

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #6 Wi-Fi Password Cracking

Michael Greene

UIN: 01213114

TASK A

Follow the steps in the lab manual, and decrypt WEP and WPA/WPA2 protected traffic.

Requirements:

- Decrypt the lab4wep.cap file (10 points) and perform a detailed traffic analysis (10 points)

```
Attacker Kali - External Workstation on CY301-MGREG034
Tue 04:12
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Aircrack-ng 1.5.2
lab4wep- lab4wep- lab4wep2
cap cap cap
[00:00:01] Tested 231 keys (got 19772 IVs)

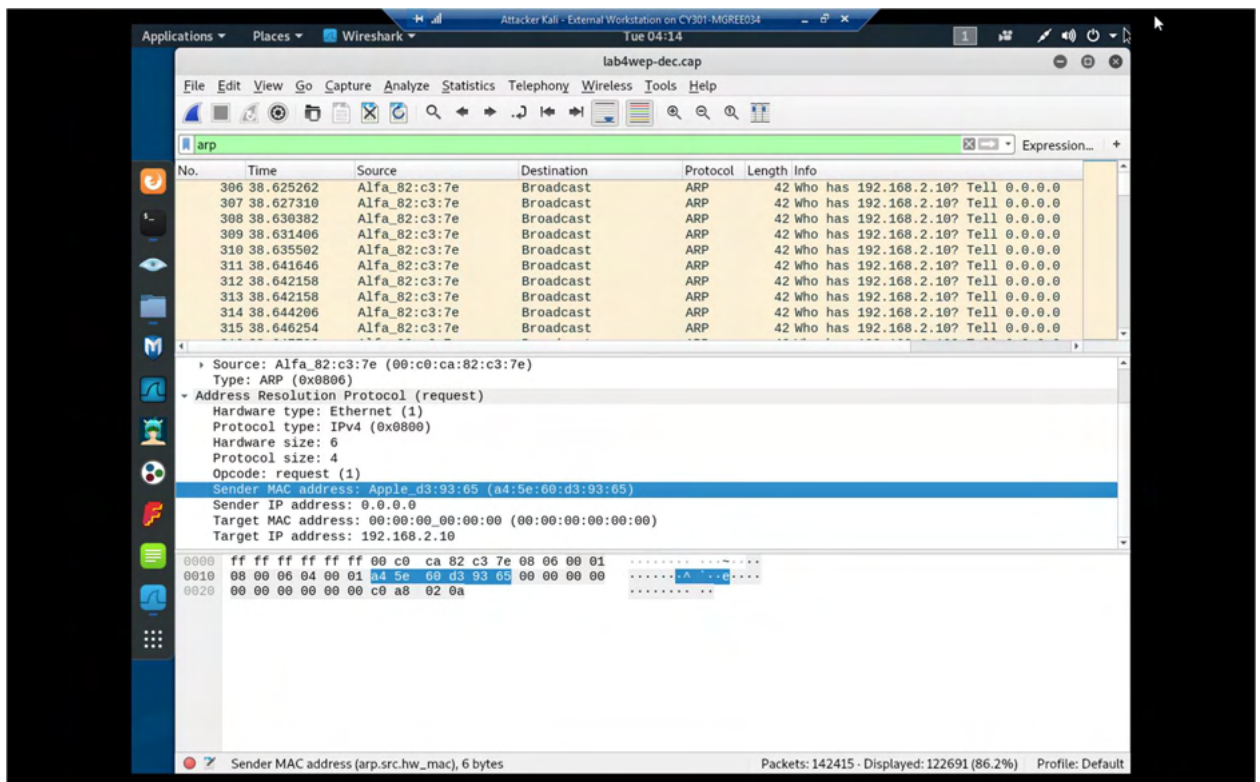
KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 38(24064)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296) 62(23296)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576)

KEY FOUND! [ F2:C7:BB:35:B9 ]
Decrypted correctly: 100%

root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap -w F2:C7:BB:35:B9 lab4wep.cap
bash: airdecap: command not found
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -w F2:C7:BB:35:B9 lab4wep.cap
Total number of stations seen 37
Total number of packets read 404693
Total number of WEP data packets 142415
Total number of WPA data packets 27852
Number of plaintext data packets 170
Number of decrypted WEP packets 142415
Number of corrupted WEP packets 0
Number of decrypted WPA packets 0
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0

root@CS2APenTest:~/CYSE301/Module V-Wireless Security# ls
lab4wep.cap lab4wep-dec.cap lab4wpa2.cap
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#
```

To decrypt the lab4wep.cap file I opened up a terminal within the folder containing the file. I then used the command **aircrack-ng lab4wep.cap** and chose the target network 1 with the WEP encryption. Once I found the key I used **airdecap -w F2:C7:BB:35:b9 lab4wep.cap** and was given the lab4wep-dec.cap file containing the decrypted data.



Opening the decrypted file in Wireshark, I observed a high amount of ARP request coming from Alfa_82:c3:7e. The ARP request appear to target one specific IP address 192.168.2.10. This could be an attacker attempting to deny traffic to that IP by flooding it with ARP requests.

- Decrypt the lab4wpa2.cap file (10 points) and perform a detailed traffic analysis (10 points)

```

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 (57.01 k/s) lab4wpa2- rockyou.txt
dec.cap
Time left: 1 day, 23 hours, 52 minutes, 9 seconds 0.00%

KEY FOUND! [ password ]

Master Key : 20 64 DE 6A 2E 73 86 96 81 91 8E BC 1E 32 49 FC
3B C9 0A 44 BC 2B 6E 94 45 4B BF BF 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 8B 64 11 00

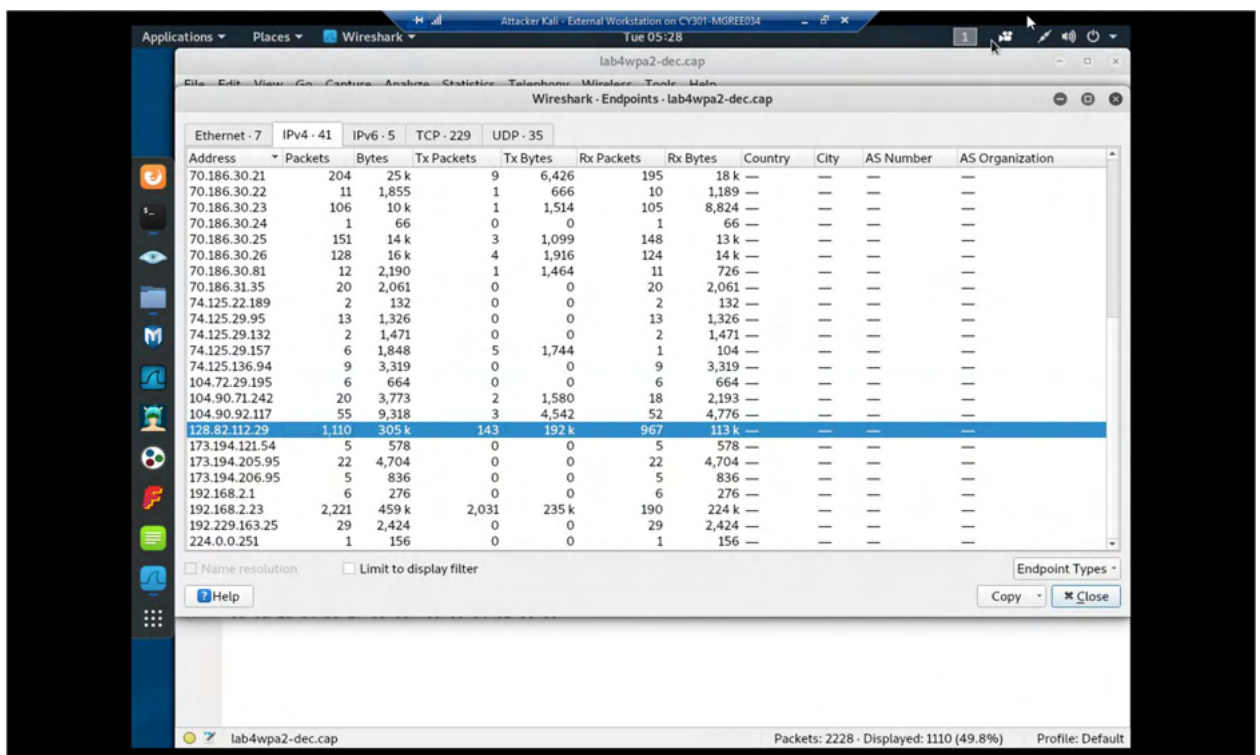
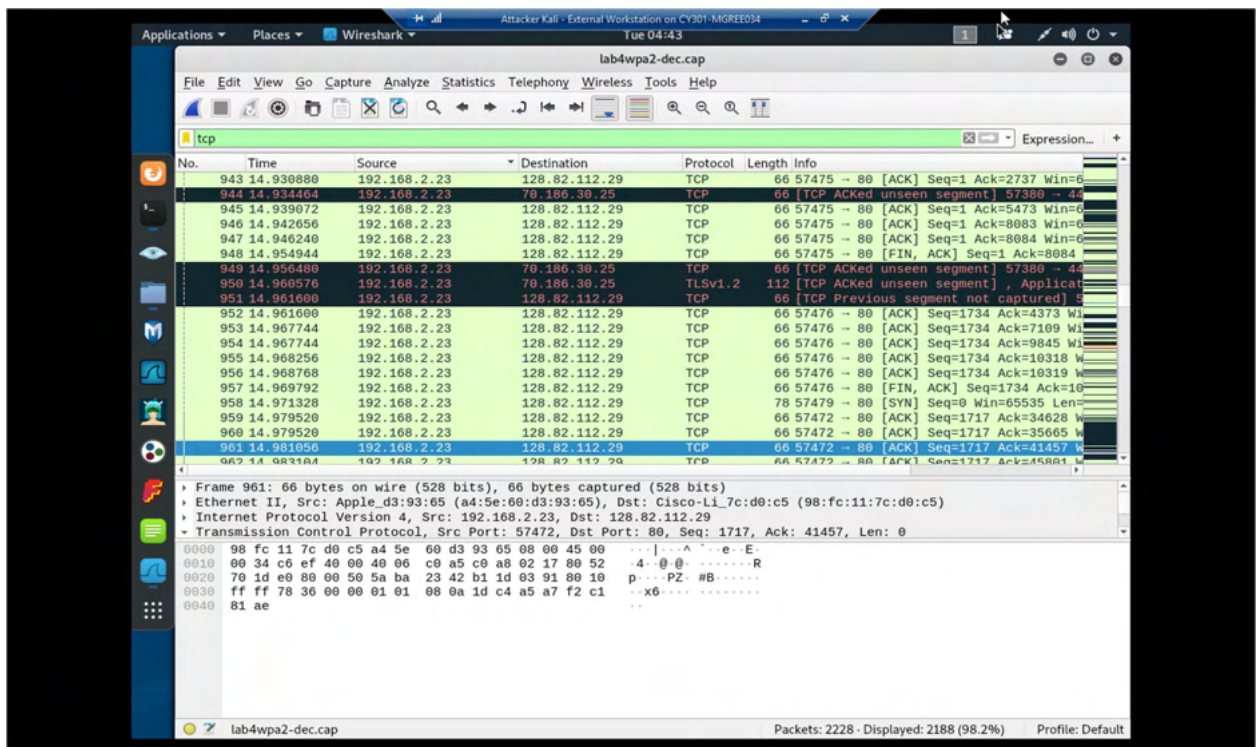
EAPOL HMAC : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47

Total number of stations seen 13
Total number of packets read 10074
Total number of WEP data packets 19
Total number of WPA data packets 2284
Number of plaintext data packets 7
Number of decrypted WEP packets 0
Number of corrupted WEP packets 0
Number of decrypted WPA packets 2228
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0

root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng lab4wpa2.cap -p password -e CCNI
lab4wep.cap lab4wep-dec.cap lab4wpa2.cap lab4wpa2-dec.cap rockyou.txt
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#

```

In order to decrypt the lab4wpa2.cap file I opened the terminal back up and unzipped the rockyou.txt wordlist. I used the command **aircrack-ng lab4wpa2.cap** and noted the ESSID which was CCNI for later in the decryption. I then used the command **aircrack-ng lab4wpa2.cap -w rockyou.txt** to perform a dictionary attack on the file. Once I found the password which was password. I used the command **airdecap-ng lab4wpa2.cap -p password -e CCNI** and received the decrypted file lab4wpa2-dec.cap.



Opening the decrypted file in Wireshark I noticed a high amount of TCP ACK's coming from 192.168.2.23 to 128.82.112.29 on port 80. The IP address with port 80 appears to be a server since port 80 is commonly associated with HTTP. The source IP appears to be sending request from multiple ports on their own machine. This may be an attempt flood the server with ACK packets to deny legitimate traffic.

TASK B

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the last digit of the hash for pjiang is **e**. Thus, I should pick up file "WPA2-P5-01.cap."

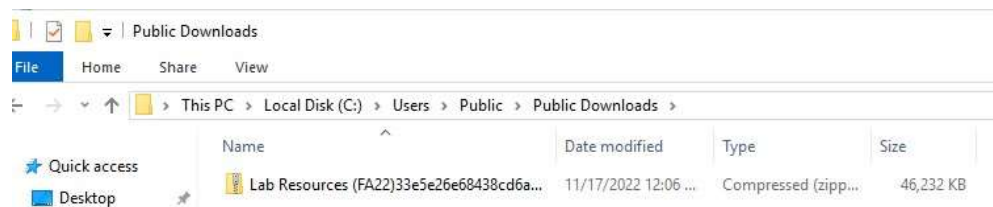
MD5 of **pjiang** is 5a618cdc3edffd8b4c661e7e9b70ce1e

You can find an online MD5 hash generator or the following command to get the hash of a text string,

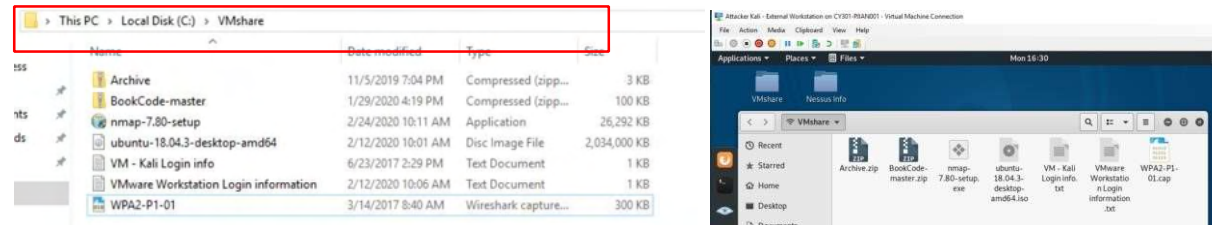
```
root@CS2APenTest:~# echo -n pjiang | md5sum
5a618cdc3edffd8b4c661e7e9b70ce1e -
root@CS2APenTest:~#
```

Last digit of your MD5	Filename
0~3	WPA2-P1-01.cap
4~5	WPA2-P2-01.cap
6~8	WPA2-P3-01.cap
9~B	WPA2-P4-01.cap
C~F	WPA2-P5-01.cap

The above files are zipped in a folder named "Lab Resources." You can locate zipped folder in the Windows 10 Host Machine under C:/Users/Public/Public Downloads. Then, unzip the following zipped file and find the assigned WPA file under sub-folder "Wireless Traffic".



Copy the file assigned to you to the "C:/VMshare" in Windows 10 Host Machine in order to access it from the Kali VMs.

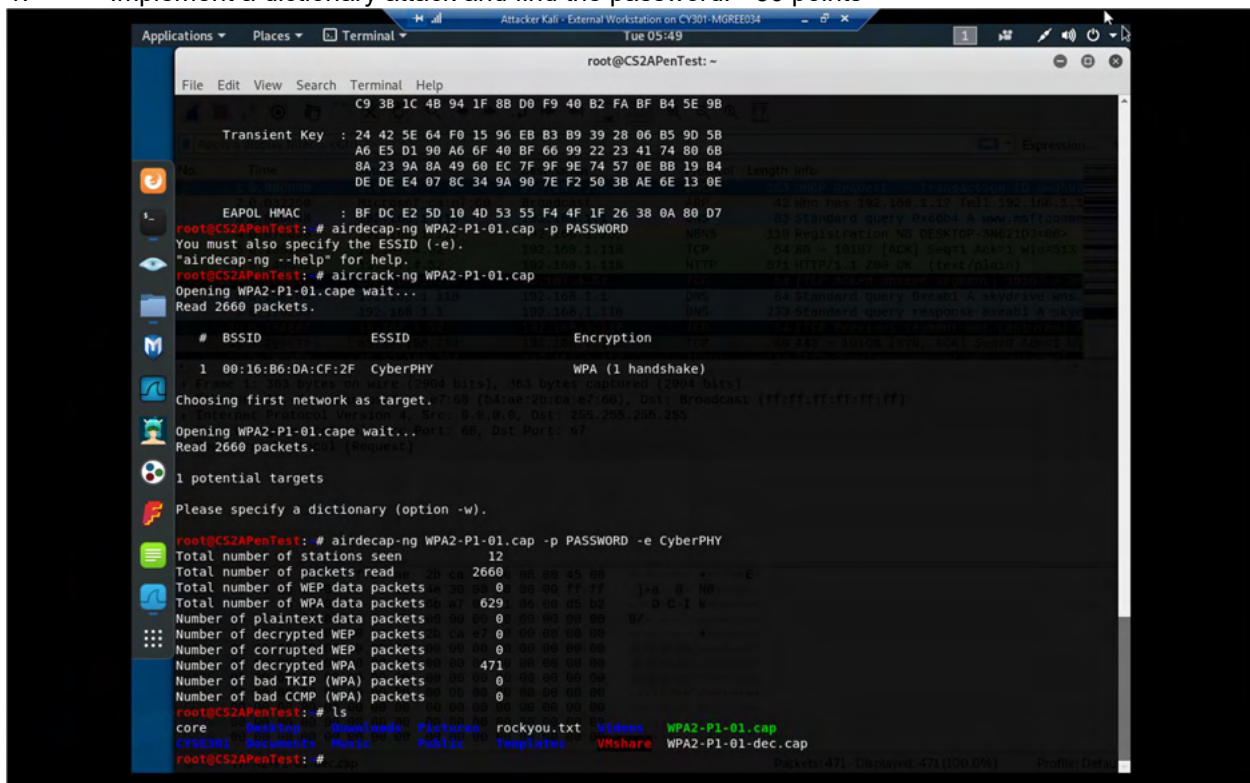


Then complete the following steps:

1. Implement a dictionary attack and find the password. - 30 points
2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -30 points

Mgree034 encrypted with MD5 was b74d4d0993f405d1411315b18a1c5071. So, I picked the file with the name **WPA2-P1-01.cap**.

1. Implement a dictionary attack and find the password. - 30 points



```
root@CS2APenTest: ~
File Edit View Search Terminal Help
C9 3B 1C 4B 94 1F 8B D0 F9 40 B2 FA BF B4 5E 9B

Transient Key : 24 42 5E 64 F0 15 96 EB B3 B9 39 28 06 B5 90 5B
A6 E5 D1 90 A6 6F 40 BF 66 99 22 23 41 74 80 6B
8A 23 9A 8A 49 60 EC 7F 9F 9E 74 57 0E BB 19 B4
DE DE E4 07 8C 34 9A 90 7E F2 50 3B AE 6E 13 0E

EAPOL HMAC : BF DC E2 5D 10 4D 53 55 F4 4F 1F 26 38 0A 80 D7
root@CS2APenTest: # airdecap-ng WPA2-P1-01.cap -p PASSWORD
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.
root@CS2APenTest: # aircrack-ng WPA2-P1-01.cap
Opening WPA2-P1-01.cape wait...
Read 2660 packets.

# BSSID ESSID Encryption
1 00:16:B6:DA:CF:2F CyberPHY WPA (1 handshake)

Choosing first network as target.
Opening WPA2-P1-01.cape wait...
Read 2660 packets.

1 potential targets

Please specify a dictionary (option -w).
root@CS2APenTest: # aircrack-ng WPA2-P1-01.cap -p PASSWORD -e CyberPHY
Total number of stations seen 12
Total number of packets read 2660
Total number of WEP data packets 30
Total number of WPA data packets 629
Number of plaintext data packets 0
Number of decrypted WEP packets 0
Number of corrupted WEP packets 0
Number of decrypted WPA packets 471
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
root@CS2APenTest: # ls
core Desktop Downloads Pictures rockyou.txt Videos WPA2-P1-01.cap
CYSE301 Documents Music Public Templates VMshare WPA2-P1-01-dec.cap
root@CS2APenTest: #
```

Using the same method as before with the WPA2 file. I first moved the file onto the Linux Kali VM. I then used the command **aircrack-ng WPA2-P1-01.cap -w rockyou.txt** to perform a dictionary attack on the file with the rockyou.txt wordlist. Once I found the password which was **PASSWORD**. I used the command **airdecap-ng WPA2-P1-01.cap** and noted the ESSID which was **CyberPHY**. I used the command **airdecap-ng WPA2-P1-01.cap -p PASSWORD -e CyberPHY** and received the decrypted file **lab4wpa2-dec.cap**.

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -30 points

Wireshark - Endpoints - WPA2-P1-01-dec.cap

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
34.192.27.249	45	22 k	29	19 k	16	2,670	—	—	—	—
65.52.108.182	9	4,875	5	4,174	4	701	—	—	—	—
65.52.108.208	20	5,919	9	3,585	11	2,334	—	—	—	—
65.52.108.213	7	1,700	6	1,646	1	54	—	—	—	—
65.52.108.232	10	5,032	6	4,335	4	697	—	—	—	—
65.52.108.254	28	11 k	16	6,152	12	5,565	—	—	—	—
65.55.163.76	28	15 k	16	11 k	12	3,224	—	—	—	—
65.55.163.78	34	21 k	16	13 k	18	7,951	—	—	—	—
74.125.28.188	23	3,459	14	1,646	9	1,813	—	—	—	—
104.72.9.125	8	3,644	5	3,470	3	174	—	—	—	—
104.72.16.178	10	3,863	5	3,384	5	479	—	—	—	—
131.253.34.249	21	7,705	11	5,153	10	2,552	—	—	—	—
172.217.4.132	14	4,685	8	2,260	6	2,425	—	—	—	—
172.217.4.142	3	249	1	119	2	130	—	—	—	—
192.168.1.1	22	3,029	11	2,153	11	876	—	—	—	—
192.168.1.118	426	151 k	216	43 k	210	107 k	—	—	—	—
192.168.1.255	25	2,372	0	0	25	2,372	—	—	—	—
204.79.197.200	12	6,573	6	5,186	6	1,387	—	—	—	—
204.79.197.213	31	16 k	20	12 k	11	3,904	—	—	—	—
224.0.0.22	7	386	0	0	7	386	—	—	—	—
224.0.0.251	3	246	0	0	3	246	—	—	—	—
224.0.0.252	16	1,118	0	0	16	1,118	—	—	—	—
239.255.255.250	4	860	0	0	4	860	—	—	—	—
255.255.255.255	2	726	0	0	2	726	—	—	—	—

Frame 165 (bytes) Reassembled TCP (338 bytes)

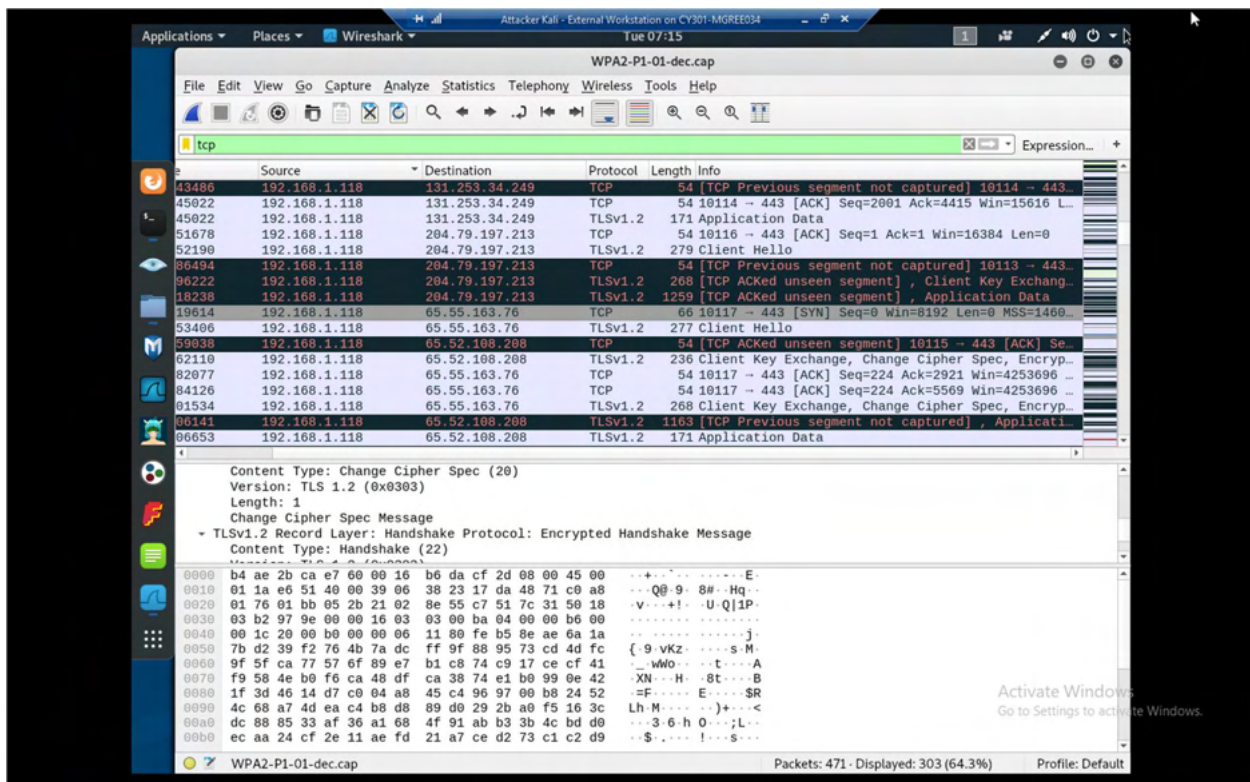
0000 f3 c9 83 1f 7e 72 12 ba 7c 81 2a fc 9b 94 08 37r...|.*....7
 0090 4e 64 e9 b2 09 6d cc 2e 3f 19 92 8f 16 03 03 00 Nd...m.?.....
 00a0 04 0e 0e 00 00 00

Wireshark - Endpoints - WPA2-P1-01-dec.cap

Source	Destination	Protocol	Length	Info
11518	192.168.1.118	NBNS	92	Name query NB WPAD<00>
18879	192.168.1.118	DNS	74	Standard query 0x5fb9 A login.live.com
20412	192.168.1.1	DNS	237	Standard query response 0x5fb9 A login.live.com..
70590	192.168.1.118	NBNS	92	Name query NB RwxQGfMDYLOV<00>
71102	192.168.1.118	NBNS	92	Name query NB MQLXTCRBPB<00>
71102	192.168.1.118	NBNS	92	Name query NB IASLBEXBT<00>
71102	fe80::75e6:f267:879... ff02::1:3	LLMNR	89	Standard query 0x2e99 A iaslbexbt
71615	fe80::75e6:f267:879... ff02::1:3	LLMNR	92	Standard query 0x0e55 A rwxqgfdylov
71614	fe80::75e6:f267:879... ff02::1:3	LLMNR	91	Standard query 0x7ec4 A mqlxcrbpbp
71614	192.168.1.118	LLMNR	71	Standard query 0x7ec4 A mqlxcrbpbp
72126	192.168.1.118	LLMNR	69	Standard query 0x2e99 A iaslbexbt
72125	192.168.1.118	LLMNR	72	Standard query 0x0e55 A rwxqgfdylov
90942	fe80::75e6:f267:879... ff02::1:3	LLMNR	89	Standard query 0x2e99 A iaslbexbt
91452	fe80::75e6:f267:879... ff02::1:3	LLMNR	91	Standard query 0x7ec4 A mqlxcrbpbp
91454	192.168.1.118	LLMNR	69	Standard query 0x2e99 A iaslbexbt
69278	192.168.1.118	NBNS	92	Name query NB WPAD<00>
92318	192.168.1.118	SSDP	215	M-SEARCH * HTTP/1.1

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 mqlxcrbpbp: type A, class IN

0000 33 33 00 01 00 03 b4 ae 2b ca e7 60 86 dd 60 00 33+...%...u...
 0010 00 00 00 25 11 01 fe 80 00 00 00 00 00 75 e6 .g...%...%...
 0020 f2 67 87 9e 3b 01 ff 02 00 00 00 00 00 00 00 14 eb 00 25 14 d1 bd da%...mqlx...
 0030 00 00 00 01 00 00 00 00 00 00 0b 6d 71 6c 65 78mqlx...
 0040 00 00 00 01 00 00 00 00 00 00 0b 6d 71 6c 65 78mqlx...
 0050 74 63 72 70 62 70 00 00 01 00 01 tcrbpb ...



After analyzing the decrypted file in Wireshark, I noticed a high amount of traffic with the IP address 192.168.1.118. There was a high amount of encrypted traffic between the suspicious IP address and various other IP addresses. I also noticed payload exchanges, and a high amount of name queries with NetBIOS and Link-Local Multicast protocols. This may be a possible intruder in the network snooping around the network for other devices.