Wireshark Lab 1

Started: Feb 19 at 5:22pm

Quiz Instructions

We will be using the Wireshark packet sniffer [http://www.wireshark.org/ (http://www.wireshark.org/)] for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer. Also, technically speaking, Wireshark captures link-layer frames as shown in Figure 1, but uses the generic term "packet" to refer to link-layer frames, network-layer datagrams, transport-layer segments, and application-layer messages, so we'll use the less-precise "packet" term here to go along with Wireshark convention). Wireshark is a free network protocol analyzer that runs on Windows, Mac, and Linux/Unix computers. It's an ideal packet analyzer for our labs – it is stable, has a large user base and well-documented support that includes a user-guide (http://www.wireshark.org/docs/wsug_html_chunked/ (http://www.wireshark.org/docs/wsug_html_chunked/)), man pages (http://www.wireshark.org/docs/man-pages/ (http://www.wireshark.org/docs/man-pages/)), and a detailed FAQ (http://www.wireshark.org/faq.html (http://www.wireshark.org/faq.html)), rich functionality that includes the capability to analyze hundreds of protocols, and a well-designed user interface. It operates in computers using Ethernet, serial (PPP), 802.11 (WiFi) wireless LANs, and many other link-layer technologies.

In order to run Wireshark, you'll need to have access to a computer that supports both Wireshark and the *libpcap* or *WinPCap* packet capture library. The *libpcap* software will be installed for you, if it is not installed within your operating system, when you install Wireshark. See http://www.wireshark.org/download.html (http://www.wireshark.org/download.html) for a list of supported operating systems and download sites.

Download and install the Wireshark software:

- Go to http://www.wireshark.org/download.html (http://www.wireshark.org/download.html) and download and install the Wireshark binary for your computer.

The Wireshark FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.

Question 1 1 pts

Your friend installed the Wireshark and tried to capture some HTTP packets with it. So, they opened their web browser and accessed a website. However, they did not get any HTTP packets. You already checked with them, and they are sure that their computer is connected to the Internet.

What is the reason for this problem.

○ The operating system automatically converts all HTTP requests to HTTPS.

○ The website is using HTTP/3, which is incompatible with Wireshark.

● They accessed a website with HTTPS protocol

○ HTTP packets are too small to be detected by Wireshark.

Question 2 1 pts

You collected a Wireshark trace which of the following protocols is not supported by the Wireshark? (Assume encryption keys are not available

●
Fortinet SSL VPN

○
MQTT

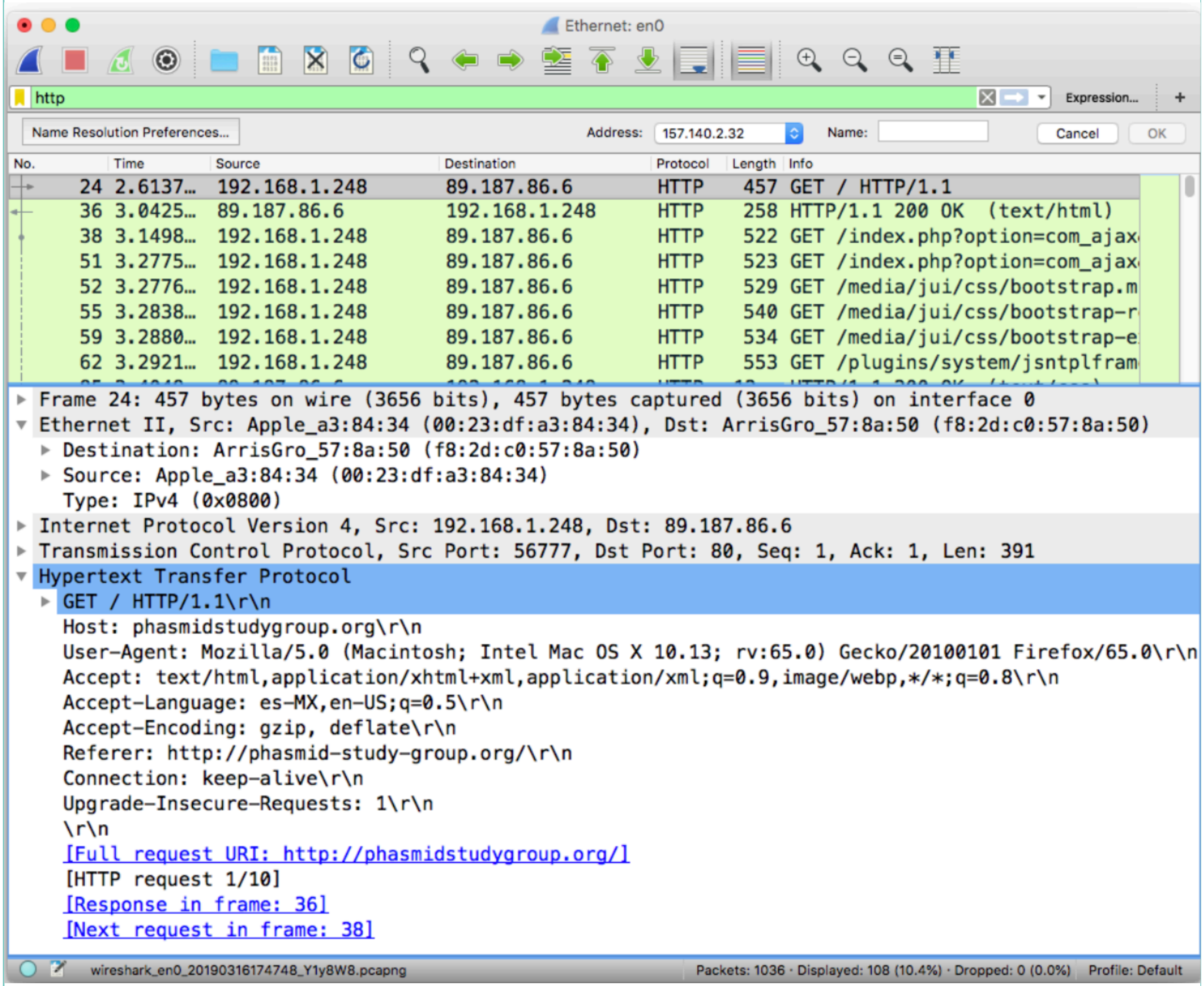
○
ICMP

○
TCP

Question 3 1 pts

Note: This question has two correct answers. one for question A and one for question B make sure you selected both of them.

Suppose you are viewing the following wireshark capture of an HTTP exchange that retrieves the home page of a site. All HTTP connections are TCP



```
No.   Time         Source          Destination     Protocol  Length  Info
  24  2.6137…      192.168.1.248   89.187.86.6     HTTP      457     GET / HTTP/1.1
  36  3.0425…      89.187.86.6     192.168.1.248   HTTP      258     HTTP/1.1 200 OK  (text/html)
  38  3.1498…      192.168.1.248   89.187.86.6     HTTP      522     GET /index.php?option=com_ajax
  51  3.2775…      192.168.1.248   89.187.86.6     HTTP      523     GET /index.php?option=com_ajax
  52  3.2776…      192.168.1.248   89.187.86.6     HTTP      529     GET /media/jui/css/bootstrap.m
  55  3.2838…      192.168.1.248   89.187.86.6     HTTP      540     GET /media/jui/css/bootstrap-r
  59  3.2880…      192.168.1.248   89.187.86.6     HTTP      534     GET /media/jui/css/bootstrap-e
  62  3.2921…      192.168.1.248   89.187.86.6     HTTP      553     GET /plugins/system/jsntplfram
```

```
▶ Frame 24: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface 0
▼ Ethernet II, Src: Apple_a3:84:34 (00:23:df:a3:84:34), Dst: ArrisGro_57:8a:50 (f8:2d:c0:57:8a:50)
  ▶ Destination: ArrisGro_57:8a:50 (f8:2d:c0:57:8a:50)
  ▶ Source: Apple_a3:84:34 (00:23:df:a3:84:34)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.1.248, Dst: 89.187.86.6
▶ Transmission Control Protocol, Src Port: 56777, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: phasmidstudygroup.org\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:65.0) Gecko/20100101 Firefox/65.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: es-MX,en-US;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://phasmid-study-group.org/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://phasmidstudygroup.org/]
    [HTTP request 1/10]
    [Response in frame: 36]
    [Next request in frame: 38]
```

```
wireshark_en0_20190316174748_Y1y8W8.pcapng    Packets: 1036 · Displayed: 108 (10.4%) · Dropped: 0 (0.0%)    Profile: Default
```

[A]-Is the packet No. 36 a response or request. Identify the source and destination ports and IPs.

[B]-In our lab's LAN with lots of computers and busy students, I captured two packets with the following grids. I have hidden one of the numbers. What could it be? Assume these are all packets that are using TCP connections.

	Packet 1 Source	Packet 1 Dest	Packet 2 Source	Packet 2 Dest
IP	192.168.1.248	89.187.86.6	192.18.1.248	<HIDDEN VAL>
Port	56777	80	56777	80

☐
[A]- Request, Source:192.168.1.248:56777, Destination: 89.187.86.6:80

☑
[A]- Response, Source: 89.187.86.6:80, Destination:192.168.1.248:56777

☐
[A]- Request, Source: 89.187.86.6:80, Destination:192.168.1.248:56777

☐
[B]- Something other than 89.187.86.6, Because it's undeterminable since we dont know anything about the connection

☐
[A]- Response, Source:192.168.1.248:56777, Destination: 89.187.86.6:80

☑
[B]- 89.187.86.6, Because a source port is associated with a single connection and since we know the sources are the same, the destinations have to be also

☐
[B]- 89.187.86.6, Although this is not a single connection but randomly multiple connections can have same ports

☐
[A]- Response, Source: 89.187.86.6:5677, Destination:192.168.1.248:80

Question 4 1 pts

Assume you have the following Wireshark trace. We tried to access a website that used HTTP protocol. We sent HTTP request at the packet number 874. How long did it take (in milliseconds) for the server to return the request?

Wireshark Trace: Trace.pcapng (https://canvas.uh.edu/courses/20819/files/6092761?wrap=1) (https://canvas.uh.edu/courses/20819/files/6092761/download?download_frd=1)

○
117

●
90

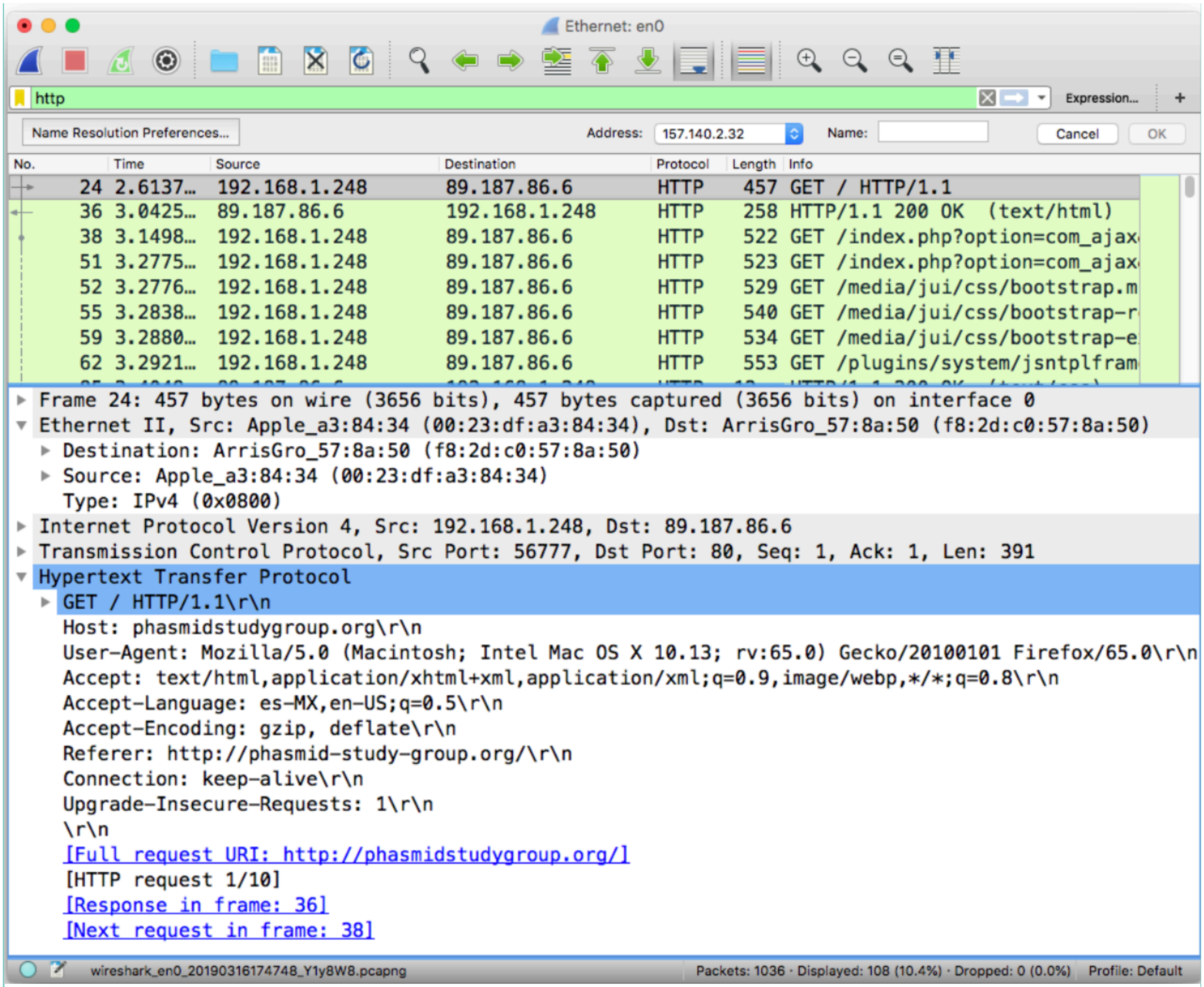
○
93

○
113

Question 5 1 pts

Note: This question has two correct answers. one for question A and one for question B make sure you selected both of them.

Suppose you are viewing the following wireshark capture of an HTTP exchange that retrieves the home page of a site. All HTTP connections are TCP



http

Address: 157.140.2.32 Name:

```
No.  Time       Source          Destination     Protocol  Length  Info
 24  2.6137…    192.168.1.248   89.187.86.6     HTTP      457     GET / HTTP/1.1
 36  3.0425…    89.187.86.6     192.168.1.248   HTTP      258     HTTP/1.1 200 OK  (text/html)
 38  3.1498…    192.168.1.248   89.187.86.6     HTTP      522     GET /index.php?option=com_ajax
 51  3.2775…    192.168.1.248   89.187.86.6     HTTP      523     GET /index.php?option=com_ajax
 52  3.2776…    192.168.1.248   89.187.86.6     HTTP      529     GET /media/jui/css/bootstrap.m
 55  3.2838…    192.168.1.248   89.187.86.6     HTTP      540     GET /media/jui/css/bootstrap-r
 59  3.2880…    192.168.1.248   89.187.86.6     HTTP      534     GET /media/jui/css/bootstrap-e
 62  3.2921…    192.168.1.248   89.187.86.6     HTTP      553     GET /plugins/system/jsntplfram
```

```
▶ Frame 24: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface 0
▼ Ethernet II, Src: Apple_a3:84:34 (00:23:df:a3:84:34), Dst: ArrisGro_57:8a:50 (f8:2d:c0:57:8a:50)
  ▶ Destination: ArrisGro_57:8a:50 (f8:2d:c0:57:8a:50)
  ▶ Source: Apple_a3:84:34 (00:23:df:a3:84:34)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.1.248, Dst: 89.187.86.6
▶ Transmission Control Protocol, Src Port: 56777, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: phasmidstudygroup.org\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:65.0) Gecko/20100101 Firefox/65.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: es-MX,en-US;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://phasmid-study-group.org/\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://phasmidstudygroup.org/]
    [HTTP request 1/10]
    [Response in frame: 36]
    [Next request in frame: 38]
```

wireshark_en0_20190316174748_Y1y8W8.pcapng   Packets: 1036 · Displayed: 108 (10.4%) · Dropped: 0 (0.0%)   Profile: Default

[A]-Is the packet No. 24 a response or request. Identify the source and destination ports and IPs.

[B]-In our lab's LAN with lots of computers and busy students, I captured two packets with the following grids. I have hidden one of the numbers. What could it be? Assume these are all packets that are using TCP connections.

	Packet 1 Source	Packet 1 Dest		Packet 2 Source	Packet 2 Dest
IP	192.168.1.248	89.187.86.6		<HIDDEN VAL>	89.187.86.6
Port	56777	80		56777	62

□
[A]- Request, Source: 192.168.1.248:80, Destination:89.187.86.6:56777

□
[A]- Request, Source: 89.187.86.6:80 , Destination:192.168.1.248:56777

□
[B]- 192.168.1.248, They are from the same connection

□
[A]- Response, Source: 89.187.86.6:80 , Destination:192.168.1.248:56777

□
[A]- Response, Source: 192.168.1.248:56777, Destination:89.187.86.6:80

☐
[B]- Something other than 92.168.1.248, Since there is already a connection from 92.168.1.248.

☑
[B]- Something other than 192.168.1.248, Different destination ports means different socket connections

☑
[A]- Request, Source: 192.168.1.248:56777, Destination:89.187.86.6:80

No new data to save. Last checked at 7:58pm Submit Quiz