School of Electrical and Electronic of Enginnering
eee 4474-01 : Experiments on Communication Networks
2조 2016142096 **조윤신** 2017142043 **김재민**

Result Report Week 1

Introduction to Wireshark

1 Experiment 1 : Getting Started

1.a Running Wireshark

Experiment Results

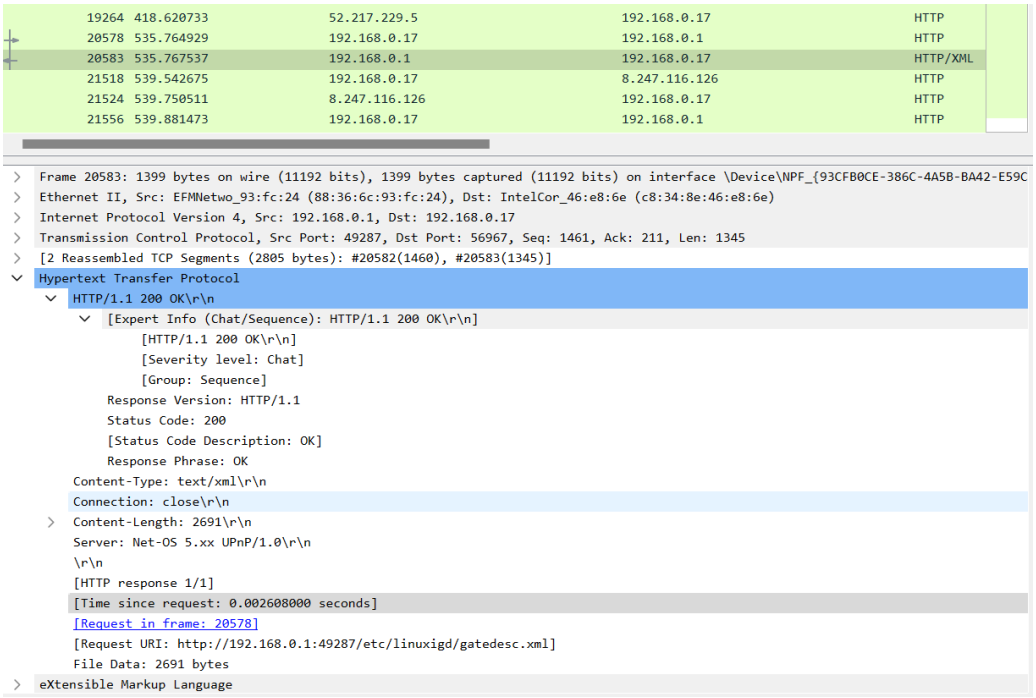


Figure 1: Wireshark Screenshot : Running Wireshark

Questions

Problem 1: List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
Answer TCP, DNS, TLSV

Problem 2: How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
Answer

Problem 3: What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?
Answer

Problem 4: Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

Answer

```
C:₩Users₩815ys₩OneDrive₩Yonsei₩2022 2학기₩2022-2 Team Project Management₩2022-2_네실₩2022-2 experiments on communication network₩Material₩week01₩week

No.     Time           Source                Destination           Protocol Length Info
  20583 535.767537     192.168.0.1           192.168.0.17          HTTP/XML 1399   HTTP/1.1 200 OK
Frame 20583: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits) on interface
\Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
Ethernet II, Src: EFMNetwo_93:fc:24 (88:36:6c:93:fc:24), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.17
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1385
    Identification: 0x16fb (5883)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9d31 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.17
Transmission Control Protocol, Src Port: 49287, Dst Port: 56967, Seq: 1461, Ack: 211, Len: 1345
[2 Reassembled TCP Segments (2805 bytes): #20582(1460), #20583(1345)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Content-Type: text/xml\r\n
    Connection: close\r\n
    Content-Length: 2691\r\n
    Server: Net-OS 5.xx UPnP/1.0\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.002608000 seconds]
    [Request in frame: 20578]
    [Request URI: http://192.168.0.1:49287/etc/linuxigd/gatedesc.xml]
    File Data: 2691 bytes
eXtensible Markup Language
```

Figure 2: Printed HTTP messages

2 Experiment 2 : HTTP

2.a HTTP : The Basic HTTP GET/response interaction

Experiment Results

No.	Time	Source	Destination	Protocol	Length	Info
440	4.308656	172.20.10.10	128.119.245.12	HTTP	662	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
479	4.557030	128.119.245.12	172.20.10.10	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 3: Lists of captured packet in the basic HTTP GET/response interaction experiment

```
No.     Time           Source                Destination           Protocol Length Info
    440 4.308656       172.20.10.10          128.119.245.12        HTTP     662    GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1
Frame 440: 662 bytes on wire (5296 bits), 662 bytes captured (5296 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-
BA42-E59C448690C9}, id 0
Ethernet II, Src: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e), Dst: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64)
Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59743, Dst Port: 80, Seq: 1, Ack: 1, Len: 608
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\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/104.0.0.0
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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
    If-None-Match: "80-5e80fe5d89731"\r\n
    If-Modified-Since: Wed, 07 Sep 2022 05:51:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 479]
```

(a) 662 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

```
No.     Time           Source                Destination           Protocol Length Info
    479 4.557030       128.119.245.12        172.20.10.10          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 479: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-
BA42-E59C448690C9}, id 0
Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
Transmission Control Protocol, Src Port: 80, Dst Port: 59743, Seq: 1, Ack: 609, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 07 Sep 2022 07:56:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    ETag: "80-5e810026d849b"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.248374000 seconds]
    [Request in frame: 440]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

(b) 243 HTTP/1.1 304 helloworld.c - adau1761_init function

Figure 4: The Basic HTTP GET/response interaction Experiments results screenshot

Questions

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

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

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

Problem 4: What is the status code returned from the server to your browser?
Answer

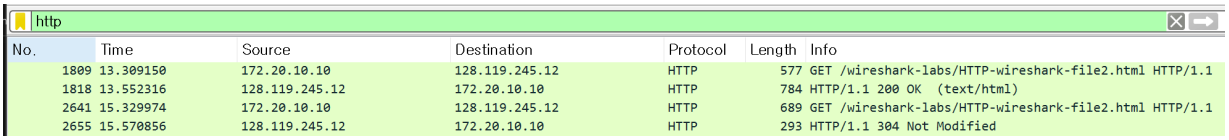
Problem 5: When was the HTML file that you are retrieving last modified at the server?
Answer

Problem 6: How many bytes of content are being returned to your browser?
Answer

Problem 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

2.b HTTP : The HTTP CONDITIONAL GET/response interaction

Experiment Results



http

No.	Time	Source	Destination	Protocol	Length	Info
1809	13.309150	172.20.10.10	128.119.245.12	HTTP	577	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1818	13.552316	128.119.245.12	172.20.10.10	HTTP	784	HTTP/1.1 200 OK (text/html)
2641	15.329974	172.20.10.10	128.119.245.12	HTTP	689	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2655	15.570856	128.119.245.12	172.20.10.10	HTTP	293	HTTP/1.1 304 Not Modified

Figure 5: Lists of captured packet in the HTTP CONDITIONAL GET/response interaction experiment

```
No.     Time           Source                Destination           Protocol Length Info
   2655 15.570856      128.119.245.12        172.20.10.10          HTTP     293    HTTP/1.1 304 Not Modified
Frame 2655: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-
BA42-E59C448690C9}, id 0
Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
Transmission Control Protocol, Src Port: 80, Dst Port: 58062, Seq: 731, Ack: 1159, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Wed, 07 Sep 2022 13:13:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5e810026d78e3"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.240882000 seconds]
    [Prev request in frame: 1809]
    [Prev response in frame: 1818]
    [Request in frame: 2641]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

(a) Experiment 2.b : GET wire shark labs wireshark file 2

```
No.     Time           Source                Destination           Protocol Length Info
   1818 13.552316      128.119.245.12        172.20.10.10          HTTP     784    HTTP/1.1 200 OK  (text/html)
Frame 1818: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-
BA42-E59C448690C9}, id 0
Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
Transmission Control Protocol, Src Port: 80, Dst Port: 58062, Seq: 1, Ack: 524, Len: 730
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: Wed, 07 Sep 2022 13:13:35 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    ETag: "173-5e810026d78e3"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.243166000 seconds]
    [Request in frame: 1809]
    [Next request in frame: 2641]
    [Next response in frame: 2655]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
```

(b) Experiment 2.b : http 1.1 200 OK

```
No.     Time           Source                Destination           Protocol Length Info
   2641 15.329974      172.20.10.10          128.119.245.12        HTTP     689    GET /wireshark-labs/HTTP-wireshark-
file2.html HTTP/1.1
Frame 2641: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-
BA42-E59C448690C9}, id 0
Ethernet II, Src: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e), Dst: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64)
Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58062, Dst Port: 80, Seq: 524, Ack: 731, Len: 635
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        Request Method: GET
        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/104.0.0.0
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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
    If-None-Match: "173-5e810026d78e3"\r\n
    If-Modified-Since: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 1809]
    [Response in frame: 2655]
```

(c) Experiment 2.b : GET wire shark labs wireshark file 2

Questions

Problem 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

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

Problem 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

```
No.     Time           Source                Destination           Protocol Length Info
   2655 15.570856      128.119.245.12        172.20.10.10          HTTP     293    HTTP/1.1 304 Not Modified
Frame 2655: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-
BA42-E59C448690C9}, id 0
Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
Transmission Control Protocol, Src Port: 80, Dst Port: 58062, Seq: 731, Ack: 1159, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Wed, 07 Sep 2022 13:13:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5e810026d78e3"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.240882000 seconds]
    [Prev request in frame: 1809]
    [Prev response in frame: 1818]
    [Request in frame: 2641]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

(d) Experiment 2.b : http 1.1 304 not modified

the “IF-MODIFIED-SINCE:” header?
Answer

Problem 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

2.c HTTP : Retrieving Long Documents

Experiment Results
Questions

Problem 12: How many HTTP GET request messages did your browser send?
Answer

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

Problem 14: What is the status code and phrase in the response?
Answer

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

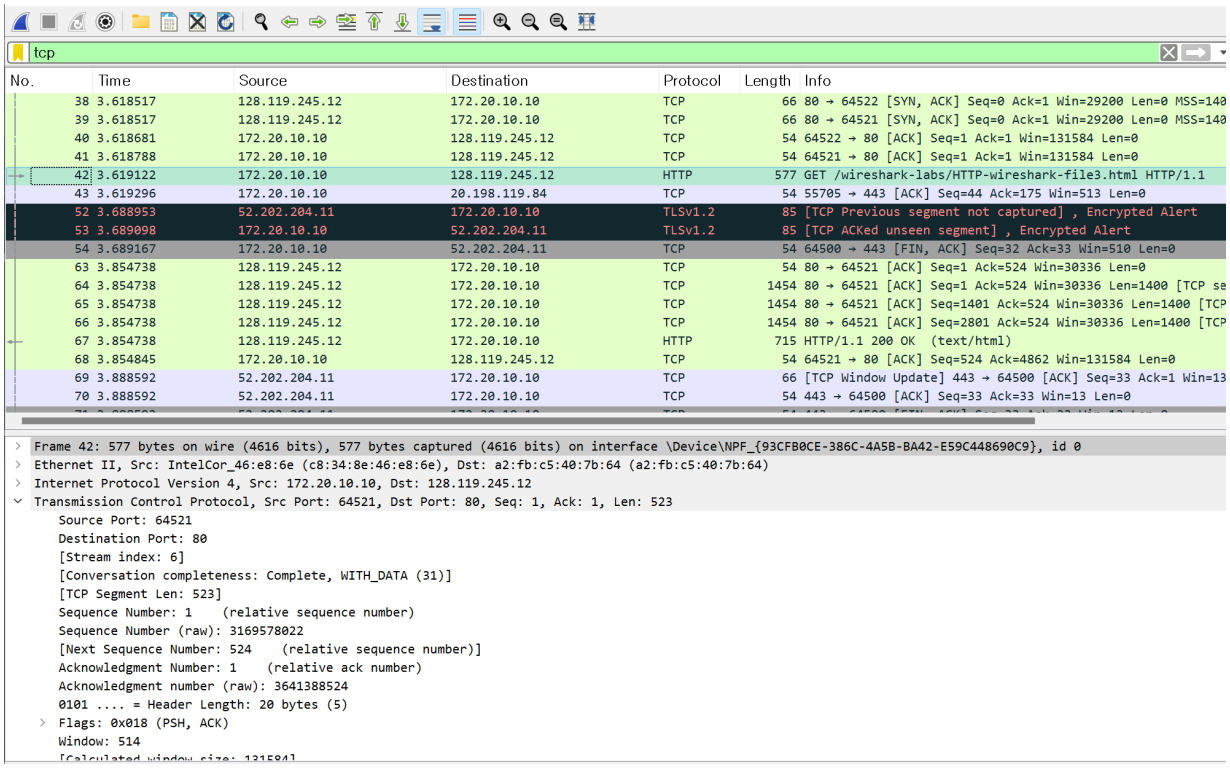


Figure 6: Wireshark Screenshot

3 Experiment 3 : DNS

3.a DNS : Traing DNS with Wireshark #1

Experiment Results

Figure 7: Wireshark Screenshot

Questions

Problem 1: Locate the DNS query and response messages. Are then sent over UDP or TCP?
Answer

Problem 2: What is the destination port for the DNS query message? What is the source port of DNS response message?
Answer

Problem 3: To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
Answer

Problem 4: Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
Answer

Problem 5: Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
Answer

Problem 6: Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer

Problem 7: This web page contains images. Before retrieving each image, does your host issue new DNS queries?
Answer

3.b DNS : Traing DNS with Wireshark #2

Experiment Results

Figure 8: Wireshark Screenshot

Questions

Problem 8: What is the destination port for the DNS query message? What is the source port of DNS response message?
Answer

Problem 9: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
Answer

Problem 10: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
Answer

Problem 11: Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
Answer

3.c DNS : Traing DNS with Wireshark #3

Experiment Results

Figure 9: Wireshark Screenshot

Questions

Problem 12: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
Answer

Problem 13: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
Answer

Problem 14: Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?
Answer

Figure 10: Wireshark Screenshot

3.d DNS : Traing DNS with Wireshark #4

Experiment Results
Questions

Problem 15: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
Answer

Problem 16: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
Answer

Problem 17: Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
Answer