Task 3: Networking Basics for Cyber Security

1) Tools and Environment

- **Operating System:** Ubuntu Linux.
- **Packet Analysis Tool:** Wireshark.
- **Network Type:** Wi-Fi .

2) Basic networking concepts (IP, MAC, DNS, TCP/UDP).

Concept	Definition
IP Address	Address of a device (like a phone number)
MAC Address	Hardware address of network card
DNS	Converts website name → IP address
TCP	Reliable communication (used by HTTP, HTTPS)
UDP	Faster but unreliable (used by DNS, streaming)
Port	Application entry point (80, 443, 53, etc.)

3)Methodology (Capturing Process)

1. Wireshark was opened and the active network interface was selected.
2. Live packet capture was started.
3. Network traffic was generated by:
   - Visiting `http://example.com`
   - Visiting `https://google.com`
   - Running `ping google.com` from the terminal
4. After traffic generation, the capture was stopped.
5. Display filters were applied to analyze specific protocols.

4) DNS Traffic Analysis

Display Filter Used: `dns`

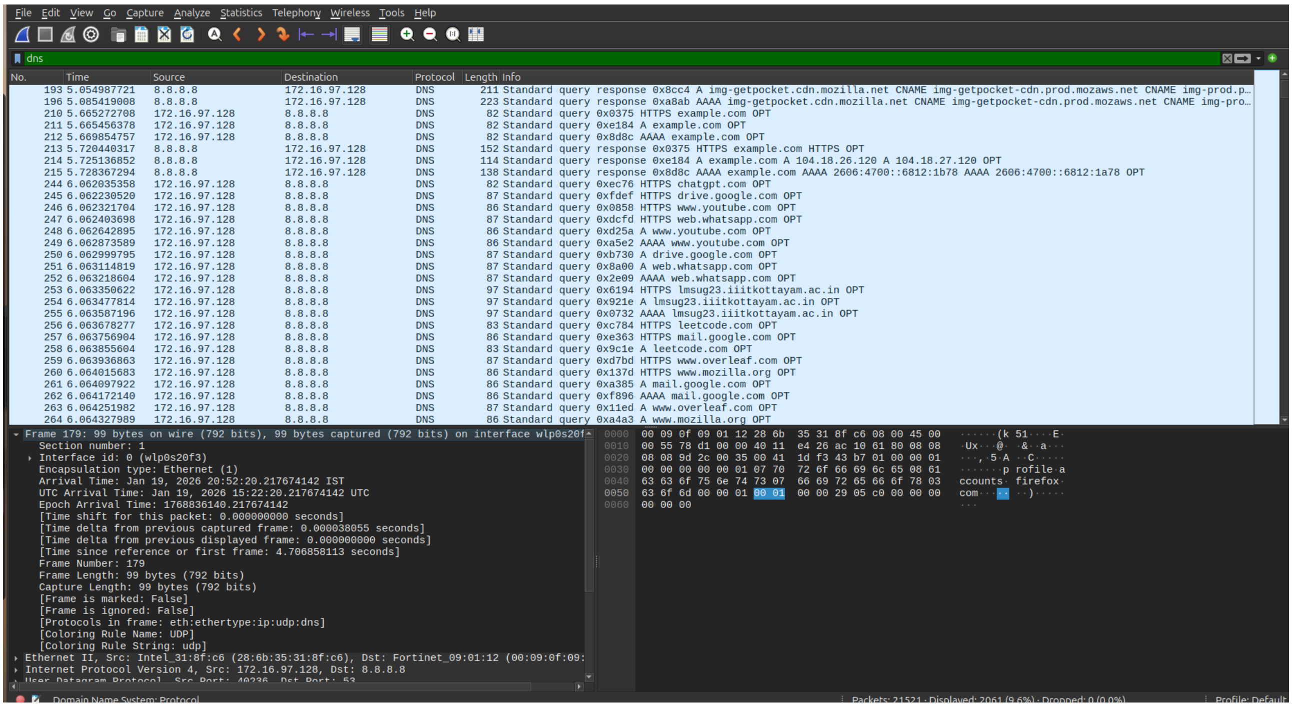
Domain Name System (DNS) traffic was captured and analyzed. DNS resolves human-readable domain names into IP addresses.

Observations:

- DNS query packets were observed.

- Domain names such as `google.com` and `example.com` were seen.
- DNS responses contained resolved IP addresses.

DNS Packet Analysis



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.     Time         Source          Destination     Protocol Length Info
    193 5.054987721  8.8.8.8         172.16.97.128   DNS      211 Standard query response 0x8cc4 A img-getpocket.cdn.mozilla.net CNAME img-getpocket-cdn.prod.mozaws.net CNAME img-prod.p…
    196 5.085419008  8.8.8.8         172.16.97.128   DNS      223 Standard query response 0xa8ab AAAA img-getpocket.cdn.mozilla.net CNAME img-getpocket-cdn.prod.mozaws.net CNAME img-pro…
    210 5.665272708  172.16.97.128   8.8.8.8         DNS       82 Standard query 0x0375 HTTPS example.com OPT
    211 5.665456378  172.16.97.128   8.8.8.8         DNS       82 Standard query 0xe184 A example.com OPT
    212 5.669854757  172.16.97.128   8.8.8.8         DNS       82 Standard query 0x8d8c AAAA example.com OPT
    213 5.720440317  8.8.8.8         172.16.97.128   DNS      152 Standard query response 0x0375 HTTPS example.com HTTPS OPT
    214 5.725136852  8.8.8.8         172.16.97.128   DNS      114 Standard query response 0xe184 A example.com A 104.18.26.120 A 104.18.27.120 OPT
    215 5.728367294  8.8.8.8         172.16.97.128   DNS      138 Standard query response 0x8d8c AAAA example.com AAAA 2606:4700::6812:1b78 AAAA 2606:4700::6812:1a78 OPT
    244 6.062035358  172.16.97.128   8.8.8.8         DNS       82 Standard query 0xec76 HTTPS chatgpt.com OPT
    245 6.062230520  172.16.97.128   8.8.8.8         DNS       87 Standard query 0xfdef HTTPS drive.google.com OPT
    246 6.062321704  172.16.97.128   8.8.8.8         DNS       86 Standard query 0x0858 HTTPS www.youtube.com OPT
    247 6.062403698  172.16.97.128   8.8.8.8         DNS       87 Standard query 0xdcfd HTTPS web.whatsapp.com OPT
    248 6.062642895  172.16.97.128   8.8.8.8         DNS       86 Standard query 0xd25a A www.youtube.com OPT
    249 6.062873589  172.16.97.128   8.8.8.8         DNS       86 Standard query 0xa5e2 AAAA www.youtube.com OPT
    250 6.062999795  172.16.97.128   8.8.8.8         DNS       87 Standard query 0xb730 A drive.google.com OPT
    251 6.063114819  172.16.97.128   8.8.8.8         DNS       87 Standard query 0x8a00 A web.whatsapp.com OPT
    252 6.063218604  172.16.97.128   8.8.8.8         DNS       87 Standard query 0x2e09 AAAA web.whatsapp.com OPT
    253 6.063350622  172.16.97.128   8.8.8.8         DNS       97 Standard query 0x6194 HTTPS lmsug23.iiitkottayam.ac.in OPT
    254 6.063477814  172.16.97.128   8.8.8.8         DNS       97 Standard query 0x921e A lmsug23.iiitkottayam.ac.in OPT
    255 6.063587196  172.16.97.128   8.8.8.8         DNS       97 Standard query 0x0732 AAAA lmsug23.iiitkottayam.ac.in OPT
    256 6.063678277  172.16.97.128   8.8.8.8         DNS       83 Standard query 0xc784 HTTPS leetcode.com OPT
    257 6.063756904  172.16.97.128   8.8.8.8         DNS       86 Standard query 0xe363 HTTPS mail.google.com OPT
    258 6.063855604  172.16.97.128   8.8.8.8         DNS       83 Standard query 0x9c1e A leetcode.com OPT
    259 6.063936863  172.16.97.128   8.8.8.8         DNS       87 Standard query 0xd7bd HTTPS www.overleaf.com OPT
    260 6.064015683  172.16.97.128   8.8.8.8         DNS       86 Standard query 0x137d HTTPS www.mozilla.org OPT
    261 6.064097922  172.16.97.128   8.8.8.8         DNS       86 Standard query 0xa385 A mail.google.com OPT
    262 6.064172140  172.16.97.128   8.8.8.8         DNS       86 Standard query 0xf896 AAAA mail.google.com OPT
    263 6.064251982  172.16.97.128   8.8.8.8         DNS       87 Standard query 0x11ed A www.overleaf.com OPT
    264 6.064327989  172.16.97.128   8.8.8.8         DNS       86 Standard query 0xa4a3 A www.mozilla.org OPT
```

```
▾ Frame 179: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface wlp0s20f
    Section number: 1
  ▸ Interface id: 0 (wlp0s20f3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 19, 2026 20:52:20.217674142 IST
    UTC Arrival Time: Jan 19, 2026 15:22:20.217674142 UTC
    Epoch Arrival Time: 1768836140.217674142
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000038055 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 4.706858113 seconds]
    Frame Number: 179
    Frame Length: 99 bytes (792 bits)
    Capture Length: 99 bytes (792 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▸ Ethernet II, Src: Intel_31:8f:c6 (28:6b:35:31:8f:c6), Dst: Fortinet_09:01:12 (00:09:0f:09:
▸ Internet Protocol Version 4, Src: 172.16.97.128, Dst: 8.8.8.8
▸ User Datagram Protocol, Src Port: 40236, Dst Port: 53
```

```
0000  00 09 0f 09 01 12 28 6b  35 31 8f c6 08 00 45 00   ······(k 51····E·
0010  00 55 78 d1 00 00 40 11  e4 26 ac 10 61 80 08 08   ·Ux···@· ·&··a···
0020  08 08 9d 2c 00 35 00 41  1d f3 43 b7 01 00 00 01   ···,·5·A ··C·····
0030  00 00 00 00 00 01 07 70  72 6f 66 69 6c 65 08 61   ·······p rofile·a
0040  63 63 6f 75 6e 74 73 07  66 69 72 65 66 6f 78 03   ccounts· firefox·
0050  63 6f 6d 00 00 01 00 01  00 00 29 05 c0 00 00 00   com····· ··)·····
0060  00 00 00                                           ···
```

Domain Name System: Protocol | Packets: 21521 · Displayed: 2061 (9.6%) · Dropped: 0 (0.0%) | Profile: Default

5) ICMP Traffic Analysis

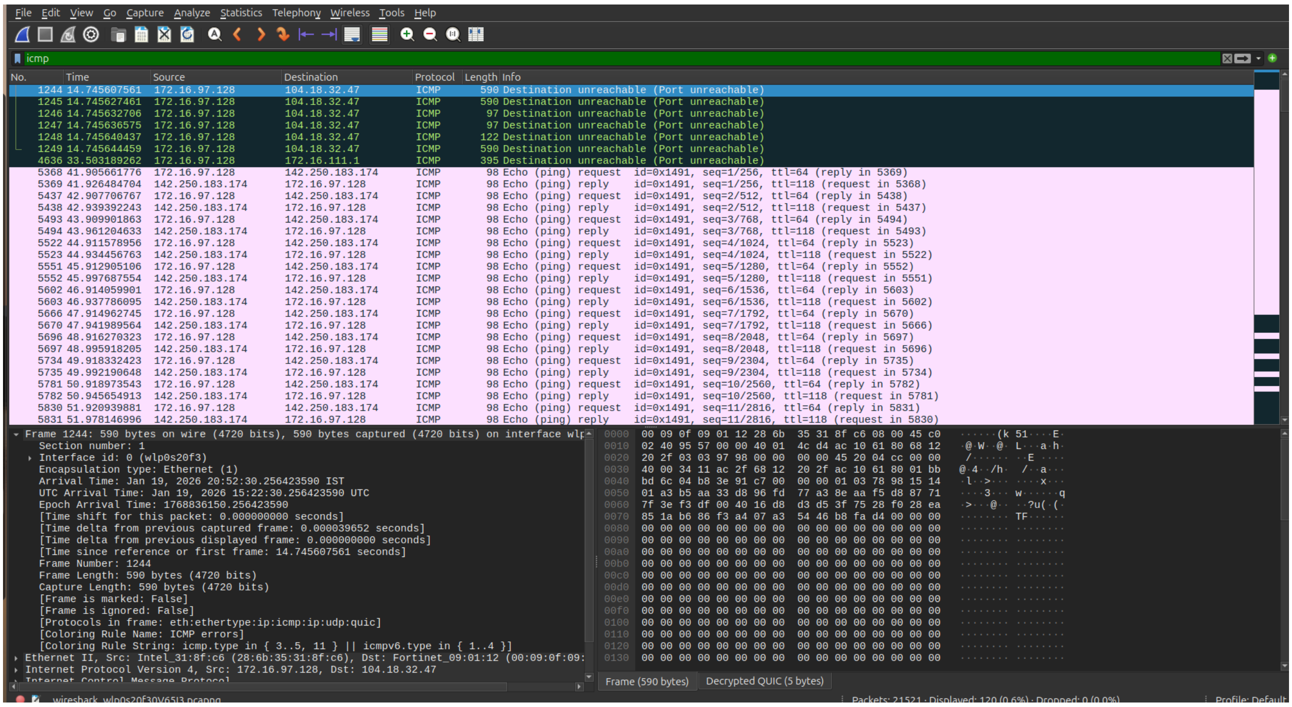
Display Filter Used: `icmp`

ICMP packets are generated using the `ping` command to test network connectivity.

Observations:

- ICMP Echo Request packets were sent.
- ICMP Echo Reply packets were received.
- Successful communication between host and destination was confirmed.

ICMP Packet Analysis:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
No.  Time         Source          Destination     Protocol Length Info
1244 14.745607561 172.16.97.128   104.18.32.47    ICMP     590 Destination unreachable (Port unreachable)
1245 14.745627461 172.16.97.128   104.18.32.47    ICMP     590 Destination unreachable (Port unreachable)
1246 14.745632706 172.16.97.128   104.18.32.47    ICMP      97 Destination unreachable (Port unreachable)
1247 14.745636575 172.16.97.128   104.18.32.47    ICMP      97 Destination unreachable (Port unreachable)
1248 14.745640437 172.16.97.128   104.18.32.47    ICMP     122 Destination unreachable (Port unreachable)
1249 14.745644459 172.16.97.128   104.18.32.47    ICMP     590 Destination unreachable (Port unreachable)
4636 33.503189262 172.16.97.128   172.16.111.1    ICMP     395 Destination unreachable (Port unreachable)
5368 41.905661776 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=1/256, ttl=64 (reply in 5369)
5369 41.926484704 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=1/256, ttl=118 (request in 5368)
5437 42.907706767 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=2/512, ttl=64 (reply in 5438)
5438 42.939392243 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=2/512, ttl=118 (request in 5437)
5493 43.909901863 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=3/768, ttl=64 (reply in 5494)
5494 43.961204633 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=3/768, ttl=118 (request in 5493)
5522 44.911578956 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=4/1024, ttl=64 (reply in 5523)
5523 44.934456763 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=4/1024, ttl=118 (request in 5522)
5551 45.912905106 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=5/1280, ttl=64 (reply in 5552)
5552 45.997687554 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=5/1280, ttl=118 (request in 5551)
5602 46.914059901 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=6/1536, ttl=64 (reply in 5603)
5603 46.937786095 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=6/1536, ttl=118 (request in 5602)
5666 47.914962745 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=7/1792, ttl=64 (reply in 5670)
5670 47.941989564 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=7/1792, ttl=118 (request in 5666)
5696 48.916270323 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=8/2048, ttl=64 (reply in 5697)
5697 48.995918205 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=8/2048, ttl=118 (request in 5696)
5734 49.918332423 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=9/2304, ttl=64 (reply in 5735)
5735 49.992190648 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=9/2304, ttl=118 (request in 5734)
5781 50.918973543 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=10/2560, ttl=64 (reply in 5782)
5782 50.945654913 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=10/2560, ttl=118 (request in 5781)
5830 51.920939881 172.16.97.128   142.250.183.174 ICMP      98 Echo (ping) request  id=0x1491, seq=11/2816, ttl=64 (reply in 5831)
5831 51.978146996 142.250.183.174 172.16.97.128   ICMP      98 Echo (ping) reply    id=0x1491, seq=11/2816, ttl=118 (request in 5830)
```

```
Frame 1244: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface wlp
  Section number: 1
  Interface id: 0 (wlp0s20f3)
  Encapsulation type: Ethernet (1)
  Arrival Time: Jan 19, 2026 20:52:30.256423590 IST
  UTC Arrival Time: Jan 19, 2026 15:22:30.256423590 UTC
  Epoch Arrival Time: 1768836150.256423590
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000039652 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 14.745607561 seconds]
  Frame Number: 1244
  Frame Length: 590 bytes (4720 bits)
  Capture Length: 590 bytes (4720 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:icmp:ip:udp:quic]
  [Coloring Rule Name: ICMP errors]
  [Coloring Rule String: icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }]
Ethernet II, Src: Intel_31:8f:c6 (28:6b:35:31:8f:c6), Dst: Fortinet_09:01:12 (00:09:0f:09:
Internet Protocol Version 4, Src: 172.16.97.128, Dst: 104.18.32.47
Internet Control Message Protocol
```

```
0000  00 09 0f 09 01 12 28 6b  35 31 8f c6 08 00 45 c0   ······(k 51····E·
0010  02 40 95 57 00 00 40 01  4c d4 ac 10 61 80 68 12   ·@·W··@· L···a·h·
0020  20 2f 03 03 97 98 00 00  00 00 45 20 04 cc 00 00    /······ ··E ····
0030  40 00 34 11 ac 2f 68 12  20 2f ac 10 61 80 01 bb   @·4··/h·  /··a···
0040  bd 6c 04 b8 3e 91 c7 00  00 00 01 03 78 98 15 14   ·l··>··· ····x···
0050  01 a3 b5 aa 33 d8 96 fd  77 a3 8e aa f5 d8 87 71   ····3··· w······q
0060  7f 3e f3 df 00 40 16 d8  d3 d5 3f 75 28 f0 28 ea   ·>···@·· ··?u(·(·
0070  85 1a b6 86 f3 a4 07 a3  54 46 b8 fa d4 00 00 00   ········ TF······
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

wireshark_wlp0s20f30V65I3.pcapng · Packets: 21521 · Displayed: 120 (0.6%) · Dropped: 0 (0.0%) · Profile: Default

6) Plain-Text Traffic Analysis (HTTP)

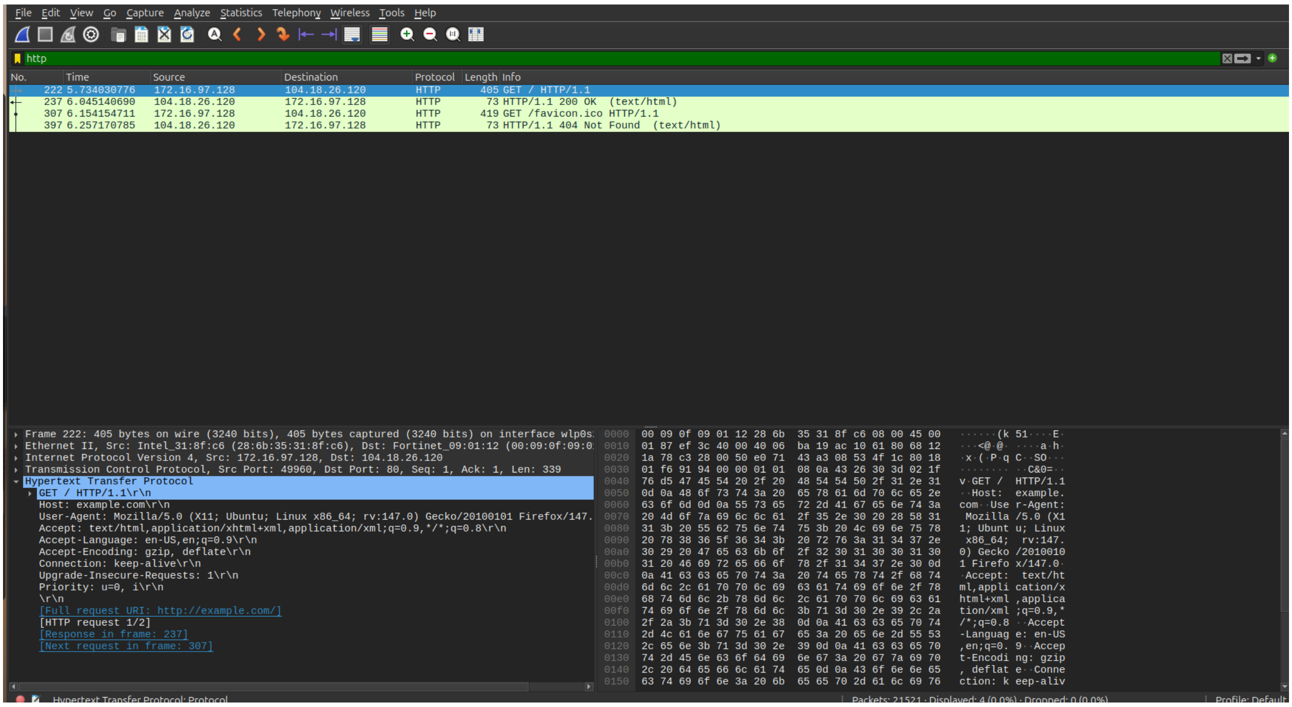
Display Filter Used: `http`

HTTP traffic was identified as plain-text traffic.

Observations:

- HTTP requests such as GET requests were readable.
- Header information and URLs were visible.
- Data was transmitted without encryption.

HTTP Plain-Text Traffic:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time         Source          Destination     Protocol Length Info
  222 5.734030776  172.16.97.128   104.18.26.120   HTTP       405 GET / HTTP/1.1
  237 6.045140690  104.18.26.120   172.16.97.128   HTTP        73 HTTP/1.1 200 OK  (text/html)
  307 6.154154711  172.16.97.128   104.18.26.120   HTTP       419 GET /favicon.ico HTTP/1.1
  397 6.257170785  104.18.26.120   172.16.97.128   HTTP        73 HTTP/1.1 404 Not Found  (text/html)
```

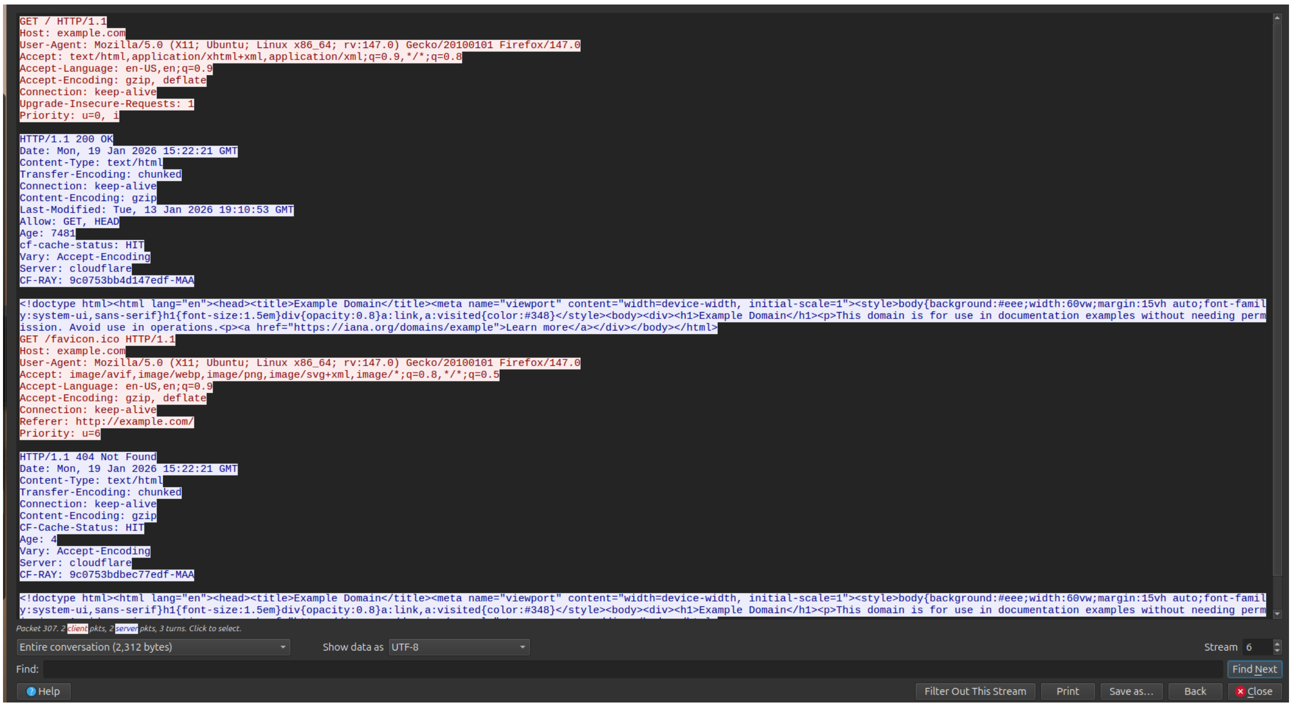
```
▸ Frame 222: 405 bytes on wire (3240 bits), 405 bytes captured (3240 bits) on interface wlp0s
▸ Ethernet II, Src: Intel_31:8f:c6 (28:6b:35:31:8f:c6), Dst: Fortinet_09:01:12 (00:09:0f:09:0
▸ Internet Protocol Version 4, Src: 172.16.97.128, Dst: 104.18.26.120
▸ Transmission Control Protocol, Src Port: 49960, Dst Port: 80, Seq: 1, Ack: 1, Len: 339
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: example.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Full request URI: http://example.com/]
    [HTTP request 1/2]
    [Response in frame: 237]
    [Next request in frame: 307]
```

```
0000  00 09 0f 09 01 12 28 6b  35 31 8f c6 08 00 45 00   ······(k 51····E·
0010  01 87 ef 3c 40 00 40 06  ba 19 ac 10 61 80 68 12   ···<@·@· ····a·h·
0020  1a 78 c3 28 00 50 e0 71  43 a3 08 53 4f 1c 80 18   ·x·(·P·q C··SO···
0030  01 f6 91 94 00 00 01 01  08 0a 43 26 30 3d 02 1f   ········ ··C&0=··
0040  76 d5 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   v·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  65 78 61 6d 70 6c 65 2e   ··Host:  example.
0060  63 6f 6d 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   com··Use r-Agent:
0070  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 58 31    Mozilla /5.0 (X1
0080  31 3b 20 55 62 75 6e 74  75 3b 20 4c 69 6e 75 78   1; Ubunt u; Linux
0090  20 78 38 36 5f 36 34 3b  20 72 76 3a 31 34 37 2e    x86_64;  rv:147.
00a0  30 29 20 47 65 63 6b 6f  2f 32 30 31 30 30 31 30   0) Gecko /2010010
00b0  31 20 46 69 72 65 66 6f  78 2f 31 34 37 2e 30 0d   1 Firefo x/147.0·
00c0  0a 41 63 63 65 70 74 3a  20 74 65 78 74 2f 68 74   ·Accept:  text/ht
00d0  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
00e0  68 74 6d 6c 2b 78 6d 6c  2c 61 70 70 6c 69 63 61   html+xml ,applica
00f0  74 69 6f 6e 2f 78 6d 6c  3b 71 3d 30 2e 39 2c 2a   tion/xml ;q=0.9,*
0100  2f 2a 3b 71 3d 30 2e 38  0d 0a 41 63 63 65 70 74   /*;q=0.8 ··Accept
0110  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
0120  2c 65 6e 3b 71 3d 30 2e  39 0d 0a 41 63 63 65 70   ,en;q=0. 9··Accep
0130  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0140  2c 20 64 65 66 6c 61 74  65 0d 0a 43 6f 6e 6e 65   , deflat e··Conne
0150  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
```

Hypertext Transfer Protocol: Protocol

Packets: 21521 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)

Profile: Default



```
GET / HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i

HTTP/1.1 200 OK
Date: Mon, 19 Jan 2026 15:22:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip
Last-Modified: Tue, 13 Jan 2026 19:10:53 GMT
Allow: GET, HEAD
Age: 7481
cf-cache-status: HIT
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 9c0753bb4d147edf-MAA

<!doctype html><html lang="en"><head><title>Example Domain</title><meta name="viewport" content="width=device-width, initial-scale=1"><style>body{background:#eee;width:60vw;margin:15vh auto;font-famil
y:system-ui,sans-serif}h1{font-size:1.5em}div{opacity:0.8}a:link,a:visited{color:#348}</style><body><div><h1>Example Domain</h1><p>This domain is for use in documentation examples without needing perm
ission. Avoid use in operations.<p><a href="https://iana.org/domains/example">Learn more</a></div></body></html>
GET /favicon.ico HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://example.com/
Priority: u=6

HTTP/1.1 404 Not Found
Date: Mon, 19 Jan 2026 15:22:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip
CF-Cache-Status: HIT
Age: 4
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 9c0753bdbec77edf-MAA

<!doctype html><html lang="en"><head><title>Example Domain</title><meta name="viewport" content="width=device-width, initial-scale=1"><style>body{background:#eee;width:60vw;margin:15vh auto;font-famil
y:system-ui,sans-serif}h1{font-size:1.5em}div{opacity:0.8}a:link,a:visited{color:#348}</style><body><div><h1>Example Domain</h1><p>This domain is for use in documentation examples without needing perm
```

Packet 307. 2 client pkts, 2 server pkts, 3 turns. Click to select.

Entire conversation (2,312 bytes) · Show data as: UTF-8 · Stream: 6

Find:

7) TCP Traffic Analysis

Display Filter Used: `tcp`

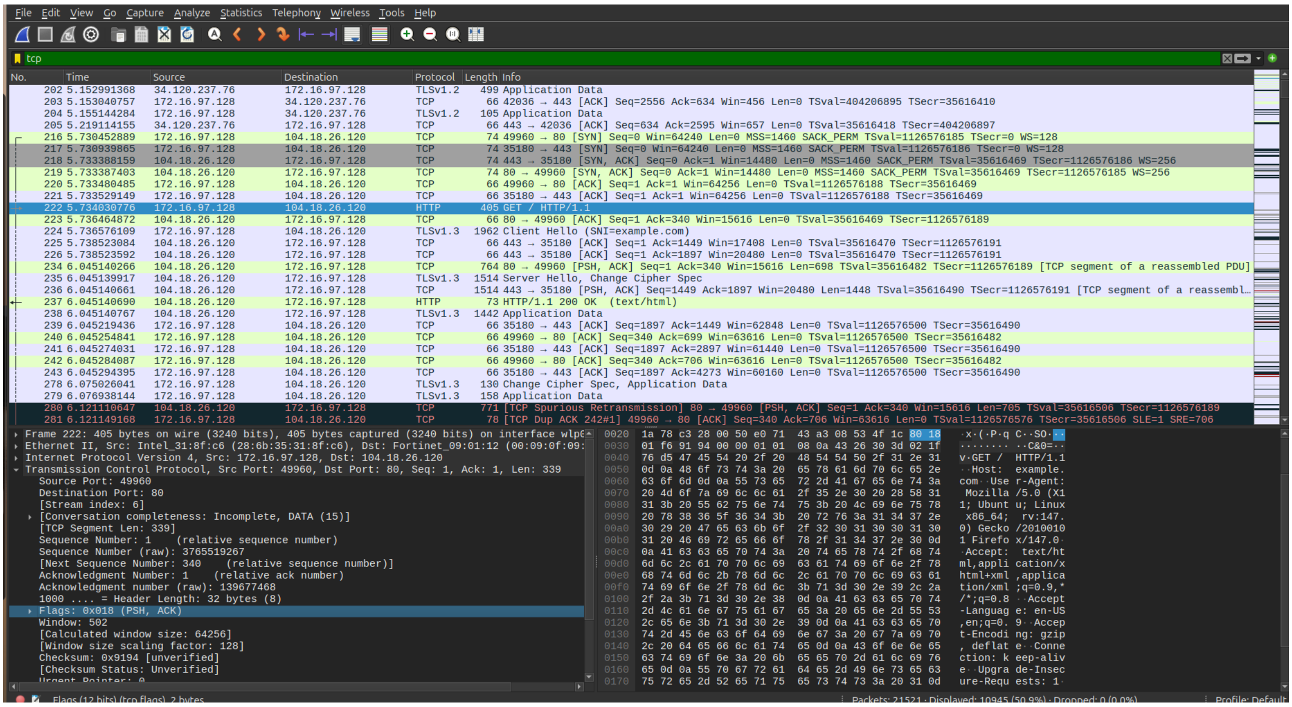
Transmission Control Protocol (TCP) traffic was analyzed to observe reliable, connection-oriented communication.

Observations:

- TCP packets were observed during web communication.

- TCP is responsible for reliable data transfer.
- Web applications primarily use TCP.

TCP Packet Analysis:



```
No.     Time         Source          Destination     Protocol Length Info
    202 5.152991368  34.120.237.76   172.16.97.128   TLSv1.2   499 Application Data
    203 5.153040757  172.16.97.128   34.120.237.76   TCP        66 42036 → 443 [ACK] Seq=2556 Ack=634 Win=456 Len=0 TSval=404206895 TSecr=35616410
    204 5.155144284  172.16.97.128   34.120.237.76   TLSv1.2   105 Application Data
    205 5.219114155  34.120.237.76   172.16.97.128   TCP        66 443 → 42036 [ACK] Seq=634 Ack=2595 Win=657 Len=0 TSval=35616418 TSecr=404206897
    216 5.730452889  172.16.97.128   104.18.26.120   TCP        74 49960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1126576185 TSecr=0 WS=128
    217 5.730939865  172.16.97.128   104.18.26.120   TCP        74 35180 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1126576186 TSecr=0 WS=128
    218 5.733388159  104.18.26.120   172.16.97.128   TCP        74 443 → 35180 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35616469 TSecr=1126576186 WS=256
    219 5.733387403  104.18.26.120   172.16.97.128   TCP        74 80 → 49960 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35616469 TSecr=1126576185 WS=256
    220 5.733480485  172.16.97.128   104.18.26.120   TCP        66 49960 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1126576188 TSecr=35616469
    221 5.733529149  172.16.97.128   104.18.26.120   TCP        66 35180 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1126576188 TSecr=35616469
    222 5.734030776  172.16.97.128   104.18.26.120   HTTP      405 GET / HTTP/1.1
    223 5.736464872  104.18.26.120   172.16.97.128   TCP        66 80 → 49960 [ACK] Seq=1 Ack=340 Win=15616 Len=0 TSval=35616469 TSecr=1126576189
    224 5.736576109  172.16.97.128   104.18.26.120   TLSv1.3  1962 Client Hello (SNI=example.com)
    225 5.738523084  104.18.26.120   172.16.97.128   TCP        66 443 → 35180 [ACK] Seq=1 Ack=1449 Win=17408 Len=0 TSval=35616470 TSecr=1126576191
    226 5.738523592  104.18.26.120   172.16.97.128   TCP        66 443 → 35180 [ACK] Seq=1 Ack=1897 Win=20480 Len=0 TSval=35616470 TSecr=1126576191
    234 6.045140266  104.18.26.120   172.16.97.128   TCP       764 80 → 49960 [PSH, ACK] Seq=1 Ack=340 Win=15616 Len=698 TSval=35616482 TSecr=1126576189 [TCP segment of a reassembled PDU]
    235 6.045139917  104.18.26.120   172.16.97.128   TLSv1.3  1514 Server Hello, Change Cipher Spec
    236 6.045140661  104.18.26.120   172.16.97.128   TCP      1514 443 → 35180 [PSH, ACK] Seq=1449 Ack=1897 Win=20480 Len=1448 TSval=35616490 TSecr=1126576191 [TCP segment of a reassembl…
    237 6.045140690  104.18.26.120   172.16.97.128   HTTP       73 HTTP/1.1 200 OK  (text/html)
    238 6.045140767  104.18.26.120   172.16.97.128   TLSv1.3  1442 Application Data
    239 6.045219436  172.16.97.128   104.18.26.120   TCP        66 35180 → 443 [ACK] Seq=1897 Ack=1449 Win=62848 Len=0 TSval=1126576500 TSecr=35616490
    240 6.045254841  172.16.97.128   104.18.26.120   TCP        66 49960 → 80 [ACK] Seq=340 Ack=699 Win=63616 Len=0 TSval=1126576500 TSecr=35616482
    241 6.045274031  172.16.97.128   104.18.26.120   TCP        66 35180 → 443 [ACK] Seq=1897 Ack=2897 Win=61440 Len=0 TSval=1126576500 TSecr=35616490
    242 6.045284087  172.16.97.128   104.18.26.120   TCP        66 49960 → 80 [ACK] Seq=340 Ack=706 Win=63616 Len=0 TSval=1126576500 TSecr=35616482
    243 6.045294395  172.16.97.128   104.18.26.120   TCP        66 35180 → 443 [ACK] Seq=1897 Ack=4273 Win=60160 Len=0 TSval=1126576500 TSecr=35616490
    278 6.075026041  172.16.97.128   104.18.26.120   TLSv1.3   130 Change Cipher Spec, Application Data
    279 6.076938144  172.16.97.128   104.18.26.120   TLSv1.3   158 Application Data
    280 6.121110647  104.18.26.120   172.16.97.128   TCP       771 [TCP Spurious Retransmission] 80 → 49960 [PSH, ACK] Seq=1 Ack=340 Win=15616 Len=705 TSval=35616506 TSecr=1126576189
    281 6.121149168  172.16.97.128   104.18.26.120   TCP        78 [TCP Dup ACK 242#1] 49960 → 80 [ACK] Seq=340 Ack=706 Win=63616 Len=0 TSval=1126576576 TSecr=35616506 SLE=1 SRE=706
```

```
▸ Frame 222: 405 bytes on wire (3240 bits), 405 bytes captured (3240 bits) on interface wlp0
▸ Ethernet II, Src: Intel_31:8f:c6 (28:6b:35:31:8f:c6), Dst: Fortinet_09:01:12 (00:09:0f:09:
▸ Internet Protocol Version 4, Src: 172.16.97.128, Dst: 104.18.26.120
▾ Transmission Control Protocol, Src Port: 49960, Dst Port: 80, Seq: 1, Ack: 1, Len: 339
    Source Port: 49960
    Destination Port: 80
    [Stream index: 6]
  ▸ [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 339]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3765519267
    [Next Sequence Number: 340    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 139677468
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0x9194 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

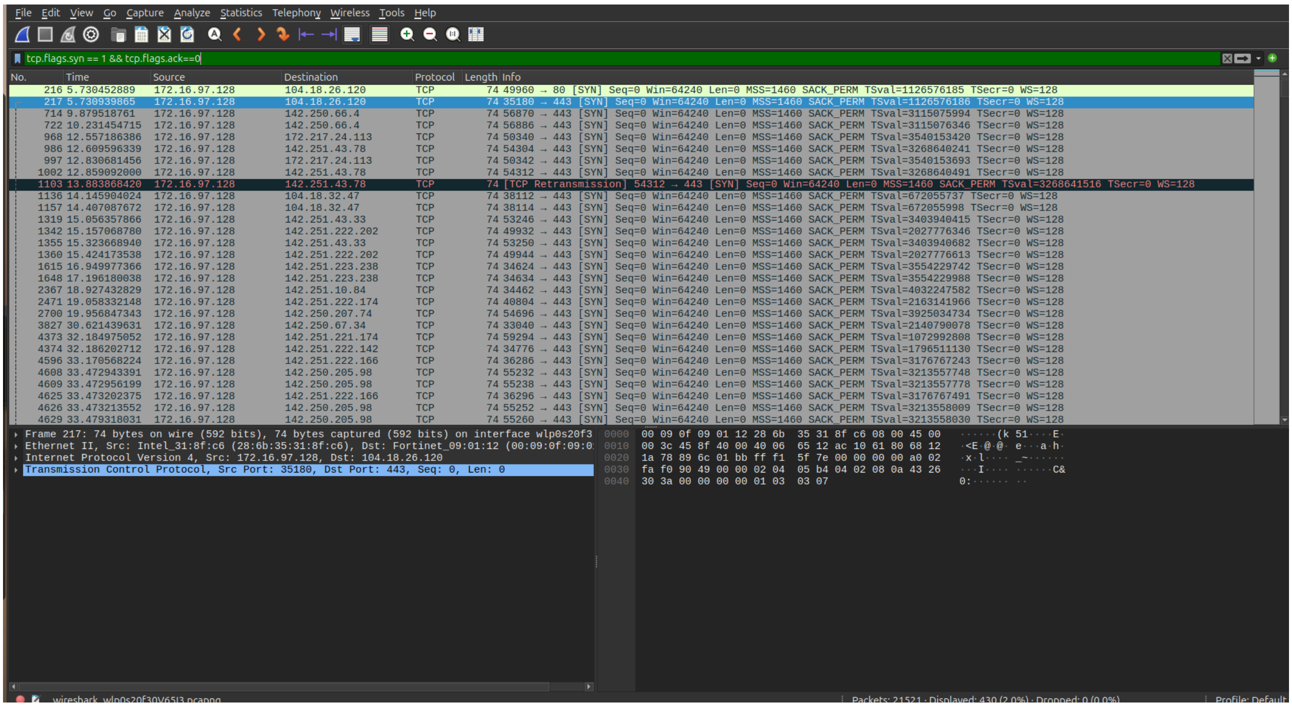
```
0020  1a 78 c3 28 00 50 e0 71  43 a3 08 53 4f 1c 80 18   ·x·(·P·q C··SO···
0030  01 f6 91 94 00 00 01 01  08 0a 43 26 30 3d 02 1f   ········ ··C&0=··
0040  76 d5 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   v·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  65 78 61 6d 70 6c 65 2e   ··Host:  example.
0060  63 6f 6d 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   com··Use r-Agent:
0070  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 58 31    Mozilla /5.0 (X1
0080  31 3b 20 55 62 75 6e 74  75 3b 20 4c 69 6e 75 78   1; Ubunt u; Linux
0090  20 78 38 36 5f 36 34 3b  20 72 76 3a 31 34 37 2e    x86_64;  rv:147.
00a0  30 29 20 47 65 63 6b 6f  2f 32 30 31 30 30 31 30   0) Gecko /2010010
00b0  31 20 46 69 72 65 66 6f  78 2f 31 34 37 2e 30 0d   1 Firefo x/147.0·
00c0  0a 41 63 63 65 70 74 3a  20 74 65 78 74 2f 68 74   ·Accept:  text/ht
00d0  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
00e0  68 74 6d 6c 2b 78 6d 6c  2c 61 70 70 6c 69 63 61   html+xml ,applica
00f0  74 69 6f 6e 2f 78 6d 6c  3b 71 3d 30 2e 39 2c 2a   tion/xml ;q=0.9,*
0100  2f 2a 3b 71 3d 30 2e 38  0d 0a 41 63 63 65 70 74   /*;q=0.8 ··Accept
0110  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
0120  2c 65 6e 3b 71 3d 30 2e  39 0d 0a 41 63 63 65 70   ,en;q=0. 9··Accep
0130  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 67 7a 69 70   t-Encodi ng: gzip
0140  2c 20 64 65 66 6c 61 74  65 0d 0a 43 6f 6e 6e 65   , deflat e··Conne
0150  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
0160  65 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   e··Upgra de-Insec
0170  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
```

```
Flags (12 bits) (tcp.flags), 2 bytes    Packets: 21521 · Displayed: 10945 (50.9%) · Dropped: 0 (0.0%)    Profile: Default
```

8) TCP Traffic Analysis

This sequence represents the TCP three-way handshake used to establish a reliable connection.

1. SYN


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1 && tcp.flags.ack==0
```

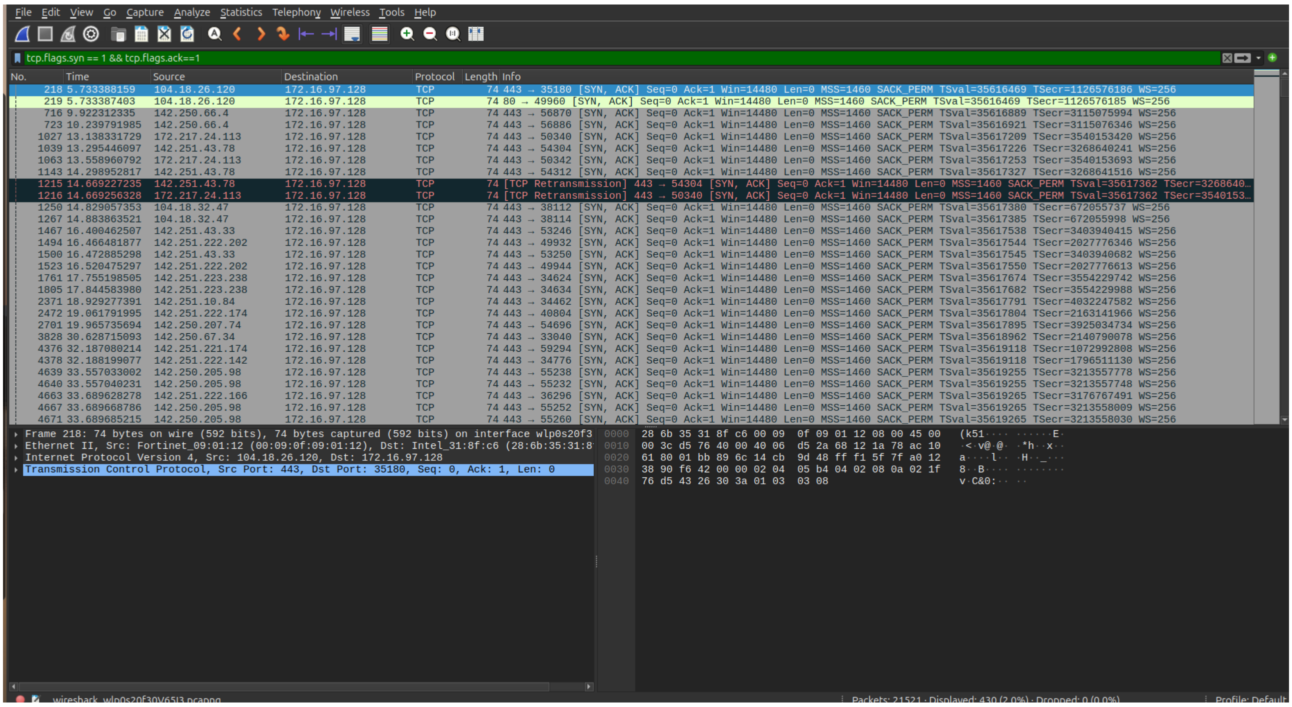
```
No.   Time           Source          Destination       Protocol  Length Info
  216 5.730452889    172.16.97.128   104.18.26.120     TCP       74 49960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1126576185 TSecr=0 WS=128
  217 5.730939865    172.16.97.128   104.18.26.120     TCP       74 35180 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1126576186 TSecr=0 WS=128
  714 9.879518761    172.16.97.128   142.250.66.4      TCP       74 56870 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3115075994 TSecr=0 WS=128
  722 10.231454715   172.16.97.128   142.250.66.4      TCP       74 56886 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3115076346 TSecr=0 WS=128
  968 12.557186386   172.16.97.128   172.217.24.113    TCP       74 50340 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3540153420 TSecr=0 WS=128
  986 12.609596339   172.16.97.128   142.251.43.78     TCP       74 54304 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3268640241 TSecr=0 WS=128
  997 12.830681456   172.16.97.128   172.217.24.113    TCP       74 50342 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3540153693 TSecr=0 WS=128
 1002 12.859092000   172.16.97.128   142.251.43.78     TCP       74 54312 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3268640491 TSecr=0 WS=128
 1103 13.883868420   172.16.97.128   142.251.43.78     TCP       74 [TCP Retransmission] 54312 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3268641516 TSecr=0 WS=128
 1136 14.145904024   172.16.97.128   104.18.32.47      TCP       74 38112 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=672055737 TSecr=0 WS=128
 1157 14.407087672   172.16.97.128   104.18.32.47      TCP       74 38114 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=672055998 TSecr=0 WS=128
 1319 15.056357866   172.16.97.128   142.251.43.33     TCP       74 53246 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3403940415 TSecr=0 WS=128
 1342 15.157068780   172.16.97.128   142.251.222.202   TCP       74 49932 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2027776346 TSecr=0 WS=128
 1355 15.323668940   172.16.97.128   142.251.43.33     TCP       74 53250 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3403940682 TSecr=0 WS=128
 1360 15.424173538   172.16.97.128   142.251.222.202   TCP       74 49944 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2027776613 TSecr=0 WS=128
 1615 16.949977366   172.16.97.128   142.251.223.238   TCP       74 34624 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3554229742 TSecr=0 WS=128
 1648 17.196180038   172.16.97.128   142.251.223.238   TCP       74 34634 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3554229988 TSecr=0 WS=128
 2367 18.927432829   172.16.97.128   142.251.10.84     TCP       74 34462 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4032247582 TSecr=0 WS=128
 2471 19.058332148   172.16.97.128   142.251.222.174   TCP       74 40804 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2163141966 TSecr=0 WS=128
 2700 19.956847343   172.16.97.128   142.250.207.74    TCP       74 54696 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3925034734 TSecr=0 WS=128
 3827 30.621439631   172.16.97.128   142.250.67.34     TCP       74 33040 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2140790078 TSecr=0 WS=128
 4373 32.184975052   172.16.97.128   142.251.221.174   TCP       74 59294 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1072992808 TSecr=0 WS=128
 4374 32.186202712   172.16.97.128   142.251.222.142   TCP       74 34776 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1796511130 TSecr=0 WS=128
 4596 33.170568224   172.16.97.128   142.251.222.166   TCP       74 36286 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3176767243 TSecr=0 WS=128
 4608 33.472943391   172.16.97.128   142.250.205.98    TCP       74 55232 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3213557748 TSecr=0 WS=128
 4609 33.472956199   172.16.97.128   142.250.205.98    TCP       74 55238 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3213557778 TSecr=0 WS=128
 4625 33.473202375   172.16.97.128   142.251.222.166   TCP       74 36296 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3176767491 TSecr=0 WS=128
 4626 33.473213552   172.16.97.128   142.250.205.98    TCP       74 55252 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3213558009 TSecr=0 WS=128
 4629 33.479318031   172.16.97.128   142.250.205.98    TCP       74 55260 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3213558030 TSecr=0 WS=128
```

```
› Frame 217: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3
› Ethernet II, Src: Intel_31:8f:c6 (28:6b:35:31:8f:c6), Dst: Fortinet_09:01:12 (00:09:0f:09:0
› Internet Protocol Version 4, Src: 172.16.97.128, Dst: 104.18.26.120
› Transmission Control Protocol, Src Port: 35180, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 09 0f 09 01 12 28 6b  35 31 8f c6 08 00 45 00   ······(k 51····E·
0010  00 3c 45 8f 40 00 40 06  65 12 ac 10 61 80 68 12   ·<E·@·@· e···a·h·
0020  1a 78 89 6c 01 bb ff f1  5f 7e 00 00 00 00 a0 02   ·x·l···· _~······
0030  fa f0 90 49 00 00 02 04  05 b4 04 02 08 0a 43 26   ···I···· ······C&
0040  30 3a 00 00 00 00 01 03  03 07                     0:······ ··
```

wireshark_wlp0s20f30V65I3.pcapng   Packets: 21521 · Displayed: 430 (2.0%) · Dropped: 0 (0.0%)   Profile: Default

2.SYN + ACK


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.syn == 1 && tcp.flags.ack==1
```

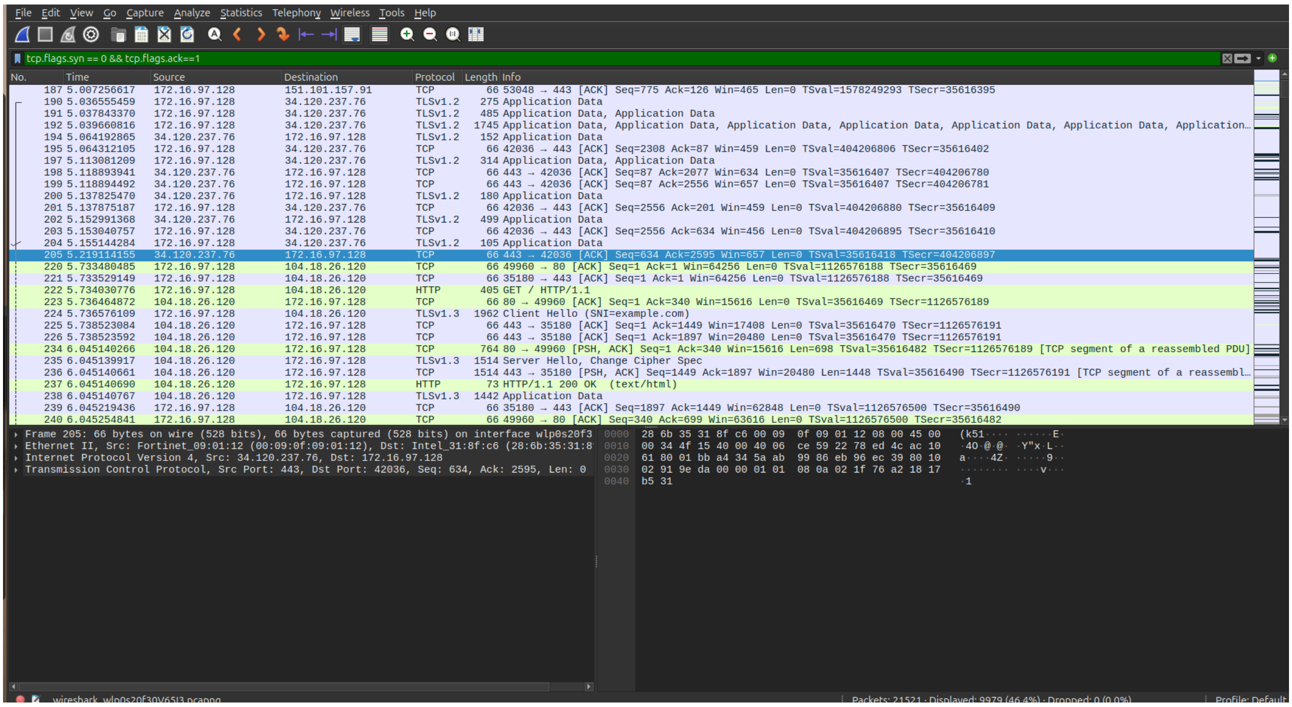
```
No.   Time           Source            Destination     Protocol  Length Info
  218 5.733388159    104.18.26.120     172.16.97.128   TCP       74 443 → 35180 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35616469 TSecr=1126576186 WS=256
  219 5.733387403    104.18.26.120     172.16.97.128   TCP       74 80 → 49960 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35616469 TSecr=1126576185 WS=256
  716 9.922312335    142.250.66.4      172.16.97.128   TCP       74 443 → 56870 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35616889 TSecr=3115075994 WS=256
  723 10.239791985   142.250.66.4      172.16.97.128   TCP       74 443 → 56886 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35616921 TSecr=3115076346 WS=256
 1027 13.138331729   172.217.24.113    172.16.97.128   TCP       74 443 → 50340 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617209 TSecr=3540153420 WS=256
 1039 13.295446097   142.251.43.78     172.16.97.128   TCP       74 443 → 54304 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617226 TSecr=3268640241 WS=256
 1063 13.558960792   172.217.24.113    172.16.97.128   TCP       74 443 → 50342 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617253 TSecr=3540153693 WS=256
 1143 14.298952817   142.251.43.78     172.16.97.128   TCP       74 443 → 54312 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617327 TSecr=3268641516 WS=256
 1215 14.669227235   142.251.43.78     172.16.97.128   TCP       74 [TCP Retransmission] 443 → 54304 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617362 TSecr=3268640…
 1216 14.669256328   172.217.24.113    172.16.97.128   TCP       74 [TCP Retransmission] 443 → 50340 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617362 TSecr=3540153…
 1250 14.829057353   104.18.32.47      172.16.97.128   TCP       74 443 → 38112 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617380 TSecr=672055737 WS=256
 1267 14.883863521   104.18.32.47      172.16.97.128   TCP       74 443 → 38114 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617385 TSecr=672055998 WS=256
 1467 16.400462507   142.251.43.33     172.16.97.128   TCP       74 443 → 53246 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617538 TSecr=3403940415 WS=256
 1494 16.466481877   142.251.222.202   172.16.97.128   TCP       74 443 → 49932 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617544 TSecr=2027776346 WS=256
 1500 16.472885298   142.251.43.33     172.16.97.128   TCP       74 443 → 53250 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617545 TSecr=3403940682 WS=256
 1523 16.520475297   142.251.222.202   172.16.97.128   TCP       74 443 → 49944 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617550 TSecr=2027776613 WS=256
 1761 17.755198505   142.251.223.238   172.16.97.128   TCP       74 443 → 34624 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617674 TSecr=3554229742 WS=256
 1805 17.844583980   142.251.223.238   172.16.97.128   TCP       74 443 → 34634 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617682 TSecr=3554229988 WS=256
 2371 18.929277391   142.251.10.84     172.16.97.128   TCP       74 443 → 34462 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617791 TSecr=4032247582 WS=256
 2472 19.061791995   142.251.222.174   172.16.97.128   TCP       74 443 → 40804 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617804 TSecr=2163141966 WS=256
 2701 19.965735694   142.250.207.74    172.16.97.128   TCP       74 443 → 54696 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35617895 TSecr=3925034734 WS=256
 3828 30.628715093   142.250.67.34     172.16.97.128   TCP       74 443 → 33040 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35618962 TSecr=2140790078 WS=256
 4376 32.187080214   142.251.221.174   172.16.97.128   TCP       74 443 → 59294 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35619118 TSecr=1072992808 WS=256
 4378 32.188199077   142.251.222.142   172.16.97.128   TCP       74 443 → 34776 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35619118 TSecr=1796511130 WS=256
 4639 33.557033002   142.250.205.98    172.16.97.128   TCP       74 443 → 55238 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35619255 TSecr=3213557778 WS=256
 4640 33.557040231   142.250.205.98    172.16.97.128   TCP       74 443 → 55232 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35619255 TSecr=3213557748 WS=256
 4663 33.689628278   142.251.222.166   172.16.97.128   TCP       74 443 → 36296 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35619265 TSecr=3176767491 WS=256
 4667 33.689668786   142.250.205.98    172.16.97.128   TCP       74 443 → 55252 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35619265 TSecr=3213558009 WS=256
 4671 33.689685215   142.250.205.98    172.16.97.128   TCP       74 443 → 55260 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=35619265 TSecr=3213558030 WS=256
```

```
› Frame 218: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlp0s20f3
› Ethernet II, Src: Fortinet_09:01:12 (00:09:0f:09:01:12), Dst: Intel_31:8f:c6 (28:6b:35:31:8
› Internet Protocol Version 4, Src: 104.18.26.120, Dst: 172.16.97.128
› Transmission Control Protocol, Src Port: 443, Dst Port: 35180, Seq: 0, Ack: 1, Len: 0
```

```
0000  28 6b 35 31 8f c6 00 09  0f 09 01 12 08 00 45 00   (k51···· ······E·
0010  00 3c d5 76 40 00 40 06  d5 2a 68 12 1a 78 ac 10   ·<·v@·@· ·*h··x··
0020  61 80 01 bb 89 6c 14 cb  9d 48 ff f1 5f 7f a0 12   a····l·· ·H··_···
0030  38 90 f6 42 00 00 02 04  05 b4 04 02 08 0a 02 1f   8··B···· ········
0040  76 d5 43 26 30 3a 01 03  03 08                     v·C&0:·· ··
```

wireshark_wlp0s20f30V65I3.pcapng   Packets: 21521 · Displayed: 430 (2.0%) · Dropped: 0 (0.0%)   Profile: Default

3.ACK


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 0 && tcp.flags.ack==1

```
No.   Time         Source          Destination     Protocol Length Info
  187 5.007256617  172.16.97.128   151.101.157.91  TCP        66 53048 → 443 [ACK] Seq=775 Ack=126 Win=465 Len=0 TSval=1578249293 TSecr=35616395
  190 5.036555459  172.16.97.128   34.120.237.76   TLSv1.2   275 Application Data
  191 5.037843370  172.16.97.128   34.120.237.76   TLSv1.2   485 Application Data, Application Data
  192 5.039660816  172.16.97.128   34.120.237.76   TLSv1.2  1745 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application…
  194 5.064192865  34.120.237.76   172.16.97.128   TLSv1.2   152 Application Data
  195 5.064312105  172.16.97.128   34.120.237.76   TCP        66 42036 → 443 [ACK] Seq=2308 Ack=87 Win=459 Len=0 TSval=404206806 TSecr=35616402
  197 5.113081209  172.16.97.128   34.120.237.76   TLSv1.2   314 Application Data, Application Data
  198 5.118893941  34.120.237.76   172.16.97.128   TCP        66 443 → 42036 [ACK] Seq=87 Ack=2077 Win=634 Len=0 TSval=35616407 TSecr=404206780
  199 5.118894492  34.120.237.76   172.16.97.128   TCP        66 443 → 42036 [ACK] Seq=87 Ack=2556 Win=657 Len=0 TSval=35616407 TSecr=404206781
  200 5.137825470  34.120.237.76   172.16.97.128   TLSv1.2   180 Application Data
  201 5.137875187  172.16.97.128   34.120.237.76   TCP        66 42036 → 443 [ACK] Seq=2556 Ack=201 Win=459 Len=0 TSval=404206880 TSecr=35616409
  202 5.152991368  34.120.237.76   172.16.97.128   TLSv1.2   499 Application Data
  203 5.153040757  172.16.97.128   34.120.237.76   TCP        66 42036 → 443 [ACK] Seq=2556 Ack=634 Win=456 Len=0 TSval=404206895 TSecr=35616410
  204 5.155144284  172.16.97.128   34.120.237.76   TLSv1.2   105 Application Data
  205 5.219114155  34.120.237.76   172.16.97.128   TCP        66 443 → 42036 [ACK] Seq=634 Ack=2595 Win=657 Len=0 TSval=35616418 TSecr=404206897
  220 5.733480485  172.16.97.128   104.18.26.120   TCP        66 49960 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1126576188 TSecr=35616469
  221 5.733529149  172.16.97.128   104.18.26.120   TCP        66 35180 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1126576188 TSecr=35616469
  222 5.734030776  172.16.97.128   104.18.26.120   HTTP      405 GET / HTTP/1.1
  223 5.736464872  104.18.26.120   172.16.97.128   TCP        66 80 → 49960 [ACK] Seq=1 Ack=340 Win=15616 Len=0 TSval=35616469 TSecr=1126576189
  224 5.736576109  172.16.97.128   104.18.26.120   TLSv1.3  1962 Client Hello (SNI=example.com)
  225 5.738523084  104.18.26.120   172.16.97.128   TCP        66 443 → 35180 [ACK] Seq=1 Ack=1449 Win=17408 Len=0 TSval=35616470 TSecr=1126576191
  226 5.738523592  104.18.26.120   172.16.97.128   TCP        66 443 → 35180 [ACK] Seq=1 Ack=1897 Win=20480 Len=0 TSval=35616470 TSecr=1126576191
  234 6.045140266  104.18.26.120   172.16.97.128   TCP       764 80 → 49960 [PSH, ACK] Seq=1 Ack=340 Win=15616 Len=698 TSval=35616482 TSecr=1126576189 [TCP segment of a reassembled PDU]
  235 6.045139917  104.18.26.120   172.16.97.128   TLSv1.3  1514 Server Hello, Change Cipher Spec
  236 6.045140661  104.18.26.120   172.16.97.128   TCP      1514 443 → 35180 [PSH, ACK] Seq=1449 Ack=1897 Win=20480 Len=1448 TSval=35616490 TSecr=1126576191 [TCP segment of a reassembl…
  237 6.045140690  104.18.26.120   172.16.97.128   HTTP       73 HTTP/1.1 200 OK  (text/html)
  238 6.045140767  104.18.26.120   172.16.97.128   TLSv1.3  1442 Application Data
  239 6.045219436  172.16.97.128   104.18.26.120   TCP        66 35180 → 443 [ACK] Seq=1897 Ack=1449 Win=62848 Len=0 TSval=1126576500 TSecr=35616490
  240 6.045254841  172.16.97.128   104.18.26.120   TCP        66 49960 → 80 [ACK] Seq=340 Ack=699 Win=63616 Len=0 TSval=1126576500 TSecr=35616482
```

```
› Frame 205: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp0s20f3
› Ethernet II, Src: Fortinet_09:01:12 (00:09:0f:09:01:12), Dst: Intel_31:8f:c6 (28:6b:35:31:8f
› Internet Protocol Version 4, Src: 34.120.237.76, Dst: 172.16.97.128
› Transmission Control Protocol, Src Port: 443, Dst Port: 42036, Seq: 634, Ack: 2595, Len: 0
```

```
0000  28 6b 35 31 8f c6 00 09  0f 09 01 12 08 00 45 00   (k51···· ······E·
0010  00 34 4f 15 40 00 40 06  ce 59 22 78 ed 4c ac 10   ·4O·@·@· ·Y"x·L··
0020  61 80 01 bb a4 34 5a ab  99 86 eb 96 ec 39 80 10   a····4Z· ·····9··
0030  02 91 9e da 00 00 01 01  08 0a 02 1f 76 a2 18 17   ········ ····v···
0040  b5 31                                              ·1
```

wireshark_wlp0s20f30V65I3.pcapng | Packets: 21521 · Displayed: 9979 (46.4%) · Dropped: 0 (0.0%) | Profile: Default

9) Encrypted Traffic Analysis (HTTPS)

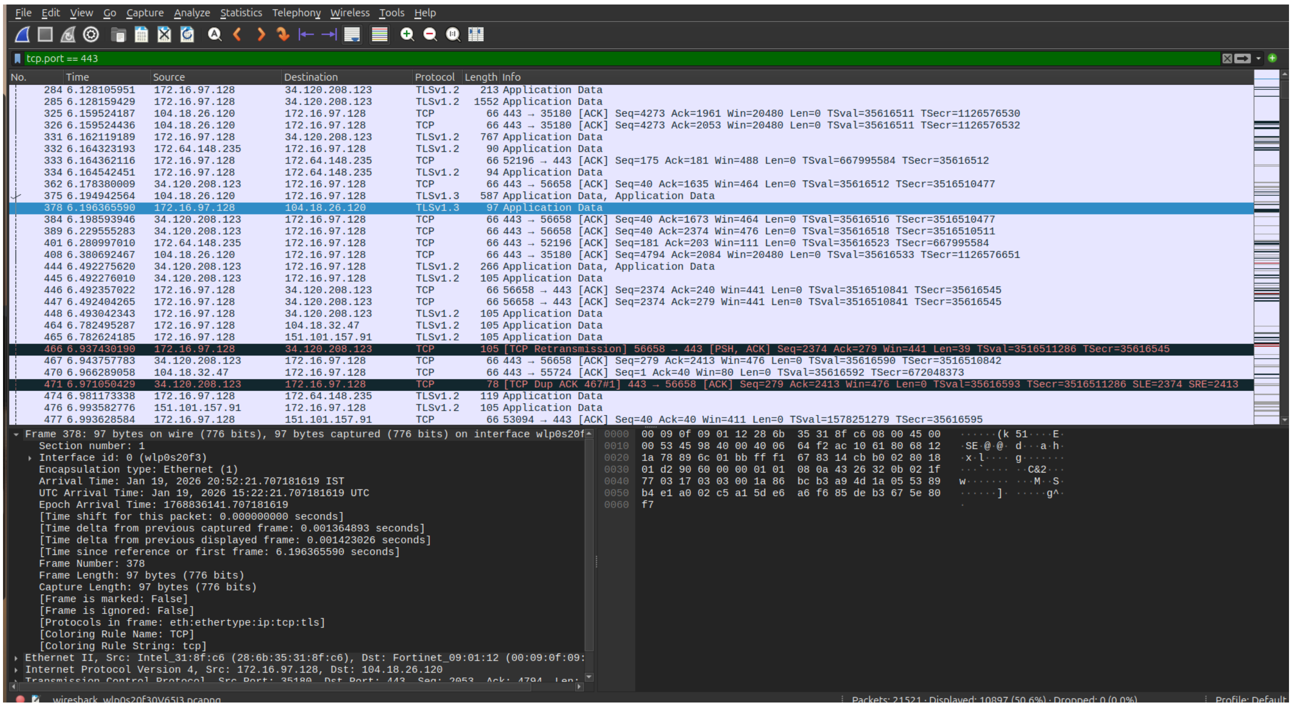
Display Filter Used: `tls` or `tcp.port == 443`

HTTPS traffic was analyzed and identified as encrypted communication.

Observations:

- Traffic appeared as TLS packets
- Packet contents were not readable
- Encryption protects data confidentiality

HTTPS Encrypted Traffic:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

```
No.   Time         Source          Destination     Protocol Length Info
  284 6.128105951  172.16.97.128   34.120.208.123  TLSv1.2   213 Application Data
  285 6.128159429  172.16.97.128   34.120.208.123  TLSv1.2  1552 Application Data
  325 6.159524187  104.18.26.120   172.16.97.128   TCP        66 443 → 35180 [ACK] Seq=4273 Ack=1961 Win=20480 Len=0 TSval=35616511 TSecr=1126576530
  326 6.159524436  104.18.26.120   172.16.97.128   TCP        66 443 → 35180 [ACK] Seq=4273 Ack=2053 Win=20480 Len=0 TSval=35616511 TSecr=1126576532
  331 6.162119189  172.16.97.128   34.120.208.123  TLSv1.2   767 Application Data
  332 6.164323193  172.64.148.235  172.16.97.128   TLSv1.2    90 Application Data
  333 6.164362116  172.16.97.128   172.64.148.235  TCP        66 52196 → 443 [ACK] Seq=175 Ack=181 Win=488 Len=0 TSval=667995584 TSecr=35616512
  334 6.164542451  172.16.97.128   172.64.148.235  TLSv1.2    94 Application Data
  362 6.178380009  34.120.208.123  172.16.97.128   TCP        66 443 → 56658 [ACK] Seq=40 Ack=1635 Win=464 Len=0 TSval=35616512 TSecr=3516510477
  375 6.194942564  104.18.26.120   172.16.97.128   TLSv1.3   587 Application Data, Application Data
  378 6.196365590  172.16.97.128   104.18.26.120   TLSv1.3    97 Application Data
  384 6.198593946  34.120.208.123  172.16.97.128   TCP        66 443 → 56658 [ACK] Seq=40 Ack=1673 Win=464 Len=0 TSval=35616516 TSecr=3516510477
  389 6.229555283  34.120.208.123  172.16.97.128   TCP        66 443 → 56658 [ACK] Seq=40 Ack=2374 Win=476 Len=0 TSval=35616518 TSecr=3516510511
  401 6.280997010  172.64.148.235  172.16.97.128   TCP        66 443 → 52196 [ACK] Seq=181 Ack=203 Win=111 Len=0 TSval=35616523 TSecr=667995584
  408 6.380692467  104.18.26.120   172.16.97.128   TCP        66 443 → 35180 [ACK] Seq=4794 Ack=2084 Win=20480 Len=0 TSval=35616533 TSecr=1126576651
  444 6.492275620  34.120.208.123  172.16.97.128   TLSv1.2   266 Application Data, Application Data
  445 6.492276010  34.120.208.123  172.16.97.128   TLSv1.2   105 Application Data
  446 6.492357022  172.16.97.128   34.120.208.123  TCP        66 56658 → 443 [ACK] Seq=2374 Ack=240 Win=441 Len=0 TSval=3516510841 TSecr=35616545
  447 6.492404265  172.16.97.128   34.120.208.123  TCP        66 56658 → 443 [ACK] Seq=2374 Ack=279 Win=441 Len=0 TSval=3516510841 TSecr=35616545
  448 6.493042343  172.16.97.128   34.120.208.123  TLSv1.2   105 Application Data
  464 6.782495287  172.16.97.128   104.18.32.47    TLSv1.2   105 Application Data
  465 6.782624185  172.16.97.128   151.101.157.91  TLSv1.2   105 Application Data
  466 6.937430190  172.16.97.128   34.120.208.123  TCP       105 [TCP Retransmission] 56658 → 443 [PSH, ACK] Seq=2374 Ack=279 Win=441 Len=39 TSval=3516511286 TSecr=35616545
  467 6.943757783  34.120.208.123  172.16.97.128   TCP        66 443 → 56658 [ACK] Seq=279 Ack=2413 Win=476 Len=0 TSval=35616590 TSecr=3516510842
  470 6.966289058  104.18.32.47    172.16.97.128   TCP        66 443 → 55724 [ACK] Seq=1 Ack=40 Win=80 Len=0 TSval=35616592 TSecr=672048373
  471 6.971050429  34.120.208.123  172.16.97.128   TCP        78 [TCP Dup ACK 467#1] 443 → 56658 [ACK] Seq=279 Ack=2413 Win=476 Len=0 TSval=35616593 TSecr=3516511286 SLE=2374 SRE=2413
  474 6.981173338  172.16.97.128   172.64.148.235  TLSv1.2   119 Application Data
  476 6.993582776  151.101.157.91  172.16.97.128   TLSv1.2   105 Application Data
  477 6.993628584  172.16.97.128   151.101.157.91  TCP        66 53094 → 443 [ACK] Seq=40 Ack=40 Win=411 Len=0 TSval=1578251279 TSecr=35616595
```

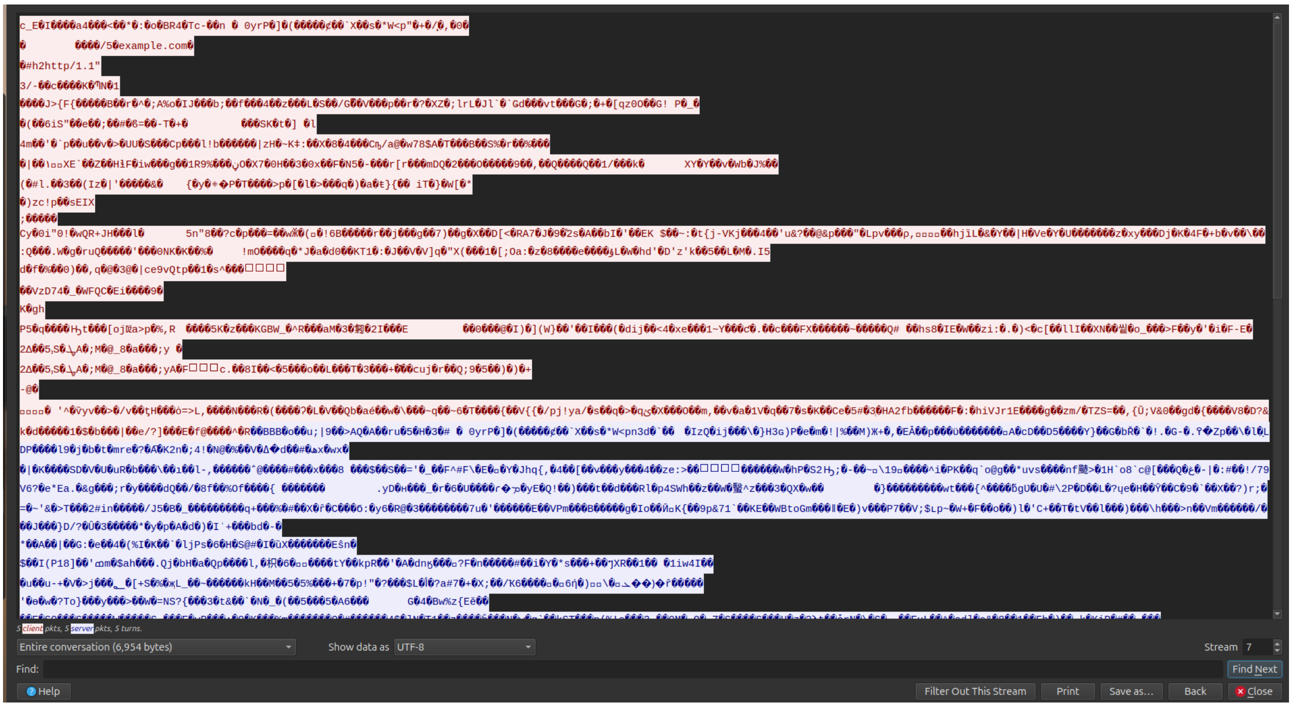
```
Frame 378: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface wlp0s20f
   Section number: 1
 > Interface id: 0 (wlp0s20f3)
   Encapsulation type: Ethernet (1)
   Arrival Time: Jan 19, 2026 20:52:21.707181619 IST
   UTC Arrival Time: Jan 19, 2026 15:22:21.707181619 UTC
   Epoch Arrival Time: 1768836141.707181619
   [Time shift for this packet: 0.000000000 seconds]
   [Time delta from previous captured frame: 0.001364893 seconds]
   [Time delta from previous displayed frame: 0.001423026 seconds]
   [Time since reference or first frame: 6.196365590 seconds]
   Frame Number: 378
   Frame Length: 97 bytes (776 bits)
   Capture Length: 97 bytes (776 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:ethertype:ip:tcp:tls]
   [Coloring Rule Name: TCP]
   [Coloring Rule String: tcp]
> Ethernet II, Src: Intel_31:8f:c6 (28:6b:35:31:8f:c6), Dst: Fortinet_09:01:12 (00:09:0f:09:
> Internet Protocol Version 4, Src: 172.16.97.128, Dst: 104.18.26.120
> Transmission Control Protocol, Src Port: 35180, Dst Port: 443, Seq: 2053, Ack: 4794, Len:
```

```
0000  00 09 0f 09 01 12 28 6b  35 31 8f c6 08 00 45 00   ······(k 51····E·
0010  00 53 45 98 40 00 40 06  64 f2 ac 10 61 80 68 12   ·SE·@·@· d···a·h·
0020  1a 78 89 6c 01 bb ff f1  67 83 14 cb b0 02 80 18   ·x·l···· g·······
0030  01 d2 90 60 00 00 01 01  08 0a 43 26 32 0b 02 1f   ···`···· ··C&2···
0040  77 03 17 03 03 00 1a 86  bc b3 a9 4d 1a 05 53 89   w······· ···M··S·
0050  b4 e1 a0 02 c5 a1 5d e6  a6 f6 85 de b3 67 5e 80   ······]· ·····g^·
0060  f7                                                 ·
```

wireshark_wlp0s20f30V65I3.pcapng

Packets: 21521 · Displayed: 10897 (50.6%) · Dropped: 0 (0.0%)

Profile: Default



```
c_E�I����a4���<��*�:�o�BR4�Tc-��n � 0yrP�]�(�����¢��`X��s�*W<p"�+�/�,�0�
�        ����/5�example.com�
�#h2http/1.1"
3/-��c����K�٦N�1
����J>{F{�����B��r�^�;A%o�IJ���b;��f���4��z���L�S��/G��V���p��r�?�XZ�;lrL�Jl`�`Gd���vt���G�;�+�[qz0O��G! P�_�
�(��6iS"��e��;��#�6=��-T�+�         ���SK�t�] �l
4m��'�`p��u��v�>�UU�S���Cp���l!b������|zH�~K‡:��X�8�4���Cђ/a@�w78$A�T���B��S%�r��%���
�|��\▫▫XE`��Z��HiF�iw���g��1R9%���ٻO�X7�0H��3�0x��F�N5�-���r[r���mDQ�2���O�����9��,��Q����Q��1/���k�      XY�Y��v�Wb�J%��
(�#l.��3��(Iz�|'�����&�    {�y�⁜�P�T����>p�[�l�>���q�)�a�ŧ}{�� iT�}�W[�*
�)zc!p��sEIX
;�����
Cy�0i"0!�wQR+JH���l�       5n"8��?c�p���=��wӜ�(▫�!6B�����r��j���g��7)��g�X��D[<�RA7�J�9�2s�A��bI�'��EK $��~:�t{j-VKj���4��'u&?��@
:Q���.W�g�ruQ�����'���0NK�K��%�     !mO����q�*J�a�d0��KT1�:�J��V�V]q�"X(���1�[;Oa:�z�8����e����ȿL�W�hd'�D'z'k��5��L�M�.I5
d�f�%��0)��,q�@�3@�|ce9vQtp��1�s^���□□□□
��VzD74�_�WFQC�Ei����9�
```

```
��J���}D/?�Û�3�����*�y�p�A�d�)�I˙+���bd�-�
*��A��|��G:�e��4�(%I�K��`�ljPs�6�H�S@#�I�ũX�������Eśn�
$��I(P18]��'ꝏm�$ah���.Qj�bH�a�Qp����l,�拫�6�▫▫����tY��kpR��'�A�dnђ���▫?F�n�����#��i�Y�*s���+��ҭXR��1�� �1iw4I��
�u��u-+�V�>j���_�[+S�%�ӿL_��~�����kH��M��5�5%���+�7�p!"�?���$L�Í�?a#7�+�X;��/K6����▫�▫6ή�)▫▫\�▫ـ��)�ȓ�����
'�e�w�?To}���y���>��W�=NS?{���3�t&��`�N�_�(��5����5�A6���       G�4�Bw%z{Eě��
```

5 client pkts, 5 server pkts, 5 turns.

Entire conversation (6,954 bytes)

Show data as UTF-8

Stream 7

Find:

10) Key Observations

- DNS traffic reveals domain names accessed by the system.
- ICMP packets confirm network connectivity.
- HTTP traffic is insecure and readable.
- HTTPS traffic is encrypted using TLS.
- Wireshark filters help isolate and analyze specific protocol.