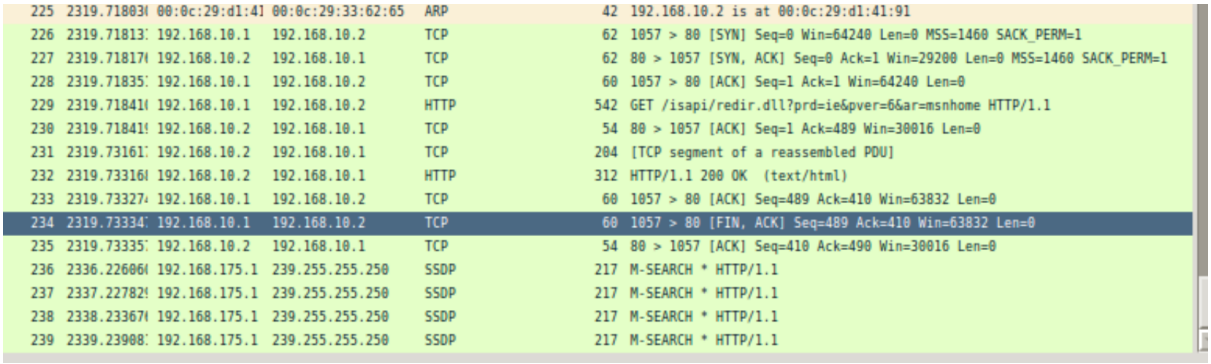
Part 1 (Apate)

Activity 1

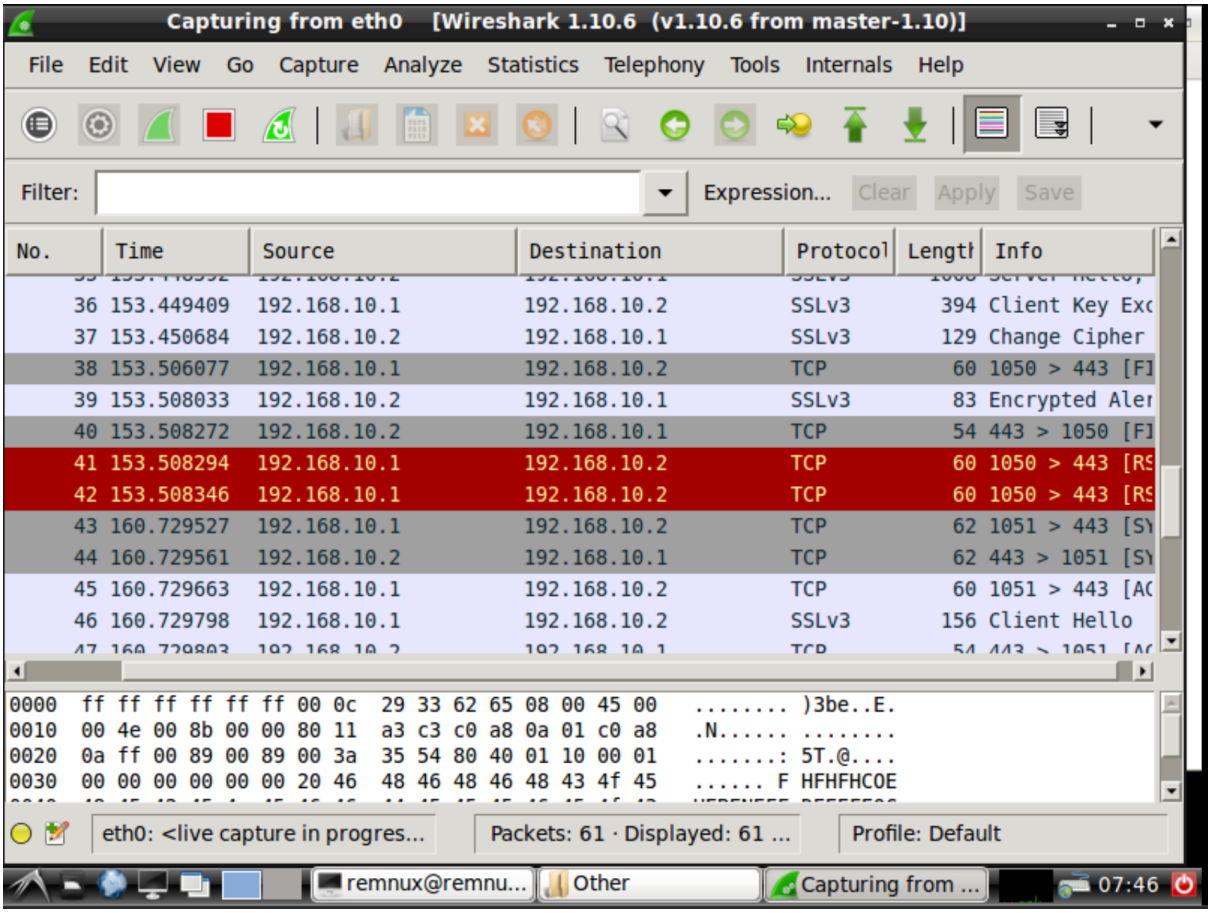
The request was shown on Wireshark; however, the default HTML page for INetSim showed up on Internet Explorer



225	2319.71803(	00:0c:29:d1:4]	00:0c:29:33:62:65	ARP	42	192.168.10.2 is at 00:0c:29:d1:41:91
226	2319.71813:	192.168.10.1	192.168.10.2	TCP	62	1057 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
227	2319.71817(	192.168.10.2	192.168.10.1	TCP	62	80 > 1057 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
228	2319.71835:	192.168.10.1	192.168.10.2	TCP	60	1057 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
229	2319.71841(	192.168.10.1	192.168.10.2	HTTP	542	GET /isapi/redir.dll?prd=ie&pver=6&ar=msnhome HTTP/1.1
230	2319.71841!	192.168.10.2	192.168.10.1	TCP	54	80 > 1057 [ACK] Seq=1 Ack=489 Win=30016 Len=0
231	2319.73161:	192.168.10.2	192.168.10.1	TCP	204	[TCP segment of a reassembled PDU]
232	2319.73316(	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)
233	2319.73327(	192.168.10.1	192.168.10.2	TCP	60	1057 > 80 [ACK] Seq=489 Ack=410 Win=63832 Len=0
234	2319.73334:	192.168.10.1	192.168.10.2	TCP	60	1057 > 80 [FIN, ACK] Seq=489 Ack=410 Win=63832 Len=0
235	2319.73335:	192.168.10.2	192.168.10.1	TCP	54	80 > 1057 [ACK] Seq=410 Ack=490 Win=30016 Len=0
236	2336.22606(	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
237	2337.22782!	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
238	2338.23367(	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
239	2339.23908:	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

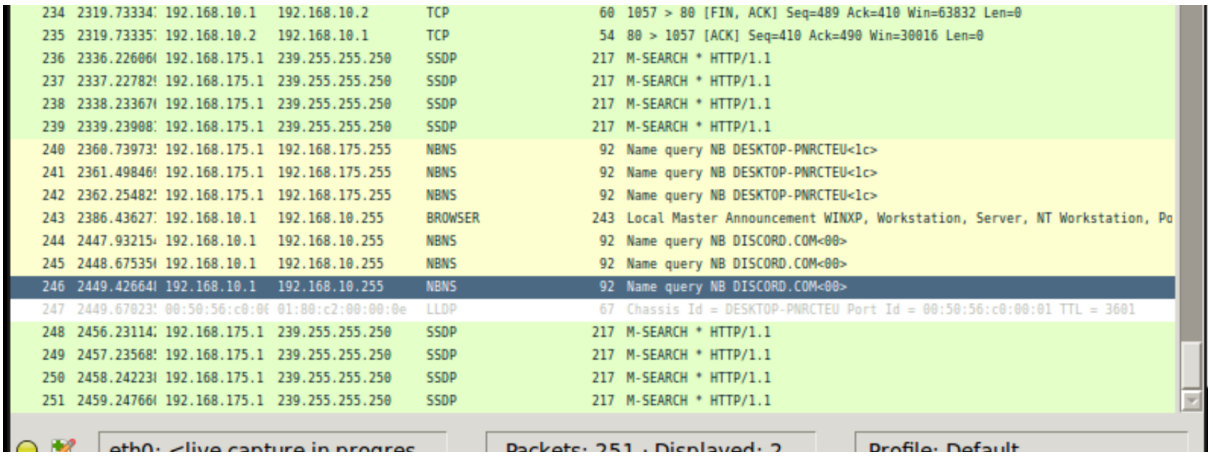
Activity 2

When I sent a request to the HTTPS server, after granting permission, the data packets begin to communicate. One notable difference is the presence of SSLV3 and SSL V2 within the packets, which is a result of the secure transmission provided by HTTPS.



Activity 3

The request showed up on Wireshark however nothing downloaded or happened on internet explorer.



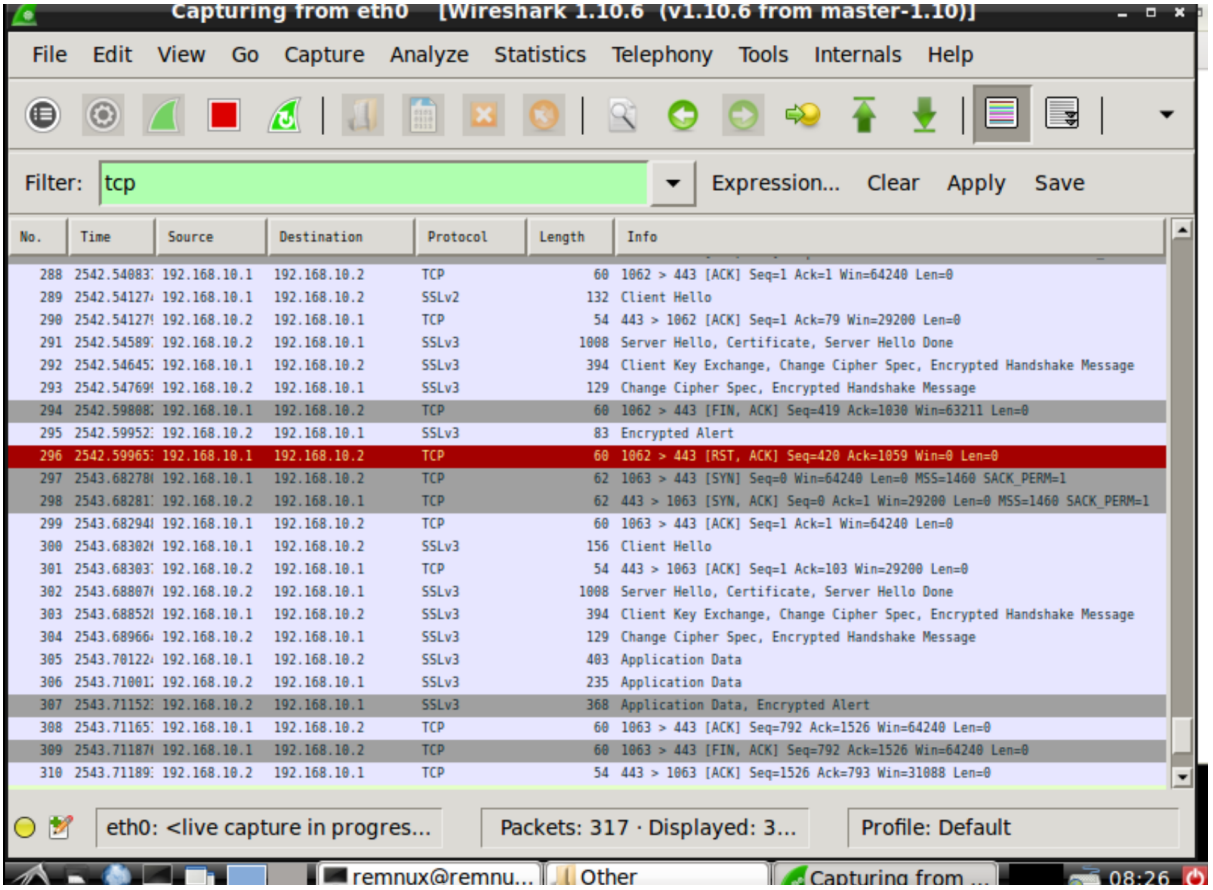
234	2319.73334	192.168.10.1	192.168.10.2	TCP	60	1057 > 80 [FIN, ACK] Seq=489 Ack=410 Win=63832 Len=0
235	2319.73335	192.168.10.2	192.168.10.1	TCP	54	80 > 1057 [ACK] Seq=410 Ack=490 Win=30016 Len=0
236	2336.22606	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
237	2337.22782	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
238	2338.23367	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
239	2339.23908	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
240	2360.73973	192.168.175.1	192.168.175.255	NBNS	92	Name query NB DESKTOP-PNRCTEU<1c>
241	2361.49846	192.168.175.1	192.168.175.255	NBNS	92	Name query NB DESKTOP-PNRCTEU<1c>
242	2362.25482	192.168.175.1	192.168.175.255	NBNS	92	Name query NB DESKTOP-PNRCTEU<1c>
243	2386.43627	192.168.10.1	192.168.10.255	BROWSER	243	Local Master Announcement WINXP, Workstation, Server, NT Workstation, Po
244	2447.93215	192.168.10.1	192.168.10.255	NBNS	92	Name query NB DISCORD.COM<00>
245	2448.67535	192.168.10.1	192.168.10.255	NBNS	92	Name query NB DISCORD.COM<00>
246	2449.42664	192.168.10.1	192.168.10.255	NBNS	92	Name query NB DISCORD.COM<00>
247	2449.67023	00:50:56:c0:0(	01:80:c2:00:00:0e	LLDP	67	Chassis Id = DESKTOP-PNRCTEU Port Id = 00:50:56:c0:00:01 TTL = 3601
248	2456.23114	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
249	2457.23568	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
250	2458.24223	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
251	2459.24766	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

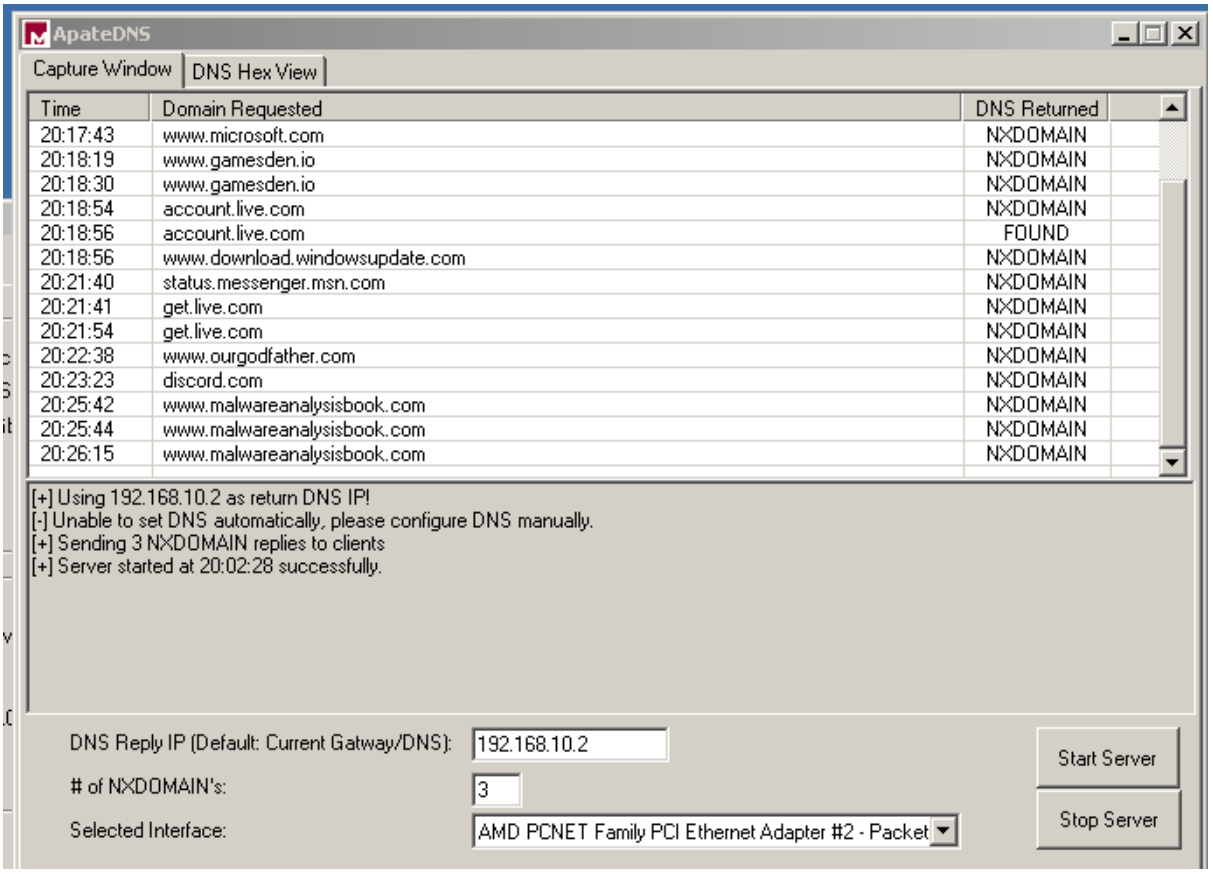
eth0: <live capture in progres... Packets: 251 · Displayed: 2 Profile: Default

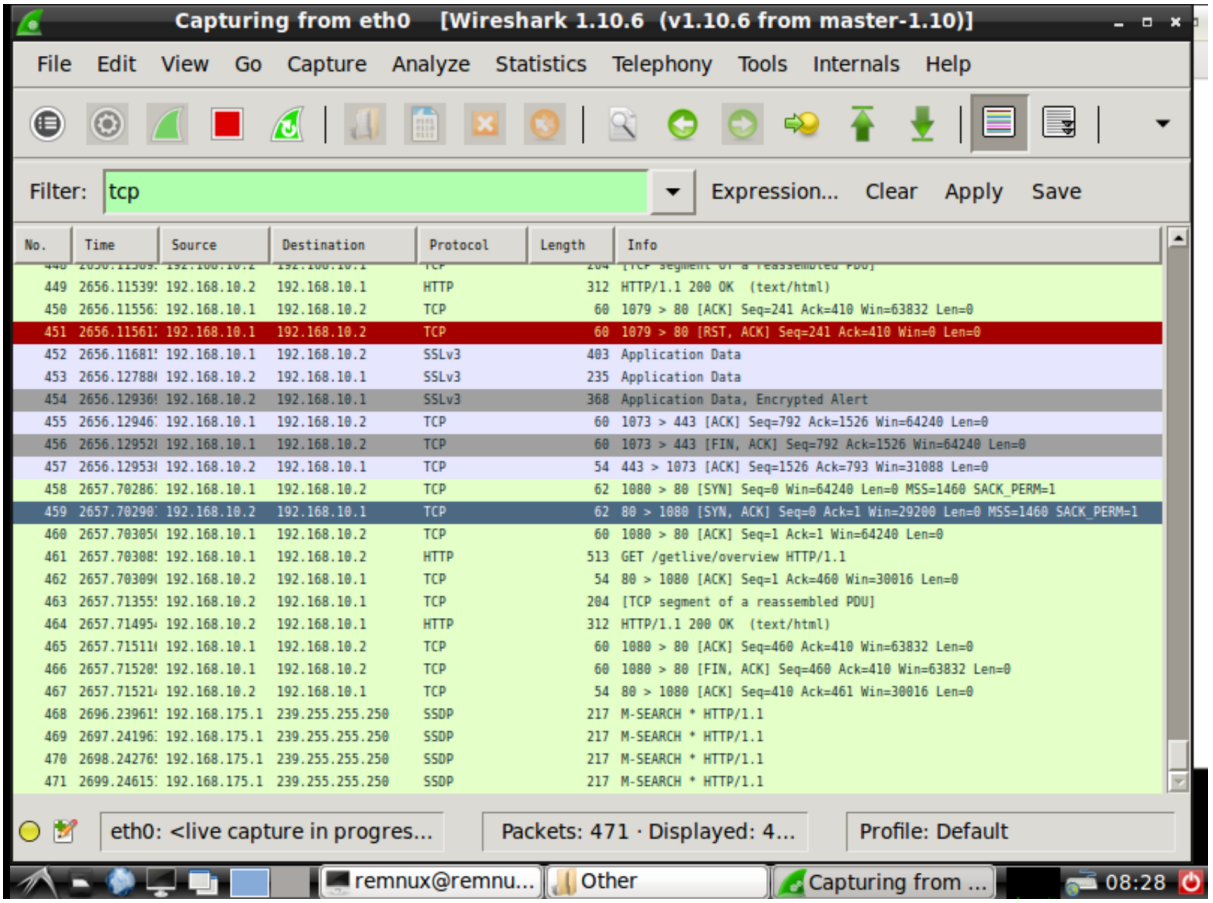
Activity 4

1. Messenger Malware

When pressing the first two links, it goes to get.live.com, and the third link redirects to status.messenger.msn.com. When closing the messenger exe, it redirects to ourgodfather.com




ApateDNS
Capture Window
DNS Hex View
Time
Domain Requested
DNS Returned
20:17:43 www.microsoft.com NXDOMAIN
20:18:19 www.gamesden.io NXDOMAIN
20:18:30 www.gamesden.io NXDOMAIN
20:18:54 account.live.com NXDOMAIN
20:18:56 account.live.com FOUND
20:18:56 www.download.windowsupdate.com NXDOMAIN
20:21:40 status.messenger.msn.com NXDOMAIN
20:21:41 get.live.com NXDOMAIN
20:21:54 get.live.com NXDOMAIN
20:22:38 www.ourgodfather.com NXDOMAIN
20:23:23 discord.com NXDOMAIN
20:25:42 www.malwareanalysisbook.com NXDOMAIN
20:25:44 www.malwareanalysisbook.com NXDOMAIN
20:26:15 www.malwareanalysisbook.com NXDOMAIN
[+] Using 192.168.10.2 as return DNS IP!
[-] Unable to set DNS automatically, please configure DNS manually.
[+] Sending 3 NXDOMAIN replies to clients
[+] Server started at 20:02:28 successfully.
DNS Reply IP (Default: Current Gatway/DNS):
192.168.10.2
# of NXDOMAIN's:
3
Selected Interface:
AMD PCNET Family PCI Ethernet Adapter #2 - Packet
Start Server
Stop Server

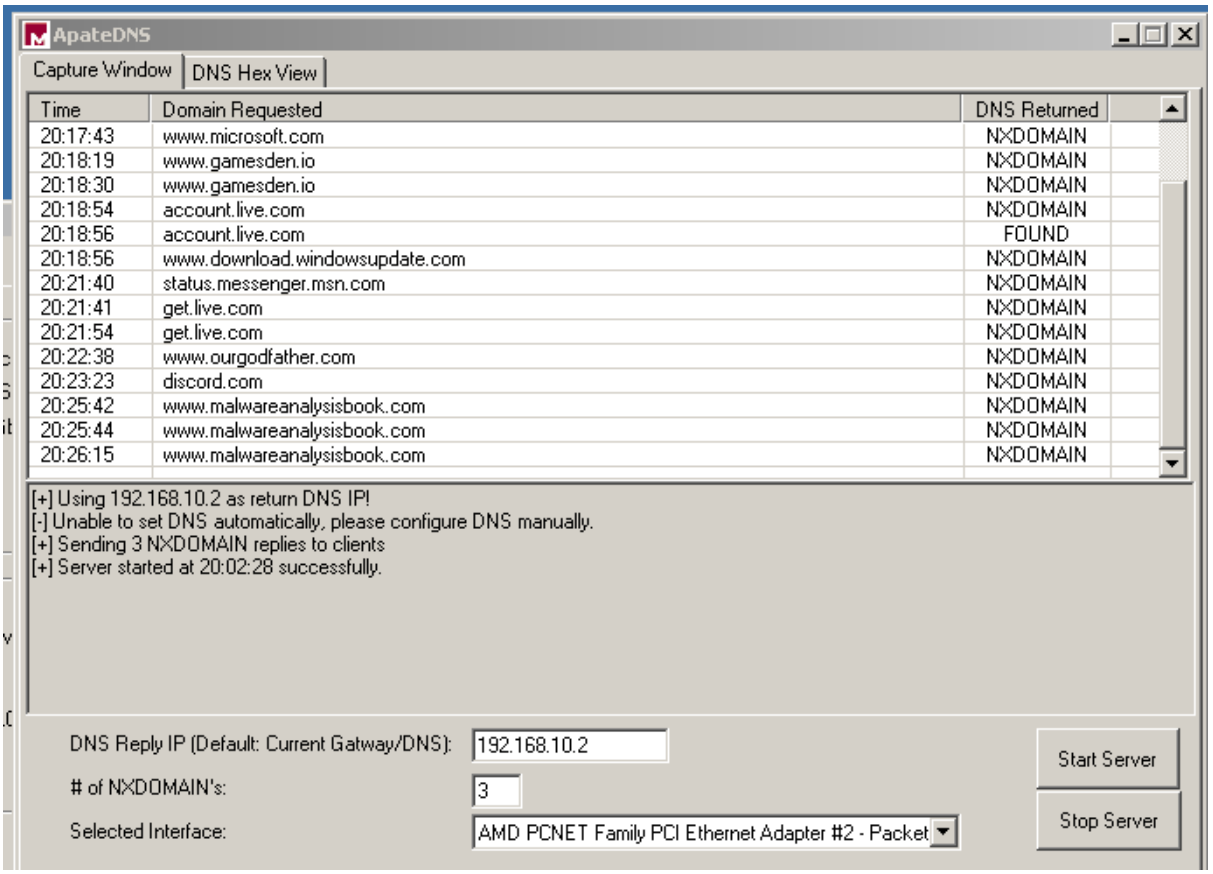

Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
449 2656.11539 192.168.10.2 192.168.10.1 HTTP 312 HTTP/1.1 200 OK (text/html)
450 2656.11556 192.168.10.1 192.168.10.2 TCP 60 1079 > 80 [ACK] Seq=241 Ack=410 Win=63832 Len=0
451 2656.11561 192.168.10.1 192.168.10.2 TCP 60 1079 > 80 [RST, ACK] Seq=241 Ack=410 Win=0 Len=0
452 2656.11681 192.168.10.1 192.168.10.2 SSLv3 403 Application Data
453 2656.12788 192.168.10.2 192.168.10.1 SSLv3 235 Application Data
454 2656.12936 192.168.10.2 192.168.10.1 SSLv3 368 Application Data, Encrypted Alert
455 2656.12946 192.168.10.1 192.168.10.2 TCP 60 1073 > 443 [ACK] Seq=792 Ack=1526 Win=64240 Len=0
456 2656.12952 192.168.10.1 192.168.10.2 TCP 60 1073 > 443 [FIN, ACK] Seq=792 Ack=1526 Win=64240 Len=0
457 2656.12953 192.168.10.2 192.168.10.1 TCP 54 443 > 1073 [ACK] Seq=1526 Ack=793 Win=31088 Len=0
458 2657.70286 192.168.10.1 192.168.10.2 TCP 62 1080 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
459 2657.70290 192.168.10.2 192.168.10.1 TCP 62 80 > 1080 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
460 2657.70305 192.168.10.1 192.168.10.2 TCP 60 1080 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
461 2657.70308 192.168.10.1 192.168.10.2 HTTP 513 GET /getlive/overview HTTP/1.1
462 2657.70309 192.168.10.2 192.168.10.1 TCP 54 80 > 1080 [ACK] Seq=1 Ack=460 Win=30016 Len=0
463 2657.71355 192.168.10.2 192.168.10.1 TCP 204 [TCP segment of a reassembled PDU]
464 2657.71495 192.168.10.2 192.168.10.1 HTTP 312 HTTP/1.1 200 OK (text/html)
465 2657.71511 192.168.10.1 192.168.10.2 TCP 60 1080 > 80 [ACK] Seq=460 Ack=410 Win=63832 Len=0
466 2657.71520 192.168.10.1 192.168.10.2 TCP 60 1080 > 80 [FIN, ACK] Seq=460 Ack=410 Win=63832 Len=0
467 2657.71521 192.168.10.2 192.168.10.1 TCP 54 80 > 1080 [ACK] Seq=410 Ack=461 Win=30016 Len=0
468 2696.23961 192.168.175.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
469 2697.24196 192.168.175.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
470 2698.24276 192.168.175.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
471 2699.24615 192.168.175.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
eth0: <live capture in progres...
Packets: 471 · Displayed: 4...
Profile: Default
remnux@remnu...
Other
Capturing from ...
08:28

2. Malware analysis book

This tries to access malwareanalysisbook.com/ad.html domain. An HTTP request was initiated for the purpose of analyzing malware, specifically in the form of a GET request. The initial HTTP request received a successful response with a status code of 200, indicating it was successful.

Firstly, ARP protocols were employed to establish a connection between the source and destination. Next, the TCP three-way handshake was executed, paving the way for the HTTP GET request to be sent to the malware analysis page. The server responded with a TCP response, which the client duly received. Subsequently, an additional HTTP message was transmitted from the server to the client, bearing a status code of OK (200). Finally, the FIN process was executed to conclude the communication.

```
485  2763.29081( 192.168.10.1   192.168.10.2   TCP      62  1085 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
486  2763.29085( 192.168.10.2   192.168.10.1   TCP      62  80 > 1085 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
487  2763.29097( 192.168.10.1   192.168.10.2   TCP      60  1085 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
488  2763.29102: 192.168.10.1   192.168.10.2   HTTP    360  GET /ad.html HTTP/1.1
489  2763.29102: 192.168.10.2   192.168.10.1   TCP      54  80 > 1085 [ACK] Seq=1 Ack=307 Win=30016 Len=0
490  2763.30093( 192.168.10.2   192.168.10.1   TCP     204  [TCP segment of a reassembled PDU]
491  2763.30238( 192.168.10.2   192.168.10.1   HTTP    312  HTTP/1.1 200 OK  (text/html)
492  2763.30254: 192.168.10.1   192.168.10.2   TCP      60  1085 > 80 [ACK] Seq=307 Ack=410 Win=63832 Len=0
493  2763.30259( 192.168.10.1   192.168.10.2   TCP      60  1085 > 80 [FIN, ACK] Seq=307 Ack=410 Win=63832 Len=0
494  2763.30260( 192.168.10.2   192.168.10.1   TCP      54  80 > 1085 [ACK] Seq=410 Ack=308 Win=30016 Len=0
```



3. Windows Update Microsoft

Malware 2 initiates its actions by sending an initial GET request to the "windowsupdate.microsoft.com" URL, but it subsequently attempts to redirect to the "practicalmalwareanalysis.com/updater.exel" domain.
The sequence of events can be summarized as follows:

The first HTTP request is a GET request for "windowsupdate.com."
The second HTTP request is made to "practicalmalwareanalysis.com/updater.exel" in order to retrieve the malware updater executable file.
The next HTTP request originates from the server to the client, signaling an OK status code.
The final HTTP request is a connection close request with a status code of 200, indicating the end of the communication.

498	2802.47655	192.168.10.1	192.168.10.2	TCP	62	1088 > 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
499	2802.47658	192.168.10.2	192.168.10.1	TCP	62	80 > 1088 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
500	2802.47678	192.168.10.1	192.168.10.2	TCP	60	1088 > 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
501	2802.47682	192.168.10.1	192.168.10.2	HTTP	512	GET / HTTP/1.1
502	2802.47683	192.168.10.2	192.168.10.1	TCP	54	80 > 1088 [ACK] Seq=1 Ack=459 Win=30016 Len=0
503	2802.48715	192.168.10.2	192.168.10.1	TCP	204	[TCP segment of a reassembled PDU]
504	2802.48855	192.168.10.2	192.168.10.1	HTTP	312	HTTP/1.1 200 OK (text/html)
505	2802.48872	192.168.10.1	192.168.10.2	TCP	60	1088 > 80 [ACK] Seq=459 Ack=410 Win=63832 Len=0
506	2802.48880	192.168.10.1	192.168.10.2	TCP	60	1088 > 80 [FIN, ACK] Seq=459 Ack=410 Win=63832 Len=0
507	2802.48881	192.168.10.2	192.168.10.1	TCP	54	80 > 1088 [ACK] Seq=410 Ack=460 Win=30016 Len=0
508	2816.24686	192.168.175.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1