



Winter – SEMESTER 2022 - 23
Course Code: MCSE505P
Course-Title: – computer Network Lab
DIGITAL ASSIGNMENT - 2
(LAB)

Name: Nidhi Singh
Reg. No: 22MAI0015

Slot-L35+L36

Faculty: - SRIMATHI C - SCOPE

HTTP :-

1. The Basic HTTP GET/response interaction

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer :-

Both of them are version 1.1 (HTTP version information is listed in the item 'Request Version')

The image shows a Wireshark packet capture of an HTTP interaction. The top pane displays a list of packets, with packet 1422 selected. The middle pane shows the details of the selected packet, which is an HTTP 200 OK response. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1420	253.328796	172.16.135.165	184.84.108.200	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
504	71.420741	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2950	615.004027	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1422	253.341233	184.84.108.200	172.16.135.165	HTTP	568	HTTP/1.1 200 OK (text/html)
519	71.672211	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified
2959	615.264399	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified

Details of Packet 1422 (HTTP/1.1 200 OK):

- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (514 bytes)
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33\r\n

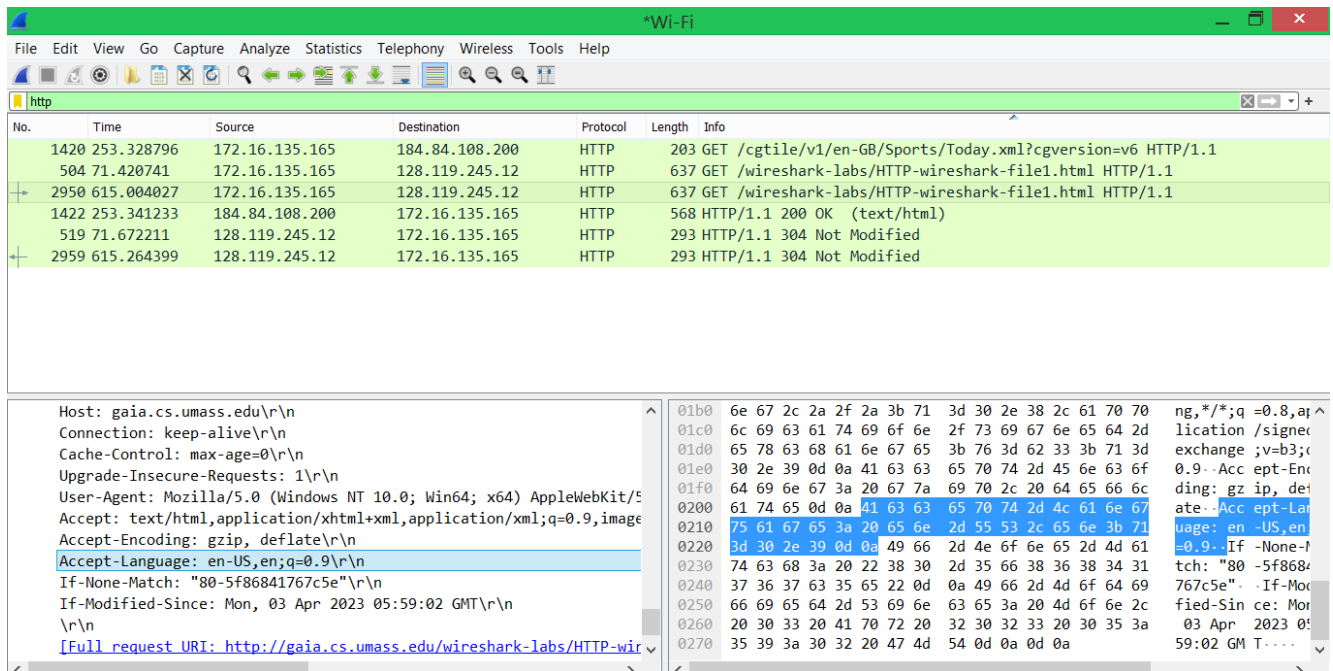
Raw Data (Hex): 0040 30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 41 00 OK..S erver: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33-X-Powered by: PHP/7.1.33-Content-Type: text/html; charset=UTF-8-Cache-Control: max-age=6708-Expires: Thu, 13 Apr 2022 12:43:11 GMT..

2. What languages (if any) does your browser indicate that it can accept to the server?

Answer :-

en-US

(languages information is listed in the item 'Accept-Language' in the HTTP GET message)



No.	Time	Source	Destination	Protocol	Length	Info
1420	253.328796	172.16.135.165	184.84.108.200	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
504	71.420741	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2950	615.004027	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1422	253.341233	184.84.108.200	172.16.135.165	HTTP	568	HTTP/1.1 200 OK (text/html)
519	71.672211	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified
2959	615.264399	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified

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/80.0.3987.122 Safari/537.36\r\n	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n	Accept-Encoding: gzip, deflate\r\n	Accept-Language: en-US,en;q=0.9\r\n	If-None-Match: \"80-5f86841767c5e\"\r\n	If-Modified-Since: Mon, 03 Apr 2023 05:59:02 GMT\r\n	\r\n	[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
-----------------------------	----------------------------	------------------------------	----------------------------------	---	--	------------------------------------	-------------------------------------	---	--	------	---

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer :-

my computer: 172.16.135.165

gaia.cs.umass.edu: 184.84.108.200

No.	Time	Source	Destination	Protocol	Length	Info
1420	253.328796	172.16.135.165	184.84.108.200	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
504	71.420741	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2950	615.004027	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1422	253.341233	184.84.108.200	172.16.135.165	HTTP	568	HTTP/1.1 200 OK (text/html)
519	71.672211	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified
2959	615.264399	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified

<p>▶ Frame 1420: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface 0</p> <p>▶ Ethernet II, Src: HonHaiPr_a7:2a:db (d8:5d:e2:a7:2a:db), Dst: HewlettPac_77:3b (68:b5:99:ce:77:3b)</p> <p>▶ Destination: HewlettPac_77:3b (68:b5:99:ce:77:3b)</p> <p>▶ Source: HonHaiPr_a7:2a:db (d8:5d:e2:a7:2a:db)</p> <p>Type: IPv4 (0x0800)</p> <p>▶ Internet Protocol Version 4, Src: 172.16.135.165, Dst: 184.84.108.200</p> <p>0100 = Version: 4</p> <p>.... 0101 = Header Length: 20 bytes (5)</p> <p>▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</p> <p>Total Length: 189</p> <p>Identification: 0x5c5b (23643)</p>	<pre> 0000 68 b5 99 ce 77 3b d8 5d e2 a7 2a db 00 00 45 00 h---w;.] ...*...E- 0010 00 bd 5c 5b 40 00 40 06 85 0d ac 10 87 a5 b8 54 ..\[@.@T 0020 6c c8 c1 d0 00 50 16 e9 74 51 d8 e1 61 61 50 18 1....P...tQ...aaP- 0030 04 00 0a 84 00 00 47 45 54 20 2f 63 67 74 69 6c -GE T /cgtil 0040 65 2f 76 31 2f 65 6e 2d 47 42 2f 53 70 6f 72 74 e/v1/en- GB/Sport 0050 73 2f 54 6f 64 61 79 2e 78 6d 6c 3f 63 67 76 65 s/Today. xml?cgve 0060 72 73 69 6f 6e 3d 76 36 20 48 54 54 50 2f 31 2e rsion=v6 HTTP/1. 0070 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 1..User- Agent: M 0080 69 63 72 6f 73 6f 66 74 2d 57 4e 53 2f 36 2e 33 icrosoft -WNS/6.3 0090 0d 0a 48 6f 73 74 3a 20 65 6e 2d 47 42 2e 61 70 ..Host: en-GB.ap 00a0 70 65 78 2d 72 66 2e 6d 73 6e 2e 63 6f 6d 0d 0a pex-rf.m sn.com.. 00b0 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e Cache-Co ntrol: n </pre>
--	--

4. What is the status code returned from the server to your browser?

Answer :-

status code:200

(status code information is listed in the HTTP OK message)

No.	Time	Source	Destination	Protocol	Length	Info
1420	253.328796	172.16.135.165	184.84.108.200	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
504	71.420741	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2950	615.004027	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1422	253.341233	184.84.108.200	172.16.135.165	HTTP	568	HTTP/1.1 200 OK (text/html)
519	71.672211	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified
2959	615.264399	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified

<p>▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]</p> <p>Response Version: HTTP/1.1</p> <p>Status Code: 200</p> <p>[Status Code Description: OK]</p> <p>Response Phrase: OK</p> <p>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33\r\n</p> <p>X-Powered-By: PHP/7.1.33\r\n</p> <p>Content-Type: text/html; charset=UTF-8\r\n</p> <p>Cache-Control: max-age=866708\r\n</p> <p>Expires: Thu, 13 Apr 2023 12:43:11 GMT\r\n</p> <p>Date: Mon, 03 Apr 2023 11:58:03 GMT\r\n</p> <p>Content-Length: 214\r\n</p>	<pre> 0030 01 f5 b7 45 00 00 48 54 54 50 2f 31 2e 31 20 32 ...E- HT TP/1.1 0040 30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 41 OK -S erver: 0050 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e apache/2. 4.6 (Ce 0060 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 tos) Ope nSSL/1. 0070 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 31 .2k-fips PHP/7. 0080 2e 33 33 0d 0a 58 2d 50 6f 77 65 72 65 64 2d 42 .33..X-P owered- 0090 79 3a 20 50 48 50 2f 37 2e 31 2e 33 33 0d 0a 43 y: PHP/7 .1.33.. 00a0 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 ontent-T ype: te 00b0 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d t/html; charse 00c0 55 54 46 2d 38 0d 0a 43 61 63 68 65 2d 43 6f 6e UTF-8..C ache-Co 00d0 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 38 36 trol: ma x-age= 00e0 36 37 30 38 0d 0a 45 78 70 69 72 65 73 3a 20 54 6708..Ex pires: 00f0 68 75 2c 20 31 33 20 41 70 72 20 32 30 32 33 20 hu, 13 A pr 202 </pre>
--	--

5. When was the HTML file that you are retrieving last modified at the server?

Answer :-

Mon, 03 Apr 2023 05:59:02 GMT\r\n

(last modified information is listed in the item 'Last-Modified' in the HTTP OK message)

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/110.0.0.0 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9\r\n
 If-None-Match: "80-5f86841767c5e"\r\n
 If-Modified-Since: Mon, 03 Apr 2023 05:59:02 GMT\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

6. How many bytes of content are being returned to your browser?

Answer :-

Content length: 331 (Content length information is listed in the item 'Content-Length' in the HTTP OK message)

[Status Code Description: OK]
 Response Phrase: OK
 Date: Mon, 03 Apr 2023 15:37:03 GMT\r\n
 Server: Apache/2.4.6 (Unix) OpenSSL/1.0.1\r\n
 Last-Modified: Mon, 03 Apr 2023 11:02:02 GMT\r\n
 ETag: "14b-5f86c7d19cac0"\r\n
 Accept-Ranges: bytes\r\n
 Content-Length: 331\r\n

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Answer :-

No, there is no more headers below.

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
1420	253.328796	172.16.135.165	184.84.108.200	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
504	71.420741	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2950	615.004027	172.16.135.165	128.119.245.12	HTTP	637	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1422	253.341233	184.84.108.200	172.16.135.165	HTTP	568	HTTP/1.1 200 OK (text/html)
519	71.672211	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified
2959	615.264399	128.119.245.12	172.16.135.165	HTTP	293	HTTP/1.1 304 Not Modified

Destination: HonHaiPr_a7:2a:db (d8:5d:e2:a7:2a:db) Source: HewlettP_ce:77:3b (68:b5:99:ce:77:3b) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 184.84.108.200, Dst: 172.16.135.165 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 554 Identification: 0x12e9 (4841) 010. = Flags: 0x2, Don't fragment 0... = Reserved bit: Not set 1... = Don't fragment: Set	0000 d8 5d e2 a7 2a db 68 b5 99 ce 77 3b 08 00 45 00 .].*. 0010 02 2a 12 e9 40 00 3b 06 d2 12 b8 54 6c c8 ac 10 .*..@ 0020 87 a5 00 50 c1 d0 d8 e1 61 61 16 e9 74 e6 50 18 ...P. 0030 01 f5 b7 45 00 00 48 54 54 50 2f 31 2e 31 20 32 ...E. 0040 30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 41 00 OK 0050 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e pache 0060 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 tOS) 0070 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 31 .2k-f 0080 2e 33 33 0d 0a 58 2d 50 6f 77 65 72 65 64 2d 42 .33.. 0090 79 3a 20 50 48 50 2f 37 2e 31 2e 33 33 0d 0a 43 y: PH 00a0 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 onten 00b0 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d t/htm 00c0 55 54 46 2d 38 0d 0a 43 61 63 68 65 2d 43 6f 6e UTF-8 00d0 74 73 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 onten
---	--

Header length in 32-bit words (ip_hdr_len), 1 byte

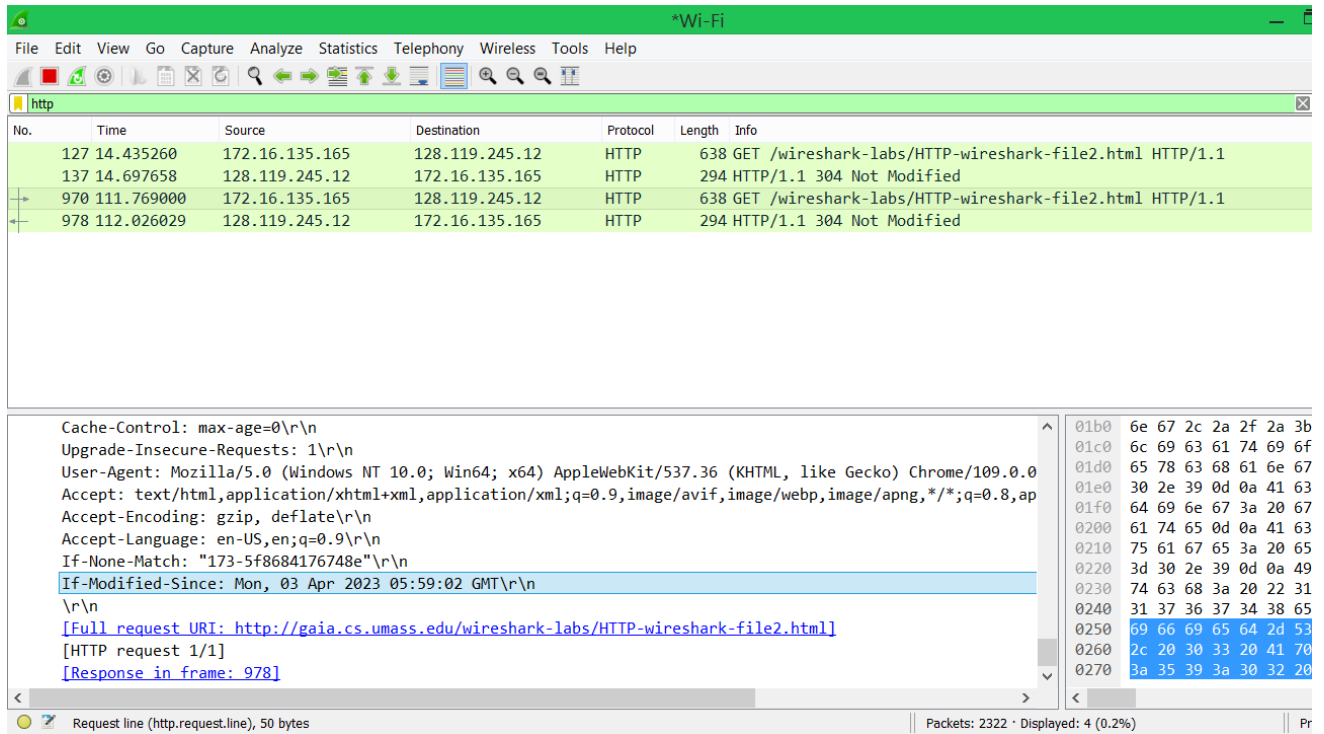
Packets: 3182 · Displayed: 6 (0.2%) · Dropped: 0 (0.0%)

2. The HTTP CONDITIONAL GET/response interaction

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Answer :-

According to the bellow Diagram , there is no IF-MODIFIED-SINCE line in the first HTTP GET, but according to the Diagram bellow, IF-MODIFIED-SINCE is found in the second HTTP GET (the web page cached locally, asking the server side, the local cache need to be updated or not).



9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer :-

According to bellow Diagram, the server explicitly return the contents of the file, but according to the Diagram 6, the server did not explicitly return the contents of the file since the file had not been modified.

No.	Time	Source	Destination	Protocol	Length	Info
127	14.435260	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
137	14.697658	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
970	111.769000	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
978	112.026029	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
2641	399.452503	172.16.135.165	23.7.161.241	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
2643	399.548619	23.7.161.241	172.16.135.165	HTTP	569	HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33\r\n
 - X-Powered-By: PHP/7.1.33\r\n
 - Content-Type: text/html; charset=UTF-8\r\n
 - Cache-Control: max-age=1007807\r\n
 - Expires: Sat, 15 Apr 2023 06:57:44 GMT\r\n

10 of 24 - Cl

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer :-

According to the Diagram , IF-MODIFIED-SINCE is found in the second HTTP GET (the web page cached locally, asking the server side, the local cache need to be updated or not). According to the Diagram , the server returning a 304 not modified follows the “IF-MODIFIED- SINCE:” header.

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list pane shows several HTTP packets. The second packet (No. 970) is an HTTP GET request for '/wireshark-labs/HTTP-wireshark-file2.html' with a status of '304 Not Modified'. The packet details pane shows the request headers, including 'Host: gaia.cs.umass.edu', 'Connection: keep-alive', 'Cache-Control: max-age=0', 'Upgrade-Insecure-Requests: 1', 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap', 'Accept-Encoding: gzip, deflate', 'Accept-Language: en-US,en;q=0.9', 'If-None-Match: "173-5f8684176748e"', and 'If-Modified-Since: Mon, 03 Apr 2023 05:59:02 GMT'. The packet bytes pane shows the raw data of the request line and headers.

No.	Time	Source	Destination	Protocol	Length	Info
127	14.435260	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
137	14.697658	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
970	111.769000	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
978	112.026029	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
2641	399.452503	172.16.135.165	23.7.161.241	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
2643	399.548619	23.7.161.241	172.16.135.165	HTTP	569	HTTP/1.1 200 OK (text/html)

Request URI: /wireshark-labs/HTTP-wireshark-file2.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/109.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5f8684176748e"\r\n
If-Modified-Since: Mon, 03 Apr 2023 05:59:02 GMT\r\n

Request line (http.request.line). 50 bytes

Packets: 4249 · Disposed: 6 (0.1%)

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer :-

According to the Diagram. The HTTP status code is 304 Not Modified and the server did not explicitly return the contents of the file since the file was cached locally.

The image shows a Wireshark network traffic capture window titled '*Wi-Fi'. The main pane displays a list of captured packets. The 'http' filter is applied. The packet list shows several HTTP GET requests. Packet 2643 is highlighted, showing an HTTP 200 OK response. The packet details pane for packet 2643 shows the 'Hypertext Transfer Protocol' section expanded, displaying the response status and headers.

No.	Time	Source	Destination	Protocol	Length	Info
127	14.435260	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
137	14.697658	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
970	111.769000	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
978	112.026029	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
2641	399.452503	172.16.135.165	23.7.161.241	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
2643	399.548619	23.7.161.241	172.16.135.165	HTTP	569	HTTP/1.1 200 OK (text/html)

[Bytes sent since last PSH flag: 515]
TCP payload (515 bytes)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.33\r\nX-Powered-By: PHP/7.1.33\r\nContent-Type: text/html; charset=UTF-8\r\n

3. Retrieving Long Documents

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
127	14.435260	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
137	14.697658	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
970	111.769000	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
978	112.026029	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
2641	399.452503	172.16.135.165	23.7.161.241	HTTP	203	GET /cgtile/v1/en-GB/Sports/Today.xml?cgversion=v6 HTTP/1.1
2643	399.548619	23.7.161.241	172.16.135.165	HTTP	569	HTTP/1.1 200 OK (text/html)
7784	1046.347943	172.16.135.165	23.198.100.200	HTTP	235	GET /Market.svc/AppTileV2?symbols=&contentType=-1&tileType=0&loc...
7787	1046.349290	172.16.135.165	23.7.161.241	HTTP	188	GET /cgtile/v1/en-GB/News/Today.xml HTTP/1.1
7791	1046.444736	23.7.161.241	172.16.135.165	HTTP	569	HTTP/1.1 200 OK (text/html)
7793	1046.479507	23.198.100.200	172.16.135.165	HTTP	545	HTTP/1.1 503 Service Unavailable (text/html)
11663	2058.791832	172.16.135.165	23.201.59.99	HTTP	151	GET /ncsi.txt HTTP/1.1
11667	2058.855417	23.201.59.99	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
11678	2059.023443	172.16.135.165	23.201.59.73	HTTP	222	GET /redirect HTTP/1.1
11680	2059.030109	172.16.135.165	172.16.135.165	HTTP	634	HTTP/1.1 302 Found (text/html)
11686	2059.039457	172.16.135.165	172.16.1.1	HTTP	270	GET /redirect.html?URI=http://www.msftncsi.com/redirect HTTP/1.1
11688	2059.045924	172.16.1.1	172.16.135.165	HTTP	681	HTTP/1.1 200 OK (text/html)
12196	2090.133482	172.16.135.165	184.26.162.217	HTTP	151	GET /ncsi.txt HTTP/1.1
12237	2090.404756	184.26.162.217	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
12623	2115.189471	172.16.135.165	184.26.162.217	HTTP	151	GET /ncsi.txt HTTP/1.1
12625	2115.195018	184.26.162.217	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
12941	2146.887113	172.16.135.165	23.201.59.73	HTTP	151	GET /ncsi.txt HTTP/1.1
12944	2146.890736	23.201.59.73	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
13237	2175.222632	172.16.135.165	184.26.162.217	HTTP	151	GET /ncsi.txt HTTP/1.1
13239	2175.225873	184.26.162.217	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)

Hypertext Transfer Protocol: Protocol Packets: 13354 · Displayed: 38 (0.3%) · Dropped: 0 (0.0%) Profile:

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
7791	1046.444736	23.7.161.241	172.16.135.165	HTTP	569	HTTP/1.1 200 OK (text/html)
7793	1046.479507	23.198.100.200	172.16.135.165	HTTP	545	HTTP/1.1 503 Service Unavailable (text/html)
11663	2058.791832	172.16.135.165	23.201.59.99	HTTP	151	GET /ncsi.txt HTTP/1.1
11667	2058.855417	23.201.59.99	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
11678	2059.023443	172.16.135.165	23.201.59.73	HTTP	222	GET /redirect HTTP/1.1
11680	2059.030109	23.201.59.73	172.16.135.165	HTTP	634	HTTP/1.1 302 Found (text/html)
11686	2059.039457	172.16.135.165	172.16.1.1	HTTP	270	GET /redirect.html?URI=http://www.msftncsi.com/redirect HTTP/1.1
11688	2059.045924	172.16.1.1	172.16.135.165	HTTP	681	HTTP/1.1 200 OK (text/html)
12196	2090.133482	172.16.135.165	184.26.162.217	HTTP	151	GET /ncsi.txt HTTP/1.1
12237	2090.404756	184.26.162.217	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
12623	2115.189471	172.16.135.165	184.26.162.217	HTTP	151	GET /ncsi.txt HTTP/1.1
12625	2115.195018	184.26.162.217	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
12941	2146.887113	172.16.135.165	23.201.59.73	HTTP	151	GET /ncsi.txt HTTP/1.1
12944	2146.890736	23.201.59.73	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
13237	2175.222632	172.16.135.165	184.26.162.217	HTTP	151	GET /ncsi.txt HTTP/1.1
13239	2175.225873	184.26.162.217	172.16.135.165	HTTP	597	HTTP/1.1 302 Found (text/html)
13293	2178.321537	172.16.135.165	23.215.215.178	HTTP	181	GET /STCA.crl HTTP/1.1
13295	2178.325198	23.215.215.178	172.16.135.165	HTTP	640	HTTP/1.1 302 Found (text/html)
13301	2178.334603	172.16.135.165	172.16.1.1	HTTP	229	GET /redirect.html?URI=http://crl.securetrust.com/STCA.crl HTTP/...
13303	2178.343153	172.16.1.1	172.16.135.165	HTTP	681	HTTP/1.1 200 OK (text/html)
13311	2178.366229	172.16.135.165	23.48.244.42	HTTP	297	GET //MFEwTzBNMEswSTAJBgUrDgMCGGUABBRu0R7X9EhEQPk4dB85gXE3Ik%2...
13313	2178.368375	23.48.244.42	172.16.135.165	HTTP	592	HTTP/1.1 404 Not Found (text/html)
13315	2178.373715	172.16.135.165	23.48.244.42	OCSP	137	Request
13317	2178.375829	23.48.244.42	172.16.135.165	HTTP	621	HTTP/1.1 302 Found (text/html)

Hypertext Transfer Protocol: Protocol Packets: 13354 · Displayed: 38 (0.3%) · Dropped: 0 (0.0%) Profile:

The image shows a Wireshark capture of network traffic. The top pane displays a list of packets, with the selected packet (No. 10) being a GET request from 172.16.1.1 to 172.16.135.165. The middle pane shows the details of this packet, identifying it as an HTTP GET request for the resource /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
13303	2178.343153	172.16.1.1	172.16.135.165	HTTP	681	HTTP/1.1 200 OK (text/html)
13311	2178.366229	172.16.135.165	23.48.244.42	HTTP	297	GET //MFEwTzBNMEswSTAJBgUrDgMCGGUABBRu0R7X9EhfEQPk4dB85gXE3Ik%2...
13313	2178.368375	23.48.244.42	172.16.135.165	HTTP	592	HTTP/1.1 404 Not Found (text/html)
13315	2178.373715	172.16.135.165	23.48.244.42	OCSP	137	Request
13317	2178.375829	23.48.244.42	172.16.135.165	HTTP	621	HTTP/1.1 302 Found (text/html)
13318	2178.376253	172.16.135.165	172.16.1.1	HTTP	263	GET /redirect.html?URI=http://ocsp.trustwave.com/ HTTP/1.1
13319	2178.379921	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)
13326	2178.397644	172.16.135.165	23.215.215.178	HTTP	182	GET /OVCA_L2.cr1 HTTP/1.1
13328	2178.399893	23.215.215.178	172.16.135.165	HTTP	642	HTTP/1.1 302 Found (text/html)
13329	2178.400320	172.16.135.165	172.16.1.1	HTTP	230	GET /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1 HTTP...
13330	2178.403776	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol

- GET /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1 HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1 HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1
 - Request URI Path: /redirect.html
 - Request URI Query: URI=http://cr1.trustwave.com/OVCA_L2.cr1
 - Request URI Query Parameter: URI=http://cr1.trustwave.com/OVCA_L2.cr1
 - Request Version: HTTP/1.1
 - Connection: Keep-Alive\r\n
 - Accept: */*\r\n
 - User-Agent: Microsoft-CryptoAPI/6.3\r\n
 - Host: phc.prontonetworks.com\r\n

0000 68 b5 99 ce 77 3b d8 5
 0010 00 d8 30 f2 40 00 40 0
 0020 01 01 c3 be 00 50 48 6
 0030 00 fb 8f 12 00 00 47 4
 0040 65 63 74 2e 68 74 6d 6
 0050 70 3a 2f 2f 63 72 6c 2
 0060 65 2e 63 6f 6d 2f 4f 5
 0070 6c 20 48 54 54 50 2f 3
 0080 65 63 74 69 6f 6e 3a 2
 0090 76 65 0d 0a 41 63 63 6
 00a0 0a 55 73 65 72 2d 41 6
 00b0 72 6f 73 6f 66 74 2d 4
 00c0 2f 36 2e 33 0d 0a 48 6
 00d0 70 72 6f 6e 74 6f 6e 6

Hypertext Transfer Protocol: Protocol | Packets: 13354 · Displayed: 38 (0.3%) · Dropped: 0 (0.0%) | Profi

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer :-

The first response packet (PDU) from the server, packet 10 contains the status code and phrase.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
13303	2178.343153	172.16.1.1	172.16.135.165	HTTP	681	HTTP/1.1 200 OK (text/html)
13311	2178.366229	172.16.135.165	23.48.244.42	HTTP	297	GET //MFEwTzBNMEswSTAJBgUrDgMCGGUABBRu0R7X9EhfEQPk4dB85gXE3Ik%2...
13313	2178.368375	23.48.244.42	172.16.135.165	HTTP	592	HTTP/1.1 404 Not Found (text/html)
13315	2178.373715	172.16.135.165	23.48.244.42	OCSP	137	Request
13317	2178.375829	23.48.244.42	172.16.135.165	HTTP	621	HTTP/1.1 302 Found (text/html)
13318	2178.376253	172.16.135.165	172.16.1.1	HTTP	263	GET /redirect.html?URI=http://ocsp.trustwave.com/ HTTP/1.1
13319	2178.379921	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)
13326	2178.397644	172.16.135.165	23.215.215.178	HTTP	182	GET /OVCA_L2.cr1 HTTP/1.1
13328	2178.399893	23.215.215.178	172.16.135.165	HTTP	642	HTTP/1.1 302 Found (text/html)
13329	2178.400320	172.16.135.165	172.16.1.1	HTTP	230	GET /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1 HTTP...
13330	2178.403776	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Mon, 03 Apr 2023 15:37:03 GMT\r\n

Server: Apache/2.4.6 (Unix) OpenSSL/1.0.1\r\n

Last-Modified: Mon, 03 Apr 2023 11:02:02 GMT\r\n

ETag: "14b-5f86c7d19cac0"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 331\r\n

0000 d8 5d e2 a7 2a db 68 b5

0010 02 9a 95 bf 40 00 40 06

0020 87 a5 00 50 c3 be c5 f1

0030 08 b3 b4 43 00 00 48 54

0040 30 30 20 4f 4b 0d 0a 44

0050 2c 20 30 33 20 41 70 72

0060 3a 33 37 3a 30 33 20 47

0070 65 72 3a 20 41 70 61 63

0080 20 28 55 6e 69 78 29 20

0090 31 2e 30 2e 31 0d 0a 4c

00a0 66 69 65 64 3a 20 4d 6f

00b0 72 20 32 30 32 33 20 31

00c0 47 4d 54 0d 0a 45 54 61

00d0 35 66 38 36 63 37 64 31

Hypertext Transfer Protocol: Protocol

Packets: 13354 · Displayed: 38 (0.3%) · Dropped: 0 (0.0%) · Profile:

14. What is the status code and phrase in the response?

Answer :-

200 OK

The image shows a Wireshark capture of an HTTP response. The packet list at the top shows a 200 OK response from 172.16.135.165 to 172.16.1.1. The packet details pane shows the response structure with status code 200 and OK. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
13303	2178.343153	172.16.1.1	172.16.135.165	HTTP	681	HTTP/1.1 200 OK (text/html)
13311	2178.366229	172.16.135.165	23.48.244.42	HTTP	297	GET //MFEwTzBNMEswSTAJBgUrDgMCGGUABBRu0R7X9EhfEQPk4dB85gXE3Ik%2...
13313	2178.368375	23.48.244.42	172.16.135.165	HTTP	592	HTTP/1.1 404 Not Found (text/html)
13315	2178.373715	172.16.135.165	23.48.244.42	OCSP	137	Request
13317	2178.375829	23.48.244.42	172.16.135.165	HTTP	621	HTTP/1.1 302 Found (text/html)
13318	2178.376253	172.16.135.165	172.16.1.1	HTTP	263	GET /redirect.html?URI=http://ocsp.trustwave.com/ HTTP/1.1
13319	2178.379921	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)
13326	2178.397644	172.16.135.165	23.215.215.178	HTTP	182	GET /OVCA_L2.cr1 HTTP/1.1
13328	2178.399893	23.215.215.178	172.16.135.165	HTTP	642	HTTP/1.1 302 Found (text/html)
13329	2178.400320	172.16.135.165	172.16.1.1	HTTP	230	GET /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1 HTTP...
13330	2178.403776	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n**
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Mon, 03 Apr 2023 15:37:03 GMT\r\n
 - Server: Apache/2.4.6 (Unix) OpenSSL/1.0.1\r\n
 - Last-Modified: Mon, 03 Apr 2023 11:02:02 GMT\r\n
 - ETag: "14b-5f86c7d19cac0"\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Length: 331\r\n

0030 08 b3 b4 43 00 00 48 54
0040 30 30 20 4f 4b 0d 0a 44
0050 2c 20 30 33 20 41 70 72
0060 3a 33 37 3a 30 33 20 47
0070 65 72 3a 20 41 70 61 63
0080 20 28 55 6e 69 78 29 2e
0090 31 2e 30 2e 31 0d 0a 4c
00a0 66 69 65 64 3a 20 4d 6f
00b0 72 20 32 30 32 33 20 31
00c0 47 4d 54 0d 0a 45 54 61
00d0 35 66 38 36 63 37 64 31
00e0 41 63 63 65 70 74 2d 52
00f0 79 74 65 73 0d 0a 43 6f
0100 6e 67 74 68 3a 20 33 33

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 13354 · Displayed: 38 (0.3%) · Dropped: 0 (0.0%) · Profile

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answer :-

According to the diagram 7, 3 TCP segments (10, 11 and 13) were needed to carry the single HTTP response and the text of the Bill of Rights

The screenshot displays a Wi-Fi network analyzer interface. The top pane shows a list of captured packets. The bottom pane provides a detailed view of a selected packet, including its structure and the reassembled TCP segment data.

No.	Time	Source	Destination	Protocol	Length	Info
13303	2178.343153	172.16.1.1	172.16.135.165	HTTP	681	HTTP/1.1 200 OK (text/html)
13311	2178.366229	172.16.135.165	23.48.244.42	HTTP	297	GET //MFEwTzBNMEswSTAJBgUrDgMCGGUABBRu0R7X9EhfEQPk4dB85gXE3Ik%2...
13313	2178.368375	23.48.244.42	172.16.135.165	HTTP	592	HTTP/1.1 404 Not Found (text/html)
13315	2178.373715	172.16.135.165	23.48.244.42	OCSP	137	Request
13317	2178.375829	23.48.244.42	172.16.135.165	HTTP	621	HTTP/1.1 302 Found (text/html)
13318	2178.376253	172.16.135.165	172.16.1.1	HTTP	263	GET /redirect.html?URI=http://ocsp.trustwave.com/ HTTP/1.1
13319	2178.379921	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)
13326	2178.397644	172.16.135.165	23.215.215.178	HTTP	182	GET /OVCA_L2.cr1 HTTP/1.1
13328	2178.399893	23.215.215.178	172.16.135.165	HTTP	642	HTTP/1.1 302 Found (text/html)
13329	2178.400320	172.16.135.165	172.16.1.1	HTTP	230	GET /redirect.html?URI=http://cr1.trustwave.com/OVCA_L2.cr1 HTTP...
13330	2178.403776	172.16.1.1	172.16.135.165	HTTP	680	HTTP/1.1 200 OK (text/html)

The bottom pane shows the detailed view of a selected packet, including its structure and the reassembled TCP segment data.

[Checksum Status: Unverified]
 Urgent Pointer: 0
 [Timestamps]
 [Time since first frame in this TCP stream: 0.010409000 seconds]
 [Time since previous frame in this TCP stream: 0.000074000 seconds]
 [SEQ/ACK analysis]
 [iRTT: 0.002753000 seconds]
 [Bytes in flight: 305]
 [Bytes sent since last PSH flag: 83]
 TCP payload (83 bytes)
 TCP segment data (83 bytes)
 [2 Reassembled TCP Segments (305 bytes): #13314(222), #13315(83)]
 Hypertext Transfer Protocol

Frame (137 bytes) Reassembled TCP (305 bytes)

Packets: 13354 · Displayed: 38 (0.3%) · Dropped: 0 (0.0%) Profile

4. HTML Documents with Embedded Objects

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer :-

According to the Diagram 8, the browser sent 3 HTTP GET request messages. Packet 10 was sent to 128.119.245.12, packet 17 was sent to 165.193.123.218, and packet 20 was sent to 134.241.6.82.

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
45	15.473361	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
49	15.726367	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
1030	310.531980	172.16.135.165	52.167.254.228	HTTP/X...	180	POST /ReportingWebService/ReportingWebService.asmx HTTP/1.1
1038	310.763380	52.167.254.228	172.16.135.165	HTTP/X...	691	HTTP/1.1 200 OK

GET /wireshark-labs/HTTP-wireshark-file4.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/109.0.0.0 Safari/537.36\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\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: en-US,en;q=0.9\r\n If-None-Match: "3ae-5f8907d1ea55d"\r\n If-Modified-Since: Wed, 05 Apr 2023 05:59:01 GMT\r\n \r\n [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]						
---	--	--	--	--	--	--

Destination Hardware Address (eth.dst), 6 bytes	Packets: 1548 · Displayed: 4 (0.3%)	2 of 24 Item collec
---	-------------------------------------	------------------------

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer :-

Two images were downloaded in parallel. According to diagram 8, the HTTP GET requests for two images were sent using packet 17 and 20, and the response packets were 25 and 54 which means the request for the second image was made before the first image was received.

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
45	15.473361	172.16.135.165	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
49	15.726367	128.119.245.12	172.16.135.165	HTTP	294	HTTP/1.1 304 Not Modified
1030	310.531980	172.16.135.165	52.167.254.228	HTTP/X...	180	POST /ReportingWebService/ReportingWebService.asmx HTTP/1.1
1038	310.763380	52.167.254.228	172.16.135.165	HTTP/X...	691	HTTP/1.1 200 OK
1662	482.283603	172.16.135.165	184.84.108.200	HTTP	188	GET /cgtile/v1/en-GB/News/Today.xml HTTP/1.1
1664	482.295363	184.84.108.200	172.16.135.165	HTTP	568	HTTP/1.1 200 OK (text/html)
1668	482.307862	172.16.135.165	23.211.192.168	HTTP	235	GET /Market.svc/AppTileV2?symbols=&contentType=-1&tileType=0&local
1670	482.357256	23.211.192.168	172.16.135.165	HTTP	546	HTTP/1.1 503 Service Unavailable (text/html)

Frame 45: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF_{FF0C1033-1F5A-4196-8DAD-F4C6C71063AC}, id 0

Section number: 1

Interface id: 0 (\Device\NPF_{FF0C1033-1F5A-4196-8DAD-F4C6C71063AC})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 5, 2023 16:36:05.529447000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1680692765.529447000 seconds

[Time delta from previous captured frame: 0.000593000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 15.473361000 seconds]

Frame Number: 45

Frame Length: 638 bytes (5104 bits)

Capture Length: 638 bytes (5104 bits)

The number of the file section this frame is in (frame.section_number)
Packets: 4655 · Displayed: 8 (0.2%)
Profile

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer :-

According to the diagram , the initial HTTP GET message should be packet 6 and the packet 9 is the response to the packet 6. Thus the server's response is 401 Authorization Required.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
155	11.057969	172.16.135.165	128.119.245.12	HTTP	632	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP
162	11.512136	128.119.245.12	172.16.135.165	HTTP	583	HTTP/1.1 404 Not Found (text/html)

Window: 238
 [Calculated window size: 238]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0xf41b [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 [Timestamps]
 [SEQ/ACK analysis]
 TCP payload (529 bytes)
 Hypertext Transfer Protocol
 HTTP/1.1 404 Not Found\r\n
 Date: Wed, 05 Apr 2023 18:02:01 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

Checksum Status (tcp.checksum.status)

Packets: 2598 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) Prof

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
60	8.809234	172.16.135.165	70.90.187.249	HTTP	546	GET /stories/storyReader\$2159 HTTP/1.1
113	9.492416	70.90.187.249	172.16.135.165	HTTP	1514	Continuation
114	9.493194	70.90.187.249	172.16.135.165	HTTP	1514	Continuation
116	9.495260	70.90.187.249	172.16.135.165	HTTP	1514	Continuation
119	10.038900	70.90.187.249	172.16.135.165	HTTP	946	Continuation
126	10.449131	70.90.187.249	172.16.135.165	HTTP	1514	Continuation

[Timestamps]
 [SEQ/ACK analysis]
 TCP payload (492 bytes)
 Hypertext Transfer Protocol
 GET /stories/storyReader\$2159 HTTP/1.1\r\n
 Host: frontier.userland.com\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 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9\r\n

Source Port (tcp.srcport), 2 bytes

Packets: 894 · Displayed: 6 (0.7%) Prof

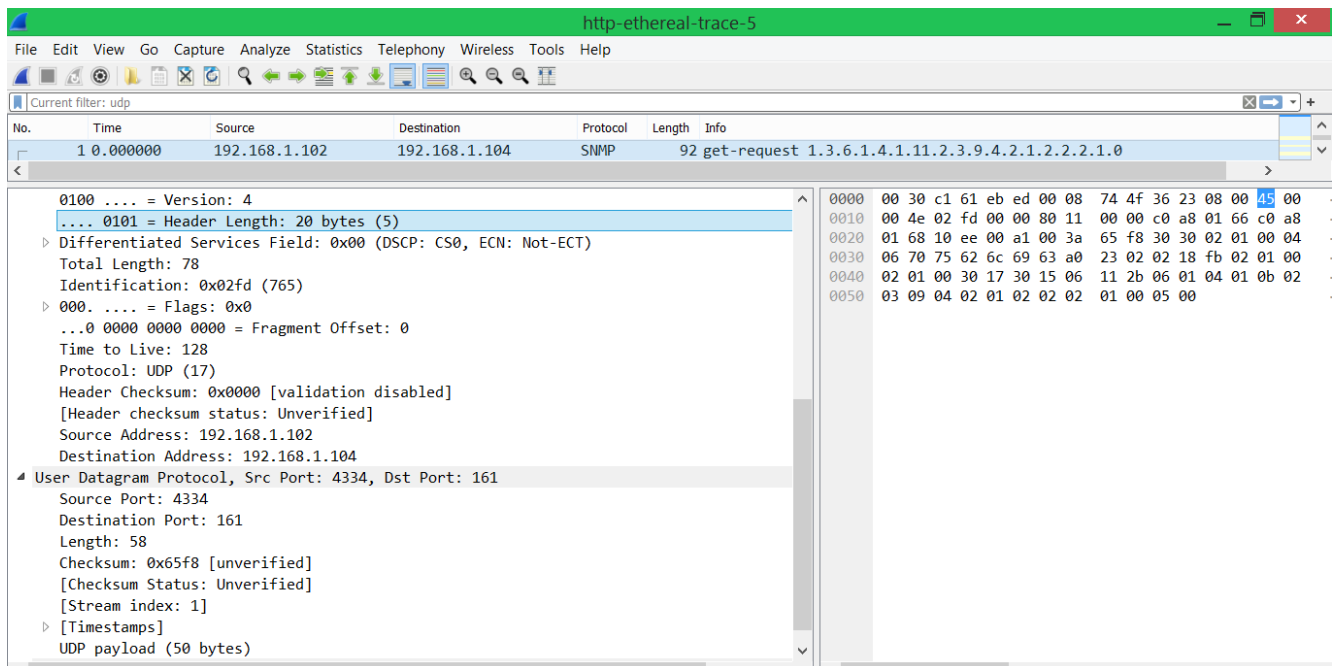
UDP :-

1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

Solution:

UDP header contains 4 fields:

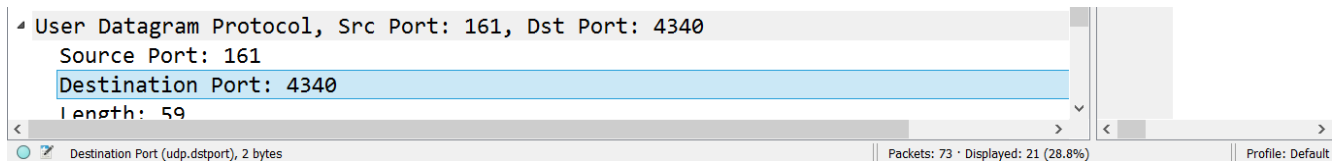
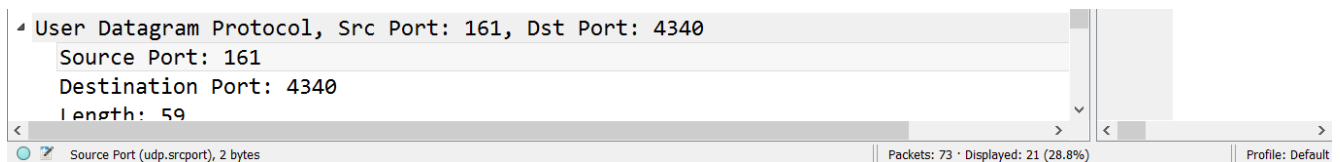
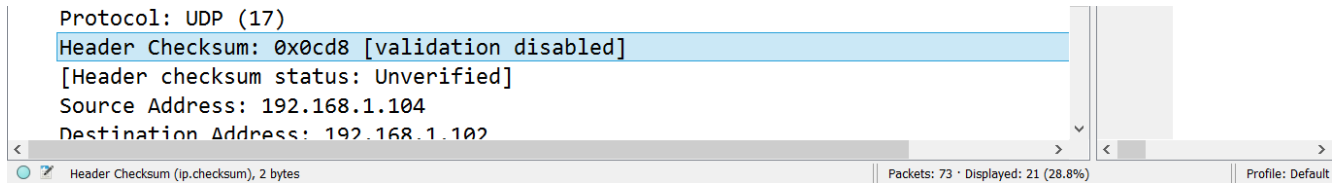
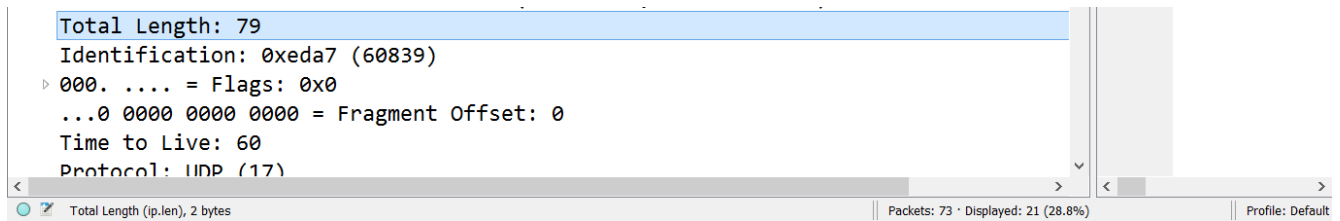
1. source port; 2. destination port; 3. length; 4. checksum



2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

Solution:

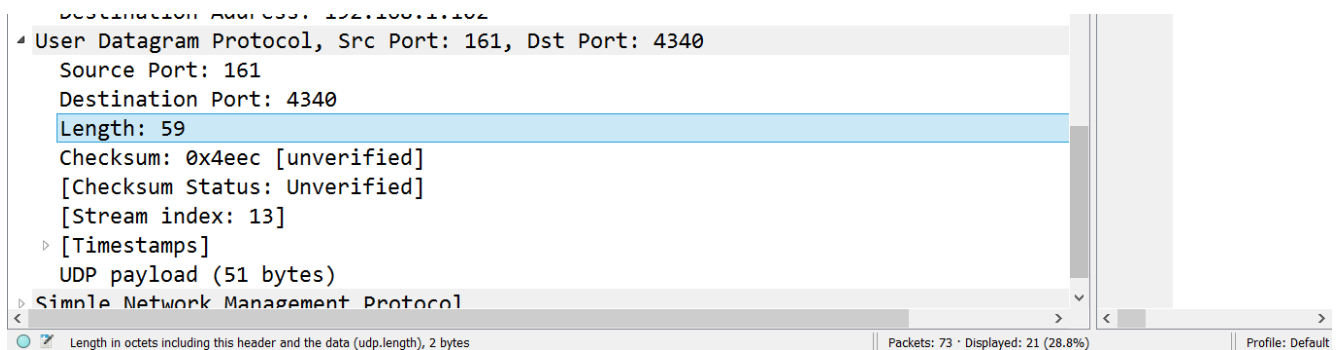
The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.



3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

Solution:

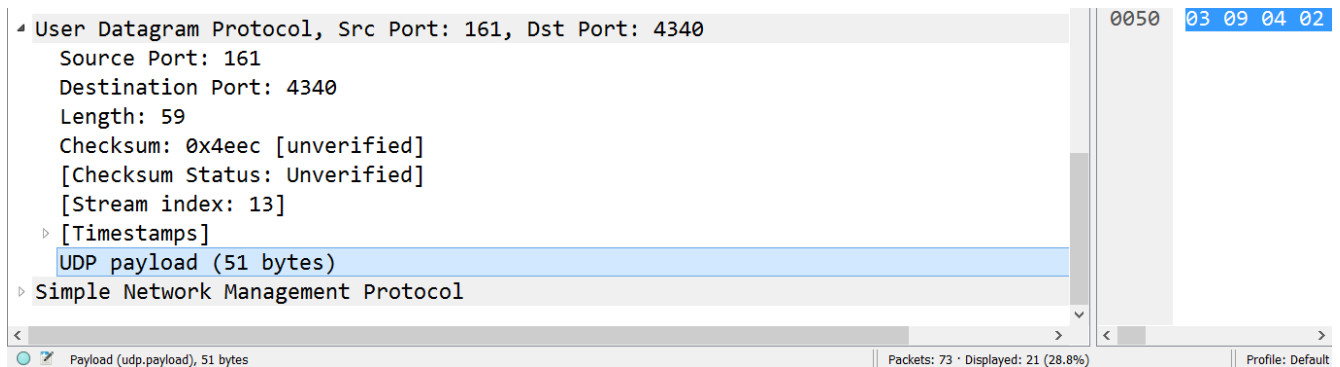
The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next. The length of UDP payload for selected packet is 59 bytes.



4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

Solution:

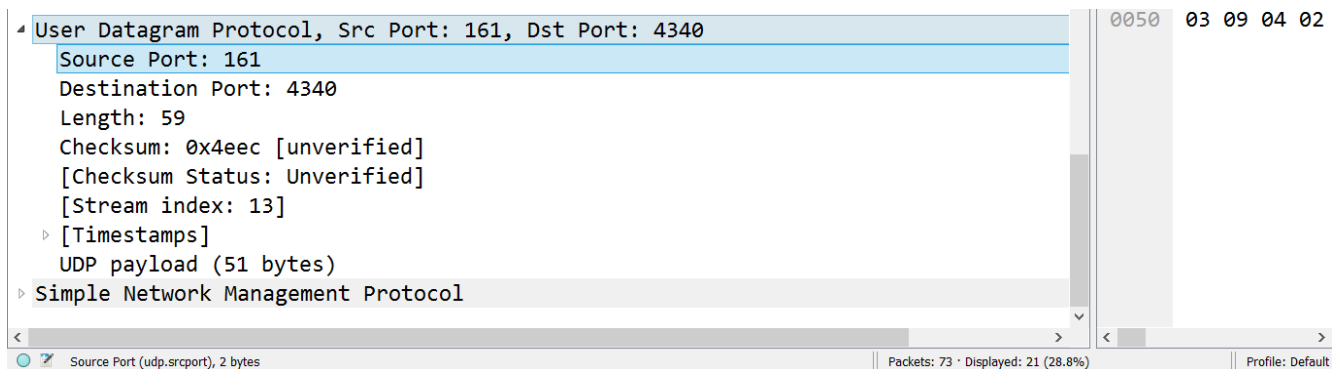
The maximum number of bytes that can be included in a UDP payload is $(2^{16} - 1)$ bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.



5. What is the largest possible source port number? (Hint: see the hint in 4.)

Solution:

The largest possible source port number is $(2^{16} - 1) = 65535$.



6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

Solution:

The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

```

Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 79
    Identification: 0xeda7 (60839)
  000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 60
    Protocol: UDP (17)
    Header Checksum: 0x0cd8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.104

```

Protocol (ip.proto), 1 byte | Packets: 73 · Displayed: 21 (28.8%) | Profile: Default

7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

Answer :-

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.

You can see that destination of first packet is the sender of second packet and sender of first packet is the destination of second packet. So we can say that communication is perform between to machine only.

Current filter: udp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
2	0.016960	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
11	3.016971	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
12	3.034127	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
13	6.033719	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
14	6.050808	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
15	9.050463	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
16	9.067492	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
17	12.067214	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
18	12.085147	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1

Source and Destination port of 1st packet :-

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
2	0.016960	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
11	3.016971	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
12	3.034127	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
13	6.033710	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1

Time to Live: 128	0000	00 30 c1 61
Protocol: UDP (17)	0010	00 4e 02 fd
Header Checksum: 0x0000 [validation disabled]	0020	01 68 10 ee
[Header checksum status: Unverified]	0030	06 70 75 62
Source Address: 192.168.1.102	0040	02 01 00 30
Destination Address: 192.168.1.104	0050	03 09 04 02
User Datagram Protocol, Src Port: 4334, Dst Port: 161		
Source Port: 4334		
Destination Port: 161		
Length: 58		

Source and Destination port of 2nd packet :-

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
2	0.016960	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
11	3.016971	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
12	3.034127	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1
13	6.033710	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1

Time to Live: 60	0000	00 08 74 4f
Protocol: UDP (17)	0010	00 4f ed a2
Header Checksum: 0x0cdd [validation disabled]	0020	01 66 00 a1
[Header checksum status: Unverified]	0030	06 70 75 62
Source Address: 192.168.1.104	0040	02 01 00 30
Destination Address: 192.168.1.102	0050	03 09 04 02
User Datagram Protocol, Src Port: 161, Dst Port: 4334		
Source Port: 161		
Destination Port: 4334		
Length: 59		

TCP :-

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows.

Answer :-

According to bellow figure, the client computer (source)'s IP address is 192.168.1.102 and the TPC source port number is 1161.

No.	Time	Source	Destination	Protocol	Length	Info
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12 <ul style="list-style-type: none"> 0100 = Version: 4 0101 = Header Length: 20 bytes (5) ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 90 Identification: 0x1e9a (7834) ▸ 010. = Flags: 0x2, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: TCP (6) Header Checksum: 0xa471 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102 Destination Address: 128.119.245.12 	0000 6 0010 6 0020 6 0030 4 0040 2 0050 2 0060 3
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50 <ul style="list-style-type: none"> Source Port: 1161 Destination Port: 80 [Stream index: 0] 	

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Answer :-

According to bellow figure, the IP address of gaia.cs.umass.edu is 128.119.245.12 and the TCP port number is 80.

No.	Time	Source	Destination	Protocol	Length	Info
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)
206	5.651141	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0
213	7.595557	192.168.1.102	199.2.53.206	TCP	62	1162 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 770
Identification: 0x58bc (22716)
▷ 010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 55
Protocol: TCP (6)
Header Checksum: 0xb0a7 [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 192.168.1.102

Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 164091, Len: 730

Source Port: 80
Destination Port: 1161
[Stream index: 0]

Internet Protocol Version 4 (ip), 20 bytes
Packets: 213 · Displayed: 202 (94.8%)
Profile: Default

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

Answer :-

According to above figure, my client computer's IP address is 192.168.1.102 and the TCP port is 1161.

No.	Time	Source	Destination	Protocol	Length	Info
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/p
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0

Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)

Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:2

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 5

Source Port: 1161
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 50]

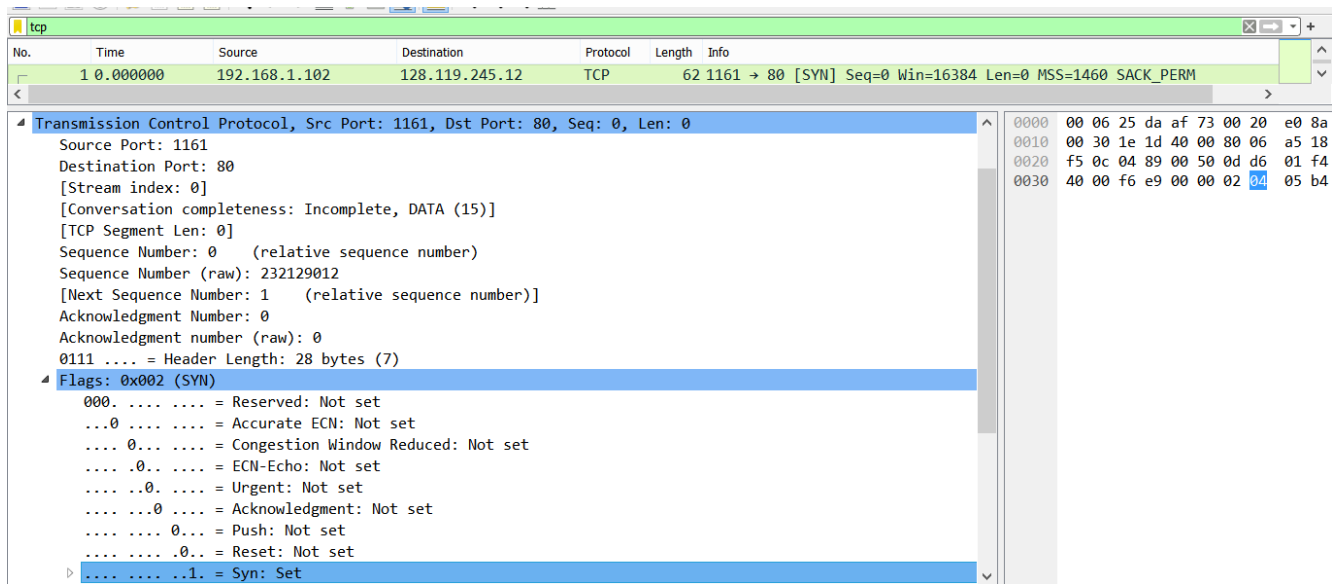
0000 00 06 25 da af 73 00 20
0010 00 5a 1e 9a 40 00 80 06
0020 f5 0c 04 89 00 50 0d d8
0030 44 70 9f 0f 00 00 0d 0a
0040 2d 2d 2d 2d 2d 2d 2d 2d
0050 2d 2d 2d 2d 2d 32 36 35
0060 35 37 32 34 2d 2d 0d 0a

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Answer :-

The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and gaia.cs.umass.edu.

According to bellow figure, in the Flags section, the Syn flag is set to 1 which indicates that this segment is a SYN segment.



5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Answer :-

According to the bellow figure, 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 the server gaia.cs.umass.edu. The server adds 1 to the initial sequence number of SYN segment form the client computer.

For this case, the initial sequence number of SYN segment from the client computer is 0, thus the value of the ACKnowledgement field in the SYNACK segment is 1.

A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM

Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0		0000 00 20 e0 8a 70 1a 00 06 25 da
Source Port: 80		0010 00 30 00 00 40 00 37 06 0c 36
Destination Port: 1161		0020 01 66 00 50 04 89 34 a2 74 19
[Stream index: 0]		0030 16 d0 77 4d 00 00 02 04 05 b4
[Conversation completeness: Incomplete, DATA (15)]		
[TCP Segment Len: 0]		
Sequence Number: 0 (relative sequence number)		
Sequence Number (raw): 883061785		
[Next Sequence Number: 1 (relative sequence number)]		
Acknowledgment Number: 1 (relative ack number)		
Acknowledgment number (raw): 232129013		
0111 = Header Length: 28 bytes (7)		
Flags: 0x012 (SYN, ACK)		
000. = Reserved: Not set		
...0 = Accurate ECN: Not set		
.... 0... = Congestion Window Reduced: Not set		
.... .0.. = ECN-Echo: Not set		
.... ..0. = Urgent: Not set		
.... ...1 = Acknowledgment: Set		
.... = Push: Not set		
.... ..0. = Reset: Not set		
....1. = Syn: Set		
....0 = Fin: Not set		

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of data length 565 bytes]

Destination Port: 1161		0000 00 20 e0 8a 70 1a 00 06
[Stream index: 0]		0010 00 30 00 00 40 00 37 06
[Conversation completeness: Incomplete, DATA (15)]		0020 01 66 00 50 04 89 34 a2
[TCP Segment Len: 0]		0030 16 d0 77 4d 00 00 02 04
Sequence Number: 0 (relative sequence number)		
Sequence Number (raw): 883061785		
[Next Sequence Number: 1 (relative sequence number)]		
Acknowledgment Number: 1 (relative ack number)		
Acknowledgment number (raw): 232129013		
0111 = Header Length: 28 bytes (7)		
Flags: 0x012 (SYN, ACK)		
Window: 5840		
[Calculated window size: 5840]		

6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

Answer :-

According to above figure, the segment No.4 contains the HTTP POST command, the sequence number of this segment is 1.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565 Source Port: 1161 Destination Port: 80 [Stream index: 0] [Conversation completeness: Incomplete, DATA (15)] [TCP Segment Len: 565] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 232129013 [Next Sequence Number: 566 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 883061786 0101 = Header Length: 20 bytes (5) Flags: 0x018 (PSH, ACK) 000. = Reserved: Not set ...0 = Accurate ECN: Not set 0... = Congestion Window Reduced: Not set 0.. = ECN-Echo: Not set0. = Urgent: Not set1 = Acknowledgment: Set1 = Push: Set0 = Reset: Not set0 = Syn: Not set	0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 0070 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0080 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 0090 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 00a0 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 00b0 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 00c0 2e 32 29 20 47 65 63 6b 6f 2f 32 30 30 00d0 30 38 20 4e 65 74 73 63 61 70 65 78 7a 00e0 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 00f0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 0100 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 0110 68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 0120 6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 0130 61 69 6e 3b 71 3d 30 2e 38 2c 76 69 64 0140 78 2d 6d 6e 67 2c 69 6d 63 61 74 69 6f 0150 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 0160 2f 67 69 66 3b 71 3d 30 2e 32 2c 74 65 0170 63 73 73 2c 2a 2f 2a 3b 71 3d 30 2e 31 0180 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 0190 65 6e 2d 75 73 2c 20 65 6e 3b 71 3d 30
---	--

No.	Time	Source	Destination	Protocol	Length	Info
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of

.... ..1 = Push: Set0 = Reset: Not set0 = Syn: Not set0 = Fin: Not set [TCP Flags:AP..] Window: 17520 [Calculated window size: [Window size scaling fact Checksum: 0x1fbd [unverif [Checksum Status: Unverif Urgent Pointer: 0	0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18 0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 2f 0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e 0070 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 55 73 0080 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 0090 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 00a0 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 00b0 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 30 00c0 2e 32 29 20 47 65 63 6b 6f 2f 32 30 30 33 30 32 00d0 30 38 20 4e 65 74 73 63 61 70 65 2f 37 2e 30 32P...4..t..P Dp...PO ST /ethe real-lab s/lab3-1 -reply.h tm HTTP/ 1.1..Hos t: gaia. cs.umass .edu..Us er-Agent : Mozill a/5.0 (W indows; U; Windo ws NT 5. 1; en-US ; rv:1.0 .2) Gecko o/200302 08 Netsc ape/7.02
--	--	--

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value (see Section 3.5.3, page 242 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.

Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Then select: *Statistics->TCP Stream Graph- >Round Trip Time Graph.*

At what time was each segment sent? When was the ACK for each segment received?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0

Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 566, Len: 0
 Source Port: 80
 Destination Port: 1161
 [Stream index: 0]
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 883061786
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 566 (relative ack number)
 Acknowledgment number (raw): 232129578
 0101 = Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 000. = Reserved: Not set
 ...0 = Accurate ECN: Not set
0 = Congestion Window Reduced: Not set
0 = ECN-Echo: Not set
0 = Urgent: Not set

Syn (tcp.flags.syn), 1 byte

Packets: 213 • Displayed: 202 (94.8%)

Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0

Sequence Number: 566 (relative sequence number)
 Sequence Number (raw): 232129578
 [Next Sequence Number: 2026 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 883061786
 0101 = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 000. = Reserved: Not set
 ...0 = Accurate ECN: Not set
0 = Congestion Window Reduced: Not set

0000 00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00 ..%.s. .p...E-
 0010 05 dc 1e 22 40 00 80 06 9f 67 c0 a8 01 66 80 77 ..."@... g...f-w
 0020 f5 0c 04 89 00 50 0d d6 04 2a 34 a2 74 1a 50 18P... .*4.t.P
 0030 44 70 3b e5 00 00 43 6f 6e 74 65 6e 74 2d 54 79 Dp;...Co ntent-Ty
 0040 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f pe; mult ipart/fo
 0050 72 6d 2d 64 61 74 61 3b 20 62 6f 75 6e 64 61 72 rm-data; boundar
 0060 79 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d y=-----
 0070 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 36 35 -----265
 0080 30 30 31 39 31 36 39 31 35 37 32 34 0d 0a 43 6f 00191691 5724..Co
 0090 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 36 ntent-Le ngth: 16
 00a0 33 34 31 31 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 3411....-----

Segments 1-6

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reasse
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a re
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a r
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a r
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
19	0.305813	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
20	0.306692	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=11933 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
21	0.307571	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=13393 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
22	0.308699	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=14853 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
23	0.309553	192.168.1.102	128.119.245.12	TCP	946	1161 → 80 [PSH, ACK] Seq=16313 Ack=1 Win=17520 Len=892 [TCP segment of a r
24	0.356437	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=10473 Win=26280 Len=0

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12				0020	f5 0c 04 89 00 50 0d d6	04 2a 34 a2 74 1a 50 18P...*4-t-P.
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 566, Ack:				0030	44 70 3b e5 00 00 43 6f	6e 74 65 6e 74 2d 54 79	Dp;...Co ntent-Ty
Source Port: 1161				0040	70 65 3a 20 6d 75 6c 74	69 70 61 72 74 2f 66 6f	pe: mult ipart/fo
Destination Port: 80				0050	72 6d 2d 64 61 74 61 3b	20 62 6f 75 6e 64 61 72	rm-data; boundar
[Stream index: 0]				0060	79 3d 2d 2d 2d 2d 2d 2d	2d 2d 2d 2d 2d 2d 2d 2d	y=-----
[Conversation completeness: Incomplete, DATA (15)]				0070	2d 2d 2d 2d 2d 2d 2d 2d	2d 2d 2d 2d 2d 2d 32 36 35	-----265
[TCP Segment Len: 1460]				0080	30 30 31 39 31 36 39 31	35 37 32 34 0d 0a 43 6f	00191691 5724..Co
Sequence Number: 566 (relative sequence number)				0090	6e 74 65 6e 74 2d 4c 65	6e 67 74 68 3a 20 31 36	ntent-Le ngth: 16
Sequence Number (raw): 232129578				00a0	33 34 31 31 0d 0a 0d 0a	2d 2d 2d 2d 2d 2d 2d 2d	3411....
[Next Sequence Number: 2026 (relative sequence number)]				00b0	2d 2d 2d 2d 2d 2d 2d 2d	2d 2d 2d 2d 2d 2d 2d 2d	-----
Acknowledgment Number: 1 (relative ack number)				00c0	2d 2d 2d 2d 2d 2d 36 35	30 30 31 39 31 36 39 31	-----265 00191691
Acknowledgment number (raw): 883061786				00d0	35 37 32 34 0d 0a 43 6f	6e 74 65 6e 74 2d 44 69	5724..Co ntent-Di
				00e0	73 70 6f 73 69 74 69 6f	6e 3a 20 66 6f 72 6d 2d	spositio n: form-
				00f0	64 61 74 61 3b 20 6e 61	6d 65 3d 22 66 69 6c 65	data; na me="file

No.	Time	Source	Destination	Protocol	Length	Info
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
12	0.124085	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201	1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a r
14	0.169118	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
19	0.305813	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460 [TCP segment of a reass
20	0.306692	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=11933 Ack=1 Win=17520 Len=1460 [TCP segment of a reass
21	0.307571	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=13393 Ack=1 Win=17520 Len=1460 [TCP segment of a reass
22	0.308699	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=14853 Ack=1 Win=17520 Len=1460 [TCP segment of a reass
23	0.309553	192.168.1.102	128.119.245.12	TCP	946	1161 → 80 [PSH, ACK] Seq=16313 Ack=1 Win=17520 Len=892 [TCP segment of a r
24	0.356437	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=10473 Win=26280 Len=0

0101 = Header Length: 20 bytes (5)	0020 f5 0c 04 89 00 50 0d d6 15 46 34 a2 74 1a 0c 10P...F4-t...
Flags: 0x010 (ACK)	0030 44 70 90 8e 00 00 6f 66 20 62 6f 6f 6b 73 0d 0a Dp...of books...
000. = Reserved: Not set	0040 61 6e 64 0d 0a 47 45 54 20 4e 45 57 20 47 55 54 and...GET NEW GUT
...0 = Accurate ECN: Not set	0050 20 66 6f 72 20 67 65 6e 65 72 61 6c 20 69 6e 66 for gen eral inf
....0 = Congestion Window Reduced: Not set	0060 6f 72 6d 61 74 69 6f 6e 0d 0a 61 6e 64 0d 0a 4d ormation ...and...M
....0 = ECN-Echo: Not set	0070 47 45 54 20 47 55 54 2a 20 66 6f 72 20 6e 65 77 GET GUT* for new
....1 = Urgent: Not set	0080 73 6c 65 74 74 65 72 73 2e 0d 0a 0d 0a 2a 2a 49 sletters**I
....1 = Acknowledgment: Set	0090 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 72 65 70 61 nformati on prepa
....0 = Push: Not set	00a0 72 65 64 20 62 79 20 74 68 65 20 50 72 6f 6a 65 red by t he Proje
....0 = Reset: Not set	00b0 63 74 20 47 75 74 65 6e 62 65 72 67 20 6c 65 67 ct Guten berg leg
....0 = Syn: Not set	00c0 61 6c 20 61 64 76 69 73 6f 72 2a 2a 0d 0a 28 54 al advis or***..(T
....0 = Fin: Not set	00d0 68 72 65 65 20 50 61 67 65 73 29 0d 0a 0d 0a 0d hree Pag es).....
	00e0 0a 2a 2a 2a 53 54 41 52 54 2a 2a 54 48 45 20 53 ***STAR T**THE S
	00f0 4d 41 4c 4c 20 50 52 49 4e 54 21 2a 2a 46 4f 52 MALL PRI NT!**FOR

ACK of segments 1-6

According to above figures, the segments 1-6 are No. 4,5,7,8,10 and 11. The ACK of segments 1-6 are No. 6,9,12,14,15,16 and 17.

Segment 1 sequence number is 1
Segment 2 sequence number is 566
Segment 3 sequence number is 2026
Segment 4 sequence number is 3486
Segment 5 sequence number is 4946
Segment 6 sequence number is 6406

Recording the sending time and received time of ACKs:

Segments no	Sent time	ACK received time	RTT
Segment 1	0.026477	0.053937	0.02746
Segment 2	0.041737	0.077294	0.035557
Segment 3	0.054026	0.124085	0.070059
Segment 4	0.054690	0.169118	0.114428
Segment 5	0.077405	0.217299	0.139894
Segment 6	0.078157	0.267802	0.189645

According to the formula:

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

EstimatedRTT after the receipt of the ACK of segment 1:

$$\text{EstimatedRTT} = \text{RTT for Segment 1} = 0.02746 \text{ s}$$

EstimatedRTT after the receipt of the ACK of segment 2:

$$\text{EstimatedRTT} = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.028472125 \text{ s}$$

EstimatedRTT after the receipt of the ACK of segment 3:

$$\text{EstimatedRTT} = 0.875 * 0.02847125 + 0.125 * 0.070059 = 0.0336704844 \text{ s}$$

EstimatedRTT after the receipt of the ACK of segment 4:

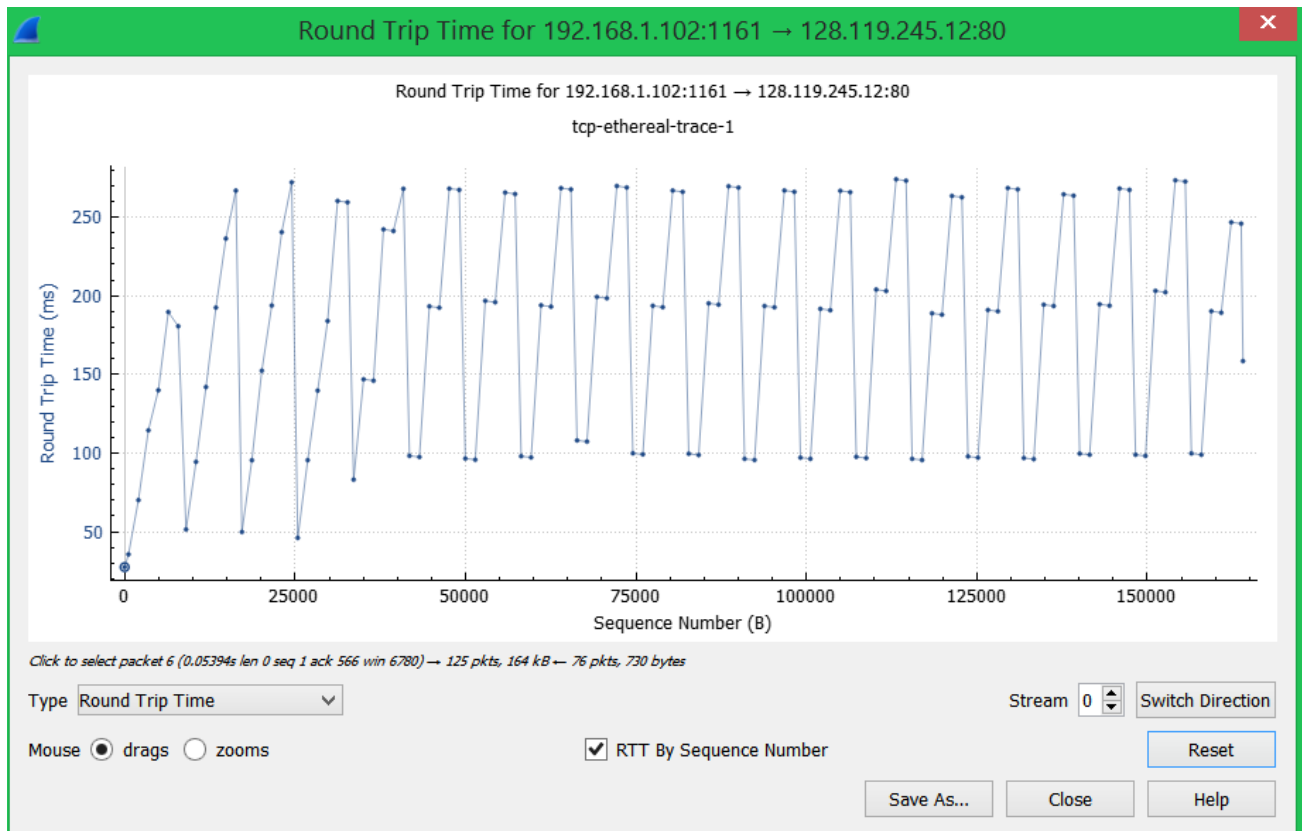
$$\text{EstimatedRTT} = 0.875 * 0.0336704844 + 0.125 * 0.114428 = 0.0437651738 \text{ s}$$

EstimatedRTT after the receipt of the ACK of segment 5:

$$\text{EstimatedRTT} = 0.875 * 0.0437651738 + 0.125 * 0.139894 \text{ s} = 0.0557812771 \text{ s}$$

EstimatedRTT after the receipt of the ACK of segment 6:

$$\text{EstimatedRTT} = 0.875 * 0.0557812771 + 0.125 * 0.189645 = 0.0725142425 \text{ s}$$



8. What is the length of each of the first six TCP segments?

1st segment length :-

565 bytes

4	0.026477	192.168.1.102	128.119.245.12	TCP	619 1161 → 80	[PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reasse
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a re
6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161	[ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse

.... 1... = Push: Set	0020 f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74
.... .0.. = Reset: Not set	0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 63
.... .0. = Syn: Not set	0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62
.... .0 = Fin: Not set	0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54
[TCP Flags:AP...]	0060 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 63
Window: 17520	0070 63 73 2e 75 6d 61 73 73 2e 65 64 75 00
[Calculated window size: 17520]	0080 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 72
[Window size scaling factor: -2 (no window scaling used)]	0090 61 2f 35 2e 30 20 28 57 69 6e 04 6f 72
Checksum: 0x1fbd [unverified]	00a0 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54
[Checksum Status: Unverified]	00b0 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3d
Urgent Pointer: 0	00c0 2e 32 29 20 47 65 63 6b 6f 2f 32 30 30
▲ [Timestamps]	00d0 30 38 20 4e 65 74 73 63 61 70 65 2f 32
[Time since first frame in this TCP stream: 0.026477000 seconds]	00e0 0d 0a 41 63 63 65 70 74 3a 20 74 65 70
[Time since previous frame in this TCP stream: 0.003212000 seconds]	00f0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f
▲ [SEQ/ACK analysis]	0100 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f
[iRTT: 0.023265000 seconds]	0110 68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74
[Bytes in flight: 565]	0120 6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74
[Bytes sent since last PSH flag: 565]	0130 61 69 6e 3b 71 3d 30 2e 39 2c 76 69 6d
TCP payload (565 bytes)	0140 78 2d 6d 6e 67 2c 69 6d 61 67 65 2f 70
[Reassembled PDU in frame: 199]	0150 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d
TCP segment data (565 bytes)	0160 2f 67 69 6e 3b 71 3d 30 2e 32 2c 74 65
	0170 63 73 73 2c 2a 2f 2a 3b 71 3d 30 2e 33
	0180 63 63 65 70 74 3d 45 61 60 63 75 61 63

2nd segment length :-

1460 bytes

No.	Time	Source	Destination	Protocol	Length	Info
2	0.023172	128.119.245.12	192.168.1.102	TCP	62 80 → 1161	[SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3	0.023265	192.168.1.102	128.119.245.12	TCP	54 1161 → 80	[ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.026477	192.168.1.102	128.119.245.12	TCP	619 1161 → 80	[PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reasse
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a re
6	0.053937	128.119.245.12	192.168.1.102	TCP	60 80 → 1161	[ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 → 80	[ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse

.... 1... = Push: Set	0020 f5 0c 04 89 00 50 0d d6 0a 2a 34 a2 74
.... .0.. = Reset: Not set	0030 44 70 3b e5 00 00 43 6f 6e 74 65 6e 74
.... .0. = Syn: Not set	0040 70 65 3a 20 6d 75 6c 74 69 70 61 72 74
.... .0 = Fin: Not set	0050 72 6d 2d 64 61 74 61 3b 20 62 6f 75 6e
[TCP Flags:AP...]	0060 79 3d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
Window: 17520	0070 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
[Calculated window size: 17520]	0080 30 30 31 39 31 36 39 31 35 37 32 34 00
[Window size scaling factor: -2 (no window scaling used)]	0090 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3d
Checksum: 0x3be5 [unverified]	00a0 33 34 31 31 0d 0a 0d 0a 2d 2d 2d 2d 2d
[Checksum Status: Unverified]	00b0 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
Urgent Pointer: 0	00c0 2d 2d 2d 2d 2d 32 36 35 30 30 31 39 33
▲ [Timestamps]	00d0 35 37 32 34 0d 0a 43 6f 6e 74 65 6e 74
[Time since first frame in this TCP stream: 0.041737000 seconds]	00e0 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f
[Time since previous frame in this TCP stream: 0.015260000 seconds]	00f0 64 61 74 61 3b 20 6e 61 6d 65 3d 22 60
▲ [SEQ/ACK analysis]	0100 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22
[iRTT: 0.023265000 seconds]	0110 63 65 2e 74 78 74 22 8d 9a 43 6f 6e 74
[Bytes in flight: 2025]	0120 2d 54 79 70 65 3a 20 74 65 79 74 2f 70
[Bytes sent since last PSH flag: 1460]	0130 6e 0d 0a 0d 0a 2a 2a 2a 54 68 69 73 20
TCP payload (1460 bytes)	0140 74 68 65 20 50 72 6f 6a 65 63 74 20 47
[Reassembled PDU in frame: 199]	0150 6e 62 65 72 67 20 45 74 65 78 74 20 6f
TCP segment data (1460 bytes)	0160 6c 69 63 65 20 69 6e 20 57 6f 6e 64 65
	0170 6e 64 2a 2a 2a 0d 0a 2a 54 68 69 73 2d
	0180 60 20 65 64 60 20 67 60 70 70 6f 6e 74

3rd segment length :-

1468 bytes

▲ [SEQ/ACK analysis]	0120 68 65 61 64 20 65 76 65 72 79 20 6d 61
[iRTT: 0.023265000 seconds]	0130 20 61 66 74 65 72 20 74 68 61 74 2e 0c
[Bytes in flight: 2920]	0140 50 6c 65 61 73 65 20 6e 6f 74 65 3a 26
[Bytes sent since last PSH flag: 1460]	0150 69 74 68 65 72 20 74 68 69 73 20 6c 6e
TCP payload (1460 bytes)	0160 6e 6f 72 20 69 74 73 20 63 6f 6e 74 65
[Reassembled PDU in frame: 199]	0170 20 61 72 65 20 66 69 6e 61 6c 20 74 65
TCP segment data (1460 bytes)	0180 60 64 60 64 60 67 60 70 70 6f 6e 74

1460 bytes

0120	06	05	75	20	09	75	20	74	05	08	20	74	06
0120	61	66	64	20	74	69	74	66	65	73	20	65	61
0130	74	66	20	67	66	65	20	68	75	66	64	72	65
0140	69	66	66	69	66	66	20	72	65	61	64	65	73
0150	0a	77	68	69	63	68	20	69	73	20	31	30	21
0160	20	74	68	65	20	65	78	70	63	67	74	65	64
0170	6d	62	65	72	20	67	66	20	63	67	6d	70	75
0180	20	75	73	65	73	73	20	63	70	20	74	69	65

1460 bytes

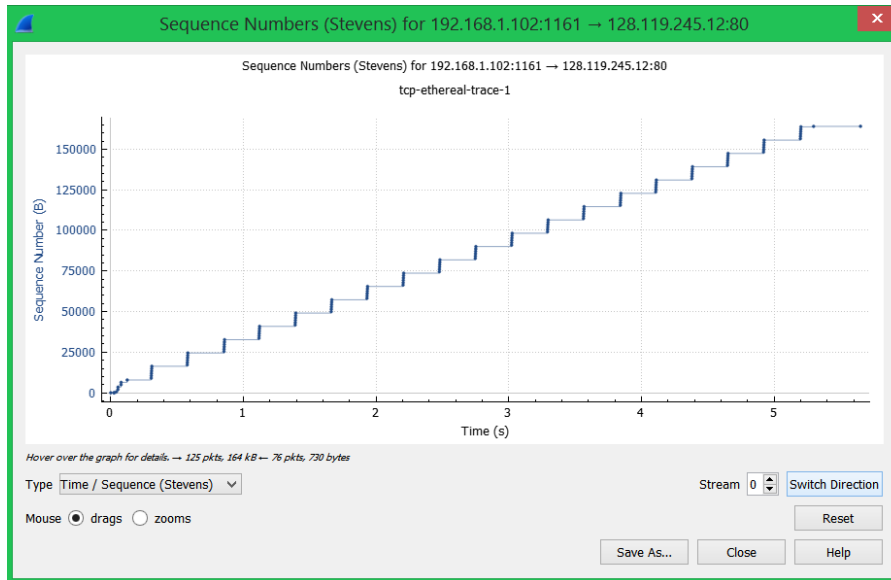
0110	0a	45	38	79	20	69	73	20	68	69	73	20	68	69	73	20
0120	0a	57	68	79	20	69	73	20	68	69	73	20	68	69	73	20
0130	61	6c	6c	65	50	72	69	6e	74	21	62	20	73	20	68	69
0140	65	6d	65	20	68	72	60	68	65	72	65	3f	20	73	20	68
0150	20	6b	6e	6f	77	3a	20	6c	61	67	77	79	65	73	20	68
0160	0a	54	68	65	79	70	74	65	6c	73	65	20	75	73	20	68
0170	75	20	6d	69	67	68	74	20	6c	73	75	65	20	75	73	20
0180	65	20	74	69	65	73	65	20	60	73	20	73	20	68	69	73

0110	74	66	75	20	65	68	20	73	61	75	20	77	65
0120	70	67	63	20	63	70	79	20	61	66	64	20	64
0130	72	69	62	75	74	65	20	74	68	69	73	20	65
0140	74	0d	0a	75	6e	64	65	72	20	74	68	65	2e
0150	6a	65	63	74	27	73	20	22	50	52	4f	4a	4e
0160	47	55	54	45	4e	42	45	52	47	22	20	74	77
0170	6d	61	72	6b	2e	0d	0a	0d	54	56	20	6b	7e
0180	74	65	20	74	68	65	73	65	20	65	74	65	7e

```
0020 f5 0c 04 89 00 50 0d d6
0030 40 00 f6 e9 00 00 02 04
```

This reviver window grows until it reaches the maximum receiver buffer size of 62780 bytes. According to the trace, the sender is never throttled due to lacking of receiver buffer space.

35



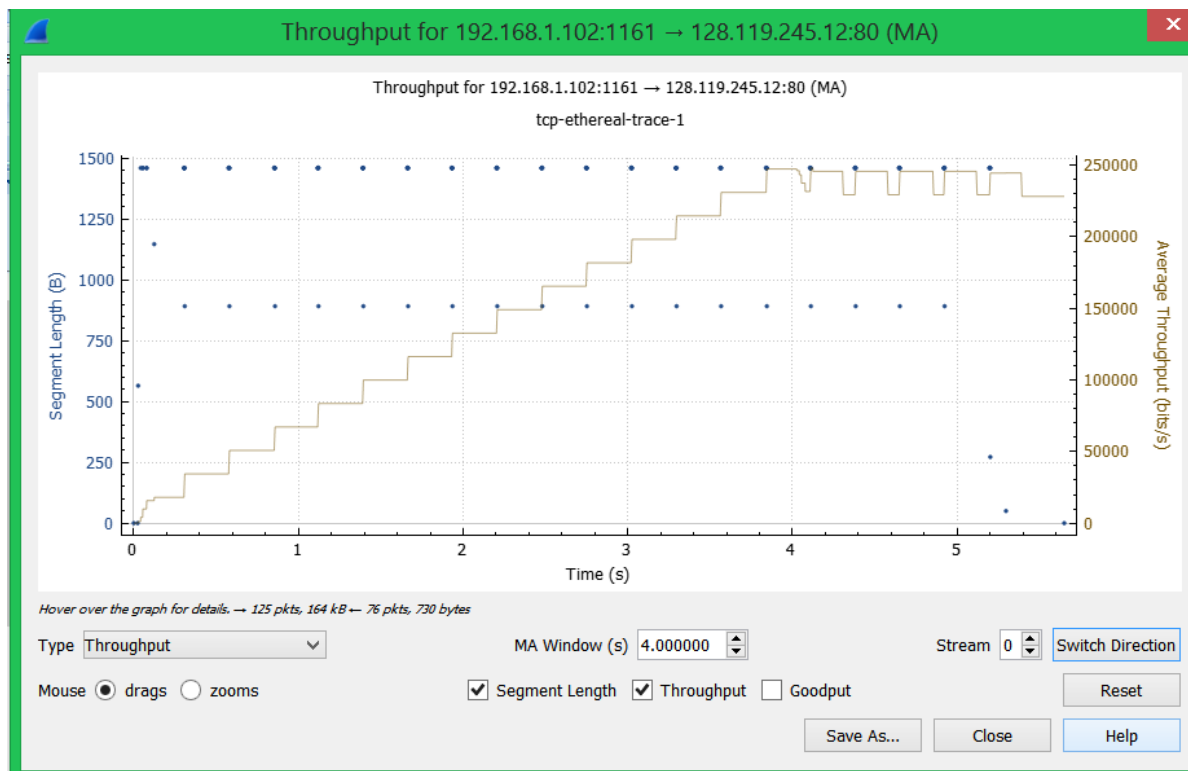
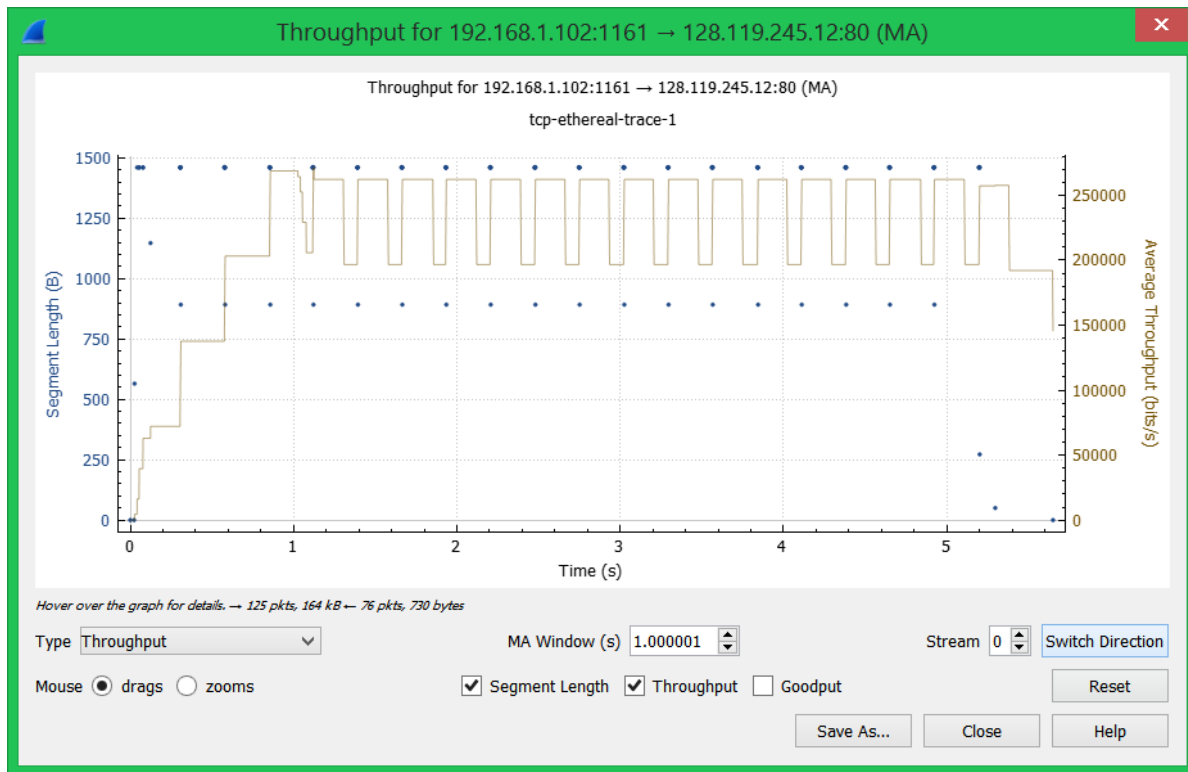
11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).

7	0.054026	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
9	0.077294	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
12	0.124085	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13	0.124185	192.168.1.102	128.119.245.12	TCP	1201 1161 -> 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a r
14	0.169118	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15	0.217299	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16	0.267802	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17	0.304807	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18	0.305040	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
19	0.305813	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
20	0.306692	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=11933 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
21	0.307571	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=13393 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
22	0.308699	192.168.1.102	128.119.245.12	TCP	1514 1161 -> 80 [ACK] Seq=14853 Ack=1 Win=17520 Len=1460 [TCP segment of a reasse
23	0.309553	192.168.1.102	128.119.245.12	TCP	946 1161 -> 80 [PSH, ACK] Seq=16313 Ack=1 Win=17520 Len=892 [TCP segment of a r
24	0.356437	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=10473 Win=26280 Len=0
25	0.400164	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=11933 Win=29200 Len=0
26	0.448613	128.119.245.12	192.168.1.102	TCP	60 80 -> 1161 [ACK] Seq=1 Ack=13393 Win=32120 Len=0

The difference between the acknowledged sequence numbers of two consecutive ACKs indicates the data received by the server between these two ACKs. The receiver is ACKing every other segment. For example, segment of No. 13 acknowledged data with 1460 bytes.

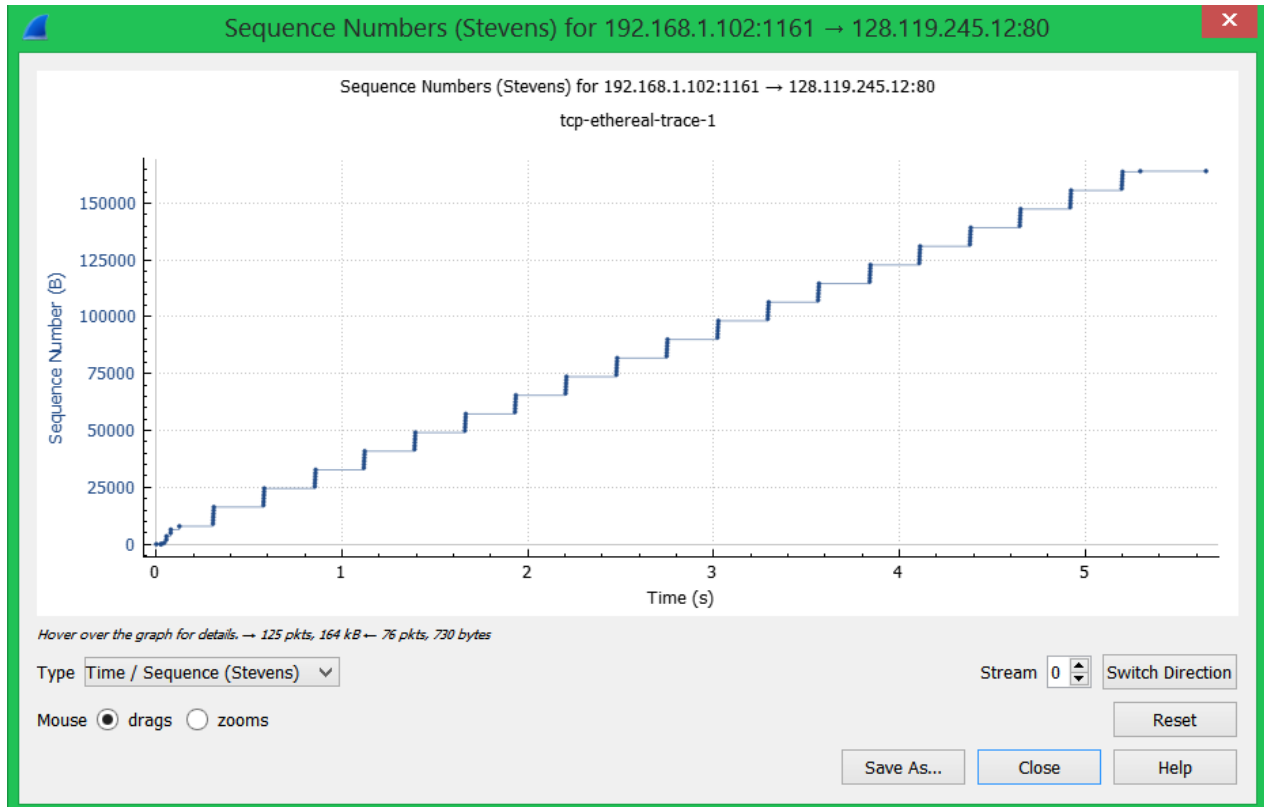
12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

The alice.txt on the hard drive is 152,138 bytes, and the download time is 1.578736000 (First TCP segment) - 0.026477 (last ACK) = 1.552259 second. Therefore, the throughput for the TCP connection is computed as 152,138/1.552259=98010.7056876462 bytes/second.



13. Use the *Time-Sequence-Graph(Stevens)* plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.

The slow start of the TCP seems to begin at about 0 seconds and then ends at about 0.17 seconds. Congestion avoidance takes over at about 0.52 seconds because it cut down the amount being sent.



14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

