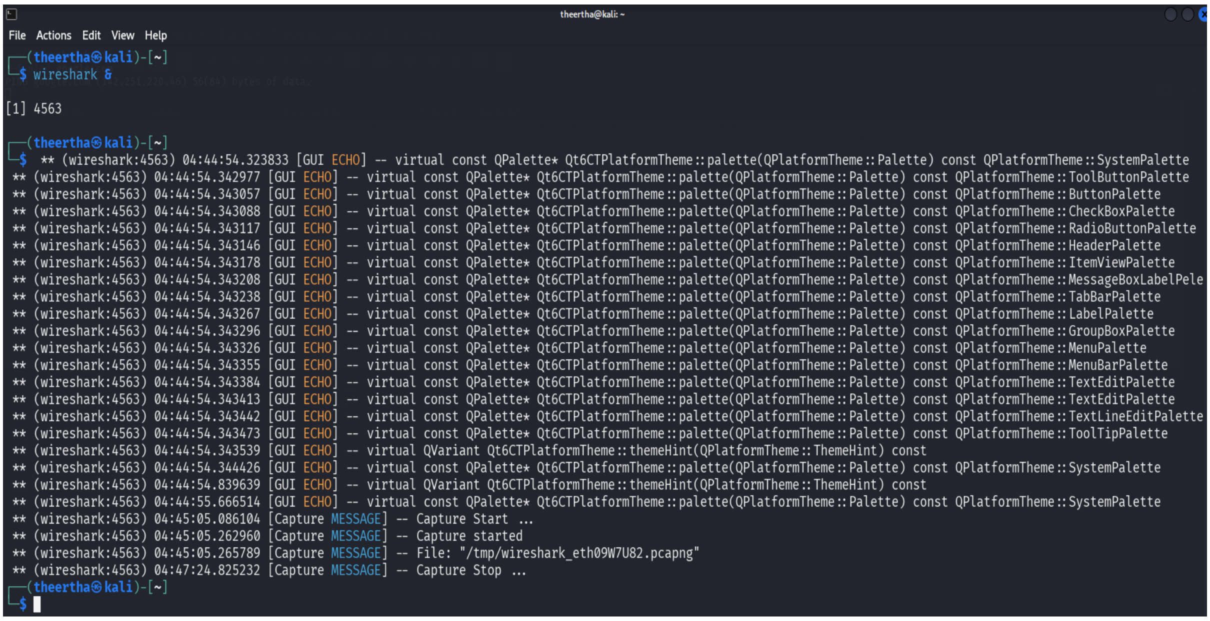
Task 5

Capture and Analyze Network Traffic Using Wireshark.

Objective: Capture live network packets and identify basic protocols and traffic types.

Launched Wireshark using:

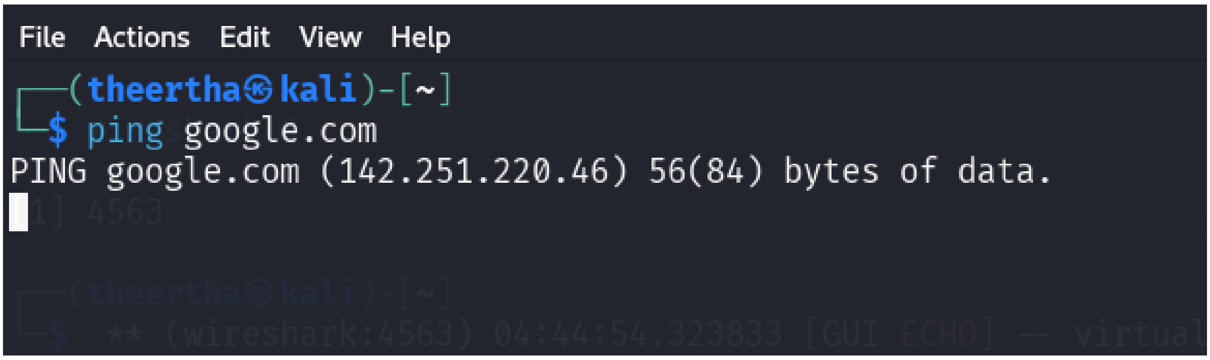
Wireshark &



```
┌──(theertha㉿kali)-[~]
└─$ wireshark &

[1] 4563

┌──(theertha㉿kali)-[~]
└─$  ** (wireshark:4563) 04:44:54.323833 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
 ** (wireshark:4563) 04:44:54.342977 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette
 ** (wireshark:4563) 04:44:54.343057 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette
 ** (wireshark:4563) 04:44:54.343088 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette
 ** (wireshark:4563) 04:44:54.343117 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette
 ** (wireshark:4563) 04:44:54.343146 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette
 ** (wireshark:4563) 04:44:54.343178 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPalette
 ** (wireshark:4563) 04:44:54.343208 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MessageBoxLabelPele
 ** (wireshark:4563) 04:44:54.343238 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TabBarPalette
 ** (wireshark:4563) 04:44:54.343267 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::LabelPalette
 ** (wireshark:4563) 04:44:54.343296 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::GroupBoxPalette
 ** (wireshark:4563) 04:44:54.343326 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuPalette
 ** (wireshark:4563) 04:44:54.343355 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuBarPalette
 ** (wireshark:4563) 04:44:54.343384 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEditPalette
 ** (wireshark:4563) 04:44:54.343413 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEditPalette
 ** (wireshark:4563) 04:44:54.343442 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextLineEditPalette
 ** (wireshark:4563) 04:44:54.343473 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolTipPalette
 ** (wireshark:4563) 04:44:54.343539 [GUI ECHO] -- virtual QVariant Qt6CTPlatformTheme::themeHint(QPlatformTheme::ThemeHint) const
 ** (wireshark:4563) 04:44:54.344426 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
 ** (wireshark:4563) 04:44:54.839639 [GUI ECHO] -- virtual QVariant Qt6CTPlatformTheme::themeHint(QPlatformTheme::ThemeHint) const
 ** (wireshark:4563) 04:44:55.666514 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
 ** (wireshark:4563) 04:45:05.086104 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:4563) 04:45:05.262960 [Capture MESSAGE] -- Capture started
 ** (wireshark:4563) 04:45:05.265789 [Capture MESSAGE] -- File: "/tmp/wireshark_eth09W7U82.pcapng"
 ** (wireshark:4563) 04:47:24.825232 [Capture MESSAGE] -- Capture Stop ...
┌──(theertha㉿kali)-[~]
└─$ 
```

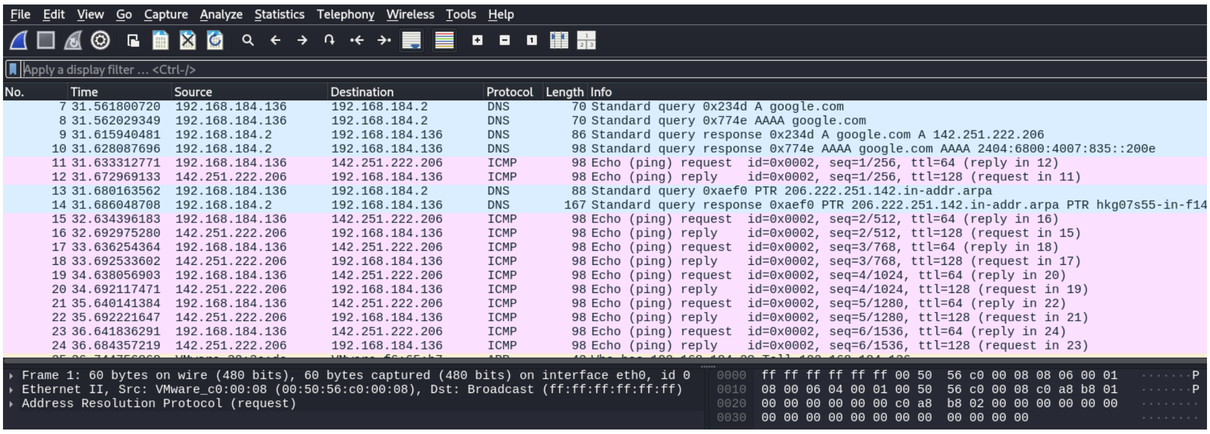
Wireshark captures live packets, but if our system is idle (no browsing, no downloads), there may be little to no traffic. Running ping ensures:

- Consistent packet flow for capture.
- Immediate ICMP Echo Requests and Replies that you can filter and analyze.



```
┌──(theertha㉿kali)-[~]
└─$ ping google.com
PING google.com (142.251.220.46) 56(84) bytes of data.
```

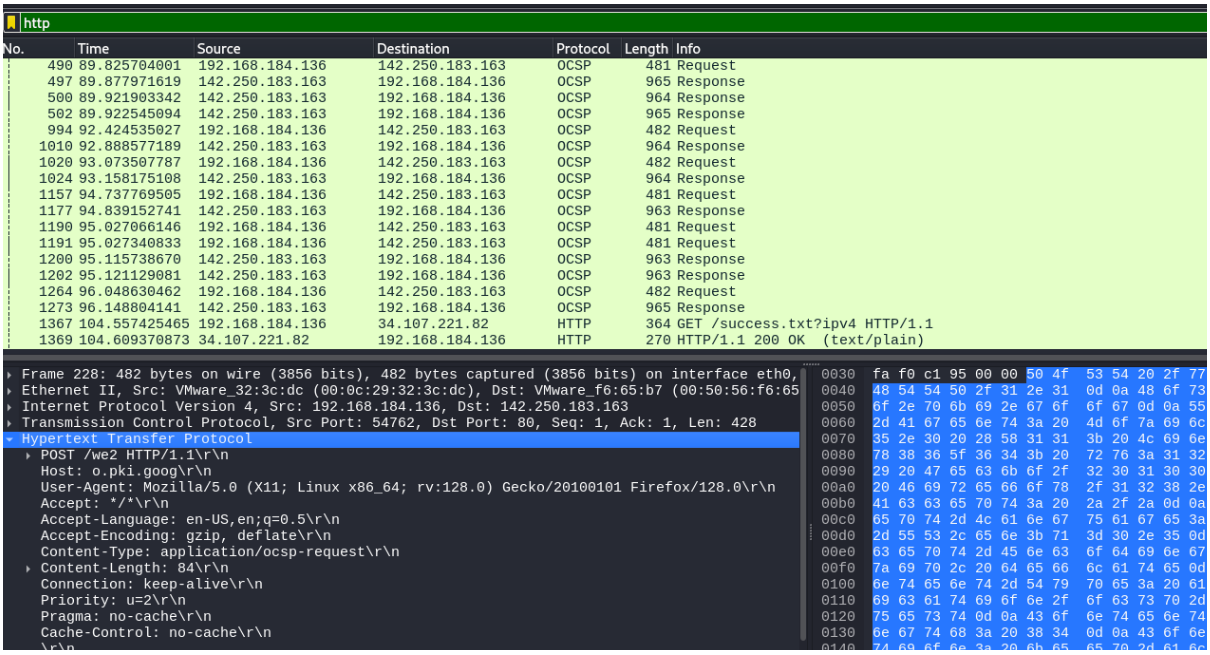
These actions generated HTTP, TCP, DNS, ICMP and TLS packets.



```
No.   Time          Source           Destination      Protocol Length Info
    7 31.561800720  192.168.184.136  192.168.184.2    DNS       70 Standard query 0x234d A google.com
    8 31.562029349  192.168.184.136  192.168.184.2    DNS       70 Standard query 0x774e AAAA google.com
    9 31.615940481  192.168.184.2    192.168.184.136  DNS       86 Standard query response 0x234d A google.com A 142.251.222.206
   10 31.628087696  192.168.184.2    192.168.184.136  DNS       98 Standard query response 0x774e AAAA google.com AAAA 2404:6800:4007:835::200e
   11 31.633312771  192.168.184.136  142.251.222.206  ICMP      98 Echo (ping) request  id=0x0002, seq=1/256, ttl=64 (reply in 12)
   12 31.672969133  142.251.222.206  192.168.184.136  ICMP      98 Echo (ping) reply    id=0x0002, seq=1/256, ttl=128 (request in 11)
   13 31.680163562  192.168.184.136  192.168.184.2    DNS       88 Standard query 0xaef0 PTR 206.222.251.142.in-addr.arpa
   14 31.686048708  192.168.184.2    192.168.184.136  DNS      167 Standard query response 0xaef0 PTR 206.222.251.142.in-addr.arpa PTR hkg07s55-in-f14
   15 32.634396183  192.168.184.136  142.251.222.206  ICMP      98 Echo (ping) request  id=0x0002, seq=2/512, ttl=64 (reply in 16)
   16 32.692975280  142.251.222.206  192.168.184.136  ICMP      98 Echo (ping) reply    id=0x0002, seq=2/512, ttl=128 (request in 15)
   17 33.636254364  192.168.184.136  142.251.222.206  ICMP      98 Echo (ping) request  id=0x0002, seq=3/768, ttl=64 (reply in 18)
   18 33.692533602  142.251.222.206  192.168.184.136  ICMP      98 Echo (ping) reply    id=0x0002, seq=3/768, ttl=128 (request in 17)
   19 34.638056903  192.168.184.136  142.251.222.206  ICMP      98 Echo (ping) request  id=0x0002, seq=4/1024, ttl=64 (reply in 20)
   20 34.692117471  142.251.222.206  192.168.184.136  ICMP      98 Echo (ping) reply    id=0x0002, seq=4/1024, ttl=128 (request in 19)
   21 35.640141384  192.168.184.136  142.251.222.206  ICMP      98 Echo (ping) request  id=0x0002, seq=5/1280, ttl=64 (reply in 22)
   22 35.692221647  142.251.222.206  192.168.184.136  ICMP      98 Echo (ping) reply    id=0x0002, seq=5/1280, ttl=128 (request in 21)
   23 36.641836291  192.168.184.136  142.251.222.206  ICMP      98 Echo (ping) request  id=0x0002, seq=6/1536, ttl=64 (reply in 24)
   24 36.684357219  142.251.222.206  192.168.184.136  ICMP      98 Echo (ping) reply    id=0x0002, seq=6/1536, ttl=128 (request in 23)
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

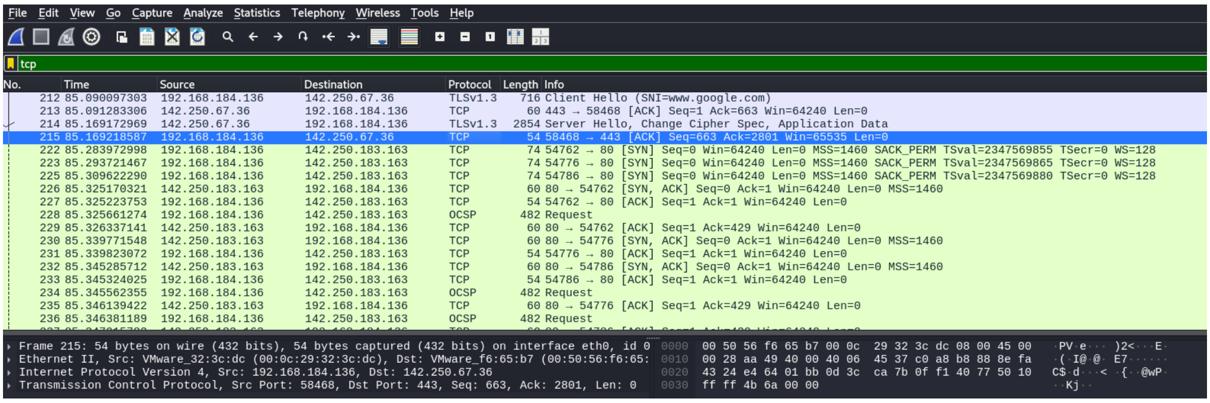
```
0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08 06 00 01   .......P
0010  08 00 06 04 00 01 00 50  56 c0 00 08 c0 a8 b8 01   .......P
0020  00 00 00 00 00 00 c0 a8  b8 02 00 00 00 00 00 00   ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........
```



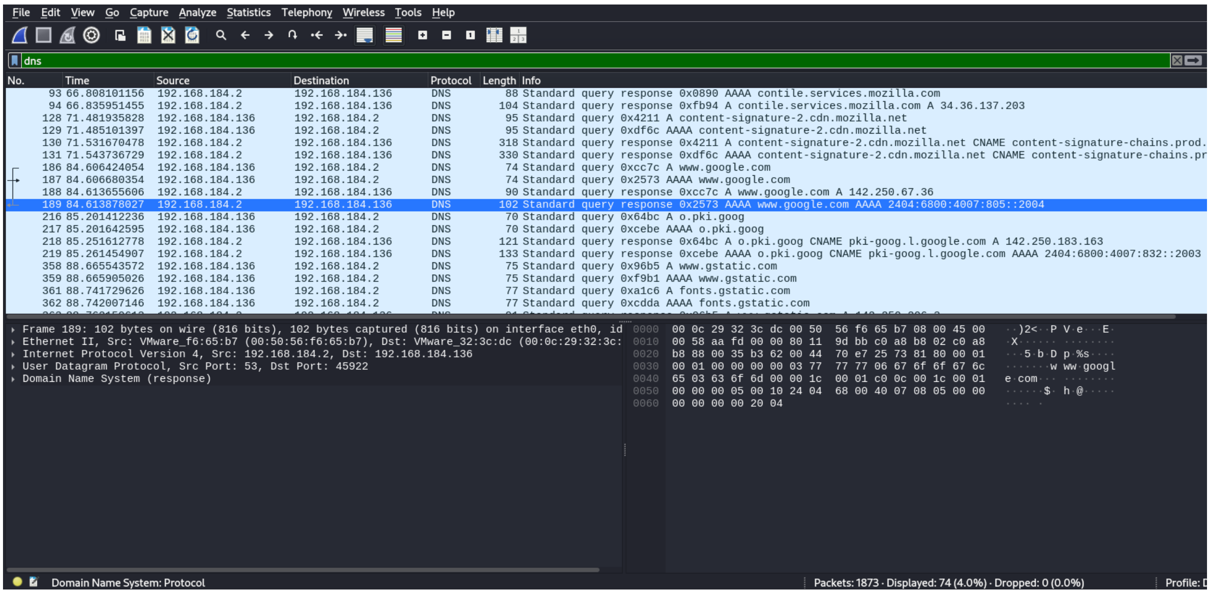
```
No.   Time           Source           Destination      Protocol Length Info
  490 89.825704001   192.168.184.136  142.250.183.163  OCSP     481 Request
  497 89.877971619   142.250.183.163  192.168.184.136  OCSP     965 Response
  500 89.921903342   142.250.183.163  192.168.184.136  OCSP     964 Response
  502 89.922545094   142.250.183.163  192.168.184.136  OCSP     965 Response
  994 92.424535027   192.168.184.136  142.250.183.163  OCSP     482 Request
 1010 92.888577189   142.250.183.163  192.168.184.136  OCSP     964 Response
 1020 93.073507787   192.168.184.136  142.250.183.163  OCSP     482 Request
 1024 93.158175108   142.250.183.163  192.168.184.136  OCSP     964 Response
 1157 94.737769505   192.168.184.136  142.250.183.163  OCSP     481 Request
 1177 94.839152741   142.250.183.163  192.168.184.136  OCSP     963 Response
 1190 95.027066146   192.168.184.136  142.250.183.163  OCSP     481 Request
 1191 95.027340833   192.168.184.136  142.250.183.163  OCSP     481 Request
 1200 95.115738670   142.250.183.163  192.168.184.136  OCSP     963 Response
 1202 95.121129081   142.250.183.163  192.168.184.136  OCSP     963 Response
 1264 96.048630462   192.168.184.136  142.250.183.163  OCSP     482 Request
 1273 96.148804141   142.250.183.163  192.168.184.136  OCSP     965 Response
 1367 104.557425465  192.168.184.136  34.107.221.82    HTTP     364 GET /success.txt?ipv4 HTTP/1.1
 1369 104.609370873  34.107.221.82    192.168.184.136  HTTP     270 HTTP/1.1 200 OK  (text/plain)
```

```
› Frame 228: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface eth0,
› Ethernet II, Src: VMware_32:3c:dc (00:0c:29:32:3c:dc), Dst: VMware_f6:65:b7 (00:50:56:f6:65
› Internet Protocol Version 4, Src: 192.168.184.136, Dst: 142.250.183.163
› Transmission Control Protocol, Src Port: 54762, Dst Port: 80, Seq: 1, Ack: 1, Len: 428
⌄ Hypertext Transfer Protocol
  › POST /we2 HTTP/1.1\r\n
    Host: o.pki.goog\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/ocsp-request\r\n
  › Content-Length: 84\r\n
    Connection: keep-alive\r\n
    Priority: u=2\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
```

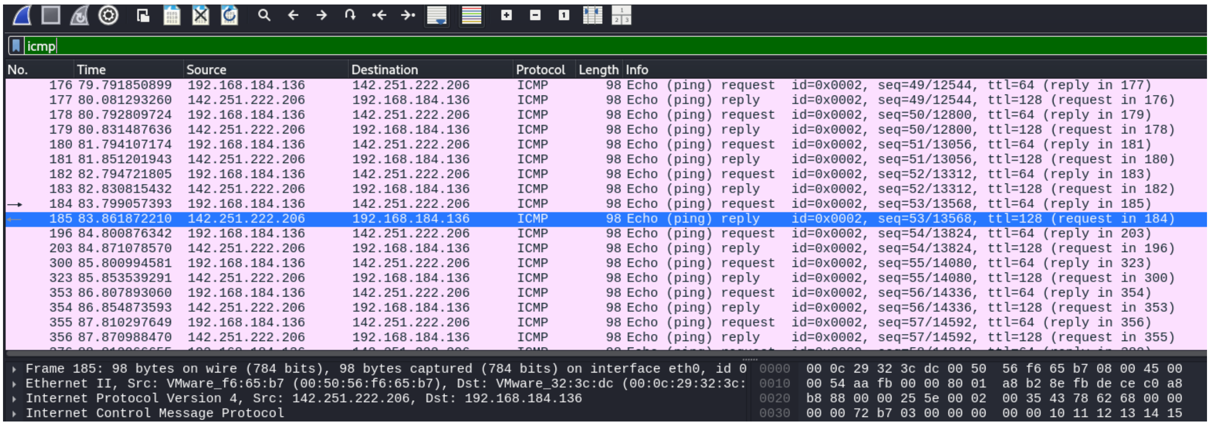
```
0030  fa f0 c1 95 00 00 50 4f  53 54 20 2f 77
0040  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73
0050  6f 2e 70 6b 69 2e 67 6f  6f 67 0d 0a 55
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c
0070  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e
0080  78 38 36 5f 36 34 3b 20  72 76 3a 31 32
0090  29 20 47 65 63 6b 6f 2f  32 30 31 30 30
00a0  20 46 69 72 65 66 6f 78  2f 31 32 38 2e
00b0  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a
00c0  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a
00d0  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d
00e0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67
00f0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d
0100  6e 74 65 6e 74 2d 54 79  70 65 3a 20 61
0110  69 63 61 74 69 6f 6e 2f  6f 63 73 70 2d
0120  75 65 73 74 0d 0a 43 6f  6e 74 65 6e 74
0130  6e 67 74 68 3a 20 38 34  0d 0a 43 6f 6e
0140  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

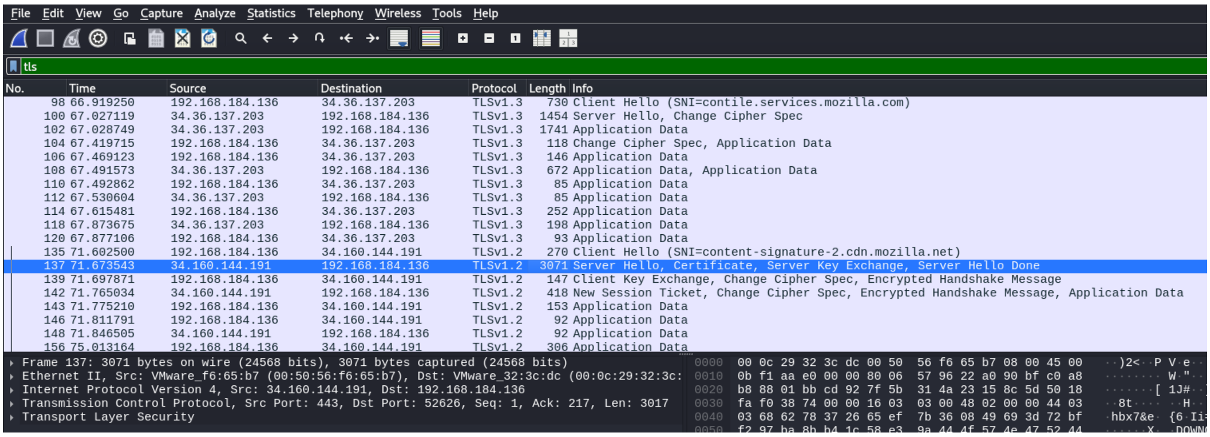
```
tcp
No.  Time         Source          Destination     Protocol Length Info
 212 85.090097303 192.168.184.136 142.250.67.36   TLSv1.3   716 Client Hello (SNI=www.google.com)
 213 85.091283306 142.250.67.36   192.168.184.136 TCP        60 443 → 58468 [ACK] Seq=1 Ack=663 Win=64240 Len=0
 214 85.169172969 142.250.67.36   192.168.184.136 TLSv1.3  2854 Server Hello, Change Cipher Spec, Application Data
 215 85.169218587 192.168.184.136 142.250.67.36   TCP        54 58468 → 443 [ACK] Seq=663 Ack=2801 Win=65535 Len=0
 222 85.283972998 192.168.184.136 142.250.183.163 TCP        74 54762 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2347569855 TSecr=0 WS=128
 223 85.293721467 192.168.184.136 142.250.183.163 TCP        74 54776 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2347569865 TSecr=0 WS=128
 225 85.309622290 192.168.184.136 142.250.183.163 TCP        74 54786 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2347569880 TSecr=0 WS=128
 226 85.325170321 142.250.183.163 192.168.184.136 TCP        60 80 → 54762 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 227 85.325223753 192.168.184.136 142.250.183.163 TCP        54 54762 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 228 85.325661274 192.168.184.136 142.250.183.163 OCSP      482 Request
 229 85.326337141 142.250.183.163 192.168.184.136 TCP        60 80 → 54762 [ACK] Seq=1 Ack=429 Win=64240 Len=0
 230 85.339771548 142.250.183.163 192.168.184.136 TCP        60 80 → 54776 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 231 85.339823072 192.168.184.136 142.250.183.163 TCP        54 54776 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 232 85.345285712 142.250.183.163 192.168.184.136 TCP        60 80 → 54786 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 233 85.345324025 192.168.184.136 142.250.183.163 TCP        54 54786 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 234 85.345562355 192.168.184.136 142.250.183.163 OCSP      482 Request
 235 85.346139422 142.250.183.163 192.168.184.136 TCP        60 80 → 54776 [ACK] Seq=1 Ack=429 Win=64240 Len=0
 236 85.346381189 192.168.184.136 142.250.183.163 OCSP      482 Request

› Frame 215: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_32:3c:dc (00:0c:29:32:3c:dc), Dst: VMware_f6:65:b7 (00:50:56:f6:65:
› Internet Protocol Version 4, Src: 192.168.184.136, Dst: 142.250.67.36
› Transmission Control Protocol, Src Port: 58468, Dst Port: 443, Seq: 663, Ack: 2801, Len: 0

0000  00 50 56 f6 65 b7 00 0c  29 32 3c dc 08 00 45 00   ·PV·e··· )2<···E·
0010  00 28 aa 49 40 00 40 06  45 37 c0 a8 b8 88 8e fa   ·(·I@·@· E7······
0020  43 24 e4 64 01 bb 0d 3c  ca 7b 0f f1 40 77 50 10   C$·d···< ·{··@wP·
0030  ff ff 4b 6a 00 00                                  ··Kj··
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
No.  Time         Source          Destination     Protocol Length Info
  93 66.808101156 192.168.184.2   192.168.184.136 DNS   88 Standard query response 0x0890 AAAA contile.services.mozilla.com
  94 66.835951455 192.168.184.2   192.168.184.136 DNS  104 Standard query response 0xfb94 A contile.services.mozilla.com A 34.36.137.203
 128 71.481935828 192.168.184.136 192.168.184.2   DNS   95 Standard query 0x4211 A content-signature-2.cdn.mozilla.net
 129 71.485101397 192.168.184.136 192.168.184.2   DNS   95 Standard query 0xdf6c AAAA content-signature-2.cdn.mozilla.net
 130 71.531670478 192.168.184.2   192.168.184.136 DNS  318 Standard query response 0x4211 A content-signature-2.cdn.mozilla.net CNAME content-signature-chains.prod.
 131 71.543736729 192.168.184.2   192.168.184.136 DNS  330 Standard query response 0xdf6c AAAA content-signature-2.cdn.mozilla.net CNAME content-signature-chains.pr
 186 84.606424054 192.168.184.136 192.168.184.2   DNS   74 Standard query 0xcc7c A www.google.com
 187 84.606680354 192.168.184.136 192.168.184.2   DNS   74 Standard query 0x2573 AAAA www.google.com
 188 84.613655606 192.168.184.2   192.168.184.136 DNS   90 Standard query response 0xcc7c A www.google.com A 142.250.67.36
 189 84.613878027 192.168.184.2   192.168.184.136 DNS  102 Standard query response 0x2573 AAAA www.google.com AAAA 2404:6800:4007:805::2004
 216 85.201412236 192.168.184.136 192.168.184.2   DNS   70 Standard query 0x64bc A o.pki.goog
 217 85.201642595 192.168.184.136 192.168.184.2   DNS   70 Standard query 0xcebe AAAA o.pki.goog
 218 85.251612778 192.168.184.2   192.168.184.136 DNS  121 Standard query response 0x64bc A o.pki.goog CNAME pki-goog.l.google.com A 142.250.183.163
 219 85.261454907 192.168.184.2   192.168.184.136 DNS  133 Standard query response 0xcebe AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4007:832::2003
 358 88.665543572 192.168.184.136 192.168.184.2   DNS   75 Standard query 0x96b5 A www.gstatic.com
 359 88.665905026 192.168.184.136 192.168.184.2   DNS   75 Standard query 0xf9b1 AAAA www.gstatic.com
 361 88.741729626 192.168.184.136 192.168.184.2   DNS   77 Standard query 0xa1c6 A fonts.gstatic.com
 362 88.742007146 192.168.184.136 192.168.184.2   DNS   77 Standard query 0xcdda AAAA fonts.gstatic.com

› Frame 189: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface eth0, id
› Ethernet II, Src: VMware_f6:65:b7 (00:50:56:f6:65:b7), Dst: VMware_32:3c:dc (00:0c:29:32:3c:
› Internet Protocol Version 4, Src: 192.168.184.2, Dst: 192.168.184.136
› User Datagram Protocol, Src Port: 53, Dst Port: 45922
› Domain Name System (response)

0000  00 0c 29 32 3c dc 00 50  56 f6 65 b7 08 00 45 00   ··)2<··P V·e···E·
0010  00 58 aa fd 00 00 80 11  9d bb c0 a8 b8 02 c0 a8   ·X······ ········
0020  b8 88 00 35 b3 62 00 44  70 e7 25 73 81 80 00 01   ···5·b·D p·%s····
0030  00 01 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 1c  00 01 c0 0c 00 1c 00 01   e·com··· ········
0050  00 00 00 05 00 10 24 04  68 00 40 07 08 05 00 00   ······$· h·@·····
0060  00 00 00 00 20 04                                  ···· ·

Domain Name System: Protocol          Packets: 1873 · Displayed: 74 (4.0%) · Dropped: 0 (0.0%)          Profile: D
```



```
icmp
No.  Time         Source          Destination     Protocol Length Info
 176 79.791850899 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=49/12544, ttl=64 (reply in 177)
 177 80.081293260 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=49/12544, ttl=128 (request in 176)
 178 80.792809724 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=50/12800, ttl=64 (reply in 179)
 179 80.831487636 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=50/12800, ttl=128 (request in 178)
 180 81.794107174 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=51/13056, ttl=64 (reply in 181)
 181 81.851201943 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=51/13056, ttl=128 (request in 180)
 182 82.794721805 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=52/13312, ttl=64 (reply in 183)
 183 82.830815432 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=52/13312, ttl=128 (request in 182)
 184 83.799057393 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=53/13568, ttl=64 (reply in 185)
 185 83.861872210 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=53/13568, ttl=128 (request in 184)
 196 84.800876342 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=54/13824, ttl=64 (reply in 203)
 203 84.871078570 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=54/13824, ttl=128 (request in 196)
 300 85.800994581 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=55/14080, ttl=64 (reply in 323)
 323 85.853539291 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=55/14080, ttl=128 (request in 300)
 353 86.807893060 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=56/14336, ttl=64 (reply in 354)
 354 86.854873593 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=56/14336, ttl=128 (request in 353)
 355 87.810297649 192.168.184.136 142.251.222.206 ICMP  98 Echo (ping) request  id=0x0002, seq=57/14592, ttl=64 (reply in 356)
 356 87.870988470 142.251.222.206 192.168.184.136 ICMP  98 Echo (ping) reply    id=0x0002, seq=57/14592, ttl=128 (request in 355)

› Frame 185: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_f6:65:b7 (00:50:56:f6:65:b7), Dst: VMware_32:3c:dc (00:0c:29:32:3c:
› Internet Protocol Version 4, Src: 142.251.222.206, Dst: 192.168.184.136
› Internet Control Message Protocol

0000  00 0c 29 32 3c dc 00 50  56 f6 65 b7 08 00 45 00
0010  00 54 aa fb 00 00 80 01  a8 b2 8e fb de ce c0 a8
0020  b8 88 00 00 25 5e 00 02  00 35 43 78 62 68 00 00
0030  00 00 72 b7 03 00 00 00  00 00 10 11 12 13 14 15
```



```
tls
```

```
No.     Time        Source            Destination       Protocol  Length Info
     98 66.919250   192.168.184.136   34.36.137.203     TLSv1.3    730 Client Hello (SNI=contile.services.mozilla.com)
    100 67.027119   34.36.137.203     192.168.184.136   TLSv1.3   1454 Server Hello, Change Cipher Spec
    102 67.028749   34.36.137.203     192.168.184.136   TLSv1.3   1741 Application Data
    104 67.419715   192.168.184.136   34.36.137.203     TLSv1.3    118 Change Cipher Spec, Application Data
    106 67.469123   192.168.184.136   34.36.137.203     TLSv1.3    146 Application Data
    108 67.491573   34.36.137.203     192.168.184.136   TLSv1.3    672 Application Data, Application Data
    110 67.492862   192.168.184.136   34.36.137.203     TLSv1.3     85 Application Data
    112 67.530604   34.36.137.203     192.168.184.136   TLSv1.3     85 Application Data
    114 67.615481   192.168.184.136   34.36.137.203     TLSv1.3    252 Application Data
    118 67.873675   34.36.137.203     192.168.184.136   TLSv1.3    198 Application Data
    120 67.877106   192.168.184.136   34.36.137.203     TLSv1.3     93 Application Data
    135 71.602500   192.168.184.136   34.160.144.191    TLSv1.2    270 Client Hello (SNI=content-signature-2.cdn.mozilla.net)
    137 71.673543   34.160.144.191    192.168.184.136   TLSv1.2   3071 Server Hello, Certificate, Server Key Exchange, Server Hello Done
    139 71.697871   192.168.184.136   34.160.144.191    TLSv1.2    147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
    142 71.765034   34.160.144.191    192.168.184.136   TLSv1.2    418 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Application Data
    143 71.775210   192.168.184.136   34.160.144.191    TLSv1.2    153 Application Data
    146 71.811791   192.168.184.136   34.160.144.191    TLSv1.2     92 Application Data
    148 71.846505   34.160.144.191    192.168.184.136   TLSv1.2     92 Application Data
    156 75.013164   192.168.184.136   34.160.144.191    TLSv1.2    306 Application Data
```

```
▸ Frame 137: 3071 bytes on wire (24568 bits), 3071 bytes captured (24568 bits)
▸ Ethernet II, Src: VMware_f6:65:b7 (00:50:56:f6:65:b7), Dst: VMware_32:3c:dc (00:0c:29:32:3c:
▸ Internet Protocol Version 4, Src: 34.160.144.191, Dst: 192.168.184.136
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 52626, Seq: 1, Ack: 217, Len: 3017
▸ Transport Layer Security
```

```
0000  00 0c 29 32 3c dc 00 50  56 f6 65 b7 08 00 45 00   ··)2<··P V·e···
0010  0b f1 aa e0 00 00 80 06  57 96 22 a0 90 bf c0 a8   ········ W·"··
0020  b8 88 01 bb cd 92 7f 5b  31 4a 23 15 8c 5d 50 18   ·······[ 1J#··
0030  fa f0 38 74 00 00 16 03  03 00 48 02 00 00 44 03   ··8t···· ··H··
0040  03 68 62 78 37 26 65 ef  7b 36 08 49 69 3d 72 bf   ·hbx7&e· {6·Ii
0050  f2 97 ba 8b b4 1c 58 e3  9a 44 4f 57 4e 47 52 44   ······X· ·DOWN
```

The following key protocols were identified and analyzed in the packet capture:

1. DNS (Domain Name System)

- Purpose: Resolves domain names (e.g., google.com) to IP addresses.
- Port: UDP 53
- Observation: DNS query and response packets were captured when initiating website access or using the ping command.

2. TCP (Transmission Control Protocol)

- Purpose: Ensures reliable, ordered, and error-checked delivery of data between devices.
- Port: Varies (commonly 80 for HTTP, 443 for HTTPS)
- Observation: TCP 3-way handshake packets (SYN, SYN-ACK, ACK) were captured when connecting to websites.

3. HTTP (Hypertext Transfer Protocol)

- Purpose: Transfers plain-text web content between browser and web server.
- Port: 80
- Observation: HTTP GET requests and responses were observed for non-secure websites like example.com.

4. ICMP (Internet Control Message Protocol)

- Purpose: Used for diagnostic functions like testing connectivity (ping).
- Port: ICMP does not use ports (it's a network-layer protocol).
- Observation: ICMP Echo Request and Echo Reply packets were captured when using ping google.com. It verifies if the destination is reachable.

5. TLS (Transport Layer Security)

- Purpose: Secures communication over the internet using encryption.
- Port: TCP 443 (HTTPS)

- Observation: TLS handshake packets were captured during access to secure websites like https://wikipedia.org, showing encrypted session initiation and certificate exchange.