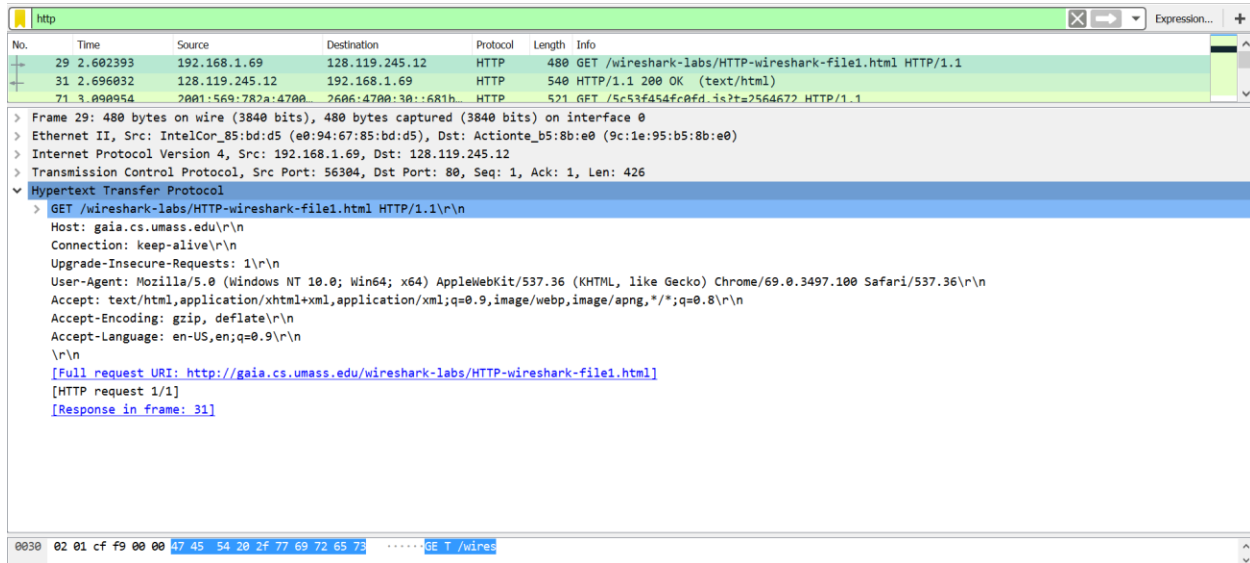


ELEC 331 Assignment 1

Basic HTTP GET/response interaction

GET Request

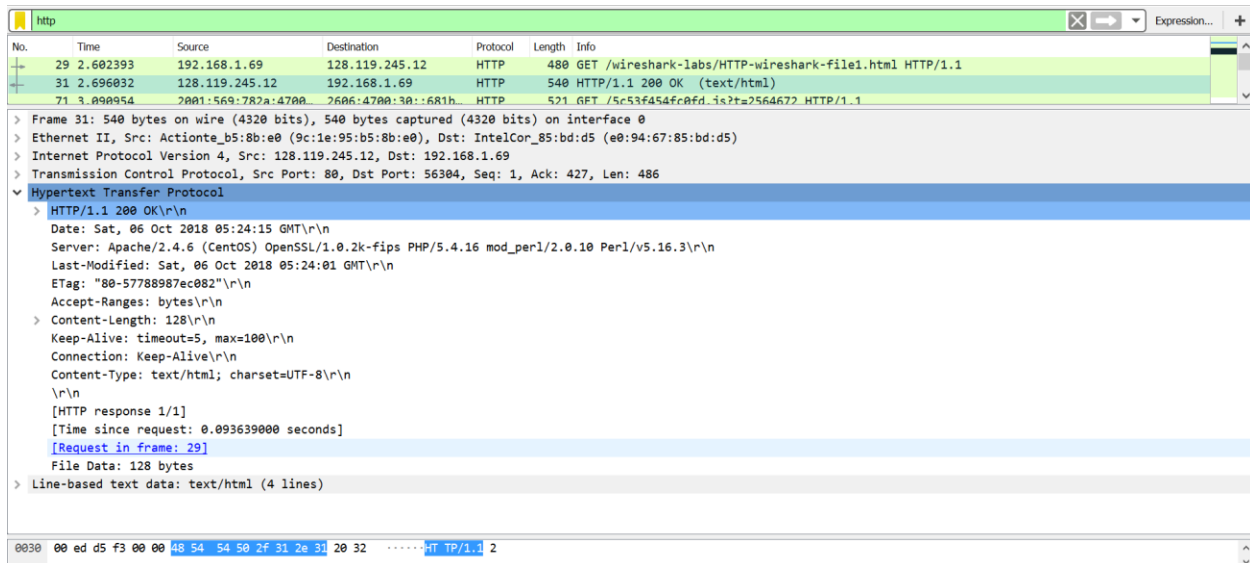


The screenshot shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows three packets: a GET request (No. 29), a 200 OK response (No. 31), and a GET request for a different resource (No. 71). The packet details pane for packet 29 is expanded, showing the Hypertext Transfer Protocol section. The request line is 'GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1'. The Host header is 'gaia.cs.umass.edu'. The User-Agent header is 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36'. The Accept header is 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8'. The Accept-Encoding header is 'gzip, deflate'. The Accept-Language header is 'en-US,en;q=0.9'. The packet bytes pane at the bottom shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
29	2.602393	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
31	2.696032	128.119.245.12	192.168.1.69	HTTP	540	HTTP/1.1 200 OK (text/html)
71	3.090954	2001:569:782a:470a::26a6:470a:30::681h	26a6:470a:30::681h	HTTP	521	GET /5c53f454f80fd.is?t=2564672 HTTP/1.1

Frame 29: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56304, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
> 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/69.0.3497.100 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9\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: 31]

GET Response



The screenshot shows a Wireshark packet capture of an HTTP 200 OK response. The packet list on the left shows the same three packets as the previous screenshot. The packet details pane for packet 31 is expanded, showing the Hypertext Transfer Protocol section. The status line is 'HTTP/1.1 200 OK'. The Date header is 'Sat, 06 Oct 2018 05:24:15 GMT'. The Server header is 'Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3'. The Last-Modified header is 'Sat, 06 Oct 2018 05:24:01 GMT'. The ETag header is '"00-57788987ec082"'. The Accept-Ranges header is 'bytes'. The Content-Length header is '128'. The Keep-Alive header is 'timeout=5, max=100'. The Connection header is 'Keep-Alive'. The Content-Type header is 'text/html; charset=UTF-8'. The packet bytes pane at the bottom shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
29	2.602393	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
31	2.696032	128.119.245.12	192.168.1.69	HTTP	540	HTTP/1.1 200 OK (text/html)
71	3.090954	2001:569:782a:470a::26a6:470a:30::681h	26a6:470a:30::681h	HTTP	521	GET /5c53f454f80fd.is?t=2564672 HTTP/1.1

Frame 31: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0), Dst: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 56304, Seq: 1, Ack: 427, Len: 486
> Hypertext Transfer Protocol
 > HTTP/1.1 200 OK\r\n
 Date: Sat, 06 Oct 2018 05:24:15 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 Last-Modified: Sat, 06 Oct 2018 05:24:01 GMT\r\n
 ETag: "00-57788987ec082"\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: 0.093639000 seconds]
 [Request in frame: 29]
 File Data: 128 bytes
 > Line-based text data: text/html (4 lines)

1. My browser is running HTTP 1.1 as indicated by the GET request. The server is also running HTTP 1.1 as indicated by the GET response.
2. My browser indicates that it can accept two languages, en-US and en, as indicated by the Accepted-Language header in the GET request.
3. The IP of my computer is 192.168.1.69. The IP of the server is 128.119.245.12.
4. The server returned status code 200 OK, indicating a successful GET request, to my browser.
5. The HTML file was last modified on Sat, 06 Oct 2018 05:24:01 GMT
6. My browser received exactly 128 bytes of content.
7. There are no headers that were not displayed in the packet-listing window.

ELEC 331 Assignment 1

HTTP CONDITIONAL GET/response interaction

First GET Request

The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows several packets, with packet 33 selected. The packet details pane shows the structure of the HTTP request, including the Host, User-Agent, and Accept headers. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
33	4.512938	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
37	4.606559	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
46	4.985729	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564674 HTTP/1.1
57	5.012522	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
104	8.389578	192.168.1.69	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
108	8.482687	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

Frame 33: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58001, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
▼ Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file2.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/69.0.3497.100 Safari/537.36\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: en-US,en;q=0.9\r\n \r\n [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
 [HTTP request 1/2]
 [Response in frame: 37]
 [Next request in frame: 104]

0000 9c 1e 95 b5 8b e0 e0 94 67 85 bd d5 08 00 45 00g.....E

First GET Response

The image shows a Wireshark packet capture of an HTTP GET response. The packet list pane shows several packets, with packet 37 selected. The packet details pane shows the structure of the HTTP response, including the Status Line, Date, Server, and Content-Type headers. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
33	4.512938	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
37	4.606559	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
46	4.985729	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564674 HTTP/1.1
57	5.012522	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
104	8.389578	192.168.1.69	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
108	8.482687	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

Frame 37: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0
> Ethernet II, Src: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0), Dst: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 58001, Seq: 1, Ack: 427, Len: 730
▼ Hypertext Transfer Protocol
 > HTTP/1.1 200 OK\r\n Date: Sat, 06 Oct 2018 05:49:21 GMT\r\n Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n Last-Modified: Sat, 06 Oct 2018 05:49:01 GMT\r\n ETag: "173-57788f1ee4abc"\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: 0.093621000 seconds]
 [Request in frame: 33]

0030 00 ed da 85 00 00 48 54 54 50 2f 31 2e 31 20 32HT TP/1.1 2

ELEC 331 Assignment 1

Second GET Request

The image shows a Wireshark packet capture of an HTTP session. The packet list on the left shows several packets, with packet 104 selected. The packet details pane on the right shows the structure of the selected packet. The Hypertext Transfer Protocol section is expanded, showing the GET request for /wireshark-labs/HTTP-wireshark-file2.html. The request includes various headers such as Host, Connection, Cache-Control, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language, If-None-Match, and If-Modified-Since. The full request URI is also displayed.

No.	Time	Source	Destination	Protocol	Length	Info
33	4.512938	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
37	4.606559	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
46	4.985729	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564674 HTTP/1.1
57	5.012522	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
104	8.389578	192.168.1.69	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
108	8.482687	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

Frame 104: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58001, Dst Port: 80, Seq: 427, Ack: 731, Len: 538
▼ Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\nIf-None-Match: "173-57788f1ee4abc"\r\nIf-Modified-Since: Sat, 06 Oct 2018 05:49:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]

Second GET Response

The image shows a Wireshark packet capture of an HTTP session. The packet list on the left shows several packets, with packet 108 selected. The packet details pane on the right shows the structure of the selected packet. The Hypertext Transfer Protocol section is expanded, showing the 304 Not Modified response. The response includes various headers such as Date, Server, Connection, Keep-Alive, and ETag. The full response is also displayed.

No.	Time	Source	Destination	Protocol	Length	Info
33	4.512938	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
37	4.606559	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
46	4.985729	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564674 HTTP/1.1
57	5.012522	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
104	8.389578	192.168.1.69	128.119.245.12	HTTP	592	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
108	8.482687	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

Frame 108: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
> Ethernet II, Src: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0), Dst: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 58001, Seq: 731, Ack: 965, Len: 239
▼ Hypertext Transfer Protocol
 > HTTP/1.1 304 Not Modified\r\nDate: Sat, 06 Oct 2018 05:49:25 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\nConnection: Keep-Alive\r\nKeep-Alive: timeout=5, max=99\r\nETag: "173-57788f1ee4abc"\r\n\r\n[HTTP response 2/2]
[Time since request: 0.093109000 seconds]
[Prev request in frame: 33]
[Prev response in frame: 37]
[Request in frame: 104]

8. No, I don't see an "IF-MODIFIED-SINCE" line in the first HTTP GET.
9. Yes. The server explicitly returned the contents of the file. We can tell because after the HTTP Headers, the payload / body of the response indicated by "Line-based text data: text/html" contains the contents of the file.
10. Yes, the second HTTP GET request contains an "IF-MODIFIED-SINCE" line, specifically: If-Modified-Since: Sat, 06 Oct 2018 05:49:01 GMT. This time corresponds to the Last Modified time from the First HTTP GET response.
11. For the second HTTP GET request, the server returned a 304 Not Modified. As such, the server did not explicitly return the contents of the file as I already have the latest version in the cache.

ELEC 331 Assignment 1

Retrieving Long Documents

HTTP GET Request

No.	Time	Source	Destination	Protocol	Length	Info
17	2.793465	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
22	2.887212	128.119.245.12	192.168.1.69	HTTP	535	HTTP/1.1 200 OK (text/html)
31	3.218422	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564676 HTTP/1.1
42	3.241572	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)

> Frame 17: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58055, Dst Port: 80, Seq: 1, Ack: 1, Len: 426

▼ Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
[HTTP request 1/1]
[Response in frame: 22]

0000 9c 1e 95 b5 8b e0 e0 94 67 85 bd d5 08 00 45 00 g....E
0010 01 d2 60 32 40 00 00 06 61 82 c0 a8 01 45 80 77 ..2... a....E.w
0020 f5 0c e2 c7 00 50 69 65 67 14 81 4e 86 38 50 18Pie g-N-8P
0030 02 01 3f 18 00 00 47 45 54 20 2f 77 69 72 65 73 ..?-GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-Lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 33 2e 68 ireshark -file3.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1..Ho

HTTP GET Response

No.	Time	Source	Destination	Protocol	Length	Info
17	2.793465	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
22	2.887212	128.119.245.12	192.168.1.69	HTTP	535	HTTP/1.1 200 OK (text/html)
31	3.218422	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564676 HTTP/1.1
42	3.241572	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)

> [4 Reassembled TCP Segments (4861 bytes): #19(1460), #20(1460), #21(1460), #22(481)]

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\nDate: Sat, 06 Oct 2018 06:03:51 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\nLast-Modified: Sat, 06 Oct 2018 05:59:01 GMT\r\nETag: "1194-5778915b3bf70"\r\nAccept-Ranges: bytes\r\nContent-Length: 4500\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]
[Time since request: 0.093747000 seconds]
[Request in frame: 17]
File Data: 4500 bytes

▼ Line-based text data: text/html (98 lines)

<html><head> \n<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n\n

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0c HTTP/1.1 200 OK.

12. Only one HTTP GET request was sent by my browser. For me, the packet number that contained the GET request message for the Bill of Rights is 17.
13. The packet number that corresponds to the GET response is 19 as indicated by the first Frame under "4 Assembled TCP segments".
14. The status code and phase of the response was 200 OK.
15. 4 TCP segments was required to carry the single HTTP response and text for the Bill of Rights.

ELEC 331 Assignment 1

HTML Documents with Embedded Objects

First HTTP GET Request

No.	Time	Source	Destination	Protocol	Length	Info
21	2.461368	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
23	2.554542	128.119.245.12	192.168.1.69	HTTP	1127	HTTP/1.1 200 OK (text/html)
24	2.580235	192.168.1.69	128.119.245.12	HTTP	451	GET /pearson.png HTTP/1.1
31	2.674344	128.119.245.12	192.168.1.69	HTTP	745	HTTP/1.1 200 OK (PNG)
50	2.848353	192.168.1.69	128.119.245.12	HTTP	465	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
72	3.040102	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564677 HTTP/1.1
104	3.062846	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
147	3.140518	128.119.245.12	192.168.1.69	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

> Frame 21: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58087, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
▼ Hypertext Transfer Protocol
 > GET /wireshark-labs/HTTP-wireshark-file4.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/69.0.3497.100 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
 [HTTP request 1/2]
 [Response in frame: 23]

0000 9c 1e 95 b5 8b e0 e0 94 67 85 bd d5 08 00 45 00g....E
0010 01 d2 60 38 40 00 80 06 61 7c c0 a8 01 45 80 77 ...@...a...Ew
0020 f5 0c e2 e7 00 50 f7 16 10 ad 94 a7 7d 34 50 18P...W...eP

Second HTTP GET Request

No.	Time	Source	Destination	Protocol	Length	Info
21	2.461368	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
23	2.554542	128.119.245.12	192.168.1.69	HTTP	1127	HTTP/1.1 200 OK (text/html)
24	2.580235	192.168.1.69	128.119.245.12	HTTP	451	GET /pearson.png HTTP/1.1
31	2.674344	128.119.245.12	192.168.1.69	HTTP	745	HTTP/1.1 200 OK (PNG)
50	2.848353	192.168.1.69	128.119.245.12	HTTP	465	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
72	3.040102	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564677 HTTP/1.1
104	3.062846	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
147	3.140518	128.119.245.12	192.168.1.69	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

> Frame 24: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58087, Dst Port: 80, Seq: 427, Ack: 1074, Len: 397
▼ Hypertext Transfer Protocol
 > GET /pearson.png HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 Connection: keep-alive\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n
 Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
 Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: en-US,en;q=0.9\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/pearson.png]
 [HTTP request 2/2]
 [Prev request in frame: 21]

0000 9c 1e 95 b5 8b e0 e0 94 67 85 bd d5 08 00 45 00g....E
0010 01 b5 60 39 40 00 80 06 61 98 c0 a8 01 45 80 77 ...9@...a...Ew
0020 f5 0c e2 e7 00 50 f7 16 12 57 94 a7 81 65 50 18P...W...eP

ELEC 331 Assignment 1

Third HTTP GET Request

No.	Time	Source	Destination	Protocol	Length	Info
21	2.461368	192.168.1.69	128.119.245.12	HTTP	480	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
23	2.554542	128.119.245.12	192.168.1.69	HTTP	1127	HTTP/1.1 200 OK (text/html)
24	2.580235	192.168.1.69	128.119.245.12	HTTP	451	GET /pearson.png HTTP/1.1
31	2.674344	128.119.245.12	192.168.1.69	HTTP	745	HTTP/1.1 200 OK (PNG)
50	2.848353	192.168.1.69	128.119.245.12	HTTP	465	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
72	3.040102	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	521	GET /5c53f454fc0fd.js?t=2564677 HTTP/1.1
104	3.062846	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
147	3.140518	128.119.245.12	192.168.1.69	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

> Frame 50: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58088, Dst Port: 80, Seq: 1, Ack: 1, Len: 411
v Hypertext Transfer Protocol
v GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\nHost: manic.cs.umass.edu\r\nConnection: keep-alive\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\nAccept: image/webp,image/apng,image/*,*/*;q=0.8\r\nReferer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]
[HTTP request 1/1]
[Response in frame: 147]

0000 9c 1e 95 b5 8b e0 e0 94 67 85 bd d5 08 00 45 00g....E
0010 01 c3 60 3e 40 00 80 06 61 85 c0 a8 01 45 80 77 ...>@...a....Ew
0020 f5 0c e2 e8 00 50 8c 85 50 74 20 21 a0 8f 50 18P..Pt !..P.

16. A total of 3 GET requests were sent by my browser. Specifically:
 - a. The first GET request was for the HTML, sent to gaia.cs.umass.edu.
 - b. The second GET request was for pearson.png, sent to gaia.cs.umass.edu.
 - c. The third GET request was for the 5th Edition cover, sent to manic.cs.umass.edu.
 - d. Both servers are under the same IP address, just different port numbers.
17. I believe that the two images were downloaded in parallel. If we were to look at the HTTP GET requests for both images, their source ports are different, indicating that these requests were sent in parallel over two different ports. If the source ports were the same, then it would be sequential.

ELEC 331 Assignment 1

HTTP Authentication

First HTTP GET Response

No.	Time	Source	Destination	Protocol	Length	Info
155	4.757101	192.168.1.69	128.119.245.12	HTTP	496	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
161	4.848876	128.119.245.12	192.168.1.69	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1342	13.879841	192.168.1.69	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1348	13.998208	128.119.245.12	192.168.1.69	HTTP	544	HTTP/1.1 200 OK (text/html)
1407	14.395065	192.168.1.69	128.119.245.12	HTTP	467	GET /favicon.ico HTTP/1.1
1412	14.411497	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	537	GET /5c53f454fc0fd.js?t=2564678 HTTP/1.1
1424	14.433734	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
1443	14.488053	128.119.245.12	192.168.1.69	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 161: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0

> Ethernet II, Src: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0), Dst: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.69

> Transmission Control Protocol, Src Port: 80, Dst Port: 58129, Seq: 1, Ack: 443, Len: 717

> Hypertext Transfer Protocol

> HTTP/1.1 401 Unauthorized\r\n

Date: Sat, 06 Oct 2018 06:25:29 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

WWW-Authenticate: Basic realm="wireshark-students only"\r\n

> Content-Length: 381\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=iso-8859-1\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.091775000 seconds]

[Request in frame: 155]

0000 e0 94 67 85 bd d5 9c 1e 95 b5 8b e0 08 00 45 00 ..g.....E.

0010 02 f5 52 f1 40 00 2f 06 be a0 80 77 f5 0c c0 a8 ..R@/..-w...

0020 01 45 00 50 e3 11 05 f1 0b 5f 65 e1 20 3e 50 18 ..E.P...._e..>P.

Second HTTP GET Request

No.	Time	Source	Destination	Protocol	Length	Info
155	4.757101	192.168.1.69	128.119.245.12	HTTP	496	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
161	4.848876	128.119.245.12	192.168.1.69	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1342	13.879841	192.168.1.69	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1348	13.998208	128.119.245.12	192.168.1.69	HTTP	544	HTTP/1.1 200 OK (text/html)
1407	14.395065	192.168.1.69	128.119.245.12	HTTP	467	GET /favicon.ico HTTP/1.1
1412	14.411497	2001:569:782a:4700::681b...	2606:4700:30::681b...	HTTP	537	GET /5c53f454fc0fd.js?t=2564678 HTTP/1.1
1424	14.433734	2606:4700:30::681b...	2001:569:782a:4700::681b...	HTTP	764	HTTP/1.1 200 OK (application/javascript)
1443	14.488053	128.119.245.12	192.168.1.69	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 1342: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits) on interface 0

> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: Actionte_b5:8b:e0 (9c:1e:95:b5:8b:e0)

> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 58147, Dst Port: 80, Seq: 1, Ack: 1, Len: 501

> Hypertext Transfer Protocol

> GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

> Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\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/69.0.3497.100 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]

[HTTP request 1/2]

0000 9c 1e 95 b5 8b e0 e0 94 67 85 bd d5 00 00 45 00 ..g.....E.

0010 02 1d 60 59 40 00 80 06 61 10 c0 a8 01 45 80 77 ..Y@...a...EW

0020 f5 0c e3 23 00 50 74 c9 4b 60 f6 05 5e 52 50 18 ..#Pt:K'..^RP.

18. For the initial HTTP GET request, the server responded with 401 Unauthorized.

19. For the second HTTP GET request, the field "Authorization: Basic" was added.

ELEC 331 Assignment 1

nslookup

1. Using nslookup, I looked up baidu.com, which had an IP of 220.181.37.10.

```
$ nslookup baidu.com
Non-authoritative answer:
Server:  cns06.eastlink.ca
Address:  64.178.142.10

Name:     baidu.com
Addresses: 123.125.115.110
           220.181.57.216
```

s

2. Using nslookup-type=soa, I looked up Oxford University (<http://www.ox.ac.uk/>), which has an authoritative server of ns2.ja.net with IP of 193.63.105.17.

```
$ nslookup -type=NS ox.ac.uk
Non-authoritative answer:
Server:  cns06.eastlink.ca
Address:  64.178.142.10

ox.ac.uk      nameserver = dns2.ox.ac.uk
ox.ac.uk      nameserver = dns1.ox.ac.uk
ox.ac.uk      nameserver = ns2.ja.net
ox.ac.uk      nameserver = dns0.ox.ac.uk

ns2.ja.net    internet address = 193.63.105.17
ns2.ja.net    AAAA IPv6 address = 2001:630:0:45::11
```


ELEC 331 Assignment 1

Tracing DNS with Wireshark

ipconfig /all (My IP and local DNS servers)

wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Dual Band Wireless-AC 3165
Physical Address. . . . . : E0-94-67-85-BD-D5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::552b:fe50:93b6:e089%7(Preferred)
IPv4 Address. . . . . : 192.168.0.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : October 6, 2018 5:34:46 PM
Lease Expires . . . . . : October 13, 2018 5:34:46 PM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPV6 IAD . . . . . : 65049703
DHCPV6 Client DUID. . . . . : 00-01-00-01-20-2E-81-F9-E0-94-67-85-BD-D5
DNS Servers . . . . . : 64.178.142.10
                        24.207.0.167
NetBIOS over Tcpip. . . . . : Enabled
```

DNS Query message

The image shows a Wireshark packet capture of a DNS query. The top pane displays a list of packets, with packet 47 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
42	3.318515	IntelCor_85:bd:d5	ArrisGro_29:a6:c8	ARP	42	192.168.0.10 is at e0:94:67:85:bd:d5
43	3.334131	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
44	3.397101	192.168.0.10	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
45	3.581987	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
46	3.581987	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
47	3.602387	192.168.0.10	64.178.142.10	DNS	72	Standard query 0x1556 A www.ietf.org

Packet Details:

- Frame 47: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
- Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: ArrisGro_29:a6:c8 (2c:99:24:29:a6:c8)
- Internet Protocol Version 4, Src: 192.168.0.10, Dst: 64.178.142.10
- User Datagram Protocol, Src Port: 58557, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x1556
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - www.ietf.org: type A, class IN
 - Name: www.ietf.org
 - [Name Length: 12]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Raw Data:

0000 00 00 00 00 00 00 77 77 77 04 69 65 74 66 65w ww.ietf

ELEC 331 Assignment 1

DNS Response message

No.	Time	Source	Destination	Protocol	Length	Info
47	3.602387	192.168.0.10	64.178.142.10	DNS	72	Standard query 0x1556 A www.ietf.org
48	3.750372	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
49	3.752321	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
50	3.869553	64.178.142.10	192.168.0.10	DNS	149	Standard query response 0x1556 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 1...
51	3.870216	192.168.0.10	104.20.0.85	TCP	66	58765 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
52	3.913434	104.20.0.85	192.168.0.10	TCP	68	80 → 58765 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1024

> User Datagram Protocol, Src Port: 53, Dst Port: 58557

▼ Domain Name System (response)

Transaction ID: 0x1556

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ www.ietf.org: type A, class IN

Name: www.ietf.org

[Name Length: 12]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

▼ Answers

> www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net

> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

[Request In: 47]

0030 00 03 00 00 00 00 03 77 77 77 04 69 65 74 66 83w ww.ietf-

3. The DNS query and response messages are all sent over UDP.
4. The destination port for the DNS query message is port 53. The source port of the DNS response message is port 53.
5. The DNS query message is being sent to an IP address of 64.178.142.10. My local DNS server for WiFi is also 64.178.142.10.
6. Inspecting the DNS query, it has a type of "A" and does not contain any answers.
7. Inspecting the DNS response, it provides 3 answers, respectively:
 - a. The canonical name of www.ietf.org with type CNAME.
 - b. Two type A DNS servers.
8. The subsequent TCP SYN packet sent has a destination IP address of 104.20.0.85, which corresponds to the first of the two type A DNS servers provided by the DNS response message.
9. No DNS queries were sent before retrieving the images.

ELEC 331 Assignment 1

DNS Query for nslookup www.mit.edu

No.	Time	Source	Destination	Protocol	Length	Info
167	12.859419	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
168	12.861862	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
169	12.931380	192.168.0.10	64.178.142.10	DNS	86	Standard query 0x0001 PTR 10.142.178.64.in-addr.arpa
170	12.941961	192.168.0.10	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
171	12.974399	64.178.142.10	192.168.0.10	DNS	117	Standard query response 0x0001 PTR 10.142.178.64.in-addr.arpa PTR cns06.eastlink.ca
172	12.976791	192.168.0.10	64.178.142.10	DNS	71	Standard query 0x0002 A www.mit.edu
173	13.084275	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
174	13.203127	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
175	13.204949	64.178.142.10	192.168.0.10	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566...
176	13.215192	192.168.0.10	64.178.142.10	DNS	71	Standard query 0x0003 AAAA www.mit.edu
177	13.298925	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
178	13.301497	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
179	13.304381	64.178.142.10	192.168.0.10	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e95...

> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 64.178.142.10
> User Datagram Protocol, Src Port: 51056, Dst Port: 53
v Domain Name System (query)
Transaction ID: 0x0003
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
v www.mit.edu: type AAAA, class IN
Name: www.mit.edu
[Name Length: 11]
0000 2c 99 24 29 a6 c8 e0 94 67 85 bd d5 08 00 45 00 , \$) ... g E:

DNS Response for nslookup www.mit.edu

No.	Time	Source	Destination	Protocol	Length	Info
167	12.859419	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
168	12.861862	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
169	12.931380	192.168.0.10	64.178.142.10	DNS	86	Standard query 0x0001 PTR 10.142.178.64.in-addr.arpa
170	12.941961	192.168.0.10	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.250 for any sources
171	12.974399	64.178.142.10	192.168.0.10	DNS	117	Standard query response 0x0001 PTR 10.142.178.64.in-addr.arpa PTR cns06.eastlink.ca
172	12.976791	192.168.0.10	64.178.142.10	DNS	71	Standard query 0x0002 A www.mit.edu
173	13.084275	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
174	13.203127	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
175	13.204949	64.178.142.10	192.168.0.10	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566...
176	13.215192	192.168.0.10	64.178.142.10	DNS	71	Standard query 0x0003 AAAA www.mit.edu
177	13.298925	192.168.0.1	239.255.255.250	IGMPv3	56	Membership Query, specific for group 239.255.255.250
178	13.301497	192.168.0.3	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
179	13.304381	64.178.142.10	192.168.0.10	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e95...

> Internet Protocol Version 4, Src: 64.178.142.10, Dst: 192.168.0.10
> User Datagram Protocol, Src Port: 53, Dst Port: 51056
v Domain Name System (response)
Transaction ID: 0x0003
Flags: 0x8100 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 0
Additional RRs: 0
v Queries
v www.mit.edu: type AAAA, class IN
Name: www.mit.edu
[Name Length: 11]
0000 e0 94 67 85 bd d5 2c 99 24 29 a6 c8 08 00 45 00 .. g... , \$) E:

10. For the last DNS query, the destination port is port 53. For the last DNS response, the source port is port 53.
11. For the last DNS query, the destination address is 64.178.142.10, which is my local DNS server.
12. For the last DNS query, the type is AAAA (IPv6) and does not contain any answers.
13. For the last DNS response, it provided 4 answers, respectively:
 - a. The canonical name of www.mit.edu of type CNAME
 - b. The canonical name of Akami's CDN for www.mit.edu.edgekey.net of type CNAME
 - c. Two DNS servers of type AAAA hosted by akamiedge

ELEC 331 Assignment 1

DNS Query for nslookup -type=NS mit.edu

No.	Time	Source	Destination	Protocol	Length	Info
8	0.488804	192.168.0.10	64.178.142.10	DNS	86	Standard query 0x0001 PTR 10.142.178.64.in-addr.arpa
9	0.541632	64.178.142.10	192.168.0.10	DNS	117	Standard query response 0x0001 PTR 10.142.178.64.in-addr.arpa PTR cns06.eastlink.ca
10	0.543580	192.168.0.10	64.178.142.10	DNS	67	Standard query 0x0002 NS mit.edu
11	0.627126	64.178.142.10	192.168.0.10	DNS	358	Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS asia2.akam.net NS asia1.akam...

> Frame 10: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: ArrisGro_29:a6:c8 (2c:99:24:29:a6:c8)
> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 64.178.142.10
> User Datagram Protocol, Src Port: 60056, Dst Port: 53
▼ Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
▼ mit.edu: type NS, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
[\[Response In: 11\]](#)

0000 2c 99 24 29 a6 c8 e0 94 67 85 bd d5 08 00 45 00 , \$).....E-
0010 00 35 6f a1 00 00 80 11 3b a8 c0 a8 00 0a 40 b2 .5o.....;.....@-
0020 8e 0a ea 98 00 35 00 21 ac b0 00 02 01 00 00 015!.....

DNS Response for nslookup-type=NS mit.edu

No.	Time	Source	Destination	Protocol	Length	Info
8	0.488804	192.168.0.10	64.178.142.10	DNS	86	Standard query 0x0001 PTR 10.142.178.64.in-addr.arpa
9	0.541632	64.178.142.10	192.168.0.10	DNS	117	Standard query response 0x0001 PTR 10.142.178.64.in-addr.arpa PTR cns06.eastlink.ca
10	0.543580	192.168.0.10	64.178.142.10	DNS	67	Standard query 0x0002 NS mit.edu
11	0.627126	64.178.142.10	192.168.0.10	DNS	358	Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS asia2.akam.net NS asia1.akam...

▼ Queries
▼ mit.edu: type NS, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
▼ Answers
> mit.edu: type NS, class IN, ns ns1-37.akam.net
> mit.edu: type NS, class IN, ns asia2.akam.net
> mit.edu: type NS, class IN, ns asia1.akam.net
> mit.edu: type NS, class IN, ns use5.akam.net
> mit.edu: type NS, class IN, ns use2.akam.net
> mit.edu: type NS, class IN, ns eur5.akam.net
> mit.edu: type NS, class IN, ns ns1-173.akam.net
> mit.edu: type NS, class IN, ns usw2.akam.net
> Additional records
[\[Request In: 10\]](#)
[Time: 0.083546000 seconds]

0000 e0 94 67 85 bd d5 2c 99 24 29 a6 c8 08 00 45 00 ..g...,\$)....E-
0010 01 58 00 00 40 00 3a 11 b0 26 40 b2 8e 0a c0 a8 .X'@:..8@.....
0020 00 0a 00 35 ea 98 01 44 a5 fd 00 02 01 00 00 015...D.....

14. For the last DNS query, the destination address is 64.178.142.10, which is my local DNS server.

15. For the last DNS query, the type is NS and does not contain any answers.

16. For the last DNS response, the MIT nameservers it provides are:

- ns1-37.akam.net
- asia2.akam.net
- asia1.akam.net
- use5.akam.net
- use2.akam.net
- eur5.akam.net
- ns1-173.akam.net
- usw2.akam.net

ELEC 331 Assignment 1

DNS Results for nslookup www.aiit.or.kr hub.ubc.ca

No.	Time	Source	Destination	Protocol	Length	Info
21	1.482590	192.168.0.10	64.178.142.10	DNS	70	Standard query 0xcae0 A hub.ubc.ca
24	1.536977	64.178.142.10	192.168.0.10	DNS	86	Standard query response 0xcae0 A hub.ubc.ca A 137.82.1.1
25	1.539824	192.168.0.10	137.82.1.1	DNS	83	Standard query 0x0001 PTR 1.1.82.137.in-addr.arpa
26	1.573742	137.82.1.1	192.168.0.10	DNS	172	Standard query response 0x0001 PTR 1.1.82.137.in-addr.arpa PTR hub.ubc.ca NS hub.ubc.ca NS dn...
27	1.575510	192.168.0.10	137.82.1.1	DNS	74	Standard query 0x0002 A www.aiit.or.kr
28	1.603609	137.82.1.1	192.168.0.10	DNS	193	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225 NS ns25.dnszi.com NS ns9.dnszi...
29	1.614969	192.168.0.10	137.82.1.1	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
30	1.643596	137.82.1.1	192.168.0.10	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

> Frame 21: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

> Ethernet II, Src: IntelCor_85:bd:d5 (e0:94:67:85:bd:d5), Dst: ArrisGro_29:a6:c8 (2c:99:24:29:a6:c8)

> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 64.178.142.10

> User Datagram Protocol, Src Port: 55552, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0xcae0

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Response In: 24]

0000 2c 99 24 29 a6 c8 e0 94 67 85 bd d5 00 00 45 00 , \$).... g....E.
0010 00 38 ef ad 00 00 80 11 3b 99 c0 a8 00 0a 40 b2 .8o..... ;.....@.

17. For the first DNS query, the destination address is 64.178.142.10, which is my local DNS server.
18. For the first DNS query, the type is A and does not contain any answers.
19. For the first DNS response, there is one answer. As we used hub.ubc.ca as the default DNS server, we must make a lookup there to find out more about www.aiit.or.kr. Once we find out that our “default” DNS server does not contain what we want, we make further calls to attempt to reach our target. Thus, the answer contained in our first DNS response is a response signifying that it does not have information about www.aiit.or.kr.