

Lachlan Sinclair

CS 372 Lab 1

10/13/2019

Question 1:

TCP, UDP, HTTP

Question 2:

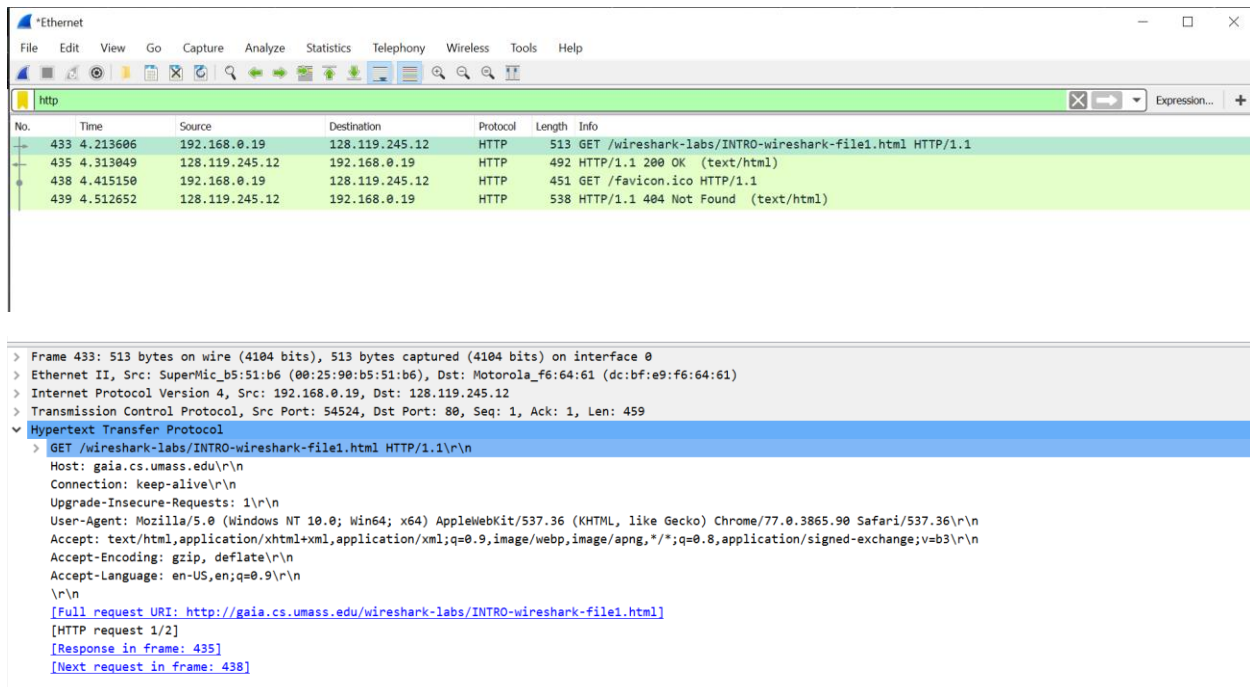
4.313049-4.213606 = **0.099443 seconds**

Question 3:

gaia.cs.umass.edu address is 128.119.245.12

my internet address is 192.168.0.19

Question 4:



The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, with the first four packets highlighted in green. These packets represent an HTTP GET request and its response. The second pane shows the details of the selected packet (frame 433), which is an HTTP GET request for the file /wireshark-labs/INTRO-wireshark-file1.html. The details pane shows the request headers, including the Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language. The full request URI is shown as http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html. The response status is shown as 200 OK (text/html) in frame 435.

No.	Time	Source	Destination	Protocol	Length	Info
433	4.213606	192.168.0.19	128.119.245.12	HTTP	513	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
435	4.313049	128.119.245.12	192.168.0.19	HTTP	492	HTTP/1.1 200 OK (text/html)
438	4.415150	192.168.0.19	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
439	4.512652	128.119.245.12	192.168.0.19	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
> Frame 433: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (08:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54524, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-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/77.0.3865.90 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 435]
    [Next request in frame: 438]
```

Wireshark interface showing a packet capture on the 'http' filter. The packet list displays four HTTP requests from 192.168.0.19 to 128.119.245.12. The selected packet (No. 433) is a GET request for /wireshark-labs/INTRO-wireshark-file1.html. The packet details pane shows the full request structure, including Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
433	4.213606	192.168.0.19	128.119.245.12	HTTP	513	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
435	4.313849	128.119.245.12	192.168.0.19	HTTP	492	HTTP/1.1 200 OK (text/html)
438	4.415150	192.168.0.19	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
439	4.512652	128.119.245.12	192.168.0.19	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 433: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54524, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
 > GET /wireshark-labs/INTRO-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/77.0.3865.90 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
 [HTTP request 1/2]
 [Response in frame: 435]
 [Next request in frame: 438]

0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu: Connecti
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep-alive
00a0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade-Insecure
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Request s: 1
00c0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c en-Agent : Mozill
00d0 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (Windows N
00e0 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x
00f0 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 64) Appl eWebKit/
0100 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML, l
0110 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Geck o) Chrom
0120 65 2f 37 37 2e 30 2e 33 38 36 35 2e 39 30 20 53 e/77.0.3 865.90 S
0130 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 afari/53 7.36
0140 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,
0150 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhtm
0160 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f l+xml,ap plicatio
0170 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 n/xml;q= 0.9,imag
0180 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e e/webp,i mage/apn
0190 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c g,*/*;q= 0.8,appl
01a0 69 63 61 74 69 6f 6e 2f 73 69 6f 6e 65 64 2d 65 ication/ signed-e
01b0 78 63 68 61 6e 67 65 3b 76 3d 62 33 0d 0a 41 63 xchange; v=b3
01c0 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g
01d0 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 zip, def late
01e0 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 cept-Lan guage: e
01f0 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 0d n-US,en; q=0.9
0200 0a

Wireshark_Ethernet_20191013154837_a12784.pcapng | Packets: 469 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%) | Profile: Default