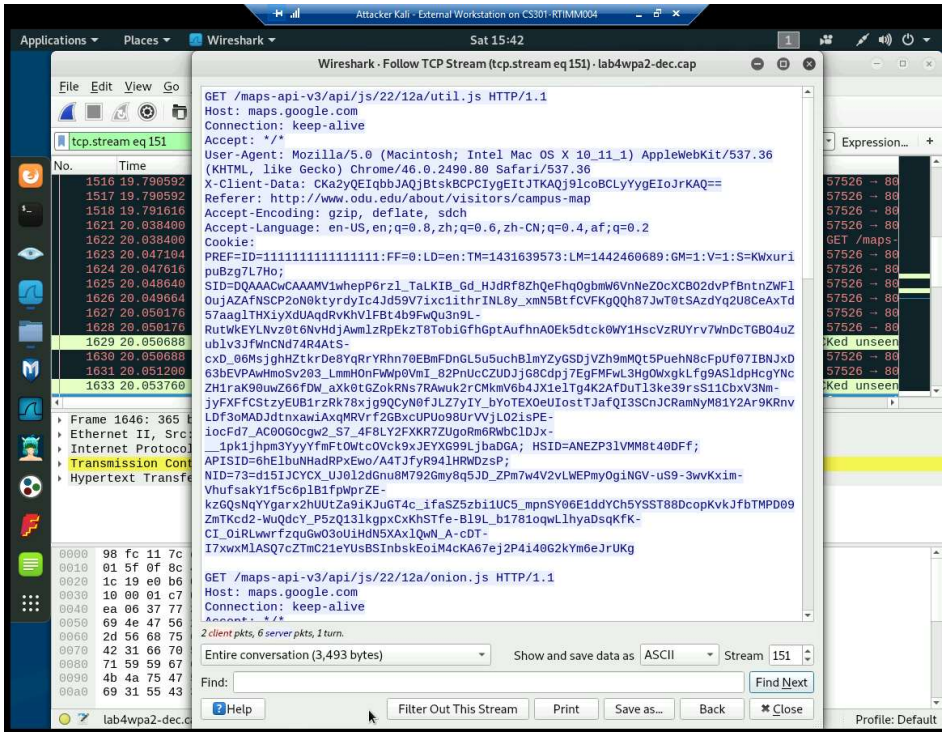
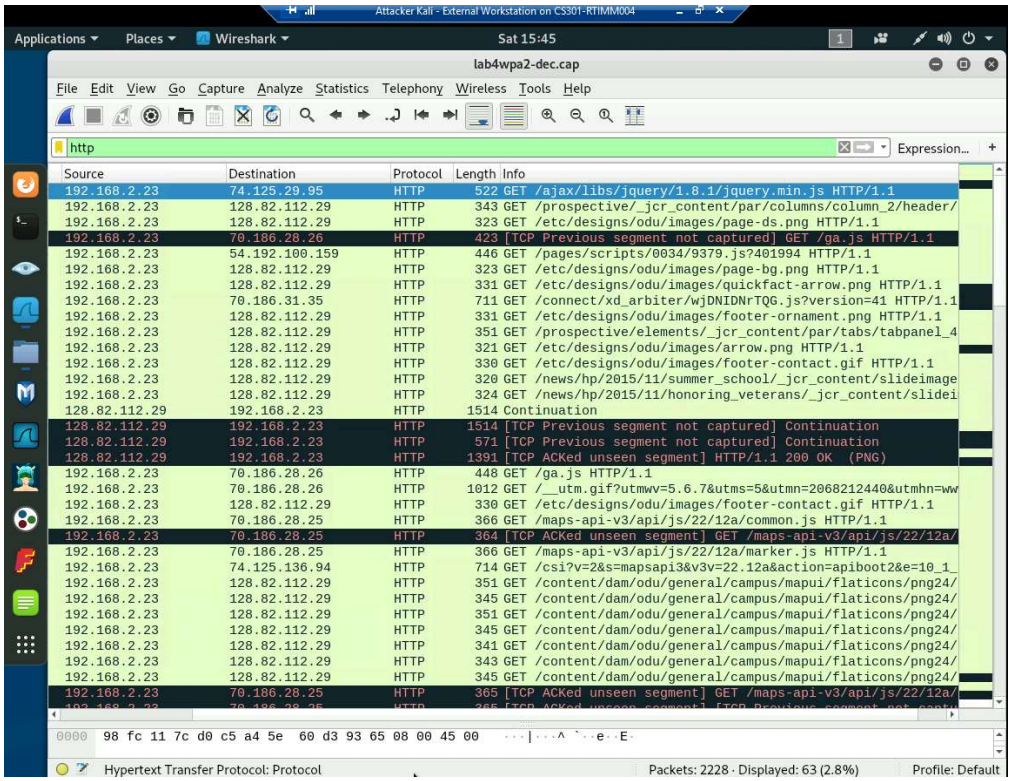
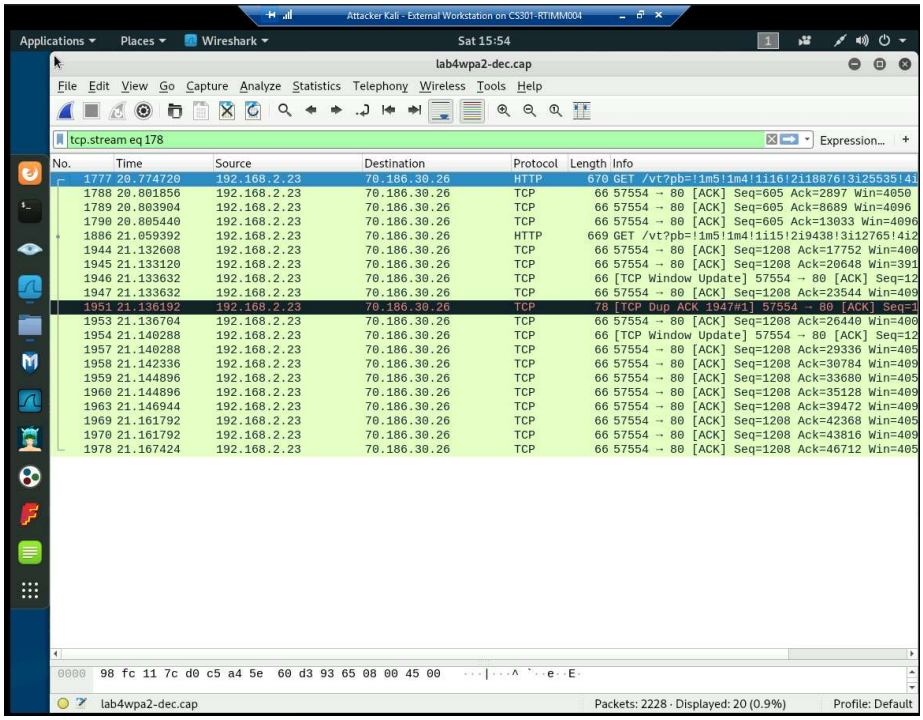
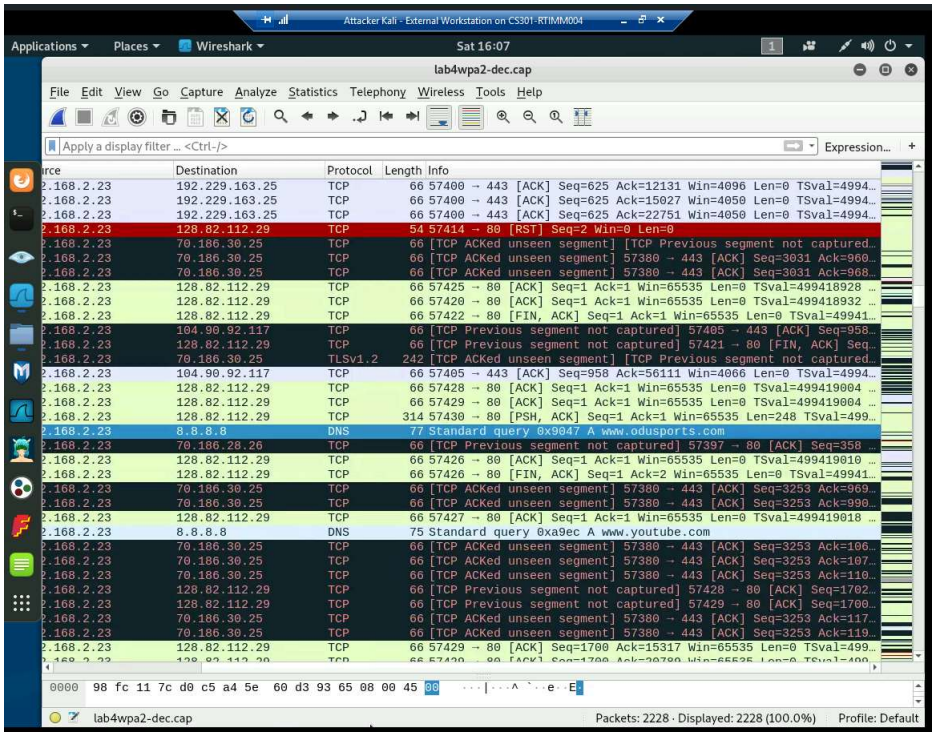


Below you can see that they are getting images/webpages/content off of the HTTP server





Above you can see HTTP ‘get’ commands.

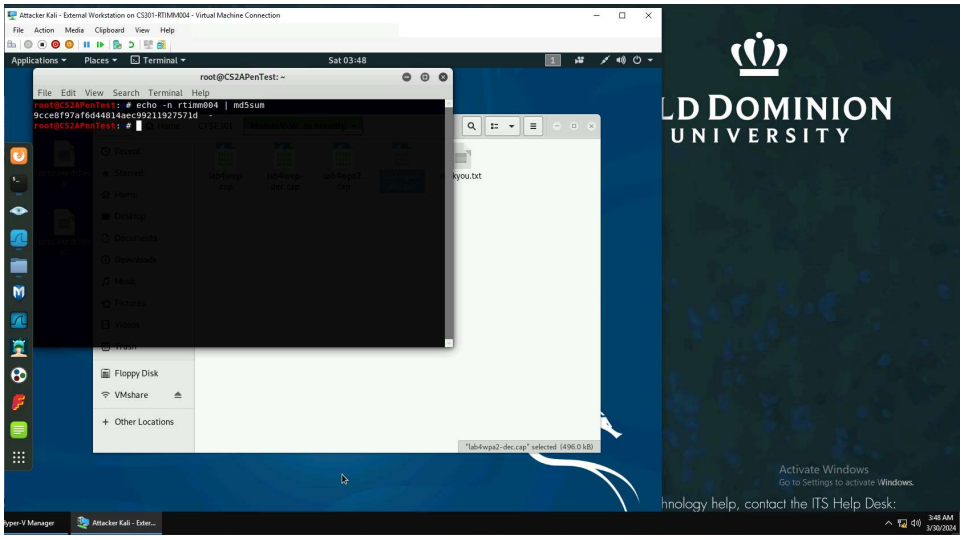


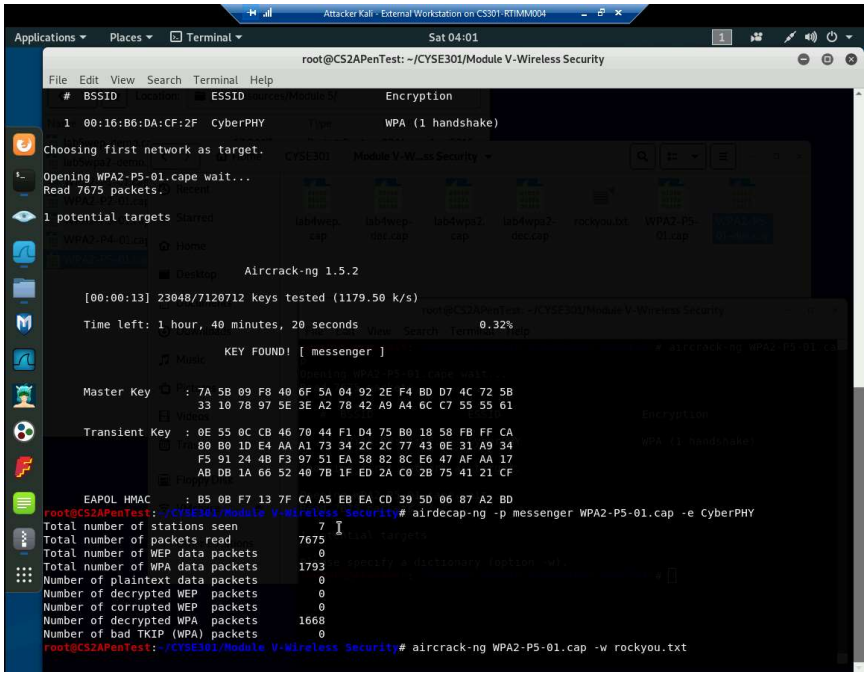
Above you can see a DNS query for youtube and ODUsports!!!

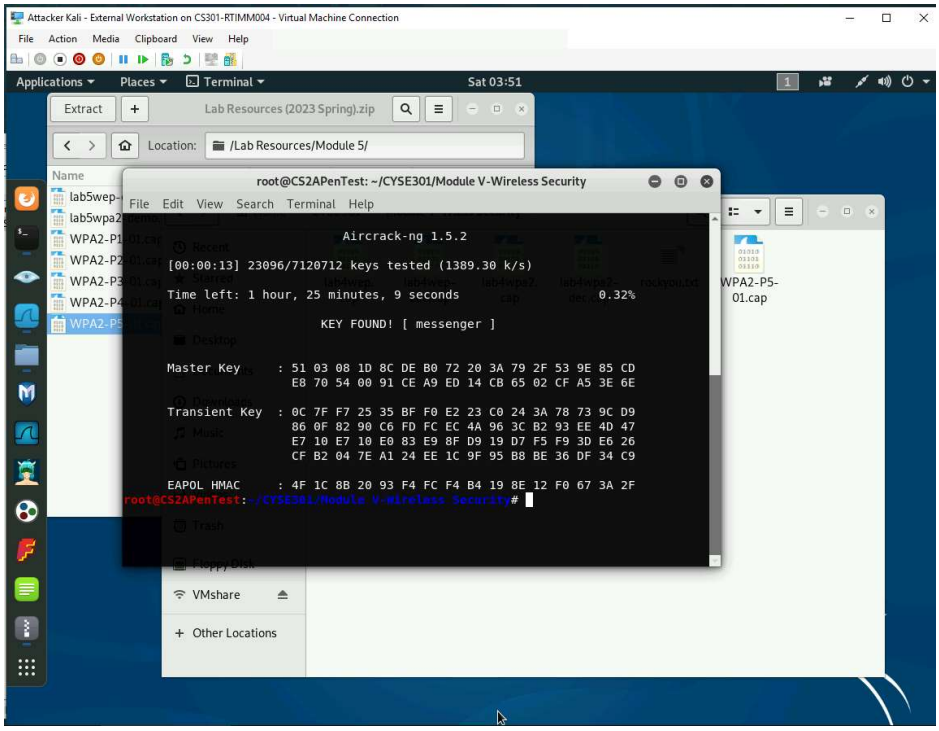
Task D

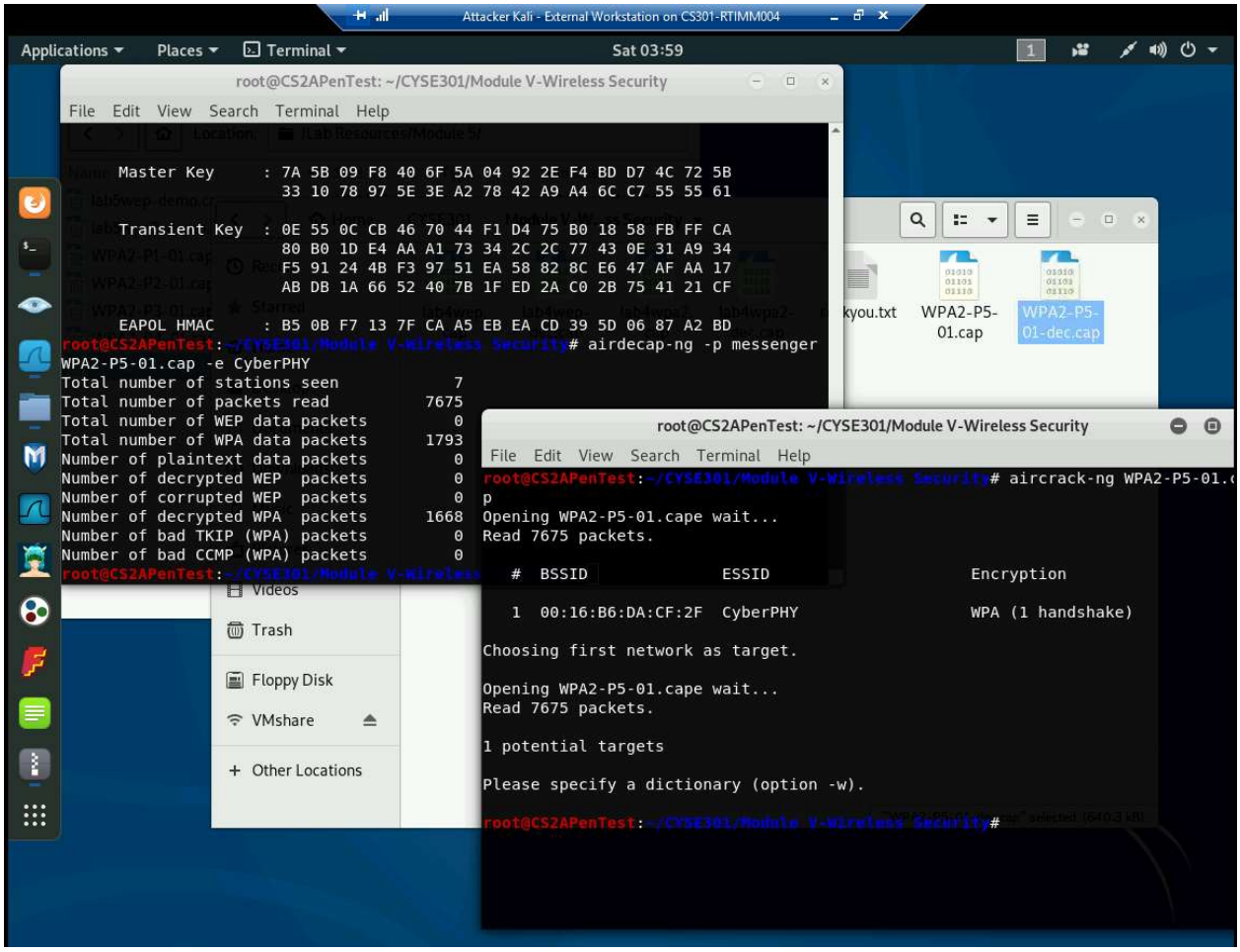
Use ‘echo -n rtimm004 | md5sum’ to get the right file.

After using the command, my hash ended in ‘d’, so I used the WPA2-P5-01.cap. The key was, after using the command, ‘aircrack-ng WPA2-P5-01.cap -w rockyou.txt’, messenger. The second screenshot reflects the output, then I redid the command to show syntax. Lastly, you can see me using airdecap and the ESSID to unencrypt the traffic.



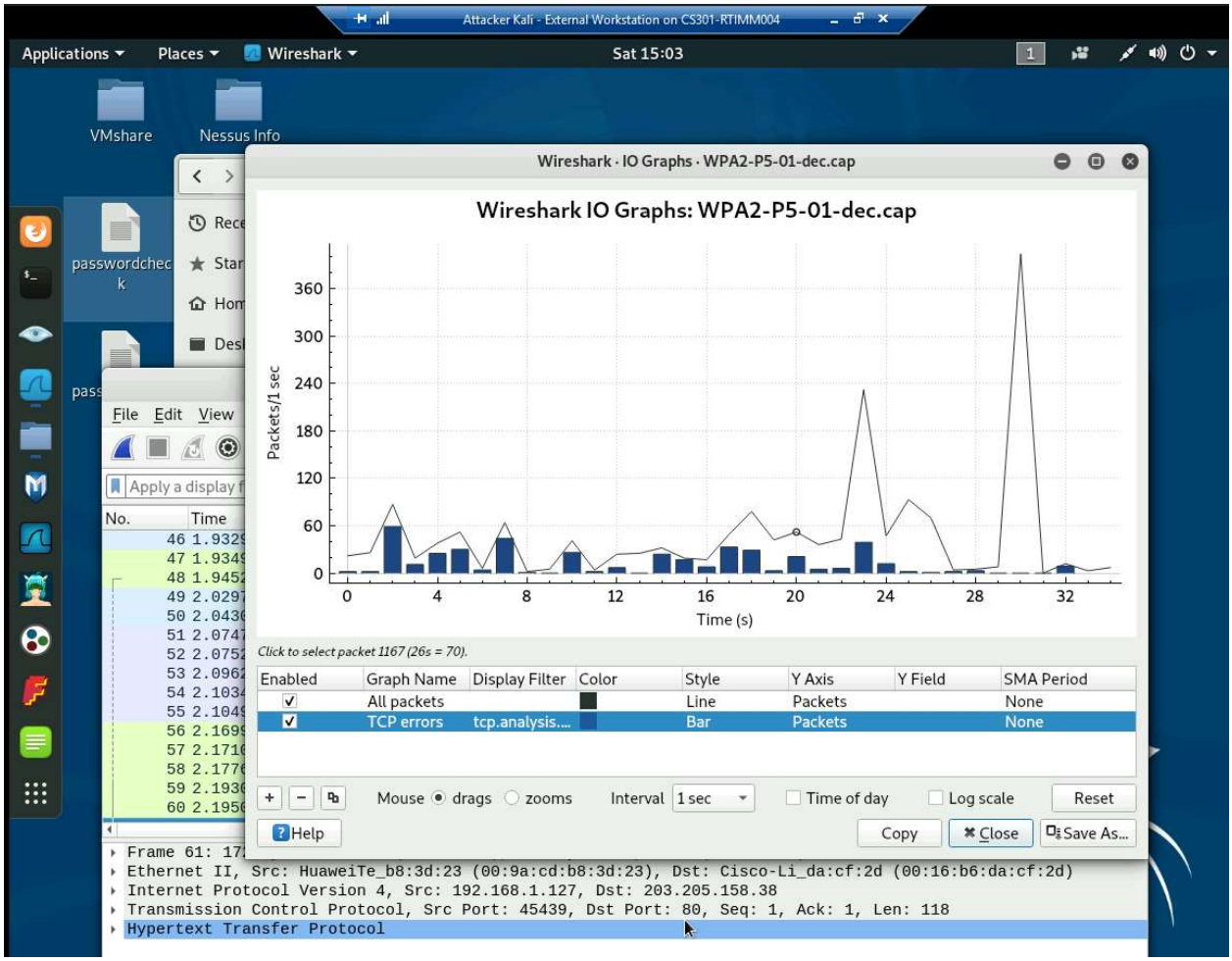


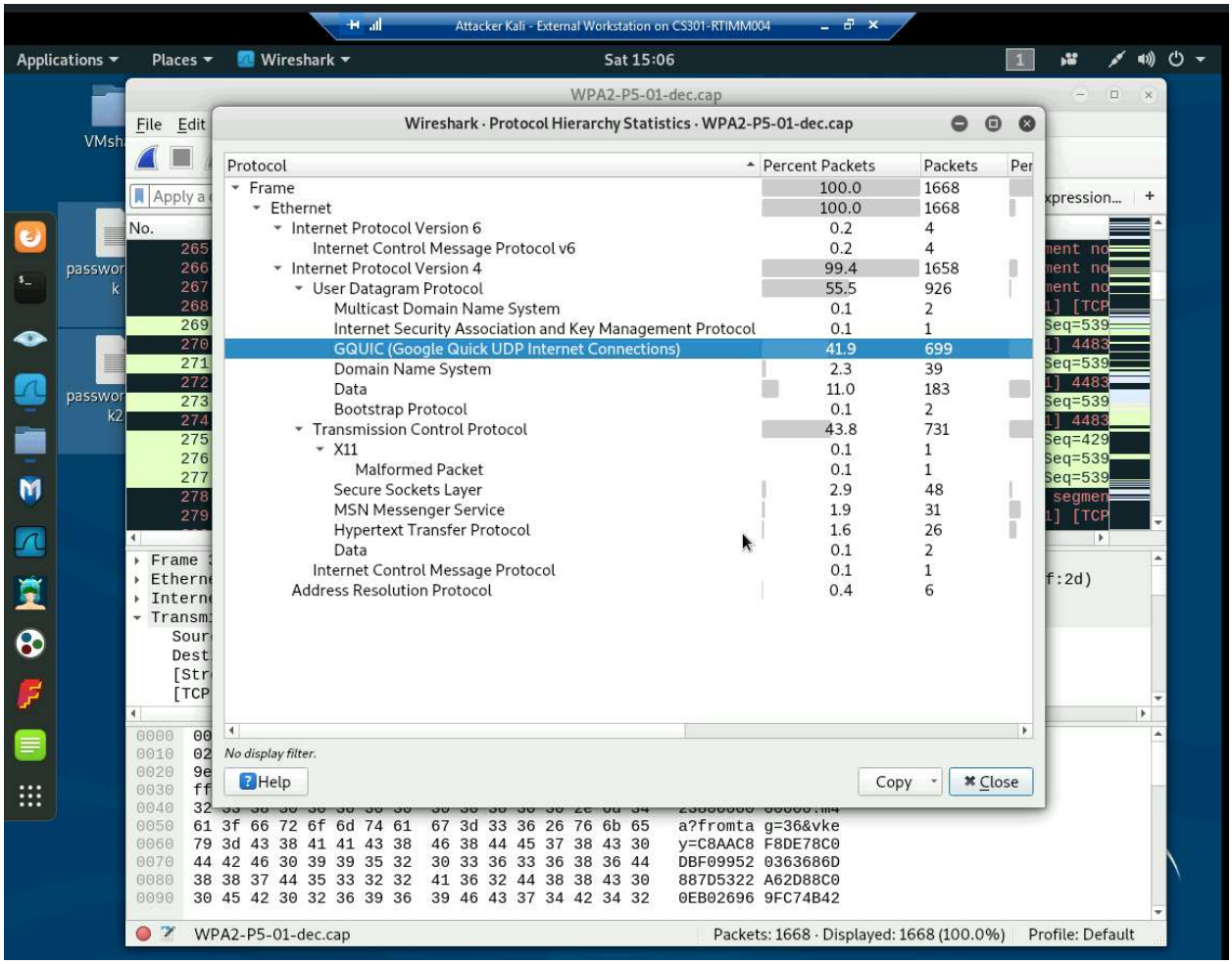

Attacker Kali - External Workstation on CS301-RTIMM004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Sat 03:51
Extract
Lab Resources (2023 Spring).zip
Location: /Lab Resources/Module 5/
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Aircrack-ng 1.5.2
[00:00:13] 23096/7120712 keys tested (1389.30 k/s)
Time left: 1 hour, 25 minutes, 9 seconds 0.32%
KEY FOUND! [messenger]
Master Key : 51 03 08 1D 8C DE B0 72 20 3A 79 2F 53 9E 85 CD
E8 70 54 00 91 CE A9 ED 14 CB 65 02 CF A5 3E 6E
Transient Key : 0C 7F F7 25 35 BF F0 E2 23 C0 24 3A 78 73 9C D9
86 0F 82 90 C6 FD FC EC 4A 96 3C B2 93 EE 4D 47
E7 10 E7 10 E0 83 E9 8F D9 19 D7 F5 F9 3D E6 26
CF B2 04 7E A1 24 EE 1C 9F 95 B8 BE 36 DF 34 C9
EAPOL HMAC : 4F 1C 8B 20 93 F4 FC F4 B4 19 8E 12 F0 67 3A 2F
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#
WPA2-P5-01.cap
VMshare
Other Locations



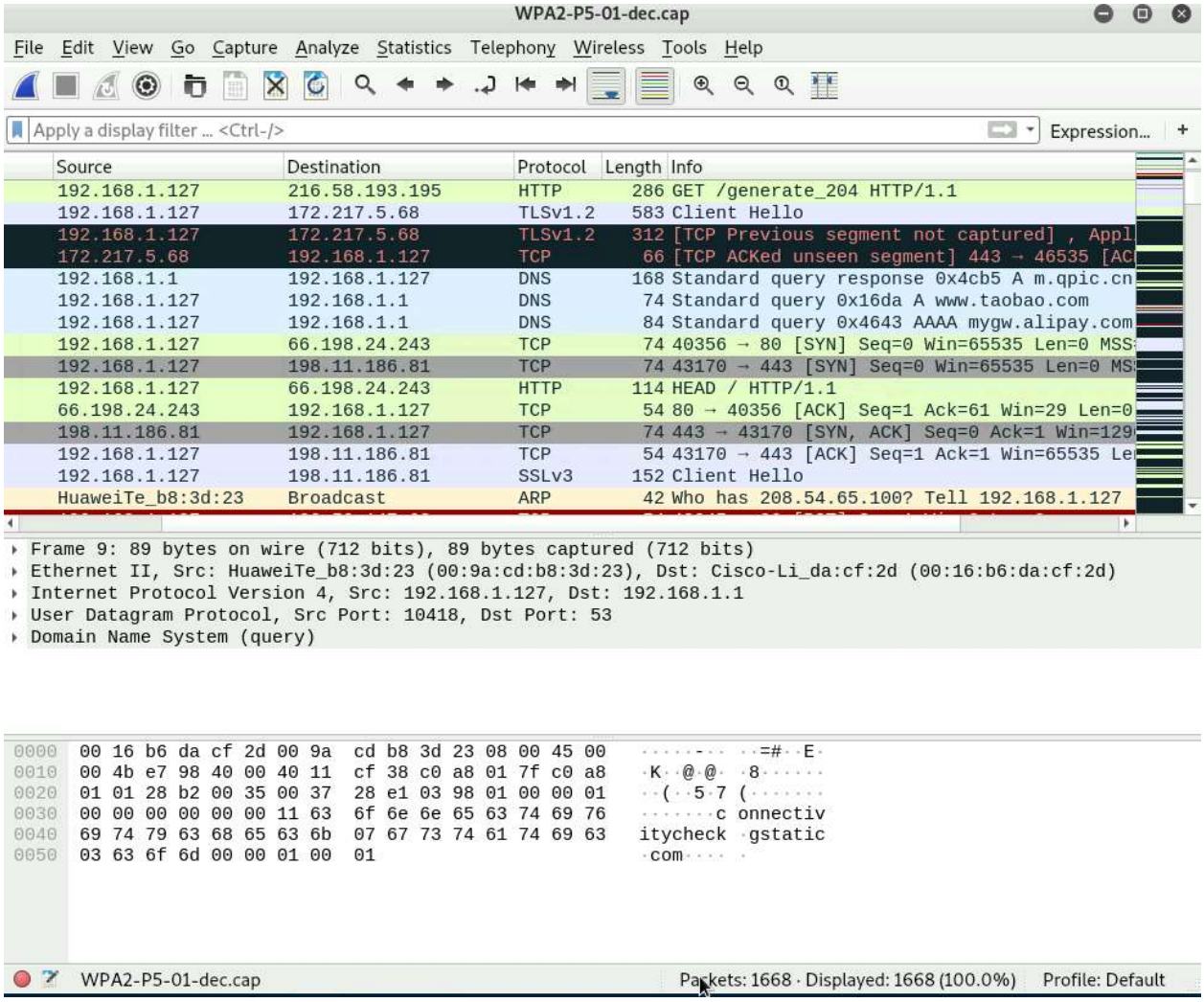
Detailed Summary

To preface, Im really trying my best to understand whats going on in these capture files. We talked about HOW to get into the files, but not WHAT to look for, so I'm really lost in all the packets. Despite this, I did find that there were alot of UDP traffic on the network. Protocols such as GQUIC were used, and I saw googlevideo within the UDP stream. I believe whoever was on the network was watching something from google. I saw m4a and mp4 files scattered throughout the traffic as well, if this helps. I also saw, very early on in the traffic, someone get on taobao. I recognized this as a chinese webstore, and also recognized alipay. Looks like someone was trying to locate these websites with DNS. Hopefully this is enough information, I've been scouring these packet files, using filters and exports, and trying to get a handle of whats going on.


Attacker Kali - External Workstation on CS301-RTIMM004
Applications
Places
Wireshark
Sat 15:03
VMshare
Nessus Info
passwordcheck
Wireshark · IO Graphs · WPA2-P5-01-dec.cap
Wireshark IO Graphs: WPA2-P5-01-dec.cap
Packets/1 sec
Time (s)
Click to select packet 1167 (26s = 70).
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...
Frame 61:
Ethernet II, Src: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23), Dst: Cisco-Li_da:cf:2d (00:16:b6:da:cf:2d)
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 203.205.158.38
Transmission Control Protocol, Src Port: 45439, Dst Port: 80, Seq: 1, Ack: 1, Len: 118
Hypertext Transfer Protocol


Attacker Kali - External Workstation on CS301-RTIMM004
Applications
Places
Wireshark
Sat 15:06
WPA2-P5-01-dec.cap
File Edit
Wireshark · Protocol Hierarchy Statistics · WPA2-P5-01-dec.cap
Protocol
Percent Packets
Packets
Frame 100.0 1668
Ethernet 100.0 1668
Internet Protocol Version 6 0.2 4
Internet Control Message Protocol v6 0.2 4
Internet Protocol Version 4 99.4 1658
User Datagram Protocol 55.5 926
Multicast Domain Name System 0.1 2
Internet Security Association and Key Management Protocol 0.1 1
GQUIC (Google Quick UDP Internet Connections) 41.9 699
Domain Name System 2.3 39
Data 11.0 183
Bootstrap Protocol 0.1 2
Transmission Control Protocol 43.8 731
X11 0.1 1
Malformed Packet 0.1 1
Secure Sockets Layer 2.9 48
MSN Messenger Service 1.9 31
Hypertext Transfer Protocol 1.6 26
Data 0.1 2
Internet Control Message Protocol 0.1 1
Address Resolution Protocol 0.4 6
No display filter.
Help
Copy
Close
0050 61 3f 66 72 6f 6d 74 61 67 3d 33 36 26 76 6b 65 a?fromta g=36&vke
0060 79 3d 43 38 41 41 43 38 46 38 44 45 37 38 43 30 y=C8AAC8 F8DE78C0
0070 44 42 46 30 39 39 35 32 30 33 36 33 36 38 36 44 DBF09952 0363686D
0080 38 38 37 44 35 33 32 32 41 36 32 44 38 38 43 30 887D5322 A62D88C0
0090 30 45 42 30 32 36 39 36 39 46 43 37 34 42 34 32 0EB02696 9FC74B42
WPA2-P5-01-dec.cap
Packets: 1668 · Displayed: 1668 (100.0%)
Profile: Default

In the picture below you can see the DNS query for taobao and alipay



Here’s a pic of all the GQUIC traffic!