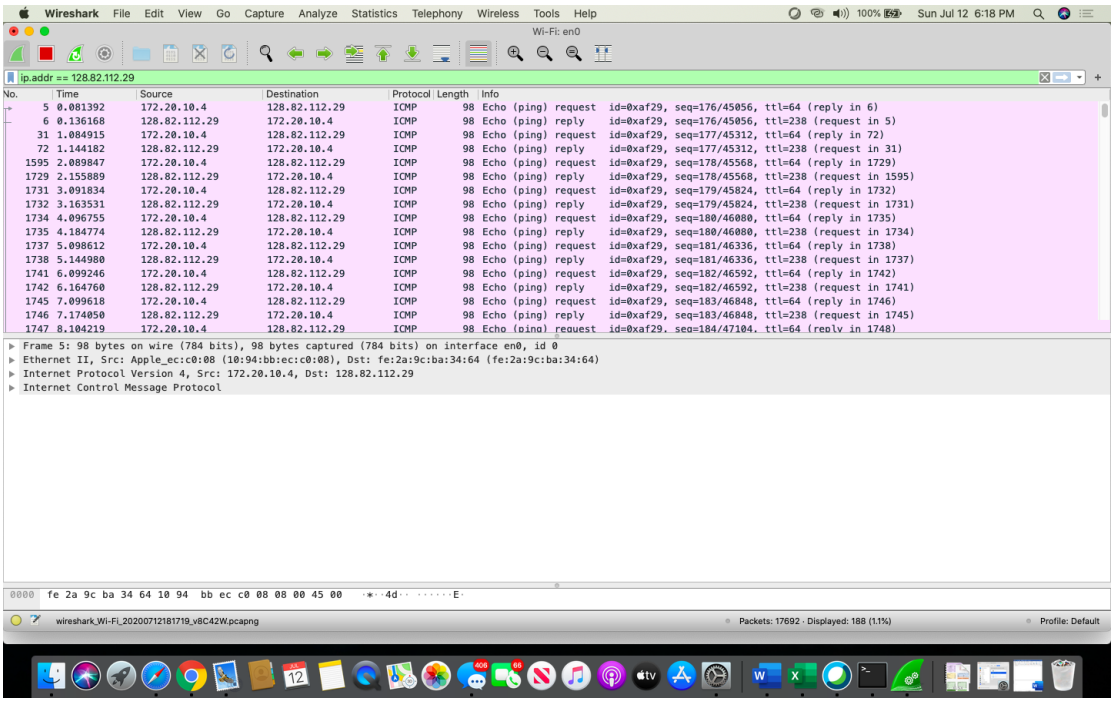
OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

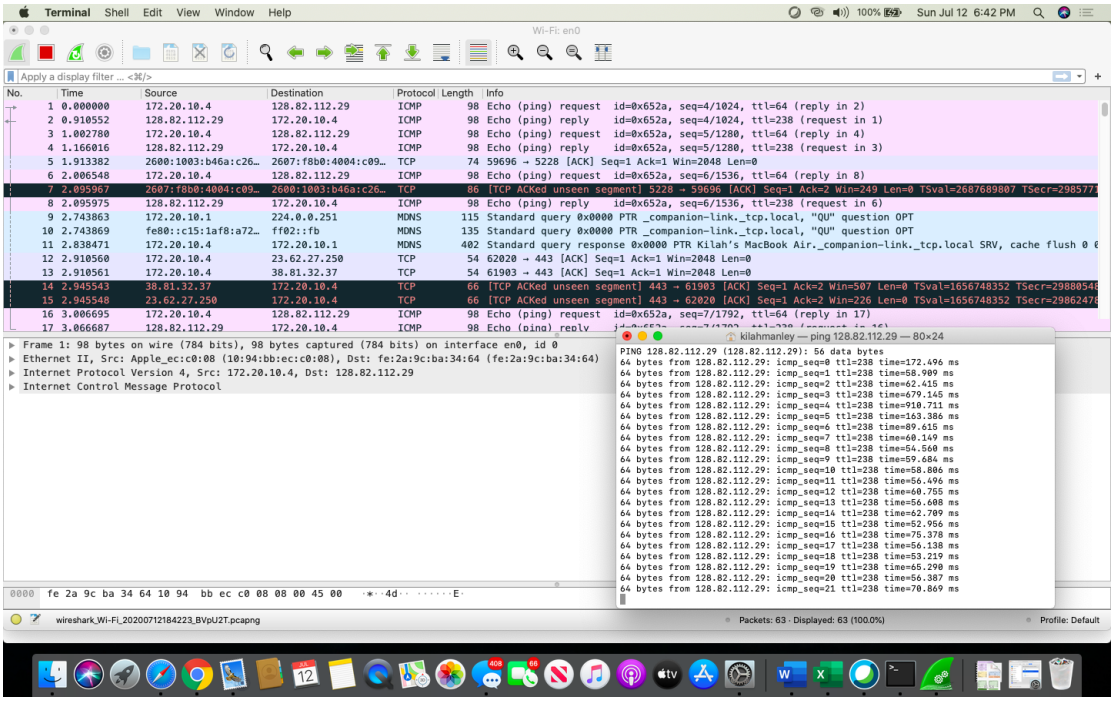
Assignment #2

Kilah

Summer 2020

Task A: Basic Wireshark and tshark practice





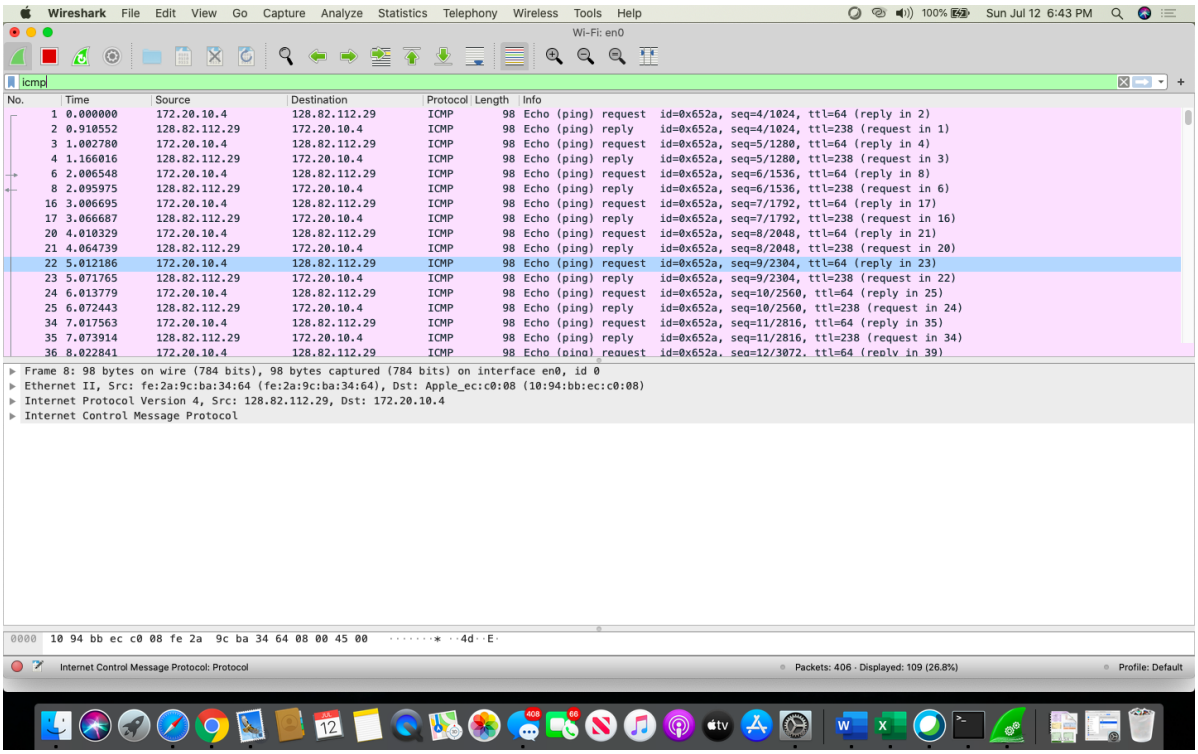


Figure 1 for Task A.1

1. Use **Wireshark** to find out all related packets when you ping the IP address "128.82.112.29"
   - When I ping the IP address 128.82.112.29, my device will send multiple ICMP packets to the target address.
   - I typed in icmp for the 128.82.112.29 ip address

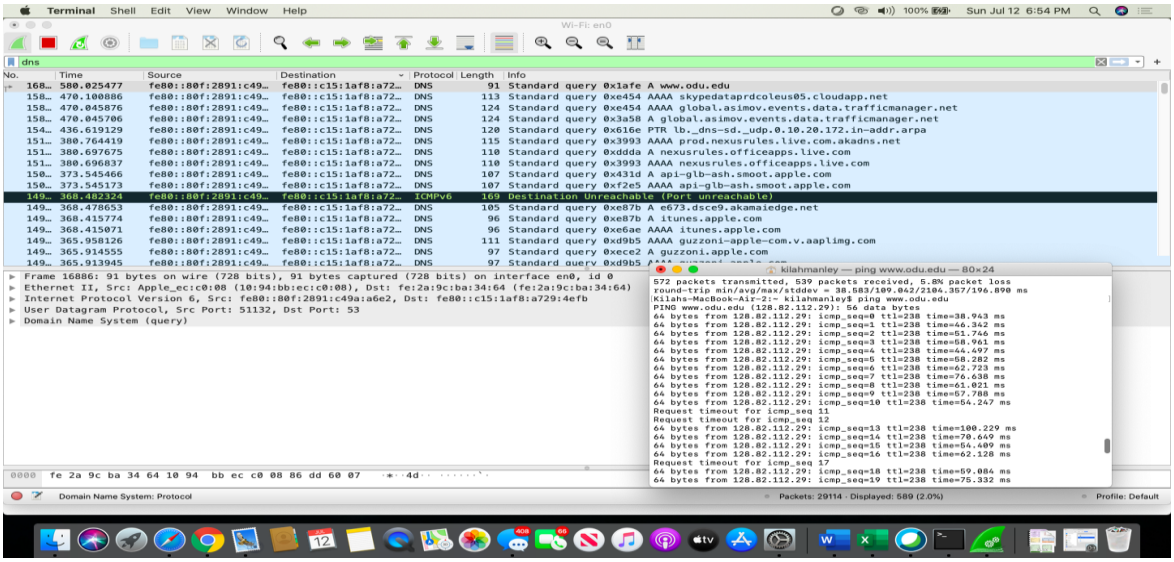
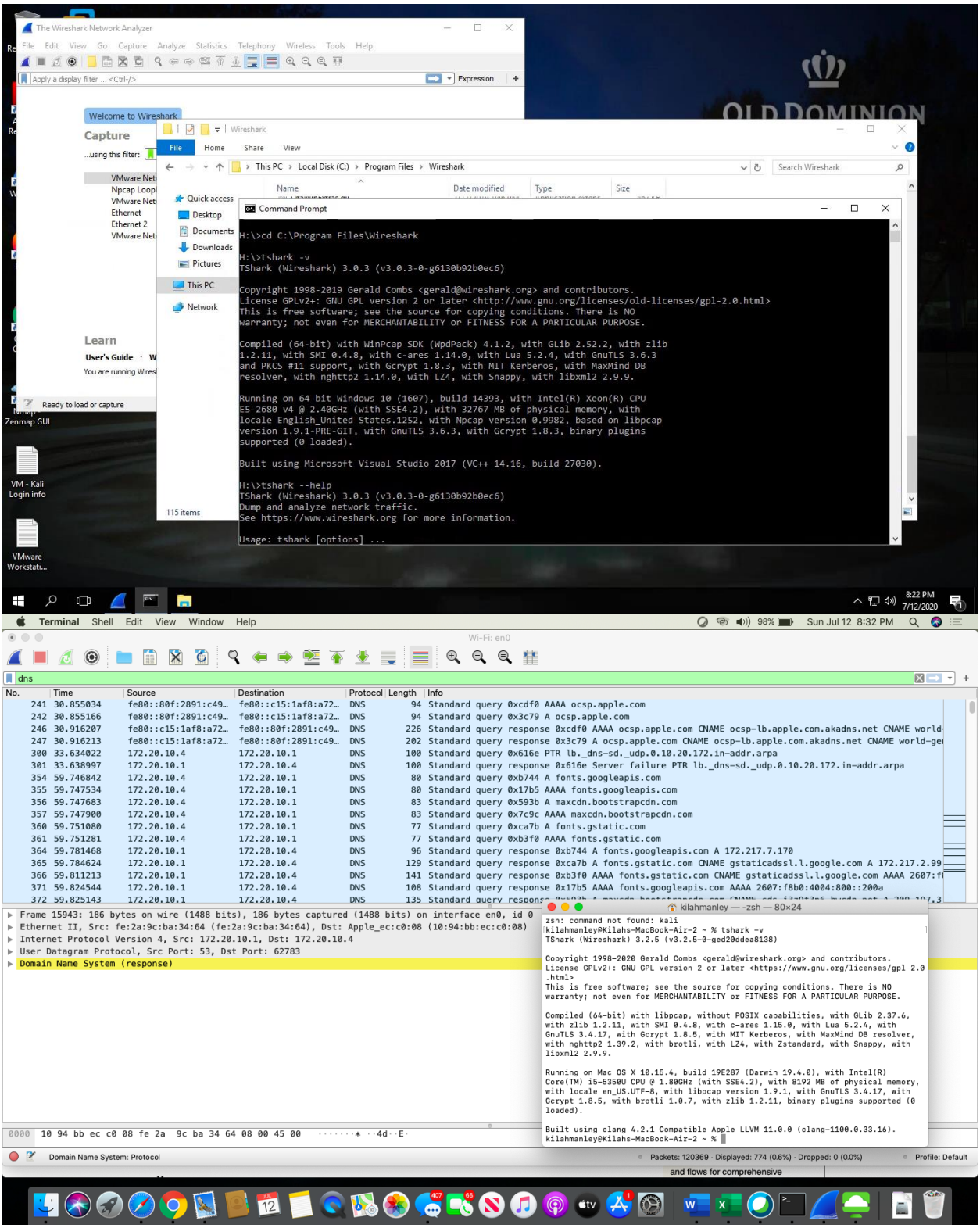


Figure 2 for Task A.2

2. Use **Wireshark** to find out all related packets when you ping the website "www.odu.edu". And mark the **new** packets generated in this traffic (compared with the result of ***task 1*** above). Hint: think about the difference between pinging an IP and pinging a URL.

- When I ping www.odu.edu , my device will send DNS packets to the DNS query to filter and look for IP address that may be alike/the same.



Figures 3 & 4 for Task A.3

3. Use **tshark** capture the DNS query for the ODU official websites. (Refer to Figure 21 in PLE Section 1.4.2
    - I had so much difficulty attempting to get tshark to work on my mac, and nothing worked**, so I used the Cybersecurity Environment and I was able to use tshark on Windows. I opened the command prompt, searched the program files for wireshark, copied the address at the top and used ‘cd’ in the command prompt to change directory and pasted the link address for wireshark to access tshark.
        - (**EDIT: I figured out how to run tshark on my macbook)

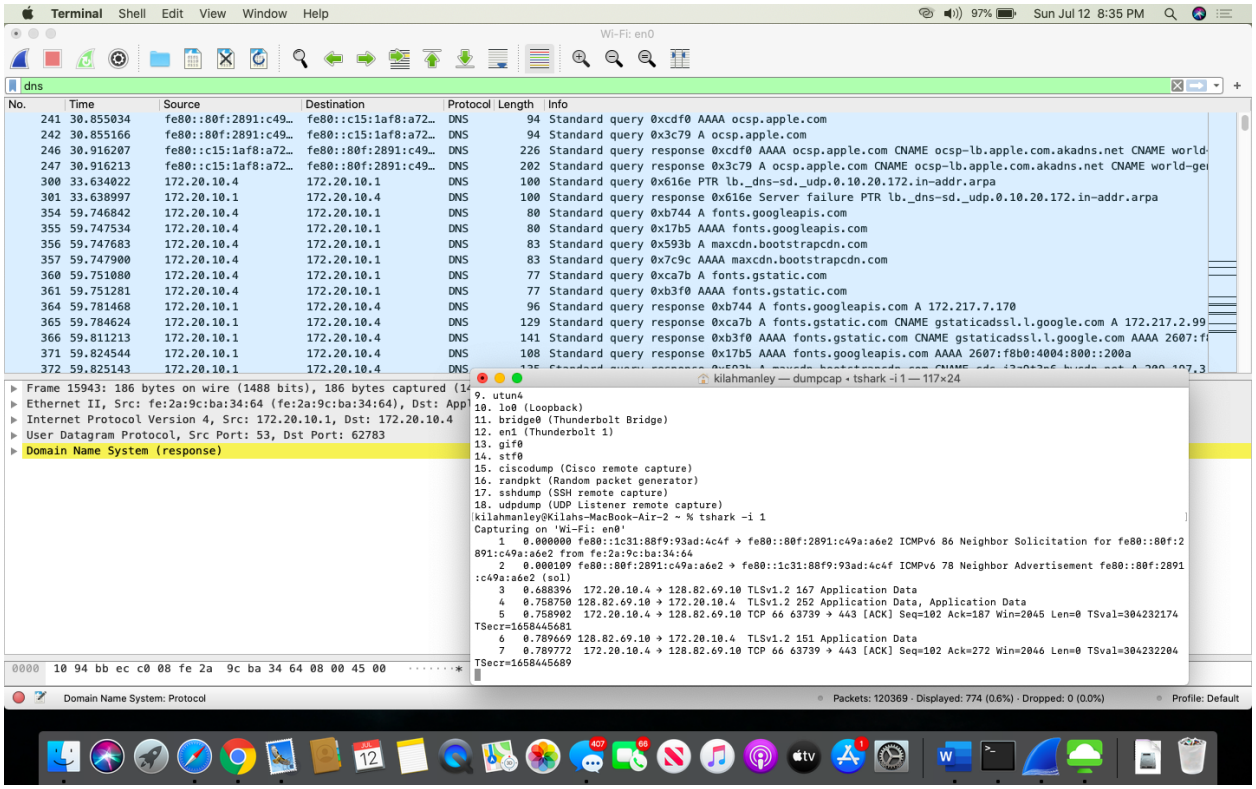
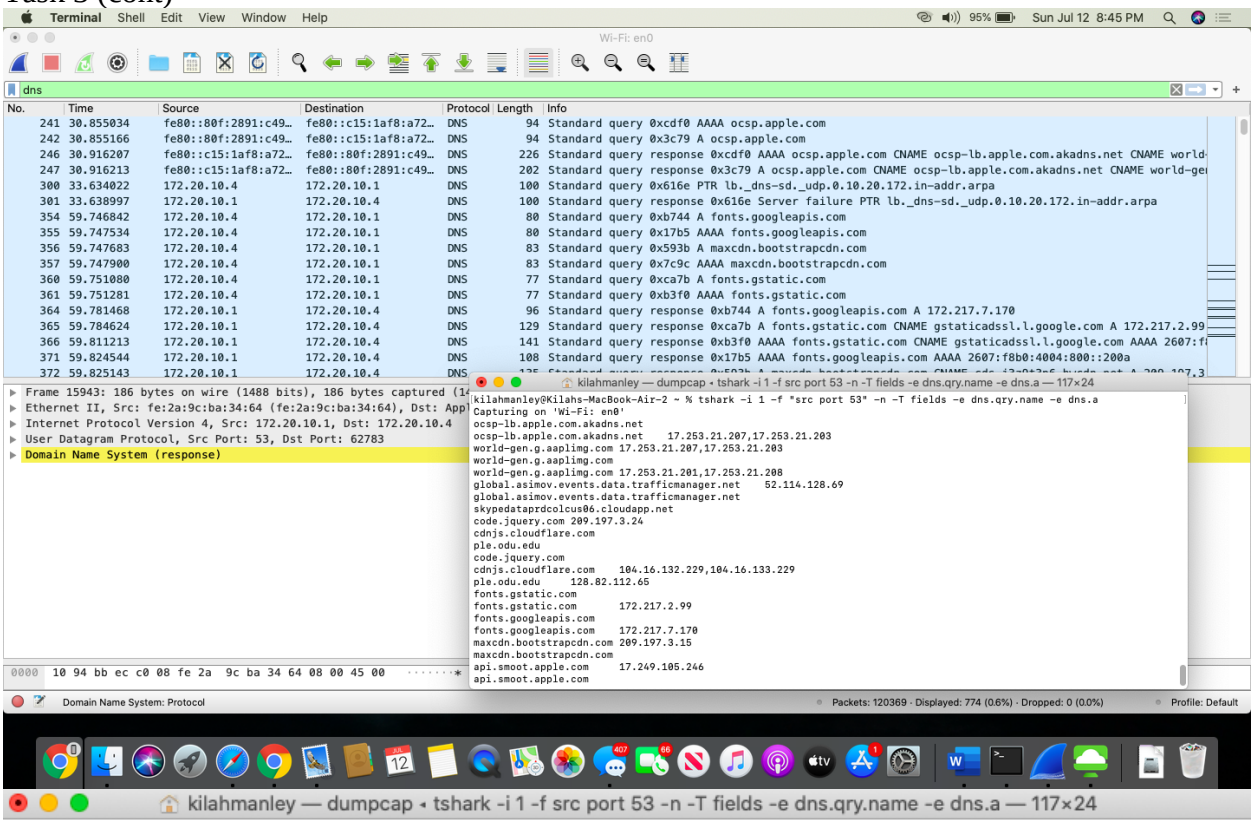


Figure 5 for Task A.3

- This figure shows me capturing data on the correct interface = Wifi

Task 3 (cont)



kilahmanley — dumpcap ◂ tshark -i 1 -f src port 53 -n -T fields -e dns.qry.name -e dns.a — 117×24

```
kilahmanley@Kilahs-MacBook-Air-2 ~ % tshark -i 1 -f "src port 53" -n -T fields -e dns.qry.name -e dns.a
Capturing on 'Wi-Fi: en0'
ocsp-lb.apple.com.akadns.net
ocsp-lb.apple.com.akadns.net    17.253.21.207,17.253.21.203
world-gen.g.aaplimg.com 17.253.21.207,17.253.21.203
world-gen.g.aaplimg.com
world-gen.g.aaplimg.com 17.253.21.201,17.253.21.208
global.asimov.events.data.trafficmanager.net    52.114.128.69
global.asimov.events.data.trafficmanager.net
skypedataprdcolcus06.cloudapp.net
code.jquery.com 209.197.3.24
cdnjs.cloudflare.com
ple.odu.edu
code.jquery.com
cdnjs.cloudflare.com    104.16.132.229,104.16.133.229
ple.odu.edu     128.82.112.65
fonts.gstatic.com
fonts.gstatic.com       172.217.2.99
fonts.googleapis.com
fonts.googleapis.com    172.217.7.170
maxcdn.bootstrapcdn.com 209.197.3.15
maxcdn.bootstrapcdn.com
api.smoot.apple.com     17.249.105.246
api.smoot.apple.com
```

Figure 6 & 7 for Task A.3

- I used ‘tshark -i 1 -f "src port 53" -n -T fields -e dns.qry.name -e dns.a’ command to capture filters
- figure 7 shows ‘www.odu.edu’ with the ip address of 128.82.112.65

4. Visiting a safe HTTP site (the one does not ask you for the username and password, or run any scripts on your browser or local machine). And use **tshark** to capture the whole process. Filter and save the HTTP traffic to your hard drive.
   - I went to tcc.edu
5. Use **Wireshark** to open the saved traffic file from your previous step, then analyze and **export (File -> Export Objects -> HTTP)** the HTTP objects from the traffic.

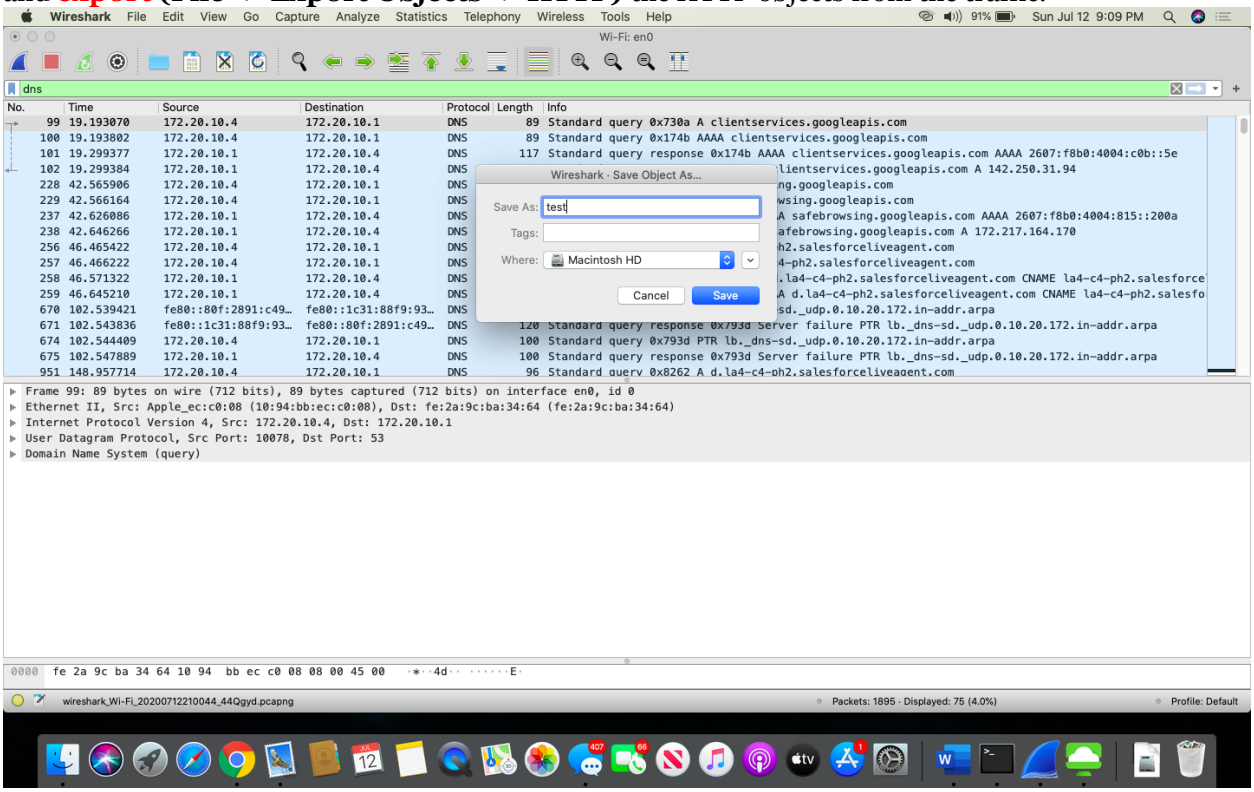


Figure 8 for A.5

Task B: Capture the FTP password

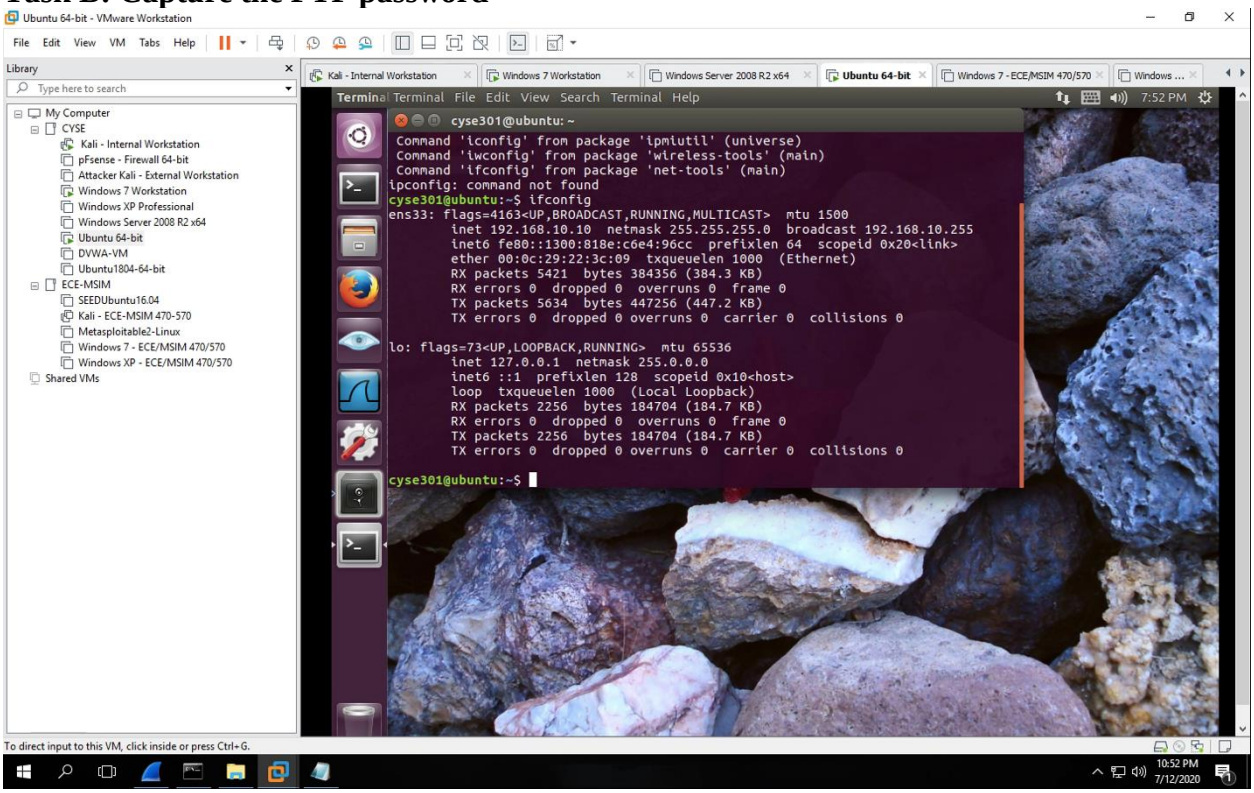


Figure 9 for B.1

- Here I opened up ubuntu and used ‘ifconfig’ to find the IP address (192.168.10.10)

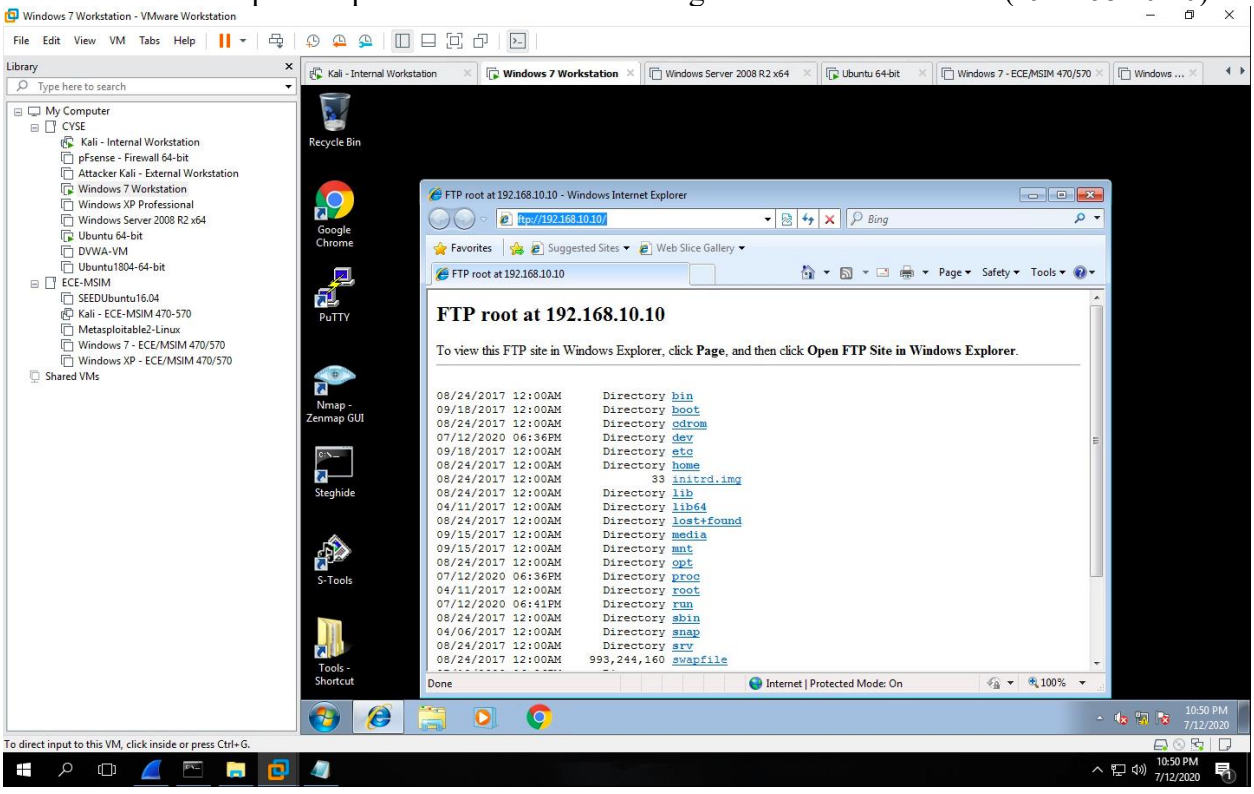
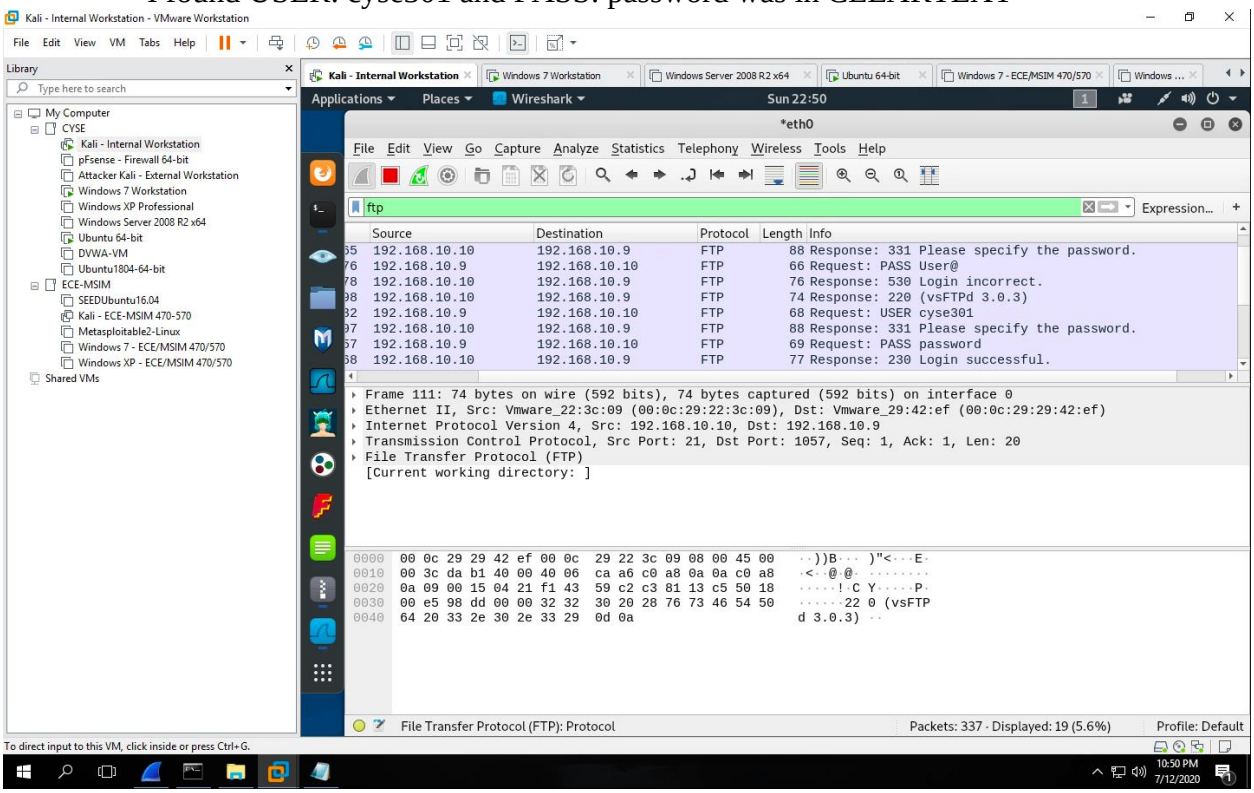


Figure 10 for Task B.

- I then opened up internal kali and ran wireshark
- Then I opened up internet explorer in Windows 7 and typed ‘ftp://192.168.10.10)
- I then went back to Internal Kali and filtered the search to ‘ftp’
- I found USER: cyse301 and PASS: password was in CLEARTEXT



Task C: Discussion

1. What is the difference between Task A-1 and Task A-1?
   - Task A-2, www.odu.edu is a domain name which will give you too many results and will take longer to process.
2. List a few websites nowadays that still use http, are they safe?
   - dictionary.com
   - Washington.edu
   - They are **not** 100% secure and safe.
3. Why does DNS use UDP Stream while HTTP uses TCP Stream?
   - As previously mentioned, in Task A-2, the response time took much longer than Task A-1. UDP is generally faster and does not require a connection (unreliable) because DNS requests are generally small.
   - TCP is connection based and must be ‘acknowledged’ and if not, it will resend the message. In UDP, the message could likely be lost and not resent (unreliable).