CYBERSECURITY

Lab Assignment-09

Ritik Tiwari

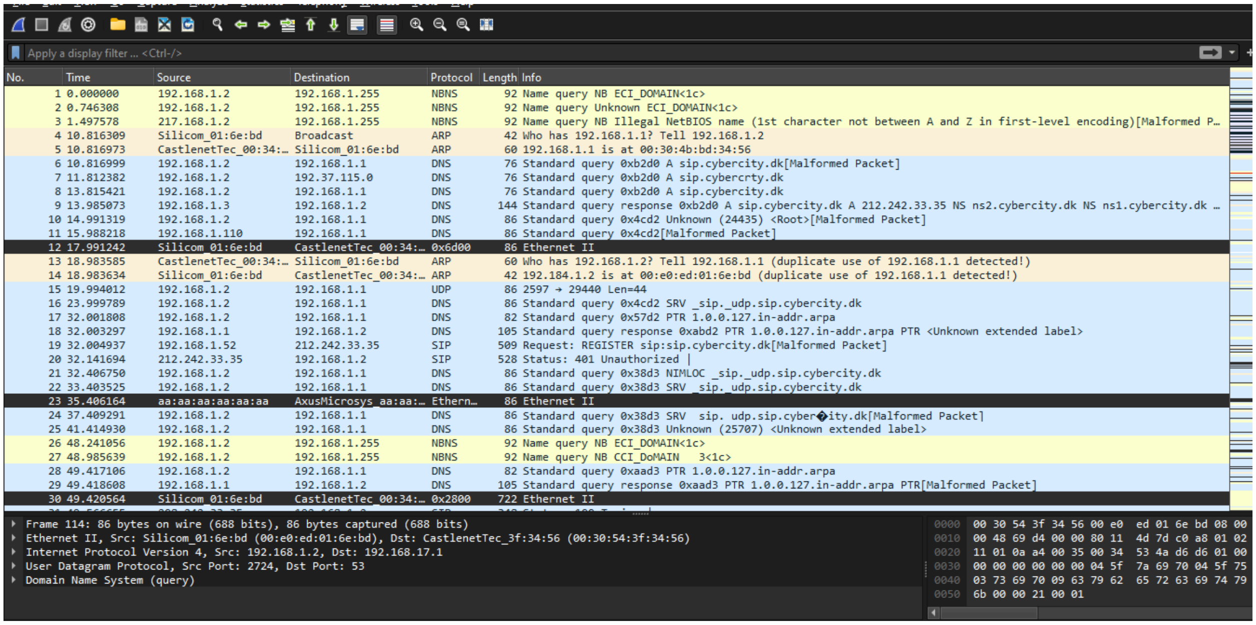
B21CS098

Questions:

Objective: Conduct a forensic analysis of network traffic captured during a Distributed Denial of Service (DDoS) attack to identify the characteristics of the attack and the attackers.

Tasks to perform:

1. Open the provided pcap file in Wireshark.



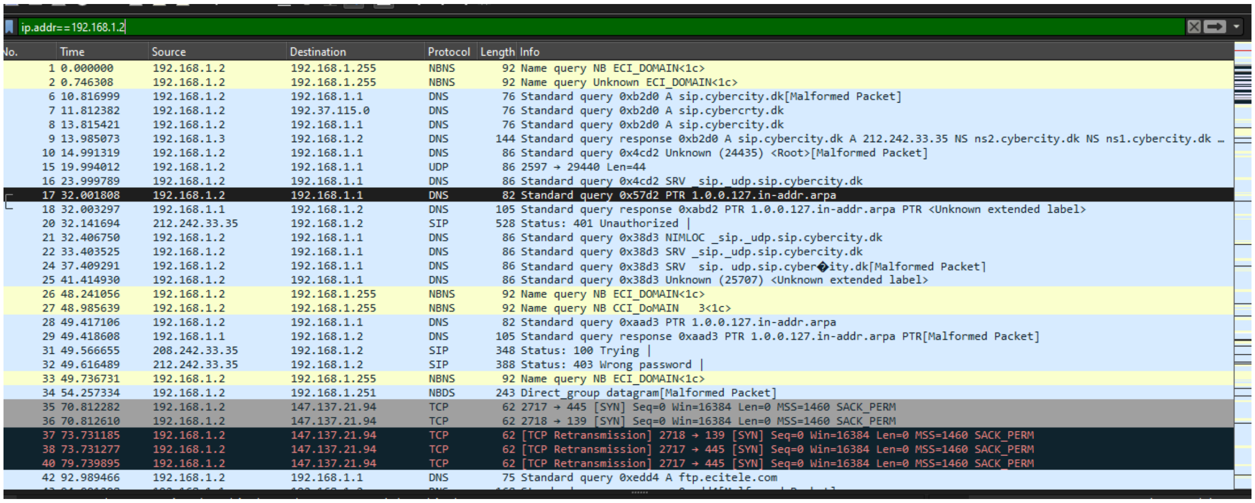
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.2	192.168.1.255	NBNS	92	Name query NB ECI_DOMAIN<1c>
2	0.746308	192.168.1.2	192.168.1.255	NBNS	92	Name query Unknown ECI_DOMAIN<1c>
3	1.497578	217.168.1.2	192.168.1.255	NBNS	92	Name query NB Illegal NetBIOS name (1st character not between A and Z in first-level encoding)[Malformed P…
4	10.816309	Silicom_01:6e:bd	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.2
5	10.816973	CastlenetTec_00:34:…	Silicom_01:6e:bd	ARP	60	192.168.1.1 is at 00:30:4b:bd:34:56
6	10.816999	192.168.1.2	192.168.1.1	DNS	76	Standard query 0xb2d0 A sip.cybercity.dk[Malformed Packet]
7	11.812382	192.168.1.2	192.37.115.0	DNS	76	Standard query 0xb2d0 A sip.cybercrty.dk
8	13.815421	192.168.1.2	192.168.1.1	DNS	76	Standard query 0xb2d0 A sip.cybercity.dk
9	13.985073	192.168.1.3	192.168.1.2	DNS	144	Standard query response 0xb2d0 A sip.cybercity.dk A 212.242.33.35 NS ns2.cybercity.dk NS ns1.cybercity.dk …
10	14.991319	192.168.1.2	192.168.1.1	DNS	86	Standard query 0x4cd2 Unknown (24435) <Root>[Malformed Packet]
11	15.988218	192.168.1.110	192.168.1.1	DNS	86	Standard query 0x4cd2[Malformed Packet]
12	17.991242	Silicom_01:6e:bd	CastlenetTec_00:34:…	0x6d00	86	Ethernet II
13	18.983585	CastlenetTec_00:34:…	Silicom_01:6e:bd	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected!)
14	18.983634	Silicom_01:6e:bd	CastlenetTec_00:34:…	ARP	42	192.184.1.2 is at 00:e0:ed:01:6e:bd (duplicate use of 192.168.1.1 detected!)
15	19.994012	192.168.1.2	192.168.1.1	UDP	86	2597 → 29440 Len=44
16	23.999789	192.168.1.2	192.168.1.1	DNS	86	Standard query 0x4cd2 SRV _sip._udp.sip.cybercity.dk
17	32.001808	192.168.1.2	192.168.1.1	DNS	82	Standard query 0x57d2 PTR 1.0.0.127.in-addr.arpa
18	32.003297	192.168.1.1	192.168.1.2	DNS	105	Standard query response 0xabd2 PTR 1.0.0.127.in-addr.arpa PTR <Unknown extended label>
19	32.004937	192.168.1.52	212.242.33.35	SIP	509	Request: REGISTER sip:sip.cybercity.dk[Malformed Packet]
20	32.141694	212.242.33.35	192.168.1.2	SIP	528	Status: 401 Unauthorized |
21	32.406750	192.168.1.2	192.168.1.1	DNS	86	Standard query 0x38d3 NIMLOC _sip._udp.sip.cybercity.dk
22	33.403525	192.168.1.2	192.168.1.1	DNS	86	Standard query 0x38d3 SRV _sip._udp.sip.cybercity.dk
23	35.406164	aa:aa:aa:aa:aa:aa	AxusMicrosys_aa:aa:…	Ethern…	86	Ethernet II
24	37.409291	192.168.1.2	192.168.1.1	DNS	86	Standard query 0x38d3 SRV sip. udp.sip.cyber�ity.dk[Malformed Packet]
25	41.414930	192.168.1.2	192.168.1.1	DNS	86	Standard query 0x38d3 Unknown (25707) <Unknown extended label>
26	48.241056	192.168.1.2	192.168.1.255	NBNS	92	Name query NB ECI_DOMAIN<1c>
27	48.985639	192.168.1.2	192.168.1.255	NBNS	92	Name query NB CCI_DoMAIN 3<1c>
28	49.417106	192.168.1.2	192.168.1.1	DNS	82	Standard query 0xaad3 PTR 1.0.0.127.in-addr.arpa
29	49.418608	192.168.1.1	192.168.1.2	DNS	105	Standard query response 0xaad3 PTR 1.0.0.127.in-addr.arpa PTR[Malformed Packet]
30	49.420564	Silicom_01:6e:bd	CastlenetTec_00:34:…	0x2800	722	Ethernet II

```
▸ Frame 114: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▸ Ethernet II, Src: Silicom_01:6e:bd (00:e0:ed:01:6e:bd), Dst: CastlenetTec_3f:34:56 (00:30:54:3f:34:56)
▸ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.17.1
▸ User Datagram Protocol, Src Port: 2724, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  00 30 54 3f 34 56 00 e0  ed 01 6e bd 08 00
0010  00 48 69 d4 00 00 80 11  4d 7d c0 a8 01 02
0020  11 01 0a a4 00 35 00 34  53 4a d6 d6 01 00
0030  00 00 00 00 00 00 04 5f  7a 69 70 04 5f 75
0040  03 73 69 70 09 63 79 62  65 72 63 69 74 79
0050  6b 00 00 21 00 01
```

2. Use Wireshark's statistical tools and filters to separate the attack traffic from legitimate traffic. This may involve filtering by IP addresses, protocols, and patterns typical of DDoS attacks, such as a high number of SYN packets.

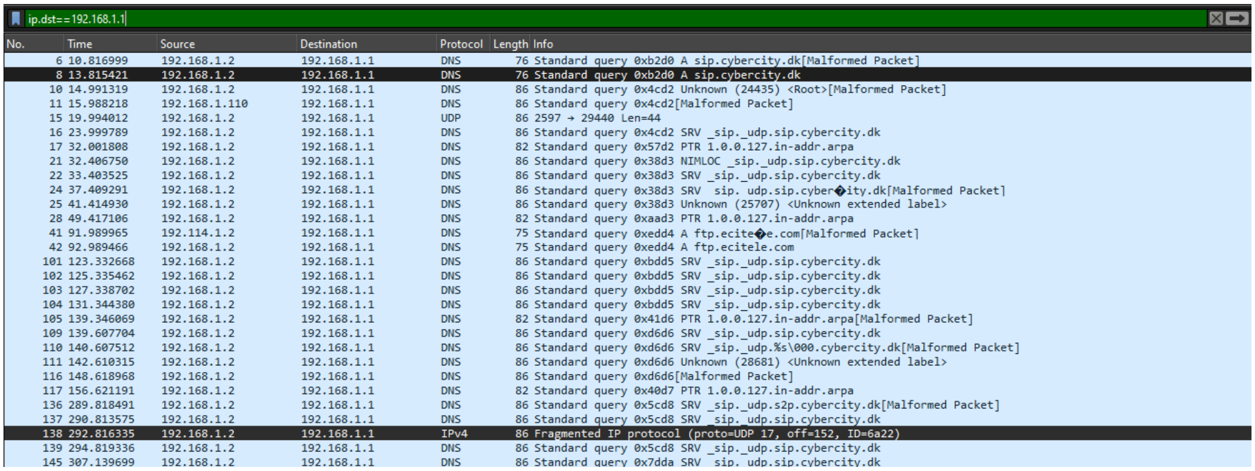
Filtering by ip addresses of the source:



```
ip.addr==192.168.1.2

No.   Time       Source          Destination     Protocol Length Info
    1 0.000000   192.168.1.2     192.168.1.255   NBNS      92 Name query NB ECI_DOMAIN<1c>
    2 0.746308   192.168.1.2     192.168.1.255   NBNS      92 Name query Unknown ECI_DOMAIN<1c>
    6 10.816999  192.168.1.2     192.168.1.1     DNS       76 Standard query 0xb2d0 A sip.cybercity.dk[Malformed Packet]
    7 11.812382  192.168.1.2     192.37.115.0    DNS       76 Standard query 0xb2d0 A sip.cybercrty.dk
    8 13.815421  192.168.1.2     192.168.1.1     DNS       76 Standard query 0xb2d0 A sip.cybercity.dk
    9 13.985073  192.168.1.3     192.168.1.2     DNS      144 Standard query response 0xb2d0 A sip.cybercity.dk A 212.242.33.35 NS ns2.cybercity.dk NS ns1.cybercity.dk …
   10 14.991319  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x4cd2 Unknown (24435) <Root>[Malformed Packet]
   15 19.994012  192.168.1.2     192.168.1.1     UDP       86 2597 → 29440 Len=44
   16 23.999789  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x4cd2 SRV _sip._udp.sip.cybercity.dk
   17 32.001808  192.168.1.2     192.168.1.1     DNS       82 Standard query 0x57d2 PTR 1.0.0.127.in-addr.arpa
   18 32.003297  192.168.1.1     192.168.1.2     DNS      105 Standard query response 0xabd2 PTR 1.0.0.127.in-addr.arpa PTR <Unknown extended label>
   20 32.141694  212.242.33.35   192.168.1.2     SIP      528 Status: 401 Unauthorized |
   21 32.406750  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 NIMLOC _sip._udp.sip.cybercity.dk
   22 33.403525  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 SRV _sip._udp.sip.cybercity.dk
   24 37.409291  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 SRV  sip. udp.sip.cyber�ity.dk[Malformed Packet]
   25 41.414930  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 Unknown (25707) <Unknown extended label>
   26 48.241056  192.168.1.2     192.168.1.255   NBNS      92 Name query NB ECI_DOMAIN<1c>
   27 48.985639  192.168.1.2     192.168.1.255   NBNS      92 Name query NB CCI_DoMAIN   3<1c>
   28 49.417106  192.168.1.2     192.168.1.1     DNS       82 Standard query 0xaad3 PTR 1.0.0.127.in-addr.arpa
   29 49.418608  192.168.1.1     192.168.1.2     DNS      105 Standard query response 0xaad3 PTR 1.0.0.127.in-addr.arpa PTR[Malformed Packet]
   31 49.566655  208.242.33.35   192.168.1.2     SIP      348 Status: 100 Trying |
   32 49.616489  212.242.33.35   192.168.1.2     SIP      388 Status: 403 Wrong password |
   33 49.736731  192.168.1.2     192.168.1.255   NBNS      92 Name query NB ECI_DOMAIN<1c>
   34 54.257334  192.168.1.2     192.168.1.251   NBDS     243 Direct_group datagram[Malformed Packet]
   35 70.812282  192.168.1.2     147.137.21.94   TCP       62 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   36 70.812610  192.168.1.2     147.137.21.94   TCP       62 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   37 73.731185  192.168.1.2     147.137.21.94   TCP       62 [TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   38 73.731277  192.168.1.2     147.137.21.94   TCP       62 [TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   40 79.739895  192.168.1.2     147.137.21.94   TCP       62 [TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   42 92.989466  192.168.1.2     192.168.1.1     DNS       75 Standard query 0xedd4 A ftp.ecitele.com
```

Filtering by ip addresses of the destination:

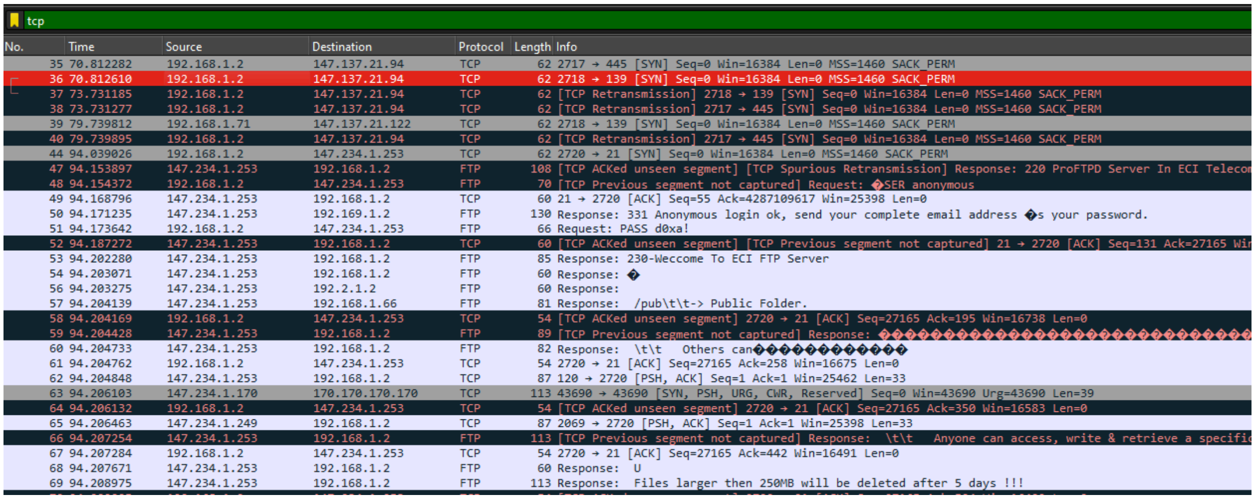


```
ip.dst==192.168.1.1

No.   Time        Source          Destination     Protocol Length Info
    6 10.816999   192.168.1.2     192.168.1.1     DNS       76 Standard query 0xb2d0 A sip.cybercity.dk[Malformed Packet]
    8 13.815421   192.168.1.2     192.168.1.1     DNS       76 Standard query 0xb2d0 A sip.cybercity.dk
   10 14.991319   192.168.1.2     192.168.1.1     DNS       86 Standard query 0x4cd2 Unknown (24435) <Root>[Malformed Packet]
   11 15.988218   192.168.1.110   192.168.1.1     DNS       86 Standard query 0x4cd2[Malformed Packet]
   15 19.994012   192.168.1.2     192.168.1.1     UDP       86 2597 → 29440 Len=44
   16 23.999789   192.168.1.2     192.168.1.1     DNS       86 Standard query 0x4cd2 SRV _sip._udp.sip.cybercity.dk
   17 32.001808   192.168.1.2     192.168.1.1     DNS       82 Standard query 0x57d2 PTR 1.0.0.127.in-addr.arpa
   21 32.406750   192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 NIMLOC _sip._udp.sip.cybercity.dk
   22 33.403525   192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 SRV _sip._udp.sip.cybercity.dk
   24 37.409291   192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 SRV  sip. udp.sip.cyber�ity.dk[Malformed Packet]
   25 41.414930   192.168.1.2     192.168.1.1     DNS       86 Standard query 0x38d3 Unknown (25707) <Unknown extended label>
   28 49.417106   192.168.1.2     192.168.1.1     DNS       82 Standard query 0xaad3 PTR 1.0.0.127.in-addr.arpa
   41 91.989965   192.114.1.2     192.168.1.1     DNS       75 Standard query 0xedd4 A ftp.ecite�e.com[Malformed Packet]
   42 92.989466   192.168.1.2     192.168.1.1     DNS       75 Standard query 0xedd4 A ftp.ecitele.com
  101 123.332668  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  102 125.335462  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  103 127.338702  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  104 131.344380  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  105 139.346069  192.168.1.2     192.168.1.1     DNS       82 Standard query 0x41d6 PTR 1.0.0.127.in-addr.arpa[Malformed Packet]
  109 139.607704  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xd6d6 SRV _sip._udp.sip.cybercity.dk
  110 140.607512  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xd6d6 SRV _sip._udp.%s\000.cybercity.dk[Malformed Packet]
  111 142.610315  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xd6d6 Unknown (28681) <Unknown extended label>
  116 148.618968  192.168.1.2     192.168.1.1     DNS       86 Standard query 0xd6d6[Malformed Packet]
  117 156.621191  192.168.1.2     192.168.1.1     DNS       82 Standard query 0x40d7 PTR 1.0.0.127.in-addr.arpa
  136 289.818491  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x5cd8 SRV _sip._udp.s2p.cybercity.dk[Malformed Packet]
  137 290.813575  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x5cd8 SRV _sip._udp.sip.cybercity.dk
  138 292.816335  192.168.1.2     192.168.1.1     IPv4      86 Fragmented IP protocol (proto=UDP 17, off=152, ID=6a22)
  139 294.819336  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x5cd8 SRV _sip._udp.sip.cybercity.dk
  145 307.139699  192.168.1.2     192.168.1.1     DNS       86 Standard query 0x7dda SRV  sip. udp.sip.cybercity.dk
```

Filter by protocols (TCP):

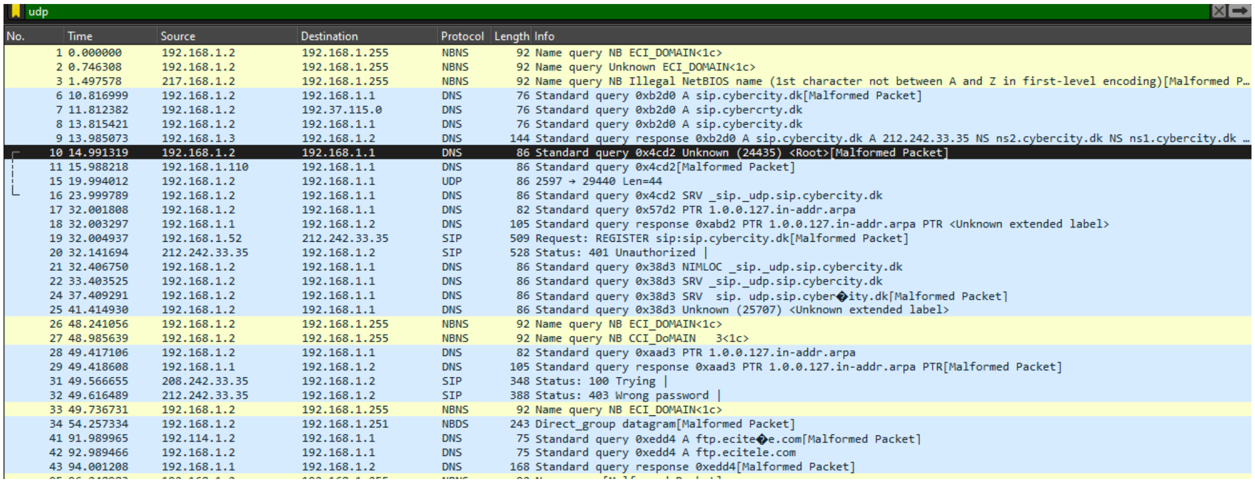
Very few packets are there



```
No.   Time       Source          Destination       Protocol Length Info
   35 70.812282  192.168.1.2     147.137.21.94     TCP       62 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   36 70.812610  192.168.1.2     147.137.21.94     TCP       62 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   37 73.731185  192.168.1.2     147.137.21.94     TCP       62 [TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   38 73.731277  192.168.1.2     147.137.21.94     TCP       62 [TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   39 79.739812  192.168.1.71    147.137.21.122    TCP       62 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   40 79.739895  192.168.1.2     147.137.21.94     TCP       62 [TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   44 94.039026  192.168.1.2     147.234.1.253     TCP       62 2720 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   47 94.153897  147.234.1.253   192.168.1.2       FTP      108 [TCP ACKed unseen segment] [TCP Spurious Retransmission] Response: 220 ProFTPD Server In ECI Telecom
   48 94.154372  192.168.1.2     147.234.1.253     FTP       70 [TCP Previous segment not captured] Request: �SER anonymous
   49 94.168796  147.234.1.253   192.168.1.2       TCP       60 21 → 2720 [ACK] Seq=55 Ack=4287109617 Win=25398 Len=0
   50 94.171235  147.234.1.253   192.169.1.2       FTP      130 Response: 331 Anonymous login ok, send your complete email address �s your password.
   51 94.173642  192.168.1.2     147.234.1.253     FTP       66 Request: PASS d0xa!
   52 94.187272  147.234.1.253   192.168.1.2       TCP       60 [TCP ACKed unseen segment] [TCP Previous segment not captured] 21 → 2720 [ACK] Seq=131 Ack=27165 Wir
   53 94.202280  147.234.1.253   192.168.1.2       FTP       85 Response: 230-Weccome To ECI FTP Server
   54 94.203071  147.234.1.253   192.168.1.2       FTP       60 Response: �
   56 94.203275  147.234.1.253   192.2.1.2         FTP       60 Response:
   57 94.204139  147.234.1.253   192.168.1.66      FTP       81 Response:  /pub\t\t-> Public Folder.
   58 94.204169  192.168.1.2     147.234.1.253     TCP       54 [TCP ACKed unseen segment] 2720 → 21 [ACK] Seq=27165 Ack=195 Win=16738 Len=0
   59 94.204428  147.234.1.253   192.168.1.2       FTP       89 [TCP Previous segment not captured] Response: ���������������������������
   60 94.204733  147.234.1.253   192.168.1.2       FTP       82 Response:  \t\t   Others can������������
   61 94.204762  192.168.1.2     147.234.1.253     TCP       54 2720 → 21 [ACK] Seq=27165 Ack=258 Win=16675 Len=0
   62 94.204848  147.234.1.253   192.168.1.2       TCP       87 120 → 2720 [PSH, ACK] Seq=1 Ack=1 Win=25462 Len=33
   63 94.206103  147.234.1.170   170.170.170.170   TCP      113 43690 → 43690 [SYN, PSH, URG, CWR, Reserved] Seq=0 Win=43690 Urg=43690 Len=39
   64 94.206132  192.168.1.2     147.234.1.253     TCP       54 [TCP ACKed unseen segment] 2720 → 21 [ACK] Seq=27165 Ack=350 Win=16583 Len=0
   65 94.206463  147.234.1.249   192.168.1.2       TCP       87 2069 → 2720 [PSH, ACK] Seq=1 Ack=1 Win=25398 Len=33
   66 94.207254  147.234.1.253   192.168.1.2       FTP      113 [TCP Previous segment not captured] Response:  \t\t   Anyone can access, write & retrieve a specifi
   67 94.207284  192.168.1.2     147.234.1.253     TCP       54 2720 → 21 [ACK] Seq=27165 Ack=442 Win=16491 Len=0
   68 94.207671  147.234.1.253   192.168.1.2       FTP       60 Response:  U
   69 94.208975  147.234.1.253   192.168.1.2       FTP      113 Response:  Files larger then 250MB will be deleted after 5 days !!!
```

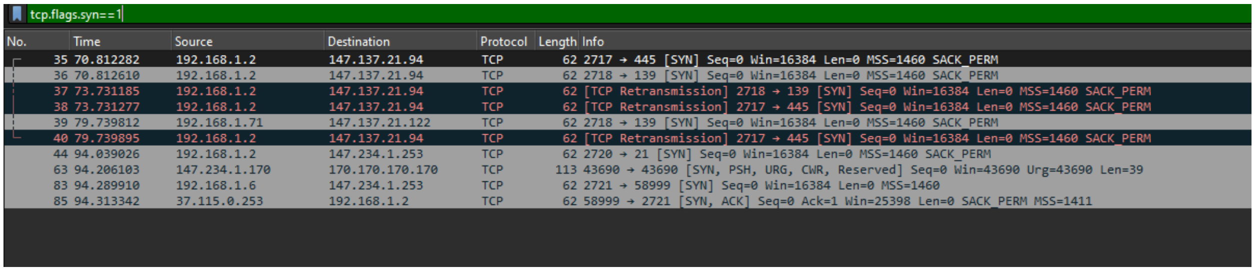
Udp:

Large number of packets are there so we have to focus on these types of packets:



```
No.   Time       Source          Destination       Protocol Length Info
    1 0.000000   192.168.1.2     192.168.1.255     NBNS      92 Name query NB ECI_DOMAIN<1c>
    2 0.746308   192.168.1.2     192.168.1.255     NBNS      92 Name query Unknown ECI_DOMAIN<1c>
    3 1.497578   217.168.1.2     192.168.1.255     NBNS      92 Name query NB Illegal NetBIOS name (1st character not between A and Z in first-level encoding)[Malformed P…
    6 10.816999  192.168.1.2     192.168.1.1       DNS       76 Standard query 0xb2d0 A sip.cybercity.dk[Malformed Packet]
    7 11.812382  192.168.1.2     192.37.115.0      DNS       76 Standard query 0xb2d0 A sip.cybercrty.dk
    8 13.815421  192.168.1.2     192.168.1.1       DNS       76 Standard query 0xb2d0 A sip.cybercity.dk
    9 13.985073  192.168.1.3     192.168.1.2       DNS      144 Standard query response 0xb2d0 A sip.cybercity.dk A 212.242.33.35 NS ns2.cybercity.dk NS ns1.cybercity.dk …
   10 14.991319  192.168.1.2     192.168.1.1       DNS       86 Standard query 0x4cd2 Unknown (24435) <Root>[Malformed Packet]
   11 15.988218  192.168.1.110   192.168.1.1       DNS       86 Standard query 0x4cd2[Malformed Packet]
   15 19.994012  192.168.1.2     192.168.1.1       UDP       86 2597 → 29440 Len=44
   16 23.999789  192.168.1.2     192.168.1.1       DNS       86 Standard query 0x4cd2 SRV _sip._udp.sip.cybercity.dk
   17 32.001808  192.168.1.2     192.168.1.1       DNS       82 Standard query 0x57d2 PTR 1.0.0.127.in-addr.arpa
   18 32.003297  192.168.1.1     192.168.1.2       DNS      105 Standard query response 0xabd2 PTR 1.0.0.127.in-addr.arpa PTR <Unknown extended label>
   19 32.004937  192.168.1.52    212.242.33.35     SIP      509 Request: REGISTER sip:sip.cybercity.dk[Malformed Packet]
   20 32.141694  212.242.33.35   192.168.1.2       SIP      528 Status: 401 Unauthorized |
   21 32.406750  192.168.1.2     192.168.1.1       DNS       86 Standard query 0x38d3 NIMLOC _sip._udp.sip.cybercity.dk
   22 33.403525  192.168.1.2     192.168.1.1       DNS       86 Standard query 0x38d3 SRV _sip._udp.sip.cybercity.dk
   24 37.409291  192.168.1.2     192.168.1.1       DNS       86 Standard query 0x38d3 SRV  sip. udp.sip.cyber�ity.dk[Malformed Packet]
   25 41.414930  192.168.1.2     192.168.1.1       DNS       86 Standard query 0x38d3 Unknown (25707) <Unknown extended label>
   26 48.241056  192.168.1.2     192.168.1.255     NBNS      92 Name query NB ECI_DOMAIN<1c>
   27 48.985639  192.168.1.2     192.168.1.255     NBNS      92 Name query NB CCI_DoMAIN   3<1c>
   28 49.417106  192.168.1.2     192.168.1.1       DNS       82 Standard query 0xaad3 PTR 1.0.0.127.in-addr.arpa
   29 49.418608  192.168.1.1     192.168.1.2       DNS      105 Standard query response 0xaad3 PTR 1.0.0.127.in-addr.arpa PTR[Malformed Packet]
   31 49.566655  208.242.33.35   192.168.1.2       SIP      348 Status: 100 Trying |
   32 49.616489  212.242.33.35   192.168.1.2       SIP      388 Status: 403 Wrong password |
   33 49.736731  192.168.1.2     192.168.1.255     NBNS      92 Name query NB ECI_DOMAIN<1c>
   34 54.257334  192.168.1.2     192.168.1.251     NBDS     243 Direct_group datagram[Malformed Packet]
   41 91.989965  192.114.1.2     192.168.1.1       DNS       75 Standard query 0xedd4 A ftp.ecite�e.com[Malformed Packet]
   42 92.989466  192.168.1.2     192.168.1.1       DNS       75 Standard query 0xedd4 A ftp.ecitele.com
   43 94.001208  192.168.1.1     192.168.1.2       DNS      168 Standard query response 0xedd4[Malformed Packet]
```

Using the syn flags:This filter is used to see what packets which are not given with valid handshakes.



tcp.flags.syn==1

No.	Time	Source	Destination	Protocol	Length	Info
35	70.812282	192.168.1.2	147.137.21.94	TCP	62	2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
36	70.812610	192.168.1.2	147.137.21.94	TCP	62	2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
37	73.731185	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
38	73.731277	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
39	79.739812	192.168.1.71	147.137.21.122	TCP	62	2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
40	79.739895	192.168.1.2	147.137.21.94	TCP	62	[TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
44	94.039026	192.168.1.2	147.234.1.253	TCP	62	2720 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
63	94.206103	147.234.1.170	170.170.170.170	TCP	113	43690 → 43690 [SYN, PSH, URG, CWR, Reserved] Seq=0 Win=43690 Urg=43690 Len=39
83	94.289910	192.168.1.6	147.234.1.253	TCP	62	2721 → 58999 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
85	94.313342	37.115.0.253	192.168.1.2	TCP	62	58999 → 2721 [SYN, ACK] Seq=0 Ack=1 Win=25398 Len=0 SACK_PERM MSS=1411

3**. Analyze the attack traffic to determine the type of DDoS attack (e.g., SYN flood, UDP flood, ICMP flood).**

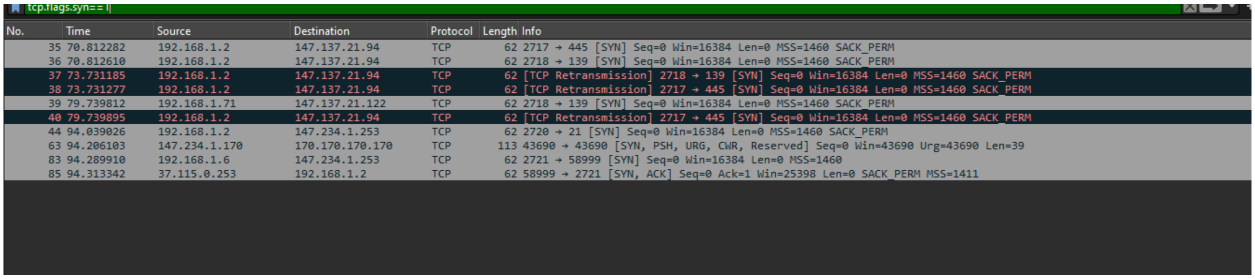
SYN flood: High volume of SYN packets with incomplete handshakes.

UDP flood: High volume of UDP packets to specific ports.

ICMP flood: High volume of ICMP Echo Request packets.

Analyze Timing and Characteristics:

1) Pay attention to the timing and characteristics of the traffic patterns observed:
2) Look for sudden spikes in traffic volume or sustained high levels of activity, which may indicate an ongoing attack.
3) Analyze the distribution of traffic across different protocols and ports.
4) Consider the source and destination IP addresses involved in the traffic and any patterns or anomalies observed.
5) Use Wireshark's statistical tools, such as IO Graphs or Packet Rate Statistics, to visualize and analyze traffic patterns over time.
6) Compare the observed traffic patterns with known signatures or indicators of DDoS attacks to identify similarities.

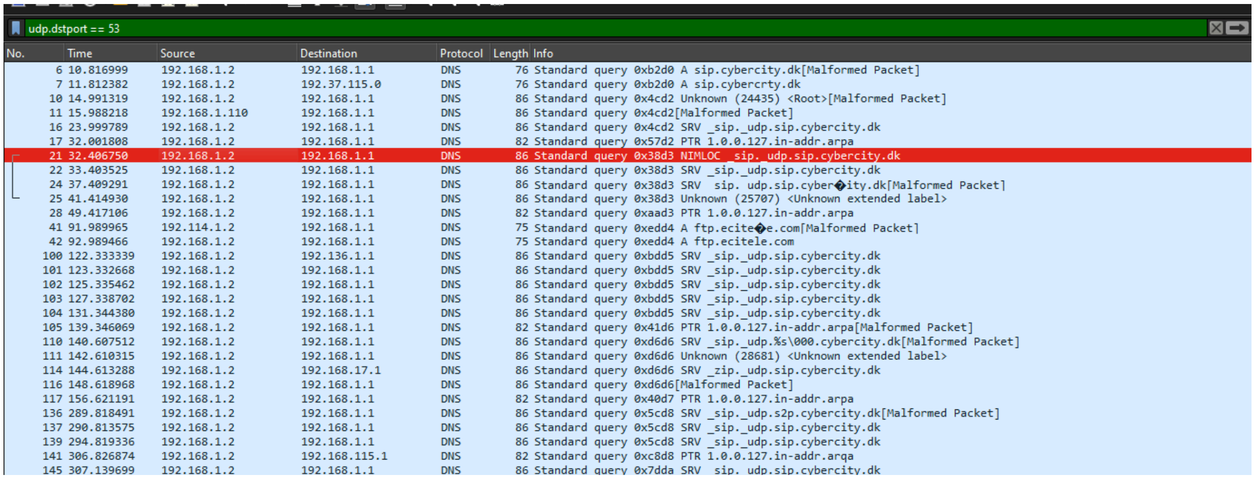


```
tcp.flags.syn==1

No.   Time       Source          Destination      Protocol Length Info
   35 70.812282  192.168.1.2     147.137.21.94    TCP       62 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   36 70.812610  192.168.1.2     147.137.21.94    TCP       62 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   37 73.731185  192.168.1.2     147.137.21.94    TCP       62 [TCP Retransmission] 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   38 73.731277  192.168.1.2     147.137.21.94    TCP       62 [TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   39 79.739812  192.168.1.71    147.137.21.122   TCP       62 2718 → 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   40 79.739895  192.168.1.2     147.137.21.94    TCP       62 [TCP Retransmission] 2717 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   44 94.039026  192.168.1.2     147.234.1.253    TCP       62 2720 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
   63 94.206103  147.234.1.170   170.170.170.170  TCP      113 43690 → 43690 [SYN, PSH, URG, CWR, Reserved] Seq=0 Win=43690 Urg=43690 Len=39
   83 94.289910  192.168.1.6     147.234.1.253    TCP       62 2721 → 58999 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
   85 94.313342  37.115.0.253    192.168.1.2      TCP       62 58999 → 2721 [SYN, ACK] Seq=0 Ack=1 Win=25398 Len=0 SACK_PERM MSS=1411
```

Here there are many packets with only syn packets that means there is incomplete handshake done. Mostly the source packet ip address is from 192.168.1.2.

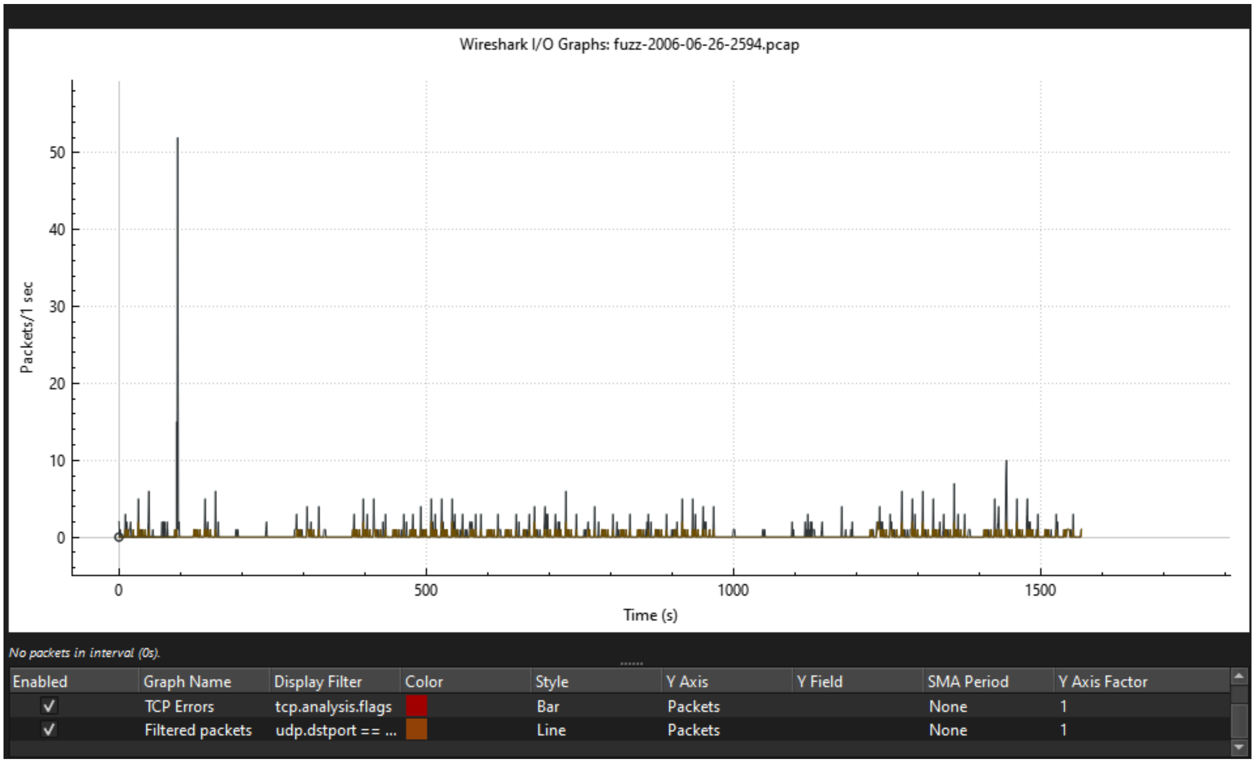
Now check for the specific udp ports:



```
udp.dstport == 53

No.   Time        Source          Destination      Protocol Length Info
    6 10.816999   192.168.1.2     192.168.1.1      DNS       76 Standard query 0xb2d0 A sip.cybercity.dk[Malformed Packet]
    7 11.812382   192.168.1.2     192.37.115.0     DNS       76 Standard query 0xb2d0 A sip.cybercrty.dk
   10 14.991319   192.168.1.2     192.168.1.1      DNS       86 Standard query 0x4cd2 Unknown (24435) <Root>[Malformed Packet]
   11 15.988218   192.168.1.110   192.168.1.1      DNS       86 Standard query 0x4cd2[Malformed Packet]
   16 23.999789   192.168.1.2     192.168.1.1      DNS       86 Standard query 0x4cd2 SRV _sip._udp.sip.cybercity.dk
   17 32.001808   192.168.1.2     192.168.1.1      DNS       82 Standard query 0x57d2 PTR 1.0.0.127.in-addr.arpa
   21 32.406750   192.168.1.2     192.168.1.1      DNS       86 Standard query 0x38d3 NIMLOC _sip._udp.sip.cybercity.dk
   22 33.403525   192.168.1.2     192.168.1.1      DNS       86 Standard query 0x38d3 SRV _sip._udp.sip.cybercity.dk
   24 37.409291   192.168.1.2     192.168.1.1      DNS       86 Standard query 0x38d3 SRV  sip. udp.sip.cyber�ity.dk[Malformed Packet]
   25 41.414930   192.168.1.2     192.168.1.1      DNS       86 Standard query 0x38d3 Unknown (25707) <Unknown extended label>
   28 49.417106   192.168.1.2     192.168.1.1      DNS       82 Standard query 0xaad3 PTR 1.0.0.127.in-addr.arpa
   41 91.989965   192.114.1.2     192.168.1.1      DNS       75 Standard query 0xedd4 A ftp.ecite�e.com[Malformed Packet]
   42 92.989466   192.168.1.2     192.168.1.1      DNS       75 Standard query 0xedd4 A ftp.ecitele.com
  100 122.333339  192.168.1.2     192.136.1.1      DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  101 123.332668  192.168.1.2     192.168.1.1      DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  102 125.335462  192.168.1.2     192.168.1.1      DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  103 127.338702  192.168.1.2     192.168.1.1      DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  104 131.344380  192.168.1.2     192.168.1.1      DNS       86 Standard query 0xbdd5 SRV _sip._udp.sip.cybercity.dk
  105 139.346069  192.168.1.2     192.168.1.1      DNS       82 Standard query 0x41d6 PTR 1.0.0.127.in-addr.arpa[Malformed Packet]
  110 140.607512  192.168.1.2     192.168.1.1      DNS       86 Standard query 0xd6d6 SRV _sip._udp.%s\000.cybercity.dk[Malformed Packet]
  111 142.610315  192.168.1.2     192.168.1.1      DNS       86 Standard query 0xd6d6 Unknown (28681) <Unknown extended label>
  114 144.613288  192.168.1.2     192.168.17.1     DNS       86 Standard query 0xd6d6 SRV _zip._udp.sip.cybercity.dk
  116 148.618968  192.168.1.2     192.168.1.1      DNS       86 Standard query 0xd6d6[Malformed Packet]
  117 156.621191  192.168.1.2     192.168.1.1      DNS       82 Standard query 0x40d7 PTR 1.0.0.127.in-addr.arpa
  136 289.818491  192.168.1.2     192.168.1.1      DNS       86 Standard query 0x5cd8 SRV _sip._udp.s2p.cybercity.dk[Malformed Packet]
  137 290.813575  192.168.1.2     192.168.1.1      DNS       86 Standard query 0x5cd8 SRV _sip._udp.sip.cybercity.dk
  139 294.819336  192.168.1.2     192.168.1.1      DNS       86 Standard query 0x5cd8 SRV _sip._udp.sip.cybercity.dk
  141 306.826874  192.168.1.2     192.168.115.1    DNS       82 Standard query 0xc8d8 PTR 1.0.0.127.in-addr.arqa
  145 307.139699  192.168.1.2     192.168.1.1      DNS       86 Standard query 0x7dda SRV  sip. udp.sip.cybercity.dk
```

Here is the IO graphs for the udp packets:
Here spikes shows the packet rate is very much higher at that timestamp.



No packets in interval (0s).

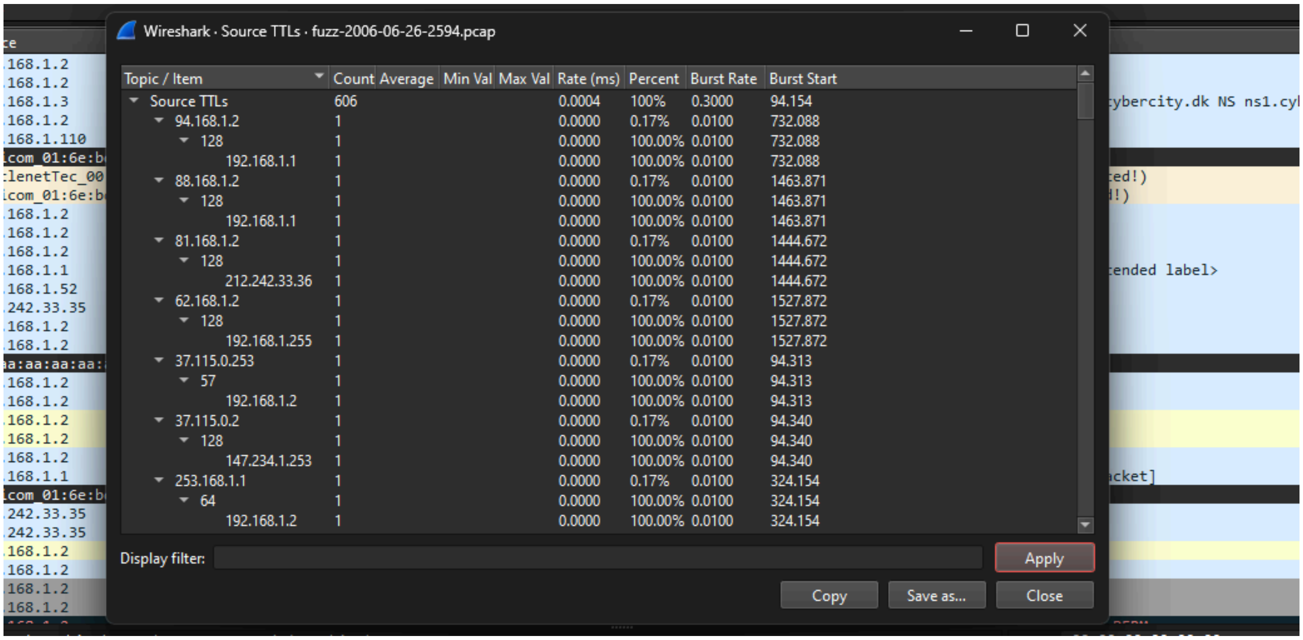
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
✓	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None	1
✓	Filtered packets	udp.dstport == ...	🟧	Line	Packets		None	1

4. Attempt to identify the source of the attack, noting that IP spoofing may have been used.

Analyze Traffic Patterns:

1) Look for consistent patterns in the traffic, such as similar packet sizes, timing, or behavior. While attackers may attempt to obfuscate their source IP addresses, they often cannot completely hide these patterns.
2) Analyze the timing of the packets. Consistent timing patterns may indicate automated attack tools.

Look for common characteristics among packets from potential sources, such as the same TTL (Time to Live) values or similar IP header options.

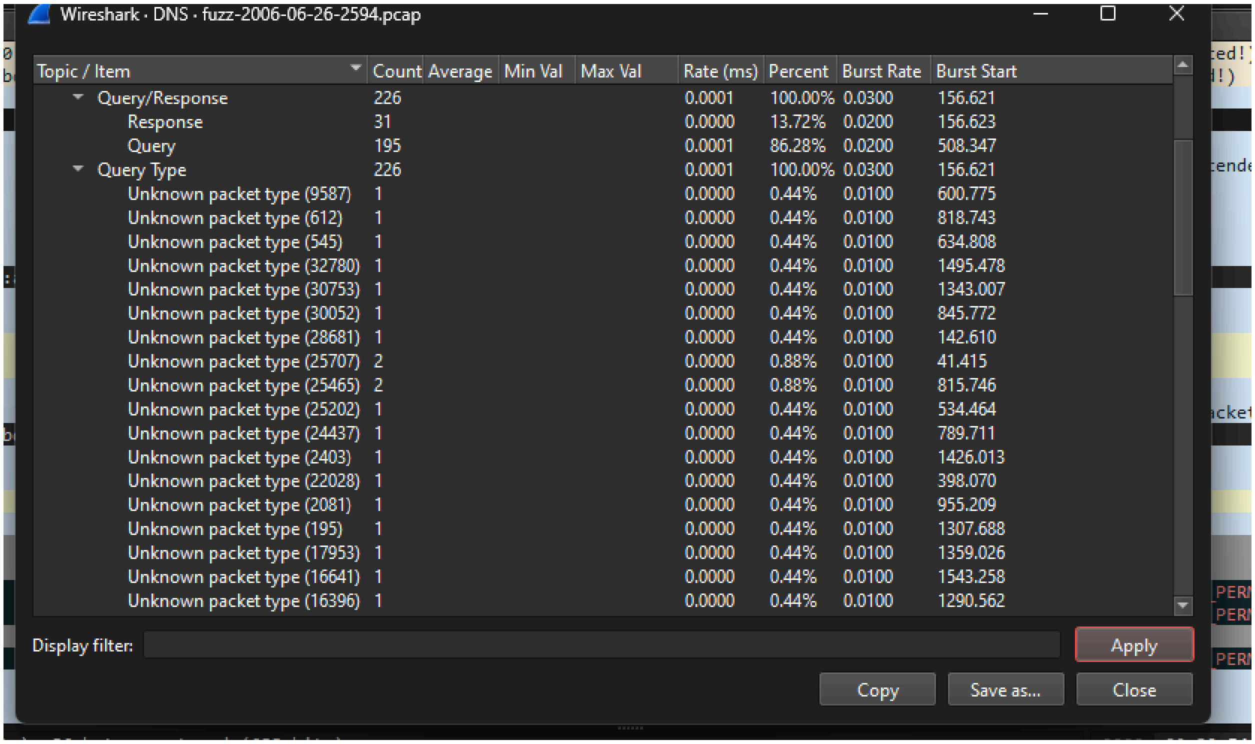


Wireshark · Source TTLs · fuzz-2006-06-26-2594.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source TTLs	606				0.0004	100%	0.3000	94.154
94.168.1.2	1				0.0000	0.17%	0.0100	732.088
128	1				0.0000	100.00%	0.0100	732.088
192.168.1.1	1				0.0000	100.00%	0.0100	732.088
88.168.1.2	1				0.0000	0.17%	0.0100	1463.871
128	1				0.0000	100.00%	0.0100	1463.871
192.168.1.1	1				0.0000	100.00%	0.0100	1463.871
81.168.1.2	1				0.0000	0.17%	0.0100	1444.672
128	1				0.0000	100.00%	0.0100	1444.672
212.242.33.36	1				0.0000	100.00%	0.0100	1444.672
62.168.1.2	1				0.0000	0.17%	0.0100	1527.872
128	1				0.0000	100.00%	0.0100	1527.872
192.168.1.255	1				0.0000	100.00%	0.0100	1527.872
37.115.0.253	1				0.0000	0.17%	0.0100	94.313
57	1				0.0000	100.00%	0.0100	94.313
192.168.1.2	1				0.0000	100.00%	0.0100	94.313
37.115.0.2	1				0.0000	0.17%	0.0100	94.340
128	1				0.0000	100.00%	0.0100	94.340
147.234.1.253	1				0.0000	100.00%	0.0100	94.340
253.168.1.1	1				0.0000	0.17%	0.0100	324.154
64	1				0.0000	100.00%	0.0100	324.154
192.168.1.2	1				0.0000	100.00%	0.0100	324.154

Display filter:

Here we can see there are many unknown packets which I can see in the Wireshark DNS statistics.



Wireshark · DNS · fuzz-2006-06-26-2594.pcap

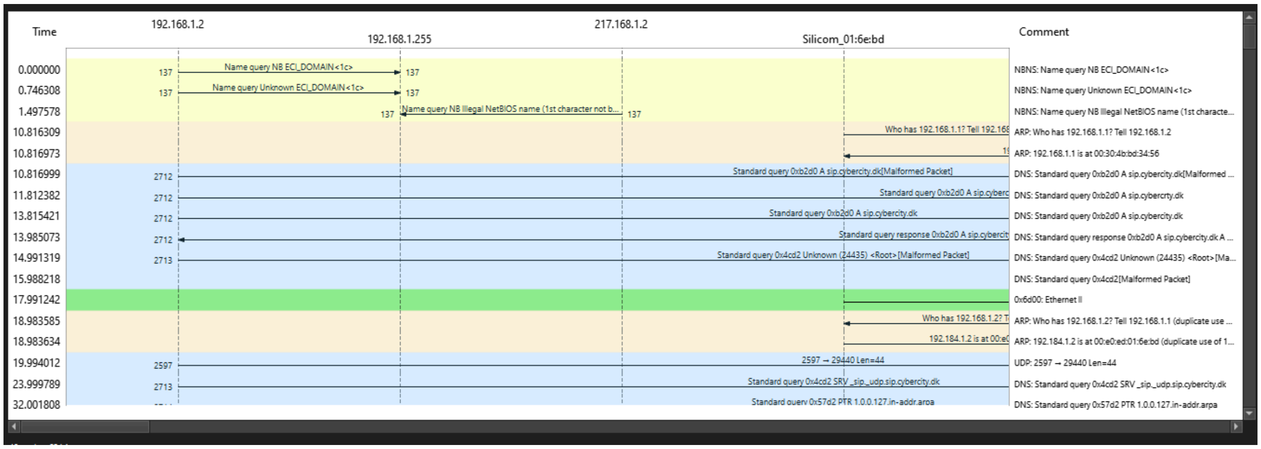
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Query/Response	226				0.0001	100.00%	0.0300	156.621
Response	31				0.0000	13.72%	0.0200	156.623
Query	195				0.0001	86.28%	0.0200	508.347
Query Type	226				0.0001	100.00%	0.0300	156.621
Unknown packet type (9587)	1				0.0000	0.44%	0.0100	600.775
Unknown packet type (612)	1				0.0000	0.44%	0.0100	818.743
Unknown packet type (545)	1				0.0000	0.44%	0.0100	634.808
Unknown packet type (32780)	1				0.0000	0.44%	0.0100	1495.478
Unknown packet type (30753)	1				0.0000	0.44%	0.0100	1343.007
Unknown packet type (30052)	1				0.0000	0.44%	0.0100	845.772
Unknown packet type (28681)	1				0.0000	0.44%	0.0100	142.610
Unknown packet type (25707)	2				0.0000	0.88%	0.0100	41.415
Unknown packet type (25465)	2				0.0000	0.88%	0.0100	815.746
Unknown packet type (25202)	1				0.0000	0.44%	0.0100	534.464
Unknown packet type (24437)	1				0.0000	0.44%	0.0100	789.711
Unknown packet type (2403)	1				0.0000	0.44%	0.0100	1426.013
Unknown packet type (22028)	1				0.0000	0.44%	0.0100	398.070
Unknown packet type (2081)	1				0.0000	0.44%	0.0100	955.209
Unknown packet type (195)	1				0.0000	0.44%	0.0100	1307.688
Unknown packet type (17953)	1				0.0000	0.44%	0.0100	1359.026
Unknown packet type (16641)	1				0.0000	0.44%	0.0100	1543.258
Unknown packet type (16396)	1				0.0000	0.44%	0.0100	1290.562

Display filter:

5. Analyze the impact of the attack on the network and the victim, looking for signs of service degradation or failure.

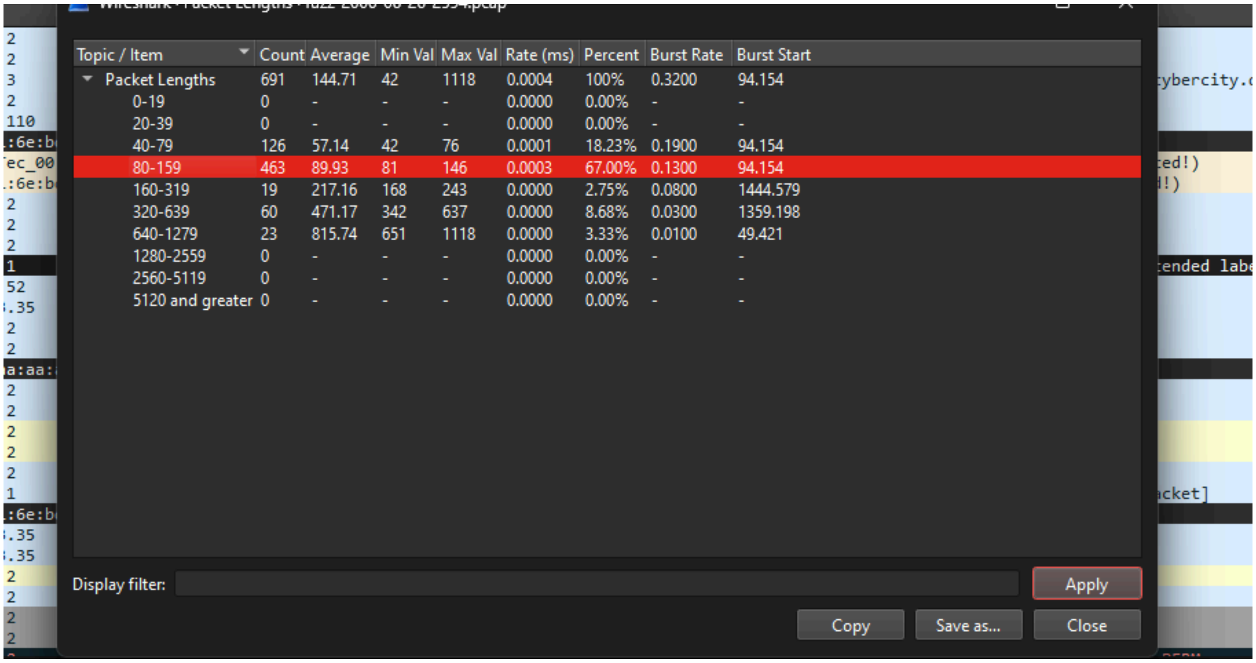
1) Look for signs of service degradation or failure in the captured traffic.
2) Check for unusually high packet loss, increased response times, or service disruptions.
3) Analyze the network traffic patterns to identify areas of congestion or overload caused by the attack.
4) Examine any error messages or alerts generated by network devices or services during the attack.

See here the flow graphs: This depicts network traffic by mapping communication patterns between endpoints. It uses nodes to depict endpoints and arrows to show traffic direction. Numerical values indicate packet volume between endpoint pairs. This interactive tool allows users to explore traffic dynamics and identify communication trends efficiently, aiding in network analysis and anomaly detection.


192.168.1.2
192.168.1.255
217.168.1.2
Silicom_01:6e:bd
137 Name query NB ECI_DOMAIN<1c> 137
137 Name query Unknown ECI_DOMAIN<1c> 137
137 Name query NB Illegal NetBIOS name (1st character not b... 137
Who has 192.168.1.1? Tell 192.168
19
2712 Standard query 0xb2d0 A sip.cybercity.dk[Malformed Packet]
2712 Standard query 0xb2d0 A sip.cyberc
2712 Standard query 0xb2d0 A sip.cybercity.dk
2712 Standard query response 0xb2d0 A sip.cybercit
2713 Standard query 0x4cd2 Unknown (24435) <Root>[Malformed Packet]
Who has 192.168.1.2? T
192.184.1.2 is at 00:e0
2597 2597 → 29440 Len=44
2713 Standard query 0x4cd2 SRV _sip._udp.sip.cybercity.dk
Standard query 0x57d2 PTR 1.0.0.127.in-addr.arpa

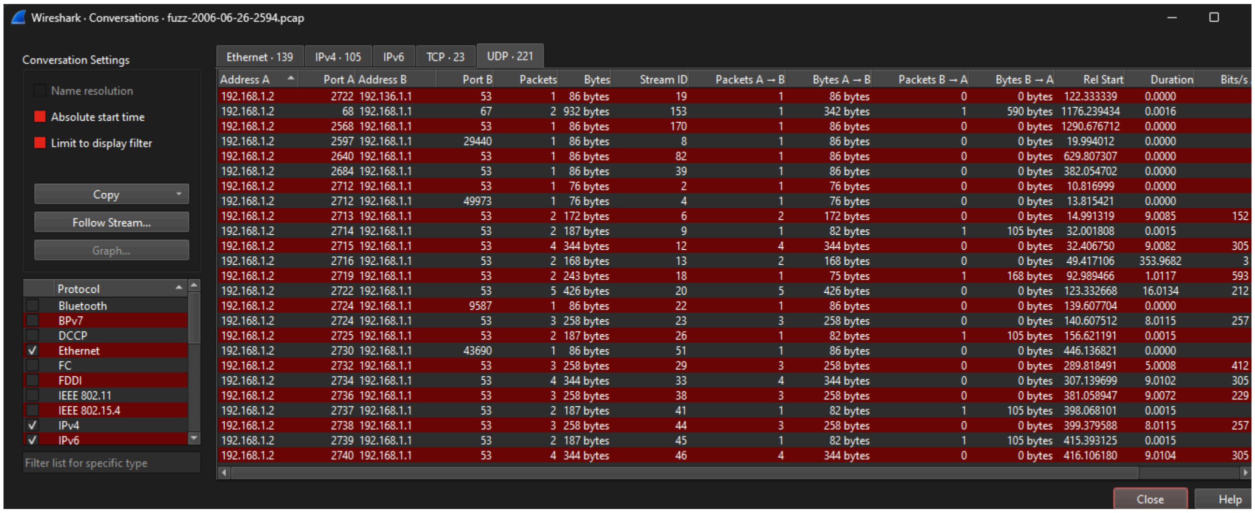
Time	Comment
0.000000	NBNS: Name query NB ECI_DOMAIN<1c>
0.746308	NBNS: Name query Unknown ECI_DOMAIN<1c>
1.497578	NBNS: Name query NB Illegal NetBIOS name (1st characte...
10.816309	ARP: Who has 192.168.1.1? Tell 192.168.1.2
10.816973	ARP: 192.168.1.1 is at 00:30:4b:bd:34:56
10.816999	DNS: Standard query 0xb2d0 A sip.cybercity.dk[Malformed ...
11.812382	DNS: Standard query 0xb2d0 A sip.cybercrty.dk
13.815421	DNS: Standard query 0xb2d0 A sip.cybercity.dk
13.985073	DNS: Standard query response 0xb2d0 A sip.cybercity.dk A ...
14.991319	DNS: Standard query 0x4cd2 Unknown (24435) <Root>[Ma...
15.988218	DNS: Standard query 0x4cd2[Malformed Packet]
17.991242	0x6d00: Ethernet II
18.983585	ARP: Who has 192.168.1.2? Tell 192.168.1.1 (duplicate use ...
18.983634	ARP: 192.184.1.2 is at 00:e0:ed:01:6e:bd (duplicate use of 1...
19.994012	UDP: 2597 → 29440 Len=44
23.999789	DNS: Standard query 0x4cd2 SRV _sip._udp.sip.cybercity.dk
32.001808	DNS: Standard query 0x57d2 PTR 1.0.0.127.in-addr.arpa

Packet Length:



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	691	144.71	42	1118	0.0004	100%	0.3200	94.154
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	126	57.14	42	76	0.0001	18.23%	0.1900	94.154
80-159	463	89.93	81	146	0.0003	67.00%	0.1300	94.154
160-319	19	217.16	168	243	0.0000	2.75%	0.0800	1444.579
320-639	60	471.17	342	637	0.0000	8.68%	0.0300	1359.198
640-1279	23	815.74	651	1118	0.0000	3.33%	0.0100	49.421
1280-2559	0	-	-	-	0.0000	0.00%	-	-
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

We can see conversions done for each packet with the given size which has a count of more than 5.



Wireshark · Conversations · fuzz-2006-06-26-2594.pcap

Conversation Settings

□ Name resolution

■ Absolute start time

■ Limit to display filter

	Protocol
□	Bluetooth
□	BPv7
□	DCCP
✓	Ethernet
□	FC
□	FDDI
□	IEEE 802.11
□	IEEE 802.15.4
✓	IPv4
✓	IPv6

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s
192.168.1.2	2722	192.136.1.1	53	1	86 bytes	19	1	86 bytes	0	0 bytes	122.333339	0.0000	
192.168.1.2	68	192.168.1.1	67	2	932 bytes	153	1	342 bytes	1	590 bytes	1176.239434	0.0016	
192.168.1.2	2568	192.168.1.1	53	1	86 bytes	170	1	86 bytes	0	0 bytes	1290.676712	0.0000	
192.168.1.2	2597	192.168.1.1	29440	1	86 bytes	8	1	86 bytes	0	0 bytes	19.994012	0.0000	
192.168.1.2	2640	192.168.1.1	53	1	86 bytes	82	1	86 bytes	0	0 bytes	629.807307	0.0000	
192.168.1.2	2684	192.168.1.1	53	1	86 bytes	39	1	86 bytes	0	0 bytes	382.054702	0.0000	
192.168.1.2	2712	192.168.1.1	53	1	76 bytes	2	1	76 bytes	0	0 bytes	10.816999	0.0000	
192.168.1.2	2712	192.168.1.1	49973	1	76 bytes	4	1	76 bytes	0	0 bytes	13.815421	0.0000	
192.168.1.2	2713	192.168.1.1	53	2	172 bytes	6	2	172 bytes	0	0 bytes	14.991319	9.0085	152
192.168.1.2	2714	192.168.1.1	53	2	187 bytes	9	1	82 bytes	1	105 bytes	32.001808	0.0015	
192.168.1.2	2715	192.168.1.1	53	4	344 bytes	12	4	344 bytes	0	0 bytes	32.406750	9.0082	305
192.168.1.2	2716	192.168.1.1	53	2	168 bytes	13	2	168 bytes	0	0 bytes	49.417106	353.9682	3
192.168.1.2	2719	192.168.1.1	53	2	243 bytes	18	1	75 bytes	1	168 bytes	92.989466	1.0117	593
192.168.1.2	2722	192.168.1.1	53	5	426 bytes	20	5	426 bytes	0	0 bytes	123.332668	16.0134	212
192.168.1.2	2724	192.168.1.1	9587	1	86 bytes	22	1	86 bytes	0	0 bytes	139.607704	0.0000	
192.168.1.2	2724	192.168.1.1	53	3	258 bytes	23	3	258 bytes	0	0 bytes	140.607512	8.0115	257
192.168.1.2	2725	192.168.1.1	53	2	187 bytes	26	1	82 bytes	1	105 bytes	156.621191	0.0015	
192.168.1.2	2730	192.168.1.1	43690	1	86 bytes	51	1	86 bytes	0	0 bytes	446.136821	0.0000	
192.168.1.2	2732	192.168.1.1	53	3	258 bytes	29	3	258 bytes	0	0 bytes	289.818491	5.0008	412
192.168.1.2	2734	192.168.1.1	53	4	344 bytes	33	4	344 bytes	0	0 bytes	307.139699	9.0102	305
192.168.1.2	2736	192.168.1.1	53	3	258 bytes	38	3	258 bytes	0	0 bytes	381.058947	9.0072	229
192.168.1.2	2737	192.168.1.1	53	2	187 bytes	41	1	82 bytes	1	105 bytes	398.068101	0.0015	
192.168.1.2	2738	192.168.1.1	53	3	258 bytes	44	3	258 bytes	0	0 bytes	399.379588	8.0115	257
192.168.1.2	2739	192.168.1.1	53	2	187 bytes	45	1	82 bytes	1	105 bytes	415.393125	0.0015	
192.168.1.2	2740	192.168.1.1	53	4	344 bytes	46	4	344 bytes	0	0 bytes	416.106180	9.0104	305