CYSE 301: Cybersecurity Technique and Operations
Assignment 5: Password Cracking (Part A)
By: Paul Cumiskey

- Task A
  - 1.
```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# groupadd cyse301

┌──(root㉿kali)-[~]
└─# groupadd pcumi001
```
```
cyse301:x:1002:
pcumi001:x:1003:
```
  - 2.
```
┌──(root㉿kali)-[~]
└─# useradd A1 -g cyse301

┌──(root㉿kali)-[~]
└─# useradd A2 -g cyse301

┌──(root㉿kali)-[~]
└─# useradd A3 -g cyse301

┌──(root㉿kali)-[~]
└─# useradd B1 -g pcumi001

┌──(root㉿kali)-[~]
└─# useradd B2 -g pcumi001

┌──(root㉿kali)-[~]
└─# useradd B3 -g pcumi001
```
```
┌──(root㉿kali)-[~]
└─# tail -n 6 /etc/passwd
A1:x:1002:1002::/home/A1:/bin/sh
A2:x:1003:1002::/home/A2:/bin/sh
A3:x:1004:1002::/home/A3:/bin/sh
B1:x:1005:1003::/home/B1:/bin/sh
B2:x:1006:1003::/home/B2:/bin/sh
B3:x:1007:1003::/home/B3:/bin/sh
```

- 3. The Passwords: A1: 123 A2: dog123 A3: Dog!123

```
┌──(root㉿kali)-[~]
└─# passwd A1
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# passwd A2
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# passwd A3
New password:
Retype new password:
passwd: password updated successfully
```

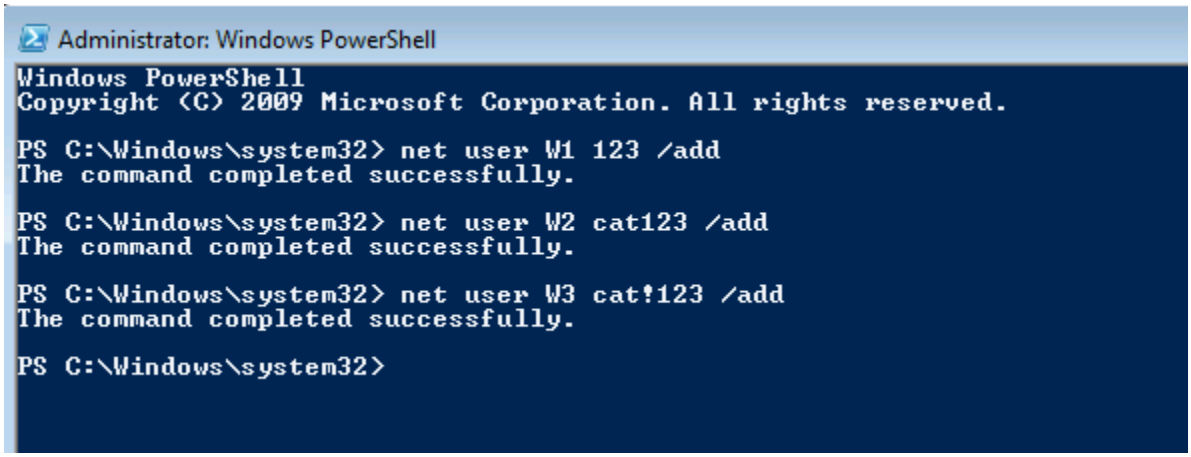
- 4.

```
┌──(root㉿kali)-[~]
└─# tail -n 6 /etc/shadow > passwdhash.txt
```

```
┌──(root㉿kali)-[~]
└─# john passwdhash.txt --wordlist=rockyou.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
```

I don't understand what the issue is. I tried to reinstall john the ripper, but it still didn't work.

- Task B



- 1.

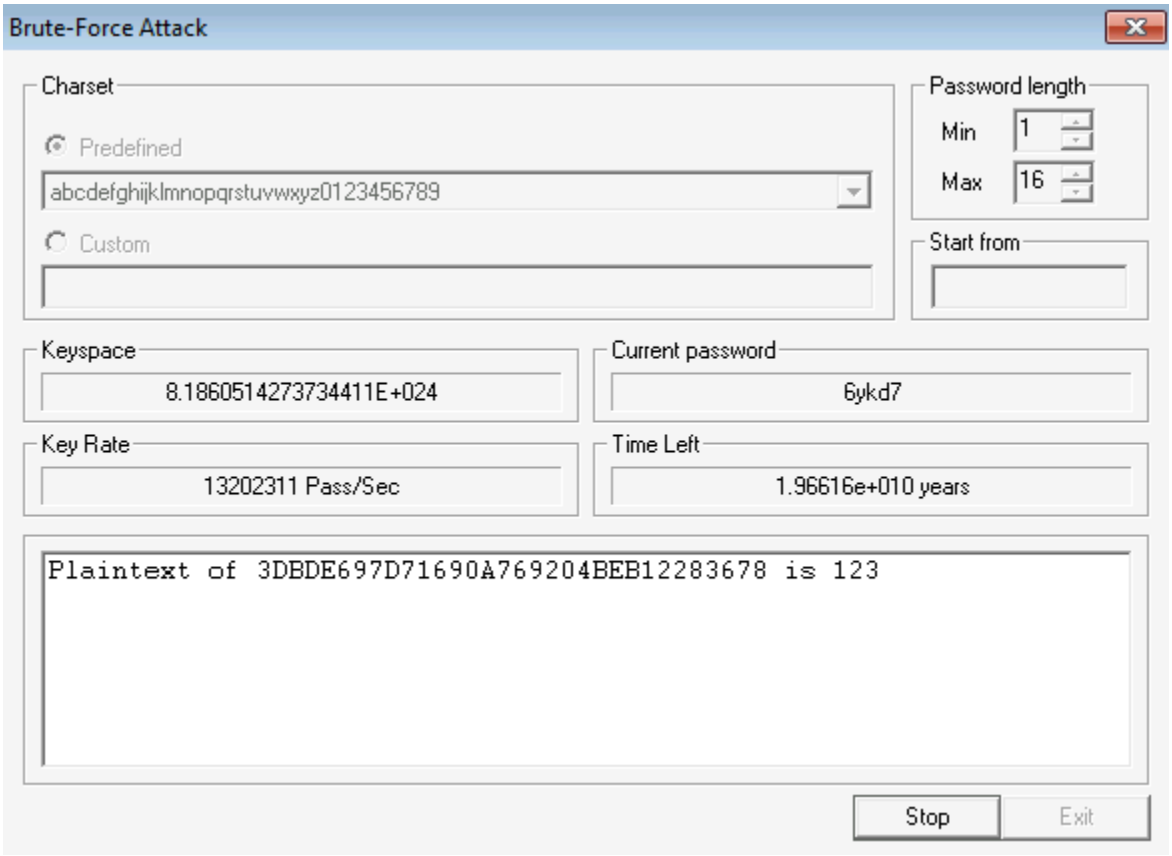
```
meterpreter > hashdumb
[-] Unknown command: hashdumb
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
pcumi001:1003:aad3b435b51404eeaad3b435b51404ee:7ccc15df1c176e21aa1431701427741f:::
W1:1004:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
W2:1005:aad3b435b51404eeaad3b435b51404ee:354ff30f08e98e711800753ee8ccd1a5:::
W3:1006:aad3b435b51404eeaad3b435b51404ee:9b291ca07a50984dbaaa9627e346f7b3:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter >
```

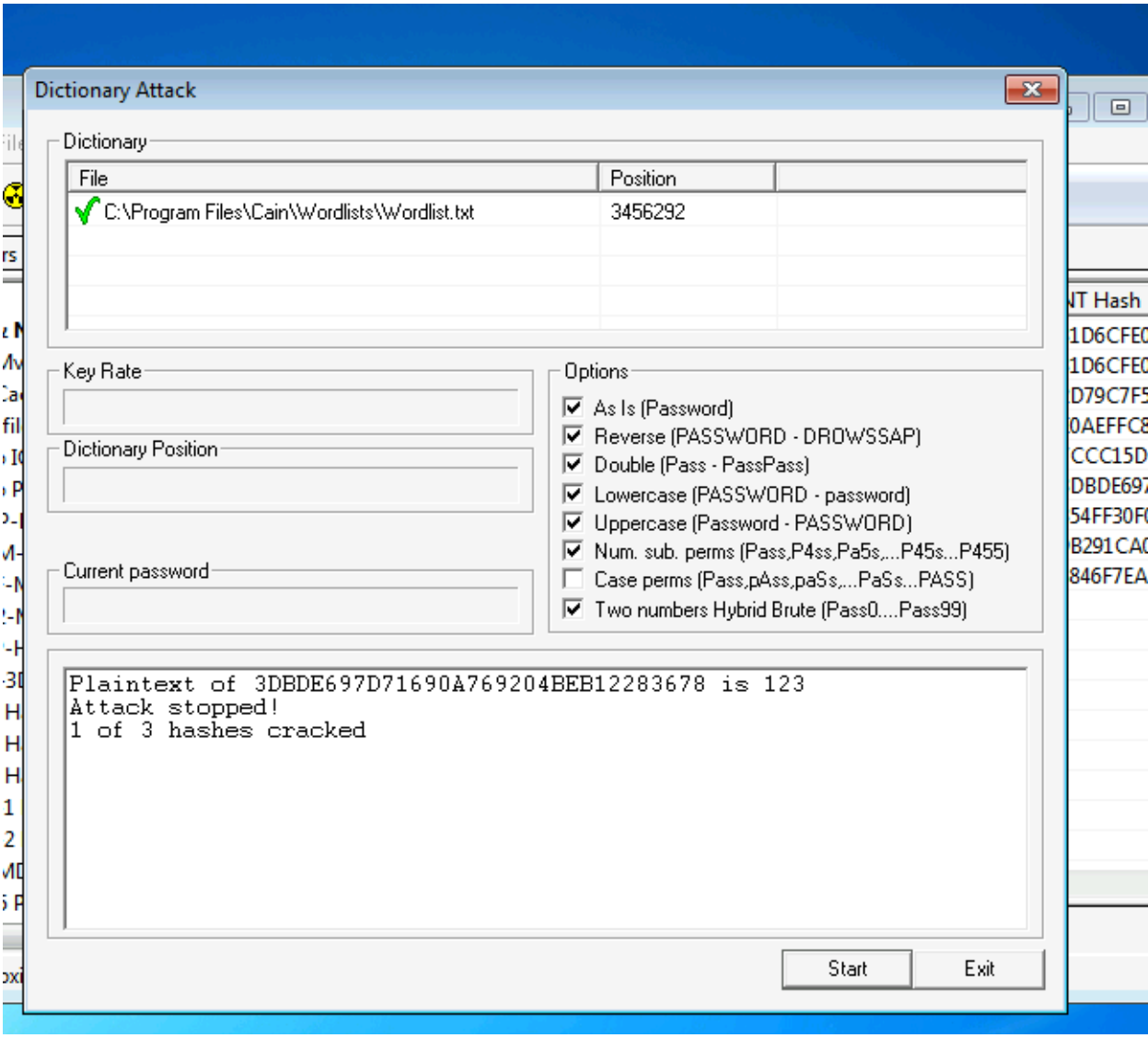
- 2.

```
┌──(root㉿kali)-[~]
└─# john lab4hashes.txt -show --format=NT
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
W1:123:1004:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
W2:cat123:1005:aad3b435b51404eeaad3b435b51404ee:354ff30f08e98e711800753ee8ccd1a5:
Window 7:password:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830

5 password hashes cracked, 3 left

┌──(root㉿kali)-[~]
└─# This is Pcumi001 / Paul Cumiskey
```

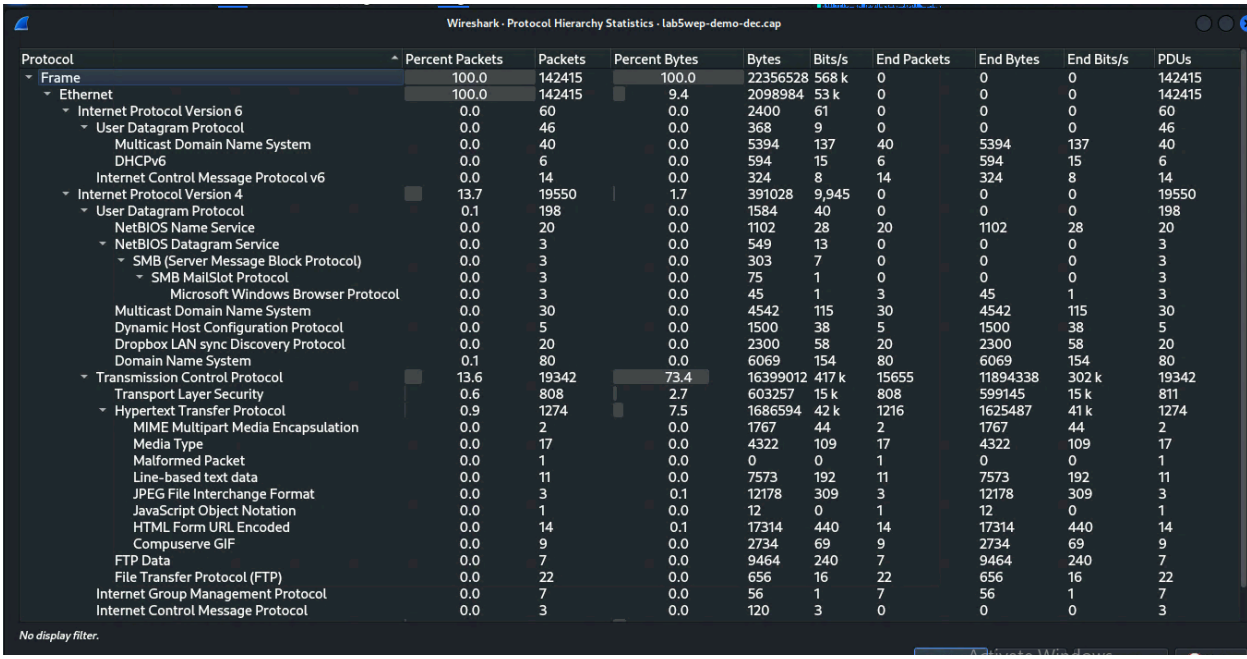
Sorry, I was following the lab guide and misnamed the file

- 3.


Brute-Force Attack
Charset
Predefined
abcdefghijklmnopqrstuvwxyz0123456789
Custom
Password length
Min
1
Max
16
Start from
Keyspace
8.1860514273734411E+024
Current password
6ykd7
Key Rate
13202311 Pass/Sec
Time Left
1.96616e+010 years
Plaintext of 3DBDE697D71690A769204BEB12283678 is 123
Stop
Exit

- 
Dictionary Attack
Dictionary
File
Position
C:\Program Files\Cain\Wordlists\Wordlist.txt
3456292
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
Plaintext of 3DBDE697D71690A769204BEB12283678 is 123
Attack stopped!
1 of 3 hashes cracked
Start
Exit
- Task C

- 1.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	142415	100.0	22356528	568 k	0	0	0	142415
Ethernet	100.0	142415	9.4	2098984	53 k	0	0	0	142415
Internet Protocol Version 6	0.0	60	0.0	2400	61	0	0	0	60
User Datagram Protocol	0.0	46	0.0	368	9	0	0	0	46
Multicast Domain Name System	0.0	40	0.0	5394	137	40	5394	137	40
DHCPv6	0.0	6	0.0	594	15	6	594	15	6
Internet Control Message Protocol v6	0.0	14	0.0	324	8	14	324	8	14
Internet Protocol Version 4	13.7	19550	1.7	391028	9,945	0	0	0	19550
User Datagram Protocol	0.1	198	0.0	1584	40	0	0	0	198
NetBIOS Name Service	0.0	20	0.0	1102	28	20	1102	28	20
NetBIOS Datagram Service	0.0	3	0.0	549	13	0	0	0	3
SMB (Server Message Block Protocol)	0.0	3	0.0	303	7	0	0	0	3
SMB MailSlot Protocol	0.0	3	0.0	75	1	0	0	0	3
Microsoft Windows Browser Protocol	0.0	3	0.0	45	1	3	45	1	3
Multicast Domain Name System	0.0	30	0.0	4542	115	30	4542	115	30
Dynamic Host Configuration Protocol	0.0	5	0.0	1500	38	5	1500	38	5
Dropbox LAN sync Discovery Protocol	0.0	20	0.0	2300	58	20	2300	58	20
Domain Name System	0.1	80	0.0	6069	154	80	6069	154	80
Transmission Control Protocol	13.6	19342	73.4	16399012	417 k	15655	11894338	302 k	19342
Transport Layer Security	0.6	808	2.7	603257	15 k	808	599145	15 k	811
Hypertext Transfer Protocol	0.9	1274	7.5	1686594	42 k	1216	1625487	41 k	1274
MIME Multipart Media Encapsulation	0.0	2	0.0	1767	44	2	1767	44	2
Media Type	0.0	17	0.0	4322	109	17	4322	109	17
Malformed Packet	0.0	1	0.0	0	0	1	0	0	1
Line-based text data	0.0	11	0.0	7573	192	11	7573	192	11
JPEG File Interchange Format	0.0	3	0.1	12178	309	3	12178	309	3
JavaScript Object Notation	0.0	1	0.0	12	0	1	12	0	1
HTML Form URL Encoded	0.0	14	0.1	17314	440	14	17314	440	14
Compuserve GIF	0.0	9	0.0	2734	69	9	2734	69	9
FTP Data	0.0	7	0.0	9464	240	7	9464	240	7
File Transfer Protocol (FTP)	0.0	22	0.0	656	16	22	656	16	22
Internet Group Management Protocol	0.0	7	0.0	56	1	7	56	1	7
Internet Control Message Protocol	0.0	3	0.0	120	3	0	0	0	3

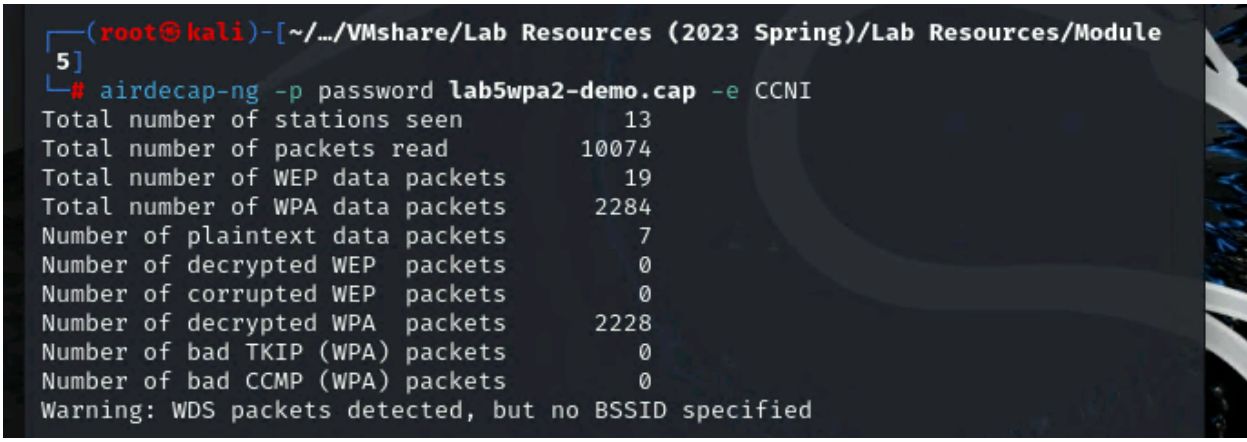
This Wireshark Protocol Hierarchy Statistics view shows that nearly all captured traffic travels over Ethernet, with IPv4 and TCP making up the majority of meaningful payload. TCP dominates the byte count (over 70%), indicating most data transfer occurs through reliable, connection-oriented sessions—likely web traffic, given the large share of HTTP/HTTPS (TLS + HTTP). UDP traffic is present but minimal, consisting mainly of service discovery and NetBIOS packets. Overall, the capture reflects a typical network session with heavy TCP

application activity and light background broadcast/multicast noise.

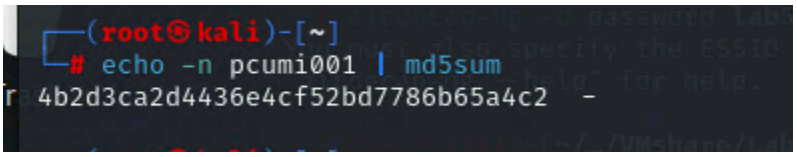
```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module
5]
└─# airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen            37
Total number of packets read        404693
Total number of WEP data packets    142415
Total number of WPA data packets     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

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module
5]
└─# ls
lab5wep-demo.cap      lab5wpa2-demo.cap  WPA2-P2-01.cap  WPA2-P4-01.cap
lab5wep-demo-dec.cap  WPA2-P1-01.cap     WPA2-P3-01.cap  WPA2-P5-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module
5]
└─#
```

- 2.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	2228	100.0	460293	142 k	0	0	0	2228
Ethernet	100.0	2228	6.8	31192	9,674	0	0	0	2228
Internet Protocol Version 6	0.1	3	0.0	120	37	0	0	0	3
User Datagram Protocol	0.0	1	0.0	8	2	0	0	0	1
Multicast Domain Name System	0.0	1	0.1	278	86	1	278	86	1
Internet Control Message Protocol v6	0.1	2	0.0	40	12	2	40	12	2
Internet Protocol Version 4	99.7	2221	9.7	44420	13 k	0	0	0	2221
User Datagram Protocol	1.5	33	0.1	264	81	0	0	0	33
Network Time Protocol	0.0	1	0.0	48	14	1	48	14	1
Multicast Domain Name System	0.0	1	0.0	114	35	1	114	35	1
GQUIC (Google Quick UDP Internet Connections)	0.1	2	0.3	1387	430	2	1387	430	2
Domain Name System	1.0	22	0.2	939	291	22	939	291	22
Data	0.3	7	0.3	1374	426	7	1374	426	7
Transmission Control Protocol	98.2	2188	82.6	379997	117 k	1998	300797	93 k	2188
Transport Layer Security	5.7	127	8.5	39288	12 k	127	39288	12 k	127
Hypertext Transfer Protocol	2.8	62	14.2	65357	20 k	61	64032	19 k	62
Portable Network Graphics	0.0	1	0.2	1060	328	1	1060	328	1
Data	0.0	1	0.1	343	106	1	343	106	1
Address Resolution Protocol	0.2	4	0.0	112	34	4	112	34	4

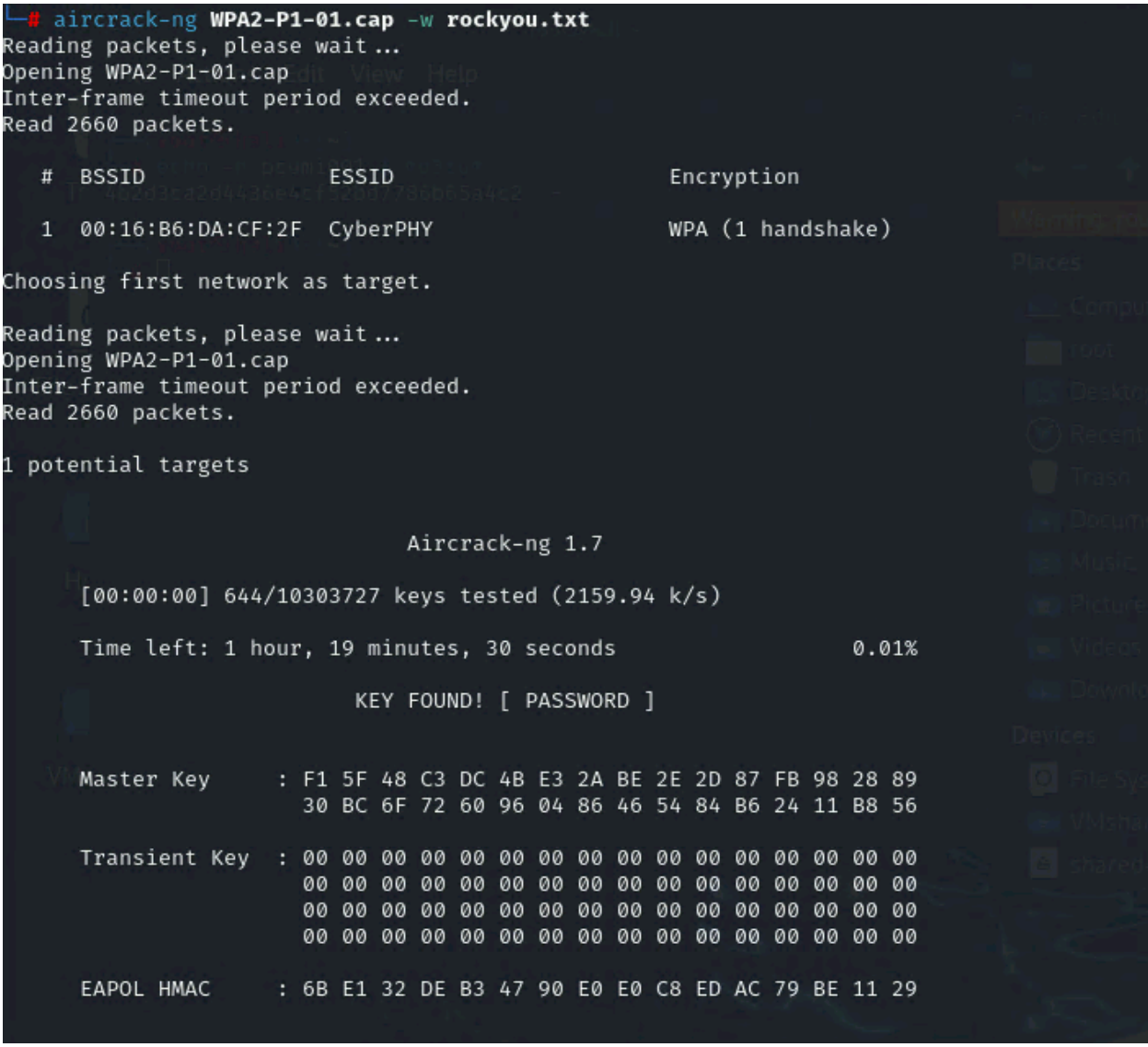


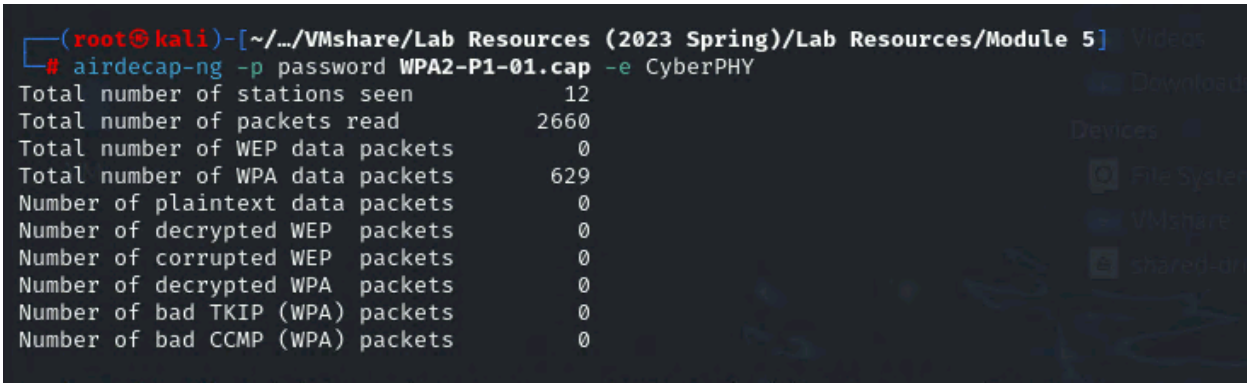
This capture is dominated by IPv4 traffic carried over TCP, which accounts for more than 80% of all bytes—suggesting a primary application flow such as web browsing or API communication. TLS traffic represents a significant portion of that, indicating encrypted HTTPS connections. There is a small amount of UDP activity, including DNS, NTP, and a bit of GQUIC, but these together make up only a tiny fraction of total traffic. Overall, the trace reflects a mostly encrypted TCP-based session with normal background service traffic.

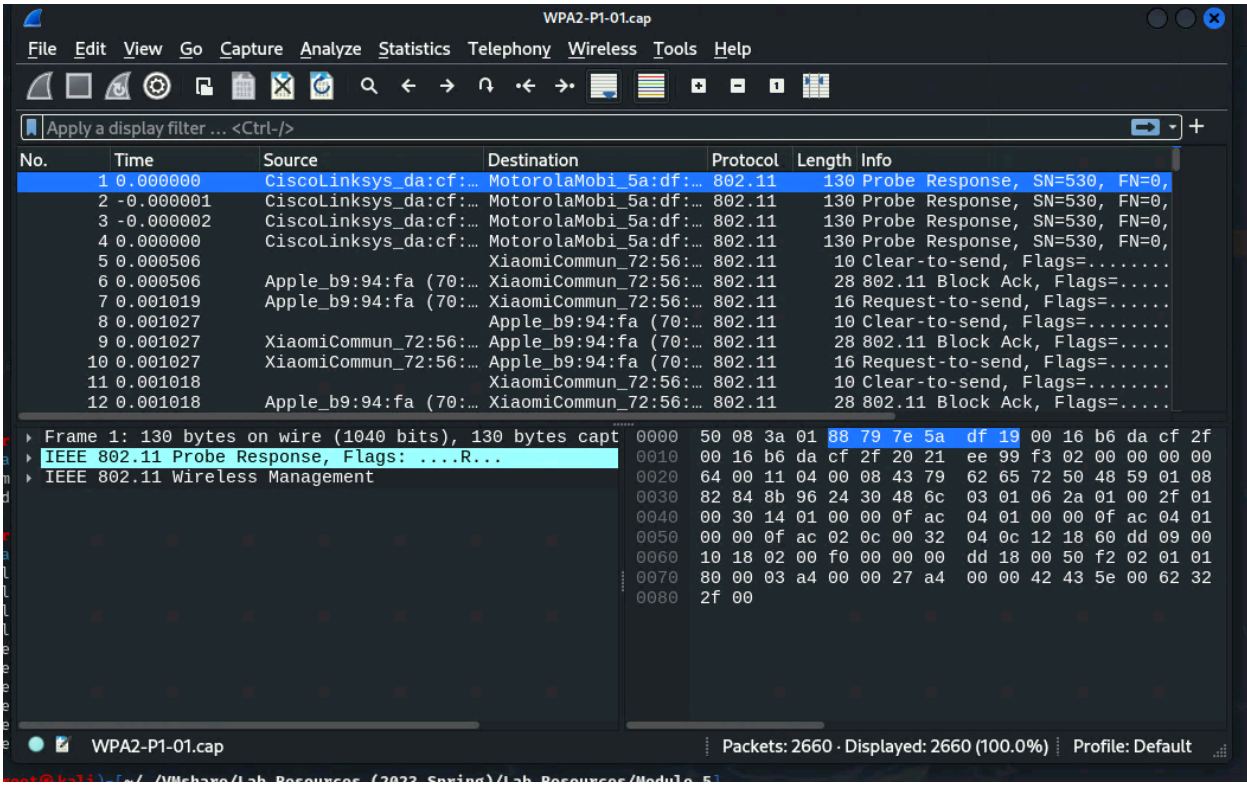
- Task D
  - 

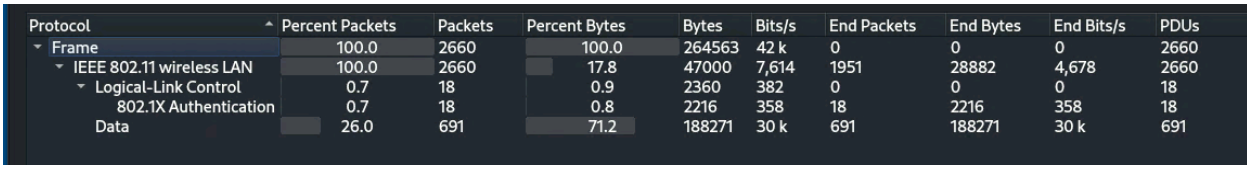
So I will be doing WPA2-P1-01.cap

- After doing the initial aircrack command for a dictionary attack, I got





- 

- 

- This trace shows pure Wi-Fi–layer activity, with all traffic occurring at the IEEE 802.11 MAC level rather than higher-layer protocols. A large share of packets are management or control frames, including 802.1X authentication, which suggests the device was joining or negotiating access to a secured wireless network. The bulk of the bytes (over 70%) come from 802.11 data frames, indicating some actual user data passing once authentication succeeded. Overall, this capture represents a Wi-Fi association and authentication sequence followed by light data transfer.