LAB - 13

Aim :- Analyzing network traffic on mobile and IoT devices to identify potential security risks.

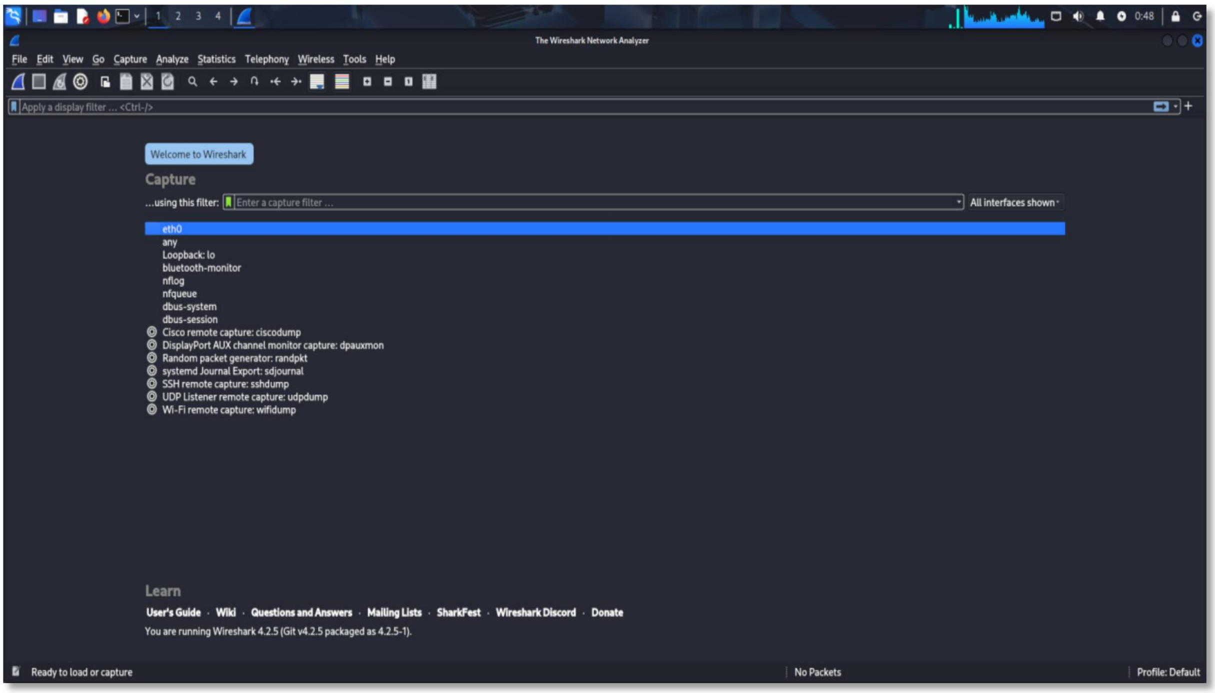
Definition:

Analyzing network traffic on mobile and IoT devices to identify potential security risks involves monitoring and inspecting the data packets exchanged between a device (mobile or IoT) and external servers, networks, or other devices. This analysis helps identify vulnerabilities or malicious activities, such as unsecured data transmission, unauthorized access attempts, or communication with known malicious IP addresses. The goal is to assess the device's communication and ensure data confidentiality, integrity, and proper authentication.

To understand how to capture and analyze network traffic from mobile devices (and simulate IoT traffic) to detect potential security threats.

Tools Used:

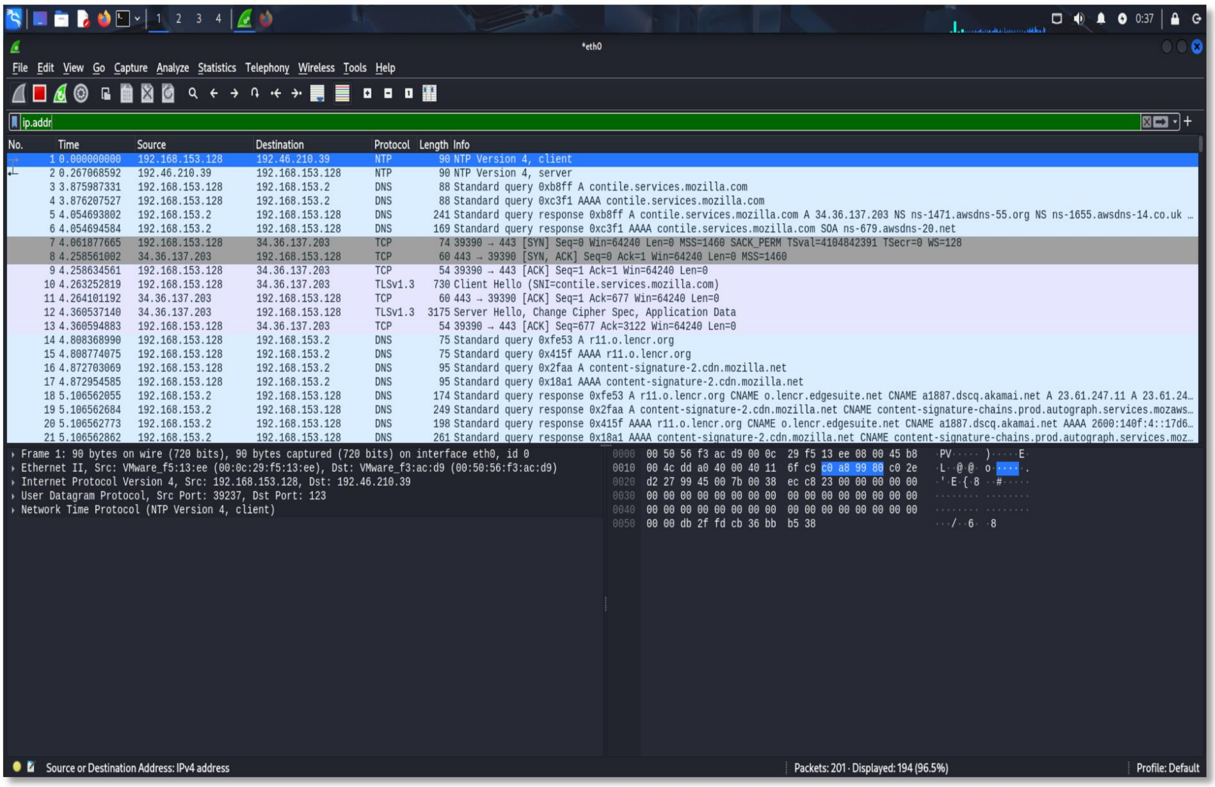
→ Wireshark (for packet capture and analysis)
→ Android phone (connected to same Wi-Fi network)
→ Windows/Linux PC (running Wireshark)
→ (No real IoT devices used – IoT traffic is simulated)



eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

You are running Wireshark 4.2.5 (Git v4.2.5 packaged as 4.2.5-1).

Ready to load or capture | No Packets | Profile: Default

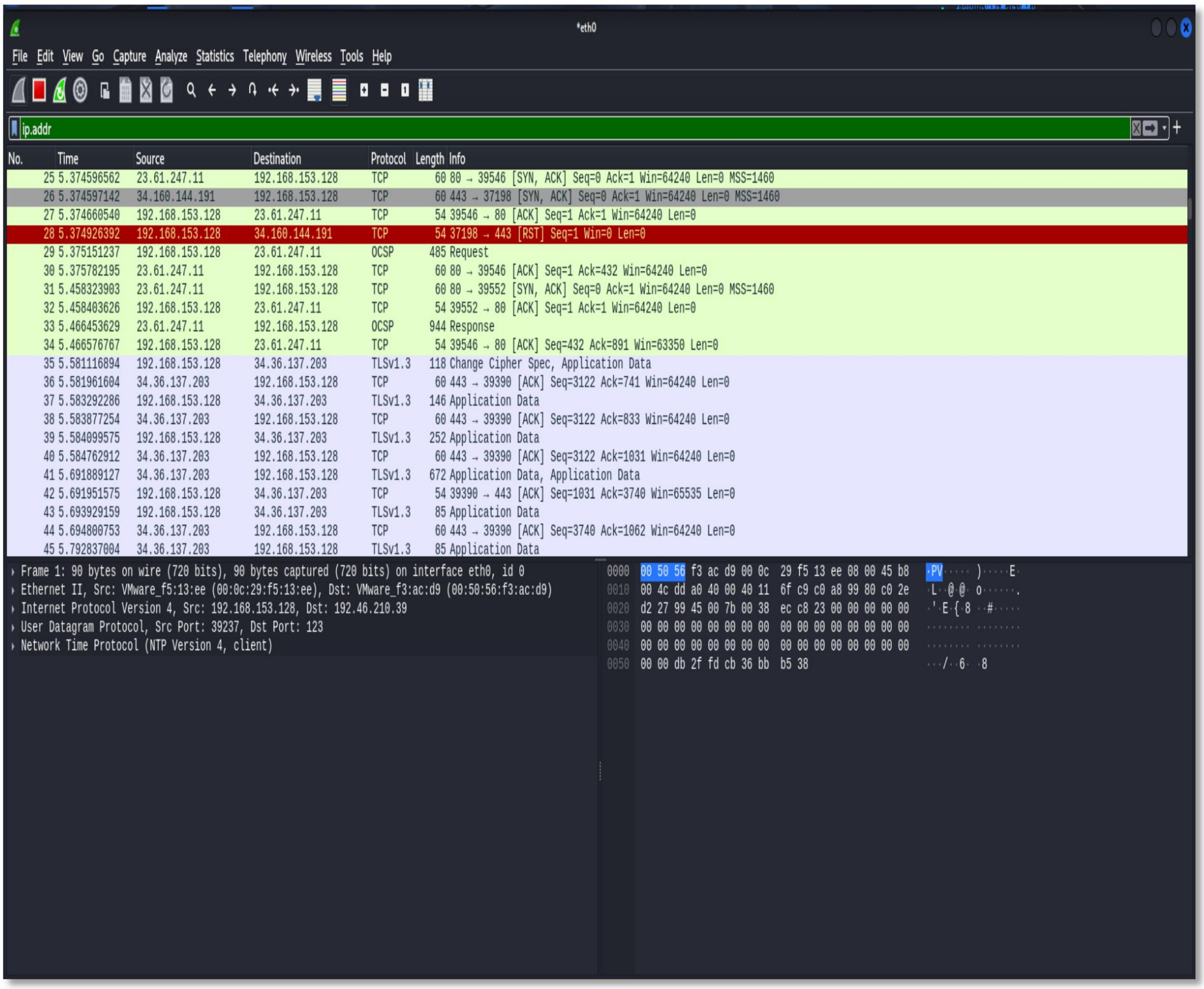

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr

```
No.  Time         Source           Destination      Protocol Length Info
   1 0.000000000  192.168.153.128  192.46.210.39    NTP        90 NTP Version 4, client
   2 0.267068592  192.46.210.39    192.168.153.128  NTP        90 NTP Version 4, server
   3 3.875987331  192.168.153.128  192.168.153.2    DNS        88 Standard query 0xb8ff A contile.services.mozilla.com
   4 3.876207527  192.168.153.128  192.168.153.2    DNS        88 Standard query 0xc3f1 AAAA contile.services.mozilla.com
   5 4.054693802  192.168.153.2    192.168.153.128  DNS       241 Standard query response 0xb8ff A contile.services.mozilla.com A 34.36.137.203 NS ns-1471.awsdns-55.org NS ns-1655.awsdns-14.co.uk …
   6 4.054694584  192.168.153.2    192.168.153.128  DNS       169 Standard query response 0xc3f1 AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net
   7 4.061877665  192.168.153.128  34.36.137.203    TCP        74 39390 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4104842391 TSecr=0 WS=128
   8 4.258561002  34.36.137.203    192.168.153.128  TCP        60 443 → 39390 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   9 4.258634561  192.168.153.128  34.36.137.203    TCP        54 39390 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  10 4.263252819  192.168.153.128  34.36.137.203    TLSv1.3   730 Client Hello (SNI=contile.services.mozilla.com)
  11 4.264101192  34.36.137.203    192.168.153.128  TCP        60 443 → 39390 [ACK] Seq=1 Ack=677 Win=64240 Len=0
  12 4.360537140  34.36.137.203    192.168.153.128  TLSv1.3  3175 Server Hello, Change Cipher Spec, Application Data
  13 4.360594883  192.168.153.128  34.36.137.203    TCP        54 39390 → 443 [ACK] Seq=677 Ack=3122 Win=64240 Len=0
  14 4.808368990  192.168.153.128  192.168.153.2    DNS        75 Standard query 0xfe53 A r11.o.lencr.org
  15 4.808774075  192.168.153.128  192.168.153.2    DNS        75 Standard query 0x415f AAAA r11.o.lencr.org
  16 4.872703069  192.168.153.128  192.168.153.2    DNS        95 Standard query 0x2faa A content-signature-2.cdn.mozilla.net
  17 4.872954585  192.168.153.128  192.168.153.2    DNS        95 Standard query 0x18a1 AAAA content-signature-2.cdn.mozilla.net
  18 5.106562055  192.168.153.2    192.168.153.128  DNS       174 Standard query response 0xfe53 A r11.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.net A 23.61.247.11 A 23.61.24…
  19 5.106562684  192.168.153.2    192.168.153.128  DNS       249 Standard query response 0x2faa A content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.services.mozaws…
  20 5.106562773  192.168.153.2    192.168.153.128  DNS       198 Standard query response 0x415f AAAA r11.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.net AAAA 2600:140f:4::17d6…
  21 5.106562862  192.168.153.2    192.168.153.128  DNS       261 Standard query response 0x18a1 AAAA content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.autograph.services.moz…
```

```
› Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_f5:13:ee (00:0c:29:f5:13:ee), Dst: VMware_f3:ac:d9 (00:50:56:f3:ac:d9)
› Internet Protocol Version 4, Src: 192.168.153.128, Dst: 192.46.210.39
› User Datagram Protocol, Src Port: 39237, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)
```

```
0000  00 50 56 f3 ac d9 00 0c  29 f5 13 ee 08 00 45 b8   ·PV·····)·····E·
0010  00 4c dd a0 40 00 40 11  6f c9 c0 a8 99 80 c0 2e   ·L··@·@·o·······.
0020  d2 27 99 45 00 7b 00 38  ec c8 23 00 00 00 00 00   ·'·E·{·8··#·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0050  00 00 db 2f fd cb 36 bb  b5 38                     ···/··6··8
```

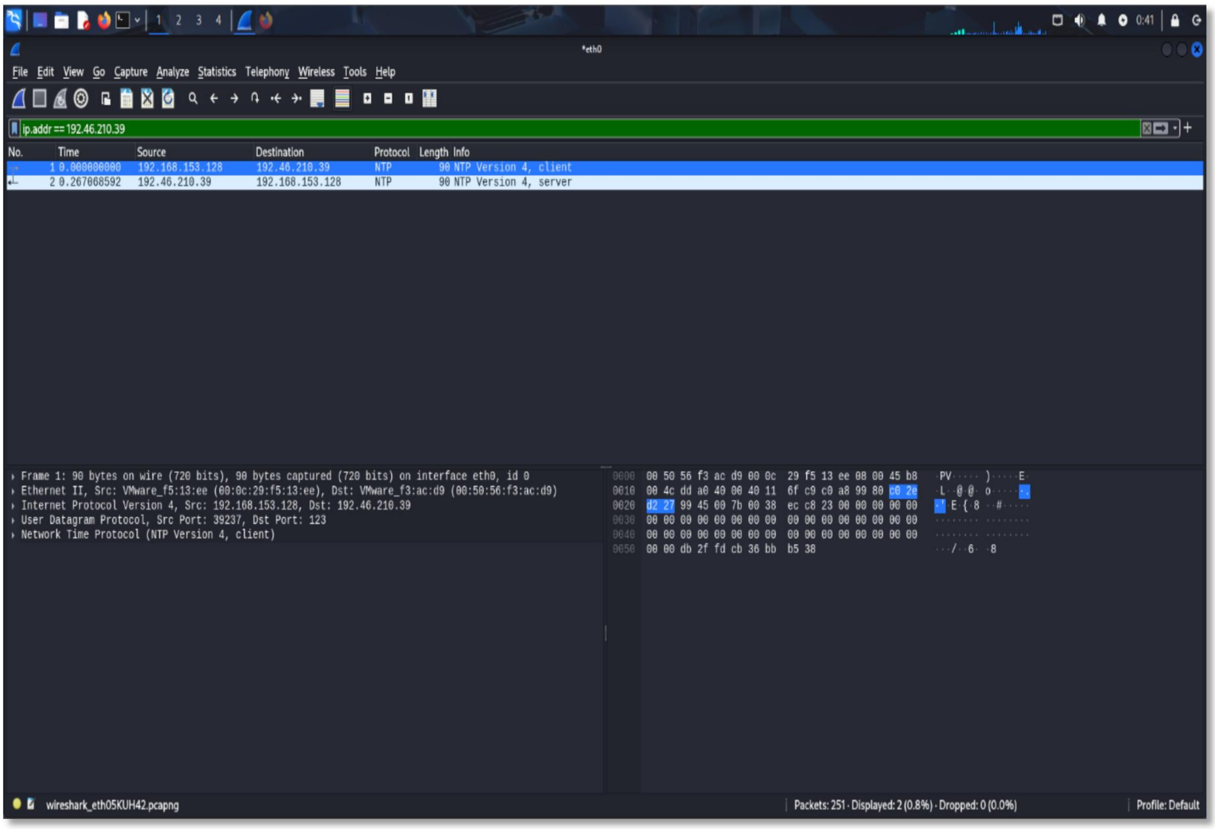
Source or Destination Address: IPv4 address | Packets: 201 · Displayed: 194 (96.5%) | Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr

```
No.  Time         Source           Destination      Protocol Length Info
  25 5.374596562  23.61.247.11     192.168.153.128  TCP        60 80 → 39546 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  26 5.374597142  34.160.144.191   192.168.153.128  TCP        60 443 → 37198 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  27 5.374660540  192.168.153.128  23.61.247.11     TCP        54 39546 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  28 5.374926392  192.168.153.128  34.160.144.191   TCP        54 37198 → 443 [RST] Seq=1 Win=0 Len=0
  29 5.375151237  192.168.153.128  23.61.247.11     OCSP      485 Request
  30 5.375782195  23.61.247.11     192.168.153.128  TCP        60 80 → 39546 [ACK] Seq=1 Ack=432 Win=64240 Len=0
  31 5.458323903  23.61.247.11     192.168.153.128  TCP        60 80 → 39552 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  32 5.458403626  192.168.153.128  23.61.247.11     TCP        54 39552 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  33 5.466453629  23.61.247.11     192.168.153.128  OCSP      944 Response
  34 5.466576767  192.168.153.128  23.61.247.11     TCP        54 39546 → 80 [ACK] Seq=432 Ack=891 Win=63350 Len=0
  35 5.581116894  192.168.153.128  34.36.137.203    TLSv1.3   118 Change Cipher Spec, Application Data
  36 5.581961604  34.36.137.203    192.168.153.128  TCP        60 443 → 39390 [ACK] Seq=3122 Ack=741 Win=64240 Len=0
  37 5.583292286  192.168.153.128  34.36.137.203    TLSv1.3   146 Application Data
  38 5.583877254  34.36.137.203    192.168.153.128  TCP        60 443 → 39390 [ACK] Seq=3122 Ack=833 Win=64240 Len=0
  39 5.584099575  192.168.153.128  34.36.137.203    TLSv1.3   252 Application Data
  40 5.584762912  34.36.137.203    192.168.153.128  TCP        60 443 → 39390 [ACK] Seq=3122 Ack=1031 Win=64240 Len=0
  41 5.691889127  34.36.137.203    192.168.153.128  TLSv1.3   672 Application Data, Application Data
  42 5.691951575  192.168.153.128  34.36.137.203    TCP        54 39390 → 443 [ACK] Seq=1031 Ack=3740 Win=65535 Len=0
  43 5.693929159  192.168.153.128  34.36.137.203    TLSv1.3    85 Application Data
  44 5.694800753  34.36.137.203    192.168.153.128  TCP        60 443 → 39390 [ACK] Seq=3740 Ack=1062 Win=64240 Len=0
  45 5.792837004  34.36.137.203    192.168.153.128  TLSv1.3    85 Application Data
```

```
› Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_f5:13:ee (00:0c:29:f5:13:ee), Dst: VMware_f3:ac:d9 (00:50:56:f3:ac:d9)
› Internet Protocol Version 4, Src: 192.168.153.128, Dst: 192.46.210.39
› User Datagram Protocol, Src Port: 39237, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)
```

```
0000  00 50 56 f3 ac d9 00 0c  29 f5 13 ee 08 00 45 b8   ·PV·····)·····E·
0010  00 4c dd a0 40 00 40 11  6f c9 c0 a8 99 80 c0 2e   ·L··@·@·o·······.
0020  d2 27 99 45 00 7b 00 38  ec c8 23 00 00 00 00 00   ·'·E·{·8··#·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0050  00 00 db 2f fd cb 36 bb  b5 38                     ···/··6··8
```



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.46.210.39

```
No.   Time          Source            Destination       Protocol  Length Info
    1 0.000000000   192.168.153.128   192.46.210.39     NTP           90 NTP Version 4, client
    2 0.267068592   192.46.210.39     192.168.153.128   NTP           90 NTP Version 4, server
```

```
› Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_f5:13:ee (00:0c:29:f5:13:ee), Dst: VMware_f3:ac:d9 (00:50:56:f3:ac:d9)
› Internet Protocol Version 4, Src: 192.168.153.128, Dst: 192.46.210.39
› User Datagram Protocol, Src Port: 39237, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)
```

```
0000  00 50 56 f3 ac d9 00 0c  29 f5 13 ee 08 00 45 b8   ·PV·····)·····E·
0010  00 4c dd a0 40 00 40 11  6f c9 c0 a8 99 80 c0 2e   ·L··@·@·o·······.
0020  d2 27 99 45 00 7b 00 38  ec c8 23 00 00 00 00 00   ·'·E·{·8··#·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0050  00 00 db 2f fd cb 36 bb  b5 38                     ···/··6··8
```

wireshark_eth05KUH42.pcapng | Packets: 251 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

Conclusion :-

Analyzing network traffic on mobile and IoT devices is a critical step in identifying potential security risks. By using tools like Wireshark, Fiddler, tcpdump, or Burp Suite, security analysts can monitor communication between devices and external servers, ensuring that sensitive data is not exposed, malicious activity is detected, and communication is properly secured. This process helps in detecting issues like unencrypted traffic, weak authentication, or unauthorized access, which are critical for maintaining the security and integrity of devices and networks.