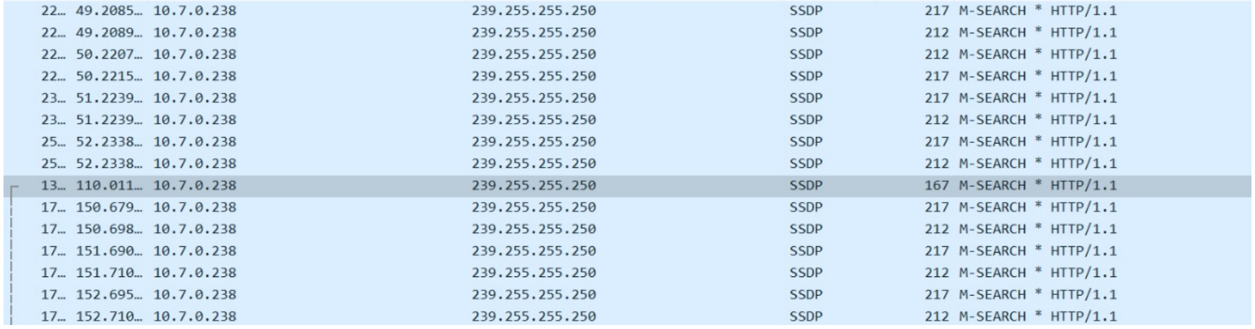
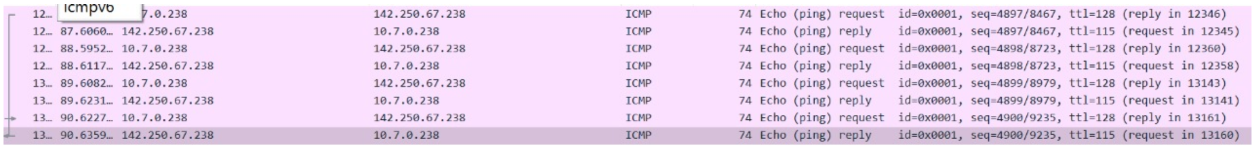
Q.4>
Q.1> Part-a>
SSDP allows devices such as printers, modems, and surveillance cameras to be discovered on a network quickly and easily. It does this by broadcasting a message to the network, which other devices can respond to.
The RFC for SSDP is RFC 2660. It is titled "Simple Service Discovery Protocol."



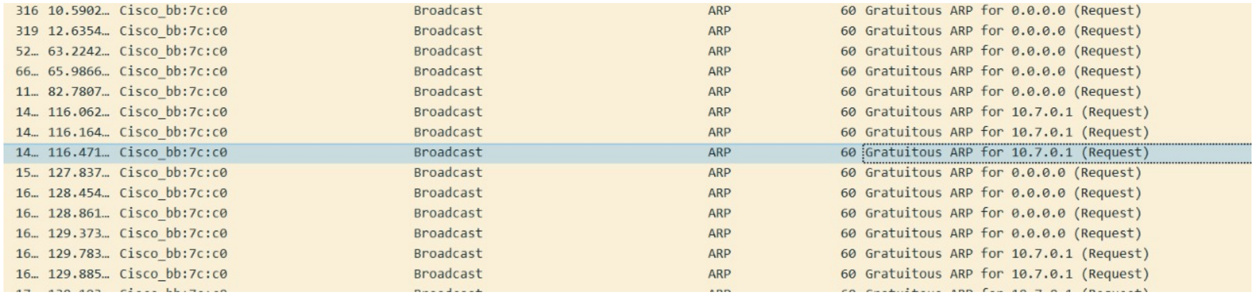
```
22… 49.2085… 10.7.0.238      239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
22… 49.2089… 10.7.0.238      239.255.255.250      SSDP      212 M-SEARCH * HTTP/1.1
22… 50.2207… 10.7.0.238      239.255.255.250      SSDP      212 M-SEARCH * HTTP/1.1
22… 50.2215… 10.7.0.238      239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
23… 51.2239… 10.7.0.238      239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
23… 51.2239… 10.7.0.238      239.255.255.250      SSDP      212 M-SEARCH * HTTP/1.1
25… 52.2338… 10.7.0.238      239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
25… 52.2338… 10.7.0.238      239.255.255.250      SSDP      212 M-SEARCH * HTTP/1.1
13… 110.011… 10.7.0.238      239.255.255.250      SSDP      167 M-SEARCH * HTTP/1.1
17… 150.679… 10.7.0.238      239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
17… 150.698… 10.7.0.238      239.255.255.250      SSDP      212 M-SEARCH * HTTP/1.1
17… 151.690… 10.7.0.238      239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
17… 151.710… 10.7.0.238      239.255.255.250      SSDP      212 M-SEARCH * HTTP/1.1
17… 152.695… 10.7.0.238      239.255.255.250      SSDP      217 M-SEARCH * HTTP/1.1
17… 152.710… 10.7.0.238      239.255.255.250      SSDP      212 M-SEARCH * HTTP/1.1
```

ICMP stands for Internet Control Message Protocol. It is a network protocol IP hosts and routers use to send error messages and status information.
The RFC for ICMP is RFC 792. It is titled "Internet Control Message Protocol."



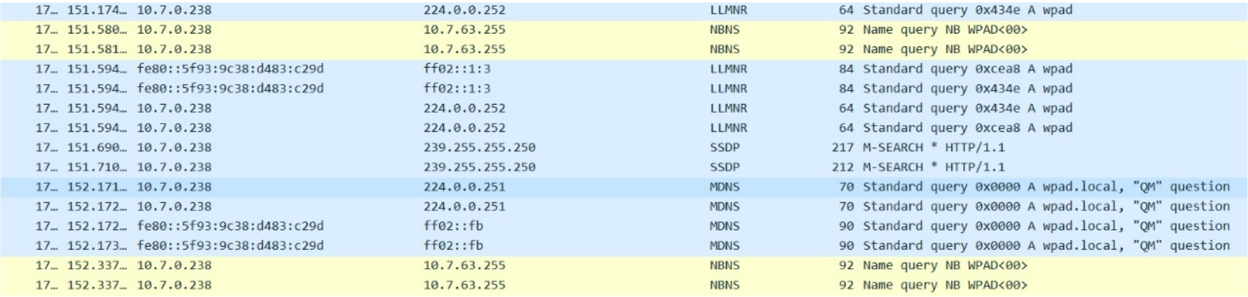
```
12… icmpv6 7.0.238          142.250.67.238   ICMP   74 Echo (ping) request  id=0x0001, seq=4897/8467, ttl=128 (reply in 12346)
12… 87.6060… 142.250.67.238  10.7.0.238       ICMP   74 Echo (ping) reply    id=0x0001, seq=4897/8467, ttl=115 (request in 12345)
12… 88.5952… 10.7.0.238      142.250.67.238   ICMP   74 Echo (ping) request  id=0x0001, seq=4898/8723, ttl=128 (reply in 12360)
12… 88.6117… 142.250.67.238  10.7.0.238       ICMP   74 Echo (ping) reply    id=0x0001, seq=4898/8723, ttl=115 (request in 12358)
13… 89.6082… 10.7.0.238      142.250.67.238   ICMP   74 Echo (ping) request  id=0x0001, seq=4899/8979, ttl=128 (reply in 13143)
13… 89.6231… 142.250.67.238  10.7.0.238       ICMP   74 Echo (ping) reply    id=0x0001, seq=4899/8979, ttl=115 (request in 13141)
13… 90.6227… 10.7.0.238      142.250.67.238   ICMP   74 Echo (ping) request  id=0x0001, seq=4900/9235, ttl=128 (reply in 13161)
13… 90.6359… 142.250.67.238  10.7.0.238       ICMP   74 Echo (ping) reply    id=0x0001, seq=4900/9235, ttl=115 (request in 13160)
```

The Address Resolution Protocol (**ARP**) is a network protocol that maps IP addresses to MAC addresses. It is used in local area networks (LANs) to determine the physical address of a device based on its IP address.
RFC 826



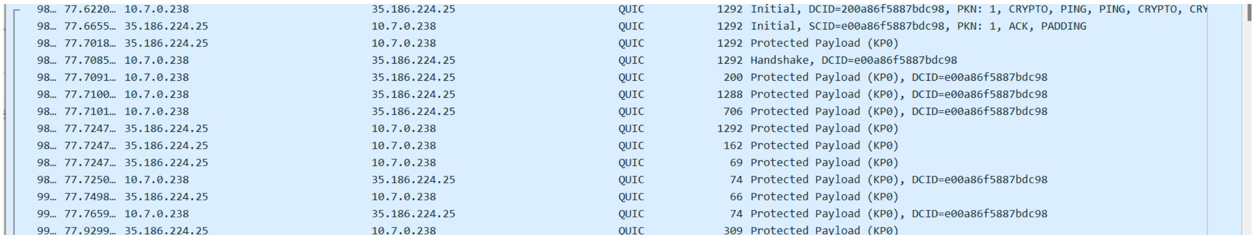
```
316 10.5902… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
319 12.6354… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
52… 63.2242… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
66… 65.9866… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
11… 82.7807… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
14… 116.062… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 10.7.0.1 (Request)
14… 116.164… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 10.7.0.1 (Request)
14… 116.471… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 10.7.0.1 (Request)
15… 127.837… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
16… 128.454… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
16… 128.861… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
16… 129.373… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 0.0.0.0 (Request)
16… 129.783… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 10.7.0.1 (Request)
16… 129.885… Cisco_bb:7c:c0     Broadcast     ARP     60 Gratuitous ARP for 10.7.0.1 (Request)
```

NBNS is a broadcast protocol, which means that it sends messages to all devices on the network.
RFC 1001



```
17… 151.174… 10.7.0.238                  224.0.0.252        LLMNR    64 Standard query 0x434e A wpad
17… 151.580… 10.7.0.238                  10.7.63.255        NBNS     92 Name query NB WPAD<00>
17… 151.581… 10.7.0.238                  10.7.63.255        NBNS     92 Name query NB WPAD<00>
17… 151.594… fe80::5f93:9c38:d483:c29d   ff02::1:3          LLMNR    84 Standard query 0xcea8 A wpad
17… 151.594… fe80::5f93:9c38:d483:c29d   ff02::1:3          LLMNR    84 Standard query 0x434e A wpad
17… 151.594… 10.7.0.238                  224.0.0.252        LLMNR    64 Standard query 0x434e A wpad
17… 151.594… 10.7.0.238                  224.0.0.252        LLMNR    64 Standard query 0xcea8 A wpad
17… 151.690… 10.7.0.238                  239.255.255.250    SSDP    217 M-SEARCH * HTTP/1.1
17… 151.710… 10.7.0.238                  239.255.255.250    SSDP    212 M-SEARCH * HTTP/1.1
17… 152.171… 10.7.0.238                  224.0.0.251        MDNS     70 Standard query 0x0000 A wpad.local, "QM" question
17… 152.172… 10.7.0.238                  224.0.0.251        MDNS     70 Standard query 0x0000 A wpad.local, "QM" question
17… 152.172… fe80::5f93:9c38:d483:c29d   ff02::fb           MDNS     90 Standard query 0x0000 A wpad.local, "QM" question
17… 152.173… fe80::5f93:9c38:d483:c29d   ff02::fb           MDNS     90 Standard query 0x0000 A wpad.local, "QM" question
17… 152.337… 10.7.0.238                  10.7.63.255        NBNS     92 Name query NB WPAD<00>
17… 152.337… 10.7.0.238                  10.7.63.255        NBNS     92 Name query NB WPAD<00>
```

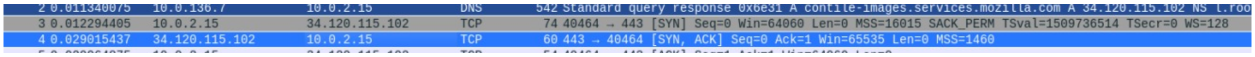
QUIC stands for Quick UDP Internet Connections. It is a new transport layer protocol designed to improve the performance of web browsing and other internet applications.
RFC 9000



```
98… 77.6220… 10.7.0.238      35.186.224.25   QUIC   1292 Initial, DCID=200a86f5887bdc98, PKN: 1, CRYPTO, PING, PING, CRYPTO, CRY
98… 77.6655… 35.186.224.25   10.7.0.238      QUIC   1292 Initial, SCID=e00a86f5887bdc98, PKN: 1, ACK, PADDING
98… 77.7018… 35.186.224.25   10.7.0.238      QUIC   1292 Protected Payload (KP0)
98… 77.7085… 10.7.0.238      35.186.224.25   QUIC   1292 Handshake, DCID=e00a86f5887bdc98
98… 77.7091… 10.7.0.238      35.186.224.25   QUIC    200 Protected Payload (KP0), DCID=e00a86f5887bdc98
98… 77.7100… 10.7.0.238      35.186.224.25   QUIC   1288 Protected Payload (KP0), DCID=e00a86f5887bdc98
98… 77.7101… 10.7.0.238      35.186.224.25   QUIC    706 Protected Payload (KP0), DCID=e00a86f5887bdc98
98… 77.7247… 35.186.224.25   10.7.0.238      QUIC   1292 Protected Payload (KP0)
98… 77.7247… 35.186.224.25   10.7.0.238      QUIC    162 Protected Payload (KP0)
98… 77.7247… 35.186.224.25   10.7.0.238      QUIC     69 Protected Payload (KP0)
98… 77.7250… 10.7.0.238      35.186.224.25   QUIC     74 Protected Payload (KP0), DCID=e00a86f5887bdc98
99… 77.7498… 35.186.224.25   10.7.0.238      QUIC     66 Protected Payload (KP0)
99… 77.7659… 10.7.0.238      35.186.224.25   QUIC     74 Protected Payload (KP0), DCID=e00a86f5887bdc98
99… 77.9299… 35.186.224.25   10.7.0.238      QUIC    309 Protected Payload (KP0)
```

Part-b>

Connection = TCP
Time of sending packet = 0.012294405
Time of response = 0.029015437
RTT = 0.029015437 - 0.012294405
=> 0.016721032 sec = 16.721032 ms



```
2 0.011340075   10.0.136.7       10.0.2.15        DNS   542 Standard query response 0x6e31 A contile-images.services.mozilla.com A 34.120.115.102 NS l.roo
3 0.012294405   10.0.2.15        34.120.115.102   TCP    74 40464 → 443 [SYN] Seq=0 Win=64060 Len=0 MSS=16015 SACK_PERM TSval=1509736514 TSecr=0 WS=128
4 0.029015437   34.120.115.102   10.0.2.15        TCP    60 443 → 40464 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
```

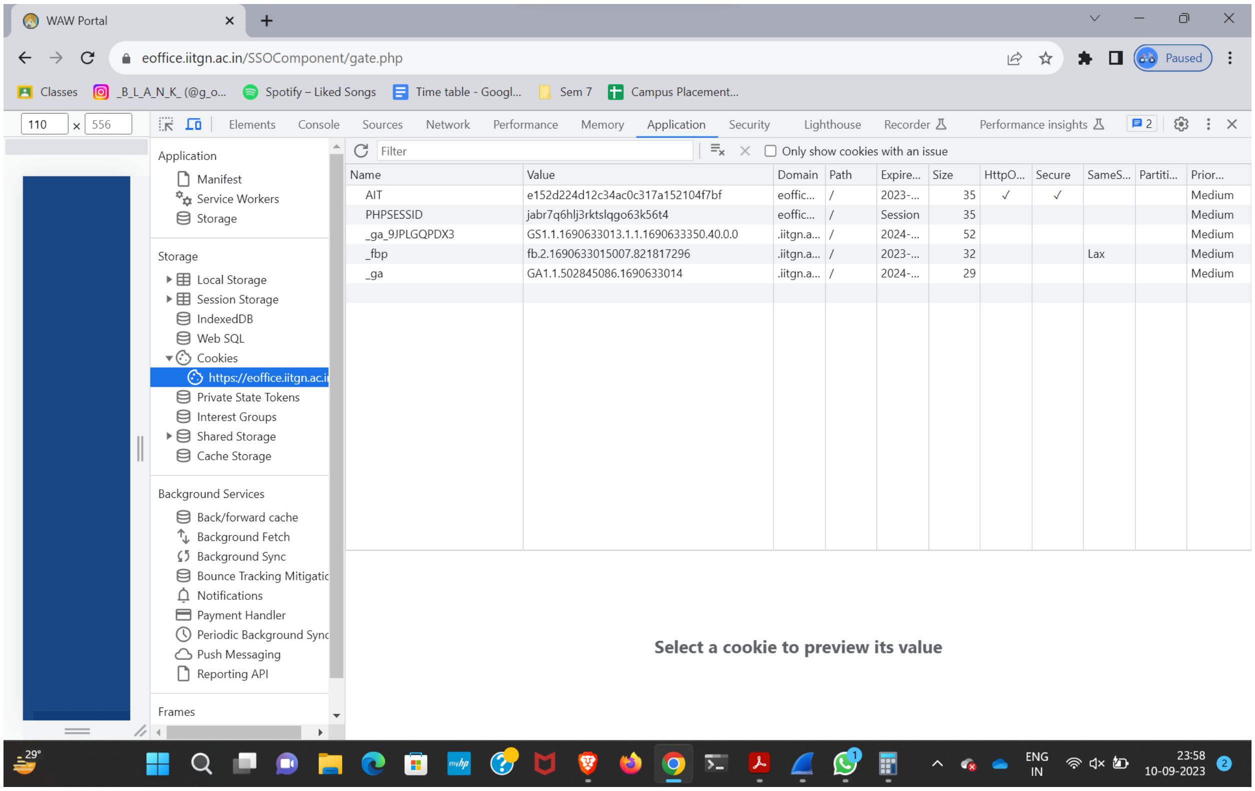
Q.2>

GitHub: Hypertext Transfer Protocol (HTTP) version 2 (HTTP/2)
Netflix: Hypertext Transfer Protocol (HTTP) version 1.1
Google: Hypertext Transfer Protocol (HTTP) version 2 (HTTP/2)

Difference between HTTP/2 and HTTP/1.1

- HTTP/2 uses a binary framing format for messages, while HTTP/1.1 uses a text-based framing format. This makes HTTP/2 more efficient and reliable.
- HTTP/2 supports multiplexing, which allows multiple requests to be sent over the same connection.
- HTTP/2 uses encryption by default, while HTTP/1.1 does not. This makes HTTP/2 more secure.

Q.3>



Name	Value	Domain	Path	Expire...	Size	HttpO...	Secure	SameS...	Partiti...	Prior...
AIT	e152d224d12c34ac0c317a152104f7bf	eoffic...	/	2023-...	35	✓	✓			Medium
PHPSESSID	jabr7q6hlj3rktslqgo63k56t4	eoffic...	/	Session	35					Medium
_ga_9JPLGQPDX3	GS1.1.1690633013.1.1.1690633350.40.0.0	.iitgn.a...	/	2024-...	52					Medium
_fbp	fb.2.1690633015007.821817296	.iitgn.a...	/	2023-...	32			Lax		Medium
_ga	GA1.1.502845086.1690633014	.iitgn.a...	/	2024-...	29					Medium

Select a cookie to preview its value

- _ga: This cookie is used by Google Analytics to track your visits to the website. It is a persistent cookie, meaning it expires after two years.
- PHPSESSID: The PHPSESSID cookie is a first-party cookie, which means it is set by the website you visit. It is a session cookie that expires when you close your browser.
- _fbp: It tracks users across different websites and serves them with targeted advertising. The _fbp cookie is persistent, meaning it expires after three months.