Lab 12 - Breaking WEP and WPA and Decrypting the Traffic

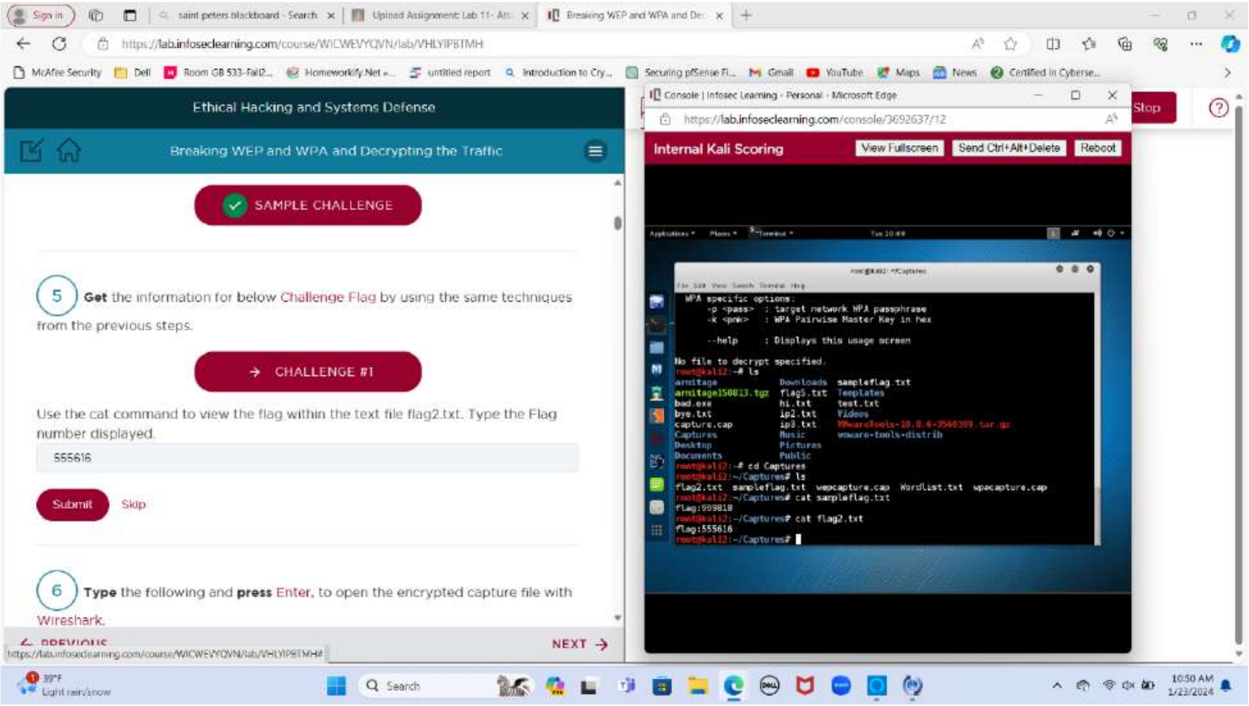
Objective:

1. Viewing Wireless Networks and Connected Devices
2. Cracking WEP
3. Cracking WPA

Takeaways:

1. “Aircrack-ng” is a network security tool available in Kali Linux used for assessing and cracking wireless security protocols.
2. “Airmon-ng” is a command-line utility in Kali Linux that is used for enabling and disabling monitor mode on wireless interfaces, allowing for wireless network monitoring and analysis.
3. “Airdecap-ng” is a tool in Kali Linux used for decrypting and decapsulating encrypted wireless network traffic captured using tools like “Airodump-ng”.
4. To decrypt a WPA packet capture in Kali Linux, you can use tools like “Aircrack-ng”, specifying the captured file and providing the correct WPA passphrase for the targeted network.

Challenges:



Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

SAMPLE CHALLENGE

5 **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

→ CHALLENGE #1

Use the cat command to view the flag within the text file flag2.txt. Type the Flag number displayed.

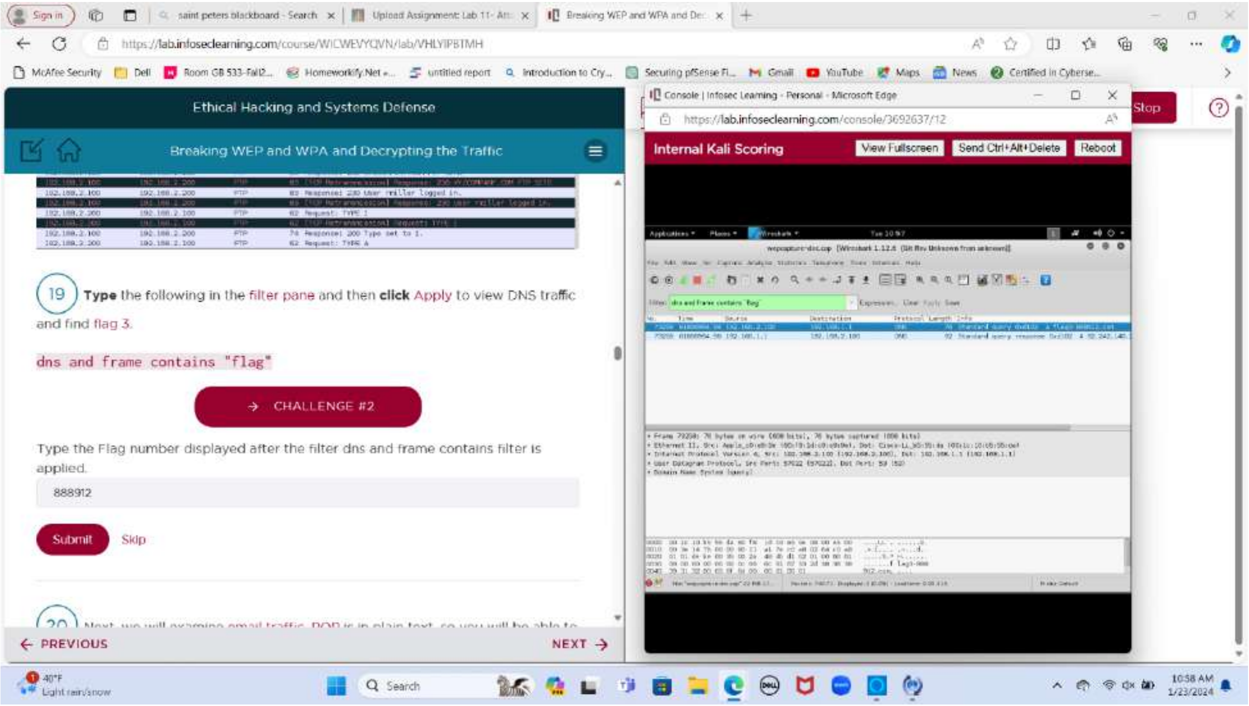
555616

Submit Skip

6 **Type** the following and **press** Enter, to open the encrypted capture file with Wireshark.

Internal Kali Scoring

```
 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.
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
root@kali2:~# cd Captures
root@kali2:~/Captures# ls
flag2.txt  sampleflag.txt  wepcapture.cap  Wordlist.txt  wpacapture.cap
root@kali2:~/Captures# cat sampleflag.txt
flag:999818
root@kali2:~/Captures# cat flag2.txt
flag:555616
root@kali2:~/Captures# 
```



Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

19 **Type** the following in the filter pane and then **click** Apply to view DNS traffic and find flag 3.

```
dns and frame contains "flag"
```

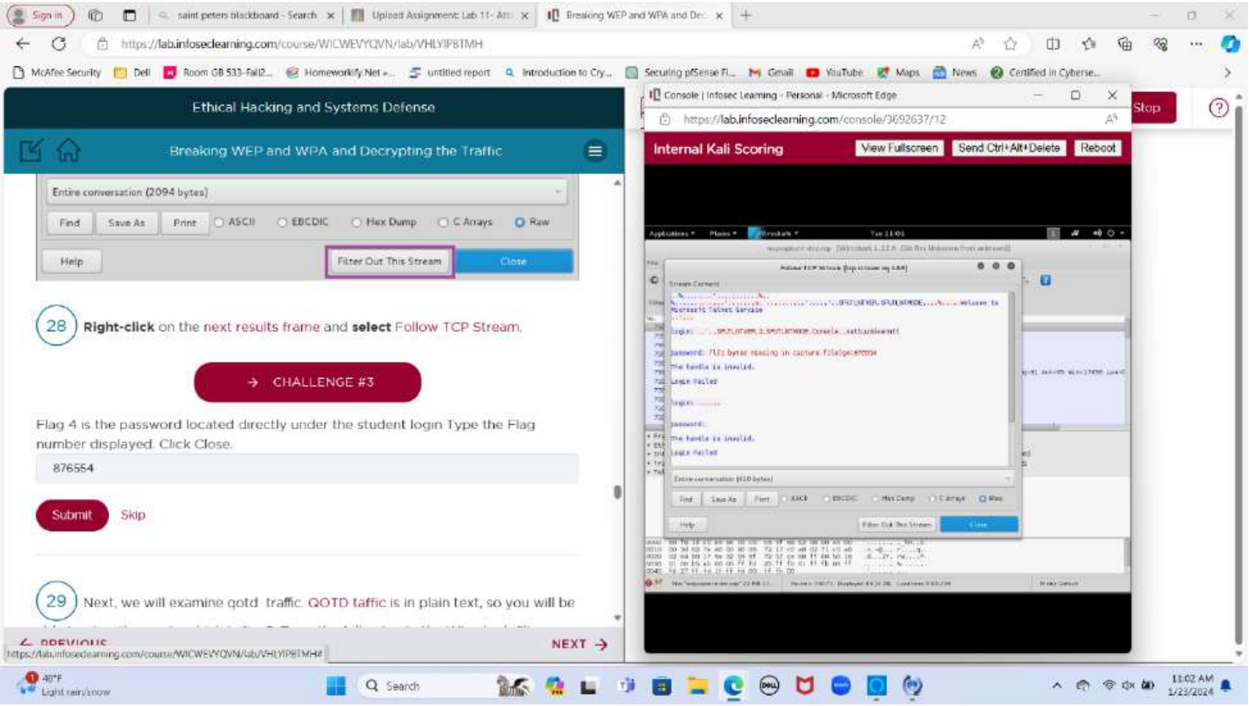
→ CHALLENGE #2

Type the Flag number displayed after the filter dns and frame contains filter is applied.

888912

Submit Skip

Internal Kali Scoring



Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

Entire conversation (2094 bytes)

Find | Save As | Print | ○ ASCII | ○ EBCDIC | ○ Hex Dump | ○ C Arrays | ● Raw

Help | Filter Out This Stream | Close

28 **Right-click** on the next results frame and **select** Follow TCP Stream.

→ CHALLENGE #3

Flag 4 is the password located directly under the student login Type the Flag number displayed. Click Close.

876554

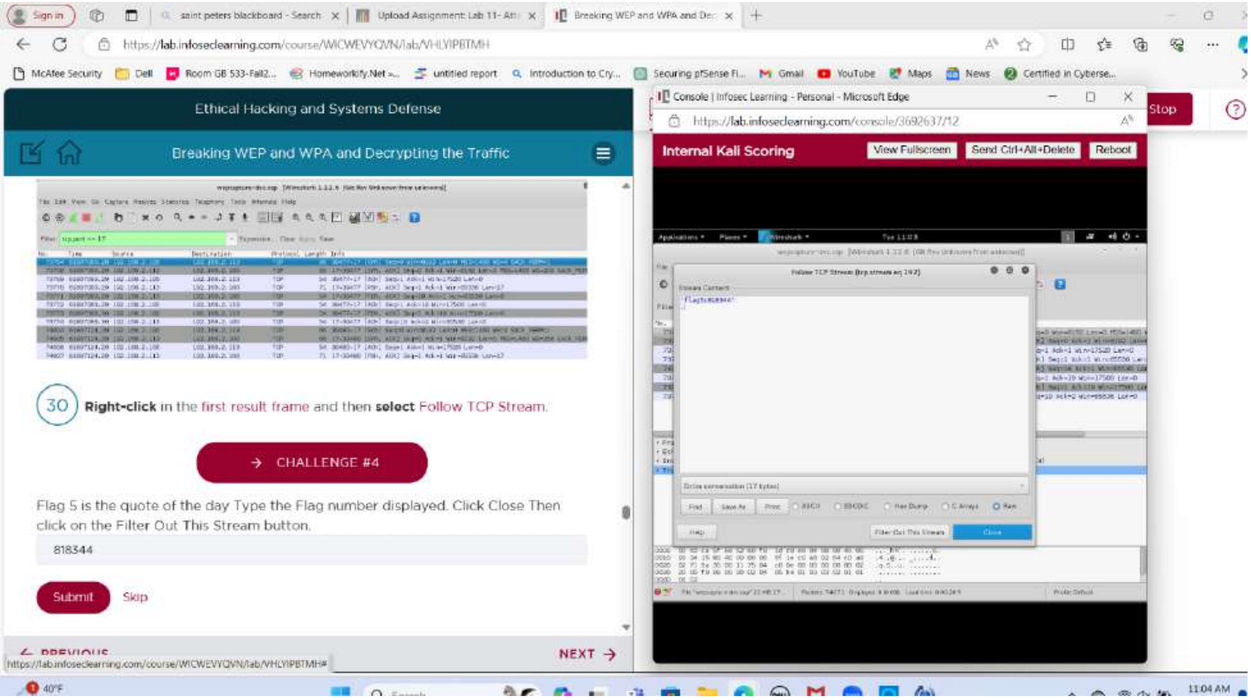
Submit Skip

29 Next, we will examine qotd traffic. QOTD taffic is in plain text, so you will be

← PREVIOUS NEXT →

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH#

```
..%..........'...........%..
%.................'...........'.....'..SFUTLNTVER.SFUTLNTMODE,...%....Welcome to
Microsoft Telnet Service
..'...
login: ..'...SFUTLNTVER.2.SFUTLNTMODE.Console..student
password: [115 bytes missing in capture file]ge:876554
The handle is invalid.
Login Failed
login: ......
password:
The handle is invalid.
Login Failed
```


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and Dec
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
McAfee Security
Dell
Room GB 533-Fall2...
Homeworkify.Net -...
untitled report
Introduction to Cry...
Securing pfSense Fi...
Gmail
YouTube
Maps
News
Certified in Cyberse...
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Stop
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications ▾
Places ▾
Wireshark ▾
Tue 11:03
Follow TCP Stream (tcp.stream eq 192)
Stream Content
Entire conversation (17 bytes)
Find
Save As
Print
○ ASCII
○ EBCDIC
○ Hex Dump
○ C Arrays
● Raw
Help
Filter Out This Stream
Close
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port == 17
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
40°F
11:04 AM

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

30 **Right-click** in the first result frame and then **select** Follow TCP Stream.

→ CHALLENGE #4

Flag 5 is the quote of the day Type the Flag number displayed. Click Close Then click on the Filter Out This Stream button.

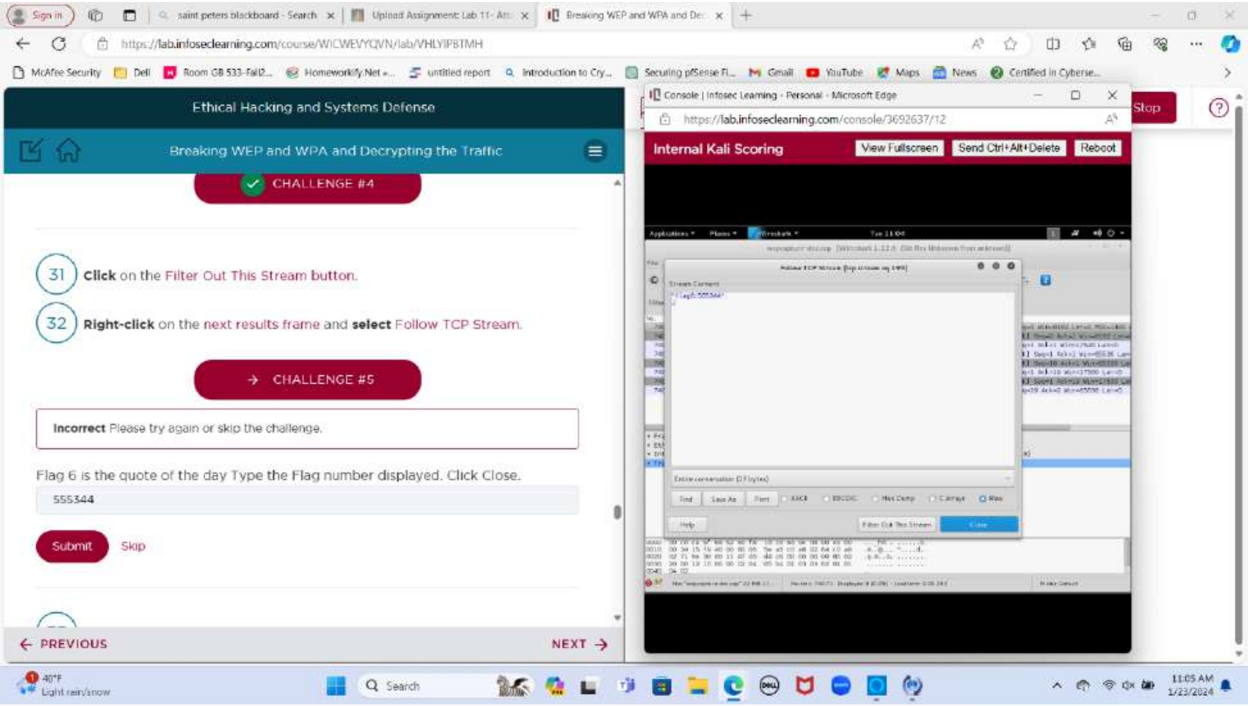
818344

Submit Skip

← PREVIOUS NEXT →

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH#

```
"flag5:818344"
```



31 **Click** on the Filter Out This Stream button.

32 **Right-click** on the next results frame and **select** Follow TCP Stream.

→ CHALLENGE #5

Incorrect Please try again or skip the challenge.

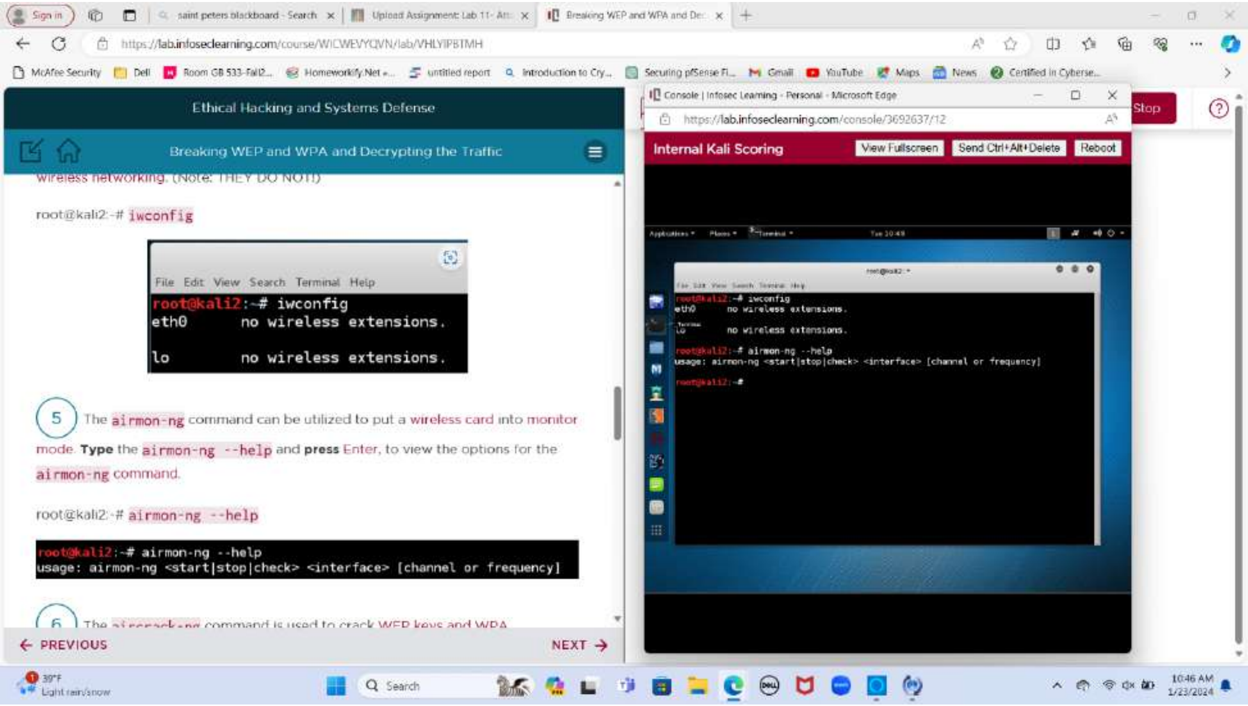
Flag 6 is the quote of the day Type the Flag number displayed. Click Close.

555344

Submit Skip

```
flag6:555344
```

Screenshots:


Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
File Edit View Search Terminal Help
← PREVIOUS
NEXT →

wireless networking. (Note: THEY DO NOT!)

root@kali2:~# iwconfig

```
root@kali2:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.
```

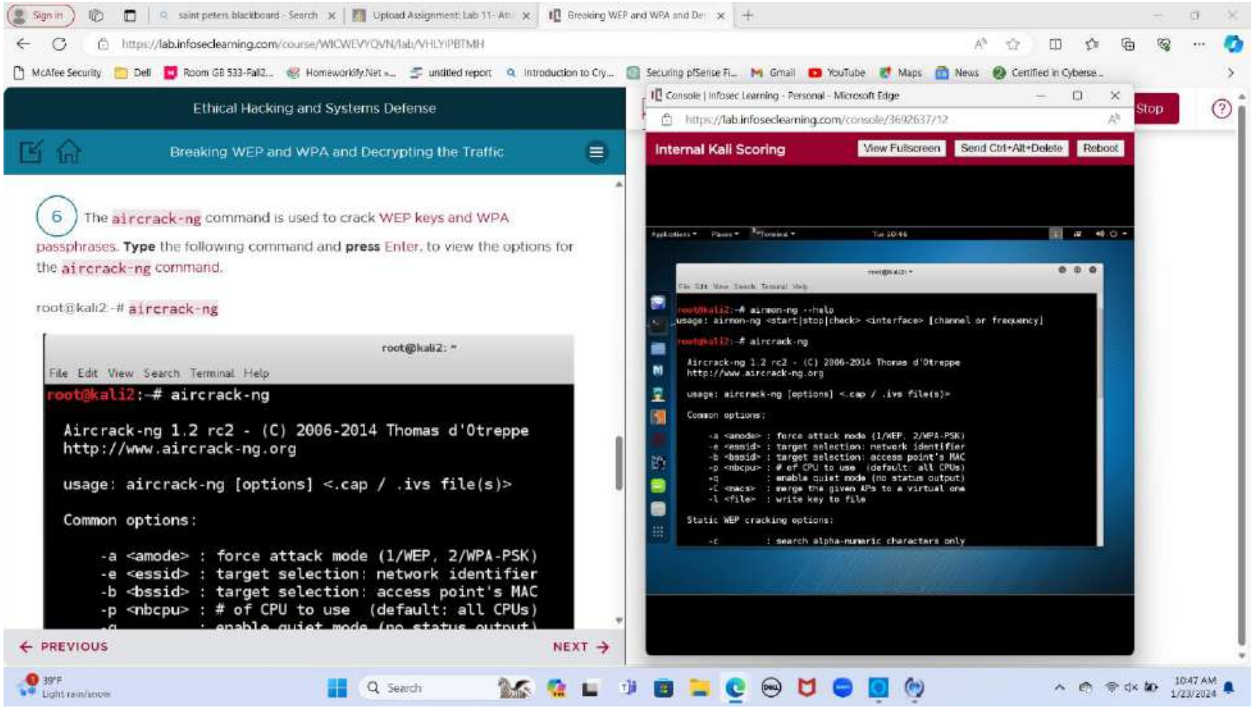
5 The airmon-ng command can be utilized to put a wireless card into monitor mode. **Type** the airmon-ng --help and **press** Enter, to view the options for the airmon-ng command.

root@kali2:~# airmon-ng --help

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

6 The aircrack-ng command is used to crack WEP keys and WPA

```
root@kali2:~# iwconfig
eth0      no wireless extensions.

lo        no wireless extensions.

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

root@kali2:~#
```

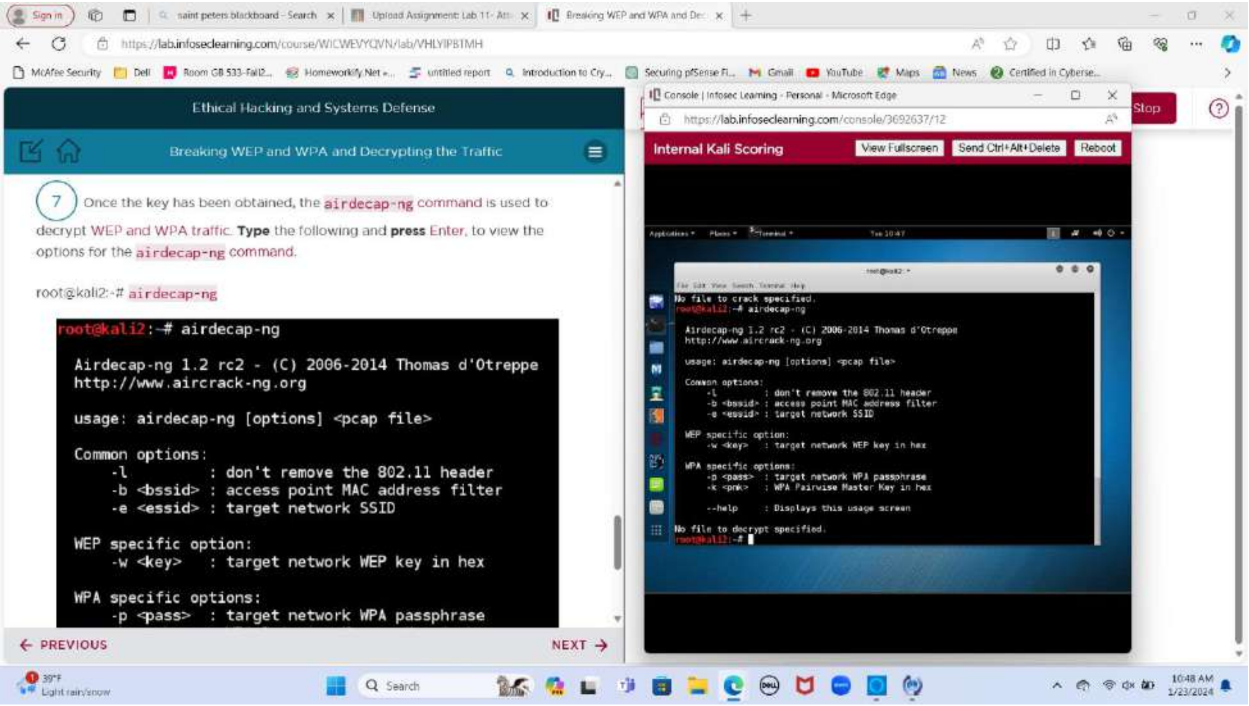

Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
← PREVIOUS
NEXT →
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
10:47 AM
1/23/2024

6 The aircrack-ng command is used to crack WEP keys and WPA passphrases. **Type** the following command and **press** Enter, to view the options for the aircrack-ng command.

root@kali2:-# 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)
```

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

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:

      -c         : search alpha-numeric characters only
```

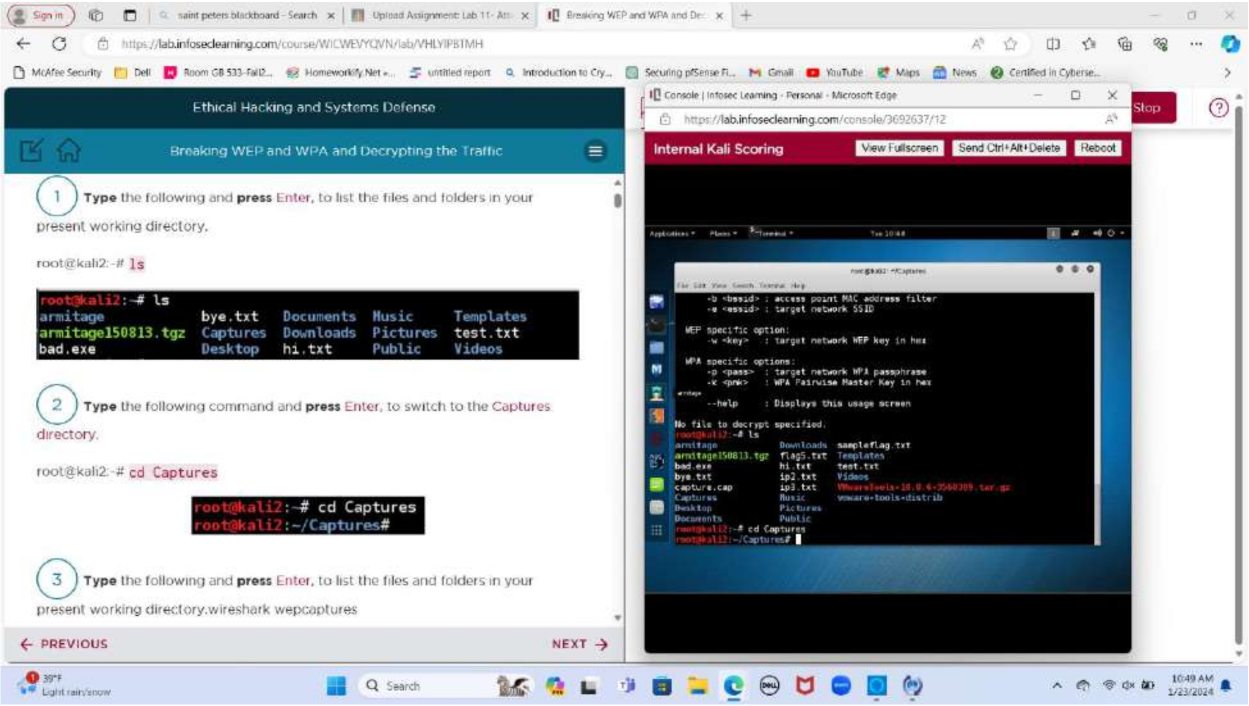

Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
← PREVIOUS
NEXT →
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
10:48 AM
1/23/2024

7 Once the key has been obtained, the airdecap-ng command is used to decrypt WEP and WPA traffic. **Type** the following and **press** Enter, to view the options for the airdecap-ng command.

root@kali2:-# 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
```

```
No file to crack specified.
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.
root@kali2:~# 
```



Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

1. **Type** the following and **press** Enter, to list the files and folders in your present working directory.

root@kali2:~# ls

```
root@kali2:~# ls
armitage             bye.txt   Documents  Music     Templates
armitage150813.tgz   Captures  Downloads  Pictures  test.txt
bad.exe              Desktop   hi.txt     Public    Videos
```

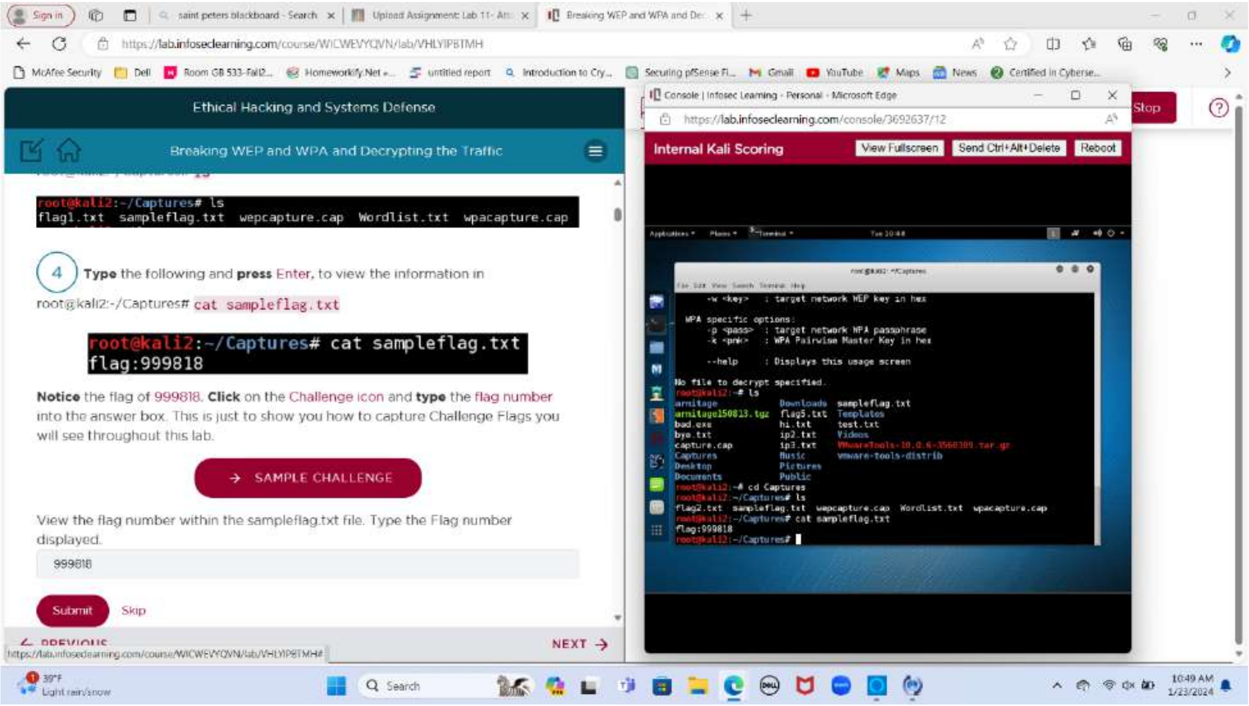
2. **Type** the following command and **press** Enter, to switch to the Captures directory.

root@kali2:~# cd Captures

```
root@kali2:~# cd Captures
root@kali2:~/Captures#
```

3. **Type** the following and **press** Enter, to list the files and folders in your present working directory.wireshark wepcaptures

```
     -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.
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
root@kali2:~# cd Captures
root@kali2:~/Captures#
```


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and De
https://lab.infosec learning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Terminal
Tue 10:48
root@kali2: ~/Captures
← PREVIOUS
NEXT →
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH#
39°F
Light rain/snow
Search
10:49 AM
1/23/2024

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

```
root@kali2:~/Captures# ls
flag1.txt  sampleflag.txt  wepcapture.cap  Wordlist.txt  wpacapture.cap
```

4. **Type** the following and **press** Enter, to view the information in

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

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

Notice the flag of 999818. **Click** on the Challenge icon and **type** the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab.

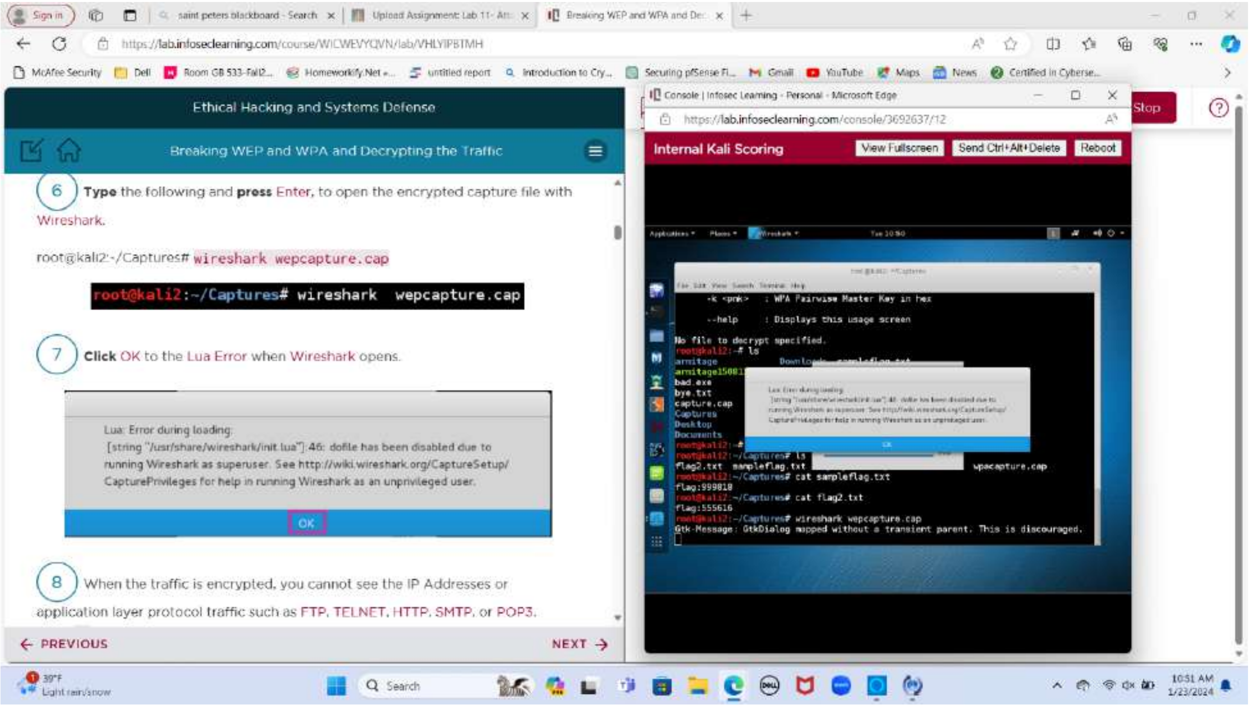
→ SAMPLE CHALLENGE

View the flag number within the sampleflag.txt file. Type the Flag number displayed.

999818

Submit Skip

```
     -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.
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
root@kali2:~# cd Captures
root@kali2:~/Captures# ls
flag2.txt  sampleflag.txt  wepcapture.cap  Wordlist.txt  wpacapture.cap
root@kali2:~/Captures# cat sampleflag.txt
flag:999818
root@kali2:~/Captures#
```



Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and Dec
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
McAfee Security
Dell
Room GB 533-Fall2...
Homeworkify.Net »...
untitled report
Introduction to Cry...
Securing pfSense Fi...
Gmail
YouTube
Maps
News
Certified in Cyberse...
Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Wireshark
Tue 10:50
PREVIOUS
NEXT
39°F
Light rain/snow
Search
10:51 AM
1/23/2024

6 **Type** the following and **press** Enter, to open the encrypted capture file with Wireshark.

root@kali2:~/Captures# wireshark wepcapture.cap

```
root@kali2:~/Captures# wireshark  wepcapture.cap
```

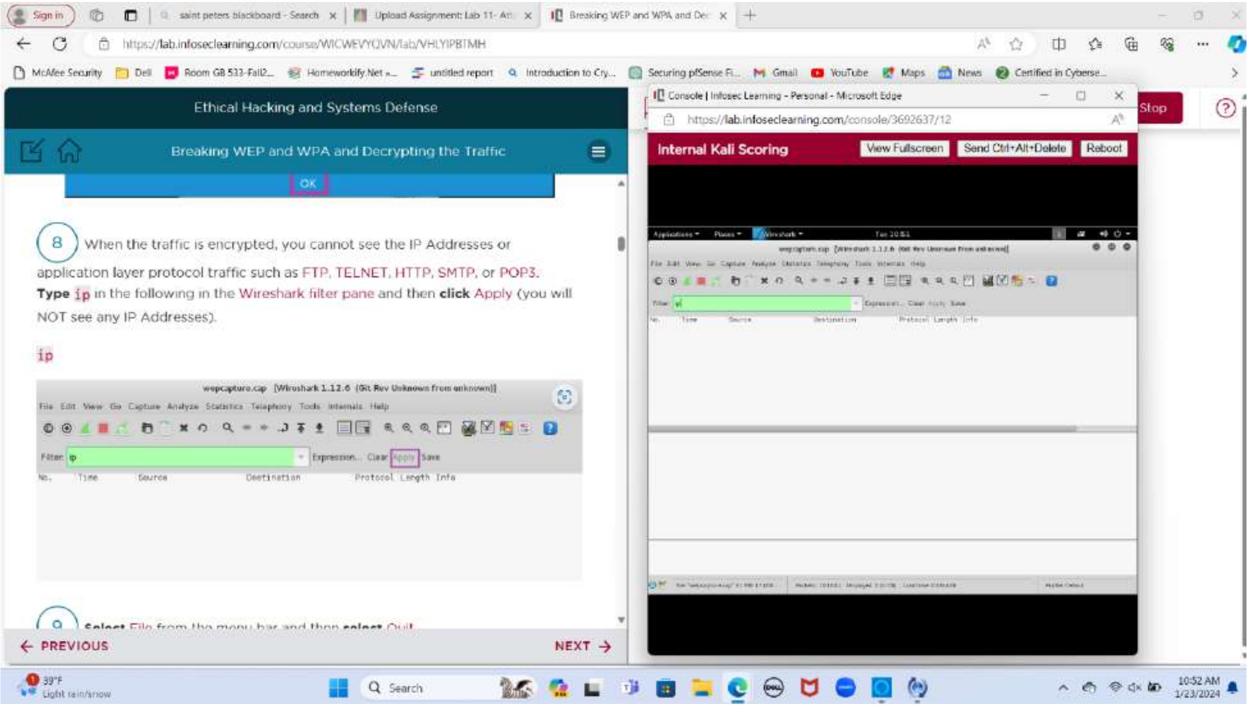
7 **Click** OK to the Lua Error when Wireshark opens.

Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.

OK

8 When the traffic is encrypted, you cannot see the IP Addresses or application layer protocol traffic such as FTP, TELNET, HTTP, SMTP, or POP3.

```
    -k <pmk>    : WPA Pairwise Master Key in hex

    --help      : Displays this usage screen

No file to decrypt specified.
root@kali2:~# ls
armitage                Downloads  sampleflag.txt
armitage15081
bad.exe
bye.txt
capture.cap
Captures
Desktop
Documents
root@kali2:~#
root@kali2:~/Captures# ls
flag2.txt  sampleflag.txt                          wpacapture.cap
root@kali2:~/Captures# cat sampleflag.txt
flag:999818
root@kali2:~/Captures# cat flag2.txt
flag:555616
root@kali2:~/Captures# wireshark wepcapture.cap
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
```

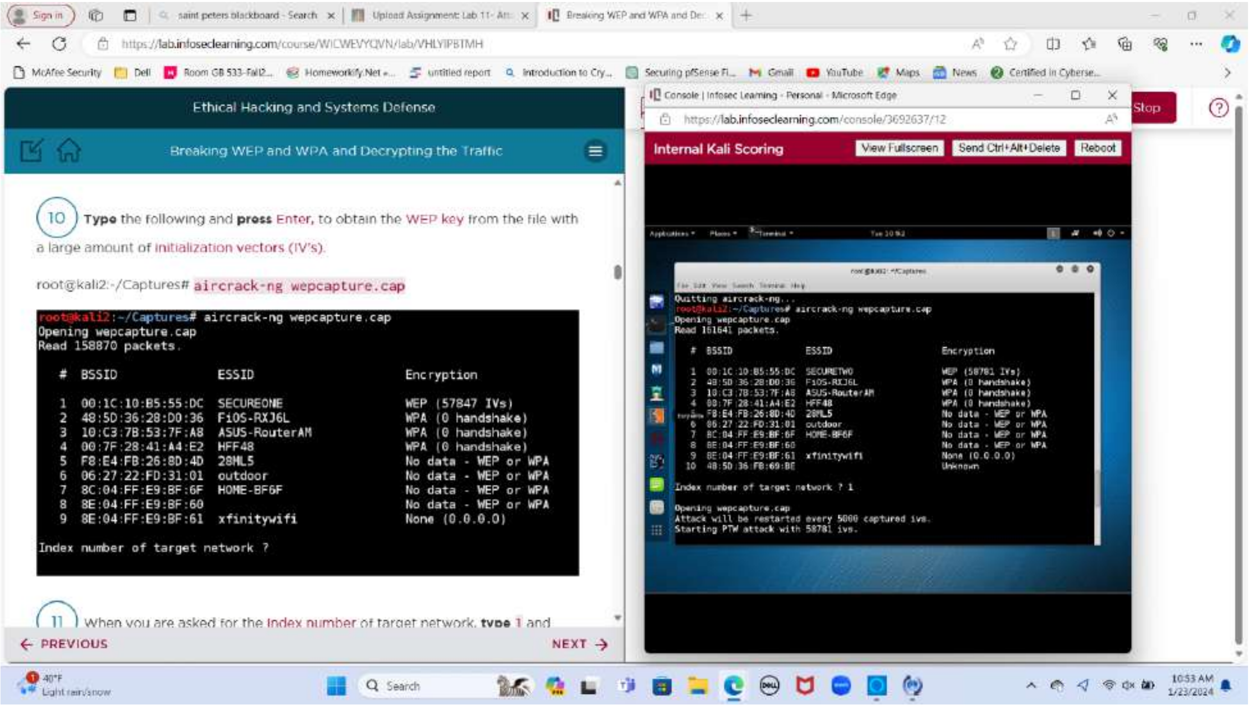


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and Dec
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
OK
wepcapture.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
PREVIOUS
NEXT
39°F
Light rain/snow
Search
10:52 AM
1/23/2024

8 When the traffic is encrypted, you cannot see the IP Addresses or application layer protocol traffic such as FTP, TELNET, HTTP, SMTP, or POP3. **Type** ip in the following in the Wireshark filter pane and then **click** Apply (you will NOT see any IP Addresses).

```
ip
```

9 **Select** File from the menu bar and then **select** Quit.


saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and Dec
https://lab.infosecleaming.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecleaming.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Terminal
PREVIOUS
NEXT
10:53 AM
1/23/2024

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

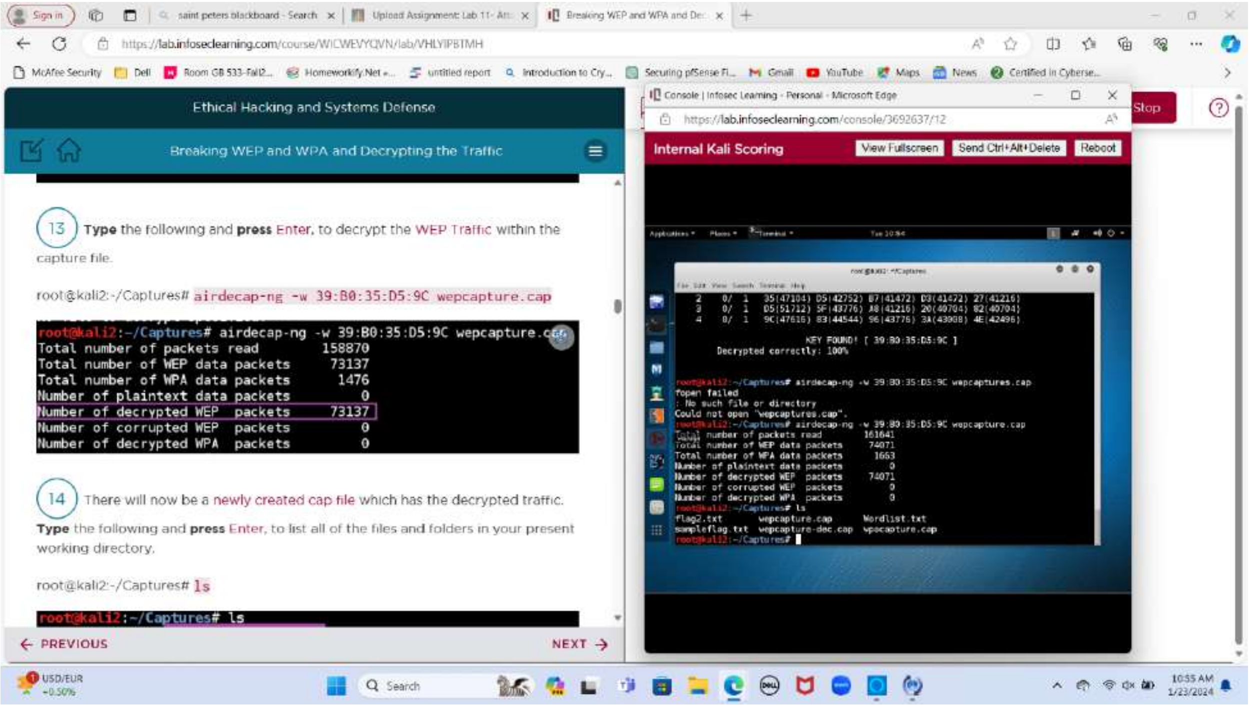
10 **Type** the following and **press** Enter, to obtain the WEP key from the file with a large amount of initialization vectors (IV's).

root@kali2:~/Captures# aircrack-ng wepcapture.cap

```
root@kali2:~/Captures# aircrack-ng wepcapture.cap
Opening wepcapture.cap
Read 158870 packets.

   #  BSSID              ESSID                      Encryption

   1  00:1C:10:B5:55:DC  SECUREONE                  WEP (57847 IVs)
   2  48:5D:36:28:D0:36  FiOS-RXJ6L                 WPA (0 handshake)
   3  10:C3:7B:53:7F:A8  ASUS-RouterAM              WPA (0 handshake)
   4  00:7F:28:41:A4:E2  HFF48                      WPA (0 handshake)
   5  F8:E4:FB:26:8D:4D  28ML5                      No data - WEP or WPA
   6  06:27:22:FD:31:01  outdoor                    No data - WEP or WPA
   7  8C:04:FF:E9:BF:6F  HOME-BF6F                  No data - WEP or WPA
   8  8E:04:FF:E9:BF:60                             No data - WEP or WPA
   9  8E:04:FF:E9:BF:61  xfinitywifi                None (0.0.0.0)

Index number of target network ?
```

11 When you are asked for the Index number of target network, **type** 1 and

```
Quitting aircrack-ng...
root@kali2:~/Captures# aircrack-ng wepcapture.cap
Opening wepcapture.cap
Read 161641 packets.

   #  BSSID              ESSID                      Encryption

   1  00:1C:10:B5:55:DC  SECURETWO                  WEP (58781 IVs)
   2  48:5D:36:28:D0:36  FiOS-RXJ6L                 WPA (0 handshake)
   3  10:C3:7B:53:7F:A8  ASUS-RouterAM              WPA (0 handshake)
   4  00:7F:28:41:A4:E2  HFF48                      WPA (0 handshake)
   5  F8:E4:FB:26:8D:40  28ML5                      No data - WEP or WPA
   6  06:27:22:FD:31:01  outdoor                    No data - WEP or WPA
   7  8C:04:FF:E9:BF:6F  HOME-BF6F                  No data - WEP or WPA
   8  8E:04:FF:E9:BF:60                             No data - WEP or WPA
   9  8E:04:FF:E9:BF:61  xfinitywifi                None (0.0.0.0)
  10  48:5D:36:FB:69:BE                             Unknown

Index number of target network ? 1

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


saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and Dec
https://lab.infosecleaming.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecleaming.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Terminal
PREVIOUS
NEXT
10:55 AM
1/23/2024

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

13 **Type** the following and **press** Enter, to decrypt the WEP Traffic within the capture file.

root@kali2:~/Captures# 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          158870
Total number of WEP data packets       73137
Total number of WPA data packets        1476
Number of plaintext data packets           0
Number of decrypted WEP  packets       73137
Number of corrupted WEP  packets           0
Number of decrypted WPA  packets           0
```

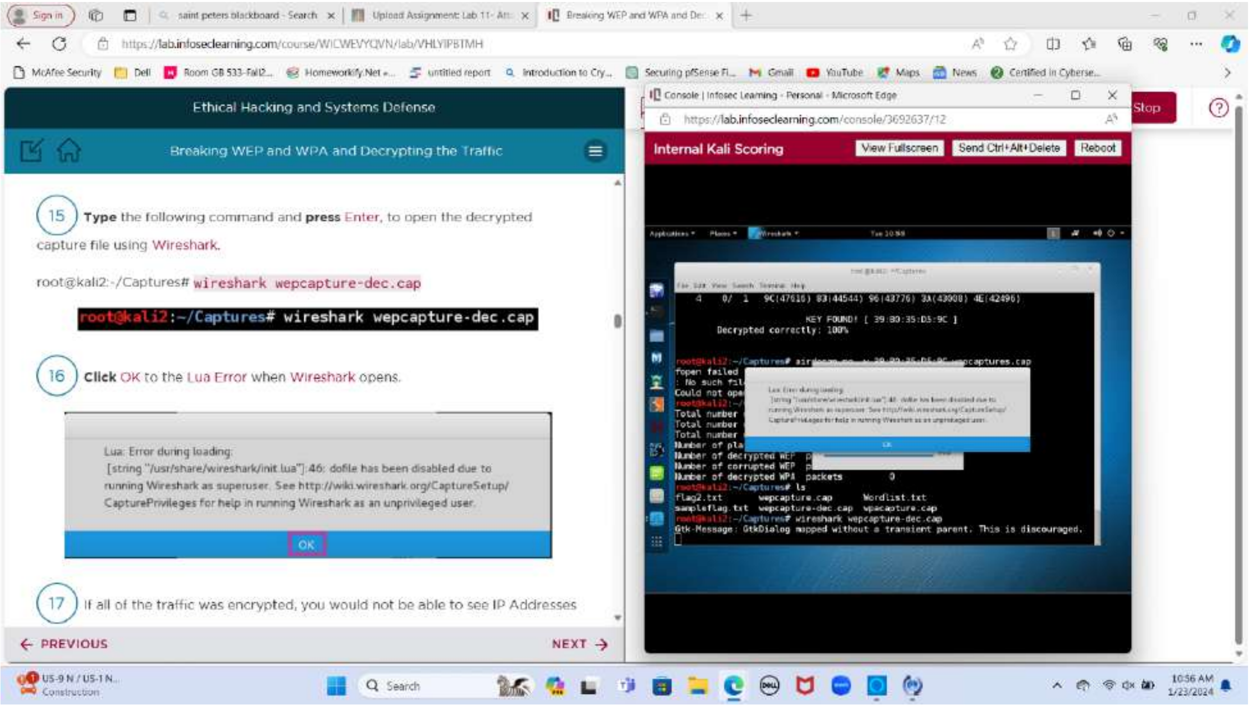
14 There will now be a newly created cap file which has the decrypted traffic.

Type the following and **press** Enter, to list all of the files and folders in your present working directory.

root@kali2:~/Captures# ls

```
root@kali2:~/Captures# ls
```

```
   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%


root@kali2:~/Captures# airdecap-ng -w 39:B0:35:D5:9C wepcaptures.cap
fopen failed
: No such file or directory
Could not open "wepcaptures.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        1653
Number of plaintext data packets           0
Number of decrypted WEP  packets       74071
Number of corrupted WEP  packets           0
Number of decrypted WPA  packets           0
root@kali2:~/Captures# ls
flag2.txt       wepcapture.cap      Wordlist.txt
sampleflag.txt  wepcapture-dec.cap  wpacapture.cap
root@kali2:~/Captures#
```



Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

15 **Type** the following command and **press** Enter, to open the decrypted capture file using Wireshark.

root@kali2:~/Captures# `wireshark wepcapture-dec.cap`

```
root@kali2:~/Captures# wireshark wepcapture-dec.cap
```

16 **Click** OK to the Lua Error when Wireshark opens.

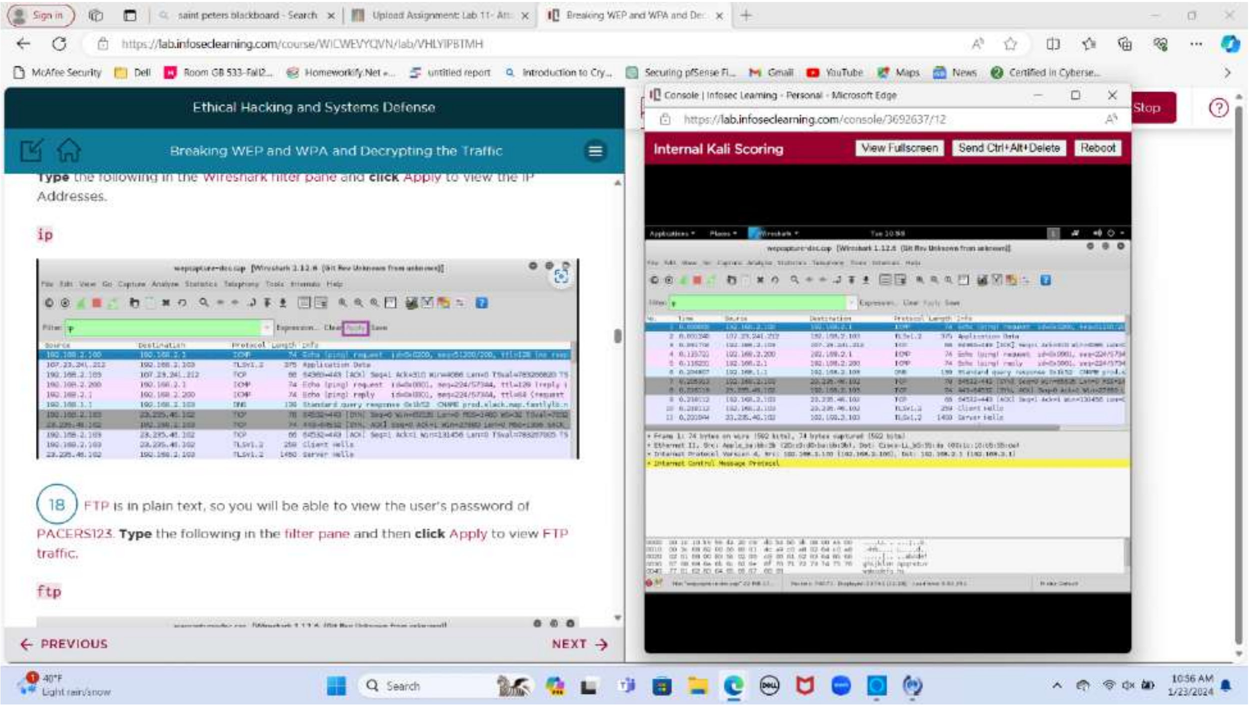
Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.

OK

17 If all of the traffic was encrypted, you would not be able to see IP Addresses

← PREVIOUS NEXT →

```
   4    0/  1   9C(47616) 83(44544) 96(43776) 3A(43008) 4E(42496)

                     KEY FOUND! [ 39:83:35:D5:9C ]
        Decrypted correctly: 100%

root@kali2:~/Captures# air[...] wpcaptures.cap
fopen failed
: No such fil
Could not ope
root@kali2:~/
Total number
Total number
Total number
Number of pla
Number of decrypted WEP  p
Number of corrupted WEP  p
Number of decrypted WPA  packets        0
root@kali2:~/Captures# ls
flag2.txt        wepcapture.cap      Wordlist.txt
sampleflag.txt  wepcapture-dec.cap  wpacapture.cap
root@kali2:~/Captures# wireshark wepcapture-dec.cap
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
```


saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and Dec
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Wireshark
Tue 10:58
wepcapture-dec.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ip
Expression... Clear Apply Save
40°F
Light rain/snow
Search
10:56 AM
1/23/2024

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

Type the following in the Wireshark filter pane and **click** Apply to view the IP Addresses.

`ip`

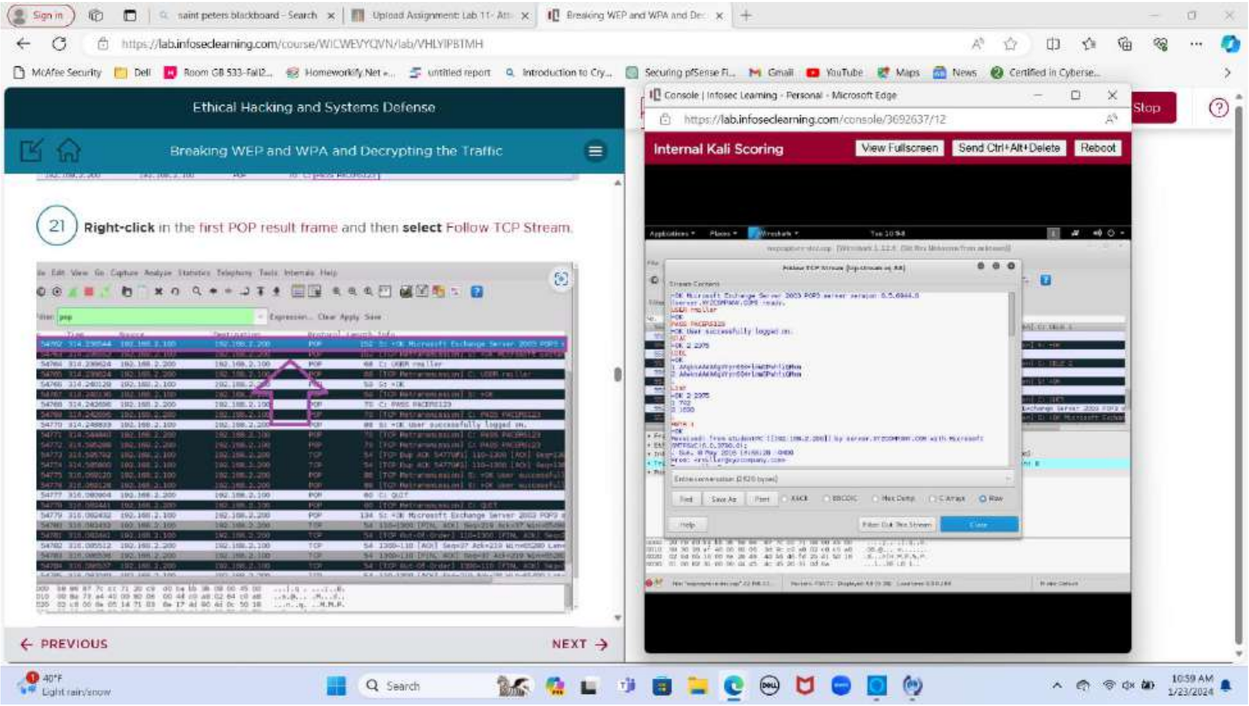
```
Source           Destination      Protocol Length Info
192.168.2.100    192.168.2.1      ICMP       74 Echo (ping) request  id=0x0200, seq=51200/200, ttl=128 (no resp
107.23.241.212   192.168.2.103    TLSv1.2   375 Application Data
192.168.2.103    107.23.241.212   TCP        66 54369→443 [ACK] Seq=1 Ack=310 Win=4086 Len=0 TSval=783260820 TS
192.168.2.200    192.168.2.1      ICMP       74 Echo (ping) request  id=0x0001, seq=224/57344, ttl=128 (reply i
192.168.2.1      192.168.2.200    ICMP       74 Echo (ping) reply    id=0x0001, seq=224/57344, ttl=64 (request
192.168.1.1      192.168.2.103    DNS       130 Standard query response 0x1b52  CNAME prod.slack.map.fastlylb.n
192.168.2.103    23.235.46.102    TCP        78 64532→443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=7832
23.235.46.102    192.168.2.103    TCP        74 443→64532 [SYN, ACK] Seq=0 Ack=1 Win=27960 Len=0 MSS=1300 SACK_
192.168.2.103    23.235.46.102    TCP        66 64532→443 [ACK] Seq=1 Ack=1 Win=131456 Len=0 TSval=783287005 TS
192.168.2.103    23.235.46.102    TLSv1.2   258 Client Hello
23.235.46.102    192.168.2.103    TLSv1.2  1450 Server Hello
```

18 FTP is in plain text, so you will be able to view the user's password of PACERS123. **Type** the following in the filter pane and then **click** Apply to view FTP traffic.

`ftp`

← PREVIOUS NEXT →

```
No.  Time      Source           Destination      Protocol Length Info
 1  0.000000  192.168.2.100    192.168.2.1      ICMP       74 Echo (ping) request  id=0x0200, seq=51200/20
 2  0.000240  107.23.241.212   192.168.2.103    TLSv1.2   375 Application Data
 3  0.001708  192.168.2.103    107.23.241.212   TCP        66 54369→443 [ACK] Seq=1 Ack=310 Win=4086 Len=0
 4  0.115720  192.168.2.200    192.168.2.1      ICMP       74 Echo (ping) request  id=0x0001, seq=224/5734
 5  0.116200  192.168.2.1      192.168.2.200    ICMP       74 Echo (ping) reply    id=0x0001, seq=224/5734
 6  0.204807  192.168.1.1      192.168.2.103    DNS       130 Standard query response 0x1b52  CNAME prod.s
 7  0.205913  192.168.2.103    23.235.46.102    TCP        78 64532→443 [SYN] Seq=0 Win=65535 Len=0 MSS=14
 8  0.208018  23.235.46.102    192.168.2.103    TCP        74 443→64532 [SYN, ACK] Seq=0 Ack=1 Win=27960 L
 9  0.210112  192.168.2.103    23.235.46.102    TCP        66 64532→443 [ACK] Seq=1 Ack=1 Win=131456 Len=C
10  0.210112  192.168.2.103    23.235.46.102    TLSv1.2   258 Client Hello
11  0.220044  23.235.46.102    192.168.2.103    TLSv1.2  1400 Server Hello

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: Apple_ba:bb:3b (20:c9:d0:ba:bb:3b), Dst: Cisco-Li_b5:35:4a (00:1c:10:b5:35:4a)
▸ Internet Protocol Version 4, Src: 192.168.2.100 (192.168.2.100), Dst: 192.168.2.1 (192.168.2.1)
▸ Internet Control Message Protocol
```



Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
← PREVIOUS
NEXT →

21 **Right-click** in the first POP result frame and then **select** Follow TCP Stream.

Follow TCP Stream (tcp.stream eq 88)

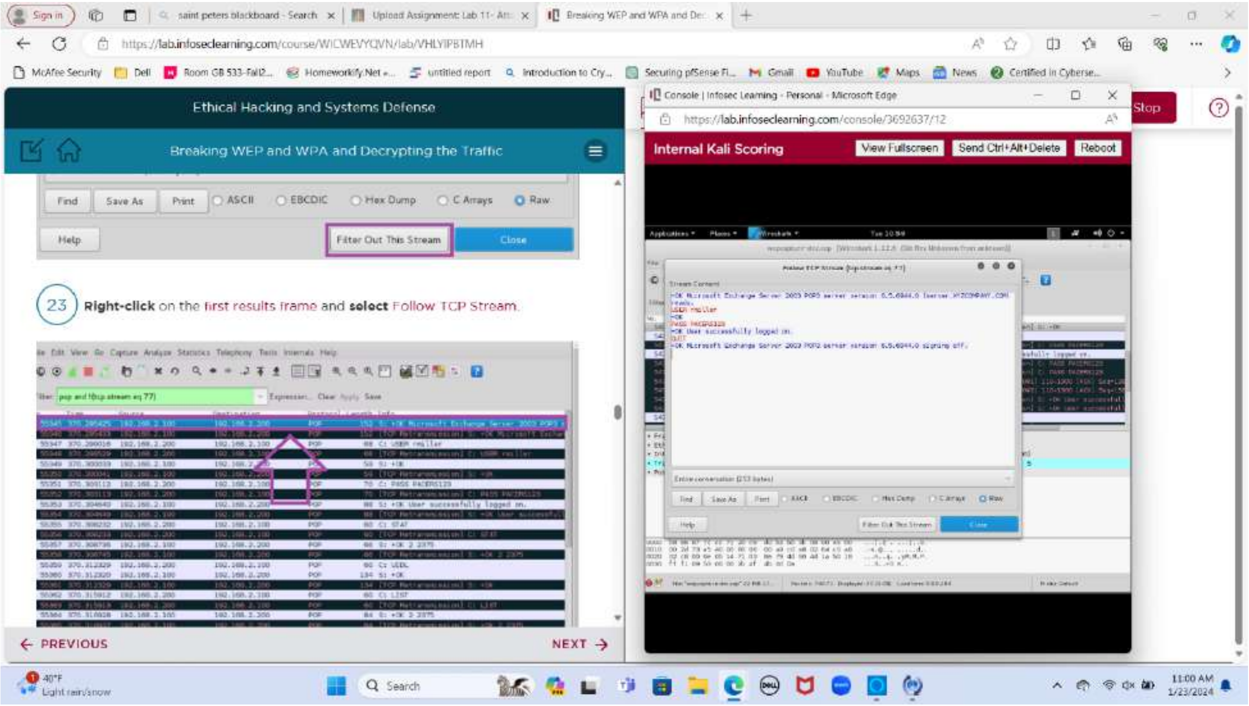
Stream Content

```
+OK Microsoft Exchange Server 2003 POP3 server version 6.5.6944.0
(server.XYZCOMPANY.COM) ready.
USER rmiller
+OK
PASS P@CERS123
+OK User successfully logged on.
STAT
+OK 2 2975
UIDL
+OK
1 AAgknAAAAAAgVrn60+1mdPwh1iQMna
2 AAeknAAAAAgVrn604+1mdPwh1iQMna
.
LIST
+OK 2 2975
1 702
2 1690
.
RETR 1
+OK
Received: from studentPC ([192.168.2.200]) by server.XYZCOMPANY.COM with Microsoft
SMTPSVC(6.0.3790.0);
 Sun, 8 May 2016 14:08:28 -0400
From: <rmiller@xyzcompany.com>
```

Entire conversation (2920 bytes)

Find | Save As | Print | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Help | Filter Out This Stream | Close



Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
← PREVIOUS
NEXT →

Find | Save As | Print | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Help | Filter Out This Stream | Close

23 **Right-click** on the first results frame and **select** Follow TCP Stream.

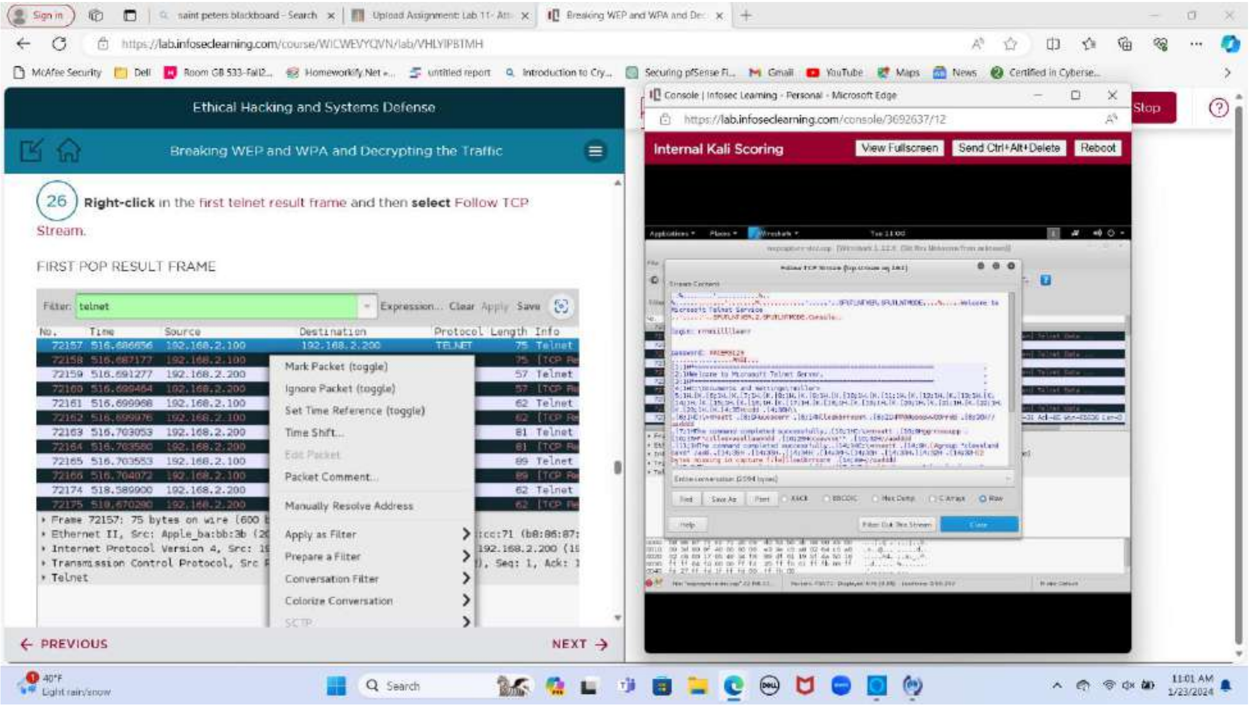
Filter: pop and !(tcp.stream eq 77)

Follow TCP Stream (tcp.stream eq 77)

Stream Content

```
+OK Microsoft Exchange Server 2003 POP3 server version 6.5.6944.0 (server.XYZCOMPANY.COM)
ready.
USER rmiller
+OK
PASS P@CERS123
+OK User successfully logged on.
QUIT
+OK Microsoft Exchange Server 2003 POP3 server version 6.5.6944.0 signing off.
```

Entire conversation (253 bytes)



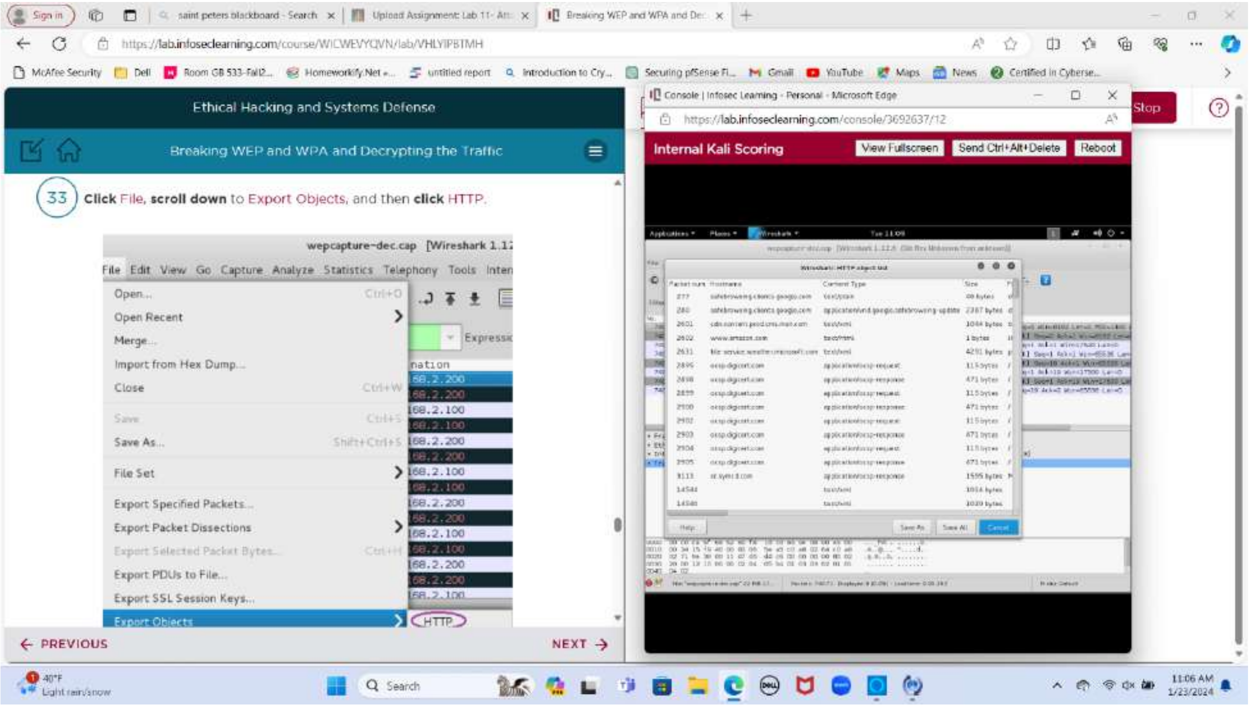
26 **Right-click** in the first telnet result frame and then **select** Follow TCP Stream.

FIRST POP RESULT FRAME

Filter: telnet

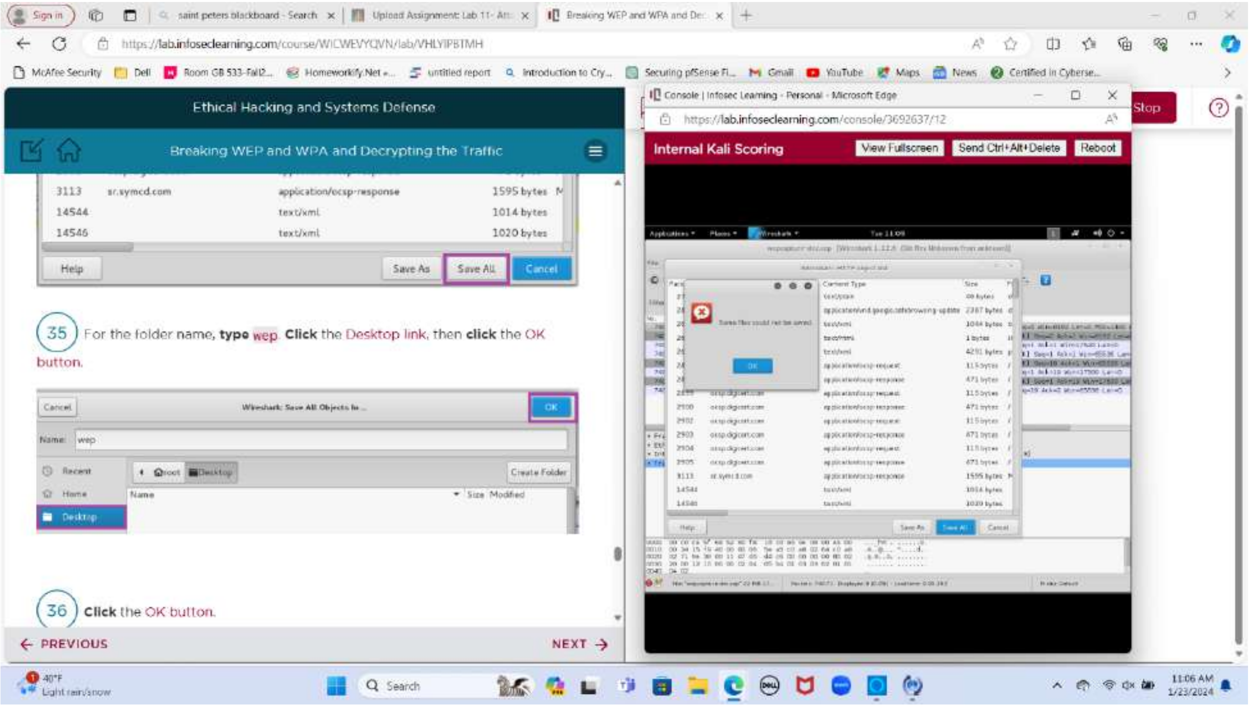
```
No.    Time        Source         Destination    Protocol Length Info
 72157 516.686656  192.168.2.100  192.168.2.200  TELNET     75 Telnet
 72158 516.687177  192.168.2.100                            75 [TCP Re
 72159 516.691277  192.168.2.200                            57 Telnet
 72160 516.699464  192.168.2.200                            57 [TCP Re
 72161 516.699968  192.168.2.100                            62 Telnet
 72162 516.699976  192.168.2.100                            62 [TCP Re
 72163 516.703053  192.168.2.200                            81 Telnet
 72164 516.703560  192.168.2.200                            81 [TCP Re
 72165 516.703553  192.168.2.100                            89 Telnet
 72166 516.704072  192.168.2.100                            89 [TCP Re
 72174 518.589900  192.168.2.200                            62 Telnet
 72175 518.670280  192.168.2.200                            62 [TCP Re
▸ Frame 72157: 75 bytes on wire (600 b
▸ Ethernet II, Src: Apple_ba:bb:3b (2                      :cc:71 (b8:86:87:
▸ Internet Protocol Version 4, Src: 19                      192.168.2.200 (19
▸ Transmission Control Protocol, Src P                      ), Seq: 1, Ack: 1
▸ Telnet
```

```
Welcome to Microsoft Telnet Service
login: [illegible]
password: [illegible]
Welcome to Microsoft Telnet Server.
C:\Documents and Settings\[illegible]
The command completed successfully.
The command completed successfully.
bytes missing in capture file
```


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Breaking WEP and WPA and Dec
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Wireshark: HTTP object list
Help
Save As
Save All
Cancel
wepcapture-dec.cap [Wireshark 1.12
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Inter
Open... Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Selected Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
HTTP
Expressio
PREVIOUS
NEXT
40°F
Light rain/snow
Search
11:06 AM
1/23/2024

33 **Click** File, **scroll down** to Export Objects, and then **click** HTTP.

Packet num	Hostname	Content Type	Size
277	safebrowsing.clients.google.com	text/plain	[illegible] bytes
280	safebrowsing.clients.google.com	application/vnd.google.safebrowsing-update	2267 bytes
2601	cdn.content.prod.cms.msn.com	text/html	1044 bytes
2602	www.amazon.com	text/html	1 bytes
2631	tile-service.weather.microsoft.com	text/xml	4291 bytes
2895	ocsp.digicert.com	application/ocsp-request	115 bytes
2898	ocsp.digicert.com	application/ocsp-response	471 bytes
2899	ocsp.digicert.com	application/ocsp-request	115 bytes
2900	ocsp.digicert.com	application/ocsp-response	471 bytes
2902	ocsp.digicert.com	application/ocsp-request	115 bytes
2903	ocsp.digicert.com	application/ocsp-response	471 bytes
2904	ocsp.digicert.com	application/ocsp-request	115 bytes
2905	ocsp.digicert.com	application/ocsp-response	471 bytes
3113	sr.symcd.com	application/ocsp-response	1595 bytes
14544		text/html	1014 bytes
14546		text/html	1020 bytes



https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

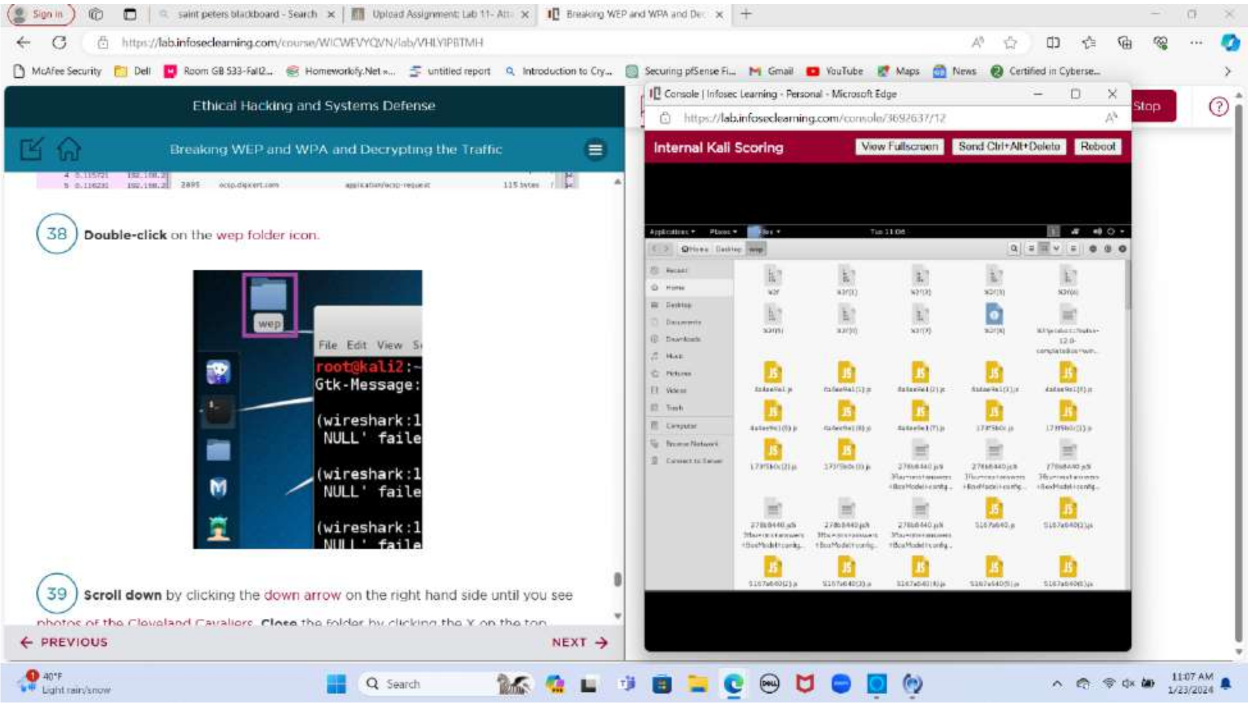
```
3113    sr.symcd.com    application/ocsp-response    1595 bytes
14544                   text/xml                     1014 bytes
14546                   text/xml                     1020 bytes
```

35 For the folder name, **type** wep. **Click** the Desktop link, then **click** the OK button.

Wireshark: Save All Objects In ...

Name: wep

36 **Click** the OK button.



https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH

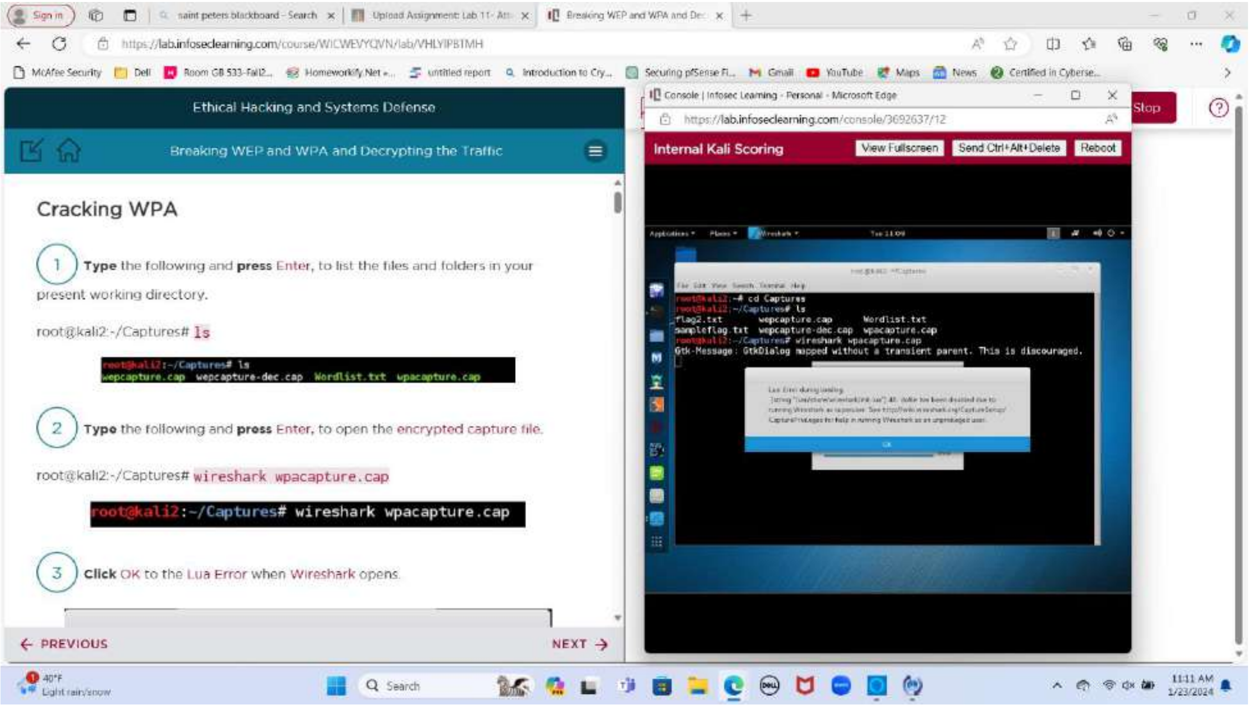
Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

38 **Double-click** on the wep folder icon.

```
root@kali2:~
Gtk-Message:

(wireshark:1
 NULL' faile

(wireshark:1
 NULL' faile

(wireshark:1
 NULL' faile
```

39 **Scroll down** by clicking the down arrow on the right hand side until you see photos of the Cleveland Cavaliers. **Close** the folder by clicking the X on the top



https://lab.infosecl earning.com/course/WICWEVYQVN/lab/VHLYIPBTMH

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

Cracking WPA

1 **Type** the following and **press** Enter, to list the files and folders in your present working directory.

root@kali2:-/Captures# `ls`

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

2 **Type** the following and **press** Enter, to open the encrypted capture file.

root@kali2:-/Captures# `wireshark wpacapture.cap`

```
root@kali2:~/Captures# wireshark wpacapture.cap
```

3 **Click** OK to the Lua Error when Wireshark opens.

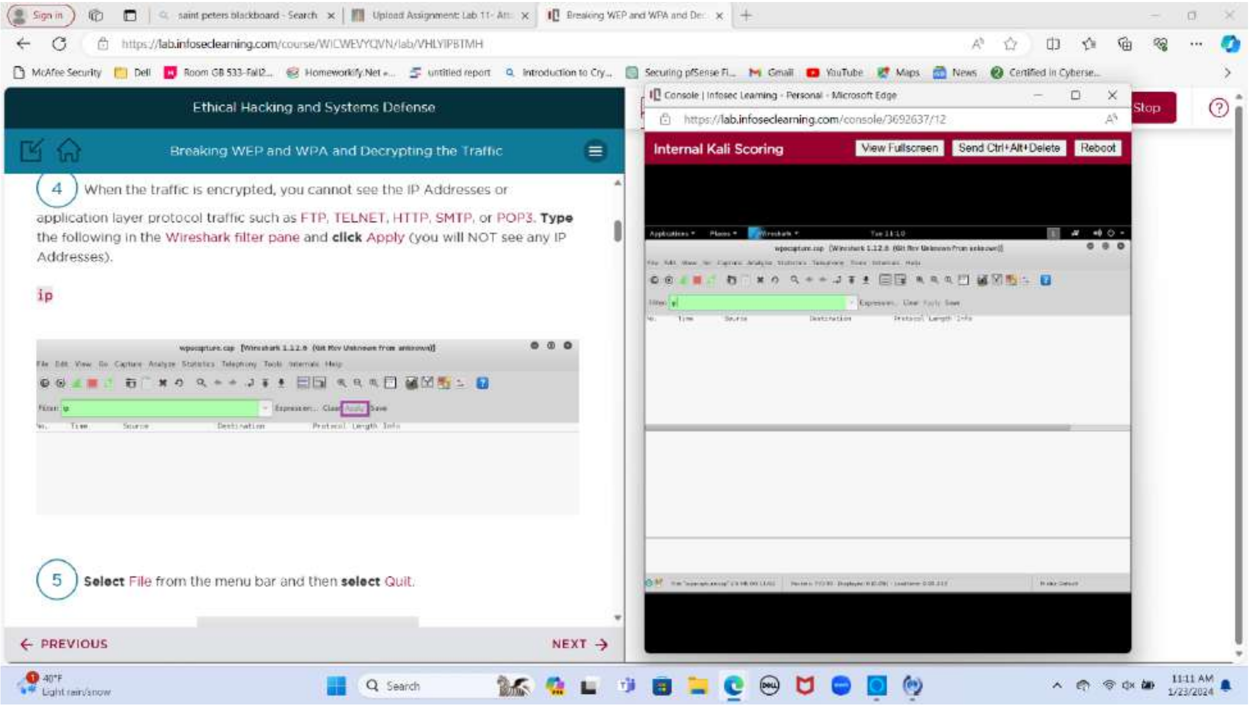
← PREVIOUS NEXT →

Internal Kali Scoring

https://lab.infoseclearning.com/console/3692637/12

```
root@kali2:~# cd Captures
root@kali2:~/Captures# ls
flag2.txt       wepcapture.cap      Wordlist.txt
sampleflag.txt  wepcapture-dec.cap  wpacapture.cap
root@kali2:~/Captures# wireshark wpacapture.cap
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
```

Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.



https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

4 When the traffic is encrypted, you cannot see the IP Addresses or application layer protocol traffic such as FTP, TELNET, HTTP, SMTP, or POP3. **Type** the following in the Wireshark filter pane and **click** Apply (you will NOT see any IP Addresses).

`ip`

wpacapture.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

Filter: ip

5 **Select** File from the menu bar and then **select** Quit.

← PREVIOUS NEXT →

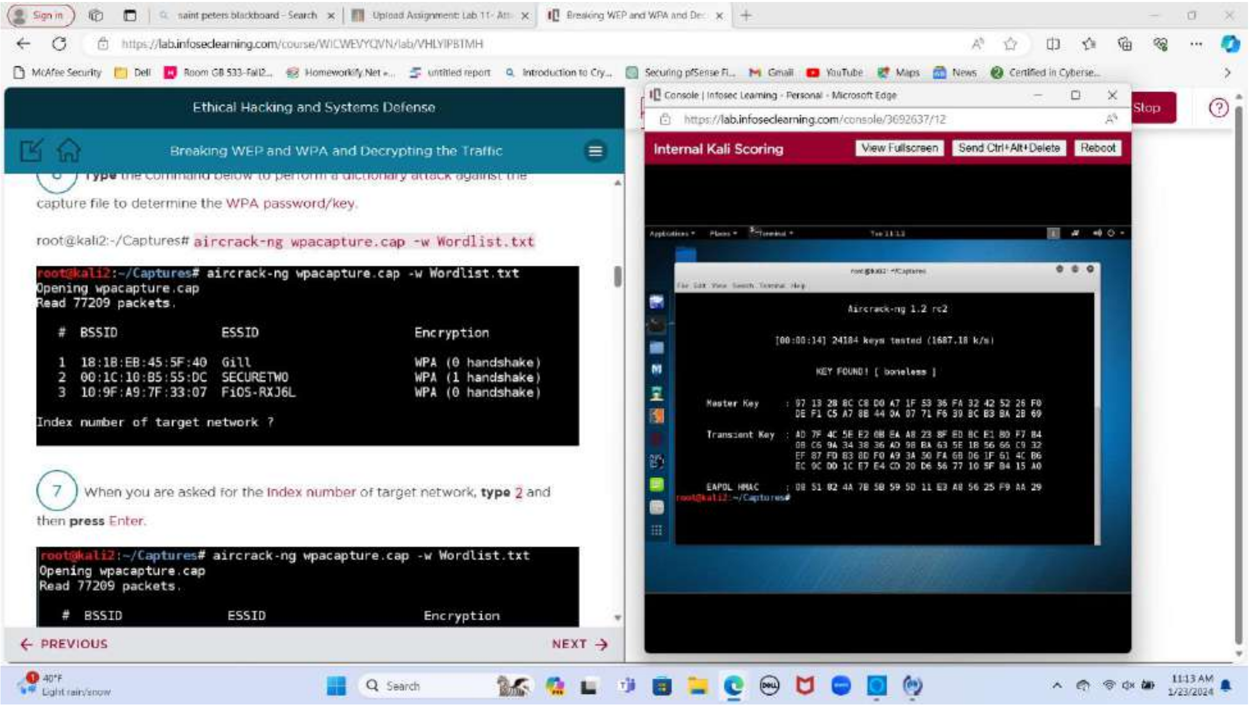
Internal Kali Scoring

https://lab.infoseclearning.com/console/3692637/12

wpacapture.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

Filter: ip

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
11:11 AM
1/23/2024



Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att:
Breaking WEP and WPA and Dec
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
McAfee Security
Dell
Room GB 533-Fall2...
Homeworkify.Net -...
untitled report
Introduction to Cry...
Securing pfSense Fi...
Gmail
YouTube
Maps
News
Certified in Cyberse...
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
← PREVIOUS
NEXT →
40°F
Light rain/snow
Search
11:13 AM
1/23/2024

6 **Type** the command below to perform a dictionary attack against the capture file to determine the WPA password/key.

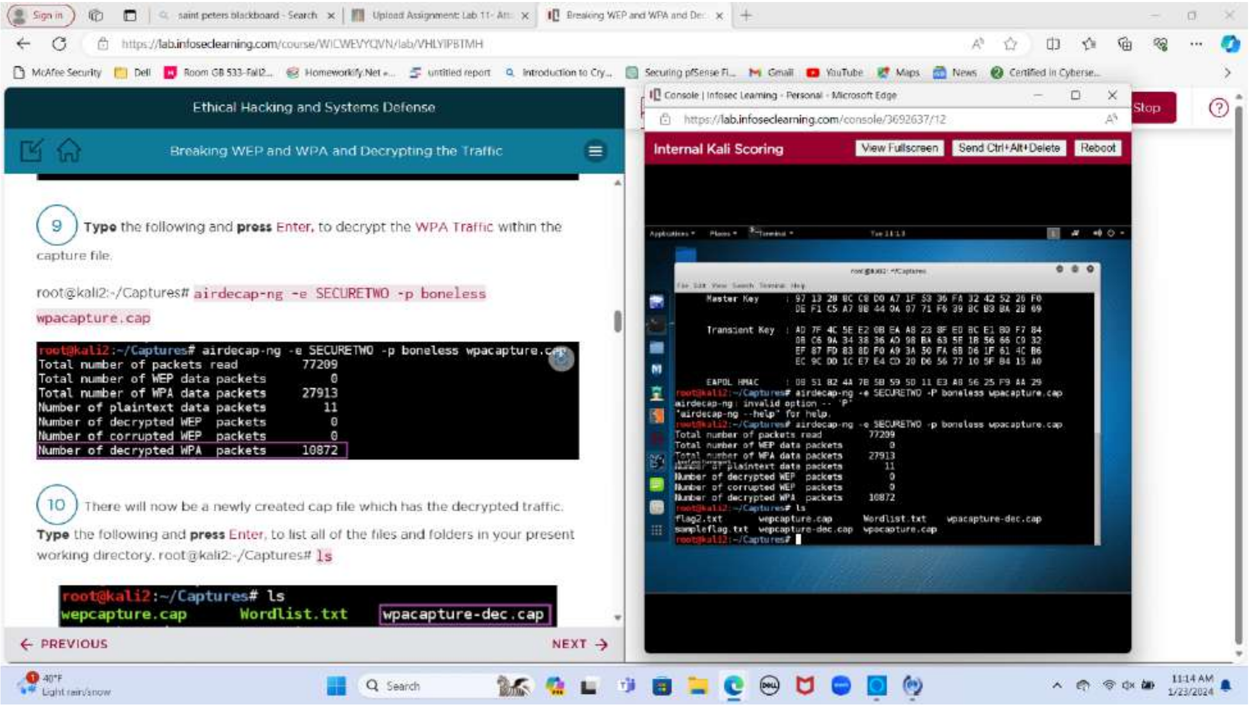
root@kali2:-/Captures# `aircrack-ng wpacapture.cap -w Wordlist.txt`

```
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 ?
```

7 When you are asked for the Index number of target network, **type** 2 and then **press** Enter.

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

   #  BSSID              ESSID                     Encryption
```

```
                          Aircrack-ng 1.2 rc2

              [00:00:14] 24184 keys tested (1687.18 k/s)

                       KEY FOUND! [ boneless ]

      Master Key     : 97 13 2B 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 BD F7 B4
                       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
root@kali2:~/Captures#
```



Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att:
Breaking WEP and WPA and Dec
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
← PREVIOUS
NEXT →
40°F
Light rain/snow
Search
11:14 AM
1/23/2024

9 **Type** the following and **press** Enter, to decrypt the WPA Traffic within the capture file.

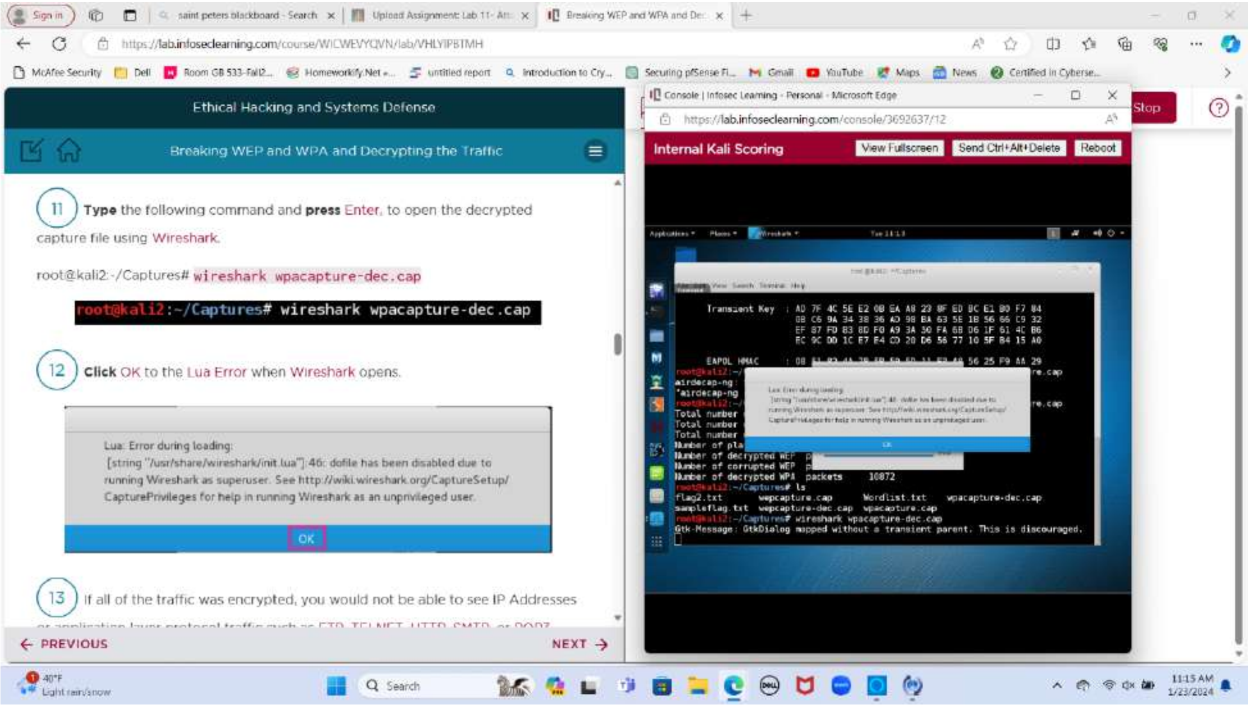
root@kali2:-/Captures# `airdecap-ng -e SECURETWO -p boneless wpacapture.cap`

```
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
```

10 There will now be a newly created cap file which has the decrypted traffic. **Type** the following and **press** Enter, to list all of the files and folders in your present working directory. root@kali2:-/Captures# `ls`

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

```
      Master Key     : 97 13 2B 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 BD F7 B4
                       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
root@kali2:~/Captures# airdecap-ng -e SECURETWO -P boneless wpacapture.cap
airdecap-ng: invalid option -- 'P'
"airdecap-ng --help" for help.
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
root@kali2:~/Captures# ls
flag2.txt       wepcapture.cap      Wordlist.txt    wpacapture-dec.cap
sampleflag.txt  wepcapture-dec.cap  wpacapture.cap
root@kali2:~/Captures#
```



Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

11 **Type** the following command and **press** Enter, to open the decrypted capture file using Wireshark.

root@kali2:~/Captures# `wireshark wpacapture-dec.cap`

```
root@kali2:~/Captures# wireshark wpacapture-dec.cap
```

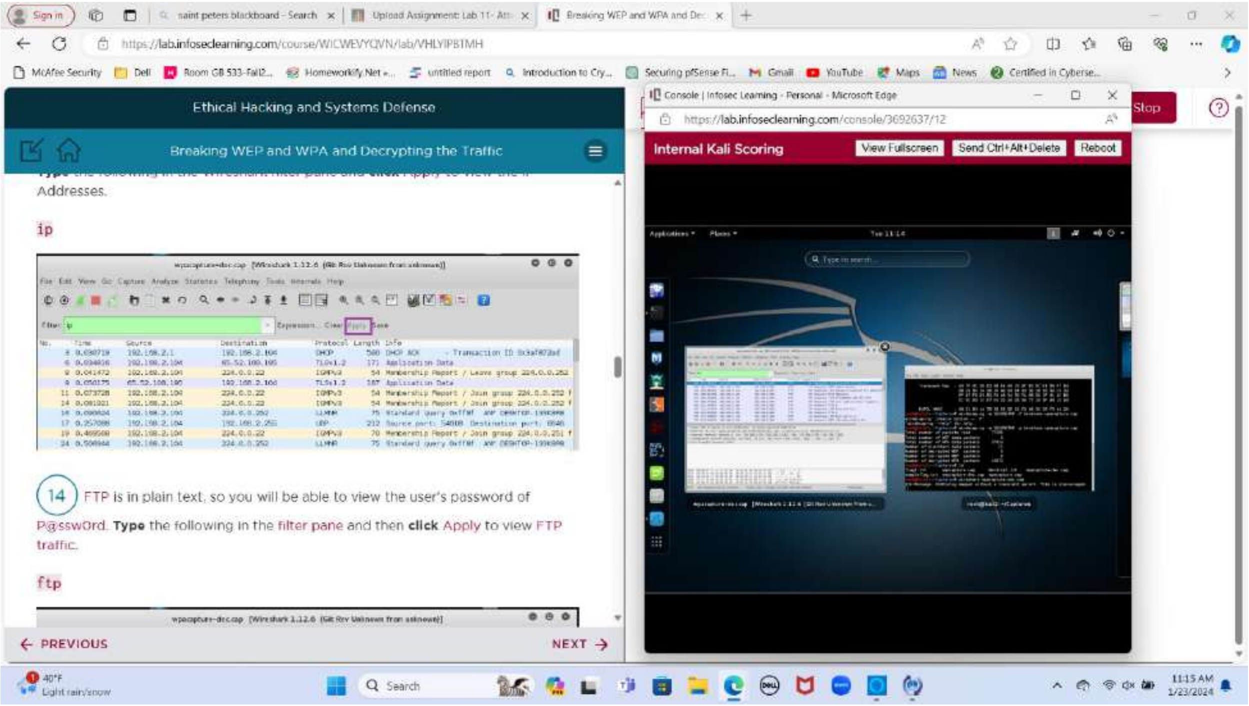
12 **Click** OK to the Lua Error when Wireshark opens.

Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.

OK

13 If all of the traffic was encrypted, you would not be able to see IP Addresses

```
      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 [illegible] 56 25 F9 AA 29
root@kali2:~/                                                        re.cap
airdecap-ng:
"airdecap-ng
root@kali2:~/                                                        re.cap
Total number
Total number
Total number
Number of pla
Number of decrypted WEP  p
Number of corrupted WEP  p
Number of decrypted WPA  packets    10872
root@kali2:~/Captures# ls
flag2.txt       wepcapture.cap      Wordlist.txt    wpacapture-dec.cap
sampleflag.txt  wepcapture-dec.cap  wpacapture.cap
root@kali2:~/Captures# wireshark wpacapture-dec.cap
Gtk-Message: GtkDialog mapped without a transient parent. This is discouraged.
```


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att...
Breaking WEP and WPA and Dec...
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Tue 11:14
Type to search...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
PREVIOUS
NEXT
40°F
Light rain/snow
Search
11:15 AM
1/23/2024

Ethical Hacking and Systems Defense

Breaking WEP and WPA and Decrypting the Traffic

Addresses.

`ip`

wpacapture-dec.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

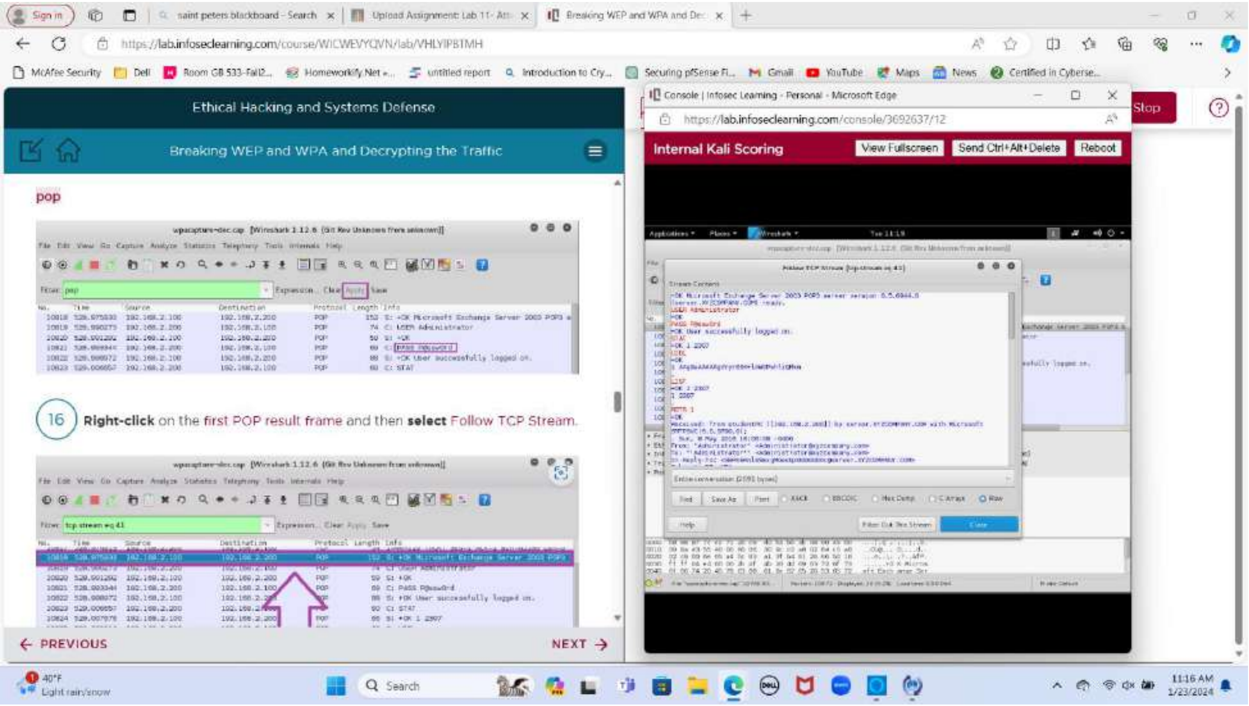
Filter: ip

```
No.  Time      Source          Destination     Protocol Length Info
  3 0.030719  192.168.2.1     192.168.2.104   DHCP       590 DHCP ACK      - Transaction ID 0x3af872af
  6 0.034016  192.168.2.104   65.52.108.195   TLSv1.2    171 Application Data
  8 0.041472  192.168.2.104   224.0.0.22      IGMPv3      54 Membership Report / Leave group 224.0.0.252
  9 0.050175  65.52.108.195   192.168.2.104   TLSv1.2    187 Application Data
 11 0.073728  192.168.2.104   224.0.0.22      IGMPv3      54 Membership Report / Join group 224.0.0.252 f
 14 0.081021  192.168.2.104   224.0.0.22      IGMPv3      54 Membership Report / Join group 224.0.0.252 f
 16 0.090024  192.168.2.104   224.0.0.252     LLMNR       75 Standard query 0xff8f  ANY DESKTOP-1998RRR
 17 0.257088  192.168.2.104   192.168.2.255   UDP        212 Source port: 54808  Destination port: 8848
 19 0.409568  192.168.2.104   224.0.0.22      IGMPv3      70 Membership Report / Join group 224.0.0.251 f
 24 0.508944  192.168.2.104   224.0.0.252     LLMNR       75 Standard query 0xff8f  ANY DESKTOP-1998RRR
```

14 FTP is in plain text, so you will be able to view the user's password of P@sswOrd. **Type** the following in the filter pane and then **click** Apply to view FTP traffic.

`ftp`

wpacapture-dec.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]



pop

wpacapture-dec.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

Filter: pop

```
No.    Time        Source          Destination     Protocol Length Info
 10818 528.975830  192.168.2.100   192.168.2.200   POP        152  S: +OK Microsoft Exchange Server 2003 POP3 s
 10819 528.990275  192.168.2.200   192.168.2.100   POP         74  C: USER Administrator
 10820 528.991202  192.168.2.100   192.168.2.200   POP         59  S: +OK
 10821 528.999344  192.168.2.200   192.168.2.100   POP         69  C: PASS P@ssw0rd
 10822 528.999972  192.168.2.100   192.168.2.200   POP         88  S: +OK User successfully logged on.
 10823 529.006657  192.168.2.200   192.168.2.100   POP         60  C: STAT
```

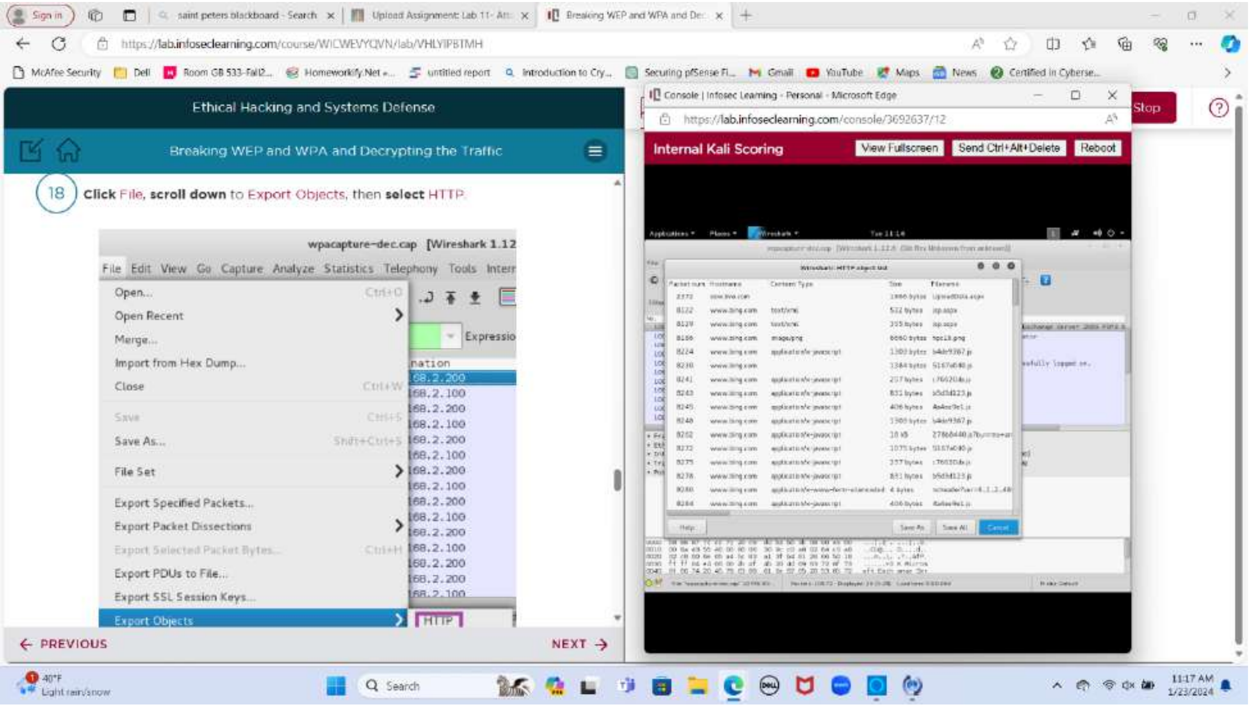
16 **Right-click** on the first POP result frame and then **select** Follow TCP Stream.

wpacapture-dec.cap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

Filter: tcp.stream eq 41

```
No.    Time        Source          Destination     Protocol Length Info
 10818 528.975830  192.168.2.100   192.168.2.200   POP        152  S: +OK Microsoft Exchange Server 2003 POP3
 10819 528.990275  192.168.2.200   192.168.2.100   POP         74  C: USER Administrator
 10820 528.991202  192.168.2.100   192.168.2.200   POP         59  S: +OK
 10821 528.993344  192.168.2.200   192.168.2.100   POP         69  C: PASS P@ssw0rd
 10822 528.999972  192.168.2.100   192.168.2.200   POP         88  S: +OK User successfully logged on.
 10823 529.006657  192.168.2.200   192.168.2.100   POP         60  C: STAT
 10824 529.007078  192.168.2.100   192.168.2.200   POP         66  S: +OK 1 2907
```

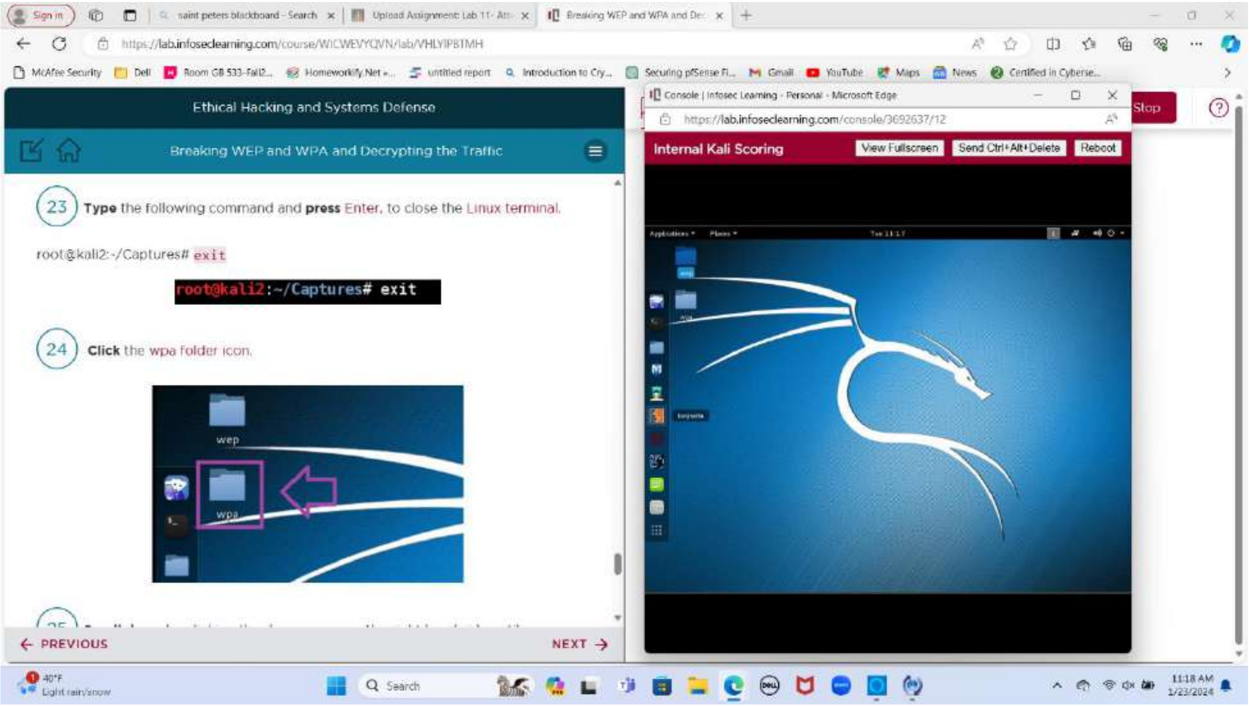
```
+OK Microsoft Exchange Server 2003 POP3 server version 6.5.6944.0
(server.XYZCOMPANY.COM) ready.
USER Administrator
+OK
PASS P@ssw0rd
+OK User successfully logged on.
STAT
+OK 1 2907
UIDL
+OK
1 AAQkADAAAgAAAAAAAAAAAAAAAAA
.
LIST
+OK 1 2907
1 2907
.
RETR 1
+OK
Received: from studentPC ([192.168.2.200]) by server.XYZCOMPANY.COM with Microsoft
SMTPSVC(6.0.3790.0);
  Sun, 8 May 2016 16:08:08 -0000
From: "Administrator" <Administrator@xyzcompany.com>
To: "Administrator" <Administrator@xyzcompany.com>
In-Reply-To: <...@server.XYZCOMPANY.com>
```


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att...
Breaking WEP and WPA and Dec...
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/VHLYIPBTMH
Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692637/12
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Wireshark
Tue 11:14
Wireshark: HTTP object list
Help
Save As
Save All
Cancel
File Edit View Go Capture Analyze Statistics Telephony Tools Intern
Open... Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Selected Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
HTTP
Expressio
← PREVIOUS
NEXT →
40°F
Light rain/snow
Search
11:17 AM
1/23/2024

18 **Click** File, **scroll down** to Export Objects, then **select** HTTP.

wpacapture-dec.cap [Wireshark 1.12

Packet num	Hostname	Content Type	Size	Filename
2372	view.live.com		1996 bytes	UploadData.aspx
8122	www.bing.com	text/xml	512 bytes	isp.aspx
8129	www.bing.com	text/xml	355 bytes	isp.aspx
8186	www.bing.com	image/png	6660 bytes	sprite.png
8224	www.bing.com	application/x-javascript	1303 bytes	b4de9367.js
8230	www.bing.com		1384 bytes	5167a040.js
8241	www.bing.com	application/x-javascript	257 bytes	c76620de.js
8243	www.bing.com	application/x-javascript	831 bytes	b5d3d123.js
8245	www.bing.com	application/x-javascript	406 bytes	4a4ac9e1.js
8248	www.bing.com	application/x-javascript	1303 bytes	b4de9367.js
8252	www.bing.com	application/x-javascript	10 kB	27868440.js?bu=rms+ar
8272	www.bing.com	application/x-javascript	1075 bytes	5167a040.js
8275	www.bing.com	application/x-javascript	257 bytes	c76620de.js
8278	www.bing.com	application/x-javascript	831 bytes	b5d3d123.js
8280	www.bing.com	application/x-www-form-urlencoded	4 bytes	scheader?ver=6.1.2.48
8284	www.bing.com	application/x-javascript	406 bytes	4a4ac9e1.js

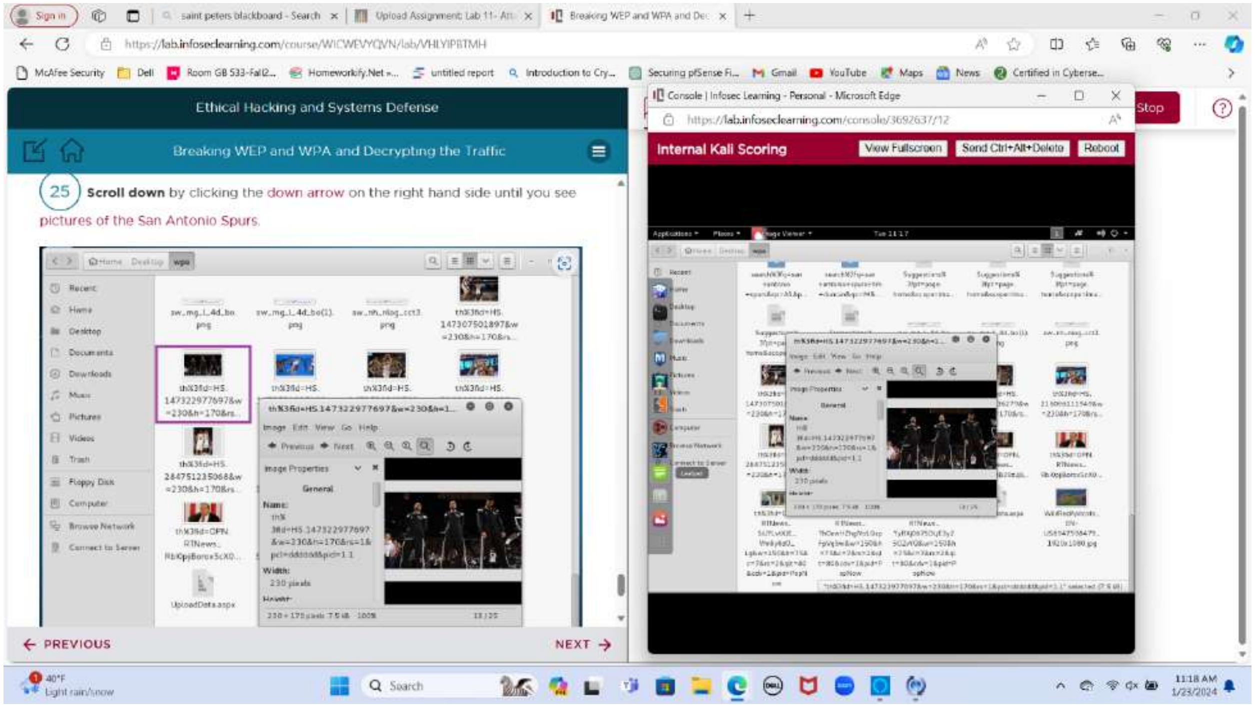

Ethical Hacking and Systems Defense
Breaking WEP and WPA and Decrypting the Traffic
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
wep
wpa
PREVIOUS
NEXT

23 **Type** the following command and **press** Enter, to close the Linux terminal.

```
root@kali2:~/Captures# exit
```

```
root@kali2:~/Captures# exit
```

24 **Click** the wpa folder icon.



25 **Scroll down** by clicking the down arrow on the right hand side until you see pictures of the San Antonio Spurs.

This is the last screen before the end of this lab.