Sniffing

Module 07

Sniffing a Network

A packet sniffer is a type of plug-and-play wiretap device attached to a computer that eavesdrops on network traffic. It monitors any bit of information entering or leaving a network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

"Sniffing" is the process of monitoring and capturing data packets passing through a given network using software or hardware devices. There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network.

Although passive sniffing was predominant in earlier days, proper network-securing architecture has been implemented (switch-based network) to mitigate this kind of attack. However, it contains a few loopholes in switch-based network implementation that can open doors for an attacker to sniff network traffic.

Attackers hack the network using sniffers, where he/she mainly targets the protocols vulnerable to sniffing. Some of the protocols vulnerable to sniffing include HTTP, FTP, SMTP, POP, and so on. The sniffed traffic comprises FTP and Telnet passwords, chat sessions, email and web traffic, DNS traffic, and so on. Once attackers obtain such sensitive information, they might attempt to impersonate target user sessions.

Thus, it is essential to assess the security of the network's infrastructure, find the loopholes in it and patch them up to ensure a secure network environment. So, as an ethical hacker/penetration tester, your duties include:

- Implementing network auditing tools such as Wireshark, Cain & Abel, etc. in attempt to find loopholes in the network
- Using security tools such as PromqryUI to detect attacks on the network, and so on

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

Lab Objectives

The objective of this lab is to make students learn to sniff a network and analyze packets for any attacks on the network.

The primary objectives of this lab are to:

- Sniff the network
- Analyze incoming and outgoing packets
- Troubleshoot the network for performance
- Secure the network from attacks

Lab Environment

In this lab, you will need:

- A Web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 90 Minutes

Overview of Sniffing Network

Sniffing is performed to collect basic information from the target and its network. It helps to find vulnerabilities and select exploits for attack. It determines network, system, and organizational information.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or nonprofit charity.

Recommended labs to assist you in sniffing the network:

- Sniffing Passwords using **Wireshark**
- Analyzing a Network Using the **Capsa Network Analyzer**
- Sniffing the Network Using the **OmniPeek Network Analyzer**
- Spoofing MAC Address Using **SMAC**
- Performing Man-in-the-Middle Attack using **Cain & Abel**
- Detecting Systems running in **Promiscuous mode** in a Network using **PromqryUI**
- Detecting **ARP Poisoning** in a **Switch** Based Network
- Detecting ARP attacks with **XArp** tool
- Performing **DNS Poisoning** in a Switch Based Network

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Sniffing Passwords Using Wireshark

Wireshark is a network packet analyzer, which is used to capture network packets and display packet data in detail.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Data traversing an HTTP channel is prone to MITM attacks, as it flows in plain-text format. Network administrators can use sniffers to troubleshoot network problems, examine security problems and debug protocol implementations. However, an attacker can use the tools such as Wireshark and sniffs the traffic flowing between the client and the server. This traffic obtained by the attacker might contain sensitive information such as login credentials, which can be used to perform malicious activities such as user-session impersonation.

As an ethical hacker, you need to perform network security assessments, and suggest proper troubleshooting techniques to mitigate attacks. This lab gives you hands-on experience of how to use Wireshark to sniff network traffic and capture it on a remote interface.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

The objective of this lab is to demonstrate sniffing to capture traffic from multiple interfaces and collect data from any network topology.

In this lab, you will learn how to:

- Capture Passwords of Local Interface and
- Capture traffic from Remote Interface

Lab Environment

In this lab, you will need:

- Wireshark, located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Wireshark**

- You can also download the latest version of Wireshark from the link https://www.wireshark.org/download.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as Host (Attacker) machine
- A virtual machine running Windows 8.1 (Victim machine)
- A Web browser with Internet connection
- **Administrative** privileges to run tools

You can download Wireshark from http://www.wireshark.org.

Lab Duration

Time: 15 Minutes

Overview of Password Sniffing

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can capture data packets only from within a given subnet, which means that it cannot sniff packets from another network. Often any laptop can plug into a network and gain access to it. Many enterprises' switch ports are open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all of the network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

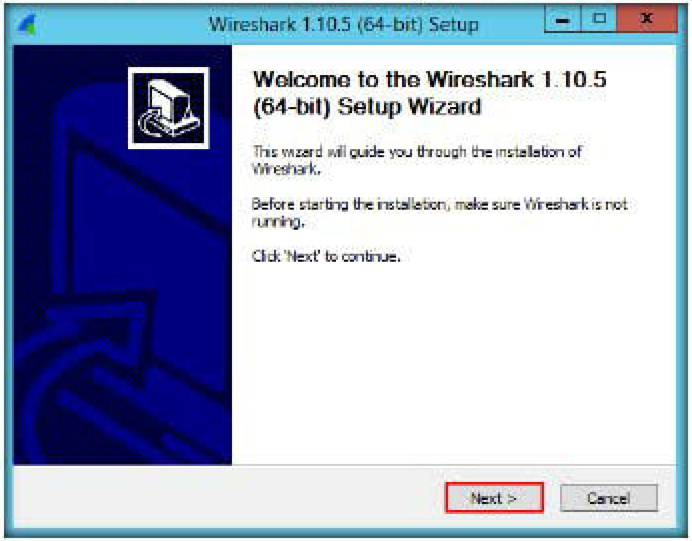
Lab Tasks

TASK 1

Install Wireshark

1. Before starting this lab, ensure that WinPcap is installed. Also, log into the virtual machine(s).
2. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Wireshark** and double-click **Wireshark-win64-1.10.5.exe**.
3. If **Open File - Security Warning** pop-up appears, click **Run**.

4. Follow the wizard-driven installation steps to install Wireshark.



Wireshark 1.10.5 (64-bit) Setup

Welcome to the Wireshark 1.10.5 (64-bit) Setup Wizard

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

FIGURE 1.1: Wireshark installation wizard

Wireshark is an open source software project, and is released under the GNU General Public License (GPL)

5. On completing the installation, launch **Wireshark** from the **Apps** screen.

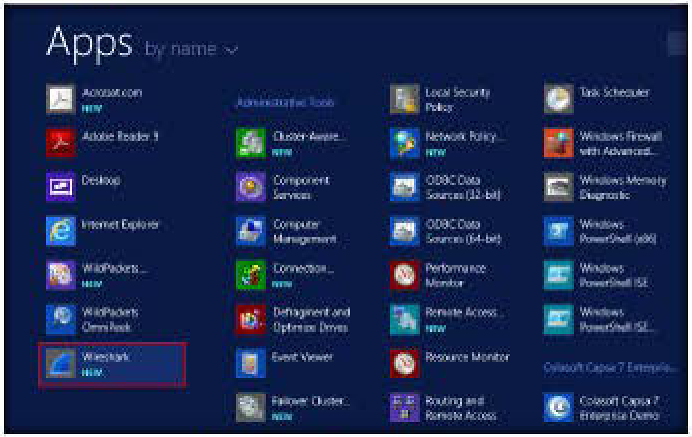


FIGURE 1.2: Windows Server 2012 - Apps screen

TASK 2

Configure Wireshark and Capture Traffic

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well.

6. The **Wireshark** main window appears, as shown in the screenshot:

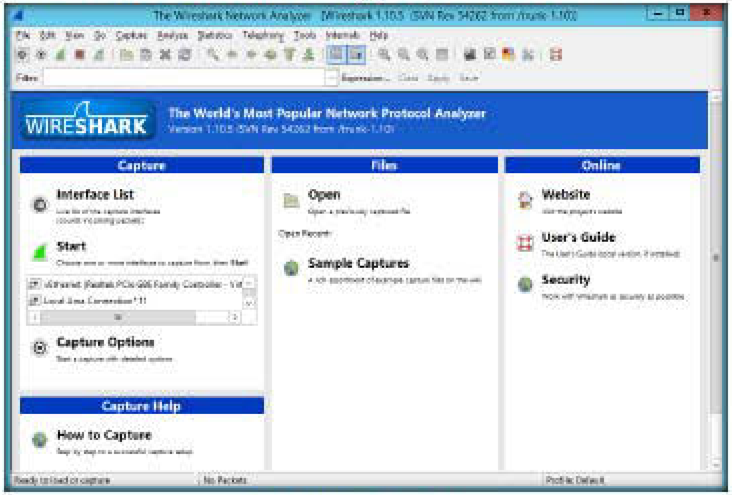

The Wireshark Network Analyzer [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.5 (SVN Rev 54262 from /trunk-1.10)
Capture
Interface List
Start
vEthernet (Realtek PCIe GBE Family Controller - Vir
Local Area Connection* 11
Capture Options
Capture Help
How to Capture
Files
Open
Open Recent:
Sample Captures
Online
Website
User's Guide
Security
Ready to load or capture
No Packets
Profile: Default

FIGURE 1.3: Wireshark Main Window

7. From the Wireshark menu bar, click **Capture → Interfaces (Ctrl+I)**.

Wireshark is used for:

Network administrators use it to troubleshoot network problems

- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

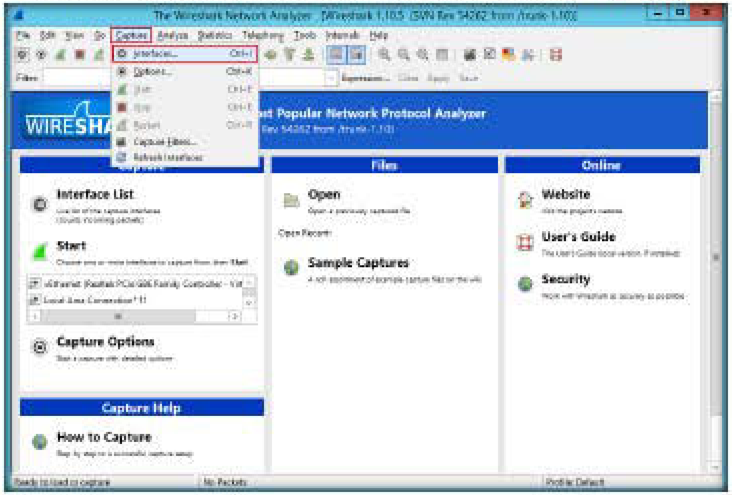
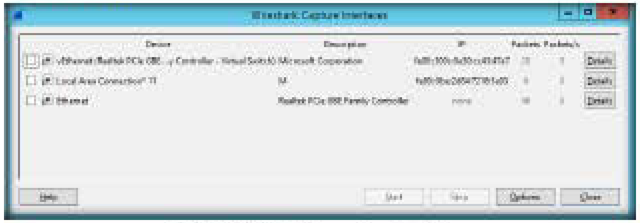


FIGURE 1.4: Wireshark Main Window with Interface Option

8. The **Wireshark: Capture Interfaces** window appears, as shown in the screenshot:

A supported network card for capturing Ethernet: Any card supported by Windows should work. See the wiki pages on Ethernet capture and offloading for issues that may affect your environment.



Wireshark: Capture Interfaces

	Device	Description	IP	Packets	Packets/s	
□	vEthernet (Realtek PCIe GBE ...y Controller - Virtual Switch)	Microsoft Corporation	fe80::300c:fa30:cc[illegible]	[illegible]	[illegible]	Details
□	Local Area Connection* 11	M	fe80::9ba:2d64:[illegible]	[illegible]	[illegible]	Details
□	Ethernet	Realtek PCIe GBE Family Controller	none	[illegible]	[illegible]	Details

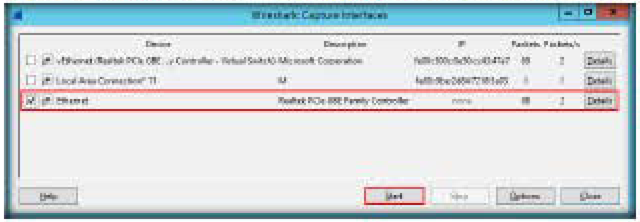
FIGURE 1.5: Wireshark Capture Interfaces Window

9. In the window, find and check the Ethernet Driver Interface connected to the system.

10. In the above screenshot, it is the **Ethernet**. The **interface** should show some packets passing through it, as it is connected to the network.

Note: This interface might vary in your lab environment.

11. Click **Start** to start capturing the traffic associated with the interface.



Wireshark: Capture Interfaces

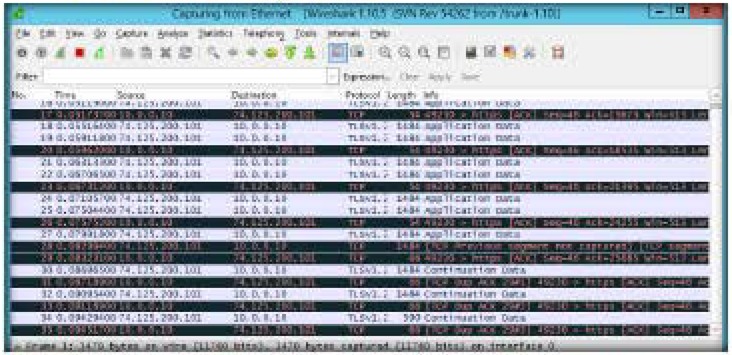
	Device	Description	IP	Packets	Packets/s	
□	vEthernet (Realtek PCIe GBE ...y Controller - Virtual Switch)	Microsoft Corporation	fe80::300c:fa30:cc[illegible]	[illegible]	[illegible]	Details
□	Local Area Connection* 11	M	fe80::9ba:2d64:[illegible]	[illegible]	[illegible]	Details
☑	Ethernet	Realtek PCIe GBE Family Controller	none	[illegible]	[illegible]	Details

FIGURE 1.6: Wireshark Capture Interfaces Window – Starting Capture

12. Wireshark starts capturing the packets generated while any traffic is received or sent from your machine.

Wireshark Features:

- Available for UNIX and Windows
- Capture live packet data from a network interface
- Display packets with very detailed protocol information
- Open and Save packet data captured
- Import and Export packet data from and to a lot of other capture programs



Capturing from Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source          Destination     Protocol Length Info
17 0.05174300 10.0.0.18      74.125.200.101  TCP      54 49230 > https [ACK] [illegible]
18 0.05516400 74.125.200.101 10.0.0.18       TLSv1.2  1484 Application Data
19 0.05811800 74.125.200.101 10.0.0.18       TLSv1.2  1484 Application Data
20 [illegible] 10.0.0.18     74.125.200.101  TCP      54 49230 > https [ACK] [illegible]
21 0.06814800 74.125.200.101 10.0.0.18       TLSv1.2  1484 Application Data
22 0.06706500 74.125.200.101 10.0.0.18       TLSv1.2  1484 Application Data
23 [illegible] 10.0.0.18     74.125.200.101  TCP      54 49230 > https [ACK] [illegible]
24 0.07105700 74.125.200.101 10.0.0.18       TLSv1.2  1484 Application Data
25 0.07504400 74.125.200.101 10.0.0.18       TLSv1.2  1484 Application Data
26 [illegible] 10.0.0.18     74.125.200.101  TCP      54 49230 > https [ACK] [illegible]
27 0.07981800 74.125.200.101 10.0.0.18       TLSv1.2  1484 Application Data
28 [illegible] 74.125.200.101 10.0.0.18      TCP      1484 [TCP Previous segment not captured] [illegible]
29 [illegible] 10.0.0.18     74.125.200.101  TCP      66 49230 > https [ACK] [illegible]
30 0.08086500 74.125.200.101 10.0.0.18       TLSv1.2  1484 Continuation Data
31 [illegible] 10.0.0.18     74.125.200.101  TCP      66 [TCP Dup ACK [illegible]] 49230 > https [ACK] [illegible]
32 0.09095400 74.125.200.101 10.0.0.18       TLSv1.2  1484 Continuation Data
33 [illegible] 10.0.0.18     74.125.200.101  TCP      66 [TCP Dup ACK [illegible]] 49230 > https [ACK] [illegible]
34 0.09429400 74.125.200.101 10.0.0.18       TLSv1.2  590 Continuation Data
35 [illegible] 10.0.0.18     74.125.200.101  TCP      66 [TCP Dup ACK [illegible]] 49230 > https [ACK] [illegible]
> Frame 1: 1470 bytes on wire (11760 bits), 1470 bytes captured (11760 bits) on interface 0
```

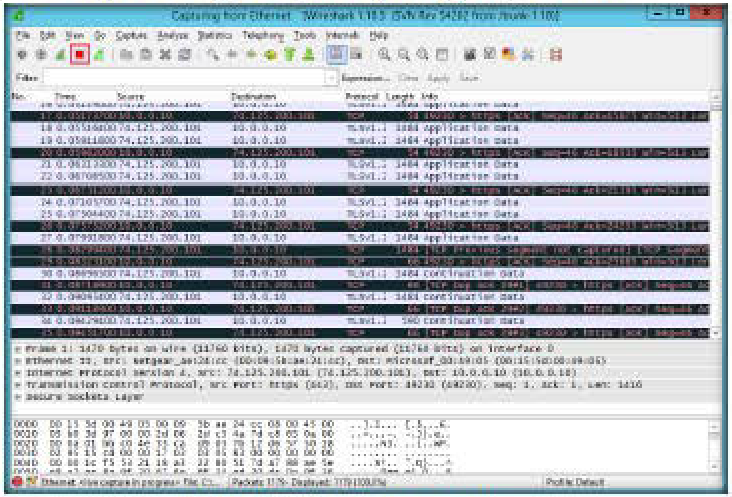
FIGURE 1.7: Wireshark Window with Packets Captured

13. Now, switch to the virtual machine (Windows 8.1), and log into your email account for which you would like to sniff the password.

TASK 3

Stop Live Capturing

14. **Stop the running live capture** by clicking ■ on the toolbar.


Capturing from Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info

```
18 0.05516400 74.125.200.101   10.0.0.10   TLSv1.2  1484 Application Data
19 0.05811800 74.125.200.101   10.0.0.10   TLSv1.2  1484 Application Data
21 0.06212300 74.125.200.101   10.0.0.10   TLSv1.2  1484 Application Data
22 0.06708500 74.125.200.101   10.0.0.10   TLSv1.2  1484 Application Data
24 0.07103700 74.125.200.101   10.0.0.10   TLSv1.2  1484 Application Data
25 0.07504400 74.125.200.101   10.0.0.10   TLSv1.2  1484 Application Data
27 0.07901800 74.125.200.101   10.0.0.10   TLSv1.2  1484 Application Data
30 0.08099300 74.125.200.101   10.0.0.10   TLSv1.2  1484 Continuation Data
32 0.08495400 74.125.200.101   10.0.0.10   TLSv1.2  1484 Continuation Data
34 0.08629800 74.125.200.101   10.0.0.10   TLSv1.2   590 Continuation Data
```

```
+ Frame 1: 1470 bytes on wire (11760 bits), 1470 bytes captured (11760 bits) on interface 0
+ Ethernet II, Src: Netgear_ae:24:cc (00:09:5b:ae:24:cc), Dst: Microsof_00:49:05 (00:15:5d:00:49:05)
+ Internet Protocol Version 4, Src: 74.125.200.101 (74.125.200.101), Dst: 10.0.0.10 (10.0.0.10)
+ Transmission Control Protocol, Src Port: https (443), Dst Port: 49230 (49230), Seq: 1, Ack: 1, Len: 1416
+ Secure Sockets Layer
```

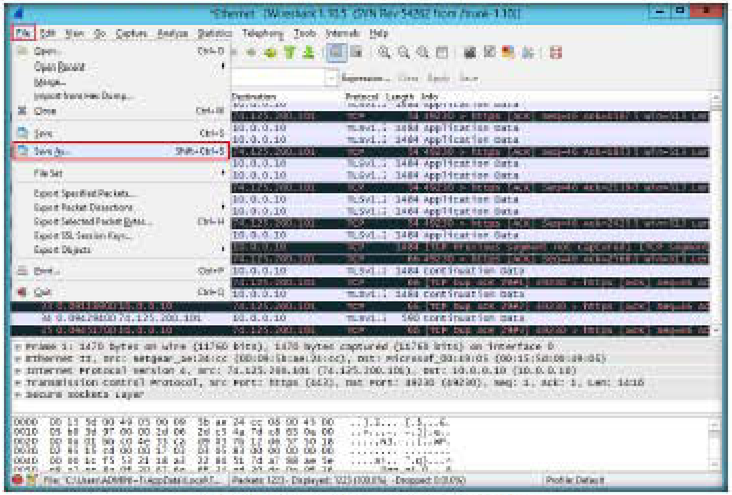
Ethernet: <live capture in progress> File: C:...
Packets: 1179 · Displayed: 1179 (100.0%)
Profile: Default

FIGURE 1.8: Wireshark Window - Stopping Live Capture

TASK 4

Save Captured Files

15. Click **File → Save As...** to save the captured packets.

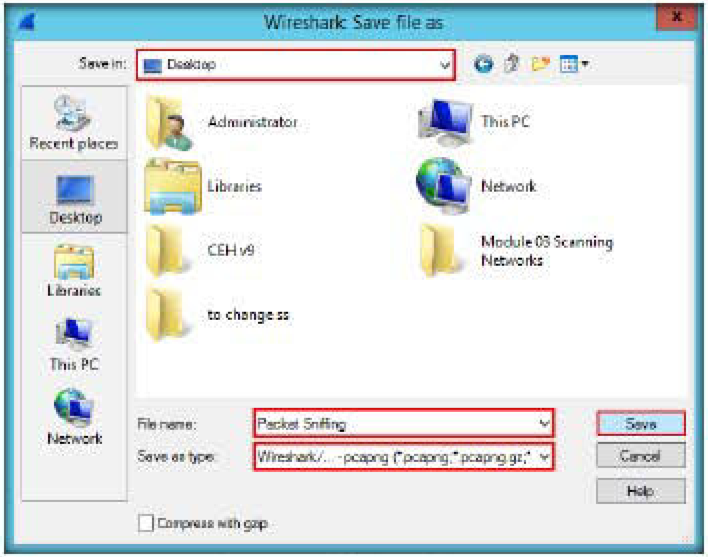

*Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Open... Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Selected Packet Bytes... Ctrl+H
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
Expression... Clear Apply Save
Destination Protocol Length Info

```
+ Frame 1: 1470 bytes on wire (11760 bits), 1470 bytes captured (11760 bits) on interface 0
+ Ethernet II, Src: Netgear_ae:24:cc (00:09:5b:ae:24:cc), Dst: Microsof_00:49:05 (00:15:5d:00:49:05)
+ Internet Protocol Version 4, Src: 74.125.200.101 (74.125.200.101), Dst: 10.0.0.10 (10.0.0.10)
+ Transmission Control Protocol, Src Port: https (443), Dst Port: 49230 (49230), Seq: 1, Ack: 1, Len: 1416
+ Secure Sockets Layer
```

File: "C:\Users\ADMINI~1\AppData\Local\T...
Packets: 1223 · Displayed: 1223 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

FIGURE 1.9: Wireshark - Saving the Captured Packets

16. Select a destination to save the file, specify a file name, and select a file format. Click **Save**. Here, **pcapng** format has been chosen.



Save in: Desktop

File name: Packet Sniffing

Save as type: Wireshark/... - pcapng (*.pcapng;*.pcapng.gz;*

☐ Compress with gzip

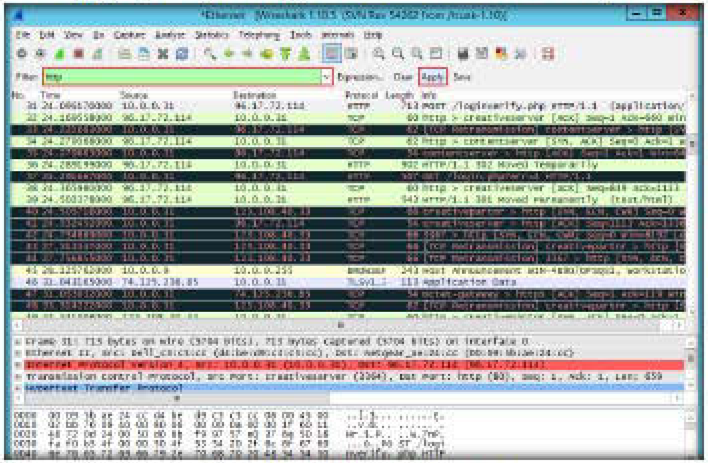
FIGURE 1.10 Wireshark Saving a packet capture

TASK 5

Look for passwords

17. Filter HTTP traffic by issuing **http** syntax in the Filter field, and click **Apply**.

18. Applying this syntax helps you narrow down the search for passwords.


*Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

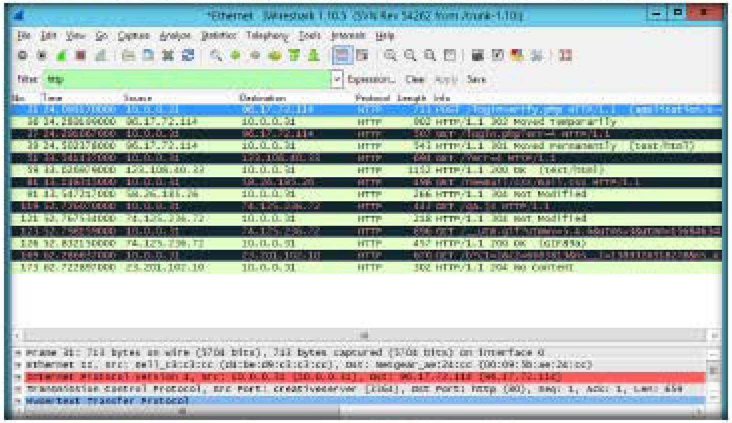
Filter: http

```
No. Time          Source        Destination   Protocol Length Info
 31 24.086170000  10.0.0.31     96.17.72.114  HTTP      713 POST /loginverify.php HTTP/1.1  (application/
 32 24.160558000  96.17.72.114  10.0.0.31     TCP        60 http > creativeserver [ACK] Seq=1 Ack=660 Win
 33 [illegible]
 34 24.279068000  96.17.72.114  10.0.0.31     TCP        62 http > contentserver [SYN, ACK] Seq=0 Ack=1 W
 35 [illegible]
 36 24.285199000  96.17.72.114  10.0.0.31     HTTP      502 HTTP/1.1 302 Moved Temporarily
 37 [illegible]
 38 24.365980000  96.17.72.114  10.0.0.31     TCP        60 http > creativeserver [ACK] Seq=449 Ack=1111
 39 24.500378000  96.17.72.114  10.0.0.31     HTTP      543 HTTP/1.1 301 Moved Permanently  (text/html)
 40 [illegible]
 41 [illegible]
 42 [illegible]
 43 [illegible]
 44 [illegible]
 45 28.125762000  10.0.0.8      10.0.0.255    BROWSER   243 Host Announcement WIN-4880/OP3Q01, Workstatio
 46 31.043185000  74.125.238.85 10.0.0.31     TLSv1.2   113 Application Data
 47 [illegible]
 48 [illegible]

+ Frame 31: 713 bytes on wire (5704 bits), 713 bytes captured (5704 bits) on interface 0
+ Ethernet II, Src: Dell_c1:c1:cc (d4:be:d9:c1:c1:cc), Dst: Netgear_ae:24:cc (00:09:5b:ae:24:cc)
+ Internet Protocol Version 4, Src: 10.0.0.31 (10.0.0.31), Dst: 96.17.72.114 (96.17.72.114)
+ Transmission Control Protocol, Src Port: creativeserver (3364), Dst Port: http (80), Seq: 1, Ack: 1, Len: 659
+ Hypertext Transfer Protocol
```

FIGURE 1.11: Wireshark - Filtering http traffic

Wireshark can save packets captured in a large number of formats of other capture programs.

19. Wireshark filters only http packets, as shown in the screenshot:


*Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

```
No.  Time          Source          Destination     Protocol Length Info
 31 24.[illegible] 10.0.0.31       98.17.72.114    HTTP      711 POST /loginverify.php HTTP/1.1  (application/x-
 36 24.288609000   98.17.72.114    10.0.0.31       HTTP      602 HTTP/1.1 302 Moved Temporarily
 37 24.[illegible] 10.0.0.31       98.17.72.114    HTTP      500 GET /login.php?err=4 HTTP/1.1
 39 24.502178000   98.17.72.114    10.0.0.31       HTTP      543 HTTP/1.1 301 Moved Permanently  (text/html)
 51 33.[illegible] 10.0.0.31       [illegible]     HTTP      [illegible]
 59 33.020604000   123.108.40.22   10.0.0.31       HTTP     1152 HTTP/1.1 200 OK  (text/html)
 81 33.[illegible] 10.0.0.31       [illegible]     HTTP      496 GET [illegible] HTTP/1.1
 91 33.547317000   58.26.185.26    10.0.0.31       HTTP      266 HTTP/1.1 304 Not Modified
119 52.[illegible] 10.0.0.31       74.125.236.72   HTTP      443 GET /ga.js HTTP/1.1
121 52.767534000   74.125.236.72   10.0.0.31       HTTP      218 HTTP/1.1 304 Not Modified
123 52.[illegible] 10.0.0.31       74.125.236.72   HTTP      898 GET /__utm.gif?[illegible]
128 52.832130000   74.125.236.72   10.0.0.31       HTTP      457 HTTP/1.1 200 OK  (GIF89a)
169 62.[illegible] 10.0.0.31       23.201.102.10   HTTP      [illegible] GET [illegible]
173 62.722897000   23.201.102.10   10.0.0.31       HTTP      302 HTTP/1.1 204 No Content
```

```
+ Frame 31: 711 bytes on wire ([illegible] bits), 711 bytes captured ([illegible] bits) on interface 0
+ Ethernet II, Src: Dell_c3:c3:cc ([illegible]), Dst: Netgear_ae:2d:cc ([illegible])
+ Internet Protocol Version 4, Src: 10.0.0.31 (10.0.0.31), Dst: 98.17.72.114 (98.17.72.114)
+ Transmission Control Protocol, Src Port: creativeserver ([illegible]), Dst Port: http (80), Seq: 1, Ack: 1, Len: 658
+ Hypertext Transfer Protocol
```

FIGURE 1.12: Wireshark - Filtering http traffic

20. Now, go to **Edit** and click **Find Packet...**

Wireshark is not an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

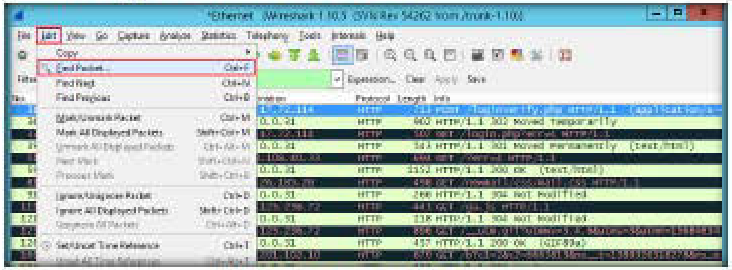
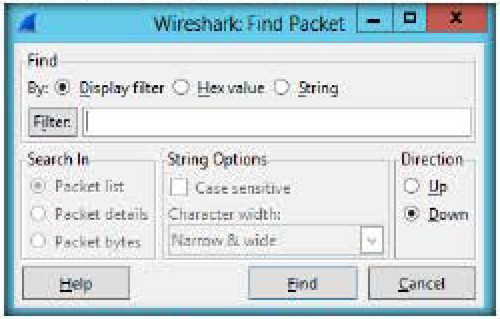

*Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Packets Shift+Ctrl+M
Unmark All Displayed Packets Ctrl+Alt+M
Next Mark Shift+Ctrl+N
Previous Mark Shift+Ctrl+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Packets Shift+Ctrl+D
Unignore All Packets Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Expression... Clear Apply Save

FIGURE 1.13: Wireshark - Finding Packet Option

21. The **Wireshark: Find Packet** window appears.



Find

By: ● Display filter ○ Hex value ○ String

Filter:

Search In: ● Packet list ○ Packet details ○ Packet bytes

String Options: □ Case sensitive; Character width: Narrow & wide

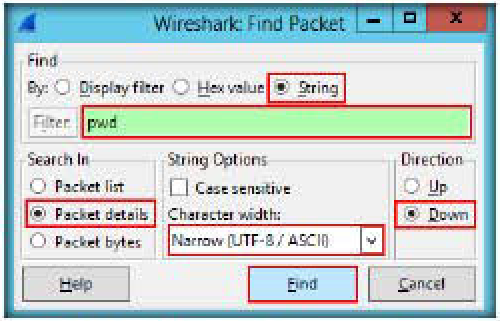
Direction: ○ Up ● Down

FIGURE 1.14: Wireshark - Find Packet Window

Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

22. Under **Find**, select **String**, type **pwd** in the **Filter** field, select **Packet details**, and select **Narrow (UTF-8 / ASCII)** from the **Character width** drop-down list.

23. Select **Down**, and click **Find**.



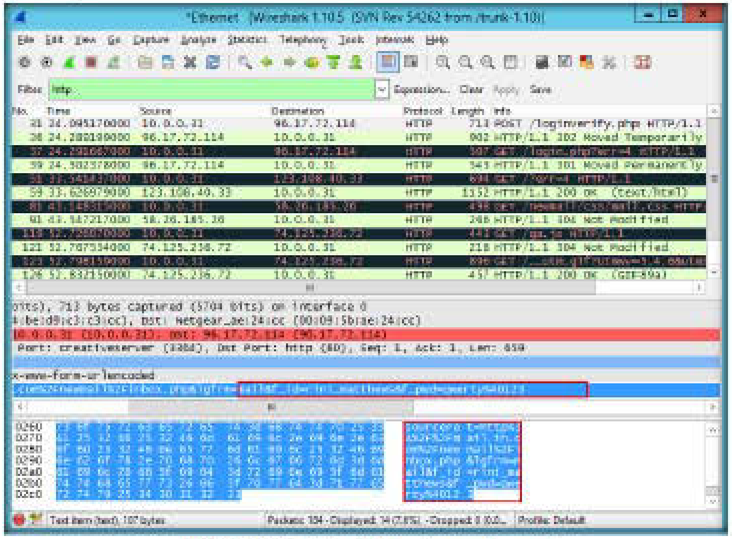
Wireshark: Find Packet

Find
By: ○ Display filter ○ Hex value ● String
Filter: pwd

Search In: ○ Packet list ● Packet details ○ Packet bytes
String Options: □ Case sensitive
Character width: Narrow (UTF-8 / ASCII)
Direction: ○ Up ● Down

FIGURE 1.15: Wireshark - Selecting Options in Find Packet Window

24. Wireshark will now display the sniffed password from the captured packets.



*Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: http

```
No.  Time          Source          Destination     Protocol Length Info
 31 24.095170000   10.0.0.31       96.17.72.114    HTTP     713 POST /loginverify.php HTTP/1.1
 36 24.280199000   96.17.72.114    10.0.0.31       HTTP     902 HTTP/1.1 302 Moved Temporarily
 37 24.291667000   10.0.0.31       96.17.72.114    HTTP     507 GET /login.php?err=4 HTTP/1.1
 39 24.302378000   96.17.72.114    10.0.0.31       HTTP     543 HTTP/1.1 301 Moved Permanently
 55 33.541437000   10.0.0.31       123.108.40.33   HTTP     694 GET /?err=4 HTTP/1.1
 59 33.626979000   123.108.40.33   10.0.0.31       HTTP    1152 HTTP/1.1 200 OK  (text/html)
 80 43.148319000   10.0.0.31       58.26.185.26    HTTP     498 GET /newmail/css/mail.css HTTP
 91 43.547217000   58.26.185.26    10.0.0.31       HTTP     246 HTTP/1.1 304 Not Modified
118 52.758070000   10.0.0.31       74.125.236.72   HTTP     443 GET /ga.js HTTP/1.1
121 52.787534000   74.125.236.72   10.0.0.31       HTTP     218 HTTP/1.1 304 Not Modified
123 52.798159000   10.0.0.31       74.125.236.72   HTTP     896 GET /__utm.gif?utmwv=5.4.6&utm
126 52.832150000   74.125.236.72   10.0.0.31       HTTP     457 HTTP/1.1 200 OK  (GIF89a)

bits), 713 bytes captured (5704 bits) on interface 0
4:be:d8:c3:c3:cc), Dst: Netgear_ae:24:cc (00:09:5b:ae:24:cc)
10.0.0.31 (10.0.0.31), Dst: 96.17.72.114 (96.17.72.114)
 Port: creativeserver (3364), Dst Port: http (80), Seq: 1, Ack: 1, Len: 659

x-www-form-urlencoded
[illegible]&pwd=[illegible]

0260  [illegible]
0270  [illegible]
0280  [illegible]
0290  [illegible]
02a0  [illegible]
02b0  [illegible]
02c0  [illegible]
```

Text item (text), 107 bytes | Packets: 304 · Displayed: 14 (7.8%) · Dropped: 0 (0.0... | Profile: Default

FIGURE 1.16: Wireshark - displaying the captured password

25. **Close** the window.

TASK 6

Capture remote network traffic using Wireshark

26. Before beginning this task, log onto the **Windows 8.1** virtual machine (assume this is the target machine) and sign into the **Jason** user account.

Note: Ensure that the **Jason** account has admin privileges.

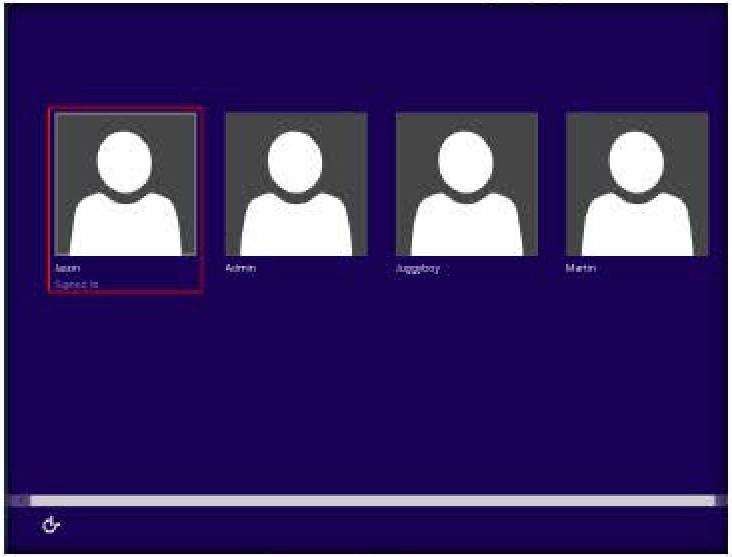


FIGURE 1.17: Login to Jason account

27. Use L0phtCrack Password auditor to sniff the user credentials of the target machine. Here, you are the attacker.

28. Switch to the host machine (**Windows Server 2012**), and navigate to **Desktop**. Hover over the lower left of the screen, right-click **Windows**, and click **Search**.

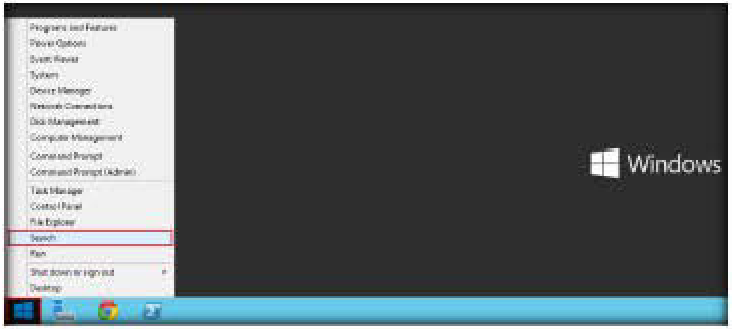


FIGURE 1.18: Selecting Search option

29. Search for **Remote Desktop Connection** (in the **Search** box) and click **Remote Desktop Connection**.

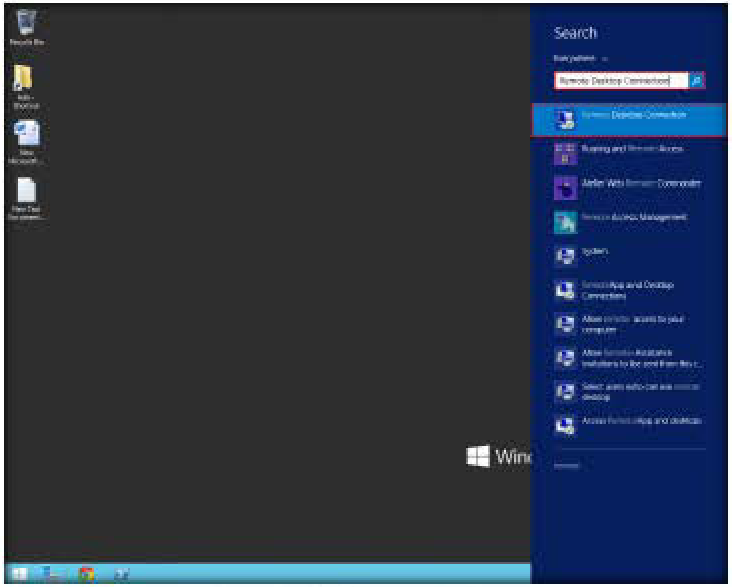
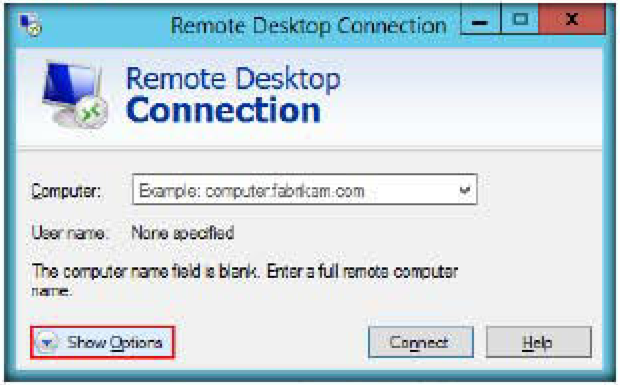


FIGURE 1.19: Searching for Remote Desktop Connection

30. The **Remote Desktop Connection** dialog box appears; click **Show Options**.


Remote Desktop Connection

Remote Desktop
Connection

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

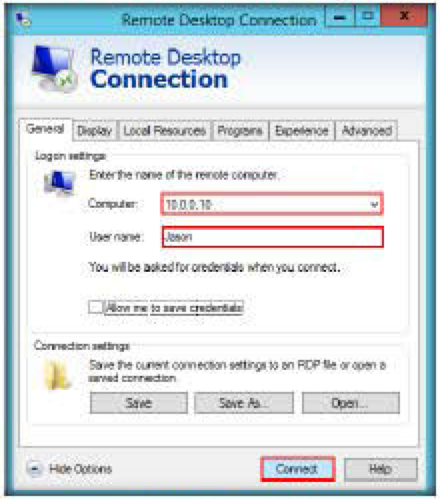
FIGURE 1.20: Remote Desktop Connection dialog box

31. The dialog box expands. Fill in the **Computer** and **User name** fields with the target machine's IP address and username.

32. Click **Connect**.

Note: The IP address and username may differ depending on your lab environment.

Here for instance, the username and password are **Jason** and **qwerty**. This is one of the user accounts in the machine with admin privileges.



Enter the name of the remote computer.

Computer: 10.0.0.10

User name: Jason

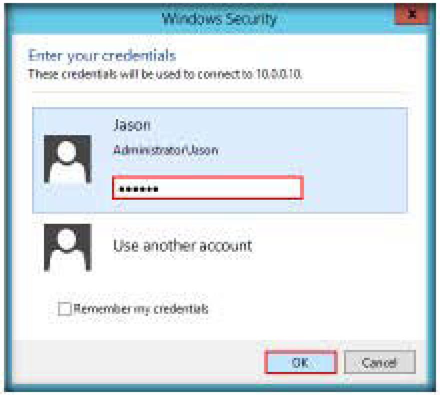
You will be asked for credentials when you connect.

□ Allow me to save credentials

Save the current connection settings to an RDP file or open a saved connection.

FIGURE 1.21: Connecting to remote desktop

33. The **Windows Security** pop-up appears. Enter the **password** (**qwerty**), and click **OK**.



Enter your credentials

These credentials will be used to connect to 10.0.0.10.

Jason

Administrator\Jason

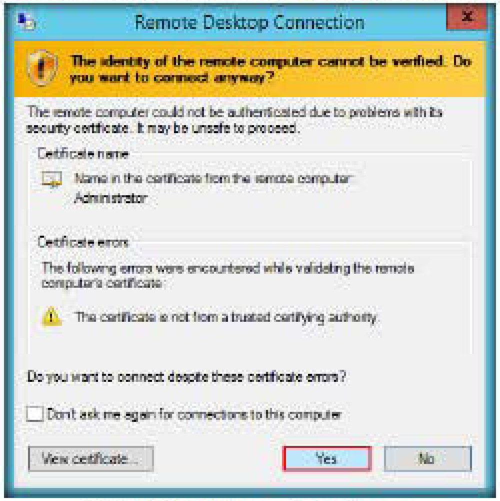
••••••

Use another account

□ Remember my credentials

FIGURE 1.22: Entering the credentials

34. The **Remote Desktop connection** pop-up appears; click **Yes**.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Administrator

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

FIGURE 1.23: Establishing Remote Desktop Connection

35. Now the target computer is remotely logged into from the host machine, as shown in the screenshot:

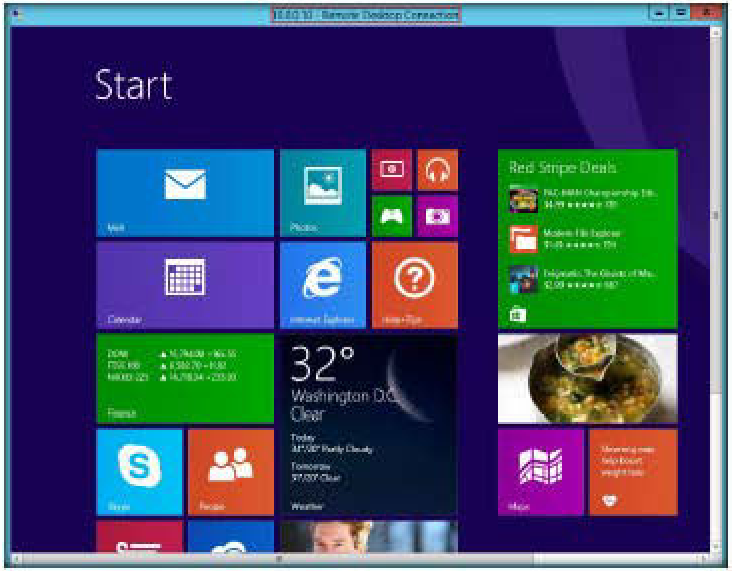


FIGURE 1.24: Remote Desktop Connection successfully established

36. Install WinPcap in this machine.

Note: If the application is already installed, skip to **step 42**.

37. Double-click Network Drive (**Z:**). If **Windows Security** pop-up appears, enter the credentials of host machine and click **OK**.

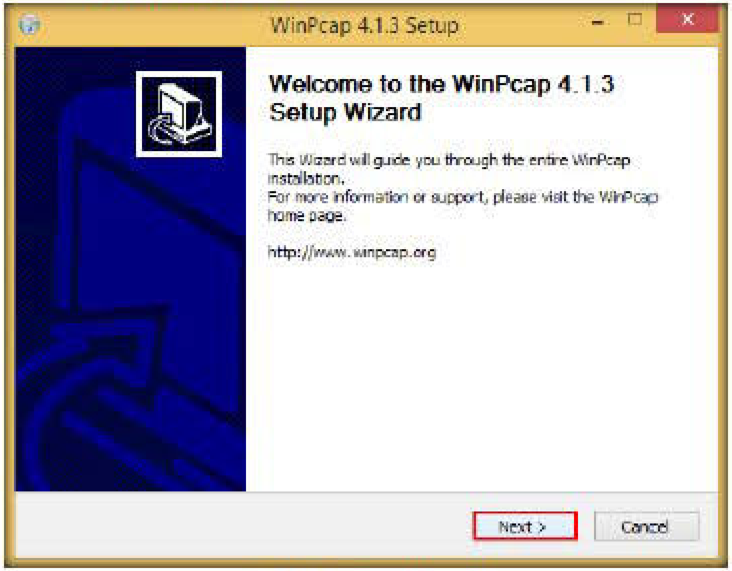
38. Navigate to **Z:\CEHv9 Lab Prerequisites\Winpcap** and double-click **WinPcap_4_1_3.exe**.

Note: If a network drive is not mapped, enter **IP address of the host machine**)**CEH-Tools\CEHv9 Lab Prerequisites\Winpcap** and double-click **WinPcap_4_1_3.exe**.

39. If a User **Account Control** dialog-box appears, click **Yes**.

40. If **Windows Security** pop-up appears, enter the credentials of host machine and click **OK**.

41. The WinPcap Setup wizard appears; follow the wizard-driven installation steps to install WinPcap.



WinPcap 4.1.3 Setup

Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

FIGURE 1.25: WinPcap installation wizard

42. Hover over the lower left of the screen; right-click **Windows,** and click **Control Panel**.

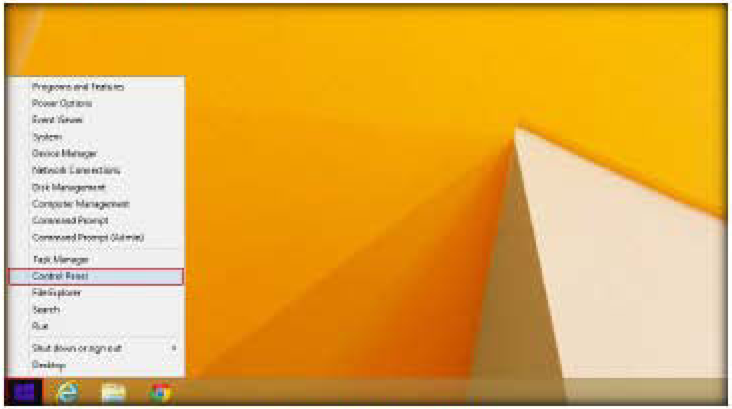


FIGURE 1.26: Selecting Control Panel

43. The **Control panel** window appears; select **Administrative Tools**.

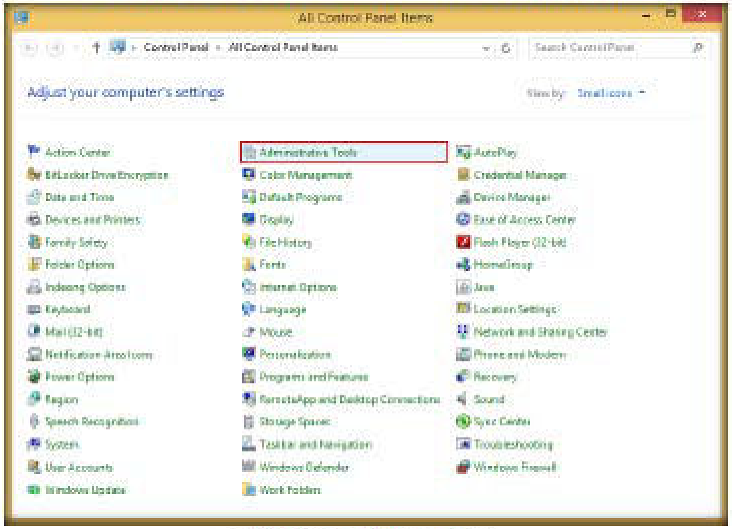
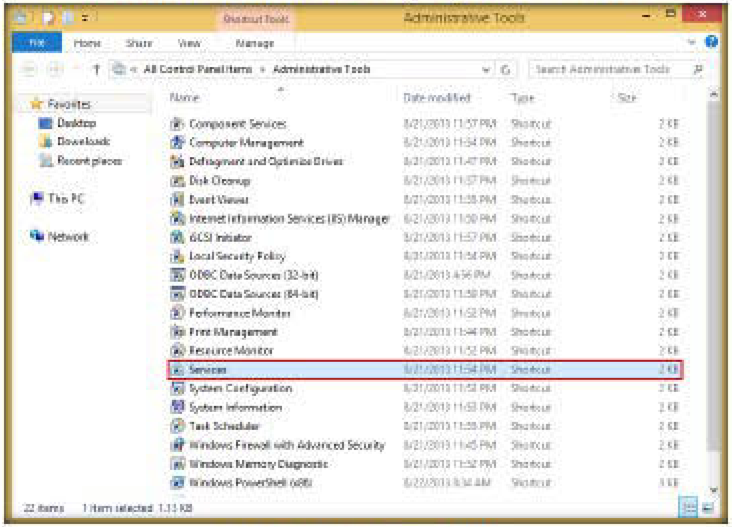


FIGURE 1.27: Selecting Administrative Tools

44. In the **Administrative Tools** control panel, double-click **Services**.



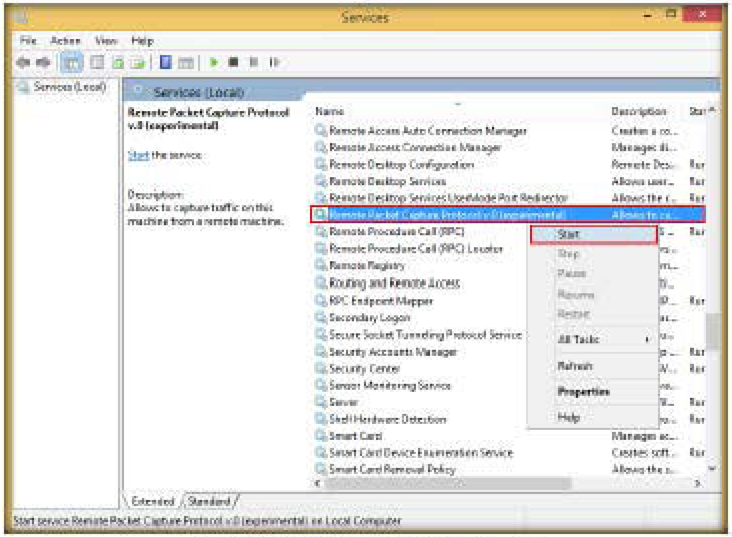
Name	Date modified	Type	Size
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
Disk Cleanup	8/21/2013 11:57 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
Internet Information Services (IIS) Manager	8/21/2013 11:50 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/21/2013 11:50 PM	Shortcut	2 KB
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Print Management	8/21/2013 11:44 PM	Shortcut	2 KB
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Services	8/21/2013 11:54 PM	Shortcut	2 KB
System Configuration	8/21/2013 11:52 PM	Shortcut	2 KB
System Information	8/21/2013 11:53 PM	Shortcut	2 KB
Task Scheduler	8/21/2013 11:55 PM	Shortcut	2 KB
Windows Firewall with Advanced Security	8/21/2013 11:45 PM	Shortcut	2 KB
Windows Memory Diagnostic	8/21/2013 11:52 PM	Shortcut	2 KB
Windows PowerShell (x86)	8/22/2013 8:34 AM	Shortcut	3 KB

22 items   1 item selected 1.13 KB

FIGURE 1.28: Launching Administrative Tools

45. In the **Services** control panel, choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service and click **Start**.

Wireshark is an open source software project, and is released under the GNU General Public License (GPL)



Remote Packet Capture Protocol v.0 (experimental)

Start the service

Description:
Allows to capture traffic on this machine from a remote machine.

Name	Description	Star
Remote Access Auto Connection Manager	Creates a co...	
Remote Access Connection Manager	Manages di...	
Remote Desktop Configuration	Remote Des...	Rur
Remote Desktop Services	Allows user...	Rur
Remote Desktop Services UserMode Port Redirector	Allows the r...	Rur
Remote Packet Capture Protocol v.0 (experimental)	Allows to ca...	
Remote Procedure Call (RPC)	S...	Rur
Remote Procedure Call (RPC) Locator	n...	
Remote Registry	m...	
Routing and Remote Access	ti...	
RPC Endpoint Mapper	P...	Rur
Secondary Logon	a...	
Secure Socket Tunneling Protocol Service	V...	
Security Accounts Manager	p...	Rur
Security Center	V...	Rur
Sensor Monitoring Service	n...	
Server	S...	Rur
Shell Hardware Detection	o...	Rur
Smart Card	Manages ac...	
Smart Card Device Enumeration Service	Creates soft...	Rur
Smart Card Removal Policy	Allows the s...	

Start service Remote Packet Capture Protocol v.0 (experimental) on Local Computer

FIGURE 1.29: Starting Remote Packet Capture Protocol v.0

46. Close the Remote Desktop Connection.

47. Launch **Wireshark** application from the **Apps** screen of the Windows Server 2012 machine.

48. The **Wireshark** main window appears, as shown in the screenshot:

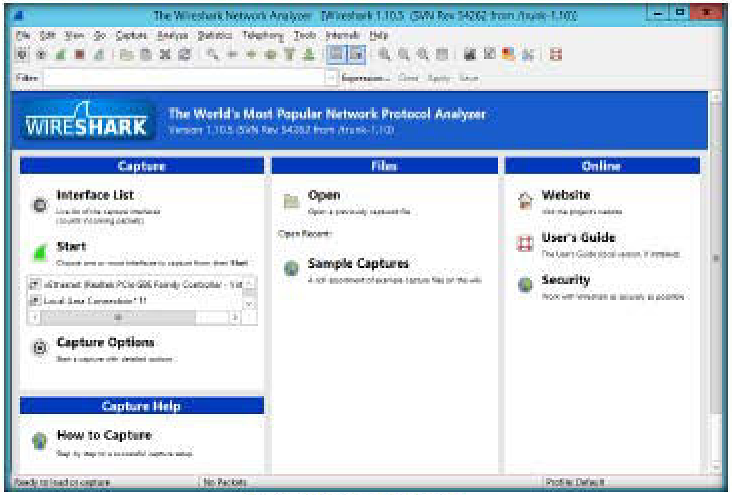

The Wireshark Network Analyzer [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.5 (SVN Rev 54262 from /trunk-1.10)
Capture
Interface List
Start
Capture Options
Capture Help
How to Capture
Files
Open
Open Recent:
Sample Captures
Online
Website
User's Guide
Security
Ready to load or capture
No Packets
Profile: Default

FIGURE 1.30: Wireshark Main Window

49. From the **Wireshark** menu bar, select **Capture → Options...**

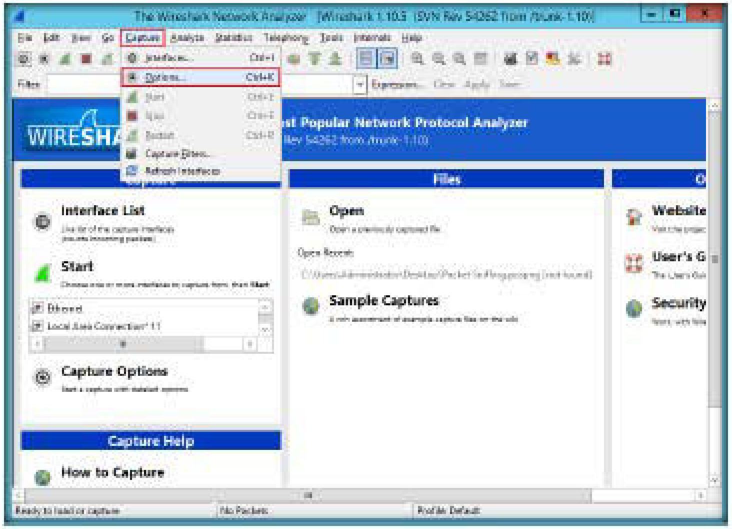
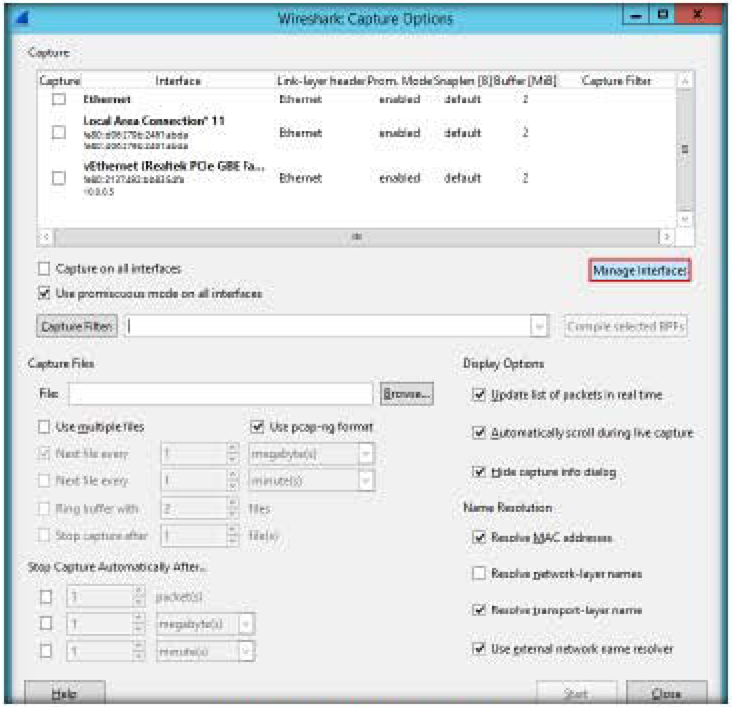


FIGURE 1.31: Selecting Options from Wireshark

50. The **Wireshark: Capture Options** window appears; click **Manage Interfaces**.



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
□	Ethernet	Ethernet	enabled	default	2	
□	Local Area Connection* 11 [illegible] [illegible]	Ethernet	enabled	default	2	
□	vEthernet (Realtek PCIe GBE Fa... [illegible] [illegible]	Ethernet	enabled	default	2	

□ Capture on all interfaces

☑ Use promiscuous mode on all interfaces

Capture Files
- File:
- □ Use multiple files
- ☑ Use pcap-ng format
- ☑ Next file every 1 megabyte(s)
- □ Next file every 1 minute(s)
- □ Ring buffer with 2 files
- □ Stop capture after 1 file(s)

Stop Capture Automatically After...
- □ 1 packet(s)
- □ 1 megabyte(s)
- □ 1 minute(s)

Display Options
- ☑ Update list of packets in real time
- ☑ Automatically scroll during live capture
- ☑ Hide capture info dialog

Name Resolution
- ☑ Resolve MAC addresses
- □ Resolve network-layer names
- ☑ Resolve transport-layer name
- ☑ Use external network name resolver

FIGURE 1.32: Selecting Options from Wireshark

51. The **Interface Management** window appears. Click the **Remote Interfaces** tab, and click **Add**.

Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

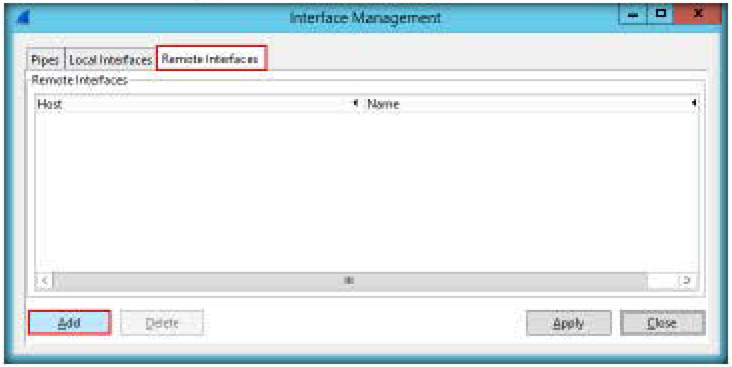


FIGURE 1.33: Interface Management window

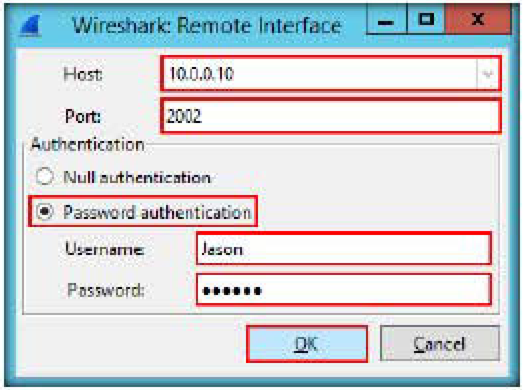
52. The **Wireshark: Remote Interface** window appears.

53. In **Host** text field, enter the IP address of the target machine and in the **Port** text field, enter the port number **2002**.

54. Under **Authentication**, select **Password authentication,** and enter the target machine's user credentials.

55. Click **OK**.

Note: The IP address and user credentials may differ in your lab environment.



Host: 10.0.0.10

Port: 2002

Authentication

○ Null authentication

● Password authentication

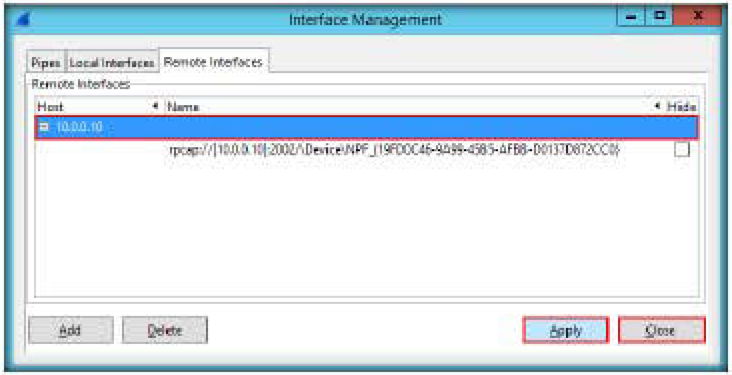
Username: Jason

Password: ••••••

FIGURE 1.34 Wireshark: Remote Interface window

56. A new remote interface is added on the **Remote Interface** tab.

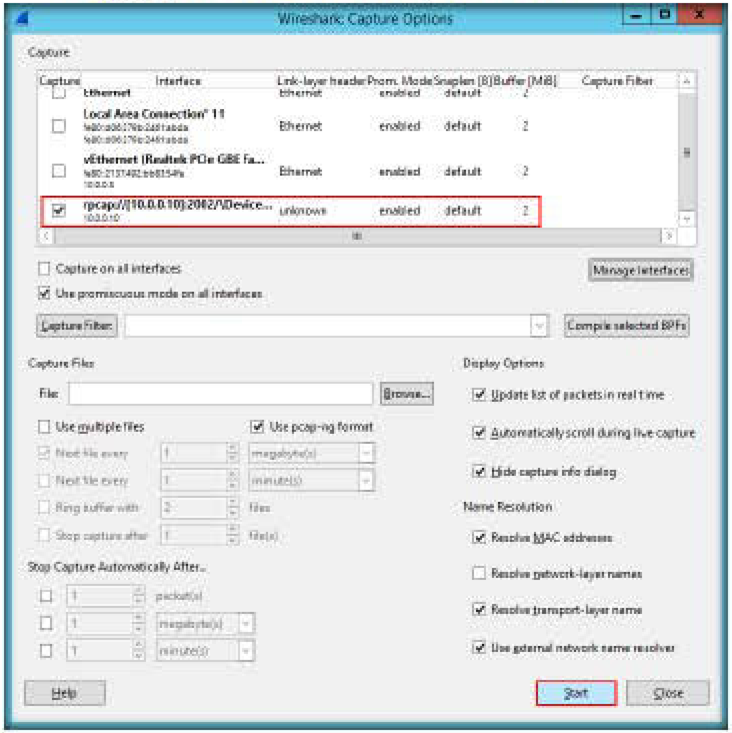
57. Select the host, click **Apply,** and click **Close**.



Host	Name	Hide
⊟ 10.0.0.10		
	rpcap://[10.0.0.10]:2002/\Device\NPF_{19FDOC46-9A99-4585-AFB8-D0137D872CC0}	□

FIGURE 1.35 Applying the newly added interface

58. The newly added remote interface appears in the **Wireshark: Capture Options** window.
59. Check the interface under which IP address of the target machine is displayed, uncheck the other interfaces, and click **Start**.



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
□	Ethernet	Ethernet	enabled	default	2	
□	Local Area Connection* 11	Ethernet	enabled	default	2	
□	vEthernet (Realtek PCIe GBE Fa...	Ethernet	enabled	default	2	
☑	rpcap://[10.0.0.10]:2002/\Device... 10.0.0.10	unknown	enabled	default	2	

□ Capture on all interfaces

☑ Use promiscuous mode on all interfaces

Capture Files

File:

□ Use multiple files ☑ Use pcap-ng format

☑ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

□ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture Automatically After...

□ 1 packet(s)

□ 1 megabyte(s)

□ 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatically scroll during live capture

☑ Hide capture info dialog

Name Resolution

☑ Resolve MAC addresses

□ Resolve network-layer names

☑ Resolve transport-layer name

☑ Use external network name resolver

FIGURE 1.36: Wireshark: Capture Options window

60. Sign into the user account **Jason** in **Windows 8.1** virtual machine. Here, you are signing in as a victim.

Note: The Remote Desktop connection gets disconnected as soon as you sign into the virtual machine.

61. Browse the Internet from the target machine.

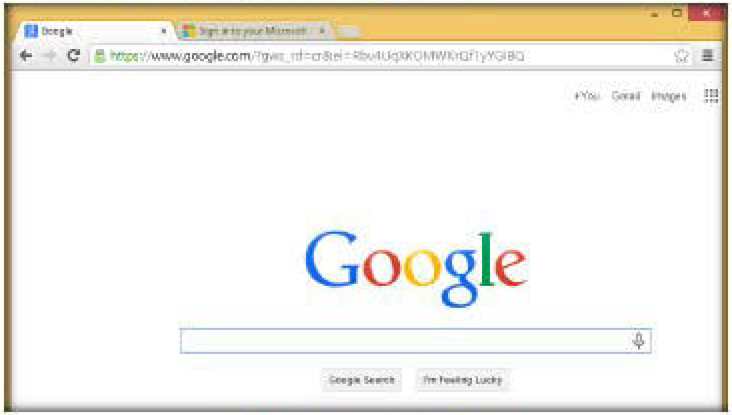
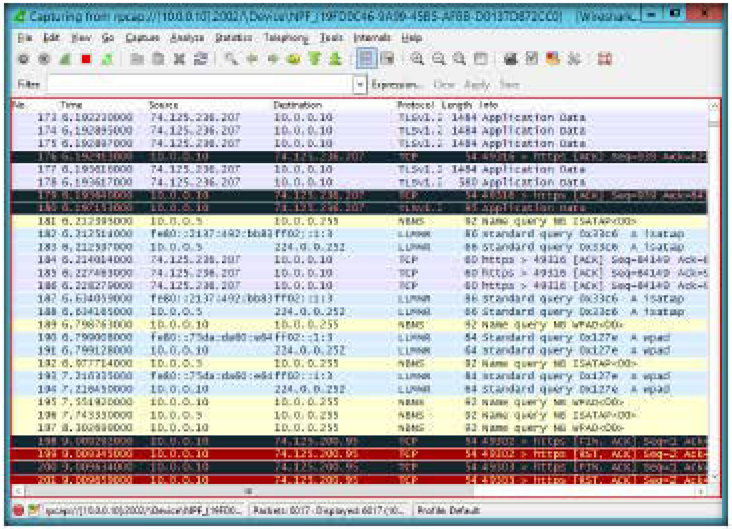

Google
Sign in to your Microsoft
https://www.google.com/?gws_rd=cr&ei=Rbv4UgXKOMWKrQf1yYGIBQ
+You
Gmail
Images
Google
Google Search
I'm Feeling Lucky

FIGURE 1.37: Browsing internet on Windows 8.1

62. Wireshark starts capturing as soon as the user (here, you) begins to browse the Internet, as shown in the screenshot:

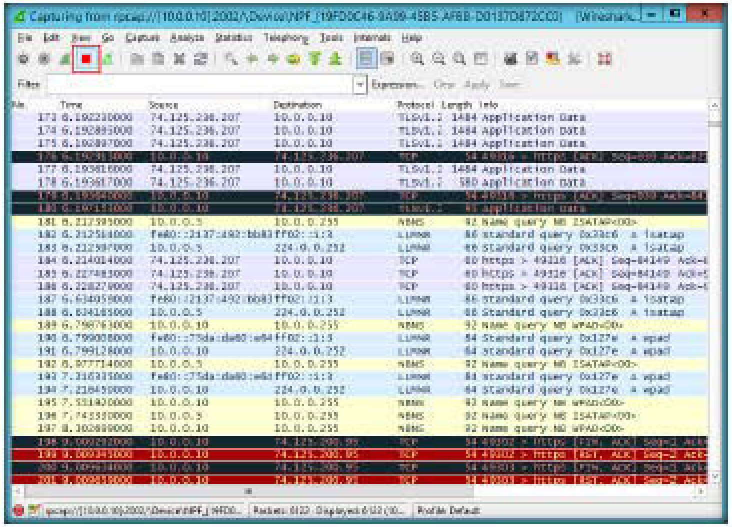

Capturing from rpcap://[10.0.0.10]:2002/\Device\NPF_{19FD0C46-9A99-45B5-AFBB-D0137D872C00} [Wireshark...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time         Source                 Destination        Protocol Length Info
  173 6.192230000  74.125.236.207         10.0.0.10          TLSv1.2  1484 Application Data
  174 6.192895000  74.125.236.207         10.0.0.10          TLSv1.2  1484 Application Data
  175 6.192897000  74.125.236.207         10.0.0.10          TLSv1.2  1484 Application Data
  176 6.192953000  10.0.0.10              74.125.236.207     TCP        54 49316 > https [ACK] Seq=939 Ack=82
  177 6.193616000  74.125.236.207         10.0.0.10          TLSv1.2  1484 Application Data
  178 6.193617000  74.125.236.207         10.0.0.10          TLSv1.2   580 Application Data
  179 6.193640000  10.0.0.10              74.125.236.207     TCP        54 49316 > https [ACK] Seq=939 Ack=84
  180 6.200153000  10.0.0.10              74.125.236.207     TLSv1.2    85 Application Data
  181 6.212395000  10.0.0.5               10.0.0.255         NBNS       92 Name query NB ISATAP<00>
  182 6.212514000  fe80::2137:492:bb83    ff02::1:3          LLMNR      86 Standard query 0x33c6  A isatap
  183 6.212597000  10.0.0.5               224.0.0.252        LLMNR      66 Standard query 0x33c6  A isatap
  184 6.214014000  74.125.236.207         10.0.0.10          TCP        60 https > 49316 [ACK] Seq=84149 Ack=
  185 6.227493000  74.125.236.207         10.0.0.10          TCP        60 https > 49316 [ACK] Seq=84149 Ack=
  186 6.228279000  74.125.236.207         10.0.0.10          TCP        60 https > 49316 [ACK] Seq=84149 Ack=
  187 6.634059000  fe80::2137:492:bb83    ff02::1:3          LLMNR      86 Standard query 0x33c6  A isatap
  188 6.634185000  10.0.0.5               224.0.0.252        LLMNR      66 Standard query 0x33c6  A isatap
  189 6.798763000  10.0.0.10              10.0.0.255         NBNS       92 Name query NB WPAD<00>
  190 6.799008000  fe80::75da:da80:e84    ff02::1:3          LLMNR      84 Standard query 0x127e  A wpad
  191 6.799128000  10.0.0.10              224.0.0.252        LLMNR      64 Standard query 0x127e  A wpad
  192 6.977714000  10.0.0.5               10.0.0.255         NBNS       92 Name query NB ISATAP<00>
  193 7.210335000  fe80::75da:da80:e8d    ff02::1:3          LLMNR      84 Standard query 0x127e  A wpad
  194 7.210450000  10.0.0.10              224.0.0.252        LLMNR      64 Standard query 0x127e  A wpad
  195 7.551420000  10.0.0.10              10.0.0.255         NBNS       92 Name query NB WPAD<00>
  196 7.743330000  10.0.0.5               10.0.0.255         NBNS       92 Name query NB ISATAP<00>
  197 8.302690000  10.0.0.10              10.0.0.255         NBNS       92 Name query NB WPAD<00>
  198 9.000292000  10.0.0.10              74.125.200.95      TCP        54 49302 > https [FIN, ACK] Seq=1 Ack
  199 9.000345000  10.0.0.10              74.125.200.95      TCP        54 49302 > https [RST, ACK] Seq=2 Ack
  200 9.005634000  10.0.0.10              74.125.200.95      TCP        54 49303 > https [FIN, ACK] Seq=1 Ack
  201 9.005658000  10.0.0.10              74.125.200.95      TCP        54 49303 > https [RST, ACK] Seq=2 Ack
```

rpcap://[10.0.0.10]:2002/\Device\NPF_{19FD0...
Packets: 6017 · Displayed: 6017 (10...
Profile: Default

FIGURE 1.38: Wireshark Window with Packets Captured

63. Stop the running live capture after a while by clicking the stop button in the menu bar.


Capturing from rpcap://[10.0.0.10]:2002/\Device\NPF_{19FD0C46-9A09-45B5-AF6B-D0137D872CC0} [Wireshark...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source                Destination     Protocol Length Info
 173 6.192230000 74.125.236.207        10.0.0.10       TLSv1.2  1484 Application Data
 174 6.192895000 74.125.236.207        10.0.0.10       TLSv1.2  1484 Application Data
 175 6.192897000 74.125.236.207        10.0.0.10       TLSv1.2  1484 Application Data
 176 6.192913000 10.0.0.10             74.125.236.207  TCP        54 49326 > https [ACK] Seq=809 Ack=82
 177 6.193816000 74.125.236.207        10.0.0.10       TLSv1.2  1484 Application Data
 178 6.193817000 74.125.236.207        10.0.0.10       TLSv1.2   580 Application Data
 179 6.193840000 10.0.0.10             74.125.236.207  TCP        54 49326 > https [ACK] Seq=809 Ack=84
 180 6.197153000 10.0.0.10             74.125.236.207  TLSv1.2    85 Application Data
 181 6.212595000 10.0.0.5              10.0.0.255      NBNS       92 Name query NB ISATAP<00>
 182 6.212564000 fe80::2137:492:bb83   ff02::1:3       LLMNR      86 Standard query 0x33c6  A isatap
 183 6.212597000 10.0.0.5              224.0.0.252     LLMNR      66 Standard query 0x33c6  A isatap
 184 6.214014000 74.125.236.207        10.0.0.10       TCP        60 https > 49326 [ACK] Seq=84149 Ack=
 185 6.227483000 74.125.236.207        10.0.0.10       TCP        60 https > 49326 [ACK] Seq=84149 Ack=
 186 6.228279000 74.125.236.207        10.0.0.10       TCP        60 https > 49326 [ACK] Seq=84149 Ack=
 187 6.634059000 fe80::2137:492:bb83   ff02::1:3       LLMNR      86 Standard query 0x33c6  A isatap
 188 6.634185000 10.0.0.5              224.0.0.252     LLMNR      66 Standard query 0x33c6  A isatap
 189 6.798763000 10.0.0.10             10.0.0.255      NBNS       92 Name query NB WPAD<00>
 190 6.799008000 fe80::75da:da60:e64   ff02::1:3       LLMNR      84 Standard query 0x127e  A wpad
 191 6.799128000 10.0.0.10             224.0.0.252     LLMNR      64 Standard query 0x127e  A wpad
 192 6.977714000 10.0.0.5              10.0.0.255      NBNS       92 Name query NB ISATAP<00>
 193 7.216335000 fe80::75da:da60:e64   ff02::1:3       LLMNR      84 Standard query 0x127e  A wpad
 194 7.218450000 10.0.0.10             224.0.0.252     LLMNR      64 Standard query 0x127e  A wpad
 195 7.551420000 10.0.0.10             10.0.0.255      NBNS       92 Name query NB WPAD<00>
 196 7.743330000 10.0.0.5              10.0.0.255      NBNS       92 Name query NB ISATAP<00>
 197 8.302689000 10.0.0.10             10.0.0.255      NBNS       92 Name query NB WPAD<00>
 198 9.009292000 10.0.0.10             74.125.200.95   TCP        54 49302 > https [FIN, ACK] Seq=2 Ack
 199 9.009345000 10.0.0.10             74.125.200.95   TCP        54 49302 > https [RST, ACK] Seq=2 Ack
 200 9.009834000 10.0.0.10             74.125.200.95   TCP        54 49303 > https [FIN, ACK] Seq=2 Ack
 201 9.009849000 10.0.0.10             74.125.200.95   TCP        54 49303 > https [RST, ACK] Seq=2 Ack
```

```
rpcap://[10.0.0.10]:2002/\Device\NPF_{19FD0...   Packets: 6122 · Displayed: 6122 (10...   Profile: Default
```

FIGURE 1.39: Stopping the running live capture

64. In this way, you can capture traffic on a remote interface using Wireshark.

65. In real time, when attackers gain the credentials of a victim machine, they attempt to capture its remote interface and monitor the traffic its user browses, to reveal confidential user information.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and "exposure" through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

2

Analyzing a Network Using Capsa Network Analyzer

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Capsa is a portable network analyzer application for both LANs and WLANs which performs real-time packet capturing capability, 24/7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It goes one step ahead of sniffing by intuitively analyzing network packets and generating meaningful information. Network administrators can use Capsa's comprehensive high-level window view for monitoring entire network, quick insight to network administrators or network engineers that allows rapidly pinpointing and resolving application problems.

Lab Objectives

The objective of this lab is to obtain information regarding the target organization that includes, but is not limited to:

- Network traffic analysis, communication monitoring
- Network communication monitoring
- Network problem diagnosis
- Network security analysis
- Network performance detecting
- Network protocol analysis

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

ColasoftCapsa Network Analyzer runs on Server 2003 /Server 2008/7 with 64-bit Edition.

Lab Environment

To complete this lab, you will need:

- ColasoftCapsa Network Analyzer located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Capsa Network Analyzer**
- You can also download the latest version of ColasoftCapsa Network Analyzer from the link http://www.colasoft.com
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Administrative privileges to run tools
- A web browser with an Internet connection

Note: This lab requires active internet connection for license-key registration

Lab Duration

Time: 5 Minutes

Overview of Sniffing

Sniffing is performed to collect basic information of the target and its network. It helps to find vulnerabilities and select exploits for attack. It determines network information, system information, password information, and organizational information.

Sniffing can be Active or Passive.

Lab Tasks

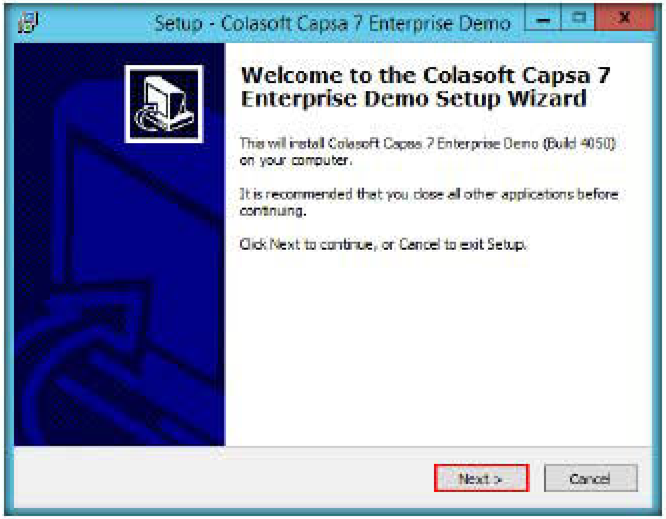
TASK 1

Install Capsa Network Analyzer

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Capsa Network Analyzer** and double-click **capsa_ent_demo_7.7.2.4050.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard-driven installation steps to install Capsa Network Analyzer.

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.



Setup - Colasoft Capsa 7 Enterprise Demo

Welcome to the Colasoft Capsa 7 Enterprise Demo Setup Wizard

This will install Colasoft Capsa 7 Enterprise Demo (Build 4050) on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

FIGURE 2.1: Colasoft Capsa installation wizard

Note: If a **Windows Security** dialog-box opens during installation, click **Install.**

4. On completing the installation, launch **Colasoft Capsa 7 Enterprise Demo** from the **Apps** screen.

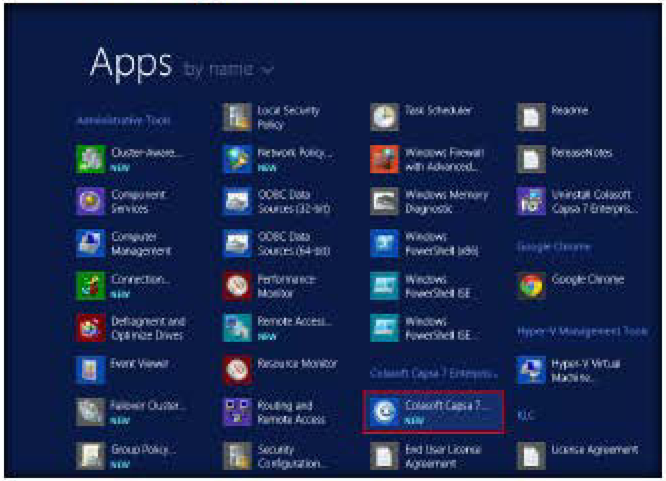
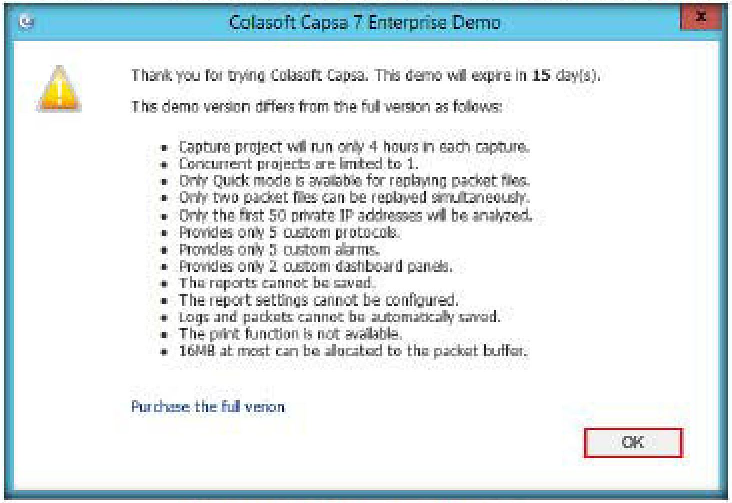


FIGURE 2.2: Launching the application from Apps screen

5. The **Colasoft Capsa 7 Enterprise Demo** dialog-box appears; click **OK**.



Colasoft Capsa 7 Enterprise Demo

Thank you for trying Colasoft Capsa. This demo will expire in **15** day(s).

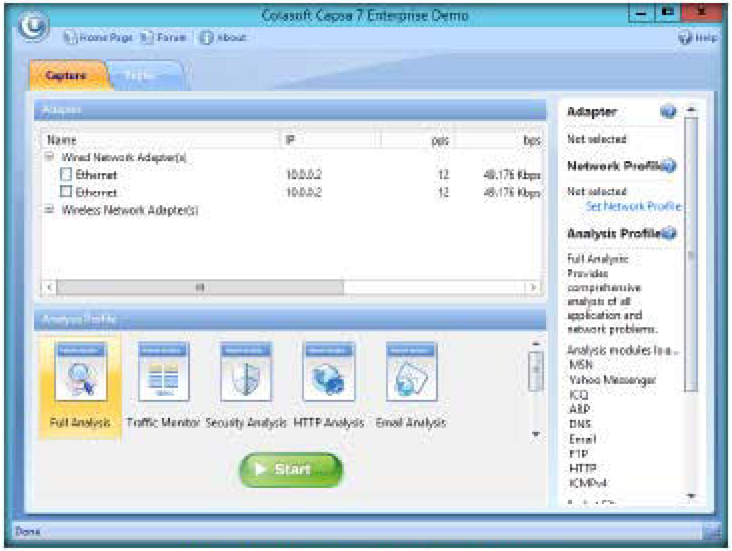
This demo version differs from the full version as follows:

- Capture project will run only 4 hours in each capture.
- Concurrent projects are limited to 1.
- Only Quick mode is available for replaying packet files.
- Only two packet files can be replayed simultaneously.
- Only the first 50 private IP addresses will be analyzed.
- Provides only 5 custom protocols.
- Provides only 5 custom alarms.
- Provides only 2 custom dashboard panels.
- The reports cannot be saved.
- The report settings cannot be configured.
- Logs and packets cannot be automatically saved.
- The print function is not available.
- 16MB at most can be allocated to the packet buffer.

Purchase the full verion

FIGURE 2.3: Colasoft Capsa 7 Enterprise Demo dialog-box

6. The **Colasoft Capsa 7 Enterprise Demo** main window appears, as shown in the following screenshot:



Name	IP	pps	bps
⊟ Wired Network Adapter(s)			
□ Ethernet	10.0.0.2	12	48.176 Kbps
□ Ethernet	10.0.0.2	12	48.176 Kbps
⊞ Wireless Network Adapter(s)			

Adapter

Not selected

Network Profile

Not selected

Set Network Profile

Analysis Profile

Full Analysis
Provides comprehensive analysis of all application and network problems.

Analysis modules in a...
MSN
Yahoo Messenger
ICQ
ARP
DNS
Email
FTP
HTTP
ICMPv4

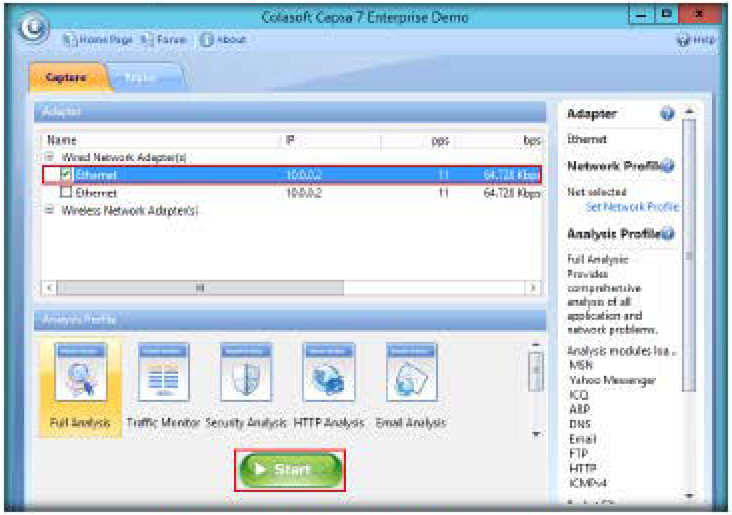
FIGURE 2.4: Colasoft Capsa Network Analyzer main window

As a network analyzer, Capsa make it easy to monitor and analyze network traffic with its intuitive and information-rich tab views.

TASK 2

Begin Packet Analysis

7. In the **Capture** tab, check **Ethernet** adapter and click **Start** to create a New Project.



Name	IP	pps	bps
⊟ Wired Network Adapter(s)			
☑ Ethernet	10.0.0.2	11	64.728 Kbps
□ Ethernet	10.0.0.2	11	64.728 Kbps
⊞ Wireless Network Adapter(s)			

FIGURE 2.5: Colasoft Capsa Network Analyzer creating a New Project

The network utilization rate is the ratio of current network traffic to the maximum traffic that a port can handle. It indicates the bandwidth use in the network.

Note: **10.0.0.2** is the IP address of the host machine, which may differ in your lab environment.

TASK 3

Analyze the Dashboard Information

8. The **Dashboard** provides graphs and charts of the statistics.

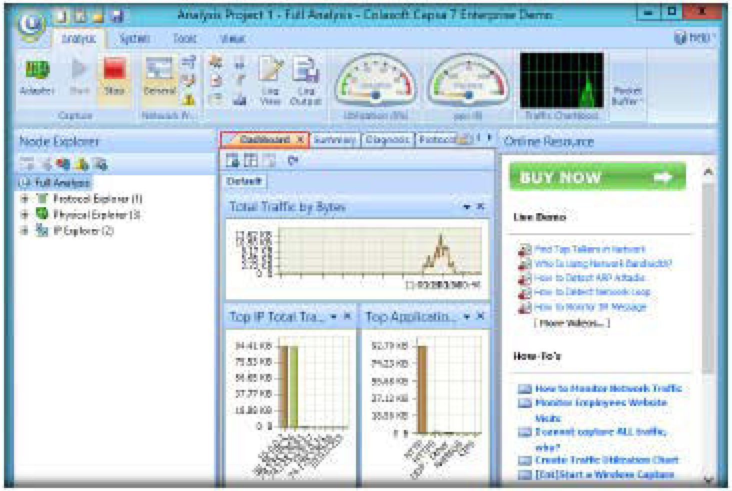
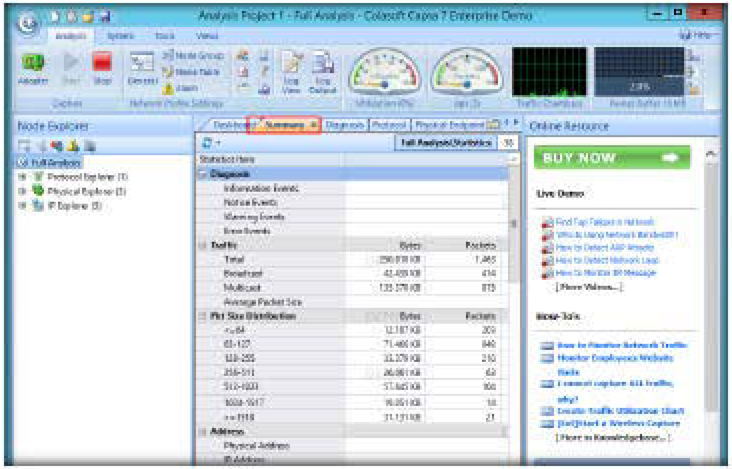


FIGURE 2.6: Colasoft Capsa Network Analyzer Dashboard

TASK 4

Examine the Summary Information

9. The **Summary** tab provides full general analysis and statistical information of the selected node in the Node Explorer window.



Statistics Item	Bytes	Packets
Diagnosis		
Information Events		
Notice Events		
Warning Events		
Error Events		
Traffic	Bytes	Packets
Total	290,878 KB	1,465
Broadcast	42,459 KB	414
Multicast	133,378 KB	875
Average Packet Size		
Pkt Size Distribution	Bytes	Packets
<=64	12,187 KB	209
65-127	71,460 KB	846
128-255	33,379 KB	210
256-511	26,081 KB	62
512-1023	57,845 KB	100
1024-1517	16,051 KB	18
>=1518	31,131 KB	21
Address		
Physical Address		
IP Address		

FIGURE 2.7: Colasoft Capsa Network Analyzer Summary

A high network utilization rate indicates the network is busy, whereas a low utilization rate indicates the network is idle.

TASK 5

Analyze the Diagnosis Information

10. The **Diagnosis** tab provides the real-time diagnosis events of global network by groups of protocol layers or security levels. With this tab you can view the performance of the protocols.

11. To view the TCP slow response, click **TCP Slow Response** in the **Transport Layer,** which in turn will highlight the slowest response in **Diagnosis Events.**

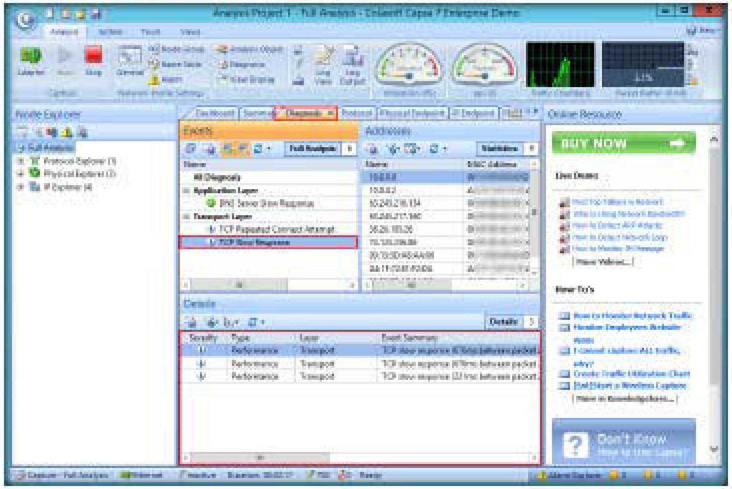
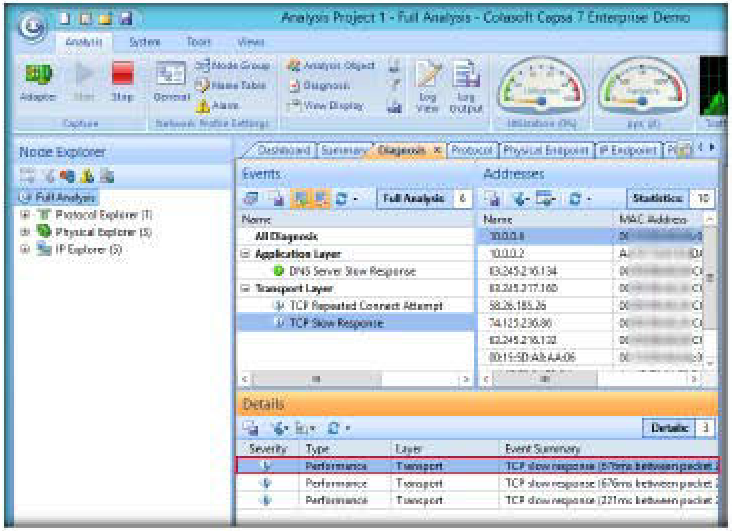


FIGURE 2.8: Colasoft Capsa Network Analyzer Diagnosis

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

12. Double-click the highlighted **Diagnosis Event** to view its detailed information.



Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Enterprise Demo

Events — Full Analysis 6

Name
All Diagnosis
Application Layer
DNS Server Slow Response
Transport Layer
TCP Repeated Connect Attempt
TCP Slow Response

Addresses — Statistics 10

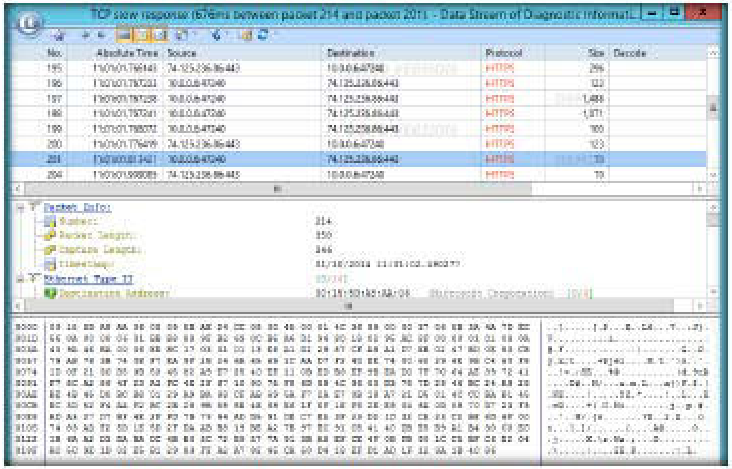
Name	MAC Address
10.0.0.8	[redacted]
10.0.0.2	[redacted]
63.245.216.134	[redacted]
63.245.217.160	[redacted]
58.26.185.26	[redacted]
74.125.236.80	[redacted]
63.245.216.132	[redacted]
00:15:5D:A8:AA:06	[redacted]

Details — Details 3

Severity	Type	Layer	Event Summary
	Performance	Transport	TCP slow response (676ms between packet
	Performance	Transport	TCP slow response (676ms between packet
	Performance	Transport	TCP slow response (221ms between packet

FIGURE 2.9: Analyzing Diagnosis Event

13. The **TCP Slow ACK - Data Stream of Diagnostic Information** window displays Absolute Time, Source, Destination, Packet Info, TCP, IP, and other information related to the event.



TCP slow response (676ms between packet 214 and packet 201) - Data Stream of Diagnostic Informat...

No.	Absolute Time	Source	Destination	Protocol	Size	Decode
195	11:01:01.796143	74.125.236.86:443	10.0.0.8:47240	HTTPS	296	
196	11:01:01.797233	10.0.0.8:47240	74.125.236.86:443	HTTPS	122	
197	11:01:01.797258	10.0.0.8:47240	74.125.236.86:443	HTTPS	1,488	
198	11:01:01.797261	10.0.0.8:47240	74.125.236.86:443	HTTPS	1,071	
199	11:01:01.798072	10.0.0.8:47240	74.125.236.86:443	HTTPS	100	
200	11:01:01.776499	74.125.236.86:443	10.0.0.8:47240	HTTPS	123	
201	11:01:00.813421	10.0.0.8:47240	74.125.236.86:443	HTTPS	70	
204	11:01:01.998089	74.125.236.86:443	10.0.0.8:47240	HTTPS	70	

```
Packet Info:
    Number:                          214
    Packet Length:                   350
    Capture Length:                  346
    Timestamp:                       01/18/2014 11:01:02.180277
Ethernet Type II                     [0/14]
    Destination Address:             00:15:5D:A8:AA:06    [Microsoft Corporation]  [0/6]
```

FIGURE 2.10: TCP Slow ACK - Data Stream of Diagnostic Information window

14. Close the **TCP Slow ACK - Data Stream of Diagnostic Information** window after analyzing the results.

TASK 6

Examine the Protocol Information

15. The **Protocol** tab lists statistics of all protocols used in network the transactions hierarchically. **Physical Endpoints** and **IP Endpoints** for the selected ports are displayed as well.

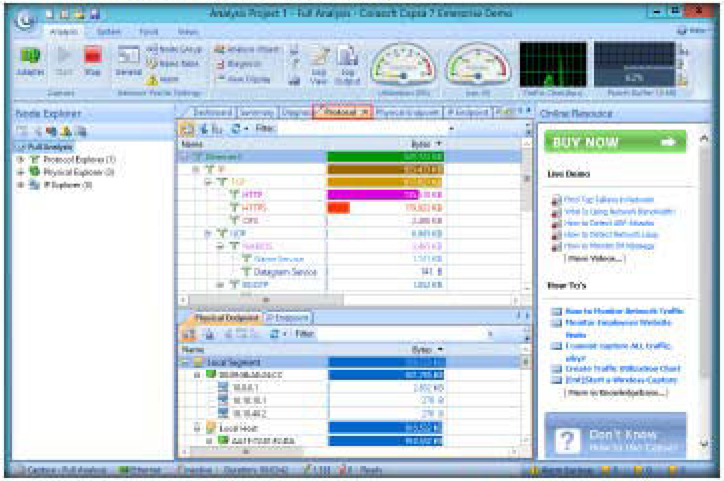

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Enterprise Demo
Node Explorer
Protocol
Physical Endpoint
IP Endpoint
Online Resource
BUY NOW
Live Demo
How To's
Don't Know How to Use Capsa?

FIGURE 2.11: Colasoft Capsa Network Analyzer Protocol analysis

TASK 7

Examine the Physical Endpoint Information

16. The **Physical Endpoint** tab lists statistics of all MAC addresses that communicate in the network hierarchically.

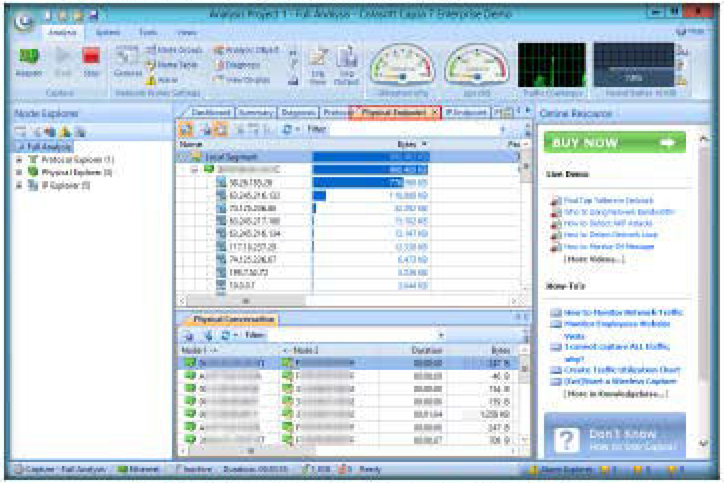

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Enterprise Demo
Node Explorer
Physical Endpoint
Physical Conversation
Online Resource
BUY NOW
Live Demo
How To's
Don't Know How to Use Capsa?

FIGURE 2.12: Colasoft Capsa Network Analyzer Physical Endpoint analysis

TASK 8

Analyze the IP Endpoint Information

17. The **IP Endpoint** tab displays statistics of all IP addresses communicating in the Network.

18. On the **IP Endpoint** tab, you can easily find the nodes with the highest **traffic volumes**, and check if there is a **multicast storm** or **broadcast storm** in your network.

As a delicate work, network analysis always requires us to view the original packets and analyze them. However, not all the network failures can be found in a very short period. Sometimes network analysis requires a long period of monitoring and must be based on the baseline of the normal network.

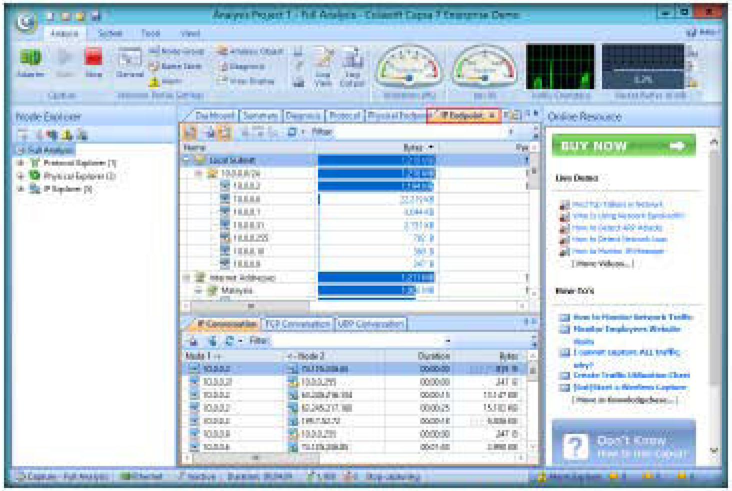


FIGURE 2.13: Colasoft Capsa Network Analyzer IP Endpoint view

TASK 9

Examine the Physical Conversations

19. The **Physical Conversation** tab presents the conversations between two MAC addresses.

TTL tells the router whether the packet should be dropped if it stays in the network for too long. TTL is initially designed to define a time scope beyond which the packet is dropped. As TTL value is deducted by at least 1 by the router when the packet passes through, TTL often indicates the number of the routers which the packet passed through before it was dropped.

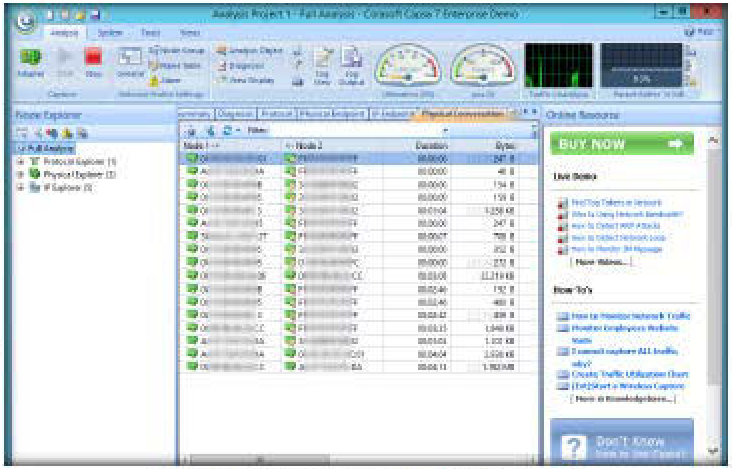


FIGURE 2.14: Colasoft Capsa Network Analyzer Physical Conversations

TASK 10

Examine the IP Conversations

20. The **IP Conversation** tab presents IP conversations between pairs of nodes.

21. The lower pane of the IP Conversation section offers **UDP** and **TCP** conversation, which you can drill down to analyze.

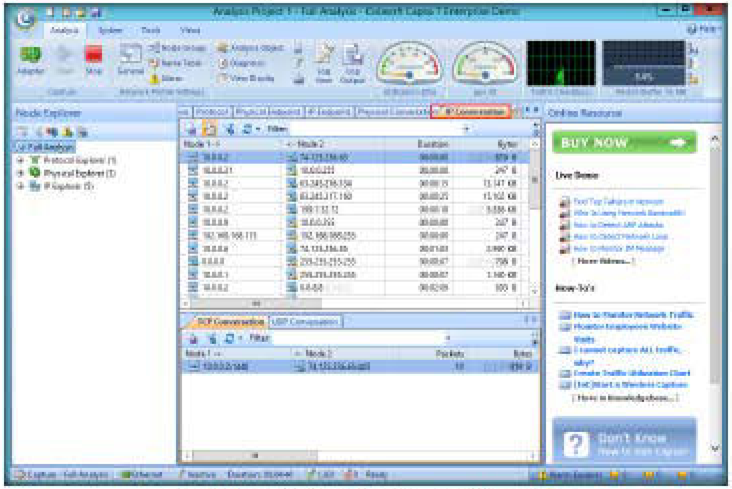


FIGURE 2.15: Colasoft Capsa Network Analyzer IP Conversations

22. Double-click a conversation in the **IP Conversation** list to view the full analysis of packets between two IPs. Here, we are checking the conversation between **10.0.0.9** and **10.0.0.255**.

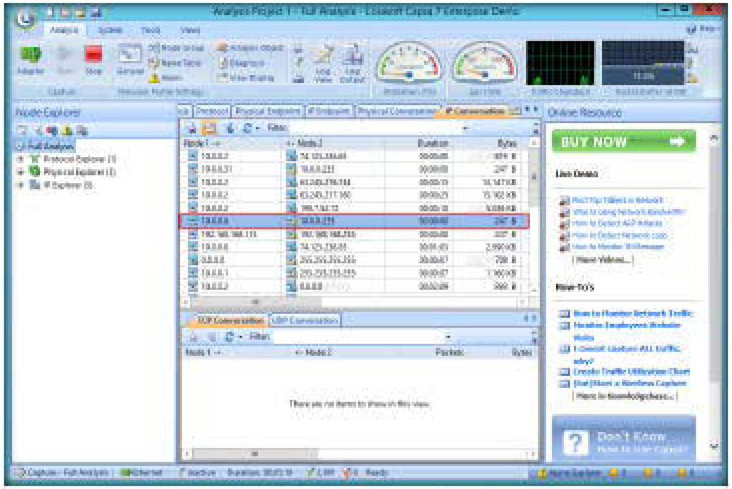
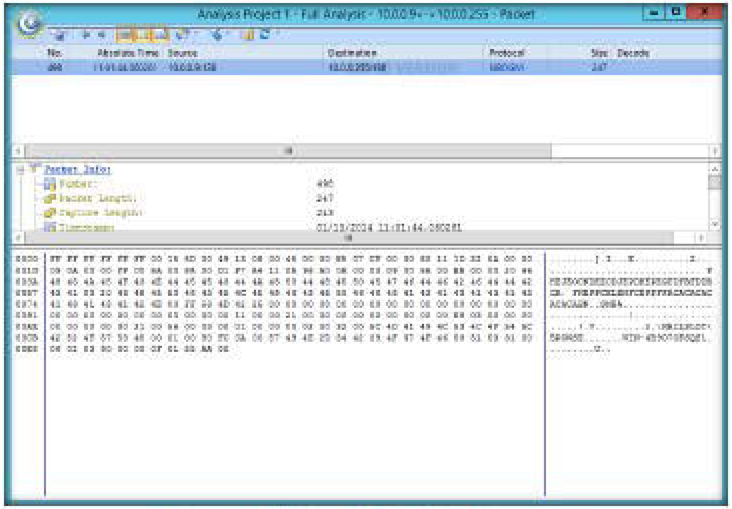


FIGURE 2.16: Colasoft Capsa Network Analyzer IP Conversations

23. A window displays full packet analysis between **10.0.0.9** and **10.0.0.255**.



Analysis Project 1 - Full Analysis - 10.0.0.9<->10.0.0.255 - Packet

Packet Info:
Number: 496
Packet Length: 247
Capture Length: 213
Timestamp: 01/13/2014 11:01:44.280281

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on. While attempting to remain undetected, the backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

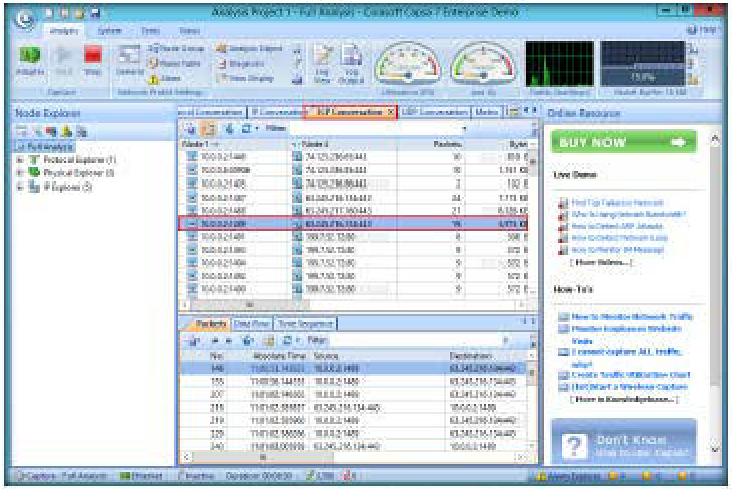
FIGURE 2.17: Full Packet Analysis of Nodes in IP Conversations

TASK 11

Examine the TCP Conversations

24. The **TCP Conversation** tab dynamically presents the real-time status of TCP conversations between pairs of nodes.

25. Double-click a node to display the full analysis of packets.



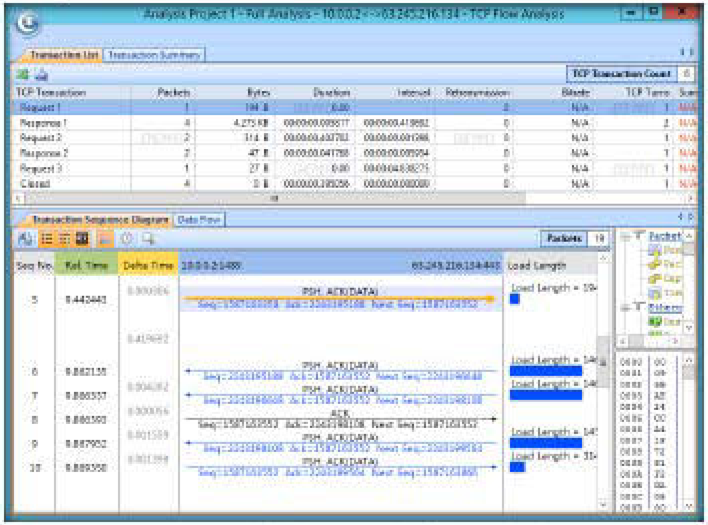
Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Enterprise Demo

FIGURE 2.18: Colasoft Capsa Network Analyzer TCP Conversations

TASK 12

Examine the Transaction List

26. **Transaction List** displays the TCP transactions between the selected pair of nodes.



Analysis Project 1 - Full Analysis - 10.0.0.2<-->63.245.216.134 - TCP Flow Analysis

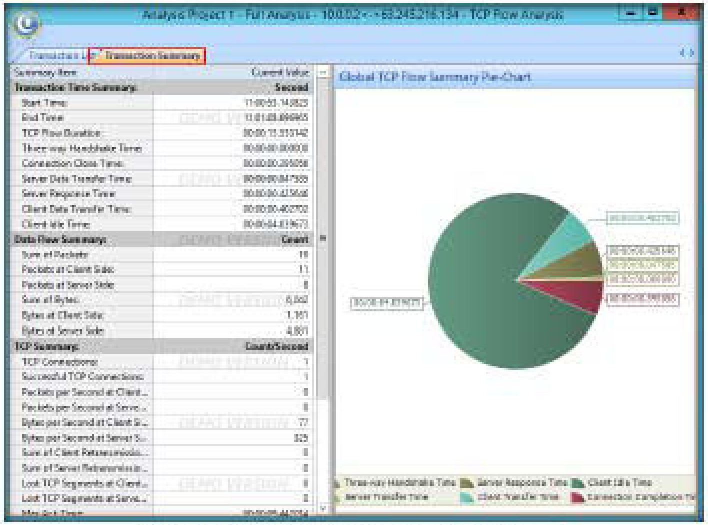
TCP Transaction	Packets	Bytes	Duration	Interval	Retransmission	Bitrate	TCP Turns	Sum
Request 1	1	194 B	0.00		0	N/A	1	N/A
Response 1	4	4.275 KB	00:00:00.095877	00:00:00.419882	0	N/A	2	N/A
Request 2	2	314 B	00:00:00.402702	00:00:00.001266	0	N/A	1	N/A
Response 2	2	47 B	00:00:00.041788	00:00:00.005954	0	N/A	1	N/A
Request 3	1	27 B	0.00	00:00:04.838275	0	N/A	1	N/A
Closed	4	0 B	00:00:00.285056	00:00:00.000000	0	N/A	1	N/A

FIGURE 2.19: Colasoft Capsa Network Analyzer Transaction List

TASK 13

Analyze the Transaction Summary

27. The **Transaction Summary** tab displays the summary of the transactions.



Analysis Project 1 - Full Analysis - 10.0.0.2<-->63.245.216.134 - TCP Flow Analysis

Summary Item	Current Value
Transaction Time Summary:	**Second**
Start Time:	11:00:53.145823
End Time:	11:01:05.499965
TCP Flow Duration:	00:00:11.310142
Three-way Handshake Time:	00:00:00.000000
Connection Close Time:	00:00:00.285058
Server Data Transfer Time:	00:00:00.847588
Server Response Time:	00:00:00.425648
Client Data Transfer Time:	00:00:00.402702
Client Idle Time:	00:00:04.839673
Data Flow Summary:	**Count**
Sum of Packets:	19
Packets at Client Side:	11
Packets at Server Side:	8
Sum of Bytes:	6,042
Bytes at Client Side:	1,161
Bytes at Server Side:	4,881
TCP Summary:	**Count/Second**
TCP Connections:	1
Successful TCP Connections:	1
Packets per Second at Client...	0
Packets per Second at Serve...	0
Bytes per Second at Client Si...	77
Bytes per Second at Server S...	325
Sum of Client Retransmissio...	0
Sum of Server Retransmissio...	0
Lost TCP Segments at Client...	0
Lost TCP Segments at Serve...	0
Max Ack Time:	00:00:05.442054

FIGURE 2.20: Colasoft Capsa Network Analyzer Transaction Summary

TASK 14

Examine the UDP Conversation

28. The **UDP Conversation** tab dynamically presents the real-time status of UDP conversations between two nodes.

29. The lower pane of this tab gives you related packets and reconstructed data flow to help you drill down to **analyze the conversations**.

In networking, an email worm is a computer worm that can copy itself to the shared folder in a system and keeps sending infected emails to stochastic email addresses. In this way, it spreads fast via SMTP mail servers.

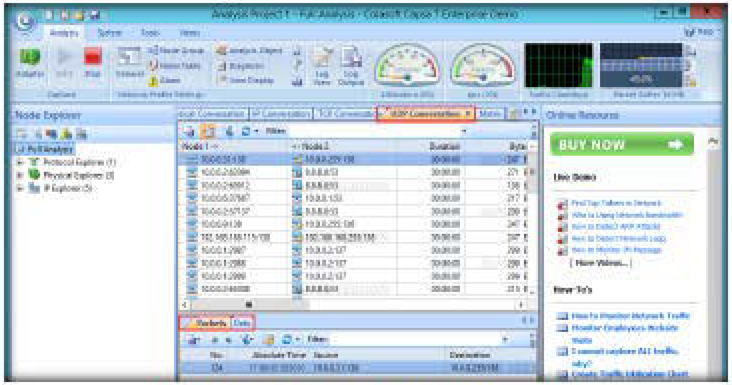


FIGURE 2.21: Colasoft Capsa Network Analyzer UDP Conversations

TASK 15

Examine the Matrix View

30. In the **Matrix** tab, you can view the nodes communicating in the network by graphically connecting them with lines.

31. The weight of each line indicates the volume of traffic between **nodes** arranged in an extensive **ellipse**.

32. You can easily navigate and shift between global statistics and details of specific network nodes by switching the corresponding nodes in the **Node Explorer** window.

Once we encounter the network malfunction or attack, the most important thing we should pay attention to is the current total network traffic, sent/received traffic, network connection, etc., to get a clear direction to find the problem. All of these statistics are included in the endpoint tabs in ColasoftCapsa.

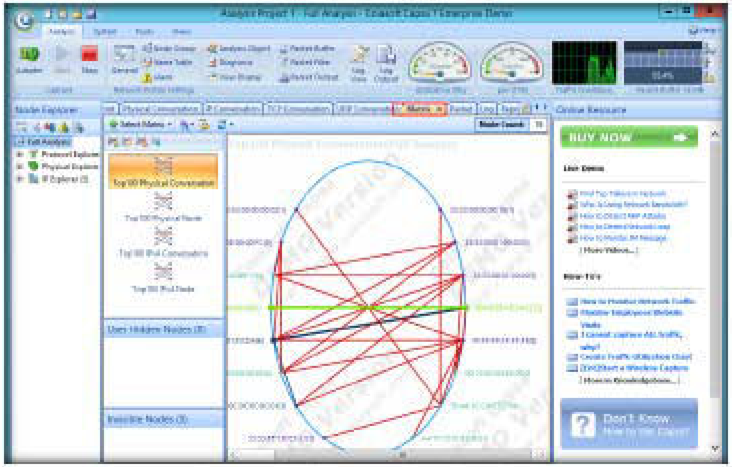


FIGURE 2.22: Colasoft Capsa Network Analyzer Matrix view

TASK 16

Analyze the Packet Details

33. The **Packet** tab provides original information for any packet. Double-click a packet to view its full analysis information of packet decode.

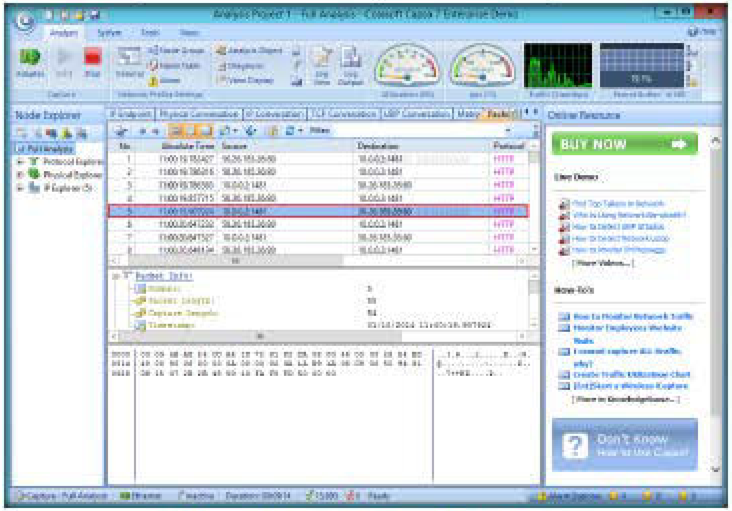


FIGURE 2.23: Colasoft Capsa Network Analyzer Packet information

Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection. A protocol is a formal description of message formats and the rules for exchanging those messages.

34. The packet decode consists of two major views: **Hex View** and **Decode View**.

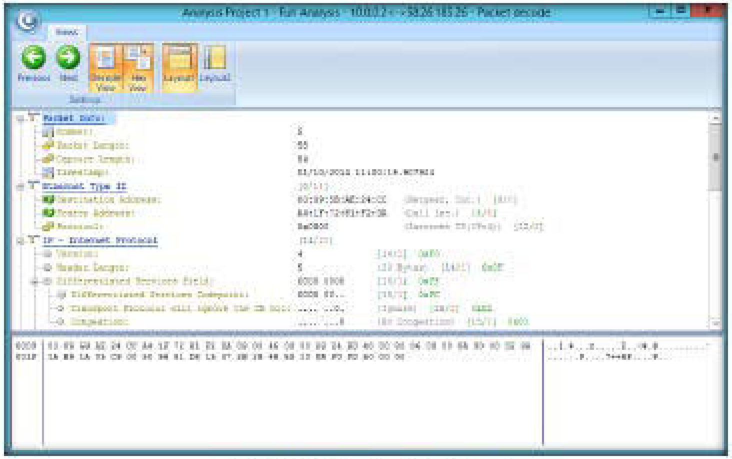


FIGURE 2.24: Full Analysis of Packet Decode

Protocol decoding is the basic functionality as well. There is a Packet tab, which collect all captured packets or traffic. Select a packet and we can see its hex digits as well as the meaning of each field. The figure below shows the structure of an ARP packet. This makes it easy to understand how the packet is encapsulated according to its protocol rule.

TASK 17

Analyze all the Logs

35. The **Log** tab provides a **Global Log**, **DNS Log**, **Email Log**, **FTP Log**, **HTTP Log**, **ICQ Log**, **MSN Log,** and **Yahoo Log.**

36. So, you can view the logs of **TCP conversations**, **Web access**, **DNS transactions**, **Email communications**, and others.

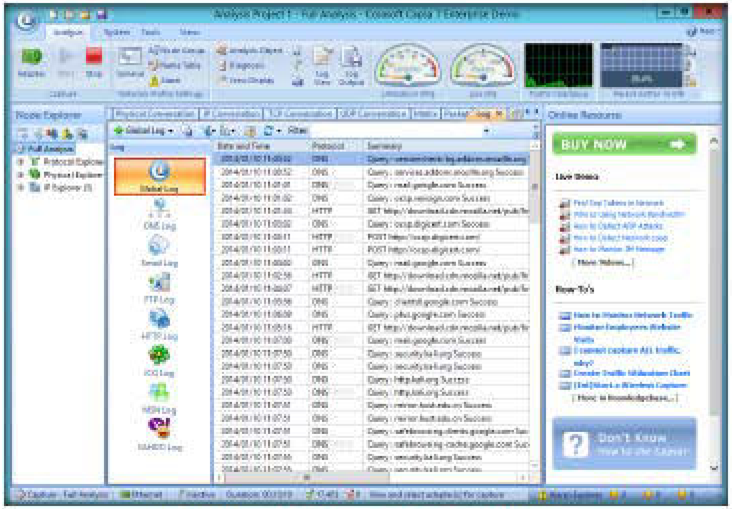


FIGURE 2.25: Colasoft Capsa Network Analyzer Global Log view

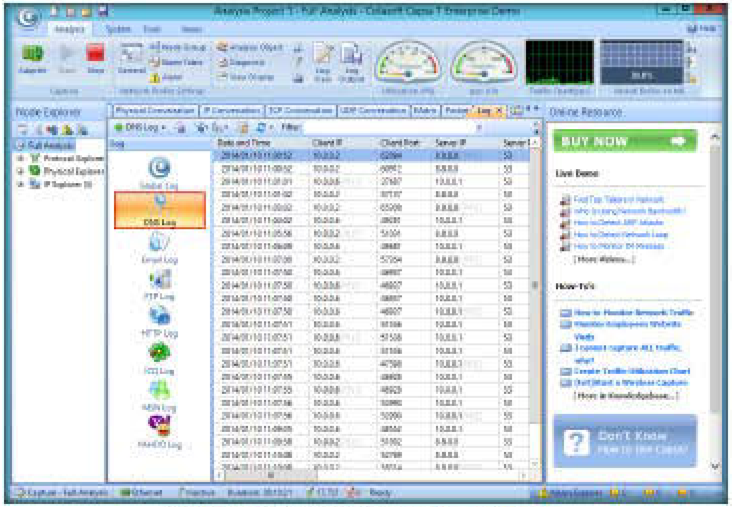


FIGURE 2.26: Colasoft Capsa Network Analyzer DNS Log view

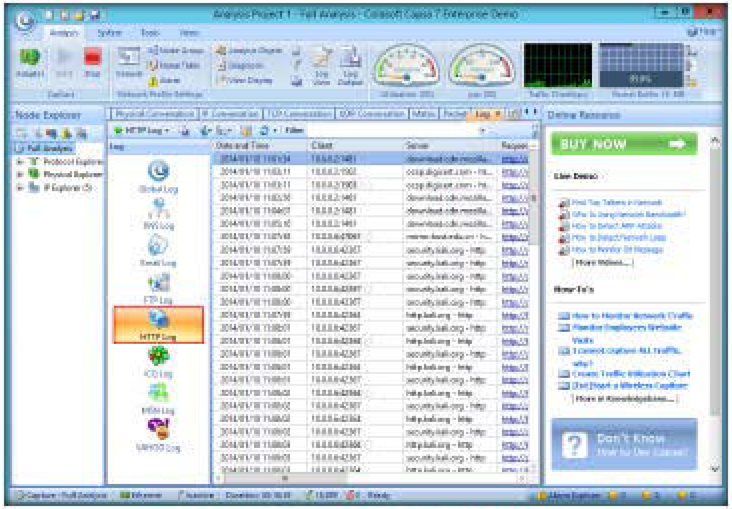
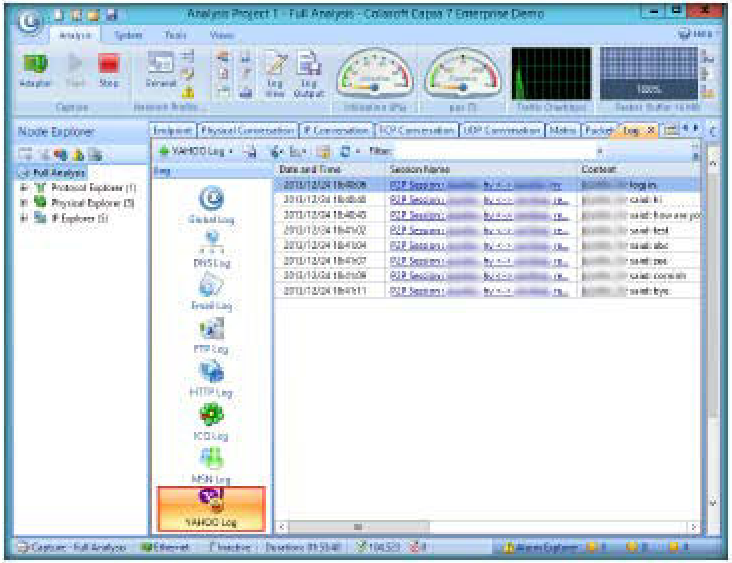


FIGURE 2.27: Colasoft Capsa Network Analyzer HTTP Log view

37. If you have MSN or Yahoo messenger running on your system, you can view the MSN and Yahoo logs.



Date and Time	Session Name	Content
2013/12/24 18:40:38	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] log in
2013/12/24 18:40:40	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] said: hi
2013/12/24 18:40:45	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] said: how are yo
2013/12/24 18:41:02	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] said: test
2013/12/24 18:41:04	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] said: abc
2013/12/24 18:41:07	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] said: pas
2013/12/24 18:41:09	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] said: connin
2013/12/24 18:41:11	P2P Session: [redacted] by <-> [redacted] (Y...	[redacted] said: bye

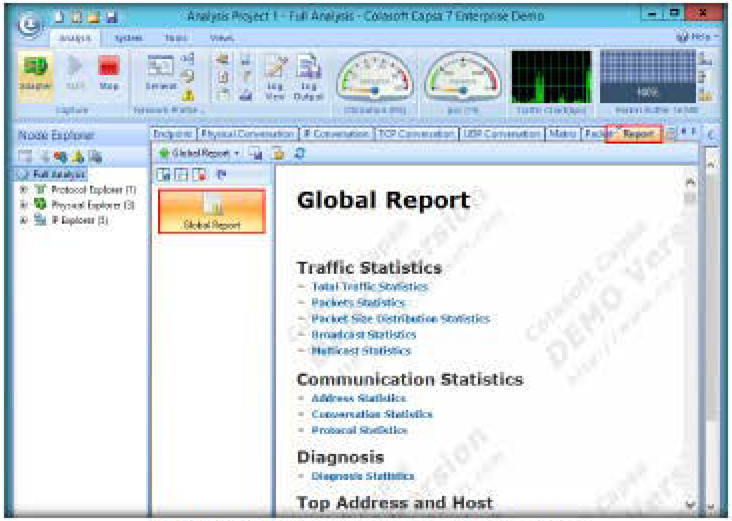
FIGURE 2.28: Colasoft Capsa Network Analyzer MSN Log view

TASK 18

Examine the Report

38. The **Report** tab provides **28** statistics reports from the global network to a specific network node.

39. You can click the respective hyperlinks for information, or you can scroll down to view a complete detailed report.



Global Report

Traffic Statistics
- Total Traffic Statistics
- Packets Statistics
- Packet Size Distribution Statistics
- Broadcast Statistics
- Multicast Statistics

Communication Statistics
- Address Statistics
- Conversation Statistics
- Protocol Statistics

Diagnosis
- Diagnosis Statistics

Top Address and Host

FIGURE 2.29: Colasoft Capsa Network Analyzer Full Analysis's Report

Almost all Trojans and worms need an access to the network, because they have to return data to the hacker. Only the useful data are sent for the Trojan to accomplish its mission. So it is a good solution to start from the aspect of traffic analysis and protocol analysis technology.

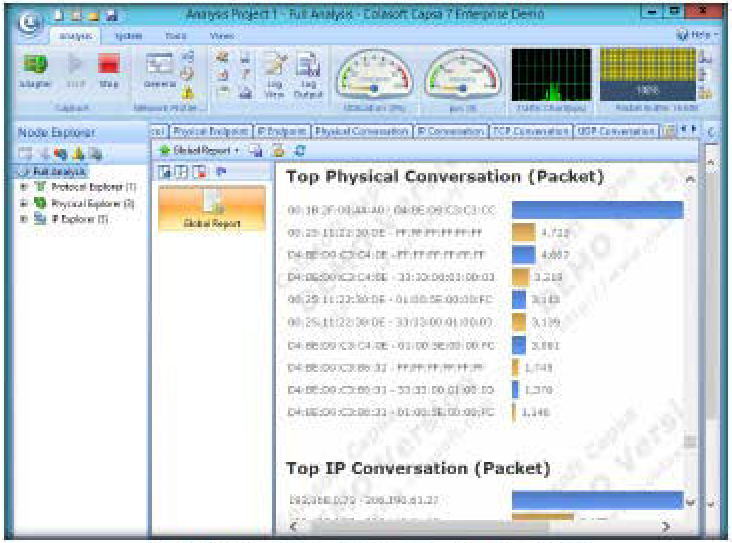

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Enterprise Demo
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (1)
Global Report
Top Physical Conversation (Packet)
00:18:2F:08:A4:A0 - 04:0E:09:C3:C3:CC
00:25:11:22:30:DE - FF:FF:FF:FF:FF:FF
4,722
04:0E:09:C3:C4:0E - FF:FF:FF:FF:FF:FF
4,667
04:0E:09:C3:C4:0E - 33:33:00:01:00:03
3,218
00:25:11:22:30:DE - 01:00:5E:00:00:FC
3,143
00:25:11:22:30:DE - 33:33:00:01:00:03
3,139
04:0E:09:C3:C4:0E - 01:00:5E:00:00:FC
3,081
04:0E:09:C3:00:32 - FF:FF:FF:FF:FF:FF
1,743
04:0E:09:C3:00:31 - 33:33:00:01:00:03
1,370
04:0E:09:C3:00:31 - 01:00:5E:00:00:FC
1,146
Top IP Conversation (Packet)
192.168.0.70 - 208.190.61.27

FIGURE 2.30: Colasoft Capsa Network Analyzer Full Analysis's Report

40. Click **Stop** after completing your task.

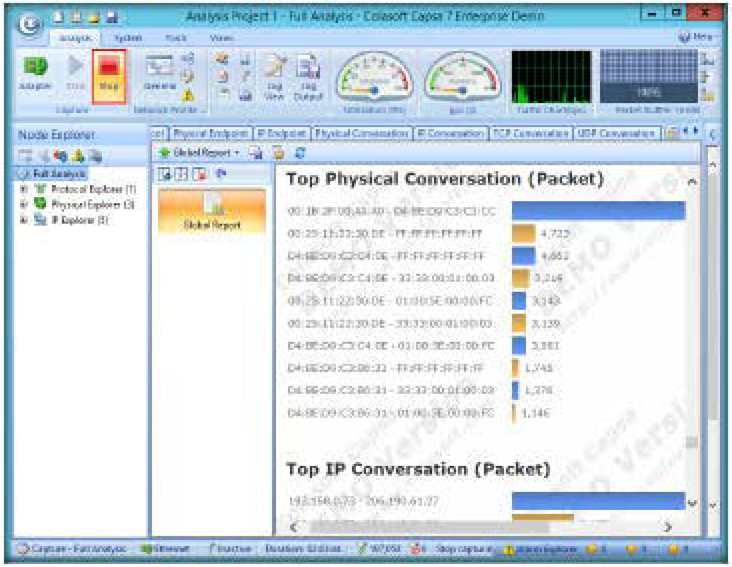

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Enterprise Demo
Stop
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (1)
Global Report
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Top Physical Conversation (Packet)
00:18:2F:00:A0:40 - D4:BE:D9:C3:C1:CC
00:25:11:22:30:DE - FF:FF:FF:FF:FF:FF 4,723
D4:BE:D9:C3:C4:0E - FF:FF:FF:FF:FF:FF 4,662
D4:BE:D9:C3:C4:0E - 33:33:00:01:00:03 3,216
00:25:11:22:30:DE - 01:00:5E:00:00:FC 3,143
00:25:11:22:30:DE - 33:33:00:01:00:03 3,129
D4:BE:D9:C3:C4:0E - 01:00:5E:00:00:FC 3,081
D4:BE:D9:C3:B0:32 - FF:FF:FF:FF:FF:FF 1,745
D4:BE:D9:C3:B0:31 - 33:33:00:01:00:03 1,276
D4:BE:D9:C3:B0:31 - 01:00:5E:00:00:FC 1,146
Top IP Conversation (Packet)
192.168.0.73 - 206.190.61.27
Stop capture

FIGURE 2.31: Colasoft Capsa Network Analyzer Stopping process

41. In real time, an attacker may perform this analysis in an attempt to obtain sensitive information, as well as to find any network loopholes.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

3

Sniffing the Network Using the OmniPeek Network Analyzer

OmniPeek is a standalone network analysis tool used to solve network problems.

ICON KEY
Valuable information
Test your knowledge
Web exercise
Workbook review

Lab Scenario

From the previous scenario, now you are aware of the importance of network sniffing. As an expert Ethical Hacker and Penetration Tester, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

In this lab, you will need:

- A web browser with internet access
- A business Email ID to download the tool
- A computer running Windows Server 2012 as host machine
- Windows 8.1 running on virtual machine as target machine
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of OmniPeek Network Analyzer

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, including

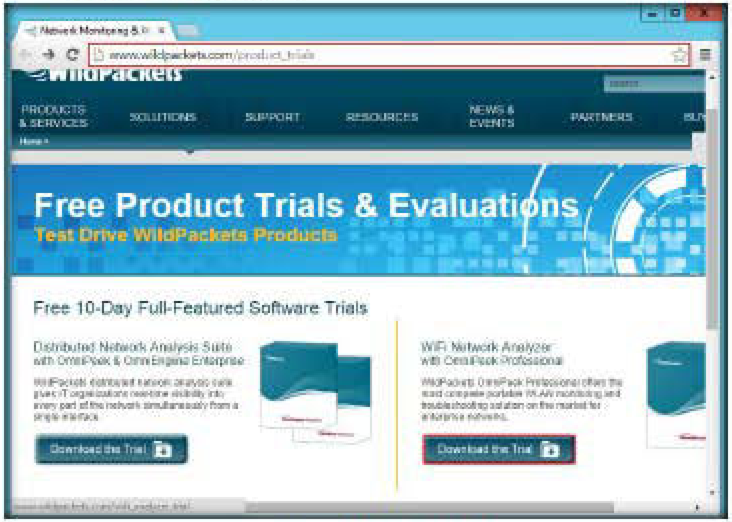
Ethernet, Gigabit, 10 Gigabit, VoIP, and Video to remote offices, and 802. 11 a/b/g/n.

Lab Tasks

TASK 1

Download and Install OmniPeek Network Analyzer

1. Launch a web browser, type http://www.wildpackets.com/product_trials in the address box, and press **Enter**.
2. OmniPeek products window appears; click the **download button** for **OmniPeek Professional.**


Network Monitoring & P
www.wildpackets.com/product_trials
WildPackets
PRODUCTS & SERVICES
SOLUTIONS
SUPPORT
RESOURCES
NEWS & EVENTS
PARTNERS
BUY
Home
Free Product Trials & Evaluations
Test Drive WildPackets Products
Free 10-Day Full-Featured Software Trials
Distributed Network Analysis Suite with OmniPeek & OmniEngine Enterprise
Download the Trial
WiFi Network Analyzer with OmniPeek Professional
Download the Trial

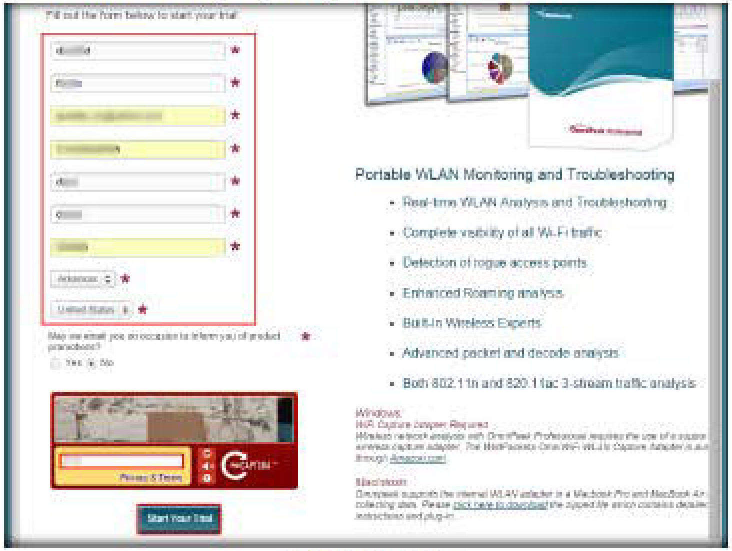
WildPackets' distributed network analysis suite gives IT organizations real-time visibility into every part of the network simultaneously from a single interface.

WildPackets' OmniPeek Professional offers the most complete portable WLAN monitoring and troubleshooting solution on the market for enterprise networks.

FIGURE 3.1: OmniPeek products window

3. Fill in the details in all the required fields, type the captcha in the field provided, and click **Start Your Trial**.

Note: You need to specify a non-personal business email ID.



Fill out the form below to start your trial

[redacted]

May we email you on occasion to inform you of product promotions? *
○ Yes ● No

Start Your Trial

Portable WLAN Monitoring and Troubleshooting

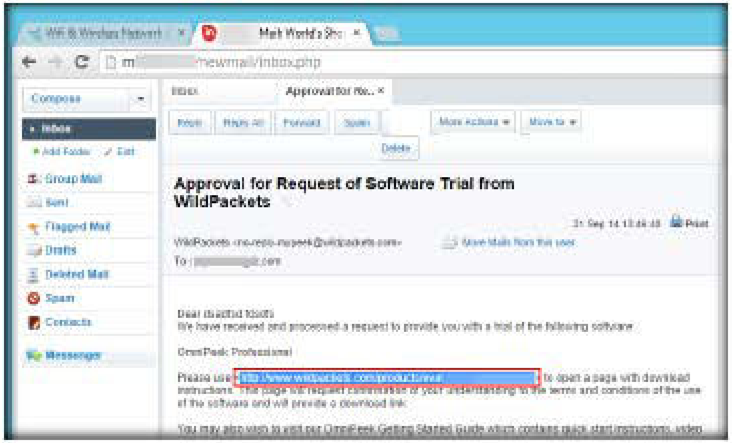
- Real-time WLAN Analysis and Troubleshooting
- Complete visibility of all Wi-Fi traffic
- Detection of rogue access points
- Enhanced Roaming analysis
- Built-In Wireless Experts
- Advanced packet and decode analysis
- Both 802.11n and 820.11ac 3-stream traffic analysis

Windows:
WiFi Capture Adapter Required
Wireless network analysis with OmniPeek Professional requires the use of a supported wireless capture adapter. The WildPackets OmniWiFi USB Capture Adapter is available through Amazon.com

Macintosh:
Omnipeek supports the internal WLAN adapter in a Macbook Pro and MacBook Air for collecting data. Please click here to download the zipped file which contains detailed instructions and plug-in.

FIGURE 3.2: Filling the details

4. Now, log into the account related to the email ID specified in the registration page, and copy the download link.



m[redacted]newmail/inbox.php

Approval for Request of Software Trial from WildPackets

31 Sep 14 13:46:48

WildPackets <no-reply-mypeek@wildpackets.com>
To : [redacted].com

Dear dsadfsd fdsdfs
We have received and processed a request to provide you with a trial of the following software:

OmniPeek Professional

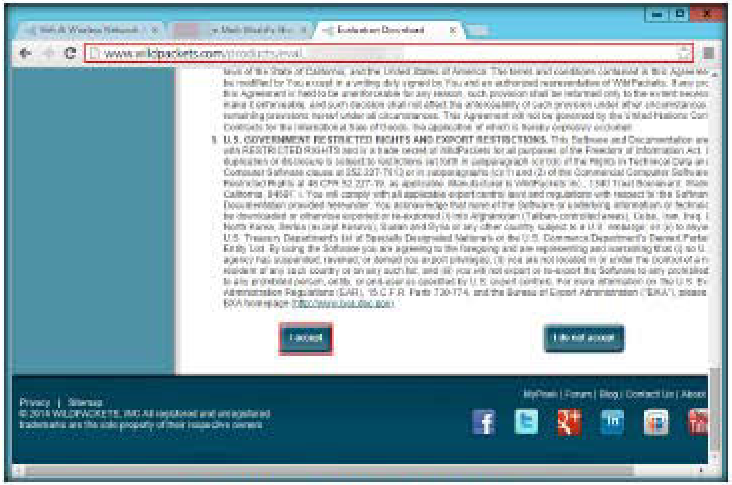
Please use http://www.wildpackets.com/product/eval to open a page with download instructions. The page will request confirmation of your understanding to the terms and conditions of the use of the software and will provide a download link.

You may also wish to visit our OmniPeek Getting Started Guide which contains quick start instructions, video

FIGURE 3.3: Email account containing the download link

5. Open a new tab, paste the download link that you copied in the previous step, and press **Enter**.

6. A webpage appears, displaying the terms and conditions. Scroll down and click **I accept**.



www.wildpackets.com/products/eval...

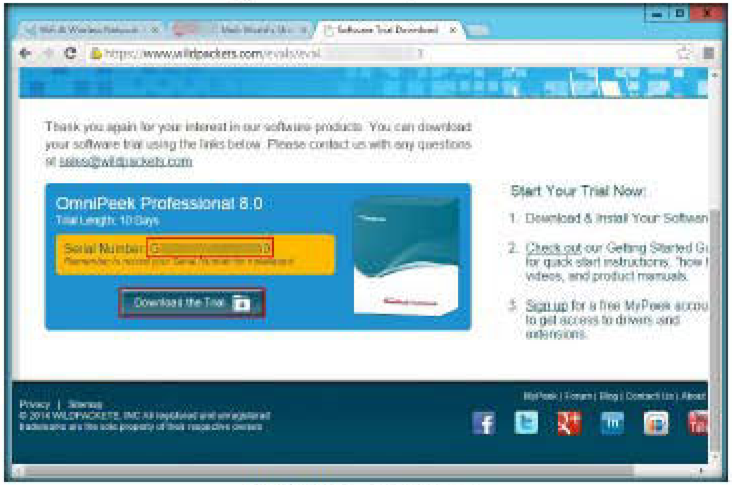
laws of the State of California, and the United States of America. The terms and conditions contained in this Agreem be modified by You except in a writing duly signed by You and an authorized representative of WildPackets. If any pro this Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necess make it enforceable, and such decision shall not affect the enforceability of such provision under other circumstances remaining provisions hereof under all circumstances. This Agreement will not be governed by the United Nations Con Contracts for the International Sale of Goods, the application of which is hereby expressly excluded.

9. U.S. GOVERNMENT RESTRICTED RIGHTS AND EXPORT RESTRICTIONS. This Software and Documentation are with RESTRICTED RIGHTS and is a trade secret of WildPackets for all purposes of the Freedom of Information Act. I duplication or disclosure is subject to restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data an Computer Software clause at 252.227-7013 or in subparagraphs (c)(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is WildPackets, Inc., 1340 Treat Boulevard, Walnu California, 94597. i. You will comply with all applicable export control laws and regulations with respect to the Softwar Documentation provided hereunder. You acknowledge that none of the Software or underlying information or technol be downloaded or otherwise exported or re-exported (i) into Afghanistan (Taliban-controlled areas), Cuba, Iran, Iraq, L North Korea, Serbia (except Kosovo), Sudan and Syria or any other country subject to a U.S. embargo; or (ii) to anyo U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Denied Partie Entity List. By using the Software you are agreeing to the foregoing and are representing and warranting that (i) no U. agency has suspended, revoked, or denied you export privileges; (ii) you are not located in or under the control of a n resident of any such country or on any such list; and (iii) you will not export or re-export the Software to any prohibited to any prohibited person, entity, or end-user as specified by U.S. export controls. For more information on the U.S. Ex Administration Regulations (EAR), 15 C.F.R. Parts 730-774, and the Bureau of Export Administration ("BXA"), please BXA homepage (http://www.bxa.doc.gov).

Evaluation Download
I accept
I do not accept
Privacy | Sitemap
© 2014 WILDPACKETS, INC All registered and unregistered trademarks are the sole property of their respective owners
MyPeek | Forum | Blog | Contact Us | About

FIGURE 3.4: Accepting the License Agreement information

7. The OmniPeek download page appears, containing the Serial number and download link. Copy the serial number, and click **Download the Trial**.



https://www.wildpackets.com/evals/eval...

Thank you again for your interest in our software products. You can download your software trial using the links below. Please contact us with any questions at sales@wildpackets.com

OmniPeek Professional 8.0
Trial Length: 10 Days

Serial Number: [redacted]
Remember to record your Serial Number for reference

Start Your Trial Now:

1. Download & Install Your Softwar
2. Check out our Getting Started G for quick start instructions, "how t videos, and product manuals.
3. Sign up for a free MyPeek accou to get access to drivers and extensions.

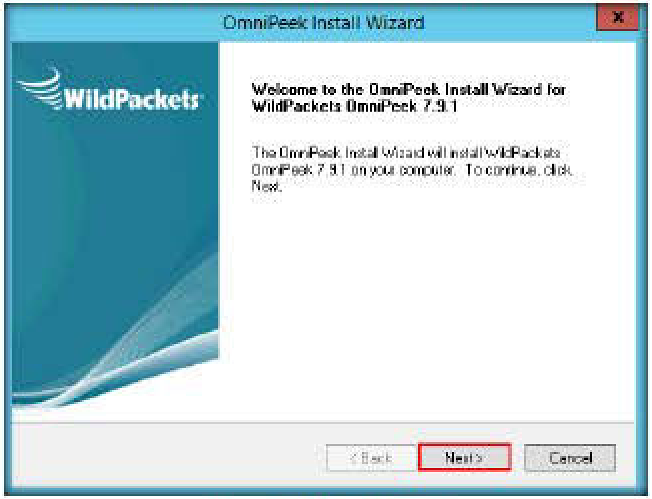
Software Trial Download
Download the Trial
Privacy | Sitemap
© 2014 WILDPACKETS, INC All registered and unregistered trademarks are the sole property of their respective owners
MyPeek | Forum | Blog | Contact Us | About

FIGURE 3.5: Downloading Omnipeek

8. On completion of download, navigate to the downloaded tool, and double-click it.

9. If the **Open File - Security Warning** pop-up appears, click **Run**.

10. The **OmniPeek Install Wizard** appears; click **Next**.



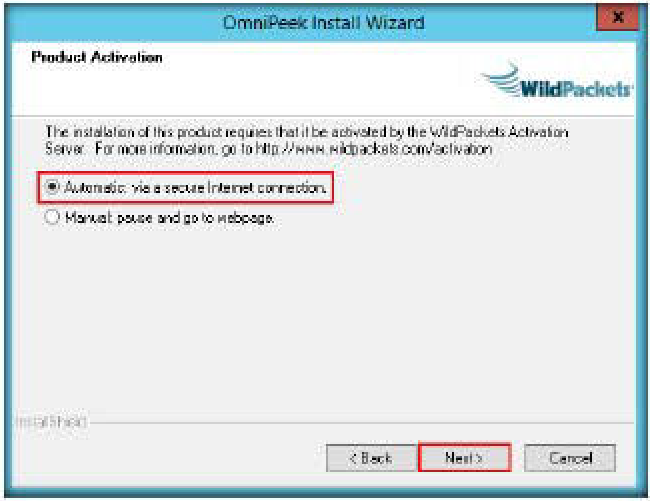
OmniPeek Install Wizard

Welcome to the OmniPeek Install Wizard for WildPackets OmniPeek 7.9.1

The OmniPeek Install Wizard will install WildPackets OmniPeek 7.9.1 on your computer. To continue, click Next.

FIGURE 3.6: OmniPeek Installation Wizard

11. The **Product Activation** step appears; select **Automatic: via a secure Internet connection,** and click **Next**.



OmniPeek Install Wizard

Product Activation

The installation of this product requires that it be activated by the WildPackets Activation Server. For more information, go to http://www.wildpackets.com/activation

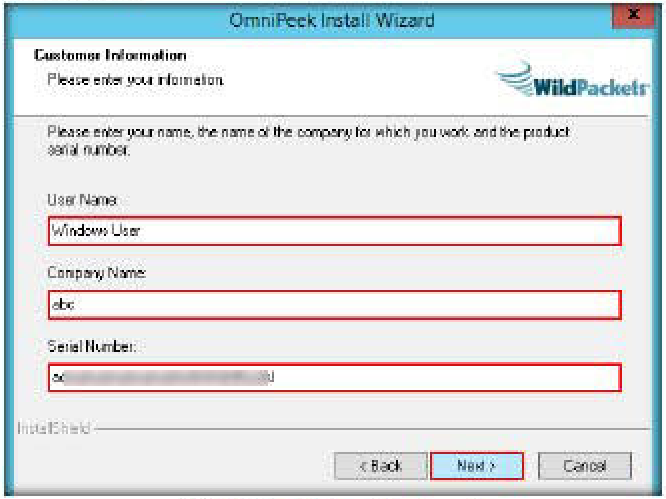
● Automatic: via a secure Internet connection.

○ Manual: pause and go to webpage.

FIGURE 3.7: OmniPeek Product Activation section

12. The **Customer Information** step appears; type a **User name**, **Company name**, and enter the **Serial Number** you noted in **step 7**.

13. Click **Next**.



OmniPeek Install Wizard

Customer Information

Please enter your information.

Please enter your name, the name of the company for which you work and the product serial number.

User Name: Windows User

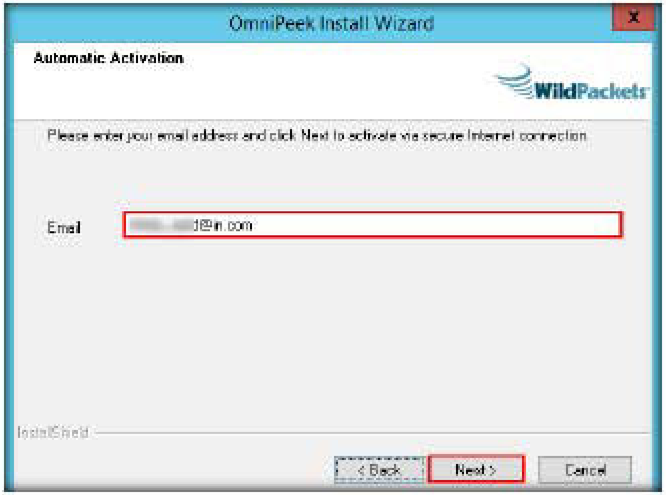
Company Name: abc

Serial Number: ad[redacted]d

FIGURE 3.8: OmniPeek Customer Information section

Note: Specify the serial key that you obtained during registration.

14. The **Automatic Activation** section appears; enter your email ID and click **Next**.



OmniPeek Install Wizard

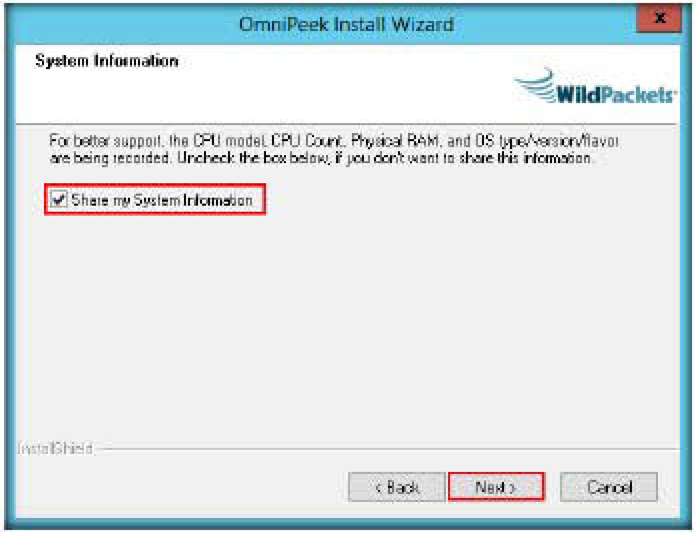
Automatic Activation

Please enter your email address and click Next to activate via secure Internet connection.

Email: [redacted]d@in.com

FIGURE 3.9: OmniPeek Automatic Activation section

15. The **System Information** section appears; check **Share my System Information,** and click **Next**.



OmniPeek Install Wizard

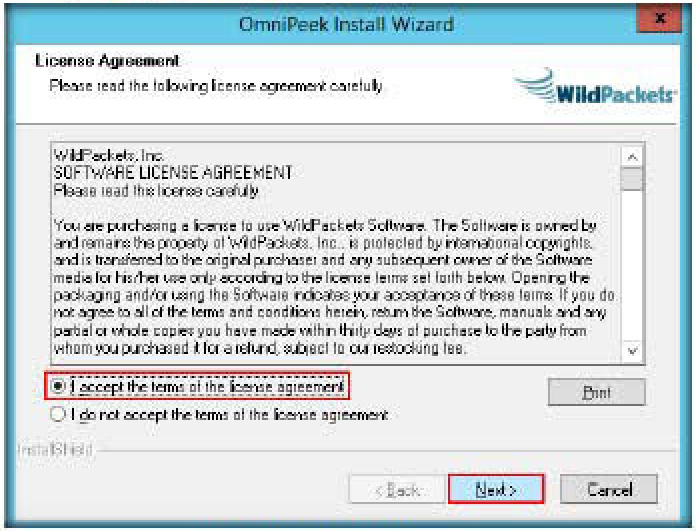
System Information

For better support, the CPU model, CPU Count, Physical RAM, and OS type/version/flavor are being recorded. Uncheck the box below, if you don't want to share this information.

☑ Share my System Information

FIGURE 3.10: OmniPeek System Information section

16. The **License Agreement** step appears; accept the terms of license agreement, and click **Next**.



OmniPeek Install Wizard

License Agreement

Please read the following license agreement carefully

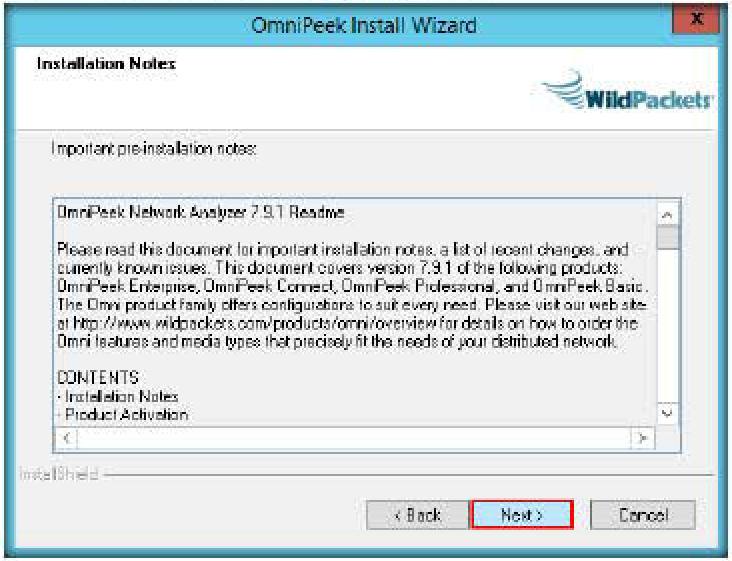
WildPackets, Inc.
SOFTWARE LICENSE AGREEMENT
Please read this license carefully

You are purchasing a license to use WildPackets Software. The Software is owned by and remains the property of WildPackets, Inc., is protected by international copyrights, and is transferred to the original purchaser and any subsequent owner of the Software media for his/her use only according to the license terms set forth below. Opening the packaging and/or using the Software indicates your acceptance of these terms. If you do not agree to all of the terms and conditions herein, return the Software, manuals and any partial or whole copies you have made within thirty days of purchase to the party from whom you purchased it for a refund, subject to our restocking fee.

● I accept the terms of the license agreement
○ I do not accept the terms of the license agreement

FIGURE 3.11: OmniPeek License Agreement section

17. The **Installation Notes** step appears; click **Next**.



Installation Notes

Important pre-installation notes:

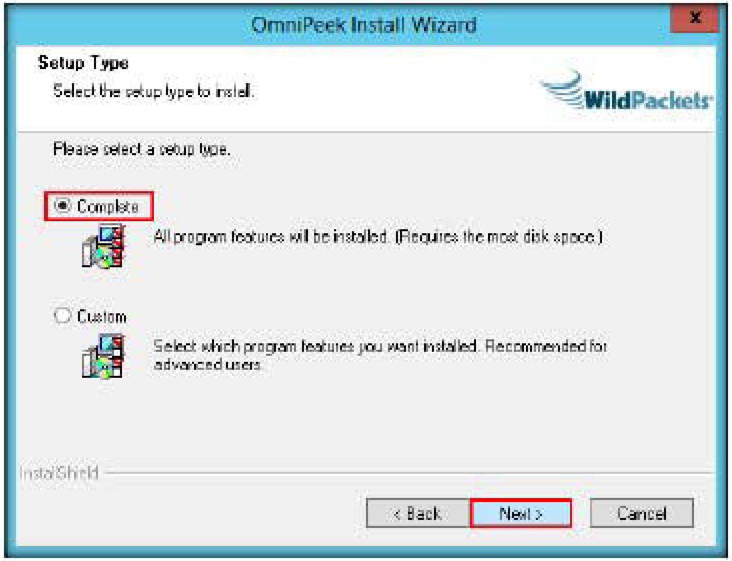
OmniPeek Network Analyzer 7.9.1 Readme

Please read this document for important installation notes, a list of recent changes, and currently known issues. This document covers version 7.9.1 of the following products: OmniPeek Enterprise, OmniPeek Connect, OmniPeek Professional, and OmniPeek Basic. The Omni product family offers configurations to suit every need. Please visit our web site at http://www.wildpackets.com/products/omni/overview for details on how to order the Omni features and media types that precisely fit the needs of your distributed network.

CONTENTS
- Installation Notes
- Product Activation

FIGURE 3.12: OmniPeek Installation Notes section

18. The **Setup Type** section appears; select **Complete,** and click **Next**.



Setup Type

Select the setup type to install.

Please select a setup type.

● Complete

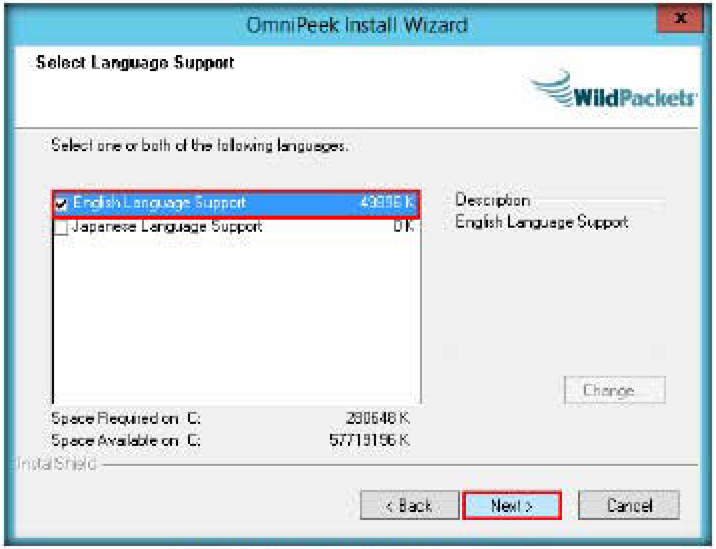
All program features will be installed. (Requires the most disk space.)

○ Custom

Select which program features you want installed. Recommended for advanced users.

FIGURE 3.13: OmniPeek Setup Type section

19. The **Select Language Support** step appears; select a language, and click **Next**.



Select one or both of the following languages.

☑ English Language Support 49936 K
□ Japanese Language Support 0 K

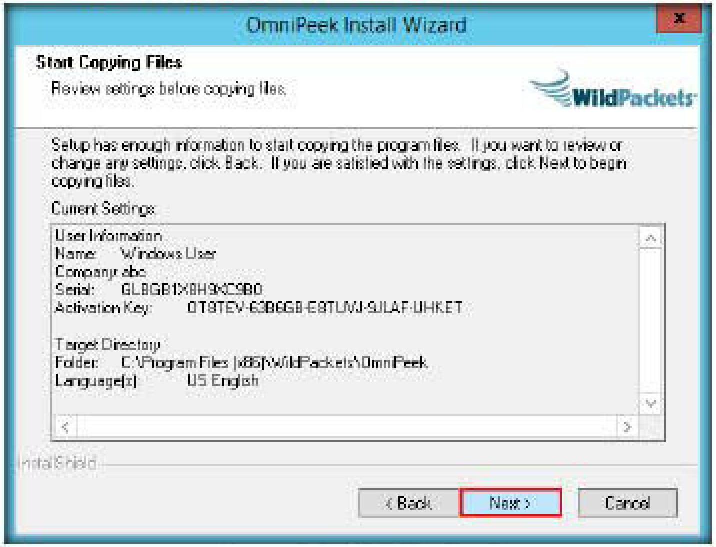
Description
English Language Support

Space Required on C: 280648 K
Space Available on C: 57719156 K

FIGURE 3.14: OmniPeek Select Language Support section

OmniPeek Enterprise provides users with the visibility and analysis they need to keep Voice and Video applications and non-media applications running optimally on the network

20. The **Start Copying Files** step appears; click **Next**.



Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

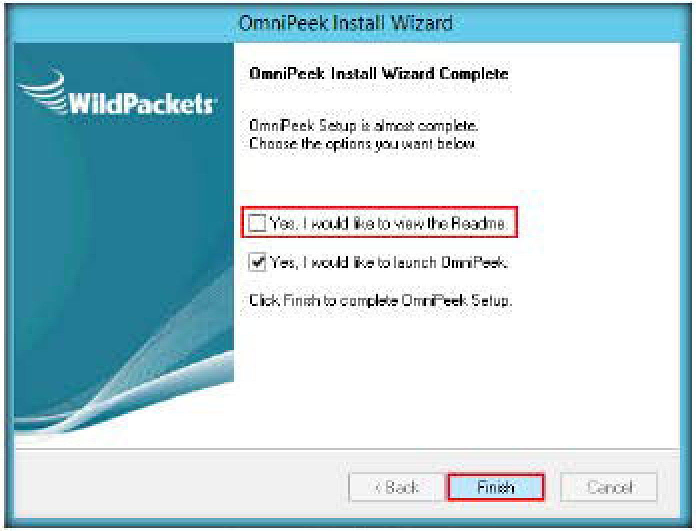
Current Settings:

```
User Information
Name:     Windows User
Company: abc
Serial:    GLBGB1X8H9XC9B0
Activation Key:        0T9TEV-63B6GB-E9TUWJ-9JLAF-UHKET

Target Directory
Folder:    C:\Program Files (x86)\WildPackets\OmniPeek
Language(s):          US English
```

FIGURE 3.15: OmniPeek Start Copying Files section

21. On the completion of installation, the **OmniPeek Install Wizard Complete** step appears; uncheck **Yes, I would like to view the Readme,** and click **Finish.**

To deploy and maintain Voice and Video over IP successfully, you need to be able to analyze and troubleshoot media traffic simultaneously with the network the media traffic is running on.



OmniPeek Install Wizard

OmniPeek Install Wizard Complete

OmniPeek Setup is almost complete.
Choose the options you want below.

☐ Yes, I would like to view the Readme.

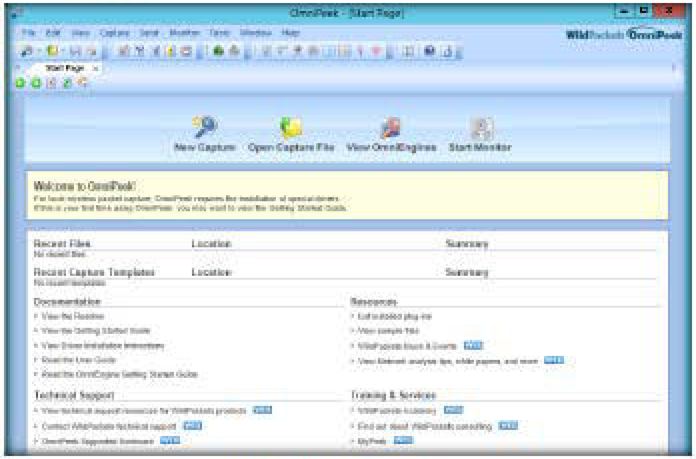
☑ Yes, I would like to launch OmniPeek.

Click Finish to complete OmniPeek Setup.

FIGURE 3.16: OmniPeek installation completed

22. If the **OmniPeek** evaluation dialog box appears, click **OK.**

23. The main window of **WildPackets OmniPeek Demo** opens, as shown in the screenshot.



Welcome to OmniPeek!
For local wireless packet capture, OmniPeek requires the installation of special drivers.
If this is your first time using OmniPeek, you may want to view the Getting Started Guide.

OmniPeek - [Start Page]
File Edit View Capture Send Monitor Tools Window Help
WildPackets OmniPeek
Start Page
New Capture
Open Capture File
View OmniEngines
Start Monitor
Recent Files
Location
Summary
No recent files
Recent Capture Templates
Location
Summary
No recent templates
Documentation
View the Readme
View the Getting Started Guide
View Driver Installation Instructions
Read the User Guide
Read the OmniEngine Getting Started Guide
Resources
List installed plug-ins
View sample files
WildPackets tours & Events
View Ethernet analysis tips, white papers, and more
Technical Support
View technical support resources for WildPackets products
Contact WildPackets technical support
OmniPeek Upgrades/ Downloads
Training & Services
WildPackets Academy
Find out about WildPackets consulting
MyPeek

FIGURE 3.17: OmniPeek main window

TASK 2

Start a New Capture

24. Now, launch the **Windows 8.1** virtual machine.

25. Switch back to **Windows Server 2012**, and create an OmniPeek capture window, as follows:

    a. Click **New Capture,** on the main screen of OmniPeek.

OmniPeek Network Analyzer offers real-time high-level view of the entire network, expert analyses, and drill-down to packets, during capture.

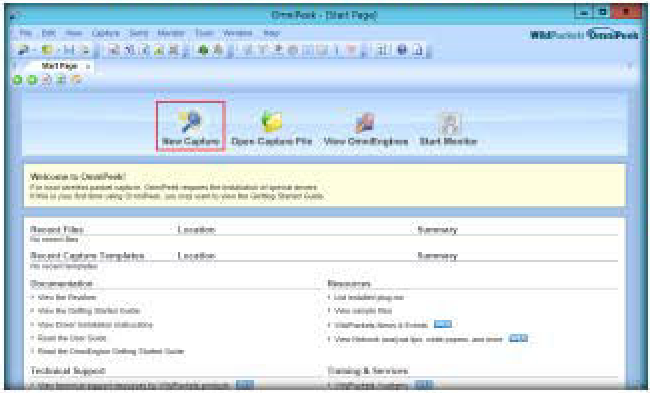
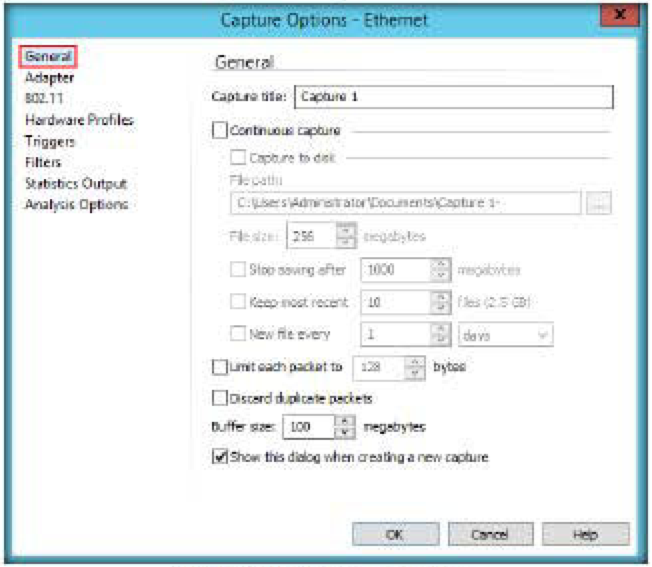


FIGURE 3.18: Starting a new capture

    b. View the **General** options in the **Capture Options** window.

    c. Leave the default general settings.

Network Coverage: With the Ethernet, Gigabit, 10G, and wireless capabilities, you can now effectively monitor and troubleshoot services running on your entire network. Using the same solution for troubleshooting wired and wireless networks reduces the total cost of ownership and illuminates network problems that would otherwise be difficult to detect.



General

Capture title: Capture 1

□ Continuous capture

□ Capture to disk

File path: C:\Users\Administrator\Documents\Capture 1-

File size: 256 megabytes

□ Stop saving after 1000 megabytes

□ Keep most recent 10 files (2.5 GB)

□ New file every 1 days

□ Limit each packet to 128 bytes

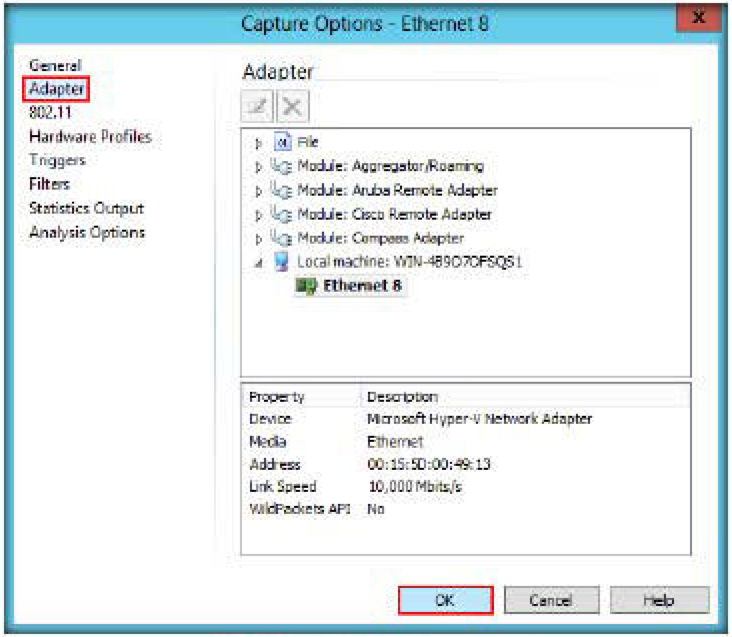
□ Discard duplicate packets

Buffer size: 100 megabytes

☑ Show this dialog when creating a new capture

FIGURE 3.19: OmniPeek capture options - General

d. Click **Adapter,** and select the adapter of the **host machine**, here **Ethernet 8**, and click **OK**.



Capture Options - Ethernet 8

Property	Description
Device	Microsoft Hyper-V Network Adapter
Media	Ethernet
Address	00:15:5D:00:49:13
Link Speed	10,000 Mbits/s
WildPackets API	No

FIGURE 3.20: OmniPeek capture options - Adapter

26. Now, click **Start Capture** to begin capturing packets. The **Start Capture** tab changes to **Stop Capture,** and traffic statistics begin to populate the **Network Dashboard**.

Dashboards display important data that every network engineer needs to know regarding the network without spending lots of time analyzing the captured data.

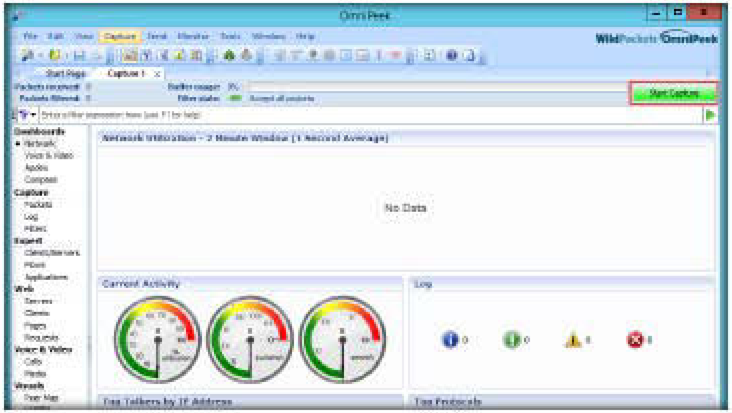


FIGURE 3.21: Starting packet capture

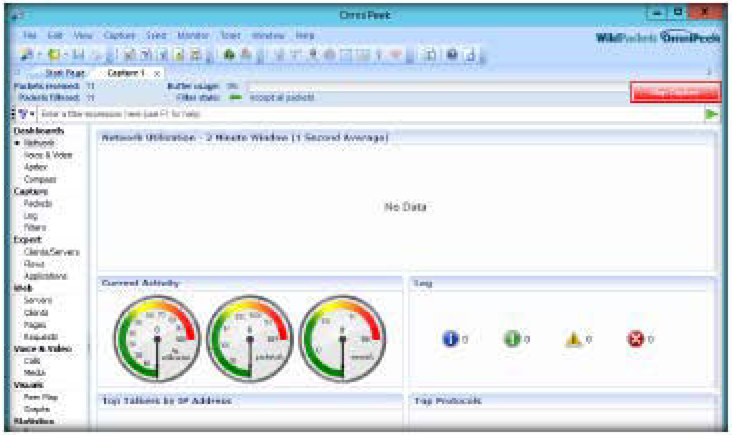


FIGURE 3.22: Start Capture tab changes to Stop Capture

27. Switch to the **Windows 8.1** machine, browse the Internet, and then switch back to the host machine (**Windows Server 2012**).

TASK 3

Analyze the Capture Results

28. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.

OmniPeek Professional expands the capabilities of OmniPeek Basic, extending its reach to all small businesses and corporate workgroups, regardless of the size of the network or the number of employees. OmniPeek Professional provides support for multiple network interfaces while still supporting up to 2 Omni Engines acting as both a full-featured network analyzer and console for remote network analysis.

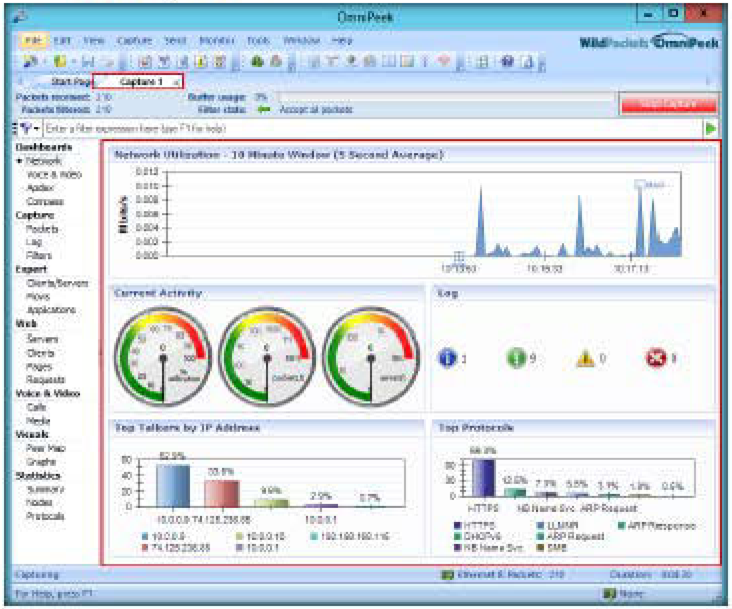
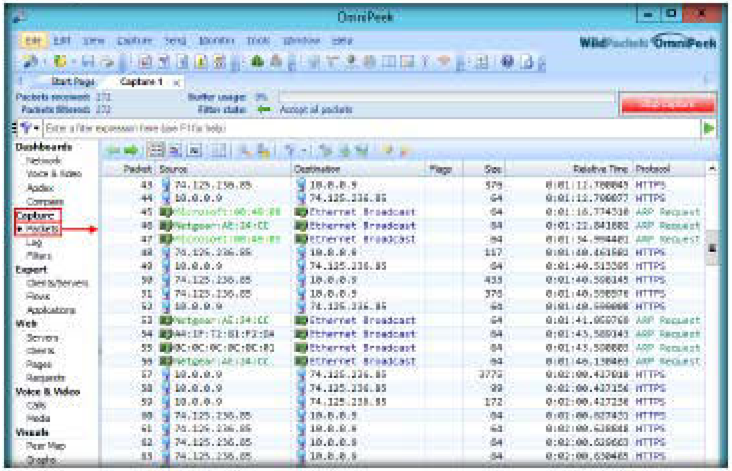


FIGURE 3.23: OmniPeek statistical analysis of the data

29. To view the captured packets, select **Packets** (under **Capture**), in the left pane.

The OmniPeek Peer Map shows all communicating nodes within your network and is drawn as a vertically-oriented ellipse, able to grow to the size necessary. It is easy to read the maps, the thicker the line between nodes, the greater the traffic, the bigger the dot, the more traffic through that node. The number of nodes displayed can also be limited to the busiest and/or active nodes, or to any OmniPeek filters that may be in use.



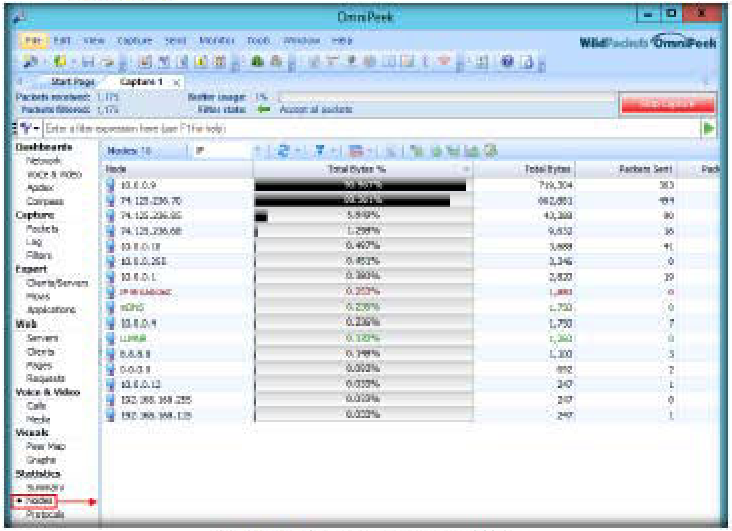
Packet	Source	Destination	Flags	Size	Relative Time	Protocol
43	74.125.236.85	10.0.0.9		579	0:01:12.700043	HTTPS
44	10.0.0.9	74.125.236.85		64	0:01:12.700077	HTTPS
45	Microsoft:00:40:88	Ethernet Broadcast		64	0:01:16.774318	ARP Request
46	Netgear:AE:24:CC	Ethernet Broadcast		64	0:01:22.841882	ARP Request
47	Microsoft:00:40:88	Ethernet Broadcast		64	0:01:34.994481	ARP Request
48	74.125.236.85	10.0.0.9		117	0:01:40.461682	HTTPS
49	10.0.0.9	74.125.236.85		64	0:01:40.513305	HTTPS
50	74.125.236.85	10.0.0.9		433	0:01:40.598145	HTTPS
51	74.125.236.85	10.0.0.9		379	0:01:40.598978	HTTPS
52	10.0.0.9	74.125.236.85		64	0:01:40.600000	HTTPS
53	Netgear:AE:24:CC	Ethernet Broadcast		64	0:01:41.059768	ARP Request
54	44:1F:72:01:F2:D4	Ethernet Broadcast		64	0:01:43.500343	ARP Request
55	0C:0C:0C:0C:0C:03	Ethernet Broadcast		64	0:01:43.500085	ARP Request
56	Netgear:AE:24:CC	Ethernet Broadcast		64	0:01:46.130063	ARP Request
57	10.0.0.9	74.125.236.85		2772	0:02:00.427048	HTTPS
58	10.0.0.9	74.125.236.85		99	0:02:00.427156	HTTPS
59	10.0.0.9	74.125.236.85		172	0:02:00.427238	HTTPS
60	74.125.236.85	10.0.0.9		64	0:02:00.627433	HTTPS
61	74.125.236.85	10.0.0.9		64	0:02:00.628848	HTTPS
62	74.125.236.85	10.0.0.9		64	0:02:00.629663	HTTPS
63	74.125.236.85	10.0.0.9		64	0:02:00.630465	HTTPS

FIGURE 3.24: OmniPeek displaying Packets captured

30. Similarly, you can view **Log**, **Filters**, **Hierarchy**, and **Peer Map** by selecting the respective options in the **Dashboard.**

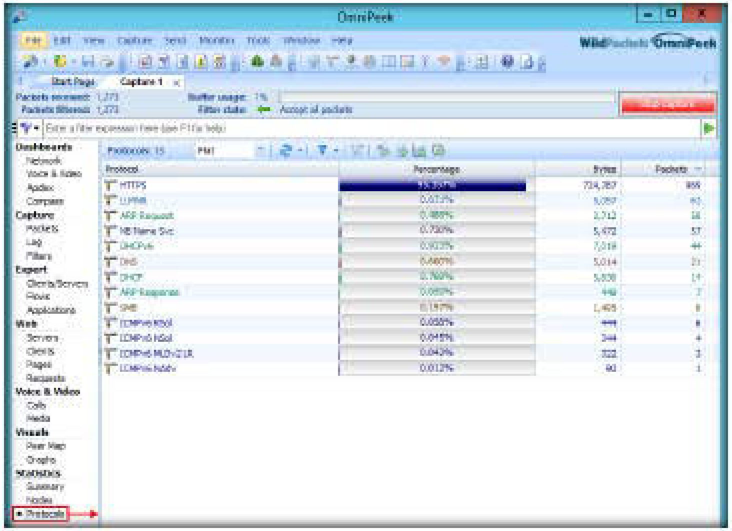
31. You can view the **Nodes** and **Protocols** from the **Statistics** section of the Dashboard.

On-the-Fly Filters: You shouldn't have to stop your analysis to change what you're looking at. OmniPeek enables you to create filters and apply them immediately. The WildPackets "select related" feature selects the packets relevant to a particular node, protocol, conversation, or expert diagnosis, with a simple right click of the mouse.



Node	Total Bytes %	Total Bytes	Packets Sent	Pack
10.0.0.9	[illegible]	719,304	383	
74.125.236.70	[illegible]	682,881	494	
74.125.236.85	5.840%	43,388	80	
74.125.236.68	1.298%	9,632	36	
10.0.0.18	0.467%	3,468	41	
10.0.0.255	0.452%	3,346	0	
10.0.0.1	0.380%	2,820	39	
IP Broadcast	0.253%	1,880	0	
mDNS	0.236%	1,750	0	
10.0.0.4	0.236%	1,750	7	
LLMNR	0.183%	1,360	0	
8.8.8.8	0.148%	1,100	3	
0.0.0.0	0.093%	692	2	
10.0.0.12	0.033%	247	1	
192.168.168.255	0.033%	247	0	
192.168.168.125	0.033%	247	1	

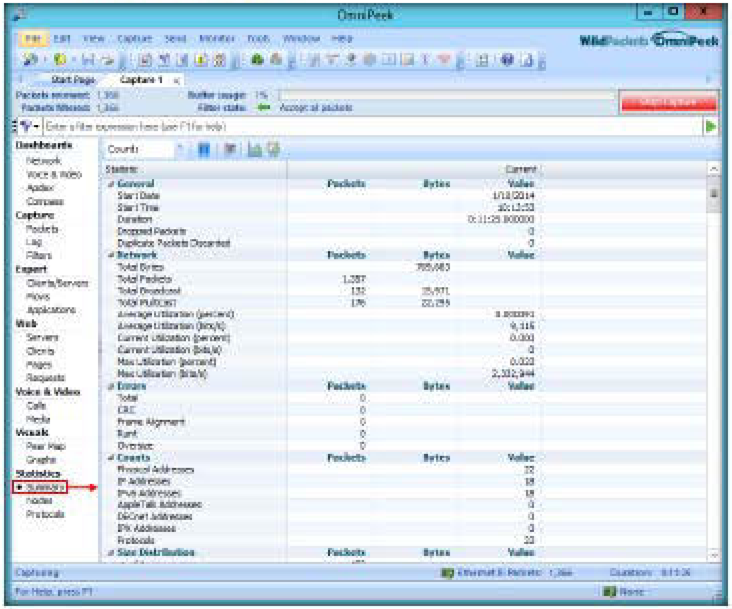
FIGURE 3.25: OmniPeek statistical reports of Nodes



Protocol	Percentage	Bytes	Packets
HTTPS	93.357%	724,787	859
LLMNR	0.613%	5,057	40
ARP Request	0.488%	3,712	58
NB Name Svc	0.720%	5,472	57
DHCPv6	0.923%	7,018	44
DNS	0.660%	5,014	21
DHCP	0.768%	5,838	14
ARP Response	0.059%	448	7
SMB	0.197%	1,495	8
ICMPv6 NSol	0.058%	444	6
ICMPv6 NSol	0.045%	344	4
ICMPv6 MLDv2 LR	0.042%	322	3
ICMPv6 NAdv	0.012%	90	1

FIGURE 3.26: OmniPeek statistical reports of Protocols

32. You can view a complete **Summary** of your network from the **Statistics** section of the **Dashboard**.



Statistic	Packets	Bytes	Current Value
General	Packets	Bytes	Value
Start Date			1/13/2014
Start Time			10:12:53
Duration			0:11:25.800000
Dropped Packets			0
Duplicate Packets Discarded			0
Network	Packets	Bytes	Value
Total Bytes		785,683	
Total Packets	1,287		
Total Broadcast	132	15,971	
Total Multicast	176	22,259	
Average Utilization (percent)			0.000091
Average Utilization (bits/s)			9,116
Current Utilization (percent)			0.000
Current Utilization (bits/s)			0
Max Utilization (percent)			0.022
Max Utilization (bits/s)			2,332,944
Errors	Packets	Bytes	Value
Total	0		
CRC	0		
Frame Alignment	0		
Runt	0		
Oversize	0		
Counts	Packets	Bytes	Value
Physical Addresses			22
IP Addresses			18
IPv6 Addresses			18
AppleTalk Addresses			0
DECnet Addresses			0
IPX Addresses			0
Protocols			22
Size Distribution	Packets	Bytes	Value

Alarms and Notifications: Using its advanced alarms and notifications, OmniPeek uncovers hard-to-diagnose network problems and notifies the occurrence of issues immediately. OmniPeek alarms query a specified monitor statistics function once per second, testing for user-specified problem and resolution conditions.

FIGURE 3.27: OmniPeek Summary details

TASK 4

Save the Capture Results

33. To save the result, go to **File → Save Report**

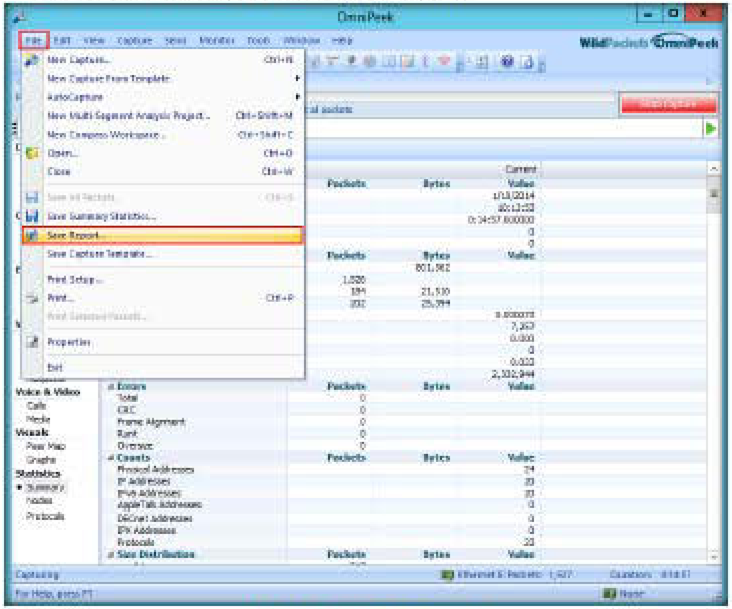
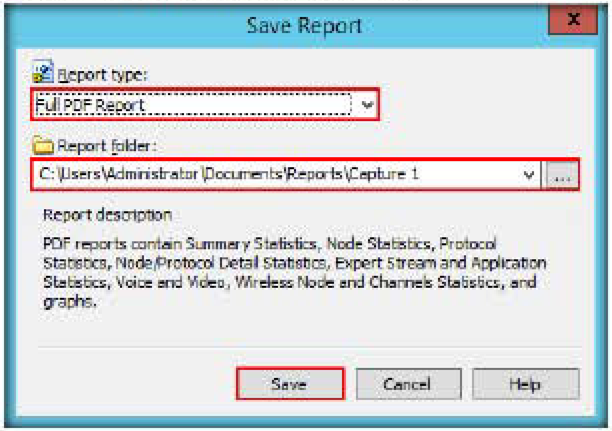


FIGURE 3.28: OmniPeek saving the results

Using OmniPeek's local capture capabilities, centralized console distributes OmniEngine intelligent software probes, Omnipliance®, TimeLine™ network recorders, and Expert Analysis.

34. Choose the format of the **Report type** and the destination **Report folder** from the **Save Report** window, and click **Save**.


Save Report

Report type: Full PDF Report

Report folder: C:\Users\Administrator\Documents\Reports\Capture 1

Report description

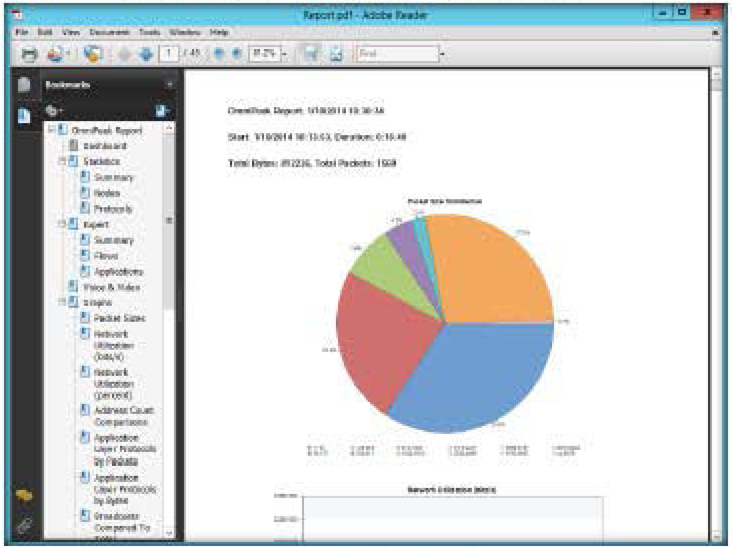
PDF reports contain Summary Statistics, Node Statistics, Protocol Statistics, Node/Protocol Detail Statistics, Expert Stream and Application Statistics, Voice and Video, Wireless Node and Channels Statistics, and graphs.

FIGURE 3.29: OmniPeek Selecting the Report format

Engineers can monitor their entire network, rapidly troubleshoot faults, and fix problems to maximize network uptime and user satisfaction.

35. The saved report can be viewed as in the screenshot below:

Compass Interactive Dashboard offers both real-time and post-capture monitoring of high-level network statistics with drill down capability into packets for the selected time range. Using the Compass dashboard, multiple files can be aggregated and analyzed simultaneously.


Report.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 45
Find
Bookmarks
OmniPeek Report
Dashboard
Statistics
Summary
Nodes
Protocols
Expert
Summary
Flows
Applications
Voice & Video
Graphs
Packet Sizes
Network Utilization (bits/s)
Network Utilization (percent)
Address Count Comparisons
Application Layer Protocols by Packets
Application Layer Protocols by Bytes
Broadcasts Compared To
Packet Size Distribution
Network Utilization (bits/s)

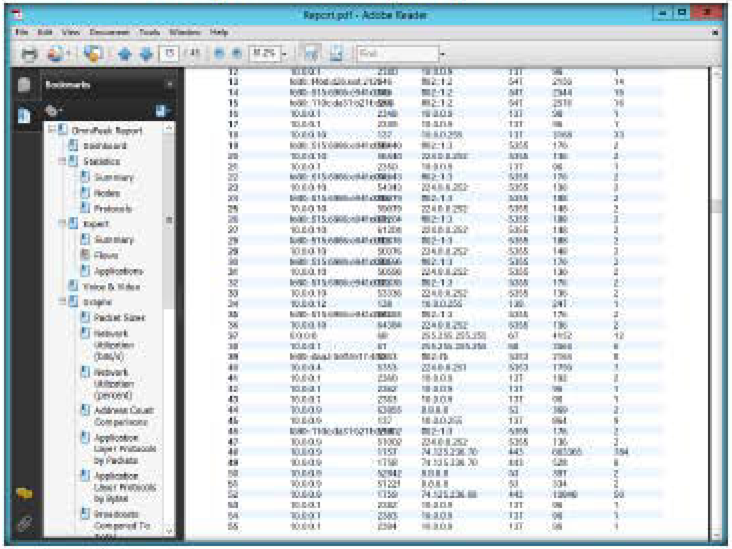
OmniPeek Report: 1/10/2014 10:30:34

Start: 1/10/2014 10:13:53, Duration: 0:16:40

Total Bytes: 812236, Total Packets: 1568

FIGURE 3.30: OmniPeek Report in PDF format

36. Scroll down the pdf to view the complete report.


Report.pdf - Adobe Reader
File Edit View Document Tools Window Help
15 / 45
Find
Bookmarks
OmniPeek Report
Dashboard
Statistics
Summary
Nodes
Protocols
Expert
Summary
Flows
Applications
Voice & Video
Graphs
Packet Sizes
Network Utilization (bits/s)
Network Utilization (percent)
Address Count Comparisons
Application Layer Protocols by Packets
Application Layer Protocols by Bytes
Broadcasts Compared To

12	10.0.0.1	2380	10.0.0.9	137	98	1
13	fe80::f6ab:d2d:aef:2129	[illegible]	ff02::1:2	547	2155	14
14	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:2	547	2344	15
15	fe80::110c:da37:6219:[illegible]	[illegible]	ff02::1:2	547	2519	16
16	10.0.0.1	2346	10.0.0.9	137	98	1
17	10.0.0.1	2339	10.0.0.9	137	98	1
18	10.0.0.10	137	10.0.0.255	137	3068	33
19	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	176	2
20	10.0.0.10	56640	224.0.0.252	5355	136	2
21	10.0.0.1	2350	10.0.0.9	137	98	1
22	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	176	2
23	10.0.0.10	54340	224.0.0.252	5355	136	2
24	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	186	2
25	10.0.0.10	55075	224.0.0.252	5355	146	2
26	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	186	2
27	10.0.0.10	61208	224.0.0.252	5355	146	2
28	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	186	2
29	10.0.0.10	50076	224.0.0.252	5355	146	2
30	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	176	2
31	10.0.0.10	50590	224.0.0.252	5355	136	2
32	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	176	2
33	10.0.0.10	53396	224.0.0.252	5355	136	2
34	10.0.0.12	138	10.0.0.255	138	241	1
35	fe80::515:6866:c94f:[illegible]	[illegible]	ff02::1:3	5355	176	2
36	10.0.0.10	64384	224.0.0.252	5355	136	2
37	0.0.0.0	68	255.255.255.255	67	4152	12
38	10.0.0.1	67	255.255.255.255	68	3968	6
39	fe80::abaa:[illegible]	[illegible]	ff02::fb	5353	3768	8
40	10.0.0.4	5353	224.0.0.251	5353	1759	1
41	10.0.0.1	2360	10.0.0.9	137	192	2
42	10.0.0.1	2362	10.0.0.9	137	98	1
43	10.0.0.1	2363	10.0.0.9	137	98	1
44	10.0.0.9	62855	8.8.8.8	53	369	2
45	10.0.0.9	137	10.0.0.255	137	864	9
46	fe80::110c:da37:6219:[illegible]	[illegible]	ff02::1:3	5355	176	2
47	10.0.0.9	51002	224.0.0.252	5355	136	2
48	10.0.0.9	1157	74.125.236.70	443	687065	784
49	10.0.0.9	1158	74.125.236.70	443	528	8
50	10.0.0.9	52942	8.8.8.8	53	397	2
51	10.0.0.9	51221	8.8.8.8	53	334	2
52	10.0.0.9	1159	74.125.236.88	443	108040	50
53	10.0.0.1	2382	10.0.0.9	137	98	1
54	10.0.0.1	2383	10.0.0.9	137	98	1
55	10.0.0.1	2384	10.0.0.9	137	98	1

FIGURE 3.31: OmniPeek Report in PDF format

37. In real time, an attacker may perform this analysis in an attempt to obtain sensitive information, as well as find any network loopholes.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	□ No
Platform Supported	
☑ Classroom	□ iLabs

Lab 4

Spoofing MAC Address Using SMAC

SMAC is a powerful and easy-to-use tool for MAC address changer (spoofer). The tool can activate a new MAC address right after changing it automatically.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

MAC duplicating or spoofing attack involves sniffing a network for MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then the attacker spoofs his or her own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker can receive all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user. If an administrator does not have the working packet-sniffing skills, it is hard to defend intrusions. So, as an Expert Ethical Hacker and Penetration Tester, you must spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. In this lab, you will learn how to spoof a MAC address to remain unknown to an attacker.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

In this lab, you will learn how to spoof a MAC address.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

In the lab, you will need:

- SMAC located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of SMAC from the link **http://www.klcconsulting.net/smac/default.htm#smac27**
- If you decide to download the latest version, then screenshots shown in the lab might differ

- A computer running Windows Server 2012 as Host and Windows Server 2008 as Victim Machine
- Administrative privileges to run tools
- A Web browser with Internet access

Lab Duration

Time: 5 Minutes

Overview of SMAC

SMAC is a powerful yet easy-to-use and intuitive Windows MAC address modifying utility (MAC address spoofing) which allows users to change MAC addresses for almost any Network Interface Cards (NICs) on the Windows 2003systems, regardless of whether the manufacturers allow this option.

Spoofing MAC protects personal and individual privacy. Many organizations track wired or wireless network users via their MAC Addresses. In addition, there are more and more Wi-Fi wireless connections and wireless network use MAC Addresses to communicate these days. Thus, wireless network security and privacy has to do with MAC addresses.

Spoofing is carried out to perform security Vulnerability Testing, penetration testing on MAC address-based authentication and authorization systems (i.e., wireless access points).

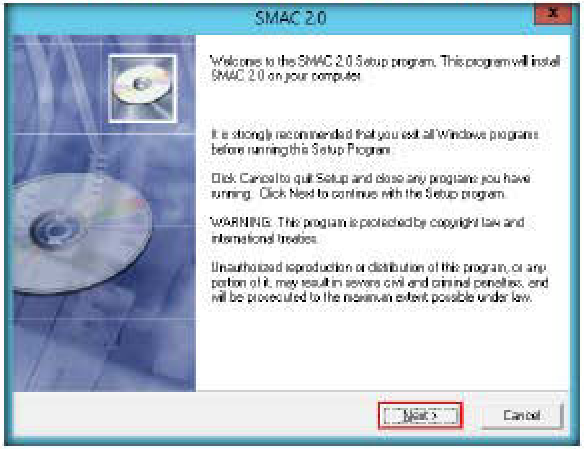
Disclaimer: Authorization to perform these tests must be obtained from the system's owner(s).

Lab Tasks

TASK 1

Install SMAC

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\MAC Spoofing Tools\SMAC**, and double-click **smac20_setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Follow the wizard-driven installation steps to install SMAC.



SMAC 2.0

Welcome to the SMAC 2.0 Setup program. This program will install SMAC 2.0 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup Program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

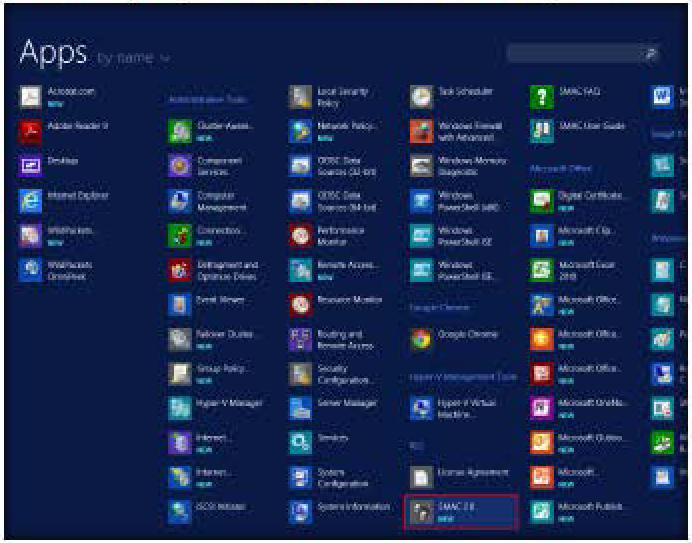
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

FIGURE 4.1: SMAC installation wizard

SMAC works on the Network Interface Card (NIC), which is on the Microsoft hardware compatibility list (HCL).

4. On completing the installation, launch **SMAC** from the **Apps** screen.



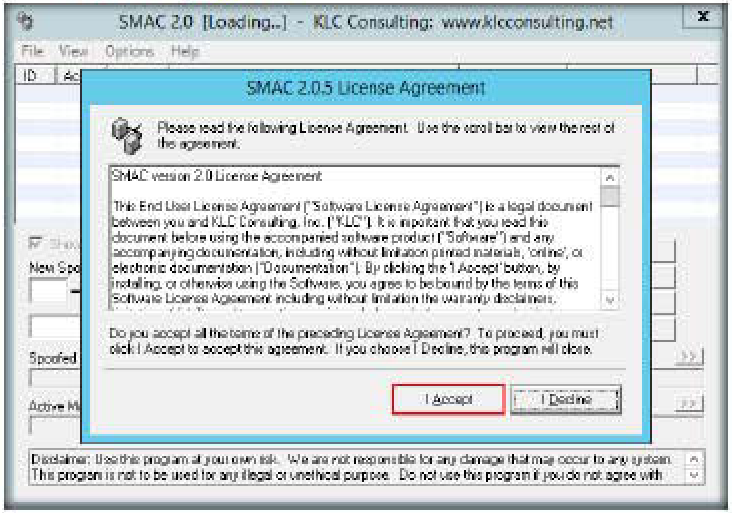
When you start SMAC program, you must start it as the administrator. You could do this by right click on the SMAC program icon and click on "Run as Administrator if not logged in as an administrator.

FIGURE 4.2 Launching SMAC from Windows Server 2012 - Apps screen

TASK 2

Configure SMAC

5. The SMAC main screen appears, along with the **License Agreement**. Click **I Accept** to continue.



SMAC 2.0 [Loading..] - KLC Consulting: www.klcconsulting.net

SMAC 2.0.5 License Agreement

Please read the following License Agreement. Use the scroll bar to view the rest of the agreement.

SMAC version 2.0 License Agreement

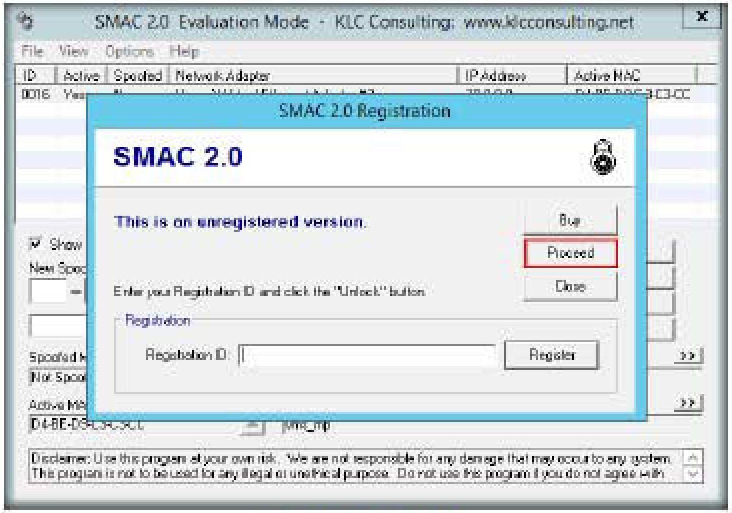
This End User License Agreement ("Software License Agreement") is a legal document between you and KLC Consulting, Inc. ("KLC"). It is important that you read this document before using the accompanied software product ("Software") and any accompanying documentation, including without limitation printed materials, 'online', or electronic documentation ("Documentation"). By clicking the 'I Accept' button, by installing, or otherwise using the Software, you agree to be bound by the terms of this Software License Agreement including without limitation the warranty disclaimers.

Do you accept all the terms of the preceding License Agreement? To proceed, you must click I Accept to accept this agreement. If you choose I Decline, this program will close.

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.3: License Agreement window

6. The **Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

SMAC 2.0 Registration

SMAC 2.0

This is an unregistered version.

Enter your Registration ID and click the "Unlock" button.

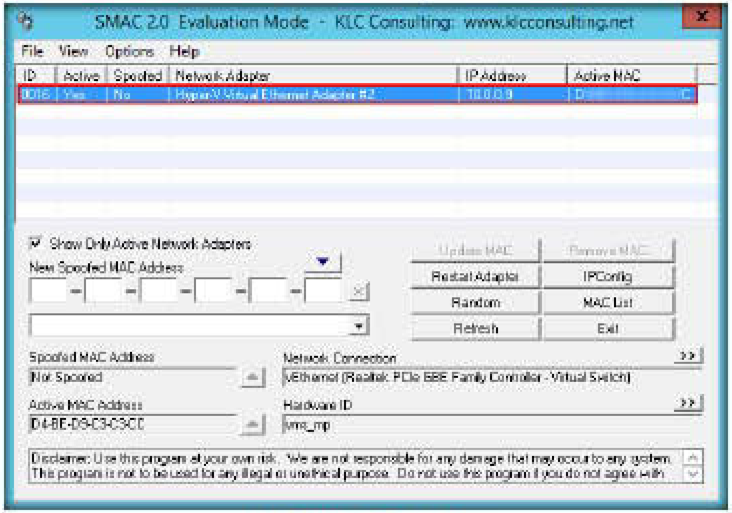
Registration

Registration ID:

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.4 Registration window

7. The SMAC main window appears. Choose the network adapter of the machine whose MAC Address is to be spoofed.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	[redacted]

☑ Show Only Active Network Adapters

New Spoofed MAC Address

Spoofed MAC Address: Not Spoofed

Active MAC Address: D4-BE-D9-C3-C3-CC

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

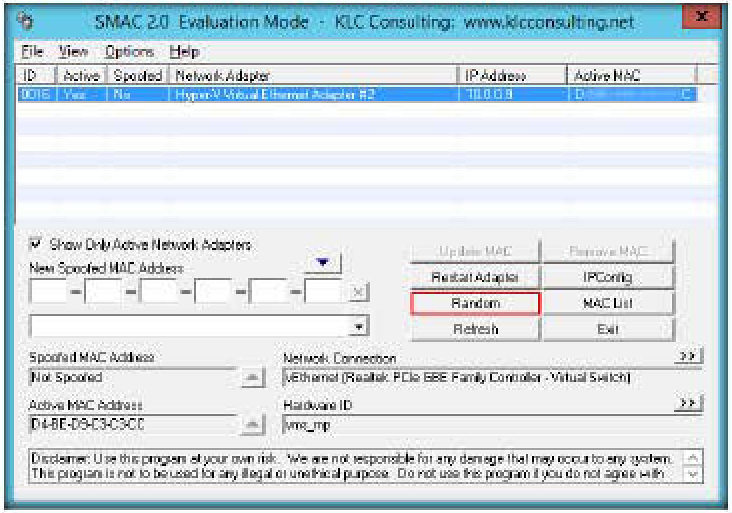
Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.5 SMAC main window

8. To generate a random MAC address, click **Random**.

SMAC helps people to protect their privacy by hiding their real MAC Addresses in the widely available Wi-Fi Wireless Network.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D[redacted]C

☑ Show Only Active Network Adapters

New Spoofed MAC Address: _ - _ - _ - _ - _ - _

Spoofed MAC Address: Not Spoofed

Active MAC Address: D4-BE-D9-C3-C3-CC

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

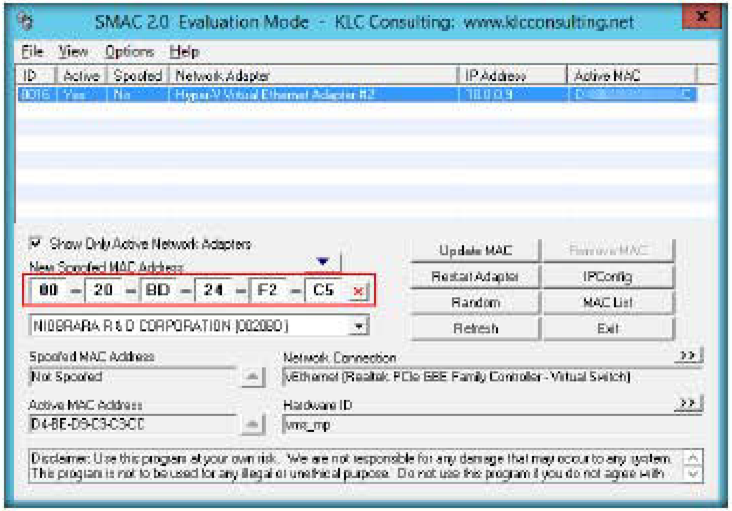
Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.6: SMAC Random button to generate MAC addresses

9. Clicking **Random** inputs a new randomly **Spoofed MAC Address**.

SMAC also helps Network and IT Security professionals to troubleshoot network problems, test Intrusion Detection / Prevention Systems (IDS/IPS,) test Incident Response plans, build high-availability solutions, recover (MAC Address based) software licenses, and so on.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D[redacted]C

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 20 - 8D - 24 - F2 - C5

NIOBRARA R & D CORPORATION [00208D]

Spoofed MAC Address: Not Spoofed

Active MAC Address: D4-BE-D9-C3-C3-CC

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

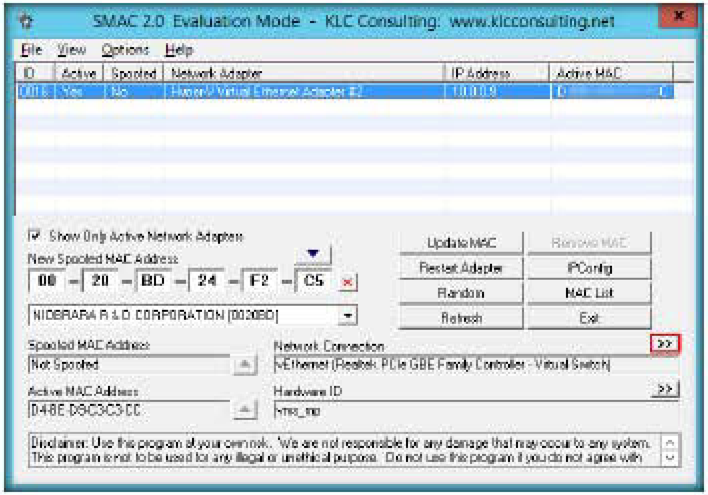
Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.7: SMAC selecting a new spoofed MAC address

10. The Network Connection or Adapter displays its respective name.

11. Click the forward arrow button on **Network Connection** to display the **Network Adapter**.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D[illegible]C

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 20 - BD - 24 - F2 - C5

NIOBRARA R & D CORPORATION [0020BD]

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

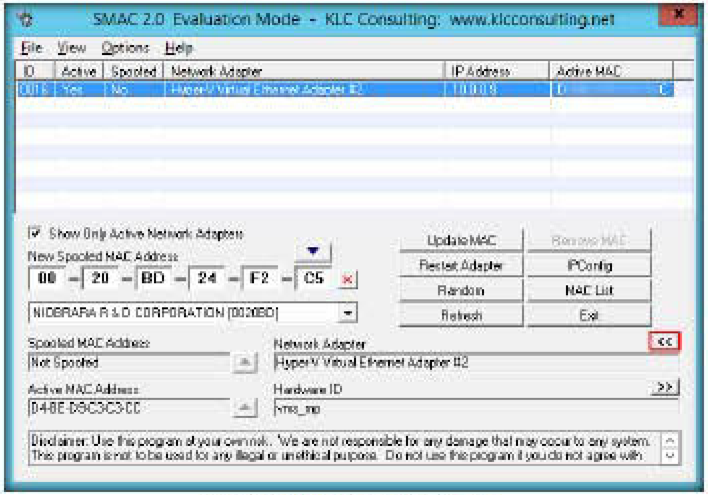
Active MAC Address: D4-BE-D9-C3-C3-CC

Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.8: SMAC Network Connection information

12. Clicking the backward arrow button on **Network Adapter** will again display the **Network Connection**. These buttons allow to toggle between the Network Connection and Network Adapter.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D[illegible]C

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 20 - BD - 24 - F2 - C5

NIOBRARA R & D CORPORATION [0020BD]

Spoofed MAC Address: Not Spoofed

Network Adapter: Hyper-V Virtual Ethernet Adapter #2

Active MAC Address: D4-BE-D9-C3-C3-CC

Hardware ID: vms_mp

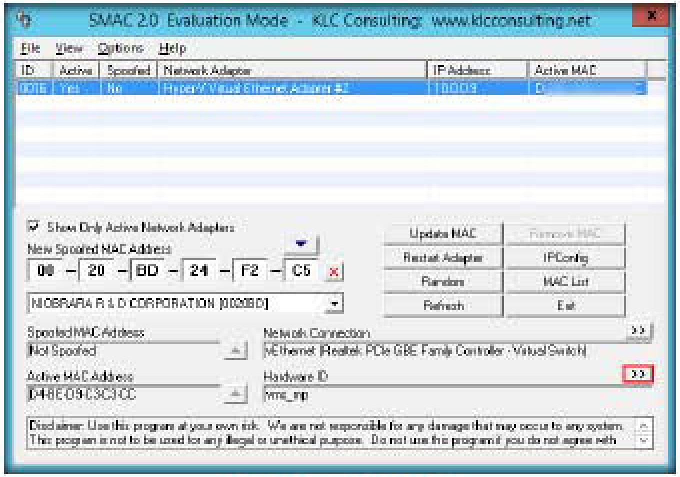
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

SMAC does not change the hardware burned-in MAC addresses. SMAC changes the software-based MAC addresses, and the new MAC addresses you change are sustained from reboots.

FIGURE 4.9: SMAC Network Adapter information

13. Similarly, the Hardware ID and Configuration ID display their respective information.

14. Click the forward arrow button on **Hardware ID** to display **Configuration ID** information.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 – 20 – BD – 24 – F2 – C5

NIOBRARA R & D CORPORATION [0020BD]

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

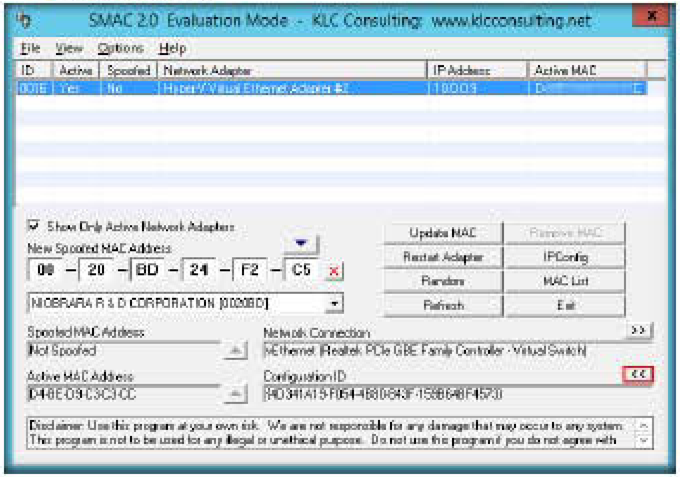
Active MAC Address: D4-BE-D9-C3-C3-CC

Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.10: SMAC Hardware ID display

15. Clicking the backward arrow button on **Configuration ID** will again display **Hardware ID information**. These buttons toggle between Hardware ID and Configuration ID.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 – 20 – BD – 24 – F2 – C5

NIOBRARA R & D CORPORATION [0020BD]

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

Active MAC Address: D4-BE-D9-C3-C3-CC

Configuration ID: {9D341A15-F064-4680-843F-159B64BF4570}

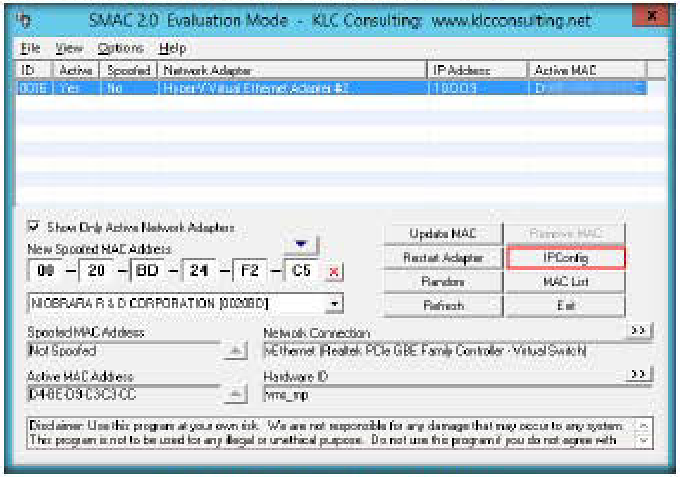
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.11: SMAC Configuration ID display

TASK 3

View IPConfig Information

16. To bring up the **ipconfig** information, click **IPConfig**.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D[redacted]

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 20 - BD - 24 - F2 - C5

NIOBRARA R & D CORPORATION [0020BD]

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

Active MAC Address: D48E-D9-C3C3-CC

Hardware ID: vms_mp

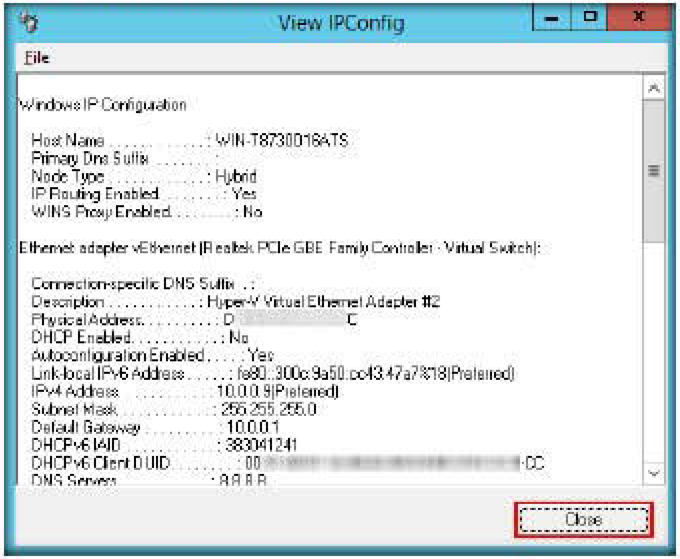
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.12: SMAC to view the information of IPConfig

17. The **IPConfig** window pops up, displaying the IP configuration details of the selected Network Adapter.

18. Click **Close** after analyzing the information.

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.



View IPConfig

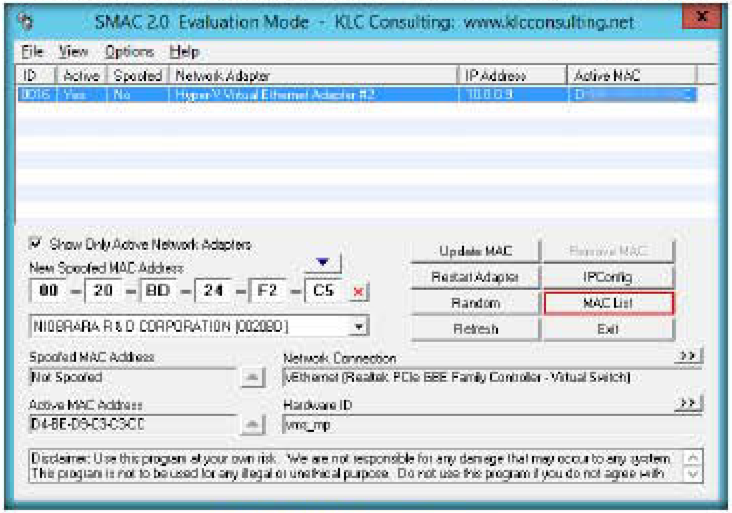
```
Windows IP Configuration

   Host Name . . . . . . . . . . : WIN-T8730D16ATS
   Primary Dns Suffix . . . . . . :
   Node Type . . . . . . . . . . : Hybrid
   IP Routing Enabled . . . . . . : Yes
   WINS Proxy Enabled . . . . . . : No

Ethernet adapter vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch):

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter #2
   Physical Address. . . . . . . . : D[redacted]C
   DHCP Enabled. . . . . . . . . . : No
   Autoconfiguration Enabled . . . : Yes
   Link-local IPv6 Address . . . . : fe80::300c:9a50:cc43:47a7%18(Preferred)
   IPv4 Address . . . . . . . . . : 10.0.0.9(Preferred)
   Subnet Mask . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . : 10.0.0.1
   DHCPv6 IAID . . . . . . . . . . : 383041241
   DHCPv6 Client DUID. . . . . . . : 00[redacted]-CC
   DNS Servers . . . . . . . . . . : 8.8.8.8
```

FIGURE 4.13: SMAC IPConfig information

TASK 4

Perform MAC Address Spoofing

19. You can also import the MAC address list into SMAC by clicking **MAC List**.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	D[redacted]

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 20 - 8D - 24 - F2 - C5

NIOBRARA R & D CORPORATION [00208D]

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

Active MAC Address: D4-BE-D9-C3-C3-CC

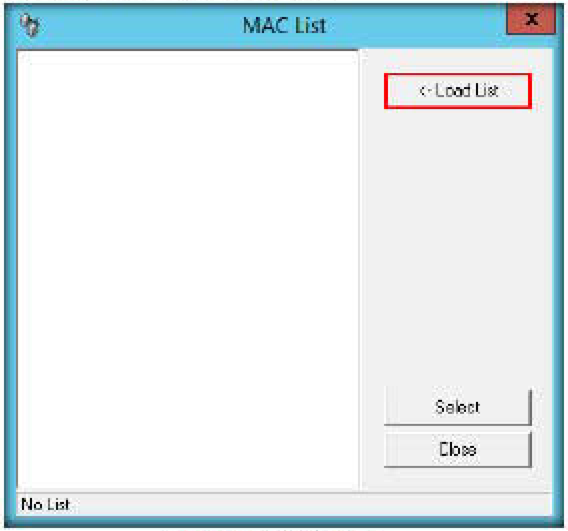
Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 4.14: SMAC listing MAC addresses

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

20. If there is no address in the MAC address field, click **Load List** to select a MAC address list file you have created.



MAC List

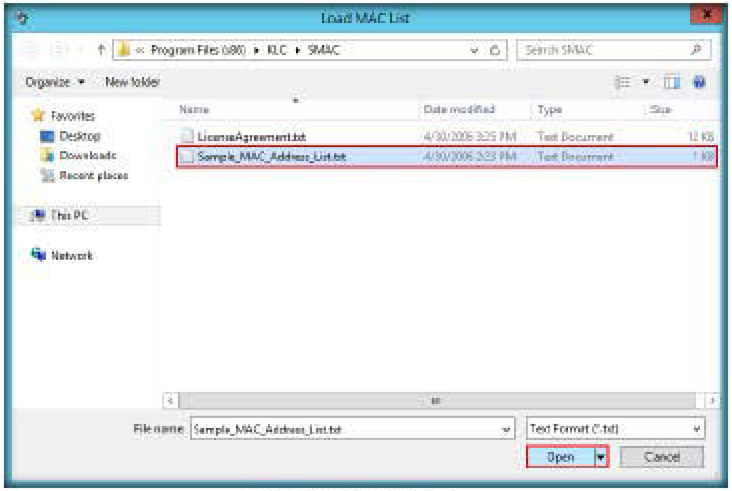
No List

FIGURE 4.15 SMAC MAC List window

When changing MAC address, you MUST assign MAC addresses according to IANA Number Assignments database. For example, "00-00-00-00-00-00" is not a valid MAC address, therefore, even though you can update this address, it may be rejected by the NIC device driver because it is not valid, and TRUE MAC address will be used instead. Otherwise, "00-00-00-00-00-00" may be accepted by the NIC device driver, however, the device will not function.

21. Select **Sample_MAC_Address_List.txt** file from the **Load MAC List** window, and click **Open**.

SMAC is created and maintained by Certified Information Systems Security Professionals (CISSPs), Certified Information System Auditors (CISAs), Microsoft Certified Systems Engineers (MCSEs), and professional software engineers.



Name	Date modified	Type	Size
LicenseAgreement.txt	4/30/2006 3:25 PM	Text Document	12 KB
Sample_MAC_Address_List.txt	4/30/2006 2:23 PM	Text Document	1 KB

File name: Sample_MAC_Address_List.txt

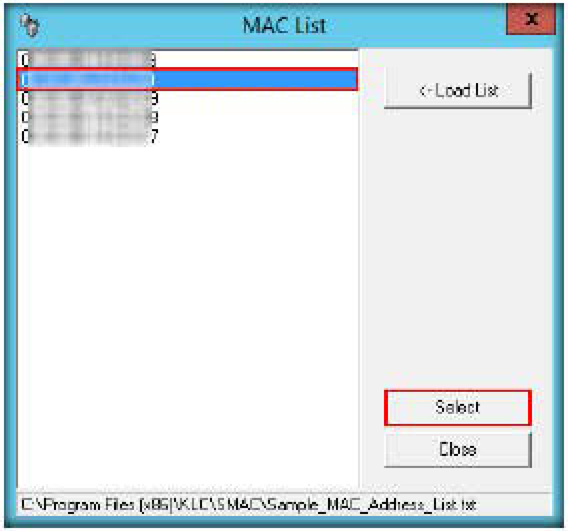
Text Format (*.txt)

FIGURE 4.16: SMAC MAC List window

22. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose a **MAC Address,** and click **Select** to copy the MAC Address to the "**New Spoofed MAC Address**" in the main SMAC screen.

SMAC displays the following information about a Network Interface Card (NIC).

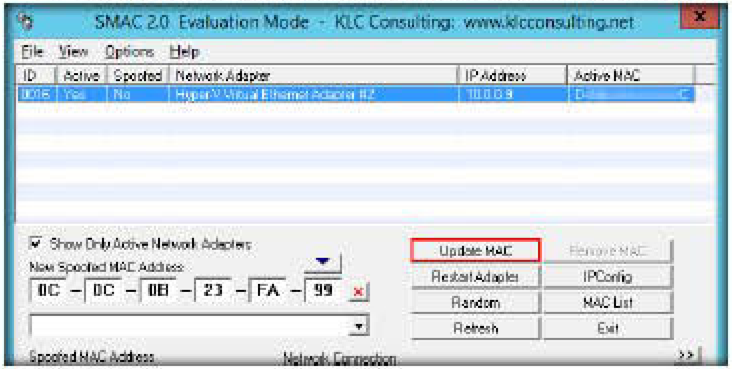
- Device ID
- Active Status
- NIC Description
- Spoofed status
- IP Address
- Active MAC address
- Spoofed MAC Address
- NIC Hardware ID
- NIC Configuration ID



C:\Program Files (x86)\KLC\SMAC\Sample_MAC_Address_List.txt

FIGURE 4.17: SMAC MAC List window

23. Click **Update MAC** to update the MAC address information of the machine.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0016	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.9	[redacted]

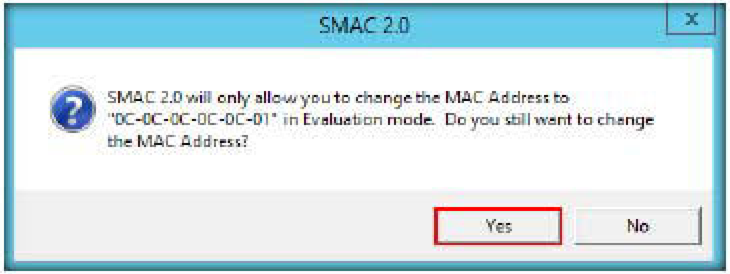
☑ Show Only Active Network Adapters

New Spoofed MAC Address: 0C - 0C - 0B - 23 - FA - 99

FIGURE 4.18: Updating MAC address

24. **SMAC 2.0** dialog-box appears, click **Yes**. It will cause a temporary disconnection in your Network Adapter.

Note: This dialog box appears only for the evaluation or trial version.

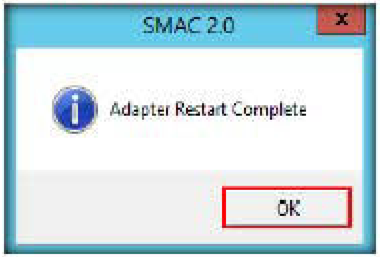


SMAC 2.0

SMAC 2.0 will only allow you to change the MAC Address to "0C-0C-0C-0C-0C-01" in Evaluation mode. Do you still want to change the MAC Address?

FIGURE 4.19: SMAC 2.0 dialog box

25. After successfully spoofing the MAC address, a **SMAC 2.0** pop-up appears, stating that the Adapter has been restarted; click **OK** to close the pop-up.



SMAC 2.0

Adapter Restart Complete

FIGURE 4.20: SMAC 2.0 dialog box

26. Once the adapter is restarted, the MAC address is assigned to your machine. By spoofing it, an attacker can simulate attacks such as ARP poisoning and MAC flooding, without revealing the actual MAC address of the attacker's machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

5

Performing Man-in-the-Middle Attack using Cain & Abel

Cain &Abel is a password recovery tool that allows recovery of passwords by sniffing the network, and cracking encrypted passwords.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You learned in the previous lab how to obtains username and passwords using Wireshark. By merely capturing enough packets, attackers can extract the username and password if victims authenticates themselves in public networks, especially on unsecured websites. Once a password is hacked, an attacker can simply log into the victim's email account or use that password to login to their PayPal and drain the victim's bank account. They can even change the password for the email. Attackers can use Wireshark to decrypt the frames with the victim's password they already have.

As a preventive measure, an organization's Administrator should advise employees not to provide sensitive information in public networks without HTTPS connections. VPN and SSH tunneling must be used to secure the network connection. As an expert Ethical Hacker and Penetration Tester you must have sound knowledge of sniffing, network protocols and their topology , TCP and UDP services, routing tables, remote access (SSH or VPN), authentication mechanism, and encryption techniques.

Another method through which you can gain username and password is by using Cain & Abel to perform man-in-the-middle (MITM) attacks.

Lab Objectives

The objective of this lab to accomplish the following information regarding the target organization that includes, but is not limited to:

- Sniff network traffic and perform ARP Poisoning
- Launch Man-in-the-Middle attack
- Sniff network for password

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

To carry-out the lab, you need:

- Cain and Abel, located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel**
- You can also download the latest version of Cain & Abel from http://www.oxid.it.
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as Host machine
- Windows 8.1 running on virtual machine as Attacker machine
- Windows 2008 Server running on virtual machine as Victim machine
- A Web browser with Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of a Man-in-the-Middle Attack

You can download Cain & Abel from http://www.oxid.it.

An MITM is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

MITM attacks come in many variations and can be carried out on a switched LAN.

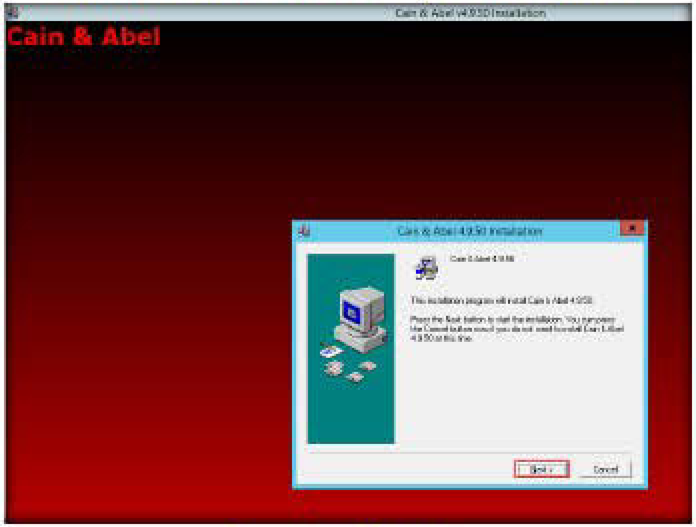
Lab Tasks

TASK 1

Man-In-The-Middle Attack

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel** and double-click **ca_setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard-driven installation steps to install Cain & Abel.



Cain & Abel v4.9.50 Installation

Cain & Abel

Cain & Abel 4.9.50 Installation

Cain & Abel 4.9.50

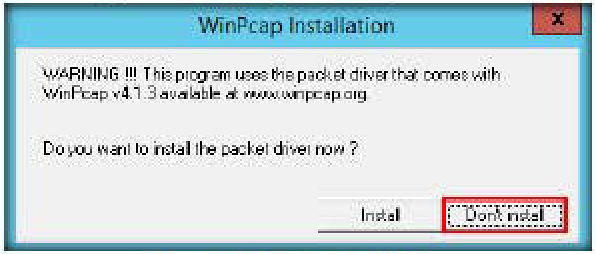
This installation program will install Cain & Abel 4.9.50.

Press the Next button to start the installation. You can press the Cancel button now if you do not want to install Cain & Abel 4.9.50 at this time.

FIGURE 5.1: Cain & Abel installation

4. The **WinPcap Installation** pop-up appears; click **Don't install,** as you have already installed it during the lab setup.

Man in the Middle attacks has the potential to eavesdrop on a switched LAN to sniff for clear-text data (McClure, Scambray). It can also be used for substitution attacks that can actively manipulate data.



WinPcap Installation

WARNING !!! This program uses the packet driver that comes with WinPcap v4.1.3 available at www.winpcap.org

Do you want to install the packet driver now ?

FIGURE 5.2: WinPcap Installation pop-up

5. Launch the **Windows Server 2008** and **Windows 8.1** virtual machines.

6. Switch back to the host machine, and launch **Cain & Abel** from the **Apps** screen.

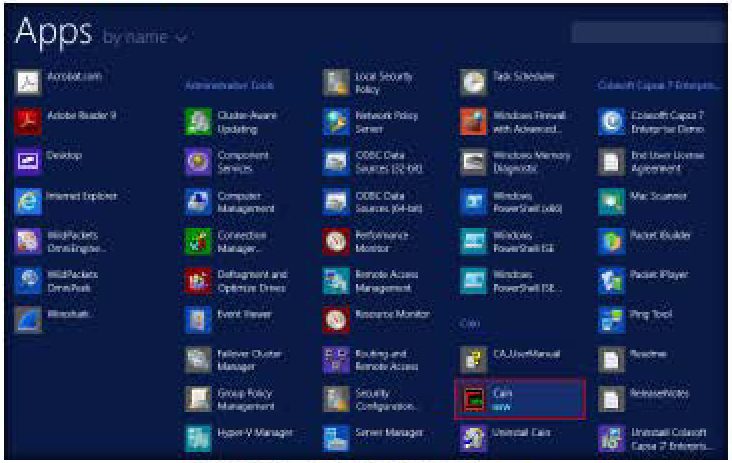
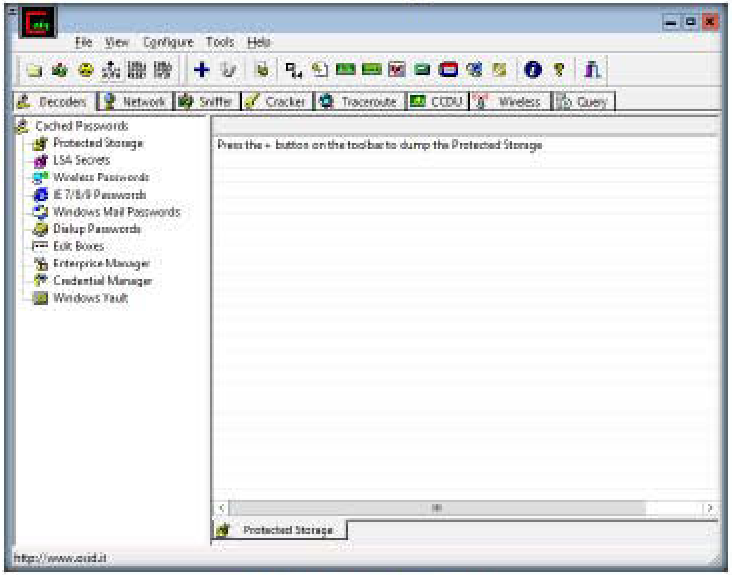


FIGURE 5.3: Launching Cain & Abel from Apps screen

7. The main Window of Cain & Abel appears, as shown in the screenshot:

Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

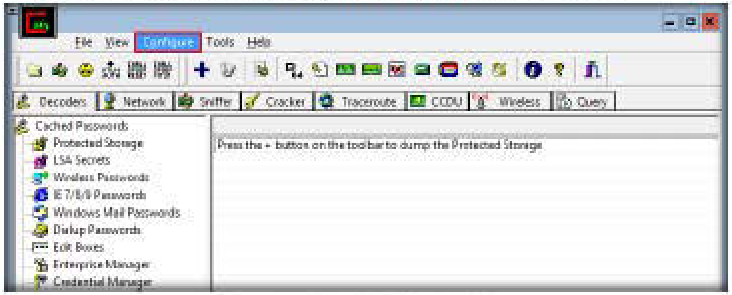


Press the + button on the toolbar to dump the Protected Storage

FIGURE 5.4: Cain & Abel Main Window

APR-SSH1 can capture and decrypt SSH version 1 session that are then saved to a text file. APR-HTTPS can intercept and forge digital certificates on the fly but because trusted authority does not sign these certificates a warning message will be displayed to the end user.

8. To configure **Ethernet card**, click **Configure** from menu bar.



Press the + button on the toolbar to dump the Protected Storage

FIGURE 5.5: Cain & Abel Configuration Option

Replay attacks can also be used to resend a sniffed password hash to authenticate an unauthorized user.

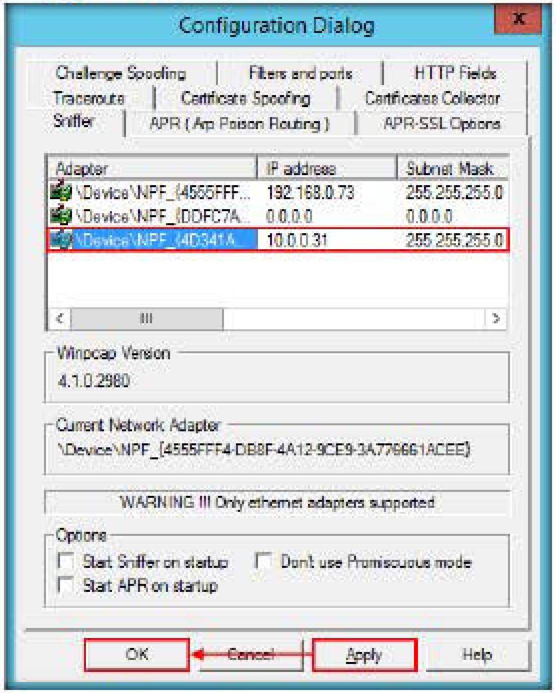
9. The **Configuration Dialog** window appears.

10. The window consists of several tabs. Click the **Sniffer** tab to select sniffing adapter.

11. Select the **Adapter** associated with the IP address of the machine, and click **Apply** and **OK**.

For IP and MAC spoofing you have to choose addresses that are not already present on the network. By default Cain uses the spoofed MAC "001122334455" for two reasons: first that address can be easily identified for troubleshooting and second it is not supposed to exist in your network.

Note: You cannot have on the same Layer-2 network two or more Cain machines using APR's MAC spoofing and the same Spoofed MAC address.



Adapter	IP address	Subnet Mask
\Device\NPF_{4555FFF...	192.168.0.73	255.255.255.0
\Device\NPF_{DDFC7A...	0.0.0.0	0.0.0.0
\Device\NPF_{4D341A...	10.0.0.31	255.255.255.0

Winpcap Version
4.1.0.2980

Current Network Adapter
\Device\NPF_{4555FFF4-DB8F-4A12-9CE9-3A776661ACEE}

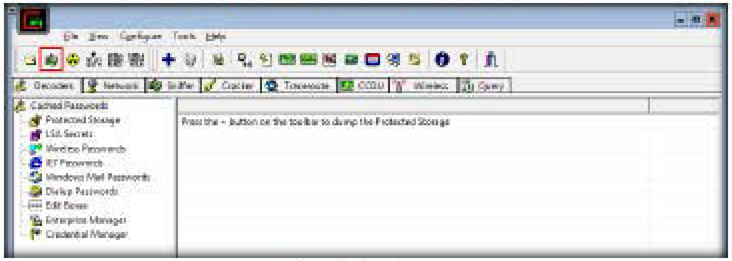
WARNING !!! Only ethernet adapters supported

Options
☐ Start Sniffer on startup
☐ Don't use Promiscuous mode
☐ Start APR on startup

FIGURE 5.6: Cain & Abel Configuration Dialog Window

12. Click **Start/Stop Sniffer** on the toolbar to begin sniffing.

The most crucial item in that list is the radioactive hazard APR. It is in this window that we select our victim(s).

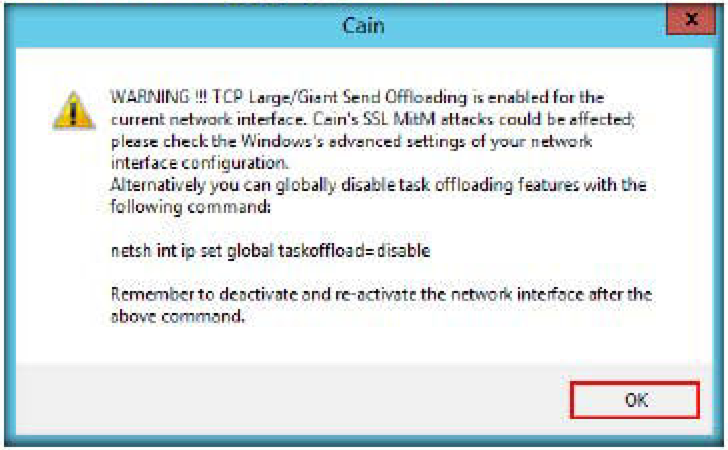


Press the + button on the toolbar to dump the Protected Storage

FIGURE 5.7: Starting a sniffer

Note: If the **Cain** Warning pop-up opens, click **OK**.

Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data.



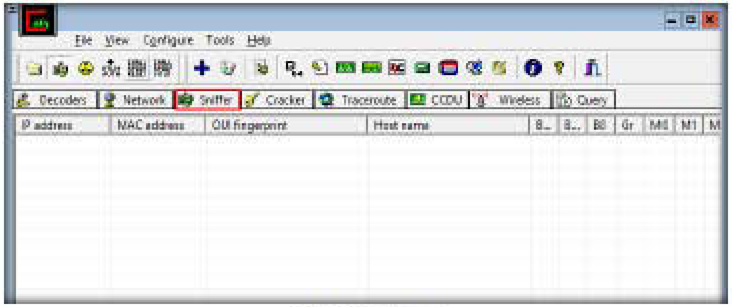
WARNING !!! TCP Large/Giant Send Offloading is enabled for the current network interface. Cain's SSL MitM attacks could be affected; please check the Windows's advanced settings of your network interface configuration.
Alternatively you can globally disable task offloading features with the following command:

```
netsh int ip set global taskoffload=disable
```

Remember to deactivate and re-activate the network interface after the above command.

FIGURE 5.8: Cain Warning pop-up

13. Now click the **Sniffer** tab.

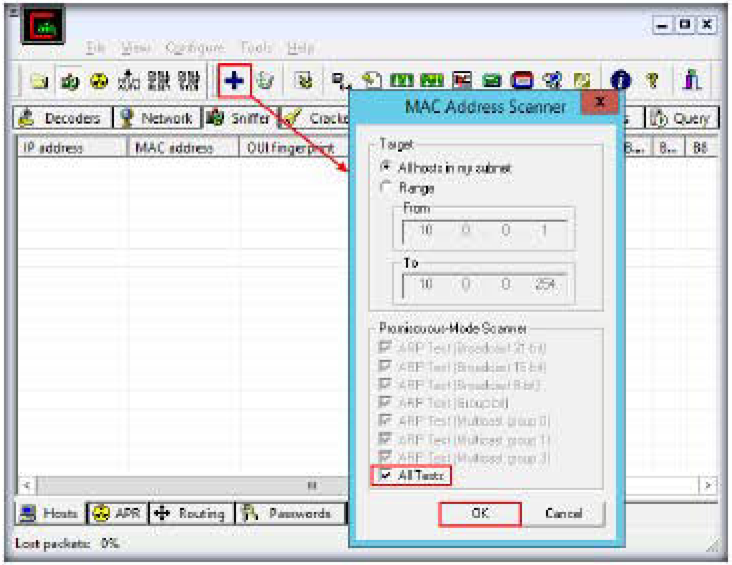


IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M

FIGURE 5.9: Sniffer tab

14. Click the plus (**+**) icon, or right click in the window, and select **Scan MAC Addresses** to scan the network for hosts.

15. The **MAC Address Scanner** window appears. Check **All hosts in my subnet** and **All Tests**, then click **OK.**


File View Configure Tools Help
Decoders Network Sniffer Cracke
Query
IP address MAC address OUI fingerprint
B... B... BB
Hosts APR Routing Passwords
Lost packets: 0%

MAC Address Scanner

Target

● All hosts in my subnet

○ Range

From 10 0 0 1

To 10 0 0 254

Promiscuous-Mode Scanner

☑ ARP Test (Broadcast 31-bit)

☑ ARP Test (Broadcast 16-bit)

☑ ARP Test (Broadcast 8-bit)

☑ ARP Test (Group bit)

☑ ARP Test (Multicast group 0)

☑ ARP Test (Multicast group 1)

☑ ARP Test (Multicast group 3)

☑ All Tests

OK Cancel

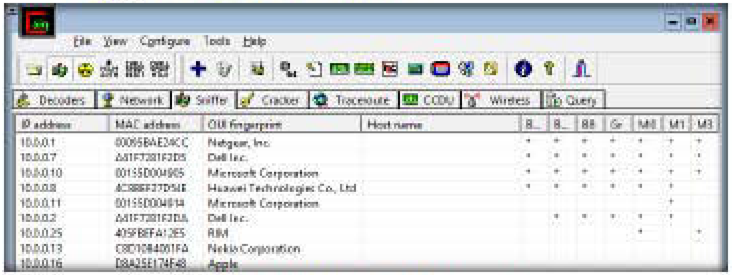
FIGURE 5.10: Cain & Abel - MAC Address Scanner Window

APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well.

16. Cain & Abel starts **scanning** for MAC addresses and **lists** all those found.

Speeding up packet capture speed by wireless packet injection.

17. After scanning is **completed**, a list of detected **MAC addresses** are displayed as shown in the screenshots:


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

IP address	MAC address	OUI fingerprint	Host name	B...	B...	BB	Gr	M0	M1	M3
10.0.0.1	00095BAE24CC	Netgear, Inc.		*	*	*	*	*	*	*
10.0.0.7	A41F7281F2D5	Dell Inc.		*	*	*	*	*	*	*
10.0.0.10	00155D004905	Microsoft Corporation		*	*	*	*	*	*	*
10.0.0.8	4C8BEF37D5EE	Huawei Technologies Co., Ltd		*	*	*	*	*	*	
10.0.0.11	00155D004814	Microsoft Corporation							*	
10.0.0.2	A41F7281F2DA	Dell Inc.			*	*	*	*	*	
10.0.0.25	405FBEFA12E5	RIM						*		*
10.0.0.13	C8D1084061FA	Nokia Corporation								
10.0.0.16	D8A25E174F48	Apple								

FIGURE 5.11: Cain & Abel - MAC Address Scanned

18. Click the **APR** tab at the lower end of the window.

APR state Half-Routing means that APR is routing the traffic correctly but only in one direction (ex: Client->Server or Server->Client). This can happen if one of the two hosts cannot be poisoned or if asymmetric routing is used on the LAN. In this state the sniffer loses all packets of an entire direction so it cannot grab authentications that use a challenge-response mechanism.

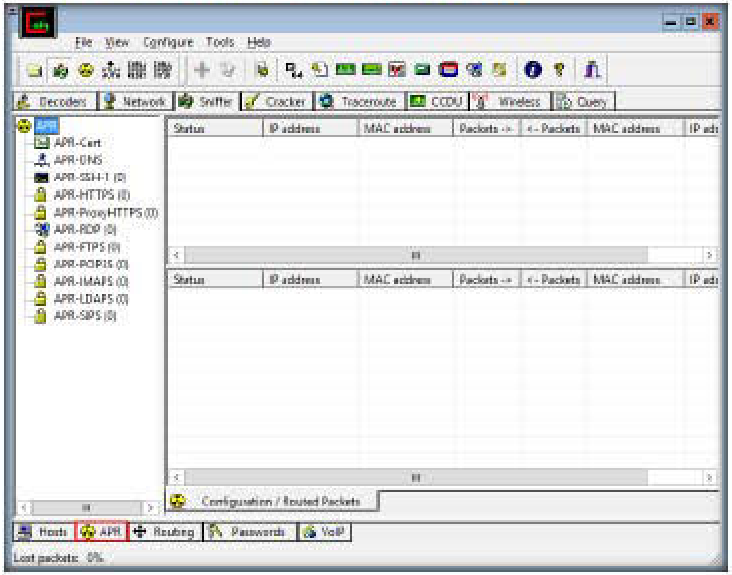

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP add
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

FIGURE 5.12: Cain & Abel ARP Tab

Note that Cain & Abel program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

19. Click anywhere on the top most section in the right pane to activate the **+** icon.

APR state Full-Routing means that the IP traffic between two hosts has been completely hijacked and APR is working in FULL-DUPLEX. (ex: Server<->Client). The sniffer will grab authentication information accordingly to the sniffer filters set.

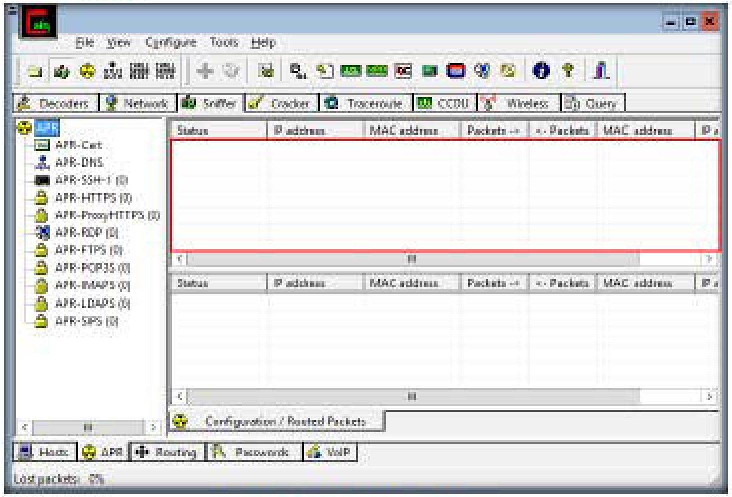
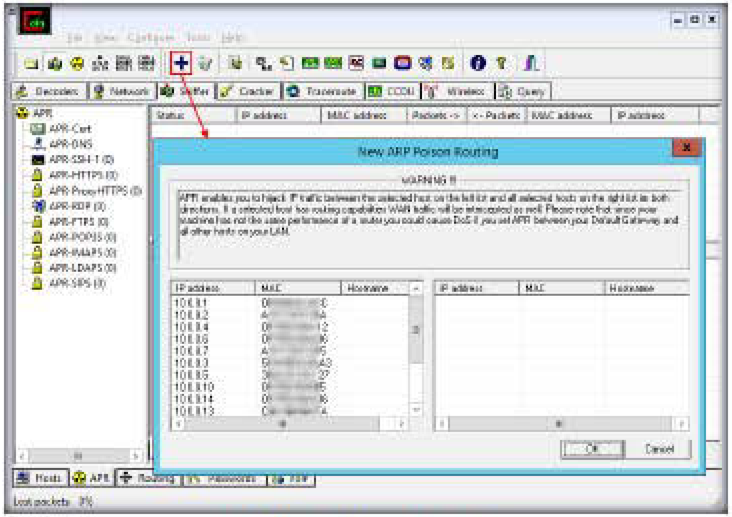

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP a
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

FIGURE 5.13: Cain & Abel Sniffer Section

20. Click the Plus (+) icon; the **New ARP Poison Routing** window opens, from which we can add IPs to listen to traffic.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Hosts APR Routing Passwords VoIP
Lost packets: 0%

New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.0.0.1	[redacted]	
10.0.0.2	[redacted]	
10.0.0.4	[redacted]	
10.0.0.6	[redacted]	
10.0.0.7	[redacted]	
10.0.0.3	[redacted]	
10.0.0.5	[redacted]	
10.0.0.10	[redacted]	
10.0.0.14	[redacted]	
10.0.0.13	[redacted]	

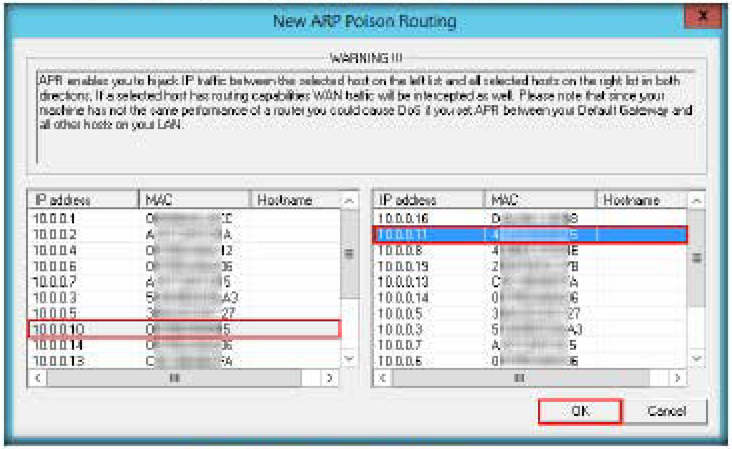
IP address	MAC	Hostname

OK Cancel

The Protected Store is a storage facility provided as part of Microsoft CryptoAPI. It's primarily use is to securely store private keys that have been issued to a user.

FIGURE 5.14: New ARP Poison Routing window

21. To monitor the traffic between two computers, select **10.0.0.10** (**Windows 8.1**) and **10.0.0.11** (**Windows Server 2008**). Click **OK**



New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.0.0.1	[redacted]	
10.0.0.2	[redacted]	
10.0.0.4	[redacted]	
10.0.0.6	[redacted]	
10.0.0.7	[redacted]	
10.0.0.3	[redacted]	
10.0.0.5	[redacted]	
10.0.0.10	[redacted]	
10.0.0.14	[redacted]	
10.0.0.13	[redacted]	

IP address	MAC	Hostname
10.0.0.16	[redacted]	
10.0.0.11	[redacted]	
10.0.0.8	[redacted]	
10.0.0.19	[redacted]	
10.0.0.13	[redacted]	
10.0.0.14	[redacted]	
10.0.0.5	[redacted]	
10.0.0.3	[redacted]	
10.0.0.7	[redacted]	
10.0.0.6	[redacted]	

OK Cancel

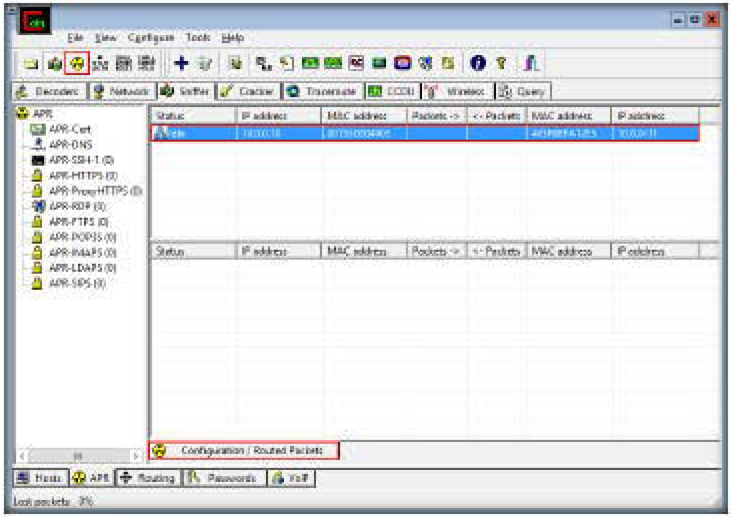
All of the information in the Protected Store is encrypted, using a key that is derived from the user's logon password. Access to the information is tightly regulated so that only the owner of the material can access it

FIGURE 5.15: Monitoring the traffic between two computers

22. Select the added IP address in the **Configuration/Routed** packets, and click **Start/Stop APR**.

Many Windows applications use this feature; Internet Explorer, Outlook and Outlook Express for example store user names and passwords using this service.

Note: If the **Couldn't bind HTTPS acceptor socket** pop-up appears, click **OK**.



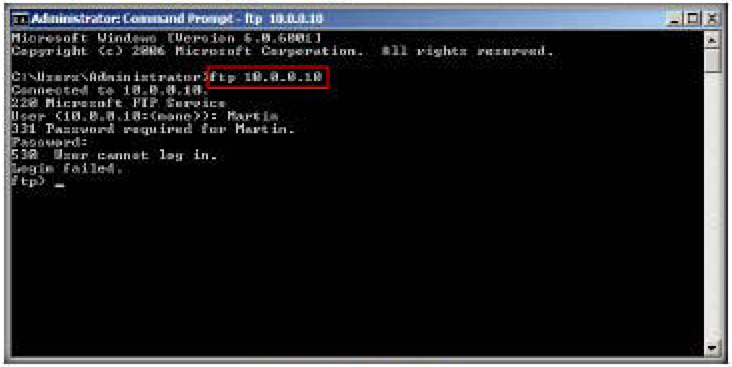
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.0.0.10	[illegible]			[illegible]	10.0.0.11

FIGURE 5.16: Cain & Abel ARP Poisoning

23. Now, launch command prompt in Windows Server 2008, and type **ftp 10.0.0.10** (IP address of Windows 8.1) and press **Enter**.

24. When prompted for a username, type "**Martin**" and press **Enter**; for a password, type "**apple**" and press **Enter**.

There is also another set used for credentials that should persist on the local machine only and cannot be used in roaming profiles, this is called "Local Credential Set" and it refers to the file \Documents and Settings\%Username%\Local Settings\Application Data\Microsoft\Credentials\%UserSID%\Credentials



Administrator: Command Prompt - ftp 10.0.0.10

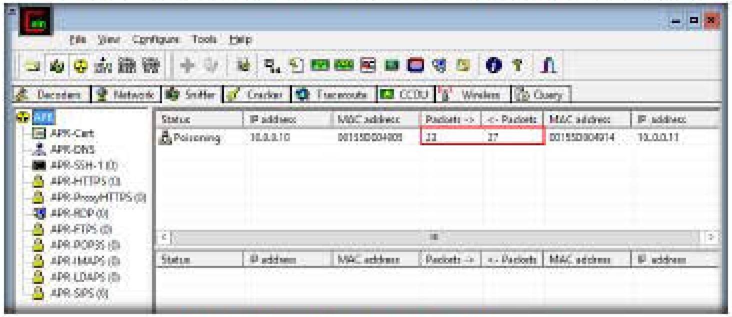
```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ftp 10.0.0.10
Connected to 10.0.0.10.
220 Microsoft FTP Service
User (10.0.0.10:(none)): Martin
331 Password required for Martin.
Password:
530 User cannot log in.
Login failed.
ftp> _
```

FIGURE 5.17: Start ftp://10.0.0.10

Note: Irrespective of a successful login (or even of login failure), Cain & Abel captures the password entered during login.

25. On the host machine, observe the tool listing some packet exchange.

Credentials are stored in the registry under the key HKEY_CURRENT_USER \Software\Microsoft\Protected Storage System Provider\.



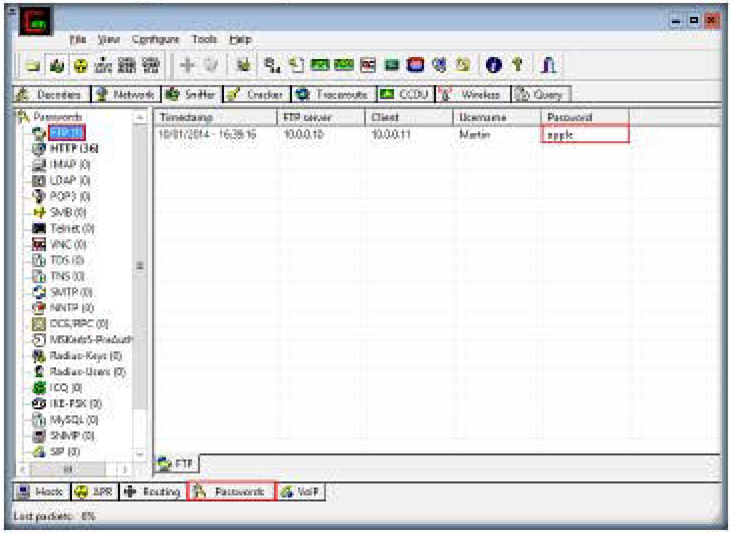
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.0.0.10	00155D004809	22	27	00155D004914	10.0.0.11

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

FIGURE 5.18: Sniffer window with more packets exchanged

26. Click the **Passwords** tab, as shown in the screenshot, to view the sniffed password for **ftp 10.0.0.10**.

This set of credentials is stored in the file \Documents and Settings\%Username%\Application Data\Microsoft\Credentials \%UserSID%\Credentials.



Timestamp	FTP server	Client	Username	Password
10/01/2014 - 16:38:16	10.0.0.10	10.0.0.11	Martin	apple

FIGURE 5.19: Passwords displayed in plain text

27. This way, an attacker can obtain passwords in clear text if the channel through which information is passing doesn't provide encryption.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and "exposure" through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab
6

Detecting Systems running in Promiscuous mode in a Network using PromqryUI

PromqryUI is a tool with a Windows GUI that can be used to detect network interfaces running in promiscuous mode.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

In an ARP storm attack, an attacker collects the IP and MAC addresses of network machines to use in later attacks. The attackers send ARP packets to a network; if an ARP packet with forged gateway MAC address is pushed to the LAN, all communications within the LAN may fail. This attack uses all resources of both victim and non-victim computers.

As a network administrator, you must always diagnose network traffic using a network analyzer and configure routers to prevent ARP flooding. Using a specific protocol analyzer technique, you should be able to identify the cause of any broadcast storm and a method for resolving it. Identify susceptible points in the network and protect them before attackers discover and exploit its vulnerabilities, especially in ARP-enabled LAN systems known for their security loopholes and thereby allow attackers to conduct various ARP attacks.

Attackers may also install network interfaces to run in promiscuous mode to capture all packets that pass over a network. As an Expert Ethical Hacker and Penetration Tester, you must be aware of tools for detecting network interfaces running in promiscuous mode that might be network sniffers. In this lab, you will learn to use PromqryUI to detect such network interfaces running in promiscuous mode.

Lab Objectives

The objective of this lab is:

- To detect promiscuous systems in a network

Lab Environment

To complete this lab, you will need:

- PromqryUI is located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Promiscuous Detection Tools\PromqryUI**
- You can also download the latest version of PromqryUI from http://www.microsoft.com/en-us/download/details.aspx?id=16883
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 (host machine)
- A computer running Windows Server 2008 on a virtual machine
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

Lab Duration

Time: 5 Minutes

Overview of PromqryUI

PromqryUI can accurately determine if a modern Windows system has network interfaces running in promiscuous mode. If so, this could indicate the presence of a network sniffer in the system.

PromqryUI cannot detect standalone sniffers or sniffers running on non-Windows operating systems.

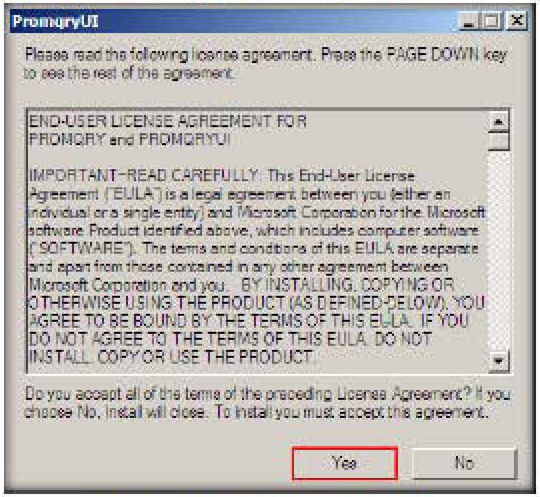
Lab Tasks

TASK 1

Extract PromqryUI

1. Log onto the **Windows Server 2008** virtual machine.
2. Navigate to **Z:\CEHv9 Module 07 Sniffing\Promiscuous Detection Tools\PromqryUI** and double-click **promqryui.exe**.
3. If the **Open File - Security Warning** pop-up appears, click **Run**.

4. Click **Yes** in the **PromqryUI License Agreement** window.



PromqryUI

Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.

END-USER LICENSE AGREEMENT FOR PROMQRY and PROMQRYUI

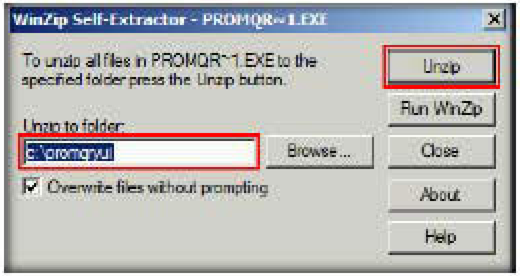
IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software Product identified above, which includes computer software ("SOFTWARE"). The terms and conditions of this EULA are separate and apart from those contained in any other agreement between Microsoft Corporation and you. BY INSTALLING, COPYING OR OTHERWISE USING THE PRODUCT (AS DEFINED BELOW), YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, DO NOT INSTALL, COPY OR USE THE PRODUCT.

Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.

FIGURE 6.1: PromqryUI - License Agreement dialog box

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

5. The **WinZip Self-Extractor** dialog box appears. Browse to a desired location (default is **c:\promqryui**) to save the unzipped folder, and click **Unzip**.



WinZip Self-Extractor - PROMQR~1.EXE

To unzip all files in PROMQR~1.EXE to the specified folder press the Unzip button.

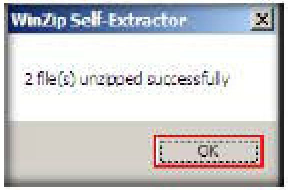
Unzip to folder: c:\promqryui

☑ Overwrite files without prompting

FIGURE 6.2: PromqryUI - WinZip Self-Extractor dialog box

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

6. The **WinZip Self-Extractor** pop-up appears; click **OK** to close it.



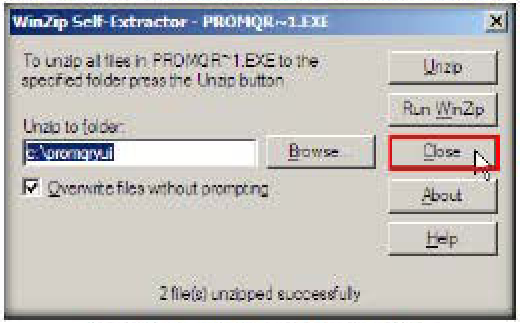
WinZip Self-Extractor

2 file(s) unzipped successfully

FIGURE 6.3: WinZip Self-Extractor dialog box

7. Now, click **Close** to close the **WinZip Self-Extractor** dialog box.

📁 Unzip to folder allows you to browse and select a destination of your choice to save the setup file.



WinZip Self-Extractor - PROMQR~1.EXE

To unzip all files in PROMQR~1.EXE to the specified folder press the Unzip button.

Unzip to folder: c:\promqryui

☑ Overwrite files without prompting

2 file(s) unzipped successfully

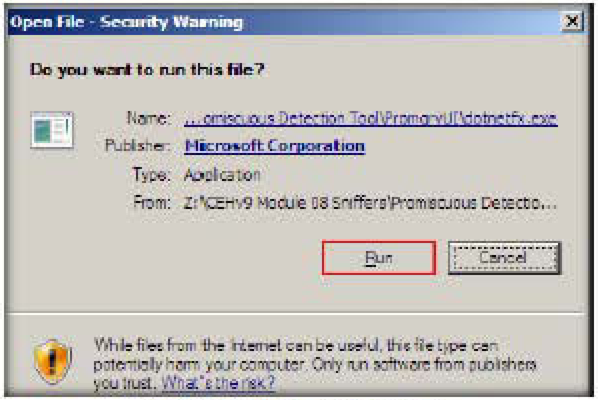
FIGURE 6.4: PromqryUI - WinZip Self-Extractor dialog box

8. Now, install **.NET Framework 1.1** by double-clicking **dotnetfx.exe**, located at **Z:\CEHv9 Module 07 Sniffing\Promiscuous Detection Tools\PromqryUI**.

TASK 2

Install .NET Framework 1.1

9. Click **Run**.



Open File - Security Warning

Do you want to run this file?

Name: ...omiscuous Detection Tool\PromqryUI\dotnetfx.exe

Publisher: Microsoft Corporation

Type: Application

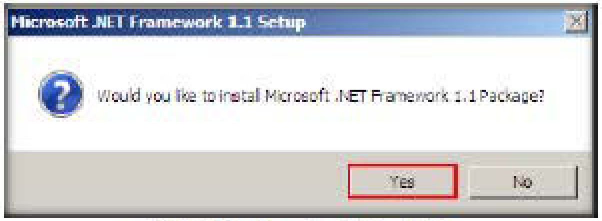
From: Z:\CEHv9 Module 08 Sniffers\Promiscuous Detectio...

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

FIGURE 6.5: Open File - Security Warning dialog box

10. Click **Yes** to initiate the .NET Framework installation.

📁 The .NET Framework version 1.1 redistributable package that includes everything you need to run applications developed using the .NET Framework.

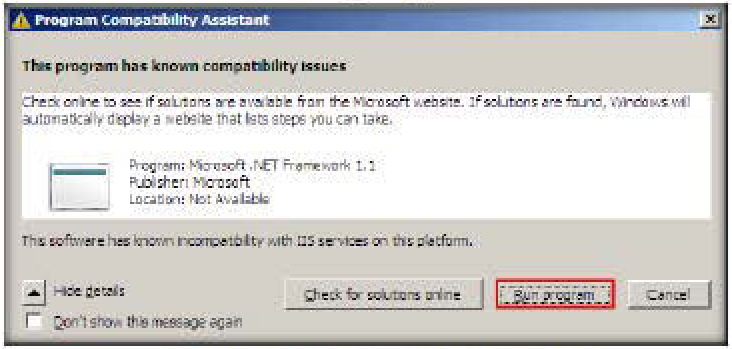


Microsoft .NET Framework 1.1 Setup

Would you like to install Microsoft .NET Framework 1.1 Package?

FIGURE 6.6: .NET Framework - Installation dialog box

11. While attempting to install .NET Framework 1.1, a **Program Compatibility Assistant** dialog box appears. Click **Run Program**.


Program Compatibility Assistant
Hide details
Don't show this message again
Check for solutions online
Run program
Cancel

This program has known compatibility issues

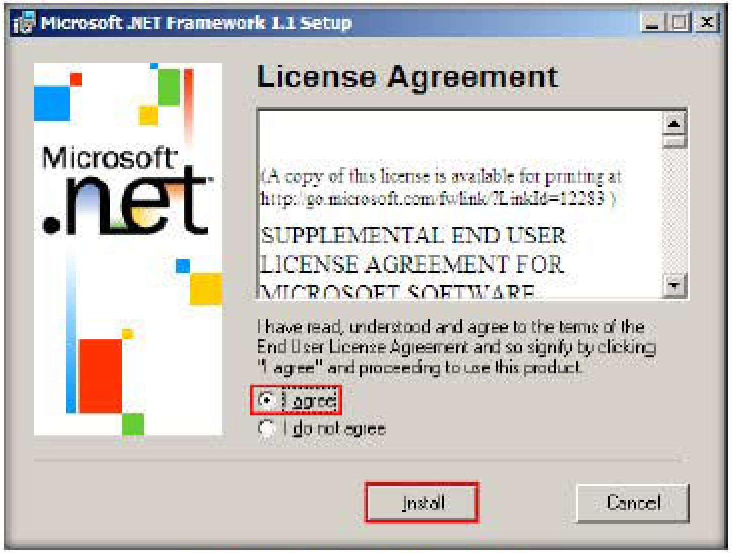
Check online to see if solutions are available from the Microsoft website. If solutions are found, Windows will automatically display a website that lists steps you can take.

Program: Microsoft .NET Framework 1.1
Publisher: Microsoft
Location: Not Available

This software has known incompatibility with IIS services on this platform.

FIGURE 6.7: .NET Framework - Program Compatibility Assistant dialog box

12. The **License Agreement** dialog box is displayed; select **I agree,** and click **Install**. Follow the wizard-driven installation steps to install **.NET Framework 1.1**.



(A copy of this license is available for printing at http://go.microsoft.com/fwlink/?LinkId=12283)

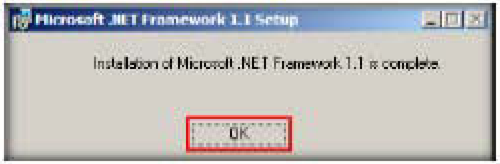
SUPPLEMENTAL END USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE

I have read, understood and agree to the terms of the End User License Agreement and so signify by clicking "I agree" and proceeding to use this product.

● I agree
○ I do not agree

FIGURE 6.8: .NET Framework - License Agreement dialog box

13. Once installation is complete, the **Microsoft .NET Framework 1.1 Setup** dialog box appears; click **OK**.


Microsoft .NET Framework 1.1 Setup

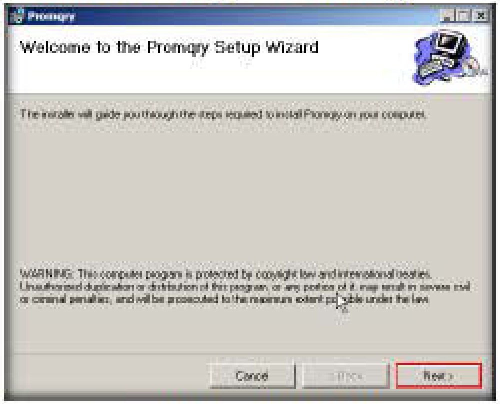
Installation of Microsoft .NET Framework 1.1 is complete.

FIGURE 6.9: .NET Framework – Installation complete message box

TASK 3

Install PromqryUI

14. Navigate to **C:\promqryui**, double-click **pqsetup.msi,** and follow the wizard-driven installation steps to install PromqryUI.


Promqry

Welcome to the Promqry Setup Wizard

The installer will guide you through the steps required to install Promqry on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

FIGURE 6.10: Promqryui installation wizard

Promiscuous mode can be used in a malicious way to sniff on a network. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this by using carefully designed firewall settings.

15. Once installation is complete, go to **Start → All Programs,** and click **Promqry** to launch it.

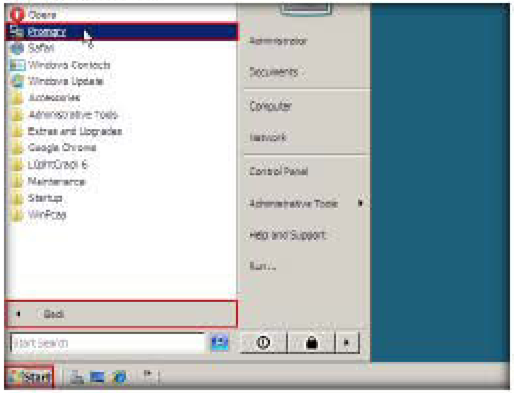
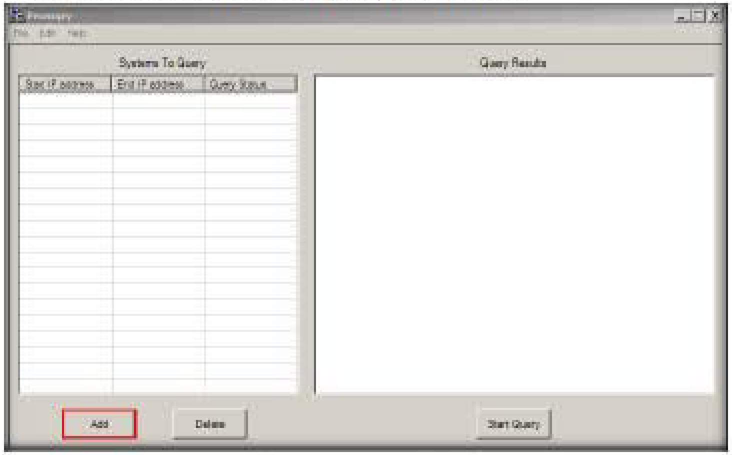


FIGURE 6.11: Windows 2008 Server - Start menu

16. The main window of Promqry appears. Click **Add**.



With the PromqryUI tool, you can add either a single system or multiple systems to query.

FIGURE 6.12: PromqryUI - Main window

17. The **Select Addition Type** dialog box appears; click **Add Single System**.

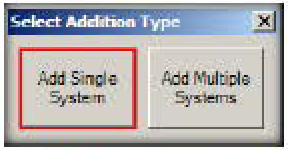
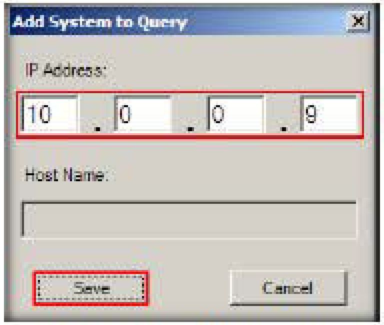


FIGURE 6.13: PromqryUI - Adding system

18. The **Add System to Query** dialog box appears; type the IP Address of the system you want to check in the **IP Address** field, and click **Save**.



IP Address: 10 . 0 . 0 . 9

Host Name:

For systems that you need to query, a range of IP addresses can be provided. Also, you can just carry a query for a local system.

FIGURE 6.14: PromqryUI - Add System to Query

Note: **10.0.0.9** is the IP address of the host machine (i.e., **Windows Server 2012**), which might differ in your lab environment.

19. Check the added IP Address in **Systems To Query** section, and click **Start Query**.

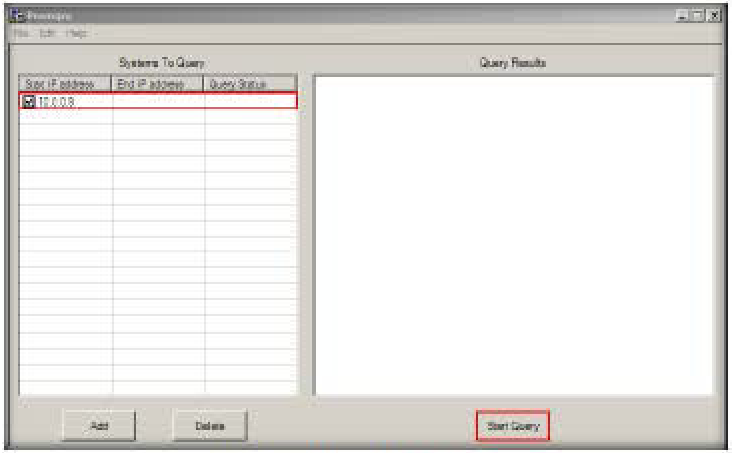
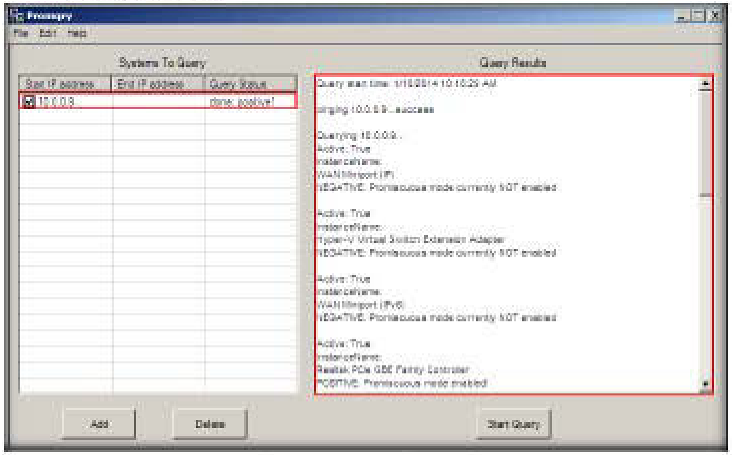


FIGURE 6.15: PromqryUI – Querying system

20. The results will be displayed in **Query Results**. Scroll down to analyze the complete results.



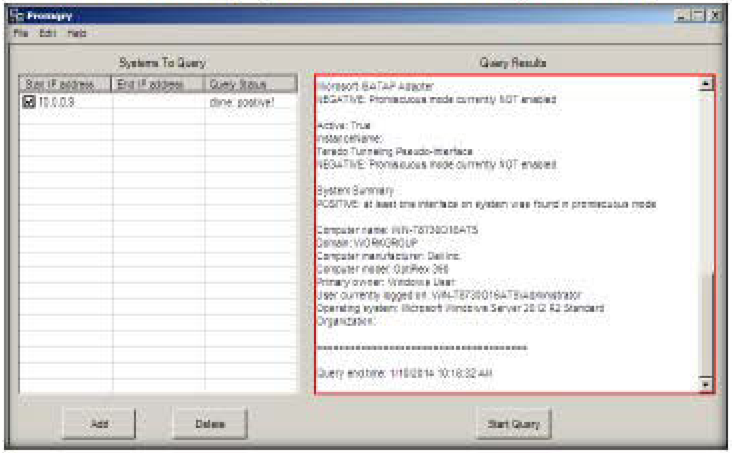
Start IP address	End IP address	Query Status
☑ 10.0.0.9		done: positive!

```
Query start time: 1/15/2014 10:10:29 AM

pinging 10.0.0.9...success

Querying 10.0.0.9...
Active: True
InstanceName:
WAN Miniport (IP)
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
Hyper-V Virtual Switch Extension Adapter
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
WAN Miniport (IPv6)
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
Realtek PCIe GBE Family Controller
POSITIVE: Promiscuous mode enabled!
```

Query results will let you know if the system is promiscuous mode or not and provides other information like Computer name, Domain, Computer Model, Manufacturer, Owner, and so on.

FIGURE 6.16: PromqryUI - Query Results

21. Scroll down the Query Results section to view the system summary.



Start IP address	End IP address	Query Status
☒ 10.0.0.9		done: positive!

```
Microsoft 6ATAP Adapter
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
Instancename:
Teredo Tunneling Pseudo-Interface
NEGATIVE: Promiscuous mode currently NOT enabled

System Summary
POSITIVE: at least one interface on system was found in promiscuous mode

Computer name: WIN-T873SO16AT5
Domain: WORKGROUP
Computer manufacturer: Dell Inc.
Computer model: OptiPlex 360
Primary owner: Windows User
User currently logged on: WIN-T873SO16AT5\Administrator
Operating system: Microsoft Windows Server 2012 R2 Standard
Organization:

****************************************

Query endtime: 1/10/2014 10:18:32 AM
```

FIGURE 6.17: PromqryUI - Query Results

22. This way, you can search for all the machines running in promiscuous mode, and block them from interacting with your machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab
7

Detecting ARP Poisoning in a Switch-Based Network

ARP spoofing is a technique by which attackers send Address Resolution Protocol messages onto a local area network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

ARP cache poisoning is a method of attacking a LAN network by updating the target computer's ARP cache with both a forged ARP request and reply packets in an effort to change the Layer 2 Ethernet MAC address (i.e., that of the network card) to one that the attacker can monitor. Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

You, as an ethical hacker and pen tester, must assess your organization or a target of evaluation for ARP poisoning vulnerabilities.

Lab Objectives

The objective of this lab is to help students understand how to:

- Perform ARP Poisoning on a switch based network
- Detect ARP Poisoning using Wireshark

Lab Environment

To perform this lab, you will need:

- A computer running with Windows Server 2012 as Host machine
- Kali Linux running as a virtual machine
- Windows 8.1 running as a virtual machine

Lab Duration

Time: 15 Minutes

Overview of ARP Poisoning

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an ARP request, it normally considers that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. Indeed, systems which haven't made an ARP request also accept the ARP reply coming from other devices.

Lab Tasks

Note: Launch the **Windows 8.1** and **Kali Linux** virtual machines before beginning this lab.

TASK 1

Install Cain & Abel

1. Switch to **Windows 8.1** machine, navigate to **Z:\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel**, double-click **ca_setup.exe**, and follow the wizard-driven installation steps to install Cain & Abel.

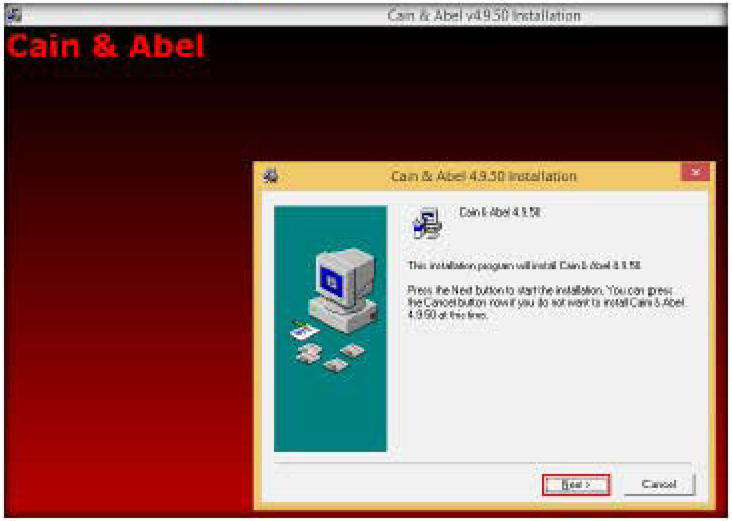
Note:

If a **User Account Control** pop-up appears, click **Yes**.

If a **Window Security** dialog-box appears, asking you to enter network credentials, type the following credentials and click **OK**:

User name: **Administrator**

Password: **qwerty@123**



Cain & Abel v4.9.50 Installation

Cain & Abel

Cain & Abel 4.9.50 Installation

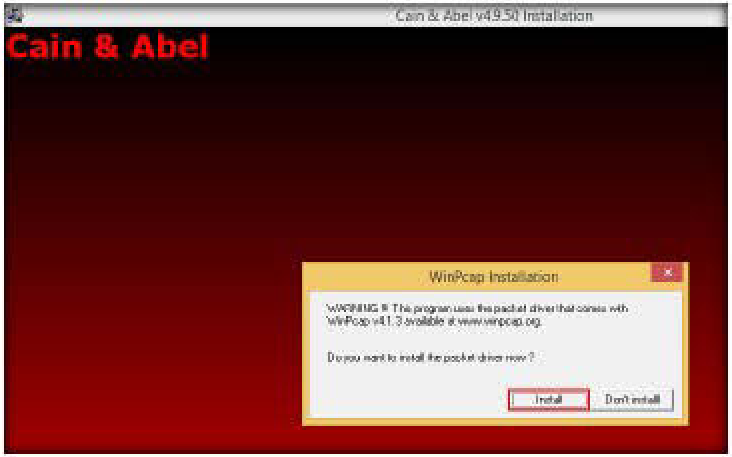
Cain & Abel 4.9.50

This installation program will install Cain & Abel 4.9.50.

Press the Next button to start the installation. You can press the Cancel button now if you do not want to install Cain & Abel 4.9.50 at this time.

FIGURE 7.1: Installing Cain & Abel

2. During installation, the **WinPcap Installation** pop-up appears; click **Install.**

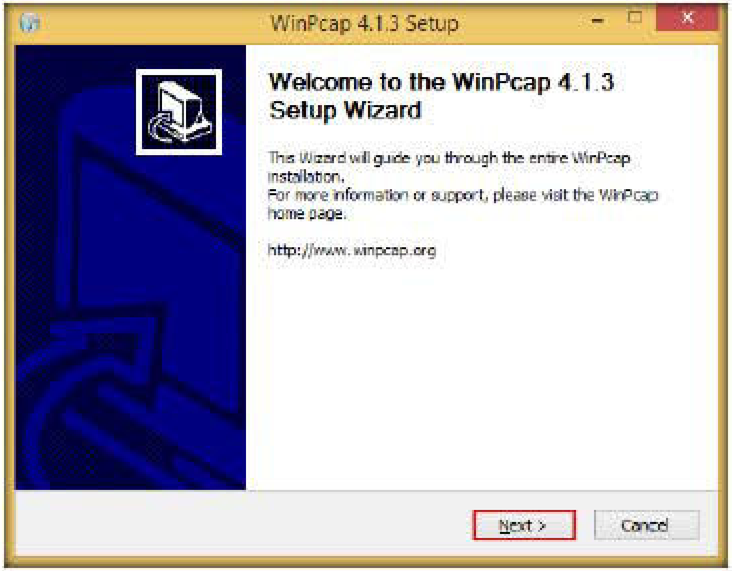


WARNING !! This program uses the packet driver that comes with WinPcap v4.1.3 available at www.winpcap.org.

Do you want to install the packet driver now ?

FIGURE 7.2: Installing WinPcap

3. Follow the wizard-driven installation steps to install WinPcap.



Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

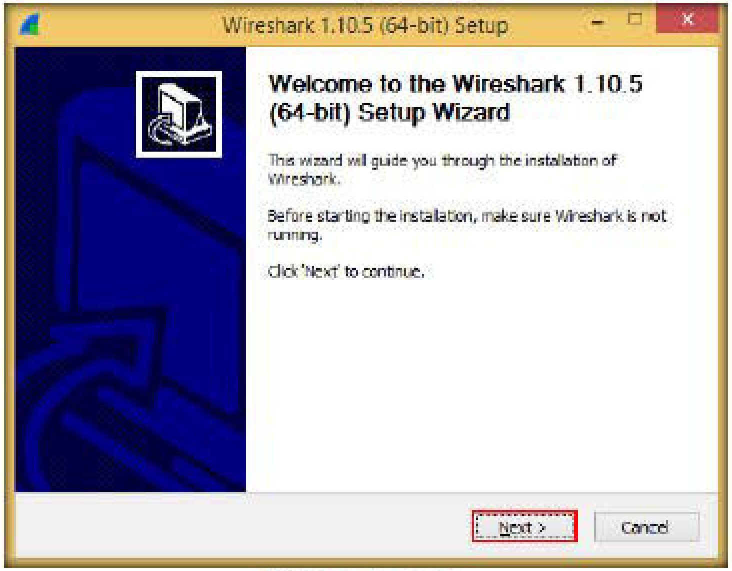
FIGURE 7.3: Installing WinPcap

TASK 2

Install Wireshark

4. Navigate to **Z:\CEHv9 Module 07 Sniffing\Sniffing Tools\Wireshark**, double-click **Wireshark-win64-1.10.5.exe**, and follow the wizard-driven installation steps to install the application.

Note: If the **User Account Control** pop-up appears, click **Yes**.



Wireshark 1.10.5 (64-bit) Setup

Welcome to the Wireshark 1.10.5 (64-bit) Setup Wizard

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

FIGURE 7.4: Installing Wireshark

TASK 3

Perform ARP Poisoning

5. Now, double-click **Cain** to launch it.

Note: If a **User Account Control** pop-up appears, click **Yes**.

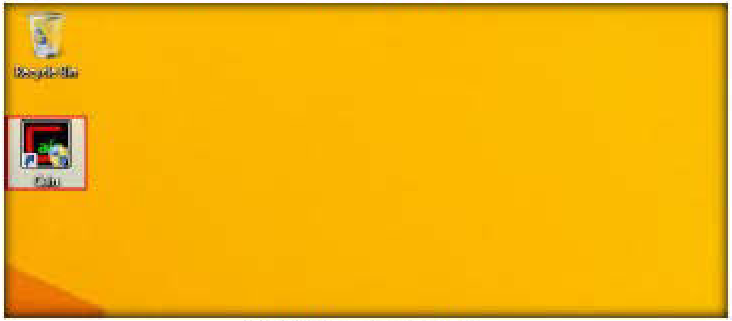


FIGURE 7.5: Launching Cain & Abel

6. The Cain window appears; click **Configure** in the menu bar.

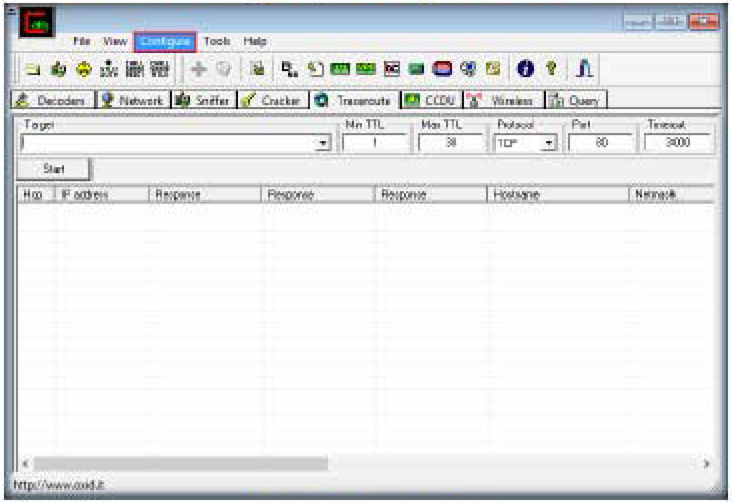
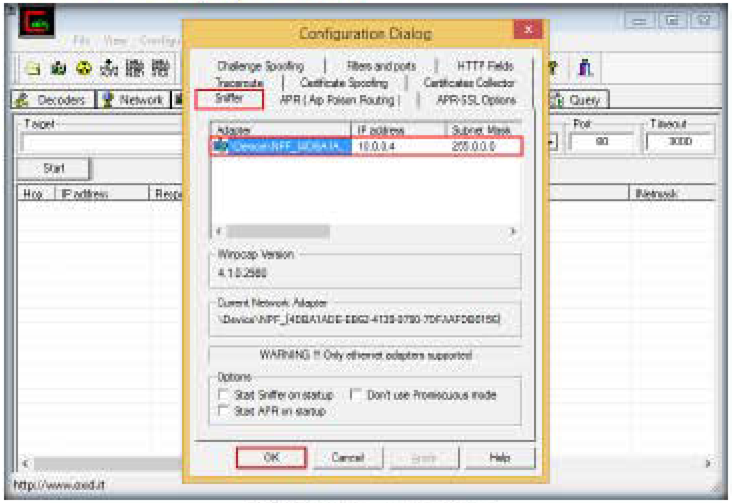


FIGURE 7.6: Configuring Cain & Abel

7. The **Configuration Dialog** window appears; click the **Sniffer** tab.

8. Select the adapter, and click **OK**.



Adapter	IP address	Subnet Mask
\Device\NPF_{4DBA1A...	10.0.0.4	255.0.0.0

Winpcap Version
4.1.0.2980

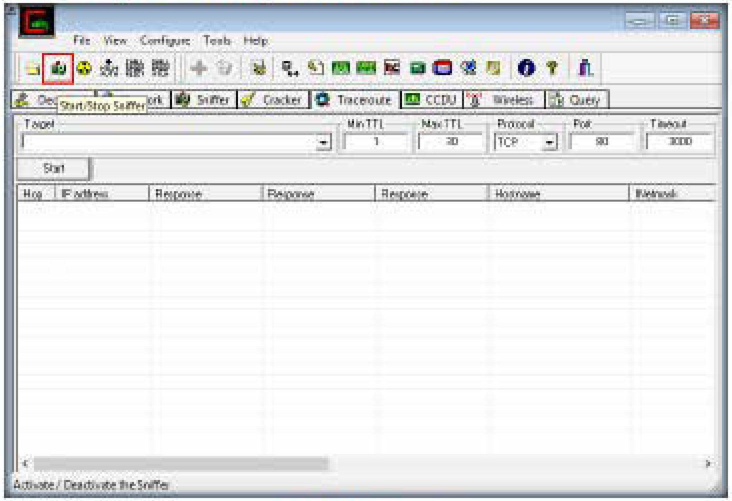
Current Network Adapter
\Device\NPF_{4DBA1ADE-EB62-4139-9780-7DFAAFDB0150}

WARNING !!! Only ethernet adapters supported

Options
□ Start Sniffer on startup □ Don't use Promiscuous mode
□ Start APR on startup

FIGURE 7.7: Configuring Cain & Abel

9. Now, click **Start/Stop Sniffer** in the toolbar.


File View Configure Tools Help
Start/Stop Sniffer
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Start

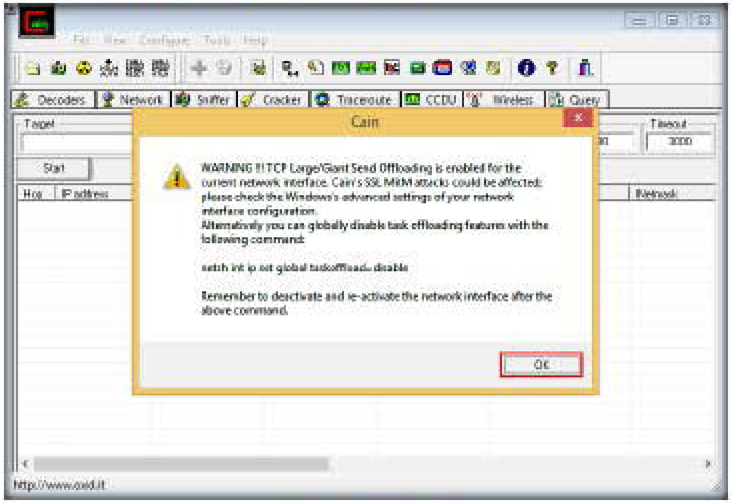
Target
Min TTL 1
Max TTL 30
Protocol TCP
Port 80
Timeout 3000

Hop	IP address	Response	Response	Response	Hostname	Netmask

Activate / Deactivate the Sniffer

FIGURE 7.8: Starting Sniffer

10. If the **Cain** pop-up appears, click **OK**.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Target
Timeout
Start
Hop IP address
Netmask
Cain
OK

WARNING !! TCP Large/Giant Send Offloading is enabled for the current network interface. Cain's SSL MITM attacks could be affected: please check the Windows's advanced settings of your network interface configuration.
Alternatively you can globally disable task offloading features with the following command:

```
netsh int ip set global taskoffload= disable
```

Remember to deactivate and re-activate the network interface after the above command.

http://www.oxid.it

FIGURE 7.9: Cain Pop-Up

11. Click the **Sniffer** tab.

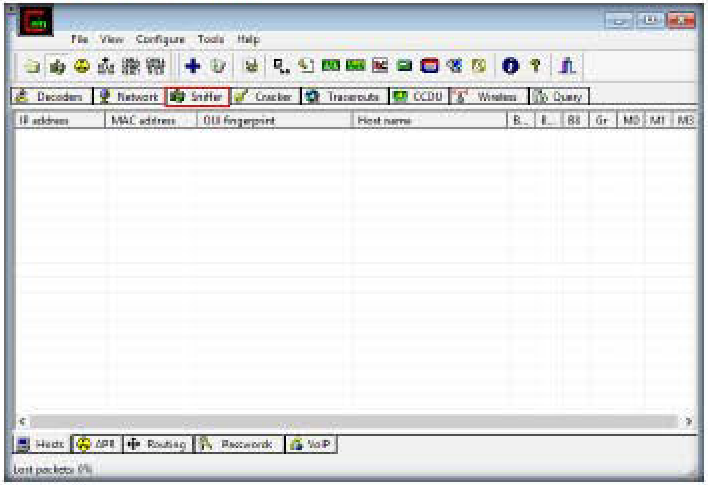


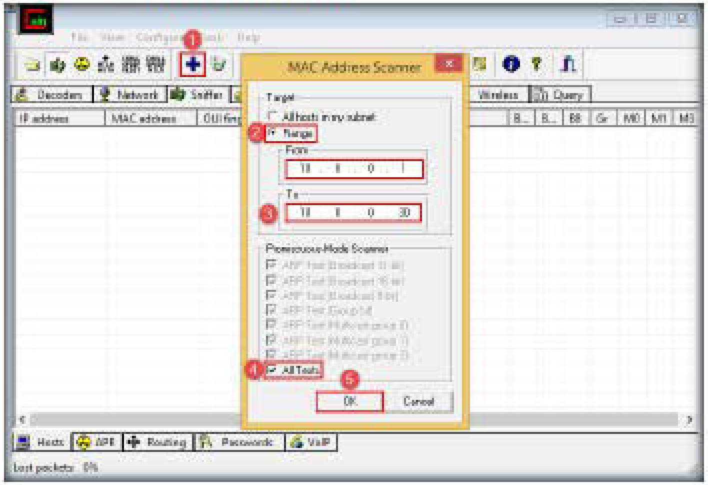
FIGURE 7.10: Clicking Sniffer Tab

12. Click **+** in the toolbar.

13. The **MAC Address Scanner** window appears; click **Range**.

14. Specify the IP address range you want to scan (here, **10.0.0.1-10.0.0.30**, which might differ in your lab environment).

15. Check **All Tests,** and click **OK**.



MAC Address Scanner

Target

○ All hosts in my subnet

● Range

From: 10 . 0 . 0 . 1

To: 10 . 0 . 0 . 30

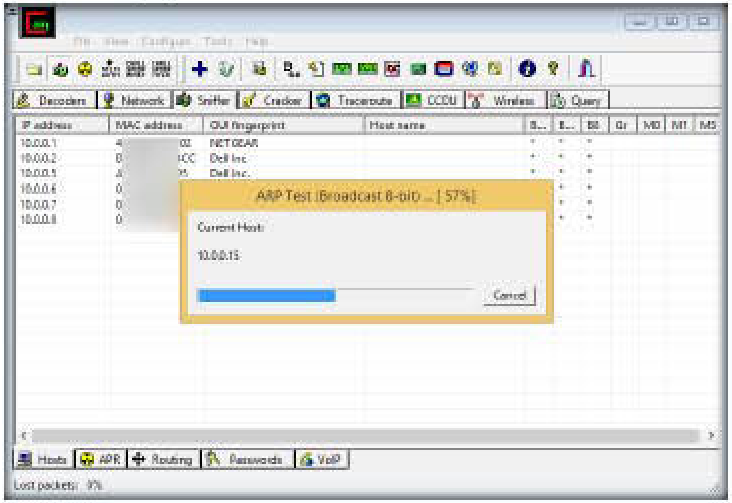
Promiscuous-Mode Scanner

☑ ARP Test (Broadcast 31-bit)
☑ ARP Test (Broadcast 16-bit)
☑ ARP Test (Broadcast 8-bit)
☑ ARP Test (Group bit)
☑ ARP Test (Multicast group 0)
☑ ARP Test (Multicast group 1)
☑ ARP Test (Multicast group 3)
☑ All Tests

OK Cancel

FIGURE 7.11: Scanning MAC Addresses

16. The application begins to perform ARP tests on the IP address range and displays it in the Sniffer window, as shown in the screenshot:



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M5
10.0.0.1	[redacted]	NETGEAR		*	*	*				
10.0.0.2	[redacted]	Dell Inc.		*	*	*				
10.0.0.5	[redacted]	Dell Inc.		*	*	*				
10.0.0.6	[redacted]				*	*				
10.0.0.7	[redacted]				*	*				
10.0.0.8	[redacted]				*	*				

ARP Test (Broadcast 8-bit) ... [57%]

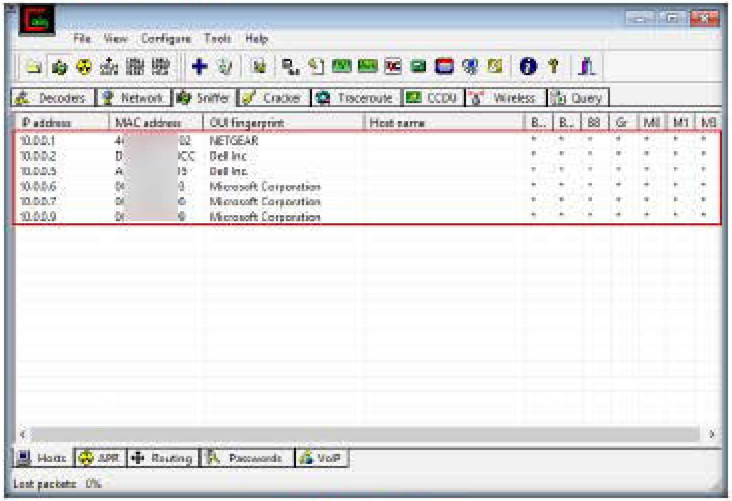
Current Host:

10.0.0.15

Cancel

FIGURE 7.12: Scanning MAC Addresses

17. On completing the ARP tests, all the MAC and their associated IP addresses that responded to the ARP requests are displayed, as shown in the screenshot:



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M5
10.0.0.1	[redacted]	NETGEAR		*	*	*	*	*	*	*
10.0.0.2	[redacted]	Dell Inc.		*	*	*	*	*	*	*
10.0.0.5	[redacted]	Dell Inc.		*	*	*	*	*	*	*
10.0.0.6	[redacted]	Microsoft Corporation		*	*	*	*	*	*	*
10.0.0.7	[redacted]	Microsoft Corporation		*	*	*	*	*	*	*
10.0.0.9	[redacted]	Microsoft Corporation		*	*	*	*	*	*	*

FIGURE 7.13: Sniffer Tab

18. Now, click the **APR** tab.

19. Click anywhere on the topmost section (in the right pane) to activate the **+** icon.

20. Once the **+** icon is activated, click it.

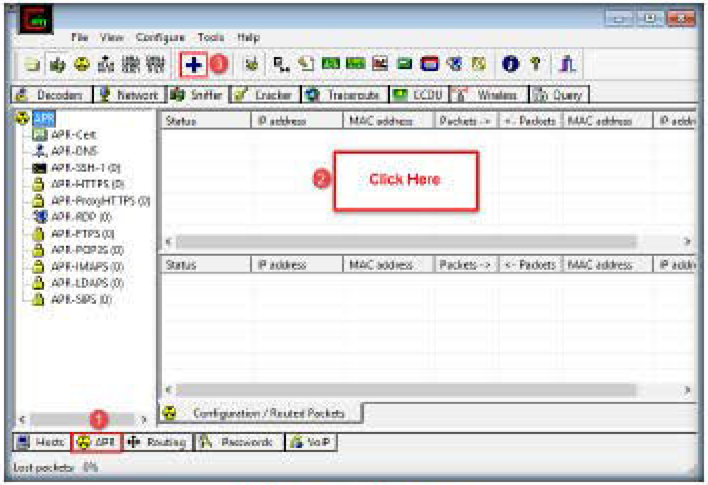
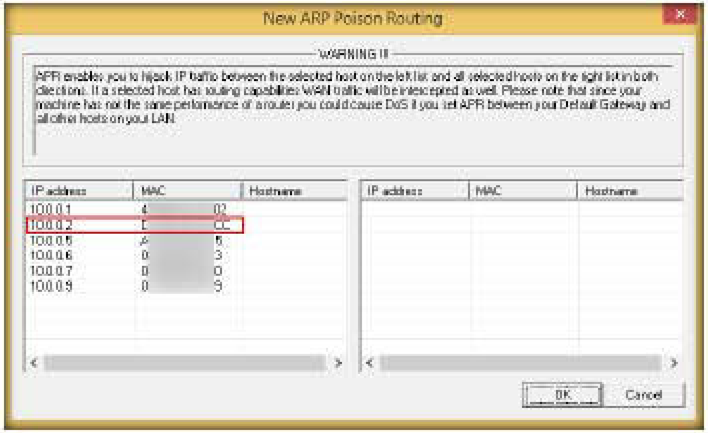


FIGURE 7.14: ARP Poison Routing

21. The **New ARP Poison Routing** window appears. Now, you need to select the machines between which you want to intercept traffic.

22. Select the first target (here, **10.0.0.2,** the **Windows Server 2012** machine) from the list of IP addresses displayed in the left pane.


New ARP Poison Routing

WARNING !!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

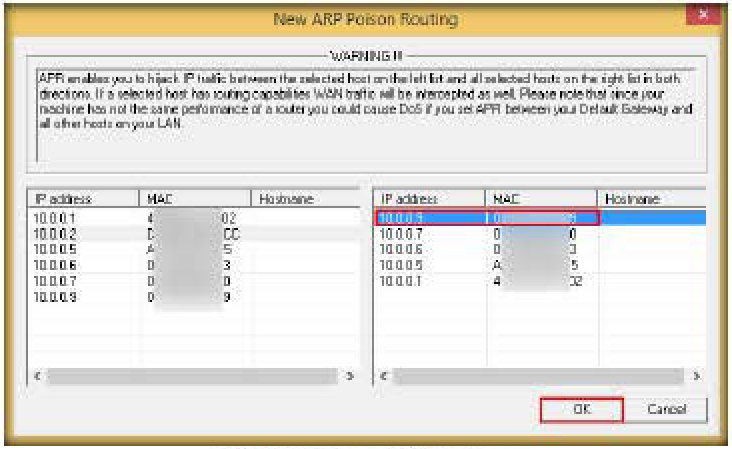
IP address	MAC	Hostname
10.0.0.1	4[redacted]02	
10.0.0.2	[redacted]CC	
10.0.0.5	A[redacted]5	
10.0.0.6	0[redacted]3	
10.0.0.7	0[redacted]0	
10.0.0.9	0[redacted]9	

IP address	MAC	Hostname

FIGURE 7.15: New ARP Poison Routing Window

23. Upon selecting the first target, a list of IP addresses excluding the first target appears in the right pane.

24. You need to select the second target IP address (here, **10.0.0.9, the Kali Linux** machine) from the right-pane. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.



New ARP Poison Routing

WARNING !!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

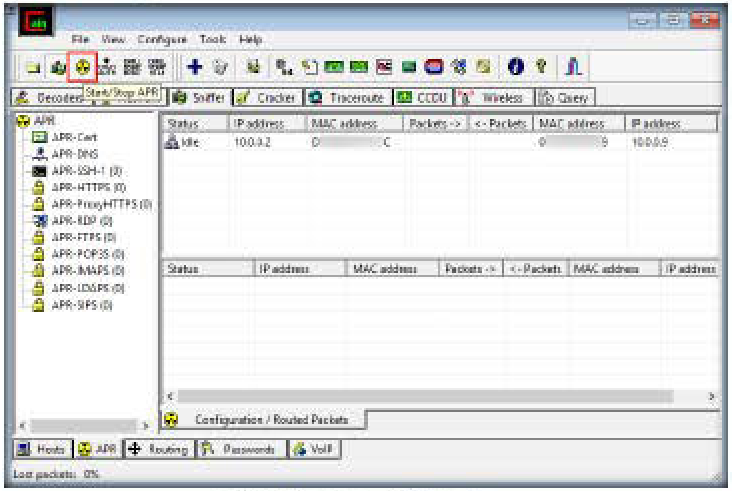
IP address	MAC	Hostname
10.0.0.1	4[redacted]02	
10.0.0.2	D[redacted]CC	
10.0.0.5	A[redacted]5	
10.0.0.6	0[redacted]3	
10.0.0.7	0[redacted]0	
10.0.0.9	0[redacted]9	

IP address	MAC	Hostname
10.0.0.9	0[redacted]9	
10.0.0.7	0[redacted]0	
10.0.0.6	0[redacted]3	
10.0.0.5	A[redacted]5	
10.0.0.1	4[redacted]02	

FIGURE 7.16: Performing ARP Poison Routing

25. Once complete, the selected targets appear in the top section.

26. Now, click the **Start/Stop APR** button to initiate the ARP Poison Routing attack.

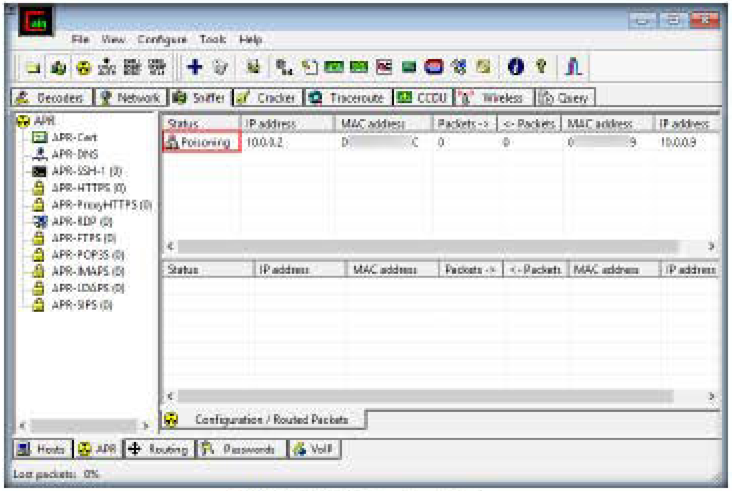


Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.0.0.2	D[redacted]C			0[redacted]9	10.0.0.9

Lost packets: 0%

FIGURE 7.17: Performing ARP Poison Routing

27. The status of the attack changes to **Poisoning**, as shown in the screenshot:


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.0.0.2	D[redacted]C	0	0	0[redacted]9	10.0.0.9

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

FIGURE 7.18: ARP Poison Routing Begun

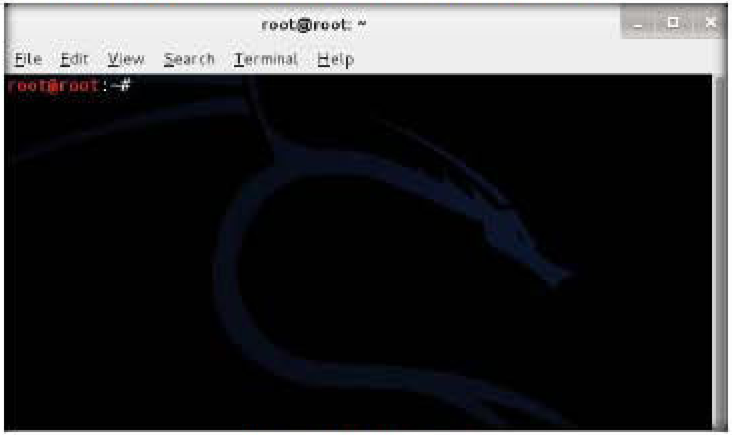
28. Cain & Abel is intercepting the traffic traversing between these two machines.

29. To generate traffic between the machines, you need to ping one target machine using the other.

TASK 4

Ping Windows 8.1 Machine

30. Switch to Kali Linux, and launch a command-line terminal.

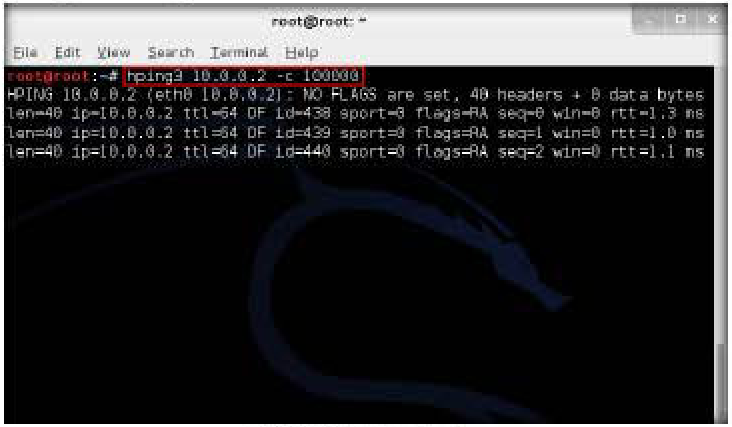


```
root@root:~#
```

FIGURE 7.19: Command Line Terminal

31. Type **hping3 [IP address of Windows Server 2012] -c 100000** and press **Enter** to ping Windows Server 2012 with 100000 packets.

Note: In this lab, the IP address of Windows Server 2012 is 10.0.0.2, which might differ in your lab environment.



```
root@root:~# hping3 10.0.0.2 -c 100000
HPING 10.0.0.2 (eth0 10.0.0.2): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=10.0.0.2 ttl=64 DF id=438 sport=0 flags=RA seq=0 win=0 rtt=1.3 ms
len=40 ip=10.0.0.2 ttl=64 DF id=439 sport=0 flags=RA seq=1 win=0 rtt=1.0 ms
len=40 ip=10.0.0.2 ttl=64 DF id=440 sport=0 flags=RA seq=2 win=0 rtt=1.1 ms
```

FIGURE 7.20: Performing Flooding

TASK 5

Detect ARP Poisoning/ IP Address Spoofing

32. Now, immediately switch to **Windows 8.1** machine, go to the **Apps** screen, and click **Wireshark** to launch it.

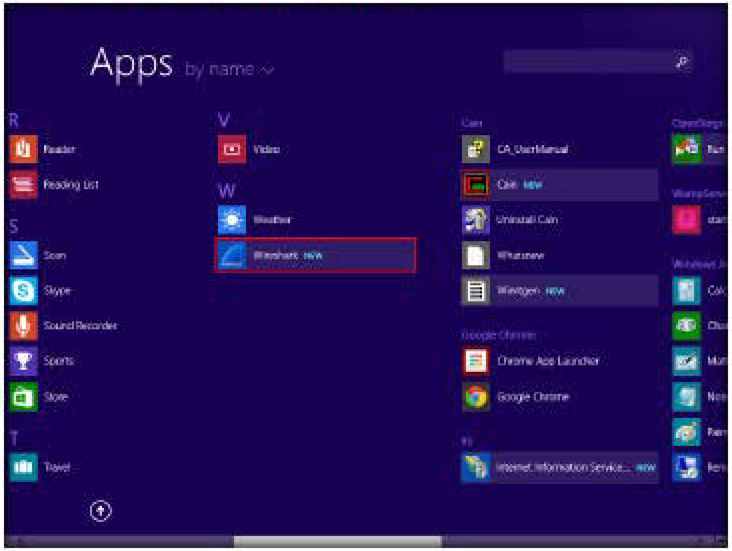


FIGURE 7.21: Launching Wireshark

33. The **Wireshark** main window appears; click **Edit** in the menu bar, and select **Preferences...**

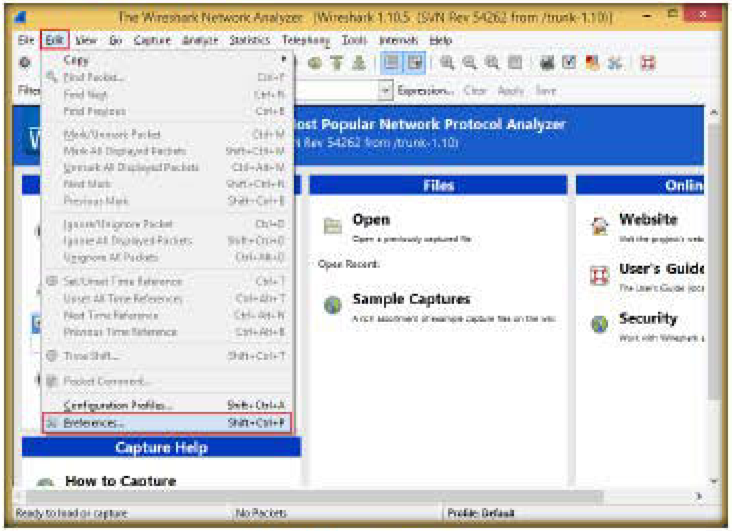
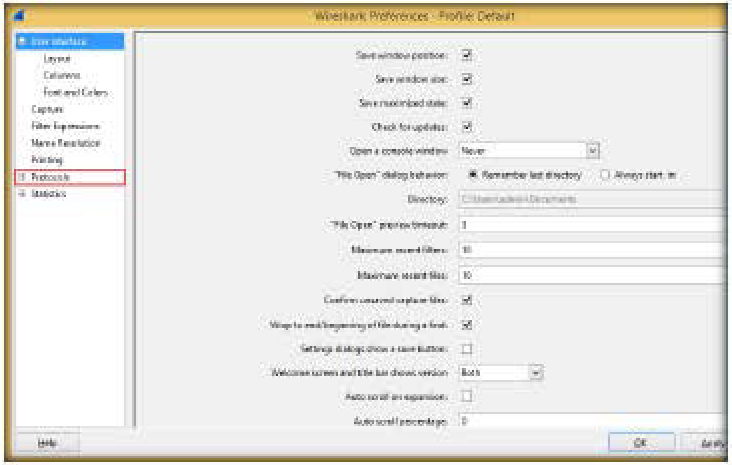

The Wireshark Network Analyzer [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Packets Shift+Ctrl+M
Unmark All Displayed Packets Ctrl+Alt+M
Next Mark Shift+Ctrl+N
Previous Mark Shift+Ctrl+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Packets Shift+Ctrl+D
Unignore All Packets Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Shift+Ctrl+T
Packet Comment...
Configuration Profiles... Shift+Ctrl+A
Preferences... Shift+Ctrl+P
Expression... Clear Apply Save
...ost Popular Network Protocol Analyzer
...Rev 54262 from /trunk-1.10)
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Onlin
Website
User's Guide
Security
Capture Help
How to Capture
Ready to load or capture
No Packets
Profile: Default

FIGURE 7.22: Launching Preferences

34. The **Wireshark Preferences** window appears; expand the **Protocols** node.



Save window position: ☑

Save window size: ☑

Save maximized state: ☑

Check for updates: ☑

Open a console window: Never

"File Open" dialog behavior: ● Remember last directory ○ Always start in:

Directory: C:\Users\admin\Documents

"File Open" preview timeout: 3

Maximum recent filters: 10

Maximum recent files: 10

Confirm unsaved capture files: ☑

Wrap to end/beginning of file during a find: ☑

Settings dialogs show a save button: □

Welcome screen and title bar shows version: Both

Auto scroll on expansion: □

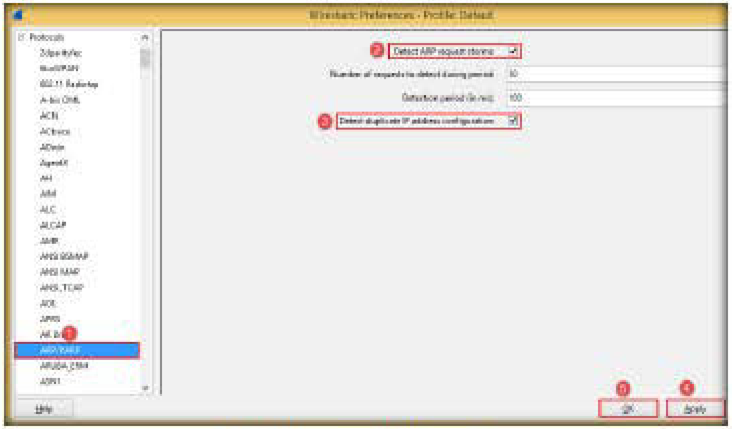
Auto scroll percentage: 0

FIGURE 7.23: Viewing Protocols

35. Select the **ARP/RARP** node.

36. Ensure that **Detect ARP request storms** and **Detect duplicate IP address configuration** are checked.

37. Click **Apply**, and then click **OK**.



Detect ARP request storms ☑

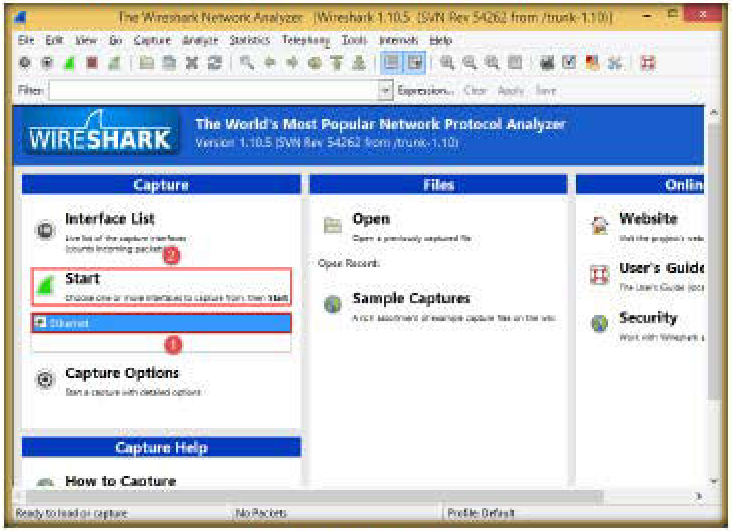
Number of requests to detect during period: 30

Detection period (in ms): 100

Detect duplicate IP address configuration ☑

FIGURE 7.24: Configuring ARP Detection Settings

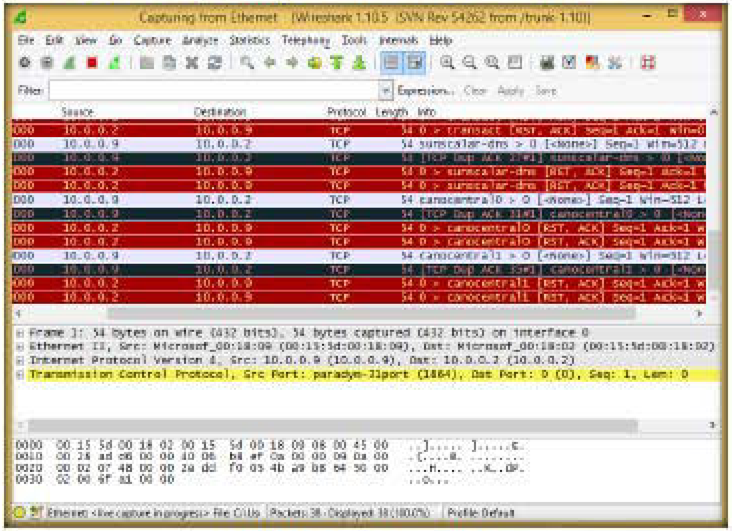
38. Now, select the interface associated with your network, then click **Start**.



The Wireshark Network Analyzer [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.5 (SVN Rev 54262 from /trunk-1.10)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Ethernet
1
2
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

FIGURE 7.25: Starting Capture

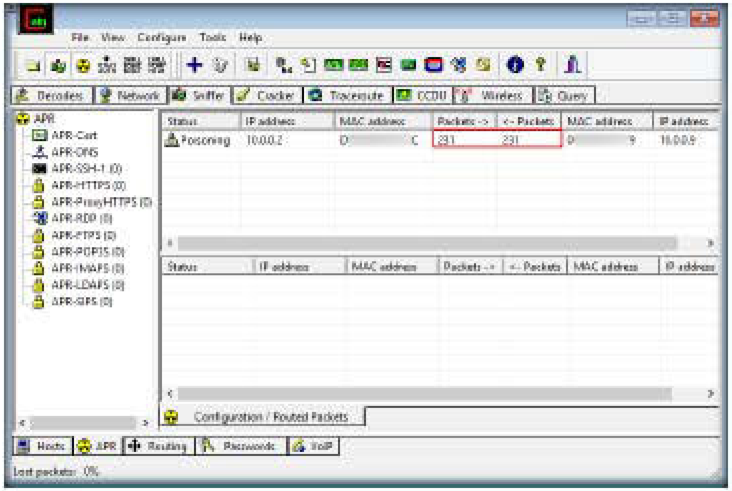
39. Wireshark begins to capture traffic between the two machines.


Capturing from Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
      Source       Destination    Protocol Length  Info
000   10.0.0.2     10.0.0.9       TCP      54 0 > transact [RST, ACK] Seq=1 Ack=1 Win=0
000   10.0.0.9     10.0.0.2       TCP      54 sunscalar-dns > 0 [<None>] Seq=1 Win=512 
000   10.0.0.9     10.0.0.2       TCP      54 [TCP Dup ACK 27#1] sunscalar-dns > 0 [<Non
000   10.0.0.2     10.0.0.9       TCP      54 0 > sunscalar-dns [RST, ACK] Seq=1 Ack=1 
000   10.0.0.2     10.0.0.9       TCP      54 0 > sunscalar-dns [RST, ACK] Seq=1 Ack=1 
000   10.0.0.9     10.0.0.2       TCP      54 canocentral0 > 0 [<None>] Seq=1 Win=512 L
000   10.0.0.9     10.0.0.2       TCP      54 [TCP Dup ACK 31#1] canocentral0 > 0 [<Non
000   10.0.0.2     10.0.0.9       TCP      54 0 > canocentral0 [RST, ACK] Seq=1 Ack=1 W
000   10.0.0.2     10.0.0.9       TCP      54 0 > canocentral0 [RST, ACK] Seq=1 Ack=1 W
000   10.0.0.9     10.0.0.2       TCP      54 canocentral1 > 0 [<None>] Seq=1 Win=512 L
000   10.0.0.9     10.0.0.2       TCP      54 [TCP Dup ACK 35#1] canocentral1 > 0 [<Non
000   10.0.0.2     10.0.0.9       TCP      54 0 > canocentral1 [RST, ACK] Seq=1 Ack=1 W
000   10.0.0.2     10.0.0.9       TCP      54 0 > canocentral1 [RST, ACK] Seq=1 Ack=1 W

⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Microsof_00:18:09 (00:15:5d:00:18:09), Dst: Microsof_00:18:02 (00:15:5d:00:18:02)
⊞ Internet Protocol Version 4, Src: 10.0.0.9 (10.0.0.9), Dst: 10.0.0.2 (10.0.0.2)
⊞ Transmission Control Protocol, Src Port: paradym-31port (1864), Dst Port: 0 (0), Seq: 1, Len: 0

0000  00 15 5d 00 18 02 00 15  5d 00 18 09 08 00 45 00   ..]..... ].....E.
0010  00 28 ad e6 00 00 40 06  b4 ef 0a 00 00 09 0a 00   .(....@. ........
0020  00 02 07 48 00 00 2a dd  f0 03 4b a9 b8 64 50 00   ...H.... ..K..dP.
0030  02 00 6f a1 00 00                                  ..o...

Ethernet: <live capture in progress> File: C:\Us | Packets: 38 · Displayed: 38 (100.0%) | Profile: Default
```

FIGURE 7.26: Wireshark Capturing Packets

40. Switch to Cain & Abel to observe the packets flowing between the two machines.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP

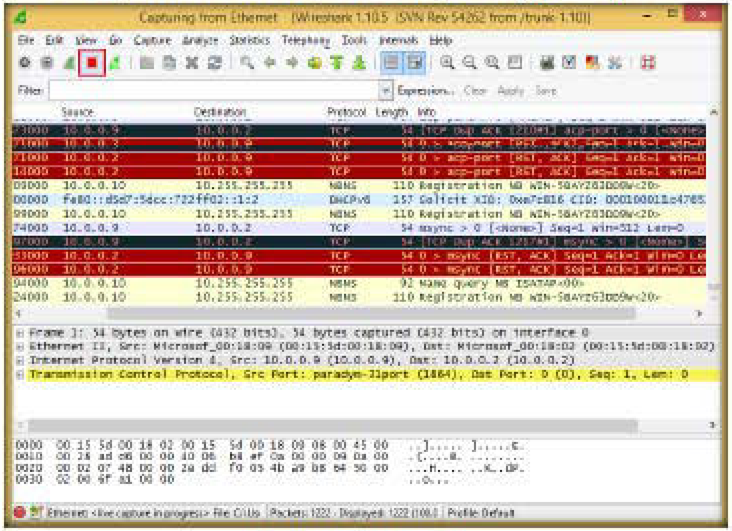
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.0.0.2	0 [redacted] C	231	231	0 [redacted] 9	10.0.0.9

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

Lost packets: 0%

FIGURE 7.27: ARP Poisoning Detected

41. Now, switch to **Wireshark,** and click **Stop** to stop packet capture.

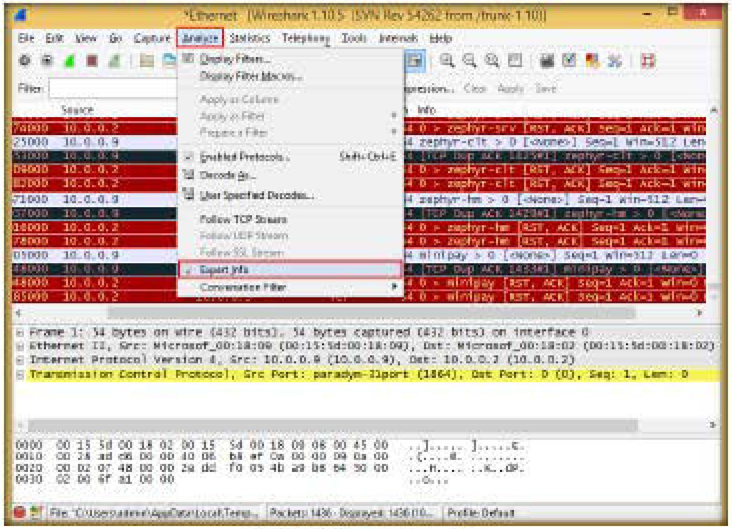

Capturing from Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Source Destination Protocol Length Info

```
23000  10.0.0.9              10.0.0.2          TCP      54 [TCP Dup ACK 1210#1] acp-port > 0 [<None>
71000  10.0.0.2              10.0.0.9          TCP      54 0 > acp-port [RST, ACK] Seq=1 Ack=1 Win=0
71000  10.0.0.2              10.0.0.9          TCP      54 0 > acp-port [RST, ACK] Seq=1 Ack=1 Win=0
14000  10.0.0.2              10.0.0.9          TCP      54 0 > acp-port [RST, ACK] Seq=1 Ack=1 Win=0
09000  10.0.0.10             10.255.255.255    NBNS    110 Registration NB WIN-5BAYZ63DD9W<20>
00000  fe80::d5d7:5dcc:722ff02::1:2            DHCPv6  157 Solicit XID: 0xa7e816 CID: 000100011c4765
99000  10.0.0.10             10.255.255.255    NBNS    110 Registration NB WIN-5BAYZ63DD9W<20>
74000  10.0.0.9              10.0.0.2          TCP      54 msync > 0 [<None>] Seq=1 Win=512 Len=0
97000  10.0.0.9              10.0.0.2          TCP      54 [TCP Dup ACK 1257#1] msync > 0 [<None>] S
53000  10.0.0.2              10.0.0.9          TCP      54 0 > msync [RST, ACK] Seq=1 Ack=1 Win=0 Le
96000  10.0.0.2              10.0.0.9          TCP      54 0 > msync [RST, ACK] Seq=1 Ack=1 Win=0 Le
94000  10.0.0.10             10.255.255.255    NBNS     92 Name query NB ISATAP<00>
24000  10.0.0.10             10.255.255.255    NBNS    110 Registration NB WIN-5BAYZ63DD9W<20>

⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Microsof_00:18:09 (00:15:5d:00:18:09), Dst: Microsof_00:18:02 (00:15:5d:00:18:02)
⊞ Internet Protocol Version 4, Src: 10.0.0.9 (10.0.0.9), Dst: 10.0.0.2 (10.0.0.2)
⊞ Transmission Control Protocol, Src Port: paradym-31port (1864), Dst Port: 0 (0), Seq: 1, Len: 0

0000  00 15 5d 00 18 02 00 15  5d 00 18 09 08 00 45 00   ..]..... ].....E.
0010  00 28 ad c6 00 00 40 06  b8 ef 0a 00 00 09 0a 00   .(....@. ........
0020  00 02 07 48 00 00 2a dd  f0 03 4b a9 b8 64 50 00   ...H.... ..K..dP.
0030  02 00 6f a1 00 00                                  ..o...
```

Ethernet: <live capture in progress> File: C:\Us
Packets: 1222 · Displayed: 1222 (100.0
Profile: Default

FIGURE 7.28: Stopping Packet Capture

42. Click **Analyze** in the menu bar, and select **Expert Info**.

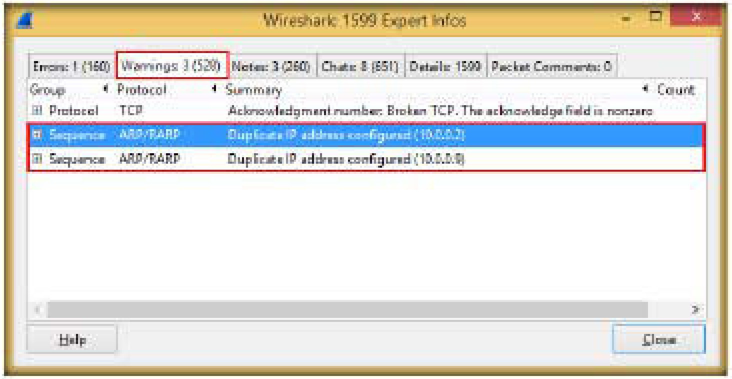

*Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Source
Info
Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Enabled Protocols... Shift+Ctrl+E
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info
Conversation Filter

```
74000  10.0.0.2   4 0 > zephyr-srv [RST, ACK] Seq=1 Ack=1 Win
25000  10.0.0.9   4 zephyr-clt > 0 [<None>] Seq=1 Win=512 Len
53000  10.0.0.9   4 [TCP Dup ACK 1425#1] zephyr-clt > 0 [<None
09000  10.0.0.2   4 0 > zephyr-clt [RST, ACK] Seq=1 Ack=1 Win
82000  10.0.0.2   4 0 > zephyr-clt [RST, ACK] Seq=1 Ack=1 Win
71000  10.0.0.9   4 zephyr-hm > 0 [<None>] Seq=1 Win=512 Len=
37000  10.0.0.9   4 [TCP Dup ACK 1429#1] zephyr-hm > 0 [<None
16000  10.0.0.2   4 0 > zephyr-hm [RST, ACK] Seq=1 Ack=1 Win=
78000  10.0.0.2   4 0 > zephyr-hm [RST, ACK] Seq=1 Ack=1 Win=
05000  10.0.0.9   4 minipay > 0 [<None>] Seq=1 Win=512 Len=0
48000  10.0.0.9   4 [TCP Dup ACK 1433#1] minipay > 0 [<None>]
48000  10.0.0.2   4 0 > minipay [RST, ACK] Seq=1 Ack=1 Win=0
85000  10.0.0.2   4 0 > minipay [RST, ACK] Seq=1 Ack=1 Win=0

⊞ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Microsof_00:18:09 (00:15:5d:00:18:09), Dst: Microsof_00:18:02 (00:15:5d:00:18:02)
⊞ Internet Protocol Version 4, Src: 10.0.0.9 (10.0.0.9), Dst: 10.0.0.2 (10.0.0.2)
⊞ Transmission Control Protocol, Src Port: paradym-31port (1864), Dst Port: 0 (0), Seq: 1, Len: 0

0000  00 15 5d 00 18 02 00 15  5d 00 18 09 08 00 45 00   ..]..... ].....E.
0010  00 28 ad c6 00 00 40 06  b8 ef 0a 00 00 09 0a 00   .(....@. ........
0020  00 02 07 48 00 00 2a dd  f0 03 4b a9 b8 64 50 00   ...H.... ..K..dP.
0030  02 00 6f a1 00 00                                  ..o...
```

File: "C:\Users\admin\AppData\Local\Temp\...
Packets: 1436 · Displayed: 1436 (10...
Profile: Default

FIGURE 7.29: Analyzing Expert Info

43. The **Expert Infos** window appears; click the **Warnings** tab. Duplicate IP addresses have been configured, using ARP protocol, as shown in the screenshot:



Wireshark 1599 Expert Infos

Errors: 1 (160) | Warnings: 3 (528) | Notes: 3 (260) | Chats: 8 (851) | Details: 1599 | Packet Comments: 0

Group	Protocol	Summary	Count
Protocol	TCP	Acknowledgment number: Broken TCP. The acknowledge field is nonzero	
Sequence	ARP/RARP	Duplicate IP address configured (10.0.0.2)	
Sequence	ARP/RARP	Duplicate IP address configured (10.0.0.9)	

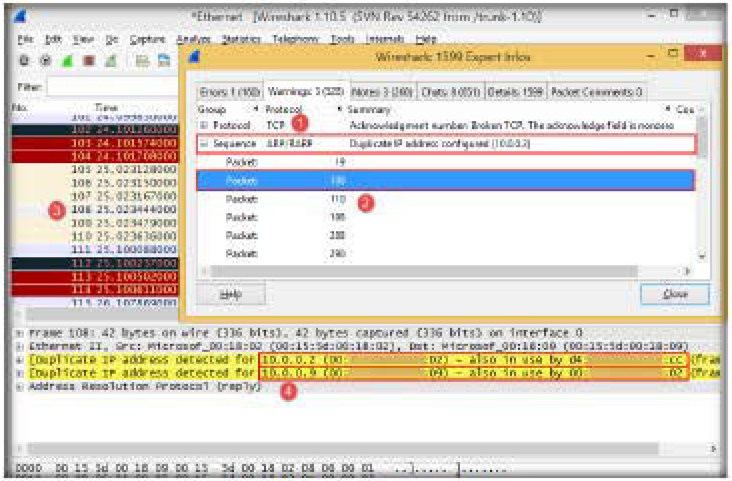
FIGURE 7.30: Viewing Warnings

44. Keep the **Expert Infos** window above the **Wireshark** window, so you can view the **packet** number and the **Packet details** section.

45. Expand a **Sequence** node, and select a packet (here, **108**).

46. On selecting the packet number, Wireshark highlights the packet, and its associated information is displayed under Packet Details.

47. Observe the warnings highlighted in yellow, as shown in the screenshot:



*Ethernet [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
1
2
3
4

Wireshark 1599 Expert Infos

Errors: 1 (160) | Warnings: 3 (528) | Notes: 3 (260) | Chats: 8 (851) | Details: 1599 | Packet Comments: 0

Group	Protocol	Summary
Protocol	TCP	Acknowledgment number: Broken TCP. The acknowledge field is nonzero
Sequence	ARP/RARP	Duplicate IP address configured (10.0.0.2)
Packet:	19	
Packet:	108	
Packet:	110	
Packet:	198	
Packet:	208	
Packet:	290	

```
Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Microsof_00:18:02 (00:15:5d:00:18:02), Dst: Microsof_00:18:09 (00:15:5d:00:18:09)
[Duplicate IP address detected for 10.0.0.2 (00:            :02) - also in use by 04:            :cc (Fram
[Duplicate IP address detected for 10.0.0.9 (00:            :09) - also in use by 00:            :02 (Fram
Address Resolution Protocol (reply)

0000  00 15 5d 00 18 09 00 15  5d 00 18 02 08 06 00 01   ..]..... ].......
```

FIGURE 7.31: Duplicate IP Address Detected

48. The yellow warnings indicate that duplicate IP addresses have been detected at one MAC address.

49. One MAC address corresponds to the attacker machine (Windows 8.1) and the other to the target machine.

50. Thus, ARP spoofing has been successfully detected using Wireshark.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 8

Detecting ARP Attacks with XArp Tool

XArp is a security application that uses advanced techniques to detect ARP-based attacks.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

ARP attacks go undetected by firewalls; hence, in this lab you will be guided to use XArp tool, which has advanced techniques for preventing such attacks and protecting data.

Lab Objectives

The objective of this lab is:

- To detect ARP attacks

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 07 Sniffing

Lab Environment

To complete this lab, you will need:

- XArp is located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Spoofing Detection Tools\XArp**
- You can also download the latest version of XArp from http://www.chrismc.de/development/xarp/index.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of XArp

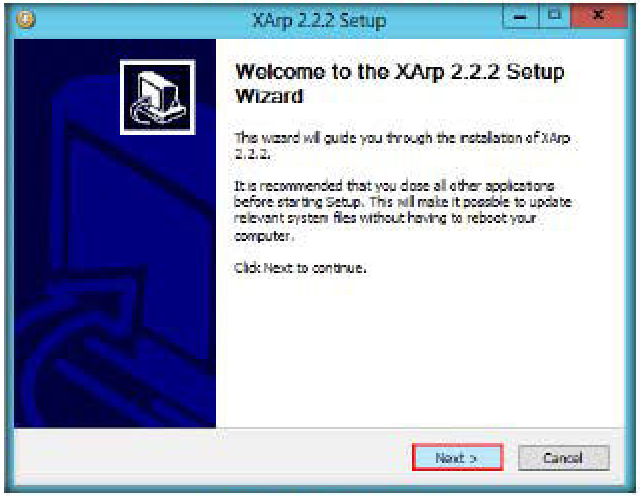
XArp helps users detect ARP attacks and keep their data private. Administrators can use XArp to monitor whole subnets for such attacks. Different security levels and fine-tuning possibilities allow typical and power users to use XArp to detect ARP attacks.

Lab Tasks

TASK 1

Launching the XArp tool

1. Navigate to **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Spoofing Detection Tools\XArp,** and double-click **xarp-2.2.2-win.exe**.
2. The **Open File - Security Warning** appears; click **Run**.
3. Follow the wizard-driven installation steps to install XArp.



XArp 2.2.2 Setup

Welcome to the XArp 2.2.2 Setup Wizard

This wizard will guide you through the installation of XArp 2.2.2.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

FIGURE 8.1: XArp Installation Wizard

4. On completing the installation, launch XArp from the Apps screen.

Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

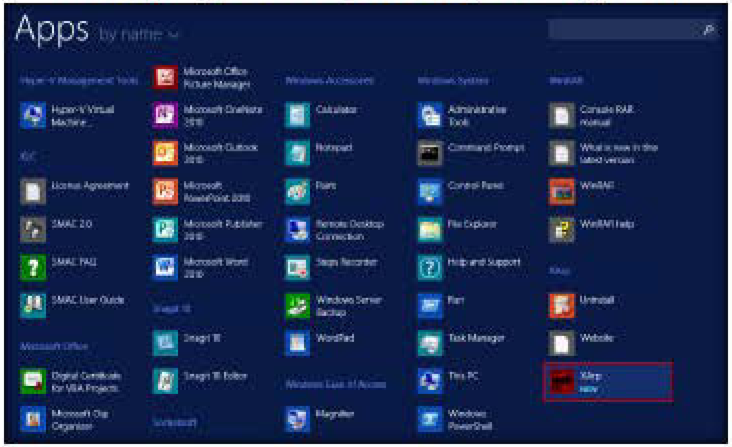
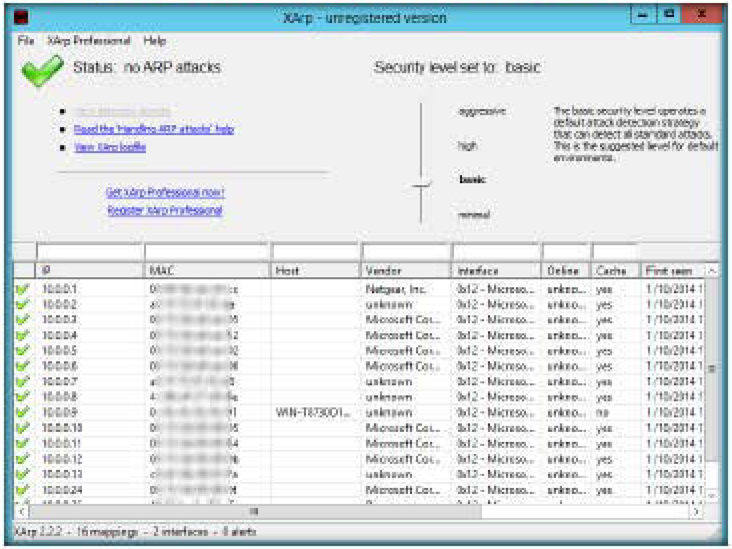


FIGURE 8.2: Windows Server 2012 - Apps

5. The main window of XArp appears, displaying a list of IPs, MAC addresses, and other information for machines in the network.

A MAC address is a unique identifier for network nodes on a LAN. MAC addresses are associated to network adapter that connects devices to networks. The MAC address is critical to locating networked hardware devices because it ensures that data packets go to the correct place. ARP tables, or cache, are used to correlate network devices' IP addresses to their MAC addresses.


XArp - unregistered version
File
XArp Professional
Help
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

Status: no ARP attacks

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.

IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
10.0.0.1	[redacted]		Netgear, Inc.	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.2	[redacted]		unknown	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.3	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.4	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.5	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.6	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.7	[redacted]		unknown	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.8	[redacted]		unknown	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.9	[redacted]	WIN-T8730O1...	unknown	0x12 - Microso...	unkno...	no	1/10/2014 1
10.0.0.10	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.11	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.12	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.13	[redacted]		unknown	0x12 - Microso...	unkno...	yes	1/10/2014 1
10.0.0.24	[redacted]		Microsoft Cor...	0x12 - Microso...	unkno...	yes	1/10/2014 1

XArp 2.2.2 - 16 mappings - 2 interfaces - 0 alerts

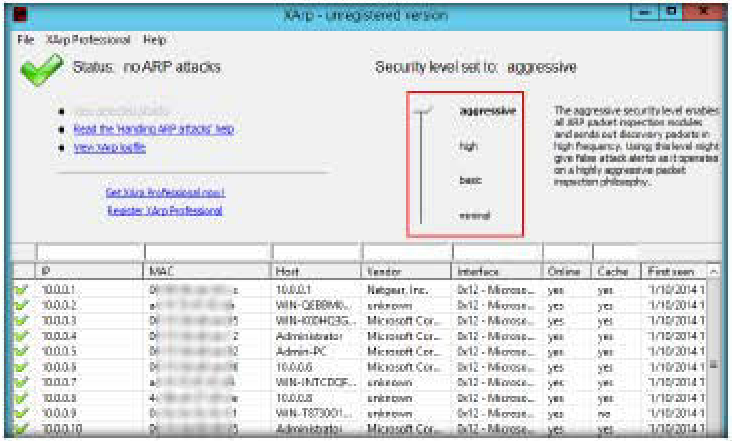
FIGURE 8.3: XArp status when security level set to high

6. On the host machine, XArp displays **no ARP attacks**.

Note: If you observe these results, log onto a virtual machine. You can run Cain & Abel to initiate ARP Poisoning of the host machine.

7. By default, the Security level is set to **basic**; set it to **aggressive**.

An attacker can alter the MAC address of the device that is used to connect the network to Internet and can disable access to the web and other external networks.


XArp - unregistered version
File XArp Professional Help
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

Status: no ARP attacks

Security level set to: aggressive

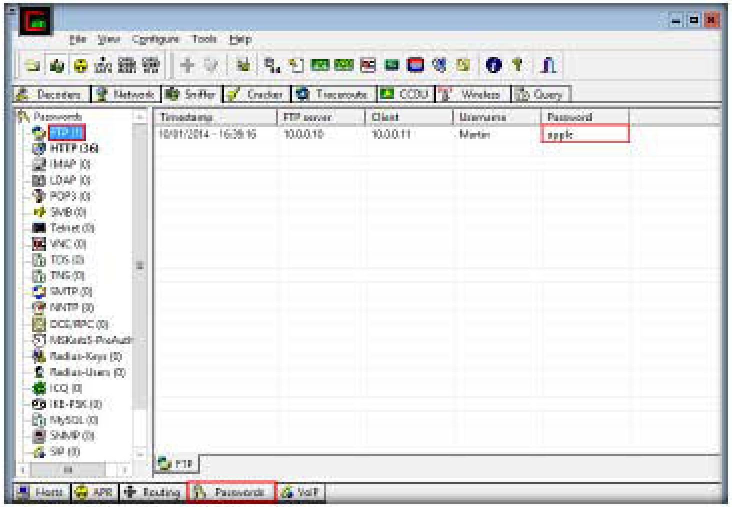
The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
✓	10.0.0.1	[redacted]	10.0.0.1	Netgear, Inc.	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.2	[redacted]	WIN-QEBBMK...	unknown	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.3	[redacted]	WIN-K0DHG3G...	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.4	[redacted]	Administrator	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.5	[redacted]	Admin-PC	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.6	[redacted]	10.0.0.6	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.7	[redacted]	WIN-INTCDGF...	unknown	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.8	[redacted]	10.0.0.8	unknown	0x12 - Microso...	yes	yes	1/10/2014 1
✓	10.0.0.9	[redacted]	WIN-T873O01...	unknown	0x12 - Microso...	yes	no	1/10/2014 1
✓	10.0.0.10	[redacted]	Administrator	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 1

FIGURE 8.4: XArp status when security level set to aggressive

8. Log onto the Windows Server 2008 and Windows 8.1 virtual machines.

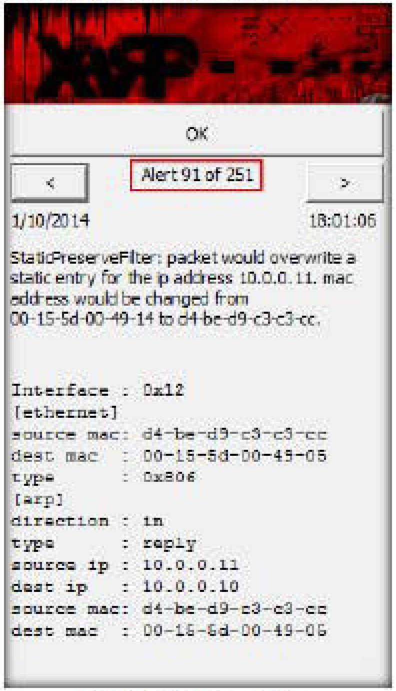
9. Perform ARP poisoning using Cain & Abel.



Timestamp	FTP server	Client	Username	Password
10/01/2014 - 16:38:16	10.0.0.10	10.0.0.11	Martin	apple

FIGURE 8.5: ARP poisoning using Cain & Abel

10. The XArp pop-up appears, displaying the Alerts.



1/10/2014 18:01:06

StaticPreserveFilter: packet would overwrite a static entry for the ip address 10.0.0.11. mac address would be changed from 00-15-5d-00-49-14 to d4-be-d9-c3-c3-cc.

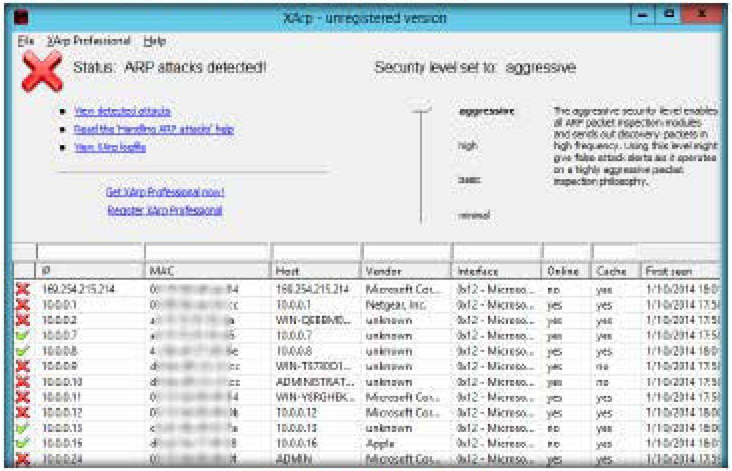
```
Interface : 0x12
[ethernet]
source mac: d4-be-d9-c3-c3-cc
dest mac  : 00-15-5d-00-49-05
type      : 0x806
[arp]
direction : in
type      : reply
source ip : 10.0.0.11
dest ip   : 10.0.0.10
source mac: d4-be-d9-c3-c3-cc
dest mac  : 00-15-5d-00-49-05
```

FIGURE 8.6: XArp displaying Alerts

XArp allows alert filtering for excluding specific hosts. Another feature includes settings for alerting intensity and how the alerts are presented. Also allows sending alerts through email and detailed alerting configuration.

11. The status changes to **ARP attacks detected**.

The simplest form of certification is the use of static, read-only entries for critical services in the ARP cache of a host. This only prevents simple attacks and does not scale on a large network, since the mapping has to be set for each pair of machines resulting in (n*n) ARP caches that have to be configured. AntiARP also provides Windows-based spoofing prevention at the kernel level.



XArp - unregistered version
File
XArp Professional
Help
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

Status: ARP attacks detected!

Security level set to: aggressive

The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
✗	169.254.215.214	[redacted]	169.254.215.214	Microsoft Cor...	0x12 - Microso...	no	yes	1/10/2014 18:0
✗	10.0.0.1	[redacted]	10.0.0.1	Netgear, Inc.	0x12 - Microso...	yes	yes	1/10/2014 17:5
✗	10.0.0.2	[redacted]	WIN-QEBBMD...	unknown	0x12 - Microso...	yes	yes	1/10/2014 17:5
✓	10.0.0.7	[redacted]	10.0.0.7	unknown	0x12 - Microso...	yes	yes	1/10/2014 17:5
✓	10.0.0.8	[redacted]	10.0.0.8	unknown	0x12 - Microso...	yes	yes	1/10/2014 18:0
✗	10.0.0.9	[redacted]	WIN-TS7I0D1...	unknown	0x12 - Microso...	yes	no	1/10/2014 17:5
✗	10.0.0.10	[redacted]	ADMINISTRAT...	unknown	0x12 - Microso...	yes	no	1/10/2014 17:5
✗	10.0.0.11	[redacted]	WIN-Y8RGHEK...	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 17:5
✗	10.0.0.12	[redacted]	10.0.0.12	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 18:0
✓	10.0.0.13	[redacted]	10.0.0.13	unknown	0x12 - Microso...	no	yes	1/10/2014 18:0
✓	10.0.0.16	[redacted]	10.0.0.16	Apple	0x12 - Microso...	no	yes	1/10/2014 18:0
✗	10.0.0.24	[redacted]	ADMIN	Microsoft Cor...	0x12 - Microso...	yes	yes	1/10/2014 17:5

FIGURE 8.7: XArp - ARP attacks detected

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab
9

Performing DNS Poisoning in a Switch Based Network

DNS spoofing (or DNS poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer)..

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Hackers employ the DNS Poisoning technique to corrupt the cache of a DNS which translates domain names into IP addresses. Hackers replace the original IP address with those of a server which they control. The ulterior motive of this hack is to redirect the traffic, intended for a particular site, to their servers in order to steal users' data.

On these servers, hackers create a clone website which resembles a bank or an e-commerce site. Users, who are unknowingly redirected to these servers, enter their banking or other financial instrument credentials on the cloned site thus giving it to the hackers.

Lab Objectives

The objective of this lab is to help students understand how to:

- Perform DNS Poisoning on a switch based network

Lab Environment

To perform the lab, you need:

- A computer running with Windows Server 2012 as the host machine
- Windows 8.1 running as a virtual machine

Lab Duration

Time: 10 Minutes

Overview of DNS Poisoning

DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses.

Lab Tasks

TASK 1

Install Cain & Abel

1. Log in to Windows 8.1 and Windows Server 2008 virtual machines before starting this lab.
2. Switch to **Windows 8.1** machine, navigate to **Z:\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel**, double-click **ca_setup.exe** and follow the wizard driven installation steps to install Cain & Abel.
3. If you have already installed the application, skip to **step no. 6**.

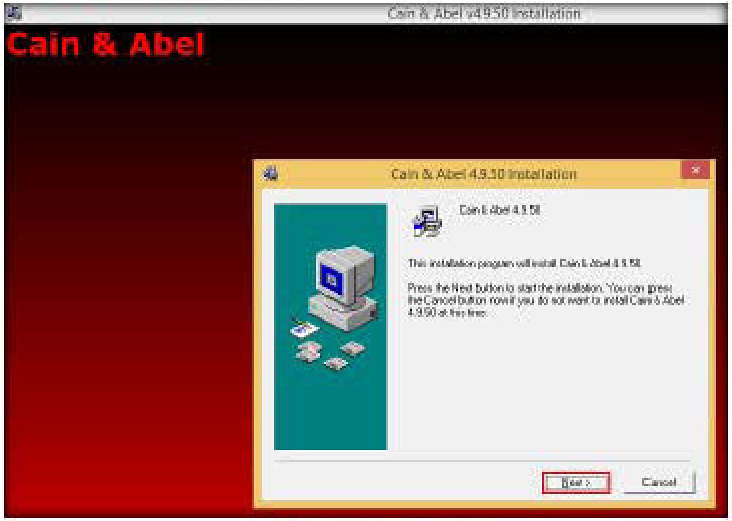
Note:

If a **User Account Control** pop-up appears, click **Yes**.

If a **Window Security** dialog box appears asking you to enter the network credentials, type in the following credentials and click **OK**:

User name: **Administrator**

Password: **qwerty@123**



Cain & Abel v4.9.50 Installation

Cain & Abel

Cain & Abel 4.9.50 Installation

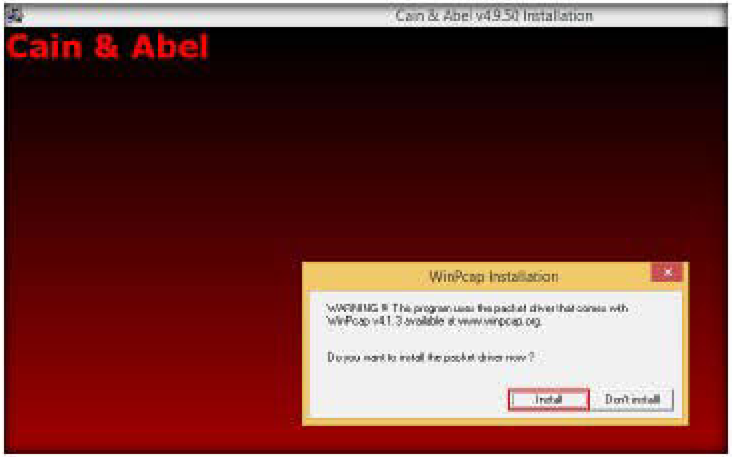
Cain & Abel 4.9.50

This installation program will install Cain & Abel 4.9.50.

Press the Next button to start the installation. You can press the Cancel button now if you do not want to install Cain & Abel 4.9.50 at this time.

FIGURE 9.1: Installing Cain & Abel

4. During installation, a **WinPcap Installation** pop-up appears, click **Install**

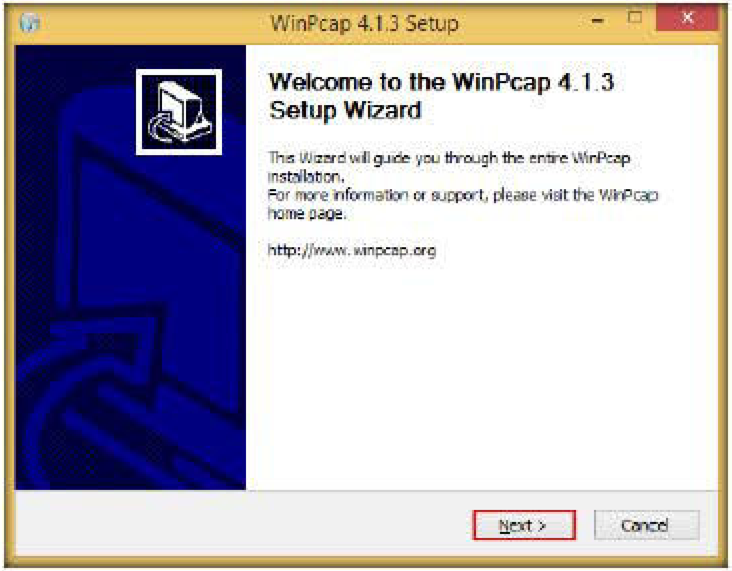


WARNING !! This program uses the packet driver that comes with WinPcap v4.1.3 available at www.winpcap.org.

Do you want to install the packet driver now ?

FIGURE 9.2: Installing WinPcap

5. Follow the wizard driven installation steps to install WinPcap



Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

FIGURE 9.3: Installing WinPcap

TASK 2

Perform ARP Poisoning

6. Now, double-click **Cain** icon on **Desktop** in order to launch the application.

   Note: If a **User Account Control** pop-up appears, click **Yes**.

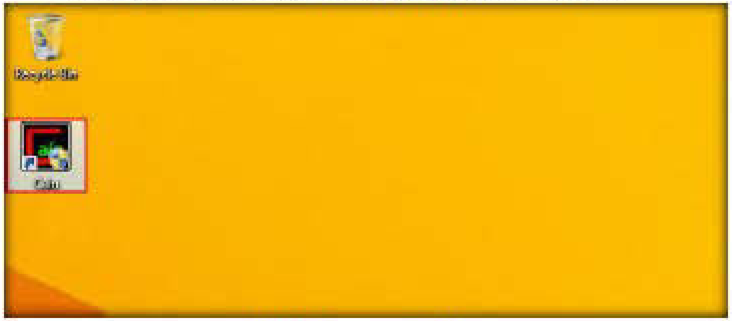


FIGURE 9.4: Launching Cain & Abel

7. Cain window appears; click **Configure** from the menu bar.

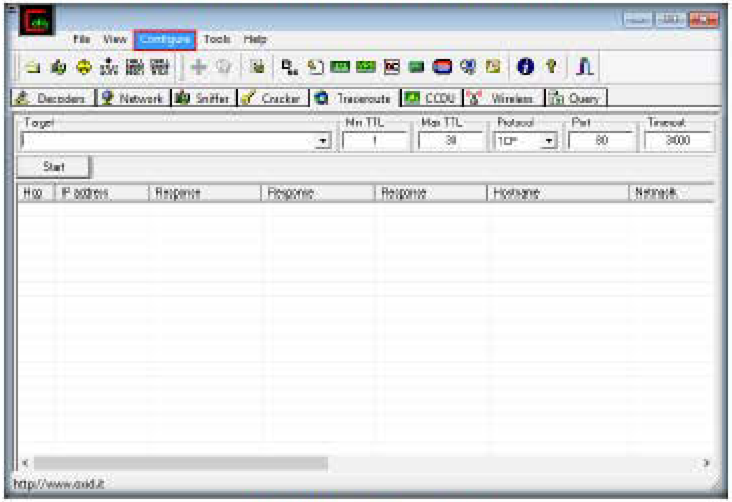
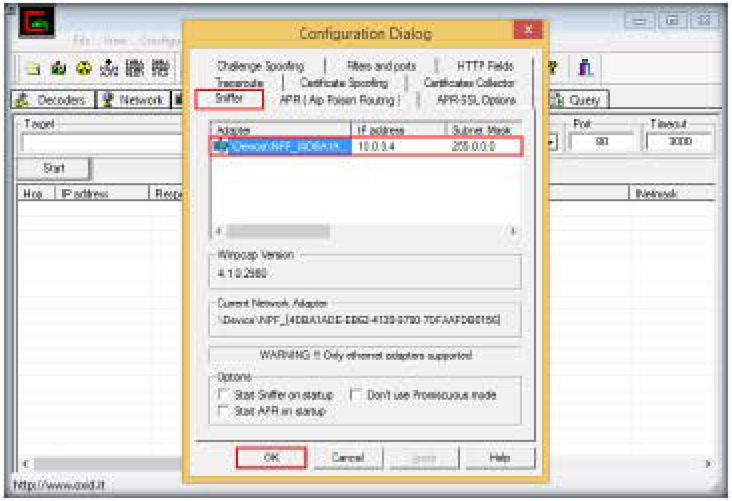

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Target
Min TTL 1
Max TTL 30
Protocol TCP
Port 80
Timeout 3000
Start
Hop IP address Response Response Response Hostname Netmask
http://www.oxid.it

FIGURE 9.5: Configuring Cain & Abel

8. **Configuration Dialog** window appears, click **Sniffer** tab.

9. Select the adapter and click **OK**.



Configuration Dialog

Adapter	IP address	Subnet Mask
\Device\NPF_{4DBA1A...	10.0.3.4	255.0.0.0

Winpcap Version
4.1.0.2980

Current Network Adapter
\Device\NPF_{4DBA1ADE-EB62-4138-9780-7DFAAFD8015C}

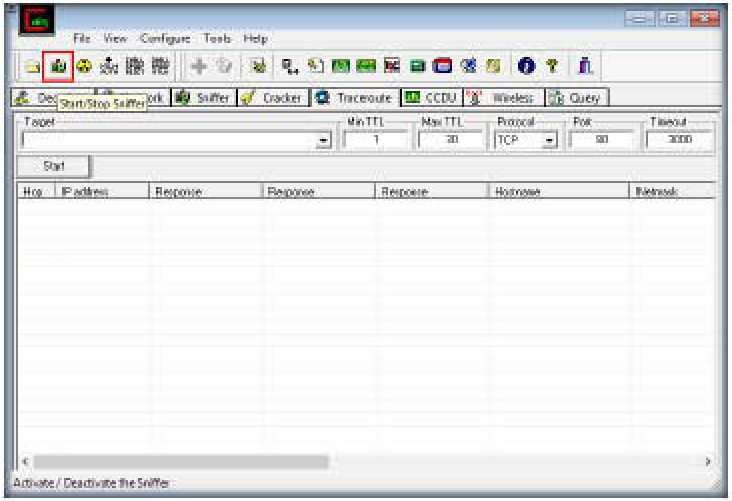
WARNING !! Only ethernet adapters supported

Options
□ Start Sniffer on startup □ Don't use Promiscuous mode
□ Start APR on startup

http://www.oxid.it

FIGURE 9.6: Configuring Cain & Abel

10. Now, click **Start/Stop Sniffer** icon on the toolbar.

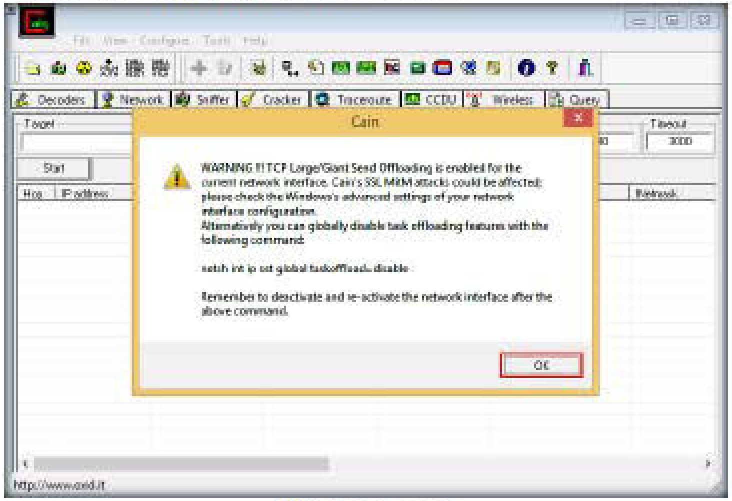


Min TTL: 1 Max TTL: 30 Protocol: TCP Port: 80 Timeout: 3000

Activate / Deactivate the Sniffer

FIGURE 9.7: Starting Sniffer

11. If a **Cain** pop-up appears, click **OK** button.



WARNING !! TCP Large/Giant Send Offloading is enabled for the current network interface. Cain's SSL MitM attacks could be affected; please check the Windows's advanced settings of your network interface configuration.
Alternatively you can globally disable task offloading features with the following command:

```
netsh int ip set global taskoffload=disable
```

Remember to deactivate and re-activate the network interface after the above command.

FIGURE 9.8: Cain Pop-Up

12. Click **Sniffer** tab.

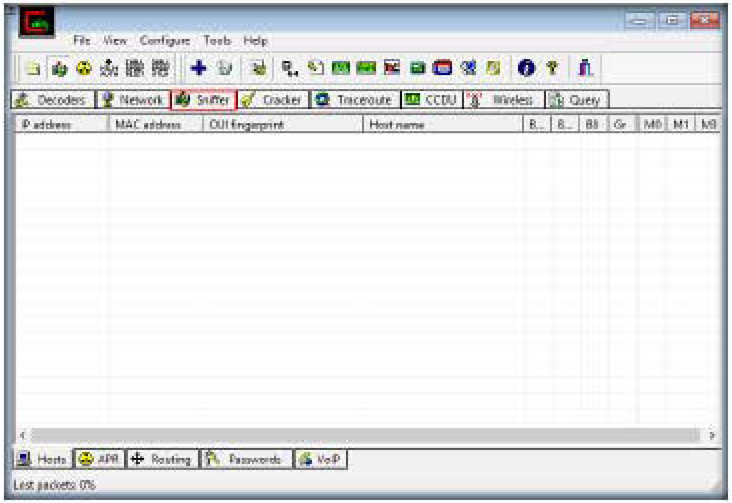


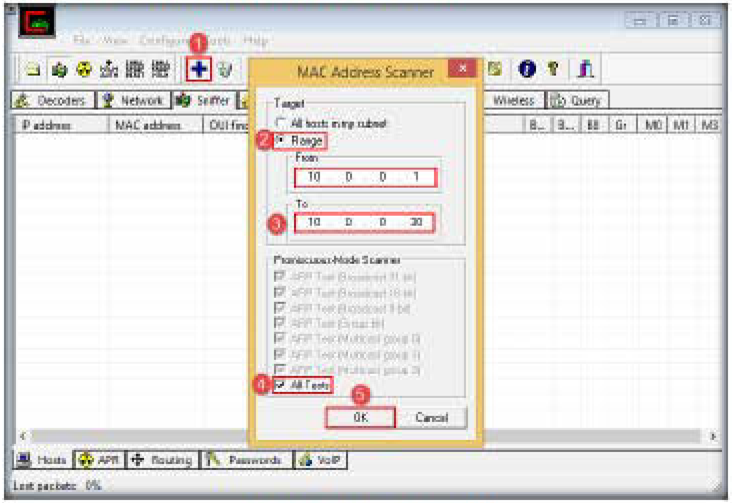
FIGURE 9.9: Clicking Sniffer Tab

13. Click **+** icon on the toolbar.

14. **MAC Address Scanner** window appears, click **Range** radio button.

15. Specify the IP address range on which you want to perform scan (here **10.0.0.1–10.0.0.30** is the IP address range used in this lab. This might vary in your lab environment).

16. Check **All Tests** option and then click **OK**.



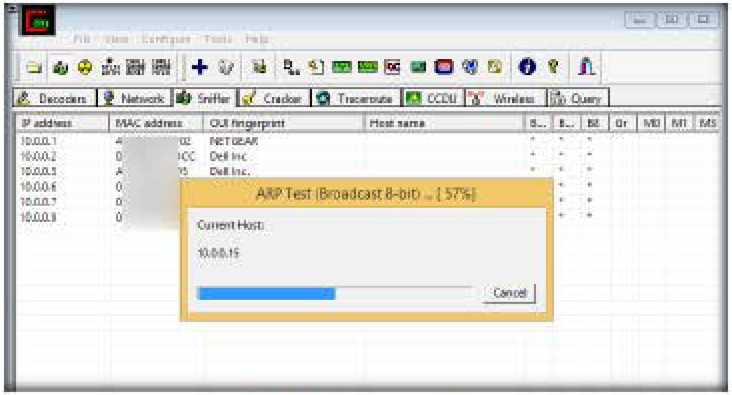
MAC Address Scanner

Target
○ All hosts in my subnet
● Range
From: 10 . 0 . 0 . 1
To: 10 . 0 . 0 . 30

Promiscuous-Mode Scanner
☑ All Tests

FIGURE 9.10: Scanning MAC Addresses

17. The application begins to perform ARP tests on the above mentioned IP address range and displays the detected address in the Sniffer window as shown in the following screenshot:



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.0.0.1	[redacted]	NETGEAR		*	*	*				
10.0.0.2	[redacted]	Dell Inc.		*	*	*				
10.0.0.3	[redacted]	Dell Inc.		*	*	*				
10.0.0.6	[redacted]				*	*				
10.0.0.7	[redacted]				*	*				
10.0.0.8	[redacted]				*	*				

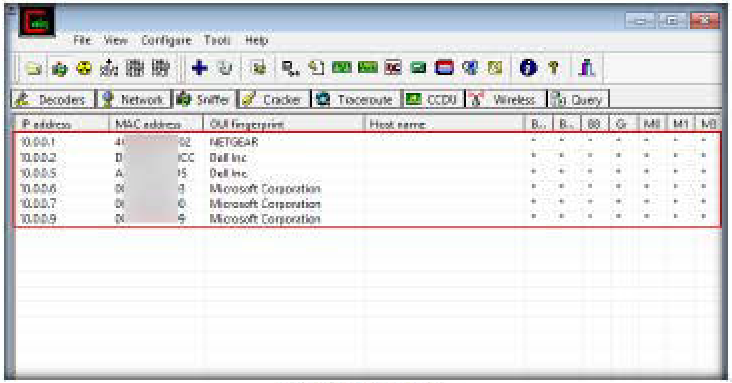
ARP Test (Broadcast 8-bit) ... [57%]

Current Host:

10.0.0.15

FIGURE 9.11: Scanning MAC Addresses

18. On completing the ARP tests, all the MAC and their associated IP addresses that responded to the ARP requests are displayed as shown in the following screenshot:


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.0.0.1	[redacted]	NETGEAR		*	*	*	*	*	*	*
10.0.0.2	[redacted]	Dell Inc.		*	*	*	*	*	*	*
10.0.0.5	[redacted]	Dell Inc.		*	*	*	*	*	*	*
10.0.0.6	[redacted]	Microsoft Corporation		*	*	*	*	*	*	*
10.0.0.7	[redacted]	Microsoft Corporation		*	*	*	*	*	*	*
10.0.0.9	[redacted]	Microsoft Corporation		*	*	*	*	*	*	*

FIGURE 9.12: Sniffer Tab

19. Now, click **APR** tab at the lower section of the screen.

20. Click anywhere on the top most section in the right-hand pane under the Sniffer tab to activate the **+** icon

21. Once the **+** icon is activated, click it.

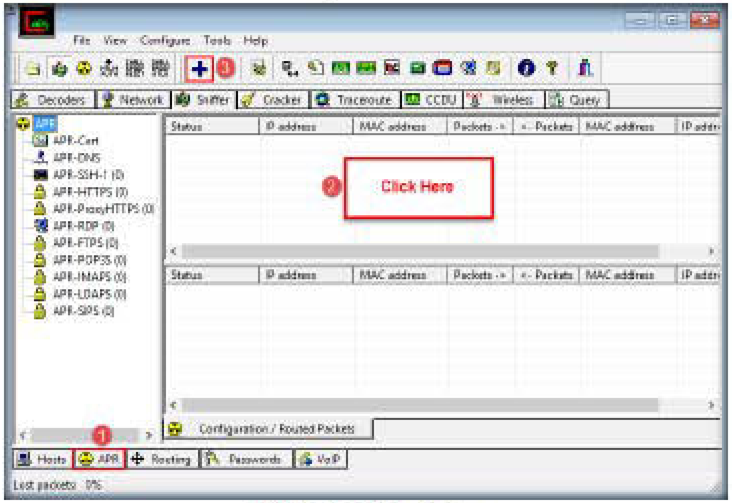
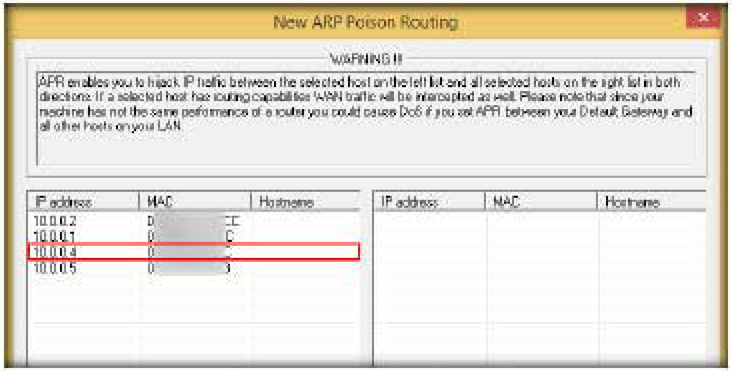

File View Configure Tools Help
3
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP addr
2
Click Here
Status IP address MAC address Packets -> <- Packets MAC address IP addr
Configuration / Routed Packets
1
Hosts APR Routing Passwords VoIP
Lost packets: 0%

FIGURE 9.13: ARP Poison Routing

22. **New ARP Poison Routing** window appears. Now, you need to select the machines whose data exchange you want to intercept.

23. Select the first target (here **10.0.0.4** which refers to **Windows Server 2008** machine) from the list of IP addresses displayed in the left-hand pane.



New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.0.0.2	[redacted]	
10.0.0.1	[redacted]	
10.0.0.4	[redacted]	
10.0.0.5	[redacted]	

IP address	MAC	Hostname

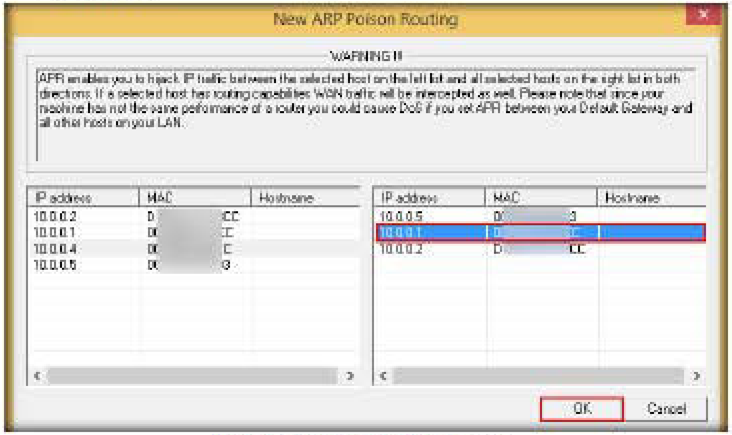
FIGURE 9.14: New ARP Poison Routing Window

Note: The IP Address of **Windows Server 2008** virtual machine might vary in your lab environment.

24. Upon selecting the first target, a list of IP addresses excluding the first target, appears in the right-hand pane.

25. You need to select the second target IP address (here **10.0.0.1** which refers to the **router**) from the right-hand pane. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

26. Click **OK**.



New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

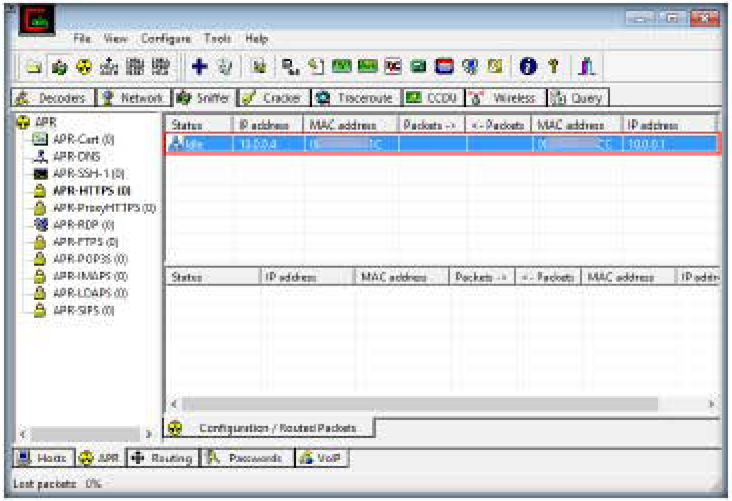
IP address	MAC	Hostname
10.0.0.2	[redacted]	
10.0.0.1	[redacted]	
10.0.0.4	[redacted]	
10.0.0.5	[redacted]	

IP address	MAC	Hostname
10.0.0.5	[redacted]	
10.0.0.1	[redacted]	
10.0.0.2	[redacted]	

FIGURE 9.15: Performing ARP Poison Routing

27. Now all the requests sent from the **Windows Server 2008** machine pass through the router.

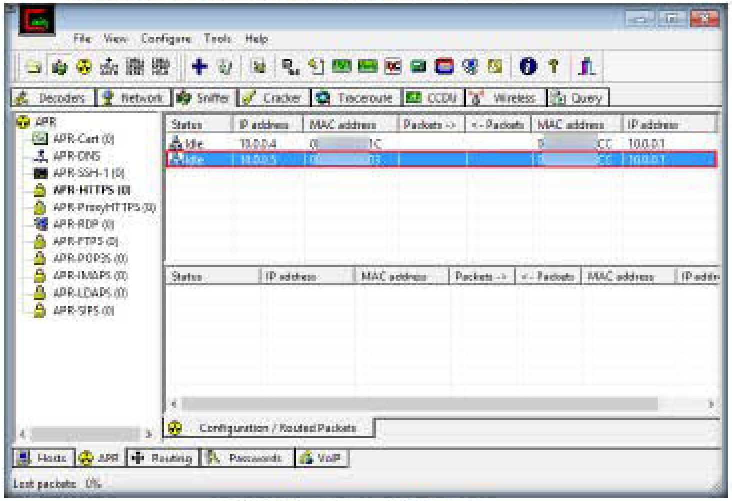
28. At this point, the selected targets appear in the top section under Sniffer tab.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.0.0.4	1[redacted]1C			0[redacted]CC	10.0.0.1

FIGURE 9.16: Performing ARP Poison Routing

29. In the same way, follow the steps **19-26** to perform ARP poison routing between **Kali Linux** virtual and the router.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.0.0.4	0[redacted]1C			0[redacted]CC	10.0.0.1
Idle	10.0.0.5	0[redacted]03			0[redacted]CC	10.0.0.1

FIGURE 9.17: Performing ARP Poison Routing

30. In this lab, we are going to perform DNS poisoning on both **Windows Server 2008** and **Kali Linux** virtual machines.

TASK 3

Perform DNS Poisoning

31. Click **APR-DNS** from the left-hand pane. When the APR-DNS section appears, right-click anywhere inside the section. A context menu appears; select **Add to list** option.

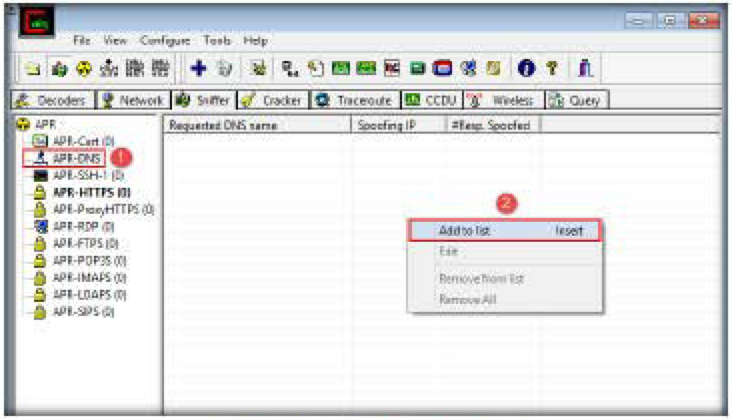
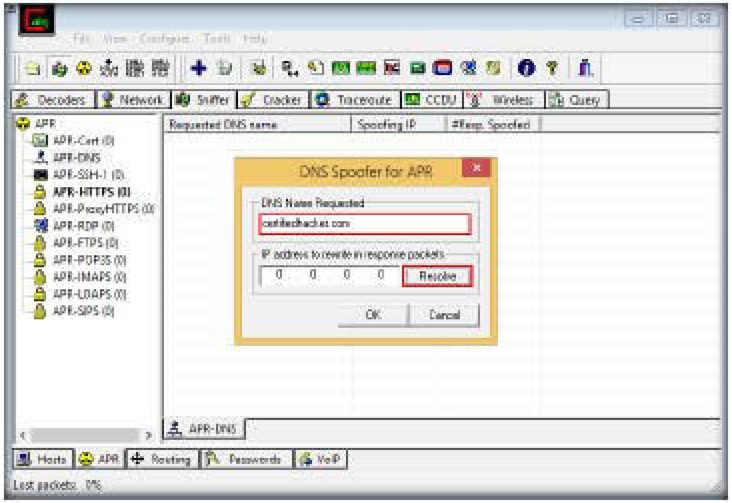


FIGURE 9.18: Configuring DNS Poison Routing

32. **DNS Spoofer for APR** dialog box appears, enter the target domain name (here **www.certifiedhacker.com)** in **DNS Name Required** field and click the **Resolve** button.

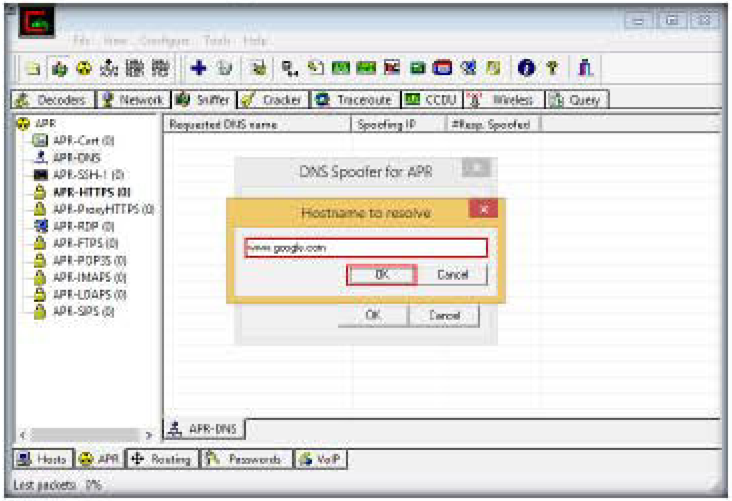


DNS Name Requested: certifiedhacker.com

IP address to rewrite in response packets: 0 . 0 . 0 . 0

FIGURE 9.19: Configuring DNS Poison Routing

33. **Hostname to Resolve** dialog box appears, enter a domain name (here **www.google.com**) and click **OK**.

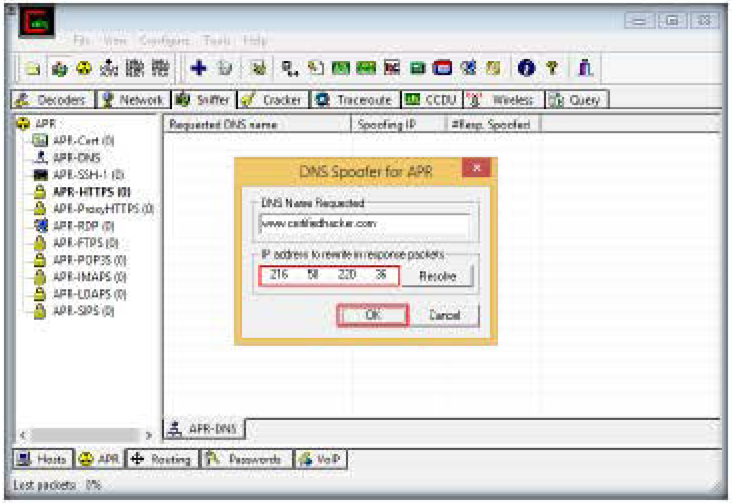


Hostname to resolve: www.google.com

FIGURE 9.20: Configuring DNS Poison Routing

34. The application automatically translates the domain name to its corresponding IP Address.

35. Click **OK**.



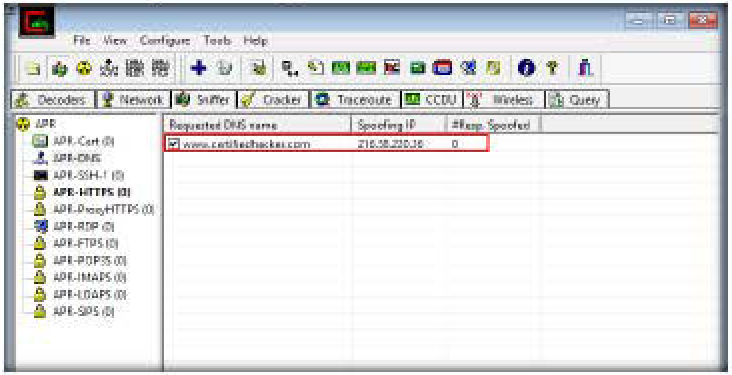
DNS Name Requested: www.certifiedhacker.com

IP address to rewrite in response packets: 216 . 58 . 220 . 36

FIGURE 9.21: Configuring DNS Poison Routing

36. By doing so, whenever a user victim attempts to browse www.certifiedhacker.com website, he/she will be redirected to www.google.com, resulting in DNS spoofing/poisoning.

37. The Requested DNS appears in the APR-DNS section.

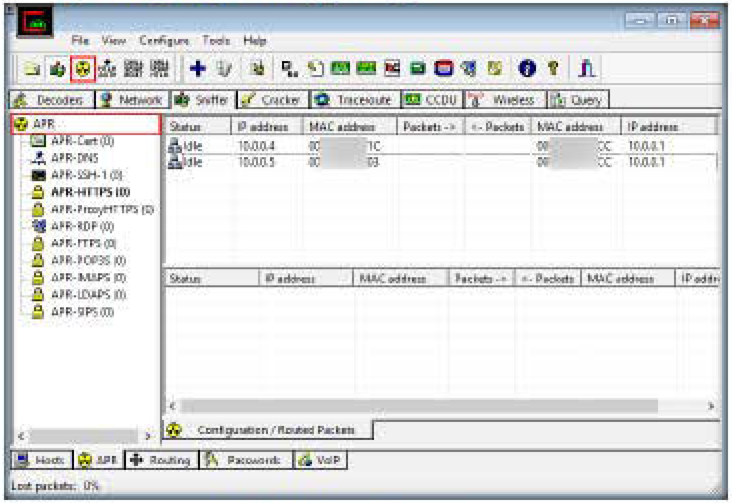


Requested DNS name	Spoofing IP	#Resp. Spoofed
☑ www.certifiedhacker.com	216.58.220.36	0

FIGURE 9.22: DNS Poison Routing Configured

38. Now you are all set to perform DNS poisoning on the victim machines Windows Server 2008 and Kali Linux.

39. Click **APR** in the left-hand pane. The ARP Poison routing section appears, click Start/Stop APR button on the toolbar to begin DNS poisoning along with ARP poisoning.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.0.0.4	00[redacted]1C			00[redacted]CC	10.0.0.1
Idle	10.0.0.5	00[redacted]03			00[redacted]CC	10.0.0.1

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP addr

FIGURE 9.23: Initiating ARP Poison Routing

40. Now switch to **Windows Server 2008** virtual machine, launch Mozilla firefox web browser, type the URL **www.certifiedhacker.com** in the address bar and press **Enter**.

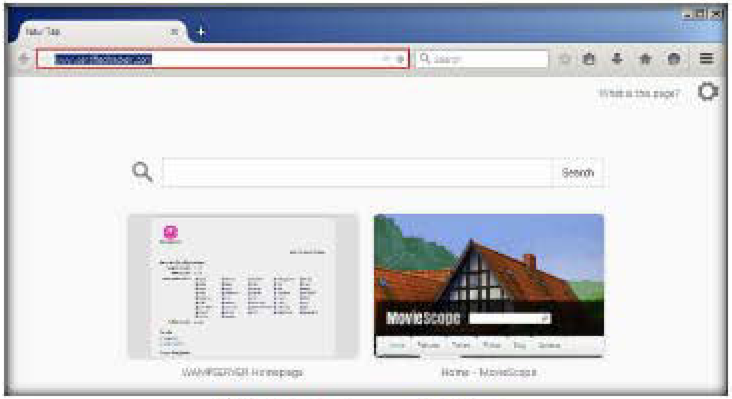


FIGURE 9.24: Browsing www.certifiedhacker.com

41. You will be redirected to **google** webpage instead of **certifiedhacker** homepage, confirming that DNS poisoning was successful.

Note: If a webpage appears stating that the connection is not trusted, click **I Understand the Risks**. Scroll down the webpage and click **Add Exception...** button. **Add Security Exception** window appears, click **Confirm Security Exception** button.

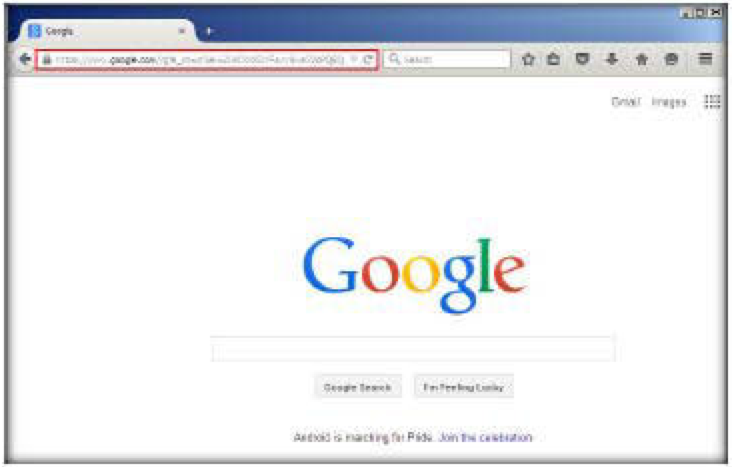


FIGURE 9.25: DNS Poisoning Performed

42. In the same way, you may attempt to browse **www.certifiedhacker.com** on **Kali Linux** machine.

43. You will be redirected www.google.com as shown in the following screenshot:

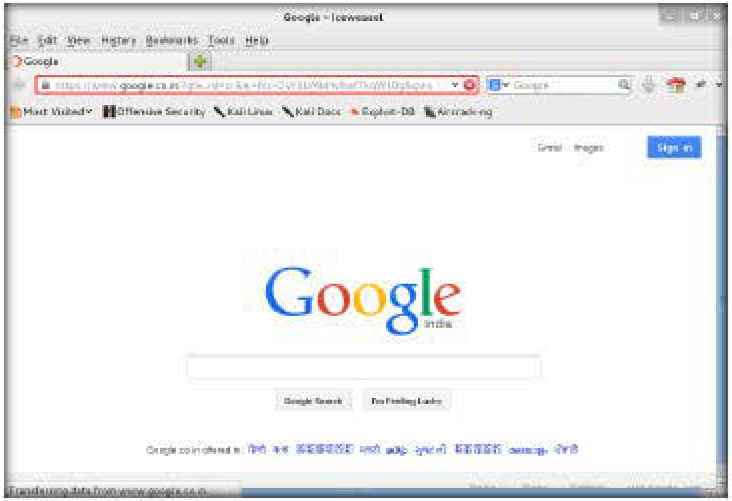


FIGURE 9.26: DNS Poisoning Performed

44. Thus, you have successfully performed DNS poison routing on the victim machines.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs