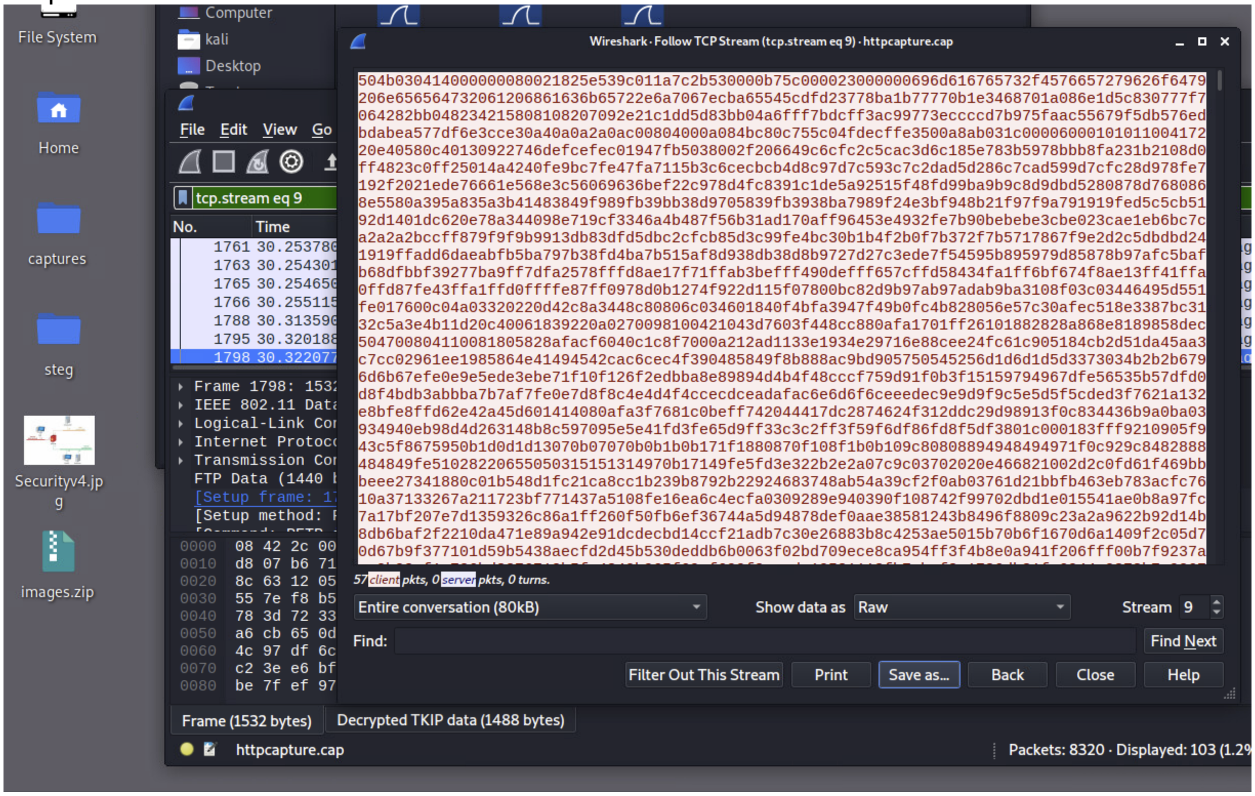
Peter Sanford
IT 2700
NetLab Lab 18
12/4/2023

1.1.2
Step 6:



tcp.stream eq 9

```
No.   Time
 1761 30.253780
 1763 30.254301
 1765 30.254650
 1766 30.255115
 1788 30.313590
 1795 30.320188
 1798 30.322077

Frame 1798: 1532
IEEE 802.11 Data
Logical-Link Cor
Internet Protoco
Transmission Cor
FTP Data (1440 b
[Setup frame: 17
[Setup method: F

0000  08 42 2c 00
0010  d8 07 b6 71
0020  8c 63 12 05
0030  55 7e f8 b5
0040  78 3d 72 33
0050  a6 cb 65 0d
0060  4c 97 df 6c
0070  c2 3e e6 bf
0080  be 7f ef 97
```

```
504b0304140000000080021825e539c011a7c2b530000b75c000023000000696d616765732f4576657279626f6479
206e6565647320612068616 36b65722e6a7067ecba65545cdfd23778ba1b77770b1e3468701a086e1d5c830777f7
064282bb048234215808108207092e21c1dd5d83bb04a6fff7bdcff3ac99773eccccd7b975faac55679f5db576ed
bdabea577df6e3cce30a40a0a2a0ac00804000a084bc80c755c04fdecffe3500a8ab031c00006000101011004172
20e40580c40130922746defcefec01947fb5038002f206649c6cfc2c5cac3d6c185e783b5978bbb8fa231b2108d0
ff4823c0ff25014a4240fe9bc7fe47fa7115b3c6cecbcb4d8c97d7c593c7c2dad5d286c7cad599d7cfc28d978fe7
192f2021ede76661e568e3c56069636bef22c978d4fc8391c1de5a92515f48fd99ba9b9c8d9dbd5280878d768086
8e5580a395a835a3b41483849f989fb39bb38d9705839fb3938ba7989f24e3bf948b21f97f9a791919fed5c5cb51
92d1401dc620e78a344098e719cf3346a4b487f56b31ad170aff96453e4932fe7b90bebebe3cbe023cae1eb6bc7c
a2a2a2bccff879f9f9b9913db83dfd5dbc2cfcb85d3c99fe4bc30b1b4f2b0f7b372f7b5717867f9e2d2c5dbdbd24
1919ffadd6daeabfb5ba797b38fd4ba7b515af8d938db38d8b9727d27c3ede7f54595b895979d85878b97afc5baf
b68dfbbf39277ba9ff7dfa2578fffd8ae17f71ffab3befff490defff657cffd58434fa1ff6bf674f8ae13ff41ffa
0ffd87fe43ffa1ffd0ffffe87ff0978d0b1274f922d115f07800bc82d9b97ab97adab9ba3108f03c03446495d551
fe017600c04a03320220d42c8a3448c80806c034601840f4bfa3947f49b0fc4b828056e57c30afec518e3387bc31
32c5a3e4b11d20c40061839220a02700981004210 43d7603f448cc880afa1701ff26101882828a868e8189858dec
504700804110081805828afacf6040c1c8f7000a212ad1133e1934e29716e88cee24fc61c905184cb2d51da45aa3
c7cc02961ee1985864e41494542cac6cec4f390485849f8b888ac9bd905750545256d1d6d1d5d3373034b2b2b679
6d6b67efe0e9e5ede3ebe71f10f126f2edbba8e89894d4b4f48cccf759d91f0b3f15159794967dfe56535b57dfd0
d8f4bdb3abbba7b7af7fe0e7d8f8c4e4d4f4ccecdceadafac6e6d6f6ceeedec9e9d9f9c5e5d5f5cded3f7621a132
e8bfe8ffd62e42a45d601414080afa3f7681c0beff742044417dc2874624f312ddc29d98913f0c834436b9a0ba03
934940eb98d4d263148b8c597095e5e41fd3fe65d9ff33c3c2ff3f59f6df86fd8f5df3801c000183fff9210905f9
43c5f8675950b1d0d1d13070b07070b0b1b0b171f1880870f108f1b0b109c80808894948494971f0c929c8482888
484849fe51028220655050315151314970b17149fe5fd3e322b2e2a07c9c03702020e466821002d2c0fd61f469bb
beee27341880c01b548d1fc21ca8cc1b239b8792b22924683748ab54a39cf2f0ab03761d21bbfb463eb783acfc76
10a37133267a211723bf771437a5108fe16ea6c4ecfa0309289e940390f108742f99702dbd1e015541ae0b8a97fc
7a17bf207e7d1359326c86a1ff260f50fb6ef36744a5d94878def0aae38581243b8496f8809c23a2a9622b92d14b
8db6baf2f2210da471e89a942e91dcdecbd14ccf21adb7c30e26883b8c4253ae5015b70b6f1670d6a1409f2c05d7
0d67b9f377101d59b5438aecfd2d45b530deddb6b0063f02bd709ece8ca954ff3f4b8e0a941f206fff00b7f9237a
```

57 client pkts, 0 server pkts, 0 turns.

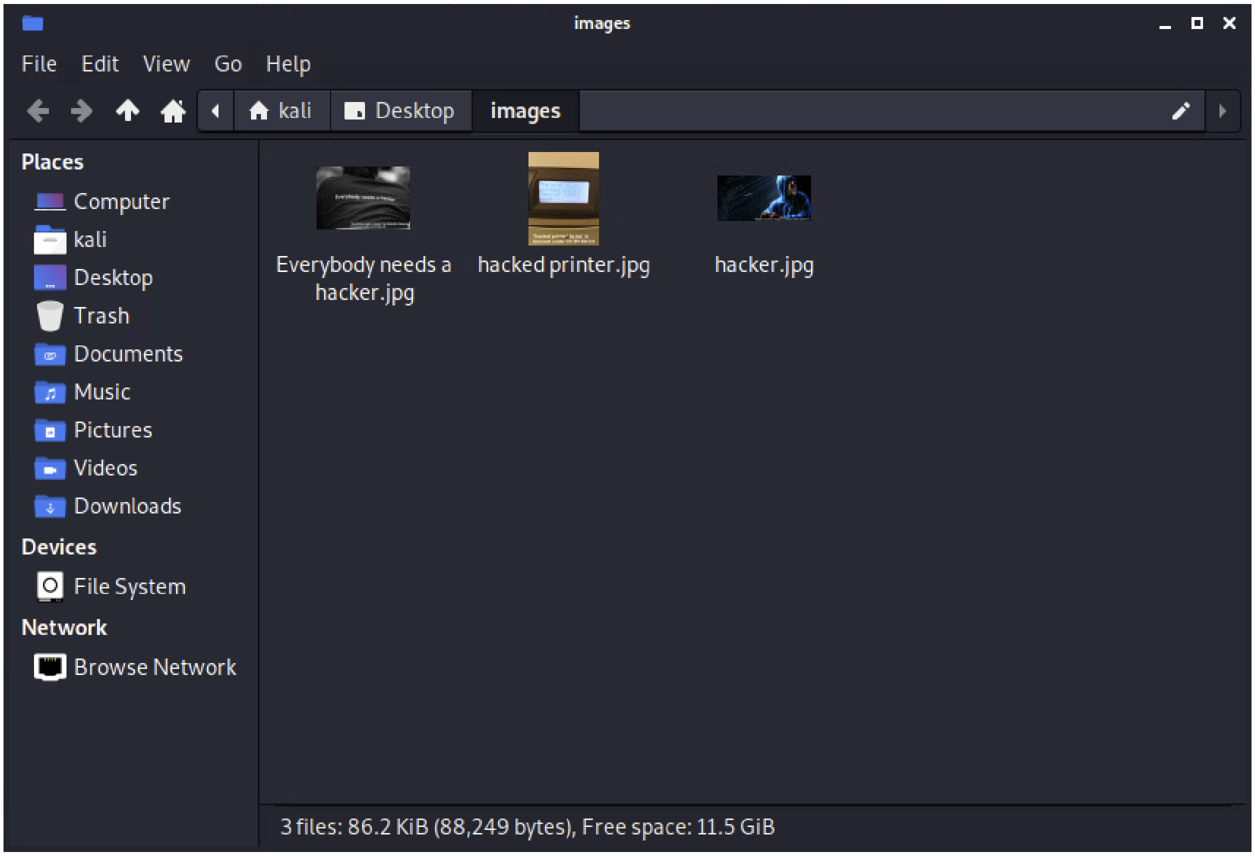
Entire conversation (80kB)   Show data as Raw   Stream 9

Find:

Frame (1532 bytes)   Decrypted TKIP data (1488 bytes)

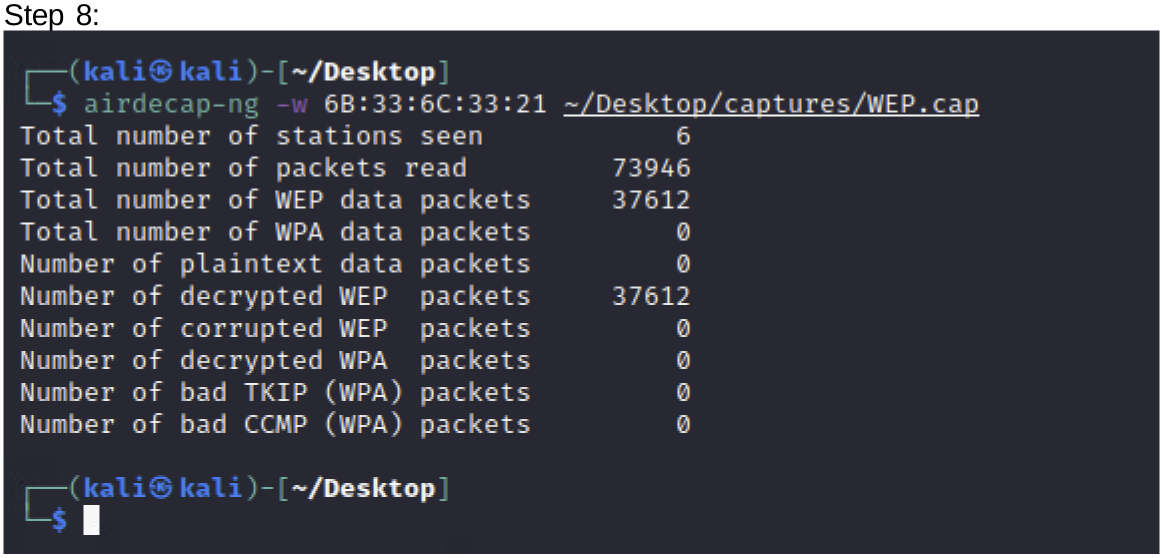
httpcapture.cap   Packets: 8320 · Displayed: 103 (1.2%

Step 10:



3 files: 86.2 KiB (88,249 bytes), Free space: 11.5 GiB

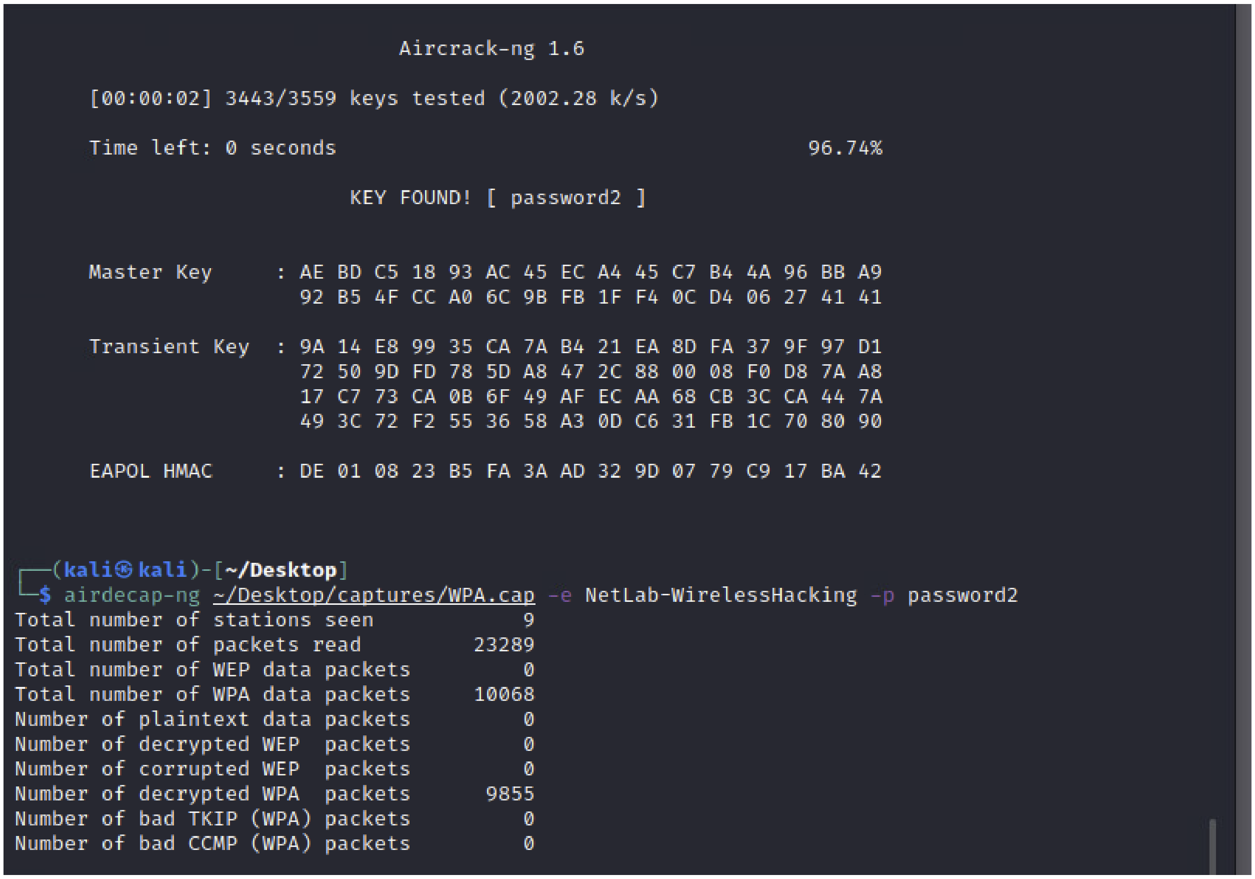
2.1
Step 8:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ airdecap-ng -w 6B:33:6C:33:21 ~/Desktop/captures/WEP.cap
Total number of stations seen            6
Total number of packets read         73946
Total number of WEP data packets     37612
Total number of WPA data packets         0
Number of plaintext data packets         0
Number of decrypted WEP  packets     37612
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

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

3.1
Step 5:



```
                          Aircrack-ng 1.6

      [00:00:02] 3443/3559 keys tested (2002.28 k/s)

      Time left: 0 seconds                                      96.74%

                      KEY FOUND! [ password2 ]


      Master Key     : AE BD C5 18 93 AC 45 EC A4 45 C7 B4 4A 96 BB A9
                       92 B5 4F CC A0 6C 9B FB 1F F4 0C D4 06 27 41 41

      Transient Key  : 9A 14 E8 99 35 CA 7A B4 21 EA 8D FA 37 9F 97 D1
                       72 50 9D FD 78 5D A8 47 2C 88 00 08 F0 D8 7A A8
                       17 C7 73 CA 0B 6F 49 AF EC AA 68 CB 3C CA 44 7A
                       49 3C 72 F2 55 36 58 A3 0D C6 31 FB 1C 70 80 90

      EAPOL HMAC     : DE 01 08 23 B5 FA 3A AD 32 9D 07 79 C9 17 BA 42


┌──(kali㉿kali)-[~/Desktop]
└─$ airdecap-ng ~/Desktop/captures/WPA.cap -e NetLab-WirelessHacking -p password2
Total number of stations seen            9
Total number of packets read         23289
Total number of WEP data packets         0
Total number of WPA data packets     10068
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      9855
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
```

Commentary:

In this lab we explored Aircrack-ng to decrypt and crack both WPA and WEP encrypted wireless packets. I learned that this tool is powerful and shows how quickly you can intercept and look at encrypted traffic if not secured correctly. Companies can use this information to update their wireless communication encryption to make it more difficult to encrypt and read sensitive information.