



**NETLAB+**<sup>®</sup>



## Security+ Lab Series

### Lab 06: Wireless Networking Attack and Mitigation Techniques

Document Version: **2018-08-28**

Copyright © 2018 Network Development Group, Inc.  
[www.netdevgroup.com](http://www.netdevgroup.com)

NETLAB Academy Edition, NETLAB Professional Edition, NETLAB+ Virtual Edition, and NETLAB+ are registered trademarks of Network Development Group, Inc.

## Contents

Introduction .....	3
Objectives.....	3
Lab Topology .....	4
Lab Settings .....	5
1 Examining Plain Text Traffic.....	6
1.1 Viewing Plain Text Wireless Traffic .....	6
2 Exploiting and Examining WEP Traffic .....	15
2.1 Decrypt and Analyze WEP Traffic.....	15
3 Exploiting and Examining WPA Traffic.....	23
3.1 Decrypt and Analyze WPA Traffic .....	23

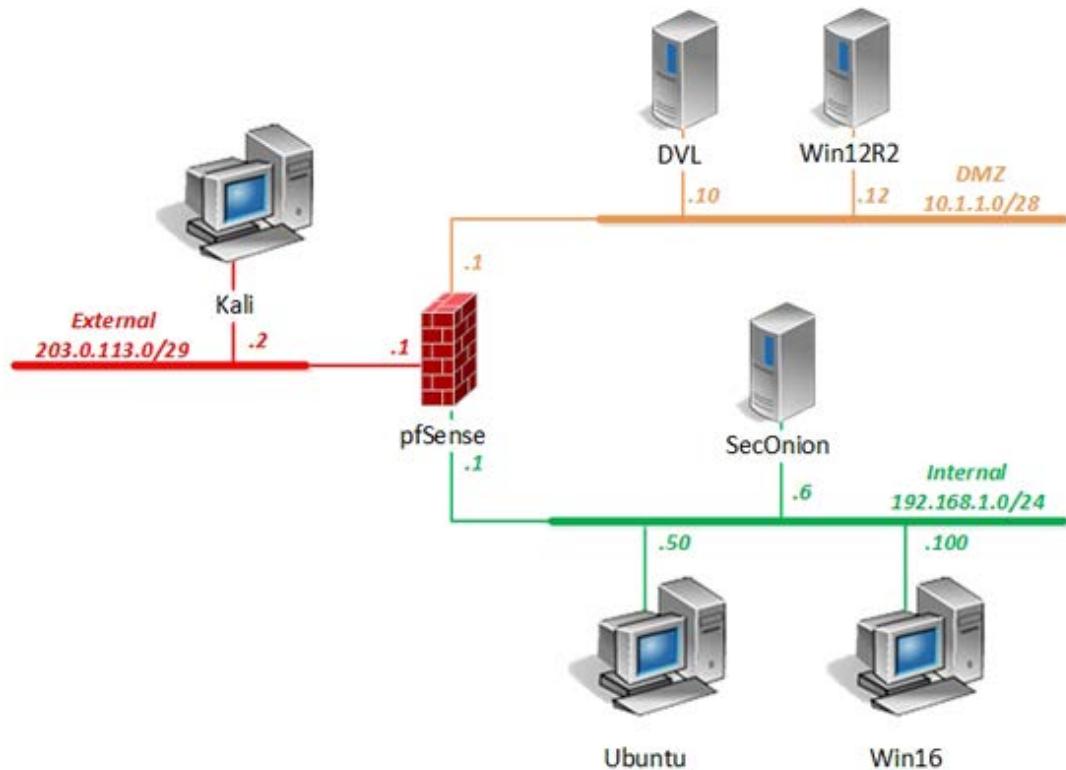
## Introduction

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

## Objectives

- Compare and contrast types of attacks

## Lab Topology



## Lab Settings

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

Virtual Machine	IP Address	Account	Password
DVL	10.1.1.10 /28	root	toor
Kali	203.0.113.2 /29	root	toor
pfSense	eth0: 192.168.1.1 /24 eth1: 10.1.1.1 /28 eth2: 203.0.113.1 /29	admin	pfsense
Sec0nion	192.168.1.6 /24	soadmin	mypassword
		root	mypassword
Ubuntu	192.168.1.50 /24	student	securepassword
		root	securepassword
Win12R2	10.1.1.12 /28	administrator	Training\$
Win16	192.168.1.100 /24	lab-user	Training\$
		Administrator	Training\$

## 1 Examining Plain Text Traffic

### 1.1 Viewing Plain Text Wireless Traffic

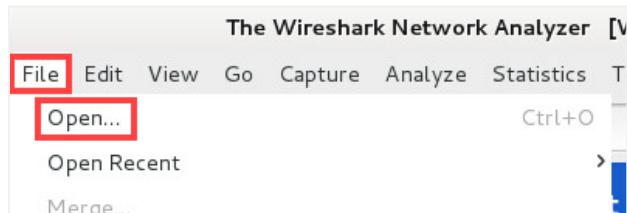
1. Launch the **Kali** virtual machine to access the graphical login screen.
2. Log in as **root** with **toor** as the password.
3. Open a new terminal window by clicking on the **terminal** icon located in the top toolbar.



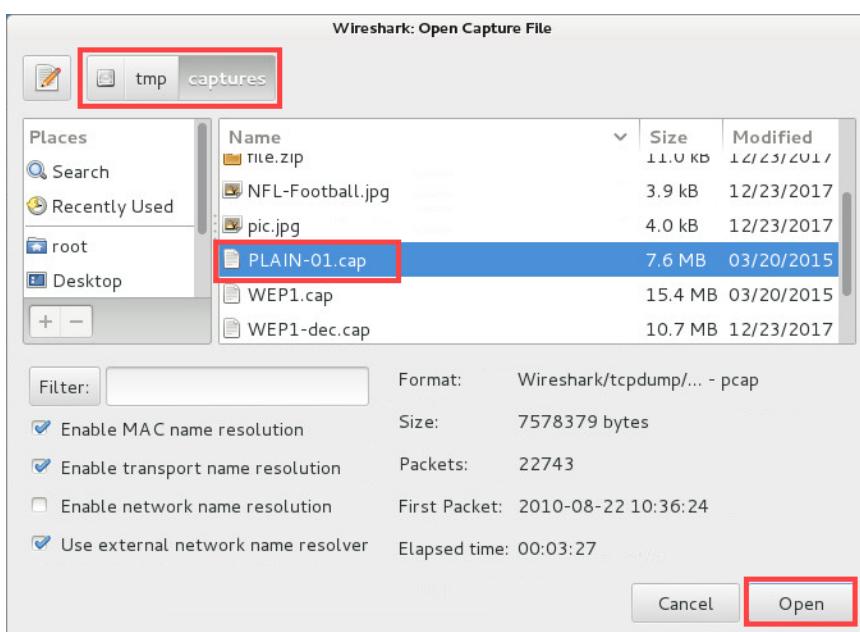
4. Open the **Wireshark** application by typing the command below in the *terminal* window, followed by pressing the **Enter** key. If prompted for a password, enter **securepassword**.

```
root@Kali - Attacker: ~# sudo wireshark
```

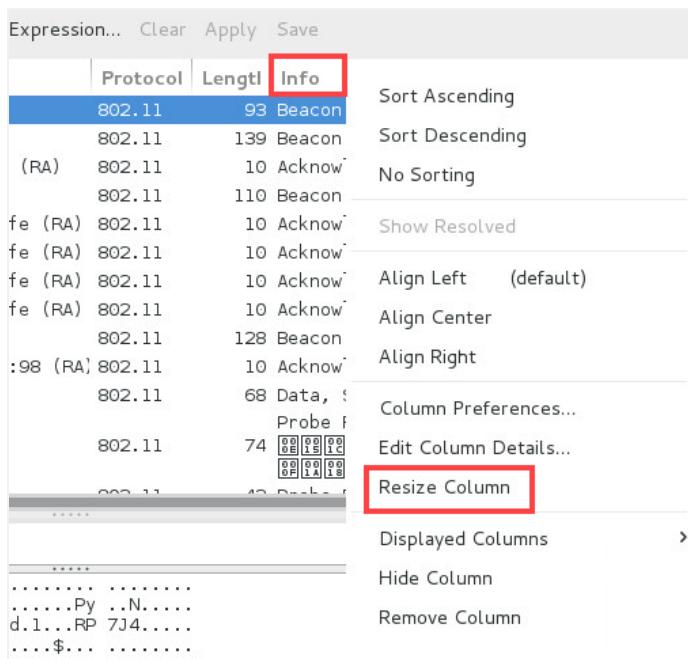
5. If prompted with a security warning, click **OK** to continue.
6. If an error appears regarding *init.lua*, click **OK** to continue.
7. Select the **File** menu option at the top of the *Wireshark* window and click on **Open**.



8. A new window appears. Navigate to **File System > tmp > captures** and select the **PLAIN-01.cap** file. Click the **Open** button.



9. Right-click on the **Info** column header and select **Resize Column** to see all information contained within this column.



10. Select on the **second frame** in the *Wireshark* capture file.

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000	Actionte_d8:b2:84	Broadcast		802.11	93	Beacon frame, SN=1941
2 0.001031	Actionte_e5:71:8c	Broadcast		802.11	139	Beacon frame, SN=2101
3 0.006139	Apple_12:2b:8a (RA)			802.11	10	Acknowledgement, Flags
4 0.014825	Netgear_8a:78:fe	Broadcast		802.11	110	Beacon frame, SN=3441,
5 0.014829		Netgear_8a:78:fe (RA)		802.11	10	Acknowledgement, Flags

11. On the bottom part of the screen, click the + icon in front of the **IEEE 802.11 wireless LAN management frame** to expand its view.



12. Dive in further by clicking the + icon in front of **Tagged parameters** followed by clicking the + icon in front of **Tag: Vender Specific: Microsof: WPA Information Element**. View the *WPA Version*.

```

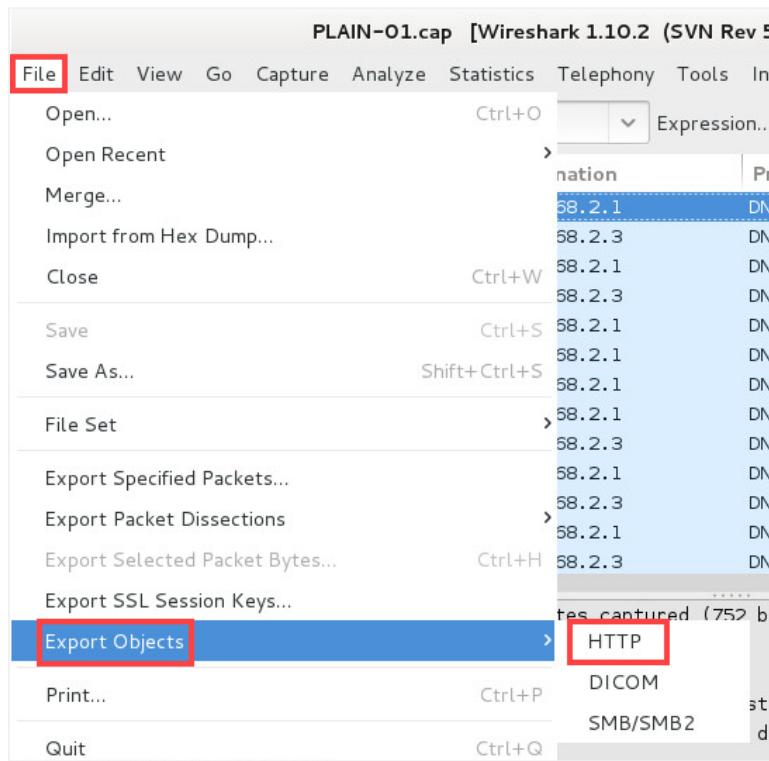
[-] IEEE 802.11 wireless LAN management frame
  [+/-] Fixed parameters (12 bytes)
  [+/-] Tagged parameters (103 bytes)
    [+/-] Tag: SSID parameter set: T4QY4
    [+/-] Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    [+/-] Tag: DS Parameter set: Current Channel: 1
    [+/-] Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    [+/-] Tag: Country Information: Country Code US, Environment Any
    [+/-] Tag: Power Constraint: 0
    [+/-] Tag: ERP Information
    [+/-] Tag: RSN Information
    [+/-] Tag: Vendor Specific: Microsof: WPA Information Element
      Tag Number: Vendor Specific (221)
      Tag length: 22
      OUI: 00-50-f2 (Microsof)
      Vendor Specific OUI Type: 1
      Type: WPA Information Element (0x01)
      WPA Version: 1
      Multicast Cipher Suite: 00-50-f2 (Microsof) AES (CCM)
        Unicast Cipher Suite Count: 1
      Unicast Cipher Suite List 00-50-f2 (Microsof) AES (CCM)

```

13. View captured *DNS requests* by typing **dns** in the *Filter:* pane. Click **Apply**.



14. 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 navigate to **Export Objects > HTTP**.



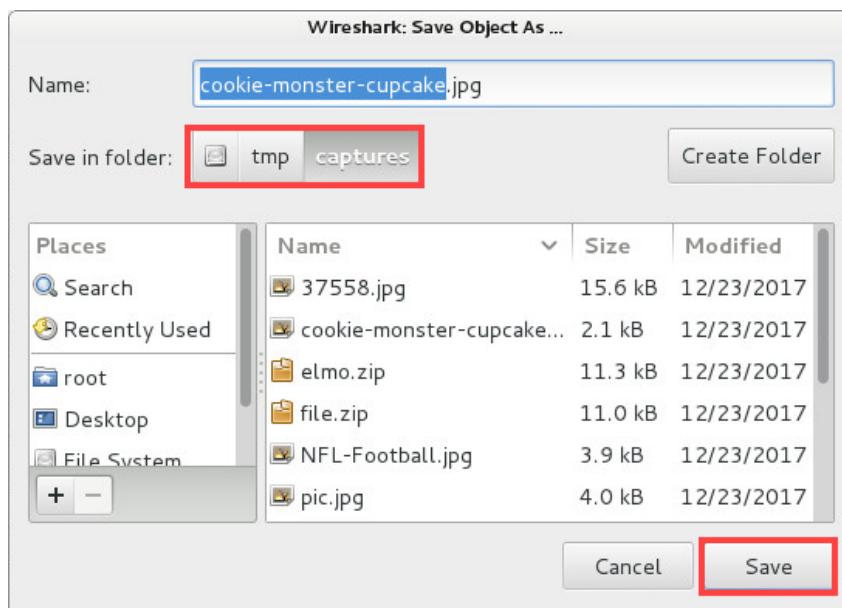
15. A new window appears. Look through the list of files that have been downloaded by wireless users. Under the *Filename* column, find the image file **cookie-monster-cupcake.jpg** and select the file. With the file selected, click the **Save As** button.

**Wireshark: HTTP object list**

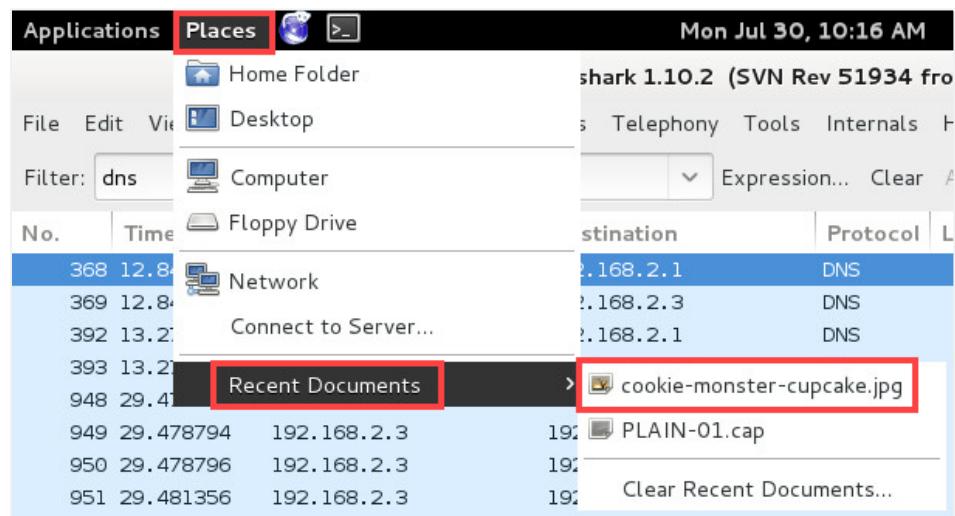
Packet num	Hostname	Content Type	Size	Filename
945	www.google.com	text/html	41 kB	images?hl=en&source=imghp&q=
1052	t0.gstatic.com	image/jpeg	3313 bytes	Cookie_Monster_What_The_He
1064	t1.gstatic.com	image/jpeg	2849 bytes	cookiemonster.jpg
1074	t1.gstatic.com	image/jpeg	2984 bytes	cookiemonster.jpg
1080	t0.gstatic.com	image/jpeg	2274 bytes	cookie%2520monster.jpg
1089	t3.gstatic.com	image/jpeg	2125 bytes	cookie-monster-cupcake.jpg
1095	t2.gstatic.com	image/jpeg	3616 bytes	the-cookie-monster-gun.jpg
1102	t2.gstatic.com	image/jpeg	3687 bytes	200901061125.jpg
1113	t3.gstatic.com	image/jpeg	5133 bytes	cookiemonster.jpg
1126	t0.gstatic.com	image/jpeg	4311 bytes	cookie_monster.jpg
1133	t1.gstatic.com	image/jpeg	2431 bytes	cookie_monster.jpg

Buttons at the bottom: Help, Save As (highlighted with a red box), Save All, Cancel.

16. In the *Save Object As* window, choose the **/tmp/captures** directory to save to and then click the **Save** button.



17. View the image by selecting the **Places** menu option located next to the *Applications* menu. Navigate to **Recent Documents > cookie-monster-cupcake.jpg**.



18. Notice the image. **Close** the *image viewer* and close out the *HTTP object list* window.



19. Within the *Wireshark* interface, pull a zip file via *FTP* out of the wireless capture file. Type **ftp-data and frame contains PK** into the *Wireshark Filter:* and click **Apply**.

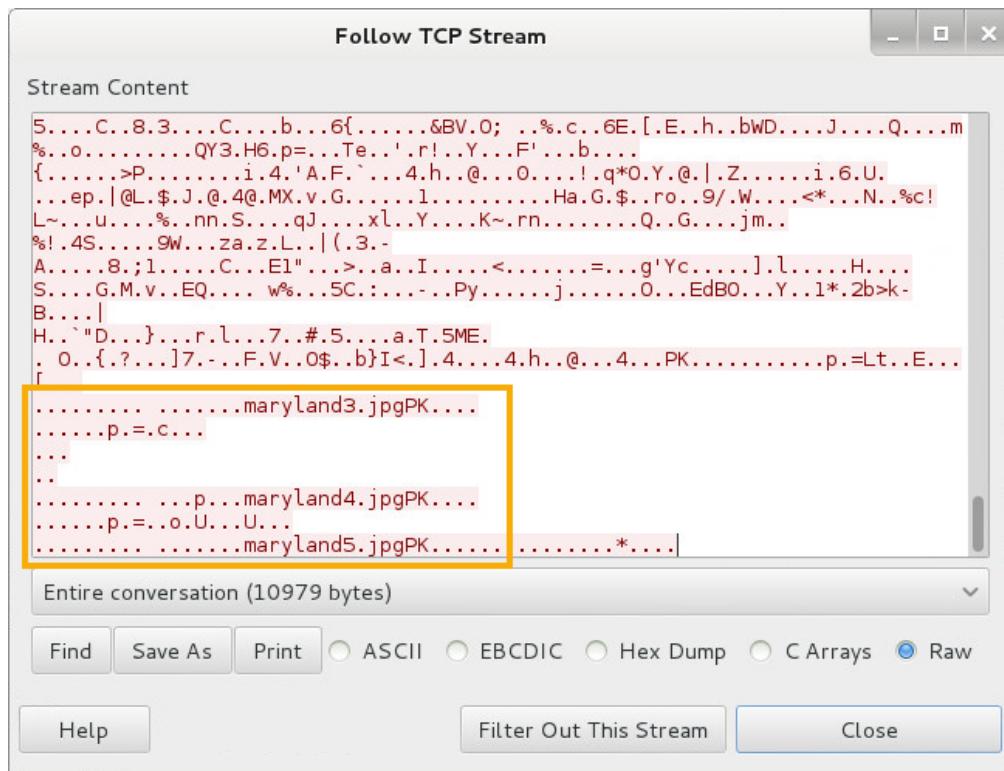


20. Right-click on the **frame 21207** in the list and select **Follow TCP Stream**.

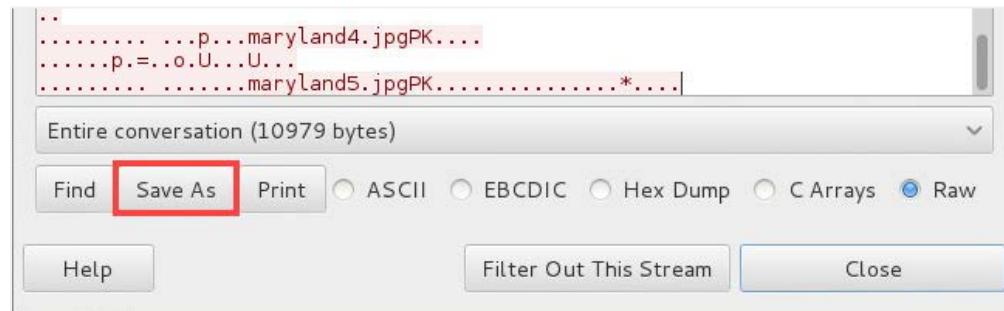
No.	Time	Source	Destination	Protocol	Length	Info
17521	159.011789	192.168.2.3	192.168.2.2	FTP-DATA	1	Mark Packet (toggle)
17702	159.058383	192.168.2.3	192.168.2.2	FTP-DATA	1	Ignore Packet (toggle)
17898	159.101903	192.168.2.3	192.168.2.2	FTP-DATA	1	Set Time Reference (toggle)
17982	159.120849	192.168.2.3	192.168.2.2	FTP-DATA	1	Time Shift...
18025	159.132109	192.168.2.3	192.168.2.2	FTP-DATA	1	Packet Comment...
18054	159.140813	192.168.2.3	192.168.2.2	FTP-DATA	1	Manually Resolve Address
18295	159.196113	192.168.2.3	192.168.2.2	FTP-DATA	1	Apply as Filter
18473	159.236108	192.168.2.3	192.168.2.2	FTP-DATA	1	Prepare a Filter
18508	159.246863	192.168.2.3	192.168.2.2	FTP-DATA	1	Conversation Filter
<b>21207</b>	<b>170.302668</b>	<b>192.168.2.3</b>	<b>192.168.2.2</b>	<b>FTP-DATA</b>	<b>1</b>	<b>Colorize Conversation</b>
21209	170.303180	192.168.2.3	192.168.2.2	FTP-DATA	1	SCTP
21215	170.305741	192.168.2.3	192.168.2.2	FTP-DATA	1	<b>Follow TCP Stream</b>
21225	170.307789	192.168.2.3	192.168.2.2	FTP-DATA	1	Follow UDP Stream
						Follow SSL Stream

Frame 21207: 1534 bytes on wire (12272 bits), 1534 bytes captured (12272 bits) IEEE 802.11 QoS Data, Flags: .....,T  
 Logical-Link Control  
 Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: 192.168.2.2 (192.168.2.2)  
 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 49423 (49423)  
 FTP Data (1460 bytes data)

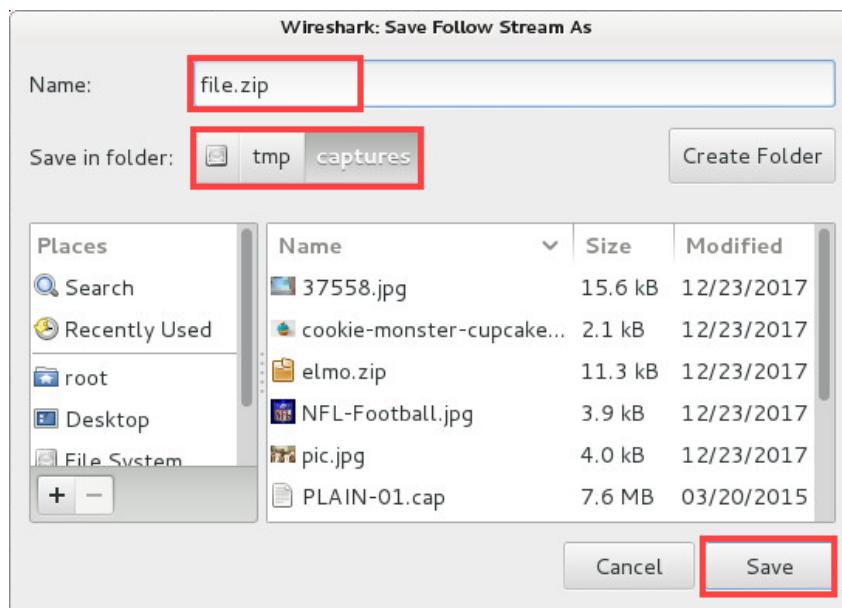
21. Examine the data shown in the *TCP stream*. Scroll to the bottom of the window and notice the “PK” attached to the end of filenames.



22. Within the *Follow TCP Stream* window, click **Save As**.



23. Type **file.zip** in the *Name* text field. Make sure the save destination is set to **/tmp/captures** and click the **Save** button.

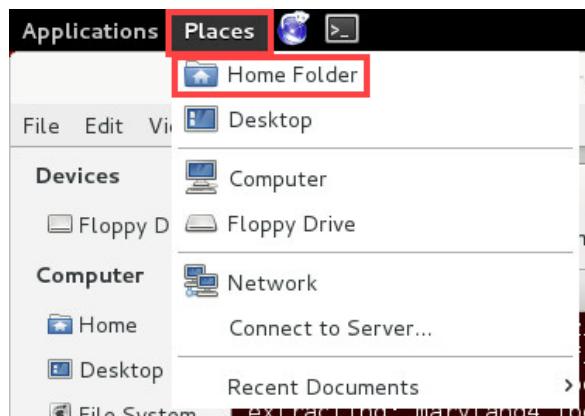


24. **Close** the *Follow TCP Stream* window.  
 25. Open a new **terminal** window and type the command below to **unzip** the file that was just pulled from the *Wireshark* capture file.

```
root@Kali - Attacker: ~# unzip /tmp/captures/file.zip
```

```
root@Kali-Attacker:~# unzip /tmp/captures/file.zip
Archive: /tmp/captures/file.zip
  inflating: maryland3.jpg
  extracting: maryland4.jpg
  extracting: maryland5.jpg
```

26. Select the **Places** menu option from the top menu pane and click on **Home Folder**.



27. Notice the three different *maryland* image files in the **/root** directory that were extracted from *file.zip*.

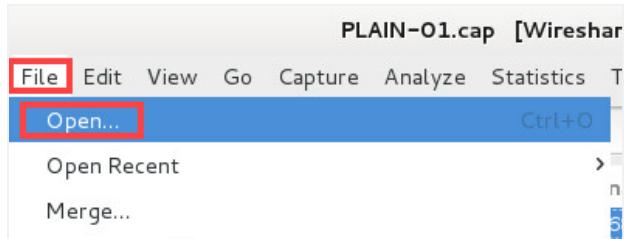


28. **Close** the *File Manager* window.  
29. Leave the *Kali* window open to continue with the next task.

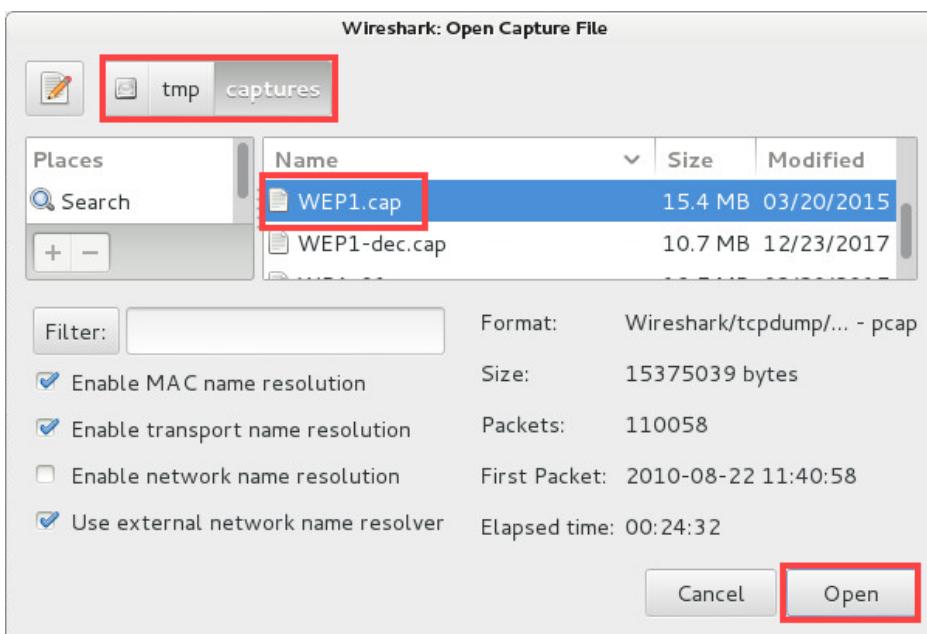
## 2 Exploiting and Examining WEP Traffic

### 2.1 Decrypt and Analyze WEP Traffic

1. Change focus on the **Wireshark** window. Select the **File** menu option and click on **Open**.



2. A new window appears. Verify that you are in the **/tmp/captures** directory. Select the **WEP1.cap** file and click the **Open** button.



3. In the **Filter:** pane, type **dns** and click **Apply**.



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

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

```
root@Kali - Attacker: ~# aircrack-ng /tmp/captures/WEP1.cap
```

6. Type **5** for the target network. Press **Enter**.

```
root@Kali-Attacker:~# aircrack-ng /tmp/captures/WEP1.cap
Opening /tmp/captures/WEP1.cap
Read 110058 packets.

#   BSSID           ESSID          Encryption
1   00:1F:90:D9:C6:28  HUANGDOM      WEP (138 IVs)
2   00:1F:90:D8:B2:84  RP7J4         WEP (7238 IVs)
3   00:26:62:E5:71:8C  T4QY4         WPA (0 handshake)
4   00:18:4D:8A:78:FE  boguswifi     WPA (0 handshake)
5   00:17:3F:F4:56:90  TOWSON22    WEP (43210 IVs)
6   00:1F:90:B1:86:F8  24SE5        No data - WEP or WPA
7   00:24:B2:DA:A8:7A
8   00:1A:70:62:9F:59  homer        None (0.0.0.0)

Index number of target network ? 5
```

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

```
Aircrack-ng 1.2 beta3

[00:00:02] Tested 7030 keys (got 29937 IVs)

KB    depth  byte(vote)
0    0/ 11   AA(39424) 2F(38656) BF(37888) BC(36608) FC(36352)
1    5/ 11   AA(35840) 93(35840) 18(35584) 28(35584) A5(35328)
2    0/  1   AA(44032) 65(37376) EB(36608) 2C(36096) 55(35840)
3    24/ 30  A0(33536) 35(33280) 4D(33280) 76(33280) 97(33280)
4    0/  2   AA(41728) D9(38144) 8E(36096) 4C(35072) F7(35072)

KEY FOUND! [ AA:AA:AA:AA:AA ]
Decrypted correctly: 100%
```

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

```
root@Kali - Attacker: ~# airdecap-ng -w AA:AA:AA:AA:AA /tmp/captures/WEP1.cap
```

```
root@Kali-Attacker:~# airdecap-ng -w AA:AA:AA:AA:AA /tmp/captures/WEP1.cap
Total number of packets read      110058
Total number of WEP data packets  50596
Total number of WPA data packets  808
Number of plaintext data packets 0
Number of decrypted WEP packets  43220
Number of corrupted WEP packets  0
Number of decrypted WPA packets  0
```

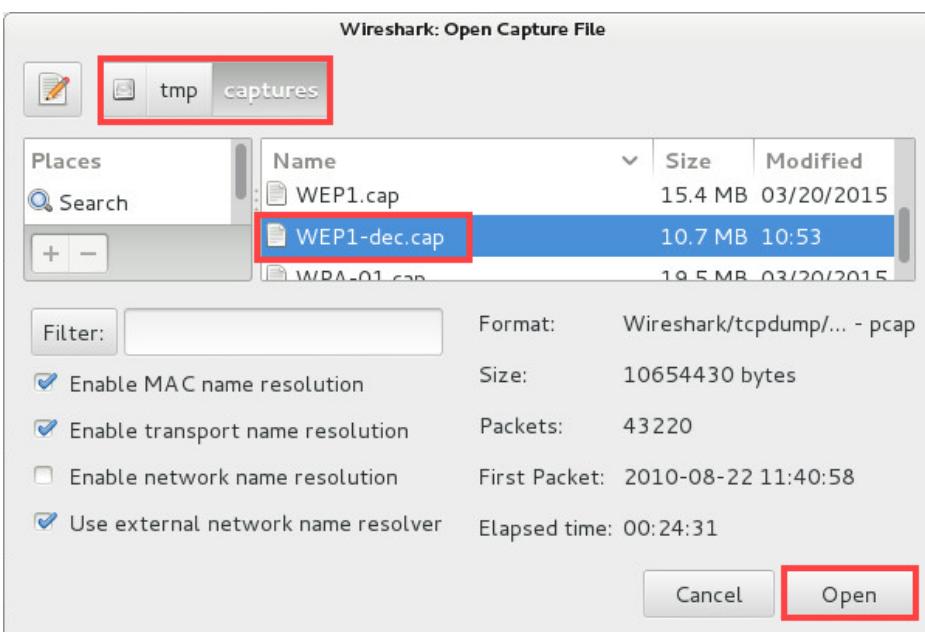


The number of *decrypted WEP packets* should be 43220.

9. Analyze the decrypted traffic with *Wireshark*. Type `sudo wireshark` into the terminal and then press **Enter**.
10. If prompted with *Lua* loading error, click **OK** to continue.
11. Within the *Wireshark* application, select the **File** menu option and click **Open**.



12. A new window appears. Navigate to the `/tmp/capture` directory and select the **WEP1-dec.cap** file. Click **Open**.

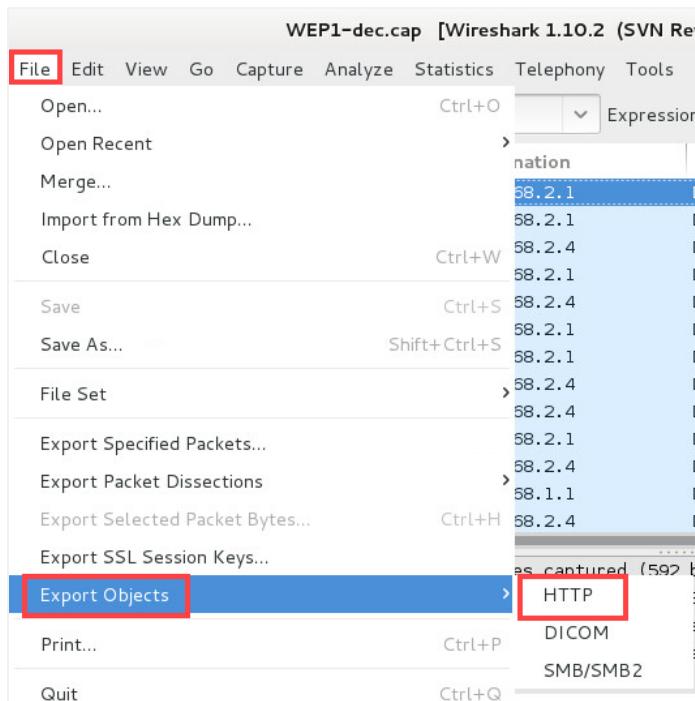


13. In the *Filter:* pane, type **dns** and click **Apply**.



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

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

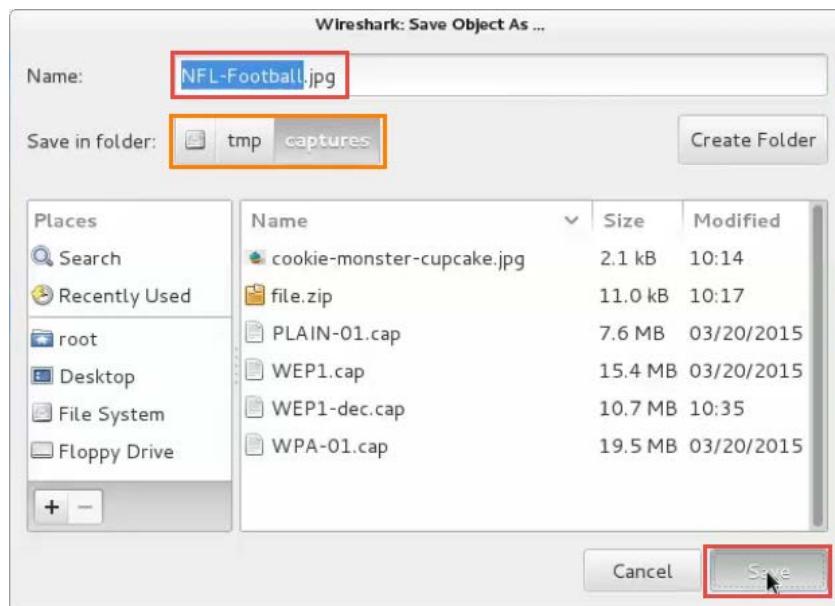


15. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, select the item **#6988 (NFL-Football.jpg)**. Once selected, click the **Save As** button.

Wireshark: HTTP object list				
Packet num	Hostname	Content Type	Size	Filename
6976	t0.gstatic.com	image/jpeg	5834 bytes	nfl.jpg
<b>6988</b>	<b>t0.gstatic.com</b>	<b>image/jpeg</b>	<b>3891 bytes</b>	<b>NFL-Football.jpg</b>
7013	t2.gstatic.com	image/jpeg	5281 bytes	1192568745.jpg
7031	t3.gstatic.com	image/jpeg	4489 bytes	NFL%2BNetwork.png
7037	t3.gstatic.com	image/jpeg	5123 bytes	nfl-steroids.jpg

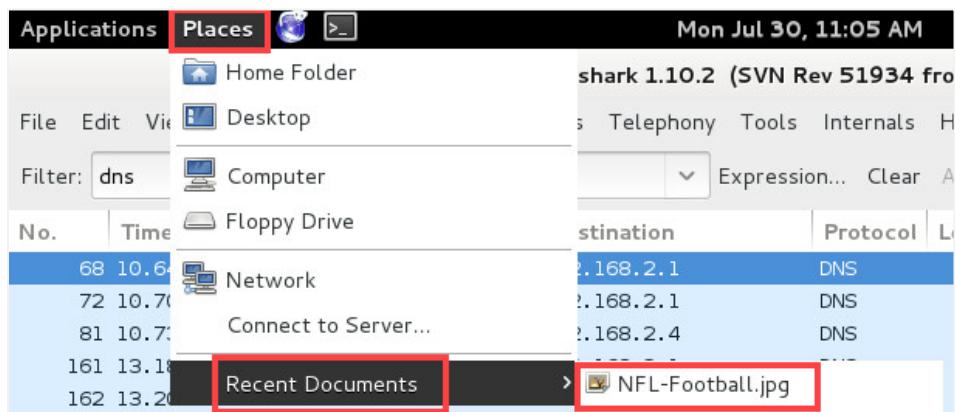
Help Save As  Save All  Cancel

16. Verify that the directory you are saving to is **/tmp/captures**. Click the **Save** button.



17. Close the *HTTP object list* window.

18. Click on the **Places** menu option and navigate to **Recent Documents**. Click on the **NFL-Football.jpg** entry to view the file.

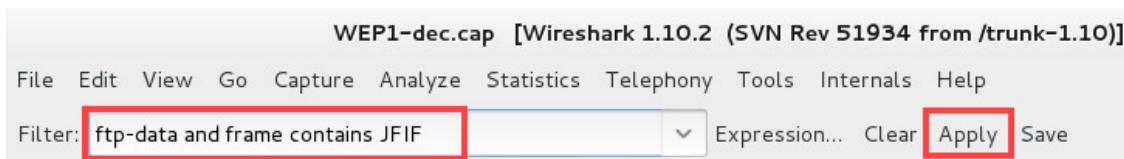


19. Notice the image that appears. Close the image viewer.

20. 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
7351	118.039430	192.168.2.3	192.168.2.4	FTP	81	Response: 220 Microsoft FTP Service
7352	118.039474	192.168.2.3	192.168.2.4	FTP	81	[TCP Retransmission] Response: 220 Micro
7359	119.884833	192.168.2.4	192.168.2.3	FTP	64	Request: USER ftp
7360	119.885362	192.168.2.4	192.168.2.3	FTP	64	[TCP Retransmission] Request: USER ftp
7361	119.885826	192.168.2.3	192.168.2.4	FTP	126	Response: 331 Anonymous access allowed,
7362	119.886386	192.168.2.3	192.168.2.4	FTP	126	[TCP Retransmission] Response: 331 Anony
7413	127.429170	192.168.2.4	192.168.2.3	FTP	77	Request: PASS hi@123244555.com
7414	127.432709	192.168.2.3	192.168.2.4	FTP	85	Response: 230 Anonymous user logged in.
7415	127.433266	192.168.2.3	192.168.2.4	FTP	85	[TCP Retransmission] Response: 230 Anony
7424	130.085025	192.168.2.4	192.168.2.3	FTP	80	Request: PORT 192,168,2,4,195,119

21. Let's pull a *JPEG* file transferred via *FTP* from the wireless capture. Type **ftp-data and frame contains JFIF** in the *Filter:* pane. Click **Apply**.



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

No.	Time	Source	Destination	Protocol	Length	Info
8347	167.317518	192.168.2.3	192.168.2.4			Mark Packet (toggle)
8350	167.319602	192.168.2.3	192.168.2.4			Ignore Packet (toggle)
8369	170.347712	192.168.2.3	192.168.2.4			Set Time Reference (toggle)
8370	170.362098	192.168.2.3	192.168.2.4			Time Shift...
8396	170.383557	192.168.2.3	192.168.2.4			Packet Comment...
8398	170.384626	192.168.2.3	192.168.2.4			Manually Resolve Address
8426	170.592960	192.168.2.3	192.168.2.4			Apply as Filter
8428	170.593522	192.168.2.3	192.168.2.4			Prepare a Filter
8458	170.800832	192.168.2.3	192.168.2.4			Conversation Filter
8460	170.801394	192.168.2.3	192.168.2.4			Colorize Conversation
8509	171.224771	192.168.2.3	192.168.2.4			SCTP
8510	171.225330	192.168.2.3	192.168.2.4			Follow TCP Stream
8540	171.446021	192.168.2.3	192.168.2.4			

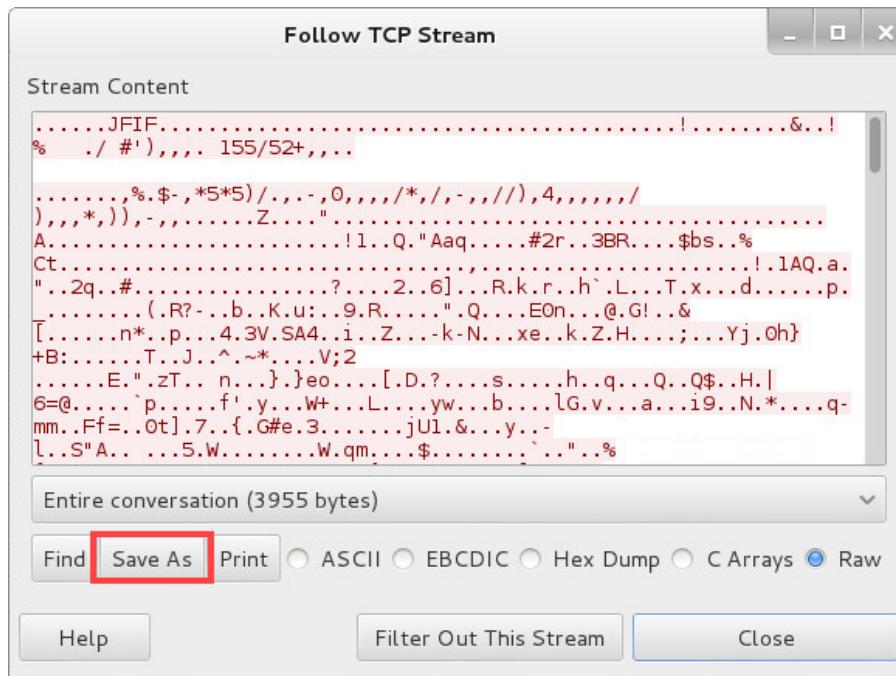
+ Frame 8347: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eth0 at 167.317518 (00:05:7d:e4:68:a0) [ethernet II] ->> (192.168.2.4) [192.168.2.3] (192.168.2.3) [192.168.2.4] (192.168.2.4) [192.168.2.3] (192.168.2.3) [192.168.2.4]

+ Ethernet II, Src: SunComm\_e4:68:a0 (00:05:7d:e4:68:a0) [eth0] (192.168.2.3) [192.168.2.4] (192.168.2.4) [192.168.2.3] (192.168.2.3) [192.168.2.4]

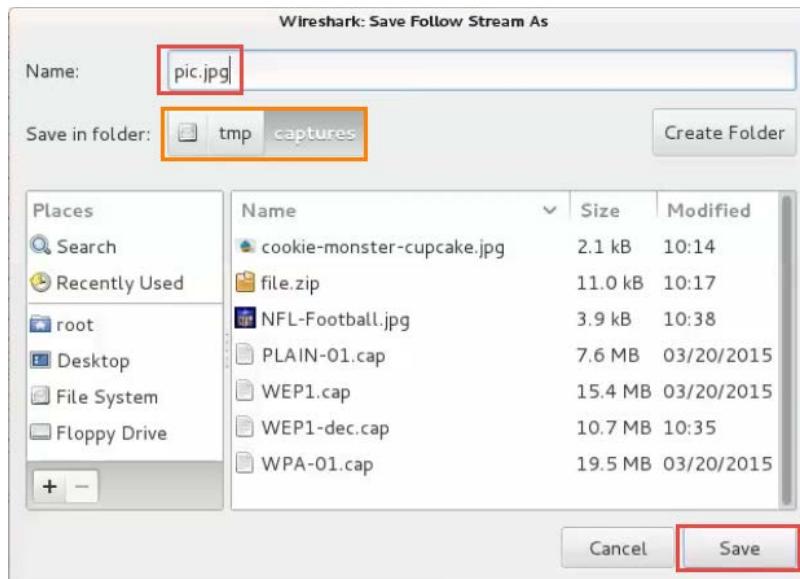
+ Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3) [192.168.2.4] (192.168.2.4) [192.168.2.3] (192.168.2.3) [192.168.2.4]

+ Transmission Control Protocol, Src Port: ftp-data (20) [192.168.2.3] (192.168.2.4) [192.168.2.3] (192.168.2.3) [192.168.2.4]

23. A new window appears. Click the **Save As** button.

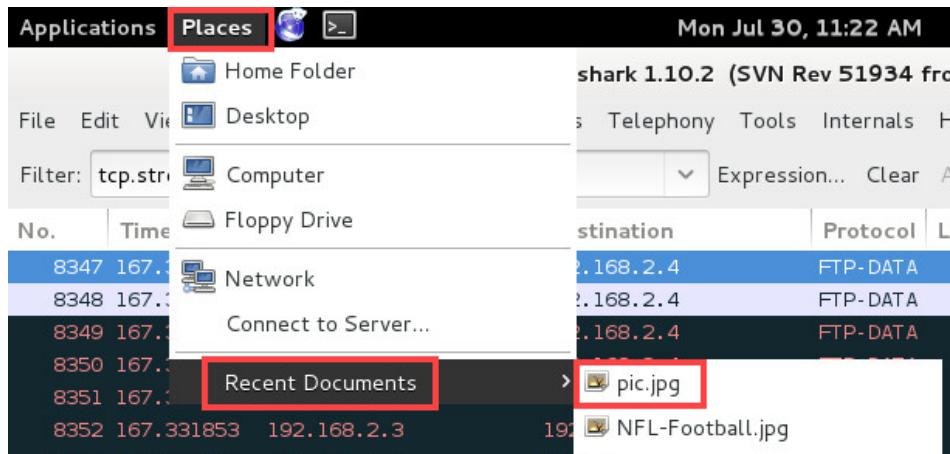


24. For the filename, type **pic.jpg**. Make sure the directory is set to **/tmp/captures** and click the **Save** button.



25. Close the *Follow TCP Stream* window.

26. Select the **Places** menu option and navigate to **Recent Documents > pic.jpg**.



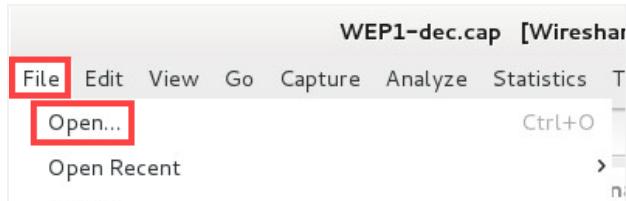
27. Notice the image in the *image viewer* window. **Close** the image viewer.

28. Leave the *Kali* window open to continue with the next task.

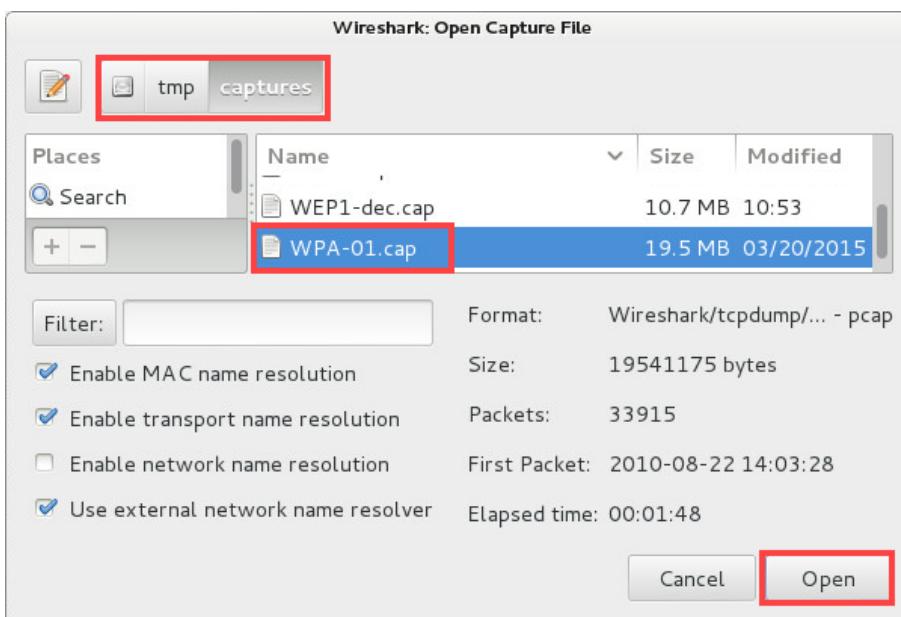
### 3 Exploiting and Examining WPA Traffic

#### 3.1 Decrypt and Analyze WPA Traffic

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



2. Navigate to the **/tmp/captures** directory and select the **WPA-01.cap** file. Click the **Open** button.



3. In the **Filter:** pane, type **ftp** and click **Apply**.



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

4. Change focus to the **terminal** window and type the command below.

```
root@Kali-Attacker:~# aircrack-ng /tmp/captures/WPA-01.cap -w /tmp/wordlists/passlist
```

5. Type **3** as the menu option. Press **Enter**.

```
root@Kali-Attacker:~# aircrack-ng /tmp/captures/WPA-01.cap -w /tmp/wordlists/passlist
Opening /tmp/captures/WPA-01.cap
Read 33915 packets.

#   BSSID           ESSID          Encryption
1   00:1F:90:D9:C6:28  HUANGDOM      WEP (19 IVs)
2   00:18:4D:8A:78:FE  boguswifi      WPA (0 handshake)
3   00:17:3F:F4:56:90  TOWSON333    WPA (1 handshake)
4   00:1F:90:D8:B2:84  RP7J4        WEP (6583 IVs)
5   00:26:62:E5:71:8C  T4QY4        WPA (0 handshake)
6   00:24:B2:DA:A8:7A  Anthony98    No data - WEP or WPA
7   00:26:F2:9B:08:4C  Anthony98    No data - WEP or WPA

Index number of target network ? 3
```

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

```
Aircrack-ng 1.2 beta3

[00:00:00] 4 keys tested (523.77 k/s)

KEY FOUND! [ breezeless ]
```

Master Key	: 69 24 A8 65 AF BF 71 4E 9E 25 25 C0 2A 71 E3 AB 59 E9 B3 6E 9A 4D B1 47 5E 1E 01 BD 9E 7B 80 AE
Transient Key	: FB 91 BB 94 87 12 4D E6 F9 D2 CC 82 71 CC 0F E5 DD D2 2A 9B 79 47 A9 B5 7C 0C 46 C6 30 82 C2 A8 3E CB 55 CD 6F 86 67 18 71 2C B8 22 D3 E2 43 F2 67 E8 63 6D EF 93 F9 EF 03 77 F5 80 5F 0A 43 61
EAPOL HMAC	: 8C EA C6 47 4C 5A CB 75 7C D2 71 82 52 9E 85 54

6. Decrypt the traffic for the wireless network **TOWSON333**. Type the command below to decrypt the traffic.

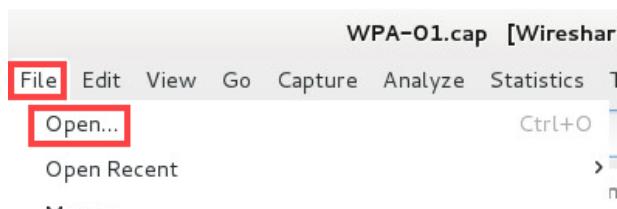
```
root@Kali-Attacker:~# airdecap-ng /tmp/captures/WPA-01.cap -e TOWSON333 -p  
breezeless
```

```
root@Kali-Attacker:~# airdecap-ng /tmp/captures/WPA-01.cap -e TOWSON333 -p breezeless
Total number of packets read      33915
Total number of WEP data packets  6602
Total number of WPA data packets  11401
Number of plaintext data packets 1
Number of decrypted WEP packets  0
Number of corrupted WEP packets  0
Number of decrypted WPA packets  11162
```

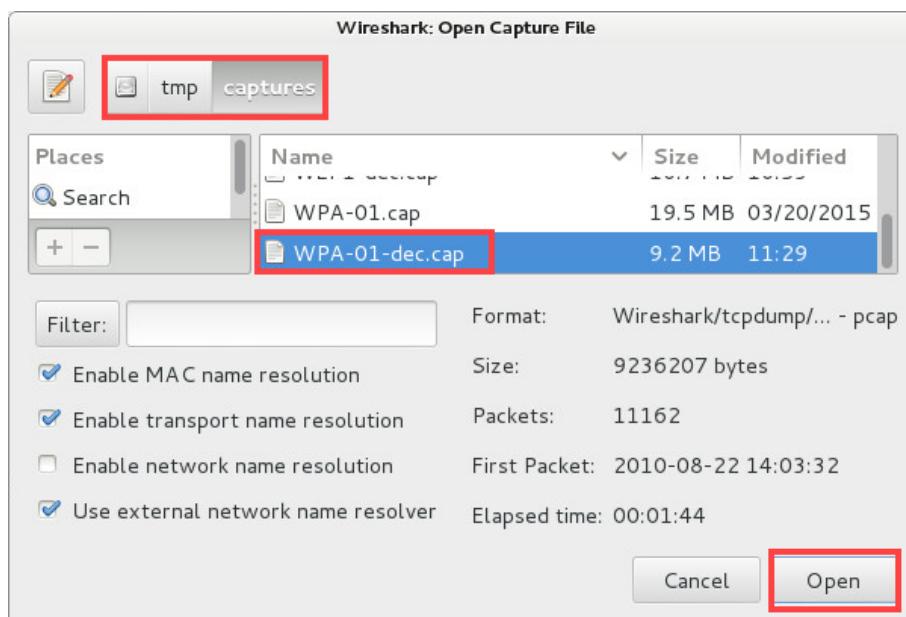


The number of decrypted WPA packets should be 11,401.

7. Change focus to the **Wireshark** application.
8. Within the **Wireshark** application, select the **File** menu option and click **Open**.



9. Navigate to the **/tmp/captures** directory and select the **WPA-01-dec.cap** file. Click **Open**.

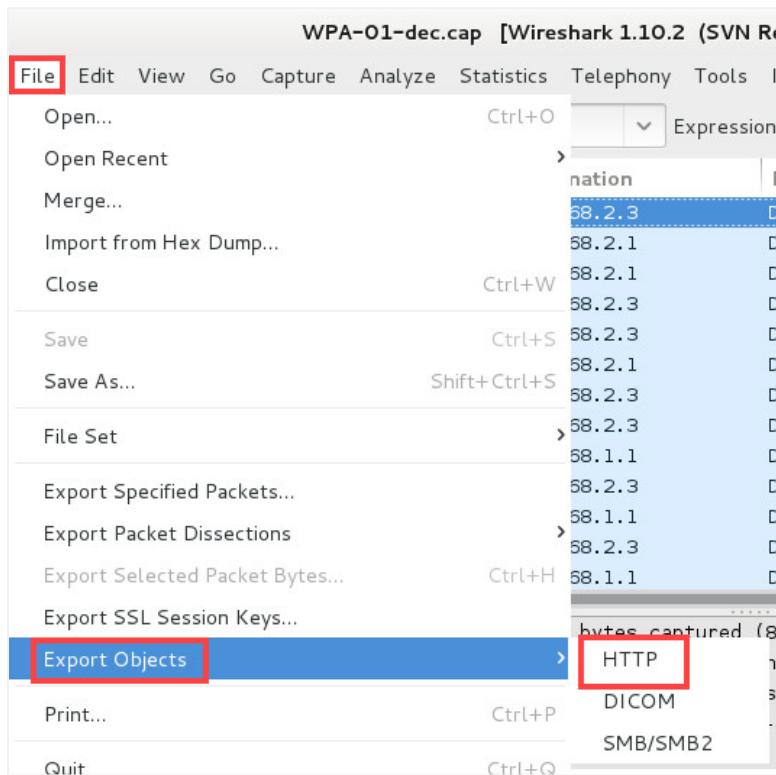


10. In the **Filter:** pane, type **dns** and click **Apply**.



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

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

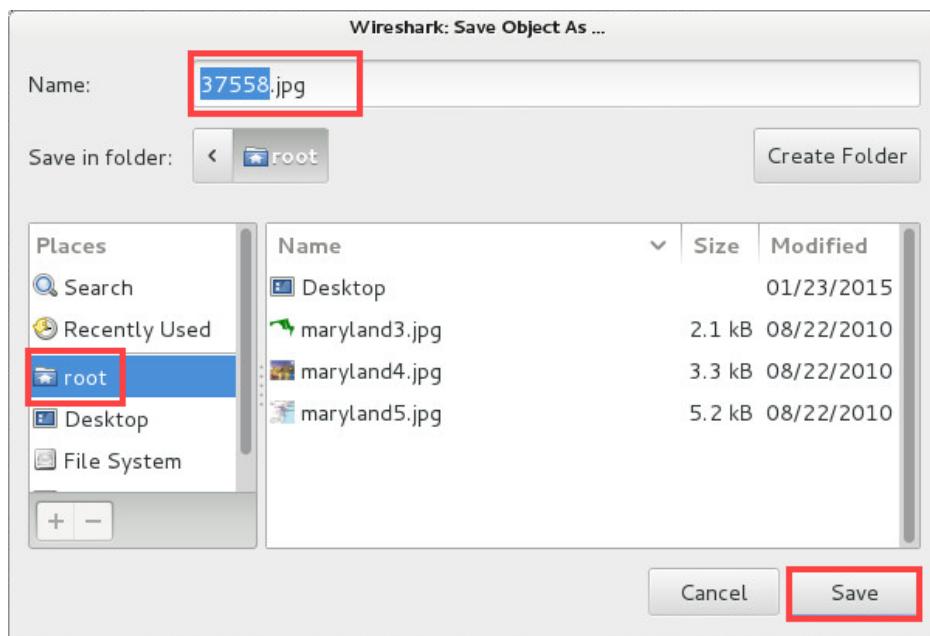


12. A new window will appear. Browse through the list and examine what the wireless users were downloading. Under the *Packet number* column, find item #10349 (37558.jpg) and select it. Click the **Save As** button.

Wireshark: HTTP object list					
Packet num	Hostname	Content Type	Size	Filename	
10286	t3.gstatic.com	image/jpeg	2739 bytes	logitech-clearchat-1536x864@1080p_10286.jpg	
10292		image/jpeg	2290 bytes		
10298	t2.gstatic.com	image/jpeg	3000 bytes	wireless_repeater-1536x864@1080p_10298.jpg	
10302	t1.gstatic.com	image/jpeg	2657 bytes	wireless-ap-network-1536x864@1080p_10302.jpg	
10349	static.howstuffworks.com	image/jpeg	15 kB	37558.jpg	
10365	www.google.com	text/html	51 kB	search?hl=en&q=	
10393	img.youtube.com	image/jpeg	1673 bytes	default.jpg	
10395	10.0.0.1	text/html	1.820 kB	index.html	

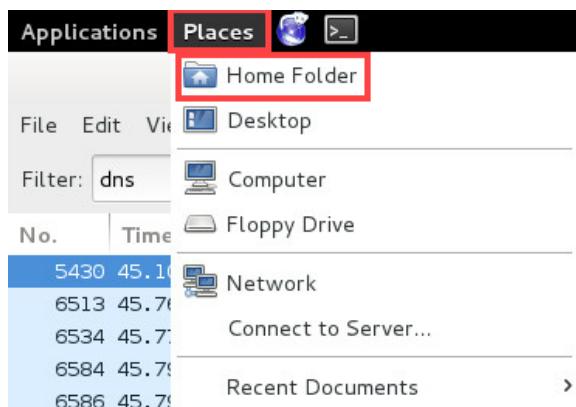
At the bottom of the dialog, there are three buttons: "Help", "Save As" (highlighted with a red box), "Save All", and "Cancel".

13. In the *Save Object As* window, select **root** from the *Places* column located on the left and click **Save**.



14. **Close** the *HTTP object list* window.

15. View the file by selecting the **Places** menu option from the top menu pane and click **Home Folder**.



Notice the new *JPEG* file in the *Home* folder.

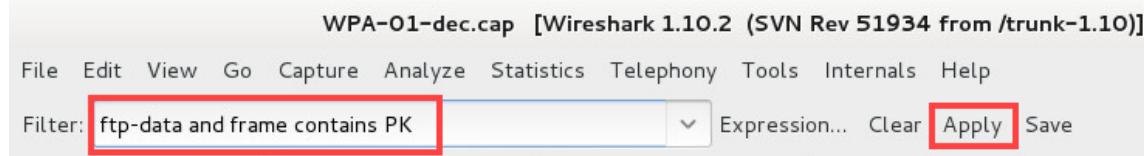
16. **Close** the *File Manager* window.

17. Change focus to the **Wireshark** application and type **ftp** in the *Filter:* pane. Click **Apply**.



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

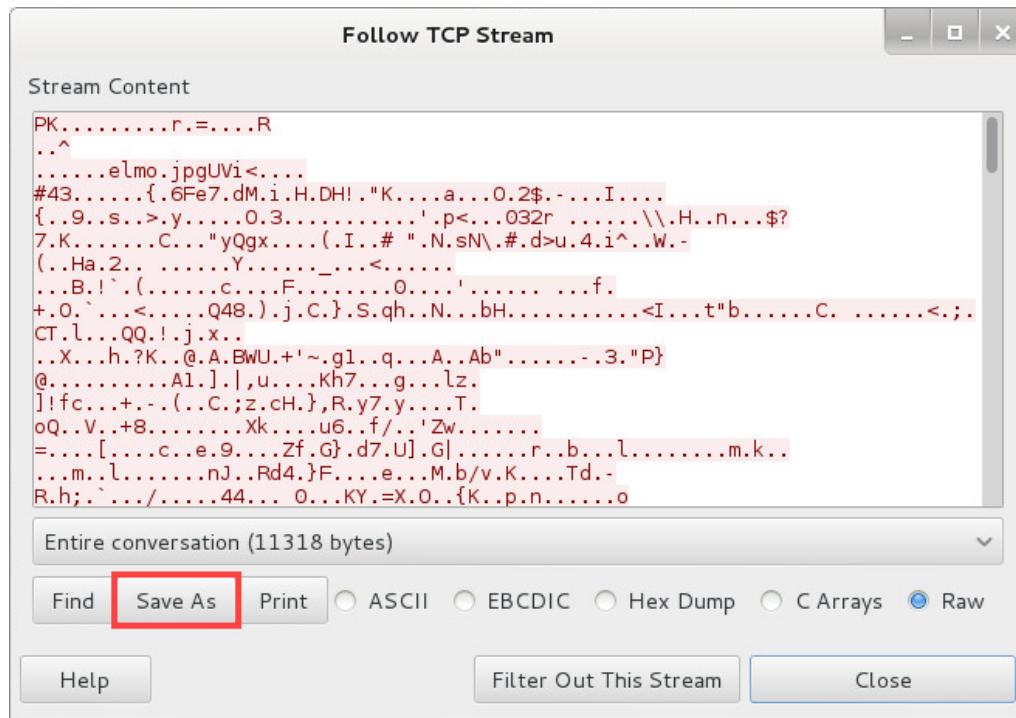
18. Scroll down through the *ftp frames* and examine some of the file names that were transferred.  
 19. Pull one of the zip files transferred via *FTP*. Type **ftp-data and frame contains PK** into the *Filter:* pane. Click **Apply**.



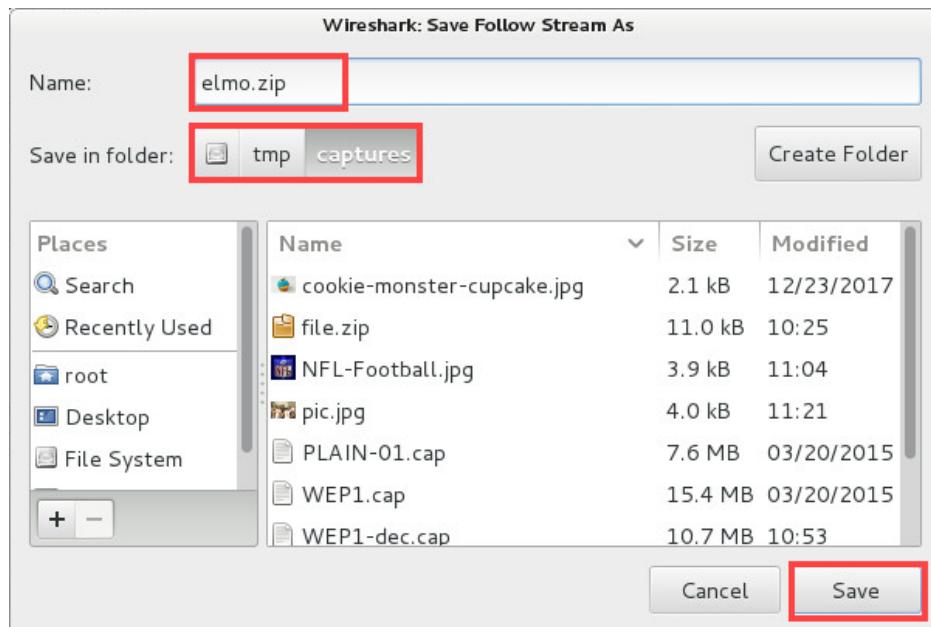
20. Right-click on the **second frame** in the list (#421) and select **Follow TCP Stream**.

No.	Time	Source	Destination	Protocol	Length	Info
211	35.066059	192.168.2.3	192.168.2.2			Mark Packet (toggle)
421	38.208899	192.168.2.3	192.168.2.2			Ignore Packet (toggle)
424	38.211459	192.168.2.3	192.168.2.2			Set Time Reference (toggle)
428	38.214019	192.168.2.3	192.168.2.2			Time Shift...
430	38.214533	192.168.2.3	192.168.2.2			Packet Comment...
534	39.691781	192.168.2.3	192.168.2.2			
537	39.694339	192.168.2.3	192.168.2.2			
540	39.696387	192.168.2.3	192.168.2.2			Manually Resolve Address
963	42.370240	192.168.2.3	192.168.2.2			Apply as Filter > 1
982	42.379965	192.168.2.3	192.168.2.2			Prepare a Filter > 1
1025	42.401984	192.168.2.3	192.168.2.2			Conversation Filter > 1
1040	42.409168	192.168.2.3	192.168.2.2			Colorize Conversation > 1
1206	42.499280	192.168.2.3	192.168.2.2			SCTP > 1
				<b>Follow TCP Stream</b>		

21. A new window appears. Click the **Save As** button.



22. For the name, type **elmo.zip**. Verify the directory you are saving the file to **/tmp/captures**. Click **Save**.



23. Close the *Follow TCP Stream* window.

24. Open a new **terminal** window. Verify that you are in the **/root** directory by typing the command below, followed by pressing **Enter**.

```
root@Kali - Attacker: ~# pwd
```

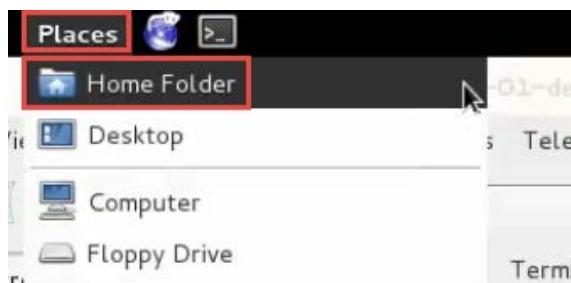
```
root@Kali-Attacker:~# pwd  
/root
```

25. Type the command below to **unzip** the contents of **elmo.zip**.

```
root@Kali - Attacker: ~# unzip /tmp/captures/elmo.zip
```

```
root@Kali-Attacker:~# unzip /tmp/captures/elmo.zip  
Archive: /tmp/captures/elmo.zip  
  inflating: elmo.jpg  
  extracting: elmo2.jpg  
  extracting: elmo3.jpg
```

26. Select the **Places** menu option located on the top menu pane and click on **Home Folder**.



Notice the extracted *Elmo* images from the zipped file.

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