

## Part 1:

1. Source Address: 192.168.1.100  
Destination Address: 128.119.245.12  
Source Port: 63917  
Destination Port: 80
2. gaia.cs.umass.edu
3. Persistent, as indicated by **Connection: keep-alive\r\n**
4. Packet number: 56, File data: 4500 bytes

[Request in frame: 48]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

File Data: 4500 bytes

5. 4 data carrying TCP segments, packet number 56

```
[4 Reassembled TCP Segments (4861 bytes): #52(1370), #53(1370), #54(1370), #56(751)]
[Frame: 52, payload: 0-1369 (1370 bytes)]
[Frame: 53, payload: 1370-2739 (1370 bytes)]
[Frame: 54, payload: 2740-4109 (1370 bytes)]
[Frame: 56, payload: 4110-4860 (751 bytes)]
[Segment count: 4]
```

6. 11 TCP packets + 2 HTTP

No.	Time	Source	Destination	Protocol	Length	Info
43	1.522239	192.168.1.100	128.119.245.12	TCP	66	63917 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
46	1.816606	128.119.245.12	192.168.1.100	TCP	66	80 → 63917 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1370 SACK_PERM WS=128
47	1.816748	192.168.1.100	128.119.245.12	TCP	54	63917 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
48	1.820699	192.168.1.100	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
51	2.141934	128.119.245.12	192.168.1.100	TCP	54	80 → 63917 [ACK] Seq=1 Ack=392 Win=30336 Len=0
52	2.141934	128.119.245.12	192.168.1.100	TCP	1424	80 → 63917 [ACK] Seq=1 Ack=392 Win=30336 Len=1370 [TCP segment of a reassembled PDU]
53	2.141934	128.119.245.12	192.168.1.100	TCP	1424	80 → 63917 [ACK] Seq=1371 Ack=392 Win=30336 Len=1370 [TCP segment of a reassembled PDU]
54	2.141934	128.119.245.12	192.168.1.100	TCP	1424	80 → 63917 [ACK] Seq=2741 Ack=392 Win=30336 Len=1370 [TCP segment of a reassembled PDU]
55	2.142196	192.168.1.100	128.119.245.12	TCP	54	63917 → 80 [ACK] Seq=392 Ack=4111 Win=65536 Len=0
56	2.142439	128.119.245.12	192.168.1.100	HTTP	805	HTTP/1.1 200 OK (text/html)
57	2.142541	192.168.1.100	128.119.245.12	TCP	54	63917 → 80 [ACK] Seq=392 Ack=4862 Win=64768 Len=0
325	7.131297	128.119.245.12	192.168.1.100	TCP	54	80 → 63917 [FIN, ACK] Seq=4862 Ack=392 Win=30336 Len=0
326	7.131432	192.168.1.100	128.119.245.12	TCP	54	63917 → 80 [ACK] Seq=392 Ack=4863 Win=64768 Len=0

7. Packet number 48

```
▼ [Conversation completeness: Complete, WITH_DATA (31)]
..0. .... = RST: Absent
...1 .... = FIN: Present
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
.... ...1 = SYN: Present
[Completeness Flags: ·FDASS]
```

There is no difference between the flag values between the HTTP GET and HTTP OK packets.

8. No
9. From its browser/system-level DNS cache

## Part 2:

10. d8:5e:d3:54:2f:a7
11. UDP
- 12.

DHCP message	Source IP	Destination IP
DHCP Discover	0.0.0.0	255.255.255.255
DHCP Offer	10.250.61.250	10.250.61.60
DHCP Request	0.0.0.0	255.255.255.255
DHCP ACK	10.250.61.250	10.250.61.60

13. 10.250.61.250 (based on DHCP Offer and ACK packets)
14. a-ii, b-iii, c-ii, d-iii
15. Option: (50) Requested IP Address (10.250.61.42) (in Discover packet)  
Option: (50) Requested IP Address (10.250.61.60) (in Request packet)
16. No, since  
DHCP Server Identifier: 10.250.61.250  
Domain Name Server: 10.250.200.3  
Router: 10.250.61.250
17. No, because Domain Name Server: 10.250.200.3 does not belong to the client's subnet 10.250.61.X

### Part 3:

18. ICMP
19. On receiving **Type: 0 (Echo (ping) reply)**, the client stops sending additional ICMP probes with higher TTL values.
20. Type: 8 (Echo (ping) request)
21. Type: 11 (Time-to-live exceeded)  
Type: 0 (Echo (ping) reply)
22. 10.250.61.113  
10.250.61.250  
10.240.0.1  
10.240.240.1  
103.120.31.121  
103.120.29.73  
103.120.29.72  
72.14.209.113  
142.250.209.75  
142.250.62.66  
72.14.232.34  
192.178.110.105  
209.85.242.111  
172.217.166.68
23. The ICMP error message carries the first 8 bytes of the IP Datagram causing the error.

#### Part 4:

24. TLSv1.2 and TLSv1.3

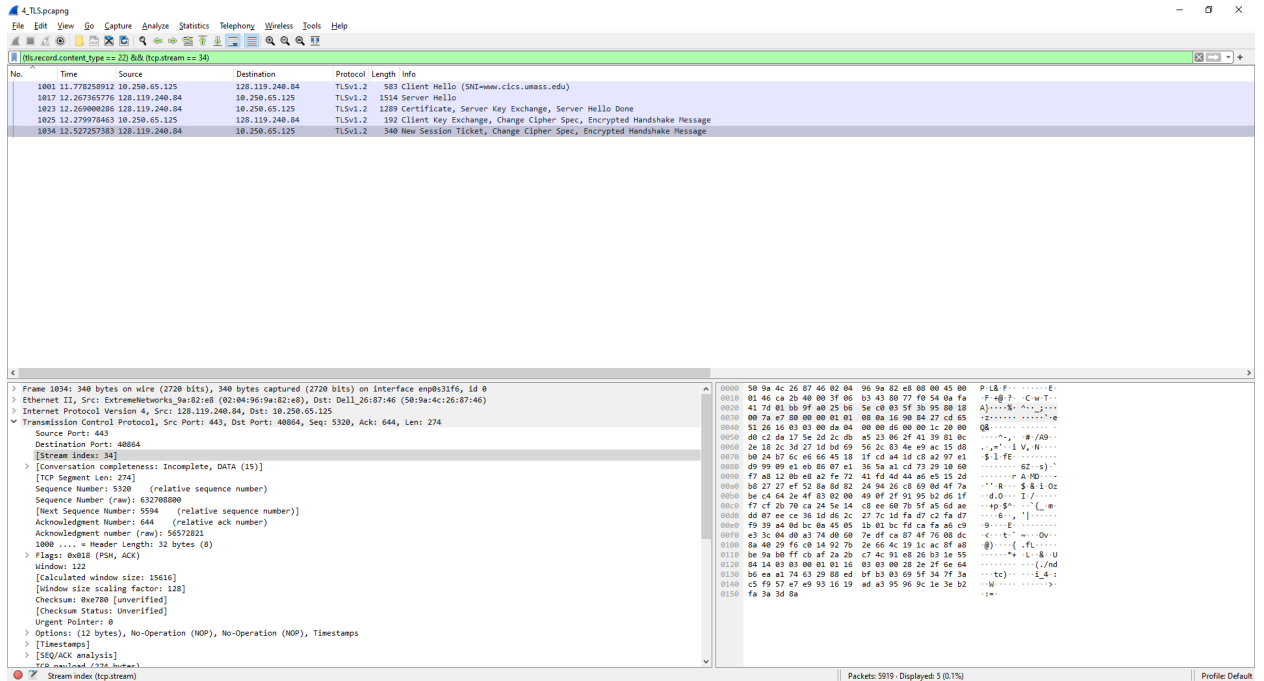
TLSv1.2

25. 393

26. 17

TLS\_AES\_128\_GCM\_SHA256 (0x1301)

27. 5

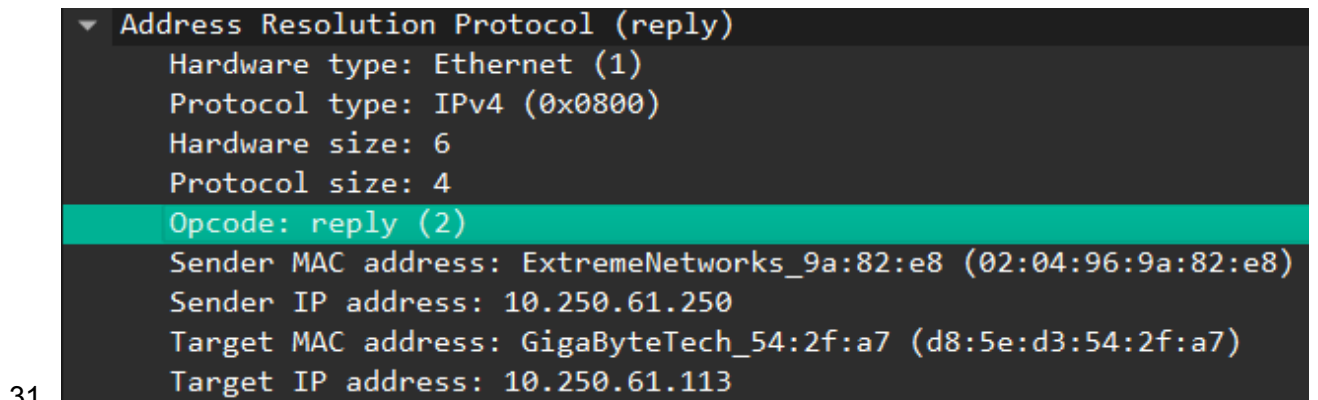


#### Part 5:

28. d8:5e:d3:54:2f:a7

29. Cannot be determined from the given trace

30. 28 bytes



31.

Hardware type: Ethernet (1) – 2 bytes

Protocol type: IPv4 (0x0800) - 2 bytes

Hardware size: 6 – 1 byte

Protocol size: 4 - 1 byte

Opcode: reply (2) – 2 bytes

Sender MAC address: ExtremeNetworks\_9a:82:e8 (02:04:96:9a:82:e8) – 6 bytes

Sender IP address: 10.250.61.250 – 4 bytes

Target MAC address: Giga-Byt\_54:2f:a7 (d8:5e:d3:54:2f:a7) – 6 bytes

Target IP address: 10.250.61.113 – 4 bytes

32. After 20 bytes

#### Part 6:

33. 00:17:f2:98:f0:6f

IP Address of the client interface cannot be determined from the given packet trace.

34. 00:16:b6:e3:e9:8d

IP Address of the WiFi AP interface cannot be determined from the given packet trace.

35.

a. Source address: Apple\_98:f0:6f (00:17:f2:98:f0:6f)

Destination address: CiscoLinksys\_e3:e9:8d (00:16:b6:e3:e9:8d)

BSS Id: CiscoLinksys\_e3:e9:8f (00:16:b6:e3:e9:8f)

b. 1478 bytes

36. 2462 or 2.462GHz. Also called as “802.11 b/g channel 11”

37. Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]

38. wlan.fc.type==1(Acknowledgement frame) → 1391

wlan.fc.type==2(Data frame) → 1783

wlan.fc.type=="management frame" → 557 frames

39. Filter: wlan.fc.type==2 && wlan.fc.retry==0

Total number of data frames “wlan.fc.type==2” = 1783

Number of transmission frames “wlan.fc.type==2 && wlan.fc.retry==0” = 1430

Number of retransmission frames = 1783 - 1430 = 353

#### NS3 Answers:

40. Nodes, Application, Channels, Network Devices, Topology helpers

41. NetAnim