IT – 304 | CN | LAB-8

(Harsh Gajjar – 202201140)

Section 1: Investigating DHCP Behaviour

Gathering a Packet Trace:

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
911	19:52:20.409181	192.168.29.143	192.168.29.1	DHCP	342	DHCP Release - Transaction ID 0xf3c0d4f4
1695	19:52:27.784152	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x38cc813d
1699	19:52:27.799943	192.168.29.1	192.168.29.143	DHCP	342	DHCP Offer - Transaction ID 0x38cc813d
1700	19:52:27.801804	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x38cc813d
1701	19:52:27.807359	192.168.29.1	192.168.29.143	DHCP	350	DHCP ACK - Transaction ID 0x38cc813d
1807	19:52:30.816676	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - Transaction ID 0x2699661d
2166	19:52:33.763783	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - Transaction ID 0x2699661d
2170	19:52:33.791859	192.168.29.1	192.168.29.143	DHCP	350	DHCP ACK - Transaction ID 0x2699661d

Using a Pre-Captured DHCP Trace File:

dhcp-wireshark-trace1-1.pcapng

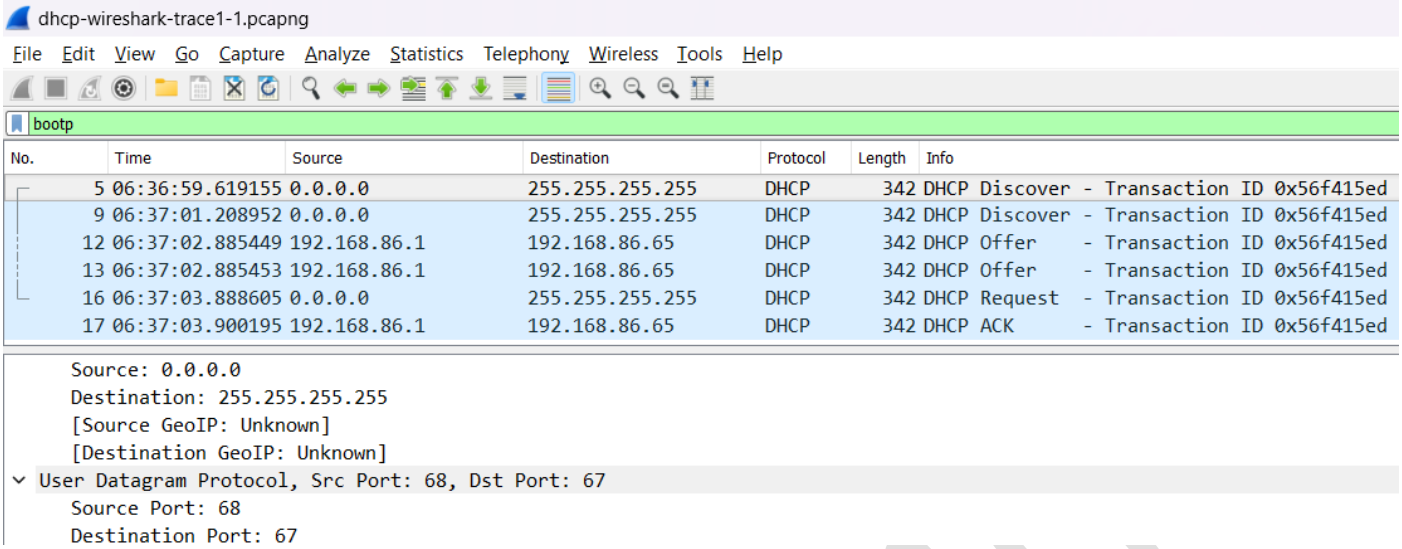
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
5	06:36:59.619155	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
9	06:37:01.208952	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
12	06:37:02.885449	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
13	06:37:02.885453	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
16	06:37:03.888605	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x56f415ed
17	06:37:03.900195	192.168.86.1	192.168.86.65	DHCP	342	DHCP ACK - Transaction ID 0x56f415ed

DHCP Questions:

Let's start by looking at the DHCP Discover message. Locate the IP datagram containing the first Discover message in your trace.



1. **Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?**

   Underlying transport protocol: UDP

2. **What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.**

   Source IP: 0.0.0.0

   This is a special address used by the client because it does not yet have an IP address assigned; hence it sends the message from 0.0.0.0, which represents "this host" on the network.

3. **What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.**

   Destination IP: 255.255.255.255

   This the broadcast address. This allows the DHCP Discover message to reach all devices in the network, including the DHCP server.

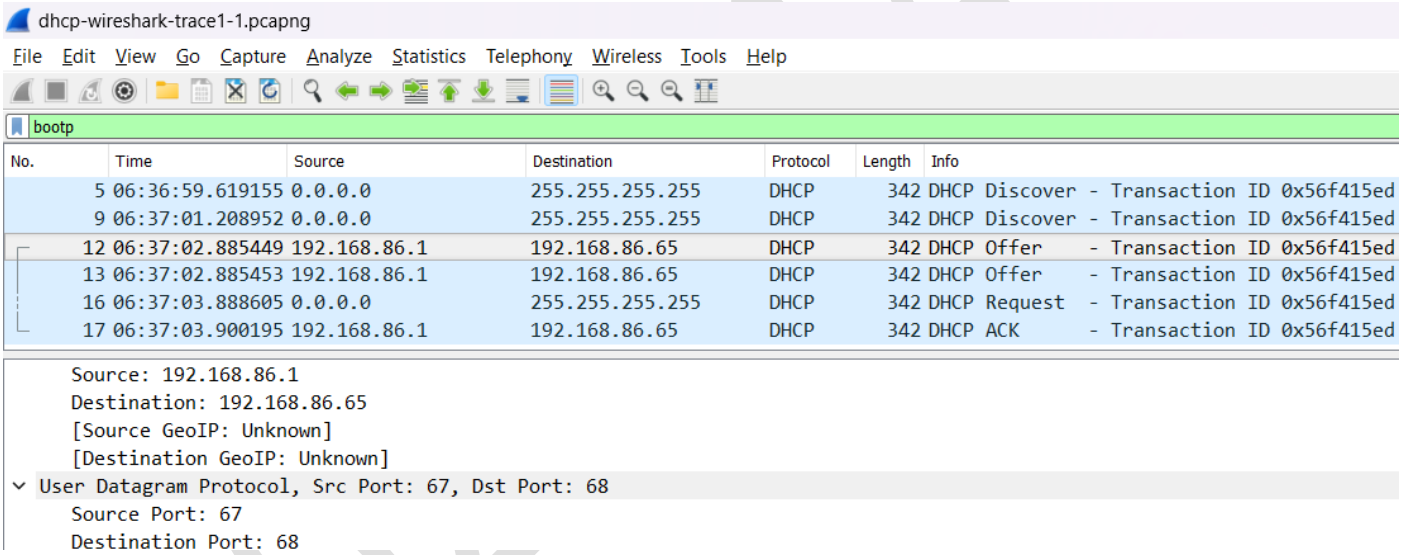
4. **What is the value in the transaction ID field of this DHCP Discover message?**

   Transaction ID: 0x56f415ed

5. **Now inspect the options field in the DHCP Discover message. What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?**

```
> Option: (53) DHCP Message Type (Discover)
> Option: (55) Parameter Request List
> Option: (57) Maximum DHCP Message Size
> Option: (61) Client identifier
> Option: (51) IP Address Lease Time
> Option: (12) Host Name
> Option: (255) End
```

Now let's look at the DHCP Offer message. Locate the IP datagram containing the DHCP Offer message in your trace that was sent by a DHCP server in the response to the DHCP Discover message that you studied in questions 1-5 above.



6. **What is the source IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain.**

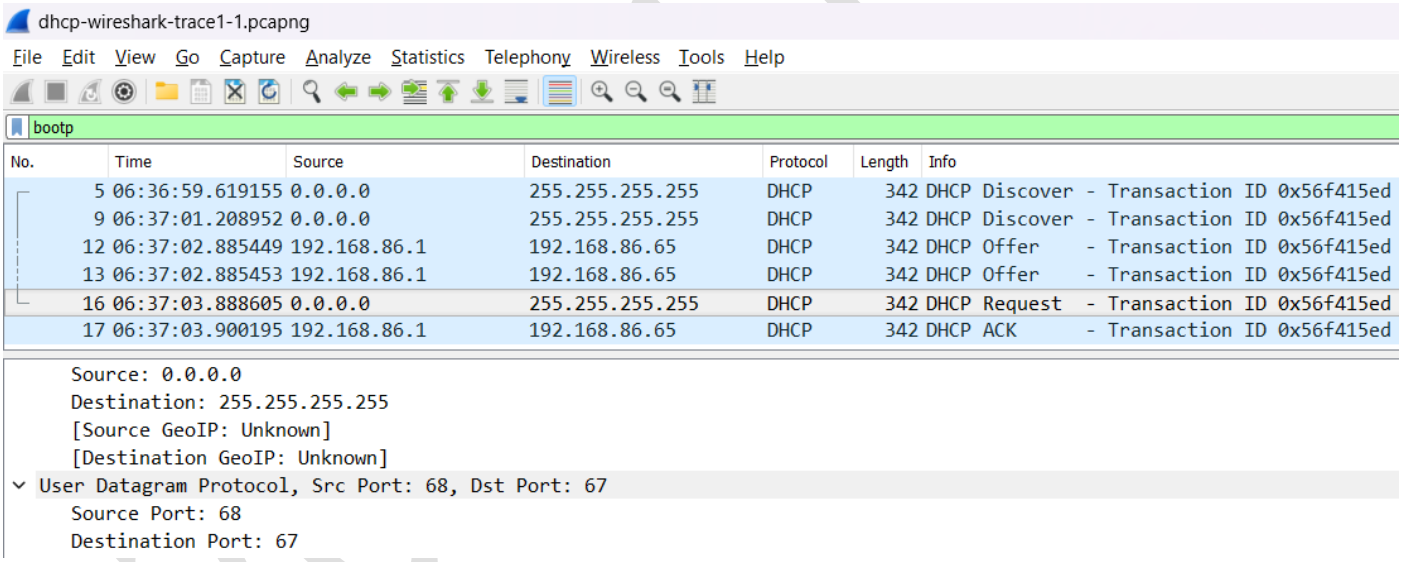
   Source IP: 192.168.86.1

   This address indicates which DHCP server is offering an IP address to the client.

7. **Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?**

```
> Option: (53) DHCP Message Type (Offer)
> Option: (54) DHCP Server Identifier
> Option: (51) IP Address Lease Time
> Option: (58) Renewal Time Value
> Option: (59) Rebinding Time Value
> Option: (1) Subnet Mask
> Option: (28) Broadcast Address
> Option: (3) Router
> Option: (15) Domain Name
> Option: (6) Domain Name Server
> Option: (255) End
```

Locate the IP datagram containing the first DHCP Request message in your trace, and answer the following questions.



8. **What is the destination IP address used in the datagram containing this Request message. Is there anything special about this address? Explain.**

   Destination IP: 255.255.255.255

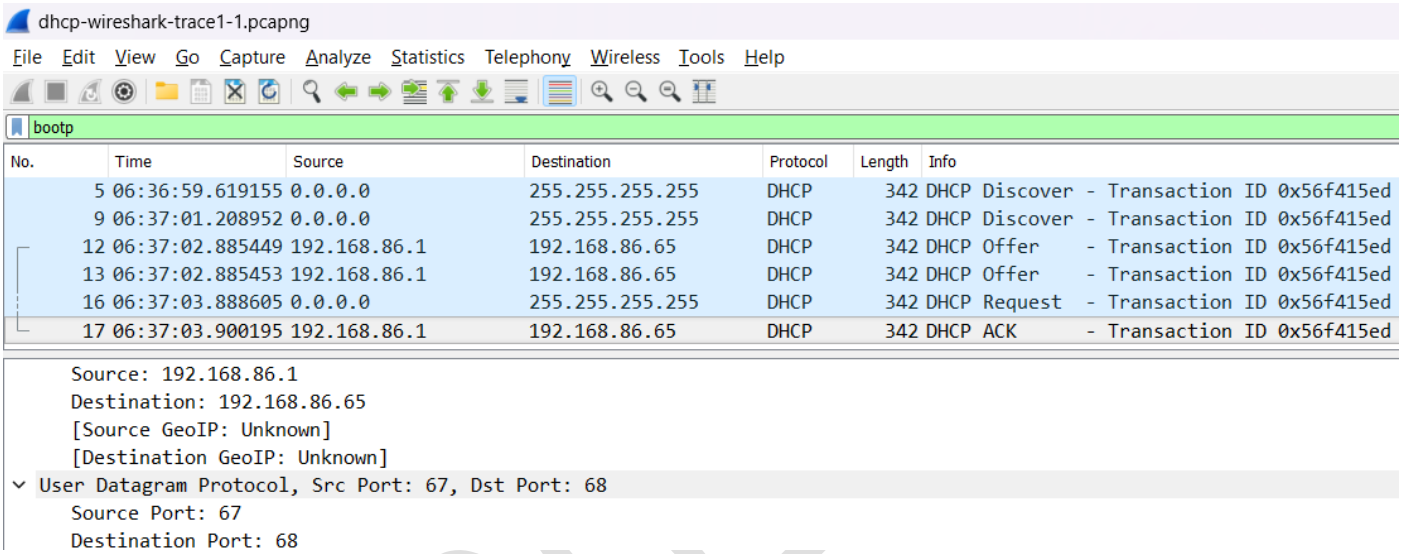
   This address shows that the client is now directly communicating with the server that sent the Offer, requesting the configuration it provided.

9. **What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?**

Transaction ID: 0x56f415ed

Yes, it matches the transaction ID of the earlier Discover and Offer messages.

Locate the IP datagram containing the first DHCP ACK message in your trace, and answer the following questions.



10. What is the source and destination IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.

Source IP: 192.168.86.1

Destination IP: 192.168.86.65

This confirms the client has been successfully assigned an IP address and can now communicate directly using its new address.

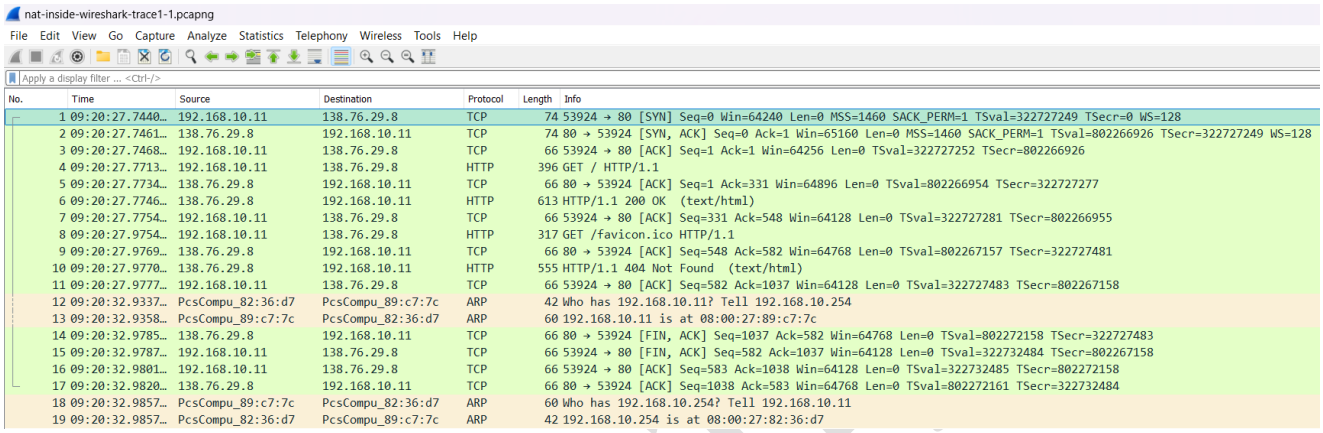
11. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?

```
Option: (3) Router
    Length: 4
    Router: 192.168.86.1
```

Section 2: Investigating NAT Behaviour

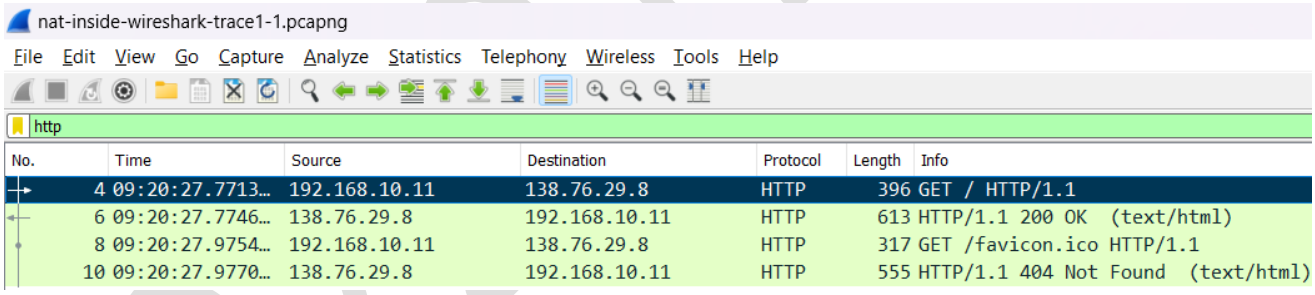
1. LAN Side Analysis:

- **Open nat-inside-wireshark-trace1-1.pcapng in Wireshark.**



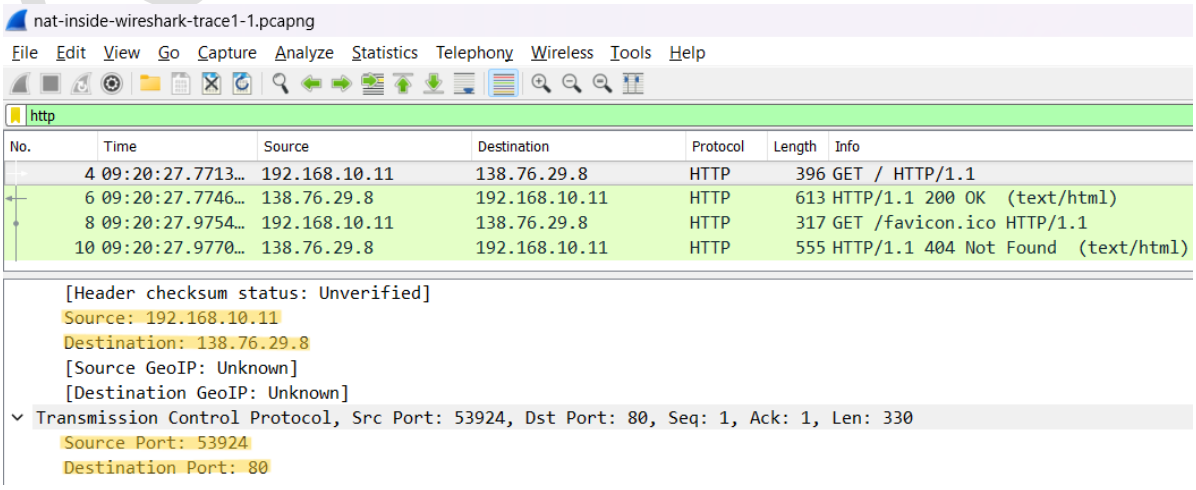
No.	Time	Source	Destination	Protocol	Length	Info
1	09:20:27.7440…	192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=322727249 TSecr=0 WS=128
2	09:20:27.7461…	138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=802266926 TSecr=322727249 WS=128
3	09:20:27.7468…	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	09:20:27.7713…	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	09:20:27.7734…	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	09:20:27.7746…	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
7	09:20:27.7754…	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	09:20:27.9754…	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	09:20:27.9769…	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	09:20:27.9770…	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	09:20:27.9777…	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12	09:20:32.9337…	PcsCompu_82:36:d7	PcsCompu_89:c7:7c	ARP	42	Who has 192.168.10.11? Tell 192.168.10.254
13	09:20:32.9358…	PcsCompu_89:c7:7c	PcsCompu_82:36:d7	ARP	60	192.168.10.11 is at 08:00:27:89:c7:7c
14	09:20:32.9785…	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
15	09:20:32.9787…	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
16	09:20:32.9801…	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
17	09:20:32.9820…	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484
18	09:20:32.9857…	PcsCompu_89:c7:7c	PcsCompu_82:36:d7	ARP	60	Who has 192.168.10.254? Tell 192.168.10.11
19	09:20:32.9857…	PcsCompu_82:36:d7	PcsCompu_89:c7:7c	ARP	42	192.168.10.254 is at 08:00:27:82:36:d7

- **Locate the HTTP GET request addressed to the web server at IP address 138.76.29.8.**



No.	Time	Source	Destination	Protocol	Length	Info
4	09:20:27.7713…	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	09:20:27.7746…	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	09:20:27.9754…	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	09:20:27.9770…	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

- **Examine the following details:**
  - **Client's IP address (private IP) and the source port of the HTTP GET request**



No.	Time	Source	Destination	Protocol	Length	Info
4	09:20:27.7713…	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	09:20:27.7746…	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
8	09:20:27.9754…	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	09:20:27.9770…	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)

Source (Client) IP: 192.168.10.11

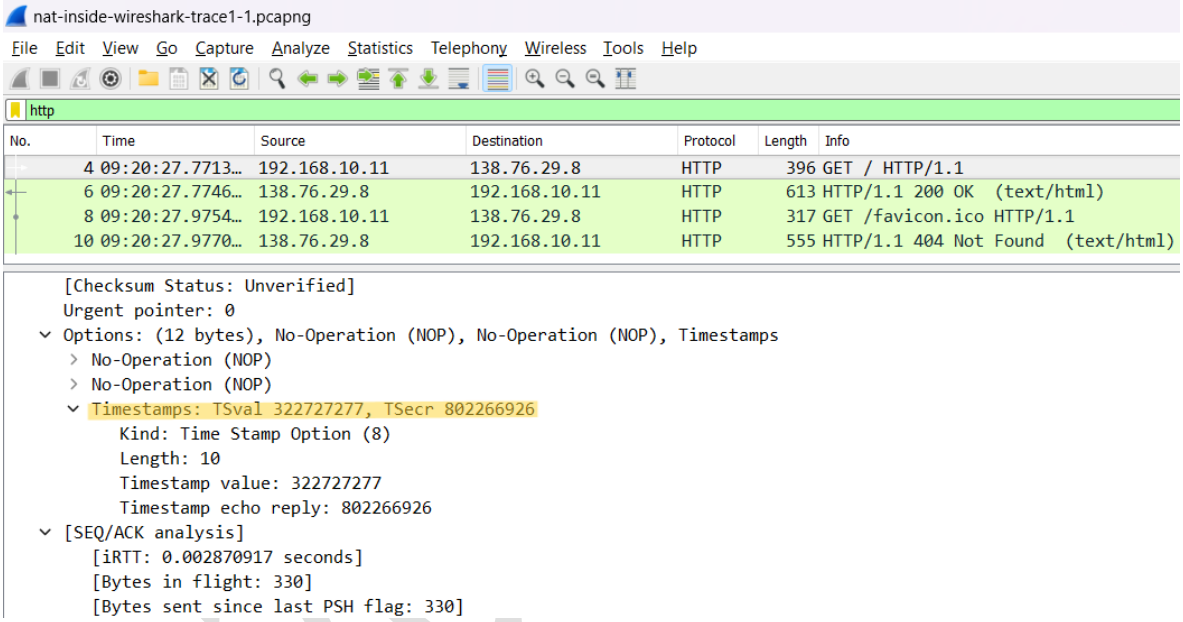
Source Port: 53924

- **The destination IP address (server) and the destination port in the TCP segment.**

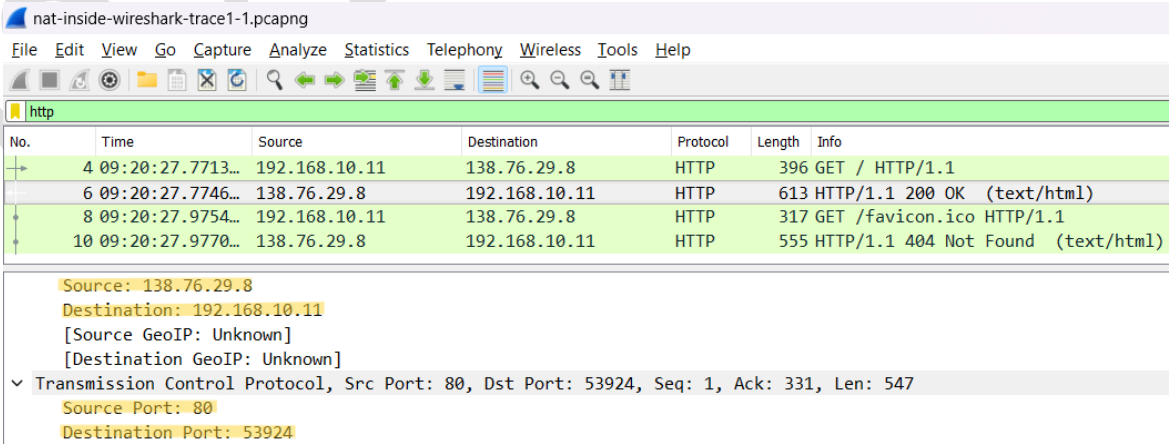
Destination IP: 138.76.29.8

Destination Port: 80

- **The timestamp of the HTTP GET request.**



- **Now, look for the HTTP response from the server (200 OK). Identify:**
  - **The source IP and port (the server's information).**



Source IP: 138.76.29.8

Source Port: 80

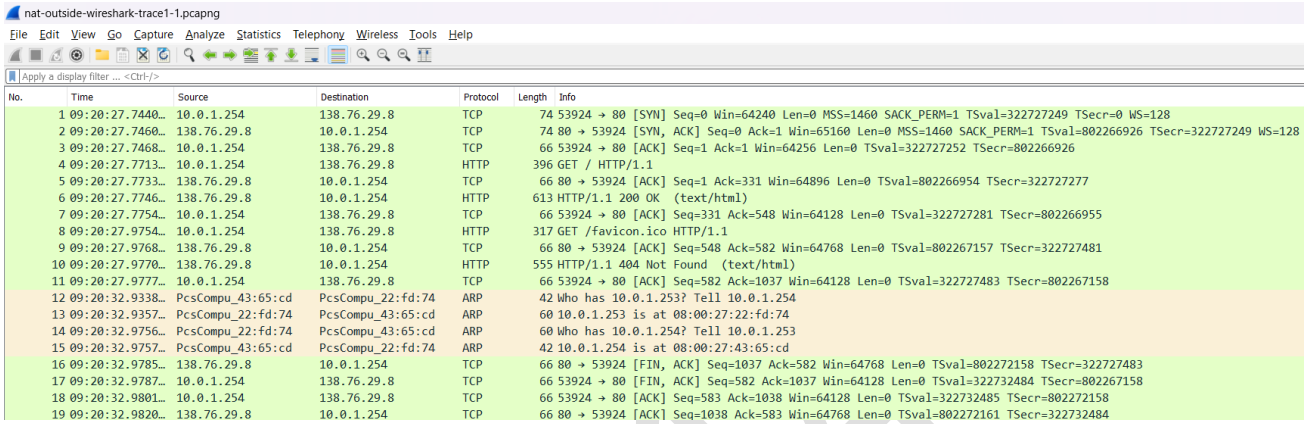
- **The destination IP and port (the client's details).**

Destination IP: 192.168.10.11

Destination Port: 53924

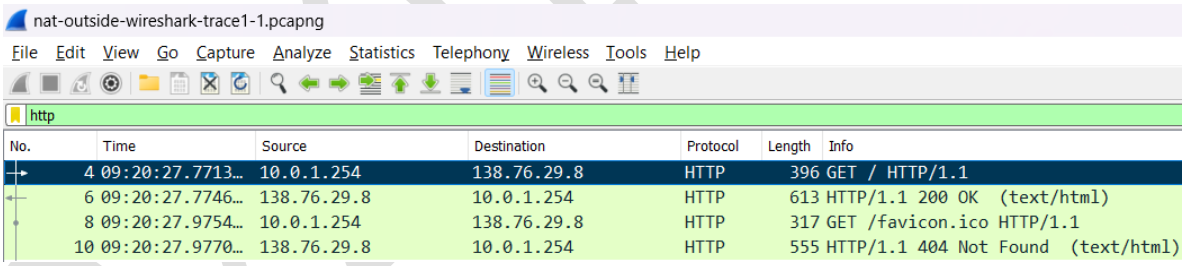
2. WAN Side (Internet) Analysis:

- **Open nat-outside-wireshark-trace1-1.pcapng in Wireshark.**



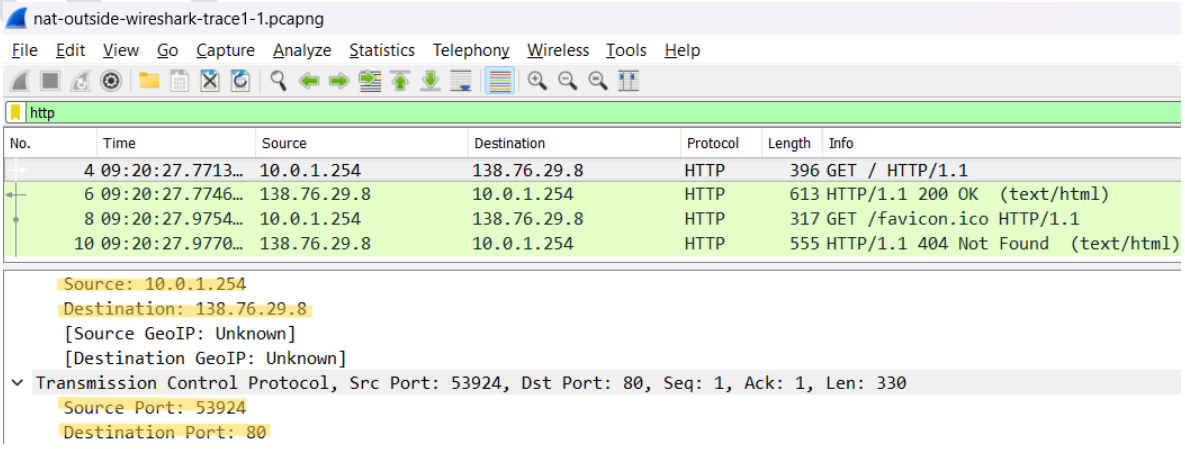
No.	Time	Source	Destination	Protocol	Length	Info
1	09:20:27.7440…	10.0.1.254	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=322727249 TSecr=0 WS=128
2	09:20:27.7460…	138.76.29.8	10.0.1.254	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=802266926 TSecr=322727249 WS=128
3	09:20:27.7468…	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	09:20:27.7713…	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	09:20:27.7733…	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	09:20:27.7746…	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	09:20:27.7754…	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	09:20:27.9754…	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	09:20:27.9768…	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	09:20:27.9770…	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	09:20:27.9777…	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12	09:20:32.9338…	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	09:20:32.9357…	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	10.0.1.253 is at 08:00:27:22:fd:74
14	09:20:32.9756…	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254? Tell 10.0.1.253
15	09:20:32.9757…	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:00:27:43:65:cd
16	09:20:32.9785…	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
17	09:20:32.9787…	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
18	09:20:32.9801…	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
19	09:20:32.9820…	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484

- **Find the HTTP GET request corresponding to the same request seen in the LAN-side capture. Pay attention to:**
  - **The time when the HTTP GET message appears in this trace.**



No.	Time	Source	Destination	Protocol	Length	Info
4	09:20:27.7713…	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
6	09:20:27.7746…	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
8	09:20:27.9754…	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
10	09:20:27.9770…	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)

  - **The changes in the IP addresses and port numbers as a result of NAT translation.**



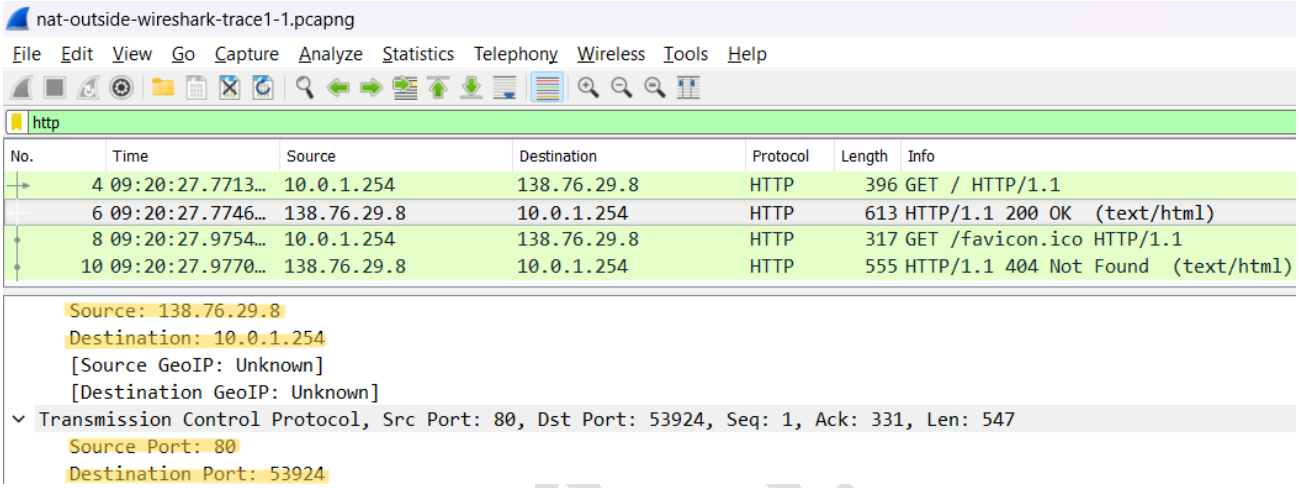
Source IP: 10.0.1.254

Destination IP: 138.76.29.8

Source Port: 53924

Destination Port: 80

- **Next, locate the HTTP response (200 OK) from the web server. Compare the source and destination IP addresses and port numbers in this response with those seen on the LAN side.**



Source IP: 138.76.29.8

Destination IP: 10.0.1.254

Source Port: 80

Destination Port: 53924

3. Compare and Analyze:

- **Compare the LAN-side and WAN-side captures for both the HTTP GET and HTTP 200 OK messages.**

<u>LAN-Side Capture:</u>

- Source (Client) IP: 192.168.10.11 (Private IP)
- Source Port: 53924
- Destination IP: 138.76.29.8 (Server Public IP)
- Destination Port: 80 (HTTP port)

<u>WAN-Side Capture (after NAT translation):</u>

- Source (Translated) IP: 10.0.1.254 (Public IP assigned by NAT)
- Source Port: 53924 (Unchanged)

- Destination IP: 138.76.29.8 (Same server Public IP)

- Destination Port: 80 (Same HTTP port)

- **Identify the differences in:**
  - **IP addresses (private vs public).**
  - **Port numbers (before and after NAT translation).**

  Differences:

  - IP Addresses: The client's private IP (192.168.10.11) is translated into a public IP (10.0.1.254) by NAT before the HTTP GET request is sent to the web server.

  - Port Numbers: The source port remains unchanged (53924) across both the LAN and WAN sides, as NAT only changes the IP address, not the port number, in this case.

- **Understand how NAT modifies these fields to facilitate communication between devices inside the LAN and external servers on the Internet.**

  NAT modifies the source IP address of outgoing packets from a private LAN IP to a public WAN IP, enabling devices on the private network to communicate with external servers on the Internet. The reverse happens for incoming responses, where the public IP is translated back to the private IP, ensuring the correct device inside the LAN receives the response.

NAT Questions:

12. **What is the source IP address and source port number of the HTTP GET request in the nat-inside-wireshark-trace1-1.pcapng trace?**

    Source IP: 192.168.10.11 (Client's Private IP)

    Source Port: 53924

13. **What are the source and destination IP addresses and port numbers of the HTTP GET request after NAT translation in the nat-outside-wireshark-trace1-1.pcapng file?**

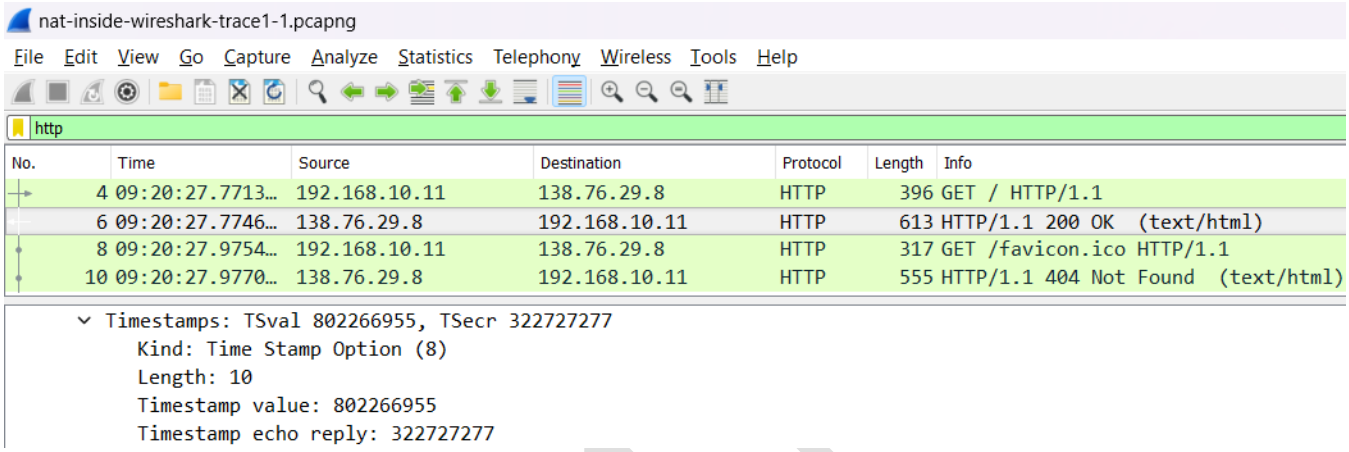
    Source IP: 10.0.1.254 (Public IP assigned by NAT)

Source Port: 53924

Destination IP: 138.76.29.8 (Web server's Public IP)

Destination Port: 80

14. What time does the HTTP 200 OK response from the web server appear in the nat-inside-wireshark-trace1-1.pcapng trace?



15. How does NAT modify the IP address and port numbers when forwarding the HTTP response from the WAN side back to the client on the LAN side?

NAT changes the destination IP address from the public IP (10.0.1.254) to the client's private IP (192.168.10.11). The port number remains the same.

16. What fields in the IP datagram are altered by NAT during translation when forwarding HTTP messages between the LAN and WAN?

NAT modifies the source IP address (for outgoing messages from the LAN) and the destination IP address (for incoming messages from the WAN). It also may change source ports in certain configurations, although in this trace, the port number remains the same.