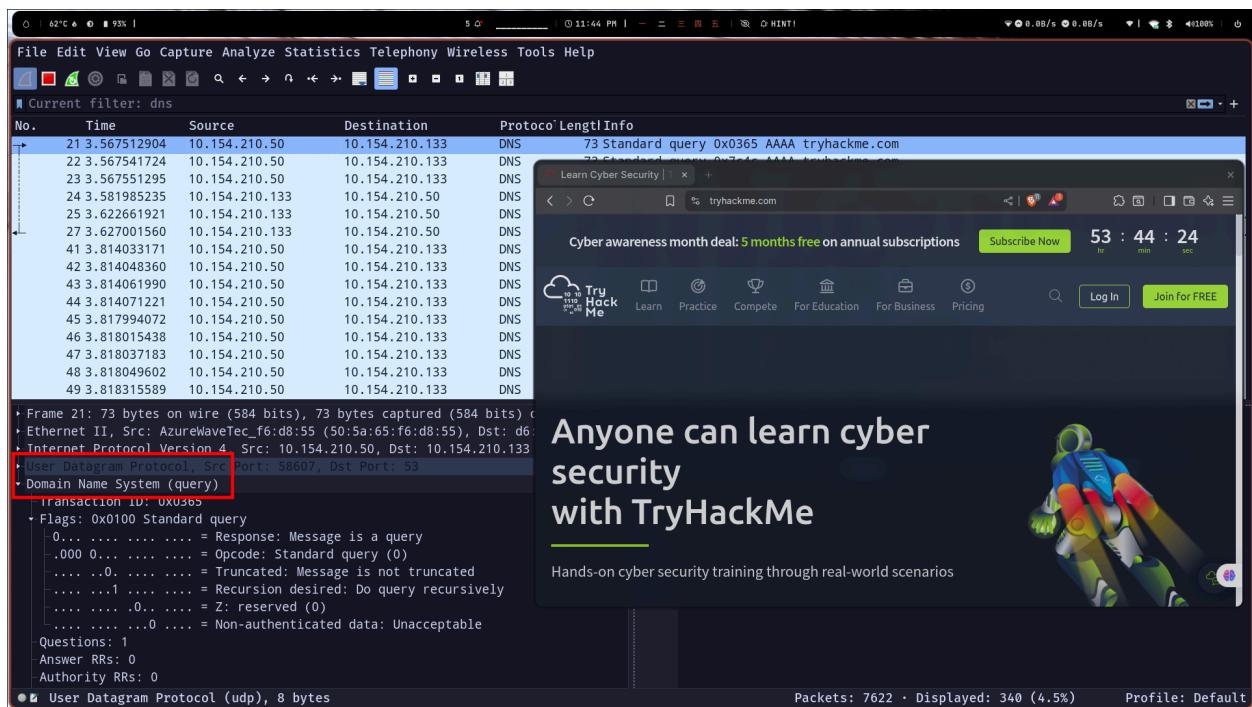


Networking - Assignment 10 - Wireshark

Praneesh R V
CB.SC.U4CYS23036

Part - 1 - DNS Capture

1, I initiated a search query in my browser to access tryhackme.com
Protocols captured: DNS-UDP



2, Source IP: 10.154.210.50

Destination IP: 10.154.210.133

DNS Query made: tryhackme.com

Response time for DNS Resolution: 3.56 seconds

```

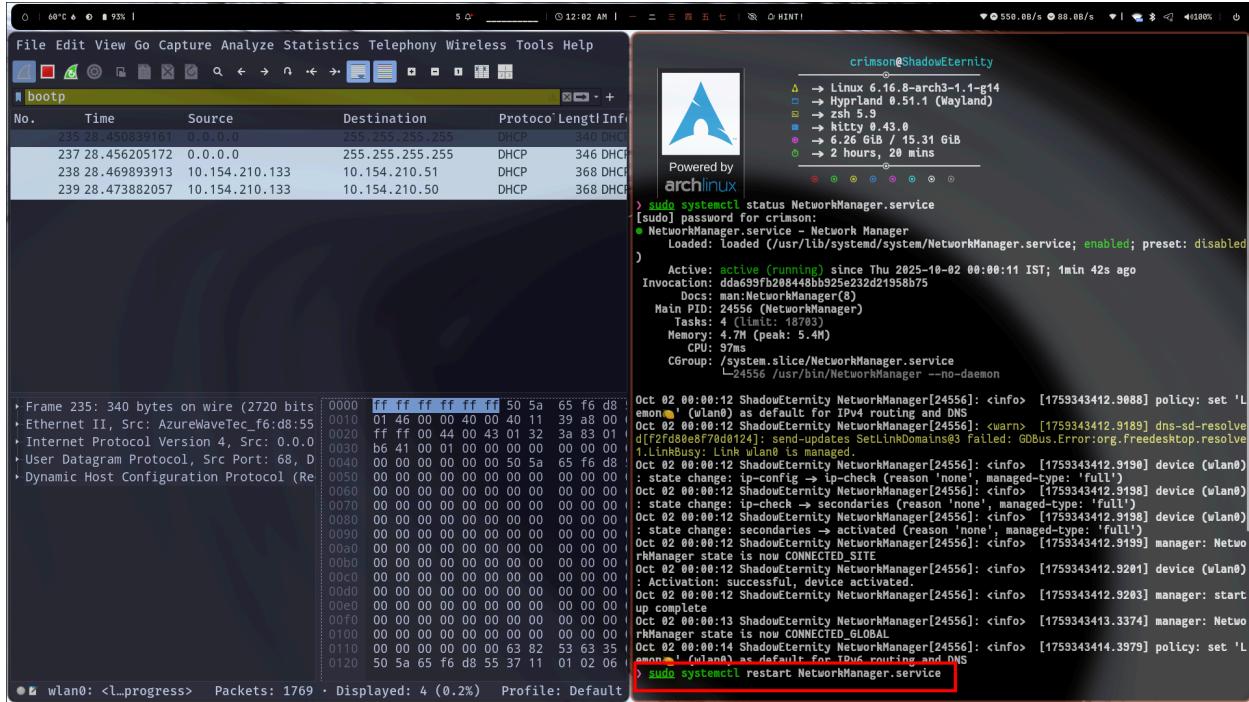
└─ Domain Name System (query)
  ├ Transaction ID: 0x0365
  └─ Flags: 0x0100 Standard query
    └ Questions: 1
      └ Answer RRs: 0
      └ Authority RRs: 0
      └ Additional RRs: 0
    └ Queries
      └─ tryhackme.com: type AAAA, class IN
        └ Name: tryhackme.com

```

Part 2 - DHCP Capture

1, by restarting my network manager, i captured my DHCP traffic

Protocols used - DHCP on UDP



2,DHCP Discover Message: Boot Request

DHCP Offer has message type, IP Address, DHCP server identifier, broadcast address, client mac address, Lease time

DHCP requests for an IP, subnet mask, DNS and broadcast address

DHCP ACK message contains Server identifier, IP address Lease Time, Router, Domain Name

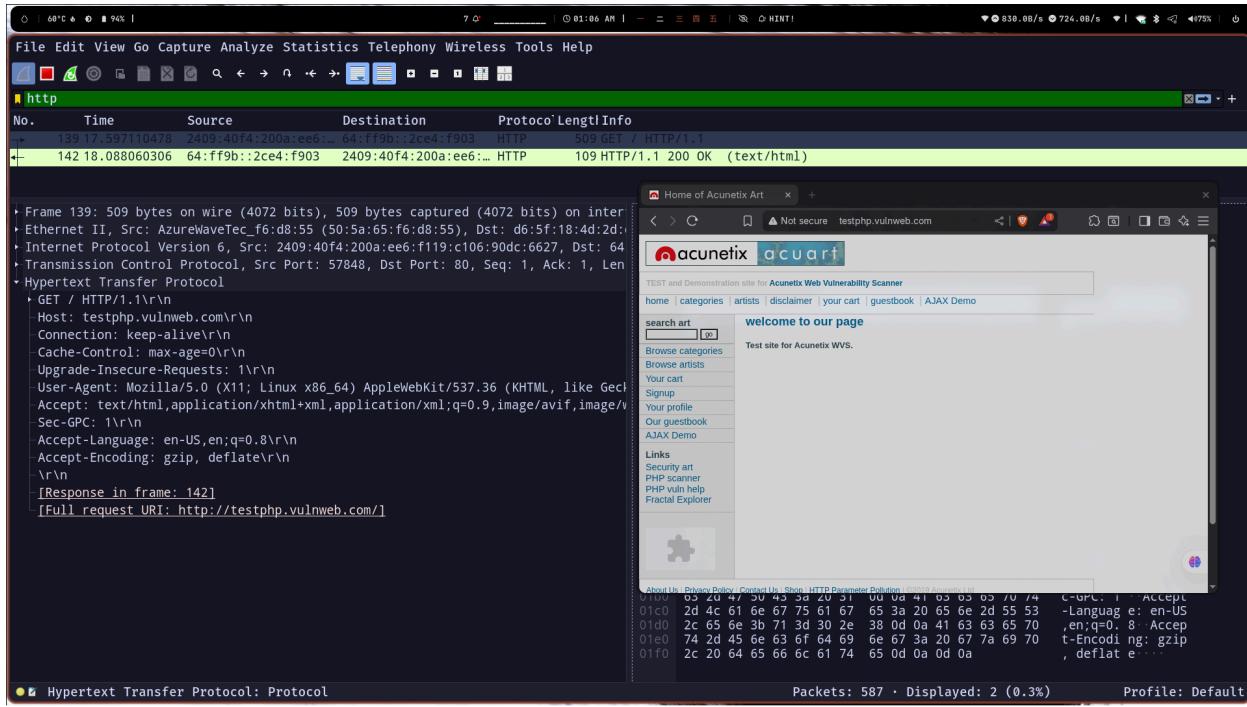
IP Assigned to client: 10.154.210.51

```
└ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf652b641
    Seconds elapsed: 0
    ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.154.210.51
    Next server IP address: 10.154.210.133
    Relay agent IP address: 0.0.0.0
    Client MAC address: AzureWaveTec_f6:d8:55 (50:5a:65:f6:d8:55)
    Client hardware address padding: 000000000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    ▶ Option: (53) DHCP Message Type (ACK)
    ▶ Option: (54) DHCP Server Identifier (10.154.210.133)
    ▶ Option: (51) IP Address Lease Time
    ▶ Option: (58) Renewal Time Value
    ▶ Option: (59) Rebinding Time Value
    ▶ Option: (1) Subnet Mask (255.255.255.0)
    ▶ Option: (28) Broadcast Address (10.154.210.255)
    ▶ Option: (3) Router
    ▶ Option: (6) Domain Name Server
    ▶ Option: (12) Host Name
    ▶ Option: (43) Vendor-Specific Information
● DHCP/BOOTP option type (dhcp.option.type), 17 bytes
```

Part 3 HTTP Capture

I set the filter to http, and opened <http://testphp.vulnweb.com/> in browser and captured the packet

Protocols used: HTTP - TCP



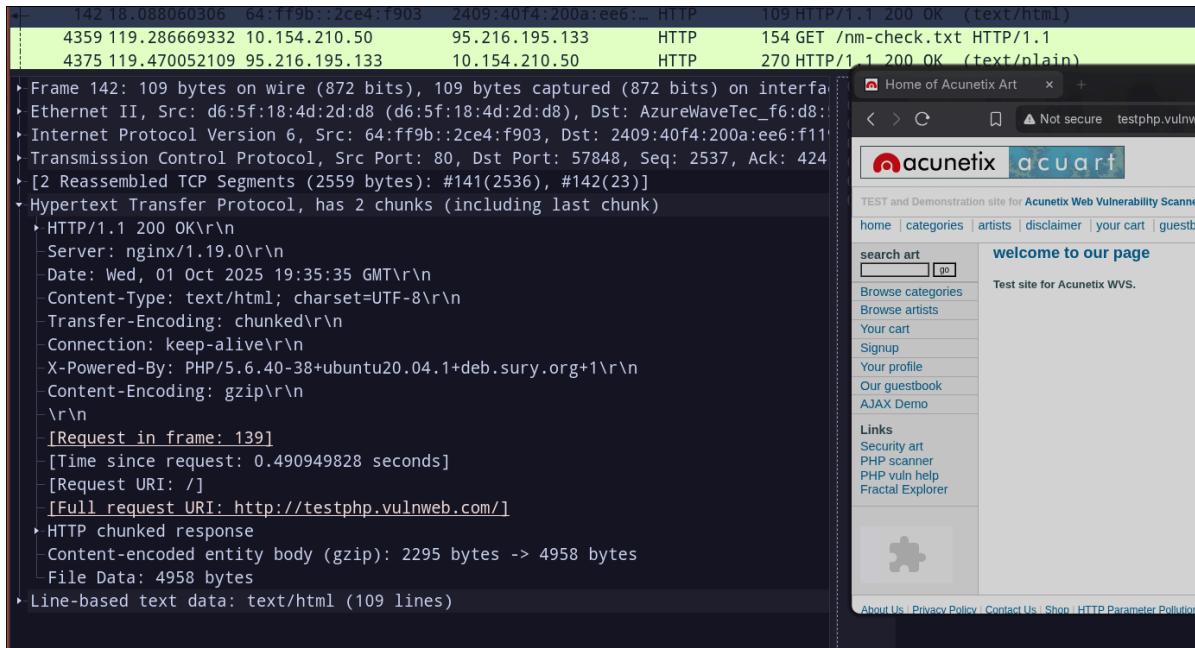
Captured details

Method - GET

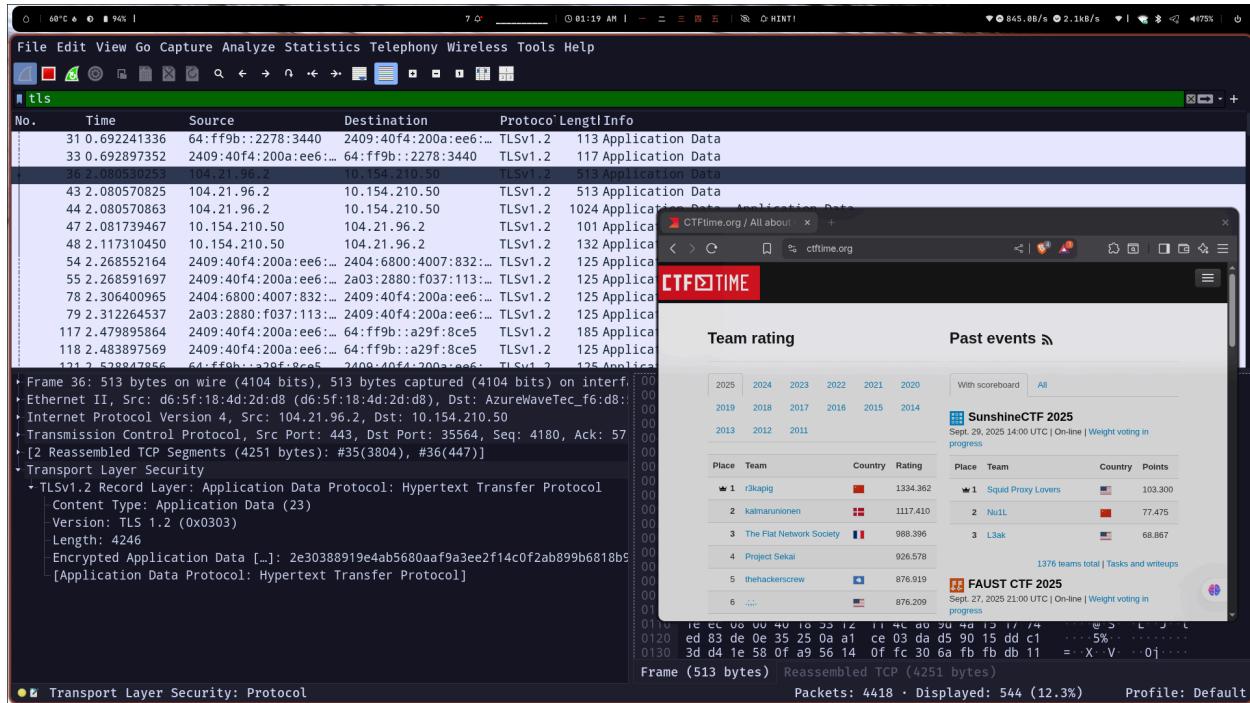
Status code - 200-OK

Response content - text/html

Content length - 109 lines



Part 4 HTTPS Capture



1, I opened <https://ctftime.org> in my browser, and put the TLS filter to capture https Protocols HTTPS(TLS) and TCP

2, **SSL/TLS handshake:** The handshake is a series of messages exchanged to establish a secure connection.

Steps:

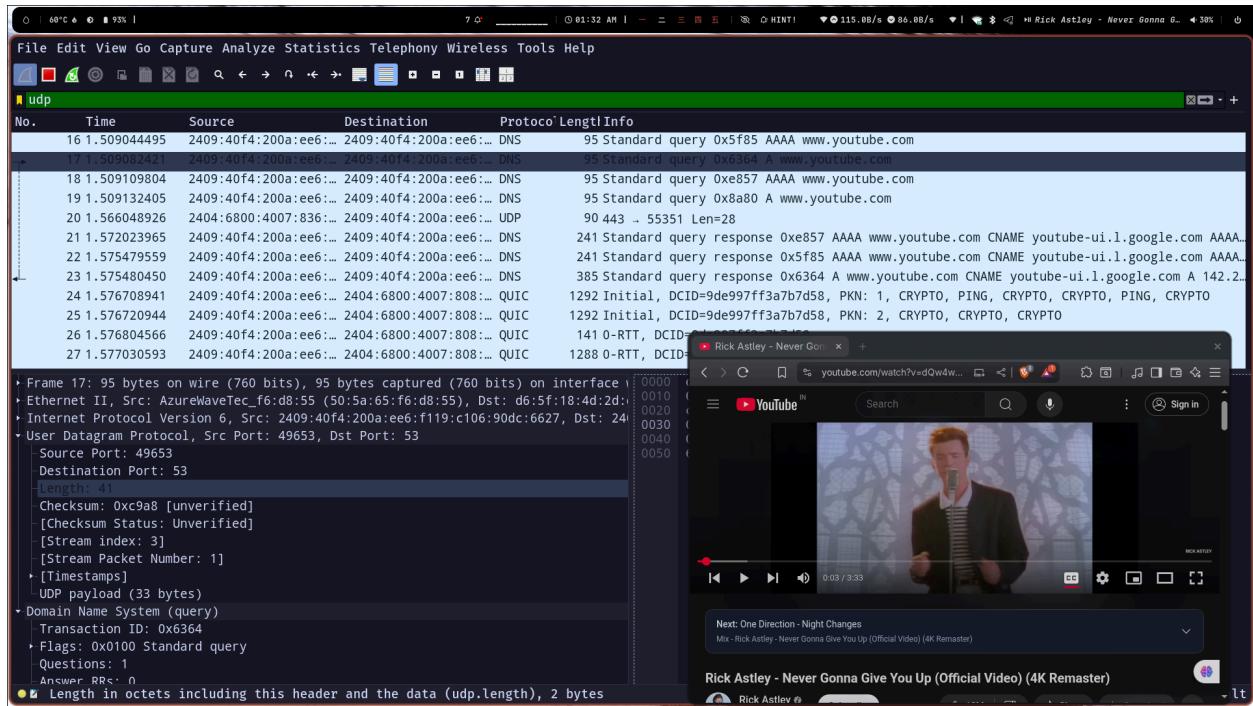
1. Client hello
2. Server hello
3. Certificate, Server Key Exchange, Server Hello Done
4. Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5. Application Data

Informations exchanged during handshake: Supported TLS versions, cipher suites, chosen TLS version, server's public certificate, Key-exchange material, Finished messages verifying integrity of handshake.

Yes, the server provided a certificate chain. It contains Subject, Issuer, Validity, Public Key, Signature Algorithm, Serial number.

Part 5 - UDP Capture

I played a youtube video on my browser and captured a UDP packet
Protocols captured - UDP, DNS

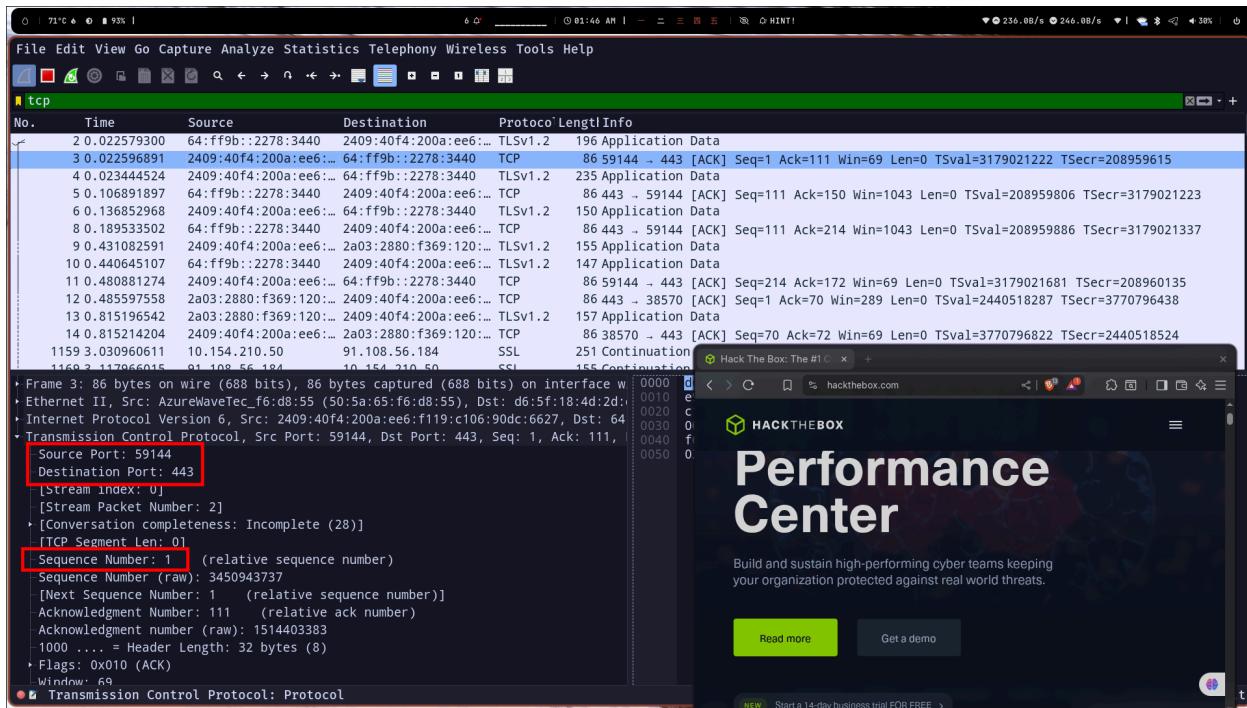


Source port: 49653, Destination port: 53

Payload size: 33 bytes

No retransmission or error occurred

Part 6 - TCP Capture



1.I opened Hackthebox.com website and captured tcp packet in wireshark

Protocol used: TCP

2.

Source Port: 443 , Destination port: 59144

Yes i can spot the 3 way handshake SYN, SYN-ACK and ACK

Sequence Number: 1

TCP uses a sliding window mechanism for flow control. Here window:69

```
Window: 69
[Calculated window size: 69]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x5cae [unverified]
[Checksum Status: Unverified]
```