4598 Lab 1

Gusho, Ernest
Bc, Ayush
Ramos, Nicolas

GitHub Repo: https://github.com/BcAyush/Computer-Communications-Labs

Team Name: Bit Busters
Lab Questions:

1. (Part 1.A.) Write the definition of a packet sniffer.

A packet sniffer is a software, like WireShark, that captures network traffic by monitoring the data packets that are sent through the network.

2. (Part 1.A) Write the definition of a packet analyzer.

A packet analyzer is a tool that takes the packets captured by the sniffer and then decodes them to a human-friendly format, allowing the user to thoroughly analyze the contents, protocols other relevant information from the packets.

3. (Part 1.A) What does the Wireshark packet capture library do?

The Wireshark packet capture library is responsible for directly capturing network traffic from the network interface card. They allow Wireshark go into "promiscuous mode" to record all traffic passing through the network adapter, even if this traffic is not directly addressed to the Wireshark host.

4. (Week 1 Lecture) What is a (data) link layer frame?

A data link layer frame is the second layer of the OSI model. It provides the transfer of frames between nodes across the physical layer. The link layer frame adds control info, synchronization, flow control and checks the bits to prevent transmission errors and ensure a reliable transmission of the data. The data link layer is divided into two parts: the Logical Link Control (LLC), which regulates error and flow management within the network layer, and the Medium Access Control (MAC), which regulates access to the transmission medium.

5. (Part 2.B.7 below) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window.

Three different protocols: HTTP, TCP, Ipv4

6. (Part 2.B.8) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

GET message sent:	07:40:28.277962
OK message received:	07:40:28.440560
Transmission time:	0.1626 seconds

7. Part 2.B.8) What is the Internet address of gaia.cs.umass.edu? What is the Internet address of your computer?

IP address of my computer (Source): 192.168.1.13

IP address of gaia.cs.umass.edu (Destination): 128.119.245.12

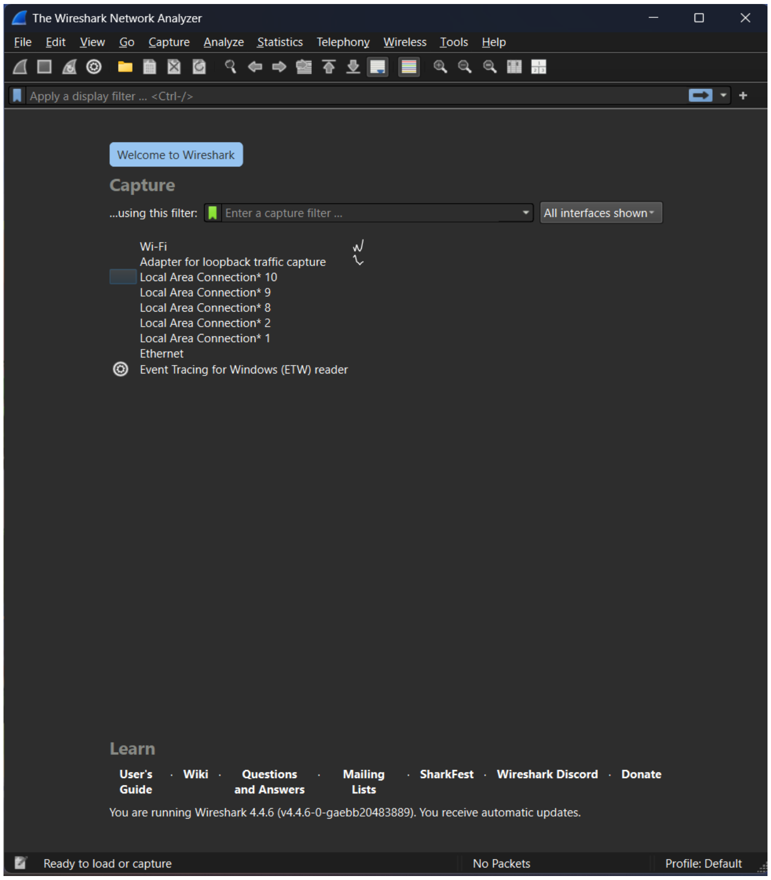
8. (Part 2.B.9) Print the two HTTP full messages (GET and OK). To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

4598 Lab 1

GitHub Repo: https://github.com/BcAyush/Computer-Communications-Labs

Gusho, Ernest
Bc, Ayush
Ramos, Nicolas

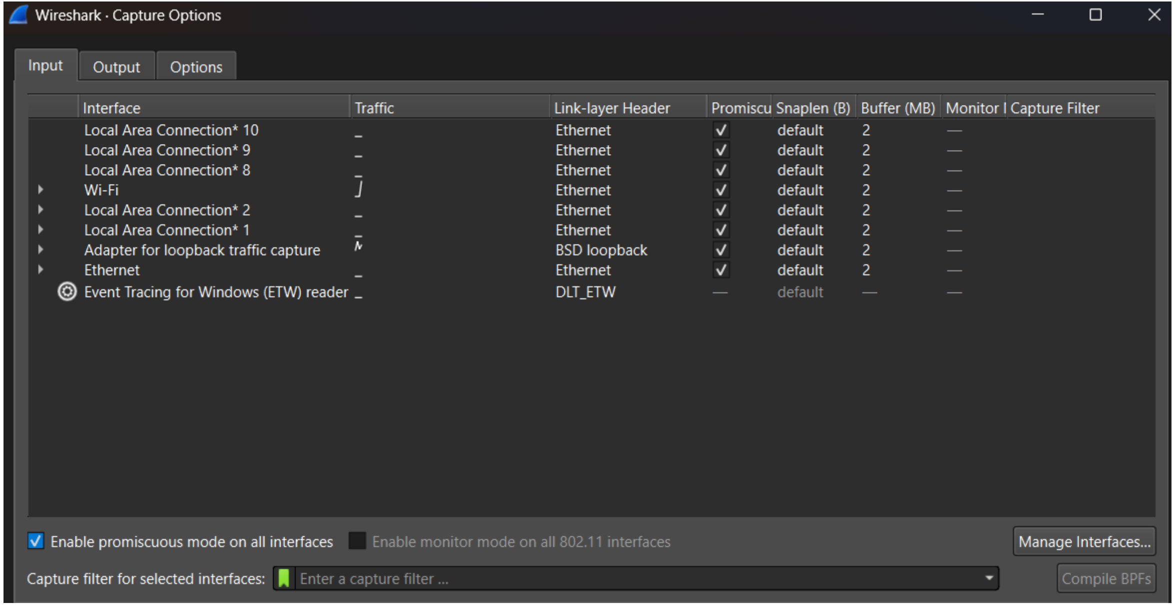
Lab Screenshots:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Ethernet
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.6 (v4.4.6-0-gaebb20483889). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Figure 1- Wireshark startup screen



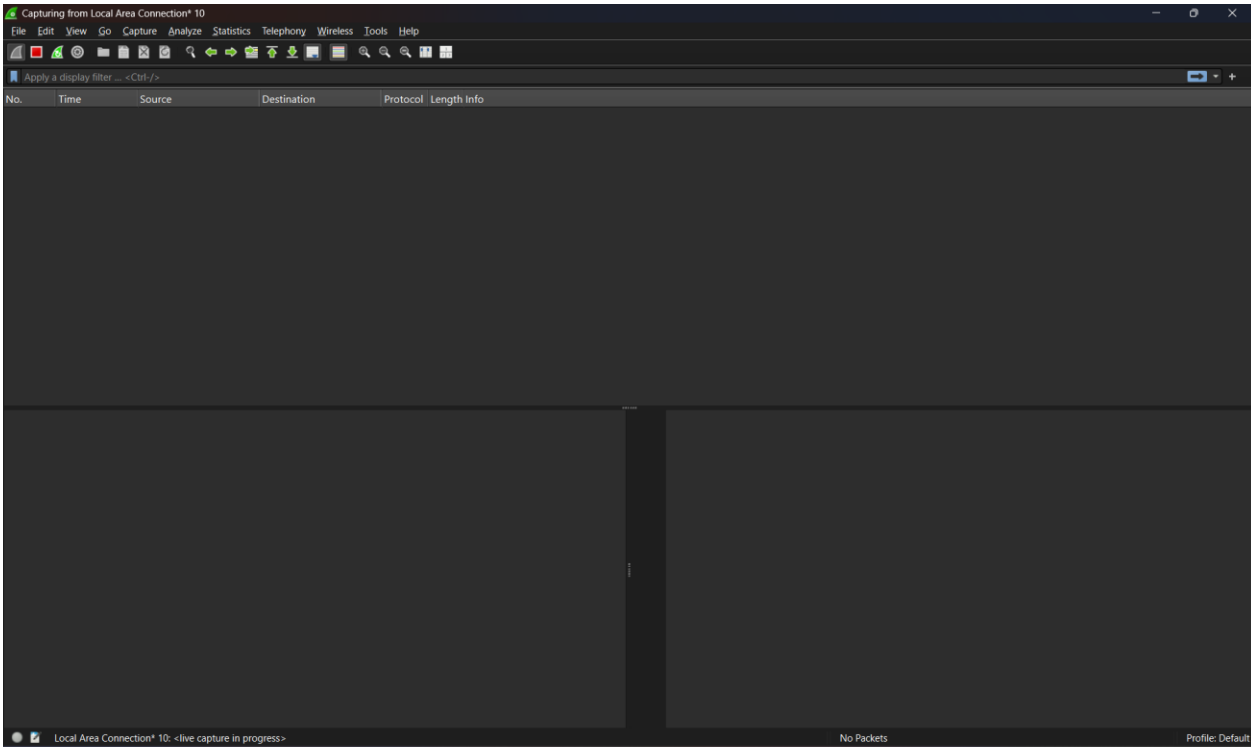
Wireshark · Capture Options

Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
Local Area Connection* 10		Ethernet	✓	default	2	—	
Local Area Connection* 9		Ethernet	✓	default	2	—	
Local Area Connection* 8		Ethernet	✓	default	2	—	
Wi-Fi		Ethernet	✓	default	2	—	
Local Area Connection* 2		Ethernet	✓	default	2	—	
Local Area Connection* 1		Ethernet	✓	default	2	—	
Adapter for loopback traffic capture		BSD loopback	✓	default	2	—	
Ethernet		Ethernet	✓	default	2	—	
Event Tracing for Windows (ETW) reader		DLT_ETW	—	default	—	—	

☑ Enable promiscuous mode on all interfaces ☐ Enable monitor mode on all 802.11 interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Figure 2 – Interface menu



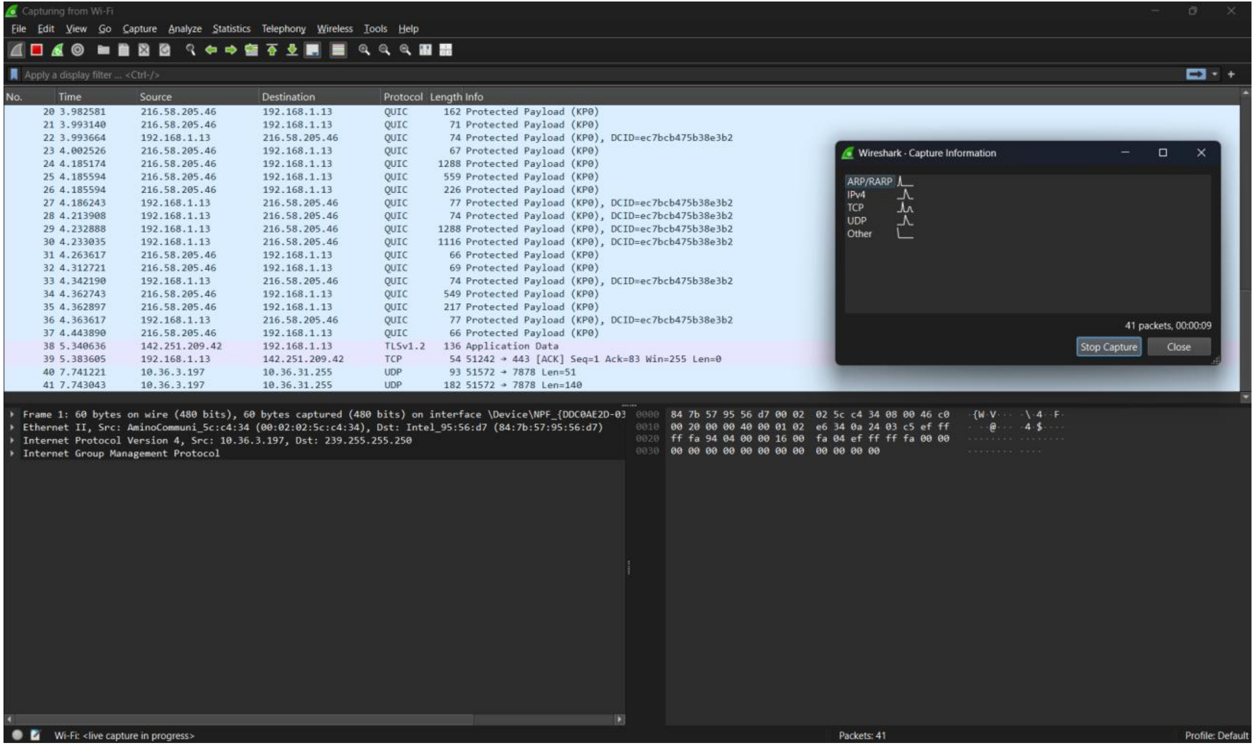
Capturing from Local Area Connection* 10

Local Area Connection* 10: <live capture in progress>

No Packets

Profile: Default

Figure 3 - Capturing screen (No internet traffic)

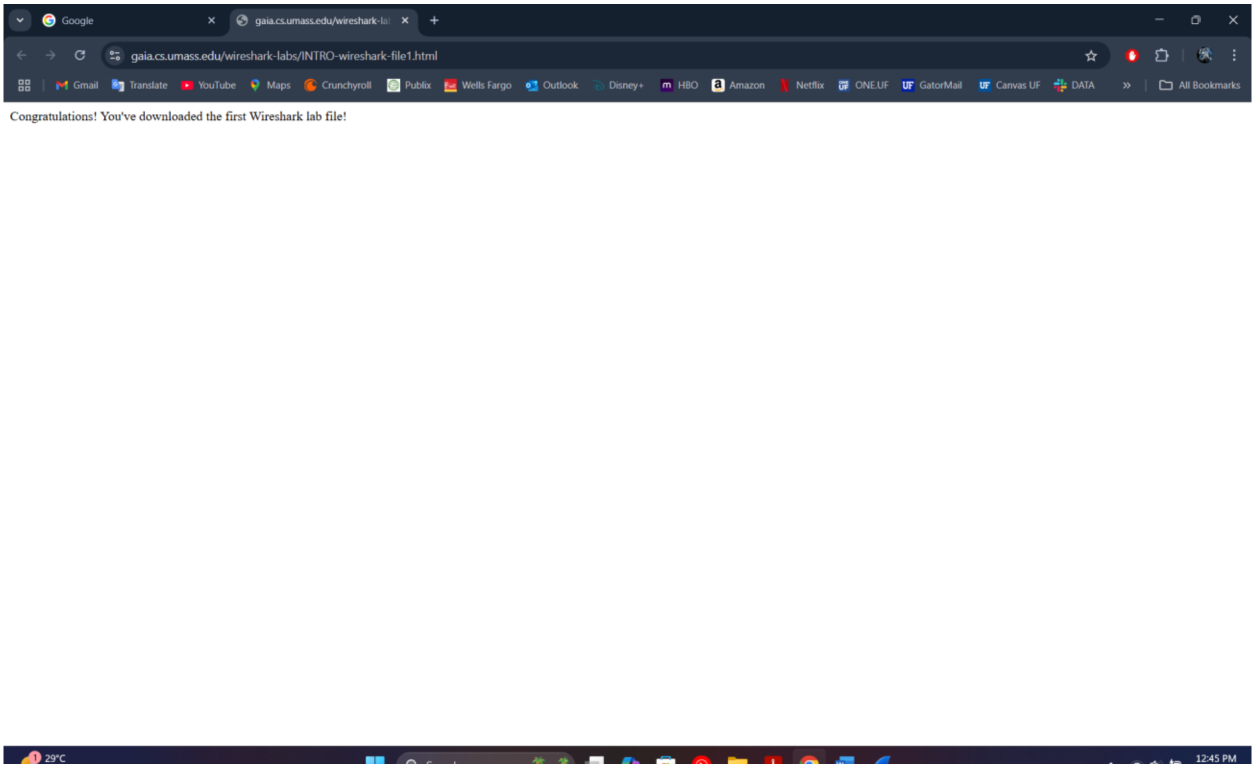

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Capture Information
ARP/RARP
IPv4
TCP
UDP
Other
41 packets, 00:00:09
Stop Capture
Close
Wi-Fi: <live capture in progress>
Packets: 41
Profile: Default

```
No.   Time       Source          Destination     Protocol Length Info
   20 3.982581   216.58.205.46   192.168.1.13    QUIC      162 Protected Payload (KP0)
   21 3.993140   216.58.205.46   192.168.1.13    QUIC       71 Protected Payload (KP0)
   22 3.993664   192.168.1.13    216.58.205.46   QUIC       74 Protected Payload (KP0), DCID=ec7bcb475b38e3b2
   23 4.002526   216.58.205.46   192.168.1.13    QUIC       67 Protected Payload (KP0)
   24 4.185174   216.58.205.46   192.168.1.13    QUIC     1288 Protected Payload (KP0)
   25 4.185594   216.58.205.46   192.168.1.13    QUIC      559 Protected Payload (KP0)
   26 4.185594   216.58.205.46   192.168.1.13    QUIC      226 Protected Payload (KP0)
   27 4.186243   192.168.1.13    216.58.205.46   QUIC       77 Protected Payload (KP0), DCID=ec7bcb475b38e3b2
   28 4.213908   192.168.1.13    216.58.205.46   QUIC       74 Protected Payload (KP0), DCID=ec7bcb475b38e3b2
   29 4.232888   192.168.1.13    216.58.205.46   QUIC     1288 Protected Payload (KP0), DCID=ec7bcb475b38e3b2
   30 4.233035   192.168.1.13    216.58.205.46   QUIC     1116 Protected Payload (KP0), DCID=ec7bcb475b38e3b2
   31 4.263617   216.58.205.46   192.168.1.13    QUIC       66 Protected Payload (KP0)
   32 4.312721   216.58.205.46   192.168.1.13    QUIC       69 Protected Payload (KP0)
   33 4.342190   192.168.1.13    216.58.205.46   QUIC       74 Protected Payload (KP0), DCID=ec7bcb475b38e3b2
   34 4.362743   216.58.205.46   192.168.1.13    QUIC      549 Protected Payload (KP0)
   35 4.362897   216.58.205.46   192.168.1.13    QUIC      217 Protected Payload (KP0)
   36 4.363617   192.168.1.13    216.58.205.46   QUIC       77 Protected Payload (KP0), DCID=ec7bcb475b38e3b2
   37 4.443890   216.58.205.46   192.168.1.13    QUIC       66 Protected Payload (KP0)
   38 5.340636   142.251.209.42  192.168.1.13    TLSv1.2   136 Application Data
   39 5.383605   192.168.1.13    142.251.209.42  TCP        54 51242 → 443 [ACK] Seq=1 Ack=83 Win=255 Len=0
   40 7.741221   10.36.3.197     10.36.31.255    UDP        93 51572 → 7878 Len=51
   41 7.743043   10.36.3.197     10.36.31.255    UDP       182 51572 → 7878 Len=140
```

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{DDC0AE2D-03
▸ Ethernet II, Src: AminoCommuni_5c:c4:34 (00:02:02:5c:c4:34), Dst: Intel_95:56:d7 (84:7b:57:95:56:d7)
▸ Internet Protocol Version 4, Src: 10.36.3.197, Dst: 239.255.255.250
▸ Internet Group Management Protocol
```

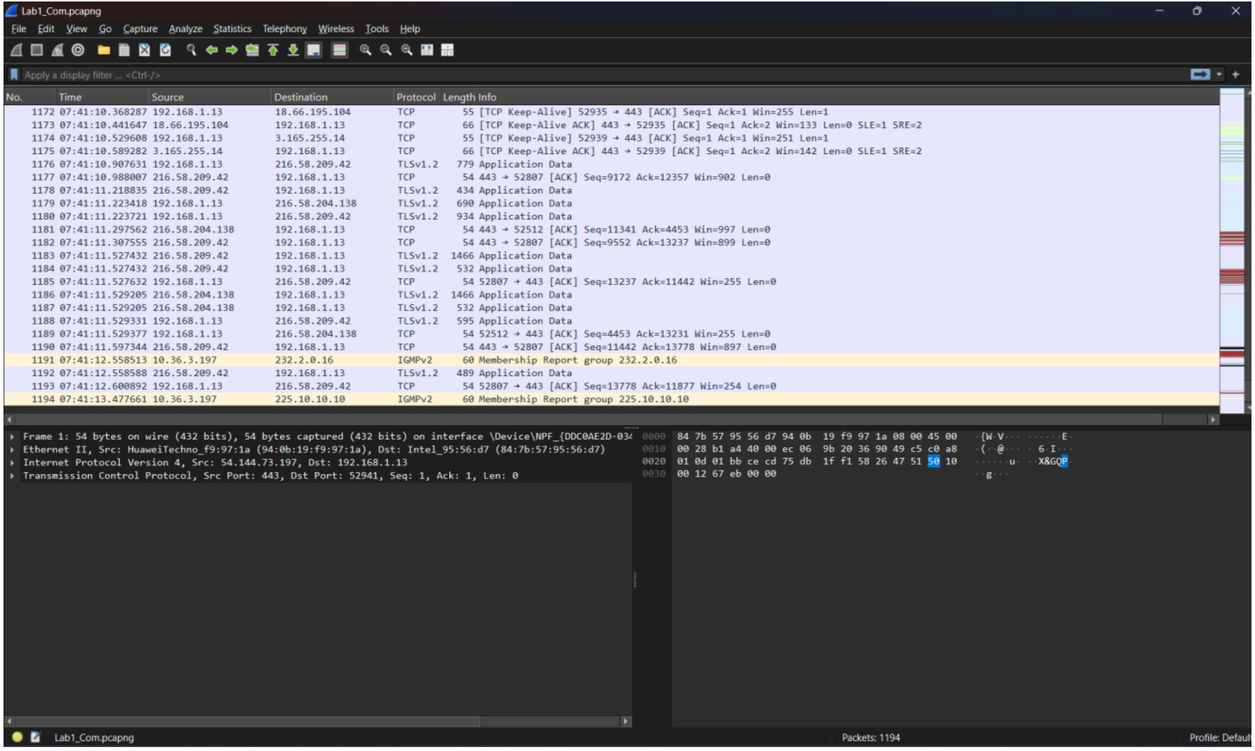
```
0000  84 7b 57 95 56 d7 00 02  02 5c c4 34 08 00 46 c0   ·{W·V··· ·\·4··F·
0010  00 20 00 00 40 00 01 02  e6 34 0a 24 03 c5 ef ff   · ··@··· ·4·$····
0020  ff fa 94 04 00 00 16 00  fa 04 ef ff ff fa 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Figure 4 - Capturing screen (Running)



Congratulations! You've downloaded the first Wireshark lab file!

Figure 5 - Lab website message

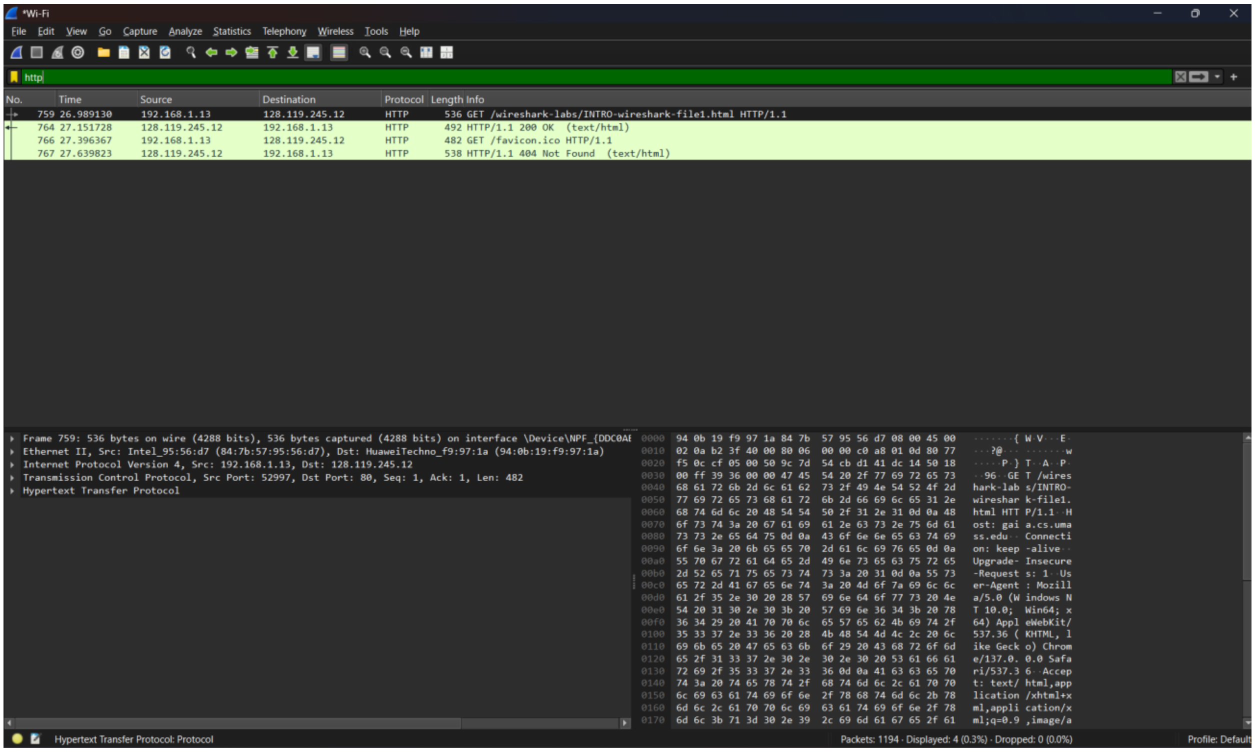

Lab1_Com.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Lab1_Com.pcapng
Packets: 1194
Profile: Defaul

```
No.     Time            Source          Destination     Protocol Length Info
   1172 07:41:10.368287 192.168.1.13    18.66.195.104   TCP        55 [TCP Keep-Alive] 52935 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
   1173 07:41:10.441647 18.66.195.104   192.168.1.13    TCP        66 [TCP Keep-Alive ACK] 443 → 52935 [ACK] Seq=1 Ack=2 Win=133 Len=0 SLE=1 SRE=2
   1174 07:41:10.529608 192.168.1.13    3.165.255.14    TCP        55 [TCP Keep-Alive] 52939 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1
   1175 07:41:10.589282 3.165.255.14    192.168.1.13    TCP        66 [TCP Keep-Alive ACK] 443 → 52939 [ACK] Seq=1 Ack=2 Win=142 Len=0 SLE=1 SRE=2
   1176 07:41:10.907631 192.168.1.13    216.58.209.42   TLSv1.2   779 Application Data
   1177 07:41:10.988007 216.58.209.42   192.168.1.13    TCP        54 443 → 52807 [ACK] Seq=9172 Ack=12357 Win=902 Len=0
   1178 07:41:11.218835 216.58.209.42   192.168.1.13    TLSv1.2   434 Application Data
   1179 07:41:11.223418 192.168.1.13    216.58.204.138  TLSv1.2   690 Application Data
   1180 07:41:11.223721 192.168.1.13    216.58.209.42   TLSv1.2   934 Application Data
   1181 07:41:11.297562 216.58.204.138  192.168.1.13    TCP        54 443 → 52512 [ACK] Seq=11341 Ack=4453 Win=997 Len=0
   1182 07:41:11.307555 216.58.209.42   192.168.1.13    TCP        54 443 → 52807 [ACK] Seq=9552 Ack=13237 Win=899 Len=0
   1183 07:41:11.527432 216.58.209.42   192.168.1.13    TLSv1.2  1466 Application Data
   1184 07:41:11.527432 216.58.209.42   192.168.1.13    TLSv1.2   532 Application Data
   1185 07:41:11.527632 192.168.1.13    216.58.209.42   TCP        54 52807 → 443 [ACK] Seq=13237 Ack=11442 Win=255 Len=0
   1186 07:41:11.529205 216.58.204.138  192.168.1.13    TLSv1.2  1466 Application Data
   1187 07:41:11.529205 216.58.204.138  192.168.1.13    TLSv1.2   532 Application Data
   1188 07:41:11.529331 192.168.1.13    216.58.209.42   TLSv1.2   595 Application Data
   1189 07:41:11.529377 192.168.1.13    216.58.204.138  TCP        54 52512 → 443 [ACK] Seq=4453 Ack=13231 Win=255 Len=0
   1190 07:41:11.597344 216.58.209.42   192.168.1.13    TCP        54 443 → 52807 [ACK] Seq=11442 Ack=13778 Win=897 Len=0
   1191 07:41:12.558513 10.36.3.197     232.2.0.16      IGMPv2     60 Membership Report group 232.2.0.16
   1192 07:41:12.558588 216.58.209.42   192.168.1.13    TLSv1.2   489 Application Data
   1193 07:41:12.600892 192.168.1.13    216.58.209.42   TCP        54 52807 → 443 [ACK] Seq=13778 Ack=11877 Win=254 Len=0
   1194 07:41:13.477661 10.36.3.197     225.10.10.10    IGMPv2     60 Membership Report group 225.10.10.10
```

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{DDC0AE2D-034
> Ethernet II, Src: HuaweiTechno_f9:97:1a (94:0b:19:f9:97:1a), Dst: Intel_95:56:d7 (84:7b:57:95:56:d7)
> Internet Protocol Version 4, Src: 54.144.73.197, Dst: 192.168.1.13
> Transmission Control Protocol, Src Port: 443, Dst Port: 52941, Seq: 1, Ack: 1, Len: 0
```

```
0000  84 7b 57 95 56 d7 94 0b  19 f9 97 1a 08 00 45 00   ·{W·V··· ······E·
0010  00 28 b1 a4 40 00 ec 06  9b 20 36 90 49 c5 c0 a8   ·(··@··· ·6·I···
0020  01 0d 01 bb ce cd 75 db  1f f1 58 26 47 51 50 10   ······u· ··X&GQP·
0030  00 12 67 eb 00 00                                  ··g···
```

Figure 6 - Capturing screen (Stopped)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol: Protocol
Profile: Default

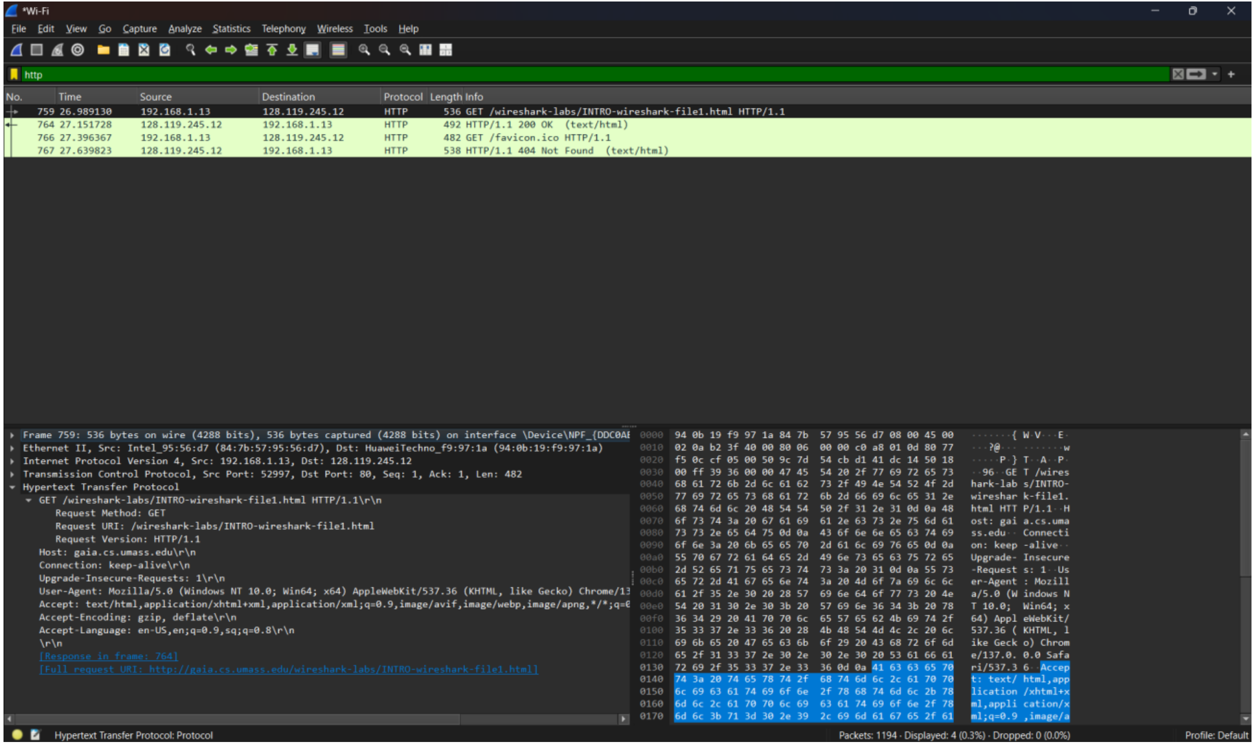
```
No.     Time            Source          Destination     Protocol Length Info
    759 26.989130       192.168.1.13    128.119.245.12  HTTP      536 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    764 27.151728       128.119.245.12  192.168.1.13    HTTP      492 HTTP/1.1 200 OK  (text/html)
    766 27.396367       192.168.1.13    128.119.245.12  HTTP      482 GET /favicon.ico HTTP/1.1
    767 27.639823       128.119.245.12  192.168.1.13    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 759: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{DDC0AE
> Ethernet II, Src: Intel_95:56:d7 (84:7b:57:95:56:d7), Dst: HuaweiTechno_f9:97:1a (94:0b:19:f9:97:1a)
> Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52997, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
> Hypertext Transfer Protocol
```

```
0000  94 0b 19 f9 97 1a 84 7b  57 95 56 d7 08 00 45 00   ·······{ W·V···E·
0010  02 0a b2 3f 40 00 80 06  00 00 c0 a8 01 0d 80 77   ···?@··· ·······w
0020  f5 0c cf 05 00 50 9c 7d  54 cb d1 41 dc 14 50 18   ·····P·} T··A··P·
0030  00 ff 39 36 00 00 47 45  54 20 2f 77 69 72 65 73   ··96··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
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··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows 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 31 33 37 2e 30 2e  30 2e 30 20 53 61 66 61   e/137.0. 0.0 Safa
0130  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63 63 65 70   ri/537.3 6··Accep
0140  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0150  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0160  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0170  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
```

Packets: 1194 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)

Figure 7 - HTTP protocol packets



```
No.      Time        Source          Destination     Protocol Length Info
    759 26.989130   192.168.1.13    128.119.245.12  HTTP      536 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    764 27.151728   128.119.245.12  192.168.1.13    HTTP      492 HTTP/1.1 200 OK  (text/html)
    766 27.396367   192.168.1.13    128.119.245.12  HTTP      482 GET /favicon.ico HTTP/1.1
    767 27.639823   128.119.245.12  192.168.1.13    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 759: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{DDC0AE
Ethernet II, Src: Intel_95:56:d7 (84:7b:57:95:56:d7), Dst: HuaweiTechno_f9:97:1a (94:0b:19:f9:97:1a)
Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52997, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/INTRO-wireshark-file1.html
    Request Version: HTTP/1.1
  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/13
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,sq;q=0.8\r\n
  \r\n
  [Response in frame: 764]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
0000  94 0b 19 f9 97 1a 84 7b  57 95 56 d7 08 00 45 00   ·······{ W·V···E·
0010  02 0a b2 3f 40 00 80 06  00 00 c0 a8 01 0d 80 77   ···?@··· ·······w
0020  f5 0c cf 05 00 50 9c 7d  54 cb d1 41 dc 14 50 18   ·····P·} T··A··P·
0030  00 ff 39 36 00 00 47 45  54 20 2f 77 69 72 65 73   ··96··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
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··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows 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 31 33 37 2e 30 2e  30 2e 30 20 53 61 66 61   e/137.0. 0.0 Safa
0130  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63 63 65 70   ri/537.3 6··Accep
0140  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0150  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0160  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0170  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
```

```
Hypertext Transfer Protocol: Protocol        Packets: 1194 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)        Profile: Default
```

Figure 8 - GET packet expanded interface

The printed HTTP GET and OK messages from Wireshark are shown in last two pages in report

```
No.     Time               Source                Destination           Protocol Length Info
    759 07:40:28.277962    192.168.1.13          128.119.245.12        HTTP     536    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1
Frame 759: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{DDC0AE2D-0343-4700-B5D9-24ADFCADB0B6},
id 0
Ethernet II, Src: Intel_95:56:d7 (84:7b:57:95:56:d7), Dst: HuaweiTechno_f9:97:1a (94:0b:19:f9:97:1a)
Internet Protocol Version 4, Src: 192.168.1.13, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52997, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    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/137.0.0.0 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=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,sq;q=0.8\r\n
    \r\n
    [Response in frame: 764]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
No.     Time               Source                Destination           Protocol Length Info
    764 07:40:28.440560    128.119.245.12        192.168.1.13          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 764: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{DDC0AE2D-0343-4700-B5D9-24ADFCADB0B6}, id 0
Ethernet II, Src: HuaweiTechno_f9:97:1a (94:0b:19:f9:97:1a), Dst: Intel_95:56:d7 (84:7b:57:95:56:d7)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.13
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0x69f0 (27120)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 44
    Protocol: TCP (6)
    Header Checksum: 0xabf0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.1.13
    [Stream index: 25]
Transmission Control Protocol, Src Port: 80, Dst Port: 52997, Seq: 1, Ack: 483, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 09 Jun 2025 11:40:27 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 09 Jun 2025 05:59:02 GMT\r\n
    ETag: "51-6371d46d5f825"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
        [Content length: 81]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [Request in frame: 759]
    [Time since request: 0.162598000 seconds]
    [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```