Juan Dominguez
Salissa Hernandez
Noah T. Nyabadza

Assignment 1

1. Mobile network operators need to constantly maintain a subscriber's approximate location using procedures such as registration, where the phone periodically informs the network of its location area, and paging, where the network broadcasts to find a device for an incoming call or data. This is bad for users because it leads to privacy concerns and issues. For instance, if the operator's records demonstrate that a user is frequently registering near a hospital or clinic, this information could be leaked or misused to expose sensitive personal details, which can enable profiling or surveillance without the user's consent. Nevertheless, this same location tracking can also be beneficial for users because it enables important services. For instance, during a 911 emergency call, the system can use the phone's location information to guide first responders to the caller, even if the caller is not able to provide their location. This enables faster response times and can drastically save lives.

2. To set up a small computer lab for 8 SMU students, the LAN would need to entail several key components.

    a. **Devices:** Each student would use a laptop connected to the network. These laptops could connect in two ways: (1) directly to a central Ethernet switch using Cat6 cables for maximum stability, or (2) wirelessly through a wireless access point (WAP) connected to the same switch. A router would then link the lab to the wider campus backbone or Internet, handling DHCP for IP addressing and NAT if required. To support collaboration, the lab could also include a shared printer or a file server accessible to all students.

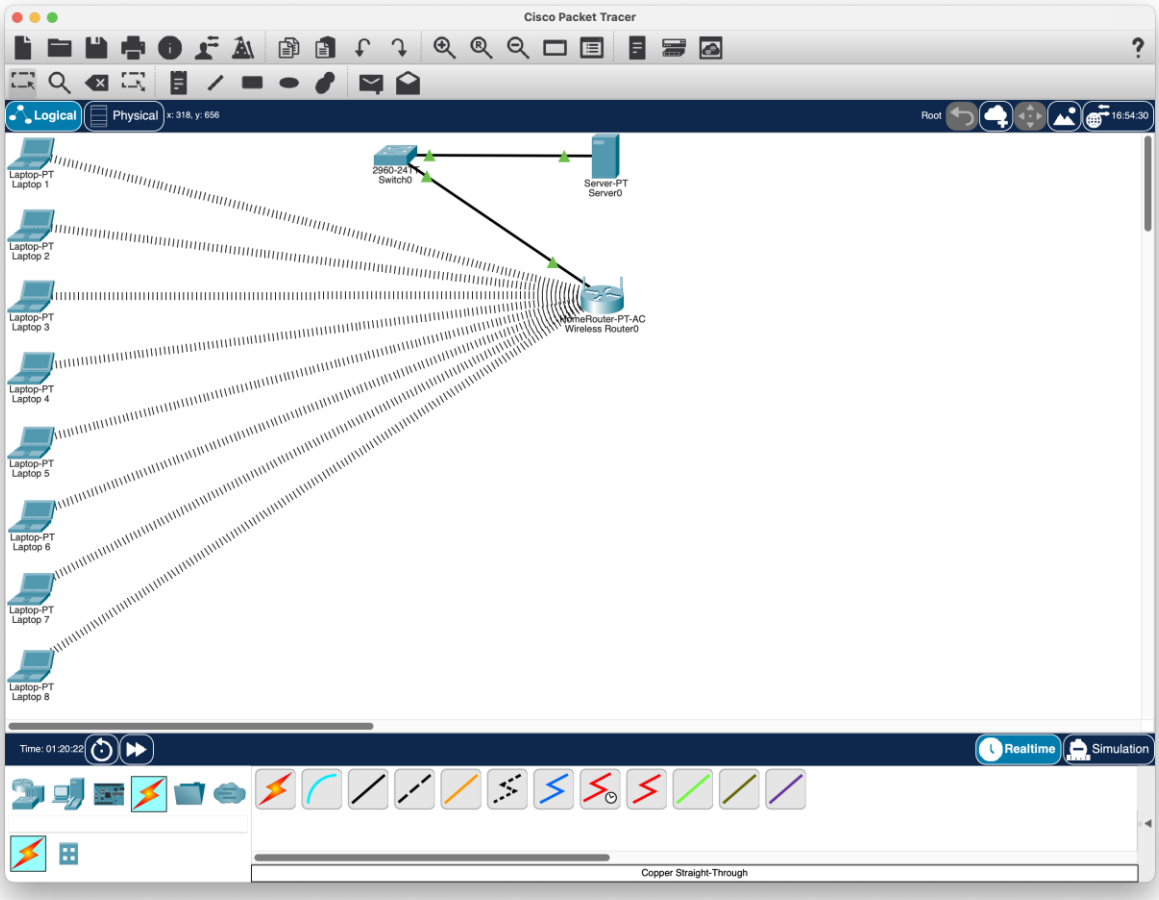
    b. **Connections:** The LAN would use a star topology, where each laptop connects either by Ethernet or Wi-Fi to the central switch and wireless access point. The switch uplinks to the router, which serves as the default gateway (192.168.10.1). The router's DHCP service automatically assigns addresses in the 192.168.10.0/24 subnet, ensuring consistency and reducing manual configuration. This setup allows each laptop to communicate with the gateway and access external resources.

    c. **Use cases:** Students would use the LAN for accessing SMU's online course materials, submitting assignments, collaborating on shared projects, and printing documents via a shared network printer. The network would also support secure file sharing and software updates. Wireless access provides mobility for students moving between seats or using mobile devices, while wired connections ensure reliability for bandwidth-intensive tasks. Overall, this laptop-based LAN balances flexibility, simplicity, and scalability, making it well-suited for a small classroom or computer lab setting.

Juan Dominguez
Salissa Hernandez
Noah T. Nyabadza

Assignment 1

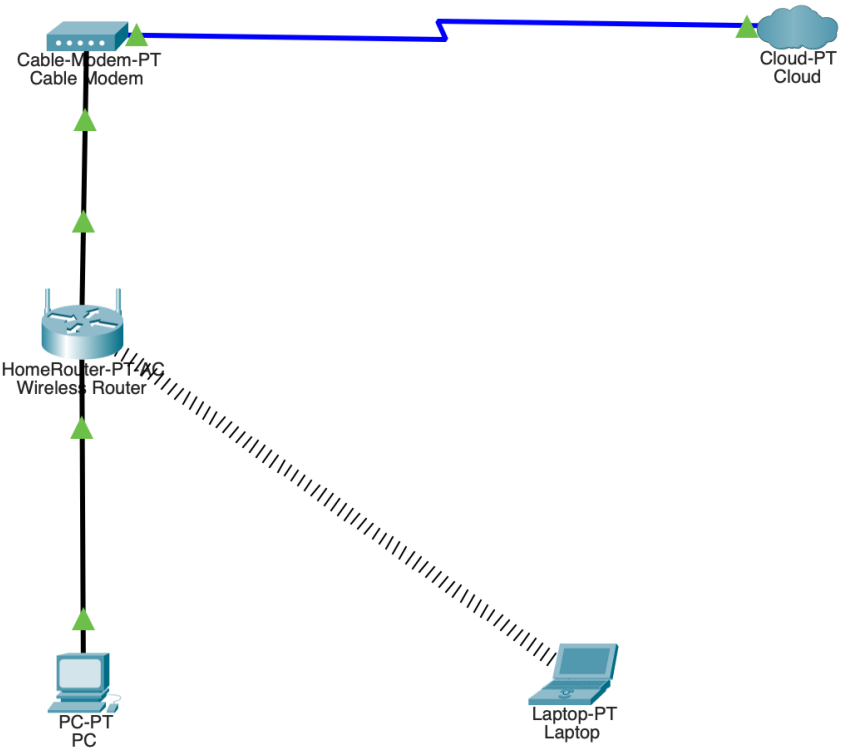
3.



Juan Dominguez
Salissa Hernandez
Noah T. Nyabadza

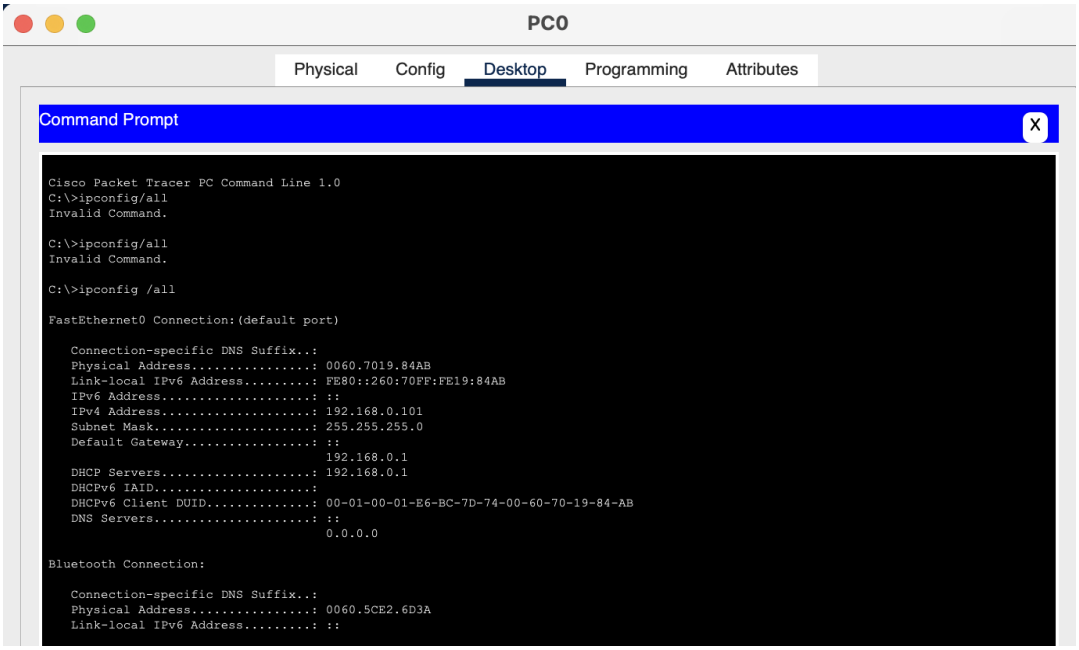
Assignment 1

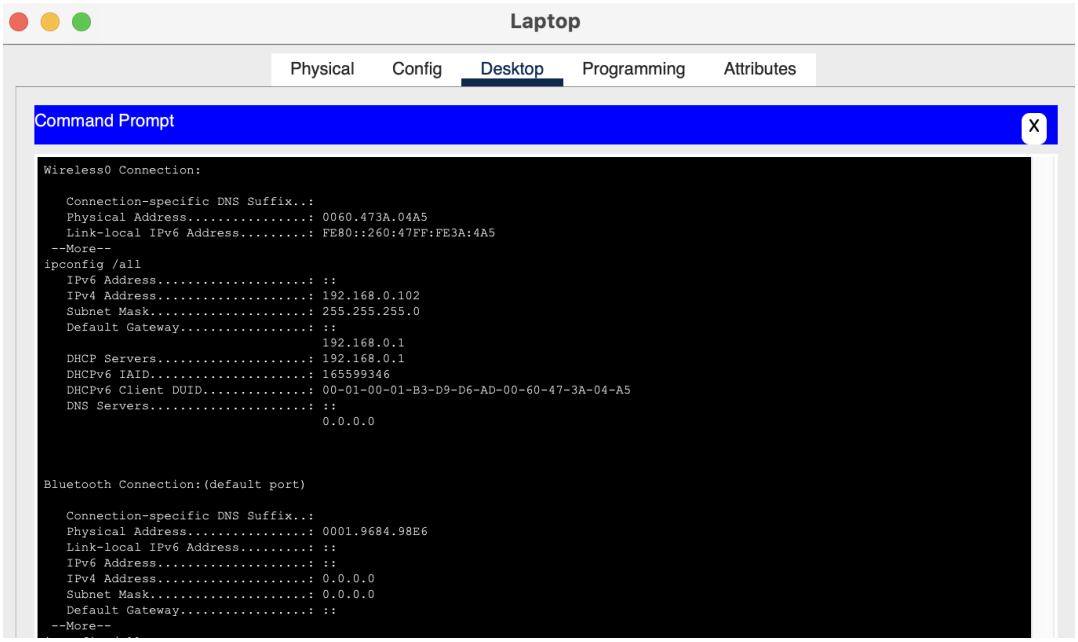
4.



Juan Dominguez
Salissa Hernandez
Noah T. Nyabadza

Assignment 1





5. Answer the following questions, based on your Wireshark experimentation:

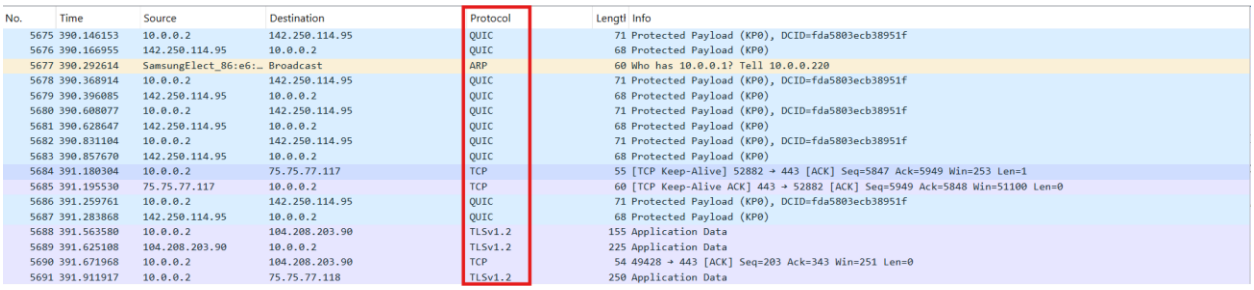
1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

   a. ARP

Juan Dominguez
Salissa Hernandez
Noah T. Nyabadza

Assignment 1

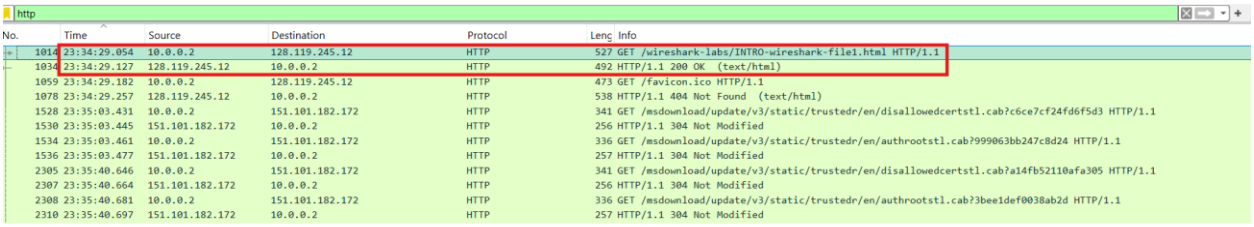
b. TCP
c. QUIC



No.	Time	Source	Destination	Protocol	Length	Info
5675	390.146153	10.0.0.2	142.250.114.95	QUIC	71	Protected Payload (KP0), DCID=fda5803ecb38951f
5676	390.166955	142.250.114.95	10.0.0.2	QUIC	68	Protected Payload (KP0)
5677	390.292614	SamsungElect_86:e6:…	Broadcast	ARP	60	Who has 10.0.0.1? Tell 10.0.0.220
5678	390.368914	10.0.0.2	142.250.114.95	QUIC	71	Protected Payload (KP0), DCID=fda5803ecb38951f
5679	390.396085	142.250.114.95	10.0.0.2	QUIC	68	Protected Payload (KP0)
5680	390.608077	10.0.0.2	142.250.114.95	QUIC	71	Protected Payload (KP0), DCID=fda5803ecb38951f
5681	390.628647	142.250.114.95	10.0.0.2	QUIC	68	Protected Payload (KP0)
5682	390.831104	10.0.0.2	142.250.114.95	QUIC	71	Protected Payload (KP0), DCID=fda5803ecb38951f
5683	390.857670	142.250.114.95	10.0.0.2	QUIC	68	Protected Payload (KP0)
5684	391.180304	10.0.0.2	75.75.77.117	TCP	55	[TCP Keep-Alive] 52882 → 443 [ACK] Seq=5847 Ack=5949 Win=253 Len=1
5685	391.195530	75.75.77.117	10.0.0.2	TCP	60	[TCP Keep-Alive ACK] 443 → 52882 [ACK] Seq=5949 Ack=5848 Win=51100 Len=0
5686	391.259761	10.0.0.2	142.250.114.95	QUIC	71	Protected Payload (KP0), DCID=fda5803ecb38951f
5687	391.283868	142.250.114.95	10.0.0.2	QUIC	68	Protected Payload (KP0)
5688	391.563580	10.0.0.2	104.208.203.90	TLSv1.2	155	Application Data
5689	391.625108	104.208.203.90	10.0.0.2	TLSv1.2	225	Application Data
5690	391.671968	10.0.0.2	104.208.203.90	TCP	54	49428 → 443 [ACK] Seq=203 Ack=343 Win=251 Len=0
5691	391.911917	10.0.0.2	75.75.77.118	TLSv1.2	250	Application Data

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

a. It took from 23:34:29.054 to 23:34:29.127 = 73 Milliseconds



http

No.	Time	Source	Destination	Protocol	Length	Info
1014	23:34:29.054	10.0.0.2	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1034	23:34:29.127	128.119.245.12	10.0.0.2	HTTP	492	HTTP/1.1 200 OK (text/html)
1059	23:34:29.182	10.0.0.2	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
1078	23:34:29.257	128.119.245.12	10.0.0.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1528	23:35:03.431	10.0.0.2	151.101.182.172	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?c6ce7cf24fd6f5d3 HTTP/1.1
1530	23:35:03.445	151.101.182.172	10.0.0.2	HTTP	256	HTTP/1.1 304 Not Modified
1534	23:35:03.461	10.0.0.2	151.101.182.172	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?999063bb247c8d24 HTTP/1.1
1536	23:35:03.477	151.101.182.172	10.0.0.2	HTTP	257	HTTP/1.1 304 Not Modified
2305	23:35:40.646	10.0.0.2	151.101.182.172	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?a14fb52110afa305 HTTP/1.1
2307	23:35:40.664	151.101.182.172	10.0.0.2	HTTP	256	HTTP/1.1 304 Not Modified
2308	23:35:40.681	10.0.0.2	151.101.182.172	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?3bee1def0038ab2d HTTP/1.1
2310	23:35:40.697	151.101.182.172	10.0.0.2	HTTP	257	HTTP/1.1 304 Not Modified

3. What is the Internet address of the gaia.cs.umass.edu (also known as www net.cs.umass.edu)?

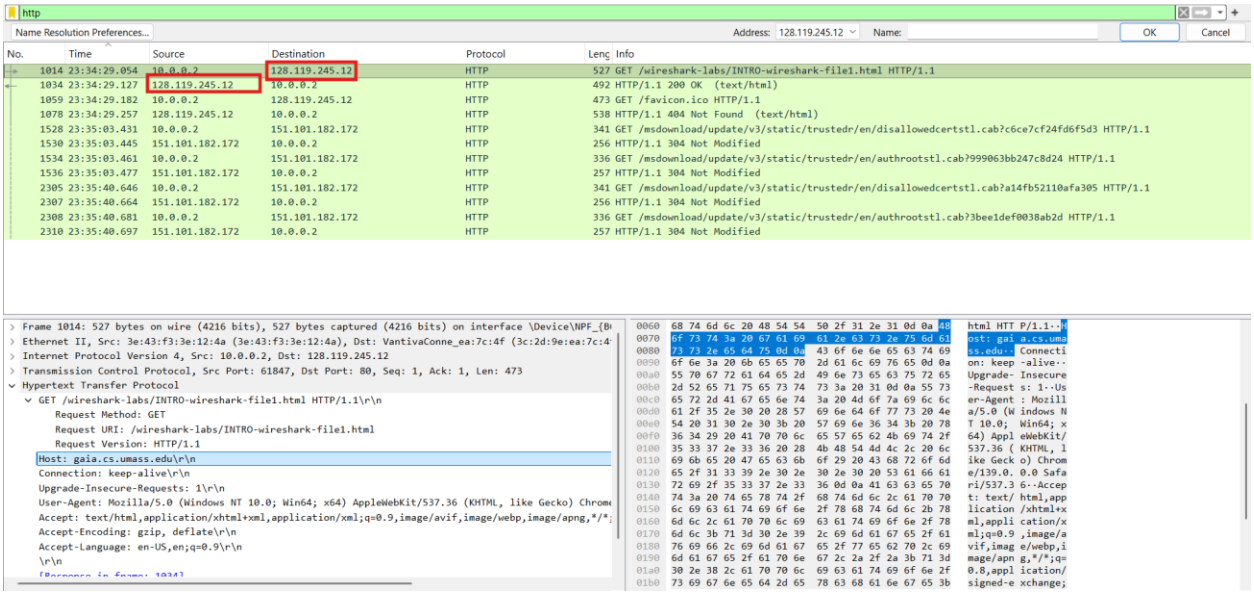
a. 128.119.245.12

What is the Internet address of your computer?

b. 10.0.0.2

Juan Dominguez
Salissa Hernandez
Noah T. Nyabadza

Assignment 1



4. Print the two HTTP messages (GET and OK) referred to in question 2 above. 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.

[GET] HTTP Message

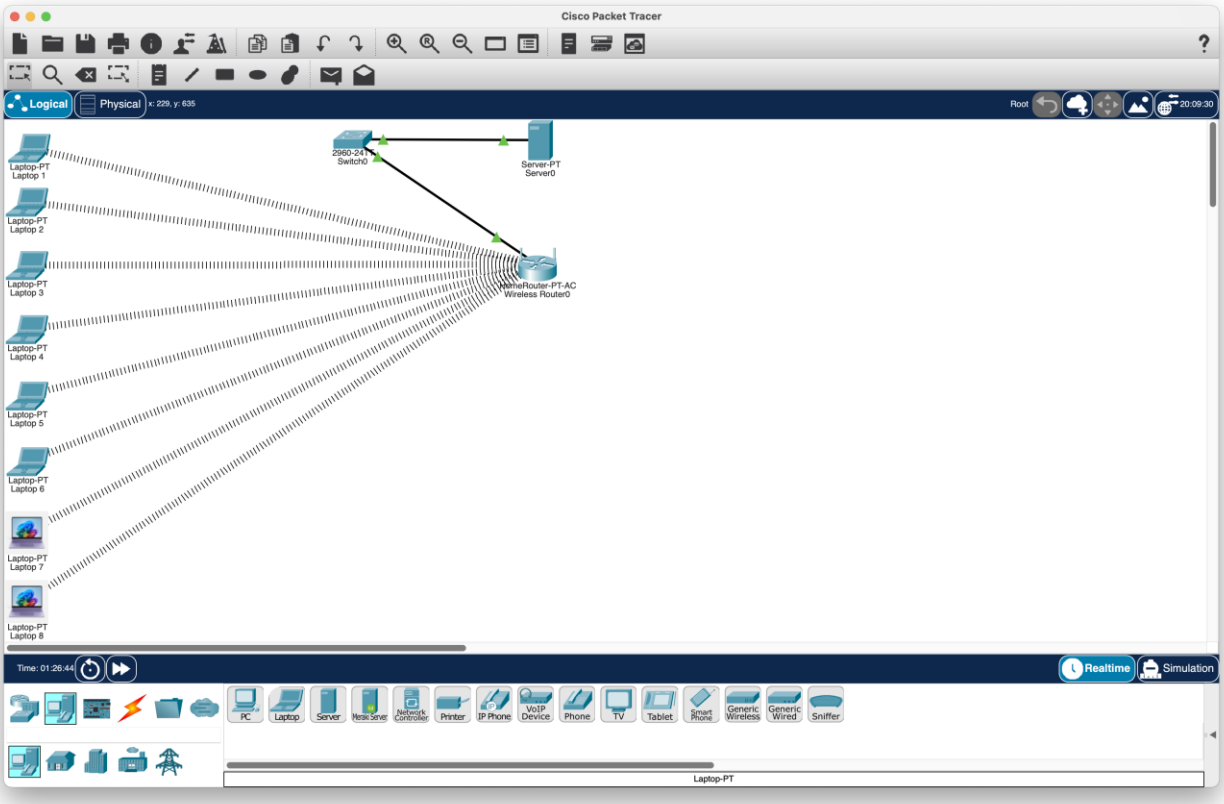
```
No.     Time         Source               Destination          Protocol Length Info
   1014 23:34:29.054 10.0.0.2             128.119.245.12       HTTP     527    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 1014: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface \Device\NPF_{BC2399D8-F85C-44A7-97CB-11D16FD39997}, id
0
Ethernet II, Src: 3e:43:f3:3e:12:4a (3e:43:f3:3e:12:4a), Dst: VantivaConne_ea:7c:4f (3c:2d:9e:ea:7c:4f)
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61847, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
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/139.0.0.0 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
    \r\n
    [Response in frame: 1034]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
No.     Time         Source               Destination          Protocol Length Info
   1034 23:34:29.127 128.119.245.12       10.0.0.2             HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 1034: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{BC2399D8-F85C-44A7-97CB-11D16FD39997}, id
0
```

[OK] HTTP Message

Juan Dominguez
Salissa Hernandez
Noah T. Nyabadza

Assignment 1

```
Ethernet II, Src: VantivaConne_ea:7c:4f (3c:2d:9e:ea:7c:4f), Dst: 3e:43:f3:3e:12:4a (3e:43:f3:3e:12:4a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 61847, Seq: 1, Ack: 474, 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: Fri, 05 Sep 2025 04:34:28 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: Thu, 04 Sep 2025 05:59:02 GMT\r\n
    ETag: "51-63df36b075b5a"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    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: 1014]
    [Time since request: 0.072711000 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)
```



6.