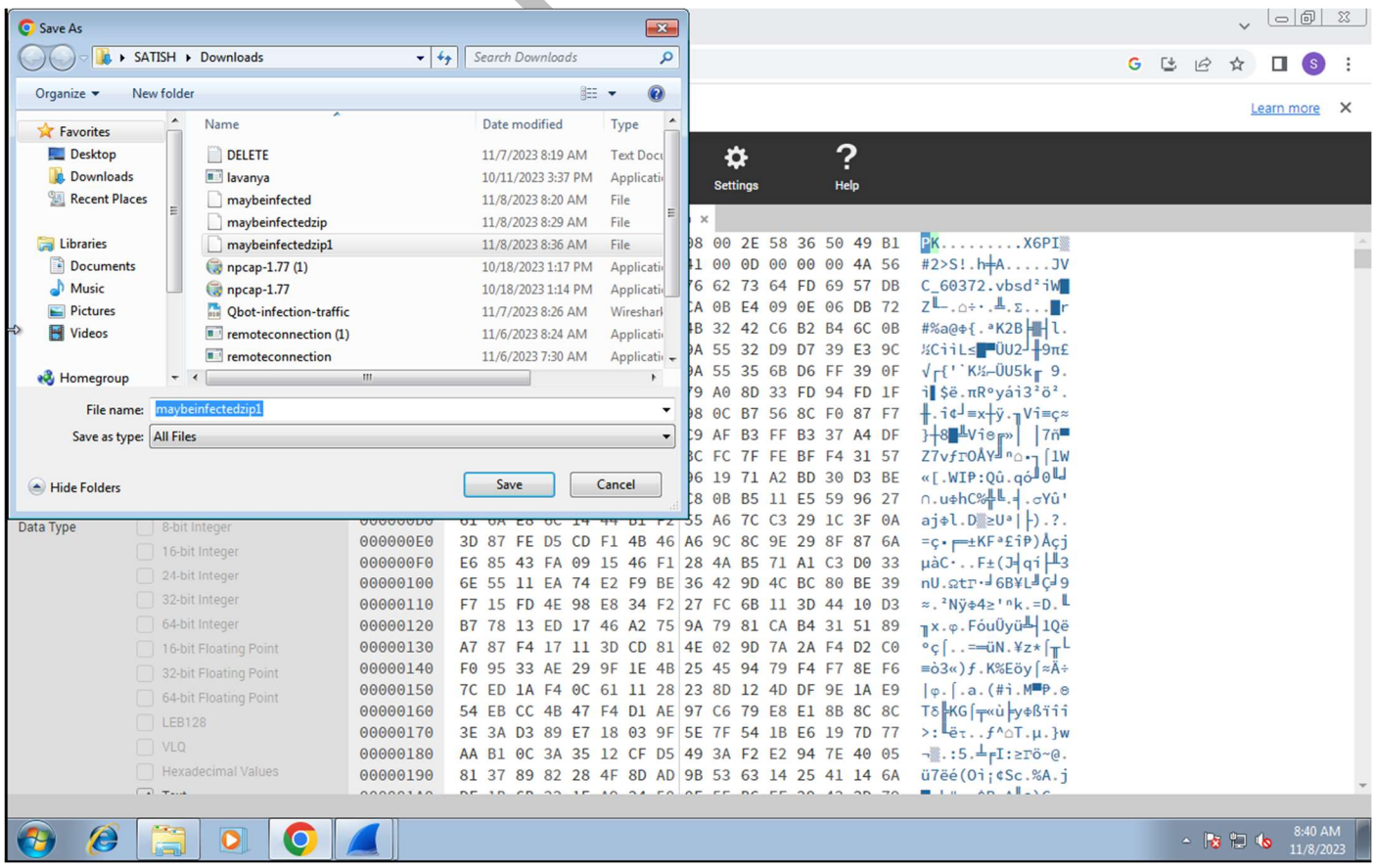


7. Trimming and Saving:

Deleted all bytes before the magic bytes "PK" (ZIP file signature).

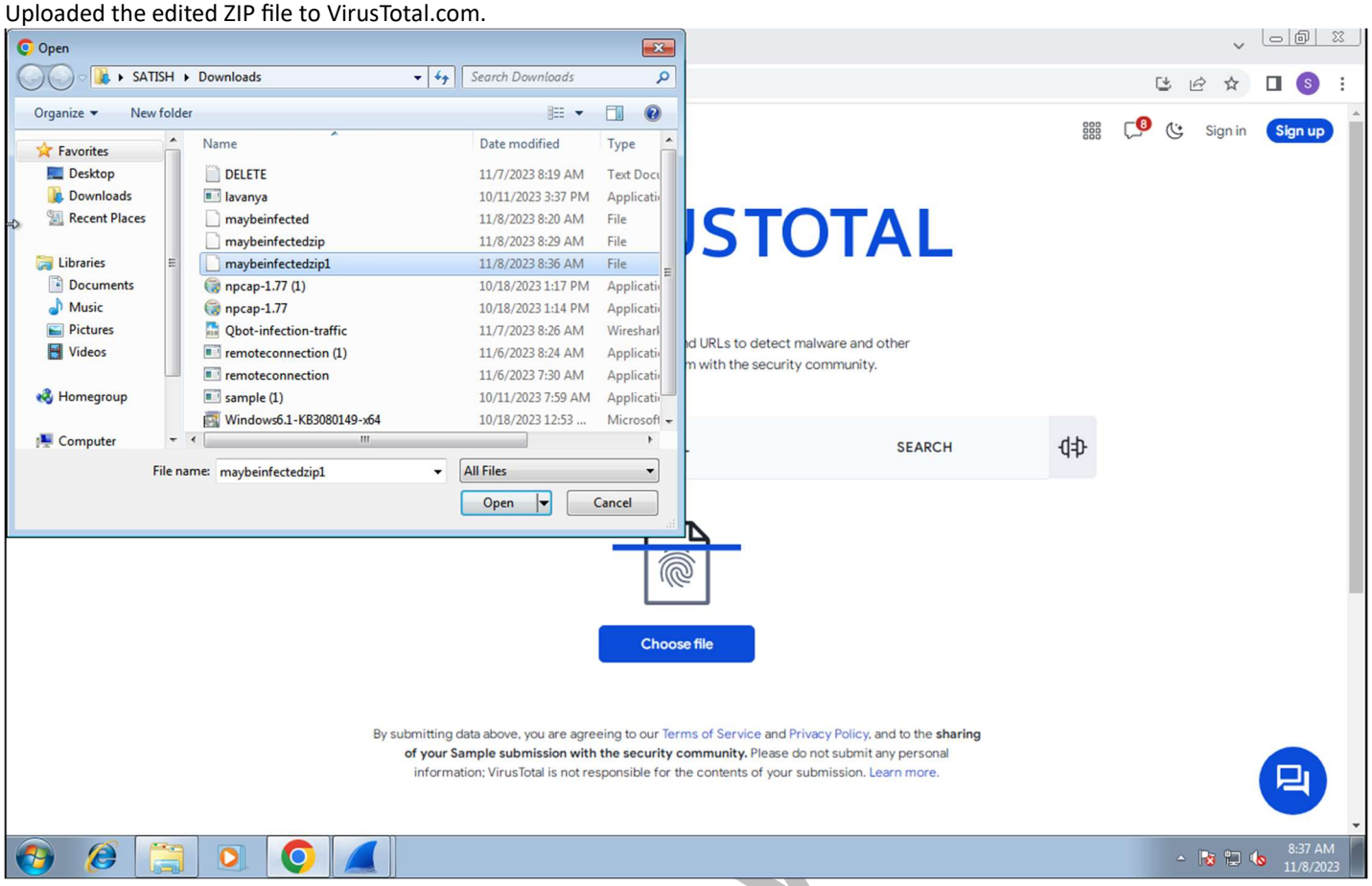
Saved the edited file.





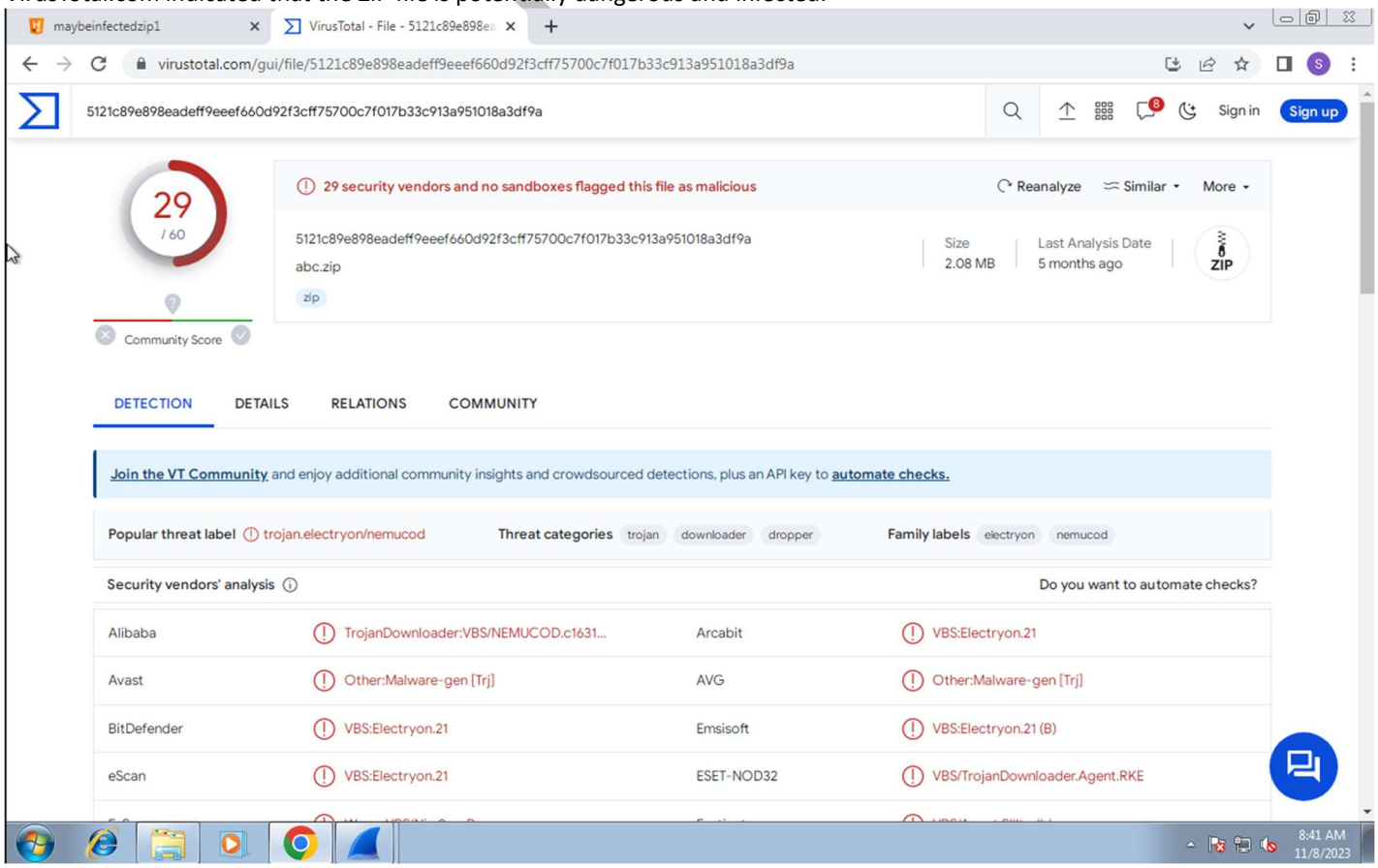
8. VirusTotal Scan:

Uploaded the edited ZIP file to VirusTotal.com.



9. Malicious Indication:

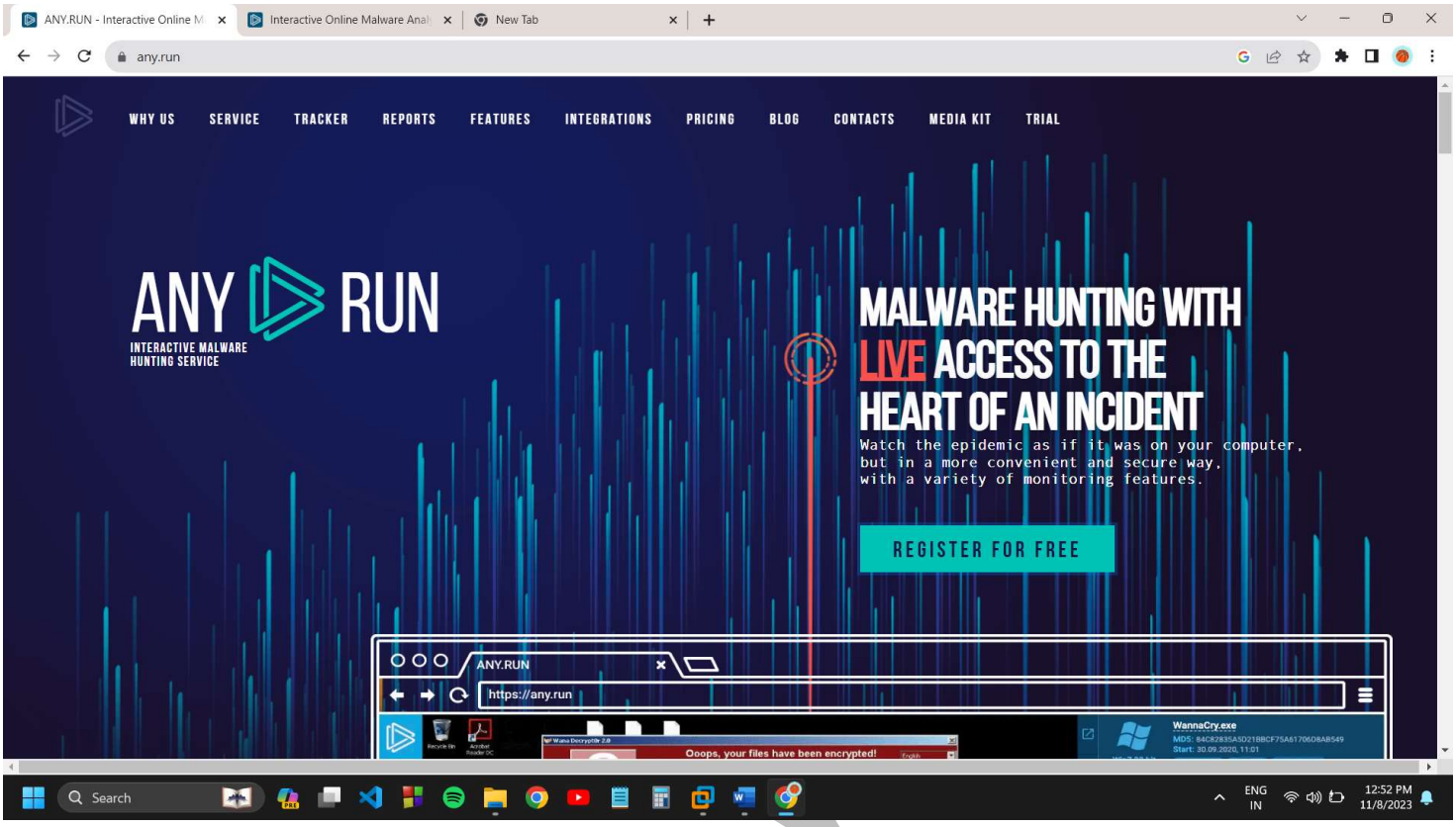
VirusTotal.com indicated that the ZIP file is potentially dangerous and infected.

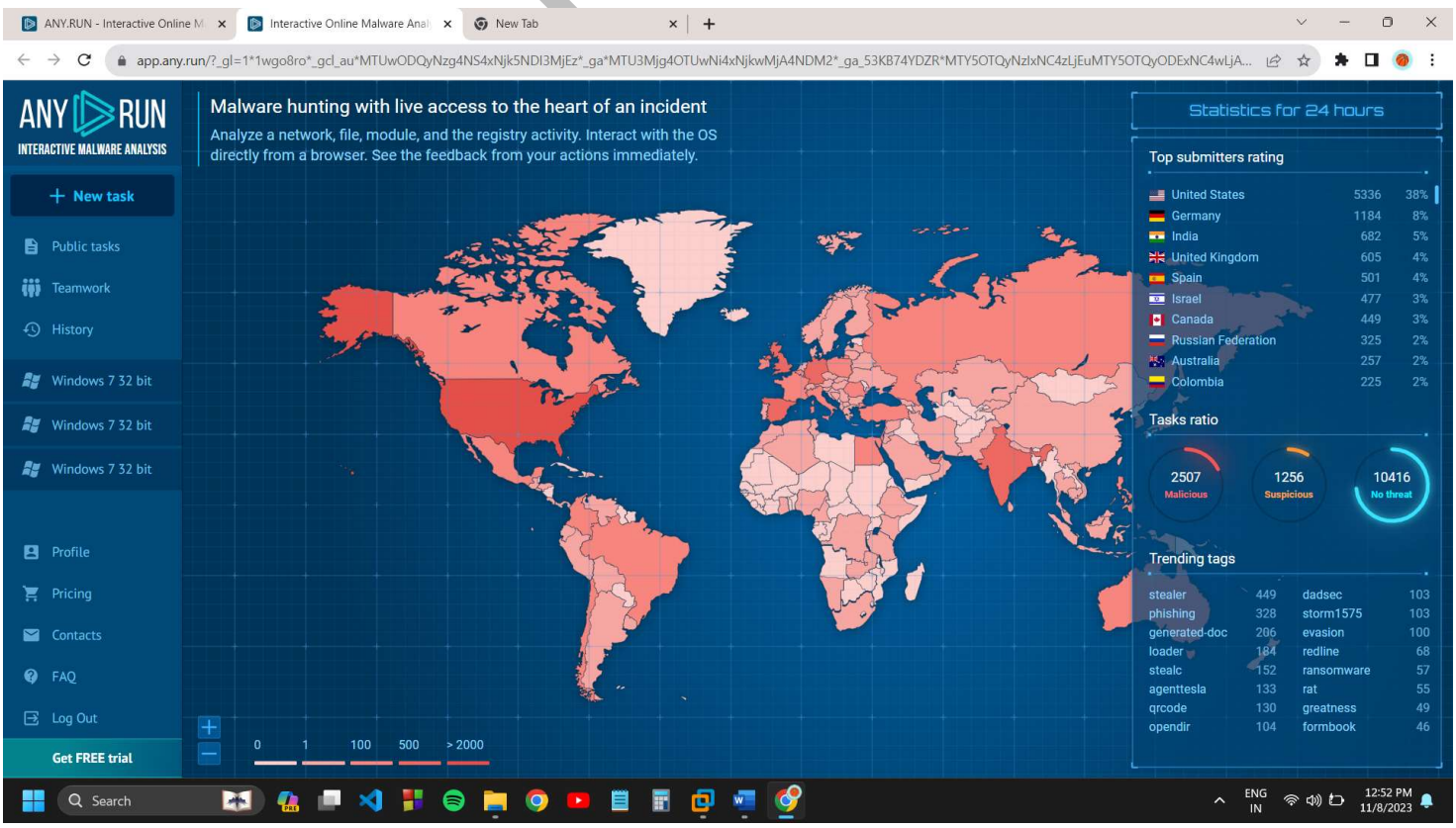


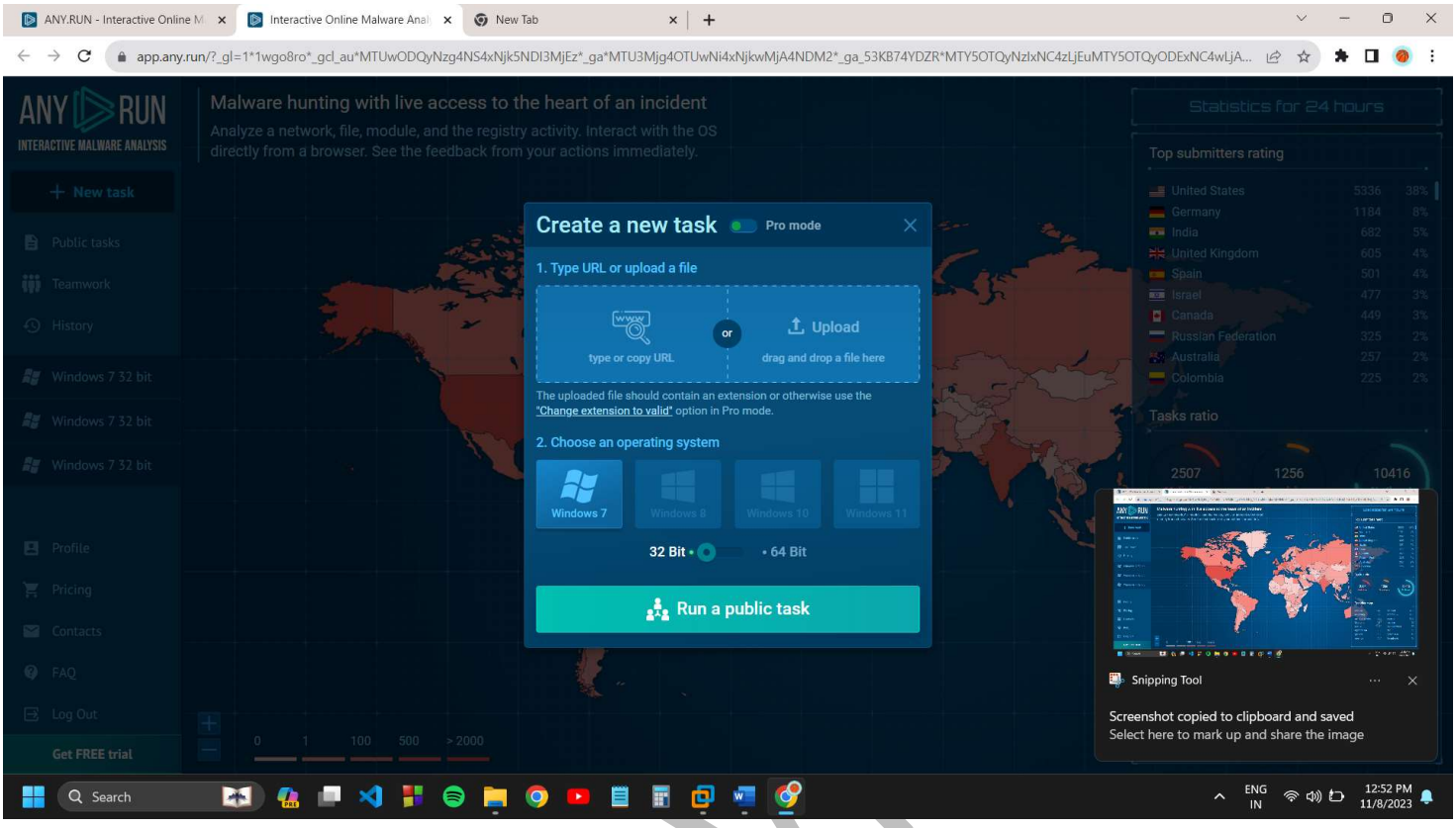
❖ DYNAMIC ANALYSIS:

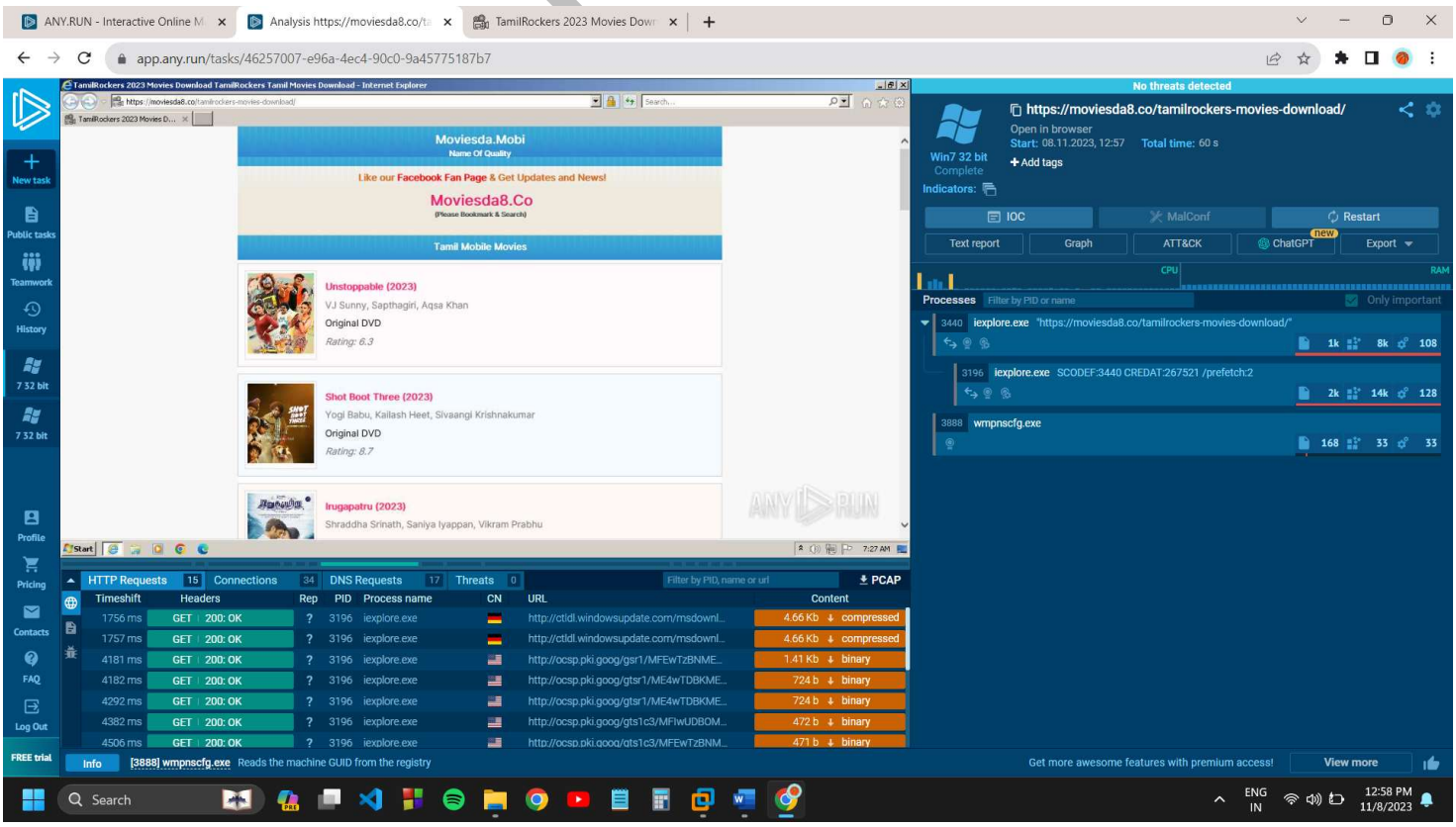
Tools used:

- Sandbox environment(ANY.RUN)






ANY.RUN - Interactive Online M
Interactive Online Malware Anal
New Tab
app.any.run/?_gl=1*1wgo8ro*_gcl_au*MTUwODQyNzg4NS4xNjk5NDI3MjEz*_ga*MTU3Mjg4OTUwNi4xNjkwMjA4NDM2*_ga_53KB74YDZR*MTY5OTQyNzIxNC4zLjEuMTY5OTQyODExNC4wLjA...
ANY RUN
INTERACTIVE MALWARE ANALYSIS
Malware hunting with live access to the heart of an incident
Analyze a network, file, module, and the registry activity. Interact with the OS directly from a browser. See the feedback from your actions immediately.
New task
Public tasks
Teamwork
History
Windows 7 32 bit
Windows 7 32 bit
Windows 7 32 bit
Profile
Pricing
Contacts
FAQ
Log Out
Get FREE trial
Create a new task
Pro mode
1. Type URL or upload a file
type or copy URL
or
Upload
drag and drop a file here
The uploaded file should contain an extension or otherwise use the "Change extension to valid" option in Pro mode.
2. Choose an operating system
Windows 7
Windows 8
Windows 10
Windows 11
32 Bit
64 Bit
Run a public task
Statistics for 24 hours
Top submitters rating
United States 5336 38%
Germany 1184 8%
India 682 5%
United Kingdom 605 4%
Spain 501 4%
Israel 477 3%
Canada 449 3%
Russian Federation 325 2%
Australia 257 2%
Colombia 225 2%
Tasks ratio
2507
1256
10416
Snipping Tool
Screenshot copied to clipboard and saved
Select here to mark up and share the image
Search
ENG IN
12:52 PM 11/8/2023


ANY.RUN - Interactive Online M
Analysis https://moviesda8.co/t
TamilRockers 2023 Movies Down
app.any.run/tasks/46257007-e96a-4ec4-90c0-9a45775187b7
TamilRockers 2023 Movies Download TamilRockers Tamil Movies Download - Internet Explorer
Moviesda.Mobi
Name Of Quality
Like our Facebook Fan Page & Get Updates and News!
Moviesda8.Co
(Please Bookmark & Search)
Tamil Mobile Movies
Unstoppable (2023)
VJ Sunny, Sapthagiri, Aqsa Khan
Original DVD
Rating: 6.3
Shot Boot Three (2023)
Yogi Babu, Kailash Heet, Sivaangi Krishnakumar
Original DVD
Rating: 8.7
Irugapatru (2023)
Shraddha Srinath, Saniya Iyappan, Vikram Prabhu
No threats detected
https://moviesda8.co/tamilrockers-movies-download/
Open in browser
Start: 08.11.2023, 12:57
Total time: 60 s
Add tags
Win7 32 bit
Complete
Indicators:
IOC
MalConf
Restart
Text report
Graph
ATT&CK
ChatGPT
Export
CPU
RAM
Processes
Filter by PID or name
Only important
3440 iexplore.exe "https://moviesda8.co/tamilrockers-movies-download/"
3196 iexplore.exe SCODEF:3440 CREDAT:267521 /prefetch:2
3888 wmpnscfg.exe
HTTP Requests 15
Connections 34
DNS Requests 17
Threats 0
PCAP
Timeshift Headers Rep PID Process name CN URL Content
1756 ms GET 200: OK ? 3196 iexplore.exe http://ctldl.windowsupdate.com/msdownl... 4.66 Kb compressed
1757 ms GET 200: OK ? 3196 iexplore.exe http://ctldl.windowsupdate.com/msdownl... 4.66 Kb compressed
4181 ms GET 200: OK ? 3196 iexplore.exe http://ocsp.pki.goog/gsr1/MFEwTzBNME... 1.41 Kb binary
4182 ms GET 200: OK ? 3196 iexplore.exe http://ocsp.pki.goog/gtsr1/ME4wTDBKME... 724 b binary
4292 ms GET 200: OK ? 3196 iexplore.exe http://ocsp.pki.goog/gtsr1/ME4wTDBKME... 724 b binary
4382 ms GET 200: OK ? 3196 iexplore.exe http://ocsp.pki.goog/gts1c3/MFIwUDBOM... 472 b binary
4506 ms GET 200: OK ? 3196 iexplore.exe http://ocsp.pki.goog/gts1c3/MFEwTzBNM... 471 b binary
Info
[3888] wmpnscfg.exe Reads the machine GUID from the registry
Get more awesome features with premium access!
View more
Search
ENG IN
12:58 PM 11/8/2023

ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Behavior MalConf Static information Video Screenshots System events Network

General Info

Add for printing

URL: https://moviesda8.co/tamilrockers-movies-download/
Full analysis: https://app.any.run/tasks/46257007-e96a-4ec4-90c0-9a45775187b7
Verdict: No threats detected
Analysis date: November 08, 2023 at 12:57:25
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:
SHA1: C933565C40EC8565A7F0599221C2A66B87D61AC1
SHA256: 41BF1E0EAF686A71FFA6B2713DAA045C3EF411A1EA21F905016FDE247A8EA496
SSDEEP: 3:N8xBR0iSGPwIgbSCn:2t0VGoBbL

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Behavior activities

Add for printing

MALICIOUS

No malicious indicators.

SUSPICIOUS

No suspicious indicators.

INFO

Checks supported languages
- wmpnscfg.exe (PID: 3888)

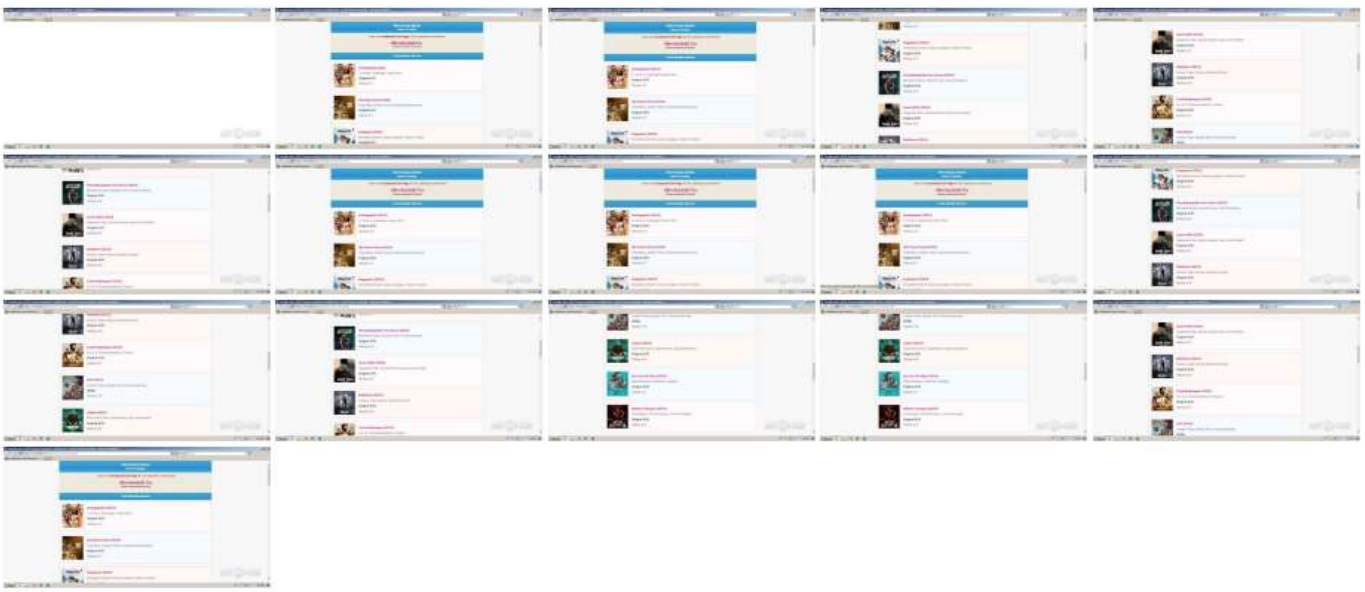
Manual execution by a user
- wmpnscfg.exe (PID: 3888)

Application launched itself
- iexplore.exe (PID: 3440)

Reads the machine GUID from the registry
- wmpnscfg.exe (PID: 3888)

Reads the computer name
- wmpnscfg.exe (PID: 3888)

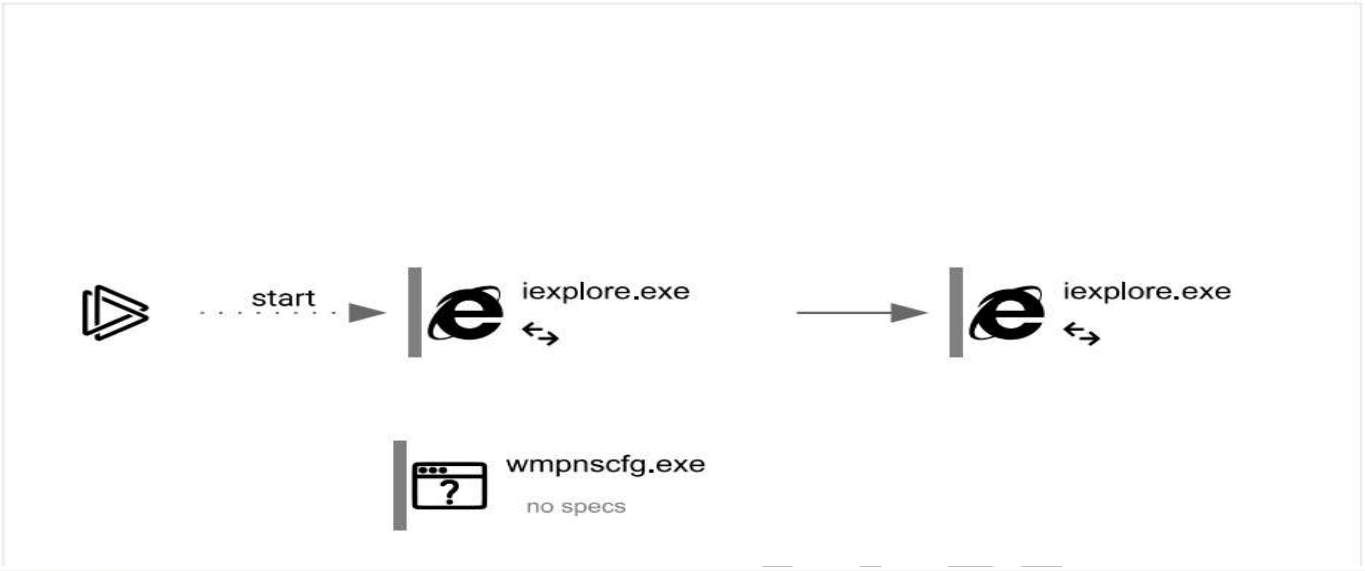
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
38	3	0	0

Behavior graph



Specs description

- Program did not start
- Low-level access to the HDD
- Process was added to the startup
- Debug information is available
- Probably Tor was used
- Behavior similar to spam
- Task has injected processes
- Executable file was dropped
- Known threat
- RAM overrun
- Network attacks were detected
- Integrity level elevation
- Connects to the network
- CPU overrun
- Process starts the services
- System was rebooted
- Task contains several apps running
- Application downloaded the executable file
- Actions similar to stealing personal data
- Task has apps ended with an error
- File is detected by antivirus software
- Inspected object has suspicious PE structure
- Behavior similar to exploiting the vulnerability
- Task contains an error or was rebooted
- The process has the malware config

Process information

PID	CMD	Path	Indicators	Parent process
3440	"C:\Program Files\Internet Explorer\iexplore.exe" "https://moviesda8.co/tamilrockers-movies-download/"	C:\Program Files\Internet Explorer\iexplore.exe	↔	explorer.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Internet Explorer
Version:	11.00.9600.16428 (winblue_gdr.131013-1700)		

PID	CMD	Path	Indicators	Parent process
3196	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3440 CREDAT:267521 /prefetch:2	C:\Program Files\Internet Explorer\iexplore.exe	↔	iexplore.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Internet Explorer
Version:	11.00.9600.16428 (winblue_gdr.131013-1700)		

PID	CMD	Path	Indicators	Parent process
3888	"C:\Program Files\Windows Media Player\wmpnscfg.exe"	C:\Program Files\Windows Media Player\wmpnscfg.exe	—	explorer.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Media Player Network Sharing Service Configuration Application
Exit code:	0	Version:	12.0.7600.16385 (win7_rtm.090713-1255)

Registry activity

Total events	Read events	Write events	Delete events
22 613	22 544	66	3

Modification events

(PID) Process:	(3440) iexplore.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation:	write	**Name:**	NTPDaysSinceLastAutoMigration
Value:	0		
(PID) Process:	(3440) iexplore.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing
Operation:	write	**Name:**	NTPLastLaunchHighDateTime
Value:	30847387		
(PID) Process:	(3440) iexplore.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\UrlBlockManager
Operation:	write	**Name:**	NextCheckForUpdateHighDateTime
Value:	30847437		
(PID) Process:	(3440) iexplore.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation:	write	**Name:**	CachePrefix
Value:	Cookie:		
(PID) Process:	(3440) iexplore.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation:	write	**Name:**	CachePrefix
Value:	Visited:		

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	34	39	0

Dropped files

PID	Process	Filename	Type
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CAF4703619713E3F18D8A9D5D88D6288_F2DAF19C1F776537105D08FC8D978464 **MD5:** 8202A1CD02E7D69597995CABBE881A12 **SHA256:** 58F381C3A0A0ACE6321DA22E40BD44A5978D98B9C9390AB9258426B5CF75A7A5	binary
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CAF4703619713E3F18D8A9D5D88D6288_F2DAF19C1F776537105D08FC8D978464 **MD5:** 0CF5C980C93C66C4757E1A8A99160AC6 **SHA256:** 4C11B6C36DB881D4E0435BE87BB97E89A8090A680797E56E654F5A466A4C49C3	binary
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F07644E38ED7C9F37D11EEC6D4335E02_17A1BB9C6401DC9652040571BD192211 **MD5:** CAC74099BB8D6CE9C2B8D45A8D29C372 **SHA256:** 7296F8A6DFE6E0C0046A8E7DA8641913CC892EC47613E56F86B8B75BC5D1DEBD	binary
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\24BD96D5497F70B3F510A6B53CD43F3E_3A89246FB90C5EE6620004F1AE0EB0EA **MD5:** 16FDB5C10A4DF5AEE308F7FB5F96C679 **SHA256:** EDF45F72F6677176778951705190DB3E36A44EA29DF72FF7BBD7F3DE7134A8708	binary
3196	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\YTOWV792\scam-2003-2023[1].jpg **MD5:** 0A20E06237FE1544A37BA1EE21502BF0 **SHA256:** E0BD56CF52D0BA15A34371EFA2C2FD87ACD27040FEBBA76251A10704452653AB	image
3196	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\YTOWV792\tamil-kudimagan-2023[1].jpg **MD5:** A0AE00E38B7A7FB11C55D7597F87DACF **SHA256:** 4D65A0110541162AEADBAE1EF26B5C80CE4E13CE4E3E989BC4B1BD4F71E99AC2	image
3196	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\MFAQUS6V\tamilrockers-movies-download[1].htm **MD5:** 88213C42E2A1F775F873ACF6CF446C06 **SHA256:** 8970F90829A80CA63D9BF4069DE059D48FC7872DA5DFB533D2E1B8BCD46AECEE	html
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	compressed

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
15	34	17	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gtsr1/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBQwkcLWD4LqGJ7bE7B1XZsEbmfwUAQU5K8rJnEaK0gnhS9SZizv8lkTcT4CDQIDvFCjJ1PwkYAi7fE%3D	unknown	binary	724 b	unknown
3196	iexplore.exe	GET	200	23.53.40.41:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d6bb2ad0af14907d	unknown	compressed	4.66 Kb	unknown
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gsr1/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS3V7W2nAf4FIMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCEHe9DWzbNvka6iEPxPBY0w0%3D	unknown	binary	1.41 Kb	unknown
3196	iexplore.exe	GET	200	23.53.40.41:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?86908589b66dbf86	unknown	compressed	61.6 Kb	unknown
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gtsr1/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBQwkcLWD4LqGJ7bE7B1XZsEbmfwUAQU5K8rJnEaK0gnhS9SZizv8lkTcT4CDQIDvFNZazTHGPUBUGY%3D	unknown	binary	724 b	unknown
3440	iexplore.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAqvpsXKY8RRQeo74ffHUxc%3D	unknown	binary	471 b	unknown
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gts1c3/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTHLnmK3f9hNLO67UdCuLvGwCQHYwQUinR%2Fr4XN7pXNPZzQ4kYU83E1HScCEGNkd7zfgP4rEhC%2BpCYwNEA%3D	unknown	binary	471 b	unknown
3196	iexplore.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEA177el9ggmWelJjG4vdGL0%3D	unknown	binary	471 b	unknown

DNS requests

Domain	IP	Reputation
ctldl.windowsupdate.com	23.53.40.41 23.53.40.40 23.53.40.49 23.53.40.83	whitelisted
ocsp.pki.goog	142.250.181.227	whitelisted
nl.yieldedshotter.com	172.255.6.54 23.109.82.219 23.109.248.184 23.109.82.33 23.109.82.94 142.91.159.136 23.109.82.5 23.109.82.239 23.109.150.207 23.109.82.14 23.109.248.177	unknown
fonts.googleapis.com	142.250.186.170	whitelisted
www.clarity.ms	13.107.246.67 13.107.213.67	whitelisted
fonts.gstatic.com	172.217.16.195	whitelisted
api.bing.com	13.107.5.80	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2588	svchost.exe	239.255.255.250:1900	–	–	–	whitelisted
3196	iexplore.exe	23.53.40.41:80	ctldl.windowsupdate.com	Akamai International B.V.	DE	unknown
4	System	192.168.100.255:137	–	–	–	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
3196	iexplore.exe	142.250.181.227:80	ocsp.pki.goog	GOOGLE	US	whitelisted
1080	svchost.exe	224.0.0.252:5355	–	–	–	unknown
3196	iexplore.exe	188.114.96.9:443	–	CLOUDFLARENET	NL	unknown
3196	iexplore.exe	142.250.186.170:443	fonts.googleapis.com	GOOGLE	US	whitelisted
3196	iexplore.exe	172.255.6.54:443	nl.yieldedshotter.com	SERVERS-COM	NL	unknown
3196	iexplore.exe	13.107.246.67:443	www.clarity.ms	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
3196	iexplore.exe	172.217.16.195:443	fonts.gstatic.com	GOOGLE	US	whitelisted
3196	iexplore.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3440	iexplore.exe	131.253.33.200:443	www.bing.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3440	iexplore.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3196	iexplore.exe	23.212.210.158:80	x1.c.lencr.org	AKAMAI-AS	AU	unknown
3196	iexplore.exe	184.24.77.54:80	r3.o.lencr.org	Akamai International B.V.	DE	unknown
3196	iexplore.exe	68.219.88.97:443	c.clarity.ms	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
3440	iexplore.exe	188.114.96.9:443	–	CLOUDFLARENET	NL	unknown

Mitigation techniques of Malware attacks:

- Educate users on malware risks and safe online practices.
- Install and regularly update reputable antivirus software.
- Keep operating systems and software up-to-date for security patches.
- Utilize firewalls to monitor and control network traffic.
- Implement email filtering to detect and block malicious content.
- Secure web browsers and use extensions that enhance security.
- Enforce strong password policies and implement multi-factor authentication.
- Segment networks to limit the impact of potential malware infections.
- Perform regular backups of critical data and store them securely.
- Develop and regularly update an incident response plan for quick and effective action.