

Manguiat, Glenn Karlo D.

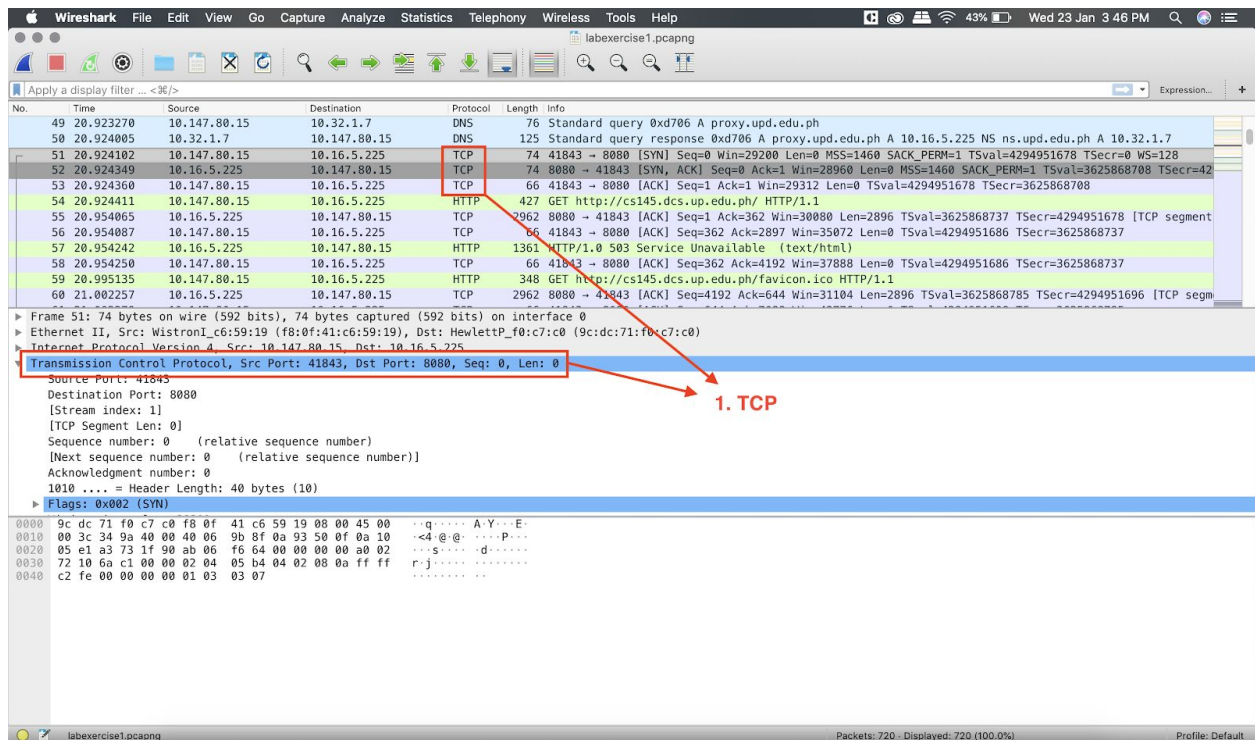
2015-13937

MQR - HONOR

CS 145 - Laboratory Exercise #1

(1a) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 8 above. Provide annotated screenshots or images of the packets that support your answer.

- TCP



- HTTP

Wireshark capture showing an HTTP GET request. The packet list shows a GET request to `http://cs145.dcs.up.edu.ph/ HTTP/1.1`. The packet details pane shows the Hypertext Transfer Protocol section, which includes the request line, host, user-agent, accept, accept-language, accept-encoding, dnt, connection, upgrade-insecure-requests, and full request URI. A red box highlights the Hypertext Transfer Protocol section, and a red arrow points to the '2. HTTP' label.

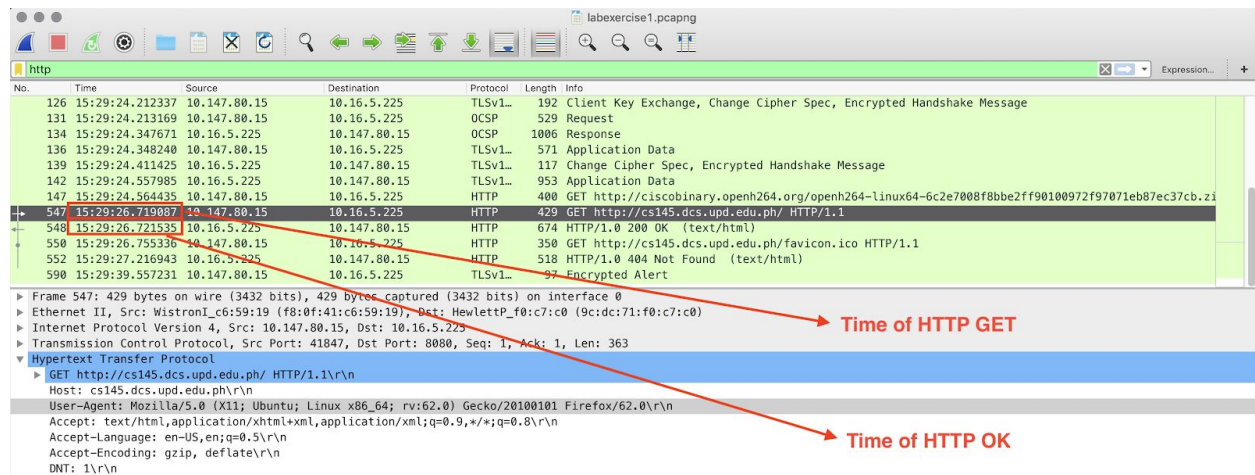
2. HTTP

- DNS

Wireshark capture showing a DNS query. The packet list shows a DNS query to `10.32.1.7`. The packet details pane shows the Domain Name System (query) section, which includes the query type, query flags, and query name. A red box highlights the Domain Name System (query) section, and a red arrow points to the '3. DNS' label.

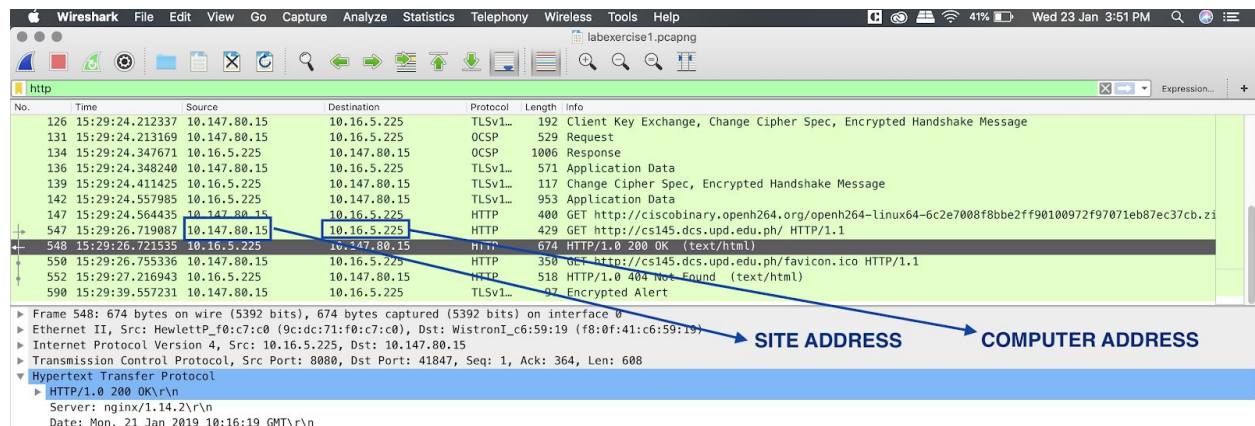
3. DNS

(1b) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? Provide annotated screenshots or images of the packets that support your answer, plus computations.



- HTTP OK time - 5:29:26.721535
- HTTP GET time - 15:29:26.719087
- It took $26.721535 - 26.719087$ seconds or **0.002448 seconds**

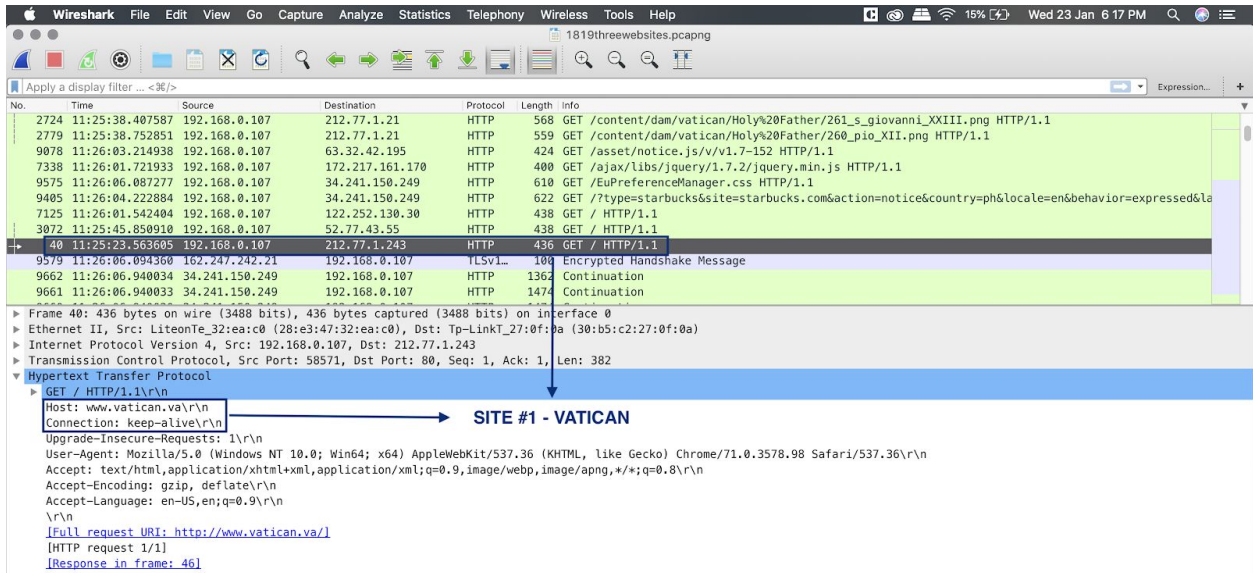
(1c) What is the Internet address of the CS 145 sample site web server? What is the Internet address of your computer?



- The Internet address of CS 145 sample web server is 10.147.80.15, while the computer's address is 10.16.5.225.

(2a) As previously mentioned, the trace file provided shows the trace for a machine/web browser which visited three websites in quick succession. What are these three websites? Provide annotated screenshots or images of the packets that support your answer.

- www.vatican.va

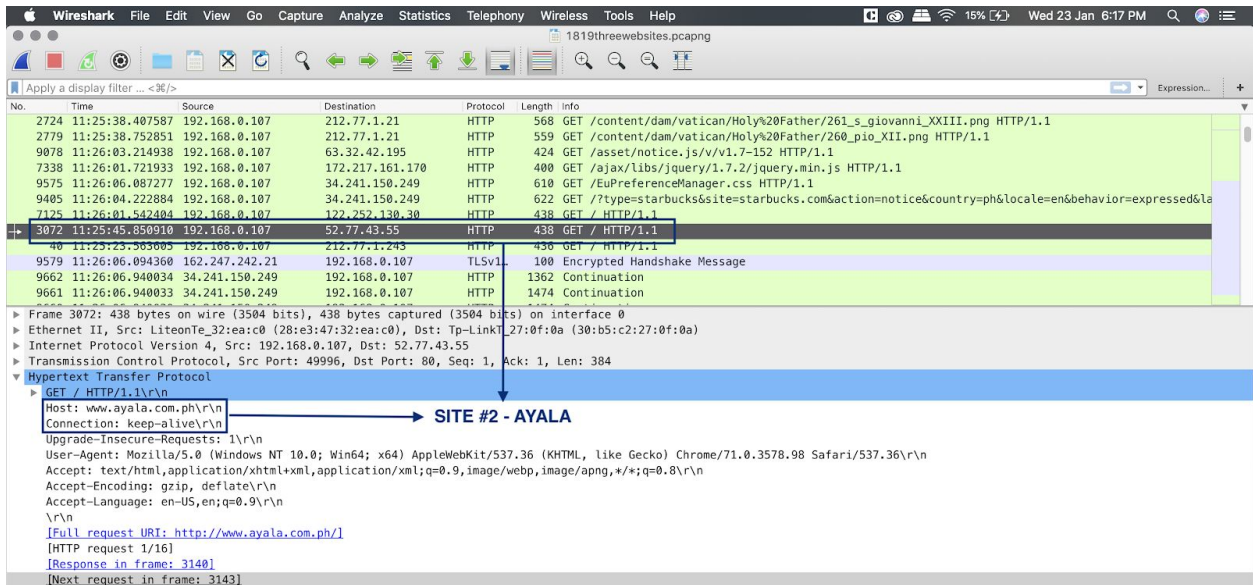


Wireshark capture showing traffic to www.vatican.va. The packet list shows a GET request for `/content/dam/vatican/Holy%20Father/261_s_giovanni_XXIII.png` at time 11:25:23.563605. The packet details pane shows the Hypertext Transfer Protocol section with the following information:

- Host: www.vatican.va/
- Connection: keep-alive
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Full request URI: <http://www.vatican.va/>
- HTTP request 1/1
- Response in frame: 461

The packet is labeled **SITE #1 - VATICAN**.

- www.ayala.com.ph

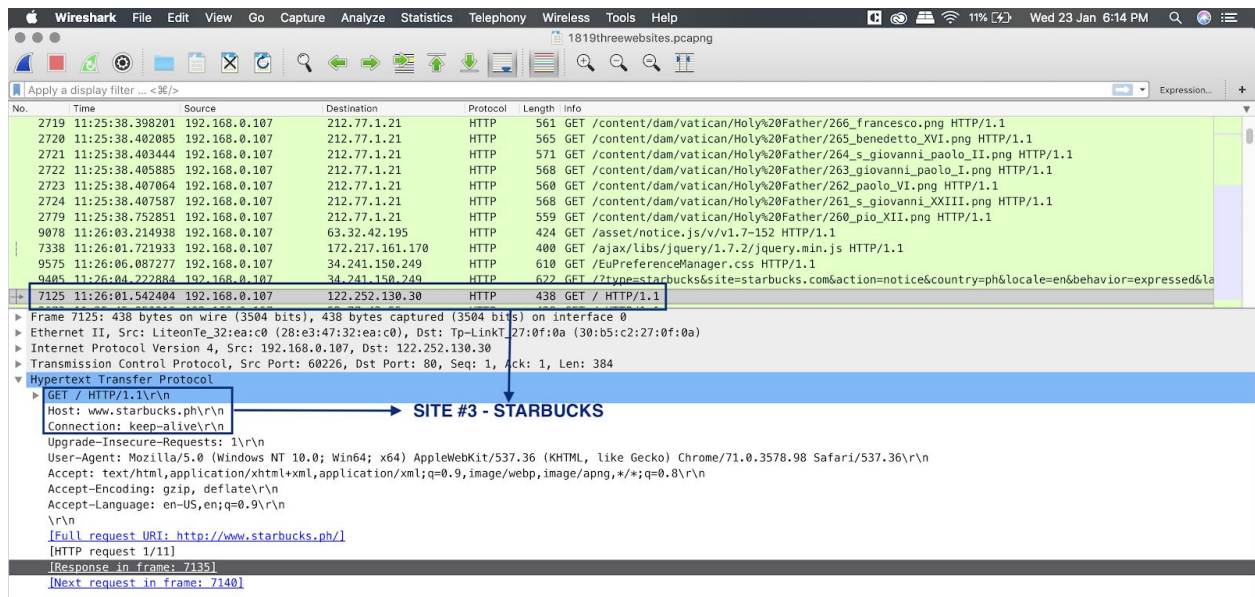


Wireshark capture showing traffic to www.ayala.com.ph. The packet list shows a GET request for `/content/dam/vatican/Holy%20Father/261_s_giovanni_XXIII.png` at time 11:25:23.563605. The packet details pane shows the Hypertext Transfer Protocol section with the following information:

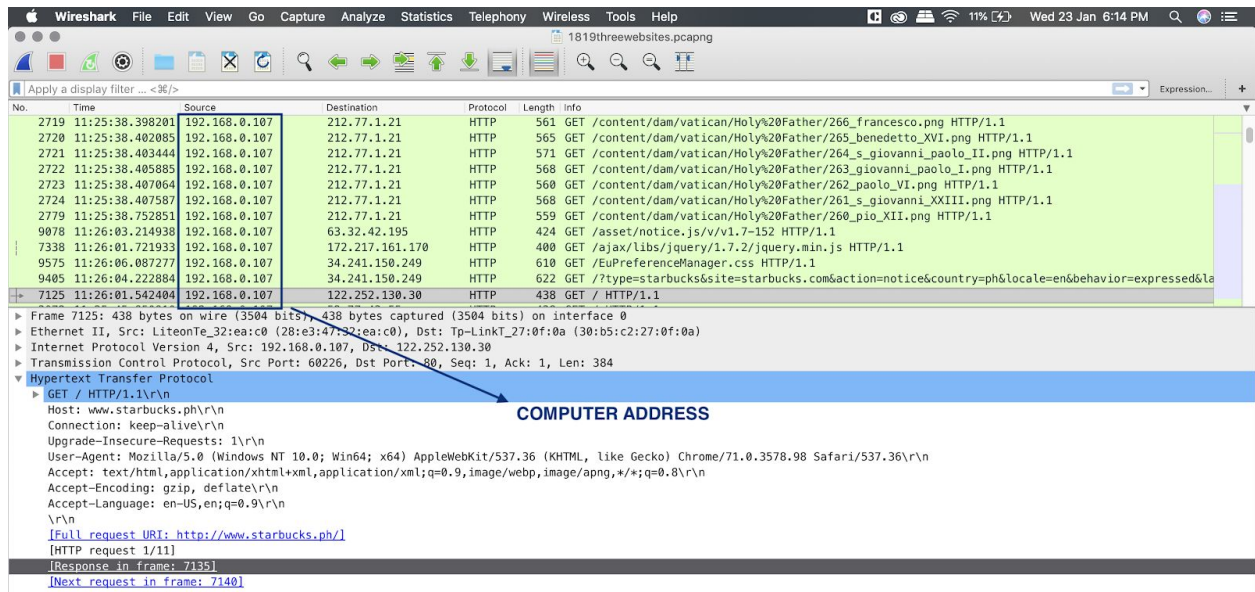
- Host: www.ayala.com.ph/
- Connection: keep-alive
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Full request URI: <http://www.ayala.com.ph/>
- HTTP request 1/16
- Response in frame: 3140
- Next request in frame: 3143

The packet is labeled **SITE #2 - AYALA**.

- www.starbucks.com.ph



(2b) What is the Internet address of the computer which produced the trace file? Provide annotated screenshots or images of the packet(s) that support your answer.



- The Internet address of the computer is 192.168.0.107.