Assignment 2.1 - What happens when you type www.gatech.edu?

Submit Assignment

Due Friday by 11:59pm **Points** 7 **Submitting** a file upload **Available** after Sep 19 at 12am

For this assignment, we are going to revisit the question for assignment 2.

Please answer the question “what happens when I type www.gatech.edu in a web browser?” using a packet capture that you will generate.

To guide your answers, visit “www.gatech.edu” in a web browser while capturing your network traffic using tcpdump.

- You should turn in a document that answers the above question in as much detail as you can. This document should include screenshots of Wireshark illustrating each step.
- Make sure you address the question at each layer of the OSI model. It is still OK to skip layer 5.
- Some things, like recursive DNS resolution, will not be present in your packet capture. Make sure you still document the process.
- Your answers should be technical rather than theoretical. Remember, we are asking you specifically what happens when you visit **www.gatech.edu** **(http://www.gatech.edu)** .

To capture your traffic and open in Wireshark:

1. Create a virtual machine using an operating system of your choice. These directions assume you will be using Ubuntu Desktop 16.04. If you have not created a virtual machine before, you will need to install software such as Virtualbox (**https://www.virtualbox.org** **(https://www.virtualbox.org)**). Virtualbox has installation instructions here: http://download.virtualbox.org/virtualbox/5.1.28/UserManual.pdf#page16
2. Create and start a virtual machine using your chosen operating system. In this example, I will be using Ubuntu 16.04 (**https://www.ubuntu.com/download/desktop** **(https://www.ubuntu.com/download/desktop)**)
3. After you've logged in to your virtual machine, open Terminal and enter the following command:

```
sudo apt install tcpdump wireshark
```

4. After tcpdump and Wireshark are installed, start up FireFox (or another web browser of your choice). FireFox is installed by default in Ubuntu 16.04.
5. Next, start capturing network traffic. In Terminal, enter the following command:

```
sudo tcpdump -w ~/Desktop/cs8803.pcap
```

6. Return to FireFox, and type "www.gatech.edu" in the search bar and press enter.
7. After the page has loaded, exit FireFox.
8. In Terminal, press CTRL + c to end the packet capture.
9. Right click the packet capture on your desktop and select "Open with Wireshark"

Assignment 2.1

Criteria	Ratings	Pts
The ARP process on your local network including screenshots of Wireshark		0.5 pts
The DNS process including recursion. You should include screenshots of the query and response in Wireshark.		0.5 pts
The HTTP request with screenshots of Wireshark.		0.5 pts
The HTTP response with screenshots of Wireshark.		0.5 pts
The IP packet with screenshots of Wireshark.		0.5 pts
Layer 2 up until it leaves the home network with screenshots of Wireshark.		0.5 pts
Layer 1 up until it leaves the home network with screenshots of Wireshark.		0.5 pts
The TCP process for the HTTP session. This should include screenshots of multiple packets in Wireshark.		0.5 pts
The UDP process for the DNS query and response. This should include screenshots of multiple packets in Wireshark.		0.5 pts
How routers and switches are involved in the whole process.		0.5 pts
How CAM and ARP tables are involved in the process.		0.5 pts
DNS cacheing.		0.5 pts
What happens at layer 6? Include examples of encoding for the HTTP response. Hint: www.gatech.edu has images.		0.5 pts
Evidence via screenshots that a PCAP was successfully created.		0.5 pts
Extra credit: Run through the whole DNS recursion process locally (you can do this via the dig command). Document this process and use screenshots from a packet capture.		0.5 pts
		Total Points: 7.5