Cyber Security Internship Report

Cyber Security Internship – Task 3

Networking Basics for Cyber Security

Submitted by: Hetal Antala

Date : 19 / 01 / 2026

1. Introduction

Networking is a fundamental concept in Cyber Security. Understanding how data flows across a network helps security professionals detect attacks, analyze suspicious traffic, and protect systems from threats.

This task focuses on learning basic networking concepts and performing live network traffic analysis using packet sniffing tools.

2. Objective

The main objectives of this task are:

- To understand basic networking concepts such as IP, MAC, DNS, TCP, and UDP
- To capture and analyze live network traffic
- To observe TCP three-way handshake
- To identify plain-text and encrypted traffic
- To analyze DNS queries
- To gain hands-on experience with Wireshark

3. Tools Used

Tool	Purpose
Wireshark	Packet capture and analysis
Web Browser	Generating HTTP/HTTPS traffic
Command Prompt	Generating network traffic using ping

4. Basic Networking Concepts

4.1 IP Address

An IP address is a unique identifier assigned to each device connected to a network.

4.2 MAC Address

A MAC address is a physical hardware address assigned to a network interface.

4.3 TCP (Transmission Control Protocol)

TCP is a reliable, connection-oriented protocol that ensures data is delivered correctly.

4.4 UDP (User Datagram Protocol)

UDP is a fast, connectionless protocol used when speed is more important than reliability.

4.5 DNS (Domain Name System)

DNS converts human-readable domain names (example.com) into IP addresses.

---

5. Packet Sniffing

Packet sniffing is the process of capturing and analyzing network packets to understand network behavior and detect security issues. Wireshark was used to perform packet sniffing in this task.

---

6. Practical Implementation

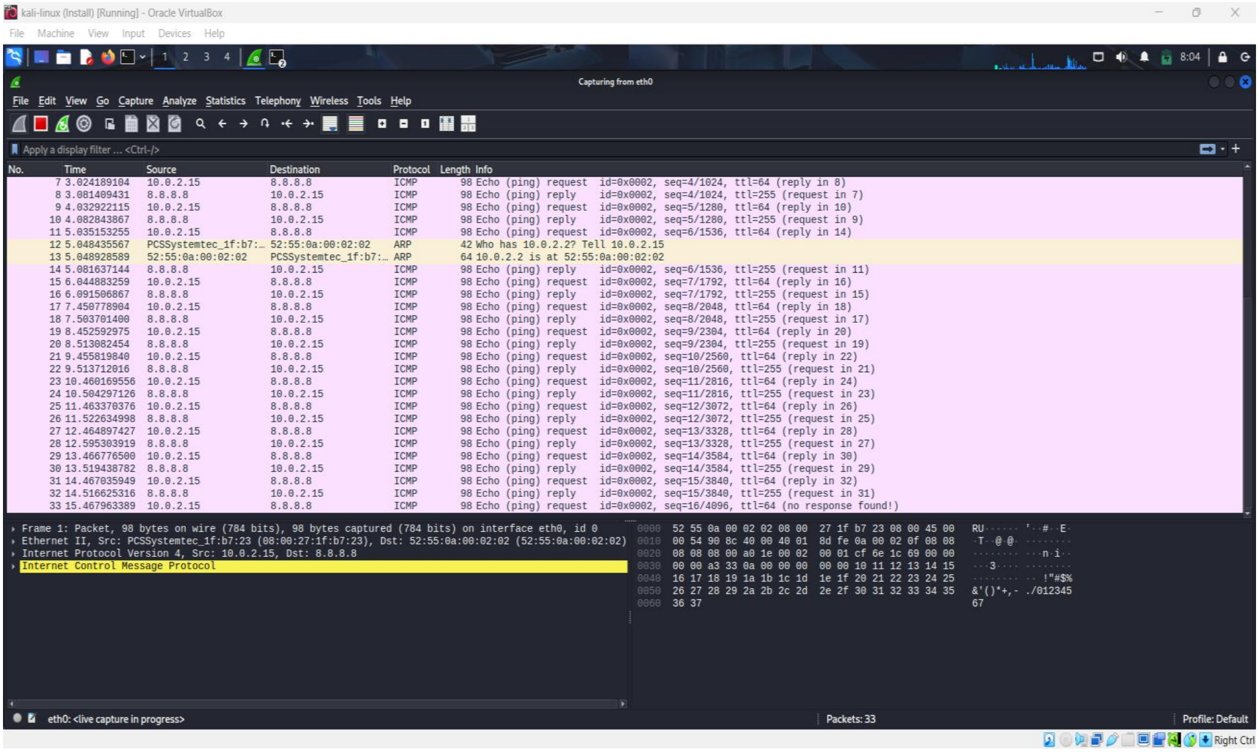
6.1 Capturing Network Traffic

- Wireshark was launched
- Active network interface (Wi-Fi/Ethernet) was selected
- Live network traffic capture was started
- Websites were accessed and ping commands were executed
- Capture was stopped after generating sufficient traffic

---

7. Analysis and Observations

7.1 ICMP Traffic Analysis (Ping Packets)


kali-linux (Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Right Ctrl

```
No.     Time           Source               Destination          Protocol  Length Info
      7 3.024189104    10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=4/1024, ttl=64 (reply in 8)
      8 3.081409431    8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=4/1024, ttl=255 (request in 7)
      9 4.032922115    10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=5/1280, ttl=64 (reply in 10)
     10 4.082843867    8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=5/1280, ttl=255 (request in 9)
     11 5.035153255    10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=6/1536, ttl=64 (reply in 14)
     12 5.048435567    PCSSystemtec_1f:b7:… 52:55:0a:00:02:02    ARP       42 Who has 10.0.2.2? Tell 10.0.2.15
     13 5.048928589    52:55:0a:00:02:02    PCSSystemtec_1f:b7:… ARP       64 10.0.2.2 is at 52:55:0a:00:02:02
     14 5.081637144    8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=6/1536, ttl=255 (request in 11)
     15 6.044883259    10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=7/1792, ttl=64 (reply in 16)
     16 6.091506867    8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=7/1792, ttl=255 (request in 15)
     17 7.450778904    10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=8/2048, ttl=64 (reply in 18)
     18 7.503701400    8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=8/2048, ttl=255 (request in 17)
     19 8.452592975    10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=9/2304, ttl=64 (reply in 20)
     20 8.513082454    8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=9/2304, ttl=255 (request in 19)
     21 9.455819840    10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=10/2560, ttl=64 (reply in 22)
     22 9.513712016    8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=10/2560, ttl=255 (request in 21)
     23 10.460169556   10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=11/2816, ttl=64 (reply in 24)
     24 10.504297126   8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=11/2816, ttl=255 (request in 23)
     25 11.463370376   10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=12/3072, ttl=64 (reply in 26)
     26 11.522634998   8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=12/3072, ttl=255 (request in 25)
     27 12.464897427   10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=13/3328, ttl=64 (reply in 28)
     28 12.595303919   8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=13/3328, ttl=255 (request in 27)
     29 13.466776500   10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=14/3584, ttl=64 (reply in 30)
     30 13.519438782   8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=14/3584, ttl=255 (request in 29)
     31 14.467035949   10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=15/3840, ttl=64 (reply in 32)
     32 14.516625316   8.8.8.8              10.0.2.15            ICMP      98 Echo (ping) reply    id=0x0002, seq=15/3840, ttl=255 (request in 31)
     33 15.467963389   10.0.2.15            8.8.8.8              ICMP      98 Echo (ping) request  id=0x0002, seq=16/4096, ttl=64 (no response found!)
```

```
› Frame 1: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
› Internet Control Message Protocol
```

```
0000  52 55 0a 00 02 02 08 00  27 1f b7 23 08 00 45 00   RU······'··#··E·
0010  00 54 90 8c 40 00 40 01  8d fe 0a 00 02 0f 08 08   ·T··@·@·········
0020  08 08 08 00 a0 1e 00 02  00 01 cf 6e 1c 69 00 00   ···········n·i··
0030  00 00 a3 33 0a 00 00 00  00 00 10 11 12 13 14 15   ···3············
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ·········· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37                                              67
```

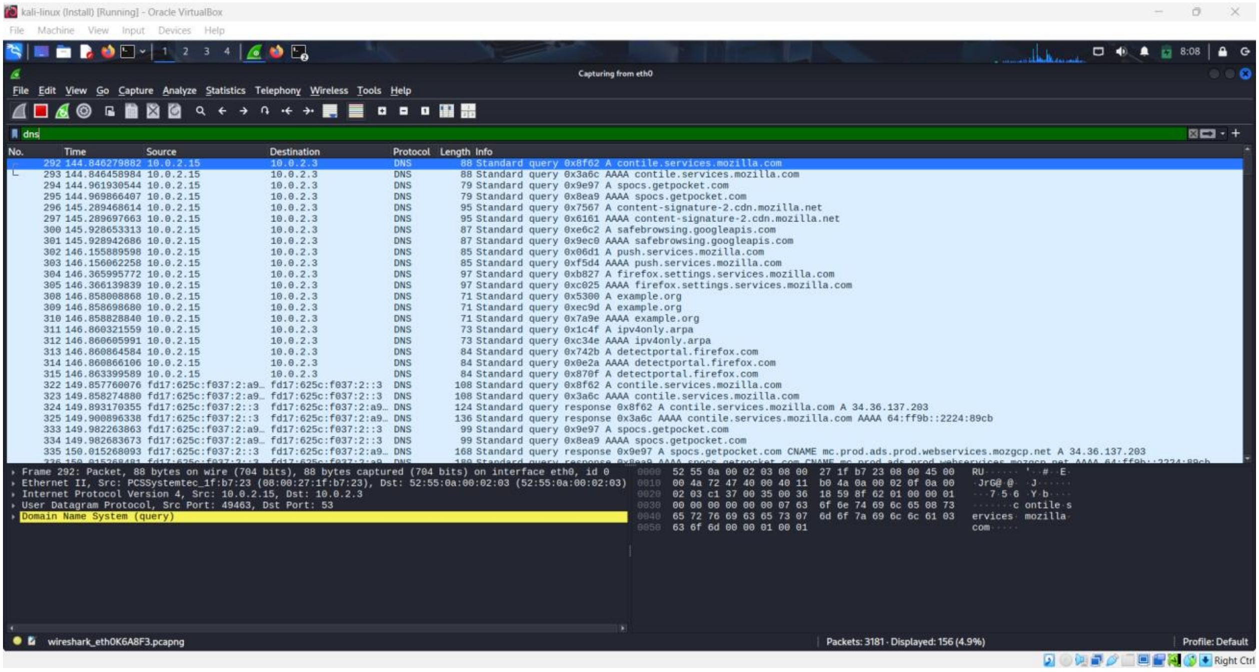
eth0: <live capture in progress>   Packets: 33   Profile: Default

This screenshot shows ICMP Echo Request and Echo Reply packets captured using Wireshark.

The system with IP address 10.0.2.15 sends ping requests to 8.8.8.8, and receives replies successfully.

This confirms network connectivity and demonstrates ICMP protocol usage for network diagnostics.

7.2 DNS Query Analysis



kali-linux (Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.  Time          Source                Destination           Protocol Length Info
292 144.846279882 10.0.2.15             10.0.2.3              DNS      88 Standard query 0x8f62 A contile.services.mozilla.com
293 144.846458984 10.0.2.15             10.0.2.3              DNS      88 Standard query 0x3a6c AAAA contile.services.mozilla.com
294 144.961930544 10.0.2.15             10.0.2.3              DNS      79 Standard query 0x9e97 A spocs.getpocket.com
295 144.969866407 10.0.2.15             10.0.2.3              DNS      79 Standard query 0x8ea9 AAAA spocs.getpocket.com
296 145.289468614 10.0.2.15             10.0.2.3              DNS      95 Standard query 0x7567 A content-signature-2.cdn.mozilla.net
297 145.289697663 10.0.2.15             10.0.2.3              DNS      95 Standard query 0x6161 AAAA content-signature-2.cdn.mozilla.net
300 145.928653313 10.0.2.15             10.0.2.3              DNS      87 Standard query 0xe6c2 A safebrowsing.googleapis.com
301 145.928942686 10.0.2.15             10.0.2.3              DNS      87 Standard query 0x9ec0 AAAA safebrowsing.googleapis.com
302 146.155889598 10.0.2.15             10.0.2.3              DNS      85 Standard query 0x06d1 A push.services.mozilla.com
303 146.15606225 8 10.0.2.15            10.0.2.3              DNS      85 Standard query 0xf5d4 AAAA push.services.mozilla.com
304 146.365995772 10.0.2.15             10.0.2.3              DNS      97 Standard query 0xb827 A firefox.settings.services.mozilla.com
305 146.366139839 10.0.2.15             10.0.2.3              DNS      97 Standard query 0xc025 AAAA firefox.settings.services.mozilla.com
308 146.858008868 10.0.2.15             10.0.2.3              DNS      71 Standard query 0x5300 A example.org
309 146.858698680 10.0.2.15             10.0.2.3              DNS      71 Standard query 0xec9d A example.org
310 146.858828840 10.0.2.15             10.0.2.3              DNS      71 Standard query 0x7a9e AAAA example.org
311 146.860321559 10.0.2.15             10.0.2.3              DNS      73 Standard query 0x1c4f A ipv4only.arpa
312 146.860605991 10.0.2.15             10.0.2.3              DNS      73 Standard query 0xc34e AAAA ipv4only.arpa
313 146.860864584 10.0.2.15             10.0.2.3              DNS      84 Standard query 0x742b A detectportal.firefox.com
314 146.860866106 10.0.2.15             10.0.2.3              DNS      84 Standard query 0x0e2a AAAA detectportal.firefox.com
315 146.863399589 10.0.2.15             10.0.2.3              DNS      84 Standard query 0x870f A detectportal.firefox.com
322 149.857760076 fd17:625c:f037:2:a9… fd17:625c:f037:2::3   DNS     108 Standard query 0x8f62 A contile.services.mozilla.com
323 149.858274880 fd17:625c:f037:2:a9… fd17:625c:f037:2::3   DNS     108 Standard query 0x3a6c AAAA contile.services.mozilla.com
324 149.893170355 fd17:625c:f037:2::3   fd17:625c:f037:2:a9… DNS     124 Standard query response 0x8f62 A contile.services.mozilla.com A 34.36.137.203
325 149.900896338 fd17:625c:f037:2::3   fd17:625c:f037:2:a9… DNS     136 Standard query response 0x3a6c AAAA contile.services.mozilla.com AAAA 64:ff9b::2224:89cb
333 149.982263863 fd17:625c:f037:2:a9… fd17:625c:f037:2::3   DNS      99 Standard query 0x9e97 A spocs.getpocket.com
334 149.982683673 fd17:625c:f037:2:a9… fd17:625c:f037:2::3   DNS      99 Standard query 0x8ea9 AAAA spocs.getpocket.com
335 150.015268093 fd17:625c:f037:2::3   fd17:625c:f037:2:a9… DNS     168 Standard query response 0x9e97 A spocs.getpocket.com CNAME mc.prod.ads.prod.webservices.mozgcp.net A 34.36.137.203
```

```
› Frame 292: Packet, 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
› User Datagram Protocol, Src Port: 49463, Dst Port: 53
› Domain Name System (query)
```

```
0000  52 55 0a 00 02 03 08 00  27 1f b7 23 08 00 45 00   RU······'··#··E·
0010  00 4a 72 47 40 00 40 11  b0 4a 0a 00 02 0f 0a 00   ·JrG@·@··J······
0020  02 03 c1 37 00 35 00 36  18 59 8f 62 01 00 00 01   ···7·5·6·Y·b····
0030  00 00 00 00 00 00 07 63  6f 6e 74 69 6c 65 08 73   ·······contile·s
0040  65 72 76 69 63 65 73 07  6d 6f 7a 69 6c 6c 61 03   ervices·mozilla·
0050  63 6f 6d 00 00 01 00 01                            com·····
```

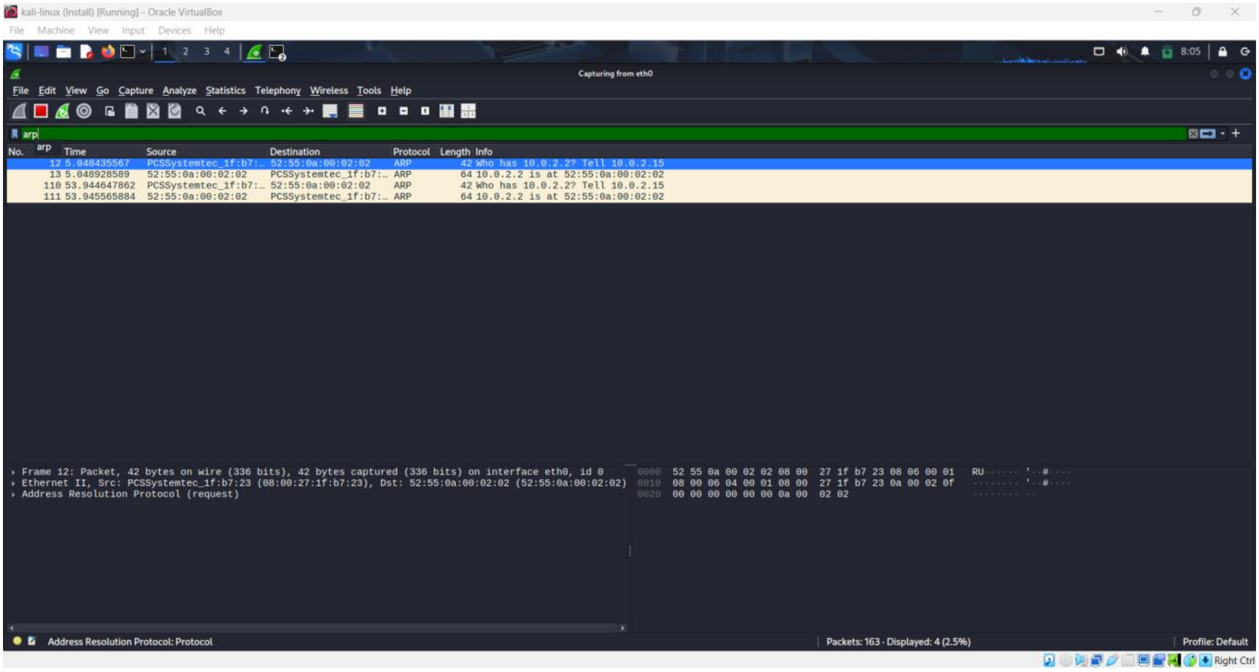
wireshark_eth0K6A8F3.pcapng | Packets: 3181 · Displayed: 156 (4.9%) | Profile: Default

This screenshot displays DNS queries captured using the "dns" filter in Wireshark.

The captured packets show domain name resolution for domains such as example.org and Mozilla services.

DNS converts human-readable domain names into IP addresses, enabling communication over the network.

7.3 ARP Protocol Analysis



kali-linux (Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp
No.   Time          Source                  Destination             Protocol Length Info
   12 5.048435567   PCSSystemtec_1f:b7:…    52:55:0a:00:02:02       ARP        42 Who has 10.0.2.2? Tell 10.0.2.15
   13 5.048928589   52:55:0a:00:02:02       PCSSystemtec_1f:b7:…    ARP        64 10.0.2.2 is at 52:55:0a:00:02:02
  110 53.944647862  PCSSystemtec_1f:b7:…    52:55:0a:00:02:02       ARP        42 Who has 10.0.2.2? Tell 10.0.2.15
  111 53.945565884  52:55:0a:00:02:02       PCSSystemtec_1f:b7:…    ARP        64 10.0.2.2 is at 52:55:0a:00:02:02
```

```
› Frame 12: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Address Resolution Protocol (request)
```

```
0000  52 55 0a 00 02 02 08 00  27 1f b7 23 08 06 00 01   RU······'··#····
0010  08 00 06 04 00 01 08 00  27 1f b7 23 0a 00 02 0f   ········'··#····
0020  00 00 00 00 00 00 0a 00  02 02                     ··········
```

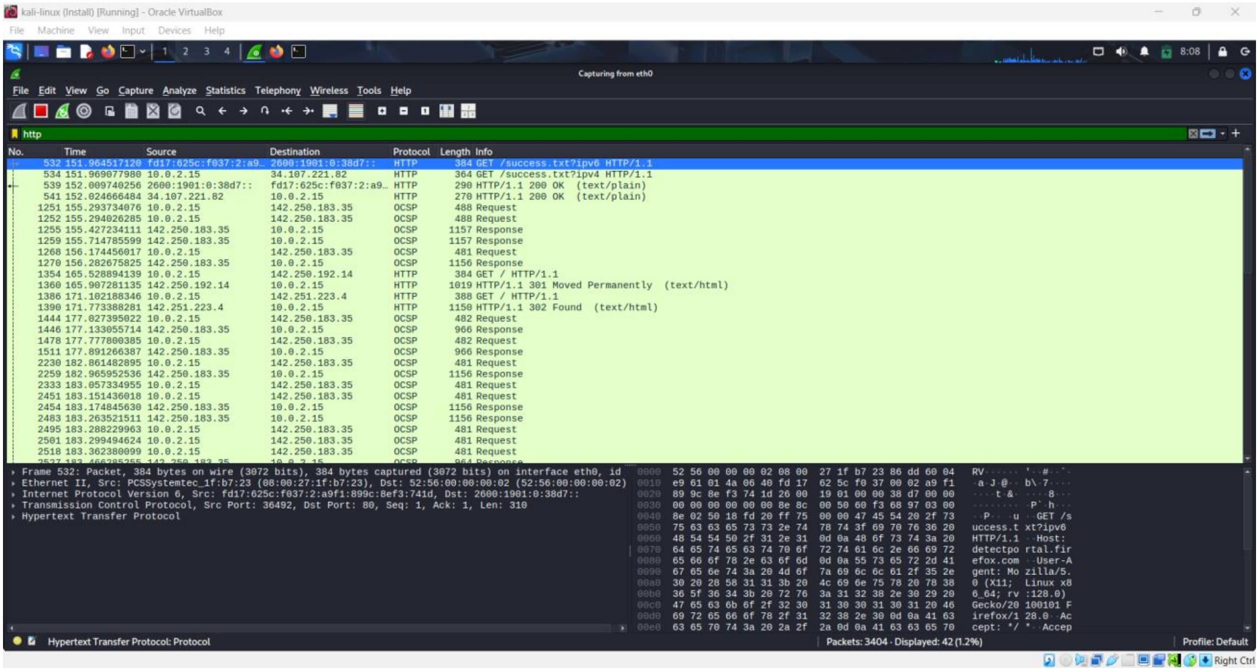
Address Resolution Protocol: Protocol
Packets: 163 · Displayed: 4 (2.5%)
Profile: Default
8:05
Right Ctrl

This screenshot shows ARP (Address Resolution Protocol) packets.

ARP is used to map IP addresses to MAC addresses within a local network.

The packet "Who has 10.0.2.2? Tell 10.0.2.15" demonstrates ARP request and response behavior.

7.4 HTTP Plain-Text Traffic Analysis


kali-linux (Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.    Time          Source                Destination           Protocol Length Info
 532 151.964517120 fd17:625c:f037:2:a9… 2600:1901:0:38d7::    HTTP      384 GET /success.txt?ipv6 HTTP/1.1
 534 151.969077980 10.0.2.15            34.107.221.82         HTTP      364 GET /success.txt?ipv4 HTTP/1.1
 539 152.009740256 2600:1901:0:38d7::   fd17:625c:f037:2:a9… HTTP      290 HTTP/1.1 200 OK  (text/plain)
 541 152.024666484 34.107.221.82        10.0.2.15             HTTP      270 HTTP/1.1 200 OK  (text/plain)
1251 155.293734076 10.0.2.15            142.250.183.35        OCSP      488 Request
1252 155.294026285 10.0.2.15            142.250.183.35        OCSP      488 Request
1255 155.427234111 142.250.183.35       10.0.2.15             OCSP     1157 Response
1259 155.714785599 142.250.183.35       10.0.2.15             OCSP     1157 Response
1268 156.174456017 10.0.2.15            142.250.183.35        OCSP      481 Request
1270 156.282675825 142.250.183.35       10.0.2.15             OCSP     1156 Response
1354 165.528894139 10.0.2.15            142.250.192.14        HTTP      384 GET / HTTP/1.1
1360 165.907281135 142.250.192.14       10.0.2.15             HTTP     1019 HTTP/1.1 301 Moved Permanently  (text/html)
1386 171.102188346 10.0.2.15            142.251.223.4         HTTP      388 GET / HTTP/1.1
1390 171.773388281 142.251.223.4        10.0.2.15             HTTP     1150 HTTP/1.1 302 Found  (text/html)
1444 177.027395022 10.0.2.15            142.250.183.35        OCSP      482 Request
1446 177.133055714 142.250.183.35       10.0.2.15             OCSP      966 Response
1478 177.777800385 10.0.2.15            142.250.183.35        OCSP      482 Request
1511 177.891266387 142.250.183.35       10.0.2.15             OCSP      966 Response
2230 182.861482895 10.0.2.15            142.250.183.35        OCSP      481 Request
2259 182.965952536 142.250.183.35       10.0.2.15             OCSP     1156 Response
2333 183.057334955 10.0.2.15            142.250.183.35        OCSP      481 Request
2451 183.151436018 10.0.2.15            142.250.183.35        OCSP      481 Request
2454 183.174845630 142.250.183.35       10.0.2.15             OCSP     1156 Response
2483 183.263521511 142.250.183.35       10.0.2.15             OCSP     1156 Response
2495 183.288229963 10.0.2.15            142.250.183.35        OCSP      481 Request
2501 183.299494624 10.0.2.15            142.250.183.35        OCSP      481 Request
2518 183.362380099 10.0.2.15            142.250.183.35        OCSP      481 Request
2527 183.466285255 142.250.183.35       10.0.2.15             OCSP      964 Response
```

```
› Frame 532: Packet, 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface eth0, id
› Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:56:00:00:00:02 (52:56:00:00:00:02)
› Internet Protocol Version 6, Src: fd17:625c:f037:2:a9f1:899c:8ef3:741d, Dst: 2600:1901:0:38d7::
› Transmission Control Protocol, Src Port: 36492, Dst Port: 80, Seq: 1, Ack: 1, Len: 310
› Hypertext Transfer Protocol
```

```
0000  52 56 00 00 00 02 08 00  27 1f b7 23 86 dd 60 04   RV······ '··#··`·
0010  e9 61 01 4a 06 40 fd 17  62 5c f0 37 00 02 a9 f1   ·a·J·@·· b\·7····
0020  89 9c 8e f3 74 1d 26 00  19 01 00 00 38 d7 00 00   ····t·&· ····8···
0030  00 00 00 00 00 00 8e 8c  00 50 60 f3 68 97 03 00   ········ ·P`·h···
0040  8e 02 50 18 fd 20 ff 75  00 00 47 45 54 20 2f 73   ··P·· ·u ··GET /s
0050  75 63 63 65 73 73 2e 74  78 74 3f 69 70 76 36 20   uccess.t xt?ipv6 
0060  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0070  64 65 74 65 63 74 70 6f  72 74 61 6c 2e 66 69 72   detectpo rtal.fir
0080  65 66 6f 78 2e 63 6f 6d  0d 0a 55 73 65 72 2d 41   efox.com ··User-A
0090  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00a0  30 20 28 58 31 31 3b 20  4c 69 6e 75 78 20 78 38   0 (X11;  Linux x8
00b0  36 5f 36 34 3b 20 72 76  3a 31 32 38 2e 30 29 20   6_64; rv :128.0) 
00c0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
00d0  69 72 65 66 6f 78 2f 31  32 38 2e 30 0d 0a 41 63   irefox/1 28.0··Ac
00e0  63 65 70 74 3a 20 2a 2f  2a 0d 0a 41 63 63 65 70   cept: */ *··Accep
```

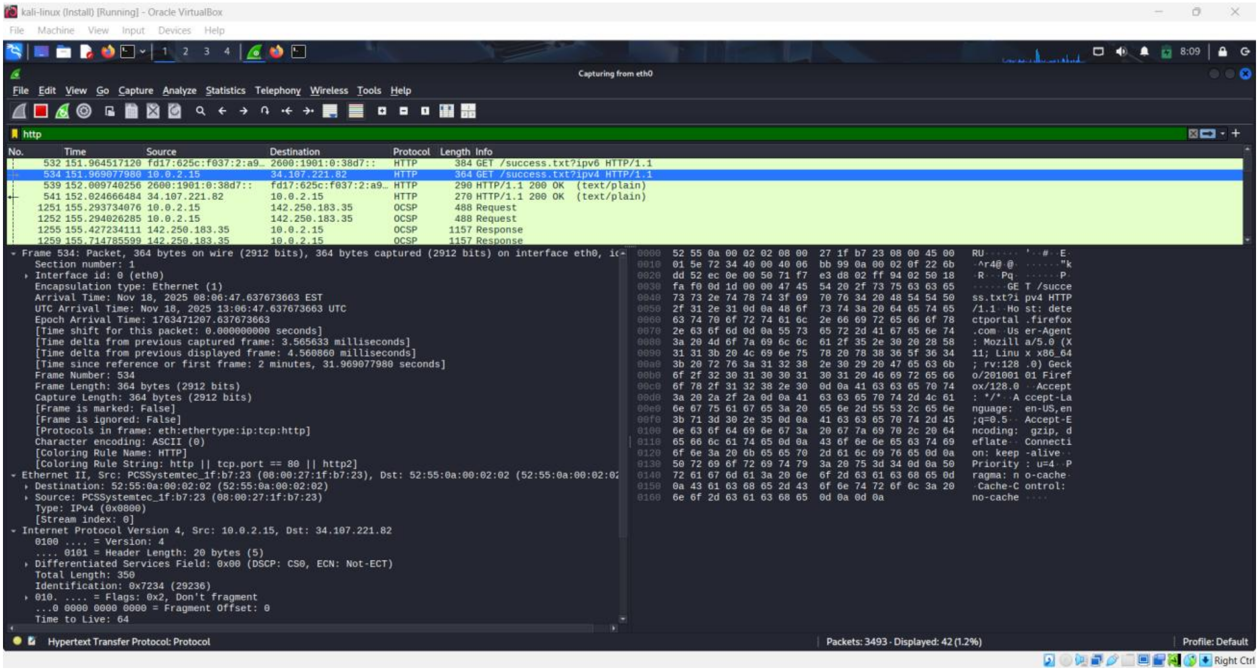
Hypertext Transfer Protocol: Protocol
Packets: 3404 · Displayed: 42 (1.2%)
Profile: Default
Right Ctrl

This screenshot shows HTTP traffic captured using the "http" filter.

The HTTP GET request and response are visible in plain text, including headers such as User-Agent.

This demonstrates that HTTP traffic is not encrypted and can be easily intercepted by attackers.

7.5 Packet Details Analysis (Deep Inspection)


kali-linux (Install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:09
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol: Protocol
Packets: 3493 · Displayed: 42 (1.2%)
Profile: Default
Right Ctrl

```
No.      Time          Source                Destination           Protocol Length Info
   532 151.964517120 fd17:625c:f037:2:a9… 2600:1901:0:38d7::    HTTP      384 GET /success.txt?ipv6 HTTP/1.1
   534 151.969077980 10.0.2.15             34.107.221.82         HTTP      364 GET /success.txt?ipv4 HTTP/1.1
   539 152.009740256 2600:1901:0:38d7::    fd17:625c:f037:2:a9… HTTP      290 HTTP/1.1 200 OK  (text/plain)
   541 152.024666484 34.107.221.82         10.0.2.15             HTTP      270 HTTP/1.1 200 OK  (text/plain)
  1251 155.293734076 10.0.2.15             142.250.183.35        OCSP      488 Request
  1252 155.294026285 10.0.2.15             142.250.183.35        OCSP      488 Request
  1255 155.427234111 142.250.183.35        10.0.2.15             OCSP     1157 Response
  1259 155.714785599 142.250.183.35        10.0.2.15             OCSP     1157 Response
```

```
▾ Frame 534: Packet, 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface eth0, ic
    Section number: 1
  ▸ Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 18, 2025 08:06:47.637673663 EST
    UTC Arrival Time: Nov 18, 2025 13:06:47.637673663 UTC
    Epoch Arrival Time: 1763471207.637673663
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 3.565633 milliseconds]
    [Time delta from previous displayed frame: 4.560860 milliseconds]
    [Time since reference or first frame: 2 minutes, 31.969077980 seconds]
    Frame Number: 534
    Frame Length: 364 bytes (2912 bits)
    Capture Length: 364 bytes (2912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    Character encoding: ASCII (0)
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
▾ Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02
  ▸ Destination: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  ▸ Source: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)
    Type: IPv4 (0x0800)
    [Stream index: 0]
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 350
    Identification: 0x7234 (29236)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
```

```
0000  52 55 0a 00 02 02 08 00  27 1f b7 23 08 00 45 00   RU······ '··#··E·
0010  01 5e 72 34 40 00 40 06  bb 99 0a 00 02 0f 22 6b   ·^r4@·@· ······"k
0020  dd 52 ec 0e 00 50 71 f7  e3 d8 02 ff 94 02 50 18   ·R···Pq· ······P·
0030  fa f0 0d 1d 00 00 47 45  54 20 2f 73 75 63 63 65   ······GE T /succe
0040  73 73 2e 74 78 74 3f 69  70 76 34 20 48 54 54 50   ss.txt?i pv4 HTTP
0050  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 64 65 74 65   /1.1··Ho st: dete
0060  63 74 70 6f 72 74 61 6c  2e 66 69 72 65 66 6f 78   ctportal .firefox
0070  2e 63 6f 6d 0d 0a 55 73  65 72 2d 41 67 65 6e 74   .com··Us er-Agent
0080  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 58   : Mozill a/5.0 (X
0090  31 31 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   11; Linu x x86_64
00a0  3b 20 72 76 3a 31 32 38  2e 30 29 20 47 65 63 6b   ; rv:128 .0) Geck
00b0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66   o/201001 01 Firef
00c0  6f 78 2f 31 32 38 2e 30  0d 0a 41 63 63 65 70 74   ox/128.0 ··Accept
00d0  3a 20 2a 2f 2a 0d 0a 41  63 63 65 70 74 2d 4c 61   : */*··A ccept-La
00e0  6e 67 75 61 67 65 3a 20  65 6e 2d 55 53 2c 65 6e   nguage:  en-US,en
00f0  3b 71 3d 30 2e 35 0d 0a  41 63 63 65 70 74 2d 45   ;q=0.5·· Accept-E
0100  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 2c 20 64   ncoding:  gzip, d
0110  65 66 6c 61 74 65 0d 0a  43 6f 6e 6e 65 63 74 69   eflate·· Connecti
0120  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
0130  50 72 69 6f 72 69 74 79  3a 20 75 3d 34 0d 0a 50   Priority : u=4··P
0140  72 61 67 6d 61 3a 20 6e  6f 2d 63 61 63 68 65 0d   ragma: n o-cache·
0150  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20   ·Cache-C ontrol: 
0160  6e 6f 2d 63 61 63 68 65  0d 0a 0d 0a               no-cache ····
```

This screenshot shows detailed packet inspection in Wireshark.

It includes Ethernet, IP, TCP, and HTTP layer information such as source and destination IP addresses, ports, and flags.

This layered view helps security analysts understand how data flows across the network.

8. Screenshots Evidence

The following screenshots were captured during analysis:

- ICMP Traffic Analysis
- DNS Query Resolution
- ARP Protocol Analysis
- HTTP Plain-Text Traffic Analysis
- Packet Details Analysis

---

9. Learning Outcome

After completing this task, the following learning outcomes were achieved:

• Understood basic networking concepts including IP, MAC, TCP, UDP, DNS, HTTP, and HTTPS
• Gained hands-on experience in capturing live network traffic using Wireshark

- Analyzed ICMP traffic to verify network connectivity
- Learned the role of packet sniffing in cybersecurity investigations
- Observed DNS queries and ARP behavior for network communication
- Differentiated between encrypted (HTTPS) and unencrypted (HTTP) traffic
- Developed practical skills in network traffic analysis and monitoring

10. Conclusion

This task provided practical exposure to network traffic analysis using Wireshark. By analyzing protocols such as ICMP, DNS, ARP, and HTTP, a clear understanding of network communication was developed. The exercise also emphasized the importance of encryption and the role of traffic analysis in identifying security risks and ensuring secure network operations.