Experiment No: 2

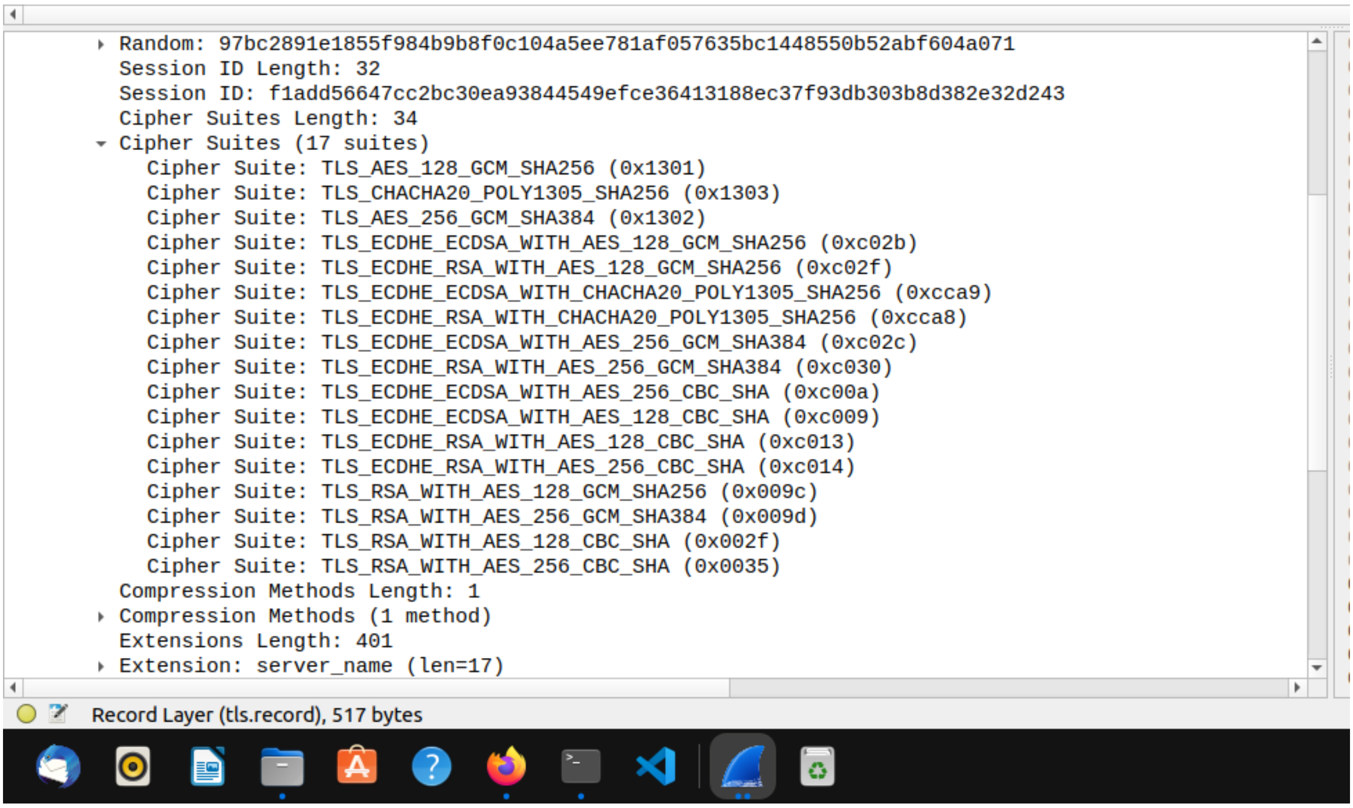
Name:Bhuvi Ghosh
SAPID:60009210191

Wireshark Overview:

- Description: Wireshark is a widely-used network protocol analyzer that allows users to capture and inspect the data traveling back and forth on a computer network in real-time.
- Features:
  - Provides detailed information about network traffic.
  - Supports a wide range of protocols, enabling analysis of various communication types.
  - Offers a user-friendly interface for both beginners and advanced users.

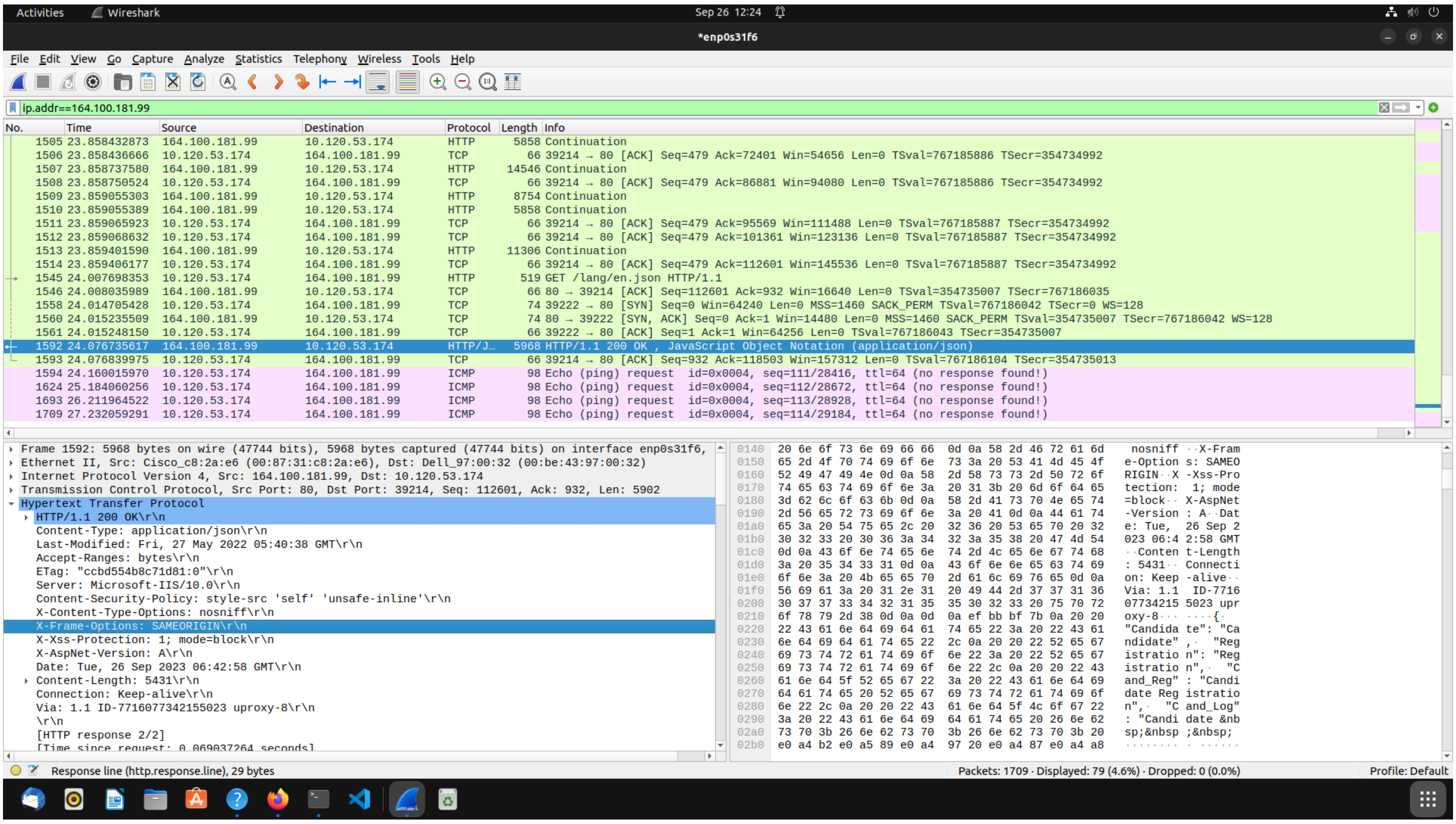
Aspect	Secured (HTTPS)	Unsecured (HTTP)
Initiation (Step 1)	Client sends a "ClientHello" message to the server, including supported cryptographic algorithms.	Client sends a "SYN" (synchronize) packet to the server, expressing an intent to establish a connection.
Response (Step 2)	Server responds with a "ServerHello" message, confirming the selected cryptographic parameters.	Server acknowledges the "SYN" with a "SYN-ACK" (synchronize-acknowledge) packet.
Confirmation (Step 3)	Client acknowledges the server's message, and both parties exchange cryptographic information to establish a secure connection.	Client sends an "ACK" (acknowledge) packet, confirming the establishment of the connection.

Criteria	HTTP	HTTPS
Protocol Type	HyperText Transfer Protocol	HyperText Transfer Protocol Secure
Encryption	No encryption, data is transmitted in plain text	Uses SSL/TLS encryption to secure data transmission
Port	Typically uses port 80	Typically uses port 443
Security	Not secure, vulnerable to eavesdropping	Secure, data is encrypted, protecting against threats
URL	Begins with "http://"	Begins with "https://"



```
    Random: 97bc2891e1855f984b9b8f0c104a5ee781af057635bc1448550b52abf604a071
    Session ID Length: 32
    Session ID: f1add56647cc2bc30ea93844549efce36413188ec37f93db303b8d382e32d243
    Cipher Suites Length: 34
    Cipher Suites (17 suites)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Compression Methods Length: 1
    Compression Methods (1 method)
    Extensions Length: 401
    Extension: server_name (len=17)
```

Record Layer (tls.record), 517 bytes



ip.addr==164.100.181.99

```
No.   Time         Source          Destination     Protocol Length Info
 1505 23.858432873 164.100.181.99  10.120.53.174   HTTP      5858 Continuation
 1506 23.858436666 10.120.53.174   164.100.181.99  TCP         66 39214 → 80 [ACK] Seq=479 Ack=72401 Win=54656 Len=0 TSval=767185886 TSecr=354734992
 1507 23.858737580 164.100.181.99  10.120.53.174   HTTP     14546 Continuation
 1508 23.858750524 10.120.53.174   164.100.181.99  TCP         66 39214 → 80 [ACK] Seq=479 Ack=86881 Win=94080 Len=0 TSval=767185886 TSecr=354734992
 1509 23.859055303 164.100.181.99  10.120.53.174   HTTP      8754 Continuation
 1510 23.859055389 164.100.181.99  10.120.53.174   HTTP      5858 Continuation
 1511 23.859065923 10.120.53.174   164.100.181.99  TCP         66 39214 → 80 [ACK] Seq=479 Ack=95569 Win=111488 Len=0 TSval=767185887 TSecr=354734992
 1512 23.859068632 10.120.53.174   164.100.181.99  TCP         66 39214 → 80 [ACK] Seq=479 Ack=101361 Win=123136 Len=0 TSval=767185887 TSecr=354734992
 1513 23.859401590 164.100.181.99  10.120.53.174   HTTP     11306 Continuation
 1514 23.859406177 10.120.53.174   164.100.181.99  TCP         66 39214 → 80 [ACK] Seq=479 Ack=112601 Win=145536 Len=0 TSval=767185887 TSecr=354734992
 1545 24.007698353 10.120.53.174   164.100.181.99  HTTP       519 GET /lang/en.json HTTP/1.1
 1546 24.008035989 164.100.181.99  10.120.53.174   TCP         66 80 → 39214 [ACK] Seq=112601 Ack=932 Win=16640 Len=0 TSval=354735007 TSecr=767186035
 1558 24.014705428 10.120.53.174   164.100.181.99  TCP         74 39222 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=767186042 TSecr=0 WS=128
 1560 24.015235509 164.100.181.99  10.120.53.174   TCP         74 80 → 39222 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354735007 TSecr=767186042 WS=128
 1561 24.015248150 10.120.53.174   164.100.181.99  TCP         66 39222 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=767186043 TSecr=354735007
 1592 24.076735617 164.100.181.99  10.120.53.174   HTTP/J…   5968 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
 1593 24.076839975 10.120.53.174   164.100.181.99  TCP         66 39214 → 80 [ACK] Seq=932 Ack=118503 Win=157312 Len=0 TSval=767186104 TSecr=354735013
 1594 24.160015970 10.120.53.174   164.100.181.99  ICMP        98 Echo (ping) request  id=0x0004, seq=111/28416, ttl=64 (no response found!)
 1624 25.184060256 10.120.53.174   164.100.181.99  ICMP        98 Echo (ping) request  id=0x0004, seq=112/28672, ttl=64 (no response found!)
 1693 26.211964522 10.120.53.174   164.100.181.99  ICMP        98 Echo (ping) request  id=0x0004, seq=113/28928, ttl=64 (no response found!)
 1709 27.232059291 10.120.53.174   164.100.181.99  ICMP        98 Echo (ping) request  id=0x0004, seq=114/29184, ttl=64 (no response found!)
```

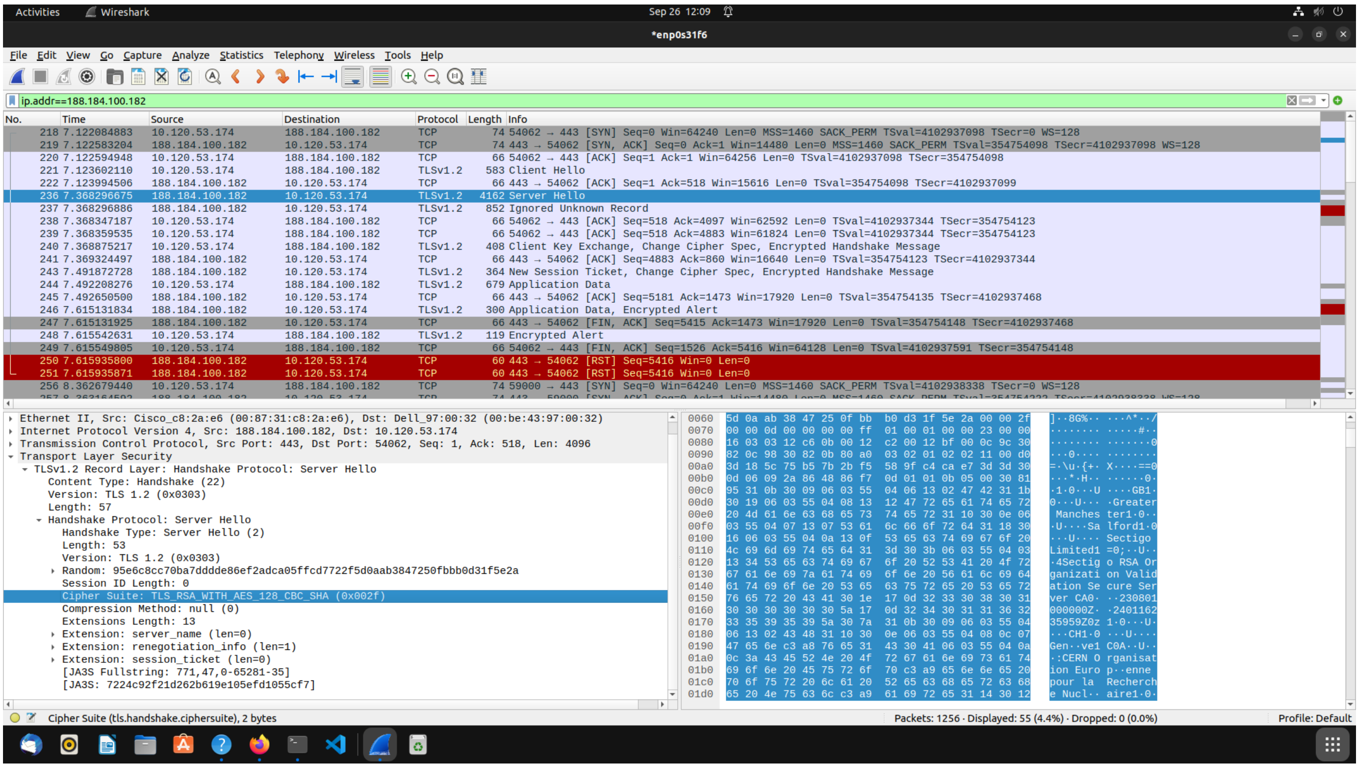
```
Frame 1592: 5968 bytes on wire (47744 bits), 5968 bytes captured (47744 bits) on interface enp0s31f6,
Ethernet II, Src: Cisco_c8:2a:e6 (00:87:31:c8:2a:e6), Dst: Dell_97:00:32 (00:be:43:97:00:32)
Internet Protocol Version 4, Src: 164.100.181.99, Dst: 10.120.53.174
Transmission Control Protocol, Src Port: 80, Dst Port: 39214, Seq: 112601, Ack: 932, Len: 5902
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Content-Type: application/json\r\n
  Last-Modified: Fri, 27 May 2022 05:40:38 GMT\r\n
  Accept-Ranges: bytes\r\n
  ETag: "ccbd554b8c71d81:0"\r\n
  Server: Microsoft-IIS/10.0\r\n
  Content-Security-Policy: style-src 'self' 'unsafe-inline'\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Frame-Options: SAMEORIGIN\r\n
  X-Xss-Protection: 1; mode=block\r\n
  X-AspNet-Version: A\r\n
  Date: Tue, 26 Sep 2023 06:42:58 GMT\r\n
  Content-Length: 5431\r\n
  Connection: Keep-alive\r\n
  Via: 1.1 ID-7716077342155023 uproxy-8\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.069037264 seconds]
```

```
0140  20 6e 6f 73 6e 69 66 66  0d 0a 58 2d 46 72 61 6d   nosniff ··X-Fram
0150  65 2d 4f 70 74 69 6f 6e  73 3a 20 53 41 4d 45 4f  e-Option s: SAMEO
0160  52 49 47 49 4e 0d 0a 58  2d 58 73 73 2d 50 72 6f  RIGIN··X -Xss-Pro
0170  74 65 63 74 69 6f 6e 3a  20 31 3b 20 6d 6f 64 65  tection:  1; mode
0180  3d 62 6c 6f 63 6b 0d 0a  58 2d 41 73 70 4e 65 74  =block·· X-AspNet
0190  2d 56 65 72 73 69 6f 6e  3a 20 41 0d 0a 44 61 74  -Version : A··Dat
01a0  65 3a 20 54 75 65 2c 20  32 36 20 53 65 70 20 32  e: Tue,  26 Sep 2
01b0  30 32 33 20 30 36 3a 34  32 3a 35 38 20 47 4d 54  023 06:4 2:58 GMT
01c0  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68  ··Conten t-Length
01d0  3a 20 35 34 33 31 0d 0a  43 6f 6e 6e 65 63 74 69  : 5431·· Connecti
01e0  6f 6e 3a 20 4b 65 65 70  2d 61 6c 69 76 65 0d 0a  on: Keep -alive··
01f0  56 69 61 3a 20 31 2e 31  20 49 44 2d 37 37 31 36  Via: 1.1  ID-7716
0200  30 37 37 33 34 32 31 35  35 30 32 33 20 75 70 72  07734215 5023 upr
0210  6f 78 79 2d 38 0d 0a 0d  0a ef bb bf 7b 0a 20 20  oxy-8··· ····{·
0220  22 43 61 6e 64 69 64 61  74 65 22 3a 20 22 43 61  "Candida te": "Ca
0230  6e 64 69 64 61 74 65 22  2c 0a 20 20 22 52 65 67  ndidate" ,·  "Reg
0240  69 73 74 72 61 74 69 6f  6e 22 3a 20 22 52 65 67  istratio n": "Reg
0250  69 73 74 72 61 74 69 6f  6e 22 2c 0a 20 20 22 43  istratio n",·  "C
0260  61 6e 64 5f 52 65 67 22  3a 20 22 43 61 6e 64 69  and_Reg" : "Candi
0270  64 61 74 65 20 52 65 67  69 73 74 72 61 74 69 6f  date Reg istratio
0280  6e 22 2c 0a 20 20 22 43  61 6e 64 5f 4c 6f 67 22  n",·  "C and_Log"
0290  3a 20 22 43 61 6e 64 69  64 61 74 65 20 26 6e 62  : "Candi date &nb
02a0  73 70 3b 26 6e 62 73 70  3b 26 6e 62 73 70 3b 20  sp;&nbsp ;&nbsp;
02b0  e0 a4 b2 e0 a5 89 e0 a4  97 20 e0 a4 87 e0 a4 a8  ········ · ······
```

Response line (http.response.line), 29 bytes

Packets: 1709 · Displayed: 79 (4.6%) · Dropped: 0 (0.0%)

Profile: Default



```
ip.addr==188.184.100.182
```

```
No.   Time          Source           Destination      Protocol Length Info
  218 7.122084883  10.120.53.174    188.184.100.182  TCP        74 54062 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4102937098 TSecr=0 WS=128
  219 7.122583204  188.184.100.182  10.120.53.174    TCP        74 443 → 54062 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354754098 TSecr=4102937098 WS=128
  220 7.122594948  10.120.53.174    188.184.100.182  TCP        66 54062 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4102937098 TSecr=354754098
  221 7.123602110  10.120.53.174    188.184.100.182  TLSv1.2   583 Client Hello
  222 7.123994506  188.184.100.182  10.120.53.174    TCP        66 443 → 54062 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=354754098 TSecr=4102937099
  236 7.368296675  188.184.100.182  10.120.53.174    TLSv1.2  4162 Server Hello
  237 7.368296886  188.184.100.182  10.120.53.174    TLSv1.2   852 Ignored Unknown Record
  238 7.368347187  10.120.53.174    188.184.100.182  TCP        66 54062 → 443 [ACK] Seq=518 Ack=4097 Win=62592 Len=0 TSval=4102937344 TSecr=354754123
  239 7.368359535  10.120.53.174    188.184.100.182  TCP        66 54062 → 443 [ACK] Seq=518 Ack=4883 Win=61824 Len=0 TSval=4102937344 TSecr=354754123
  240 7.368875217  10.120.53.174    188.184.100.182  TLSv1.2   408 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  241 7.369324497  188.184.100.182  10.120.53.174    TCP        66 443 → 54062 [ACK] Seq=4883 Ack=860 Win=16640 Len=0 TSval=354754123 TSecr=4102937344
  243 7.491872728  188.184.100.182  10.120.53.174    TLSv1.2   364 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  244 7.492208276  10.120.53.174    188.184.100.182  TLSv1.2   679 Application Data
  245 7.492650500  188.184.100.182  10.120.53.174    TCP        66 443 → 54062 [ACK] Seq=5181 Ack=1473 Win=17920 Len=0 TSval=354754135 TSecr=4102937468
  246 7.615131834  188.184.100.182  10.120.53.174    TLSv1.2   300 Application Data, Encrypted Alert
  247 7.615131925  188.184.100.182  10.120.53.174    TCP        66 443 → 54062 [FIN, ACK] Seq=5415 Ack=1473 Win=17920 Len=0 TSval=354754148 TSecr=4102937468
  248 7.615542631  10.120.53.174    188.184.100.182  TLSv1.2   119 Encrypted Alert
  249 7.615549805  10.120.53.174    188.184.100.182  TCP        66 54062 → 443 [FIN, ACK] Seq=1526 Ack=5416 Win=64128 Len=0 TSval=4102937591 TSecr=354754148
  250 7.615935800  188.184.100.182  10.120.53.174    TCP        60 443 → 54062 [RST] Seq=5416 Win=0 Len=0
  251 7.615935871  188.184.100.182  10.120.53.174    TCP        60 443 → 54062 [RST] Seq=5416 Win=0 Len=0
  256 8.362679440  10.120.53.174    188.184.100.182  TCP        74 59000 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4102938338 TSecr=0 WS=128
  257 8.363164592  188.184.100.182  10.120.53.174    TCP        74 443 → 59000 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354754222 TSecr=4102938338 WS=128
```

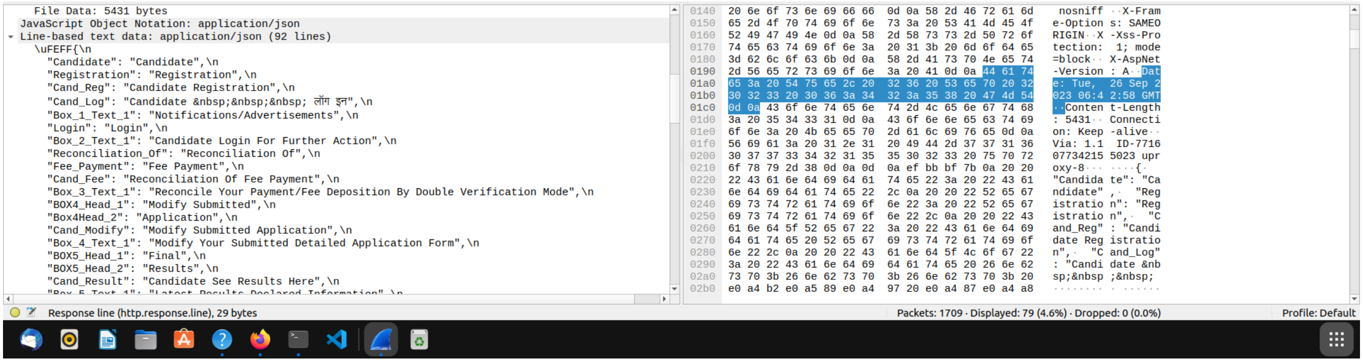
```
▸ Ethernet II, Src: Cisco_c8:2a:e6 (00:87:31:c8:2a:e6), Dst: Dell_97:00:32 (00:be:43:97:00:32)
▸ Internet Protocol Version 4, Src: 188.184.100.182, Dst: 10.120.53.174
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 54062, Seq: 1, Ack: 518, Len: 4096
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 57
    ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 53
        Version: TLS 1.2 (0x0303)
      ▸ Random: 95e6c8cc70ba7dddde86ef2adca05ffcd7722f5d0aab3847250fbbb0d31f5e2a
        Session ID Length: 0
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Compression Method: null (0)
        Extensions Length: 13
      ▸ Extension: server_name (len=0)
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: session_ticket (len=0)
        [JA3S Fullstring: 771,47,0-65281-35]
        [JA3S: 7224c92f21d262b619e105efd1055cf7]
```

```
0060  5d 0a ab 38 47 25 0f bb  b0 d3 1f 5e 2a 00 00 2f   ]··8G%·· ···^*··/
0070  00 00 0d 00 00 00 00 ff  01 00 01 00 00 23 00 00   ········ ·····#··
0080  16 03 03 12 c6 0b 00 12  c2 00 12 bf 00 0c 9c 30   ········ ·······0
0090  82 0c 98 30 82 0b 80 a0  03 02 01 02 02 11 00 d0   ···0···· ········
00a0  3d 18 5c 75 b5 7b 2b f5  58 9f c4 ca e7 3d 3d 30   =·\u·{+· X····==0
00b0  0d 06 09 2a 86 48 86 f7  0d 01 01 0b 05 00 30 81   ···*·H·· ······0·
00c0  95 31 0b 30 09 06 03 55  04 06 13 02 47 42 31 1b   ·1·0···U ····GB1·
00d0  30 19 06 03 55 04 08 13  12 47 72 65 61 74 65 72   0···U··· ·Greater
00e0  20 4d 61 6e 63 68 65 73  74 65 72 31 10 30 0e 06    Manches ter1·0··
00f0  03 55 04 07 13 07 53 61  6c 66 6f 72 64 31 18 30   ·U····Sa lford1·0
0100  16 06 03 55 04 0a 13 0f  53 65 63 74 69 67 6f 20   ···U···· Sectigo 
0110  4c 69 6d 69 74 65 64 31  3d 30 3b 06 03 55 04 03   Limited1 =0;··U··
0120  13 34 53 65 63 74 69 67  6f 20 52 53 41 20 4f 72   ·4Sectig o RSA Or
0130  67 61 6e 69 7a 61 74 69  6f 6e 20 56 61 6c 69 64   ganizati on Valid
0140  61 74 69 6f 6e 20 53 65  63 75 72 65 20 53 65 72   ation Se cure Ser
0150  76 65 72 20 43 41 30 1e  17 0d 32 33 30 38 30 31   ver CA0· ··230801
0160  30 30 30 30 30 30 5a 17  0d 32 34 30 31 31 36 32   000000Z· ·2401162
0170  33 35 39 35 39 5a 30 7a  31 0b 30 09 06 03 55 04   35959Z0z 1·0···U·
0180  06 13 02 43 48 31 10 30  0e 06 03 55 04 08 0c 07   ···CH1·0 ···U····
0190  47 65 6e c3 a8 76 65 31  43 30 41 06 03 55 04 0a   Gen··ve1 C0A··U··
01a0  0c 3a 43 45 52 4e 20 4f  72 67 61 6e 69 73 61 74   ·:CERN O rganisat
01b0  69 6f 6e 20 45 75 72 6f  70 c3 a9 65 6e 6e 65 20   ion Euro p··enne 
01c0  70 6f 75 72 20 6c 61 20  52 65 63 68 65 72 63 68   pour la  Recherch
01d0  65 20 4e 75 63 6c c3 a9  61 69 72 65 31 14 30 12   e Nucl·· aire1·0·
```

Cipher Suite (tls.handshake.ciphersuite), 2 bytes

Packets: 1256 · Displayed: 55 (4.4%) · Dropped: 0 (0.0%)

Profile: Default



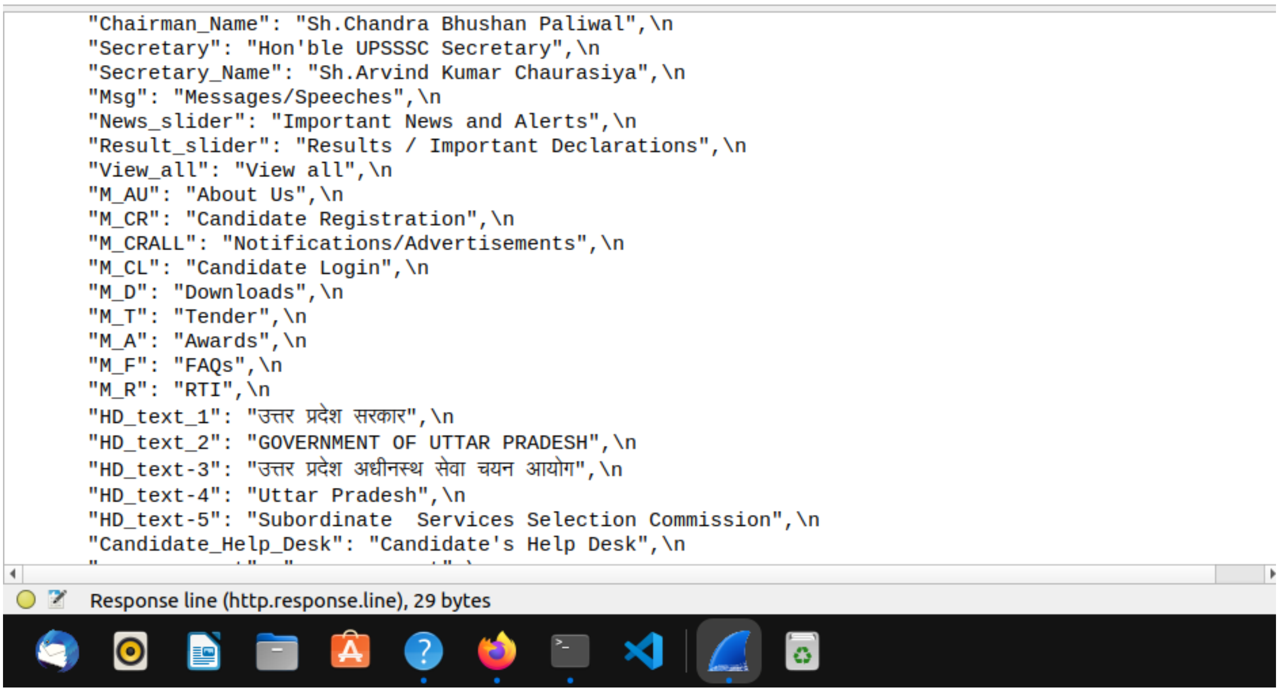
```
    File Data: 5431 bytes
  JavaScript Object Notation: application/json
▾ Line-based text data: application/json (92 lines)
    \uFEFF{\n
      "Candidate": "Candidate",\n
      "Registration": "Registration",\n
      "Cand_Reg": "Candidate Registration",\n
      "Cand_Log": "Candidate &nbsp;&nbsp;&nbsp; लॉग इन",\n
      "Box_1_Text_1": "Notifications/Advertisements",\n
      "Login": "Login",\n
      "Box_2_Text_1": "Candidate Login For Further Action",\n
      "Reconciliation_Of": "Reconciliation Of",\n
      "Fee_Payment": "Fee Payment",\n
      "Cand_Fee": "Reconciliation Of Fee Payment",\n
      "Box_3_Text_1": "Reconcile Your Payment/Fee Deposition By Double Verification Mode",\n
      "BOX4_Head_1": "Modify Submitted",\n
      "Box4Head_2": "Application",\n
      "Cand_Modify": "Modify Submitted Application",\n
      "Box_4_Text_1": "Modify Your Submitted Detailed Application Form",\n
      "BOX5_Head_1": "Final",\n
      "BOX5_Head_2": "Results",\n
      "Cand_Result": "Candidate See Results Here",\n
      "Box_5_Text_1": "Latest Results Declared Information",\n
```

```
0140  20 6e 6f 73 6e 69 66 66  0d 0a 58 2d 46 72 61 6d    nosniff ··X-Fram
0150  65 2d 4f 70 74 69 6f 6e  73 3a 20 53 41 4d 45 4f   e-Option s: SAMEO
0160  52 49 47 49 4e 0d 0a 58  2d 58 73 73 2d 50 72 6f   RIGIN··X -Xss-Pro
0170  74 65 63 74 69 6f 6e 3a  20 31 3b 20 6d 6f 64 65   tection:  1; mode
0180  3d 62 6c 6f 63 6b 0d 0a  58 2d 41 73 70 4e 65 74   =block·· X-AspNet
0190  2d 56 65 72 73 69 6f 6e  3a 20 41 0d 0a 44 61 74   -Version : A··Dat
01a0  65 3a 20 54 75 65 2c 20  32 36 20 53 65 70 20 32   e: Tue,  26 Sep 2
01b0  30 32 33 20 30 36 3a 34  32 3a 35 38 20 47 4d 54   023 06:4 2:58 GMT
01c0  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
01d0  3a 20 35 34 33 31 0d 0a  43 6f 6e 6e 65 63 74 69   : 5431·· Connecti
01e0  6f 6e 3a 20 4b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: Keep -alive··
01f0  56 69 61 3a 20 31 2e 31  20 49 44 2d 37 37 31 36   Via: 1.1  ID-7716
0200  30 37 37 33 34 32 31 35  35 30 32 33 20 75 70 72   07734215 5023 upr
0210  6f 78 79 2d 38 0d 0a 0d  0a ef bb bf 7b 0a 20 20   oxy-8··· ····{· 
0220  22 43 61 6e 64 69 64 61  74 65 22 3a 20 22 43 61   "Candida te": "Ca
0230  6e 64 69 64 61 74 65 22  2c 0a 20 20 22 52 65 67   ndidate" ,·  "Reg
0240  69 73 74 72 61 74 69 6f  6e 22 3a 20 22 52 65 67   istratio n": "Reg
0250  69 73 74 72 61 74 69 6f  6e 22 2c 0a 20 20 22 43   istratio n",·  "C
0260  61 6e 64 5f 52 65 67 22  3a 20 22 43 61 6e 64 69   and_Reg" : "Candi
0270  64 61 74 65 20 52 65 67  69 73 74 72 61 74 69 6f   date Reg istratio
0280  6e 22 2c 0a 20 20 22 43  61 6e 64 5f 4c 6f 67 22   n",·  "C and_Log"
0290  3a 20 22 43 61 6e 64 69  64 61 74 65 20 26 6e 62   : "Candi date &nb
02a0  73 70 3b 26 6e 62 73 70  3b 26 6e 62 73 70 3b 20   sp;&nbsp ;&nbsp; 
02b0  e0 a4 b2 e0 a5 89 e0 a4  97 20 e0 a4 87 e0 a4 a8   ········ · ······
```

Response line (http.response.line), 29 bytes

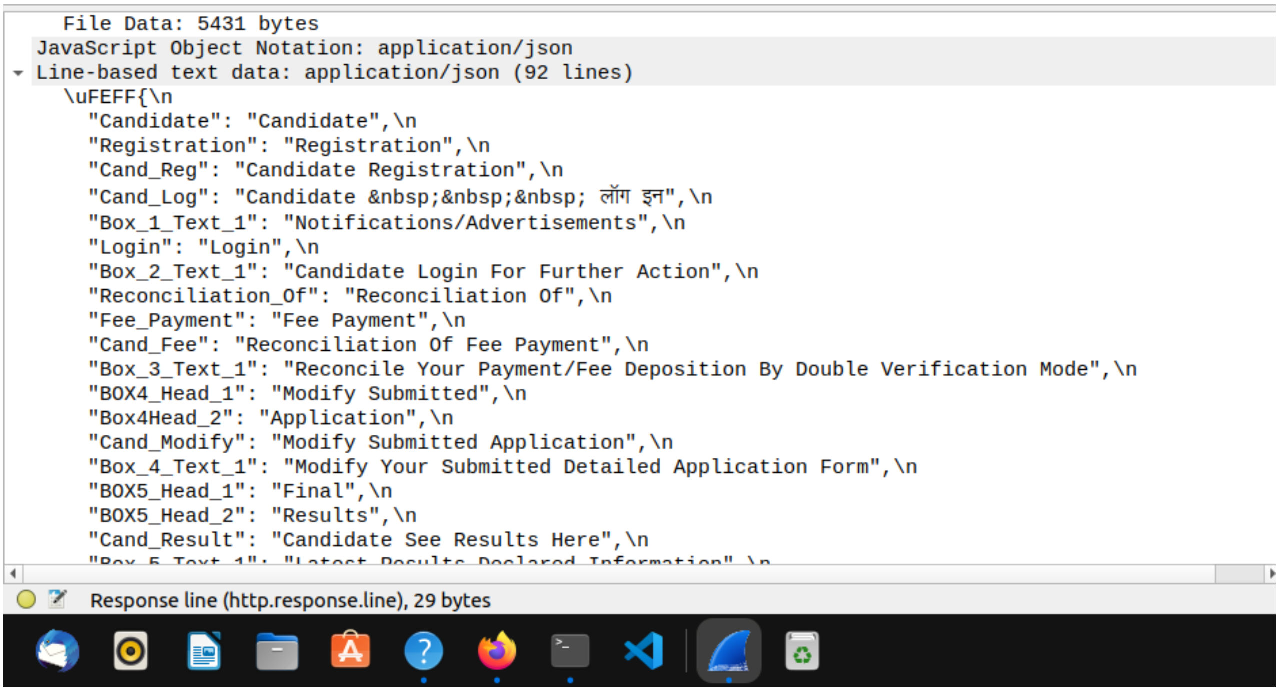
Packets: 1709 · Displayed: 79 (4.6%) · Dropped: 0 (0.0%)

Profile: Default



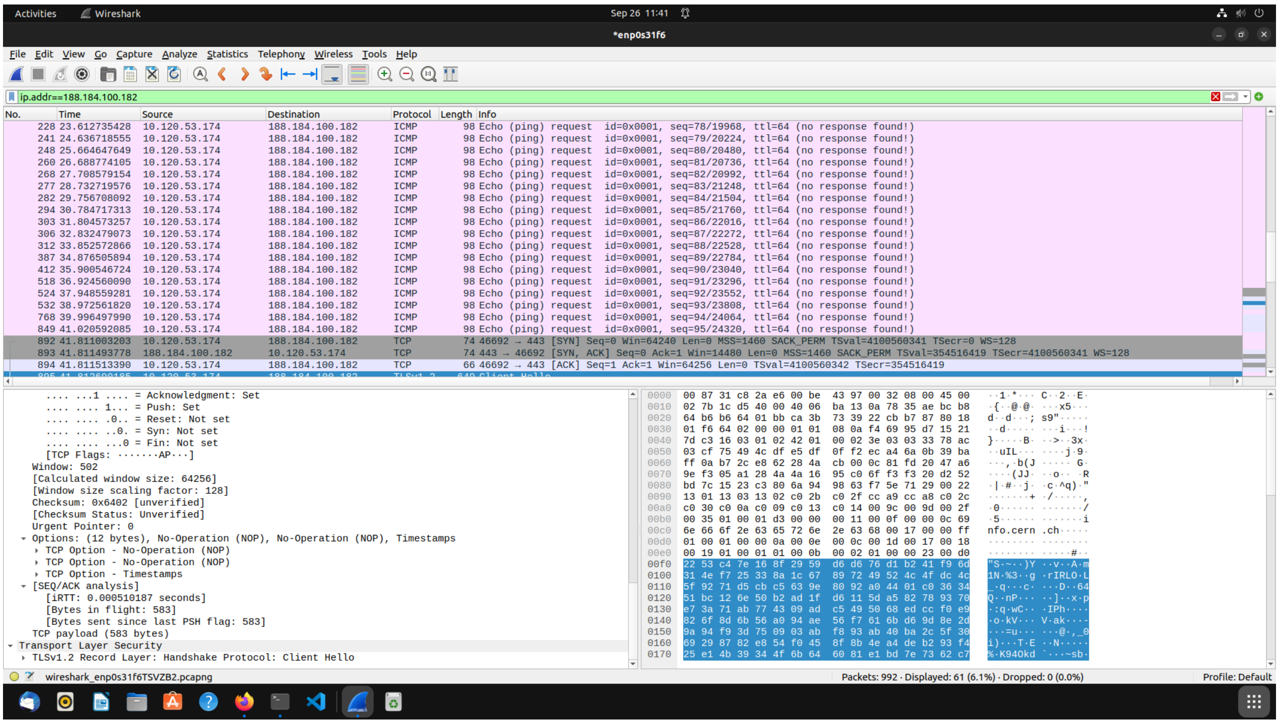
```
      "Chairman_Name": "Sh.Chandra Bhushan Paliwal",\n
      "Secretary": "Hon'ble UPSSSC Secretary",\n
      "Secretary_Name": "Sh.Arvind Kumar Chaurasiya",\n
      "Msg": "Messages/Speeches",\n
      "News_slider": "Important News and Alerts",\n
      "Result_slider": "Results / Important Declarations",\n
      "View_all": "View all",\n
      "M_AU": "About Us",\n
      "M_CR": "Candidate Registration",\n
      "M_CRALL": "Notifications/Advertisements",\n
      "M_CL": "Candidate Login",\n
      "M_D": "Downloads",\n
      "M_T": "Tender",\n
      "M_A": "Awards",\n
      "M_F": "FAQs",\n
      "M_R": "RTI",\n
      "HD_text_1": "उत्तर प्रदेश सरकार",\n
      "HD_text_2": "GOVERNMENT OF UTTAR PRADESH",\n
      "HD_text-3": "उत्तर प्रदेश अधीनस्थ सेवा चयन आयोग",\n
      "HD_text-4": "Uttar Pradesh",\n
      "HD_text-5": "Subordinate  Services Selection Commission",\n
      "Candidate_Help_Desk": "Candidate's Help Desk",\n
```

Response line (http.response.line), 29 bytes



```
    File Data: 5431 bytes
  JavaScript Object Notation: application/json
▾ Line-based text data: application/json (92 lines)
    \uFEFF{\n
      "Candidate": "Candidate",\n
      "Registration": "Registration",\n
      "Cand_Reg": "Candidate Registration",\n
      "Cand_Log": "Candidate &nbsp;&nbsp;&nbsp; लॉग इन",\n
      "Box_1_Text_1": "Notifications/Advertisements",\n
      "Login": "Login",\n
      "Box_2_Text_1": "Candidate Login For Further Action",\n
      "Reconciliation_Of": "Reconciliation Of",\n
      "Fee_Payment": "Fee Payment",\n
      "Cand_Fee": "Reconciliation Of Fee Payment",\n
      "Box_3_Text_1": "Reconcile Your Payment/Fee Deposition By Double Verification Mode",\n
      "BOX4_Head_1": "Modify Submitted",\n
      "Box4Head_2": "Application",\n
      "Cand_Modify": "Modify Submitted Application",\n
      "Box_4_Text_1": "Modify Your Submitted Detailed Application Form",\n
      "BOX5_Head_1": "Final",\n
      "BOX5_Head_2": "Results",\n
      "Cand_Result": "Candidate See Results Here",\n
      "Box_5_Text_1": "Latest Results Declared Information",\n
```

Response line (http.response.line), 29 bytes


Activities
Wireshark
Sep 26 11:41
*enp0s31f6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==188.184.100.182
```

```
No.     Time          Source           Destination      Protocol Length Info
    228 23.612735428  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=78/19968, ttl=64 (no response found!)
    241 24.636718555  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=79/20224, ttl=64 (no response found!)
    248 25.664647649  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=80/20480, ttl=64 (no response found!)
    260 26.688774105  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=81/20736, ttl=64 (no response found!)
    268 27.708579154  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=82/20992, ttl=64 (no response found!)
    277 28.732719576  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=83/21248, ttl=64 (no response found!)
    282 29.756708092  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=84/21504, ttl=64 (no response found!)
    294 30.784717313  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=85/21760, ttl=64 (no response found!)
    303 31.804573257  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=86/22016, ttl=64 (no response found!)
    306 32.832479073  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=87/22272, ttl=64 (no response found!)
    312 33.852572866  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=88/22528, ttl=64 (no response found!)
    387 34.876505894  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=89/22784, ttl=64 (no response found!)
    412 35.900546724  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=90/23040, ttl=64 (no response found!)
    518 36.924560090  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=91/23296, ttl=64 (no response found!)
    524 37.948559281  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=92/23552, ttl=64 (no response found!)
    532 38.972561820  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=93/23808, ttl=64 (no response found!)
    768 39.996497990  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=94/24064, ttl=64 (no response found!)
    849 41.020592085  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=95/24320, ttl=64 (no response found!)
    892 41.811003203  10.120.53.174    188.184.100.182  TCP        74 46692 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4100560341 TSecr=0 WS=128
    893 41.811493778  188.184.100.182  10.120.53.174    TCP        74 443 → 46692 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354516419 TSecr=4100560341 WS=128
    894 41.811513390  10.120.53.174    188.184.100.182  TCP        66 46692 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4100560342 TSecr=354516419
```

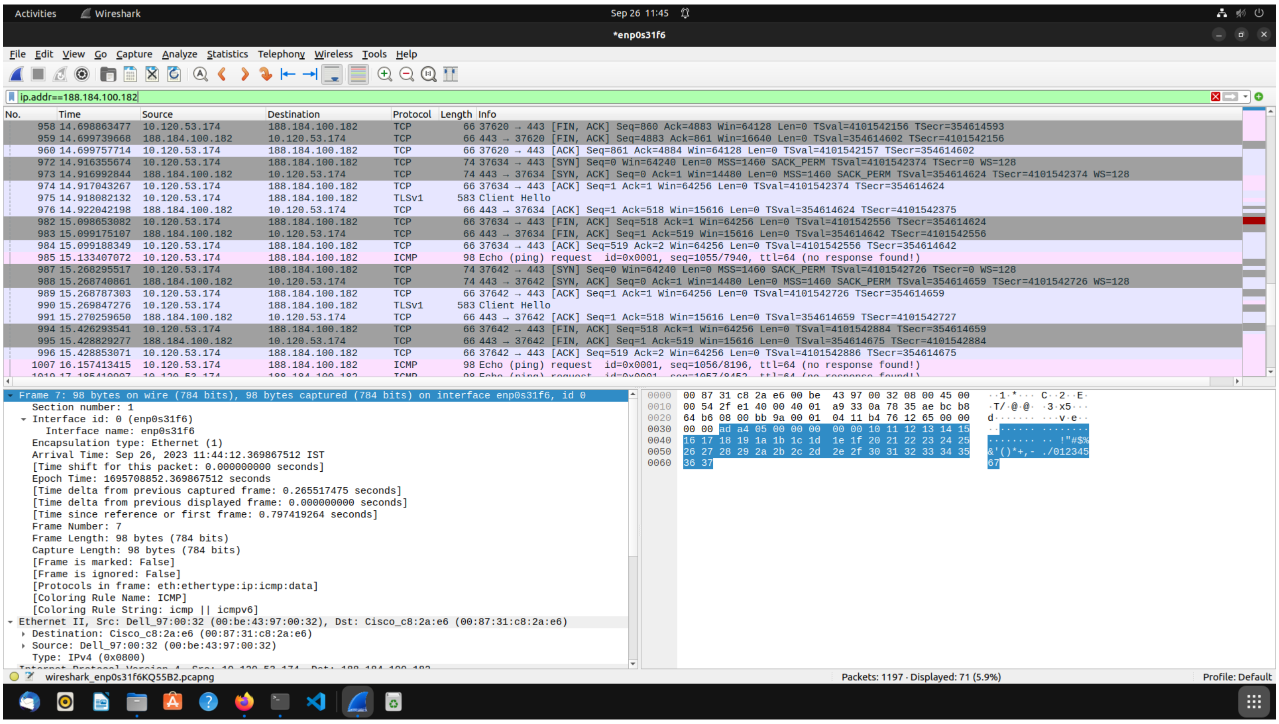
```
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······AP···]
  Window: 502
  [Calculated window size: 64256]
  [Window size scaling factor: 128]
  Checksum: 0x6402 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
▾ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ TCP Option - No-Operation (NOP)
  ▸ TCP Option - No-Operation (NOP)
  ▸ TCP Option - Timestamps
▾ [SEQ/ACK analysis]
    [iRTT: 0.000510187 seconds]
    [Bytes in flight: 583]
    [Bytes sent since last PSH flag: 583]
  TCP payload (583 bytes)
▾ Transport Layer Security
  ▸ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
```

```
0000  00 87 31 c8 2a e6 00 be  43 97 00 32 08 00 45 00   ··1·*··· C··2··E·
0010  02 7b 1c d5 40 00 40 06  ba 13 0a 78 35 ae bc b8   ·{··@·@· ···x5···
0020  64 b6 b6 64 01 bb ca 3b  73 39 22 cb b7 87 80 18   d··d···; s9"·····
0030  01 f6 64 02 00 00 01 01  08 0a f4 69 95 d7 15 21   ··d····· ···i···!
0040  7d c3 16 03 01 02 42 01  00 02 3e 03 03 33 78 ac   }·····B· ··>··3x·
0050  03 cf 75 49 4c df e5 df  0f f2 ec a4 6a 0b 39 ba   ··uIL··· ····j·9·
0060  ff 0a b7 2c e8 62 28 4a  cb 00 0c 81 fd 20 47 a6   ···,·b(J ····· G·
0070  9e f3 05 a1 28 4a 4a 16  95 c0 6f f3 f3 20 d2 52   ····(JJ· ··o·· ·R
0080  bd 7c 15 23 c3 80 6a 94  98 63 f7 5e 71 29 00 22   ·|·#··j· ·c·^q)·"
0090  13 01 13 03 13 02 c0 2b  c0 2f cc a9 cc a8 c0 2c   ·······+ ·/·····,
00a0  c0 30 c0 0a c0 09 c0 13  c0 14 00 9c 00 9d 00 2f   ·0······ ·······/
00b0  00 35 01 00 01 d3 00 00  00 11 00 0f 00 00 0c 69   ·5······ ·······i
00c0  6e 66 6f 2e 63 65 72 6e  2e 63 68 00 17 00 00 ff   nfo.cern .ch·····
00d0  01 00 01 00 00 0a 00 0e  00 0c 00 1d 00 17 00 18   ········ ········
00e0  00 19 01 00 01 01 00 0b  00 02 01 00 00 23 00 d0   ········ ·····#··
00f0  22 53 c4 7e 16 8f 29 59  d6 d6 76 d1 b2 41 f9 6d   "S·~··)Y ··v··A·m
0100  31 4e f7 25 33 8a 1c 67  89 72 49 52 4c 4f dc 4c   1N·%3··g ·rIRLO·L
0110  5f 92 71 d5 cb c5 63 9e  80 92 a0 44 01 c0 36 34   _·q···c· ···D··64
0120  51 bc 12 6e 50 b2 ad 1f  d6 11 5d a5 82 78 93 70   Q··nP··· ··]··x·p
0130  e7 3a 71 ab 77 43 09 ad  c5 49 50 68 ed cc f0 e9   ·:q·wC·· ·IPh····
0140  82 6f 8d 6b 56 a0 94 ae  56 f7 61 6b d6 9d 8e 2d   ·o·kV··· V·ak···-
0150  9a 94 f9 3d 75 09 03 ab  f8 93 ab 40 ba 2c 5f 30   ···=u··· ···@·,_0
0160  69 29 87 82 e8 54 f0 45  8f 8b 4e a4 de b2 93 f4   i)···T·E ··N·····
0170  25 e1 4b 39 34 4f 6b 64  60 81 e1 bd 7e 73 62 c7   %·K94Okd `···~sb·
```

wireshark_enp0s31f6TSVZB2.pcapng

Packets: 992 · Displayed: 61 (6.1%) · Dropped: 0 (0.0%)

Profile: Default


Activities
Wireshark
Sep 26 11:45
*enp0s31f6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==188.184.100.182
```

```
No.     Time          Source           Destination      Protocol Length Info
    958 14.698863477  10.120.53.174    188.184.100.182  TCP        66 37620 → 443 [FIN, ACK] Seq=860 Ack=4883 Win=64128 Len=0 TSval=4101542156 TSecr=354614593
    959 14.699739668  188.184.100.182  10.120.53.174    TCP        66 443 → 37620 [FIN, ACK] Seq=4883 Ack=861 Win=16640 Len=0 TSval=354614602 TSecr=4101542156
    960 14.699757714  10.120.53.174    188.184.100.182  TCP        66 37620 → 443 [ACK] Seq=861 Ack=4884 Win=64128 Len=0 TSval=4101542157 TSecr=354614602
    972 14.916355674  10.120.53.174    188.184.100.182  TCP        74 37634 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101542374 TSecr=0 WS=128
    973 14.916992844  188.184.100.182  10.120.53.174    TCP        74 443 → 37634 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354614624 TSecr=4101542374 WS=128
    974 14.917043267  10.120.53.174    188.184.100.182  TCP        66 37634 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4101542374 TSecr=354614624
    975 14.918082132  10.120.53.174    188.184.100.182  TLSv1     583 Client Hello
    976 14.922042198  188.184.100.182  10.120.53.174    TCP        66 443 → 37634 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=354614624 TSecr=4101542375
    982 15.098653082  10.120.53.174    188.184.100.182  TCP        66 37634 → 443 [FIN, ACK] Seq=518 Ack=1 Win=64256 Len=0 TSval=4101542556 TSecr=354614624
    983 15.099175107  188.184.100.182  10.120.53.174    TCP        66 443 → 37634 [FIN, ACK] Seq=1 Ack=519 Win=15616 Len=0 TSval=354614642 TSecr=4101542556
    984 15.099188349  10.120.53.174    188.184.100.182  TCP        66 37634 → 443 [ACK] Seq=519 Ack=2 Win=64256 Len=0 TSval=4101542556 TSecr=354614642
    985 15.133407072  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=1055/7940, ttl=64 (no response found!)
    987 15.268295517  10.120.53.174    188.184.100.182  TCP        74 37642 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101542726 TSecr=0 WS=128
    988 15.268740861  188.184.100.182  10.120.53.174    TCP        74 443 → 37642 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354614659 TSecr=4101542726 WS=128
    989 15.268787303  10.120.53.174    188.184.100.182  TCP        66 37642 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4101542726 TSecr=354614659
    990 15.269847276  10.120.53.174    188.184.100.182  TLSv1     583 Client Hello
    991 15.270259650  188.184.100.182  10.120.53.174    TCP        66 443 → 37642 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=354614659 TSecr=4101542727
    994 15.426293541  10.120.53.174    188.184.100.182  TCP        66 37642 → 443 [FIN, ACK] Seq=518 Ack=1 Win=64256 Len=0 TSval=4101542884 TSecr=354614659
    995 15.428829277  188.184.100.182  10.120.53.174    TCP        66 443 → 37642 [FIN, ACK] Seq=1 Ack=519 Win=15616 Len=0 TSval=354614675 TSecr=4101542884
    996 15.428853071  10.120.53.174    188.184.100.182  TCP        66 37642 → 443 [ACK] Seq=519 Ack=2 Win=64256 Len=0 TSval=4101542886 TSecr=354614675
   1007 16.157413415  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=1056/8196, ttl=64 (no response found!)
```

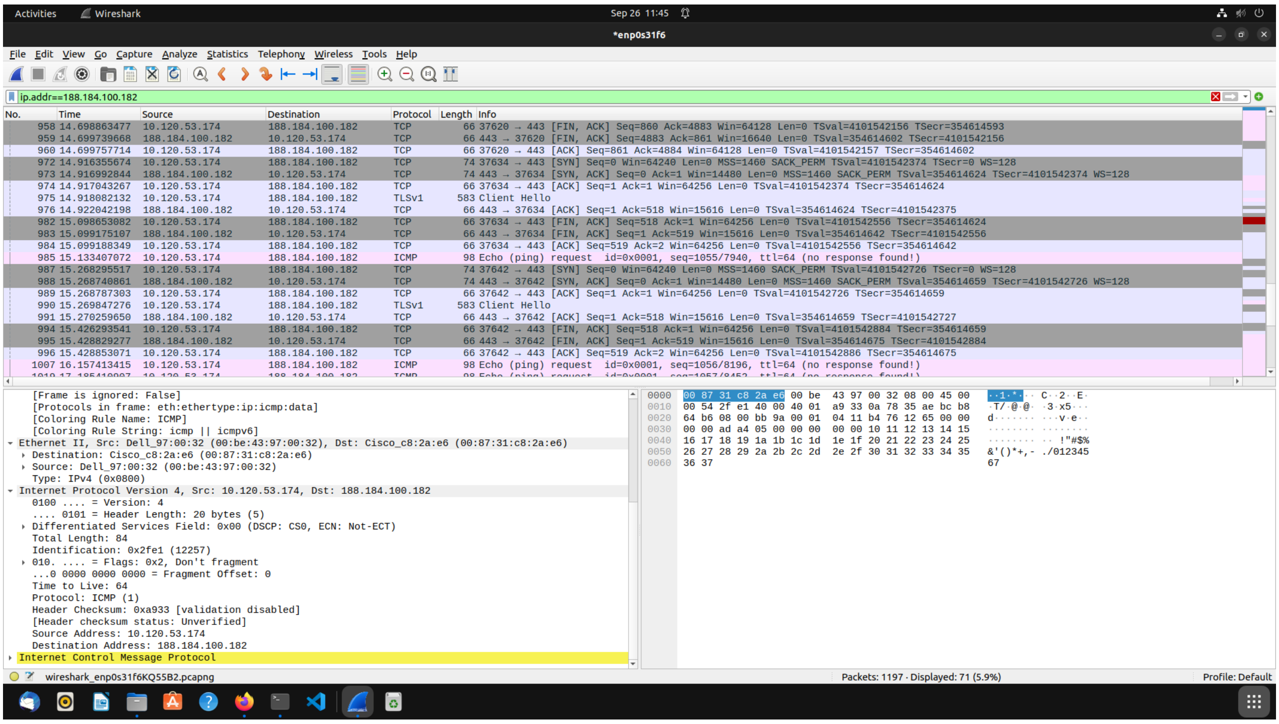
```
▾ Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s31f6, id 0
    Section number: 1
  ▾ Interface id: 0 (enp0s31f6)
      Interface name: enp0s31f6
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 26, 2023 11:44:12.369867512 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1695708852.369867512 seconds
    [Time delta from previous captured frame: 0.265517475 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.797419264 seconds]
    Frame Number: 7
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
▾ Ethernet II, Src: Dell_97:00:32 (00:be:43:97:00:32), Dst: Cisco_c8:2a:e6 (00:87:31:c8:2a:e6)
  ▸ Destination: Cisco_c8:2a:e6 (00:87:31:c8:2a:e6)
  ▸ Source: Dell_97:00:32 (00:be:43:97:00:32)
    Type: IPv4 (0x0800)
```

```
0000  00 87 31 c8 2a e6 00 be  43 97 00 32 08 00 45 00   ··1·*··· C··2··E·
0010  00 54 2f e1 40 00 40 01  a9 33 0a 78 35 ae bc b8   ·T/·@·@· ·3·x5···
0020  64 b6 08 00 bb 9a 00 01  04 11 b4 76 12 65 00 00   d······· ···v·e··
0030  00 00 ad a4 05 00 00 00  00 00 10 11 12 13 14 15   ········ ········
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
```

wireshark_enp0s31f6KQ55B2.pcapng

Packets: 1197 · Displayed: 71 (5.9%)

Profile: Default


Activities
Wireshark
Sep 26 11:45
*enp0s31f6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

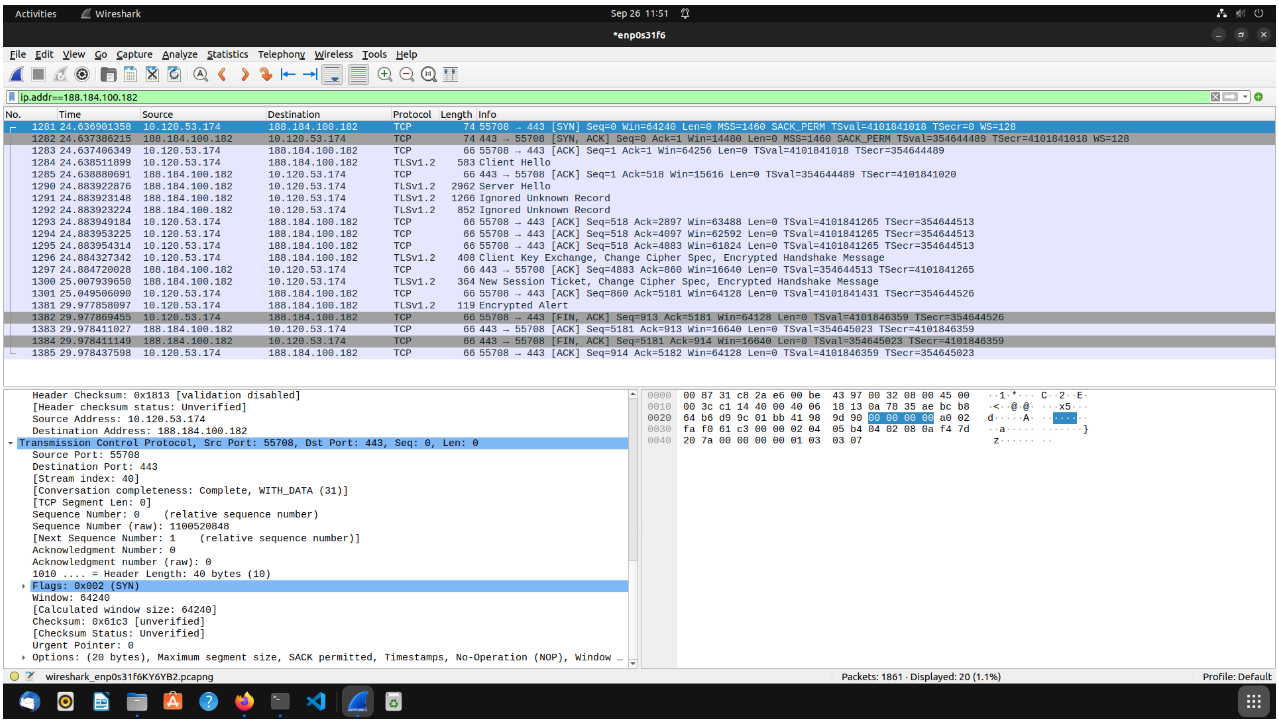
```
ip.addr==188.184.100.182
```

```
No.   Time          Source           Destination      Protocol Length Info
  958 14.698863477  10.120.53.174    188.184.100.182  TCP        66 37620 → 443 [FIN, ACK] Seq=860 Ack=4883 Win=64128 Len=0 TSval=4101542156 TSecr=354614593
  959 14.699739668  188.184.100.182  10.120.53.174    TCP        66 443 → 37620 [FIN, ACK] Seq=4883 Ack=861 Win=16640 Len=0 TSval=354614602 TSecr=4101542156
  960 14.699757714  10.120.53.174    188.184.100.182  TCP        66 37620 → 443 [ACK] Seq=861 Ack=4884 Win=64128 Len=0 TSval=4101542157 TSecr=354614602
  972 14.916355674  10.120.53.174    188.184.100.182  TCP        74 37634 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101542374 TSecr=0 WS=128
  973 14.916992844  188.184.100.182  10.120.53.174    TCP        74 443 → 37634 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354614624 TSecr=4101542374 WS=128
  974 14.917043267  10.120.53.174    188.184.100.182  TCP        66 37634 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4101542374 TSecr=354614624
  975 14.918082132  10.120.53.174    188.184.100.182  TLSv1     583 Client Hello
  976 14.922042198  188.184.100.182  10.120.53.174    TCP        66 443 → 37634 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=354614624 TSecr=4101542375
  982 15.098653082  10.120.53.174    188.184.100.182  TCP        66 37634 → 443 [FIN, ACK] Seq=518 Ack=1 Win=64256 Len=0 TSval=4101542556 TSecr=354614624
  983 15.099175107  188.184.100.182  10.120.53.174    TCP        66 443 → 37634 [FIN, ACK] Seq=1 Ack=519 Win=15616 Len=0 TSval=354614642 TSecr=4101542556
  984 15.099188349  10.120.53.174    188.184.100.182  TCP        66 37634 → 443 [ACK] Seq=519 Ack=2 Win=64256 Len=0 TSval=4101542556 TSecr=354614642
  985 15.133407072  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=1055/7940, ttl=64 (no response found!)
  987 15.268295517  10.120.53.174    188.184.100.182  TCP        74 37642 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101542726 TSecr=0 WS=128
  988 15.268740861  188.184.100.182  10.120.53.174    TCP        74 443 → 37642 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354614659 TSecr=4101542726 WS=128
  989 15.268787303  10.120.53.174    188.184.100.182  TCP        66 37642 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4101542726 TSecr=354614659
  990 15.269847276  10.120.53.174    188.184.100.182  TLSv1     583 Client Hello
  991 15.270259650  188.184.100.182  10.120.53.174    TCP        66 443 → 37642 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=354614659 TSecr=4101542727
  994 15.426293541  10.120.53.174    188.184.100.182  TCP        66 37642 → 443 [FIN, ACK] Seq=518 Ack=1 Win=64256 Len=0 TSval=4101542884 TSecr=354614659
  995 15.428829277  188.184.100.182  10.120.53.174    TCP        66 443 → 37642 [FIN, ACK] Seq=1 Ack=519 Win=15616 Len=0 TSval=354614675 TSecr=4101542884
  996 15.428853071  10.120.53.174    188.184.100.182  TCP        66 37642 → 443 [ACK] Seq=519 Ack=2 Win=64256 Len=0 TSval=4101542886 TSecr=354614675
 1007 16.157413415  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=1056/8196, ttl=64 (no response found!)
 1010 17.185410907  10.120.53.174    188.184.100.182  ICMP       98 Echo (ping) request  id=0x0001, seq=1057/8452, ttl=64 (no response found!)
```

```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
▾ Ethernet II, Src: Dell_97:00:32 (00:be:43:97:00:32), Dst: Cisco_c8:2a:e6 (00:87:31:c8:2a:e6)
  ▸ Destination: Cisco_c8:2a:e6 (00:87:31:c8:2a:e6)
  ▸ Source: Dell_97:00:32 (00:be:43:97:00:32)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.120.53.174, Dst: 188.184.100.182
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x2fe1 (12257)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xa933 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.120.53.174
    Destination Address: 188.184.100.182
▸ Internet Control Message Protocol
```

```
0000  00 87 31 c8 2a e6 00 be  43 97 00 32 08 00 45 00   ··1·*··· C··2··E·
0010  00 54 2f e1 40 00 40 01  a9 33 0a 78 35 ae bc b8   ·T/·@·@· ·3·x5···
0020  64 b6 08 00 bb 9a 00 01  04 11 b4 76 12 65 00 00   d······· ···v·e··
0030  00 00 ad a4 05 00 00 00  00 00 10 11 12 13 14 15   ········ ········
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
```

wireshark_enp0s31f6KQ55B2.pcapng   Packets: 1197 · Displayed: 71 (5.9%)   Profile: Default


Activities
Wireshark
Sep 26 11:51
*enp0s31f6
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

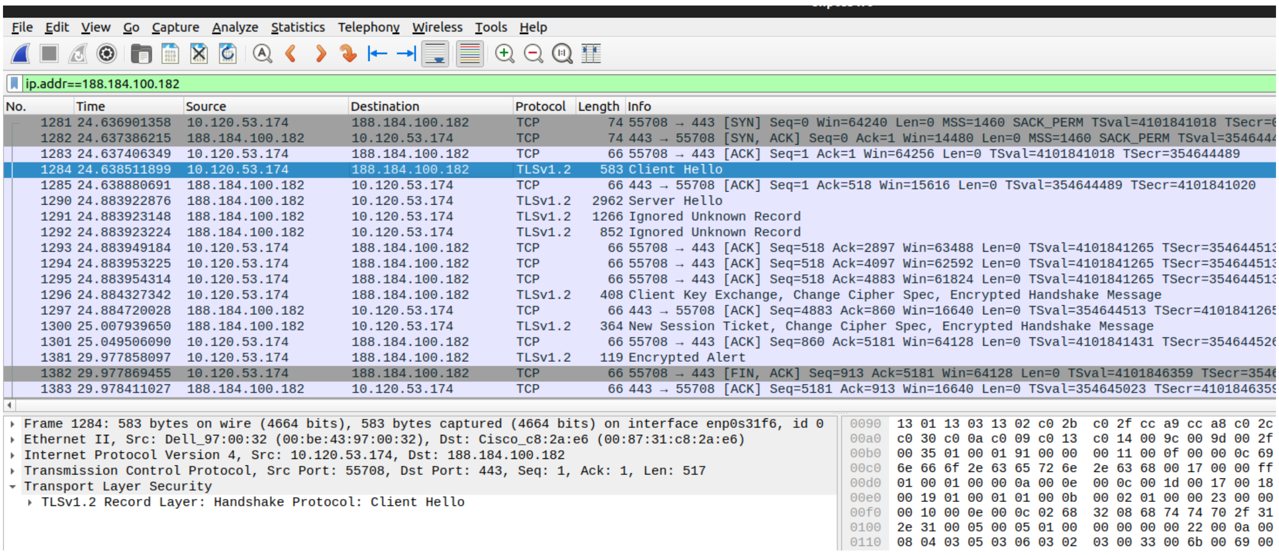
```
ip.addr==188.184.100.182
```

```
No.   Time          Source           Destination      Protocol Length Info
 1281 24.636901358  10.120.53.174    188.184.100.182  TCP        74 55708 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101841018 TSecr=0 WS=128
 1282 24.637386215  188.184.100.182  10.120.53.174    TCP        74 443 → 55708 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354644489 TSecr=4101841018 WS=128
 1283 24.637406349  10.120.53.174    188.184.100.182  TCP        66 55708 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4101841018 TSecr=354644489
 1284 24.638511899  10.120.53.174    188.184.100.182  TLSv1.2   583 Client Hello
 1285 24.638880691  188.184.100.182  10.120.53.174    TCP        66 443 → 55708 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=354644489 TSecr=4101841020
 1290 24.883922876  188.184.100.182  10.120.53.174    TLSv1.2  2962 Server Hello
 1291 24.883923148  188.184.100.182  10.120.53.174    TLSv1.2  1266 Ignored Unknown Record
 1292 24.883923224  188.184.100.182  10.120.53.174    TLSv1.2   852 Ignored Unknown Record
 1293 24.883949184  10.120.53.174    188.184.100.182  TCP        66 55708 → 443 [ACK] Seq=518 Ack=2897 Win=63488 Len=0 TSval=4101841265 TSecr=354644513
 1294 24.883953225  10.120.53.174    188.184.100.182  TCP        66 55708 → 443 [ACK] Seq=518 Ack=4097 Win=62592 Len=0 TSval=4101841265 TSecr=354644513
 1295 24.883954314  10.120.53.174    188.184.100.182  TCP        66 55708 → 443 [ACK] Seq=518 Ack=4883 Win=61824 Len=0 TSval=4101841265 TSecr=354644513
 1296 24.884327342  10.120.53.174    188.184.100.182  TLSv1.2   408 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 1297 24.884720028  188.184.100.182  10.120.53.174    TCP        66 443 → 55708 [ACK] Seq=4883 Ack=860 Win=16640 Len=0 TSval=354644513 TSecr=4101841265
 1300 25.007939650  188.184.100.182  10.120.53.174    TLSv1.2   364 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
 1301 25.049506090  10.120.53.174    188.184.100.182  TCP        66 55708 → 443 [ACK] Seq=860 Ack=5181 Win=64128 Len=0 TSval=4101841431 TSecr=354644526
 1381 29.977858097  10.120.53.174    188.184.100.182  TLSv1.2   119 Encrypted Alert
 1382 29.977869455  10.120.53.174    188.184.100.182  TCP        66 55708 → 443 [FIN, ACK] Seq=913 Ack=5181 Win=64128 Len=0 TSval=4101846359 TSecr=354644526
 1383 29.978411027  188.184.100.182  10.120.53.174    TCP        66 443 → 55708 [ACK] Seq=5181 Ack=913 Win=16640 Len=0 TSval=354645023 TSecr=4101846359
 1384 29.978411149  188.184.100.182  10.120.53.174    TCP        66 443 → 55708 [FIN, ACK] Seq=5181 Ack=914 Win=16640 Len=0 TSval=354645023 TSecr=4101846359
 1385 29.978437598  10.120.53.174    188.184.100.182  TCP        66 55708 → 443 [ACK] Seq=914 Ack=5182 Win=64128 Len=0 TSval=4101846359 TSecr=354645023
```

```
    Header Checksum: 0x1813 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.120.53.174
    Destination Address: 188.184.100.182
▾ Transmission Control Protocol, Src Port: 55708, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 55708
    Destination Port: 443
    [Stream index: 40]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1100520848
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x61c3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window …
```

```
0000  00 87 31 c8 2a e6 00 be  43 97 00 32 08 00 45 00   ··1·*··· C··2··E·
0010  00 3c c1 14 40 00 40 06  18 13 0a 78 35 ae bc b8   ·<··@·@· ···x5···
0020  64 b6 d9 9c 01 bb 41 98  9d 90 00 00 00 00 a0 02   d·····A· ········
0030  fa f0 61 c3 00 00 02 04  05 b4 04 02 08 0a f4 7d   ··a····· ·······}
0040  20 7a 00 00 00 00 01 03  03 07                      z······ ··
```

wireshark_enp0s31f6KY6YB2.pcapng   Packets: 1861 · Displayed: 20 (1.1%)   Profile: Default

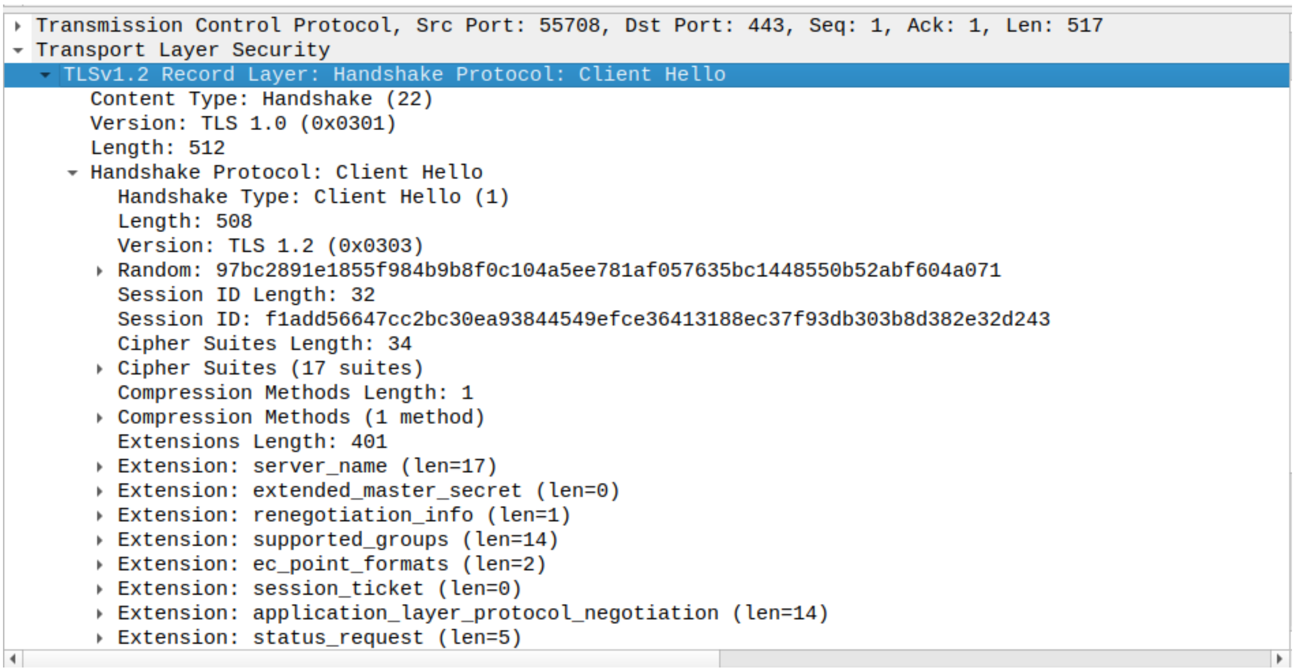


```
ip.addr==188.184.100.182
```

```
No.   Time          Source          Destination     Protocol Length Info
 1281 24.636901358  10.120.53.174   188.184.100.182 TCP        74 55708 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4101841018 TSecr=
 1282 24.637386215  188.184.100.182 10.120.53.174   TCP        74 443 → 55708 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM TSval=354644
 1283 24.637406349  10.120.53.174   188.184.100.182 TCP        66 55708 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4101841018 TSecr=354644489
 1284 24.638511899  10.120.53.174   188.184.100.182 TLSv1.2   583 Client Hello
 1285 24.638880691  188.184.100.182 10.120.53.174   TCP        66 443 → 55708 [ACK] Seq=1 Ack=518 Win=15616 Len=0 TSval=354644489 TSecr=4101841020
 1290 24.883922876  188.184.100.182 10.120.53.174   TLSv1.2  2962 Server Hello
 1291 24.883923148  188.184.100.182 10.120.53.174   TLSv1.2  1266 Ignored Unknown Record
 1292 24.883923224  188.184.100.182 10.120.53.174   TLSv1.2   852 Ignored Unknown Record
 1293 24.883949184  10.120.53.174   188.184.100.182 TCP        66 55708 → 443 [ACK] Seq=518 Ack=2897 Win=63488 Len=0 TSval=4101841265 TSecr=35464451
 1294 24.883953225  10.120.53.174   188.184.100.182 TCP        66 55708 → 443 [ACK] Seq=518 Ack=4097 Win=62592 Len=0 TSval=4101841265 TSecr=35464451
 1295 24.883954314  10.120.53.174   188.184.100.182 TCP        66 55708 → 443 [ACK] Seq=518 Ack=4883 Win=61824 Len=0 TSval=4101841265 TSecr=35464451
 1296 24.884327342  10.120.53.174   188.184.100.182 TLSv1.2   408 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 1297 24.884720028  188.184.100.182 10.120.53.174   TCP        66 443 → 55708 [ACK] Seq=4883 Ack=860 Win=16640 Len=0 TSval=354644513 TSecr=410184126
 1300 25.007939650  188.184.100.182 10.120.53.174   TLSv1.2   364 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
 1301 25.049506090  10.120.53.174   188.184.100.182 TCP        66 55708 → 443 [ACK] Seq=860 Ack=5181 Win=64128 Len=0 TSval=4101841431 TSecr=35464452
 1381 29.977858097  10.120.53.174   188.184.100.182 TLSv1.2   119 Encrypted Alert
 1382 29.977869455  10.120.53.174   188.184.100.182 TCP        66 55708 → 443 [FIN, ACK] Seq=913 Ack=5181 Win=64128 Len=0 TSval=4101846359 TSecr=354
 1383 29.978411027  188.184.100.182 10.120.53.174   TCP        66 443 → 55708 [ACK] Seq=5181 Ack=913 Win=16640 Len=0 TSval=354645023 TSecr=410184635
```

```
▸ Frame 1284: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface enp0s31f6, id 0
▸ Ethernet II, Src: Dell_97:00:32 (00:be:43:97:00:32), Dst: Cisco_c8:2a:e6 (00:87:31:c8:2a:e6)
▸ Internet Protocol Version 4, Src: 10.120.53.174, Dst: 188.184.100.182
▸ Transmission Control Protocol, Src Port: 55708, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▾ Transport Layer Security
  ▸ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
```

```
0090  13 01 13 03 13 02 c0 2b  c0 2f cc a9 cc a8 c0 2c
00a0  c0 30 c0 0a c0 09 c0 13  c0 14 00 9c 00 9d 00 2f
00b0  00 35 01 00 01 91 00 00  00 11 00 0f 00 00 0c 69
00c0  6e 66 6f 2e 63 65 72 6e  2e 63 68 00 17 00 00 ff
00d0  01 00 01 00 00 0a 00 0e  00 0c 00 1d 00 17 00 18
00e0  00 19 01 00 01 01 00 0b  00 02 01 00 00 23 00 00
00f0  00 10 00 0e 00 0c 02 68  32 08 68 74 74 70 2f 31
0100  2e 31 00 05 00 05 01 00  00 00 00 00 22 00 0a 00
0110  08 04 03 05 03 06 03 02  03 00 33 00 6b 00 69 00
```



```
▸ Transmission Control Protocol, Src Port: 55708, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
      ▸ Random: 97bc2891e1855f984b9b8f0c104a5ee781af057635bc1448550b52abf604a071
        Session ID Length: 32
        Session ID: f1add56647cc2bc30ea93844549efce36413188ec37f93db303b8d382e32d243
        Cipher Suites Length: 34
      ▸ Cipher Suites (17 suites)
        Compression Methods Length: 1
      ▸ Compression Methods (1 method)
        Extensions Length: 401
      ▸ Extension: server_name (len=17)
      ▸ Extension: extended_master_secret (len=0)
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: supported_groups (len=14)
      ▸ Extension: ec_point_formats (len=2)
      ▸ Extension: session_ticket (len=0)
      ▸ Extension: application_layer_protocol_negotiation (len=14)
      ▸ Extension: status_request (len=5)
```

Conclusion:

- Wireshark is a powerful tool for network analysis, providing insights into the details of data transmission.
- Understanding the TCP handshake process helps differentiate between secured (HTTPS) and unsecured (HTTP) connections.
- The choice between HTTP and HTTPS significantly impacts the security of data transmitted over the network.