



SECURITY+ V4 LAB SERIES

Lab 18: Wireless Networking Attack and Mitigation Techniques

Document Version: **2023-02-27**

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	3.4: Given a scenario, install and configure wireless security settings
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	20: Wireless Security

Copyright © 2023 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.
KALI LINUX™ is a trademark of Offensive Security.
Microsoft®, Windows®, and Windows Server® are trademarks of the Microsoft group of companies.
VMware is a registered trademark of VMware, Inc.
SECURITY ONION is a trademark of Security Onion Solutions LLC.
Android is a trademark of Google LLC.
pfSense® is a registered mark owned by Electric Sheep Fencing LLC ("ESF").
All trademarks are property of their respective owners.

Contents

Introduction	3
Objective	3
Lab Topology.....	4
Lab Settings.....	5
1 Examining Plain Text Traffic.....	6
1.1 Viewing Plain Text Wireless Traffic	6
1.1.1 Extract Image from Capture.....	8
1.1.2 Extract Zip File from FTP Traffic	12
2 Exploiting and Examining WEP Traffic	16
2.1 Decrypt and Analyze WEP Traffic.....	16
3 Exploiting and Examining WPA Traffic.....	24
3.1 Exploiting and Examining WPA Traffic	24

Introduction

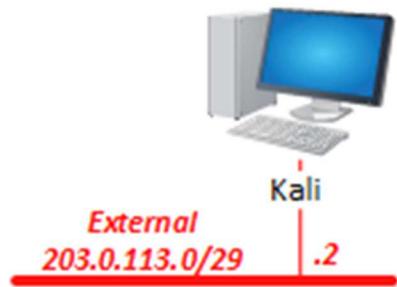
In this lab, you will be conducting wireless security practices using various tools.

Objective

In this lab, you will perform the following tasks:

- Examining Plain Text Traffic
- Exploiting and Examining WEP Traffic
- Exploiting and Examining WPA Traffic

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali	203.0.113.2	kali	kali

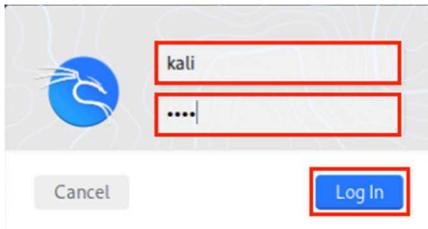
1 Examining Plain Text Traffic

1.1 Viewing Plain Text Wireless Traffic

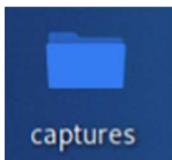
1. Click on the **Kali** tab to access the *Kali* VM.



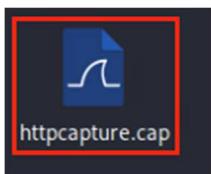
2. Log in to the *Kali* VM as username **kali**, password **kali**.



3. On the desktop, find and double-click to open the folder named **captures**.



4. In the pop-up window. Double-click the **httpcapture.cap** file to open it in *Wireshark*.



5. Click the **maximize** button shown on the screenshot to maximize the window to full-screen inside the VM.



6. Select the **first frame** in the *Wireshark* capture file.

A screenshot of the Wireshark application. The main pane displays a list of network frames. The first frame, which is a Beacon frame from 'Cisco-Li_01:bb:3e' to 'Broadcast' on port 802.11, is highlighted with a red box. The details and bytes panes below show the frame's structure.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_01:bb:3e	Broadcast	802.11	125	Beacon frame, SN=682, FN=0, Flags=..., BI=100, SSID=NetLab-WirelessHacking
2	0.310689	192.168.0.166	224.0.0.251	MDNS	396	Standard query response 0x0000 TXT, cache flush PTR _apple-mobdev2._tcp.local PTR 1c:36:
3	0.314300	fe80::1cc1:20c1:34c...	ff02::fb	MDNS	416	Standard query response 0x0000 TXT, cache flush PTR _apple-mobdev2._tcp.local PTR 1c:36:
4	0.820245	Tp-LinkT_71:42:08	Broadcast	ARP	98	Who has 192.168.0.101? Tell 192.168.0.1

7. In the middle of the screen, click the arrow icon in front of the *IEEE 802.11 Wireless Management* to expand its view.

```
20 1.447328 Cisco-EI_01.00.3e SamsungE73.a7.5a 802.11 119 Probe Resp
  ▶ Frame 1: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits)
  ▶ IEEE 802.11 Beacon frame, Flags: .....
  ▶ IEEE 802.11 Wireless Management
```

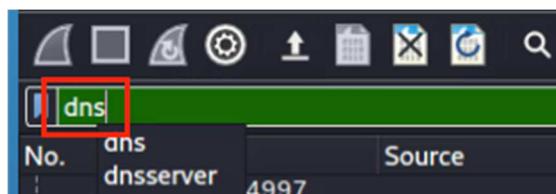
8. Dive in further by clicking the arrow icon in front of *Tagged parameters* followed by clicking the **arrow** icon in front of *Tag: Vender Specific: Microsoft Corp.: WPA Information Element*. View the *WPA Version*.

```
▶ Frame 1: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits)
▶ IEEE 802.11 Beacon frame, Flags: .....
IEEE 802.11 Wireless Management
  ▶ Fixed parameters (12 bytes)
    ▶ Tagged parameters (89 bytes)
      ▶ Tag: SSID parameter set: NetLab-WirelessHacking
      ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24(B), 36, 54, [Mbit/sec]
      ▶ Tag: DS Parameter set: Current Channel: 7
      ▶ Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
      ▶ Tag: ERP Information
      ▶ Tag: ERP Information
      ▶ Tag: Extended Supported Rates 6(B), 9, 12(B), 48, [Mbit/sec]
      ▶ Tag: Vendor Specific: Broadcom
      ▶ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
        Tag Number: Vendor Specific (221)
        Tag length: 24
        OUI: 00:50:f2 (Microsoft Corp.)
        Vendor Specific OUI Type: 1
        Type: WPA Information Element (0x01)
        ▶ WPA Version: 1
          Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) TKIP
          Unicast Cipher Suite Count: 1
          ▶ Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) TKIP
```

Drag the handle to make the packet detail section area larger.

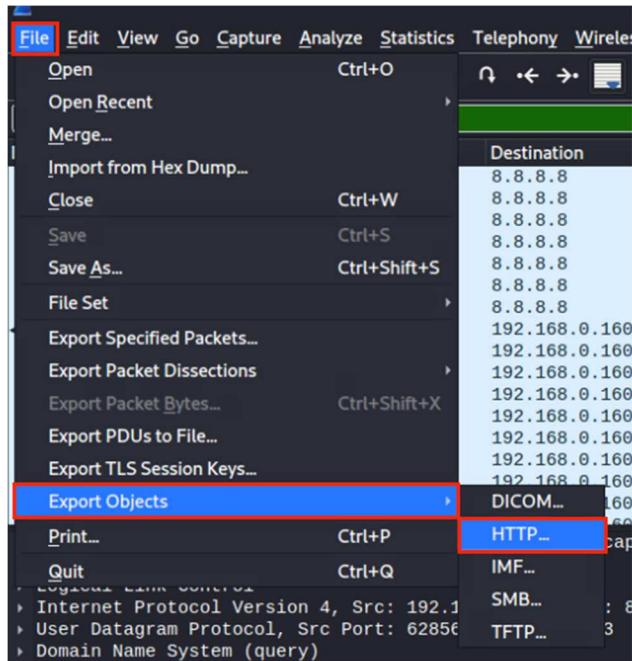
```
7:9a 802.11 119 Probe Response, SN=703, FN=0, Flags=....R.
7:00 802.11 119 Probe Response, SN=703, FN=0, Flags=....R.
red (1000 bits)
```

9. View captured *DNS requests* by typing *dns* in the *Filter pane*, then press **Enter**.



1.1.1 Extract Image from Capture

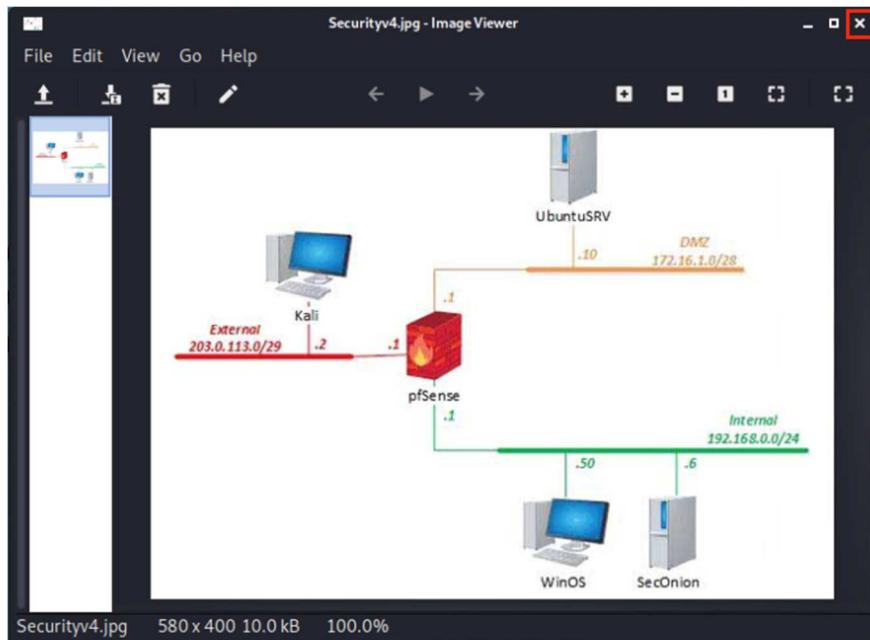
- With *Wireshark*, we can export images and files that have passed through the capture communication channel. Try exporting a file by clicking on the **File** menu option on the top pane and navigating to **Export Objects > HTTP**.



- A new window appears. Look through the list of files that have been downloaded by wireless users. Under the *Filename* column, find the image file **Securityv4.jpg** and select the file. (Or, find the number 5393 under the *Packet* column.). With the file selected, click the **Preview** button.

Wireshark - Export - HTTP object list					
Text Filter:		Content Type: All Content-Types			
Packet	Hostname	Content Type	Size	Filename	
4533	3.93.56.222		1,415 bytes	ndg.css	
4541	3.93.56.222		1,428 bytes	ndg.css	
4756	3.93.56.222		1,428 bytes	ndg.css	
4764	3.93.56.222		1,419 bytes	ndg.css	
4769	3.93.56.222		1,428 bytes	ndg.css	
4803	3.93.56.222	application/javascript	985 bytes	jquery.browser.js	
4982	3.93.56.222		1,428 bytes	affix.js	
4986	3.93.56.222		265 bytes	affix.js	
5177	3.93.56.222	application/javascript	1,039 bytes	default.js	
5273	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5278	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3	
5361	3.93.56.222	image/svg+xml	1,749 bytes	ndg_logo.svg	
5365	3.93.56.222	image/svg+xml	1,728 bytes	ndg_logo_light.svg	
5369	3.93.56.222	image/png	1,909 bytes	email_light.png	
5393	3.93.56.222	image/jpeg	10kB	Securityv4.jpg	
5854	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5866	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5870	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3	
5874	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5890	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5898	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3	

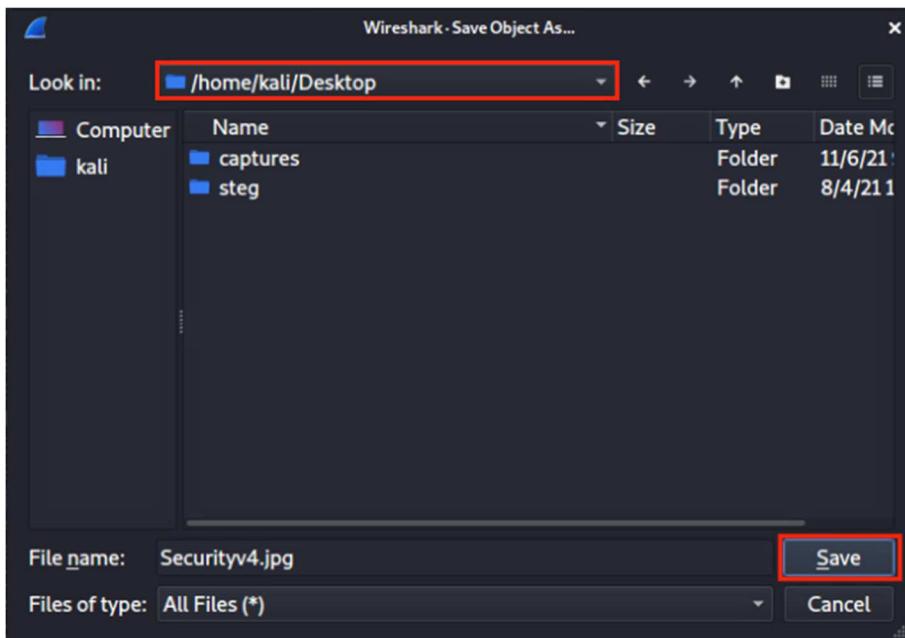
3. A preview window will open, showing a topology. Click the X to close the preview. Feel free to select and preview other image files being captured. Close the preview window once you finish examining them.



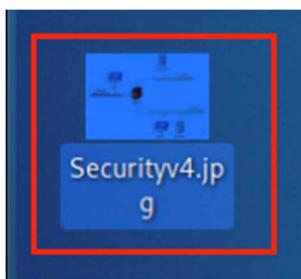
4. Alternatively, you can choose to save the *Securityv4.jpg* file. Having the file selected, click the **Save** button.

Wireshark · Export · HTTP object list					
Packet	Hostname	Content Type	Size	Filename	
4533	3.93.56.222		1,415 bytes	ndg.css	
4541	3.93.56.222		1,428 bytes	ndg.css	
4756	3.93.56.222		1,428 bytes	ndg.css	
4764	3.93.56.222		1,419 bytes	ndg.css	
4769	3.93.56.222		1,428 bytes	ndg.css	
4803	3.93.56.222	application/javascript	985 bytes	jquery.browser.js	
4982	3.93.56.222		1,428 bytes	affix.js	
4986	3.93.56.222		265 bytes	affix.js	
5177	3.93.56.222	application/javascript	1,039 bytes	default.js	
5273	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5278	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3	
5361	3.93.56.222	image/svg+xml	1,749 bytes	ndg_logo.svg	
5365	3.93.56.222	image/svg+xml	1,728 bytes	ndg_logo_light.svg	
5369	3.93.56.222	image/png	1,909 bytes	email_light.png	
5393	3.93.56.222	image/jpeg	10kB	Securityv4.jpg	
5854	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5866	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5870	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3	
5874	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5890	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3	
5898	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3	

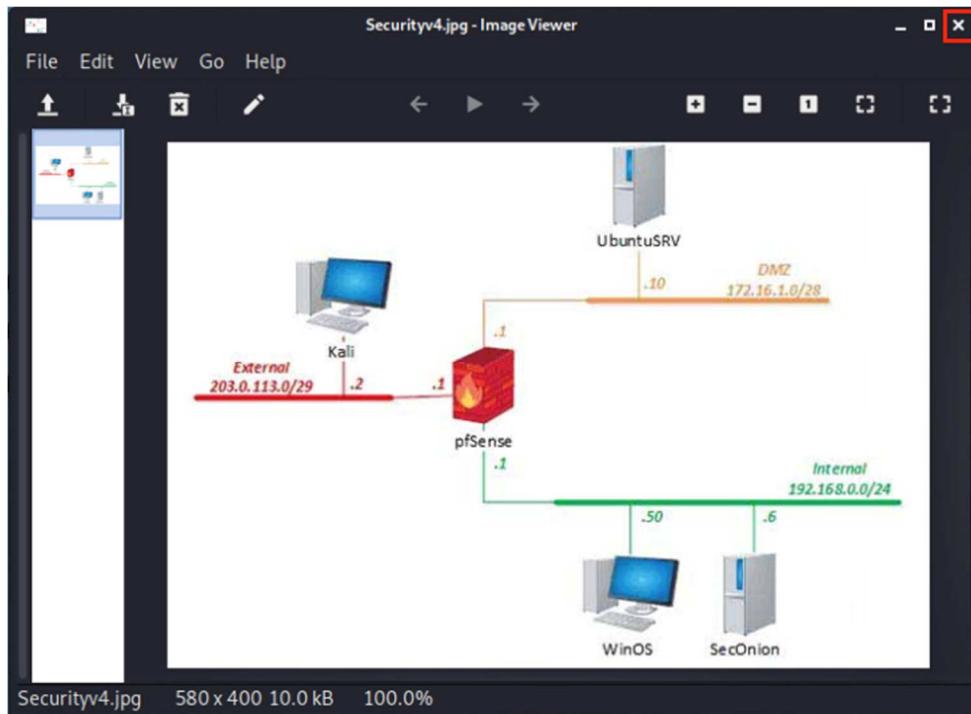
- In the **Save Object As** window, choose the **/home/kali/Desktop** directory to save to and click the **Save** button.



- View the image by selecting the **Show desktop** menu option located next to the *Applications* menu. Double-click to open **Securityv4.jpg**.



7. The same topology image opens. **Close** the *image viewer*.



8. Click the **Show** desktop button again to restore the windows. Close the *HTTP object list* window.

Packet	Hostname	Content Type	Size	Filename
4533	3.93.56.222		1,415 bytes	ndg.css
4541	3.93.56.222		1,428 bytes	ndg.css
4756	3.93.56.222		1,428 bytes	ndg.css
4764	3.93.56.222		1,419 bytes	ndg.css
4769	3.93.56.222		1,428 bytes	ndg.css
4803	3.93.56.222	application/javascript	985 bytes	jquery.browser.js
4982	3.93.56.222		1,428 bytes	affix.js
4986	3.93.56.222		265 bytes	affix.js
5177	3.93.56.222	application/javascript	1,039 bytes	default.js
5273	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3
5278	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3
5361	3.93.56.222	image/svg+xml	1,749 bytes	ndg_logo.svg
5365	3.93.56.222	image/svg+xml	1,728 bytes	ndg_logo_light.svg
5369	3.93.56.222	image/png	1,909 bytes	email_light.png
5393	3.93.56.222	image/jpeg	10kB	Securityv4.jpg
5854	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3
5866	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3
5870	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3
5874	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3
5890	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1c3
5898	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1c3

1.1.2 Extract Zip File from FTP Traffic

- Within the *Wireshark* interface, type **ftp** into the *Filter:* and press **Enter**. Because FTP is not encrypted, you will be able to see captured FTP traffic as well as clear-text usernames and passwords. Analyze the FTP traffic.



You will want to disable the anonymous user access and use a secured FTP service for file sharing.

No.	Time	Source	Destination	Protocol	Length Info
1259 16.405870	3.93.56.222	192.168.0.105		FTP	131 Response: 220 Microsoft FTP Service
1338 20.016354	192.168.0.105	3.93.56.222		FTP	120 Request: USER anonymous
1347 20.064301	3.93.56.222	192.168.0.105		FTP	176 Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
1442 22.816660	192.168.0.105	3.93.56.222		FTP	120 Request: PASS anonymous
1446 22.863941	3.93.56.222	192.168.0.105		FTP	125 Response: 230 User logged in.
1450 22.865191	192.168.0.105	3.93.56.222		FTP	110 Request: SYST
1452 22.911642	3.93.56.222	192.168.0.105		FTP	120 Response: 215 Windows_NT
1725 30.152244	192.168.0.105	3.93.56.222		FTP	131 Request: PORT 192,168,0,105,130,91
1733 30.199962	3.93.56.222	192.168.0.105		FTP	134 Response: 200 PORT command successful.
1741 30.201196	192.168.0.105	3.93.56.222		FTP	121 Request: RETR images.zip
1747 30.249850	3.93.56.222	192.168.0.105		FTP	158 Response: 125 Data connection already open; Transfer starting.
1958 30.440198	3.93.56.222	192.168.0.105		FTP	128 Response: 226 Transfer complete.
2562 56.187777	192.168.0.105	3.93.56.222		FTP	132 Request: PORT 192,168,0,105,151,129
2563 56.235175	3.93.56.222	192.168.0.105		FTP	134 Response: 200 PORT command successful.
2575 56.236284	192.168.0.105	3.93.56.222		FTP	121 Request: RETR images.zip

Frame 1259: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits)
 > IEEE 802.11 Data, Flags: .p....F.
 > Logical-Link Control
 > Internet Protocol Version 4, Src: 3.93.56.222, Dst: 192.168.0.105
 > Transmission Control Protocol, Src Port: 21, Dst Port: 37536, Seq: 1, Ack: 1, Len: 27
 > File Transfer Protocol (FTP)
 [Current working directory:]

- Next, we will pull a zip file via *FTP* out of the wireless capture file. Type **ftp-data** and **frame contains PK** into the *Wireshark Filter:* and press **Enter**.



You will want to disable the anonymous user access and use a secured FTP service for file sharing.

No.	Time	Source	Destination	Protocol	Length Info
1886 30.383167	3.93.56.222	192.168.0.105		FTP-DA...	1532 FTP Data: 1440 bytes (PORT) (RETR images.zip)
2746 56.482515	3.93.56.222	192.168.0.105		FTP-DA...	1532 FTP Data: 1440 bytes (PORT) (RETR images.zip)

- Right-click on either the **frame 1886** or **2746** in the list and select **Follow, TCP Stream**.



You will want to disable the anonymous user access and use a secured FTP service for file sharing.

No.	Time	Source	Destination	Protocol	Length Info
1886 30.383167	3.93.56.222	192.168.0.105		FTP-DA...	1532 FTP Data: 1440 bytes (PORT) (RETR images.zip)
2746 56.482515	3.93.56.222	192.168.0.105		FTP-DA...	1532 FTP Data: 1440 bytes (PORT) (RETR images.zip)

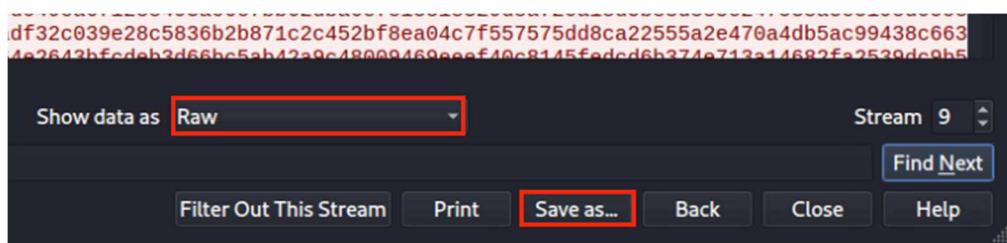
Frame 1886: 1532 bytes on wire (12256 bits), 1532 bytes captured (12256 bits)
 > IEEE 802.11 Data, Flags: .p....F.
 > Logical-Link Control
 > Internet Protocol Version 4, Src: 3.93.56.222, Dst: 192.168.0.105
 > Transmission Control Protocol, Src Port: 21 (Setup frame: 1725)
 > Dest Port: 2 (Setup method: PORT)
 > Length: 1532 (1440 bytes data)
 > Command: RETR images.zip
 > Command frame: 1741

Mark/Unmark Packet Ctrl+M
 Ignore/Unignore Packet Ctrl+D
 Set/Unset Time Reference Ctrl+T
 Time Shift... Ctrl+Shift+T
 Packet Comment... Ctrl+Alt+C
 Edit Resolved Name
 Apply as Filter
 Prepare as Filter
 Conversation Filter
 Colorize Conversation
 SCTP
 Follow Ctrl+Alt+Shift+T
 Copy
 Protocol Preferences
 Decode As...
 Show Packet in New Window
 UDP Stream Ctrl+Alt+Shift+U
 TLS Stream Ctrl+Alt+Shift+S
 HTTP Stream Ctrl+Alt+Shift+H
 HTTP/2 Stream
 QUIC Stream

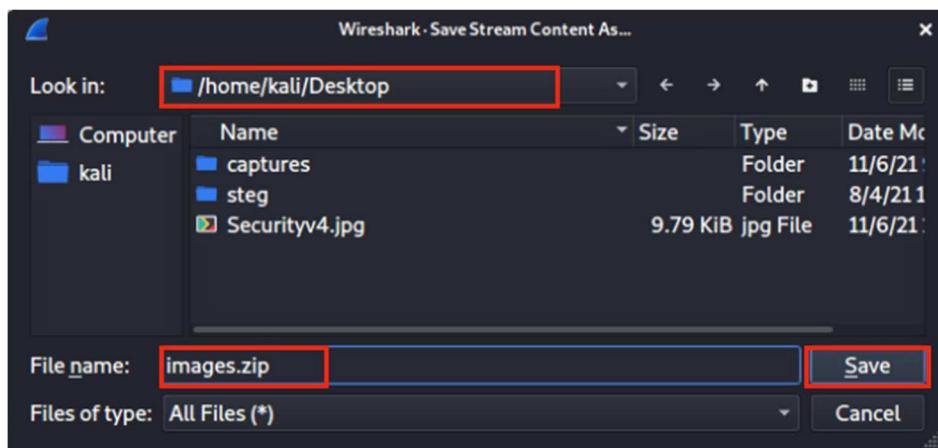
4. Examine the data shown in the *TCP stream*. Scroll to the bottom of the window and notice the *PK* attached to the end of filenames.



5. Within the *Follow TCP Stream* window, click **Show data as Raw**, then click **Save As...**.



- Type **images.zip** in the **Name** text field. Set the save destination to **/home/kali/Desktop** and click the **Save** button.

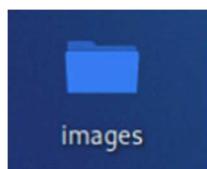


- Close** the *Follow TCP Stream* window.
- Open a new *Terminal* window and type the command below to **unzip** the file that was just pulled from the *Wireshark* capture file.

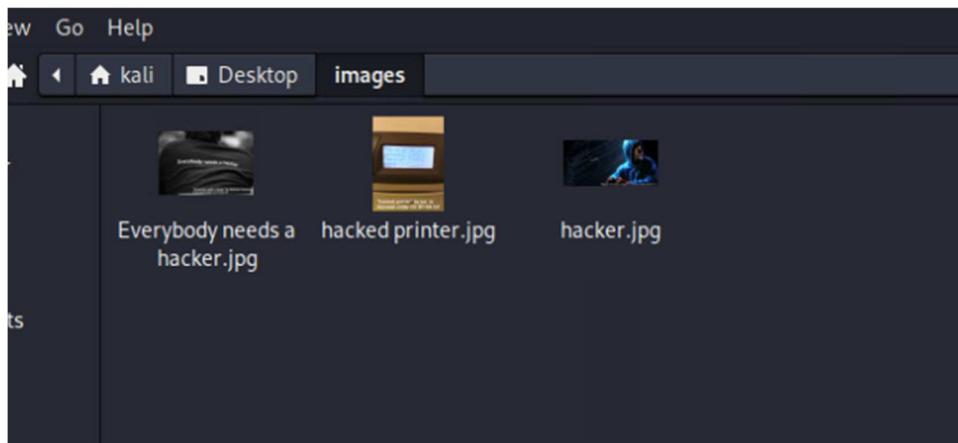
```
kali@kali$ unzip ~/Desktop/images.zip -d ~/Desktop
```

```
(kali㉿kali)-[~]
$ unzip ~/Desktop/images.zip -d ~/Desktop
Archive: /home/Kali/Desktop/images.zip
  inflating: /home/Kali/Desktop/images/Everybody needs a hacker.jpg
  inflating: /home/Kali/Desktop/images/hacked printer.jpg
  inflating: /home/Kali/Desktop/images/hacker.jpg
```

- Select the **Show desktop** menu option from the top menu pane and double-click on the **images** Folder.



10. Notice the three different image files in the **images** directory that were extracted from *images.zip*.
Feel free to open each of them and check the content.

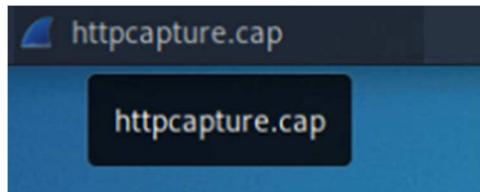


11. Close the *images* window.
12. Leave the *Kali* window open to continue with the next task.

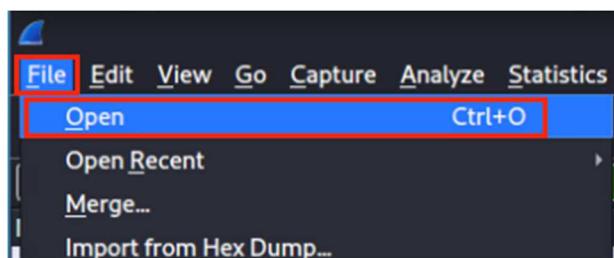
2 Exploiting and Examining WEP Traffic

2.1 Decrypt and Analyze WEP Traffic

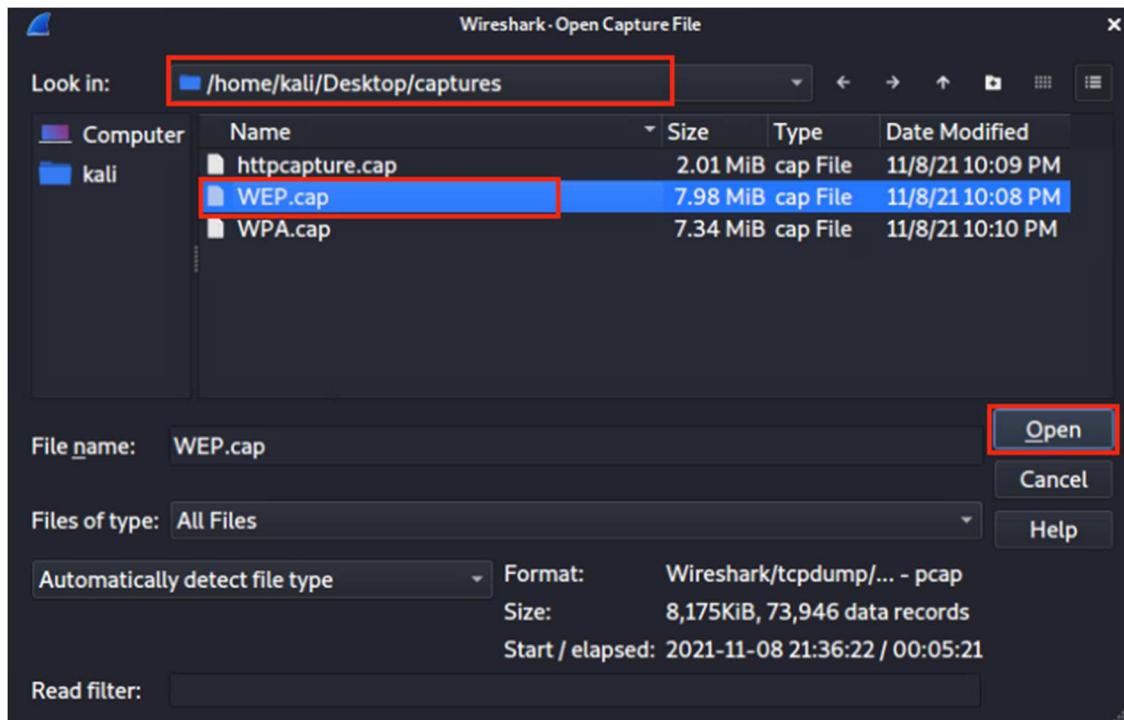
1. Click on the **httpcapture.cap** Wireshark window to restore it.



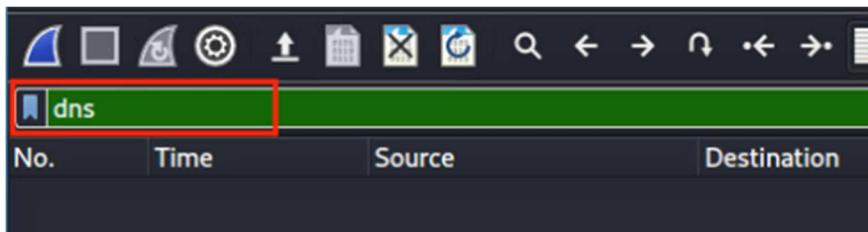
2. Select the **File** menu option and click on **Open**.



3. A new window appears. Verify that you are in the **/home/kali/Desktop/captures** directory. Select the **WEP.cap** file and click the **Open** button.



4. In the *Filter*: pane, type dns and press **Enter**.



You will not see any traffic displayed because the wireless traffic is encrypted.

5. Close the **Wireshark** application by selecting the **File** menu option and clicking on **Quit**.
6. Change focus to the **terminal** window and enter the command as shown below.

```
kali㉿kali$ aircrack-ng ~/Desktop/captures/WEP.cap
```



7. After a few seconds, the *aircrack-ng* program will be able to crack the *64-bit WEP key*. Notice the output.

```
Aircrack-ng 1.6

[00:00:02] Tested 8694 keys (got 15851 IVs)

KB      depth   byte(vote)
0       4/ 5    6B(20480) 23(19968) 91(19712) EA(19712) 2B(19456) 7E(19456)
1       0/ 2    33(22784) E5(22016) 15(20480) 42(20480) DE(20480) AD(20224)
2       17/ 22   6C(18944) E8(18944) 14(18944) 27(18944) 84(18944) 18(18688)
3       0/ 4    33(22784) 98(21504) D0(21248) 9E(20992) D3(20736) AD(20480)
4       7/ 10   30(20480) 4C(20224) 5E(20224) 34(19968) 04(19712) 57(19712)

KEY FOUND! [ 6B:33:6C:33:21 ] (ASCII: k3l3! )
Decrypted correctly: 100%
```

8. After the *WEP* key is obtained, decrypt the network traffic with **airdecap-ng**. Enter the command shown below to decrypt the traffic.

```
kali㉿kali:~$ airdecap-ng -w 6B:33:6C:33:21 ~/Desktop/captures/WEP.cap
```

```
(kali㉿kali)-[~]
$ 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
```

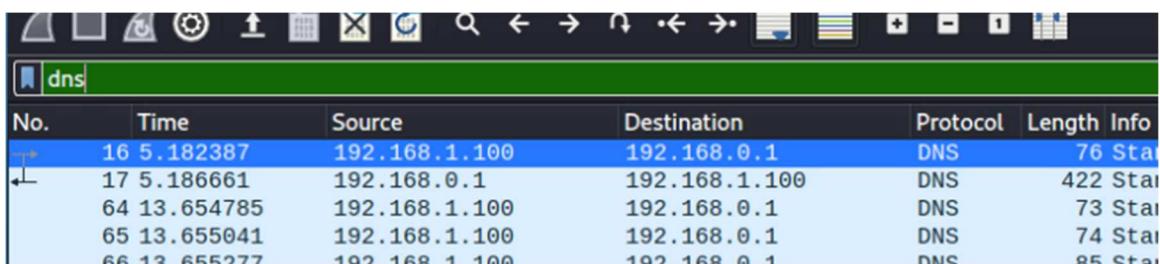


The number of *decrypted WEP packets* should be 37612.

9. Analyze the decrypted traffic with *Wireshark*. Change the focus to the captures window, double-click the **WEP-dec.cap** to open it in *Wireshark*.

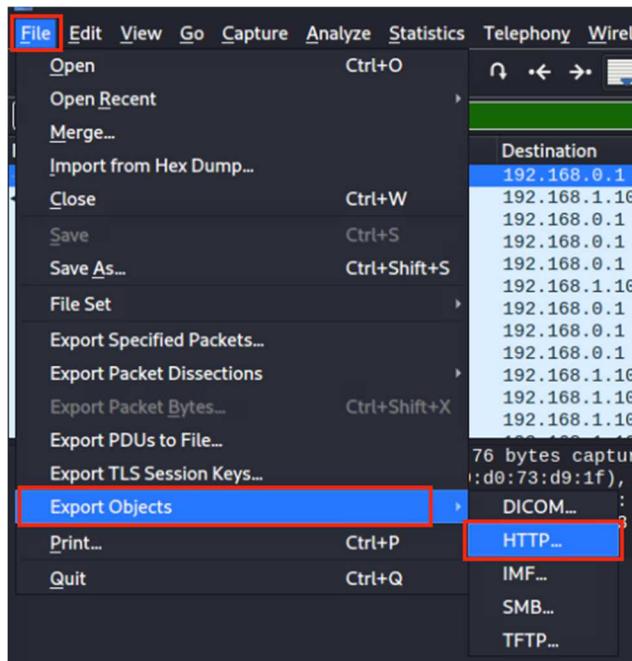


10. In the *Filter*: pane, type **dns** and press **Enter**.



Notice that you can now see the *DNS* requests within the wireless traffic because the *WEP* traffic was decrypted with *airdecap-ng*.

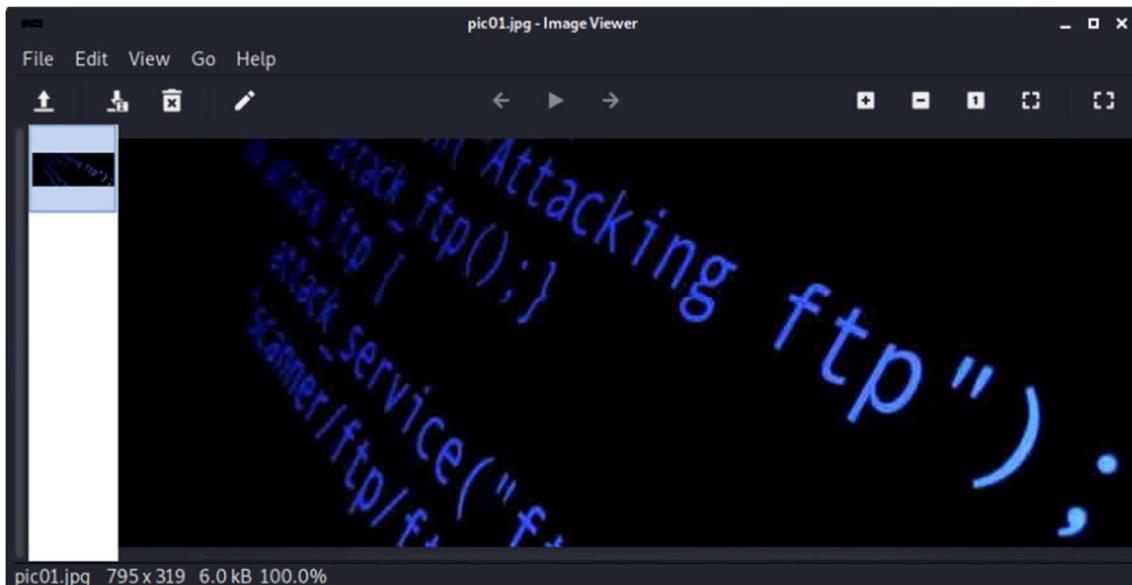
11. Select the **File** menu option and navigate to **Export Objects > HTTP**.



12. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, select item #33076 (**pic01.jpg**). Once selected, click the **Preview** button.

Wireshark · Export · HTTP object list				
Text Filter:		Content Type: All Content-Types		
Packet	Hostname	Content Type	Size	Filename
33068	3.92.4.86:8000	image/jpeg	8,904 bytes	pic02.jpg
33076	3.92.4.86:8000	image/jpeg	5,965 bytes	pic01.jpg
33088	3.92.4.86:8000	image/jpeg	9,697 bytes	pic03.jpg
33197	3.92.4.86:8000	application/javascript	9,085 bytes	skel.min.js
33209	3.92.4.86:8000	application/javascript	12kB	util.js
33268	3.92.4.86:8000		1,428 bytes	main.js
33272	3.92.4.86:8000		1,428 bytes	main.js
33273	3.92.4.86:8000		471 bytes	main.js
33312	3.92.4.86:8000		1,428 bytes	overlay.png
33555	3.92.4.86:8000	image/jpeg	5,965 bytes	pic01.jpg
33672	3.92.4.86:8000	text/css	32kB	main.css
33679	3.92.4.86:8000		1,428 bytes	pic02.jpg
33682	3.92.4.86:8000		1,428 bytes	pic02.jpg
33686	3.92.4.86:8000		562 bytes	pic02.jpg
33693	3.92.4.86:8000	image/jpeg	5,965 bytes	pic01.jpg
33742	3.92.4.86:8000		481 bytes	jquery.min.js
33812	3.92.4.86:8000	application/javascript	9,085 bytes	skel.min.js
33824	3.92.4.86:8000	application/javascript	12kB	util.js
33882	3.92.4.86:8000	text/css	29kB	font-awesome.min.css
33978	3.92.4.86:8000	image/png	4,385 bytes	overlay.png
34223	3.92.4.86:8000	image/jpeg	5,965 bytes	pic01.jpg
34270	3.92.4.86:8000		5,965 bytes	pic01.jpg

13. The *Image Viewer* window opens, showing the image content.



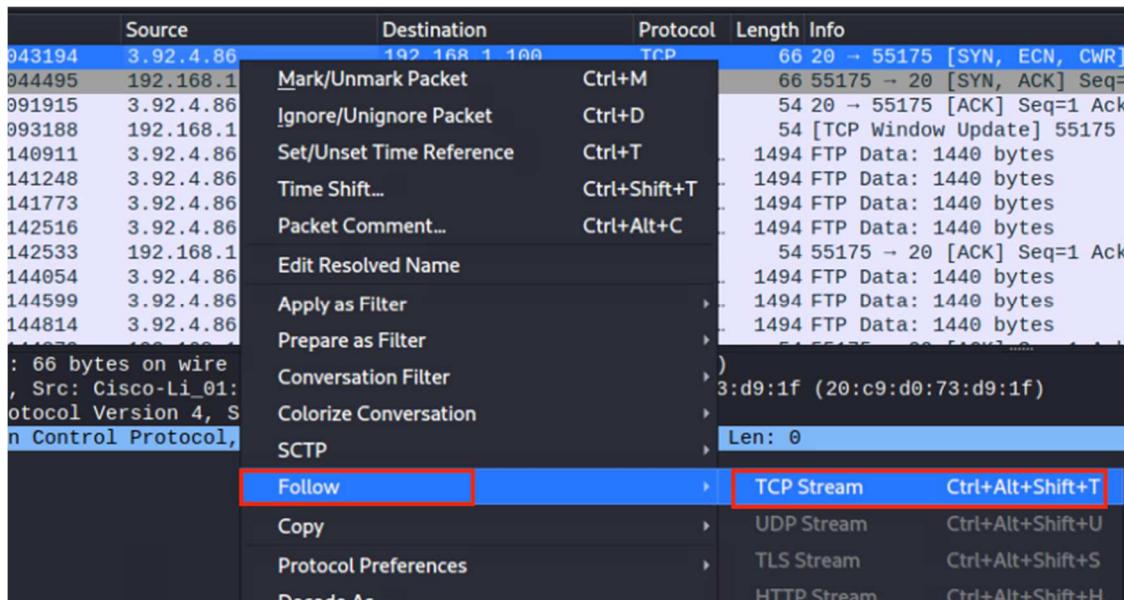
14. Close the *Image Viewer* window.
 15. Close the HTTP object list window.
 16. Change focus to the **Wireshark** application and type **ftp** into the *Filter:* pane. Click **Apply**. You will be able to see decrypted FTP traffic as well as clear-text usernames and passwords. Analyze the FTP traffic.

No.	Time	Source	Destination	Protocol	Length	Info
35011	186.001169	3.92.4.86	192.168.1.100	FTP	93	Response: 220 Microsoft FTP Service
35013	186.002838	192.168.1.100	3.92.4.86	FTP	82	Request: USER anonymous
35014	186.049287	3.92.4.86	192.168.1.100	FTP	138	Response: 331 Anonymous access allowed,
35016	186.050813	192.168.1.100	3.92.4.86	FTP	82	Request: PASS anonymous
35018	186.099244	192.168.1.100	3.92.4.86	FTP	71	[TCP ACKed unseen segment] Request: PWD

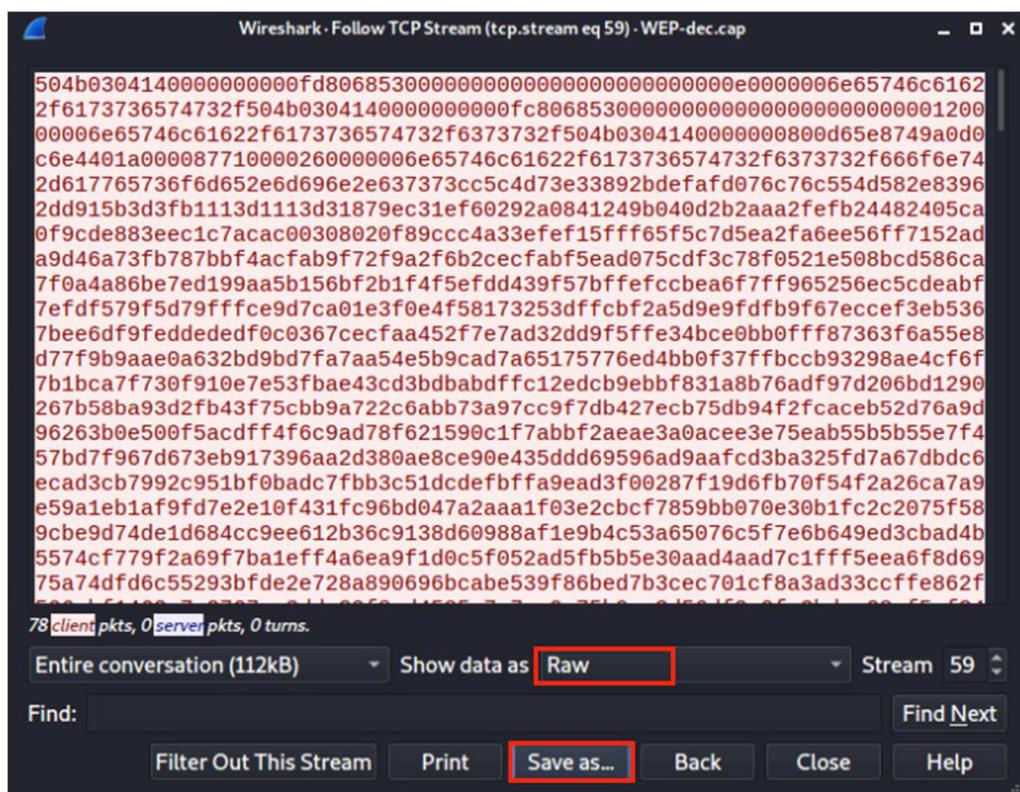
17. Let's pull a ZIP file transferred via *FTP* from the wireless capture. Type **tcp.stream eq 59** in the *Filter:* pane. Press **Enter**.

No.	Time	Source	Destination	Protocol
36301	262.043194	3.92.4.86	192.168.1.100	TCP

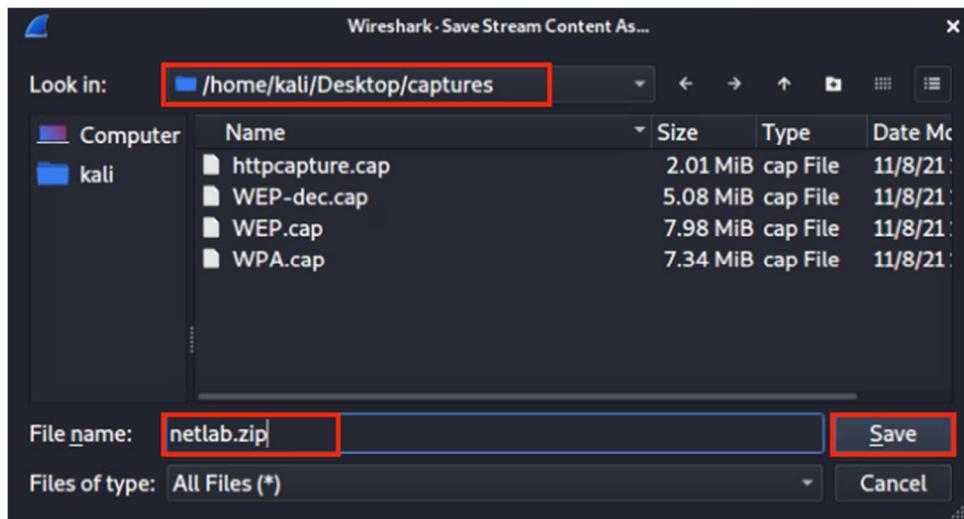
18. Right-click on the **first frame** in the list and select **Follow, TCP Stream**.



19. A new window appears. Change the *Show data as* to **Raw**, then click the **Save as** button.

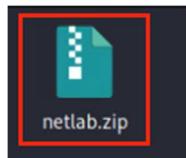


20. For the filename, type **netlab.zip**. Make sure the directory is set to **/home/kali/Desktop/captures** and click the **Save** button.

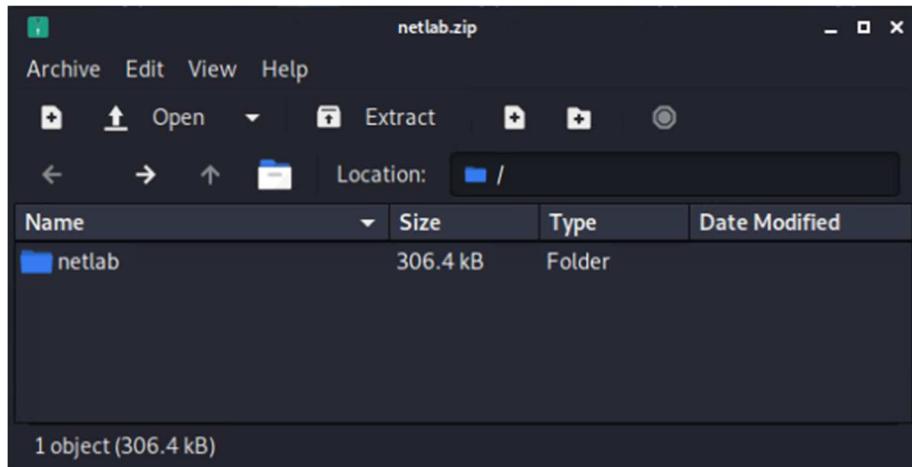


21. Close the *Follow TCP Stream* window.

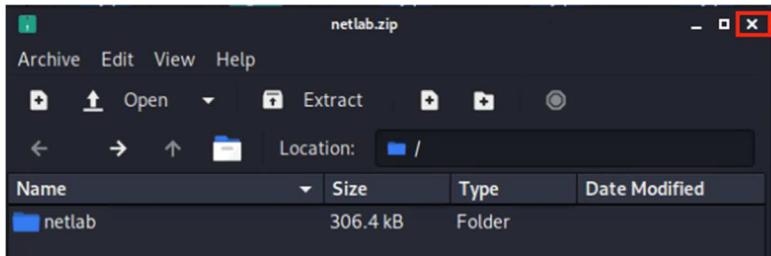
22. Change focus to the captures window. Double-click on the **netlab.zip** file to open it.



23. A new window opens, showing the content of the zip file. Feel free to check the content in the **netlab** folder.



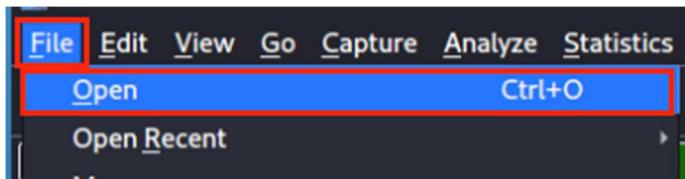
24. Once you finished observing the files, close the **netlab.zip** window.



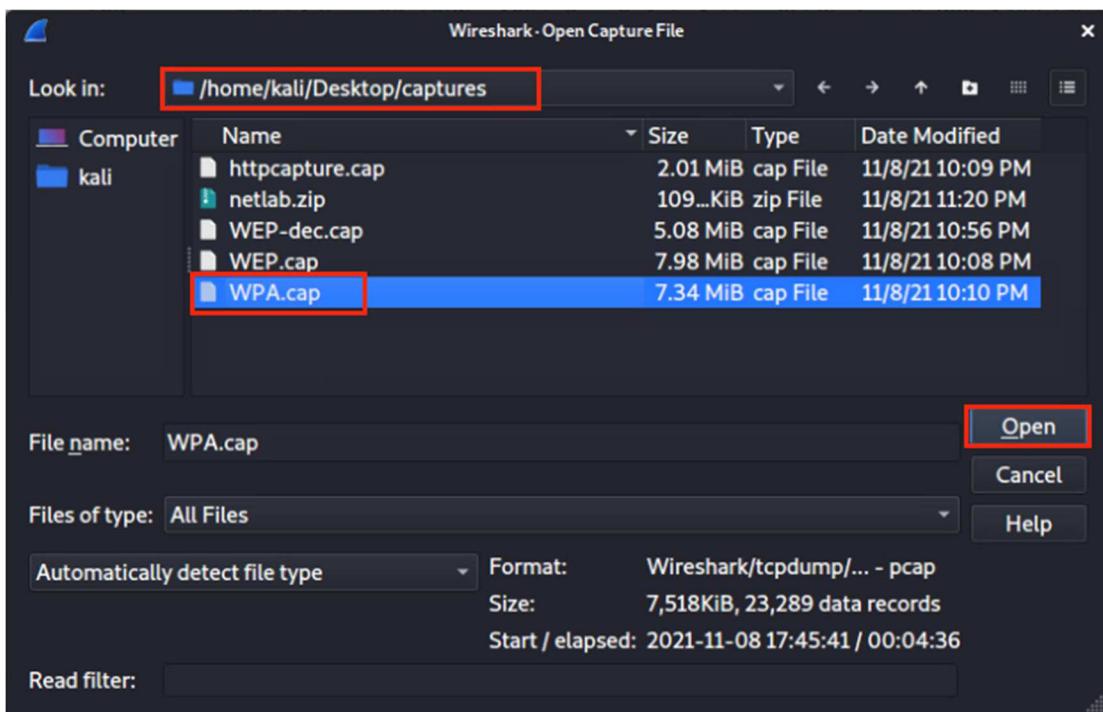
3 Exploiting and Examining WPA Traffic

3.1 Exploiting and Examining WPA Traffic

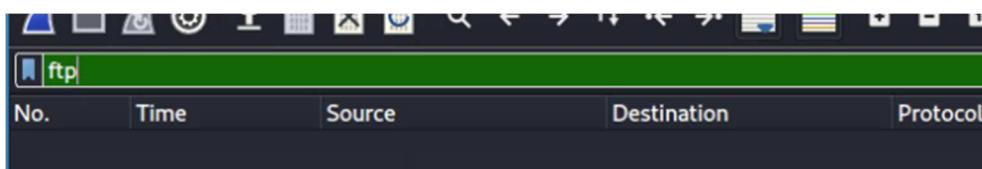
1. Change focus to the **Wireshark** application. Open a **WPA** capture file by selecting the **File** menu option. Click **Open**.



2. Navigate to the **/home/kali/Desktop/captures** directory and select the **WPA.cap** file. Click the **Open** button.



3. In the **Filter:** pane, type **ftp** and press **Enter**.



You will not see any traffic because the wireless network traffic is encrypted.

4. Close Wireshark, change focus to the terminal window, and type the command shown below.

```
kali㉿kali ~$ aircrack-ng ~/Desktop/captures/WPA.cap -w /usr/share/john/password.lst
```

```
(kali㉿kali)-[~]
$ aircrack-ng ~/Desktop/captures/WPA.cap -w /usr/share/john/password.lst
```

5. After a couple of seconds, the *WPA passphrase* is obtained.

```
Aircrack-ng 1.6

[00:00:02] 3567/3559 keys tested (2165.89 k/s)

Time left: -208441375 day, 15 hours, 49 minutes, 20 seconds    100.22%
KEY FOUND! [ password2 ]

Master Key      : 9B 10 BF E7 37 51 02 96 90 8F FB 6A 65 D9 9A F0
                  D5 D4 27 57 F9 9F F1 1A F2 CF FD 2A EB FA 6E D8

Transient Key   : 2F B7 64 0C 7C A6 45 2B 6C 94 62 91 9E 51 F6 50
                  01 C2 44 3D 30 22 34 4E 91 8B 3F 33 B6 F4 EE 0B
                  AE 1E 3F 24 E4 F2 A9 F4 05 2F EA 85 DC 94 CD 70
                  4E 88 E0 77 2C 66 D2 45 B3 88 45 97 A1 A5 46 63

EAPOL HMAC     : 84 61 C4 90 D7 B8 24 5A 9F 7B 9F 3B 25 39 BE 5E
```

6. Decrypt the traffic for the wireless network **NetLab-WirelessHacking**. Type the command shown below to decrypt the traffic.

```
(kali㉿kali)-[~]
$ 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
```



The number of decrypted of WPA packets should be 9855.

7. Change focus to the **Captures** window.
8. Double-click the **WPA-dec.cap** file to open it in *Wireshark*.



9. In the *Filter:* pane, type dns and press **Enter**.

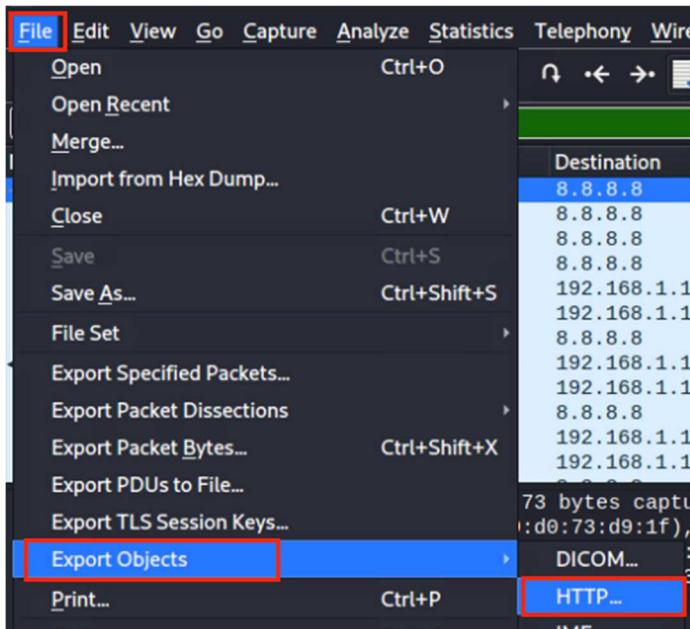
The screenshot shows the Wireshark interface with a packet list window. The filter bar at the top has "dns" typed into it. The packet list shows three DNS requests from 192.168.1.100 to 8.8.8.8. The columns are No., Time, Source, Destination, Protocol, and Length.

No.	Time	Source	Destination	Protocol	Length
19	2.550034	192.168.1.100	8.8.8.8	DNS	73
20	2.550182	192.168.1.100	8.8.8.8	DNS	74
21	2.550210	192.168.1.100	8.8.8.8	DNS	75

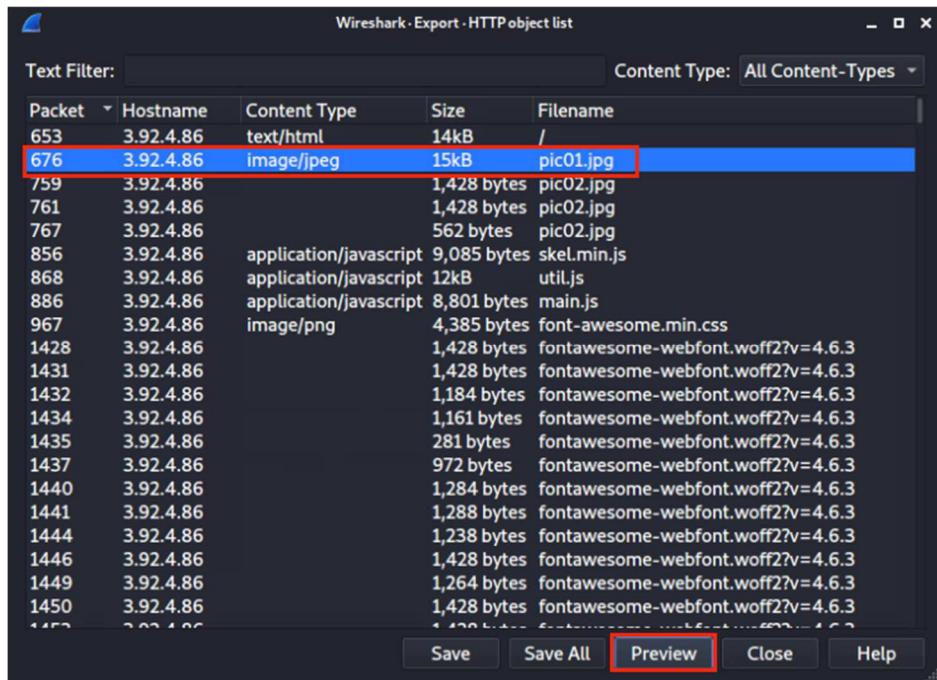


You will now be able to see *DNS* requests with the decrypted wireless traffic.

10. Select the **File** menu option and navigate to **Export Objects > HTTP**.



11. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, find item #676 (pic01.jpg) and select it. Click the **Preview** button.



Packet	Hostname	Content Type	Size	Filename
653	3.92.4.86	text/html	14kB	/
676	3.92.4.86	image/jpeg	15kB	pic01.jpg
759	3.92.4.86		1,428 bytes	pic02.jpg
761	3.92.4.86		1,428 bytes	pic02.jpg
767	3.92.4.86		562 bytes	pic02.jpg
856	3.92.4.86	application/javascript	9,085 bytes	skel.min.js
868	3.92.4.86	application/javascript	12kB	util.js
886	3.92.4.86	application/javascript	8,801 bytes	main.js
967	3.92.4.86	image/png	4,385 bytes	font-awesome.min.css
1428	3.92.4.86		1,428 bytes	fontawesome-webfont.woff2?v=4.6.3
1431	3.92.4.86		1,428 bytes	fontawesome-webfont.woff2?v=4.6.3
1432	3.92.4.86		1,184 bytes	fontawesome-webfont.woff2?v=4.6.3
1434	3.92.4.86		1,161 bytes	fontawesome-webfont.woff2?v=4.6.3
1435	3.92.4.86		281 bytes	fontawesome-webfont.woff2?v=4.6.3
1437	3.92.4.86		972 bytes	fontawesome-webfont.woff2?v=4.6.3
1440	3.92.4.86		1,284 bytes	fontawesome-webfont.woff2?v=4.6.3
1441	3.92.4.86		1,288 bytes	fontawesome-webfont.woff2?v=4.6.3
1444	3.92.4.86		1,238 bytes	fontawesome-webfont.woff2?v=4.6.3
1446	3.92.4.86		1,428 bytes	fontawesome-webfont.woff2?v=4.6.3
1449	3.92.4.86		1,264 bytes	fontawesome-webfont.woff2?v=4.6.3
1450	3.92.4.86		1,428 bytes	fontawesome-webfont.woff2?v=4.6.3
1452	3.92.4.86		1,428 bytes	fontawesome-webfont.woff2?v=4.6.3

12. The *Image Viewer* window opens, showing the content of the image.



13. Close the *Image Viewer* window and the HTTP object list window.

14. Change focus to the **Wireshark** application and type **ftp** in the *Filter:* pane. Press **Enter**.

No.	Time	Source	Destination	Protocol	Length	Info
6229	144.473167	3.92.4.86	192.168.1.100	FTP	93	Response: 220 Microsoft FTP Service
6231	144.478739	192.168.1.100	3.92.4.86	FTP	82	Request: USER anonymous
6232	144.532025	3.92.4.86	192.168.1.100	FTP	138	Response: 331 Anonymous access allowed
6234	144.688579	192.168.1.100	3.92.4.86	FTP	82	Request: PASS anonymous
6235	144.735231	3.92.4.86	192.168.1.100	FTP	87	Response: 230 User logged in.



You will now be able to see the decrypted *FTP* traffic along with clear text usernames and passwords.

15. Scroll down through the *ftp frames* and examine some of the file names that were transferred.

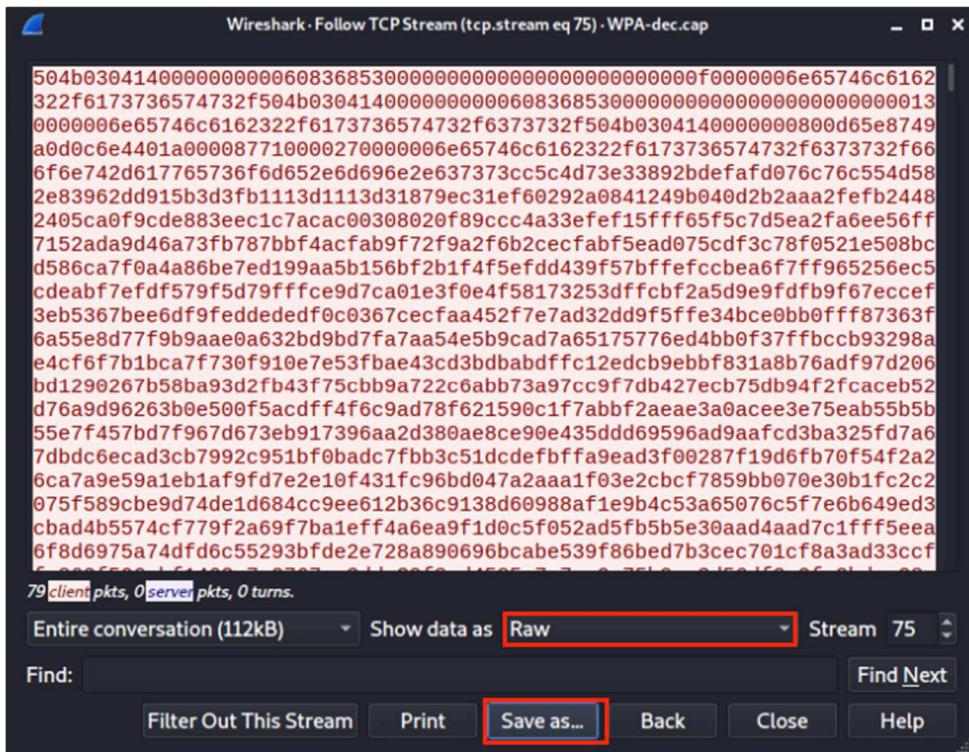
16. Pull one of the zip files transferred via *FTP*. Type **tcp.stream eq 75** into the *Filter:* pane. Press **Enter**.

No.	Time	Source	Destination	Protocol
6825	156.692511	3.92.4.86	192.168.1.100	TCP
6827	156.694093	192.168.1.100	3.92.4.86	TCP

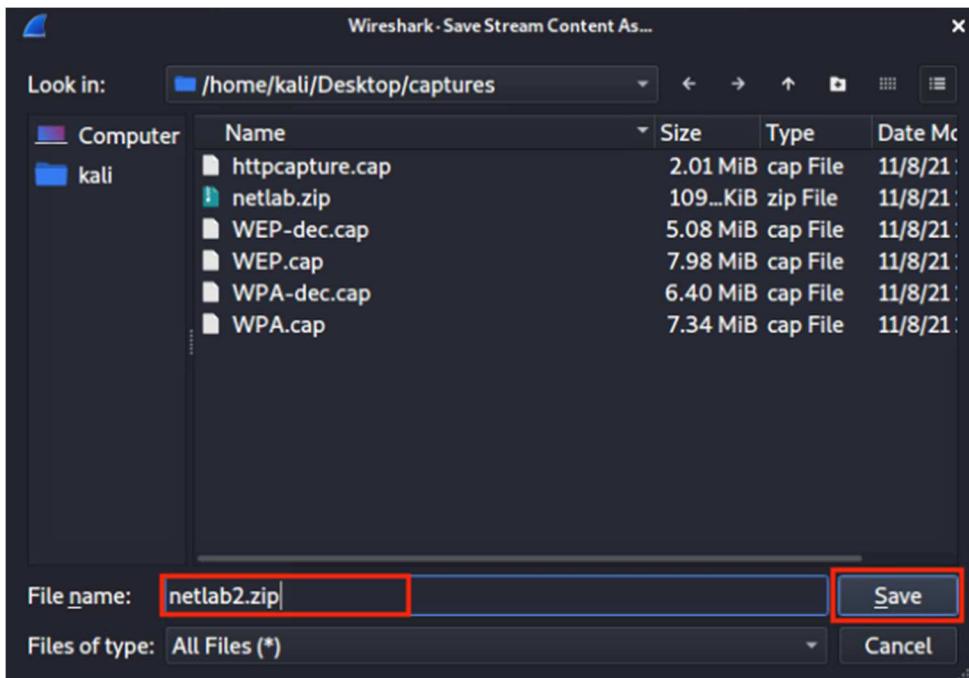
17. Right-click on the **first frame** in the list (#6825) and select **Follow > TCP Stream**.

No.	Time	Source	Destination	Protocol	Length	Info
6825	156.692511	3.92.4.86	192.168.1.100	TCP	66	→ 54313 [SYN, ECN, CWR] Seq=0 Win=666
6827	156.694093	192.168.1.100				Mark/Unmark Packet Ctrl+M
6829	156.740836	3.92.4.86				Ignore/Unignore Packet Ctrl+D
6830	156.742337	3.92.4.86				Set/Unset Time Reference Ctrl+T
6831	156.742356	192.168.1.100				Time Shift... Ctrl+Shift+T
6832	156.742758	3.92.4.86				Packet Comment... Ctrl+Alt+C
6833	156.743054	3.92.4.86				Edit Resolved Name
6834	156.743469	3.92.4.86				Apply as Filter
6836	156.743755	192.168.1.100				Prepare as Filter
6837	156.744318	3.92.4.86				Conversation Filter
6838	156.744386	192.168.1.100				Colorize Conversation
6839	156.744812	3.92.4.86				SCTP
						Follow TCP Stream Ctrl+Alt+Shift+T

18. A new window appears. Change the *Show data as* to **Raw**, then click the **Save as** button.



19. For the name, type **netlab2.zip**. Verify the directory you are saving the file to is **/home/kali/Desktop/captures**. Click **Save**.

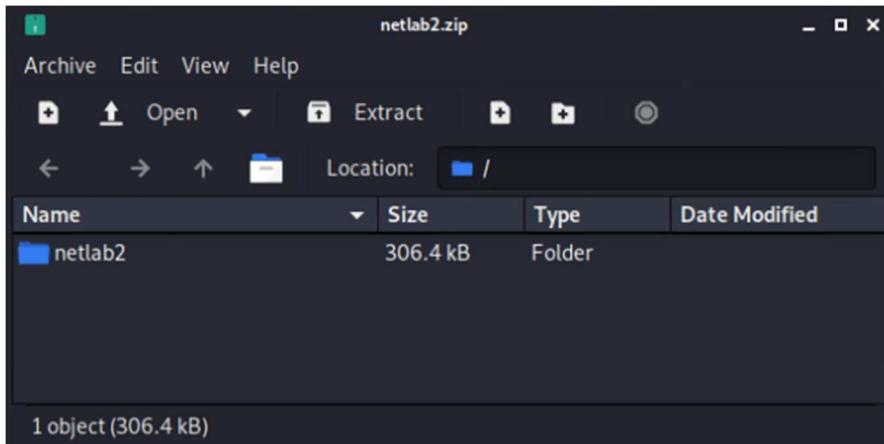


20. Close the *Follow TCP Stream* window.

21. Change focus to the captures window. Double-click the **netlab2.zip** file to open it.



22. A new window opens, showing the content of the zip file. Feel free to check the content in the **netlab2** folder.



23. The lab is now complete; you may end the reservation.