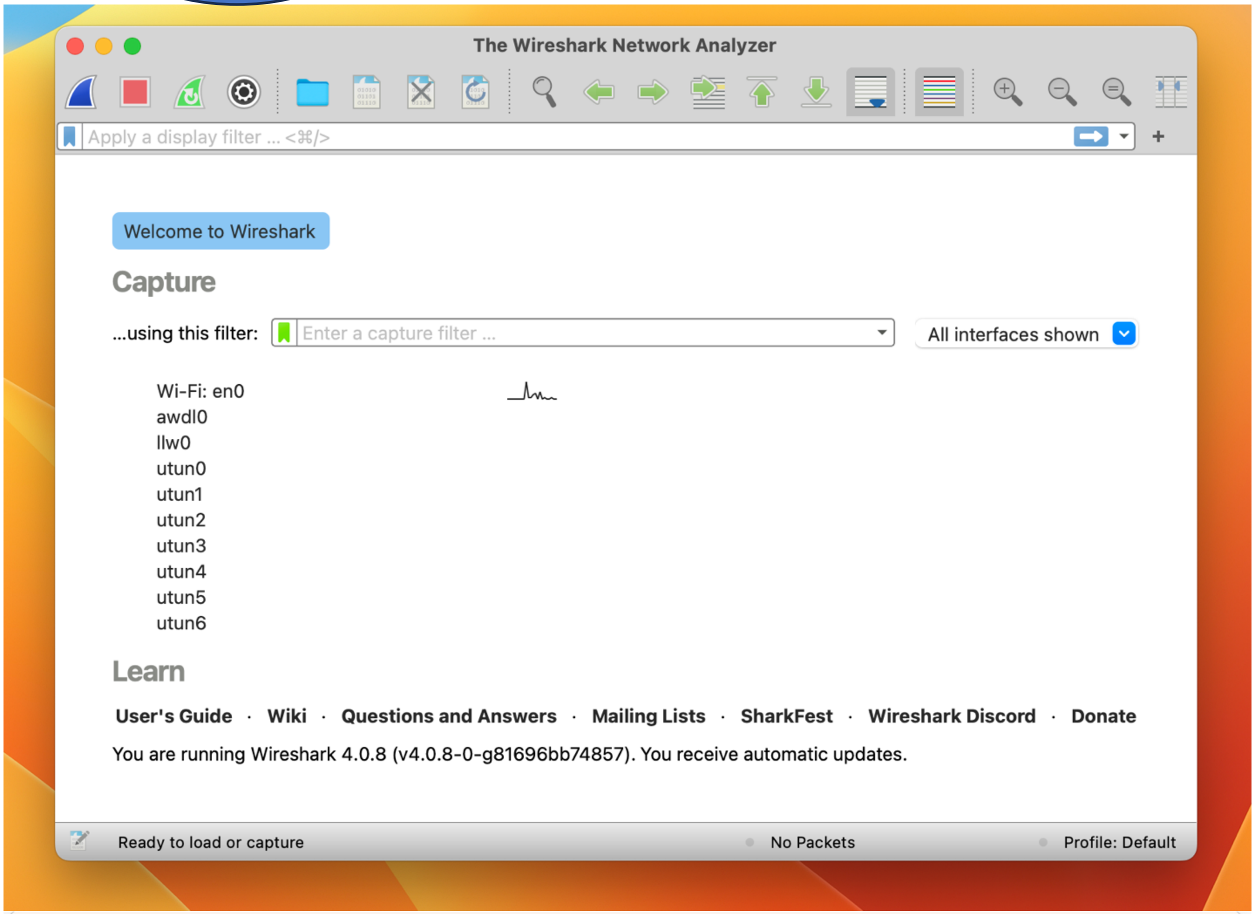
Task 1



Apply a display filter … <⌘/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter … All interfaces shown

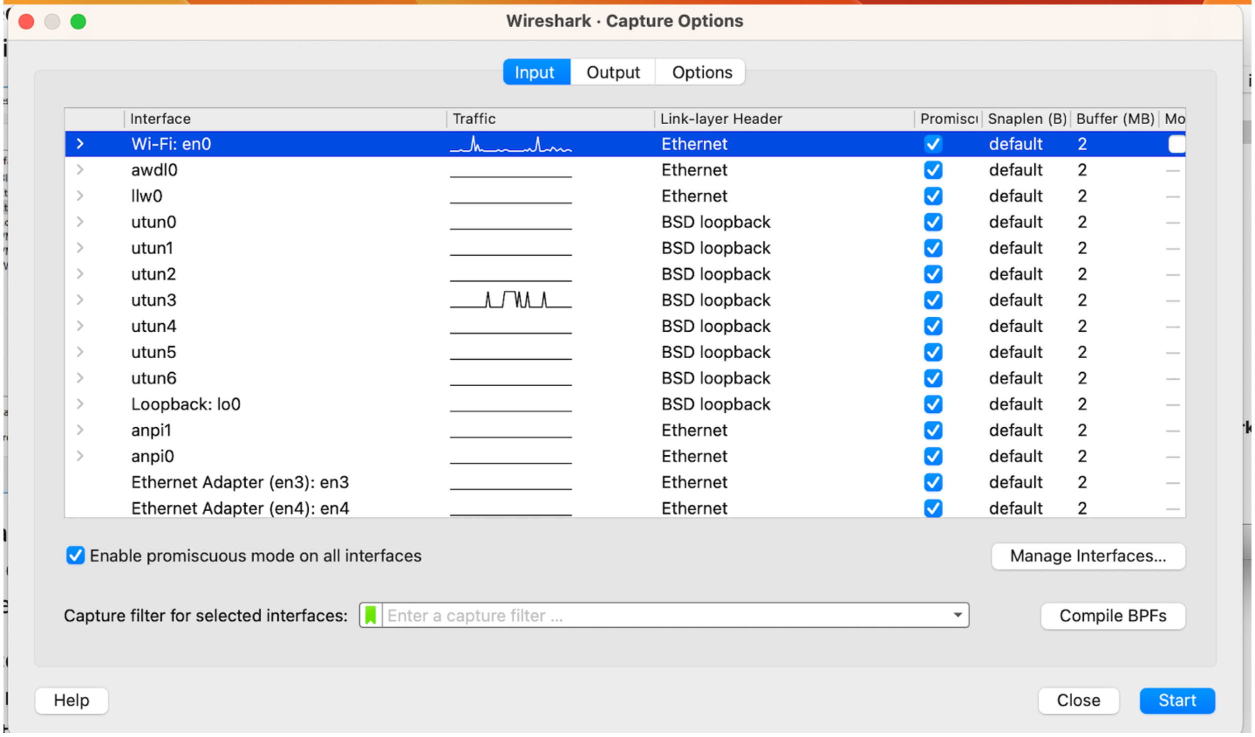
Wi-Fi: en0
awdl0
llw0
utun0
utun1
utun2
utun3
utun4
utun5
utun6

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.8 (v4.0.8-0-g81696bb74857). You receive automatic updates.

Ready to load or capture   No Packets   Profile: Default

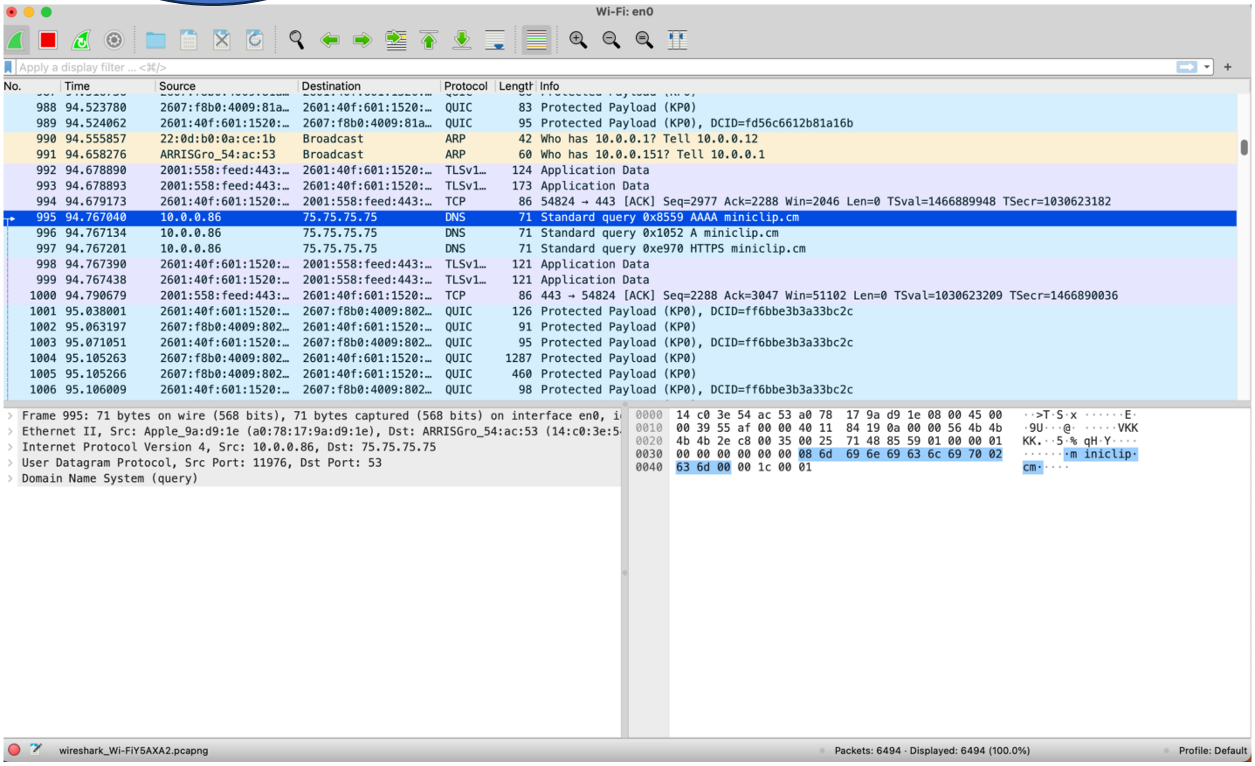


Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Mo
Wi-Fi: en0		Ethernet	☑	default	2	□
awdl0		Ethernet	☑	default	2	—
llw0		Ethernet	☑	default	2	—
utun0		BSD loopback	☑	default	2	—
utun1		BSD loopback	☑	default	2	—
utun2		BSD loopback	☑	default	2	—
utun3		BSD loopback	☑	default	2	—
utun4		BSD loopback	☑	default	2	—
utun5		BSD loopback	☑	default	2	—
utun6		BSD loopback	☑	default	2	—
Loopback: lo0		BSD loopback	☑	default	2	—
anpi1		Ethernet	☑	default	2	—
anpi0		Ethernet	☑	default	2	—
Ethernet Adapter (en3): en3		Ethernet	☑	default	2	—
Ethernet Adapter (en4): en4		Ethernet	☑	default	2	—

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

Task 2



Wi-Fi: en0

Apply a display filter … <⌘/>

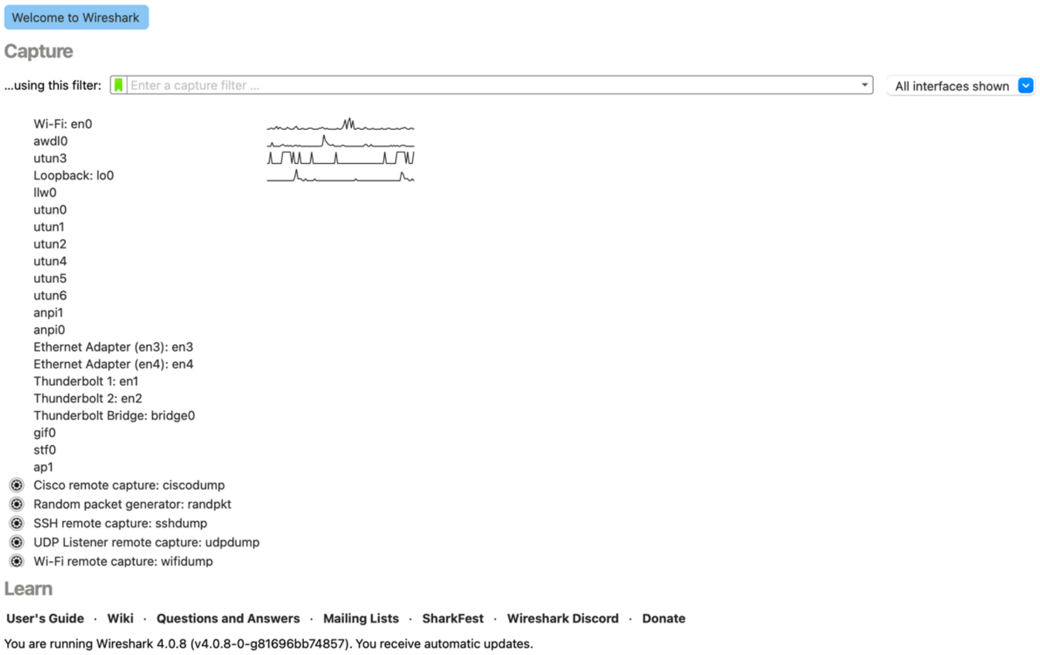
```
No.    Time        Source                  Destination             Protocol  Length Info
  988 94.523780   2607:f8b0:4009:81a…     2601:40f:601:1520:…     QUIC        83 Protected Payload (KP0)
  989 94.524062   2601:40f:601:1520:…     2607:f8b0:4009:81a…     QUIC        95 Protected Payload (KP0), DCID=fd56c6612b81a16b
  990 94.555857   22:0d:b0:0a:ce:1b       Broadcast               ARP         42 Who has 10.0.0.1? Tell 10.0.0.12
  991 94.658276   ARRISGro_54:ac:53       Broadcast               ARP         60 Who has 10.0.0.151? Tell 10.0.0.1
  992 94.678890   2001:558:feed:443:…     2601:40f:601:1520:…     TLSv1…     124 Application Data
  993 94.678893   2001:558:feed:443:…     2601:40f:601:1520:…     TLSv1…     173 Application Data
  994 94.679173   2601:40f:601:1520:…     2001:558:feed:443:…     TCP         86 54824 → 443 [ACK] Seq=2977 Ack=2288 Win=2046 Len=0 TSval=1466889948 TSecr=1030623182
  995 94.767040   10.0.0.86               75.75.75.75             DNS         71 Standard query 0x8559 AAAA miniclip.cm
  996 94.767134   10.0.0.86               75.75.75.75             DNS         71 Standard query 0x1052 A miniclip.cm
  997 94.767201   10.0.0.86               75.75.75.75             DNS         71 Standard query 0xe970 HTTPS miniclip.cm
  998 94.767390   2601:40f:601:1520:…     2001:558:feed:443:…     TLSv1…     121 Application Data
  999 94.767438   2601:40f:601:1520:…     2001:558:feed:443:…     TLSv1…     121 Application Data
 1000 94.790679   2001:558:feed:443:…     2601:40f:601:1520:…     TCP         86 443 → 54824 [ACK] Seq=2288 Ack=3047 Win=51102 Len=0 TSval=1030623209 TSecr=1466890036
 1001 95.038001   2601:40f:601:1520:…     2607:f8b0:4009:802…     QUIC       126 Protected Payload (KP0), DCID=ff6bbe3b3a33bc2c
 1002 95.063197   2607:f8b0:4009:802…     2601:40f:601:1520:…     QUIC        91 Protected Payload (KP0)
 1003 95.071051   2601:40f:601:1520:…     2607:f8b0:4009:802…     QUIC        95 Protected Payload (KP0), DCID=ff6bbe3b3a33bc2c
 1004 95.105263   2607:f8b0:4009:802…     2601:40f:601:1520:…     QUIC      1287 Protected Payload (KP0)
 1005 95.105266   2607:f8b0:4009:802…     2601:40f:601:1520:…     QUIC       460 Protected Payload (KP0)
 1006 95.106009   2601:40f:601:1520:…     2607:f8b0:4009:802…     QUIC        98 Protected Payload (KP0), DCID=ff6bbe3b3a33bc2c
```

```
> Frame 995: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, i
> Ethernet II, Src: Apple_9a:d9:1e (a0:78:17:9a:d9:1e), Dst: ARRISGro_54:ac:53 (14:c0:3e:5
> Internet Protocol Version 4, Src: 10.0.0.86, Dst: 75.75.75.75
> User Datagram Protocol, Src Port: 11976, Dst Port: 53
> Domain Name System (query)
```

```
0000  14 c0 3e 54 ac 53 a0 78  17 9a d9 1e 08 00 45 00   ··>T·S·x ······E·
0010  00 39 55 af 00 00 40 11  84 19 0a 00 00 56 4b 4b   ·9U···@· ·····VKK
0020  4b 4b 2e c8 00 35 00 25  71 48 85 59 01 00 00 01   KK.··5·% qH·Y····
0030  00 00 00 00 00 00 08 6d  69 6e 69 63 6c 69 70 02   ······m iniclip·
0040  63 6d 00 00 1c 00 01                               cm·····
```

wireshark_Wi-FiY5AXA2.pcapng   Packets: 6494 · Displayed: 6494 (100.0%)   Profile: Default

Task 3



Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...   All interfaces shown

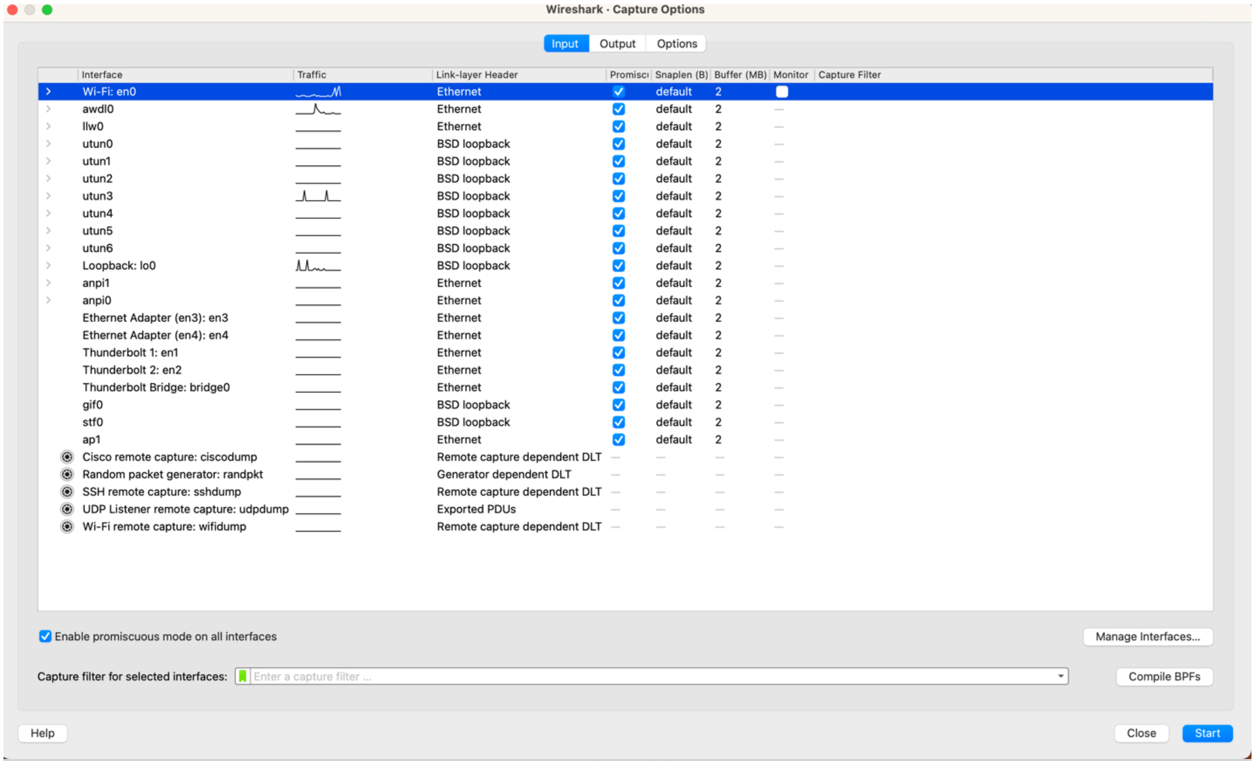
Wi-Fi: en0
awdl0
utun3
Loopback: lo0
llw0
utun0
utun1
utun2
utun4
utun5
utun6
anpi1
anpi0
Ethernet Adapter (en3): en3
Ethernet Adapter (en4): en4
Thunderbolt 1: en1
Thunderbolt 2: en2
Thunderbolt Bridge: bridge0
gif0
stf0
ap1
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.8 (v4.0.8-0-g81696bb74857). You receive automatic updates.

Task 3



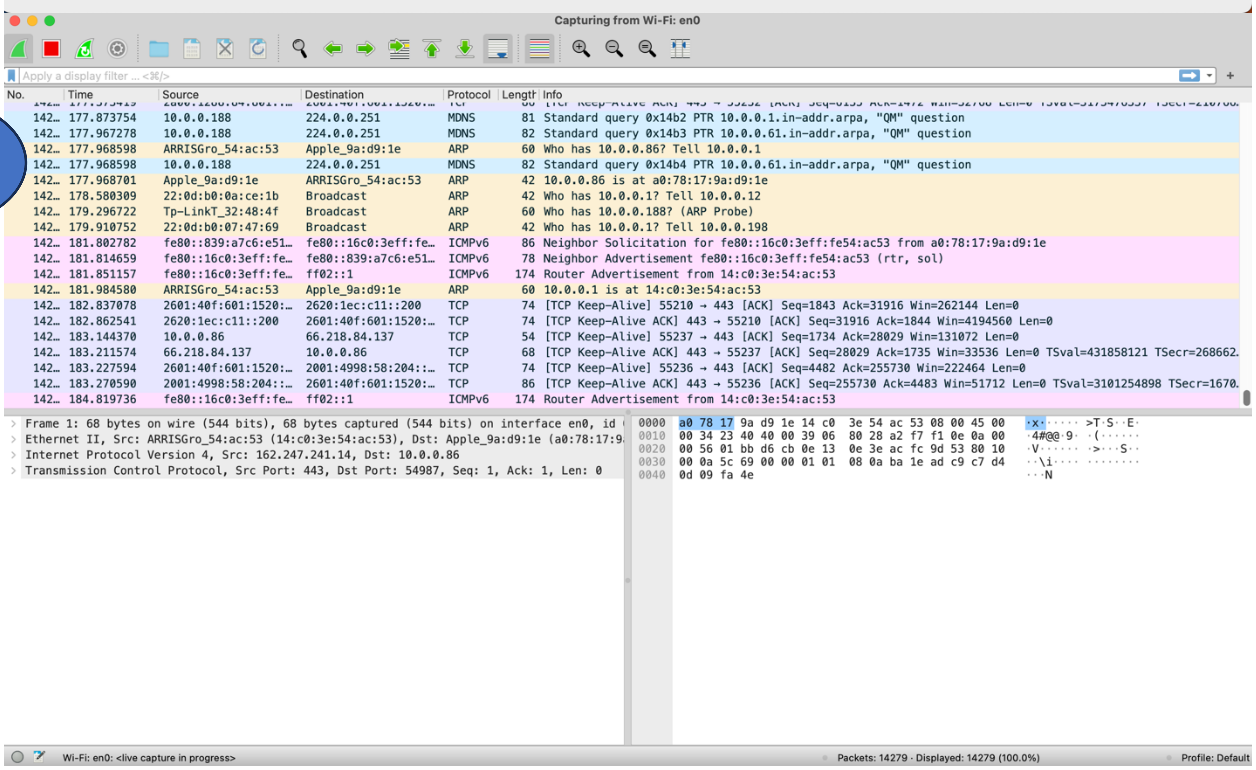
Wireshark · Capture Options

	Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
›	Wi-Fi: en0		Ethernet	☑	default	2	□	
›	awdl0		Ethernet	☑	default	2	—	
›	llw0		Ethernet	☑	default	2	—	
›	utun0		BSD loopback	☑	default	2	—	
›	utun1		BSD loopback	☑	default	2	—	
›	utun2		BSD loopback	☑	default	2	—	
›	utun3		BSD loopback	☑	default	2	—	
›	utun4		BSD loopback	☑	default	2	—	
›	utun5		BSD loopback	☑	default	2	—	
›	utun6		BSD loopback	☑	default	2	—	
›	Loopback: lo0		BSD loopback	☑	default	2	—	
›	anpi1		Ethernet	☑	default	2	—	
›	anpi0		Ethernet	☑	default	2	—	
	Ethernet Adapter (en3): en3		Ethernet	☑	default	2	—	
	Ethernet Adapter (en4): en4		Ethernet	☑	default	2	—	
	Thunderbolt 1: en1		Ethernet	☑	default	2	—	
	Thunderbolt 2: en2		Ethernet	☑	default	2	—	
	Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—	
	gif0		BSD loopback	☑	default	2	—	
	stf0		BSD loopback	☑	default	2	—	
	ap1		Ethernet	☑	default	2	—	
◉	Cisco remote capture: ciscodump		Remote capture dependent DLT	—	—	—	—	
◉	Random packet generator: randpkt		Generator dependent DLT	—	—	—	—	
◉	SSH remote capture: sshdump		Remote capture dependent DLT	—	—	—	—	
◉	UDP Listener remote capture: udpdump		Exported PDUs	—	—	—	—	
◉	Wi-Fi remote capture: wifidump		Remote capture dependent DLT	—	—	—	—	

☑ Enable promiscuous mode on all interfaces

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

Task 4



Capturing from Wi-Fi: en0

Apply a display filter ... <⌘/>

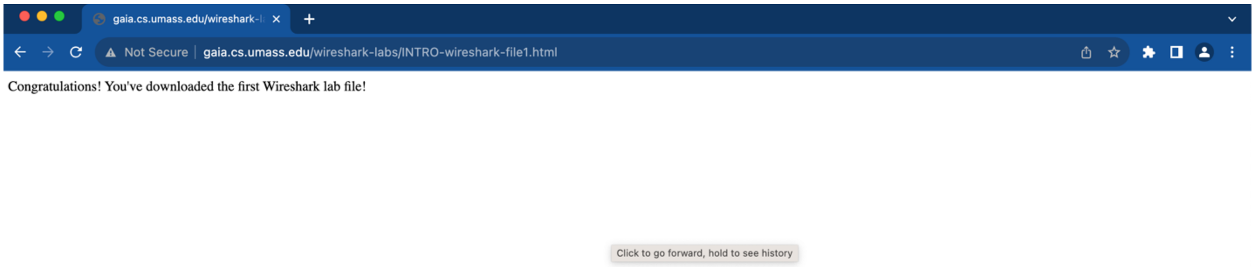
```
No.   Time        Source                Destination           Protocol Length Info
142…  177.873754  10.0.0.188            224.0.0.251           MDNS      81  Standard query 0x14b2 PTR 10.0.0.1.in-addr.arpa, "QM" question
142…  177.967278  10.0.0.188            224.0.0.251           MDNS      82  Standard query 0x14b3 PTR 10.0.0.61.in-addr.arpa, "QM" question
142…  177.968598  ARRISGro_54:ac:53     Apple_9a:d9:1e        ARP       60  Who has 10.0.0.86? Tell 10.0.0.1
142…  177.968598  10.0.0.188            224.0.0.251           MDNS      82  Standard query 0x14b4 PTR 10.0.0.61.in-addr.arpa, "QM" question
142…  177.968701  Apple_9a:d9:1e        ARRISGro_54:ac:53     ARP       42  10.0.0.86 is at a0:78:17:9a:d9:1e
142…  178.580309  22:0d:b0:0a:ce:1b     Broadcast             ARP       42  Who has 10.0.0.1? Tell 10.0.0.12
142…  179.296722  Tp-LinkT_32:48:4f     Broadcast             ARP       60  Who has 10.0.0.188? (ARP Probe)
142…  179.910752  22:0d:b0:07:47:69     Broadcast             ARP       42  Who has 10.0.0.1? Tell 10.0.0.198
142…  181.802782  fe80::839:a7c6:e51…   fe80::16c0:3eff:fe…   ICMPv6    86  Neighbor Solicitation for fe80::16c0:3eff:fe54:ac53 from a0:78:17:9a:d9:1e
142…  181.814659  fe80::16c0:3eff:fe…   fe80::839:a7c6:e51…   ICMPv6    78  Neighbor Advertisement fe80::16c0:3eff:fe54:ac53 (rtr, sol)
142…  181.851157  fe80::16c0:3eff:fe…   ff02::1               ICMPv6   174  Router Advertisement from 14:c0:3e:54:ac:53
142…  181.984580  ARRISGro_54:ac:53     Apple_9a:d9:1e        ARP       60  10.0.0.1 is at 14:c0:3e:54:ac:53
142…  182.837078  2601:40f:601:1520:…   2620:1ec:c11::200     TCP       74  [TCP Keep-Alive] 55210 → 443 [ACK] Seq=1843 Ack=31916 Win=262144 Len=0
142…  182.862541  2620:1ec:c11::200     2601:40f:601:1520:…   TCP       74  [TCP Keep-Alive ACK] 443 → 55210 [ACK] Seq=31916 Ack=1844 Win=4194560 Len=0
142…  183.144370  10.0.0.86             66.218.84.137         TCP       54  [TCP Keep-Alive] 55237 → 443 [ACK] Seq=1734 Ack=28029 Win=131072 Len=0
142…  183.211574  66.218.84.137         10.0.0.86             TCP       68  [TCP Keep-Alive ACK] 443 → 55237 [ACK] Seq=28029 Ack=1735 Win=33536 Len=0 TSval=431858121 TSecr=268662.
142…  183.227594  2601:40f:601:1520:…   2001:4998:58:204::…   TCP       74  [TCP Keep-Alive] 55236 → 443 [ACK] Seq=4482 Ack=255730 Win=222464 Len=0
142…  183.270590  2001:4998:58:204::…   2601:40f:601:1520:…   TCP       86  [TCP Keep-Alive ACK] 443 → 55236 [ACK] Seq=255730 Ack=4483 Win=51712 Len=0 TSval=3101254898 TSecr=1670.
142…  184.819736  fe80::16c0:3eff:fe…   ff02::1               ICMPv6   174  Router Advertisement from 14:c0:3e:54:ac:53
```

```
> Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface en0, id
> Ethernet II, Src: ARRISGro_54:ac:53 (14:c0:3e:54:ac:53), Dst: Apple_9a:d9:1e (a0:78:17:9
> Internet Protocol Version 4, Src: 162.247.241.14, Dst: 10.0.0.86
> Transmission Control Protocol, Src Port: 443, Dst Port: 54987, Seq: 1, Ack: 1, Len: 0
```

```
0000  a0 78 17 9a d9 1e 14 c0  3e 54 ac 53 08 00 45 00   ·x······ >T·S··E·
0010  00 34 23 40 40 00 39 06  80 28 a2 f7 f1 0e 0a 00   ·4#@@·9· ·(······
0020  00 56 01 bb d6 cb 0e 13  0e 3e ac fc 9d 53 80 10   ·V······ ·>···S··
0030  00 0a 5c 69 00 00 01 01  08 0a ba 1e ad c9 c7 d4   ··\i···· ········
0040  0d 09 fa 4e                                        ···N
```

Wi-Fi: en0: <live capture in progress>   Packets: 14279 · Displayed: 14279 (100.0%)   Profile: Default

Task 5


gaia.cs.umass.edu/wireshark-l
Not Secure
Click to go forward, hold to see history

gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

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

Task 5

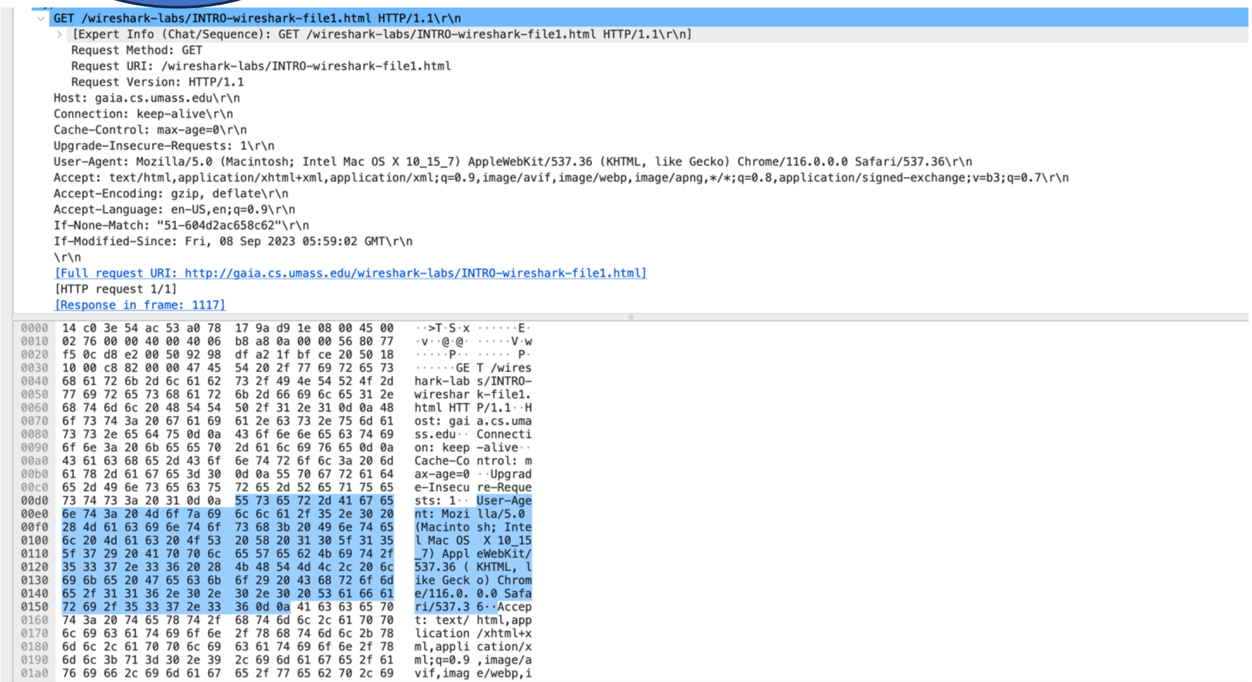
Task5. Highlight in green the HTTP message exchange with gaia.cs.umass.edu on the image in your Word document.

```
1114    204.743781    10.0.0.86        128.119.245.12          HTTP    644      GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
```

```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "51-604d2ac658c62"
If-Modified-Since: Fri, 08 Sep 2023 05:59:02 GMT
```

```
HTTP/1.1 304 Not Modified
Date: Fri, 08 Sep 2023 17:26:58 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "51-604d2ac658c62"
```

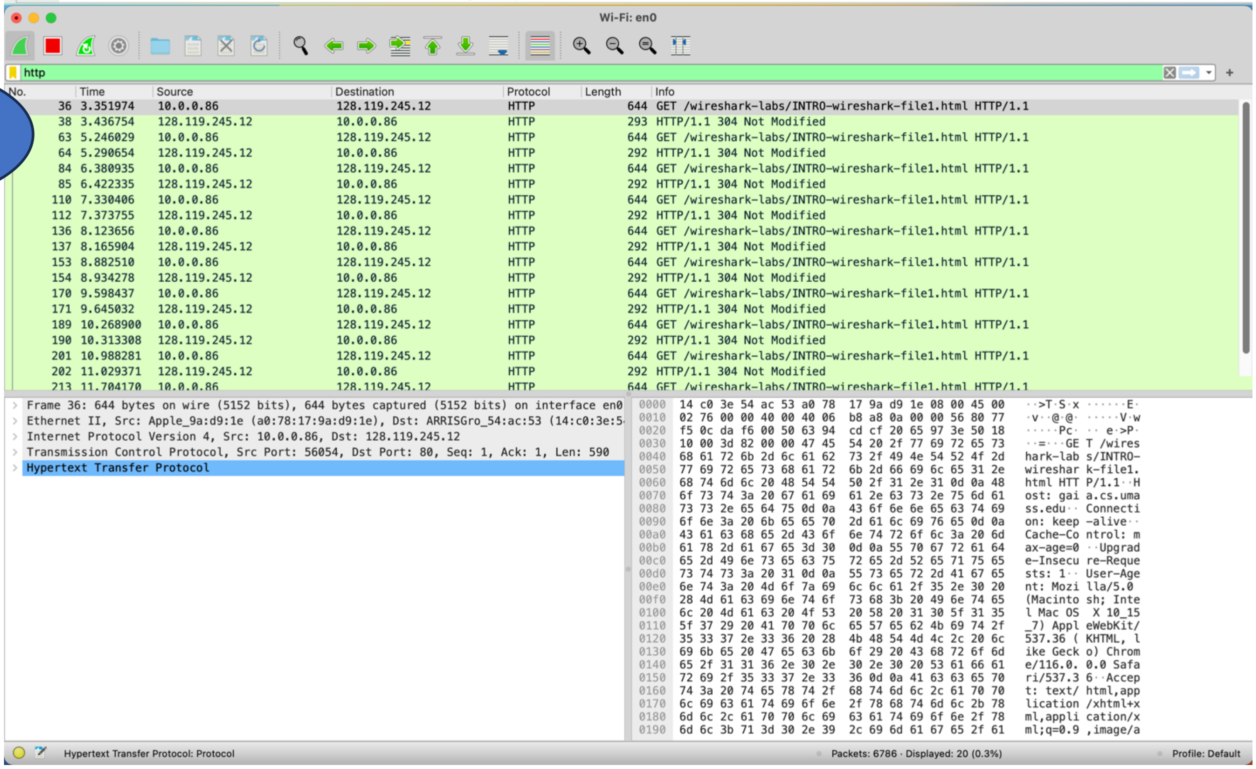
Task 5



```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): 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
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 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\r\n
If-None-Match: "51-604d2ac658c62"\r\n
If-Modified-Since: Fri, 08 Sep 2023 05:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 1117]
```

```
0000  14 c0 3e 54 ac 53 a0 78  17 9a d9 1e 08 00 45 00   ··>T·S·x ······E·
0010  02 76 00 00 40 00 40 06  b8 a8 0a 00 00 56 80 77   ·v··@·@· ·····V·w
0020  f5 0c d8 e2 00 50 92 98  df a2 1f bf ce 20 50 18   ·····P·· ····· P·
0030  10 00 c8 82 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 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  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 6d   Cache-Co ntrol: m
00b0  61 78 2d 61 67 65 3d 30  0d 0a 55 70 67 72 61 64   ax-age=0 ··Upgrad
00c0  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu re-Reque
00d0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
00e0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00f0  28 4d 61 63 69 6e 74 6f  73 68 3b 20 49 6e 74 65   (Macinto sh; Inte
0100  6c 20 4d 61 63 20 4f 53  20 58 20 31 30 5f 31 35   l Mac OS  X 10_15
0110  5f 37 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   _7) Appl eWebKit/
0120  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0130  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0140  65 2f 31 31 36 2e 30 2e  30 2e 30 20 53 61 66 61   e/116.0. 0.0 Safa
0150  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63 63 65 70   ri/537.3 6··Accep
0160  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0170  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0180  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0190  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
01a0  76 69 66 2c 69 6d 61 67  65 2f 77 65 62 70 2c 69   vif,imag e/webp,i
```

Task 6



```
http
```

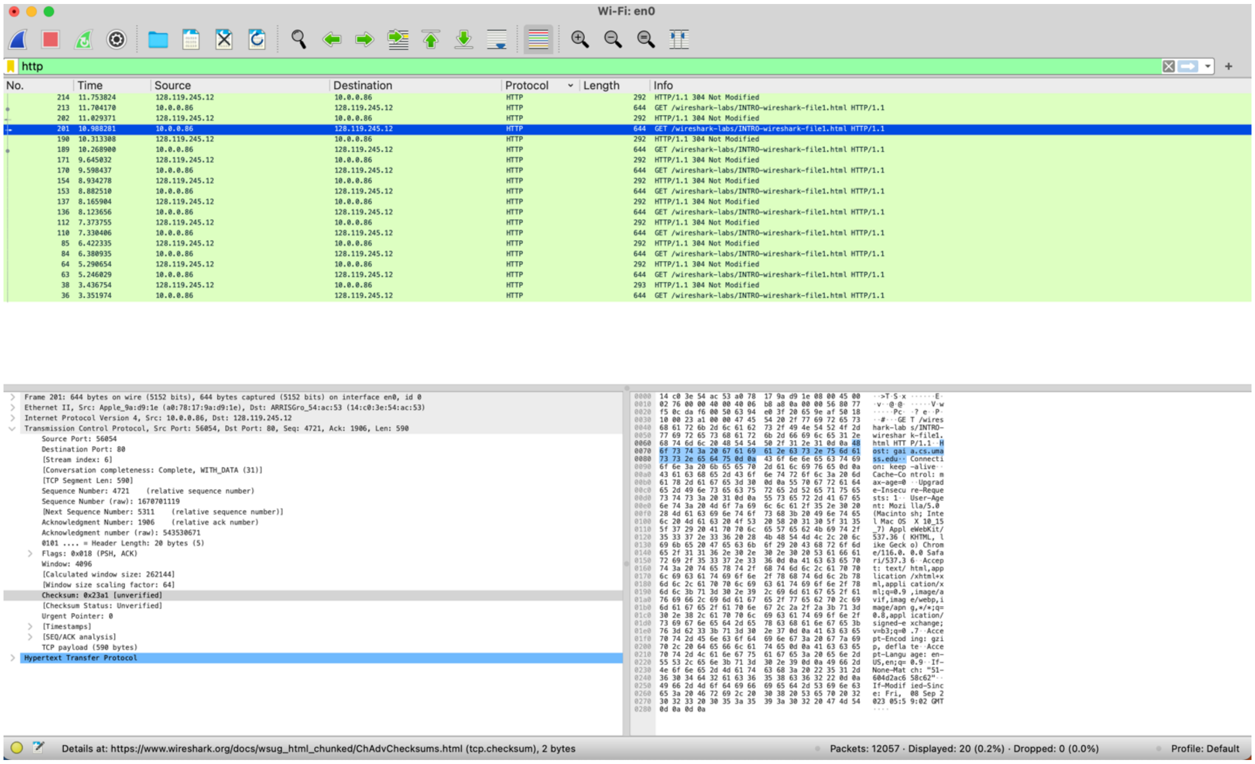
```
No.     Time         Source          Destination      Protocol  Length  Info
     36 3.351974     10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
     38 3.436754     128.119.245.12  10.0.0.86        HTTP         293  HTTP/1.1 304 Not Modified
     63 5.246029     10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
     64 5.290654     128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
     84 6.380935     10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
     85 6.422335     128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
    110 7.330406     10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    112 7.373755     128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
    136 8.123656     10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    137 8.165904     128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
    153 8.882510     10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    154 8.934278     128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
    170 9.598437     10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    171 9.645032     128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
    189 10.268900    10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    190 10.313308    128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
    201 10.988281    10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    202 11.029371    128.119.245.12  10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
    213 11.704170    10.0.0.86       128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
```

```
> Frame 36: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface en0
> Ethernet II, Src: Apple_9a:d9:1e (a0:78:17:9a:d9:1e), Dst: ARRISGro_54:ac:53 (14:c0:3e:5
> Internet Protocol Version 4, Src: 10.0.0.86, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56054, Dst Port: 80, Seq: 1, Ack: 1, Len: 590
> Hypertext Transfer Protocol
```

```
0000  14 c0 3e 54 ac 53 a0 78  17 9a d9 1e 08 00 45 00   ··>T·S·x ······E·
0010  02 76 00 00 40 00 40 06  b8 a8 0a 00 00 56 80 77   ·v··@·@· ·····V·w
0020  f5 0c da f6 00 50 63 94  cd cf 20 65 97 3e 50 18   ·····Pc· ·· e·>P·
0030  10 00 3d 82 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 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  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 6d   Cache-Co ntrol: m
00b0  61 78 2d 61 67 65 3d 30  0d 0a 55 70 67 72 61 64   ax-age=0 ··Upgrad
00c0  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu re-Reque
00d0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
00e0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00f0  28 4d 61 63 69 6e 74 6f  73 68 3b 20 49 6e 74 65   (Macinto sh; Inte
0100  6c 20 4d 61 63 20 4f 53  20 58 20 31 30 5f 31 35   l Mac OS  X 10_15
0110  5f 37 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   _7) Appl eWebKit/
0120  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0130  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0140  65 2f 31 31 36 2e 30 2e  30 2e 30 20 53 61 66 61   e/116.0. 0.0 Safa
0150  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63 63 65 70   ri/537.3 6··Accep
0160  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0170  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0180  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0190  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: 6786 · Displayed: 20 (0.3%) · Profile: Default

Task 7



```
http
```

```
No.   Time        Source           Destination      Protocol  Length  Info
  214 11.753824   128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
  213 11.704170   10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  202 11.029371   128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
  201 10.988281   10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  190 10.313308   128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
  189 10.268900   10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  171 9.645032    128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
  170 9.598437    10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  154 8.934278    128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
  153 8.882510    10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  137 8.165904    128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
  136 8.123656    10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  112 7.373755    128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
  110 7.330406    10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   85 6.422335    128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
   84 6.380935    10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   64 5.290654    128.119.245.12   10.0.0.86        HTTP         292  HTTP/1.1 304 Not Modified
   63 5.246029    10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   38 3.436754    128.119.245.12   10.0.0.86        HTTP         293  HTTP/1.1 304 Not Modified
   36 3.351974    10.0.0.86        128.119.245.12   HTTP         644  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
```

```
> Frame 201: 644 bytes on wire (5152 bits), 644 bytes captured (5152 bits) on interface en0, id 0
> Ethernet II, Src: Apple_9a:d9:1e (a0:78:17:9a:d9:1e), Dst: ARRISGro_54:ac:53 (14:c0:3e:54:ac:53)
> Internet Protocol Version 4, Src: 10.0.0.86, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 56054, Dst Port: 80, Seq: 4721, Ack: 1906, Len: 590
    Source Port: 56054
    Destination Port: 80
    [Stream index: 6]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 590]
    Sequence Number: 4721    (relative sequence number)
    Sequence Number (raw): 1670701119
    [Next Sequence Number: 5311    (relative sequence number)]
    Acknowledgment Number: 1906    (relative ack number)
    Acknowledgment number (raw): 543530671
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 4096
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0x23a1 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (590 bytes)
> Hypertext Transfer Protocol
```

```
0000  14 c0 3e 54 ac 53 a0 78  17 9a d9 1e 08 00 45 00   ··>T·S·x ······E·
0010  02 76 00 00 40 00 40 06  b8 a8 0a 00 00 56 80 77   ·v··@·@· ·····V·w
0020  f5 0c da f6 00 50 63 94  e0 3f 20 65 9e af 50 18   ·····Pc· ·? e··P·
0030  10 00 23 a1 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 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  43 61 63 68 65 2d 43 6f  6e 74 72 6f 6c 3a 20 6d   Cache-Co ntrol: m
00b0  61 78 2d 61 67 65 3d 30  0d 0a 55 70 67 72 61 64   ax-age=0 ··Upgrad
00c0  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu re-Reque
00d0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
00e0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00f0  28 4d 61 63 69 6e 74 6f  73 68 3b 20 49 6e 74 65   (Macinto sh; Inte
0100  6c 20 4d 61 63 20 4f 53  20 58 20 31 30 5f 31 35   l Mac OS  X 10_15
0110  5f 37 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   _7) Appl eWebKit/
0120  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0130  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0140  65 2f 31 31 36 2e 30 2e  30 2e 30 20 53 61 66 61   e/116.0. 0.0 Safa
0150  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63 63 65 70   ri/537.3 6··Accep
0160  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0170  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0180  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
0190  6d 6c 3b 71 3d 30 2e 39  2c 69 6d 61 67 65 2f 61   ml;q=0.9 ,image/a
01a0  76 69 66 2c 69 6d 61 67  65 2f 77 65 62 70 2c 69   vif,imag e/webp,i
01b0  6d 61 67 65 2f 61 70 6e  67 2c 2a 2f 2a 3b 71 3d   mage/apn g,*/*;q=
01c0  30 2e 38 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   0.8,appl ication/
01d0  73 69 67 6e 65 64 2d 65  78 63 68 61 6e 67 65 3b   signed-e xchange;
01e0  76 3d 62 33 3b 71 3d 30  2e 37 0d 0a 41 63 63 65   v=b3;q=0 .7··Acce
01f0  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0200  70 2c 20 64 65 66 6c 61  74 65 0d 0a 41 63 63 65   p, defla te··Acce
0210  70 74 2d 4c 61 6e 67 75  61 67 65 3a 20 65 6e 2d   pt-Langu age: en-
0220  55 53 2c 65 6e 3b 71 3d  30 2e 39 0d 0a 49 66 2d   US,en;q= 0.9··If-
0230  4e 6f 6e 65 2d 4d 61 74  63 68 3a 20 22 35 31 2d   None-Mat ch: "51-
0240  36 30 34 64 32 61 63 36  35 38 63 36 32 22 0d 0a   604d2ac6 58c62"··
0250  49 66 2d 4d 6f 64 69 66  69 65 64 2d 53 69 6e 63   If-Modif ied-Sinc
0260  65 3a 20 46 72 69 2c 20  30 38 20 53 65 70 20 32   e: Fri,  08 Sep 2
0270  30 32 33 20 30 35 3a 35  39 3a 30 32 20 47 4d 54   023 05:5 9:02 GMT
0280  0d 0a 0d 0a                                        ····
```

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (tcp.checksum), 2 bytes

Packets: 12057 · Displayed: 20 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

Task 8

Wireshark, a program used for monitoring computer networks, can sometimes be misused if it falls into the wrong hands. It has the potential to be used for malicious purposes, such as spying on visited websites and capturing IDs and passwords. This could lead to the compromise of sensitive information. In today's world, where many businesses operate online and people often work remotely, if individuals with malicious intent use a program like Wireshark to monitor browsing habits and interactions, it can negatively impact businesses on a global scale.

While Wireshark can be a helpful tool, it also has the capacity to cause trouble. For instance, it can eavesdrop on network conversations, steal private data like passwords, and even manipulate data in transit. Malicious actors can also overload a network with excessive traffic to disrupt its functioning. In addition, they can exploit Wireshark to identify vulnerabilities in a network for future attacks. Public Wi-Fi networks are particularly vulnerable to privacy invasions when Wireshark is used for unauthorized surveillance.

I believe that Wireshark should not be freely accessible to the general public because the information it can extract has the potential to harm individuals. Wireshark itself is a critical program for ensuring citizens' safety when used correctly and responsibly, but it should only be entrusted to individuals with good intentions. However, providing access to Wireshark for educational purposes in schools is of paramount importance. It helps students, network experts, and security professionals learn about networks and how to safeguard them effectively.

Professionals employ Wireshark for beneficial purposes. Yet, when Wireshark is readily available to everyone, it becomes easier for malicious individuals to employ it for nefarious activities. While there are laws in place to penalize those who misuse it, enforcement may not always deter malicious use, so only trusted professionals should be able to use Wireshark and teach wire shark for further enhancement of the program to be used for the safety of the citizens.