

WIRESHARK

Pranay Gupta 20161088

Shubh Maheshwari 20161170

Part 1 (HTTP)

Part A :

- 1) Browser - HTTP 1.1; Server - HTTP 1.1; Accept Language en-US,en;q=0.5
- 2) Computer IP - 10.1.40.164 ; Server IP - 10.4.20.103
- 3) 200 OK
- 4) Last Modified : Mon, 26 Feb 2018 06:59:01 GMT
- 5) 128

Part B.

- 1) No.
- 2) Yes. All the contents are available in the Line-Based text data field
- 3) Yes it contains the if-modified since flag. If-Modified-Since : If-Modified-Since: Mon, 26 Feb 2018 06:59:01 GMT. This contains the time and date of the last modification of the file from the previous GET request.
- 4) The status code returned is 304 Not Modified. This does not explicitly return the contents of the file because its loaded from the cache.

Part 2(DNS)

96	1.575681932	10.1.40.164	10.4.20.103	TCP	74	38530 -> 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=904829653 TSecr=0 WS=128
97	1.575734618	10.1.40.164	10.4.20.222	DNS	76	Standard query 0xb2d3 A proxy.iiit.ac.in
98	1.575742289	10.1.40.164	10.4.20.264	DNS	76	Standard query 0xb2d3 A proxy.iiit.ac.in
99	1.576075994	10.4.20.222	10.1.40.164	DNS	160	Standard query response 0xb2d3 A proxy.iiit.ac.in A 10.4.20.103 NS ns4.iiit.ac.in NS ns3.iiit.ac.in A 10.4.20.222 A 10.4.20.264
100	1.576336298	10.4.20.264	10.1.40.164	DNS	160	Standard query response 0xb2d3 A proxy.iiit.ac.in A 10.4.20.103 NS ns3.iiit.ac.in NS ns4.iiit.ac.in A 10.4.20.222 A 10.4.20.264

Frame 97: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: Dell_07:83:77 (18:db:f2:07:83:77), Dst: Cisco_76:47:49 (64:00:f1:76:47:49)
Internet Protocol Version 4, Src: 10.1.40.164, Dst: 10.4.20.222
User Datagram Protocol, Src Port: 47482, Dst Port: 53
Domain Name System (query)

- 1) UDP
- 2) I received 1 answer in each of the response messages.
 - ▼ Answers
 - ▼ proxy.iiit.ac.in: type A, class IN, addr 10.4.20.103
 - Name: proxy.iiit.ac.in
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 86400
 - Data length: 4
 - Address: 10.4.20.103
- 3) Yes. They both have the ip address of 10.4.20.103. Which was the provided in the answers of the dns response messages.
- 4) No.

No.	Time	Source	Destination	Protocol	Length	Info
53	15.676075984	10.4.20.222	10.1.40.164	DNS	160	Standard query response 0xb2d3 A proxy.iiit.ac.in A 10.4.20.103 NS ns4.iiit.ac.in NS ns3.iiit.ac.in A 10.4.20.222 A 10.4.20.2
100	1.576336298	10.4.20.204	10.1.40.164	DNS	160	Standard query response 0xb2d3 A proxy.iiit.ac.in A 10.4.20.103 NS ns3.iiit.ac.in NS ns4.iiit.ac.in A 10.4.20.222 A 10.4.20.2

▶ Frame 99: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
 ▶ Ethernet II, Src: Cisco 76:47:49 (64:00:f1:76:47:49), Dst: Dell 07:83:77 (18:db:f2:07:83:77)
 ▶ Internet Protocol Version 4, Src: 10.4.20.222, Dst: 10.1.40.164
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 47402
 ▶ Domain Name System (response)

0020 28 a4 00 35 b9 2a 00 7e f5 c1 32 d3 85 80 80 01 (.5.*.-.1.....
 0030 80 01 80 02 00 02 05 70 72 07 70 79 04 69 09 09p roxy.iiit
 0040 74 02 01 03 02 00 0e 00 00 01 00 01 c0 0c 00 01 .ac.in.
 0050 80 01 80 01 51 80 00 04 0a 04 14 07 c0 12 00 02 ...Q.....g.....
 0060 80 01 80 01 51 80 00 00 03 66 73 34 c0 12 c0 12 ...Q.....ns4.....
 0070 80 02 00 01 00 01 51 80 00 00 03 66 73 33 c0 12Q.....ns3.....
 0080 c0 50 80 01 00 01 00 01 51 80 00 04 0a 04 14 0e P.....Q.....

- 5)
- 6) Destination port of DNS query message is 53. Source port of DNS query message is also 53.
- 7) The DNS query message is of type A. It does not contain any answers.

No.	Time	Source	Destination	Protocol	Length	Info
281	6.078264873	10.4.20.222	10.1.40.181	DNS	138	Standard query response 0xc333 A ntp.ubuntu.com A 91.189.89.198 A 91.189.94.4 A 91.189.91.157 A 91.189.89.199
282	6.078271776	10.4.20.222	10.1.40.181	DNS	138	Standard query response 0xc617 AAAA ntp.ubuntu.com AAAA 2001:67c:1560:8083::c8 AAAA 2001:67c:1560:8083::c7
283	6.078543786	10.4.20.204	10.1.40.181	DNS	138	Standard query response 0xc333 A ntp.ubuntu.com A 91.189.89.199 A 91.189.94.4 A 91.189.89.198 A 91.189.91.157
424	12.783788922	10.1.40.164	10.4.20.222	DNS	71	Standard query 0xb425 A www.mit.edu
425	12.783820495	10.1.40.164	10.4.20.204	DNS	71	Standard query 0xb425 A www.mit.edu
426	12.903030467	10.4.20.222	10.1.40.164	DNS	160	Standard query response 0xb425 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.89.56.63
434	13.851467787	10.4.20.204	10.1.40.164	DNS	160	Standard query response 0xb425 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.89.56.63
491	14.369590238	10.1.40.164	10.4.20.222	DNS	76	Standard query 0xdd07 A proxy.iiit.ac.in
494	14.36995125	10.4.20.222	10.1.40.164	DNS	160	Standard query response 0xdd07 A proxy.iiit.ac.in A 10.4.20.103 NS ns3.iiit.ac.in NS ns4.iiit.ac.in A 10.4.20.222 A 10.4.20.2

▶ Frame 122: 160 bytes on wire (1280 bits), 71 bytes captured (568 bits) on interface 0
 ▶ Ethernet II, Src: Dell 07:83:77 (18:db:f2:07:83:77), Dst: Cisco 76:47:49 (64:00:f1:76:47:49)
 ▶ Internet Protocol Version 4, Src: 10.1.40.164, Dst: 10.4.20.204
 ▶ User Datagram Protocol, Src Port: 47402, Dst Port: 53
 ▶ Domain Name System (query)

[Response in: 434]
 Transaction ID: 0xb425
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 ▶ www.mit.edu: type A, class IN

- 8) The response message contains 3 answers. One answer is of type A and the other two are of type CNAME.3
- 9) The DNS query is sent to the 10.4.20.222.Yes.
- 10) The query message is of type NS and it does not contain any answers.
- 11) The dns response message provides several MIT nameservers.
 - a) use2.akam.net
 - b) asia2.akam.net
 - c) use5.akam.net
 - d) usw2.akam.net
 - e) ns1-173.akam.net
 - f) asia1.akam.net
 - g) ns1-37.akam.net
 - h) eur5.akam.net

Their IP addresses can be found under the additional records header

Part 3(TCP)

- 1) Source - IP address: 192.168.1.102, Port Number: 1161
Destination - IP address 128.119.245.12, Port Number: 80
- 2) The IP address of gaia.cs.umass.edu is 128.119.245.12 (todo).
- 3) Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. The value is 0 in the given trace. The syn flag bit is used to identify the syn segment.
- 4) The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0. The value of the ACKnowledgement field in the SYNACK segment is 1. The value of the ACKnowledgement field in the SYNACK segment is determined by adding 1 to the initial sequence number of SYN segment from the client computer. Here, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the acknowledgement field in the SYN_ACK segment is 1. The SYN flag and Acknowledgement flag in the segment are set to 1 (Set) and they indicate that this segment is a SYNACK segment.
- 5) The sequence number of this segment has the value of 1.
- 6) Length of 1st TCP segment is 565 bytes and length of other 5 TCP segments is 1460 bytes.
- 7) The minimum amount of buffer space (receiver window) advertised at gaia.cs.umass.edu for the entire trace is 5840 byte. No, the sender is not throttled due to lacking of receiver buffer space.
- 8) No, there are no retransmitted segments in the trace file. This can be verified by checking whether the sequence numbers of the TCP segments in the given trace are monotonically increasing or not.

Part 4(UDP)

- 1) There are 4 fields in the UDP header
 - a) Source Port
 - b) Destination Port
 - c) Length
 - d) Checksum
- 2) The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next. The length is 36. (28 data bytes + 8 bytes of header).

```
Source Port: 48582
Destination Port: 2008
Length: 36
Checksum: 0x920d [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
▼ Data (28 bytes)
Data: 42432032336c61666572726172692d4c656e6f766f2d5a35...
[Length: 28]
```

- 3) Yes, The source address is same as my ip address.

- 4) The destination address is 255.255.255.255
- 5) $(2^{16}) - 1 - 8(\text{header size}) = 65527$
- 6) $2^{16} - 1 = 65535$
- 7) The IP protocol number for UDP is 0x11 hex system. (17 in decimal system)
- 8) It's also a 16-bit field of one's complement of one's complement sum of a pseudo UDP header + UDP datagram. The Pseudo UDP header also consists of 5 fields,
 - source address: 32 bits/4 bytes, taken from IP header
 - destination address: 32 bits/4 bytes, taken from IP header
 - reserved: 8 bits/1 byte, set to all 0s.
 - protocol: 8 bits/1 byte, taken from IP header
 - length
- 9) The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.