

AM.SC.U4CSE23042

Jithin Jyothi

1.

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays the details of the selected packet (No. 137), which is an HTTP GET request for `/wireshark-labs/HTTP-wireshark-file1.html`. The request includes headers such as `Host: gaia.cs.umass.edu`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36`, and `Accept-Encoding: gzip, deflate`. The bottom pane shows the packet list with two entries: a GET request (No. 118) and an HTTP 304 Not Modified response (No. 137).

No.	Time	Source	Destination	Protocol	Length	Info
118	3.657758	192.168.205.55	128.119.245.12	HTTP	651	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
137	3.928558	128.119.245.12	192.168.205.55	HTTP	293	HTTP/1.1 304 Not Modified

2.

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays the details of the selected packet (No. 137), which is an HTTP GET request for `/wireshark-labs/HTTP-wireshark-file1.html`. The request includes headers such as `Host: gaia.cs.umass.edu`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36`, and `Accept-Encoding: gzip, deflate`. The bottom pane shows the packet list with two entries: a GET request (No. 118) and an HTTP 304 Not Modified response (No. 137).

No.	Time	Source	Destination	Protocol	Length	Info
118	3.657758	192.168.205.55	128.119.245.12	HTTP	651	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
137	3.928558	128.119.245.12	192.168.205.55	HTTP	293	HTTP/1.1 304 Not Modified

3.

IP Address of my computer : 192.168.205.55

IP Address of gaia.cs.umass.edu : 128.119.245.12

```

▶ Frame 118: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Device
▶ Ethernet II, Src: HP_72:ff:51 (64:4e:d7:72:ff:51), Dst: Fortinet_09:00:22 (00:09:0f:09:00:22)
▶ Internet Protocol Version 4, Src: 192.168.205.55, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 51626, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
▼ Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n

```

4.

911	24.567099	192.168.205.55	128.119.245.12	HTTP	651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
914	24.830060	128.119.245.12	192.168.205.55	HTTP	293 HTTP/1.1 304 Not Modified

233	4.778556	192.168.205.55	128.119.245.12	HTTP	651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
258	5.382737	128.119.245.12	192.168.205.55	HTTP	540 HTTP/1.1 200 OK (text/html)
585	8.764266	192.168.205.55	49.44.177.171	HTTP	165 GET /connecttest.txt HTTP/1.1
592	8.802016	49.44.177.171	192.168.205.55	HTTP	241 HTTP/1.1 200 OK (text/plain)

304 Not Modified - is the status code that I received.

200 OK – was used to get the last-modified.

5.

```

▼ Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Tue, 02 Sep 2025 05:04:35 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 02 Sep 2025 05:04:02 GMT\r\n
    ETag: "80-63dca6aa606b3"\r\n
    Accept-Ranges: bytes\r\n

```

6.

651 Bytes

```

▶ Frame 233: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Device\NPF_{81C20AA4-AAC2-4898-92E9-2E9E105B0EDA}, id 0
▶ Ethernet II, Src: HP_72:ff:51 (64:4e:d7:72:ff:51), Dst: Fortinet_09:00:22 (00:09:0f:09:00:22)
▶ Internet Protocol Version 4, Src: 192.168.205.55, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 53797, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
▼ Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36 Edg/139.0.0.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n

```

7.

```

▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36 Edg/139.0.0.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "80-63db7117b380a"\r\n
    If-Modified-Since: Mon, 01 Sep 2025 05:59:01 GMT\r\n
  \r\n
  [Response in frame: 258]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

```

8.

233	4.778556	192.168.205.55	128.119.245.12	HTTP	651	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
258	5.382737	128.119.245.12	192.168.205.55	HTTP	540	HTTP/1.1 200 OK (text/html)
585	8.764266	192.168.205.55	49.44.177.171	HTTP	165	GET /connecttest.txt HTTP/1.1
592	8.802016	49.44.177.171	192.168.205.55	HTTP	241	HTTP/1.1 200 OK (text/plain)

```

> Frame 258: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{81C20AA4-AAC2-4898-92E9-2E9E105B0EDA}, id 0
> Ethernet II, Src: Fortinet_09:00:22 (00:09:0f:09:00:22), Dst: HP_72:ff:51 (64:4e:d7:72:ff:51)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.205.55
> Transmission Control Protocol, Src Port: 80, Dst Port: 53797, Seq: 1, Ack: 598, Len: 486
> Hypertext Transfer Protocol
▼ Line-based text data: text/html (4 lines)
  <html>\n
  Congratulations. You've downloaded the file \n
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\n
  </html>\n

```

Yes, the server returned the contents of the file, which can be seen in text/html

9.

```

▼ Hypertext Transfer Protocol
  > GET /connecttest.txt HTTP/1.1\r\n
    Connection: Close\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: www.msftconnecttest.com\r\n
  \r\n
  [Response in frame: 592]
  [Full request URI: http://www.msftconnecttest.com/connecttest.txt]

```

There is no If-Modified-Since visible here. The file was not modified.

10.

The HTTP status code seen here is 200 OK . The server returned text/plain and it contains Microsoft Connect Test

233	4.778556	192.168.205.55	128.119.245.12	HTTP	651 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
258	5.382737	128.119.245.12	192.168.205.55	HTTP	540 HTTP/1.1 200 OK (text/html)
585	8.764266	192.168.205.55	49.44.177.171	HTTP	165 GET /connecttest.txt HTTP/1.1
592	8.802016	49.44.177.171	192.168.205.55	HTTP	241 HTTP/1.1 200 OK (text/plain)

```
> Frame 592: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{81C20AA4-AAC2-4898-92E9-2E9E105B0EDA}, id 0
> Ethernet II, Src: Fortinet_09:00:22 (00:09:0f:09:00:22), Dst: HP_72:ff:51 (64:4e:d7:72:ff:51)
> Internet Protocol Version 4, Src: 49.44.177.171, Dst: 192.168.205.55
> Transmission Control Protocol, Src Port: 80, Dst Port: 53806, Seq: 1, Ack: 112, Len: 187
> Hypertext Transfer Protocol
▼ Line-based text data: text/plain (1 lines)
    Microsoft Connect Test
```

11.

DNS are transmitted over UDP (User Datagram Protocol)

```
▶ Frame 224: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{81C20AA4-AAC2-4898-92E9-2E9E105B0EDA}, id 0
▶ Ethernet II, Src: HP_72:ff:51 (64:4e:d7:72:ff:51), Dst: Fortinet_09:00:22 (00:09:0f:09:00:22)
▶ Internet Protocol Version 4, Src: 192.168.205.55, Dst: 192.168.0.251
▶ User Datagram Protocol, Src Port: 60297, Dst Port: 53
▶ Domain Name System (query)
```

DNS Query

223	4.772169	192.168.205.55	192.168.0.251	DNS	77 Standard query 0x1a35 A gaia.cs.umass.edu
224	4.772518	192.168.205.55	192.168.0.251	DNS	77 Standard query 0x3625 HTTPS gaia.cs.umass.edu

DNS Response

225	4.772831	192.168.0.251	192.168.205.55	DNS	93 Standard query response 0x1a35 A gaia.cs.umass.edu A 128.119.245.12
226	4.773027	192.168.0.251	192.168.205.55	DNS	130 Standard query response 0x3625 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu

12.

Destination : 192.168.0.251 and Source : 192.168.205.55

90	2.822873	192.168.205.55	192.168.0.251	DNS	81 Standard query 0x9d86 HTTPS teams.cloud.microsoft
91	2.823524	192.168.0.251	192.168.205.55	DNS	215 Standard query response 0x9d86 HTTPS teams.cloud.microsoft CNVPE teams-cloud-microsoft-s-0005.dual-s-msedge.net CNVPE s-0005.dual-s-msedge.net SOA ns1.dual-s-msedge.net
92	2.823524	192.168.0.251	192.168.205.55	DNS	187 Standard query response 0x8092 A teams.cloud.microsoft CNVPE teams-cloud-microsoft-s-0005.dual-s-msedge.net CNVPE s-0005.dual-s-msedge.net A 52.123.129.14 A 52.123.128.14
94	2.825516	192.168.0.251	192.168.205.55	DNS	113 Standard query response 0x9d86 A 00080134025800909.ingest.us.sentry.io A 34.120.195.249
223	4.772169	192.168.205.55	192.168.0.251	DNS	77 Standard query 0x1a35 A gaia.cs.umass.edu
224	4.772518	192.168.205.55	192.168.0.251	DNS	77 Standard query 0x3625 HTTPS gaia.cs.umass.edu
225	4.772831	192.168.0.251	192.168.205.55	DNS	93 Standard query response 0x1a35 A gaia.cs.umass.edu A 128.119.245.12
226	4.773027	192.168.0.251	192.168.205.55	DNS	130 Standard query response 0x3625 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu
230	4.777040	192.168.205.55	192.168.0.251	DNS	77 Standard query 0xc678 A gaia.cs.umass.edu
231	4.777592	192.168.0.251	192.168.205.55	DNS	93 Standard query response 0xc678 A gaia.cs.umass.edu A 128.119.245.12
237	4.793296	192.168.205.55	192.168.0.251	DNS	96 Standard query 0x648d A functional.events.data.microsoft.com

13.

223	4.772169	192.168.205.55	192.168.0.251	DNS	77 Standard query 0x1a35 A gaia.cs.umass.edu
-----	----------	----------------	---------------	-----	--

The DNS query message is sent from 192.168.205.55 to 192.168.0.251

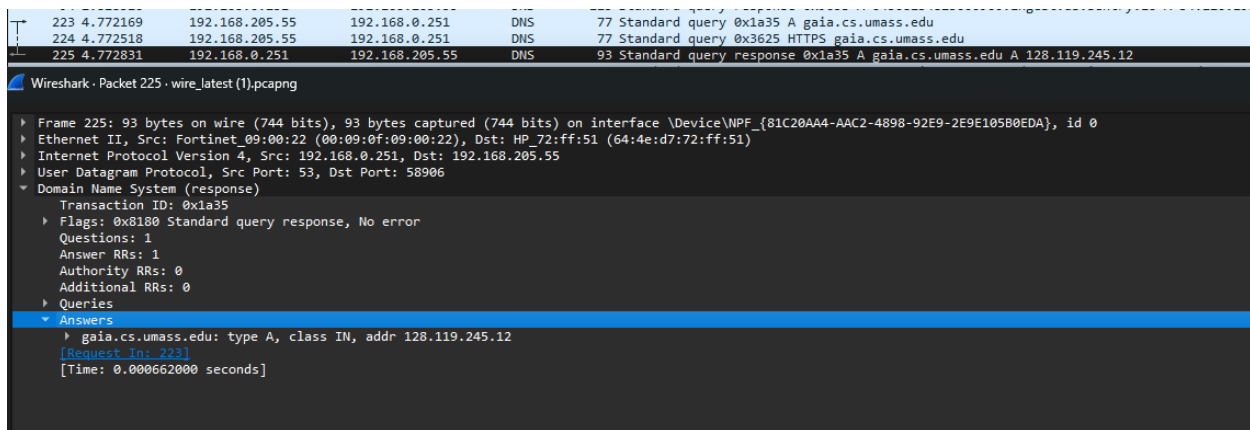
```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : am.amrita.edu
Description . . . . . : Intel(R) Ethernet Connection (17) I219-LM
Physical Address. . . . . : 64-4E-D7-72-FF-51
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . : fe80::bef:e579:e81d:d969%10(Preferred)
IPv4 Address. . . . . : 192.168.205.55(Preferred)
Subnet Mask . . . . . : 255.255.252.0
Lease Obtained. . . . . : 08 September 2025 14:15:16
Lease Expires . . . . . : 10 September 2025 08:47:01
Default Gateway . . . . . : 192.168.207.254
DHCP Server . . . . . : 192.168.0.251
DHCPv6 IAID . . . . . : 107237079
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-29-CA-EC-64-4E-D7-72-FF-51
DNS Servers . . . . . : 192.168.0.251
                        192.168.0.250
Primary WINS Server . . . . . : 192.168.0.250
NetBIOS over Tcpip. . . . . : Enabled
```

DNS Servers : 192.168.0.251 and 192.168.0.250

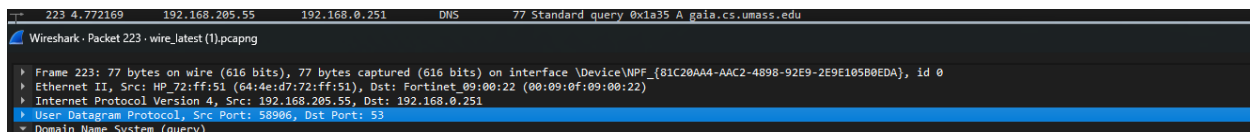
Yes they are the same.

14.

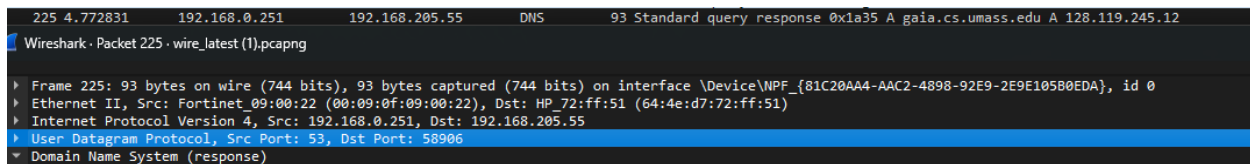


1 answer is provided. The answer contains the type, class, address. The type is A.

15.



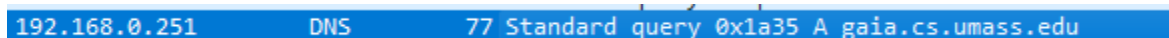
The destination port is 53.



Source port is: 53

16.

DNS query msg is sent to 192.168.0.251



Yes, this is the ip of one of the dns servers.



17.

223	4.772169	192.168.205.55	192.168.0.251	DNS	77 Standard query 0x1a35 A gaia.cs.umass.edu
224	4.772518	192.168.205.55	192.168.0.251	DNS	77 Standard query 0x3625 HTTPS gaia.cs.umass.edu
225	4.772831	192.168.0.251	192.168.205.55	DNS	93 Standard query response 0x1a35 A gaia.cs.umass.edu A 128.119.245.12
226	4.773037	192.168.0.251	192.168.205.55	DNS	130 Standard query response 0x3625 HTTPS gaia.cs.umass.edu 604 unix1.cs.um

Before getting the response of 0x1a35, the query of 0x3625 (highlighted) was sent.

18.

234	4.778710	128.119.245.12	192.168.205.55	TCP	66 80 → 53798 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=256
235	4.778742	192.168.205.55	128.119.245.12	TCP	54 53798 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
236	4.778828	128.119.245.12	192.168.205.55	TCP	60 80 → 53797 [ACK] Seq=1 Ack=598 Win=15872 Len=0
241	4.850334	192.168.205.55	128.119.245.12	TCP	66 53798 → 443 [FIN] Seq=0 Win=65536 Len=0 MSS=1460 WS=256 SACK_PERM