

## DEC\_20 Assessment

### Question No: 5

#### 1) Examine HTTP GET request details.

Examined the GET request from the website

The image shows a Wireshark network traffic capture of an HTTP GET request. The top pane displays a list of network packets, with packet 497 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
497	126.4.639822	172.16.30.150	44.228.249.3	HTTP	497	GET /login.php HTTP/1.1

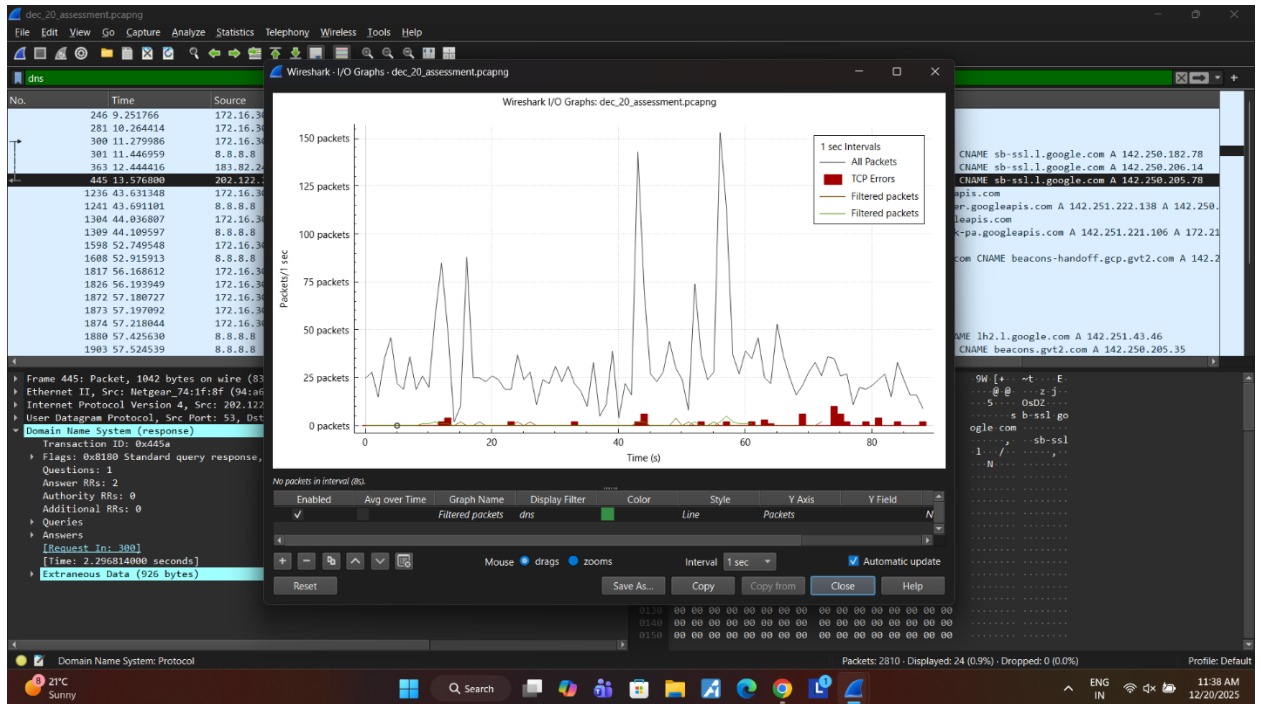
**Packet Details:**

- Frame 126: Packet, 497 bytes on wire (3976 bits), 497 bytes captured (3976 bits) on interface \Device\NPF...
- Ethernet II, Src: LiteonTechno\_a3:5b:2b (d0:39:57:a3:5b:2b), Dst: Sonicwall\_ee:46:3d (18:b1:69:ee:46:3d)
- Internet Protocol Version 4, Src: 172.16.30.150, Dst: 44.228.249.3
- Transmission Control Protocol, Src Port: 54472, Dst Port: 80, Seq: 1, Ack: 1, Len: 443
- Source Port: 54472
- Destination Port: 80
- [Stream index: 1]
- [Conversation completeness: Incomplete (12)]
- [TCP Segment Len: 443]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 627386775
- [Next Sequence Number: 444 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment Number (raw): 4184655733
- 0101 ... e Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 251
- [Calculated window size: 251]
- Window size scaling factor: -1 (unknown)
- Unknown Authentication Extensions

**Raw Data:**

```
0000 18 b1 69 ee 46 3d d0 39 57 a3 5b 2b 08 00 45 00 ...i F= 9 M [+ E
0010 01 e3 f6 c0 00 00 00 06 11 c6 ac 10 1e 96 2c e4 ...@.....,
0020 f9 03 d4 c8 00 50 25 65 29 97 f9 6c cb 5d 5b 18 ...P$e } l lP
0030 00 fb d1 bc 00 00 47 45 54 20 2f 6c 6f 67 69 6e ...GE T /login
0040 2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 ...php HT P/1.1 H
0050 6f 73 74 3a 20 74 65 73 74 70 68 70 2e 76 75 6c ...ost: tes tphp.vul
0060 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 ...nueb.com Connec
0070 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 ...tion: ke ep-alive
0080 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ...Upgrad e-Insecu
0090 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a ...re-Request: 1
00a0 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 ...User-Age nt: Mozi
00b0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 ...lla/5.0 (Windows
00c0 20 4e 54 20 31 38 2e 30 3b 20 57 69 6e 36 34 3b ...NT 10.0 ; Win64;
00d0 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 ...x64) Ap pleWebKi
00e0 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c ...t/537.36 (KHTML,
00f0 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 ...like Gecko) Chr
0100 6f 64 65 2f 31 34 31 2e 30 2e 30 2e 30 20 53 61 ...ome/163.0.0.0 Sa
0110 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 ...fari/537.36 Acc
0120 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 ...ept: tex t/html,a
0130 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c ...pplicati on/shitel
0140 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e ...xml,app lication
0150 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 .../xml;q=0.9,image
```

### For DNS Activity captured I/O Graph



### 3) Note DHCP IP assignment timeline.

DHCP IP assignment noted by using wireshark.

IP Address: 172.16.31.183

The image shows a Wireshark packet capture of DHCP traffic. The top pane displays a list of packets, and the bottom pane shows the details of a selected DHCP Request packet (No. 491).

No.	Time	Source	Destination	Protocol	Length	Info
491	15.219458	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xf3d4ec9d
492	15.220973	172.16.30.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0xf3d4ec9d
623	18.803414	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xf3d4ec9d
624	18.804943	172.16.30.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0xf3d4ec9d
770	24.947573	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xcd4bdf8e
771	24.947573	172.16.30.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0xcd4bdf8e
806	26.177127	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xcd4bdf8e
807	26.178071	172.16.30.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0xcd4bdf8e
1516	49.831235	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0xcab43aca
1517	49.834278	172.16.30.1	255.255.255.255	DHCP	295	DHCP NAK - Transaction ID 0xcab43aca
1518	49.834278	0.0.0.0	255.255.255.255	DHCP	372	DHCP Request - Transaction ID 0xcab43aca
1519	49.835487	172.16.30.1	255.255.255.255	DHCP	295	DHCP NAK - Transaction ID 0xcab43aca
1550	51.776480	0.0.0.0	255.255.255.255	DHCP	378	DHCP Request - Transaction ID 0xb2ff1d7d
1551	51.777725	172.16.30.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0xb2ff1d7d
1689	55.156247	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xb7beabea
1690	55.156247	172.16.30.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0xb7beabea
2427	72.359803	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xc515f56
2428	72.359803	172.16.30.1	255.255.255.255	DHCP	324	DHCP ACK - Transaction ID 0xc515f56

**Packet Details (No. 491):**

- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: Intel\_3e:43:56 (2c:6d:c1:3e:43:56)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option (53) DHCP Message Type (Request)
- Option (61) Client identifier
  - Length: 4
  - Option (50) Requested IP Address (172.16.31.183)
    - Requested IP Address: 172.16.31.183
  - Option (12) Host Name
  - Option (81) Client Fully Qualified Domain Name
  - Option (60) Vendor class identifier
  - Option (55) Parameter Request List
  - Option (255) End

**Packet Bytes:**

0000 ff ff ff ff ff ff 2c 6d c1 3e 43 56 08 00 45 00 .....>CV E-  
0010 01 5e 73 d9 00 00 80 11 c5 b6 00 00 00 ff ff .....^s.....  
0020 ff ff 00 44 00 43 01 4a 13 b1 01 01 06 00 f3 d4 .....D C J.....  
0030 ec 9d 00 02 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0040 00 00 00 00 00 00 2c 6d c1 3e 43 56 00 00 00 00 .....>CV.....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0110 00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01 .....c Se5.....  
0120 2c 6d c1 3e 43 56 32 0a ac 10 1f b7 0c 0f 4c 41 .....>CVZ LA.....  
0130 50 54 4f 50 2d 4b 43 4f 43 45 51 43 41 51 12 00 .....PTOP-KCO CECOCQ.....  
0140 00 00 4c 41 50 54 4f 50 2d 4b 43 4f 43 45 51 43 .....LAPTOP-KCOCECQ.....  
0150 41 3c 08 4d 53 46 54 20 35 2e 30 37 0e 01 03 06 .....Ac MSFT 5.07.....

Dynamic Host Configuration Protocol: Protocol

Packets: 2810 - Displayed: 18 (0.6%) - Dropped: 0 (0.0%)

Profile: Default

21°C Sunny

ENG IN

11:37 AM

12/20/2025