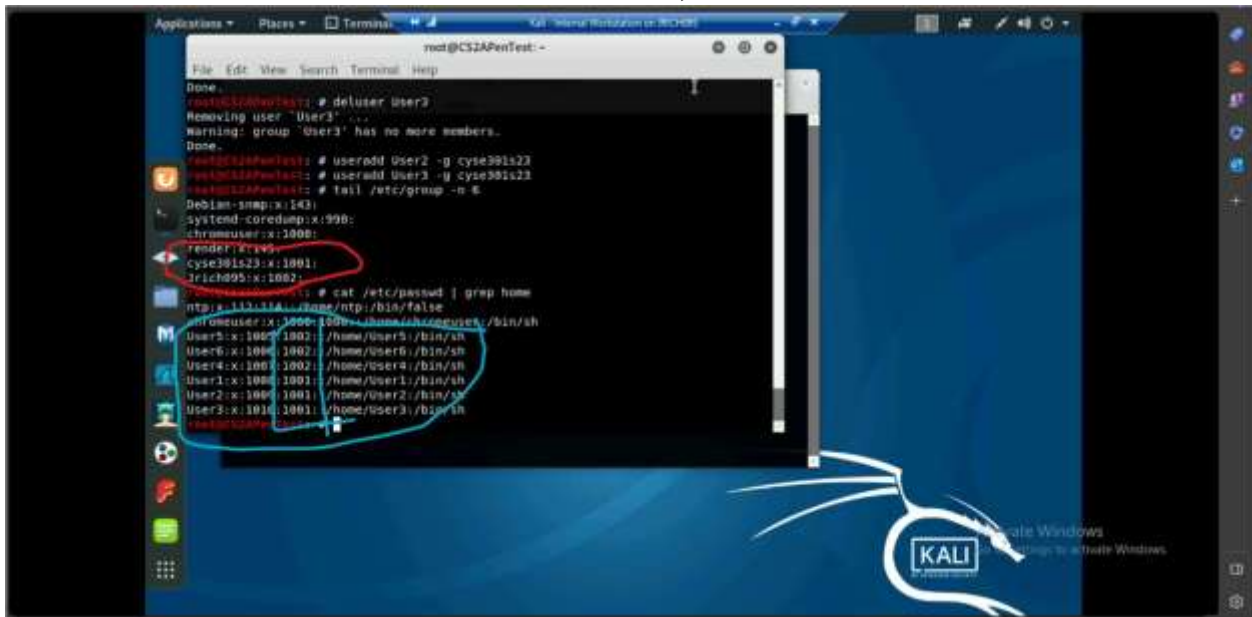


Old Dominion University  
CYSE 301 Cybersecurity Techniques and Operations  
Assignment #5 Password Cracking

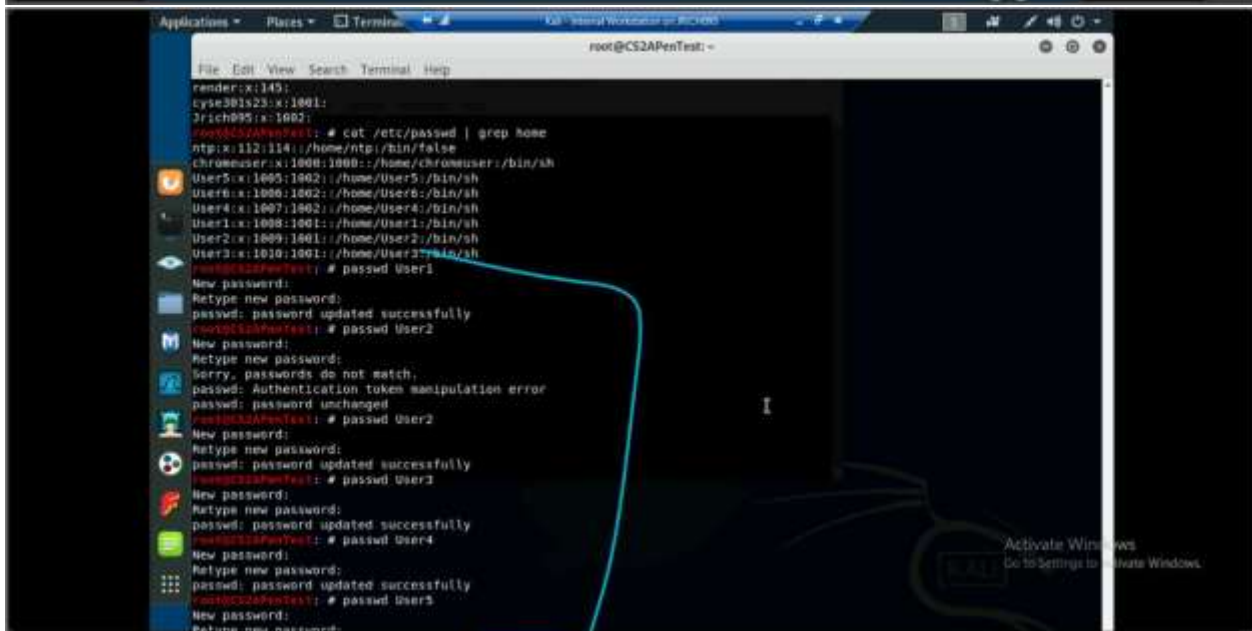
Jadyn Richardson  
01221594

Password Cracking

## Task A.)



```
root@CS2APenTest:~# deluser User3
Done.
root@CS2APenTest:~# useradd User2 -g cyse301s23
Done.
root@CS2APenTest:~# useradd User1 -g cyse301s23
Done.
root@CS2APenTest:~# tail /etc/group -n 6
Debian-snap:x:143:
systemd-coredump:x:990:
chromouser:x:1000:
render:x:149:
cyse301s23:x:1001:
Trich095:x:1002:
root@CS2APenTest:~# cat /etc/passwd | grep home
ntp:x:112:114:/:home/ntp:/bin/false
User5:x:1005:1002:/:home/User5:/bin/sh
User6:x:1006:1002:/:home/User6:/bin/sh
User4:x:1007:1002:/:home/User4:/bin/sh
User1:x:1008:1001:/:home/User1:/bin/sh
User2:x:1009:1001:/:home/User2:/bin/sh
User3:x:1010:1001:/:home/User3:/bin/sh
```



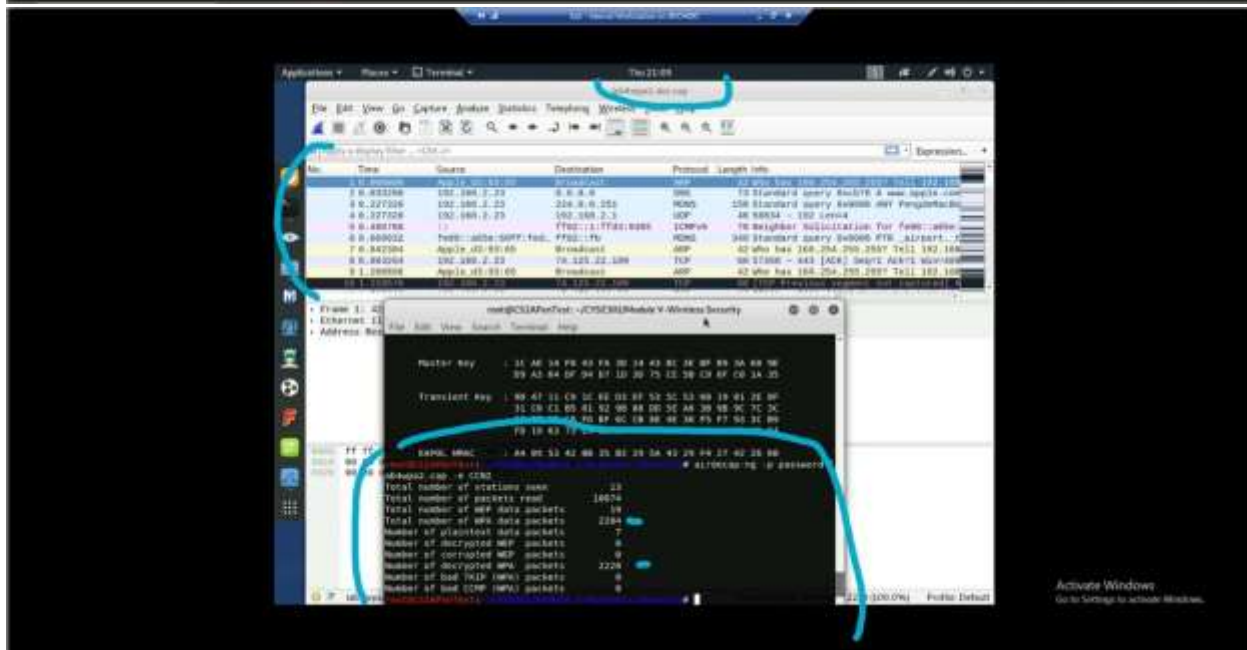
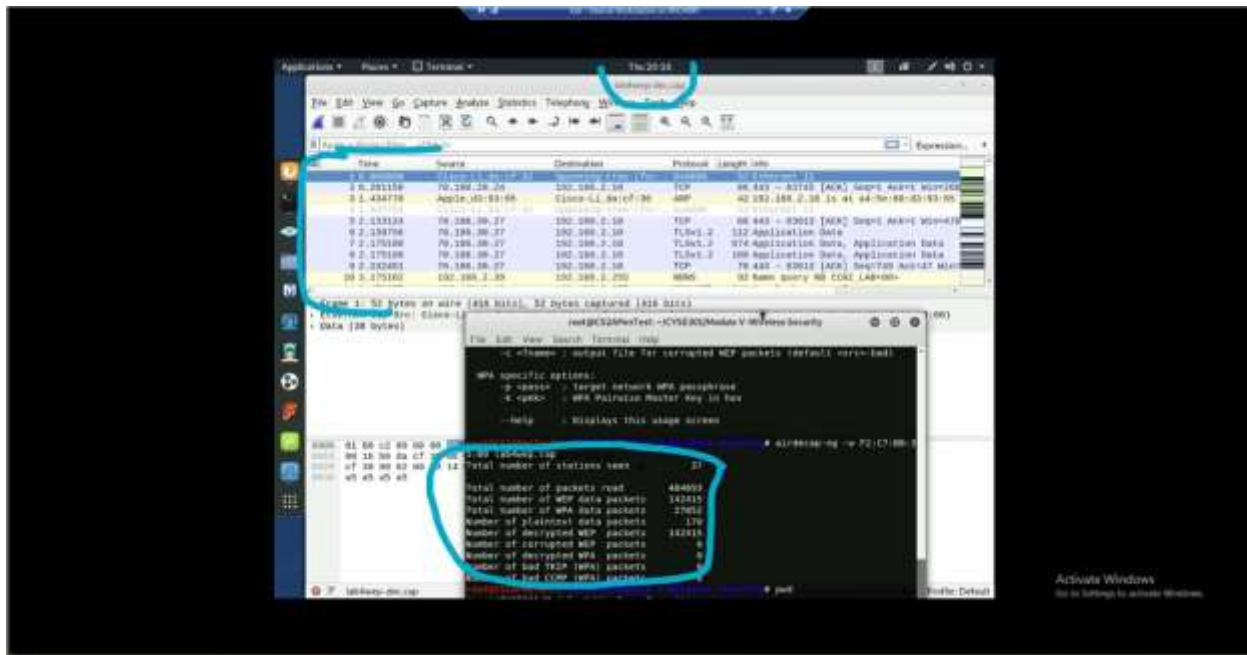
```
root@CS2APenTest:~# cat /etc/passwd | grep home
ntp:x:112:114:/:home/ntp:/bin/false
chromouser:x:1000:1000:/:home/chromouser:/bin/sh
User5:x:1005:1002:/:home/User5:/bin/sh
User6:x:1006:1002:/:home/User6:/bin/sh
User4:x:1007:1002:/:home/User4:/bin/sh
User1:x:1008:1001:/:home/User1:/bin/sh
User2:x:1009:1001:/:home/User2:/bin/sh
User3:x:1010:1001:/:home/User3:/bin/sh
root@CS2APenTest:~# passwd User1
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd User2
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
root@CS2APenTest:~# passwd User2
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd User3
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd User4
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd User5
New password:
Retype new password:
```

Selected Passwords: password, P@55w0rd, GreenGiant89, ascendant, \*e&r9D-yK, S@nt@C1@5









The above two screenshots show the process of decrypting the capture file.

## WireShark Analysis



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Sh/s	Dis Packets	Et
Frame	100.0	142415	100.0	22754518	366.6	0	0
Ethernet II	100.0	142415	8.9	13934215	50.6	0	0
User Datagram Protocol	0.0	40	0.0	2406	43	0	0
Multicast Domain Name System	0.0	40	0.0	3264	137	40	33
DHCPv6	0.0	4	0.0	304	15	6	33
Internet Control Message Protocol v6	0.0	14	0.0	124	8	14	33
Internet Protocol Version 4	13.7	28750	1.7	301528	3.945	0	0
User Datagram Protocol	8.1	196	0.9	1084	40	0	0
NetBIOS Name Service	0.0	20	0.0	1102	26	20	33
NetBIOS Datagram Service	0.0	7	0.0	348	13	7	0
SMB (Server Message Block Protocol)	0.0	3	0.0	303	7	0	0
SMB Mailslot Protocol	0.0	3	0.0	76	1	0	0
Microsoft Windows Browser Protocol	0.0	3	0.0	45	1	0	46
Microsoft Disk Operating System	0.0	30	0.0	4042	115	30	46
Ethernet LAN specific Discovery Protocol	0.0	20	0.0	2302	56	20	33
Domain Name System	0.1	30	0.0	6006	154	60	60
Bootstrap Protocol	0.0	3	0.0	2300	26	1	29
Transmission Control Protocol	13.6	12342	73.6	1129912	4174	12644	111
Secure Sockets Layer	0.8	708	2.7	509250	13.6	705	58
Multicast Packet	0.0	12	0.0	9	0	12	9
Hypertext Transfer Protocol	0.9	1296	7.7	175230	43.6	1296	36
Microsoft Message Encryption	0.0	2	0.0	1767	44	2	30
Media Type	0.0	18	0.0	4038	115	18	43
Lower-level text data	0.0	11	0.0	7876	193	11	71
JPEG File Interchange Format	0.0	3	0.1	1278	309	3	15
Application Object Extension	0.0	1	0.0	62	1	1	0
HTML, ETags, Encoded	0.0	14	0.1	17314	449	14	23
Compressed GIF	0.0	9	0.2	2736	69	9	27
FTP Data	0.0	7	0.0	3454	246	7	0
File Transfer Protocol (FTP)	0.0	22	0.0	656	14	22	1
Internet Group Management Protocol	0.0	7	0.0	36	1	7	36
Internet Control Message Protocol	0.0	3	0.0	120	3	3	11
Data	1.2	2726	9.7	2375200	55.4	1730	21
Address Resolution Protocol	0.2	12289	25.4	3420348	874	12289	34

No.	Time	Source	Destination	Protocol	Length	Info
1428	0.1114100	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1114876	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1115036	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1115174	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1115385	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1117996	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1118620	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1119496	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1120372	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1121248	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1122124	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1122999	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1123875	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1124751	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1125627	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1126503	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1127379	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1128255	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1129131	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1130007	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1130883	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1131759	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1132635	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1133511	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1134387	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1135263	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1136139	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1137015	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1137891	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1138767	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1139643	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1140519	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1141395	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1142271	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1143147	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1144023	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1144899	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1145775	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1146651	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1147527	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1148403	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1149279	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1150155	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1151031	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1151907	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1152783	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1153659	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1154535	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1155411	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1156287	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1157163	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1158039	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1158915	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1159791	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1160667	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1161543	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1162419	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1163295	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1164171	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1165047	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1165923	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1166799	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1167675	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1168551	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1169427	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1170303	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1171179	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1172055	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1172931	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1173807	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1174683	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1175559	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1176435	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1177311	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1178187	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1179063	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1179939	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1180815	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1181691	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1182567	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1183443	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1184319	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1185195	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1186071	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1186947	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1187823	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1188699	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1189575	A1FA, 82:c9:7b	Broadcast	ARP	42	Who has 192.168.2.17? Tell 192.168.2.4
1429	0.1190451	A1FA, 82:c9:7b	Broadcast			



The screenshot shows a Wireshark interface with a packet list table. A red circle highlights a packet with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
134	0.117448	PeerghatBook-Fro.L	plsa.google.com	TLSv1.2	118	Application Data

Below the packet list, the packet details pane shows:

- Frame 130: 118 bytes on wire (956 bits), 118 bytes captured (956 bits) on interface 0
- Ethernet II, Src: PeerghatBook-Fro-Lanal (aa:bb:cc:dd:ee:ff), Dst: Egress-L1-To-0/0/0 (00:00:00:00:00:00)
- Transmission Control Protocol, Src Port: 57292, Dst Port: 443, Seq: 167, Len: 58
- Destination Port: 443
- Internet Protocol Version 4 (ip), 20 bytes

Activate Windows  
Go to Settings to activate Windows.

The screenshot shows the 'Protocol Hierarchy Statistics' window in Wireshark. The tree view displays the following data:

Protocol	Received Packets	Packets	Received Bytes	Bytes
Frame	200.0	2228	200.0	4602
Ethernet	200.0	2228	8.8	1125
Internet Protocol Version 6	0.1	2	0.0	128
User Datagram Protocol	0.0	1	0.0	8
Multicast Domain Name System	0.0	1	0.1	276
Internet Control Message Protocol v6	0.1	2	0.0	80
User Datagram Protocol	0.1	222	0.0	2142
Network Time Protocol	0.0	1	0.0	48
Multicast Domain Name System	0.0	1	0.0	128
IGMP (Google Stack LDP Internet Connectivity)	0.1	2	0.3	168
Domain Name System	1.0	22	0.2	939
Data	0.3	7	0.3	1374
Transmission Control Protocol	98.2	2186	82.6	3790
Secure Sockets Layer	1.7	22	8.5	3228
Hypertext Transfer Protocol	2.8	63	14.5	6652
Portable Network Graphics	0.0	1	0.2	1066
Data	0.0	1	0.1	343
Address Resolution Protocol	0.2	4	0.0	102

Activate Windows  
Go to Settings to activate Windows.

Wireshark - Resolved Addresses (pcap/CVE2021)Module V-Wireless Security/labexp2-decap.pcap

Resolved addresses found in /root/.Wireshark/Module V-Wireless Security/labexp2-decap.pcap

Comments

No entries.

Hosts

38 entries.

70.186.28.21	glsn.google.com
70.186.28.21	glsn.google.com
70.186.28.21	glsn.google.com
70.186.28.21	glsn.google.com
70.186.28.21	glsn.google.com
70.186.28.21	glsn.google.com
70.186.28.21	glsn.google.com
101.190.2.25	PeugeotMacbook-Pro.local
70.186.28.24	glsn.google.com
70.186.28.24	glsn.google.com
Fe80::c6da:5eff::Fe80::c6da	PeugeotMacbook-Pro.local

Services

6873 entries.

www-change	2718/tcp
www-change	2718/tcp
ftp	4444/tcp
ftp	4444/tcp
de-avastinternet	1025/tcp
de-avastinternet	1025/tcp
er-latawpsa	3000/tcp
er-latawpsa	3000/tcp
radius-rtty	8000/tcp
radius-rtty	8000/tcp
stunnel	3975/tcp
stunnel	3975/tcp
de-server	1250/tcp
de-server	1250/tcp
argus-1w	2052/tcp
argus-1w	2052/tcp
gmsn-lan	9840/tcp

Activate Windows  
Go to Settings to activate Windows.

Wireshark - Display Filter: labexp2-decap.pcap

Address	Pkts	Bytes	To Pkts	To Bytes	From Pkts	From Bytes	Country	City	AS Number	AS Organization
70.186.30.21	204	254	0	6,434	190	384	---	---	---	---
70.186.30.23	11	1,855	1	444	10	1,189	---	---	---	---
70.186.30.23	300	1016	1	1,574	205	8,824	---	---	---	---
70.186.30.24	1	90	0	0	1	84	---	---	---	---
70.186.30.25	351	144	3	1,099	348	131	---	---	---	---
70.186.30.26	120	564	4	1,915	126	545	---	---	---	---
70.186.30.40	11	1,200	1	1,464	11	716	---	---	---	---
70.186.30.38	20	2,090	0	0	20	1,961	---	---	---	---
74.125.23.99	1	132	0	0	1	132	---	---	---	---
74.125.23.95	13	1,320	0	0	13	1,320	---	---	---	---
74.125.23.132	1	1,475	0	0	1	1,475	---	---	---	---
74.125.23.107	8	1,848	0	1,744	1	104	---	---	---	---
74.125.236.84	9	5,319	0	0	9	5,319	---	---	---	---
104.12.19.195	9	666	0	0	9	666	---	---	---	---
104.80.70.117	51	5,310	0	4,542	51	4,771	---	---	---	---
173.204.122.54	5	570	0	0	5	570	---	---	---	---
173.204.122.54	1	570	0	0	1	570	---	---	---	---
173.204.122.54	1	570	0	0	1	570	---	---	---	---
173.204.122.54	1	570	0	0	1	570	---	---	---	---
173.204.122.54	1	570	0	0	1	570	---	---	---	---
192.168.2.23	2,211	4584	2,030	2054	390	2264	---	---	---	---
192.168.2.23	1	4584	0	0	1	2,424	---	---	---	---
192.168.2.23	1	170	0	0	1	170	---	---	---	---

Display Filter: Limit to display filter

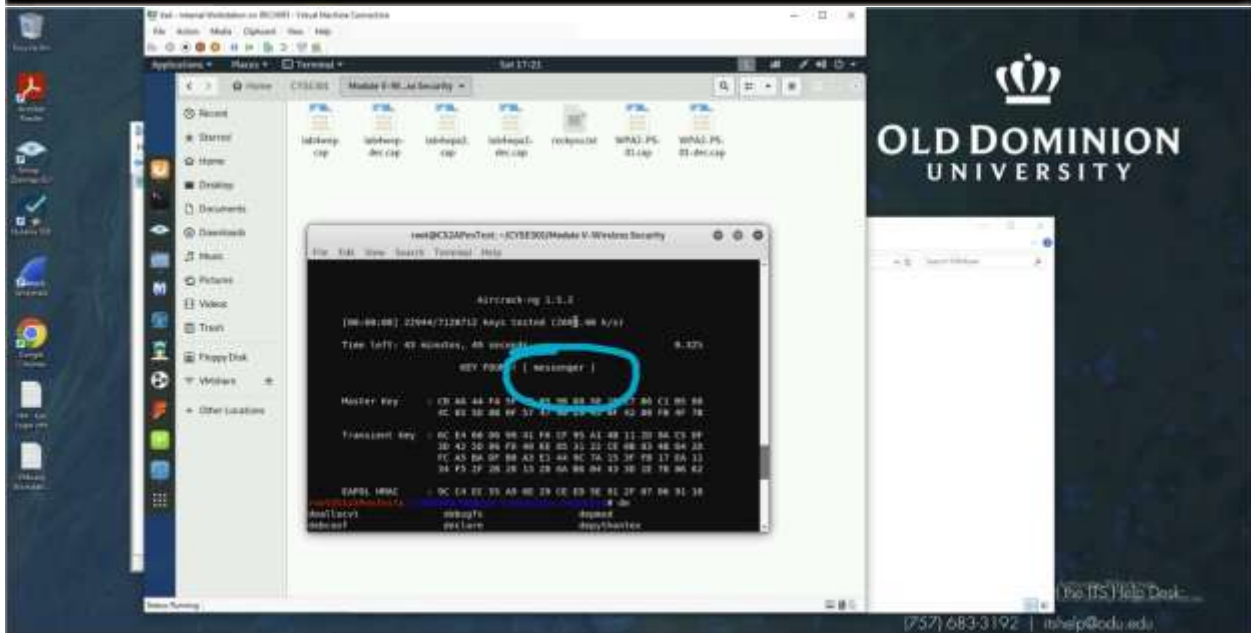
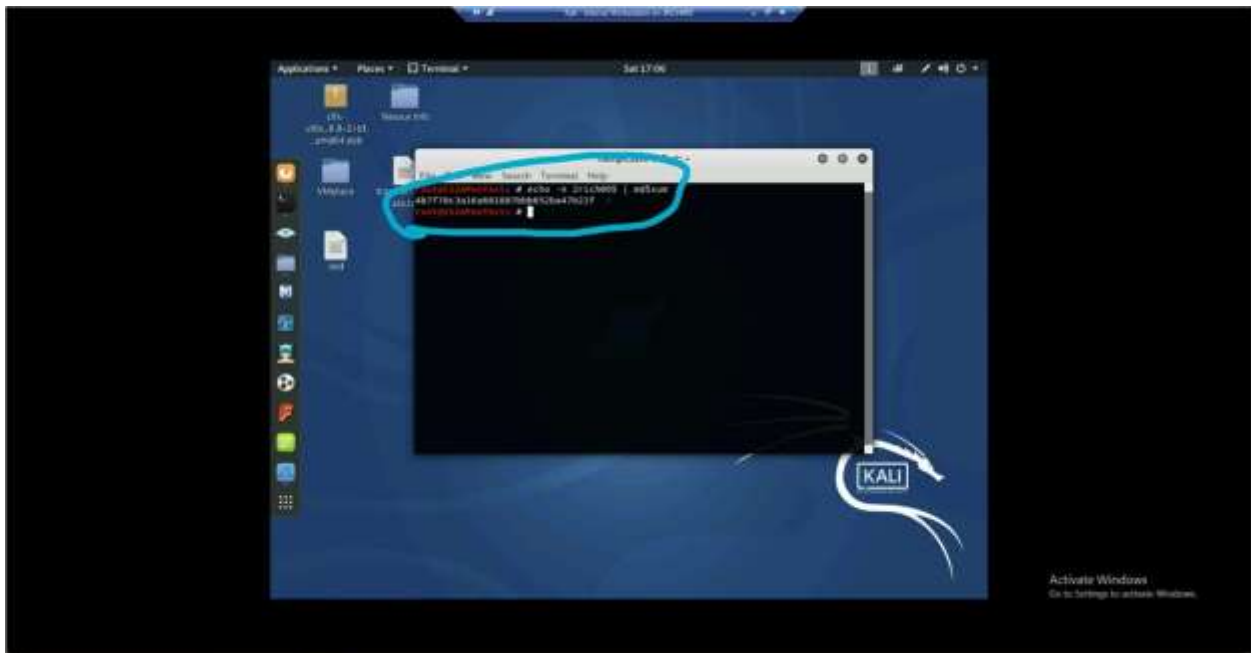
Display Type: Copy

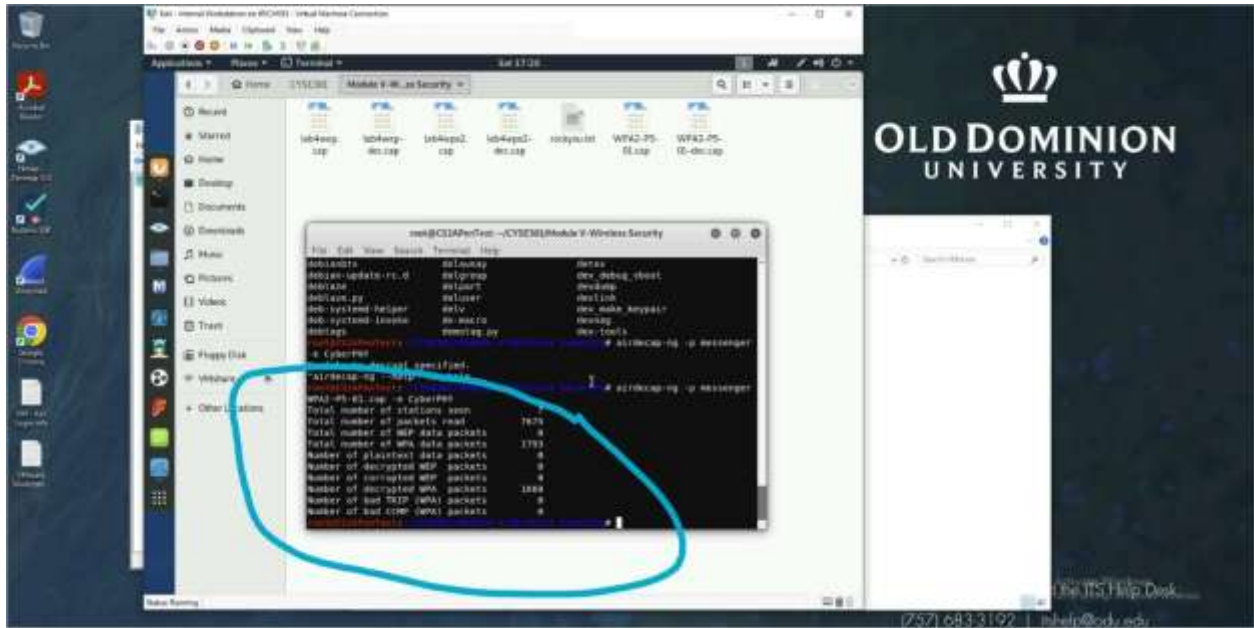
Summary: Packets: 2234 | Displayed: 2208 (99.2%) | Matched: 111.6%

Activate Windows  
Go to Settings to activate Windows.



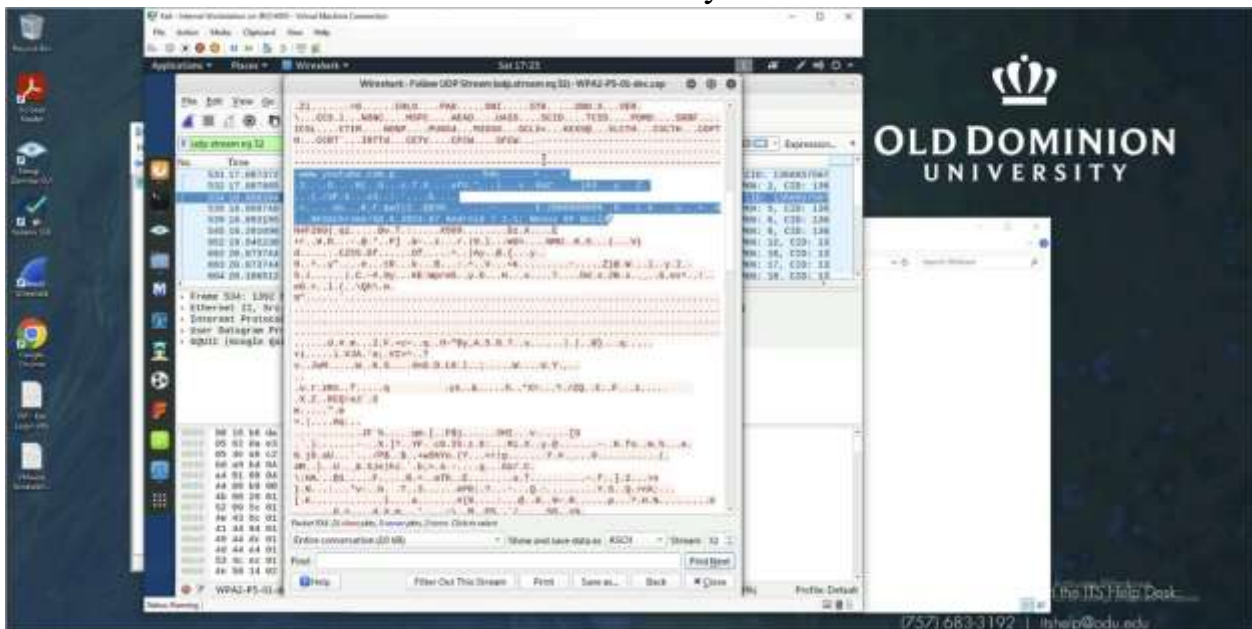




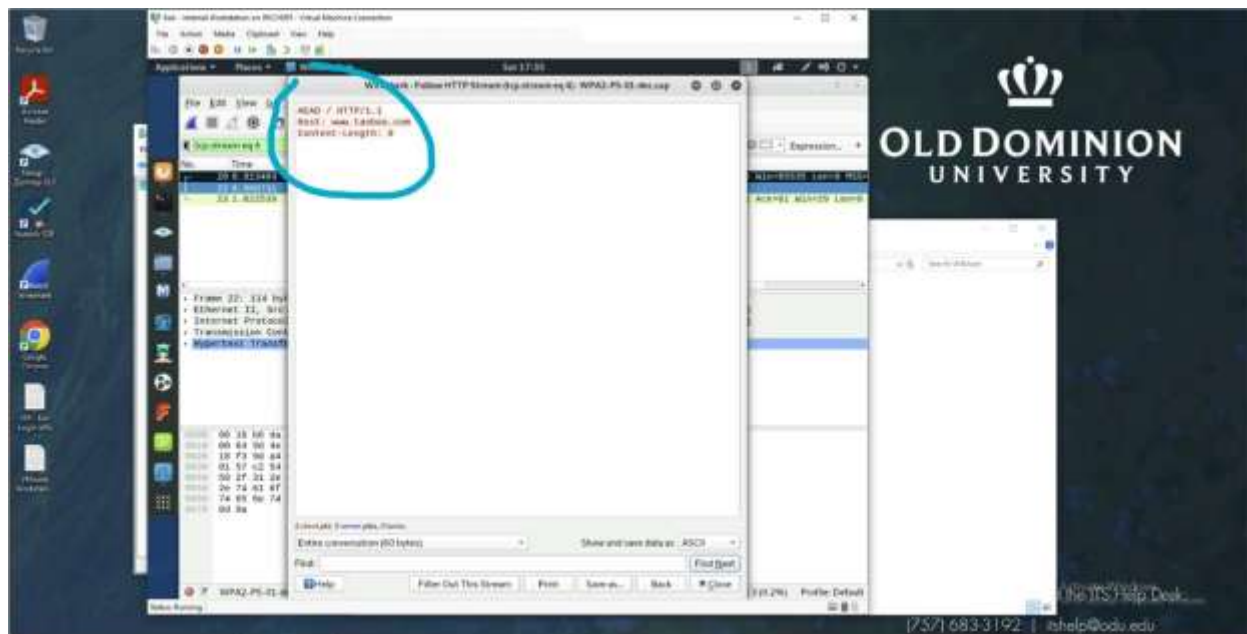


In the 3 screenshots above, I find the file that I need to crack into, find the password with a dic onary a ack, and then decrypt the Wireshark file.

### Wireshark Analysis 3







In these Wireshark screenshots, we can see what websites users are going to. The websites that I observed users going to were Taobao, a Chinese shopping website, someone going to a website to stream music as evident from the key word of “NextRadio”, and an android user watching YouTube through google images.