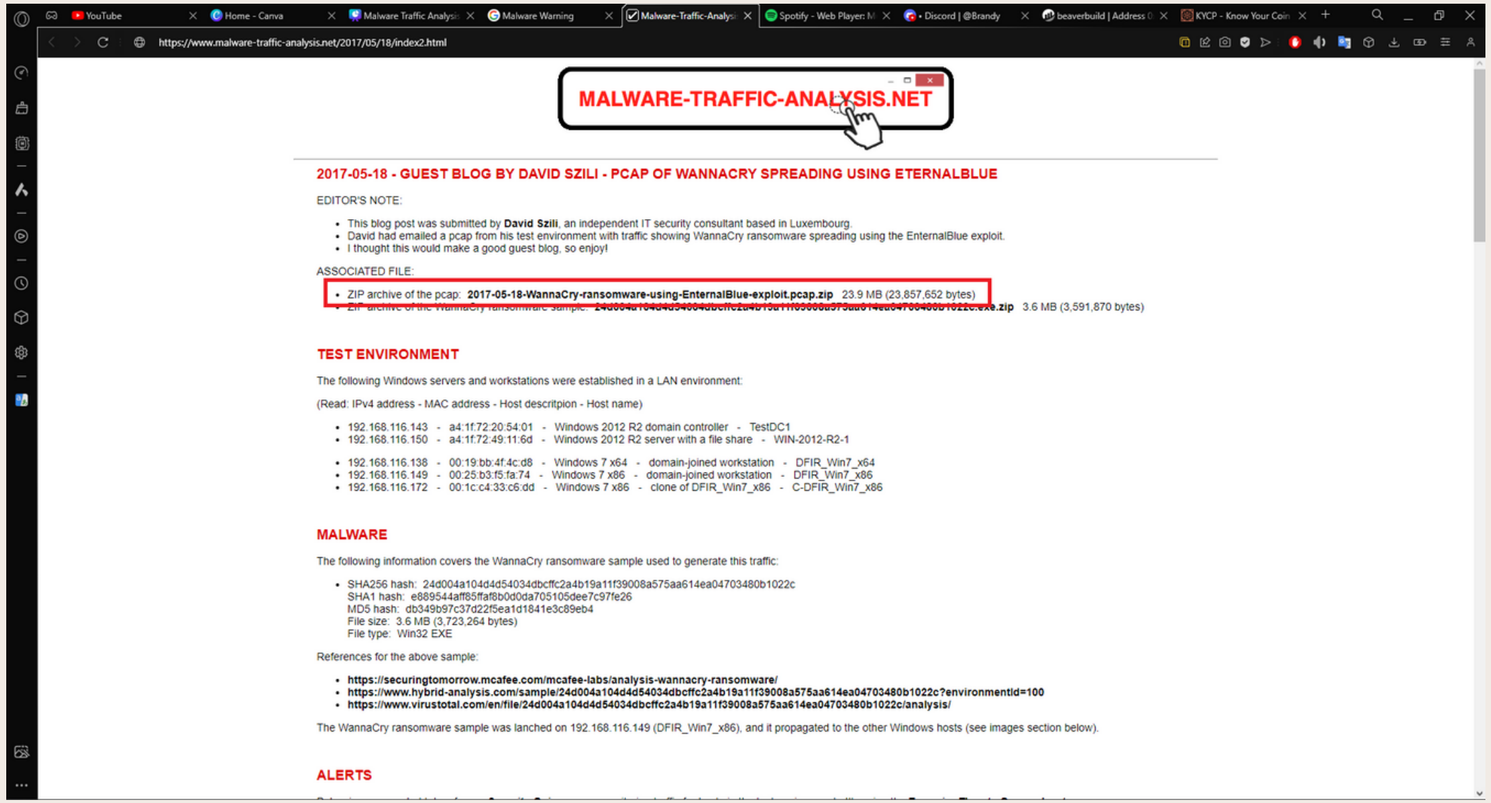
MALWARE TRAFFIC ANALYSIS

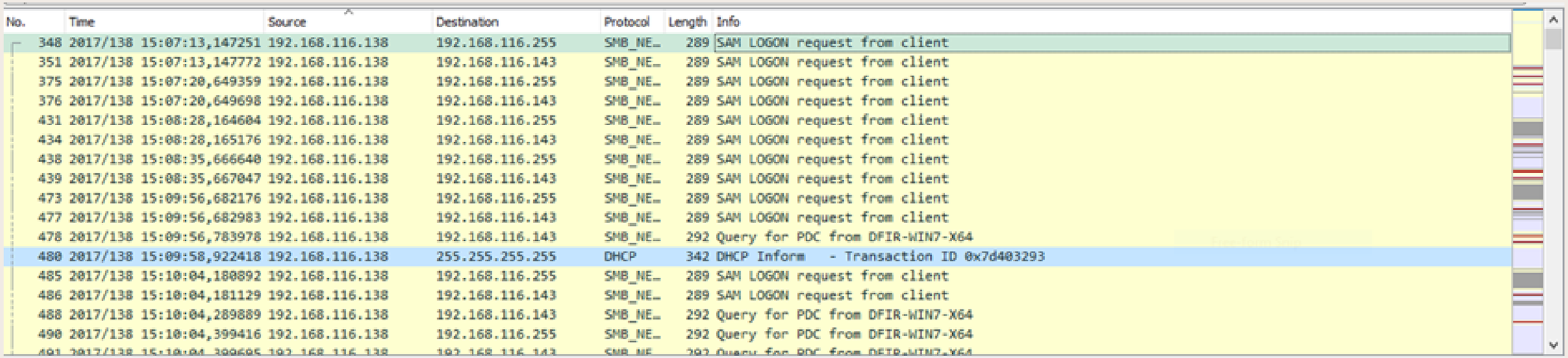
WANNACRY SPREADING

2540125384 – BENEDICTO MARVELOUS ALIDAJAYA
2540118933 – JOHN ORLOND
2540124702 – MATTHEW KURNIAWAN

PCAP FILE

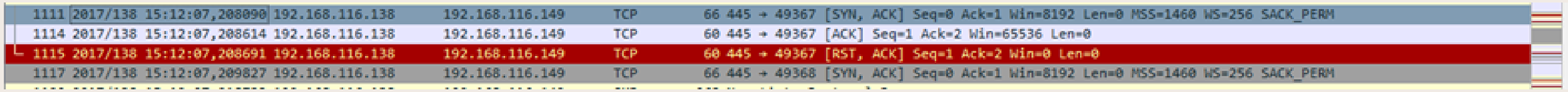
Analysis malware menggunakan file pcap yang didapat dari website malware-traffic-analysis.net dengan link pcap sebagai berikut : https://www.malware-traffic-analysis.net/2017/05/18/2017-05-18-WannaCry-ransomware-using-EnternalBlue-exploit.pcap.zip



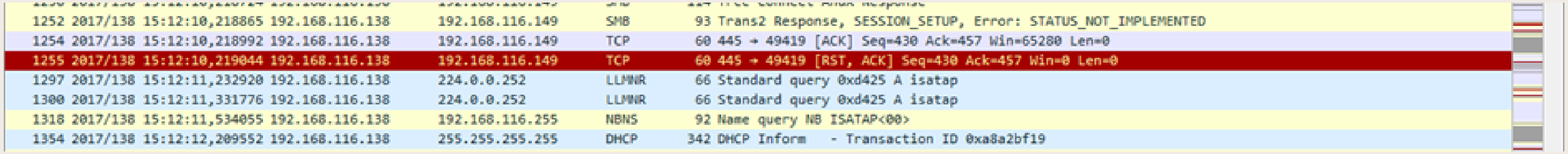


No.	Time	Source	Destination	Protocol	Length	Info
348	2017/138 15:07:13,147251	192.168.116.138	192.168.116.255	SMB_NE…	289	SAM LOGON request from client
351	2017/138 15:07:13,147772	192.168.116.138	192.168.116.143	SMB_NE…	289	SAM LOGON request from client
375	2017/138 15:07:20,649359	192.168.116.138	192.168.116.255	SMB_NE…	289	SAM LOGON request from client
376	2017/138 15:07:20,649698	192.168.116.138	192.168.116.143	SMB_NE…	289	SAM LOGON request from client
431	2017/138 15:08:28,164604	192.168.116.138	192.168.116.255	SMB_NE…	289	SAM LOGON request from client
434	2017/138 15:08:28,165176	192.168.116.138	192.168.116.143	SMB_NE…	289	SAM LOGON request from client
438	2017/138 15:08:35,666640	192.168.116.138	192.168.116.255	SMB_NE…	289	SAM LOGON request from client
439	2017/138 15:08:35,667047	192.168.116.138	192.168.116.143	SMB_NE…	289	SAM LOGON request from client
473	2017/138 15:09:56,682176	192.168.116.138	192.168.116.255	SMB_NE…	289	SAM LOGON request from client
477	2017/138 15:09:56,682983	192.168.116.138	192.168.116.143	SMB_NE…	289	SAM LOGON request from client
478	2017/138 15:09:56,783978	192.168.116.138	192.168.116.143	SMB_NE…	292	Query for PDC from DFIR-WIN7-X64
480	2017/138 15:09:58,922418	192.168.116.138	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x7d403293
485	2017/138 15:10:04,180892	192.168.116.138	192.168.116.255	SMB_NE…	289	SAM LOGON request from client
486	2017/138 15:10:04,181129	192.168.116.138	192.168.116.143	SMB_NE…	289	SAM LOGON request from client
488	2017/138 15:10:04,289889	192.168.116.138	192.168.116.143	SMB_NE…	292	Query for PDC from DFIR-WIN7-X64
490	2017/138 15:10:04,399416	192.168.116.138	192.168.116.255	SMB_NE…	292	Query for PDC from DFIR-WIN7-X64
491	2017/138 15:10:04,399695	192.168.116.138	192.168.116.143	SMB_NE…	292	Query for PDC from DFIR-WIN7-X64

Berikut adalah tampilan pcap saat dibuka dengan Wireshark dengan setting time diubah menjadi yyyy/mm/dd hh//mm/ss.

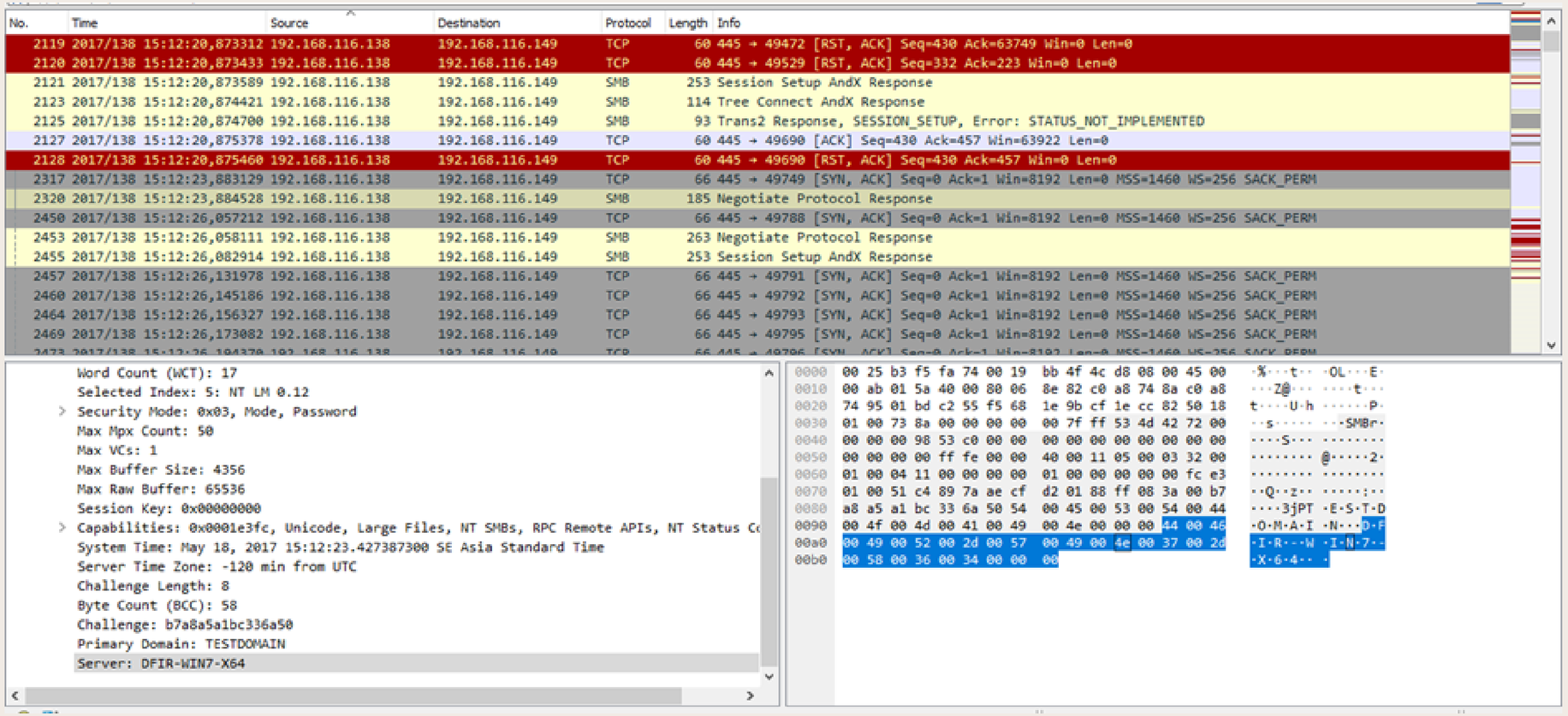


Pada jam 15.12.07, IP 192.168.116.138 mencoba melakukan koneksi pada 192.168.116.149 dengan mengirim SYN, ACK. Lalu dibalas dengan mengirimkan ACK, Tetapi IP 192.168.116.138 mengirimkann request RST,ACK.

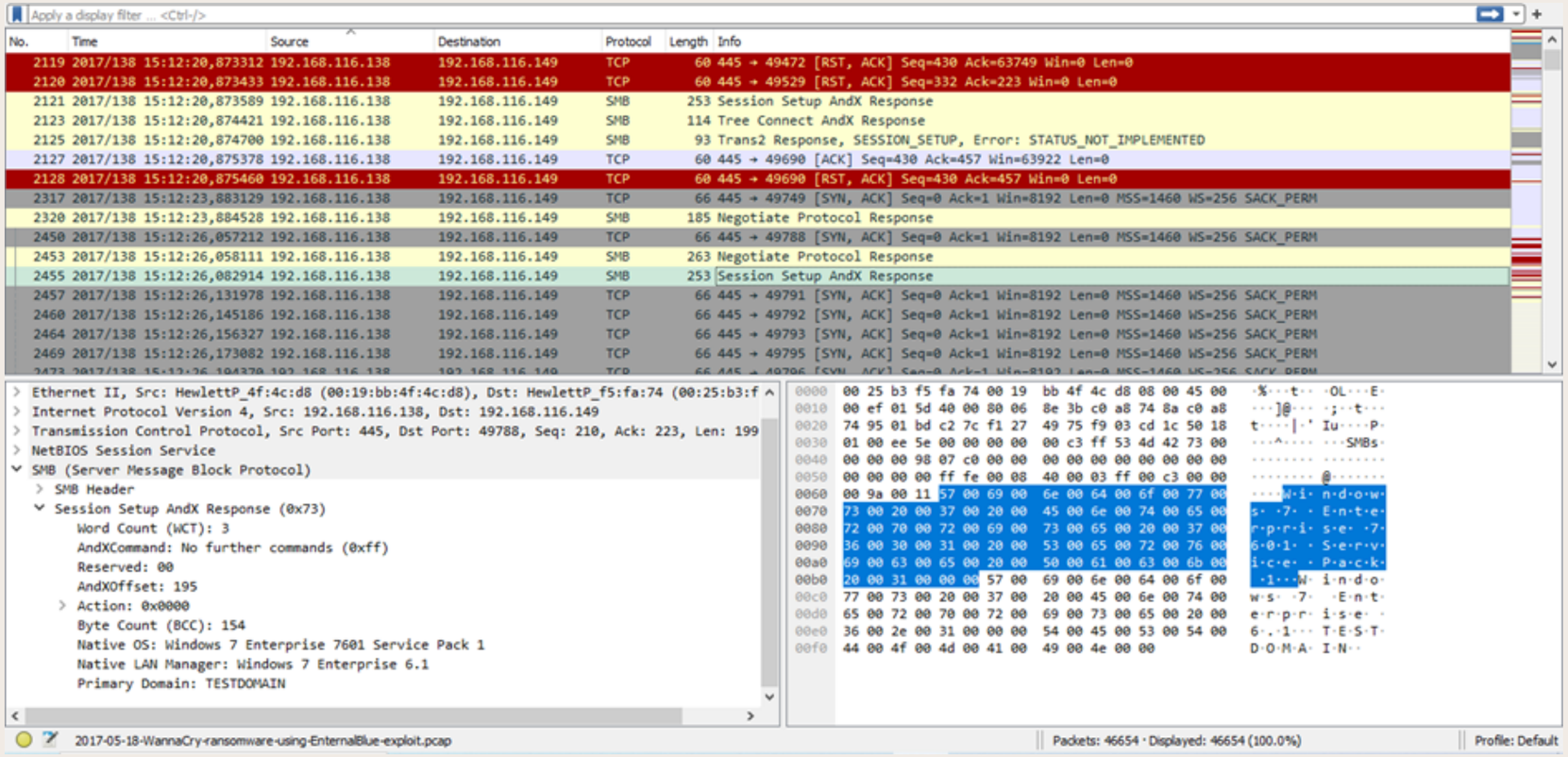


1252	2017/138 15:12:10,218865	192.168.116.138	192.168.116.149	SMB	93 Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
1254	2017/138 15:12:10,218992	192.168.116.138	192.168.116.149	TCP	60 445 → 49419 [ACK] Seq=430 Ack=457 Win=65280 Len=0
1255	2017/138 15:12:10,219044	192.168.116.138	192.168.116.149	TCP	60 445 → 49419 [RST, ACK] Seq=430 Ack=457 Win=0 Len=0
1297	2017/138 15:12:11,232920	192.168.116.138	224.0.0.252	LLMNR	66 Standard query 0xd425 A isatap
1300	2017/138 15:12:11,331776	192.168.116.138	224.0.0.252	LLMNR	66 Standard query 0xd425 A isatap
1318	2017/138 15:12:11,534055	192.168.116.138	192.168.116.255	NBNS	92 Name query NB ISATAP<00>
1354	2017/138 15:12:12,209552	192.168.116.138	255.255.255.255	DHCP	342 DHCP Inform - Transaction ID 0xa8a2bf19

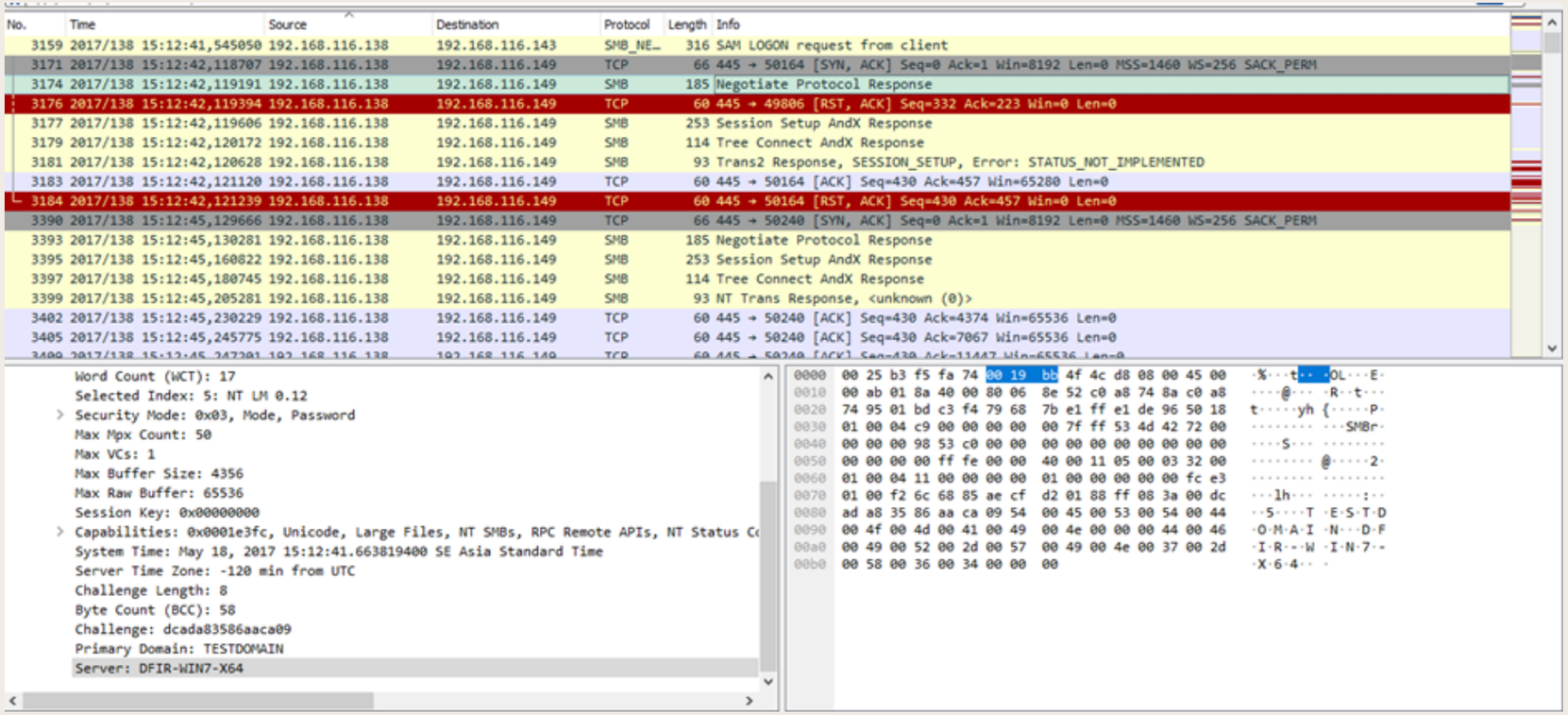
Hal tersebut kembali berulang pada jam 15.12.10 dengan source IP dan Destination IP yang sama.



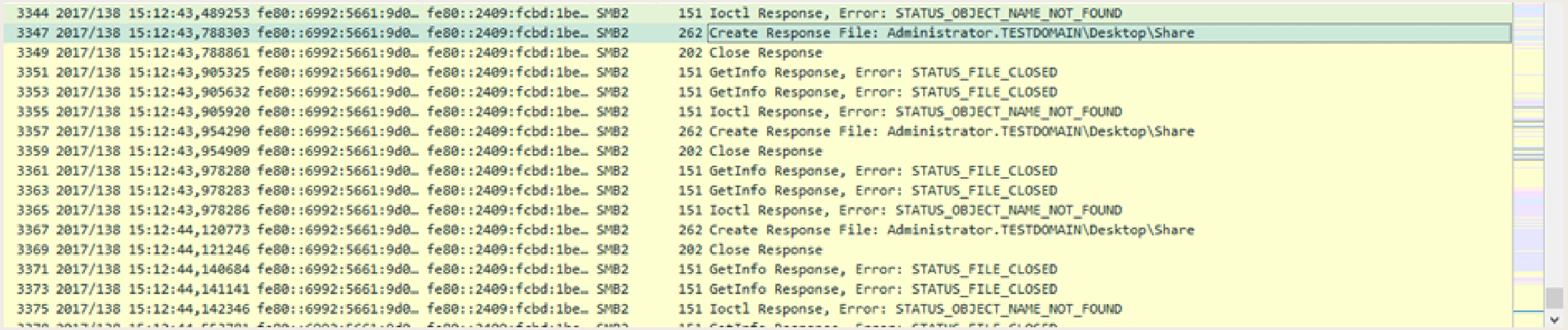
Pada pukul 15.12.23, koneksi berhasil disambungkan lalu IP 192.168.116.128 mengirimkan negotiate protocol response dengan mengirimkan SMB dengan nama Windows 7 Enterprise yang dikoneksikan ke Test Domain



Pada waktu yang sama, session juga berhasil terbuat dan siap untuk menerima respond dari IP korban

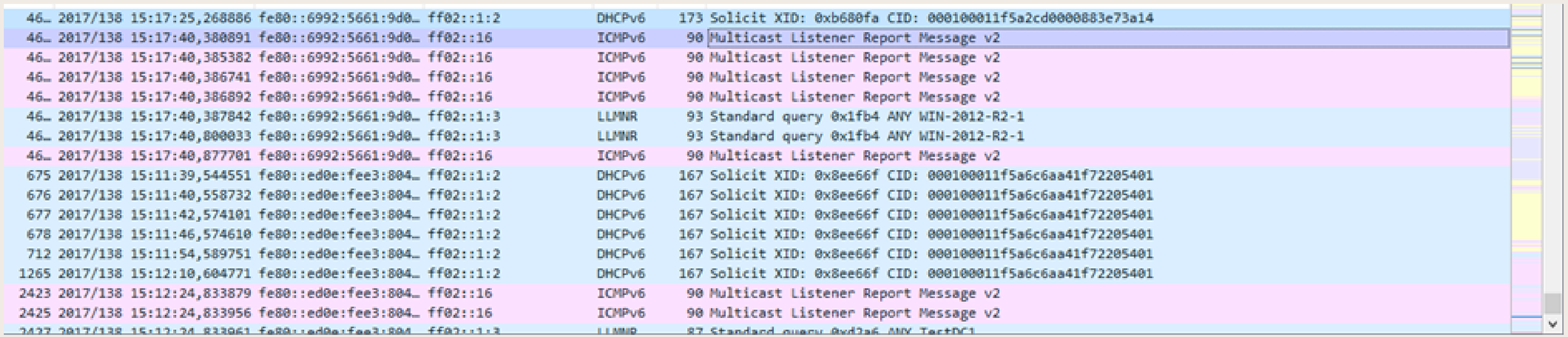


Lalu pada 15.12.43, IP 192.168.116.138 mengirimkan file Windows 7 Enterprise X64 dengan protocol SMB.



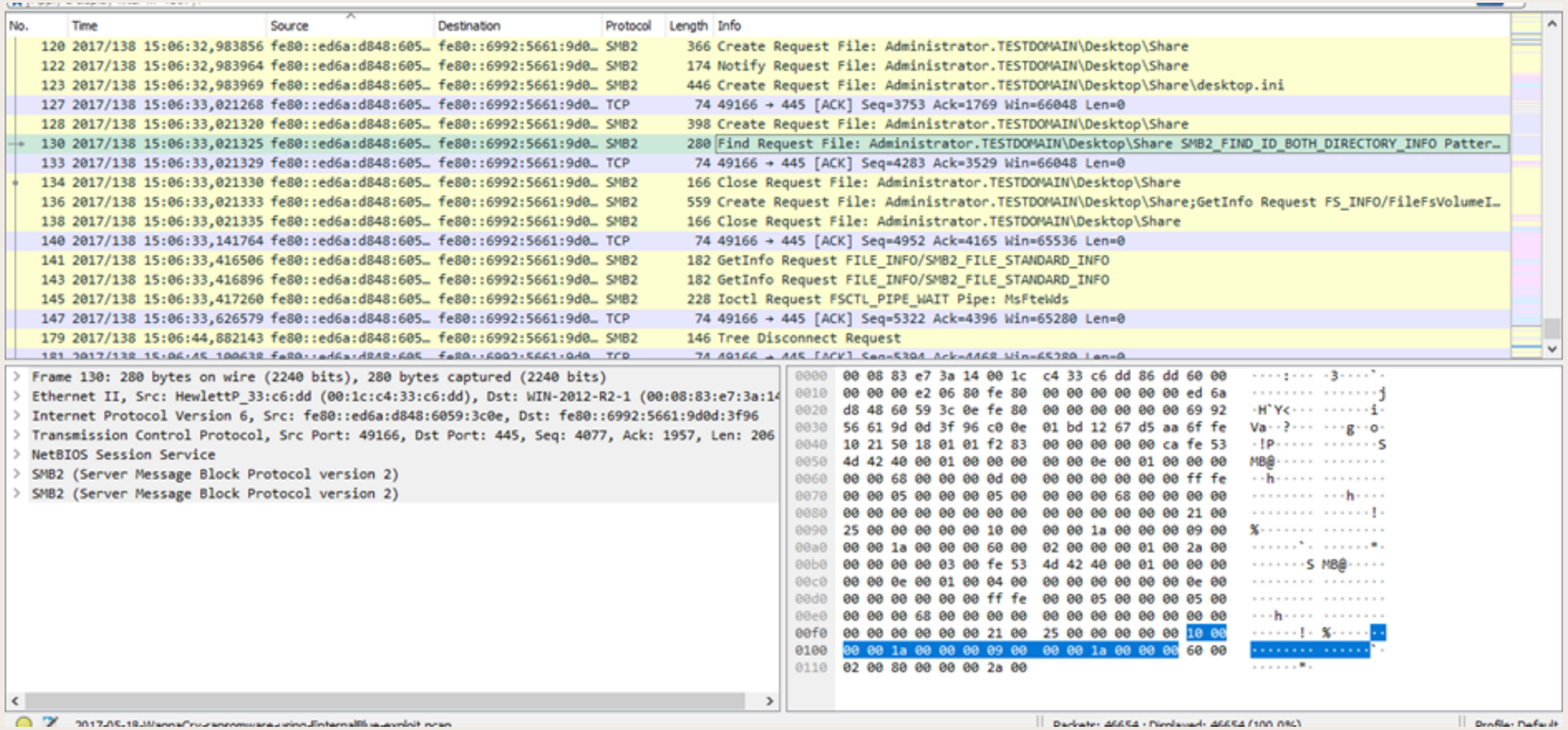
```
3344 2017/138 15:12:43,489253 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3347 2017/138 15:12:43,788303 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   262 Create Response File: Administrator.TESTDOMAIN\Desktop\Share
3349 2017/138 15:12:43,788861 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   202 Close Response
3351 2017/138 15:12:43,905325 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 GetInfo Response, Error: STATUS_FILE_CLOSED
3353 2017/138 15:12:43,905632 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 GetInfo Response, Error: STATUS_FILE_CLOSED
3355 2017/138 15:12:43,905920 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3357 2017/138 15:12:43,954290 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   262 Create Response File: Administrator.TESTDOMAIN\Desktop\Share
3359 2017/138 15:12:43,954909 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   202 Close Response
3361 2017/138 15:12:43,978280 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 GetInfo Response, Error: STATUS_FILE_CLOSED
3363 2017/138 15:12:43,978283 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 GetInfo Response, Error: STATUS_FILE_CLOSED
3365 2017/138 15:12:43,978286 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
3367 2017/138 15:12:44,120773 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   262 Create Response File: Administrator.TESTDOMAIN\Desktop\Share
3369 2017/138 15:12:44,121246 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   202 Close Response
3371 2017/138 15:12:44,140684 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 GetInfo Response, Error: STATUS_FILE_CLOSED
3373 2017/138 15:12:44,141141 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 GetInfo Response, Error: STATUS_FILE_CLOSED
3375 2017/138 15:12:44,142346 fe80::6992:5661:9d0… fe80::2409:fcbd:1be… SMB2   151 Ioctl Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
```

Kemudian, IP 192.168.116.138 melakukan bruteforce IP pada local LAN (informasi didapat dari malware-traffic-analysis.net) hingga 15.12.42, Lalu pada 15.12.43 IP 192.168.116.138 melakukan create response file untuk Administrator.TESTDOMAIN\Desktop\Share

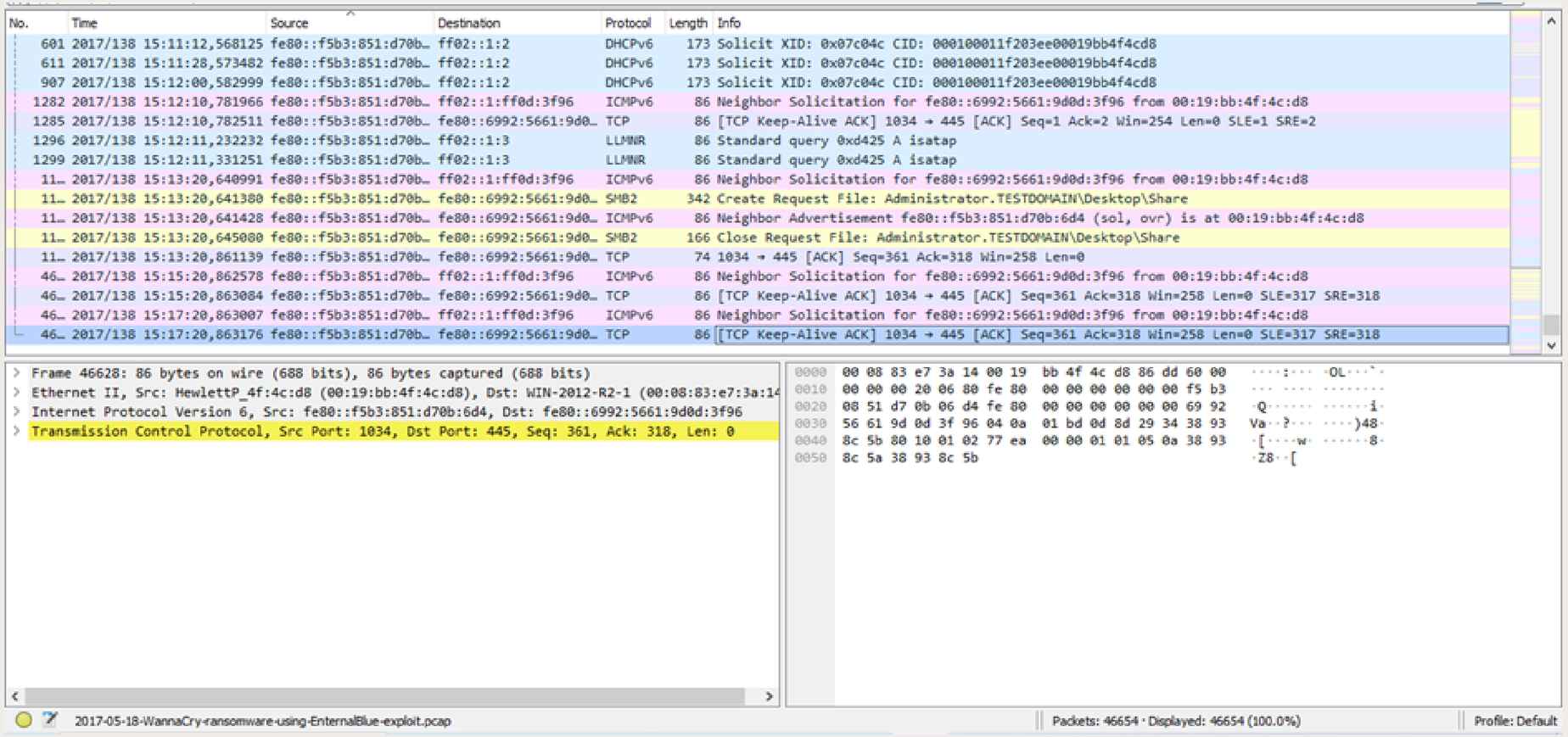


46…	2017/138	15:17:25,268886	fe80::6992:5661:9d0…	ff02::1:2	DHCPv6	173 Solicit XID: 0xb680fa CID: 000100011f5a2cd0000883e73a14
46…	2017/138	15:17:40,380891	fe80::6992:5661:9d0…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46…	2017/138	15:17:40,385382	fe80::6992:5661:9d0…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46…	2017/138	15:17:40,386741	fe80::6992:5661:9d0…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46…	2017/138	15:17:40,386892	fe80::6992:5661:9d0…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
46…	2017/138	15:17:40,387842	fe80::6992:5661:9d0…	ff02::1:3	LLMNR	93 Standard query 0x1fb4 ANY WIN-2012-R2-1
46…	2017/138	15:17:40,800033	fe80::6992:5661:9d0…	ff02::1:3	LLMNR	93 Standard query 0x1fb4 ANY WIN-2012-R2-1
46…	2017/138	15:17:40,877701	fe80::6992:5661:9d0…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
675	2017/138	15:11:39,544551	fe80::ed0e:fee3:804…	ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
676	2017/138	15:11:40,558732	fe80::ed0e:fee3:804…	ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
677	2017/138	15:11:42,574101	fe80::ed0e:fee3:804…	ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
678	2017/138	15:11:46,574610	fe80::ed0e:fee3:804…	ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
712	2017/138	15:11:54,589751	fe80::ed0e:fee3:804…	ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
1265	2017/138	15:12:10,604771	fe80::ed0e:fee3:804…	ff02::1:2	DHCPv6	167 Solicit XID: 0x8ee66f CID: 000100011f5a6c6aa41f72205401
2423	2017/138	15:12:24,833879	fe80::ed0e:fee3:804…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
2425	2017/138	15:12:24,833956	fe80::ed0e:fee3:804…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
2427	2017/138	15:12:24,833961	fe80::ed0e:fee3:804…	ff02::1:3	LLMNR	87 Standard query 0xd2a6 ANY TestDC1

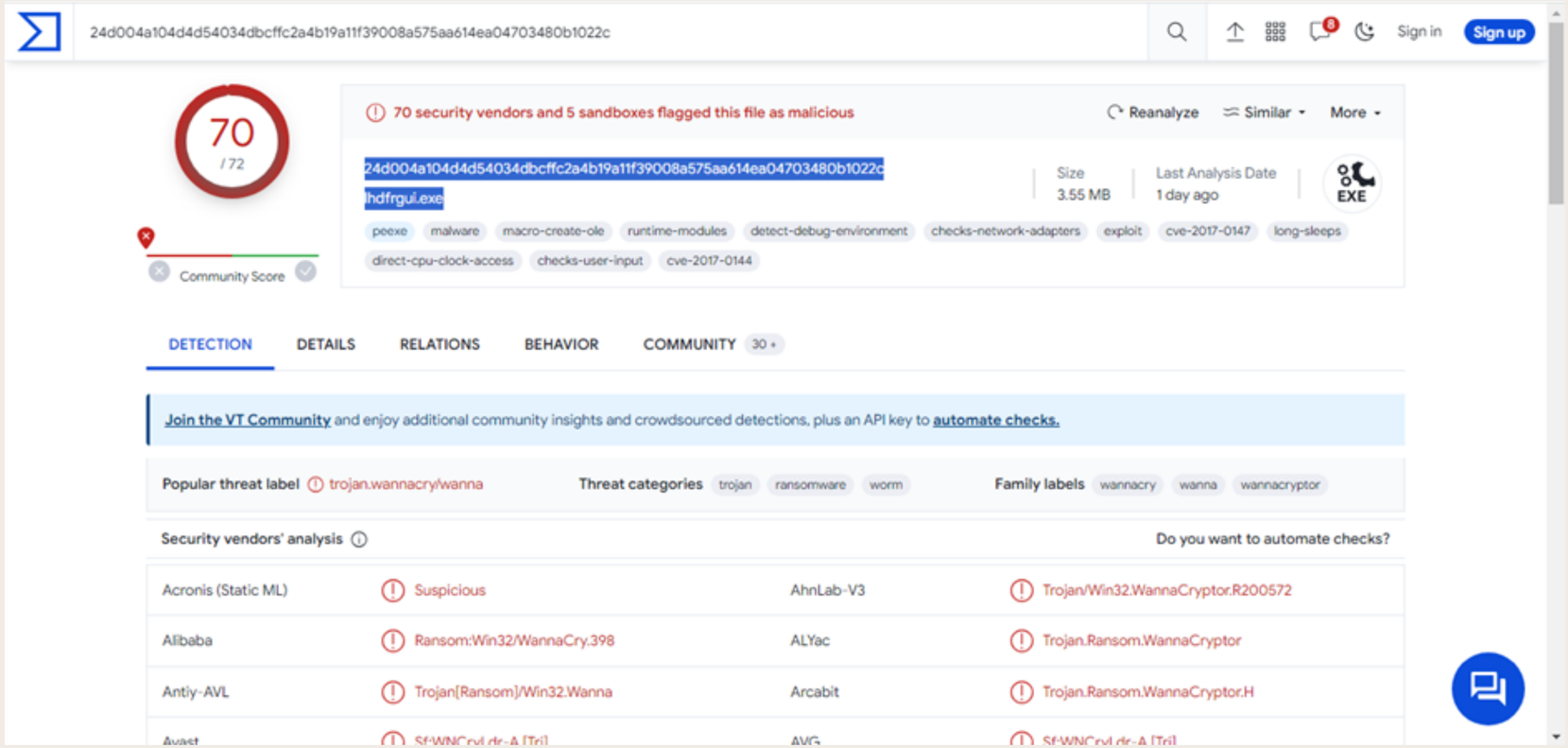
Pada 15.17.40, file tersebut mulai digunakan sebagai listener hingga hari setelahnya.



Pada hari setelahnya pada pukul 15.06.32. file tersebut kembali diakses.



Kemudian pada pukul 15.17.20 melakukan stay alive pada malware agar tetap meninfeksi system sampai dibayar oleh korban.



File windows 7 enterprise juga memiliki isi berupa file exe yang bernama 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022clhdfrgui.exe yang ketika diupload ke virustotal merupakan virus dengan angka 70/72.

THANK YOU VERY MUCH!