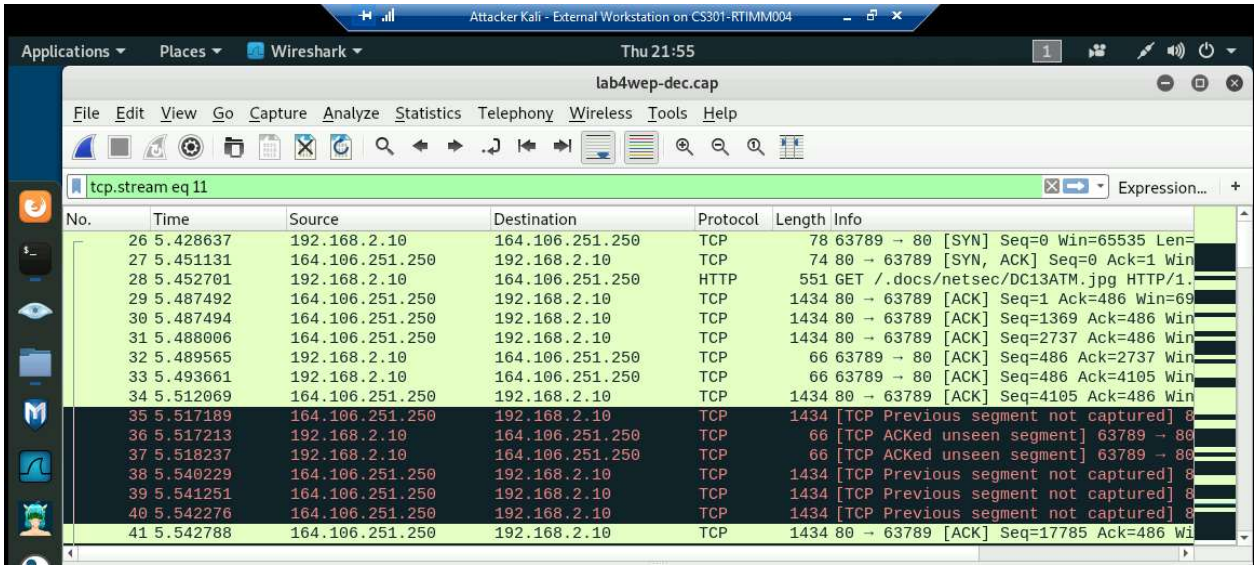
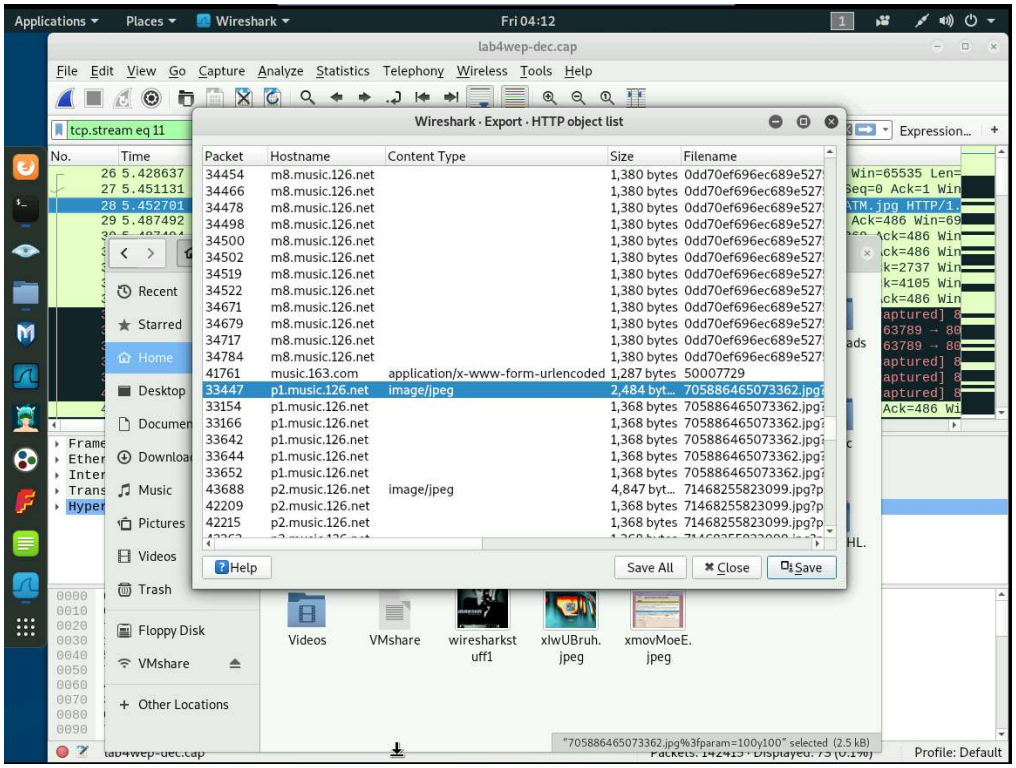
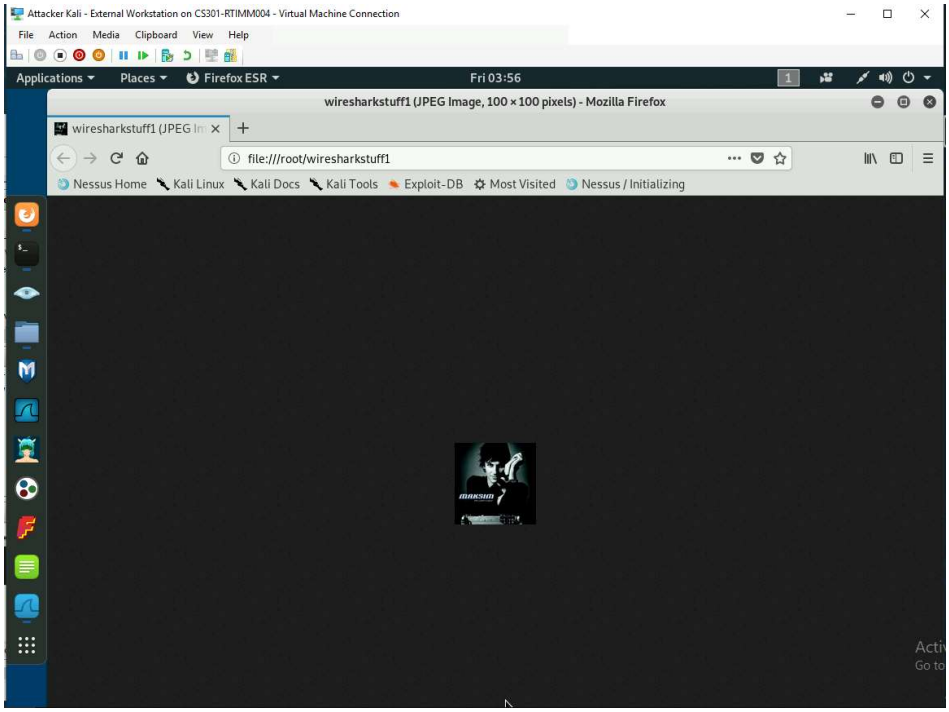
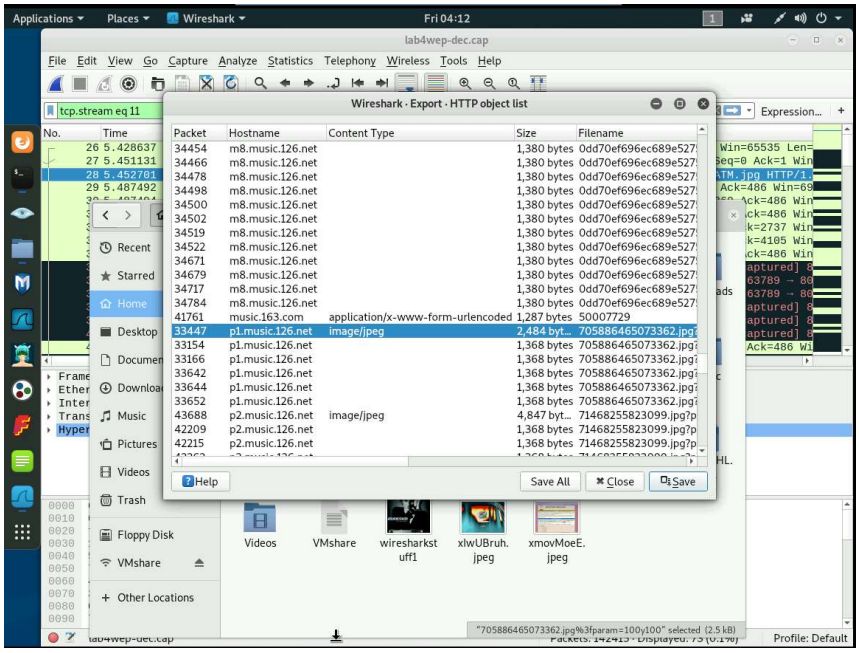


A picture of the HTTP object export, where you can see the hostnames, the files, and their sizes. I'm assuming the user was trying to get music off these sites.



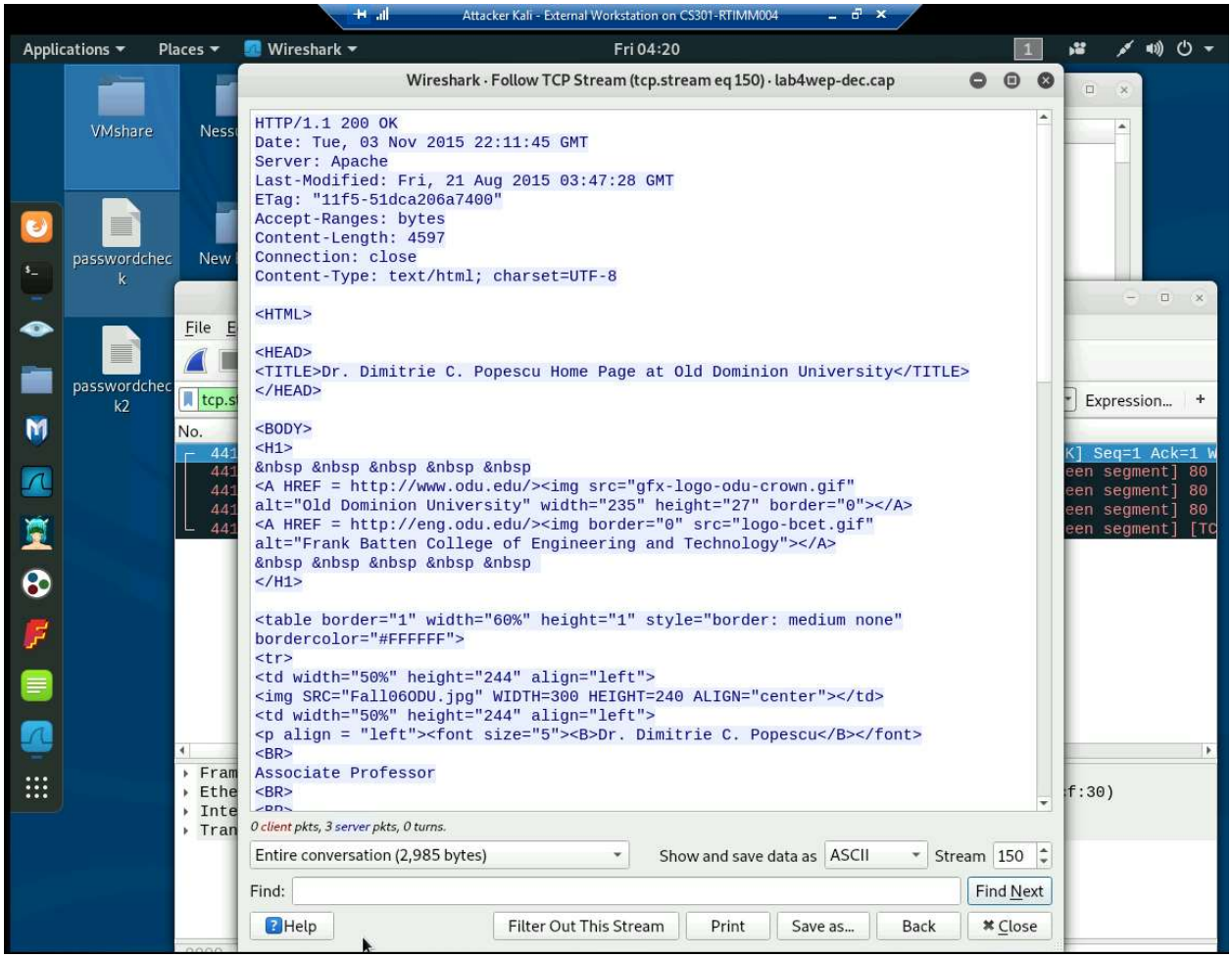
Here is a jpeg of one of the files from HTTP. It's an album cover. Below this image is where I got it from the HTTP object export.



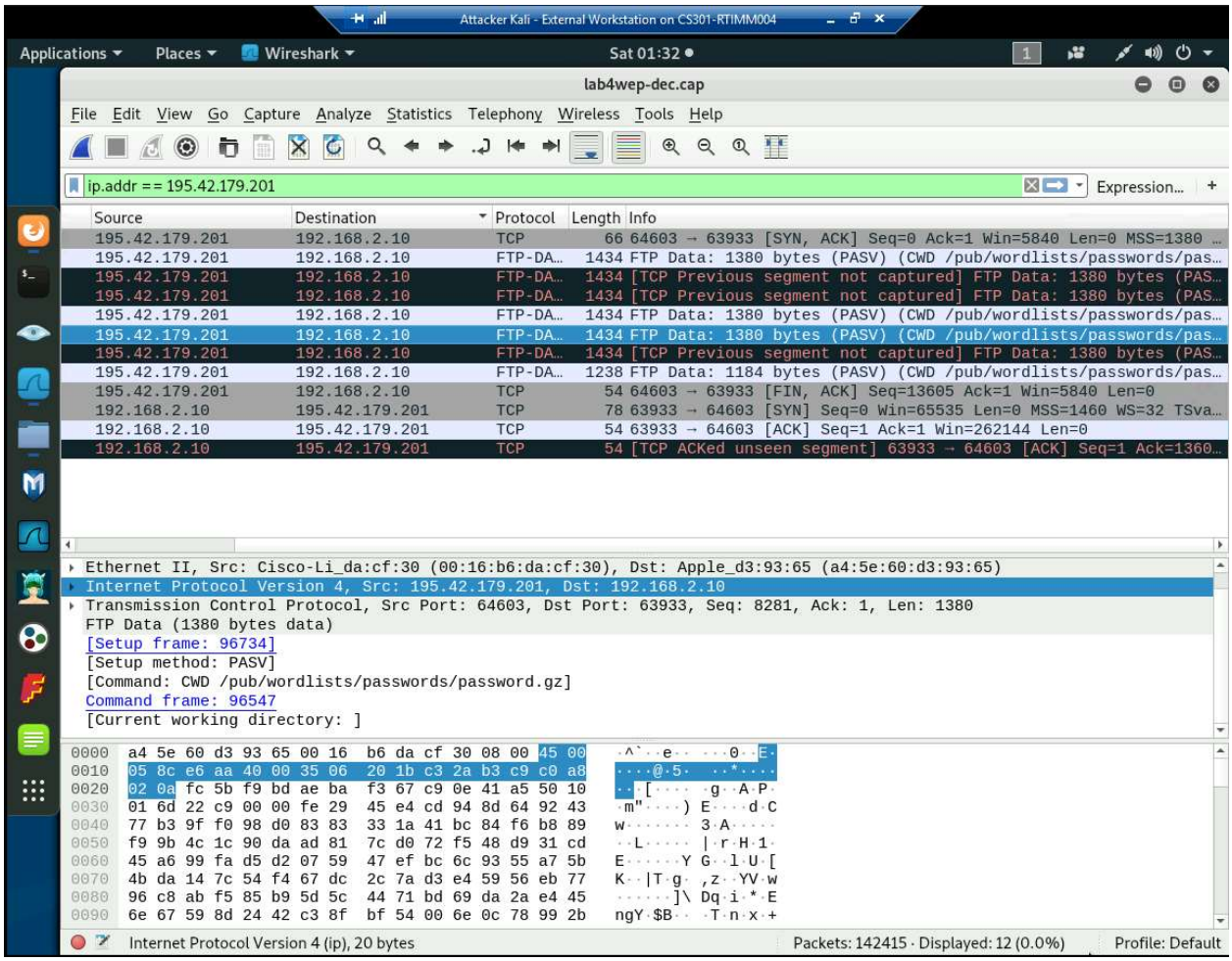


Found something that seemed out of place. There were a few times I would follow the TCP stream and find professor information. This

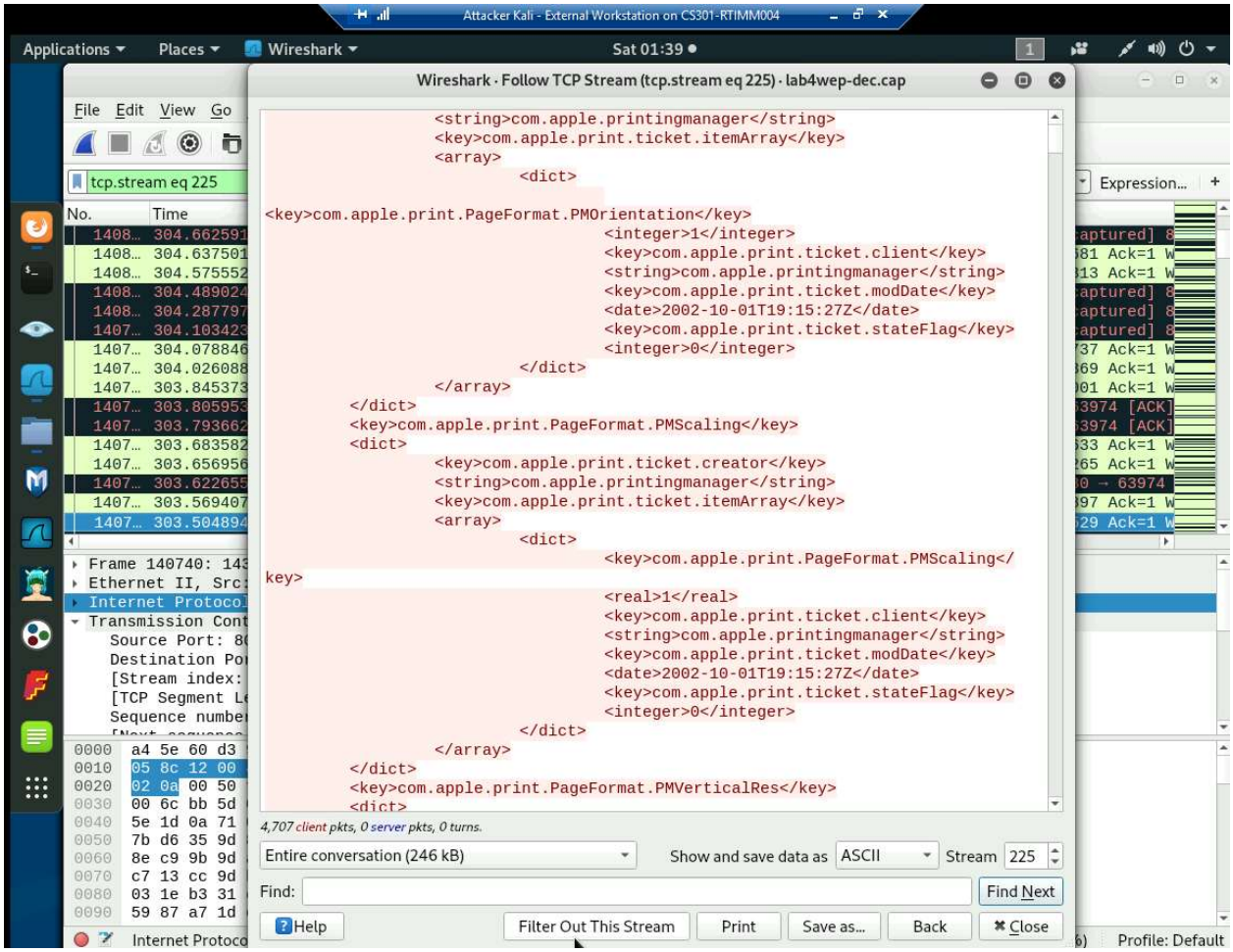
professor works in the electrical and computer engineering department at ODU. Learned a couple of things from him when scrolling down, like that he's a Ph.D! (For over 20 years!!!!)



The picture below shows the ftp-data filter, where I can see that 195.42.179.201 is in the passwords.gz directory.

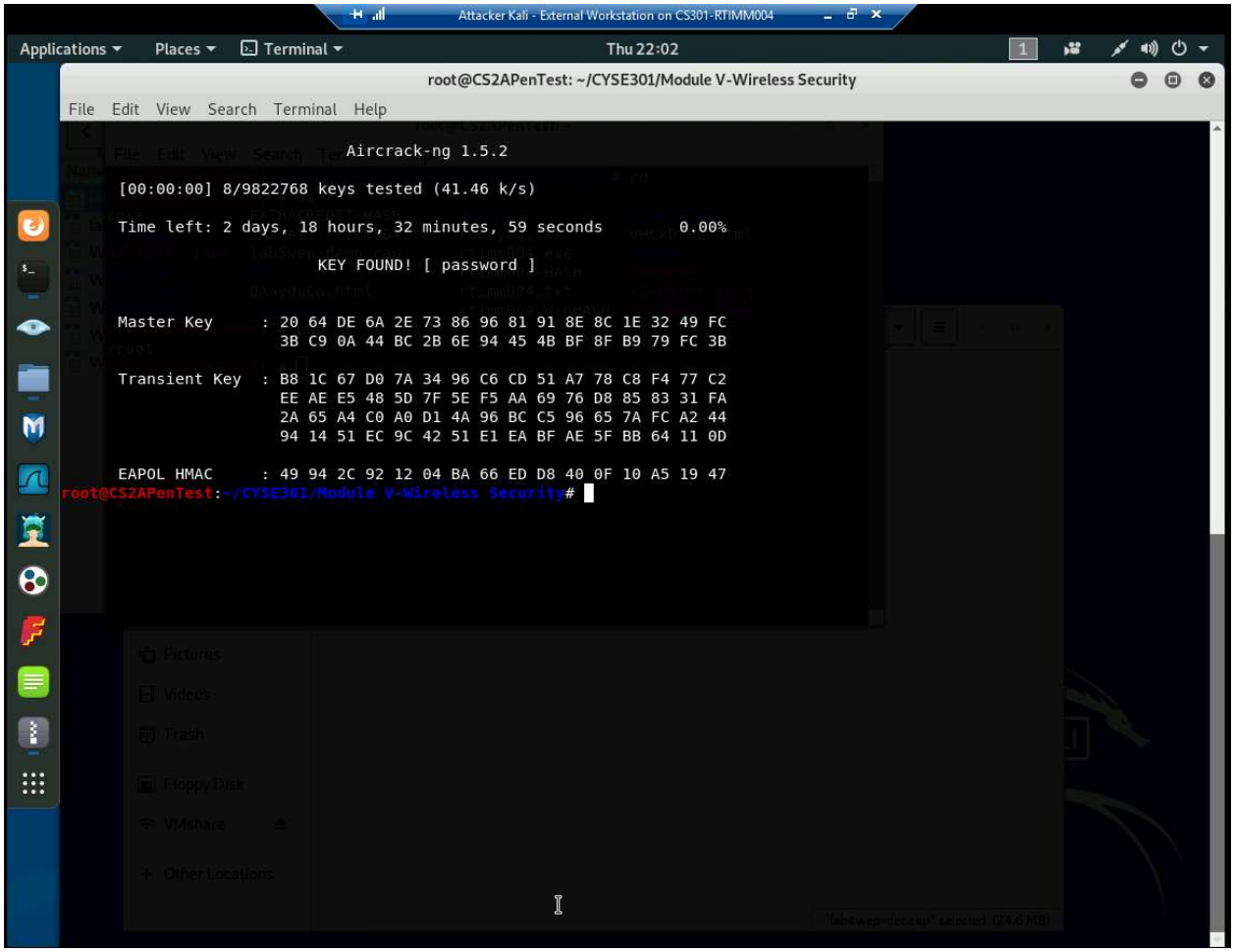


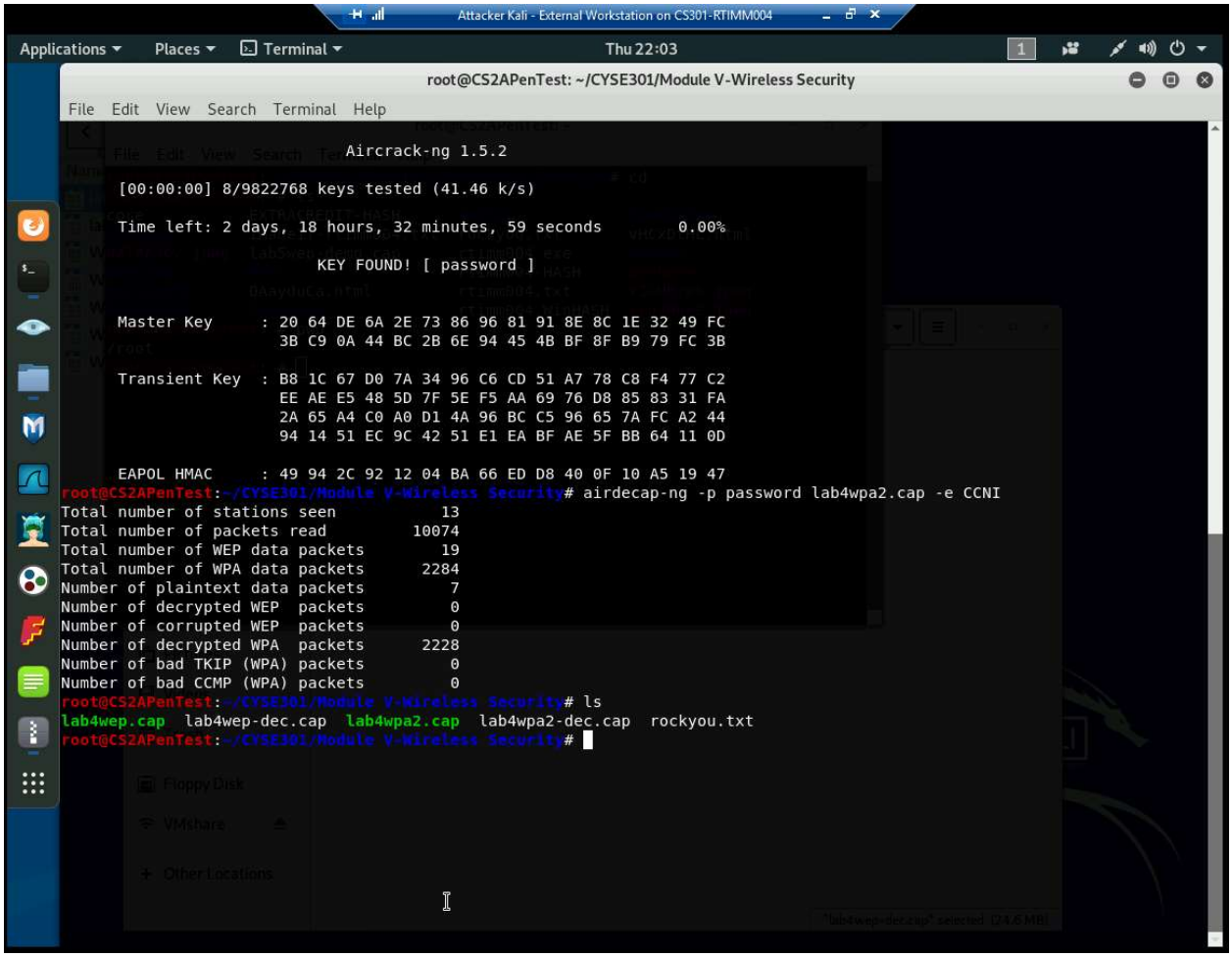
Here’s the HTML page I couldn’t understand.



2. Decrypt the lab4wpa2.cap file and perform a detailed traffic analysis.

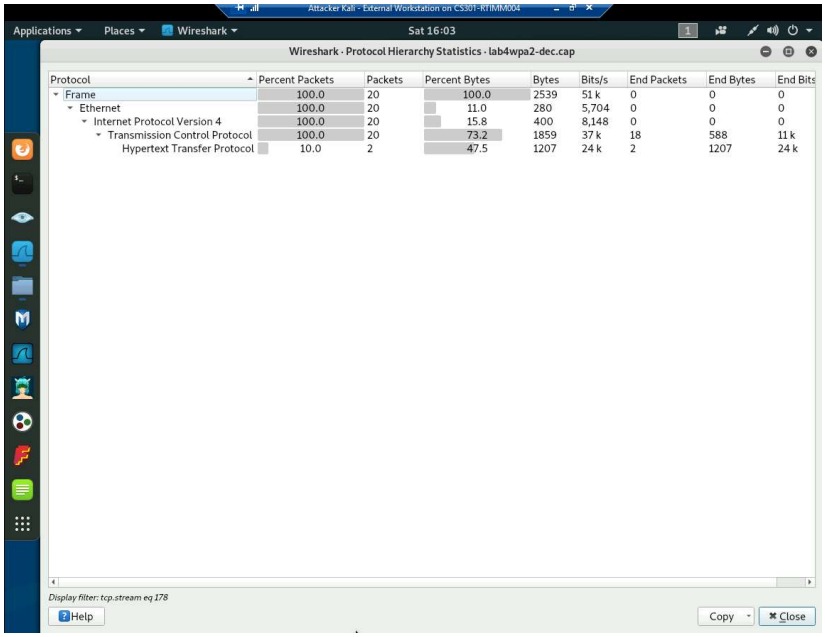
Below are two images of me using aircrack to get the password, and using airdecap respectively (with password) to get the de.cap file. I didn’t get the command itself for the first one, but I got the output alright.

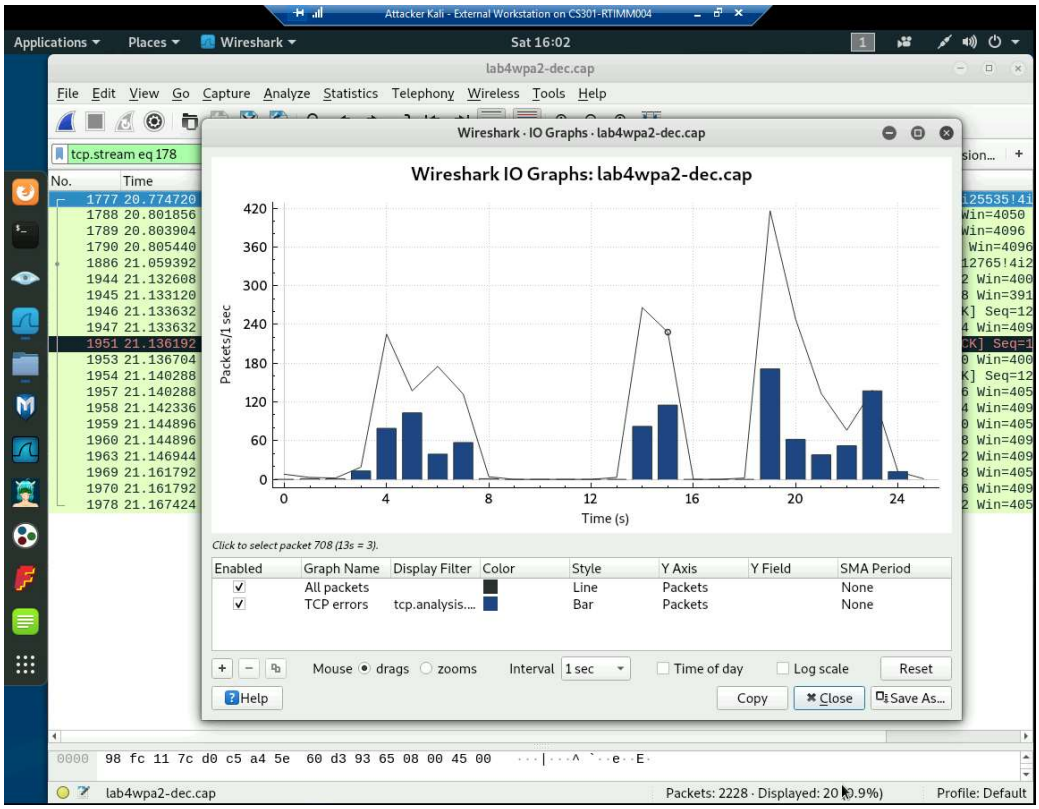

Attacker Kali - External Workstation on CS301-RTIMM004
Applications
Places
Terminal
Thu 22:02
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Aircrack-ng 1.5.2
[00:00:00] 8/9822768 keys tested (41.46 k/s)
Time left: 2 days, 18 hours, 32 minutes, 59 seconds 0.00%
KEY FOUND! [password]
Master Key : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
3B C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B
Transient Key : B8 1C 67 D0 7A 34 96 C6 CD 51 A7 78 C8 F4 77 C2
EE AE E5 48 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA
2A 65 A4 C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44
94 14 51 EC 9C 42 51 E1 EA BF AE 5F BB 64 11 0D
EAPOL HMAC : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#



Detailed summary: This was was definitely easier to read than the first. (No more ARP WALLS!!!!!!!) In a nutshell, it seems that whoever is 192.168.2.23 is going through ODU, checking the local news, youtube, odusports, and looking at general campus maps. There was a standard query for PengdeMacBook-Pro, I believe this is the source of all the traffic. You can also see that pngs of the maps are downloaded off of the web server. Most if not all of this map interaction can be seen from HTTP.

Screenshots


Attacker Kali - External Workstation on CS301-RTIMM004
Applications
Places
Wireshark
Sat 16:03
Wireshark · Protocol Hierarchy Statistics · lab4wpa2-dec.cap
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits
Frame 100.0 20 100.0 2539 51 k 0 0 0
Ethernet 100.0 20 11.0 280 5,704 0 0 0
Internet Protocol Version 4 100.0 20 15.8 400 8,148 0 0 0
Transmission Control Protocol 100.0 20 73.2 1859 37 k 18 588 11 k
Hypertext Transfer Protocol 10.0 2 47.5 1207 24 k 2 1207 24 k
Display filter: tcp.stream eq 178
Help
Copy
Close


Attacker Kali - External Workstation on CS301-RTIMM004
Applications
Places
Wireshark
Sat 16:02
lab4wpa2-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 178
No. Time
1777 20.774720
1788 20.801856
1789 20.803904
1790 20.805440
1886 21.059392
1944 21.132608
1945 21.133120
1946 21.133632
1947 21.133632
1951 21.136192
1953 21.136704
1954 21.140288
1957 21.140288
1958 21.142336
1959 21.144896
1960 21.144896
1963 21.146944
1969 21.161792
1970 21.161792
1978 21.167424
Wireshark · IO Graphs · lab4wpa2-dec.cap
Wireshark IO Graphs: lab4wpa2-dec.cap
Packets/1 sec
Time (s)
Click to select packet 708 (13s = 3).
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period
All packets Line Packets None
TCP errors tcp.analysis.... Bar Packets None
Mouse drags zooms Interval 1 sec Time of day Log scale Reset
Help Copy Close Save As...
0000 98 fc 11 7c d0 c5 a4 5e 60 d3 93 65 08 00 45 00
lab4wpa2-dec.cap
Packets: 2228 · Displayed: 20
Profile: Default