

OLD DOMINION

CYSE301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #6 – Wifi password cracking

AUSTIN CUPP

01183567

Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places Wireshark Thu 16:43

lab4wep.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_04:7d:e1	Broadcast	802.11	263	Beacon frame, SN=513, FN=0, Flags=..
2	-0.000017	IntelCor_3b:c8:c9 (...)	Cisco_fa:3b:a2 (58:...	802.11	28	802.11 Block Ack, Flags=.....
3	0.000523	Apple_28:d8:50	Cisco-Li_7c:d0:c5	802.11	150	QoS Data, SN=2829, FN=0, Flags=.p..R
4	0.000522		Cisco-Li_7c:d0:c7 (...)	802.11	10	Acknowledgement, Flags=.....
5	0.002571	Apple_28:d8:50	Cisco-Li_7c:d0:c5	802.11	457	QoS Data, SN=2830, FN=0, Flags=.p...
6	0.002591		Apple_28:d8:50 (30:...	802.11	10	Acknowledgement, Flags=.....
7	0.014858	Apple_28:d8:50	Cisco-Li_7c:d0:c5	802.11	146	QoS Data, SN=2831, FN=0, Flags=.p...
8	0.017930	Apple_28:d8:50	Cisco-Li_7c:d0:c5	802.11	146	QoS Data, SN=2831, FN=0, Flags=.p..R
9	0.024088	Cisco-Li_7c:ce:63	Broadcast	802.11	112	Beacon frame, SN=2018, FN=0, Flags=.
10	0.024088	Cisco-Li_7c:ce:63	Broadcast	802.11	112	Beacon frame, SN=2018, FN=0, Flags=.

Frame 1: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits)

- IEEE 802.11 Beacon frame, Flags:
- IEEE 802.11 wireless LAN

0000 80 00 00 00 ff ff ff ff ff ff f4 7f 35 04 7d e15..

0010 f4 7f 35 04 7d e1 10 20 22 f0 ee 46 0a 03 00 005..

0020 66 00 31 14 00 01 00 01 06 98 24 30 48 60 6c 03 f.1.....\$0H.l

0030 01 06 05 04 00 01 00 00 07 06 55 53 20 01 0b 1eUS

0040 0b 05 08 00 2a 8d 5b 2a 01 00 2d 1a ac 19 1b ff*.[*.....

0050 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 000

0060 00 00 00 00 00 00 30 14 01 00 00 0f ac 04 01 000

0070 00 0f ac 04 01 00 00 0f ac 02 28 00 3d 16 06 000

0080 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00@

0090 00 00 00 00 7f 08 00 10 00 00 00 40 00 01 85 1e@

00a0 02 00 8f 00 0f 00 ff 03 59 00 4b 48 33 31 2d 41Y.KH31-A

Hyper-V Manager pfsense - Firewall 6... Attacker Kali - Ext...

4:43 PM 12/1/2022

Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places Wireshark Thu 16:47

lab4wep.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

Wireshark - Protocol Hierarchy Statistics - lab4wep.cap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	404693	100.0	40709169	1,031 k
IEEE 802.11 wireless LAN	116.7	472392	20.7	8415672	213 k
Logical-Link Control	0.1	280	0.1	31207	790
Spanning Tree Protocol	0.0	137	0.0	5891	149
Internet Protocol Version 4	0.0	3	0.0	60	1
Transmission Control Protocol	0.0	3	0.0	120	3
Address Resolution Protocol	0.0	1	0.0	28	0
802.1X Authentication	0.0	117	0.1	22717	575
Extensible Authentication Protocol	0.0	110	0.1	21617	547
Malformed Packet	0.0	12	0.0	0	0
Data	49.7	200952	75.2	30623474	775 k

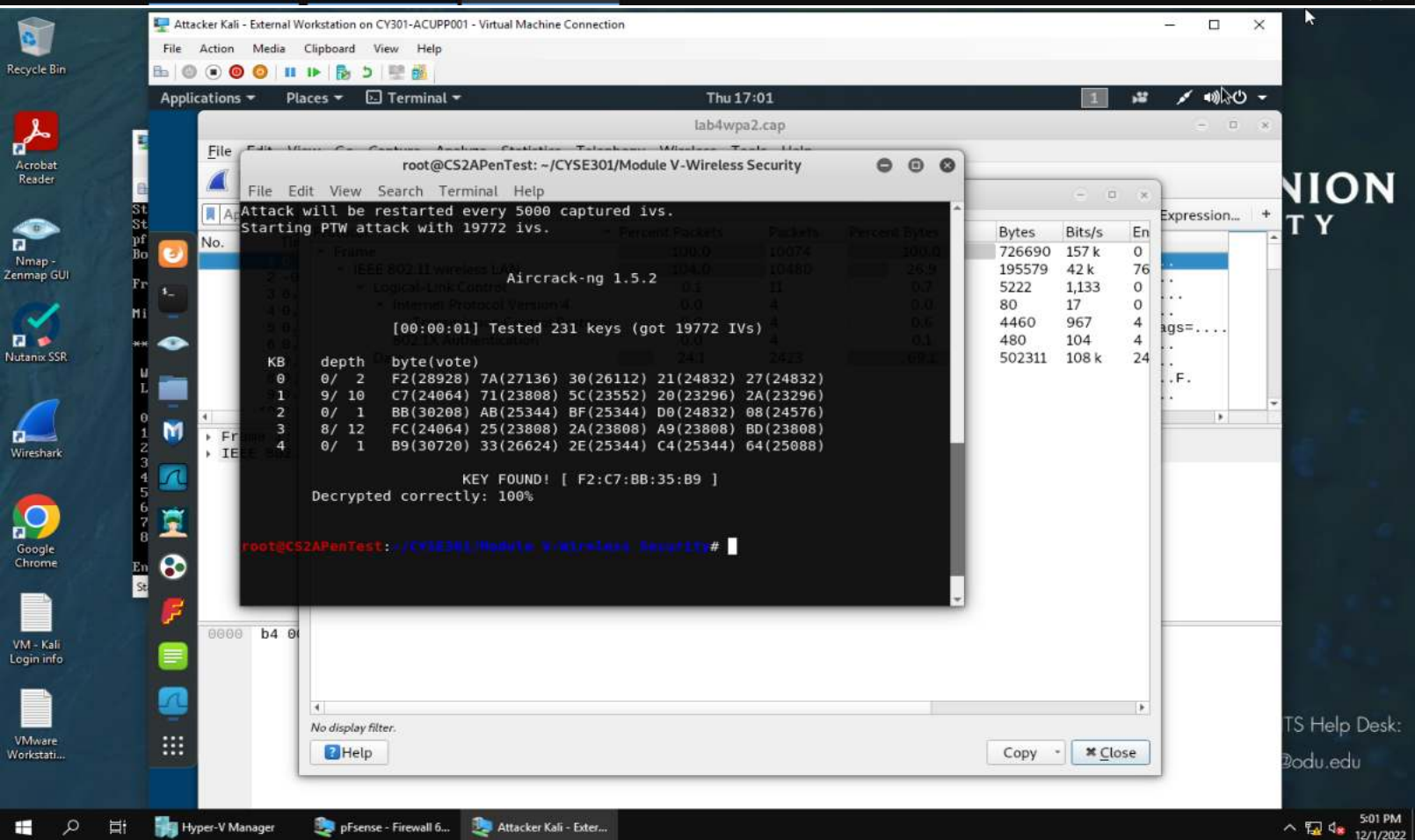
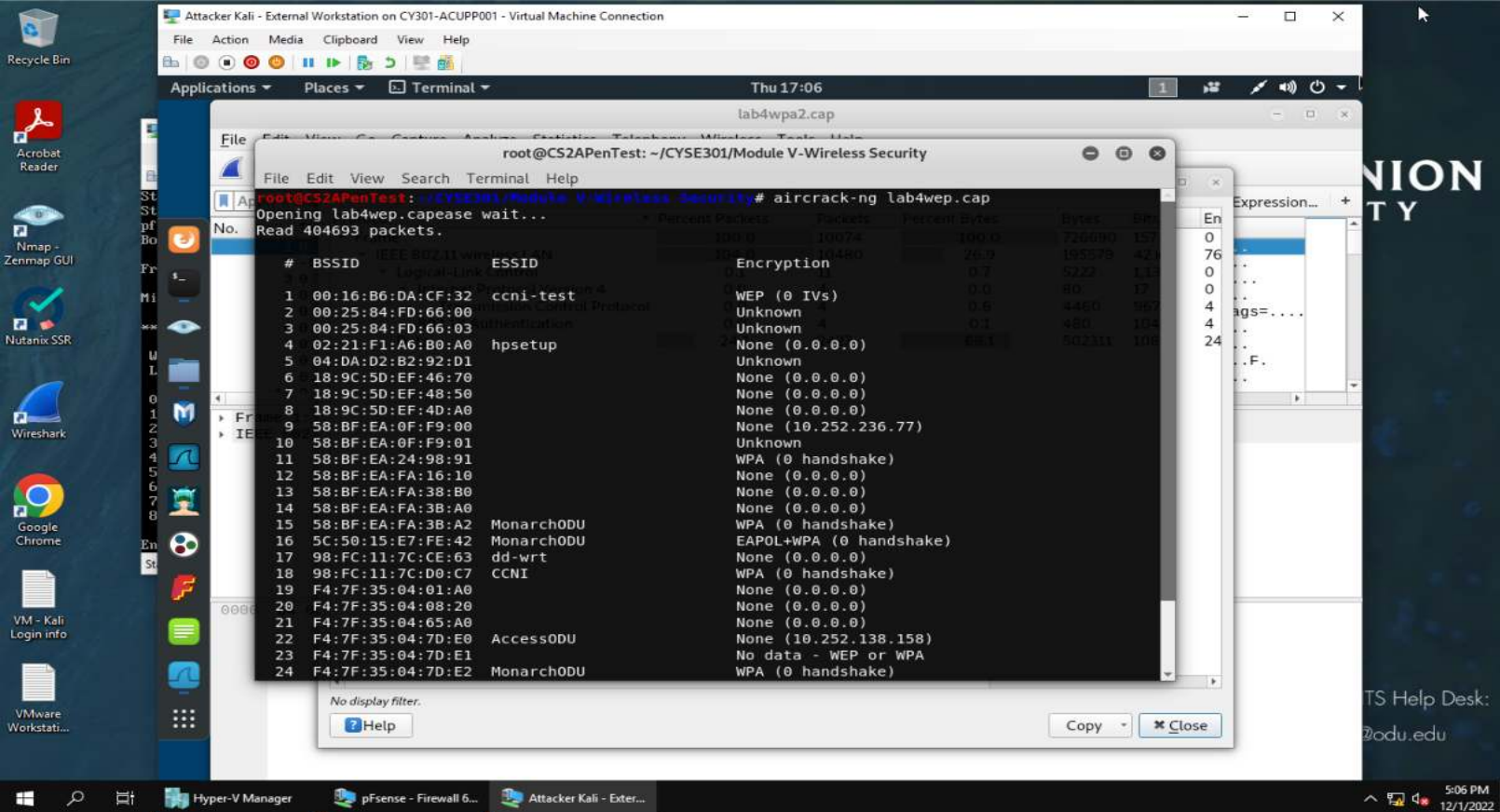
No display filter.

Help Copy Close

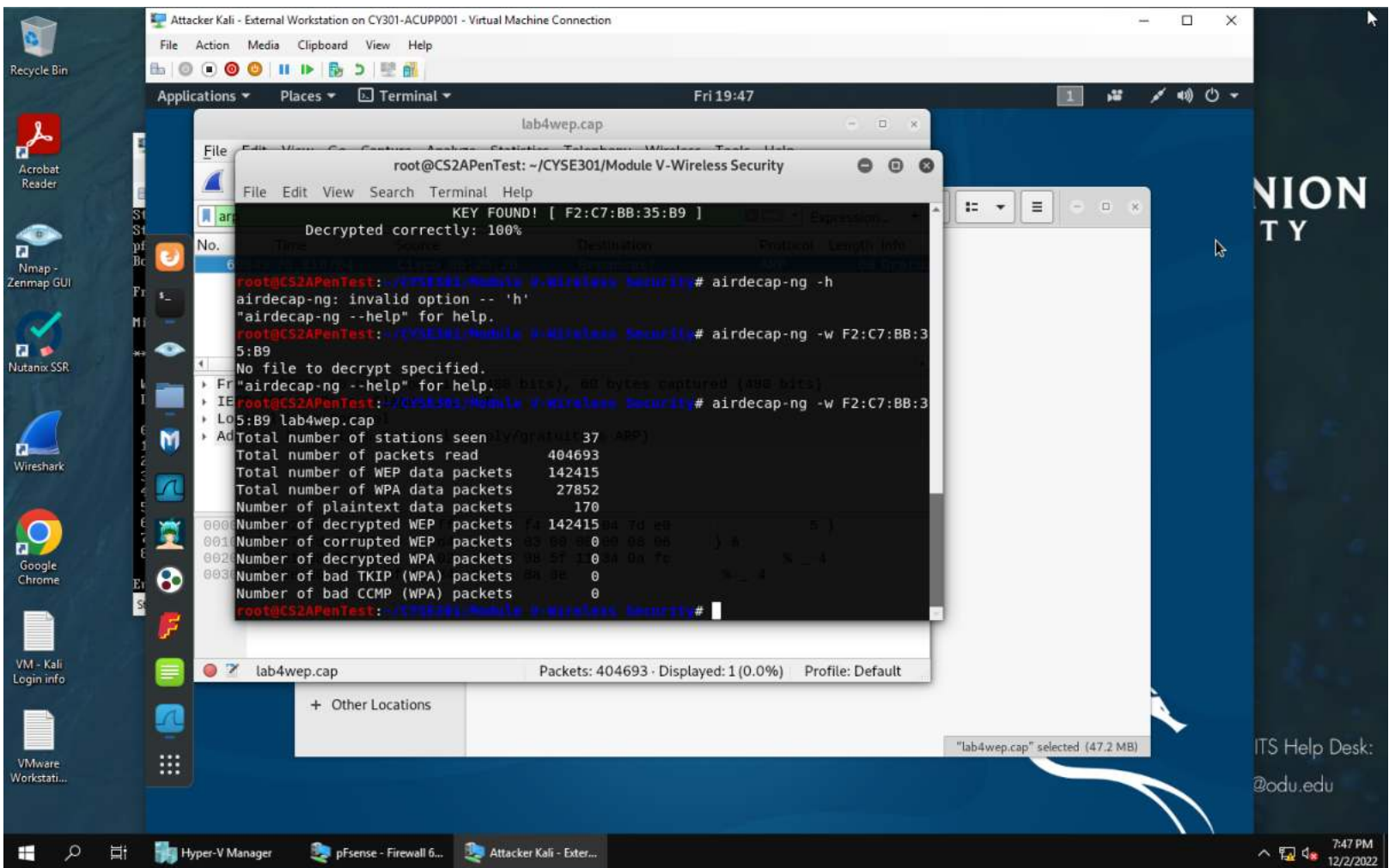
Hyper-V Manager pfsense - Firewall 6... Attacker Kali - Ext...

4:47 PM 12/1/2022

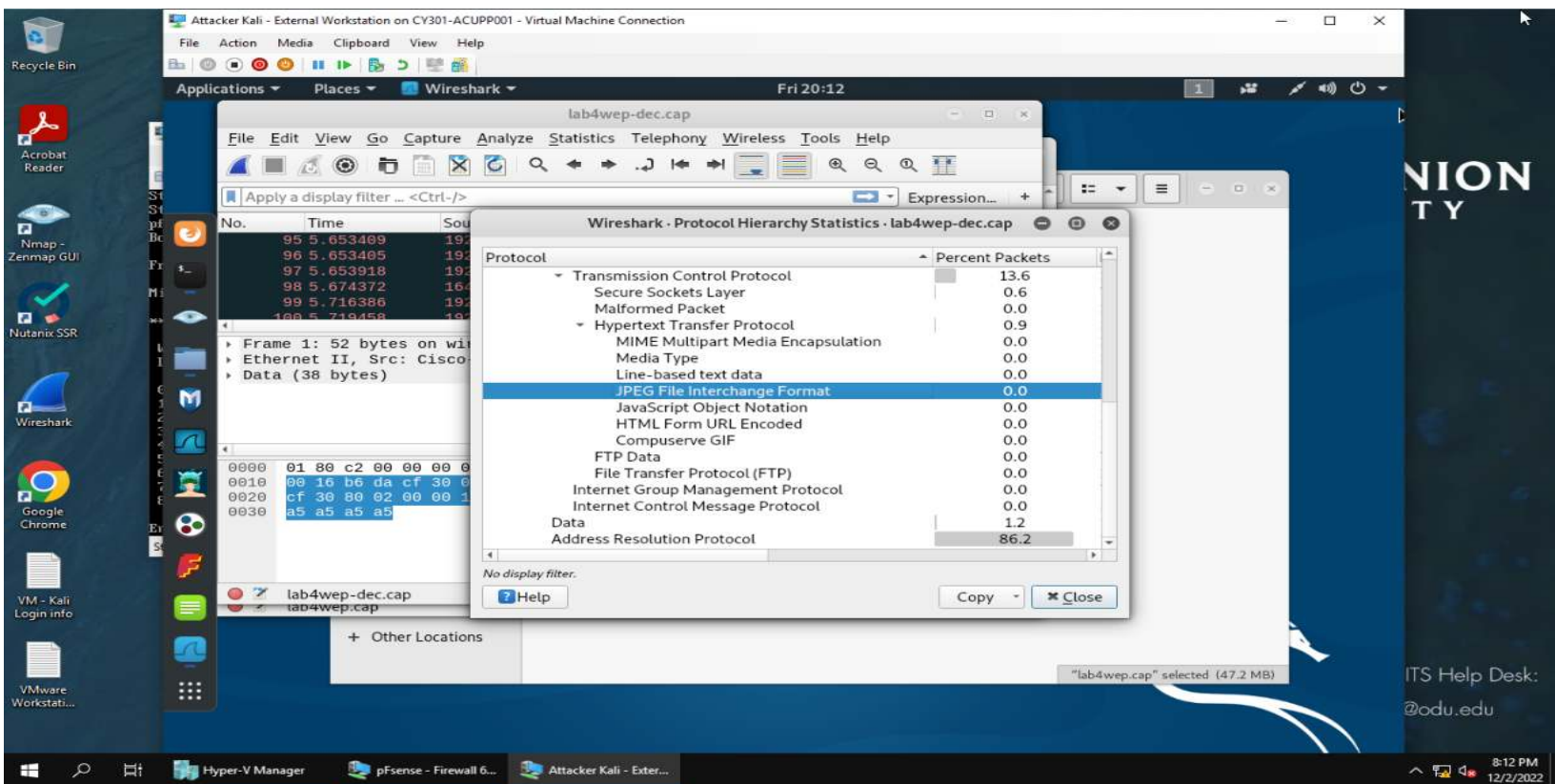
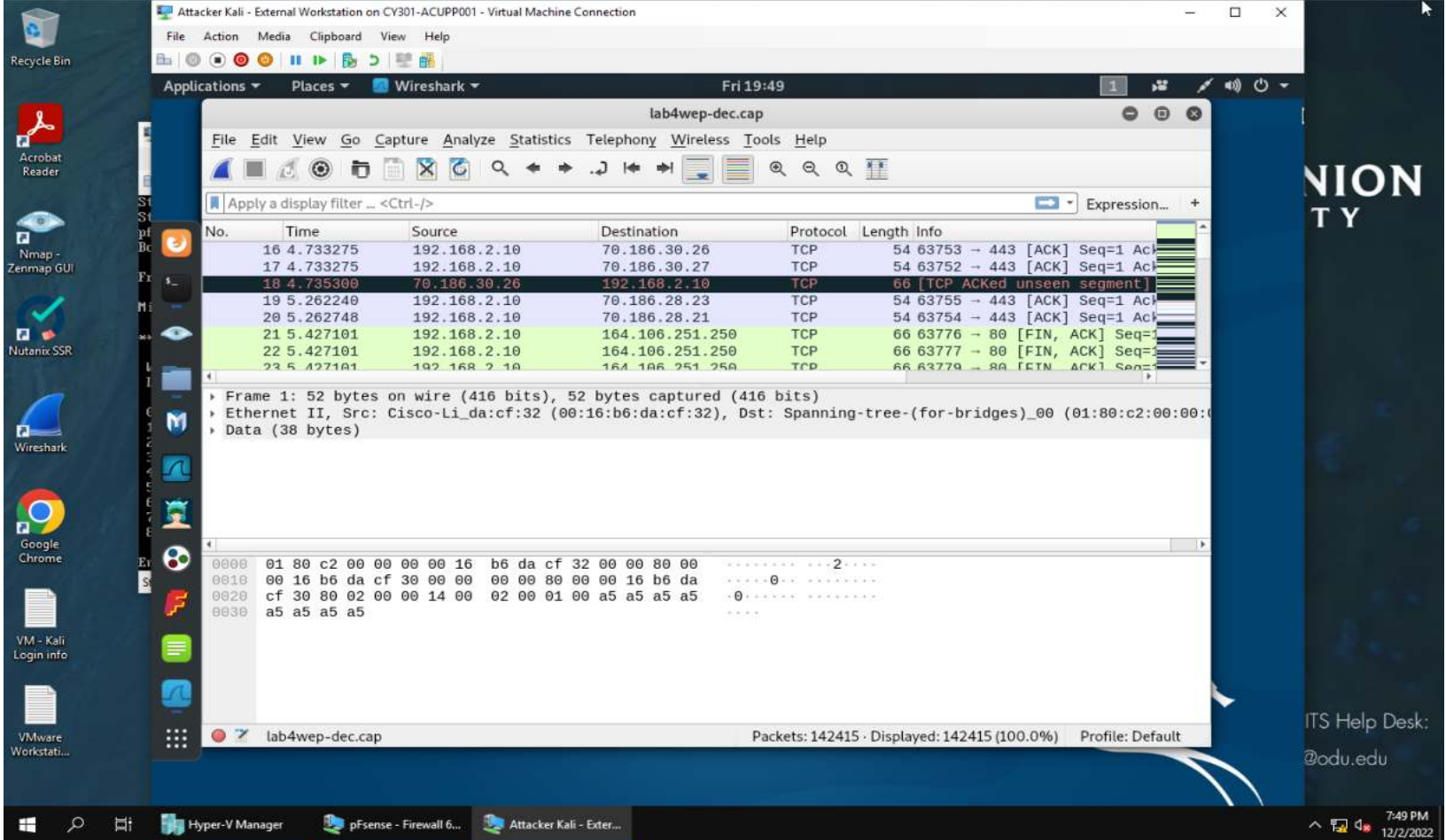
A1. Traffic and heirarchy of lab4wep.cap before decryption



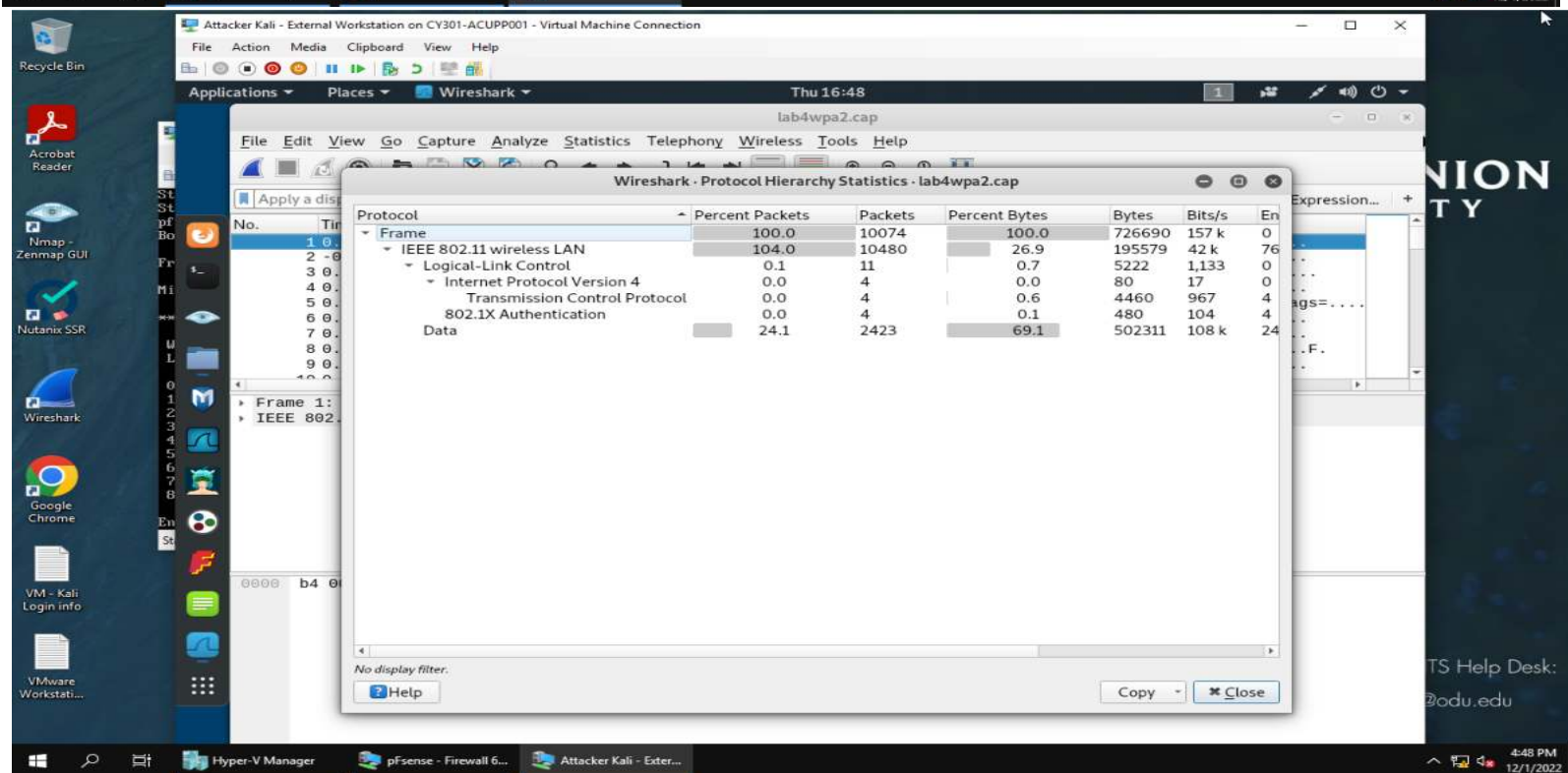
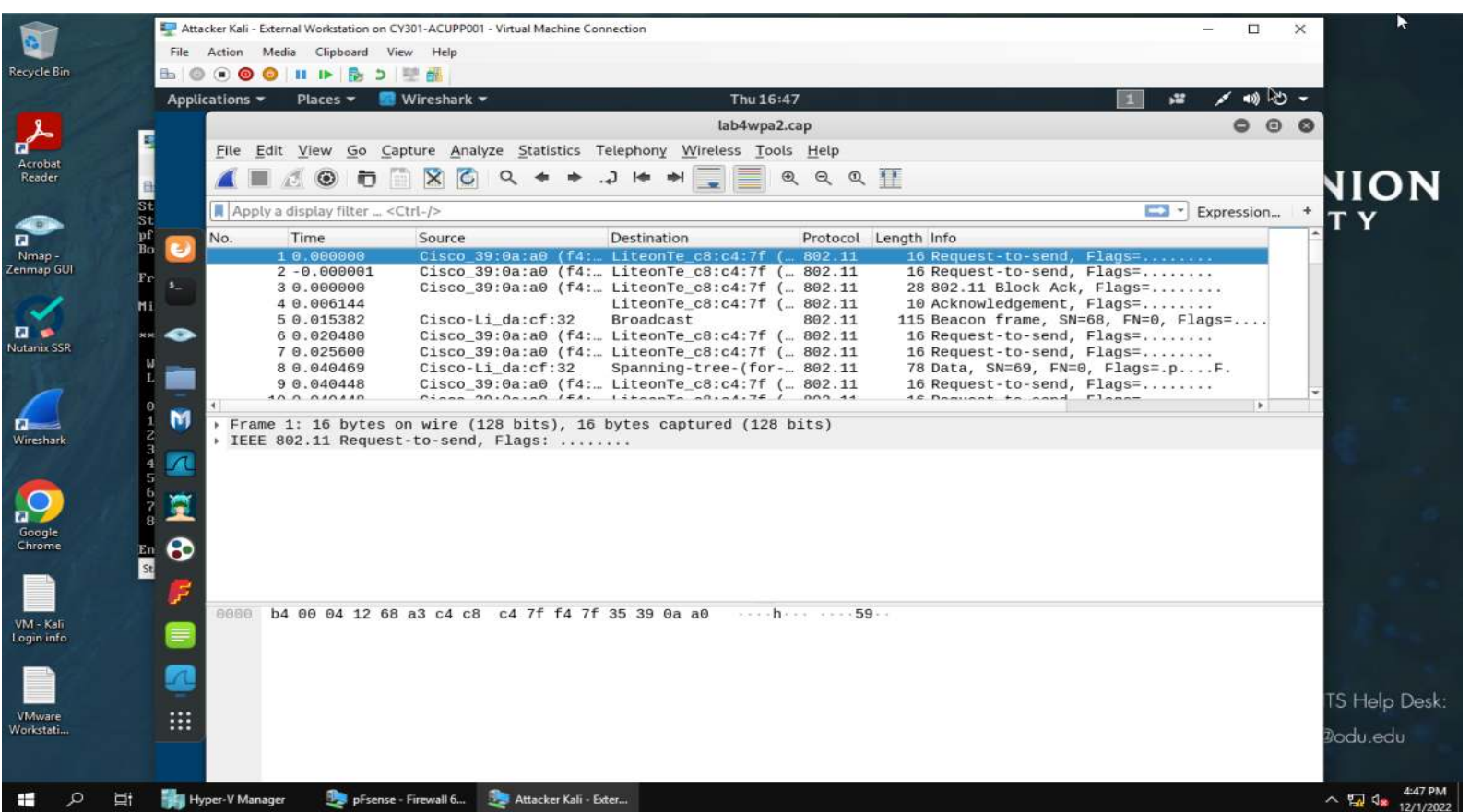
A1. The file is decrypted



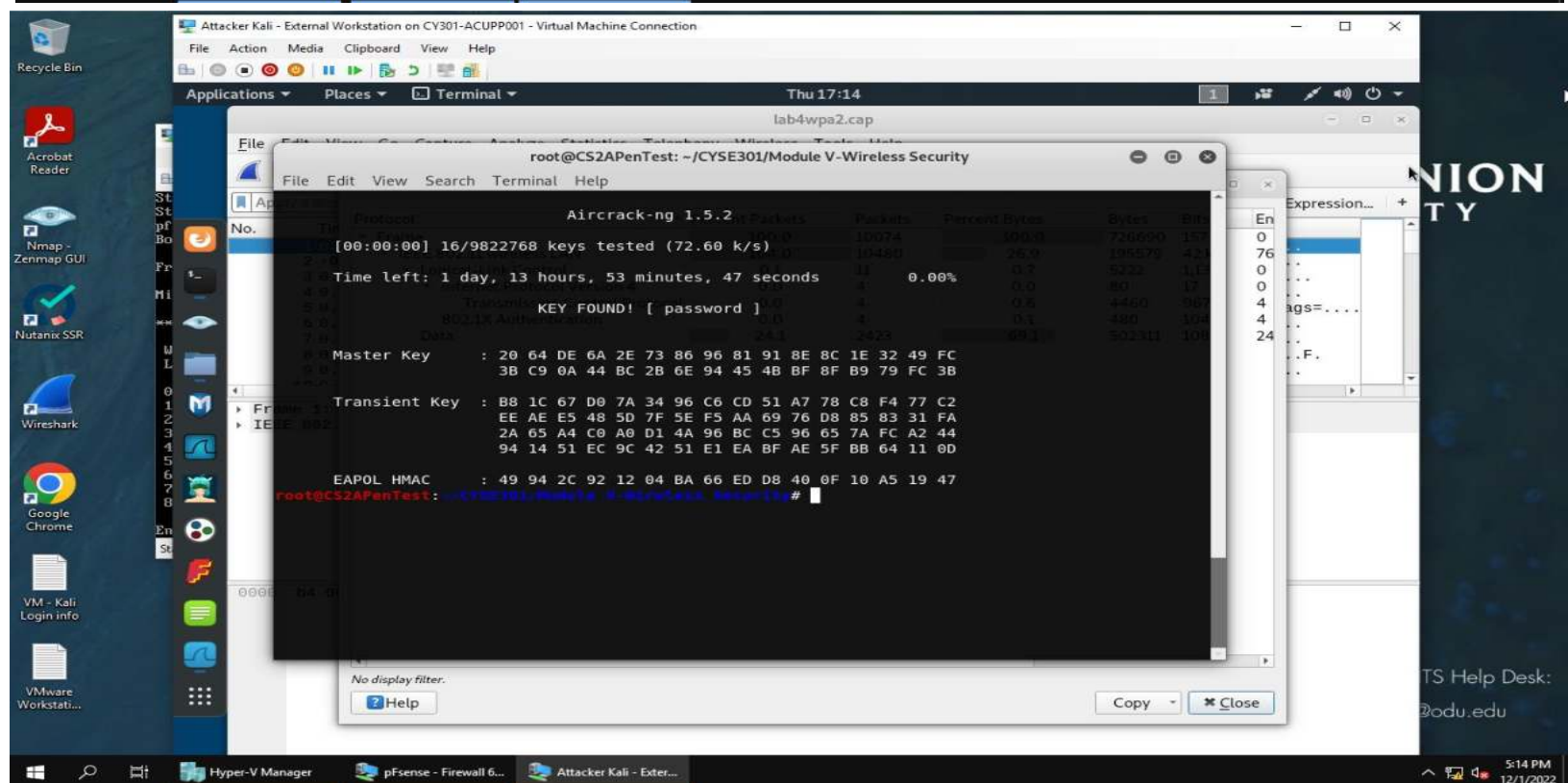
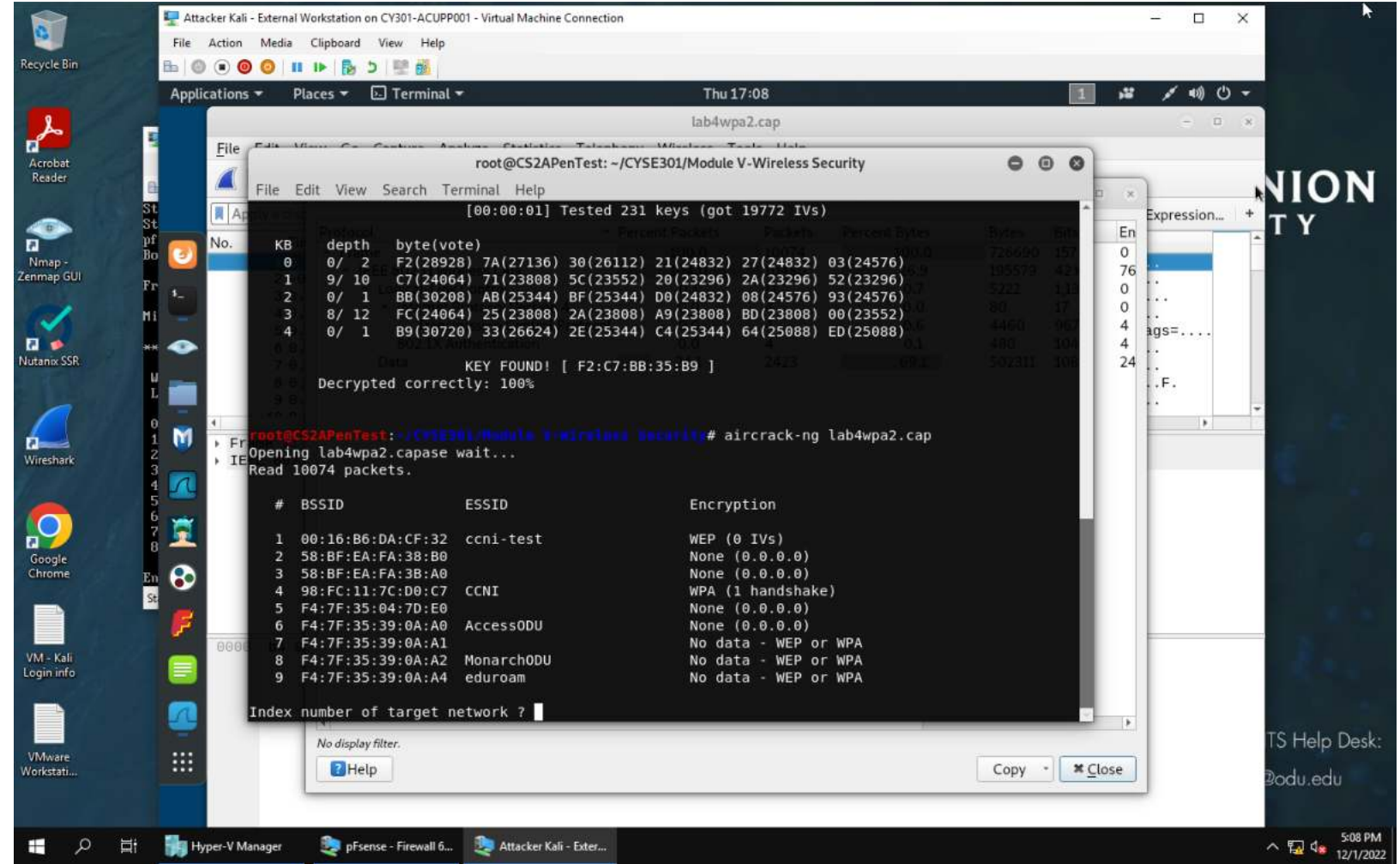
A1. The key is used to prove decryption



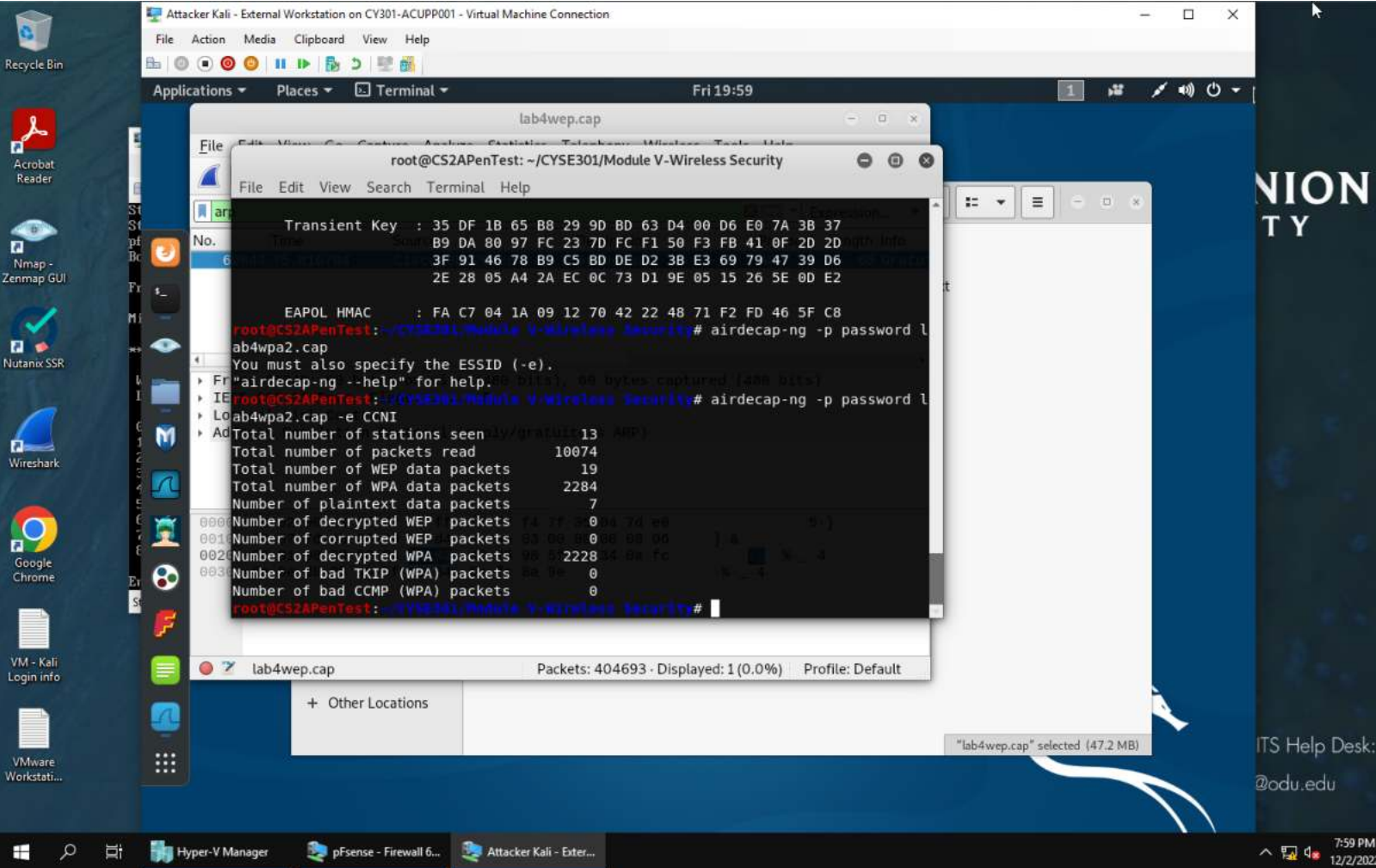
A1. There are a large number of ARP packets present for ARP broadcasts to discover the address.



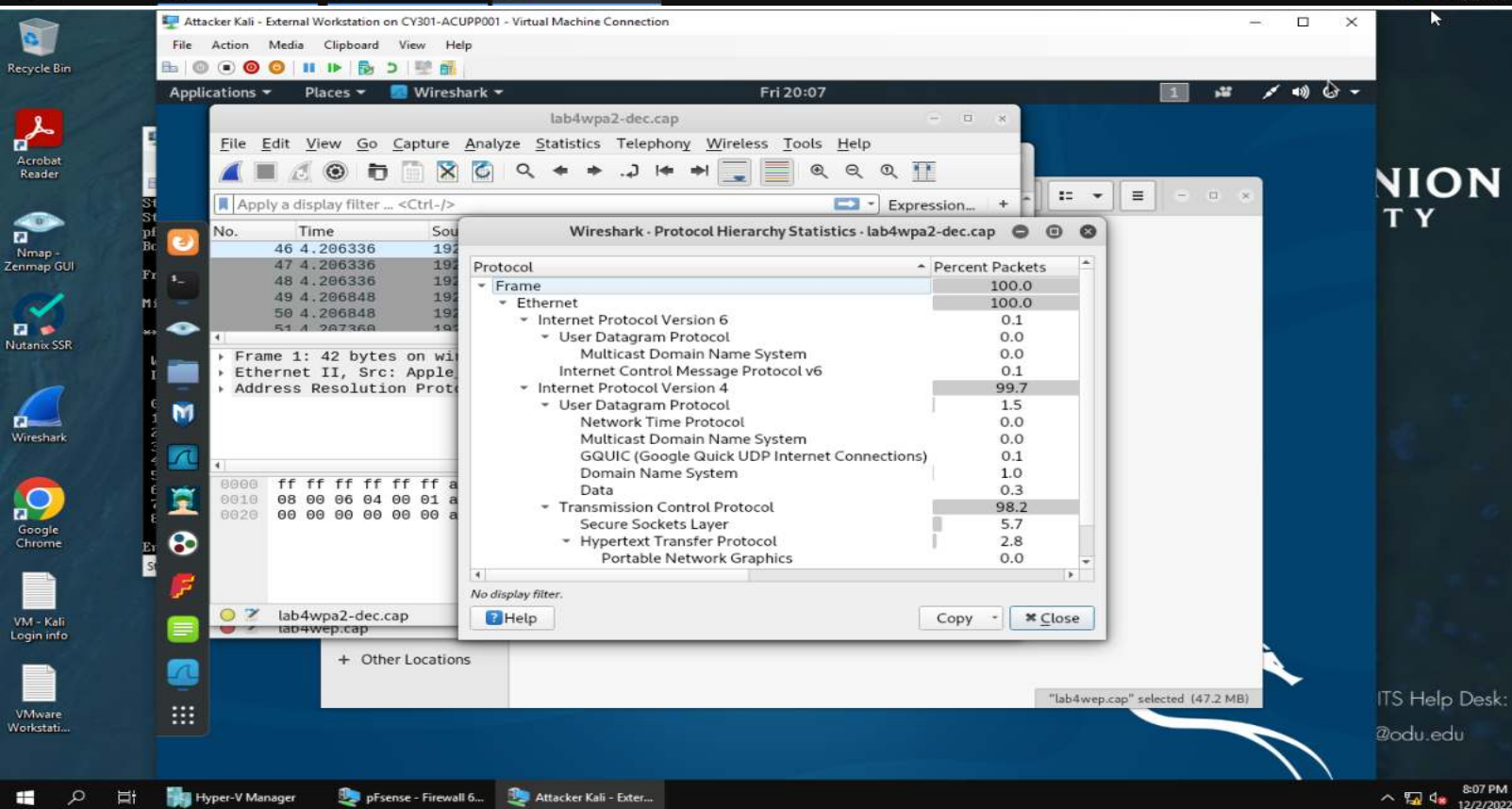
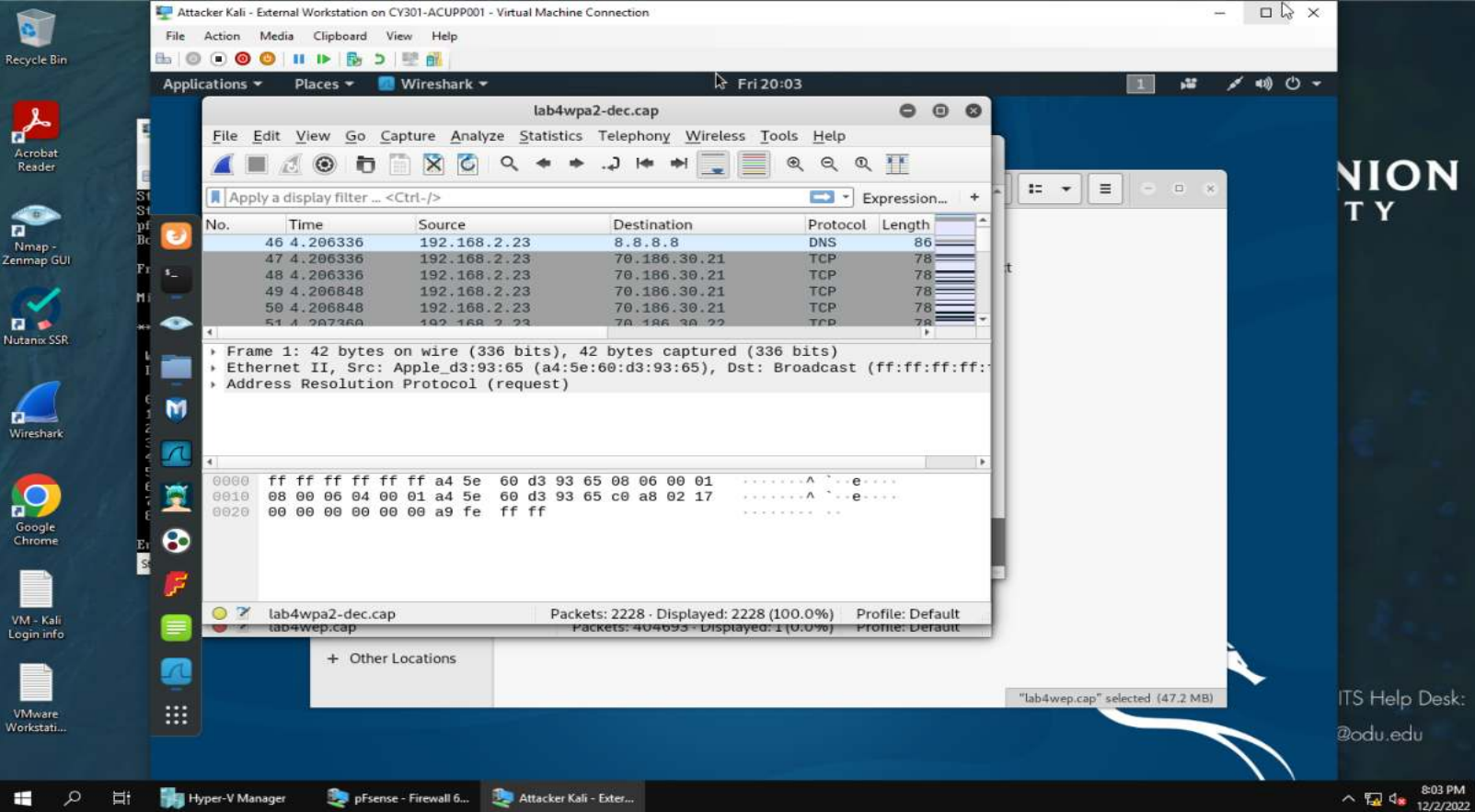
A2. Traffic and hierarchy of lab4wpa2.cap before decryption



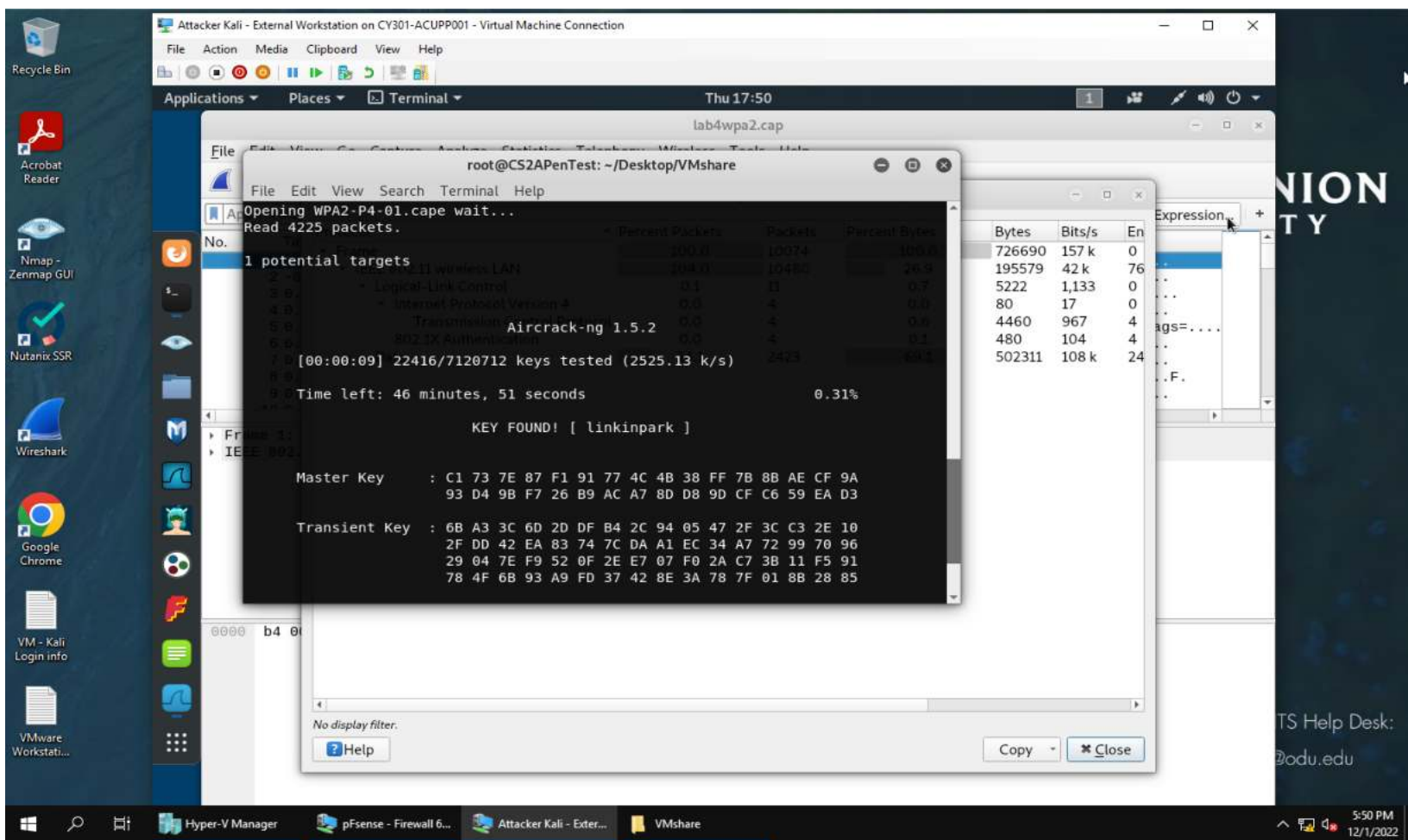
A2. The file is decrypted



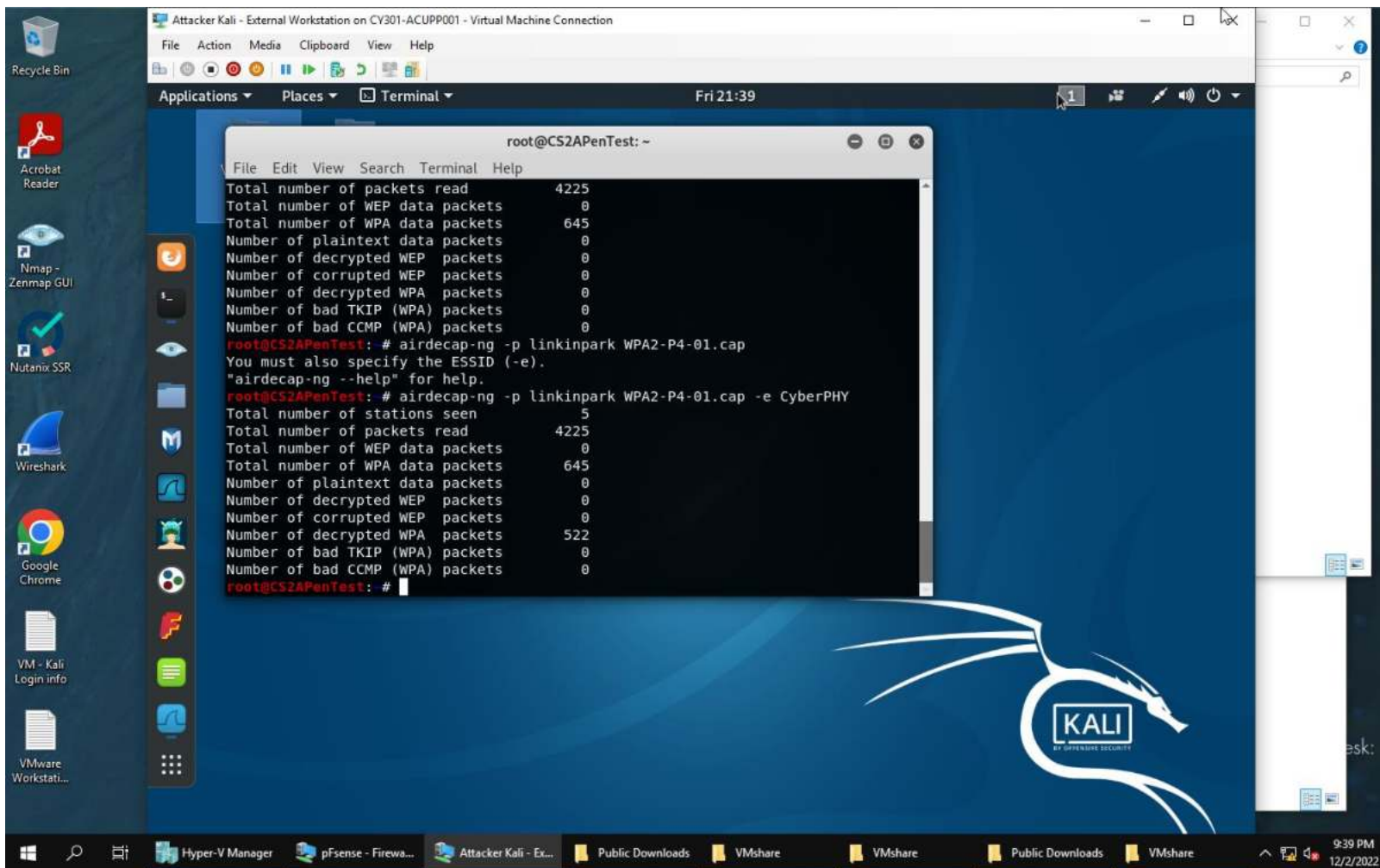
A2. The key is used to prove decryption, screenshot shows commands used



A2. There are a large number of TCP packets present appearing to be a syn-ack flood.



B1. A dictionary attack is implemented, and the password is found, linkinpark



B2. The key is used to prove decryption, screenshot shows command

Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places Wireshark Fri 21:41

WPA2-P4-01-dec.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length
1	0.000000	0.0.0.0	255.255.255.255	DHCP	356
2	0.011265	0.0.0.0	255.255.255.255	DHCP	368
3	0.641104	42.62.94.2	192.168.1.127	TCP	217
4	1.610888	192.168.1.1	192.168.1.127	DNS	164
5	1.621128	192.168.1.1	192.168.1.127	DNS	168
6	1.731728	66.198.24.243	192.168.1.127	TCP	54

Frame 1: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits)
Ethernet II, Src: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Discover)

0000 ff ff ff ff ff ff 00 9a cd b8 3d 23 08 00 45 10E.
0010 01 56 00 00 40 00 00 39 88 00 00 00 00 ff ff -V-@-@-9-
0020 ff ff 00 44 00 00 43 01 42 fe c7 01 01 06 00 20 56 -D-C-B-V
0030 4b d5 00 00 00 00 00 00 00 00 00 00 00 00 00 K-
0040 00 00 00 00 00 00 00 00 9a cd b8 3d 23 08 00 00 00E.
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
WPA2-P4-01-dec.cap Packets: 522 - Displayed: 522 (100.0%) Profile: Default

9:41 PM 12/2/2022

Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places Wireshark Fri 21:42

WPA2-P4-01-dec.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length
1	0.000000	0.0.0.0	255.255.255.255	DHCP	356
2	0.011265	0.0.0.0	255.255.255.255	DHCP	368
3	0.641104	42.62.94.2	192.168.1.127	TCP	217
4	1.610888	192.168.1.1	192.168.1.127	DNS	164
5	1.621128	192.168.1.1	192.168.1.127	DNS	168
6	1.731728	66.198.24.243	192.168.1.127	TCP	54

Frame 1: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits)
Ethernet II, Src: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Discover)

0000 ff ff ff ff ff ff 00 9a cd b8 3d 23 08 00 45 10E.
0010 01 56 00 00 40 00 00 39 88 00 00 00 00 ff ff -V-@-@-9-
0020 ff ff 00 44 00 00 43 01 42 fe c7 01 01 06 00 20 56 -D-C-B-V
0030 4b d5 00 00 00 00 00 00 00 00 00 00 00 00 00 K-
0040 00 00 00 00 00 00 00 00 9a cd b8 3d 23 08 00 00 00E.
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
WPA2-P4-01-dec.cap Packets: 522 - Displayed: 522 (100.0%) Profile: Default

Wireshark - Protocol Hierarchy Statistics - WPA2-P4-01-dec.cap

Protocol	Percent Packets
Frame	100.0
Ethernet	100.0
Internet Protocol Version 4	100.0
User Datagram Protocol	29.7
QUIC (Google Quick UDP Internet Connections)	0.6
Domain Name System	4.4
Data	24.3
Bootstrap Protocol	0.4
Transmission Control Protocol	69.9
X11	0.2
Malformed Packet	0.2
Secure Sockets Layer	10.2
MSN Messenger Service	10.9
Hypertext Transfer Protocol	1.1
MP4 / ISOBMFF file format	0.2
JavaScript Object Notation	0.4
Data	1.3
Internet Control Message Protocol	0.4

No display filter.

Help Copy Close

9:42 PM 12/2/2022

B2. We have a large % of the traffic is UDP or TCP packets as presented in the hierarchy for WPA2-P4-01-dec.cap.

