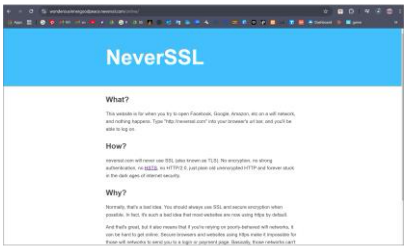
Wireshark Lab 1

By : Najla Mohammed Alfayez - 421202010

Part 1: Capturing HTTP Traffic.

Task 1: Start Wireshark and capture packets.

Task 2: Filter HTTP packets and analyze them.



wondersuinnergoodpeace.neverssl.com/online/

NeverSSL

What?

This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.

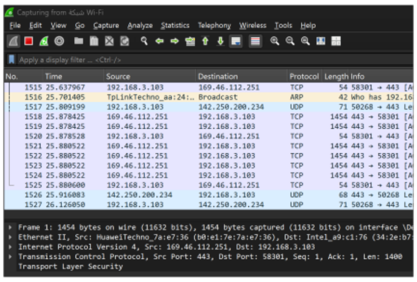
How?

neverssl.com will never use SSL (also known as TLS). No encryption, no strong authentication, no HSTS, no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

Why?

Normally, that's a bad idea. You should always use SSL and secure encryption when possible. In fact, it's such a bad idea that most websites are now using https by default.

And that's great, but it also means that if you're relying on poorly-behaved wifi networks, it can be hard to get online. Secure browsers and websites using https make it impossible for those wifi networks to send you to a login or payment page. Basically, those networks can't



Capturing from شبكة Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

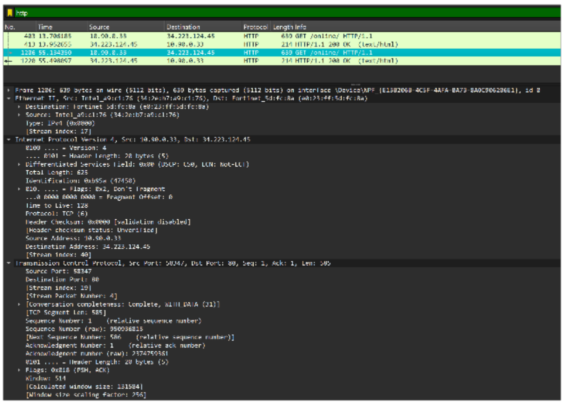
```
No.   Time      Source             Destination      Protocol Length Info
 1515 25.637967 192.168.3.103      169.46.112.251   TCP        54 58301 → 443 [A
 1516 25.701405 TpLinkTechno_aa:24:… Broadcast      ARP        42 Who has 192.16
 1517 25.809199 192.168.3.103      142.250.200.234  UDP        71 50268 → 443 Le
 1518 25.878425 169.46.112.251     192.168.3.103    TCP      1454 443 → 58301 [A
 1519 25.878425 169.46.112.251     192.168.3.103    TCP      1454 443 → 58301 [A
 1520 25.878528 192.168.3.103      169.46.112.251   TCP        54 58301 → 443 [A
 1521 25.880522 169.46.112.251     192.168.3.103    TCP      1454 443 → 58301 [A
 1522 25.880522 169.46.112.251     192.168.3.103    TCP      1454 443 → 58301 [A
 1523 25.880522 169.46.112.251     192.168.3.103    TCP      1454 443 → 58301 [A
 1524 25.880522 169.46.112.251     192.168.3.103    TCP      1454 443 → 58301 [A
 1525 25.880600 192.168.3.103      169.46.112.251   TCP        54 58301 → 443 [A
 1526 25.916083 142.250.200.234    192.168.3.103    UDP        68 443 → 50268 Le
 1527 26.126050 192.168.3.103      142.250.200.234  UDP        71 50268 → 443 Le

 Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \De
 Ethernet II, Src: HuaweiTechno_7a:e7:36 (b0:e1:7e:7a:e7:36), Dst: Intel_a9:c1:76 (34:2e:b7
 Internet Protocol Version 4, Src: 169.46.112.251, Dst: 192.168.3.103
 Transmission Control Protocol, Src Port: 443, Dst Port: 58301, Seq: 1, Ack: 1, Len: 1400
 Transport Layer Security
```

Part 2: Analyzing TCP/IP Traffic.

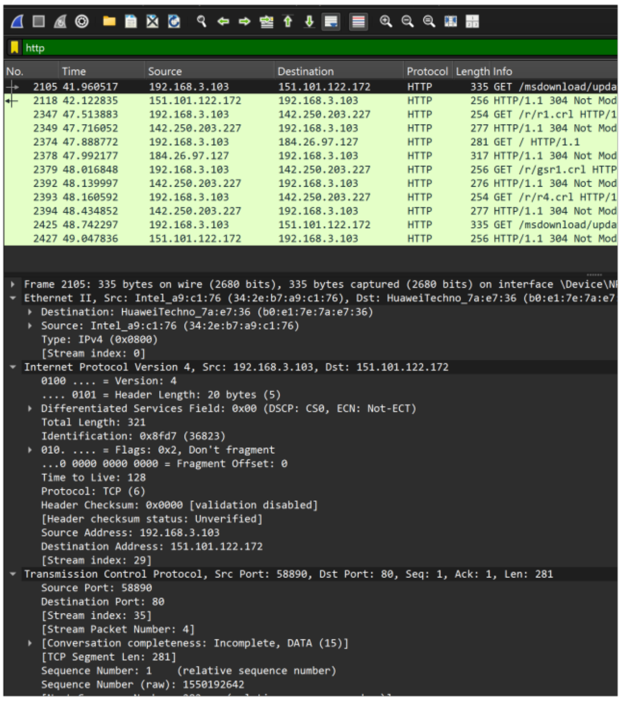
Task 1: Filter TCP packets

Task 2: Analyze TCP handshake and investigate Data Transfer and Termination



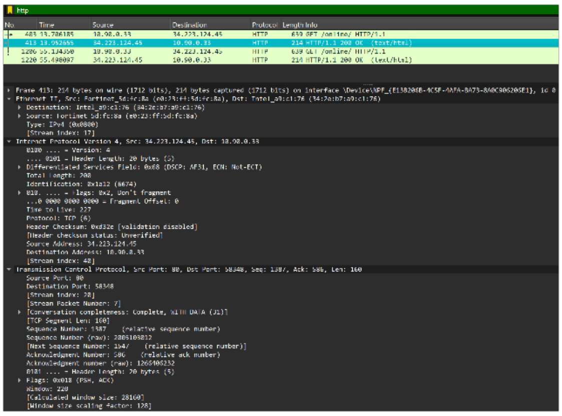
```
No.   Time      Source          Destination     Protocol Length Info
  403 13.706185 10.90.0.33      34.223.124.45   HTTP       639 GET /online/ HTTP/1.1
  413 13.952655 34.223.124.45   10.90.0.33      HTTP       214 HTTP/1.1 200 OK  (text/html)
 1206 55.134350 10.90.0.33      34.223.124.45   HTTP       639 GET /online/ HTTP/1.1
 1220 55.490097 34.223.124.45   10.90.0.33      HTTP       214 HTTP/1.1 200 OK  (text/html)

 Frame 1206: 639 bytes on wire (5112 bits), 639 bytes captured (5112 bits) on interface \Device\NPF_{E1382068-4C5F-4AFA-BA73-8A0C906206E1}, id 0
 Ethernet II, Src: Intel_a9:c1:76 (34:2e:b7:a9:c1:76), Dst: Fortinet_5d:fc:8a (e0:23:ff:5d:fc:8a)
   Destination: Fortinet_5d:fc:8a (e0:23:ff:5d:fc:8a)
   Source: Intel_a9:c1:76 (34:2e:b7:a9:c1:76)
   Type: IPv4 (0x0800)
   [Stream index: 17]
 Internet Protocol Version 4, Src: 10.90.0.33, Dst: 34.223.124.45
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 625
   Identification: 0xb95a (47450)
   010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0x0000 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 10.90.0.33
   Destination Address: 34.223.124.45
   [Stream index: 40]
 Transmission Control Protocol, Src Port: 58347, Dst Port: 80, Seq: 1, Ack: 1, Len: 585
   Source Port: 58347
   Destination Port: 80
   [Stream index: 19]
   [Stream Packet Number: 4]
   [Conversation completeness: Complete, WITH_DATA (31)]
   [TCP Segment Len: 585]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 950036815
   [Next Sequence Number: 586    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 2374759361
   0101 .... = Header Length: 20 bytes (5)
   Flags: 0x018 (PSH, ACK)
   Window: 514
   [Calculated window size: 131584]
   [Window size scaling factor: 256]
```



```
No.   Time      Source          Destination     Protocol Length Info
 2105 41.960517 192.168.3.103   151.101.122.172 HTTP       335 GET /msdownload/upda
 2118 42.122835 151.101.122.172 192.168.3.103   HTTP       256 HTTP/1.1 304 Not Mod
 2347 47.513883 192.168.3.103   142.250.203.227 HTTP       254 GET /r/r1.crl HTTP/1
 2349 47.716052 142.250.203.227 192.168.3.103   HTTP       277 HTTP/1.1 304 Not Mod
 2374 47.888772 192.168.3.103   184.26.97.127   HTTP       281 GET / HTTP/1.1
 2378 47.992177 184.26.97.127   192.168.3.103   HTTP       317 HTTP/1.1 304 Not Mod
 2379 48.016848 192.168.3.103   142.250.203.227 HTTP       256 GET /r/gsr1.crl HTTP
 2392 48.139997 142.250.203.227 192.168.3.103   HTTP       276 HTTP/1.1 304 Not Mod
 2393 48.160592 192.168.3.103   142.250.203.227 HTTP       254 GET /r/r4.crl HTTP/1
 2394 48.434852 142.250.203.227 192.168.3.103   HTTP       277 HTTP/1.1 304 Not Mod
 2425 48.742297 192.168.3.103   151.101.122.172 HTTP       335 GET /msdownload/upda
 2427 49.047836 151.101.122.172 192.168.3.103   HTTP       256 HTTP/1.1 304 Not Mod

 Frame 2105: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface \Device\NP
 Ethernet II, Src: Intel_a9:c1:76 (34:2e:b7:a9:c1:76), Dst: HuaweiTechno_7a:e7:36 (b0:e1:7e:7a:e7
   Destination: HuaweiTechno_7a:e7:36 (b0:e1:7e:7a:e7:36)
   Source: Intel_a9:c1:76 (34:2e:b7:a9:c1:76)
   Type: IPv4 (0x0800)
   [Stream index: 0]
 Internet Protocol Version 4, Src: 192.168.3.103, Dst: 151.101.122.172
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 321
   Identification: 0x8fd7 (36823)
   010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0x0000 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.3.103
   Destination Address: 151.101.122.172
   [Stream index: 29]
 Transmission Control Protocol, Src Port: 58890, Dst Port: 80, Seq: 1, Ack: 1, Len: 281
   Source Port: 58890
   Destination Port: 80
   [Stream index: 35]
   [Stream Packet Number: 4]
   [Conversation completeness: Incomplete, DATA (15)]
   [TCP Segment Len: 281]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 1550192642
```



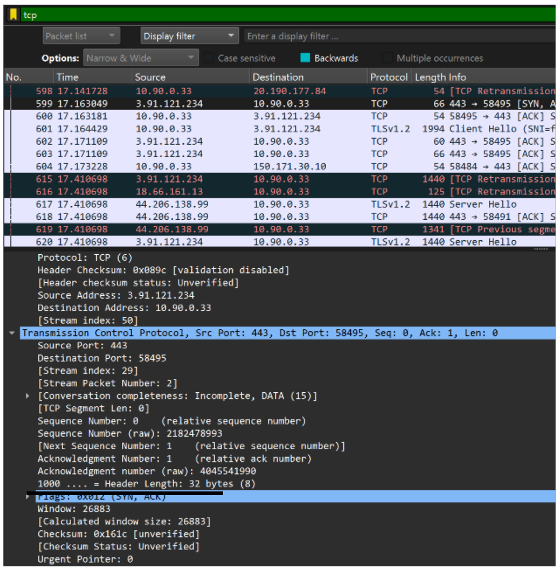
```
No.   Time      Source          Destination     Protocol Length Info
  403 13.706185 10.90.0.33      34.223.124.45   HTTP       639 GET /online/ HTTP/1.1
  413 13.952655 34.223.124.45   10.90.0.33      HTTP       214 HTTP/1.1 200 OK  (text/html)
 1206 55.134350 10.90.0.33      34.223.124.45   HTTP       639 GET /online/ HTTP/1.1
 1220 55.490097 34.223.124.45   10.90.0.33      HTTP       214 HTTP/1.1 200 OK  (text/html)

 Frame 413: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface \Device\NPF_{E1382068-4C5F-4AFA-BA73-8A0C906206E1}, id 0
 Ethernet II, Src: Fortinet_5d:fc:8a (e0:23:ff:5d:fc:8a), Dst: Intel_a9:c1:76 (34:2e:b7:a9:c1:76)
   Destination: Intel_a9:c1:76 (34:2e:b7:a9:c1:76)
   Source: Fortinet_5d:fc:8a (e0:23:ff:5d:fc:8a)
   Type: IPv4 (0x0800)
   [Stream index: 17]
 Internet Protocol Version 4, Src: 34.223.124.45, Dst: 10.90.0.33
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
   Differentiated Services Field: 0x68 (DSCP: AF31, ECN: Not-ECT)
   Total Length: 200
   Identification: 0x1a12 (6674)
   010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 227
   Protocol: TCP (6)
   Header Checksum: 0xd32e [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 34.223.124.45
   Destination Address: 10.90.0.33
   [Stream index: 40]
 Transmission Control Protocol, Src Port: 80, Dst Port: 58348, Seq: 1387, Ack: 586, Len: 160
   Source Port: 80
   Destination Port: 58348
   [Stream index: 20]
   [Stream Packet Number: 7]
   [Conversation completeness: Complete, WITH_DATA (31)]
   [TCP Segment Len: 160]
   Sequence Number: 1387    (relative sequence number)
   Sequence Number (raw): 2805103012
   [Next Sequence Number: 1547    (relative sequence number)]
   Acknowledgment Number: 586    (relative ack number)
   Acknowledgment number (raw): 1266406232
   0101 .... = Header Length: 20 bytes (5)
   Flags: 0x018 (PSH, ACK)
   Window: 220
   [Calculated window size: 28160]
   [Window size scaling factor: 128]
```

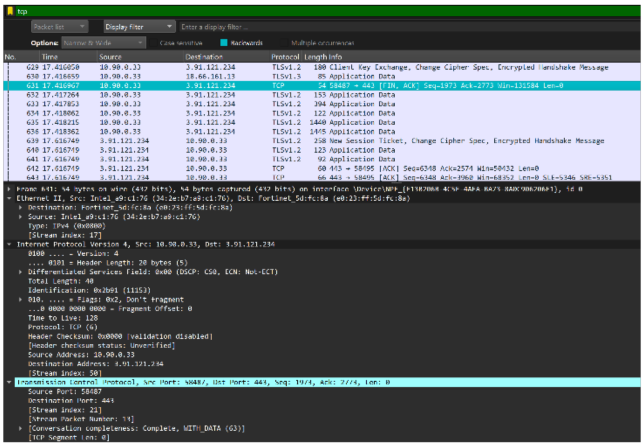
Part 3: Capturing and Analyzing UDP Traffic

Task 1: Generate UDP traffic and capture packets

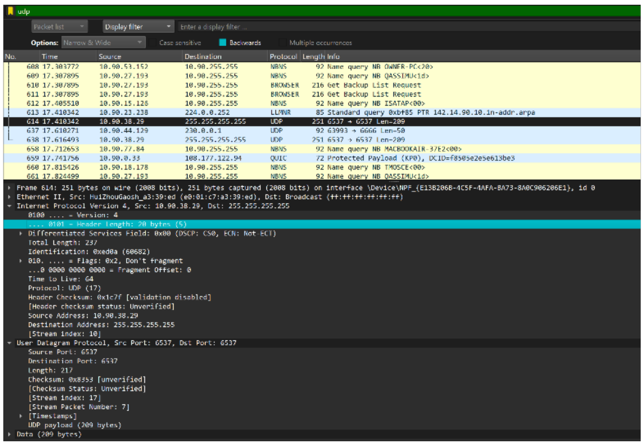
Task 2: Filter and analysis UDP Packets



```
tcp
Packet list   Display filter   Enter a display filter ...
Options: Narrow & Wide   Case sensitive   Backwards   Multiple occurrences
No.   Time       Source          Destination     Protocol Length Info
  598 17.141728  10.90.0.33      20.190.177.84   TCP        54 [TCP Retransmission
  599 17.163049  3.91.121.234    10.90.0.33      TCP        66 443 → 58495 [SYN, A
  600 17.163181  10.90.0.33      3.91.121.234    TCP        54 58495 → 443 [ACK] S
  601 17.164429  10.90.0.33      3.91.121.234    TLSv1.2  1994 Client Hello (SNI=f
  602 17.171109  3.91.121.234    10.90.0.33      TCP        60 443 → 58495 [ACK] S
  603 17.171109  3.91.121.234    10.90.0.33      TCP        66 443 → 58495 [ACK] S
  604 17.173228  10.90.0.33      150.171.30.10   TCP        54 58484 → 443 [ACK] S
  615 17.410698  3.91.121.234    10.90.0.33      TCP      1440 [TCP Retransmission
  616 17.410698  18.66.161.13    10.90.0.33      TCP       125 [TCP Retransmission
  617 17.410698  44.206.138.99   10.90.0.33      TLSv1.2  1440 Server Hello
  618 17.410698  44.206.138.99   10.90.0.33      TCP      1440 443 → 58491 [ACK] S
  619 17.410698  44.206.138.99   10.90.0.33      TCP      1341 [TCP Previous segme
  620 17.410698  3.91.121.234    10.90.0.33      TLSv1.2  1440 Server Hello
    Protocol: TCP (6)
    Header Checksum: 0x089c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 3.91.121.234
    Destination Address: 10.90.0.33
    [Stream index: 50]
Transmission Control Protocol, Src Port: 443, Dst Port: 58495, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 58495
    [Stream index: 29]
    [Stream Packet Number: 2]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2182478993
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4045541990
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x012 (SYN, ACK)
    Window: 26883
    [Calculated window size: 26883]
    Checksum: 0x161c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```



```
tcp
Packet list   Display filter   Enter a display filter ...
Options: Narrow & Wide   Case sensitive   Backwards   Multiple occurrences
No.   Time       Source          Destination     Protocol Length Info
  629 17.416050  10.90.0.33      3.91.121.234    TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  630 17.416659  10.90.0.33      18.66.161.13    TLSv1.3    85 Application Data
  631 17.416967  10.90.0.33      3.91.121.234    TCP        54 58487 → 443 [FIN, ACK] Seq=1973 Ack=2773 Win=131584 Len=0
  632 17.417264  10.90.0.33      3.91.121.234    TLSv1.2   153 Application Data
  633 17.417853  10.90.0.33      3.91.121.234    TLSv1.2   394 Application Data
  634 17.418062  10.90.0.33      3.91.121.234    TLSv1.2   122 Application Data
  635 17.418215  10.90.0.33      3.91.121.234    TLSv1.2  1440 Application Data
  636 17.418362  10.90.0.33      3.91.121.234    TLSv1.2  1445 Application Data
  639 17.616749  3.91.121.234    10.90.0.33      TLSv1.2   258 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  640 17.616749  3.91.121.234    10.90.0.33      TLSv1.2   123 Application Data
  641 17.616749  3.91.121.234    10.90.0.33      TLSv1.2    92 Application Data
  642 17.616749  3.91.121.234    10.90.0.33      TCP        60 443 → 58495 [ACK] Seq=6348 Ack=2574 Win=50432 Len=0
  643 17.616749  3.91.121.234    10.90.0.33      TCP        66 443 → 58495 [ACK] Seq=6348 Ack=3960 Win=68352 Len=0 SLE=5346 SRE=5351
Frame 631: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{E13B206B-4C5F-4AFA-BA73-8A0C906206E1}, id 0
Ethernet II, Src: Intel_a9:c1:76 (34:2e:b7:a9:c1:76), Dst: Fortinet_5d:fc:8a (e0:23:ff:5d:fc:8a)
    Destination: Fortinet_5d:fc:8a (e0:23:ff:5d:fc:8a)
    Source: Intel_a9:c1:76 (34:2e:b7:a9:c1:76)
    Type: IPv4 (0x0800)
    [Stream index: 17]
Internet Protocol Version 4, Src: 10.90.0.33, Dst: 3.91.121.234
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x2b91 (11153)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.90.0.33
    Destination Address: 3.91.121.234
    [Stream index: 50]
Transmission Control Protocol, Src Port: 58487, Dst Port: 443, Seq: 1973, Ack: 2773, Len: 0
    Source Port: 58487
    Destination Port: 443
    [Stream index: 21]
    [Stream Packet Number: 13]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
```



```
udp
Packet list   Display filter   Enter a display filter ...
Options: Narrow & Wide   Case sensitive   Backwards   Multiple occurrences
No.   Time       Source          Destination      Protocol Length Info
  608 17.303772  10.90.53.152    10.90.255.255    NBNS       92 Name query NB OWNER-PC<20>
  609 17.307895  10.90.27.193    10.90.255.255    NBNS       92 Name query NB QASSIMU<1d>
  610 17.307895  10.90.27.193    10.90.255.255    BROWSER   216 Get Backup List Request
  611 17.307895  10.90.27.193    10.90.255.255    BROWSER   216 Get Backup List Request
  612 17.405510  10.90.15.126    10.90.255.255    NBNS       92 Name query NB ISATAP<00>
  613 17.410342  10.90.23.238    224.0.0.252      LLMNR      85 Standard query 0xbf85 PTR 142.14.90.10.in-addr.arpa
  614 17.410342  10.90.38.29     255.255.255.255  UDP       251 6537 → 6537 Len=209
  637 17.610271  10.90.44.129    230.0.0.1        UDP        92 63993 → 6666 Len=50
  638 17.616493  10.90.38.29     255.255.255.255  UDP       251 6537 → 6537 Len=209
  658 17.712653  10.90.77.84     10.90.255.255    NBNS       92 Name query NB MACBOOKAIR-37E2<00>
  659 17.741756  10.90.0.33      108.177.122.94   QUIC       72 Protected Payload (KP0), DCID=f8505e2e5e613be3
  660 17.815426  10.90.18.178    10.90.255.255    NBNS       92 Name query NB TMOSCE<00>
  661 17.824499  10.90.27.193    10.90.255.255    NBNS       92 Name query NB QASSIMU<1d>
Frame 614: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits) on interface \Device\NPF_{E13B206B-4C5F-4AFA-BA73-8A0C906206E1}, id 0
Ethernet II, Src: HuiZhouGaosh_a3:39:ed (e0:01:c7:a3:39:ed), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.90.38.29, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 237
    Identification: 0xed0a (60682)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x1c7f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.90.38.29
    Destination Address: 255.255.255.255
    [Stream index: 10]
User Datagram Protocol, Src Port: 6537, Dst Port: 6537
    Source Port: 6537
    Destination Port: 6537
    Length: 217
    Checksum: 0x8353 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 17]
    [Stream Packet Number: 7]
    [Timestamps]
    UDP payload (209 bytes)
Data (209 bytes)
```

Part 4 :

Task 1 :

	TCP or UDP	Reasons
Reliability and connection establishment	TCP	Uses a **three-way handshake** (SYN, SYN-ACK, ACK) to establish a reliable connection before data transfer.
Data integrity and ordering	TCP	Ensures **error detection, retransmission of lost packets**, and **correct packet ordering** before delivering to the application.

	TCP	UDP
USECASE	File Transfer (FTP, HTTP, Email)	Live Streaming, Online Gaming, VoIP (Zoom, Skype)
performance	**Secure and reliable** but slower due to connection setup and error correction.	**Fast** but less reliable (no retransmissions or ordering).