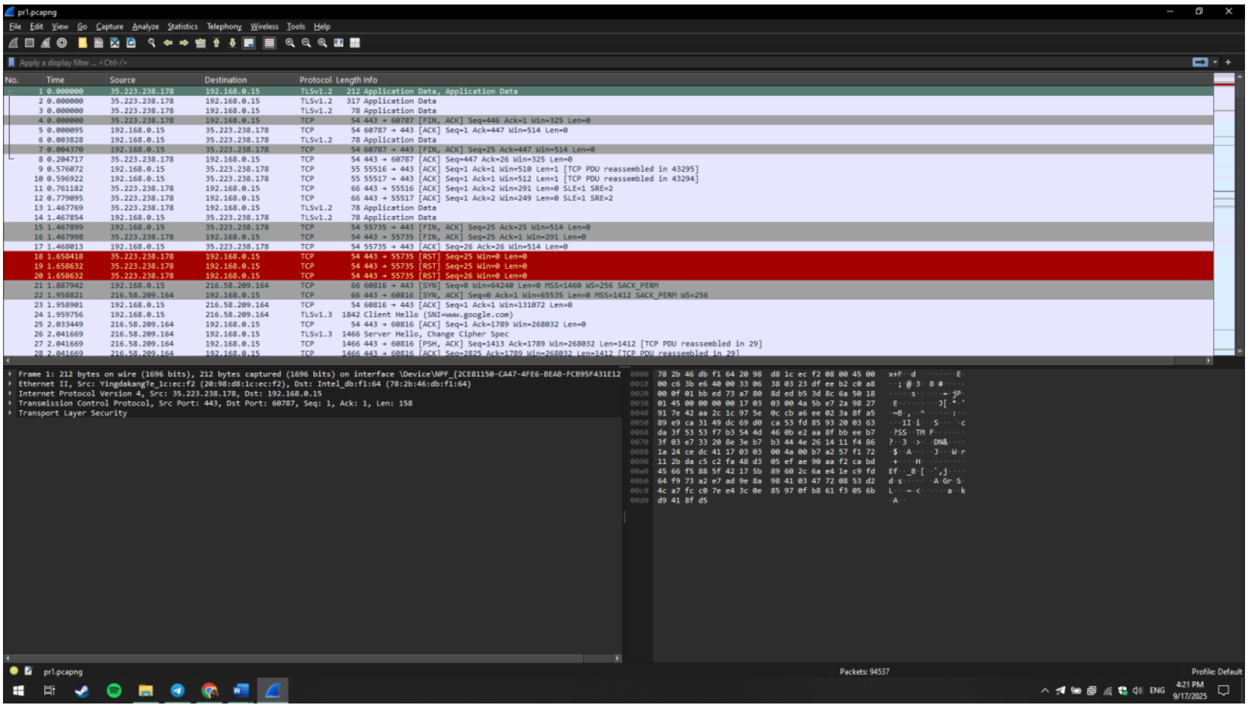
Assignment 1

Topic: Network Traffic Analysis: Packet Capture and Detection of Anomalies/Attacks

Objective:
To gain hands-on experience in capturing and analyzing network traffic, identifying normal communication patterns, and detecting possible anomalies or malicious activities using professional tools.

Tasks

1. **Environment Setup**
   - Wireshark
   - RadminVPN
   - Some RandomVpn
2. **Traffic Capture**

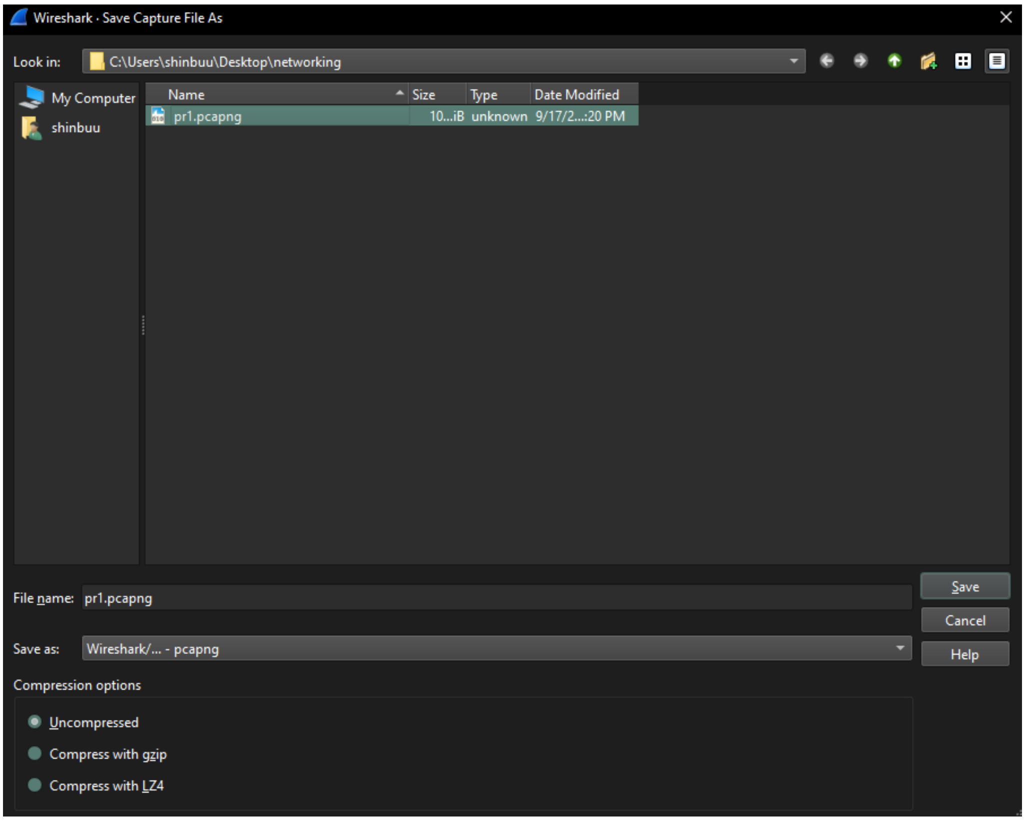

pr1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
pr1.pcapng
Packets: 94537
Profile: Default
ENG
4:21 PM
9/17/2025

```
No.  Time      Source           Destination      Protocol Length Info
   1 0.000000  35.223.238.178   192.168.0.15     TLSv1.2   212 Application Data, Application Data
   2 0.000000  35.223.238.178   192.168.0.15     TLSv1.2   317 Application Data
   3 0.000000  35.223.238.178   192.168.0.15     TLSv1.2    78 Application Data
   4 0.000000  35.223.238.178   192.168.0.15     TCP        54 443 → 60787 [FIN, ACK] Seq=446 Ack=1 Win=325 Len=0
   5 0.000095  192.168.0.15     35.223.238.178   TCP        54 60787 → 443 [ACK] Seq=1 Ack=447 Win=514 Len=0
   6 0.003828  192.168.0.15     35.223.238.178   TLSv1.2    78 Application Data
   7 0.004370  192.168.0.15     35.223.238.178   TCP        54 60787 → 443 [FIN, ACK] Seq=25 Ack=447 Win=514 Len=0
   8 0.204717  35.223.238.178   192.168.0.15     TCP        54 443 → 60787 [ACK] Seq=447 Ack=26 Win=325 Len=0
   9 0.576072  192.168.0.15     35.223.238.178   TCP        55 55516 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP PDU reassembled in 43295]
  10 0.596922  192.168.0.15     35.223.238.178   TCP        55 55517 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP PDU reassembled in 43294]
  11 0.761182  35.223.238.178   192.168.0.15     TCP        66 443 → 55516 [ACK] Seq=1 Ack=2 Win=291 Len=0 SLE=1 SRE=2
  12 0.779095  35.223.238.178   192.168.0.15     TCP        66 443 → 55517 [ACK] Seq=1 Ack=2 Win=249 Len=0 SLE=1 SRE=2
  13 1.467769  35.223.238.178   192.168.0.15     TLSv1.2    78 Application Data
  14 1.467854  192.168.0.15     35.223.238.178   TLSv1.2    78 Application Data
  15 1.467899  192.168.0.15     35.223.238.178   TCP        54 55735 → 443 [FIN, ACK] Seq=25 Ack=25 Win=514 Len=0
  16 1.467998  35.223.238.178   192.168.0.15     TCP        54 443 → 55735 [FIN, ACK] Seq=25 Ack=1 Win=291 Len=0
  17 1.468013  192.168.0.15     35.223.238.178   TCP        54 55735 → 443 [ACK] Seq=26 Ack=26 Win=514 Len=0
  18 1.658418  35.223.238.178   192.168.0.15     TCP        54 443 → 55735 [RST] Seq=25 Win=0 Len=0
  19 1.658632  35.223.238.178   192.168.0.15     TCP        54 443 → 55735 [RST] Seq=25 Win=0 Len=0
  20 1.658632  35.223.238.178   192.168.0.15     TCP        54 443 → 55735 [RST] Seq=26 Win=0 Len=0
  21 1.887942  192.168.0.15     216.58.209.164   TCP        66 60816 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  22 1.958821  216.58.209.164   192.168.0.15     TCP        66 443 → 60816 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
  23 1.958901  192.168.0.15     216.58.209.164   TCP        54 60816 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
  24 1.959756  192.168.0.15     216.58.209.164   TLSv1.3  1842 Client Hello (SNI=www.google.com)
  25 2.033449  216.58.209.164   192.168.0.15     TCP        54 443 → 60816 [ACK] Seq=1 Ack=1789 Win=268032 Len=0
  26 2.041669  216.58.209.164   192.168.0.15     TLSv1.3  1466 Server Hello, Change Cipher Spec
  27 2.041669  216.58.209.164   192.168.0.15     TCP      1466 443 → 60816 [PSH, ACK] Seq=1413 Ack=1789 Win=268032 Len=1412 [TCP PDU reassembled in 29]
  28 2.041669  216.58.209.164   192.168.0.15     TCP      1466 443 → 60816 [ACK] Seq=2825 Ack=1789 Win=268032 Len=1412 [TCP PDU reassembled in 29]
```

```
▸ Frame 1: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on interface \Device\NPF_{2CE81150-CA47-4FE6-BEAB-FCB95F431E12
▸ Ethernet II, Src: YingdakangTe_1c:ec:f2 (20:98:d8:1c:ec:f2), Dst: Intel_db:f1:64 (78:2b:46:db:f1:64)
▸ Internet Protocol Version 4, Src: 35.223.238.178, Dst: 192.168.0.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 60787, Seq: 1, Ack: 1, Len: 158
▸ Transport Layer Security
```

```
0000  78 2b 46 db f1 64 20 98  d8 1c ec f2 08 00 45 00   x+F··d ·······E·
0010  00 c6 3b e6 40 00 33 06  38 03 23 df ee b2 c0 a8   ··;·@·3· 8·#····
0020  00 0f 01 bb ed 73 a7 80  8d ed b5 3d 8c 6a 50 18   ·····s·· ···=·jP·
0030  01 45 00 00 00 00 17 03  03 00 4a 5b e7 2a 98 27   ·E······ ··J[·*·'
0040  91 7e 42 aa 2c 1c 97 5e  0c cb a6 ee 02 3a 8f a5   ·~B·,··^ ·····:··
0050  89 e9 ca 31 49 dc 69 d0  ca 53 fd 85 93 20 03 63   ···1I·i· ·S··· ·c
0060  da 3f 53 53 f7 b3 54 4d  46 0b e2 aa 8f bb ee b7   ·?SS··TM F·······
0070  3f 03 e7 33 20 8e 3e b7  b3 44 4e 26 14 11 f4 86   ?··3 ·>· ·DN&····
0080  1a 24 ce dc 41 17 03 03  00 4a 00 b7 a2 57 f1 72   ·$··A··· ·J···W·r
0090  11 2b da c5 c2 fa 48 d3  05 ef ae 90 aa f2 ca bd   ·+····H· ········
00a0  45 66 f5 88 5f 42 17 5b  89 60 2c 6a e4 1e c9 fd   Ef··_B·[ ·`,j····
00b0  64 f9 73 a2 e7 ad 9e 8a  98 41 03 47 72 08 53 d2   d·s····· ·A·Gr·S·
00c0  4c a7 fc c0 7e e4 3c 0e  85 97 0f b8 61 f3 05 6b   L···~·<· ····a··k
00d0  d9 41 8f d5                                        ·A··
```

   - Capture traffic from your own machine for at least 5 minutes (web browsing, file downloads, DNS requests).
   - Save the capture file in `.pcap` format.


Wireshark · Save Capture File As

Look in: C:\Users\shinbuu\Desktop\networking

My Computer

shinbuu

Name	Size	Type	Date Modified
pr1.pcapng	10...iB	unknown	9/17/2...:20 PM

File name: pr1.pcapng

Save as: Wireshark/... - pcapng

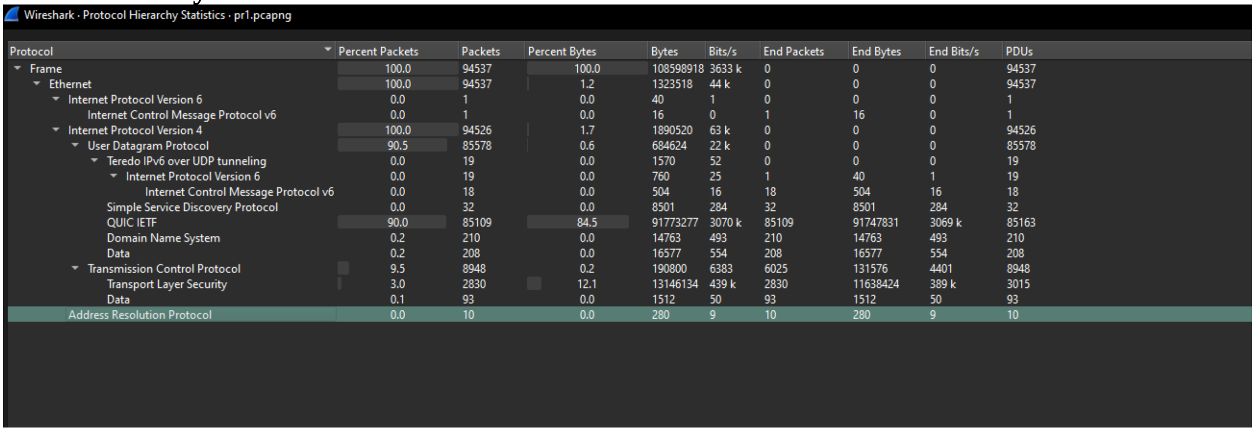
Compression options

● Uncompressed

○ Compress with gzip

○ Compress with LZ4

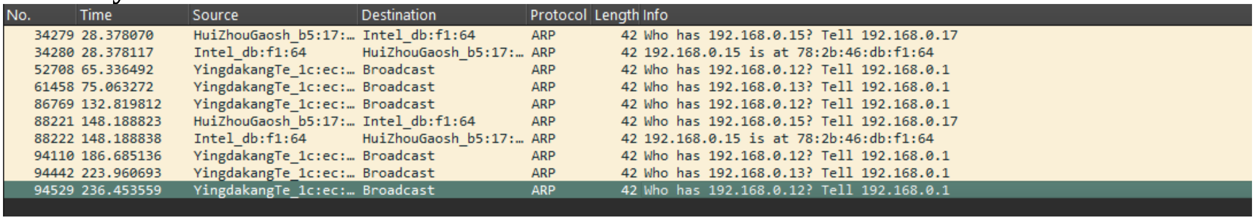
3. **Protocol Analysis**

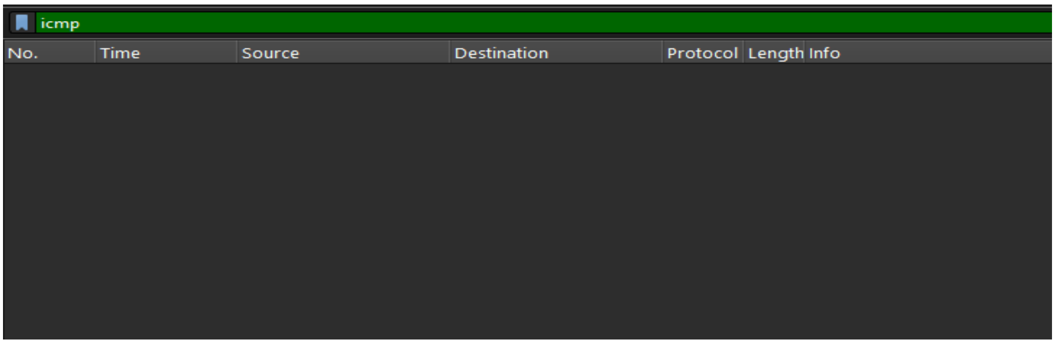

Wireshark · Protocol Hierarchy Statistics · pr1.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	94537	100.0	108598918	3633 k	0	0	0	94537
Ethernet	100.0	94537	1.2	1323518	44 k	0	0	0	94537
Internet Protocol Version 6	0.0	1	0.0	40	1	0	0	0	1
Internet Control Message Protocol v6	0.0	1	0.0	16	0	1	16	0	1
Internet Protocol Version 4	100.0	94526	1.7	1890520	63 k	0	0	0	94526
User Datagram Protocol	90.5	85578	0.6	684624	22 k	0	0	0	85578
Teredo IPv6 over UDP tunneling	0.0	19	0.0	1570	52	0	0	0	19
Internet Protocol Version 6	0.0	19	0.0	760	25	1	40	1	19
Internet Control Message Protocol v6	0.0	18	0.0	504	16	18	504	16	18
Simple Service Discovery Protocol	0.0	32	0.0	8501	284	32	8501	284	32
QUIC IETF	90.0	85109	84.5	91773277	3070 k	85109	91747831	3069 k	85163
Domain Name System	0.2	210	0.0	14763	493	210	14763	493	210
Data	0.2	208	0.0	16577	554	208	16577	554	208
Transmission Control Protocol	9.5	8948	0.2	190800	6383	6025	131576	4401	8948
Transport Layer Security	3.0	2830	12.1	13146134	439 k	2830	11638424	389 k	3015
Data	0.1	93	0.0	1512	50	93	1512	50	93
Address Resolution Protocol	0.0	10	0.0	280	9	10	280	9	10

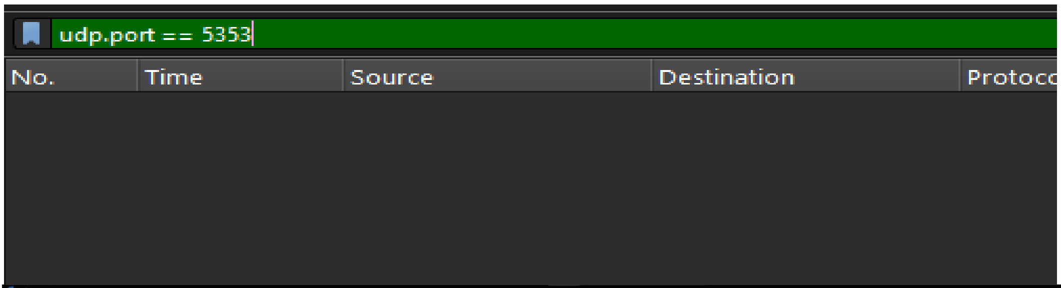
- Identify the most frequent protocols in the captured data (HTTP/HTTPS, DNS, ARP, ICMP, etc.).
- Create a short summary table (protocol → percentage of traffic).

4. **Anomaly / Attack Detection**

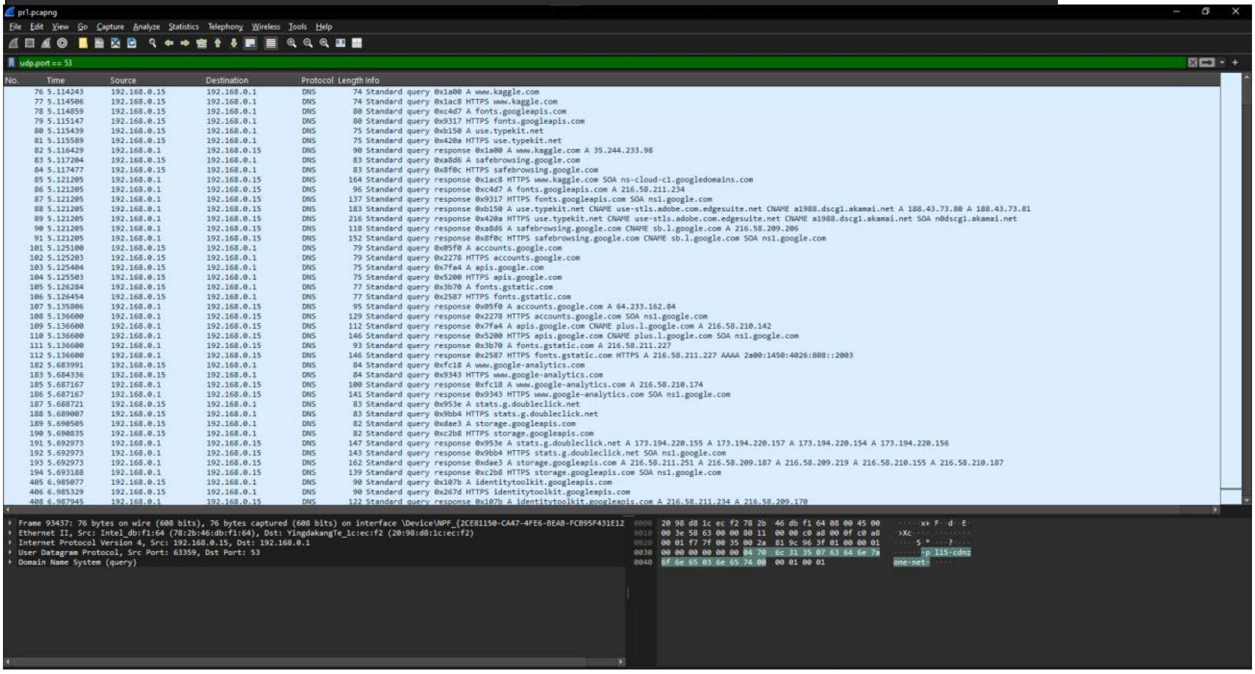

No.	Time	Source	Destination	Protocol	Length	Info
34279	28.378070	HuiZhouGaosh_b5:17:…	Intel_db:f1:64	ARP	42	Who has 192.168.0.15? Tell 192.168.0.17
34280	28.378117	Intel_db:f1:64	HuiZhouGaosh_b5:17:…	ARP	42	192.168.0.15 is at 78:2b:46:db:f1:64
52708	65.336492	YingdakangTe_1c:ec:…	Broadcast	ARP	42	Who has 192.168.0.12? Tell 192.168.0.1
61458	75.063272	YingdakangTe_1c:ec:…	Broadcast	ARP	42	Who has 192.168.0.13? Tell 192.168.0.1
86769	132.819812	YingdakangTe_1c:ec:…	Broadcast	ARP	42	Who has 192.168.0.12? Tell 192.168.0.1
88221	148.188823	HuiZhouGaosh_b5:17:…	Intel_db:f1:64	ARP	42	Who has 192.168.0.15? Tell 192.168.0.17
88222	148.188838	Intel_db:f1:64	HuiZhouGaosh_b5:17:…	ARP	42	192.168.0.15 is at 78:2b:46:db:f1:64
94110	186.685136	YingdakangTe_1c:ec:…	Broadcast	ARP	42	Who has 192.168.0.12? Tell 192.168.0.1
94442	223.960693	YingdakangTe_1c:ec:…	Broadcast	ARP	42	Who has 192.168.0.13? Tell 192.168.0.1
94529	236.453559	YingdakangTe_1c:ec:…	Broadcast	ARP	42	Who has 192.168.0.12? Tell 192.168.0.1



```
icmp
No.    Time    Source    Destination    Protocol  Length  Info
```



```
udp.port == 5353
No.    Time    Source    Destination    Protocc
```



pr1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port == 53
No.   Time       Source          Destination     Protocol Length Info
   76 5.114243   192.168.0.15    192.168.0.1     DNS       74 Standard query 0x1a00 A www.kaggle.com
   77 5.114506   192.168.0.15    192.168.0.1     DNS       74 Standard query 0x1ac8 HTTPS www.kaggle.com
   78 5.114859   192.168.0.15    192.168.0.1     DNS       80 Standard query 0xc4d7 A fonts.googleapis.com
   79 5.115147   192.168.0.15    192.168.0.1     DNS       80 Standard query 0x9317 HTTPS fonts.googleapis.com
   80 5.115439   192.168.0.15    192.168.0.1     DNS       75 Standard query 0xb150 A use.typekit.net
   81 5.115589   192.168.0.15    192.168.0.1     DNS       75 Standard query 0x420a HTTPS use.typekit.net
   82 5.116429   192.168.0.1     192.168.0.15    DNS       90 Standard query response 0x1a00 A www.kaggle.com A 35.244.233.98
   83 5.117204   192.168.0.15    192.168.0.1     DNS       83 Standard query 0xa8d6 A safebrowsing.google.com
   84 5.117477   192.168.0.15    192.168.0.1     DNS       83 Standard query 0x8f0c HTTPS safebrowsing.google.com
   85 5.121205   192.168.0.1     192.168.0.15    DNS      164 Standard query response 0x1ac8 HTTPS www.kaggle.com SOA ns-cloud-c1.googledomains.com
   86 5.121205   192.168.0.1     192.168.0.15    DNS       96 Standard query response 0xc4d7 A fonts.googleapis.com A 216.58.211.234
   87 5.121205   192.168.0.1     192.168.0.15    DNS      137 Standard query response 0x9317 HTTPS fonts.googleapis.com SOA ns1.google.com
   88 5.121205   192.168.0.1     192.168.0.15    DNS      183 Standard query response 0xb150 A use.typekit.net CNAME use-stls.adobe.com.edgesuite.net CNAME a1988.dscg1.akamai.net A 188.43.73.80 A 188.43.73.81
   89 5.121205   192.168.0.1     192.168.0.15    DNS      216 Standard query response 0x420a HTTPS use.typekit.net CNAME use-stls.adobe.com.edgesuite.net CNAME a1988.dscg1.akamai.net SOA n0dscg1.akamai.net
   90 5.121205   192.168.0.1     192.168.0.15    DNS      118 Standard query response 0xa8d6 A safebrowsing.google.com CNAME sb.l.google.com A 216.58.209.206
   91 5.121205   192.168.0.1     192.168.0.15    DNS      152 Standard query response 0x8f0c HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
  101 5.125100   192.168.0.15    192.168.0.1     DNS       79 Standard query 0x05f0 A accounts.google.com
  102 5.125203   192.168.0.15    192.168.0.1     DNS       79 Standard query 0x2278 HTTPS accounts.google.com
  103 5.125404   192.168.0.15    192.168.0.1     DNS       75 Standard query 0x7fa4 A apis.google.com
  104 5.125503   192.168.0.15    192.168.0.1     DNS       75 Standard query 0x5200 HTTPS apis.google.com
  105 5.126284   192.168.0.15    192.168.0.1     DNS       77 Standard query 0x3b70 A fonts.gstatic.com
  106 5.126454   192.168.0.15    192.168.0.1     DNS       77 Standard query 0x2587 HTTPS fonts.gstatic.com
  107 5.135806   192.168.0.1     192.168.0.15    DNS       95 Standard query response 0x05f0 A accounts.google.com A 64.233.162.84
  108 5.136600   192.168.0.1     192.168.0.15    DNS      129 Standard query response 0x2278 HTTPS accounts.google.com SOA ns1.google.com
  109 5.136600   192.168.0.1     192.168.0.15    DNS      112 Standard query response 0x7fa4 A apis.google.com CNAME plus.l.google.com A 216.58.210.142
  110 5.136600   192.168.0.1     192.168.0.15    DNS      146 Standard query response 0x5200 HTTPS apis.google.com CNAME plus.l.google.com SOA ns1.google.com
  111 5.136600   192.168.0.1     192.168.0.15    DNS       93 Standard query response 0x3b70 A fonts.gstatic.com A 216.58.211.227
  112 5.136600   192.168.0.1     192.168.0.15    DNS      146 Standard query response 0x2587 HTTPS fonts.gstatic.com HTTPS A 216.58.211.227 AAAA 2a00:1450:4026:808::2003
  182 5.683991   192.168.0.15    192.168.0.1     DNS       84 Standard query 0xfc18 A www.google-analytics.com
  183 5.684336   192.168.0.15    192.168.0.1     DNS       84 Standard query 0x9343 HTTPS www.google-analytics.com
  185 5.687167   192.168.0.1     192.168.0.15    DNS      100 Standard query response 0xfc18 A www.google-analytics.com A 216.58.210.174
  186 5.687167   192.168.0.1     192.168.0.15    DNS      141 Standard query response 0x9343 HTTPS www.google-analytics.com SOA ns1.google.com
  187 5.688721   192.168.0.15    192.168.0.1     DNS       83 Standard query 0x953e A stats.g.doubleclick.net
  188 5.689007   192.168.0.15    192.168.0.1     DNS       83 Standard query 0x9bb4 HTTPS stats.g.doubleclick.net
  189 5.690505   192.168.0.15    192.168.0.1     DNS       82 Standard query 0xdae3 A storage.googleapis.com
  190 5.690835   192.168.0.15    192.168.0.1     DNS       82 Standard query 0xc2b8 HTTPS storage.googleapis.com
  191 5.692973   192.168.0.1     192.168.0.15    DNS      147 Standard query response 0x953e A stats.g.doubleclick.net A 173.194.220.155 A 173.194.220.157 A 173.194.220.154 A 173.194.220.156
  192 5.692973   192.168.0.1     192.168.0.15    DNS      143 Standard query response 0x9bb4 HTTPS stats.g.doubleclick.net SOA ns1.google.com
  193 5.692973   192.168.0.1     192.168.0.15    DNS      162 Standard query response 0xdae3 A storage.googleapis.com A 216.58.211.251 A 216.58.209.187 A 216.58.209.219 A 216.58.210.155 A 216.58.210.187
  194 5.693188   192.168.0.1     192.168.0.15    DNS      139 Standard query response 0xc2b8 HTTPS storage.googleapis.com SOA ns1.google.com
  405 6.985077   192.168.0.15    192.168.0.1     DNS       90 Standard query 0x107b A identitytoolkit.googleapis.com
  406 6.985329   192.168.0.15    192.168.0.1     DNS       90 Standard query 0x267d HTTPS identitytoolkit.googleapis.com
  408 6.987945   192.168.0.1     192.168.0.15    DNS      122 Standard query response 0x107b A identitytoolkit.googleapis.com A 216.58.211.234 A 216.58.209.170
```

```
> Frame 93437: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{2CE81150-CA47-4FE6-BEA8-FCB95F431E12
> Ethernet II, Src: Intel_db:f1:64 (78:2b:46:db:f1:64), Dst: YingdakangTe_1c:ec:f2 (20:98:d8:1c:ec:f2)
> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 63359, Dst Port: 53
> Domain Name System (query)
```

```
0000  20 98 d8 1c ec f2 78 2b  46 db f1 64 08 00 45 00   ······x+F··d··E·
0010  00 3e 58 63 00 00 80 11  00 00 c0 a8 00 0f c0 a8   ·>Xc············
0020  00 01 f7 7f 00 35 00 2a  81 9c 96 3f 01 00 00 01   ·····5·*···?····
0030  00 00 00 00 00 00 04 70  6c 31 35 07 63 64 6e 7a   ·······p l15·cdnz
0040  6f 6e 65 03 6e 65 74 00  00 01 00 01               one·net·····
```

- Detect at least two anomalies in the traffic (e.g., repeated failed DNS requests, ARP spoofing attempts, unusual port scanning activity).
- Mark suspicious flows and justify why they may indicate malicious activity.