Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

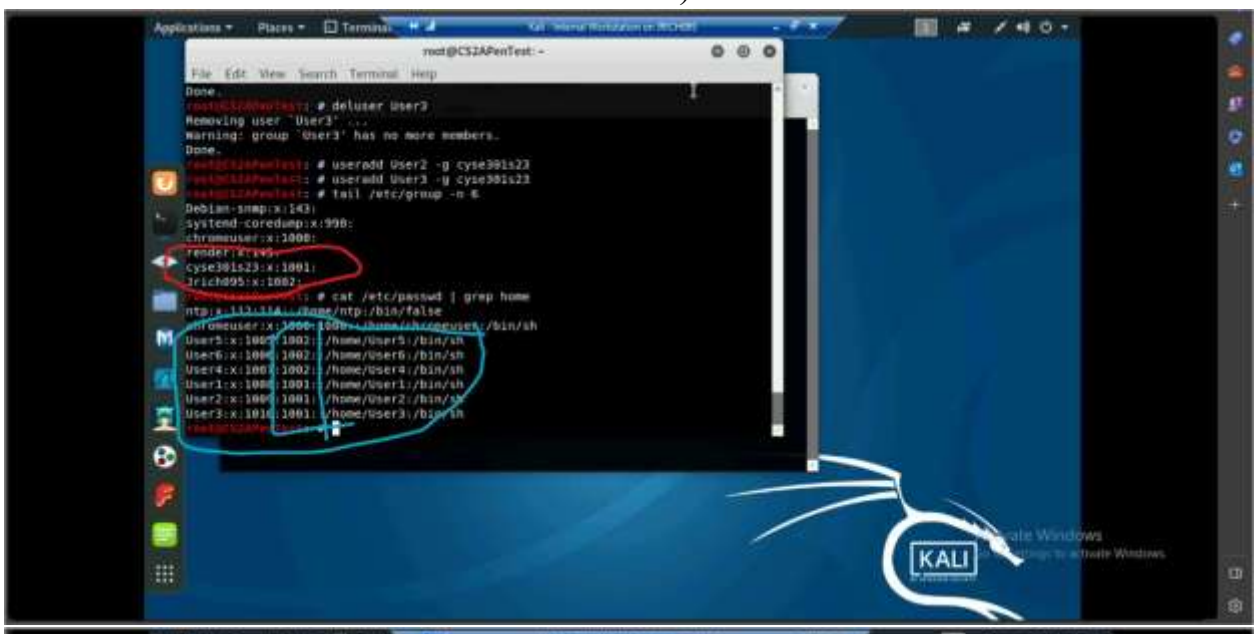
Assignment #5 Password Cracking

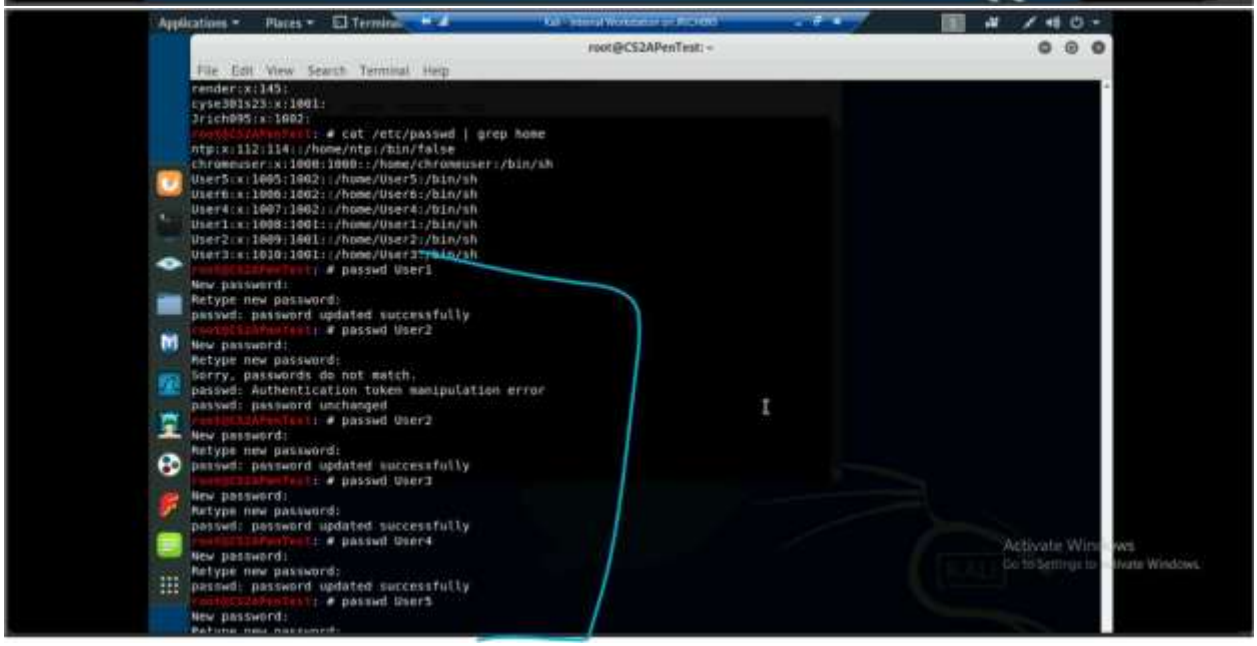
Jadyn Richardson

01221594

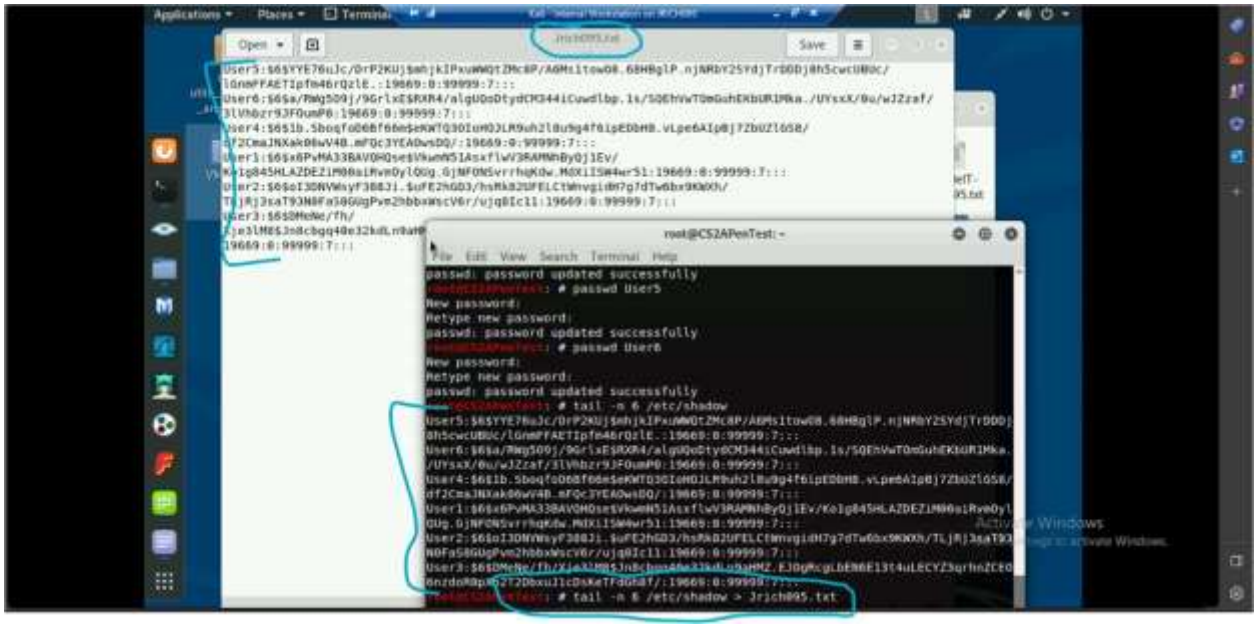
Password Cracking

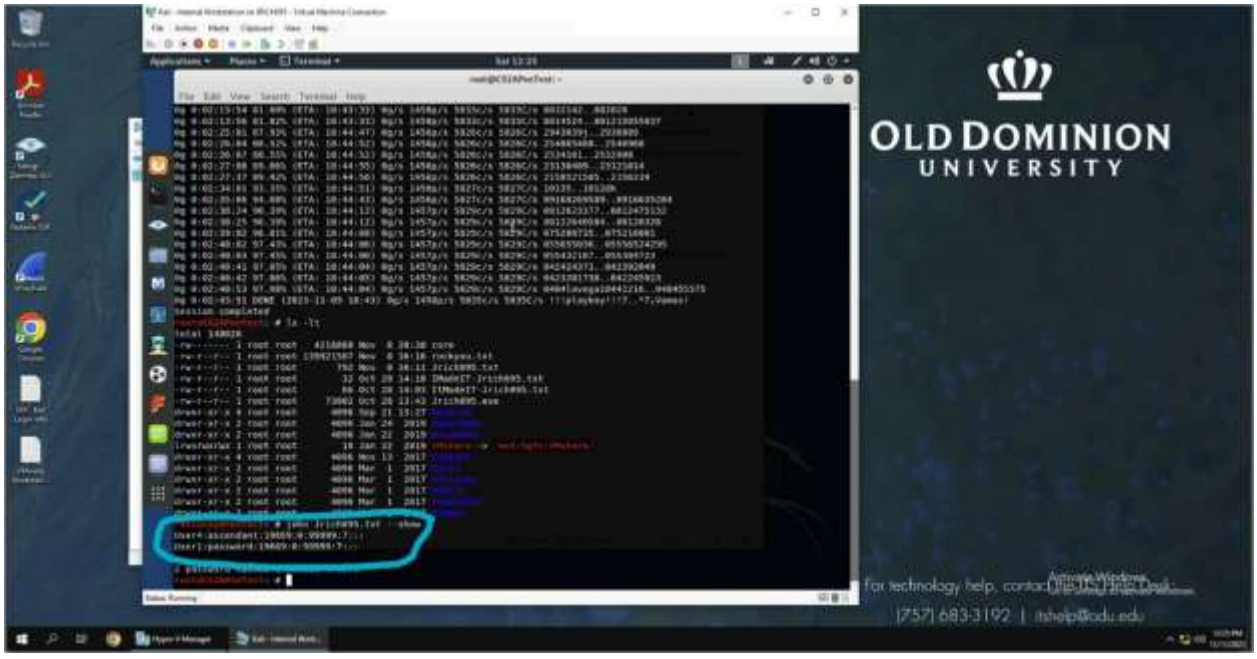
Task A.)





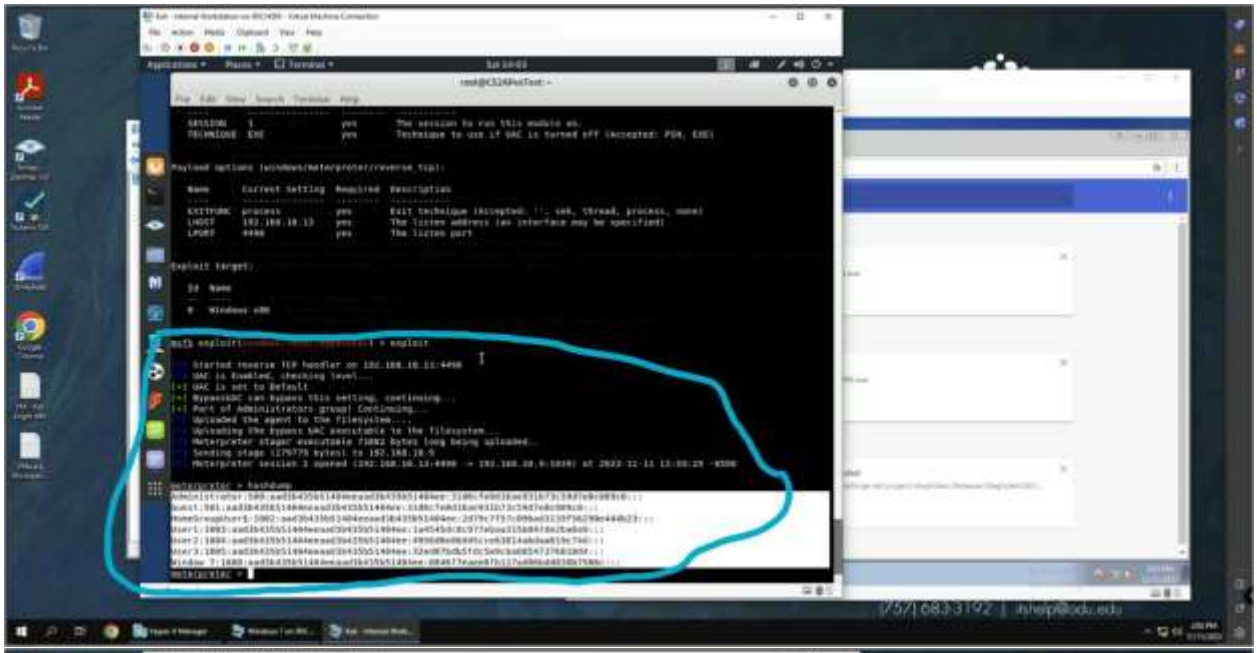
Selected Passwords: password, P@55w0rd, GreenGiant89, ascendant, *e&r9D-yK, S@nt@C1@5

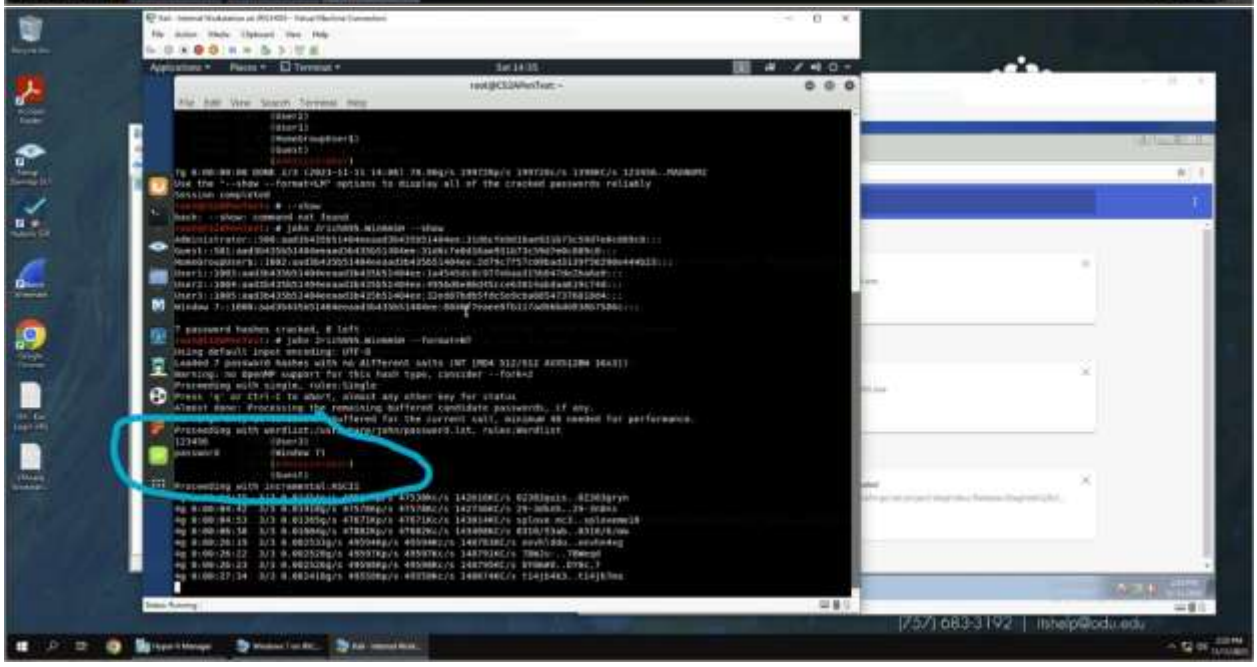


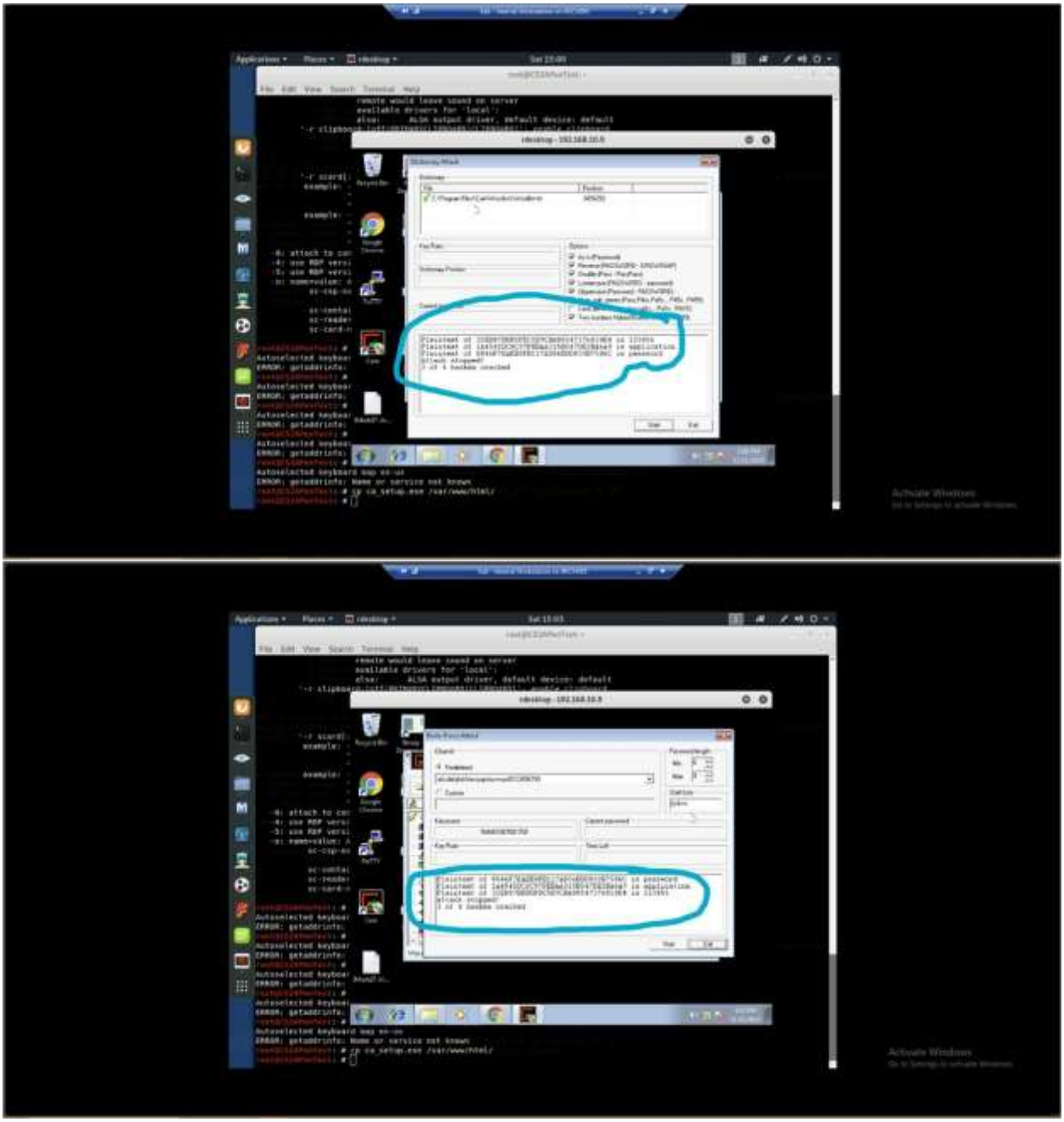


The above 4 screenshots show task A.1-A.4 in order.

Task B:



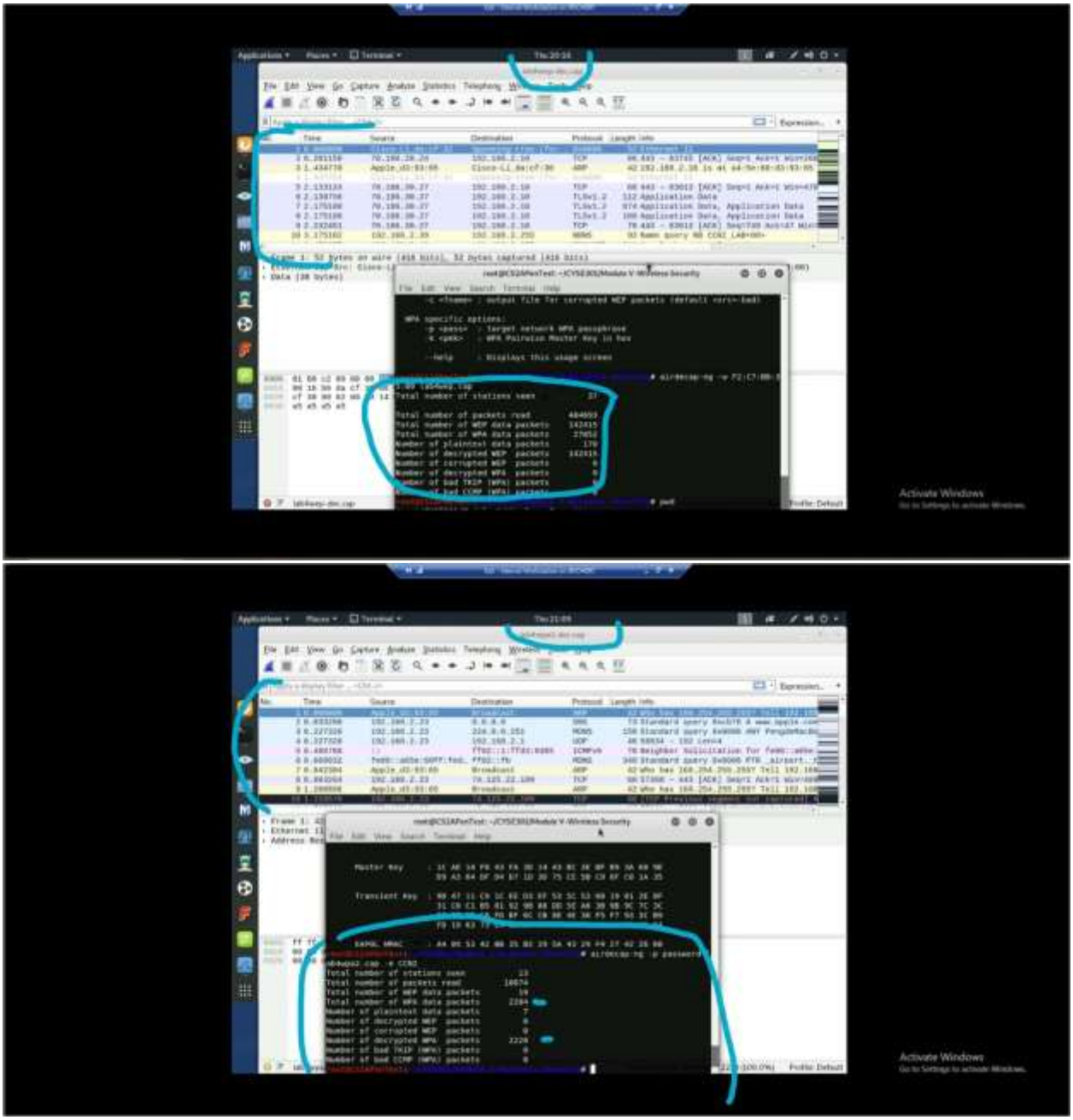




The above 4 screenshots show Task B1-B3 in order.

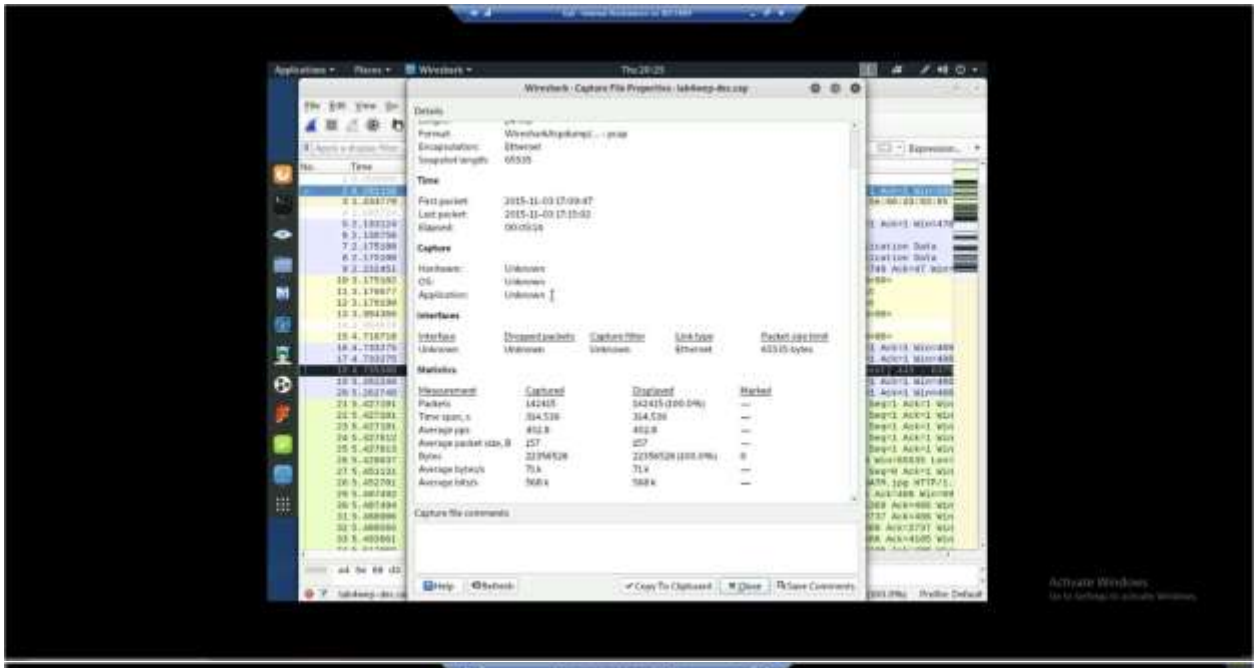
Wi-Fi Password Cracking

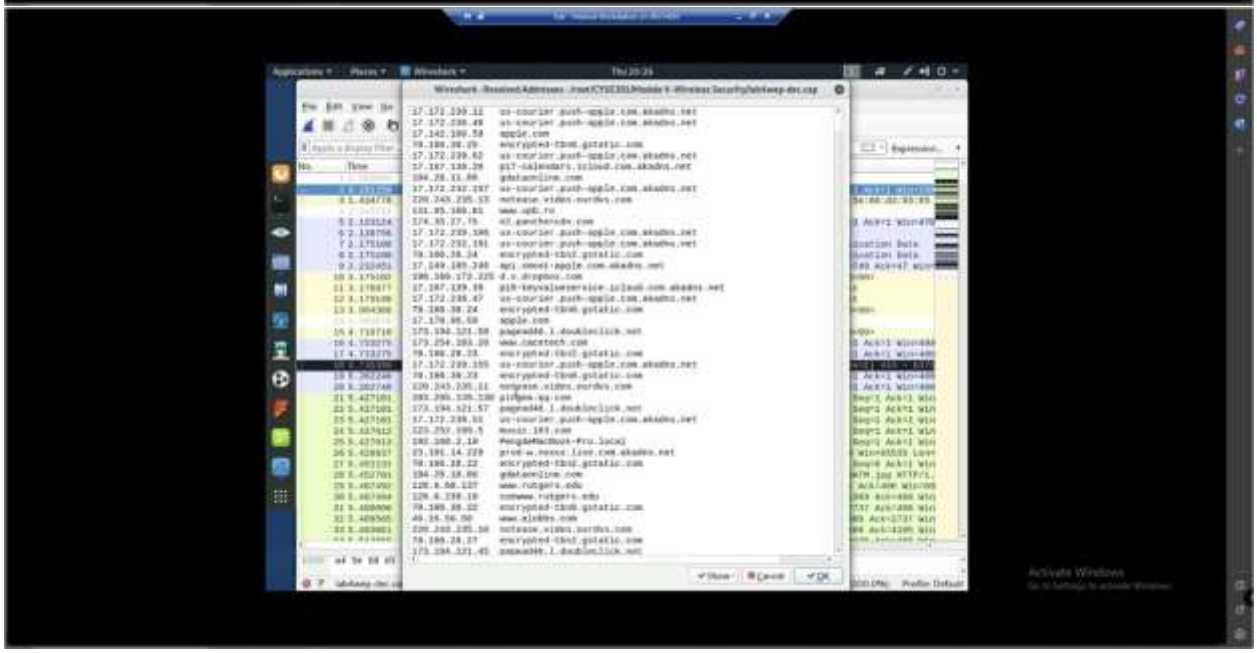
Task A.)

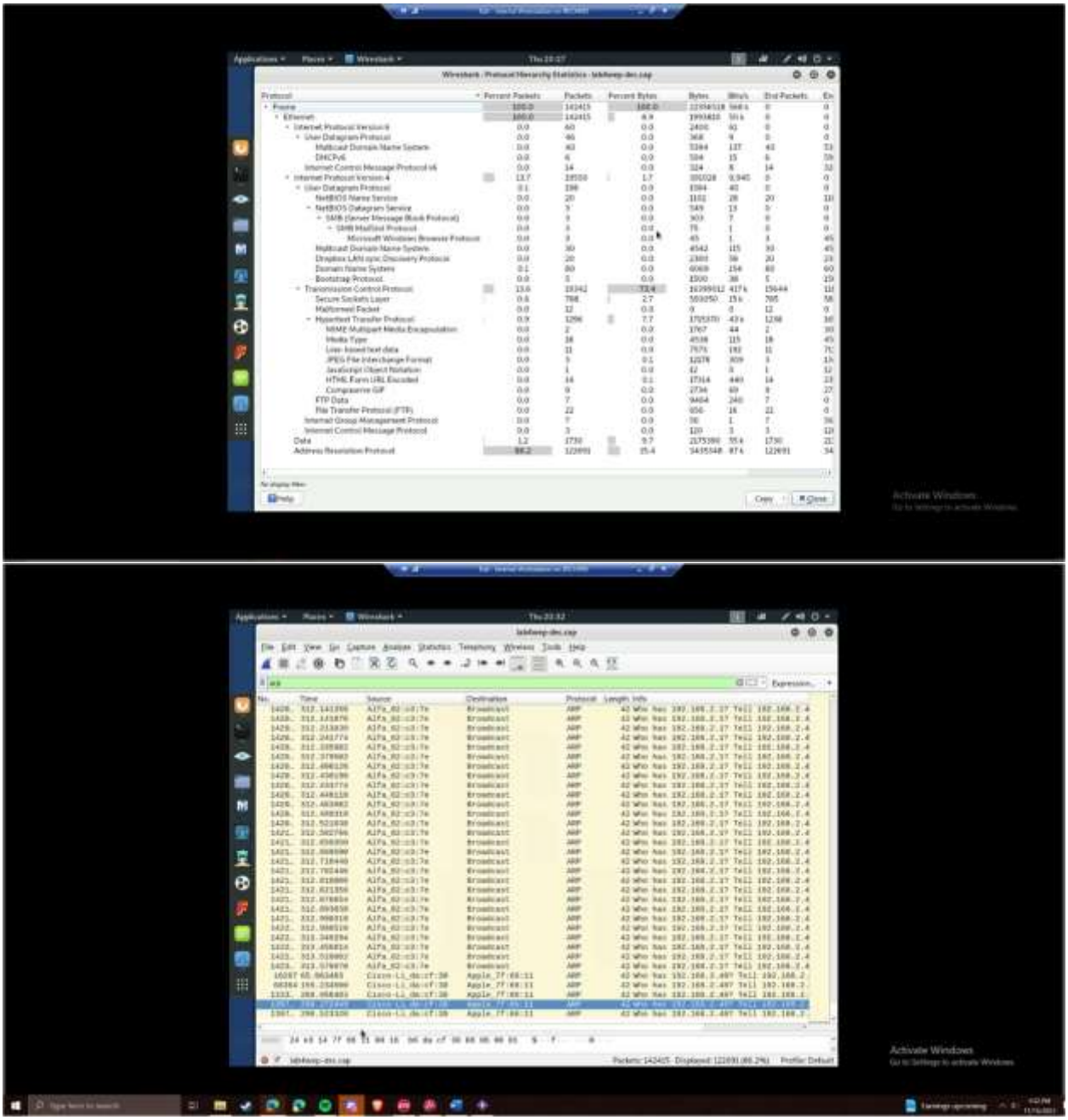


The above two screenshots show the process of decryp ng the capture file.

WireShark Analysis

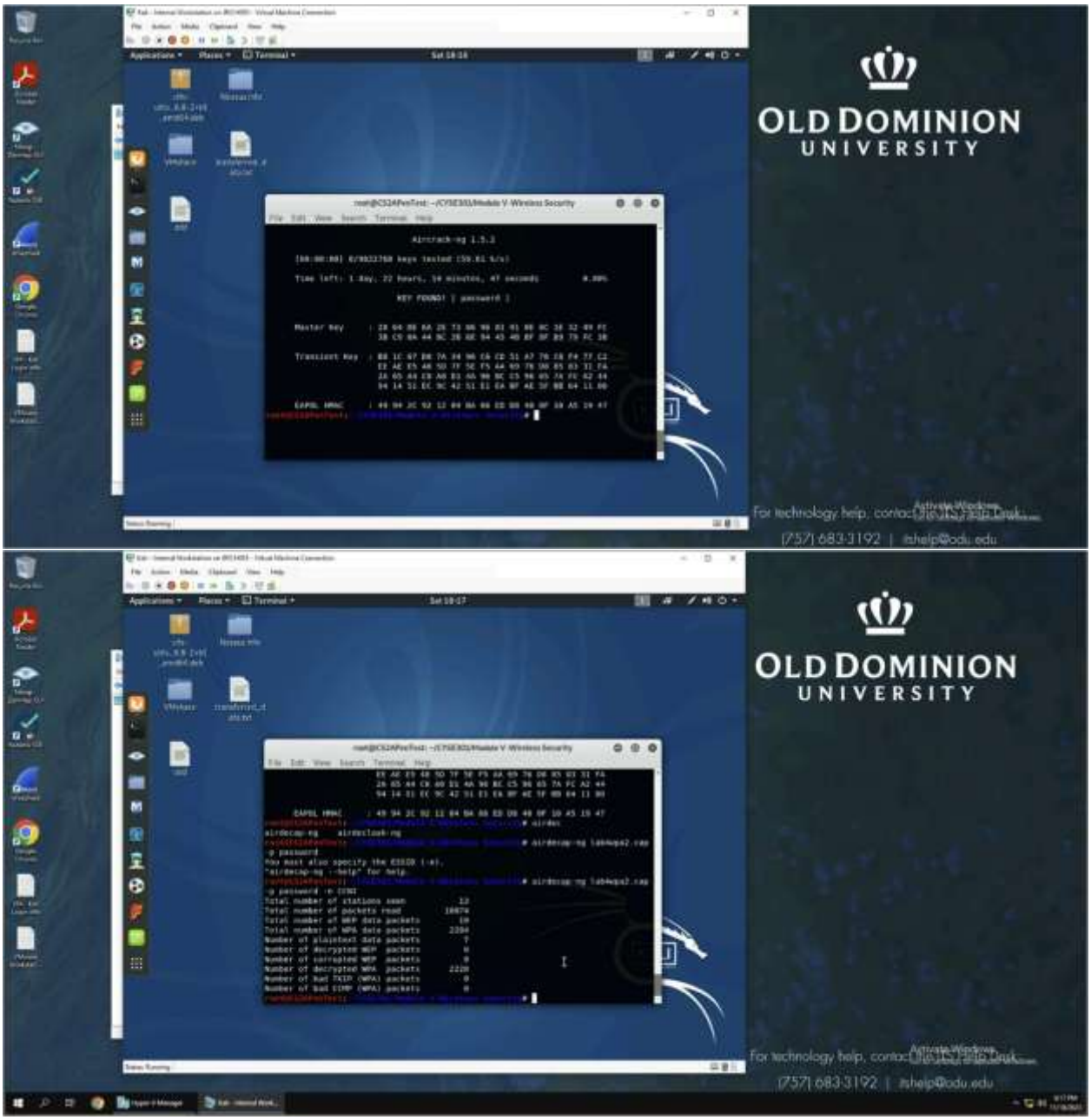

Wireshark · Capture File Properties · lab4wep-dec.cap
Details
Time
Capture
Interfaces
Statistics
Capture file comments


Wireshark · Resolved Addresses · root/CYSE301/Module 5 -Wireless Security/lab4wep-dec.cap



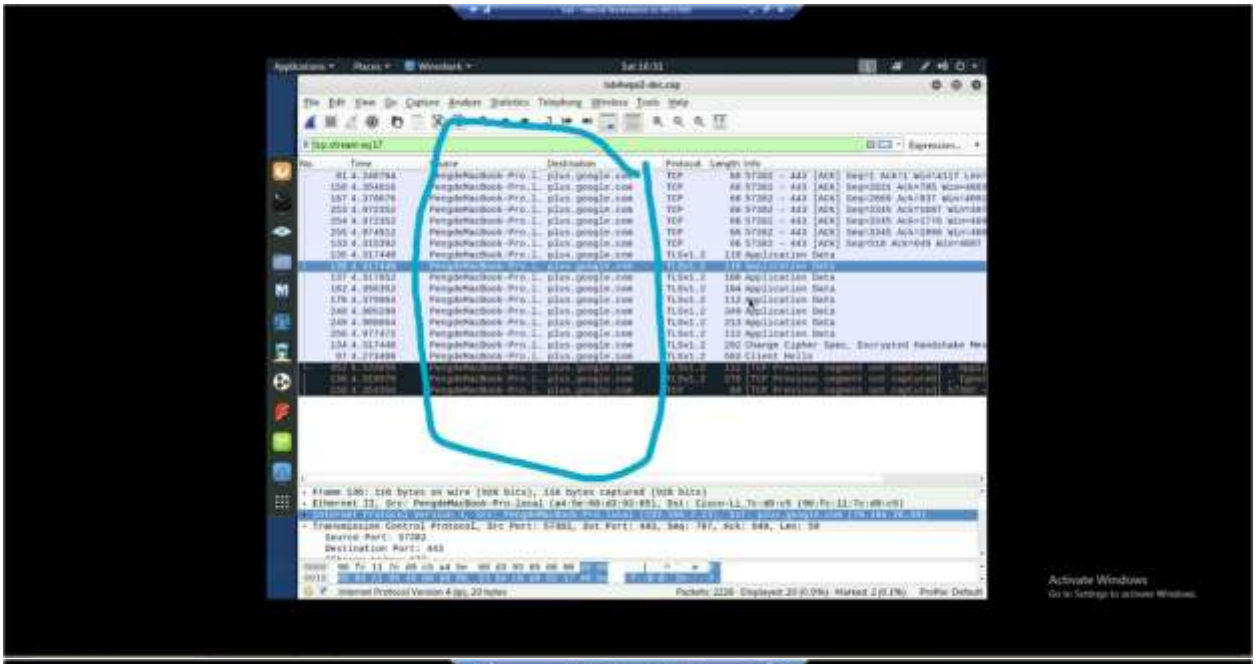
From these screenshots, we can see a lot of informa on about what is going on in these captures. From the first screenshot, we can see that the conversa on was only about five minutes long, how many packets were captured, and how many bytes there are in total. From the second screenshot, we can see what websites were visited. In the third screenshot, we can see the various websites that have been visited. Users visited sites for music and various apple services. Looking at the protocol hierarchy, there is suspicious ac vity in the address resolu on protocol being so big. There is a MAC address sending too many ARP broadcast signals to a ack the network.

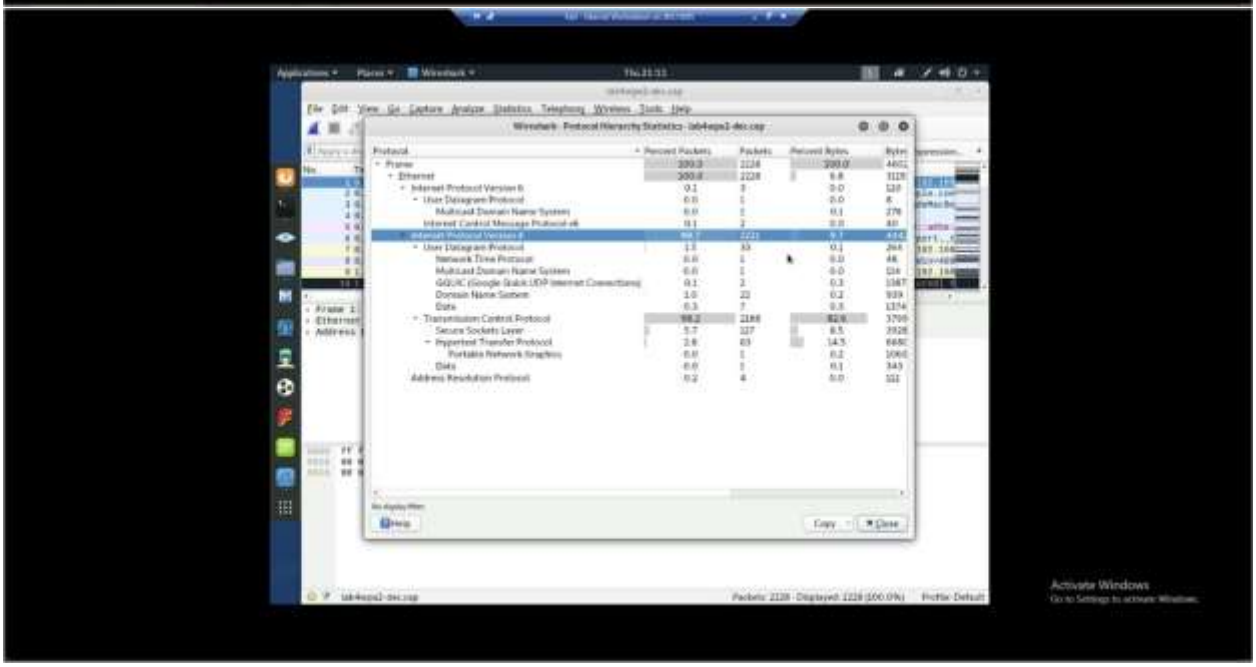
WPA cracking

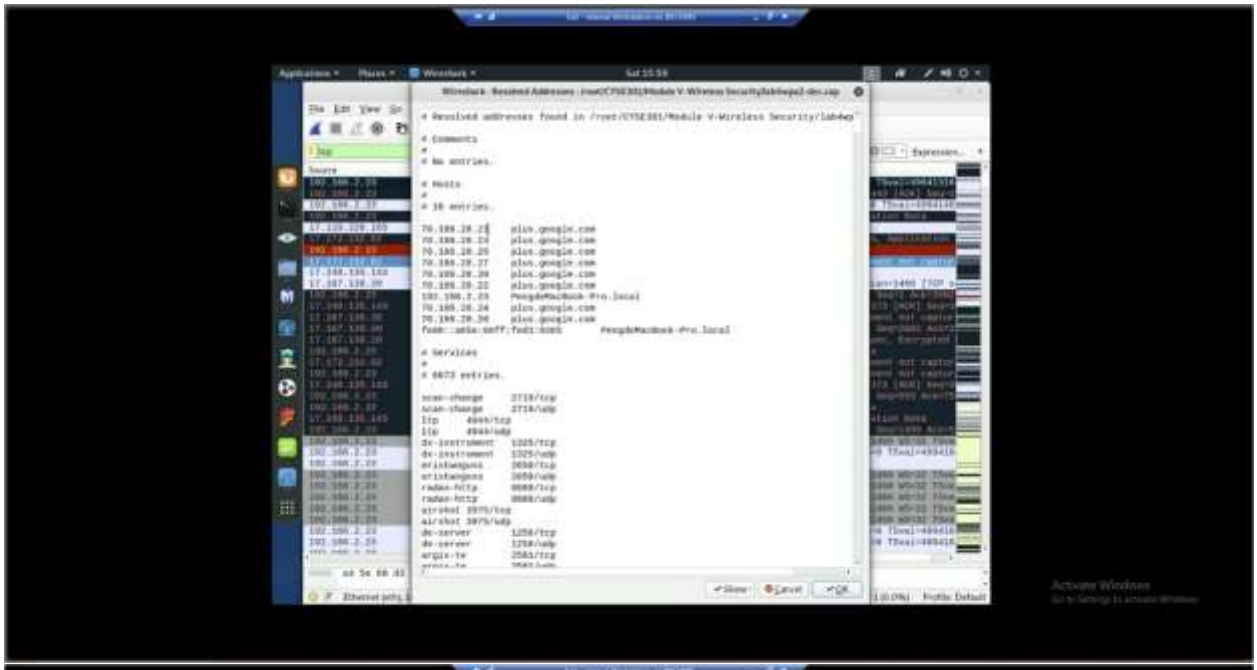


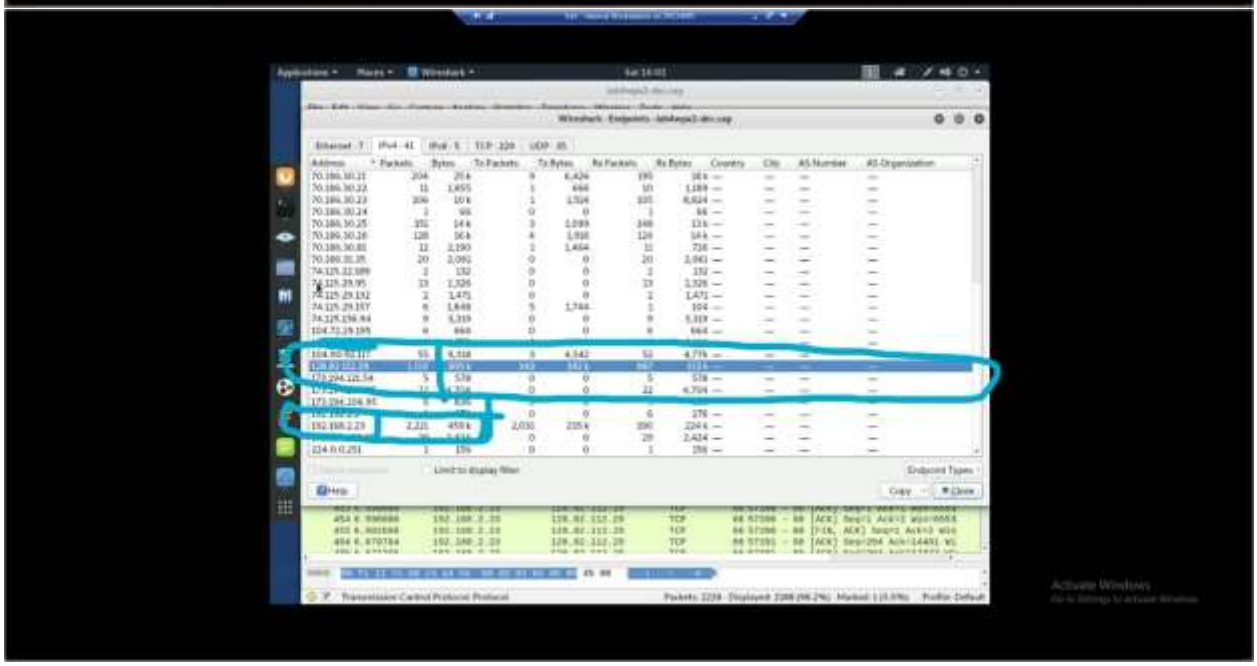
The above 2 screenshots show the process of cracking the password and decryp ng the capture file.

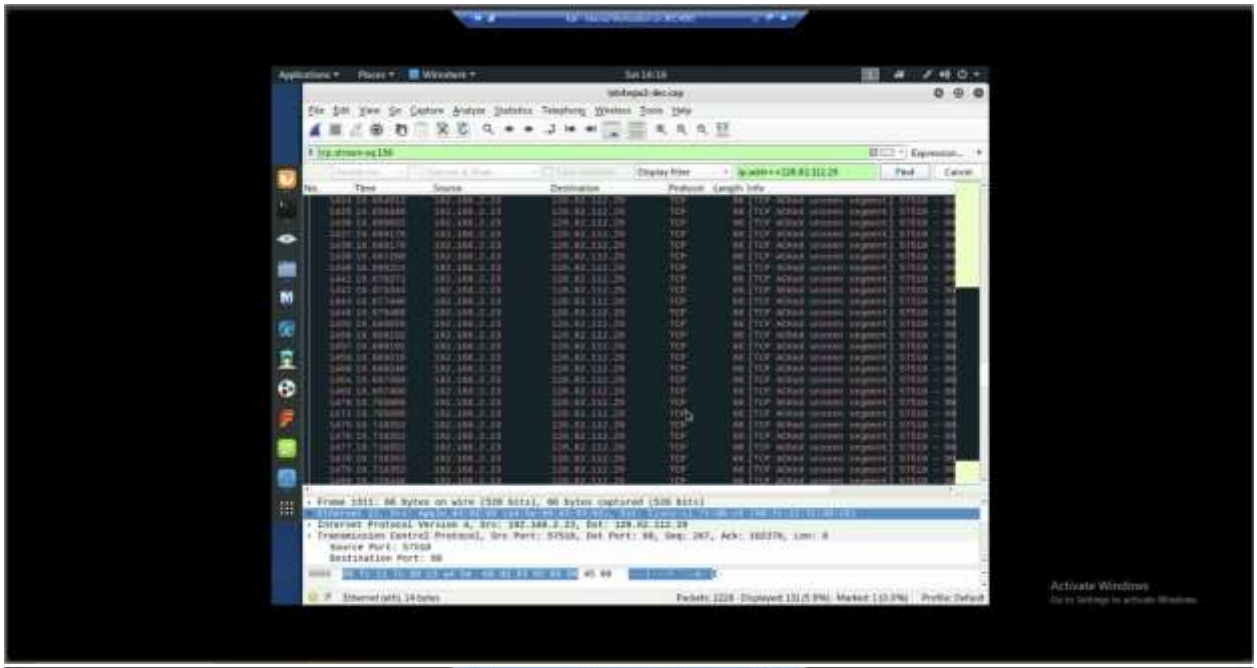
Wireshark Analysis 2

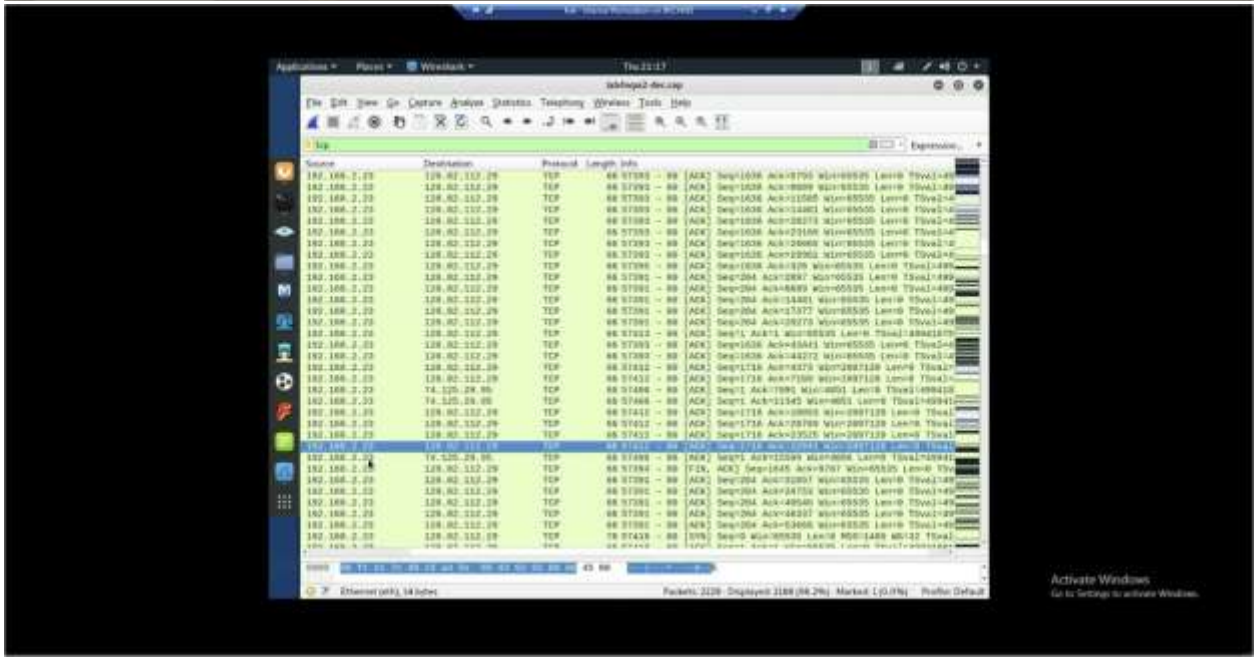

Activate Windows
Go to Settings to activate Windows.

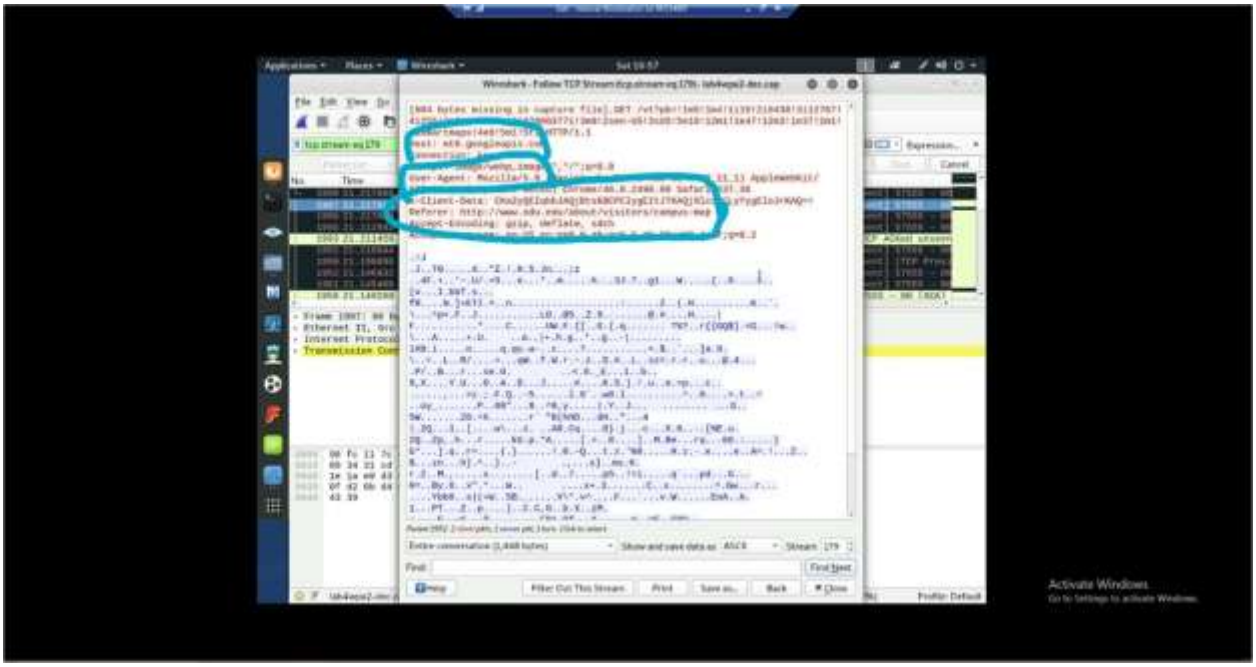

Wireshark · Protocol Hierarchy Statistics · lab4wpa2-dec.cap
Activate Windows
Go to Settings to activate Windows.


Wireshark · Resolved Addresses · root/CYSE301/Module V- Wireless Security/lab4wpa2-dec.cap
Resolved addresses found in /root/CYSE301/Module V-Wireless Security/lab4wp
Comments
#
No entries.
Hosts
#
10 entries.
70.186.28.21 plus.google.com
70.186.28.23 plus.google.com
70.186.28.25 plus.google.com
70.186.28.27 plus.google.com
70.186.28.29 plus.google.com
70.186.28.31 plus.google.com
192.168.2.23 PeeqsMacBook-Pro.local
70.186.28.34 plus.google.com
70.186.28.36 plus.google.com
fe80::a6de:ceff:fe81:9365 PeeqsMacBook-Pro.local
Services
#
6673 entries.
scan-change 2718/tcp
scan-change 2718/udp
ltp 4944/tcp
ltp 4944/udp
dx-instrument 1025/tcp
dx-instrument 1025/udp
wristwagons 3650/tcp
wristwagons 3650/udp
radan-http 8080/tcp
radan-http 8080/udp
airshot 3975/tcp
airshot 3975/udp
dn-server 1258/tcp
dn-server 1258/udp
argis-te 2582/tcp
Show
Cancel
OK
Activate Windows


Wireshark · Endpoints · lab4wpa2-dec.cap
Ethernet · 7
IPv4 · 41
IPv6 · 5
TCP · 220
UDP · 85
Address
Packets
Bytes
Tx Packets
Tx Bytes
Rx Packets
Rx Bytes
Country
City
AS Number
AS Organization
70.186.30.21 204 25 k 9 6,424 195 18 k
70.186.30.22 11 1,655 5 666 10 1,189
70.186.30.23 206 19 k 1 1,514 105 6,824
70.186.30.24 1 66 0 0 1 66
70.186.30.25 35 14 k 3 1,093 248 13 k
70.186.30.26 128 16 k 4 1,936 124 14 k
70.186.30.81 11 2,190 1 1,464 11 726
70.186.31.35 20 2,061 0 0 20 2,061
74.125.22.189 1 132 0 0 1 132
74.125.29.95 13 1,326 0 0 13 1,326
74.125.29.132 1 1,471 0 0 1 1,471
74.125.29.157 6 1,848 5 1,744 1 104
74.125.156.84 9 5,319 0 0 9 5,319
104.71.19.195 8 664 0 0 8 664
104.80.92.117 55 9,316 5 4,542 50 4,774
128.82.112.29 1,109 805 k 443 151 k 667 654 k
173.194.32.54 5 578 0 0 5 578
173.194.194.95 1 66 0 0 1 66
192.168.2.23 2,225 459 k 2,030 235 k 195 224 k
224.0.0.251 1 176 0 0 1 176
Limit to display filter
Endpoint Types
Help
Copy
Close
Transmission Control Protocol Protocol
Activate Windows

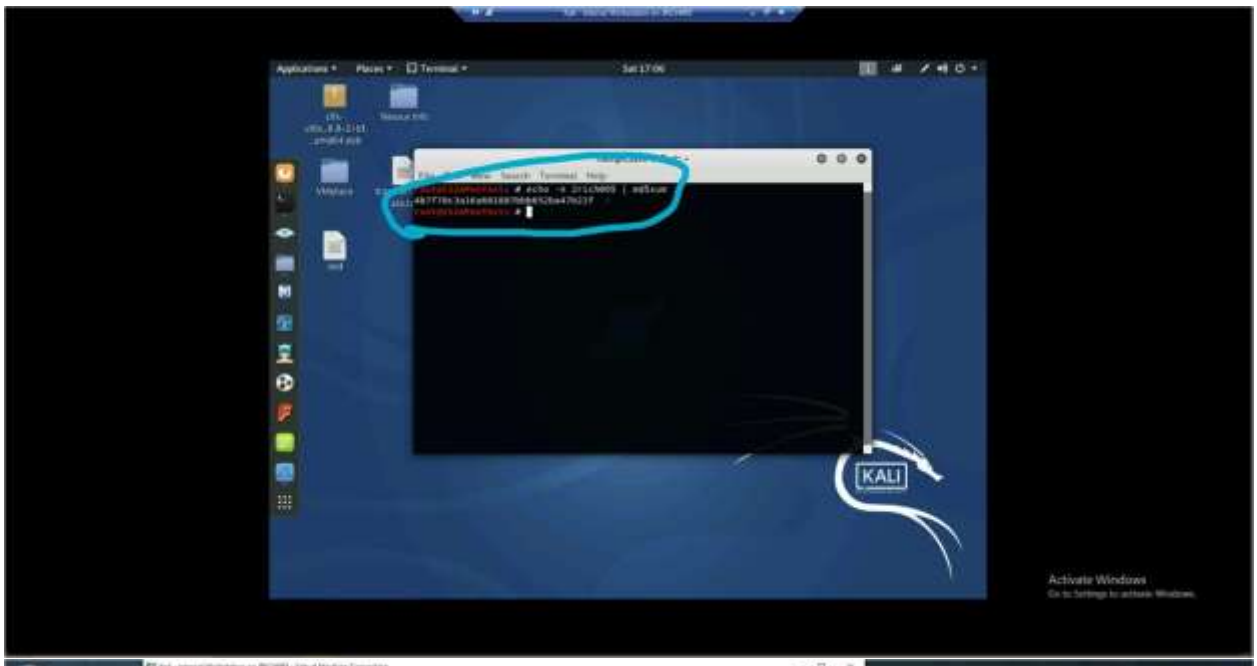

Activate Windows
Go to Settings to activate Windows.

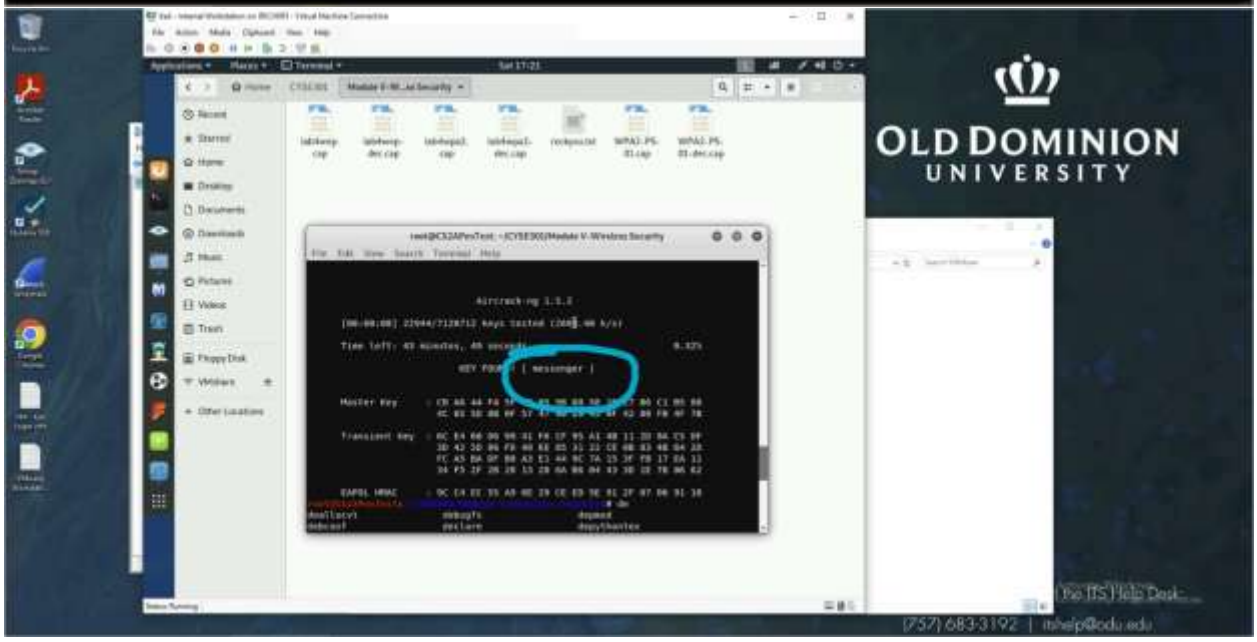

Activate Windows
Go to Settings to activate Windows.

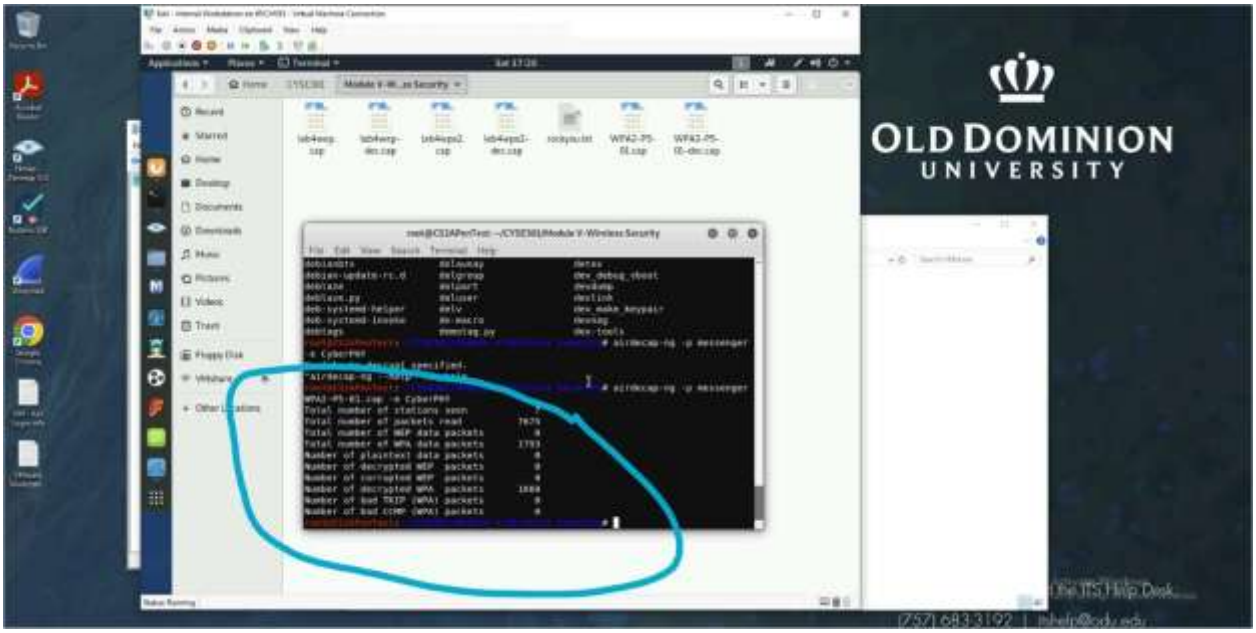


In these screenshots, we can see that the most ac vity is seen through a TCP conversa on between two par es. We can also see the different websites that are visited in this capture. The majority of them are google.com. From the last screenshot, we can see that the Peng MacBook user is visi ng google maps using Mozilla Firefox, and we referred there by a campus maps link on ODU.

Task B

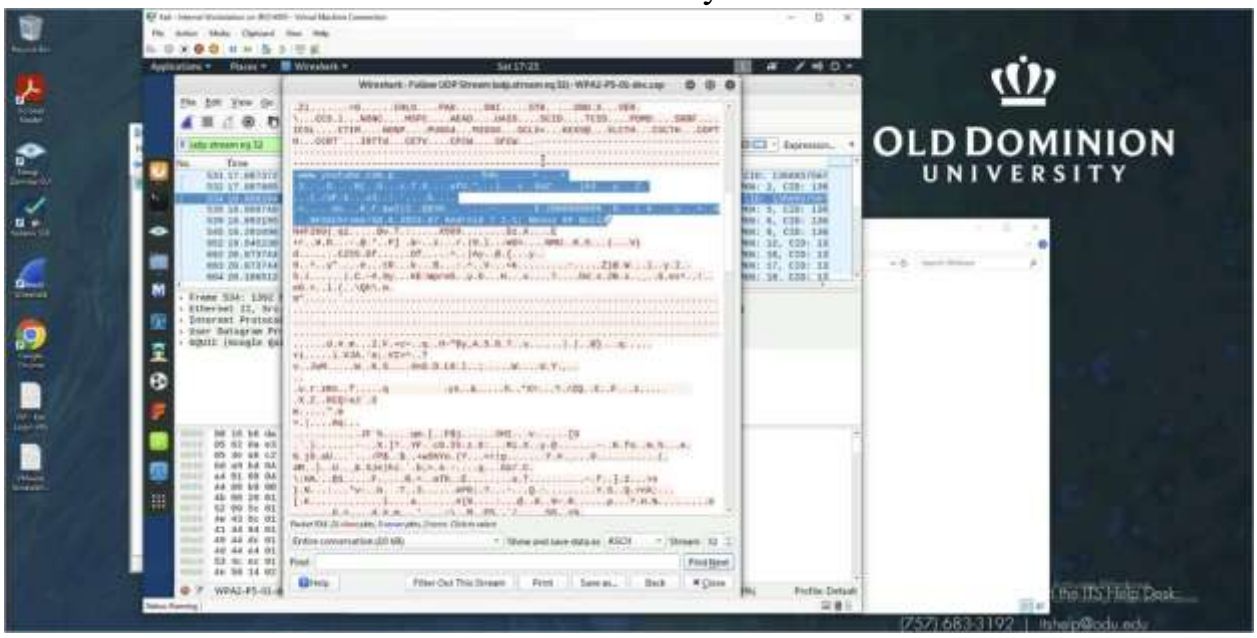

KALI
Activate Windows

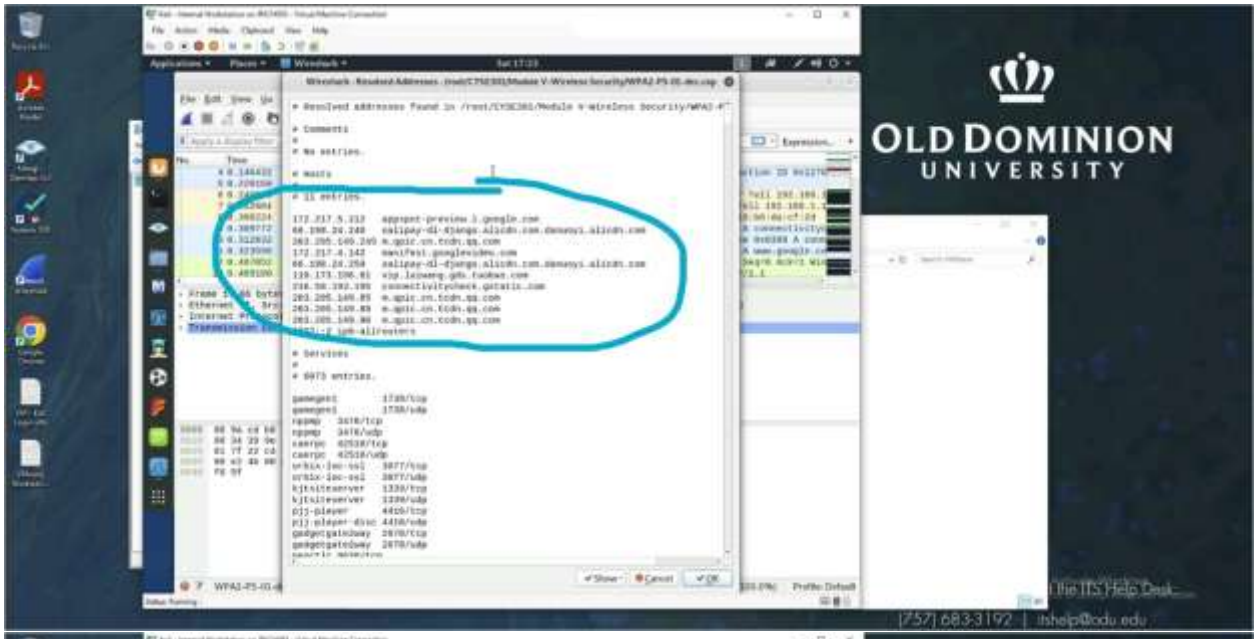

OLD DOMINION
UNIVERSITY
(757) 683-3192 | itshelp@odu.edu

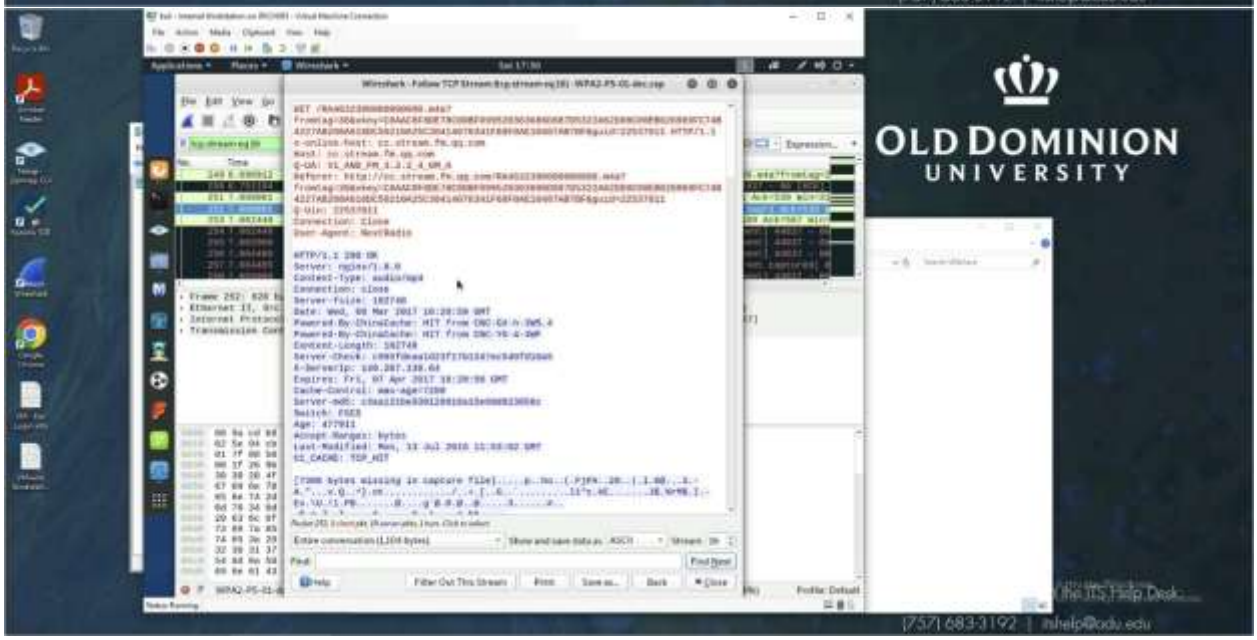


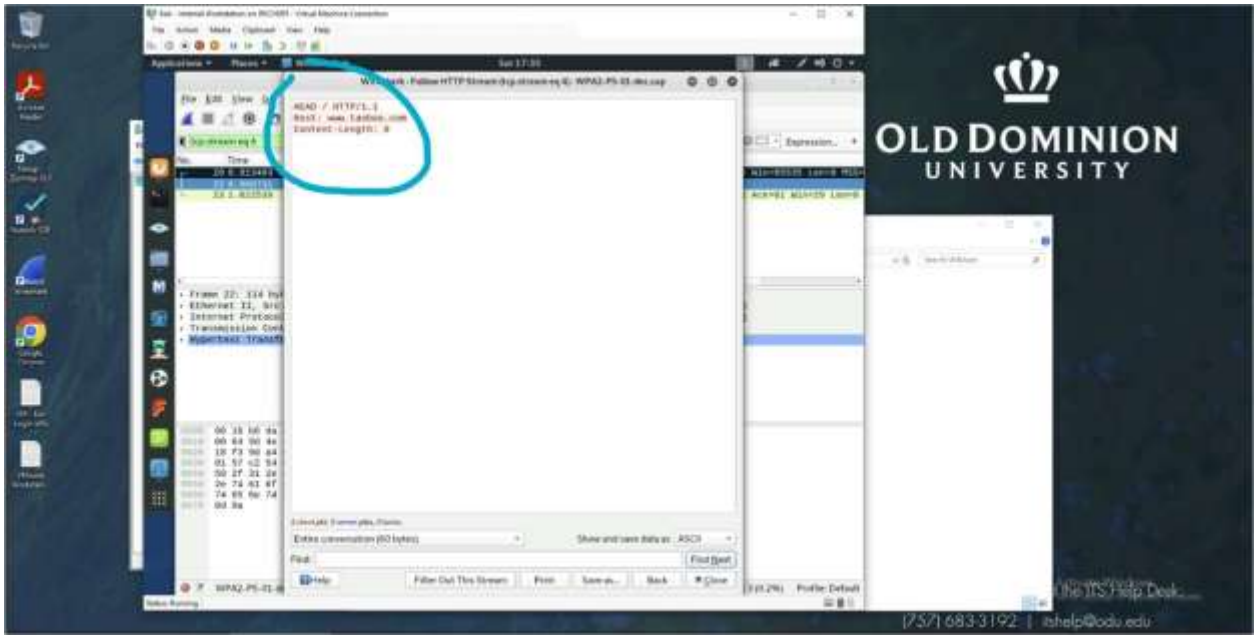
In the 3 screenshots above, I find the file that I need to crack into, find the password with a dic onary a ack, and then decrypt the Wireshark file.

Wireshark Analysis 3




OLD DOMINION
UNIVERSITY
[757] 683-3192 | itshelp@odu.edu


OLD DOMINION
UNIVERSITY
[757] 683-3192 | itshelp@odu.edu



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.