

1.

- a. The IP address of my computer is 192.168.1.254, the IP address of the website given is 160.153.92.101

Work:

http						
No.	Time	Source	Destination	Protocol	Length	Info
116	5.117125	192.168.1.254	160.153.92.101	HTTP	484	GET / HTTP/1.1
123	5.201062	160.153.92.101	192.168.1.254	HTTP	749	HTTP/1.1 200 OK (text/html)

- b. Three different protocols that occur when I run the sniffer are: DNS, TCP, and HTTP.

Work:

HTTP:

79	5.546860	192.168.1.254	160.153.92.101	HTTP
----	----------	---------------	----------------	------

TCP:

48	4.038396	192.168.1.254	160.153.92.101	TCP
----	----------	---------------	----------------	-----

DNS:

47	4.038088	2603:9001:300:54f4::	2603:9001:300:54f4::	DNS	125	Standard query response 0x7e07 A www.dpgraph.com CNAME dpgraph.com A 160.153.92.101
----	----------	----------------------	----------------------	-----	-----	---

- c. No, it kept the connection open. We can determine this as there are no tcp finish flags. ie:

tcp.flags.fin == 1						
No.	Time	Source	Destination	Protocol	Length	Info

- d. It ran http 1.1 as displayed in the screenshot in part a

2.

- a. 3

http.request.method == "GET"						
Filter Buttons Preferences... Label: Enter a description for the filter button						
Comment: Enter a comment for the filter button						
No.	Time	Source	Destination	Protocol	Length	Info
241	7.688055	192.168.1.254	64.24.91.226	HTTP	483	GET / HTTP/1.1
266	7.913247	192.168.1.254	64.24.91.226	HTTP	436	GET /banner/ads.pl?page=01 HTTP/1.1
282	8.064221	192.168.1.254	64.24.91.226	HTTP	445	GET /images/coverupbanner468x60.gif HTTP/1.1

b. 1

The image shows the Wireshark interface. At the top, a filter bar contains the text `http.response.code == 200`. Below the filter bar, there are input fields for 'Label' and 'Comment'. The main packet list table is visible, with the following data:

No.	Time	Source	Destination	Protocol	Length	Info
286	8.135536	64.24.91.226	192.168.1.254	HTTP	652	HTTP/1.1 200 OK (GIF87a)

c. 445 bytes:

The image shows the Wireshark interface. The packet list table at the top has the following data:

No.	Time	Source	Destination	Protocol	Length	Info
282	8.064221	192.168.1.254	64.24.91.226	HTTP	445	GET /images/coverupbanner468x60.gif HTTP/1.1

Below the packet list, the 'Wireshark · Packet 282 · Wi-Fi' pane is open, showing the details of the selected packet:

▶ Frame 282: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF...