Assignment 6: Wi-Fi Password Cracking

CYSE 301: Cybersecurity Technique and Operations

Carl Lochstampfor — UIN cloch001

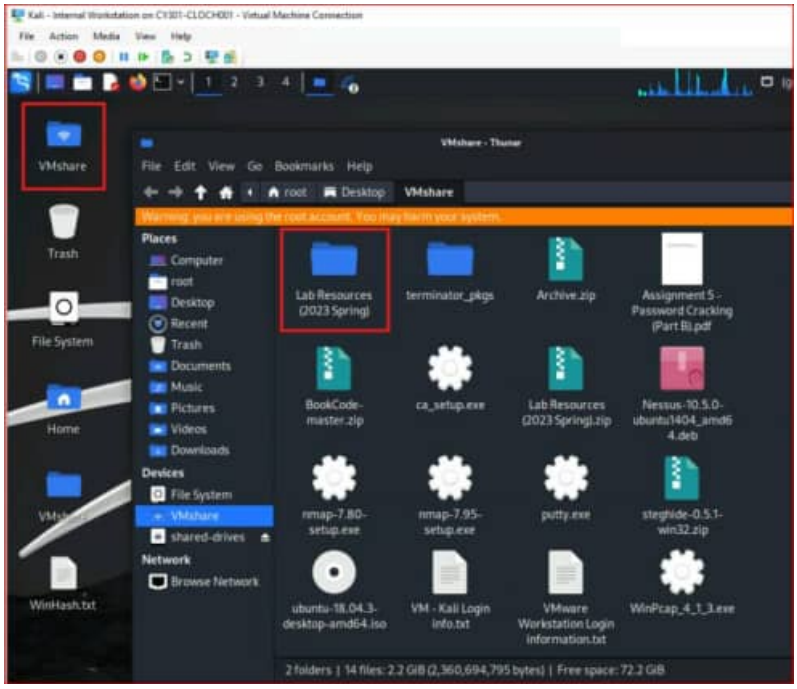
April 3, 2026

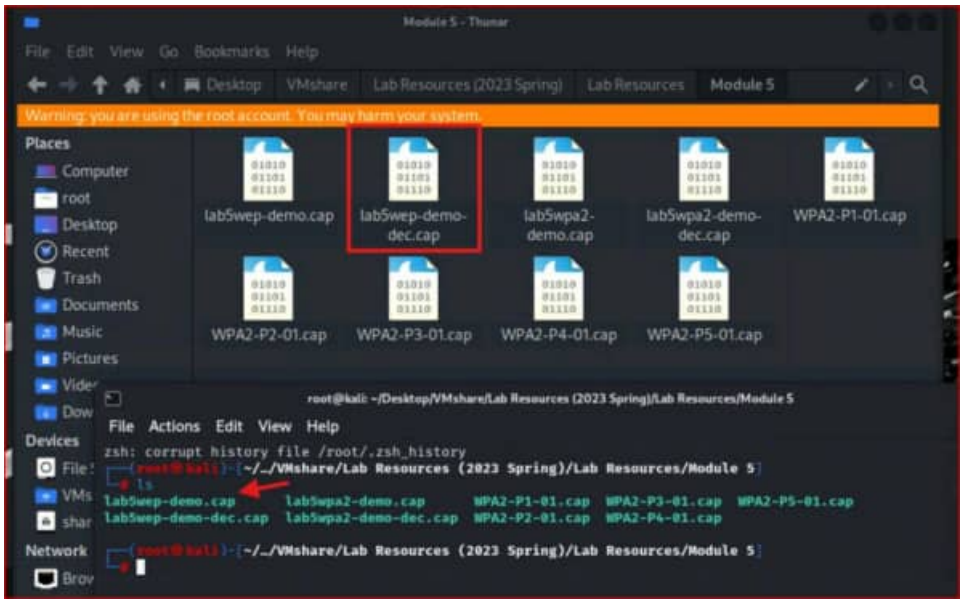
Task C: 20 points

Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

1. Decrypt the lab5wep-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

Step 1: Navigate to Module 5 on the VM





Step 2: Crack the WEP Key

Command >> *aircrack-ng lab5wep-demo.cap*

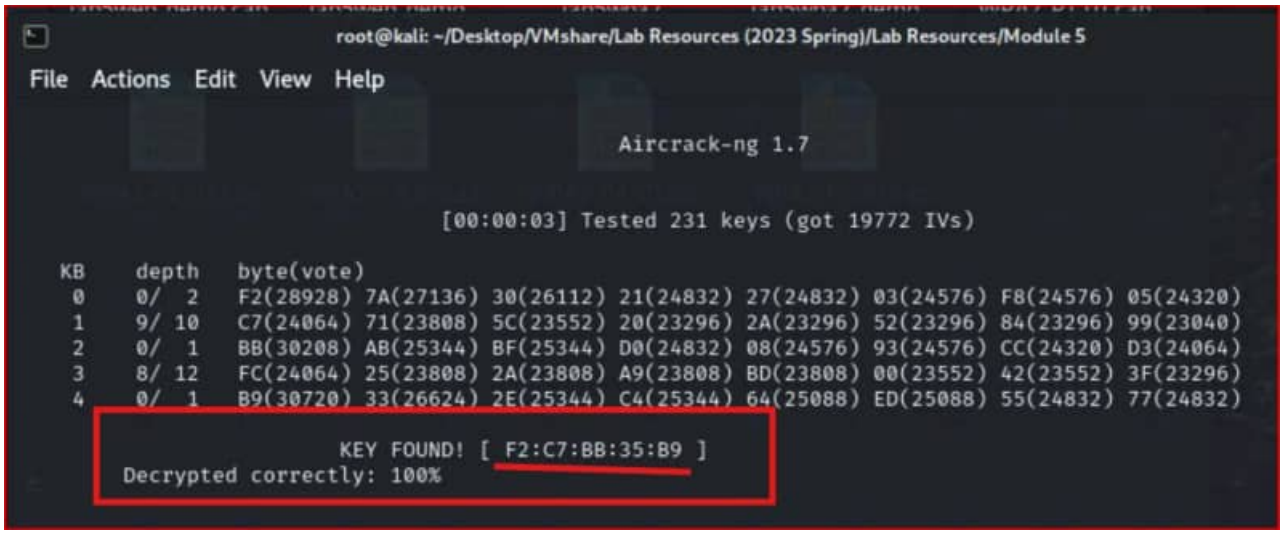
```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng lab5wep-demo.cap
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:32  ccni-test                 WEP (19772 IVs)
   2  00:25:84:FD:66:00                            Unknown
   3  00:25:84:FD:66:03                            Unknown
   4  02:21:F1:A6:B0:A0  hpsetup                   Unknown
   5  04:DA:D2:B2:92:D1                            Unknown
   6  18:9C:5D:EF:46:70                            Unknown
   7  18:9C:5D:EF:48:50                            Unknown
   8  18:9C:5D:EF:4D:A0                            Unknown
   9  58:BF:EA:0F:F9:00                            Unknown
  10  58:BF:EA:0F:F9:01                            Unknown
  11  58:BF:EA:24:98:91                            WPA (0 handshake)
  12  58:BF:EA:FA:16:10                            Unknown
  13  58:BF:EA:FA:38:B0                            Unknown
  14  58:BF:EA:FA:3B:A0                            Unknown
  15  58:BF:EA:FA:3B:A2  MonarchODU                WPA (0 handshake)
  16  5C:50:15:E7:FE:42  MonarchODU                EAPOL+WPA (0 handshake)
  17  98:FC:11:7C:CE:63  dd-wrt                    Unknown
  18  98:FC:11:7C:D0:C7  CCNI                      WPA (0 handshake)
  19  F4:7F:35:04:01:A0                            Unknown
  20  F4:7F:35:04:08:20                            Unknown
  21  F4:7F:35:04:65:A0                            Unknown
  22  F4:7F:35:04:7D:E0  AccessODU                 Unknown
  23  F4:7F:35:04:7D:E1                            Unknown
  24  F4:7F:35:04:7D:E2  MonarchODU                WPA (0 handshake)
  25  F4:7F:35:04:7D:E4  eduroam                   Unknown
  26  F4:7F:35:39:0A:A0                            Unknown
  27  F4:7F:35:42:0E:C2                            Unknown

Index number of target network ? 1
```

Results: Key Found, F2:C7:BB:35:B9


root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Aircrack-ng 1.7
[00:00:03] 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)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832)
KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%

Step 3: Decrypt the WEP Traffic

Command >> *airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap*

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.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
Warning: WDS packets detected, but no BSSID specified
```

Step 4: Open Decrypted File in Wireshark

Protocols showing >> HTTP and FTP (Statistics >> Protocol Hierarchy)

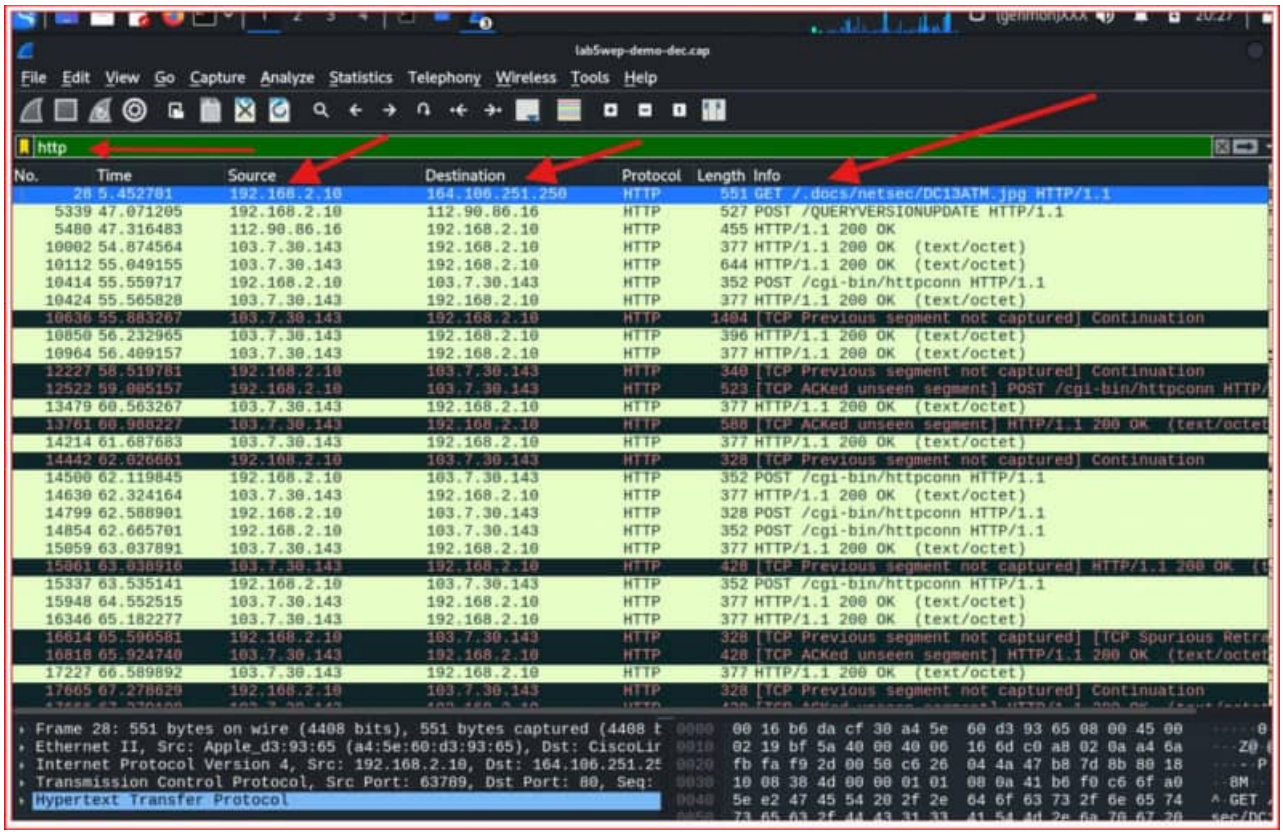
Wireshark · Protocol Hierarchy Statistics · lab5wep-demo-dec.cap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	142415	100.0	22356528	568 k	0	0	0
Ethernet	100.0	142415	9.4	2098984	53 k	0	0	0
Internet Protocol Version 6	0.0	60	0.0	2400	61	0	0	0
User Datagram Protocol	0.0	46	0.0	368	9	0	0	0
Multicast Domain Name System	0.0	40	0.0	5394	137	40	5394	137
DHCPv6	0.0	6	0.0	594	15	6	594	15
Internet Control Message Protocol v6	0.0	14	0.0	324	8	14	324	8
Internet Protocol Version 4	13.7	19550	1.7	391028	9,945	0	0	0
User Datagram Protocol	0.1	198	0.0	1584	40	0	0	0
NetBIOS Name Service	0.0	20	0.0	1102	28	20	1102	28
NetBIOS Datagram Service	0.0	3	0.0	549	13	0	0	0
SMB (Server Message Block Protocol)	0.0	3	0.0	303	7	0	0	0
SMB MailSlot Protocol	0.0	3	0.0	75	1	0	0	0
Microsoft Windows Browser Protocol	0.0	3	0.0	45	1	3	45	1
Multicast Domain Name System	0.0	30	0.0	4542	115	30	4542	115
Dynamic Host Configuration Protocol	0.0	5	0.0	1500	38	5	1500	38
Dropbox LAN sync Discovery Protocol	0.0	20	0.0	2300	58	20	2300	58
Domain Name System	0.1	80	0.0	6069	154	80	6069	154
Transmission Control Protocol	13.6	19342	73.4	16399012	417 k	15655	11894338	302 k
Transport Layer Security	0.6	808	2.7	603257	15 k	808	599145	15 k
Hypertext Transfer Protocol	0.9	1274	7.5	1686594	42 k	1216	1625487	41 k
MIME Multipart Media Encapsulation	0.0	2	0.0	1767	44	2	1767	44
Media Type	0.0	17	0.0	4322	109	17	4322	109
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Line-based text data	0.0	11	0.0	7573	192	11	7573	192
JPEG File Interchange Format	0.0	3	0.1	12178	309	3	12178	309
JavaScript Object Notation	0.0	1	0.0	12	0	1	12	0
HTML Form URL Encoded	0.0	14	0.1	17314	440	14	17314	440
Compuserve GIF	0.0	9	0.0	2734	69	9	2734	69
FTP Data	0.0	7	0.0	9464	240	7	9464	240
File Transfer Protocol (FTP)	0.0	22	0.0	656	16	22	656	16
Internet Group Management Protocol	0.0	7	0.0	56	1	7	56	1
Internet Control Message Protocol	0.0	3	0.0	120	3	0	0	0
Data	1.2	1733	9.7	2175402	55 k	1733	2175402	55 k
Address Resolution Protocol	86.2	122691	15.8	3540522	90 k	122691	3540522	90 k

HTTP

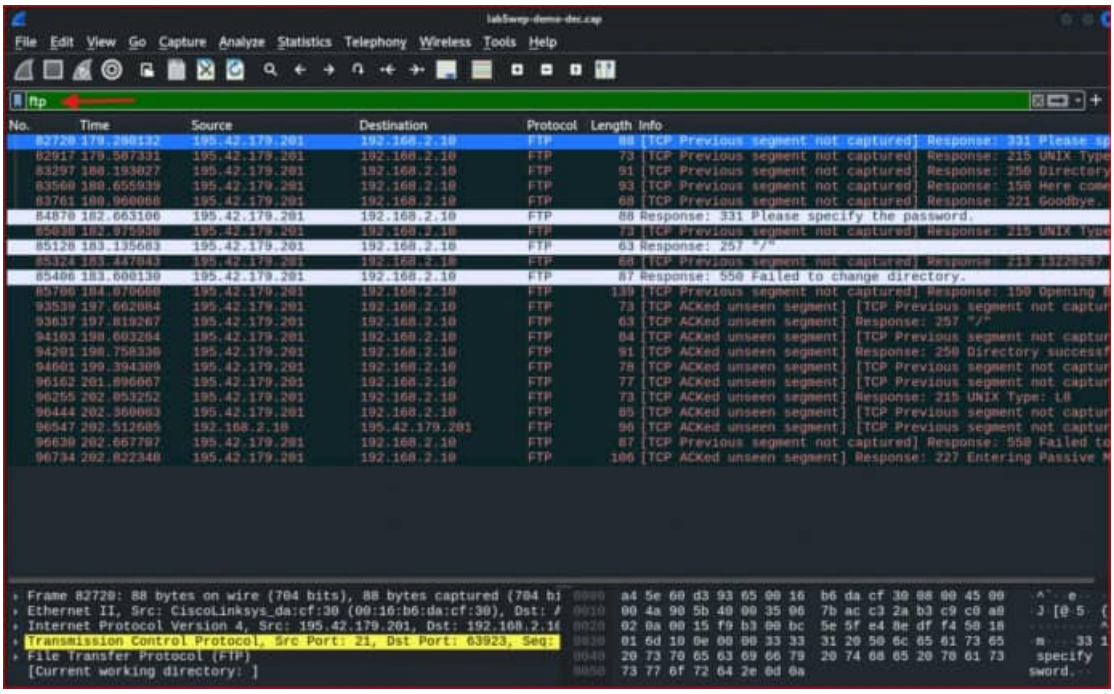
Wireshark · Protocol Hierarchy Statistics · lab5wep-demo-dec.cap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	1274	100.0	1739746	46 k	0	0	0	1274
Ethernet	100.0	1274	1.0	17836	479	0	0	0	1274
Internet Protocol Version 4	100.0	1274	1.5	25480	684	0	0	0	1274
Transmission Control Protocol	100.0	1274	97.5	1696430	45 k	0	0	0	1274
Hypertext Transfer Protocol	100.0	1274	96.9	1686594	45 k	1216	1625487	43 k	1274
MIME Multipart Media Encapsulation	0.2	2	0.1	1767	47	2	1767	47	2
Media Type	1.3	17	0.2	4322	116	17	4322	116	17
Malformed Packet	0.1	1	0.0	0	0	1	0	0	1
Line-based text data	0.9	11	0.4	7573	203	11	7573	203	11
JPEG File Interchange Format	0.2	3	0.7	12178	327	3	12178	327	3
JavaScript Object Notation	0.1	1	0.0	12	0	1	12	0	1
HTML Form URL Encoded	1.1	14	1.0	17314	465	14	17314	465	14
Compuserve GIF	0.7	9	0.2	2734	73	9	2734	73	9


labSwep-demo-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
28 5.452781 192.168.2.10 164.106.251.250 HTTP 551 GET /.docs/netsec/DC13ATM.jpg HTTP/1.1
5339 47.071205 192.168.2.10 112.90.86.16 HTTP 527 POST /QUERYVERSIONUPDATE HTTP/1.1
5480 47.316483 112.90.86.16 192.168.2.10 HTTP 455 HTTP/1.1 200 OK
10002 54.874564 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
10112 55.049155 103.7.30.143 192.168.2.10 HTTP 644 HTTP/1.1 200 OK (text/octet)
10414 55.559717 192.168.2.10 103.7.30.143 HTTP 352 POST /cgi-bin/httpconn HTTP/1.1
10424 55.565828 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
10636 55.883267 103.7.30.143 192.168.2.10 HTTP 1484 [TCP Previous segment not captured] Continuation
10850 56.232965 103.7.30.143 192.168.2.10 HTTP 396 HTTP/1.1 200 OK (text/octet)
10964 56.409157 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
12227 58.519781 192.168.2.10 103.7.30.143 HTTP 340 [TCP Previous segment not captured] Continuation
12522 59.005157 192.168.2.10 103.7.30.143 HTTP 523 [TCP ACKed unseen segment] POST /cgi-bin/httpconn HTTP/
13479 60.563267 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
13761 60.980227 103.7.30.143 192.168.2.10 HTTP 588 [TCP ACKed unseen segment] HTTP/1.1 200 OK (text/octet
14214 61.687683 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
14442 62.026661 192.168.2.10 103.7.30.143 HTTP 328 [TCP Previous segment not captured] Continuation
14500 62.119845 192.168.2.10 103.7.30.143 HTTP 352 POST /cgi-bin/httpconn HTTP/1.1
14630 62.324164 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
14799 62.588901 192.168.2.10 103.7.30.143 HTTP 328 POST /cgi-bin/httpconn HTTP/1.1
14854 62.665701 192.168.2.10 103.7.30.143 HTTP 352 POST /cgi-bin/httpconn HTTP/1.1
15059 63.037891 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
15061 63.038910 103.7.30.143 192.168.2.10 HTTP 428 [TCP Previous segment not captured] HTTP/1.1 200 OK (t
15337 63.535141 192.168.2.10 103.7.30.143 HTTP 352 POST /cgi-bin/httpconn HTTP/1.1
15948 64.552515 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
16346 65.182277 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
16614 65.596581 192.168.2.10 103.7.30.143 HTTP 328 [TCP Previous segment not captured] [TCP Spurious Retra
16818 65.924740 103.7.30.143 192.168.2.10 HTTP 428 [TCP ACKed unseen segment] HTTP/1.1 200 OK (text/octet
17227 66.589892 103.7.30.143 192.168.2.10 HTTP 377 HTTP/1.1 200 OK (text/octet)
17665 67.278620 192.168.2.10 103.7.30.143 HTTP 328 [TCP Previous segment not captured] Continuation
Frame 28: 551 bytes on wire (4408 bits), 551 bytes captured (4408 t
Ethernet II, Src: Apple_d3:93:65 (a4:5e:60:d3:93:65), Dst: CiscoLir
Internet Protocol Version 4, Src: 192.168.2.10, Dst: 164.106.251.25
Transmission Control Protocol, Src Port: 63789, Dst Port: 80, Seq:
Hypertext Transfer Protocol
0000 00 16 b6 da cf 30 a4 5e 60 d3 93 65 08 00 45 00
0010 02 19 bf 5a 40 00 40 06 16 6d c0 a8 02 0a a4 6a
0020 fb fa f9 2d 00 50 c6 26 04 4a 47 b8 7d 8b 80 18
0030 10 08 38 4d 00 00 01 01 08 0a 41 b6 f0 c6 6f a0
0040 5e e2 47 45 54 20 2f 2e 64 6f 63 73 2f 6e 65 74

FTP


Wireshark · Protocol Hierarchy Statistics · labSwep-demo-dec.cap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes End Bits/s PDUs
Frame 100.0 22 100.0 1844 626 0 0 0 22
Ethernet 100.0 22 16.7 308 104 0 0 0 22
Internet Protocol Version 4 100.0 22 23.9 440 149 0 0 0 22
Transmission Control Protocol 100.0 22 59.4 1096 372 0 0 0 22
File Transfer Protocol (FTP) 100.0 22 35.6 656 222 22 656 222 22


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
No. Time Source Destination Protocol Length Info
82720 179.280132 195.42.179.201 192.168.2.10 FTP 88 [TCP Previous segment not captured] Response: 331 Please sp
82917 179.587331 195.42.179.201 192.168.2.10 FTP 73 [TCP Previous segment not captured] Response: 215 UNIX Type
83297 180.193027 195.42.179.201 192.168.2.10 FTP 91 [TCP Previous segment not captured] Response: 250 Directory
83560 180.655939 195.42.179.201 192.168.2.10 FTP 93 [TCP Previous segment not captured] Response: 150 Here come
83761 180.960068 195.42.179.201 192.168.2.10 FTP 68 [TCP Previous segment not captured] Response: 221 Goodbye.
84870 182.663106 195.42.179.201 192.168.2.10 FTP 88 Response: 331 Please specify the password.
85088 182.975930 195.42.179.201 192.168.2.10 FTP 73 [TCP Previous segment not captured] Response: 215 UNIX Type
85120 183.135683 195.42.179.201 192.168.2.10 FTP 63 Response: 257 "/"
85324 183.447043 195.42.179.201 192.168.2.10 FTP 68 [TCP Previous segment not captured] Response: 213 13220287
85400 183.600130 195.42.179.201 192.168.2.10 FTP 87 Response: 550 Failed to change directory.
85700 184.070080 195.42.179.201 192.168.2.10 FTP 139 [TCP Previous segment not captured] Response: 150 Opening
93539 197.662084 195.42.179.201 192.168.2.10 FTP 73 [TCP ACKed unseen segment] [TCP Previous segment not captur
93637 197.819267 195.42.179.201 192.168.2.10 FTP 63 [TCP ACKed unseen segment] Response: 257 "/"
94103 198.603284 195.42.179.201 192.168.2.10 FTP 84 [TCP ACKed unseen segment] [TCP Previous segment not captur
94201 198.758330 195.42.179.201 192.168.2.10 FTP 91 [TCP ACKed unseen segment] Response: 250 Directory successf
94601 199.394309 195.42.179.201 192.168.2.10 FTP 78 [TCP ACKed unseen segment] [TCP Previous segment not captur
96102 201.896067 195.42.179.201 192.168.2.10 FTP 77 [TCP ACKed unseen segment] [TCP Previous segment not captur
96255 202.053252 195.42.179.201 192.168.2.10 FTP 73 [TCP ACKed unseen segment] Response: 215 UNIX Type: L8
96444 202.360083 195.42.179.201 192.168.2.10 FTP 85 [TCP ACKed unseen segment] [TCP Previous segment not captur
96547 202.512685 192.168.2.10 195.42.179.201 FTP 90 [TCP ACKed unseen segment] [TCP Previous segment not captur
96630 202.667707 195.42.179.201 192.168.2.10 FTP 87 [TCP Previous segment not captured] Response: 550 Failed to
96734 202.822340 195.42.179.201 192.168.2.10 FTP 106 [TCP ACKed unseen segment] Response: 227 Entering Passive M
Frame 82720: 88 bytes on wire (704 bits), 88 bytes captured (704 bi
Ethernet II, Src: CiscoLinksys_da:cf:30 (00:16:b6:da:cf:30), Dst: A
Internet Protocol Version 4, Src: 195.42.179.201, Dst: 192.168.2.10
Transmission Control Protocol, Src Port: 21, Dst Port: 63923, Seq:
File Transfer Protocol (FTP)
[Current working directory:]
0000 a4 5e 60 d3 93 65 00 16 b6 da cf 30 08 00 45 00
0010 00 4a 90 5b 40 00 35 06 7b ac c3 2a b3 c9 c0 a8
0020 02 0a 00 15 f9 b3 00 bc 5e 5f e4 8e df f4 50 18
0030 01 6d 10 0e 00 00 33 33 31 20 50 6c 65 61 73 65
0040 20 73 70 65 63 69 66 79 20 74 68 65 20 70 61 73
0050 73 77 6f 72 64 2e 0d 0a

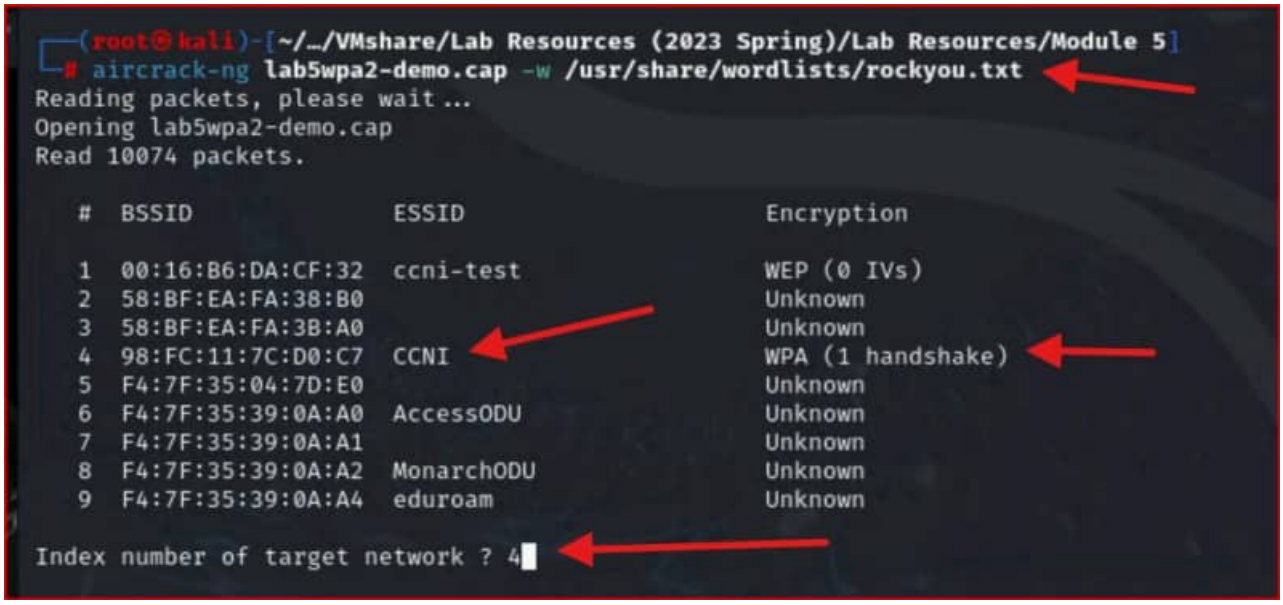
Task C.1 — WEP Traffic Analysis:

After decrypting lab5wep-demo.cap using the cracked WEP key (F2:C7:BB:35:B9), the Protocol Hierarchy Statistics revealed 142,415 total packets. The decrypted traffic exposed multiple plaintext protocols including HTTP (1,274 packets), FTP (22 packets), DNS (80 packets), and ARP (122,691 packets). HTTP traffic showed web requests between 192.168.2.10 and external servers, including file downloads (JPEG images, GIF files). FTP traffic from 195.42.179.201 revealed directory browsing and file transfer commands in plaintext, demonstrating the serious security risk of using WEP encryption.

2. Decrypt the lab5wpa2-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

Step 5: Crack WPA2 Demo File

Command >> aircrack-ng lab5wpa2-demo.cap -w /usr/share/wordlists/rockyou.txt



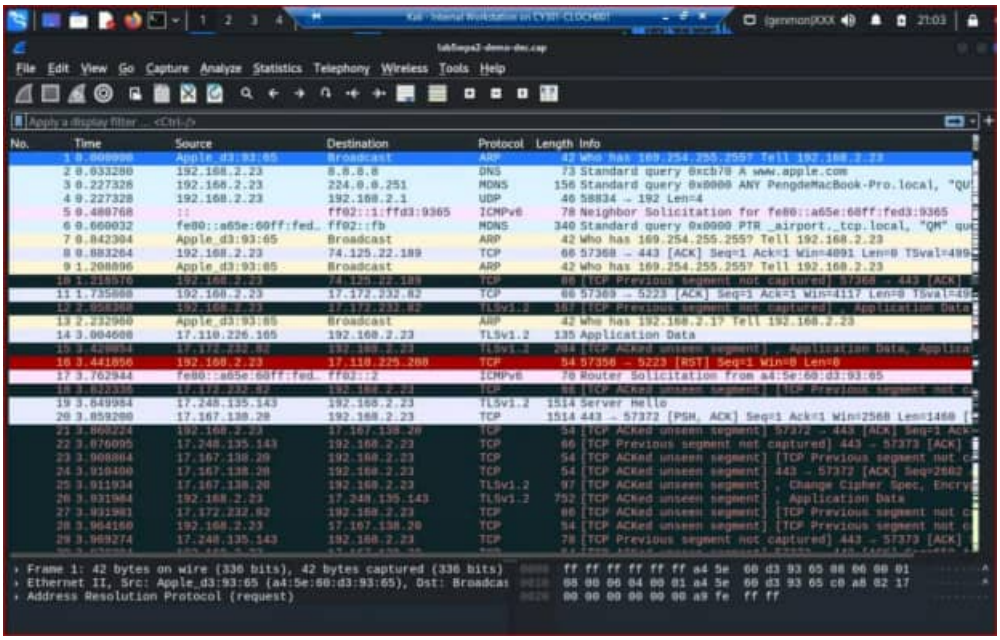
Result: Key found, password

Step 6: Decrypt the WPA2 Traffic

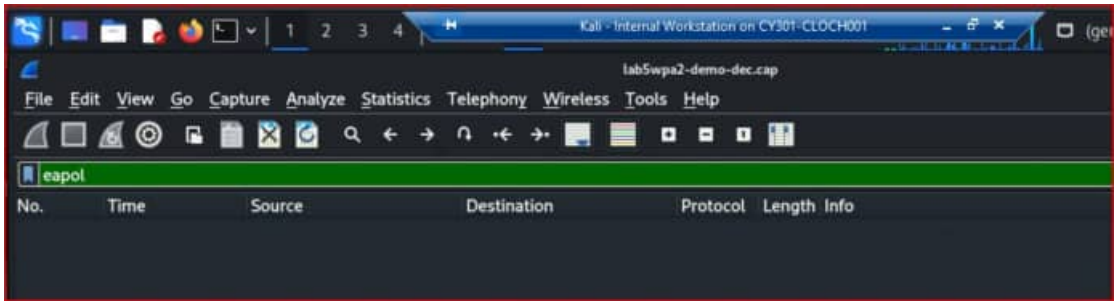
Command >> airdecap-ng -p password lab5wpa2-demo.cap -e CCNI

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
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
Warning: WDS packets detected, but no BSSID specified
```

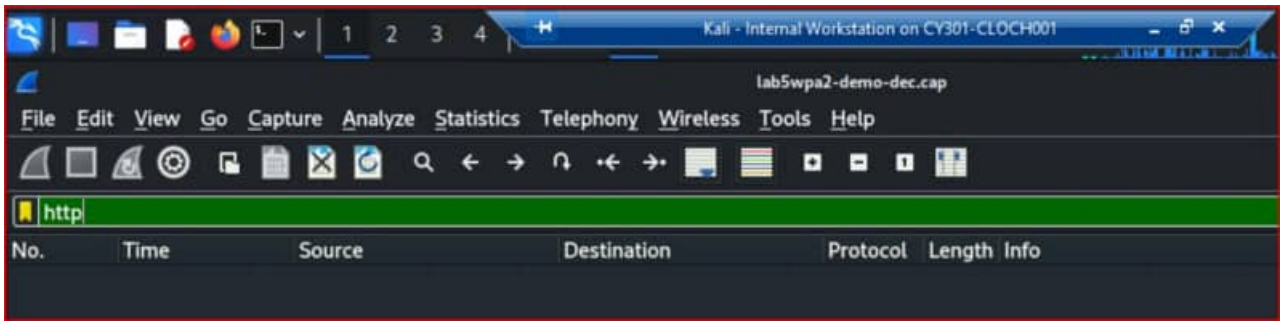
Step 7: Open Decrypted WPA2 File in Wireshark

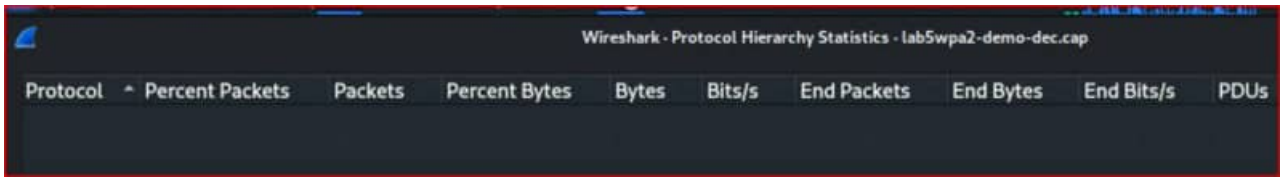


Filter: eapol (no results)

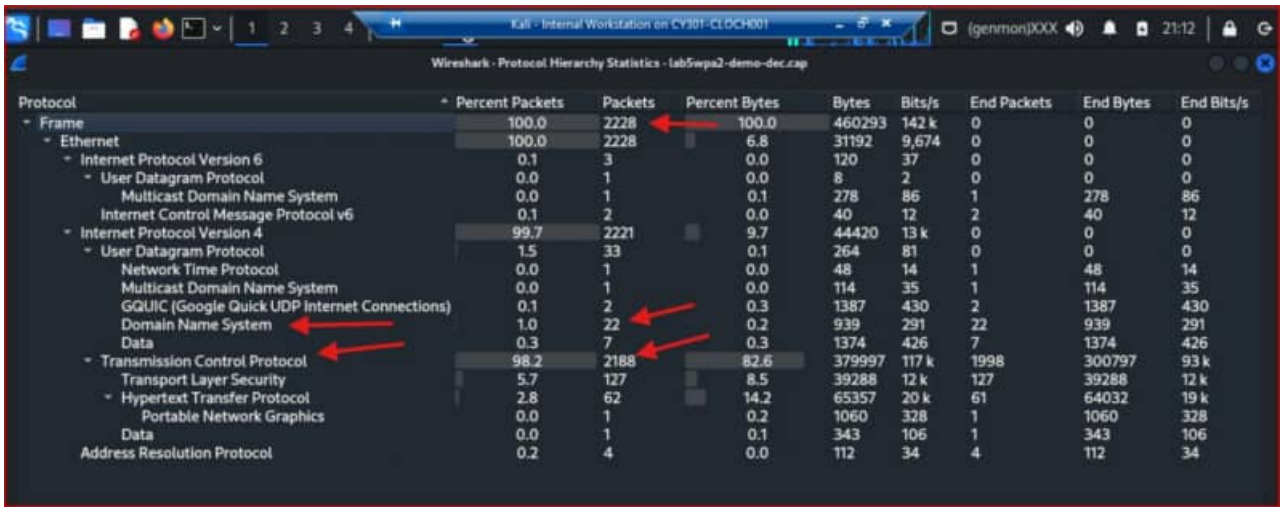


Filter: http (no results)





General Results:



Task C.2 — Protocol Hierarchy Statistics for lab5wpa2-demo-dec.cap

After decrypting lab5wpa2-demo.cap using the cracked WPA2 password ("password") for the CCNI network, the Protocol Hierarchy Statistics revealed 2,228 total decrypted packets. The traffic is dominated by TCP (98.2%), with Transport Layer Security (TLS) accounting for 127 packets, indicating most web traffic is encrypted at the application layer via HTTPS. HTTP traffic (62 packets) was also present, along with DNS (22 packets) used for domain name resolution, and a small amount of ARP (4 packets). Compared to the WEP capture, the WPA2 traffic contains significantly fewer packets and no plaintext FTP sessions, reflecting a more security-conscious network environment. However, the successful decryption demonstrates that WPA2 is still vulnerable to dictionary attacks when weak passwords like "password" are used.

Task D: 30 points

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 **(i.e., cloch001).** For example, the last digit of the hash for svatsa is **8**. Thus, I should pick up the file "WPA2-P3-01.cap."

*MD5 of **svatsa** is fe2943715a4e07c670b242559f5974f**8***

```
┌──(root㉿kali)-[~]
└─# echo -n svatsa | md5sum
fe2943715a4e07c670b242559f5974f8  -
```

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

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 (2023 Spring)." You can locate the zipped folder in your VMshare in any Kali Linux VM. Then, extract the zipped file and find the assigned WPA file under the sub-folder "WPA traffic."
- Please note that - it is recommended to copy the zip file to your local folder before extracting the whole file in the VMshare folder.

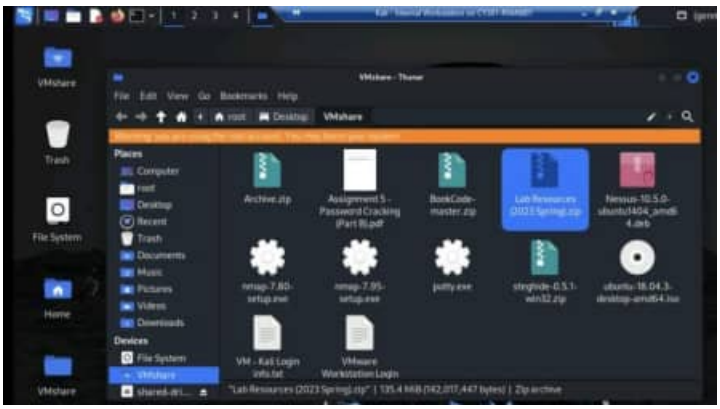


Figure 1 Location of Lab Resource (2023 Spring) in the VMshare folder.

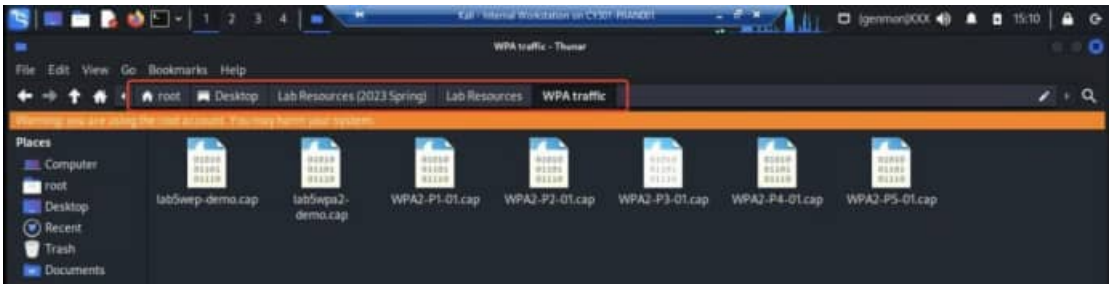
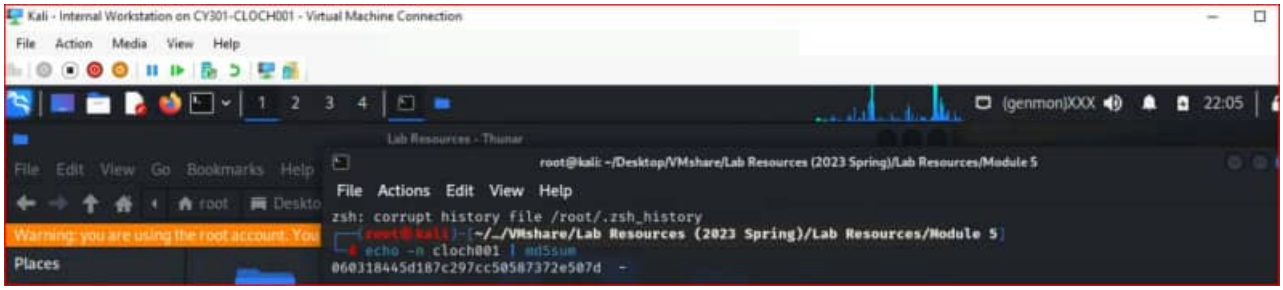


Figure 2 I copied the zip file to the Desktop and then extracted it to access the WPA traffic folder.

Then complete the following steps:

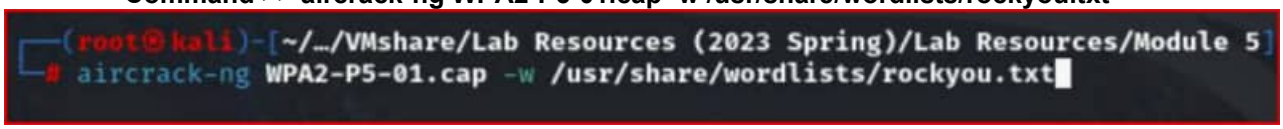
1. Implement a dictionary attack and decrypt the traffic using the correct file based on your last character of md5 hash for your midas name. - 20 points
2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file (using wireshark). -10 points

Command >> echo -n cloch001 | md5sum (d is the last character, thus WPA2-P5-01.cap)

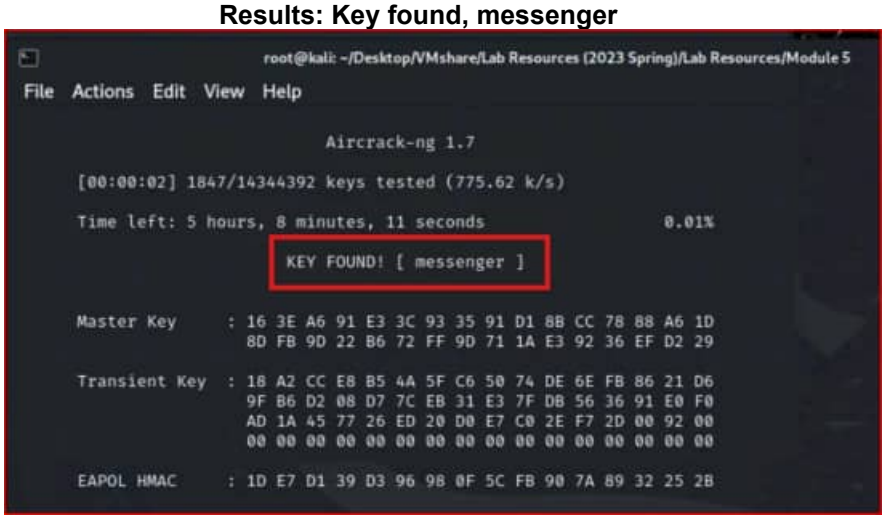


Step 8: Task D: Crack WPA2-P5-01.cap

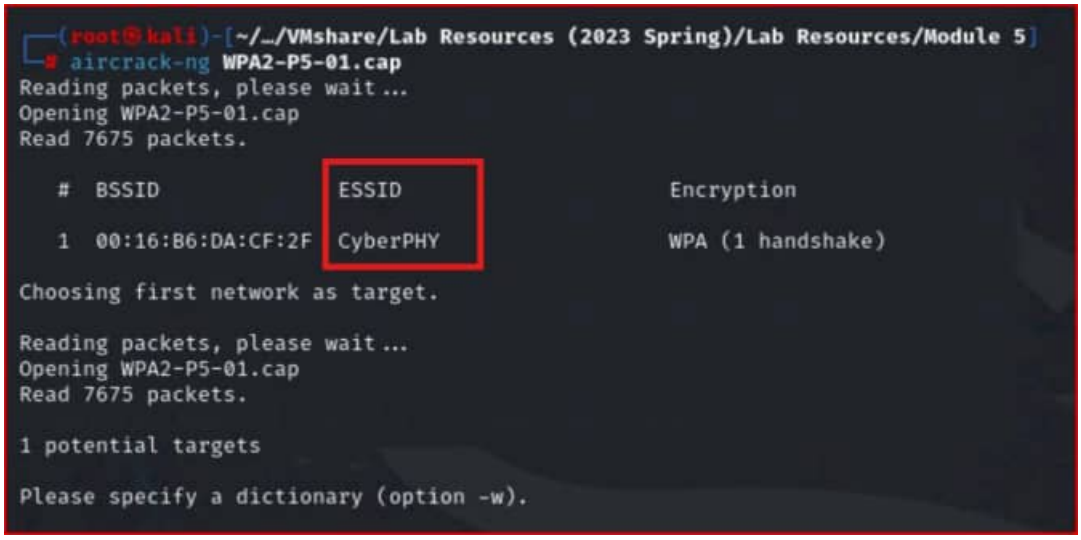
Command >> aircrack-ng WPA2-P5-01.cap -w /usr/share/wordlists/rockyou.txt



Results: Key found, messenger

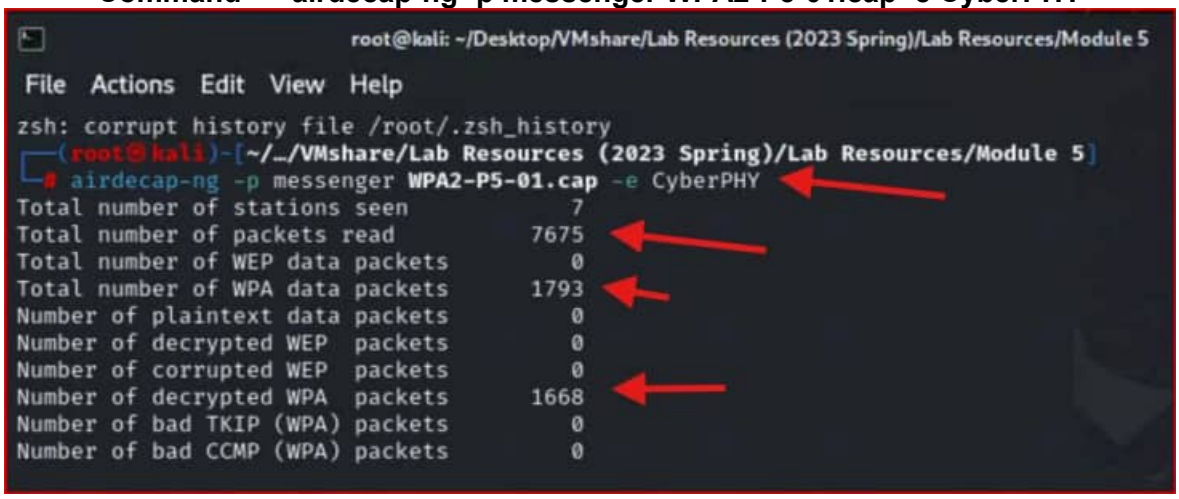


Command >> aircrack-ng WPA2-P5-01.cap (grabs the ESSID)


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng WPA2-P5-01.cap
Reading packets, please wait...
Opening WPA2-P5-01.cap
Read 7675 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:2F CyberPHY WPA (1 handshake)
Choosing first network as target.
Reading packets, please wait...
Opening WPA2-P5-01.cap
Read 7675 packets.
1 potential targets
Please specify a dictionary (option -w).

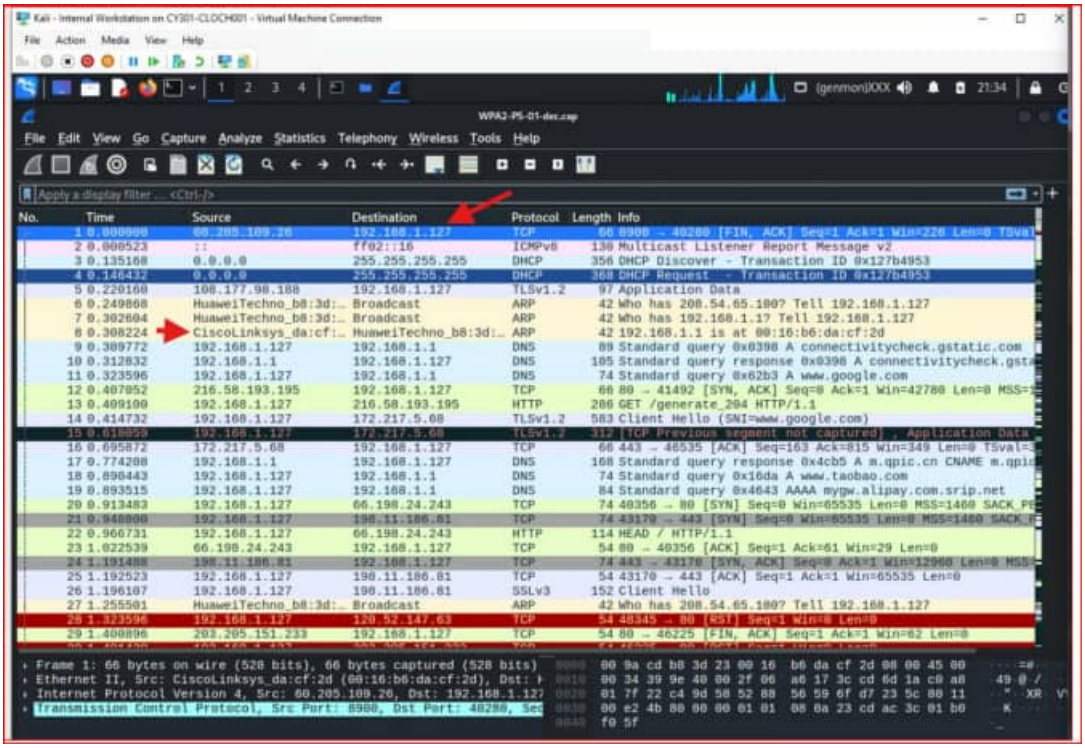
Step 9: Decrypt Task D Traffic

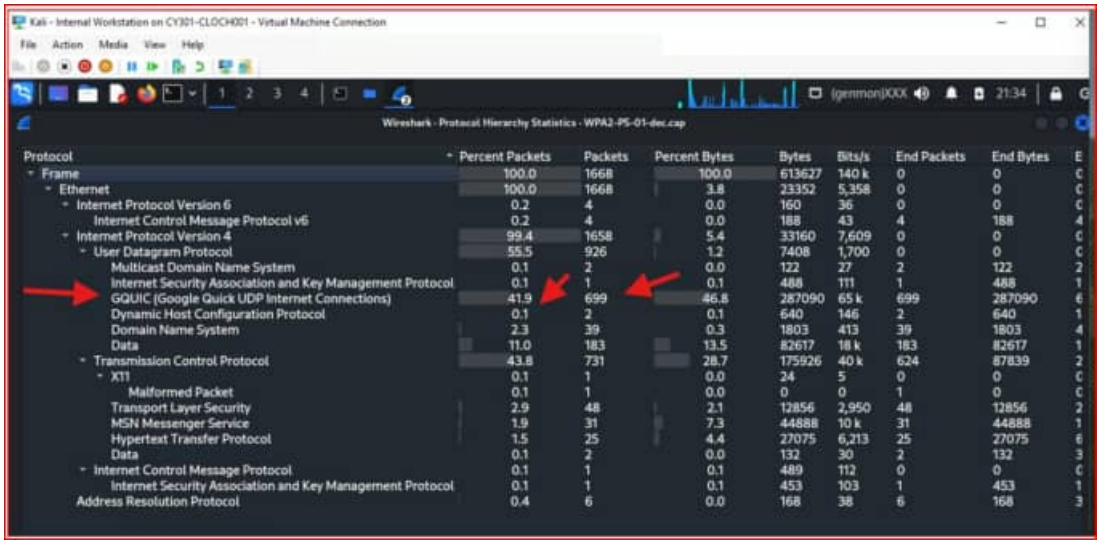
Command >> airdecap-ng -p messenger WPA2-P5-01.cap -e CyberPHY



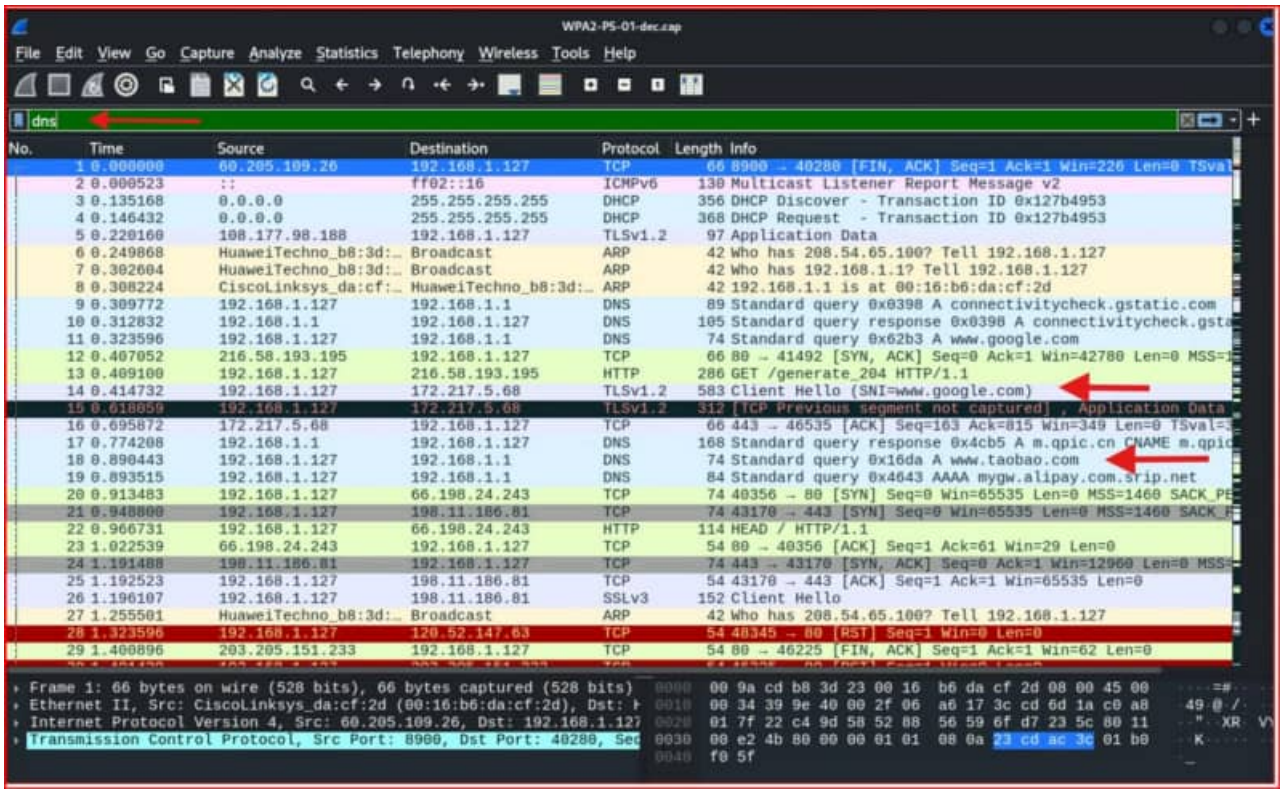
Command >> airdecap-ng -p messenger WPA2-P5-01.cap -e CyberPHY

Step 10: Open Task D File in Wireshark



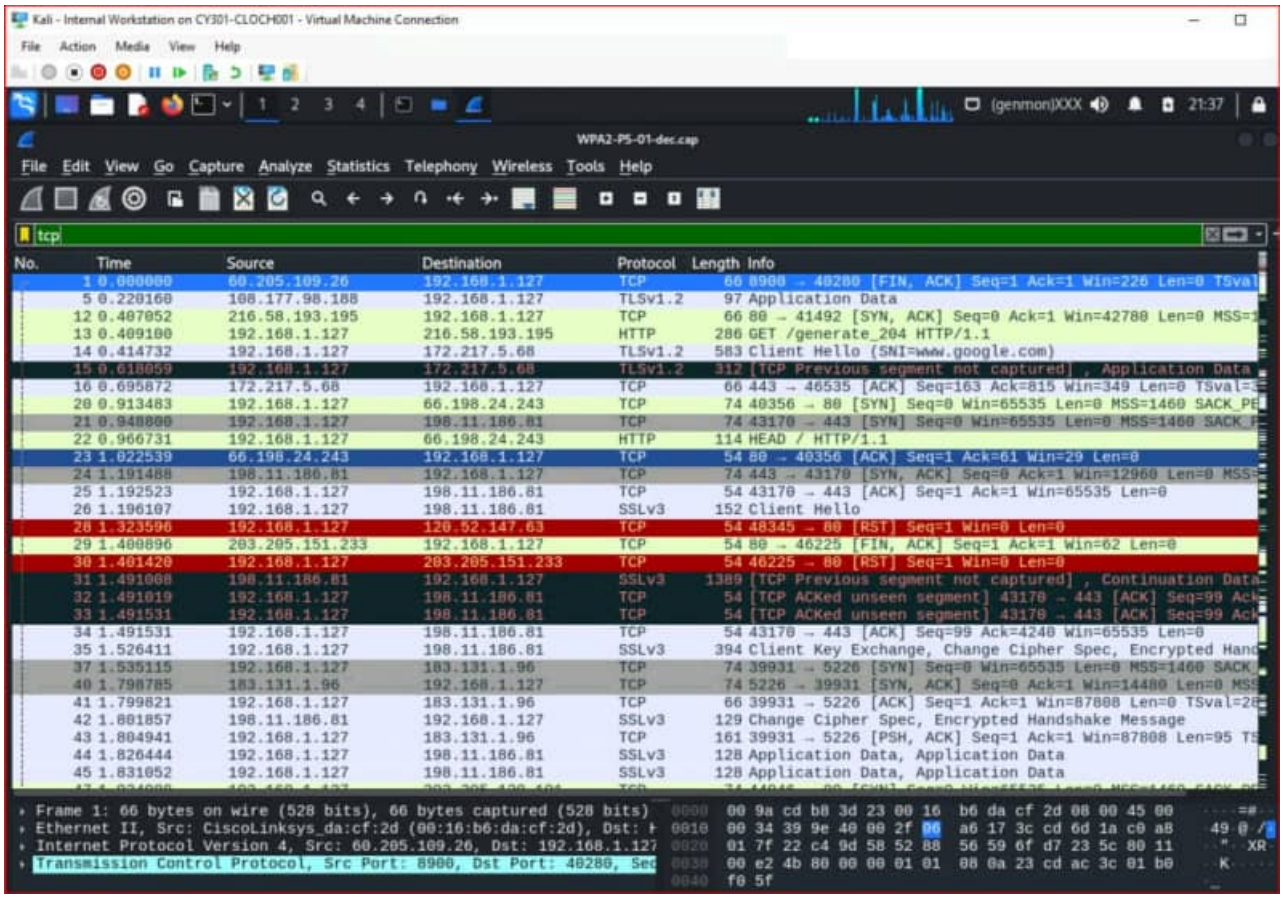

Kali - Internal Workstation on CY301-CLOCH001 - Virtual Machine Connection
Wireshark · Protocol Hierarchy Statistics · WPA2-PS-01-dec.cap
Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes
Frame | 100.0 | 1668 | 100.0 | 613627 | 140 k | 0 | 0
Ethernet | 100.0 | 1668 | 3.8 | 23352 | 5,358 | 0 | 0
Internet Protocol Version 6 | 0.2 | 4 | 0.0 | 160 | 36 | 0 | 0
Internet Control Message Protocol v6 | 0.2 | 4 | 0.0 | 188 | 43 | 4 | 188
Internet Protocol Version 4 | 99.4 | 1658 | 5.4 | 33160 | 7,609 | 0 | 0
User Datagram Protocol | 55.5 | 926 | 1.2 | 7408 | 1,700 | 0 | 0
Multicast Domain Name System | 0.1 | 2 | 0.0 | 122 | 27 | 2 | 122
Internet Security Association and Key Management Protocol | 0.1 | 1 | 0.1 | 488 | 111 | 1 | 488
GQUIC (Google Quick UDP Internet Connections) | 41.9 | 699 | 46.8 | 287090 | 65 k | 699 | 287090
Dynamic Host Configuration Protocol | 0.1 | 2 | 0.1 | 640 | 146 | 2 | 640
Domain Name System | 2.3 | 39 | 0.3 | 1803 | 413 | 39 | 1803
Data | 11.0 | 183 | 13.5 | 82617 | 18 k | 183 | 82617
Transmission Control Protocol | 43.8 | 731 | 28.7 | 175926 | 40 k | 624 | 87839
X11 | 0.1 | 1 | 0.0 | 24 | 5 | 0 | 0
Malformed Packet | 0.1 | 1 | 0.0 | 0 | 0 | 1 | 0
Transport Layer Security | 2.9 | 48 | 2.1 | 12856 | 2,950 | 48 | 12856
MSN Messenger Service | 1.9 | 31 | 7.3 | 44888 | 10 k | 31 | 44888
Hypertext Transfer Protocol | 1.5 | 25 | 4.4 | 27075 | 6,213 | 25 | 27075
Data | 0.1 | 2 | 0.0 | 132 | 30 | 2 | 132
Internet Control Message Protocol | 0.1 | 1 | 0.1 | 489 | 112 | 0 | 0
Internet Security Association and Key Management Protocol | 0.1 | 1 | 0.1 | 453 | 103 | 1 | 453
Address Resolution Protocol | 0.4 | 6 | 0.0 | 168 | 38 | 6 | 168

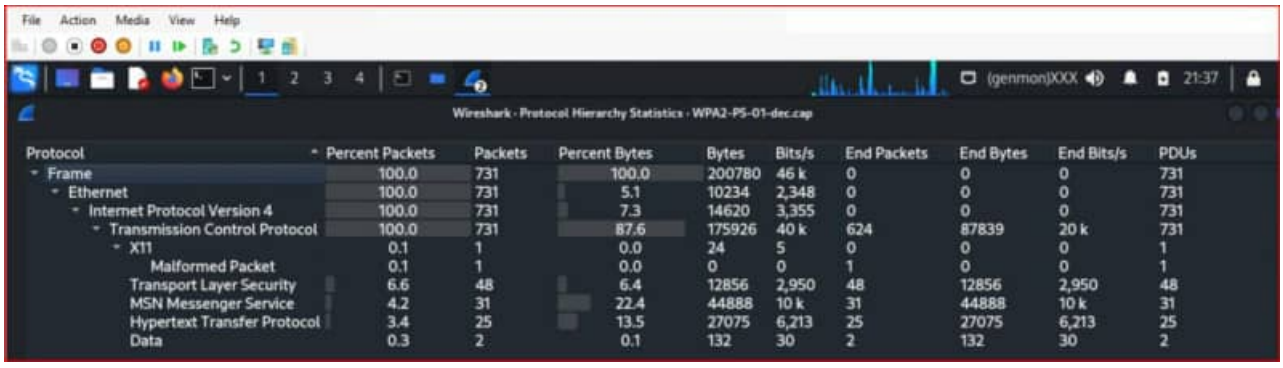
Filter: DNS


WPA2-PS-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1 0.000000 60.205.109.26 192.168.1.127 TCP 66 8900 → 40280 [FIN, ACK] Seq=1 Ack=1 Win=226 Len=0 TSval
2 0.000523 :: ff02::16 ICMPv6 130 Multicast Listener Report Message v2
3 0.135168 0.0.0.0 255.255.255.255 DHCP 356 DHCP Discover - Transaction ID 0x127b4953
4 0.146432 0.0.0.0 255.255.255.255 DHCP 368 DHCP Request - Transaction ID 0x127b4953
5 0.220160 108.177.98.188 192.168.1.127 TLSv1.2 97 Application Data
6 0.249868 HuaweiTechno_b8:3d:… Broadcast ARP 42 Who has 208.54.65.100? Tell 192.168.1.127
7 0.302604 HuaweiTechno_b8:3d:… Broadcast ARP 42 Who has 192.168.1.1? Tell 192.168.1.127
8 0.308224 CiscoLinksys_da:cf:… HuaweiTechno_b8:3d:… ARP 42 192.168.1.1 is at 00:16:b6:da:cf:2d
9 0.309772 192.168.1.127 192.168.1.1 DNS 89 Standard query 0x0398 A connectivitycheck.gstatic.com
10 0.312832 192.168.1.1 192.168.1.127 DNS 105 Standard query response 0x0398 A connectivitycheck.gsta
11 0.323596 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x62b3 A www.google.com
12 0.407052 216.58.193.195 192.168.1.127 TCP 66 80 → 41492 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=1
13 0.409100 192.168.1.127 216.58.193.195 HTTP 286 GET /generate_204 HTTP/1.1
14 0.414732 192.168.1.127 172.217.5.68 TLSv1.2 583 Client Hello (SNI=www.google.com)
15 0.618859 192.168.1.127 172.217.5.68 TLSv1.2 312 [TCP Previous segment not captured] , Application Data
16 0.695872 172.217.5.68 192.168.1.127 TCP 66 443 → 46535 [ACK] Seq=163 Ack=815 Win=349 Len=0 TSval=
17 0.774208 192.168.1.1 192.168.1.127 DNS 168 Standard query response 0x4cb5 A m.qpic.cn CNAME m.qpic
18 0.890443 192.168.1.127 192.168.1.1 DNS 74 Standard query 0x16da A www.taobao.com
19 0.893515 192.168.1.127 192.168.1.1 DNS 84 Standard query 0x4643 AAAA mygw.alipay.com.srip.net
20 0.913483 192.168.1.127 66.198.24.243 TCP 74 40356 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PE
21 0.948800 192.168.1.127 198.11.186.81 TCP 74 43170 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_
22 0.966731 192.168.1.127 66.198.24.243 HTTP 114 HEAD / HTTP/1.1
23 1.022539 66.198.24.243 192.168.1.127 TCP 54 80 → 40356 [ACK] Seq=1 Ack=61 Win=29 Len=0
24 1.191488 198.11.186.81 192.168.1.127 TCP 74 443 → 43170 [SYN, ACK] Seq=0 Ack=1 Win=12960 Len=0 MSS=
25 1.192523 192.168.1.127 198.11.186.81 TCP 54 43170 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
26 1.196107 192.168.1.127 198.11.186.81 SSLv3 152 Client Hello
27 1.255501 HuaweiTechno_b8:3d:… Broadcast ARP 42 Who has 208.54.65.100? Tell 192.168.1.127
28 1.323596 192.168.1.127 120.52.147.63 TCP 54 40345 → 80 [RST] Seq=1 Win=0 Len=0
29 1.400896 203.205.151.233 192.168.1.127 TCP 54 80 → 46225 [FIN, ACK] Seq=1 Ack=1 Win=62 Len=0
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: CiscoLinksys_da:cf:2d (00:16:b6:da:cf:2d), Dst:
Internet Protocol Version 4, Src: 60.205.109.26, Dst: 192.168.1.127
Transmission Control Protocol, Src Port: 8900, Dst Port: 40280, Seq
0000 00 9a cd b8 3d 23 00 16 b6 da cf 2d 08 00 45 00
0010 00 34 39 9e 40 00 2f 06 a6 17 3c cd 6d 1a c0 a8
0020 01 7f 22 c4 9d 58 52 88 56 59 6f d7 23 5c 80 11
0030 00 e2 4b 80 00 00 01 01 08 0a 23 cd ac 3c 01 b0
0040 f0 5f


Wireshark · Protocol Hierarchy Statistics · WPA2-P5-01-dec.cap
Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes
Frame | 100.0 | 1668 | 100.0 | 613627 | 140 k | 0 | 0
Ethernet | 100.0 | 1668 | 3.8 | 23352 | 5,358 | 0 | 0
Internet Protocol Version 6 | 0.2 | 4 | 0.0 | 160 | 36 | 0 | 0
Internet Control Message Protocol v6 | 0.2 | 4 | 0.0 | 188 | 43 | 4 | 188
Internet Protocol Version 4 | 99.4 | 1658 | 5.4 | 33160 | 7,609 | 0 | 0
User Datagram Protocol | 55.5 | 926 | 1.2 | 7408 | 1,700 | 0 | 0
Multicast Domain Name System | 0.1 | 2 | 0.0 | 122 | 27 | 2 | 122
Internet Security Association and Key Management Protocol | 0.1 | 1 | 0.1 | 488 | 111 | 1 | 488
GQUIC (Google Quick UDP Internet Connections) | 41.9 | 699 | 46.8 | 287090 | 65 k | 699 | 287090
Dynamic Host Configuration Protocol | 0.1 | 2 | 0.1 | 640 | 146 | 2 | 640
Domain Name System | 2.3 | 39 | 0.3 | 1803 | 413 | 39 | 1803
Data | 11.0 | 183 | 13.5 | 82617 | 18 k | 183 | 82617
Transmission Control Protocol | 43.8 | 731 | 28.7 | 175926 | 40 k | 624 | 87839
X11 | 0.1 | 1 | 0.0 | 24 | 5 | 0 | 0
Malformed Packet | 0.1 | 1 | 0.0 | 0 | 0 | 1 | 0
Transport Layer Security | 2.9 | 48 | 2.1 | 12856 | 2,950 | 48 | 12856
MSN Messenger Service | 1.9 | 31 | 7.3 | 44888 | 10 k | 31 | 44888
Hypertext Transfer Protocol | 1.5 | 25 | 4.4 | 27075 | 6,213 | 25 | 27075
Data | 0.1 | 2 | 0.0 | 132 | 30 | 2 | 132
Internet Control Message Protocol | 0.1 | 1 | 0.1 | 489 | 112 | 0 | 0
Internet Security Association and Key Management Protocol | 0.1 | 1 | 0.1 | 453 | 103 | 1 | 453
Address Resolution Protocol | 0.4 | 6 | 0.0 | 168 | 38 | 6 | 168

Filter: TCP


Kali - Internal Workstation on CY301-CLOCH001 - Virtual Machine Connection
WPA2-P5-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1 0.000000 60.205.109.26 192.168.1.127 TCP 66 8900 → 40280 [FIN, ACK] Seq=1 Ack=1 Win=226 Len=0 TSval
5 0.220160 108.177.98.188 192.168.1.127 TLSv1.2 97 Application Data
12 0.407052 216.58.193.195 192.168.1.127 TCP 66 80 → 41492 [SYN, ACK] Seq=0 Ack=1 Win=42780 Len=0 MSS=
13 0.409100 192.168.1.127 216.58.193.195 HTTP 286 GET /generate_204 HTTP/1.1
14 0.414732 192.168.1.127 172.217.5.68 TLSv1.2 583 Client Hello (SNI=www.google.com)
15 0.618059 192.168.1.127 172.217.5.68 TLSv1.2 312 [TCP Previous segment not captured] , Application Data
16 0.695872 172.217.5.68 192.168.1.127 TCP 66 443 → 46535 [ACK] Seq=163 Ack=815 Win=349 Len=0 TSval=
20 0.913483 192.168.1.127 66.198.24.243 TCP 74 40356 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PE
21 0.948800 192.168.1.127 198.11.186.81 TCP 74 43170 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_
22 0.966731 192.168.1.127 66.198.24.243 HTTP 114 HEAD / HTTP/1.1
23 1.022539 66.198.24.243 192.168.1.127 TCP 54 80 → 40356 [ACK] Seq=1 Ack=61 Win=29 Len=0
24 1.191488 198.11.186.81 192.168.1.127 TCP 74 443 → 43170 [SYN, ACK] Seq=0 Ack=1 Win=12960 Len=0 MSS=
25 1.192523 192.168.1.127 198.11.186.81 TCP 54 43170 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
26 1.196107 192.168.1.127 198.11.186.81 SSLv3 152 Client Hello
28 1.323596 192.168.1.127 120.52.147.63 TCP 54 48345 → 80 [RST] Seq=1 Win=0 Len=0
29 1.400896 203.205.151.233 192.168.1.127 TCP 54 80 → 46225 [FIN, ACK] Seq=1 Ack=1 Win=62 Len=0
30 1.401420 192.168.1.127 203.205.151.233 TCP 54 46225 → 80 [RST] Seq=1 Win=0 Len=0
31 1.491008 198.11.186.81 192.168.1.127 SSLv3 1389 [TCP Previous segment not captured] , Continuation Data
32 1.491019 192.168.1.127 198.11.186.81 TCP 54 [TCP ACKed unseen segment] 43170 → 443 [ACK] Seq=99 Ack
33 1.491531 192.168.1.127 198.11.186.81 TCP 54 [TCP ACKed unseen segment] 43170 → 443 [ACK] Seq=99 Ack
34 1.491531 192.168.1.127 198.11.186.81 TCP 54 43170 → 443 [ACK] Seq=99 Ack=4240 Win=65535 Len=0
35 1.526411 192.168.1.127 198.11.186.81 SSLv3 394 Client Key Exchange, Change Cipher Spec, Encrypted Hand
37 1.535115 192.168.1.127 183.131.1.96 TCP 74 39931 → 5226 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_
40 1.798785 183.131.1.96 192.168.1.127 TCP 74 5226 → 39931 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS
41 1.799821 192.168.1.127 183.131.1.96 TCP 66 39931 → 5226 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=2
42 1.801857 198.11.186.81 192.168.1.127 SSLv3 129 Change Cipher Spec, Encrypted Handshake Message
43 1.804941 192.168.1.127 183.131.1.96 TCP 161 39931 → 5226 [PSH, ACK] Seq=1 Ack=1 Win=87808 Len=95 T
44 1.826444 192.168.1.127 198.11.186.81 SSLv3 128 Application Data, Application Data
45 1.831052 192.168.1.127 198.11.186.81 SSLv3 128 Application Data, Application Data
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: CiscoLinksys_da:cf:2d (00:16:b6:da:cf:2d), Dst:
Internet Protocol Version 4, Src: 60.205.109.26, Dst: 192.168.1.12
Transmission Control Protocol, Src Port: 8900, Dst Port: 40280, Se
0000 00 9a cd b8 3d 23 00 16 b6 da cf 2d 08 00 45 00
0010 00 34 39 9e 40 00 2f 06 a6 17 3c cd 6d 1a c0 a8
0020 01 7f 22 c4 9d 58 52 88 56 59 6f d7 23 5c 80 11
0030 00 e2 4b 80 00 00 01 01 08 0a 23 cd ac 3c 01 b0
0040 f0 5f


Wireshark · Protocol Hierarchy Statistics · WPA2-P5-01-dec.cap
Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s | PDUs
Frame | 100.0 | 731 | 100.0 | 200780 | 46 k | 0 | 0 | 0 | 731
Ethernet | 100.0 | 731 | 5.1 | 10234 | 2,348 | 0 | 0 | 0 | 731
Internet Protocol Version 4 | 100.0 | 731 | 7.3 | 14620 | 3,355 | 0 | 0 | 0 | 731
Transmission Control Protocol | 100.0 | 731 | 87.6 | 175926 | 40 k | 624 | 87839 | 20 k | 731
X11 | 0.1 | 1 | 0.0 | 24 | 5 | 0 | 0 | 0 | 1
Malformed Packet | 0.1 | 1 | 0.0 | 0 | 0 | 1 | 0 | 0 | 1
Transport Layer Security | 6.6 | 48 | 6.4 | 12856 | 2,950 | 48 | 12856 | 2,950 | 48
MSN Messenger Service | 4.2 | 31 | 22.4 | 44888 | 10 k | 31 | 44888 | 10 k | 31
Hypertext Transfer Protocol | 3.4 | 25 | 13.5 | 27075 | 6,213 | 25 | 27075 | 6,213 | 25
Data | 0.3 | 2 | 0.1 | 132 | 30 | 2 | 132 | 30 | 2

Task D — WPA2-P5-01-dec.cap Traffic Analysis

After performing a dictionary attack on WPA2-P5-01.cap using rockyou.txt, the WPA2 password for the **CyberPHY** network was successfully cracked as **"messenger"**. Using airdecap-ng, 1,668 of 1,793 WPA data packets were decrypted. Traffic analysis in Wireshark revealed that the client device at **192.168.1.127** was connected through a CiscoLinksys access point (00:16:b6:da:cf:2d). The dominant protocol was **GQUIC** (Google Quick UDP Internet Connections) at 41.9% of packets, indicating heavy Google service usage. **DNS queries** revealed the user was visiting sites including google.com, taobao.com, and alipay.com, suggesting possible international browsing activity. Notably, **MSN Messenger Service** traffic (31 packets, 7.3% of bytes) was detected, revealing the use of an instant messaging application. **TLS/SSL** traffic (48 packets) confirmed that some communications were encrypted at the application layer. **HTTP** traffic (25 packets) was also present in plaintext. This capture demonstrates that even with WPA2 encryption, a weak dictionary-based password like "messenger" leaves the entire network vulnerable to traffic decryption and analysis.