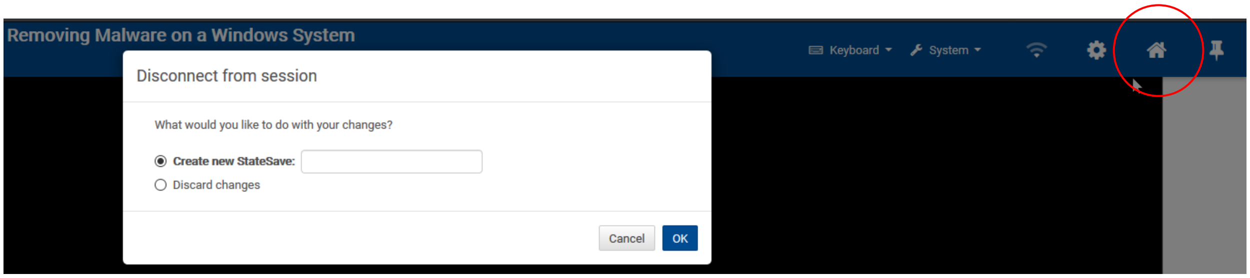
Lab #3 (Required): Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic[*]

Introduction to Information Security (IST623)
School of Information Studies
Syracuse University

Disclaimer: The contents of this document are solely for educational purpose. Misused knowledge of this lab may result in damage of data, security breach, privacy violation, or other undesirable situations. Therefore, using knowledge of this lab other than for the original purpose is prohibited.

**** Save Your Lab Status!**** You may need to save your lab from time to time as each session allows you to be logged in only for two hours at a time. To save your current status in the lab environment, **click** the **Home** icon button (🏠) in the top right corner and choose **Create new StateSave** if it's your first time saving or **Overwrite existing StateSave** if you have saved it before.



Disconnect from session

What would you like to do with your changes?

● Create new StateSave:

○ Discard changes

Learning Objectives

The Wireshark protocol analyzer is multi-faceted. In fact, a person can use Wireshark for many years and not use all of the various capabilities of Wireshark. For instance, Wireshark can be used by a security analyst to find anomalies in network traffic indicative of viruses or exfiltration of information. At the same time, even on the same traffic from the same organization, it can be used to troubleshoot application performance issues or benchmark VoIP latencies.

NetWitness Investigator provides a high-level overview of all the traffic in the packet capture file. While Wireshark looks at every packet, NetWitness categorizes and organizes traffic so that anomalous patterns become more apparent. Using both tools together might be required to show a complete picture for a forensic investigation.

In this lab, we begin by using Wireshark to analyze the specifics of wireless transmissions and then move on to analyze the network packets using a more security-specific tool, NetWitness

[*] Customized lab manual by Dr. Joon S. Park at the School of Information Studies for the virtual online labs provided by Jones & Bartlett Learning.

Investigator. It is also noteworthy that Wireshark is available at no charge while NetWitness is a commercial product that is widely utilized and may be encountered in any well-equipped cyber forensics lab or in many field investigations.

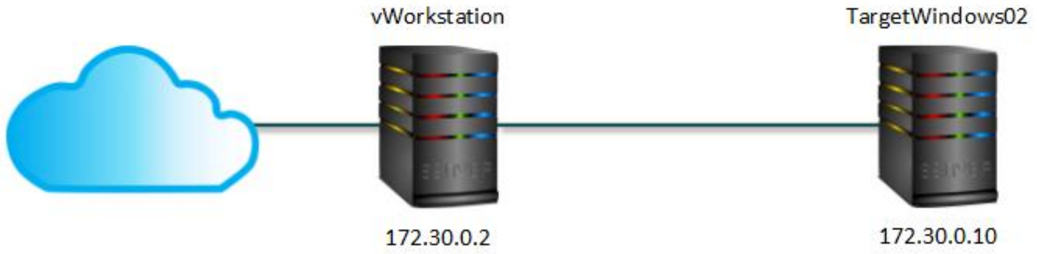
Upon completing this lab, you will be able to:

- Analyze the wireless-specific fields of network traffic packets using Wireshark.
- Identify the fields of network traffic packets that remain the same regardless of whether the packets traverse wires or fly through the air wirelessly.
- Use features of the NetWitness Investigator tool to analyze traffic with wireless content.
- Determine which tool, Wireshark or NetWitness Investigator, is the preferred tool for a given task.
- Utilize both Wireshark and NetWitness Investigator together to provide a complete picture of the interactions being investigated.
- Be able to generalize your new knowledge of Wi-Fi traffic to other types of wireless traffic analyzed by using the Wireshark analyzer.
- Differentiate between the more generalized capabilities of Wireshark and the more specialized cybersecurity analysis-focused uses of NetWitness Investigator.

Lab Structure

This lab has the following parts that should be completed in the order specified.

1. In the first part of the lab, you will use an existing capture file to view the wireless aspects of networks and some of the aspects of network traffic that remain the same regardless of the physical transport, be it wired or wireless.
2. In the second part of the lab, you will utilize the same capture file but with a more security-focused tool, NetWitness Investigator.
3. In the third part of the lab, you will answer a challenge question which will help you understand the limitations of Wireshark.



Tools and Software

The following software and/or utilities are required to complete this lab. You are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Wireshark
- NetWitness Investigator

Lab Deliverables

- Upon completion of this lab, you are required to provide the following deliverables.
    - One PDF file that includes:
        - Screenshots from Part 1: Steps #10, #12, #14 and #20
        - Screenshots from Part 2: Step #10
        - Your summary from Step #11 of Part 2 (in 200 words)
        - Your summary from Step #13 of Part 2 (in 200 words)
        - Your answer on the Challenge Question from Part 3 (in 200 words)

- Lab Report Submission
    - Please submit your deliverables through the LMS Submission.
    - The screenshots should be readable.
    - Make sure you include all the items required in your report.

Part 1: Analyze Wireless Traffic with Wireshark

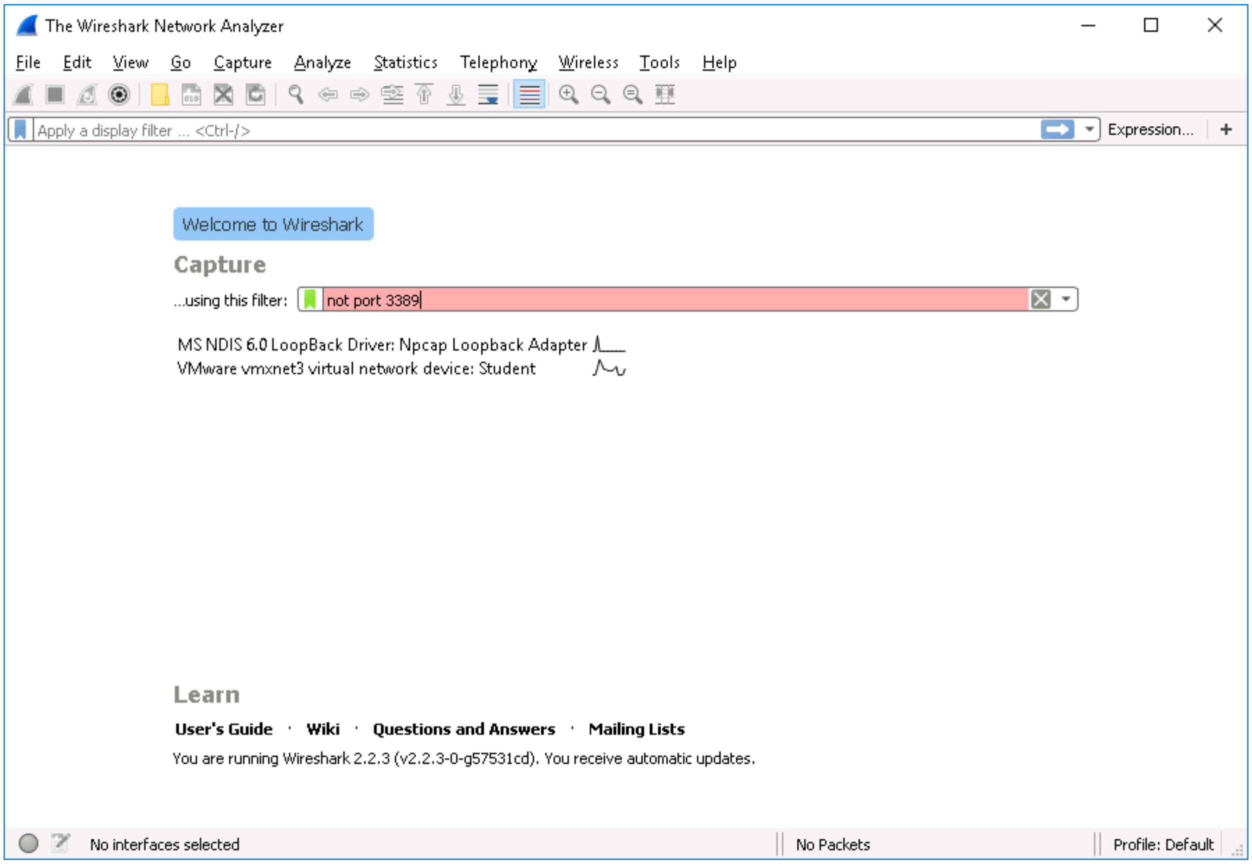
Note: In this part of the lab, you will load a file of traffic that has been previously captured by Wireshark so that all of the packets reviewed in the lab are the same for every student and match the instructions. Throughout this part of the lab, you should spend a few moments looking at the data captured by Wireshark and familiarize yourself with the Wireshark format and the English language descriptions Wireshark uses to explain frame details. You may need this information to answer the questions at the end of the lab.

1. On the vWorkstation desktop, **double-click** the **Connections** folder.

2. In the Connections folder, **double-click** the **TargetWindows02 RDP** shortcut to open a remote connection to the **TargetWindows02** machine. If prompted, **type** the following credentials and **click OK**. The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

   Username: **Administrator**
   Password: **P@ssw0rd!**

3. On the TargetWindows02 taskbar, **click** the **Wireshark icon** (a blue shark fin,) to launch the Wireshark application. Your welcome screen may not match the figure below.



Apply a display filter … <Ctrl-/>

...using this filter: not port 3389

MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter
VMware vmxnet3 virtual network device: Student

You are running Wireshark 2.2.3 (v2.2.3-0-g57531cd). You receive automatic updates.

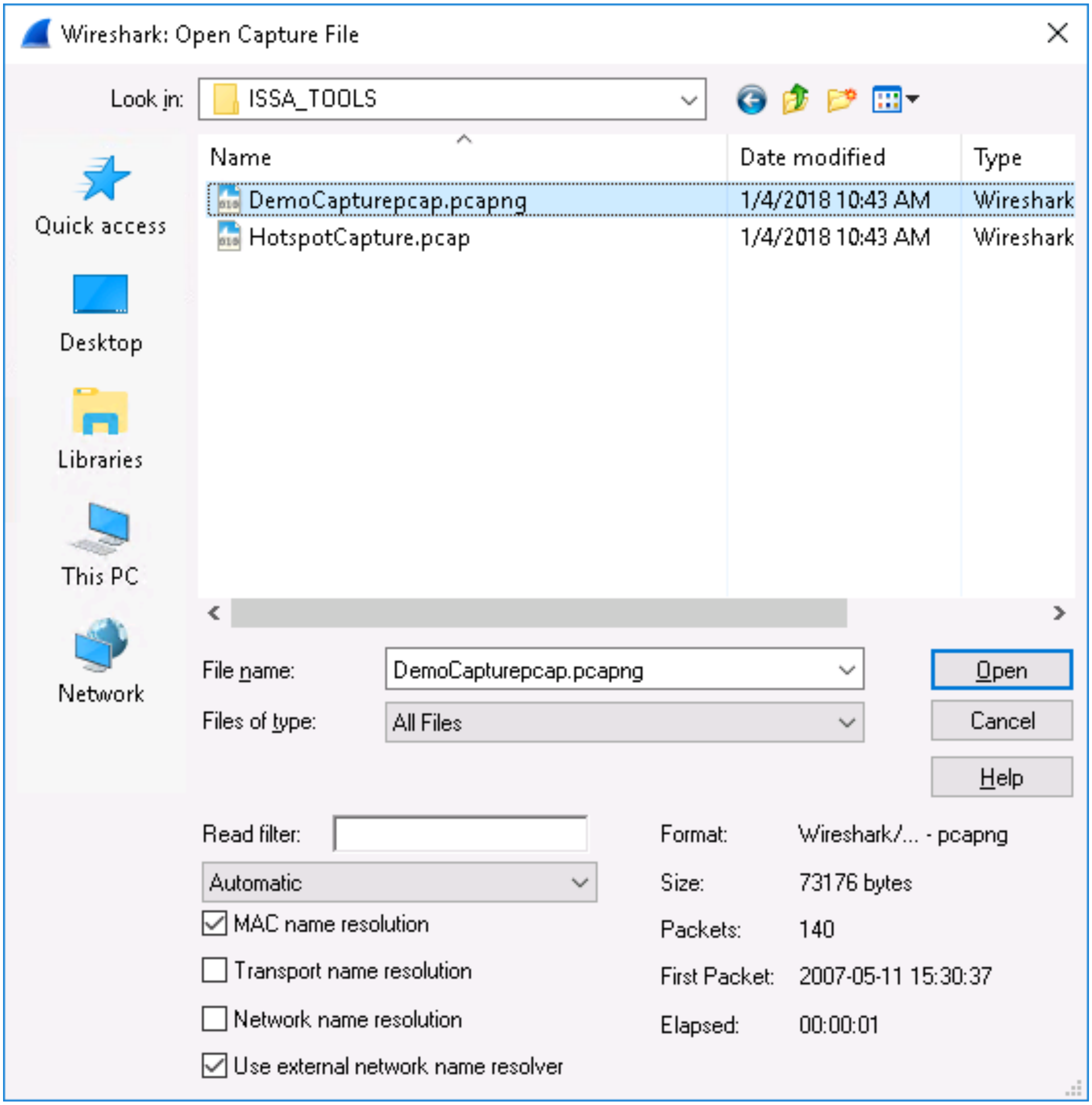
No interfaces selected | No Packets | Profile: Default

Figure 1 Wireshark Screen

4. From the Wireshark menu bar, **click File** and **select Open** to open the Open Capture File dialog box.

5. In the dialog box, **navigate** to the **ISSA_TOOLS** folder (**This PC > Local Disk (C:) > ISSA_TOOLS**) and **double-click** the **DemoCapturepcap file** to open it.

> **Note:** Wireshark capture files, like the DemoCapturepcap file found in this lab, have a ".pcapng" extension, which stands for packet capture, next generation.



Wireshark: Open Capture File

Look in: ISSA_TOOLS

Name	Date modified	Type
DemoCapturepcap.pcapng	1/4/2018 10:43 AM	Wireshark
HotspotCapture.pcap	1/4/2018 10:43 AM	Wireshark

File name: DemoCapturepcap.pcapng

Files of type: All Files

Read filter:

Automatic

☑ MAC name resolution

□ Transport name resolution

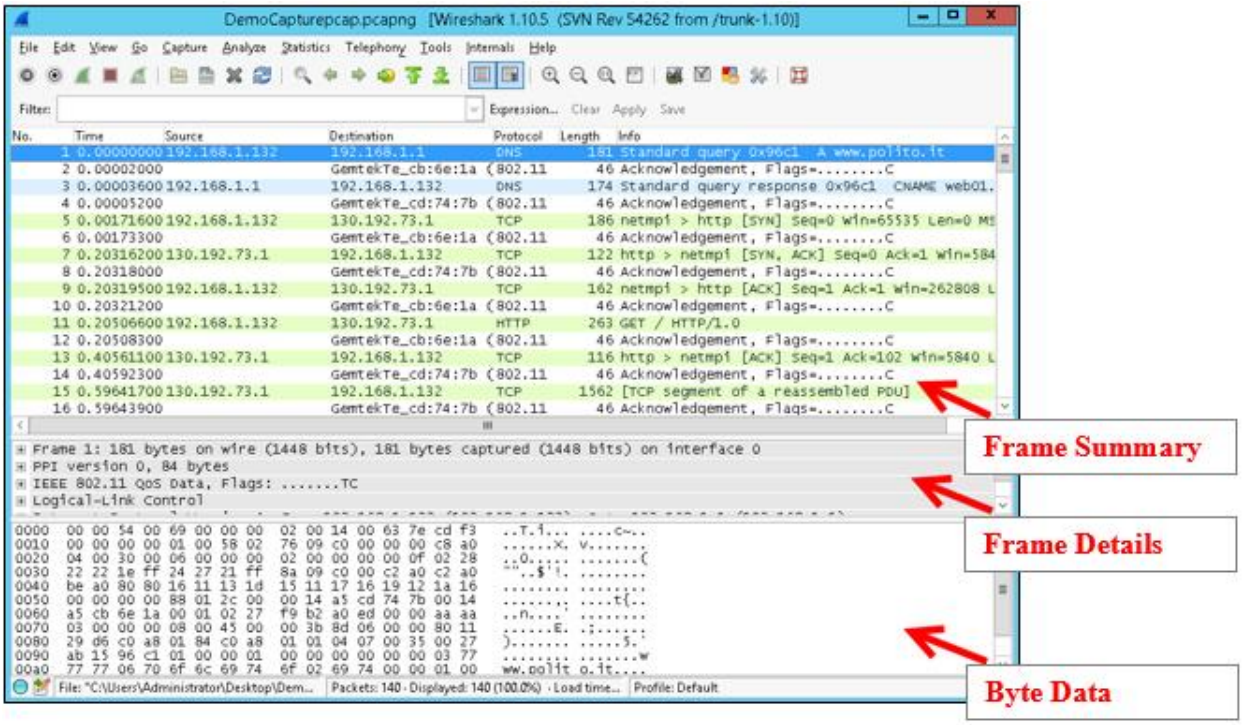
□ Network name resolution

☑ Use external network name resolver

Format:	Wireshark/... - pcapng
Size:	73176 bytes
Packets:	140
First Packet:	2007-05-11 15:30:37
Elapsed:	00:00:01

Figure 2 Wireshark: Open Capture File

The Wireshark output is shown in the three panes: Frame Summary, Frame Details, and Byte Data.



DemoCapturepcap.pcapng [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
Frame Summary
Frame Details
Byte Data

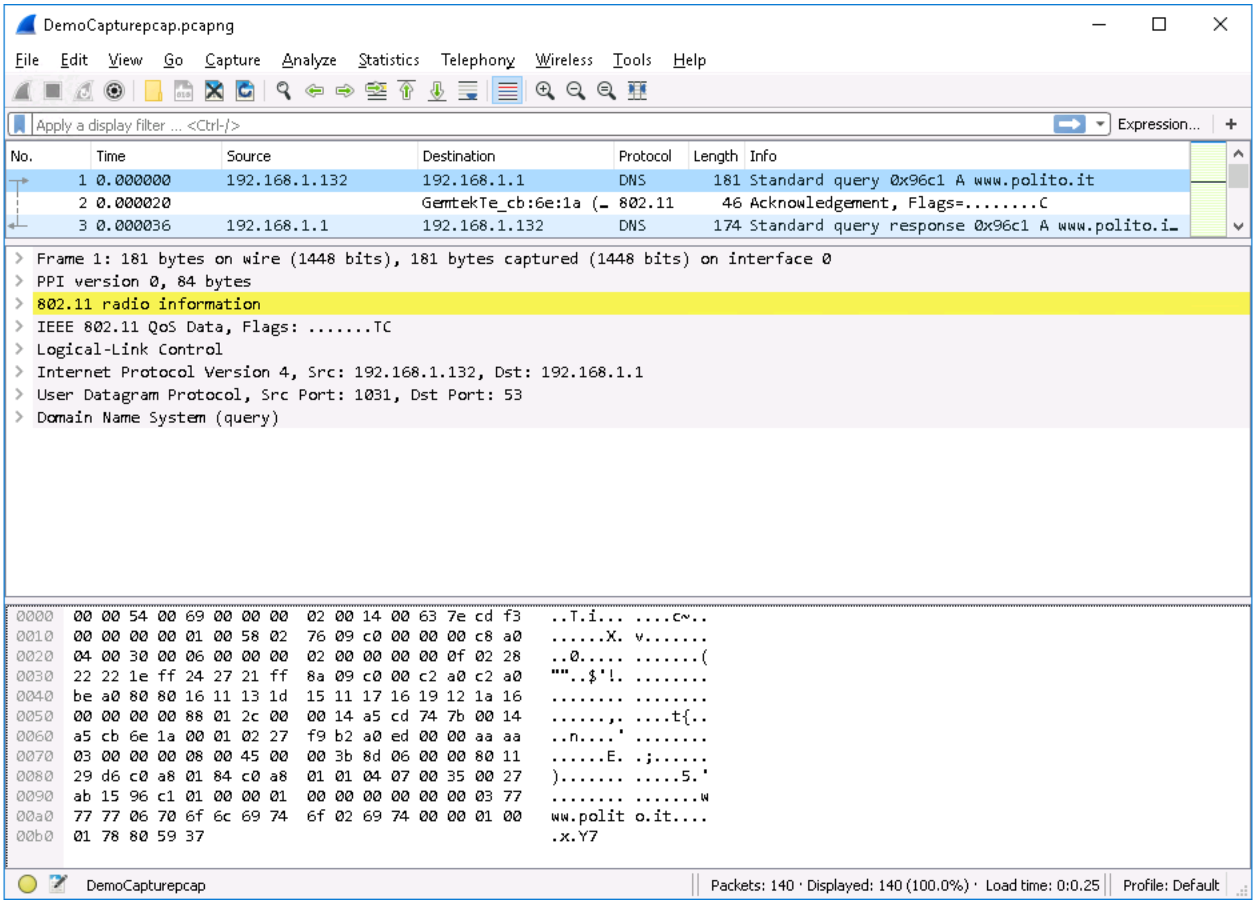
```
No.   Time        Source         Destination             Protocol  Length Info
    1 0.00000000  192.168.1.132  192.168.1.1             DNS        181 Standard query 0x96c1  A www.polito.it
    2 0.00002000                 GemtekTe_cb:6e:1a (802.11           46 Acknowledgement, Flags=........C
    3 0.00003600  192.168.1.1    192.168.1.132           DNS        174 Standard query response 0x96c1  CNAME web01.
    4 0.00005200                 GemtekTe_cd:74:7b (802.11           46 Acknowledgement, Flags=........C
    5 0.00171600  192.168.1.132  130.192.73.1            TCP        186 netmpi > http [SYN] Seq=0 Win=65535 Len=0 MS
    6 0.00173300                 GemtekTe_cb:6e:1a (802.11           46 Acknowledgement, Flags=........C
    7 0.20316200  130.192.73.1   192.168.1.132           TCP        122 http > netmpi [SYN, ACK] Seq=0 Ack=1 Win=584
    8 0.20318000                 GemtekTe_cd:74:7b (802.11           46 Acknowledgement, Flags=........C
    9 0.20319500  192.168.1.132  130.192.73.1            TCP        162 netmpi > http [ACK] Seq=1 Ack=1 Win=262808 L
   10 0.20321200                 GemtekTe_cb:6e:1a (802.11           46 Acknowledgement, Flags=........C
   11 0.20506600  192.168.1.132  130.192.73.1            HTTP       263 GET / HTTP/1.0
   12 0.20508300                 GemtekTe_cb:6e:1a (802.11           46 Acknowledgement, Flags=........C
   13 0.40561100  130.192.73.1   192.168.1.132           TCP        116 http > netmpi [ACK] Seq=1 Ack=102 Win=5840 L
   14 0.40592300                 GemtekTe_cd:74:7b (802.11           46 Acknowledgement, Flags=........C
   15 0.59641700  130.192.73.1   192.168.1.132           TCP       1562 [TCP segment of a reassembled PDU]
   16 0.59643900                 GemtekTe_cd:74:7b (802.11           46 Acknowledgement, Flags=........C

⊞ Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
⊞ PPI version 0, 84 bytes
⊞ IEEE 802.11 QoS Data, Flags: .......TC
⊞ Logical-Link Control

0000  00 00 54 00 69 00 00 00  02 00 14 00 63 7e cd f3   ..T.i... ....c~..
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   ""..$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....

File: "C:\Users\Administrator\Desktop\Dem... | Packets: 140 · Displayed: 140 (100.0%) · Load time... | Profile: Default
```

Figure 3 Wireshark Output Panes

The bottom pane of the Wireshark window displays the Byte Data. All the information in the packet is displayed in hexadecimal on the left and in decimal (in characters when possible) on the right. This can be a useful feature, especially if passwords you are looking for are unencrypted.

6. In the **Frame Summary** pane, **click** the **first frame** and **review** the **Frame Details pane**.

7. **Drag** the **top border** of the frame detail pane up until only the summaries of frames 1-3 are shown and the rest of the frame summary pane is covered by the frame detail pane, as shown in Figure 4.


DemoCapturepcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time      Source          Destination          Protocol  Length Info
  1  0.000000  192.168.1.132   192.168.1.1          DNS          181 Standard query 0x96c1 A www.polito.it
  2  0.000020                  GemtekTe_cb:6e:1a (… 802.11        46 Acknowledgement, Flags=........C
  3  0.000036  192.168.1.1     192.168.1.132        DNS          174 Standard query response 0x96c1 A www.polito.i…
```

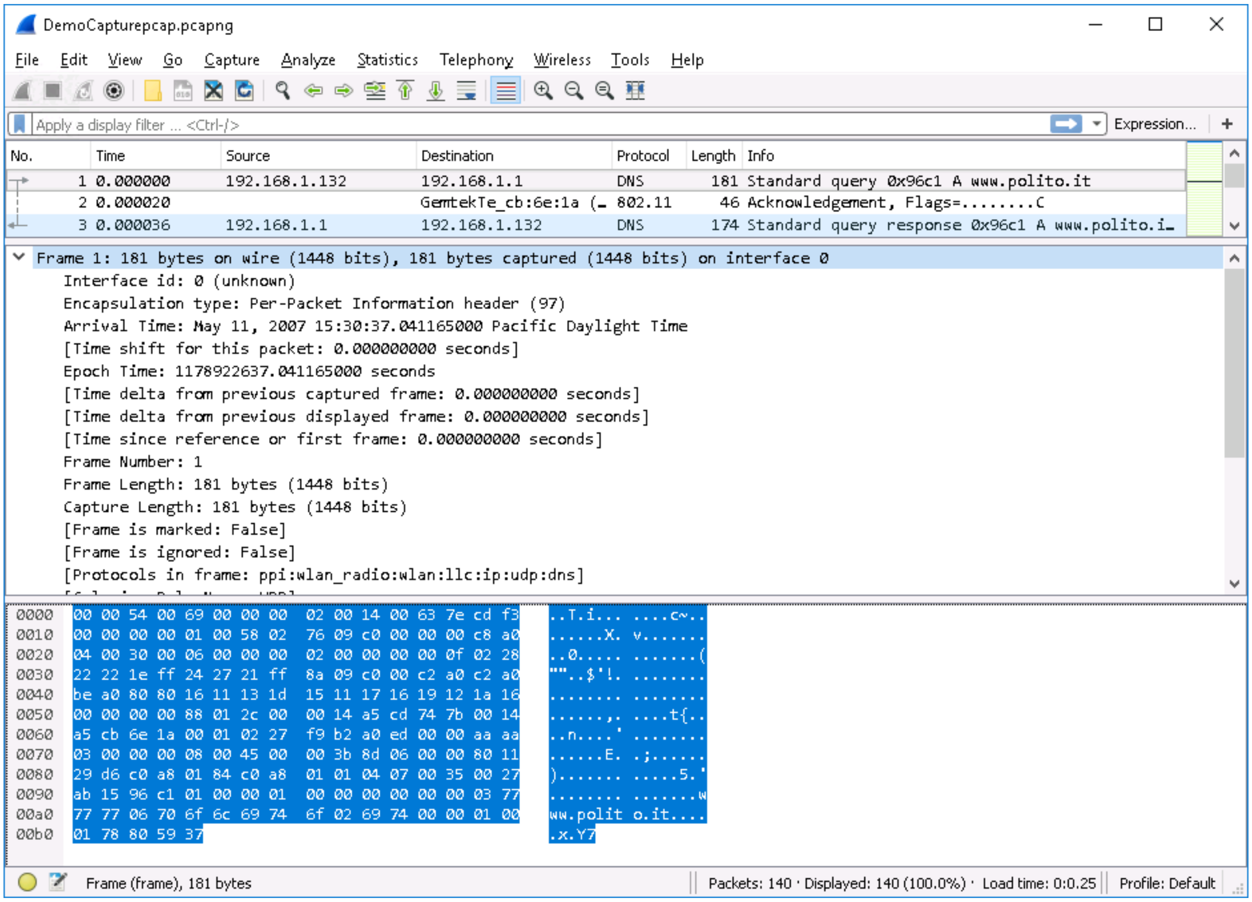
```
> Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
> PPI version 0, 84 bytes
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.132, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 1031, Dst Port: 53
> Domain Name System (query)
```

```
0000  00 00 54 00 69 00 00 00  02 00 14 00 63 7e cd f3   ..T.i... ....c~..
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   ""..$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
00b0  01 78 80 59 37                                     .x.Y7
```

Figure 4 Frame Details for the First Frame

You can drag the frame borders to change the view of your data at any time. You can also **expand** each line in the frame details pane by clicking the arrow or **collapse** the details by clicking the down arrow at the beginning of each line.

8. In the **Frame Details** pane, **click** the right (greater-than) arrow at the beginning of the **Frame 1** line to expand the Frame Header detail.


DemoCapturepcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time      Source         Destination           Protocol Length Info
  1  0.000000  192.168.1.132  192.168.1.1           DNS       181 Standard query 0x96c1 A www.polito.it
  2  0.000020                 GemtekTe_cb:6e:1a (…  802.11     46 Acknowledgement, Flags=........C
  3  0.000036  192.168.1.1    192.168.1.132         DNS       174 Standard query response 0x96c1 A www.polito.i…
```

```
Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
    Interface id: 0 (unknown)
    Encapsulation type: Per-Packet Information header (97)
    Arrival Time: May 11, 2007 15:30:37.041165000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1178922637.041165000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 181 bytes (1448 bits)
    Capture Length: 181 bytes (1448 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: ppi:wlan_radio:wlan:llc:ip:udp:dns]
```

```
0000  00 00 54 00 69 00 00 00  02 00 14 00 63 7e cd f3   ..T.i... ....c~..
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   ""..$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
00b0  01 78 80 59 37                                     .x.Y7
```

Frame (frame), 181 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.25 | Profile: Default

Figure 5 Wireless Packet

Notice the fields related to time. This part of the display will be the same for wired or wireless traffic. The **Encapsulation type: Per-Packet Information header**, a field unique to wireless traffic, however, confirms that this is a wireless packet.

> **Note:** Many people believe that it is necessary to enable the Wireless Toolbar (View > Wireless Toolbar) any time they are looking at wireless traffic. However, even if you were to enable the Wireless Toolbar at this point, the options would remain "greyed out" because the toolbar is used only when capturing live traffic, and then only if the AirPcap interface is enabled. In this virtual lab, you will use a pre-captured file and are not capturing live traffic, so it is not necessary to turn on the Wireless Toolbar.

9. In the frame detail pane, **expand** the **PPI version 0** line to display the **Per-Packet Information** encapsulation.

10. In the **Frame Details** pane, **expand** the **Flags** line **AND** the **802.11-Common** line to display the details of them. **Make a screen capture** showing those expanded fields. Paste the screen capture into your lab report.

    A **Data Link Type (DLT)** of 105 indicates that data is transferred over an 802.11n wireless network. **Rate:300.0 Mbps** indicates the maximum rate of transmission.

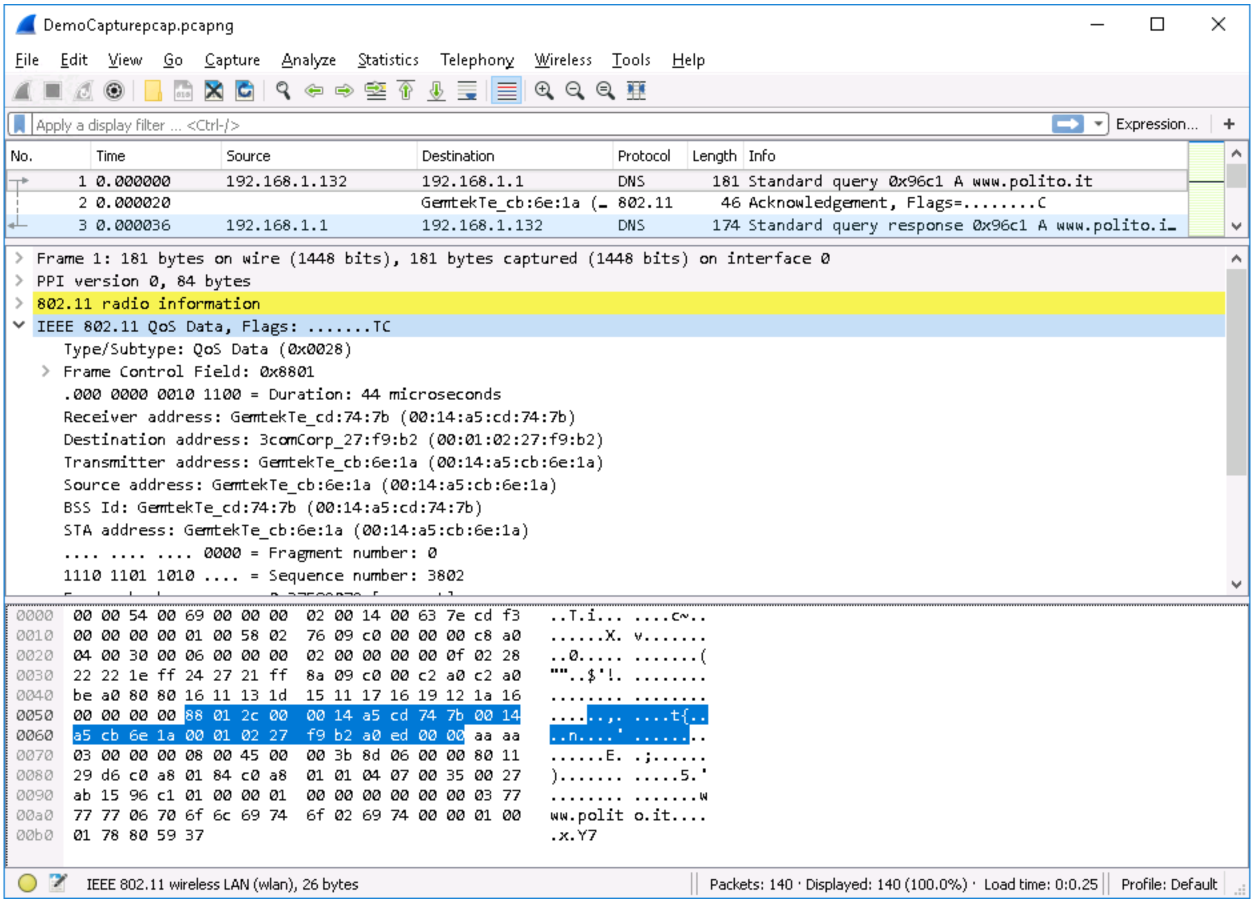
Note: The detailed information that Wireshark provides about the antennae, signal strengths, and other aspects of the wireless communications environment can be useful for installation, antenna placement, and troubleshooting. It can also be valuable in terms of computer forensics because it can be used to map who is able to communicate with whom, the measured strength of signals, what frequencies are used, and other data. In addition to forensics on standard Wi-Fi and other forms of traditional wireless communications, this information can also be useful for jamming certain frequencies, for determining which devices were likely used to set off remote bombs and Improvised Explosive Devices (IEDs), and a spectrum of other things.

11. Collapse all the lines. In the **Frame Details** pane, **expand** the **IEEE 802.11 QoS Data, Flags** line.

    In this group of fields, Wireshark displays information about the transmitters and receivers of the data, which enable the network administrator to determine which Media Access Control (MAC) addresses match each transmitter and receiver.

Note: Remember, Wireshark displays transmitter/receiver addresses in both full hexadecimal (00:14:a5:cd:74:7b) and a kind of shorthand, in this case, GemtekTe_cd:74:7b. That shorthand code is Wireshark's translation of the first part of the receiver address (00:14:a5) into the manufacturer's name or alphanumeric designation (GemtekTe_). The IEEE has compiled a list of company names that correspond to the first six characters of the MAC ID, which can be accessed on its Web site at http://standards.ieee.org/develop/regauth/oui/public.html). Search for Gemtek or 3Com.

Although Wireshark's translation is most likely correct, it is also possible that some manufacturers, especially those that have acquired other companies, will have more than one numeric designation that resolves to their name or alphanumeric designation. It is therefore better to refer to the entire hexadecimal representation of the address rather than the shorthand.


DemoCapturepcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time        Source          Destination          Protocol  Length  Info
   1 0.000000    192.168.1.132   192.168.1.1          DNS          181  Standard query 0x96c1 A www.polito.it
   2 0.000020                    GemtekTe_cb:6e:1a (…  802.11        46  Acknowledgement, Flags=........C
   3 0.000036    192.168.1.1     192.168.1.132        DNS          174  Standard query response 0x96c1 A www.polito.i…
```

```
> Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
> PPI version 0, 84 bytes
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    Destination address: 3comCorp_27:f9:b2 (00:01:02:27:f9:b2)
    Transmitter address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    Source address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    BSS Id: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    STA address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    .... .... .... 0000 = Fragment number: 0
    1110 1101 1010 .... = Sequence number: 3802
```

```
0000  00 00 54 00 69 00 00 00  02 00 14 00 63 7e cd f3   ..T.i... ....c~..
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   ""..$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
00b0  01 78 80 59 37                                     .x.Y7
```

IEEE 802.11 wireless LAN (wlan), 26 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.25 | Profile: Default

Figure 6 Frame Address Information

12. Locate the “**Destination address: 3Com_27:f9:b2 (00:01:02:27:f9:b2)**” line in the Frame Details field and select it. You should be able to see the corresponding byte data highlighted in the bottom pane. **Make a screen capture** showing your entire Wireshark window. Paste the screen capture into your lab report.

Note: There are literally hundreds of fields of data available, depending on the wireless communications protocols that are present and those that are captured, and there are a thousand different ways to interpret them.

The fields that have been examined thus far are unique to wireless networking. There are important aspects to know about capturing wireless data with Wireshark.

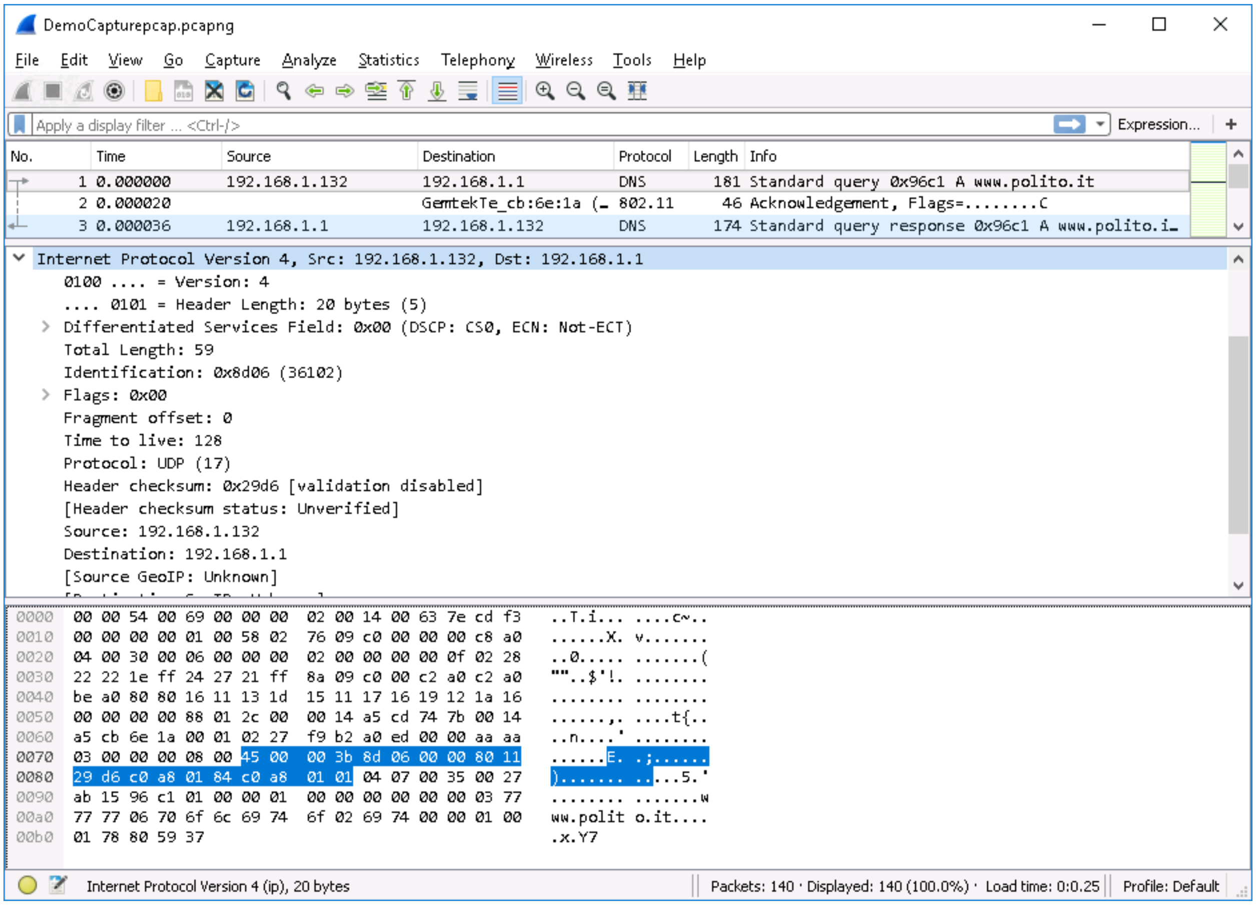
Wireshark is regularly installed with a packet capture library called WinPcap. Based on the wireless interfaces and how the capture is set up, Wireshark will display the fields it can capture. However, it is possible that in some cases, there will be wireless information that Wireshark cannot capture, or when it can capture only the essence of the command and control information, but not the information itself.

For this reason, packet capture add-ons, such as AirPcap, are frequently installed with Wireshark. These add-ons enable you to capture more wireless information. Most network analysts feel that AirPcap is absolutely required for capturing wireless traffic between devices or between other devices and, say, a wireless access point, depending on your goals and the objectives of the capture. From this point of the lab forward, all the data captured will be common to both wired and wireless networking and would have been captured with Wireshark using AirPcap or WinPcap.

13. Collapse all the lines. In the frame details pane, **expand** the **Domain Name System (query)** line to view the fields related to an Internet query.

14. In the **Frame Details** pane, **expand** the **Flags** line and familiarize yourself with the data available. **Expand** the **Queries** line**.** Notice that the data indicates that someone tried to access the **www.polito.it website**. **Make a screen capture** showing your entire Wireshark window. Paste the screen capture into your lab report.

15. Explore the other lines, including **Logical-Link Control, Internet Protocol Version 4,** and **User Datagram** Protocol (UDP), by extending or collapsing the details, using the scrollbar as necessary to view more information about the packets captured. Familiarize yourself with the data available.



```
No.   Time      Source          Destination          Protocol  Length Info
    1 0.000000  192.168.1.132   192.168.1.1          DNS        181 Standard query 0x96c1 A www.polito.it
    2 0.000020                  GemtekTe_cb:6e:1a (… 802.11      46 Acknowledgement, Flags=........C
    3 0.000036  192.168.1.1     192.168.1.132        DNS        174 Standard query response 0x96c1 A www.polito.i…
```

```
Internet Protocol Version 4, Src: 192.168.1.132, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0x8d06 (36102)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x29d6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.132
    Destination: 192.168.1.1
    [Source GeoIP: Unknown]
```

```
0000  00 00 54 00 69 00 00 00  02 00 14 00 63 7e cd f3   ..T.i... ....c~..
0010  00 00 00 00 01 00 58 02  76 09 c0 00 00 00 c8 a0   ......X. v.......
0020  04 00 30 00 06 00 00 00  02 00 00 00 00 0f 02 28   ..0..... .......(
0030  22 22 1e ff 24 27 21 ff  8a 09 c0 00 c2 a0 c2 a0   ""..$'!. ........
0040  be a0 80 80 16 11 13 1d  15 11 17 16 19 12 1a 16   ........ ........
0050  00 00 00 00 88 01 2c 00  00 14 a5 cd 74 7b 00 14   ......,. ....t{..
0060  a5 cb 6e 1a 00 01 02 27  f9 b2 a0 ed 00 00 aa aa   ..n....' ........
0070  03 00 00 00 08 00 45 00  00 3b 8d 06 00 00 80 11   ......E. .;......
0080  29 d6 c0 a8 01 84 c0 a8  01 01 04 07 00 35 00 27   )....... .....5.'
0090  ab 15 96 c1 01 00 00 01  00 00 00 00 00 00 03 77   ........ .......w
00a0  77 77 06 70 6f 6c 69 74  6f 02 69 74 00 00 01 00   ww.polit o.it....
00b0  01 78 80 59 37                                     .x.Y7
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.25 | Profile: Default

Figure 7 Internet Protocol Data

Investigating Wireless Traffic: The ultimate payload, regardless of whether the packet is sent through the air or on a wire, is a Domain Name System query. In this case, the DNS information is being requested for www.polito.it. Any DNS request, regardless of whether the packet is sent wirelessly or via wire, includes the same fields in a Wireshark packet capture, but the wireless portion of the frame information requires special consideration in a forensic investigation.

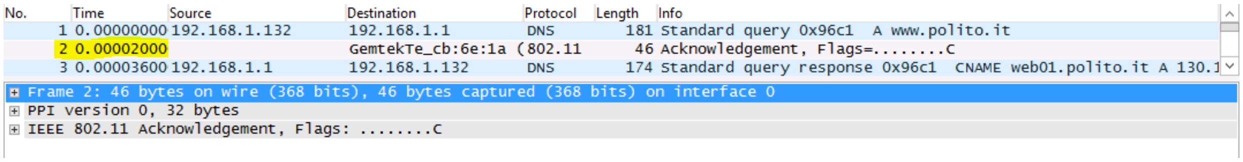
Suppose that a forensic investigator needed to monitor all Web traffic within a coffee shop to determine which Web sites were accessed by the subject of an investigation, then the fact that the Web query was conducted wirelessly is unimportant to the investigation except perhaps that the investigation was aided by getting easy access to unencrypted airborne packets. An investigator might choose to set a filter on the resulting capture file that shows only DNS requests. In this way, the investigator can determine which Web sites the subject *wished* to visit, and then is able to visit those Web sites himself later to determine the nature of the Web sites.

It is also possible to set a filter that displays both the DNS requests and their resulting DNS responses to determine which Web sites existed at the time the capture file was made, as opposed to which Web sites still existed when subsequent research was done. Consider, for example, a drug or human trafficking case. The owner of an illegal Web site might shut down the Web site after a subject is taken into custody, but before the research is completed. This type of filter will allow investigators to determine that while they were unable to access the Web site, the subject was able to complete the transaction. Packet capture files can also display the results of the Web page requests, such as any audio and video content, and they can provide further analysis using NetWitness Investigator.

On the other hand, a key part of another investigation might be to determine what information was gathered by the subject of an investigation, or to determine by whom certain information was gathered. The investigator might use information in a packet capture, either by linking the Layer 2 Media Access Control address and/or the Layer 3 IP address to specific wireless information. In this case, the wireless information that is captured becomes the central point of the investigation. As has happened many times, forensic investigators (often law enforcement) track illegal content, such as child pornography, to a quiet residential neighbourhood, obtain legal search warrants based on probable cause, and execute a search of the premises only to find that there is no illegal pornographic content or other content covered by the warrant present. At this point, the investigators could give up, or they could do further research on the wireless portion of captured traffic to determine that none of the devices owned by the residents of the home or their guests' mobile wireless devices were responsible for the traffic. What could have happened? Criminals sitting in a car outside the home-or a nearby coffee shop, hotel, or other location-could have used the wireless access point to transmit and receive illegal information and then departed the scene. Investigative tools such as video surveillance, stakeouts, sting operations, and similar law enforcement tools could be brought into play to further the investigation, but the wireless part of the captured traffic is a critical part of guiding the investigation and possibly of ultimately prosecuting the suspects.

Note: In the next steps, you will explore the information in Frames 2 and 3. **Frame 2** is a wireless command and control packet acknowledging receipt of **Frame 1**.

16. In the **Frame Summary** pane, **click Frame 2** to display the related data in the **Frame Detail** pane.

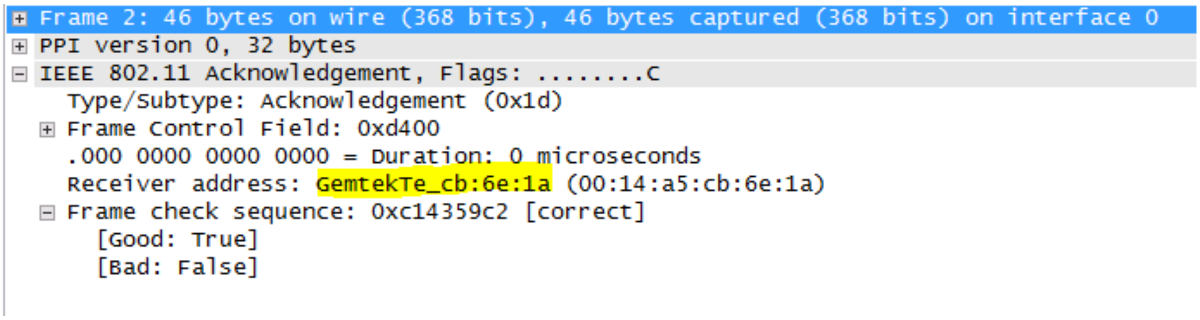


```
No.   Time        Source          Destination          Protocol Length Info
    1 0.00000000 192.168.1.132   192.168.1.1          DNS         181 Standard query 0x96c1  A www.polito.it
    2 0.00002000                 GemtekTe_cb:6e:1a (802.11         46 Acknowledgement, Flags=........C
    3 0.00003600 192.168.1.1     192.168.1.132        DNS         174 Standard query response 0x96c1  CNAME web01.polito.it A 130.1
⊞ Frame 2: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
⊞ PPI version 0, 32 bytes
⊞ IEEE 802.11 Acknowledgement, Flags: ........C
```

Figure 8 Frame 2 in Frame Summary Pane

17. In the **Frame Details** pane, **expand** the **IEEE 802.11 Acknowledgement, Flags** lines to view the details in those fields.

    Notice that the receiver address for **Frame 2** (00:14:a5:cb:6e:1a) is the same as the transmitter address in **Frame 1**.

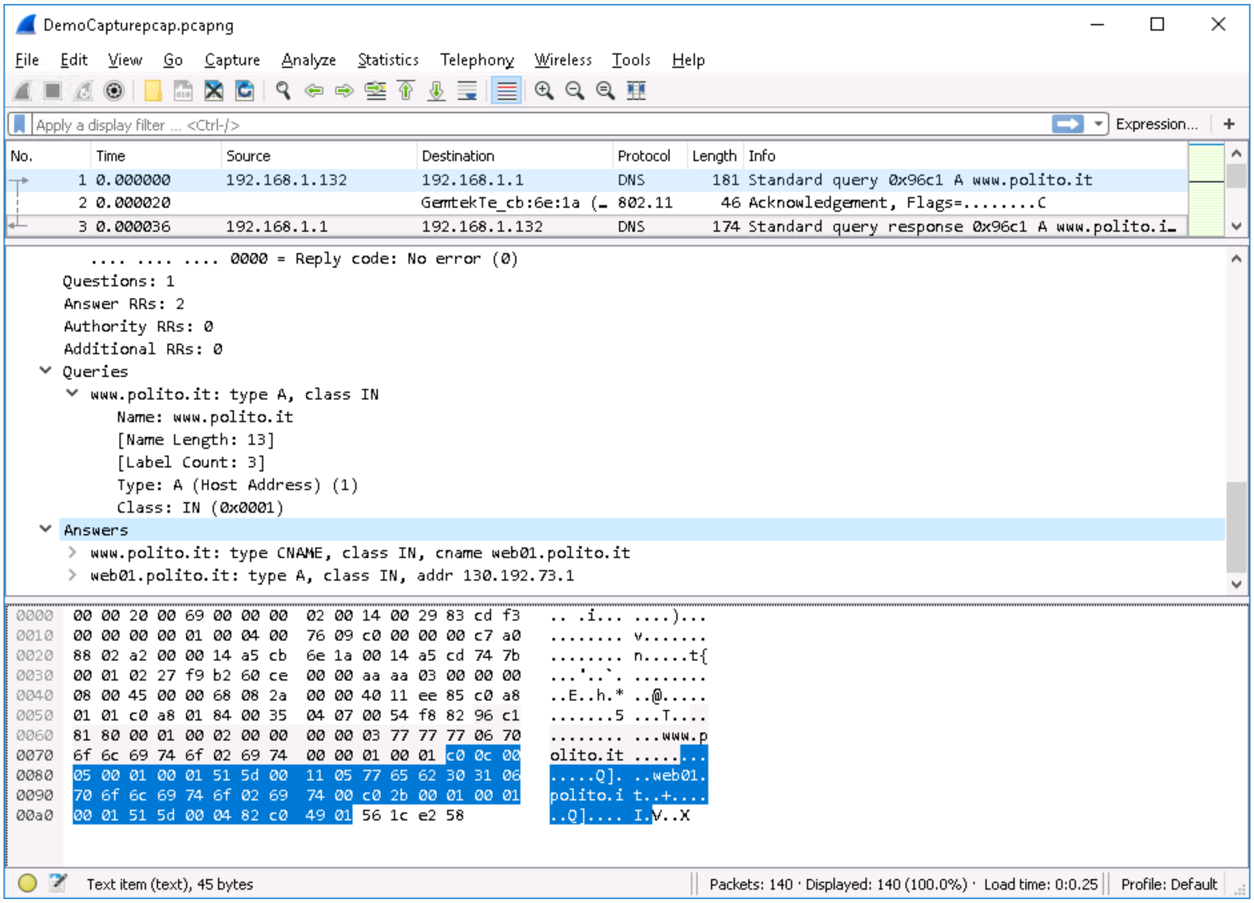


```
⊞ Frame 2: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
⊞ PPI version 0, 32 bytes
⊟ IEEE 802.11 Acknowledgement, Flags: ........C
    Type/Subtype: Acknowledgement (0x1d)
  ⊞ Frame Control Field: 0xd400
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
  ⊟ Frame check sequence: 0xc14359c2 [correct]
      [Good: True]
      [Bad: False]
```

Figure 9 802.11 Acknowledgement in Frame Detail

18. In the **Frame Summary** pane, **click Frame 3** to display the related data in the **Frame Detail** pane.

19. In the **Frame Details** pane, **expand** the **Domain Name System (response), Answers** lines to view the details in those fields. Use the scrollbar as necessary to locate this header line.


DemoCapturepcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time      Source         Destination         Protocol Length Info
   1 0.000000  192.168.1.132  192.168.1.1         DNS         181 Standard query 0x96c1 A www.polito.it
   2 0.000020                 GemtekTe_cb:6e:1a (… 802.11       46 Acknowledgement, Flags=........C
   3 0.000036  192.168.1.1    192.168.1.132       DNS         174 Standard query response 0x96c1 A www.polito.i…
```

```
    .... .... .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
v Queries
  v www.polito.it: type A, class IN
        Name: www.polito.it
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
v Answers
  > www.polito.it: type CNAME, class IN, cname web01.polito.it
  > web01.polito.it: type A, class IN, addr 130.192.73.1
```

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 29 83 cd f3   .. .i... ....)...
0010  00 00 00 00 01 00 04 00  76 09 c0 00 00 00 c7 a0   ........ v.......
0020  88 02 a2 00 00 14 a5 cb  6e 1a 00 14 a5 cd 74 7b   ........ n.....t{
0030  00 01 02 27 f9 b2 60 ce  00 00 aa aa 03 00 00 00   ...'..`. ........
0040  08 00 45 00 00 68 08 2a  00 00 40 11 ee 85 c0 a8   ..E..h.* ..@.....
0050  01 01 c0 a8 01 84 00 35  04 07 00 54 f8 82 96 c1   .......5 ...T....
0060  81 80 00 01 00 02 00 00  00 00 03 77 77 77 06 70   ........ ...www.p
0070  6f 6c 69 74 6f 02 69 74  00 00 01 00 01 c0 0c 00   olito.it ........
0080  05 00 01 00 01 51 5d 00  11 05 77 65 62 30 31 06   .....Q]. ..web01.
0090  70 6f 6c 69 74 6f 02 69  74 00 c0 2b 00 01 00 01   polito.i t..+....
00a0  00 01 51 5d 00 04 82 c0  49 01 56 1c e2 58         ..Q].... I.V..X
```

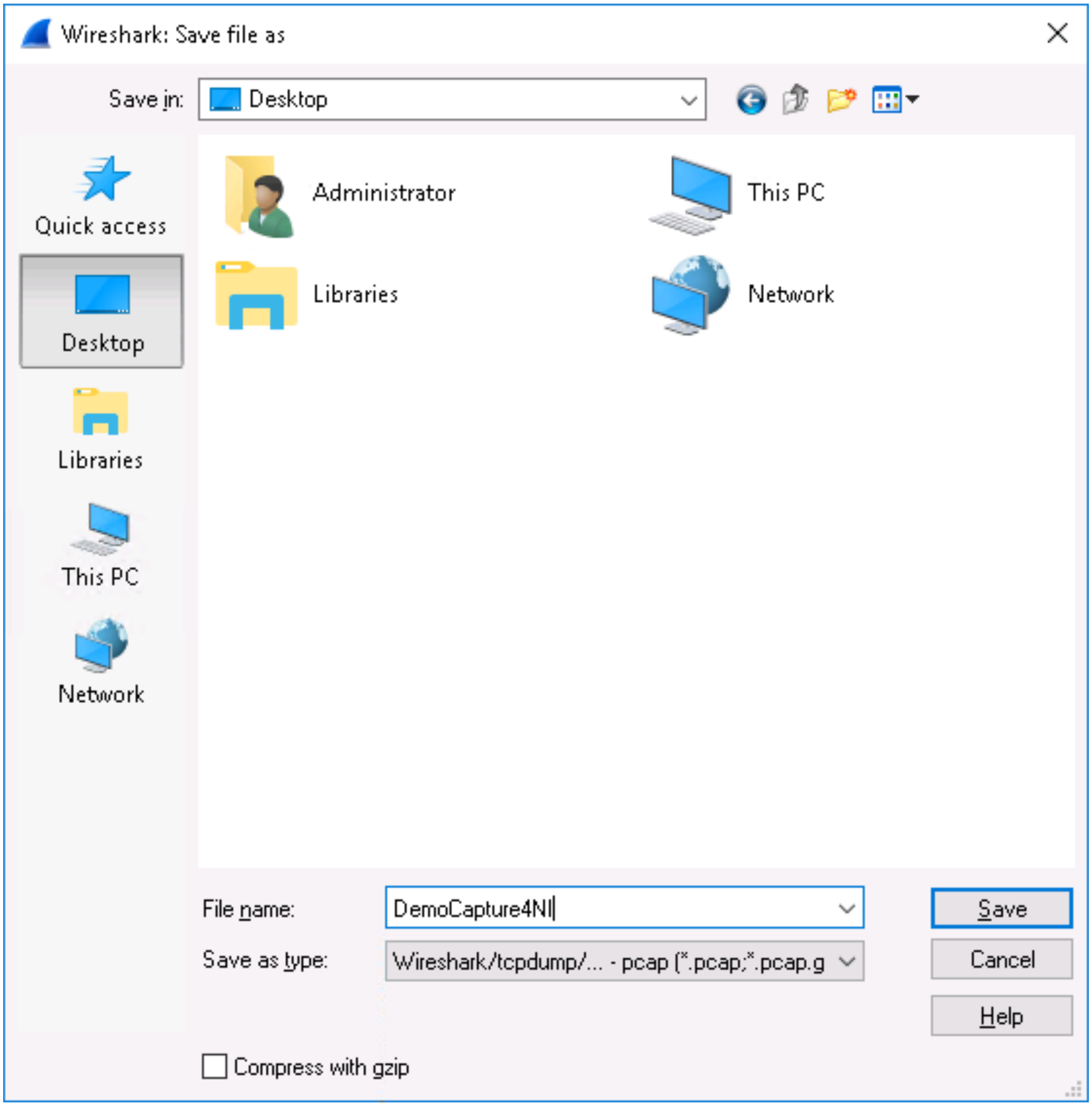
Text item (text), 45 bytes | Packets: 140 · Displayed: 140 (100.0%) · Load time: 0:0.25 | Profile: Default

Figure 10 DNS Response for www.polito.it

20. In the **Frame Details** pane, **expand all the headings in the Answers** section. These fields detail the response to the DNS query. Data shown in these fields includes the IP address for polito.it (130.192.73.1) and other DNS information, such as a DNS *time to live* (or, the time before the DNS cache for this entry must be refreshed) of 23 hours, 59 minutes, 25 seconds. **Make a screen capture** showing the details of **Answers** in those fields. Paste the screen capture into your lab report.

Note: In Part 2 of this lab, you will analyze these same packets using NetWitness Investigator. It is important to realize that NetWitness can also be used to capture and save network traffic without ever using Wireshark, but if you are using Wireshark for packet capture and a cursory analysis as you did in Part 1 of this lab, you will need to save the captured frames in a format that NetWitness can interpret. The current release of NetWitness Investigator does not support the pcapng file format, so you must first save the DemoCapturepcap.pcapng file in the older *.pcap format.

21. **Click "File > Save As"** from the Wireshark menu. **Click** the **Desktop** icon, **select "Wireshark/tcpdump/… - pcap"** from the drop-down option in the **Save as type** box, and **type "DemoCapture4NI"** in the **File name** box.



Save in: Desktop

File name: DemoCapture4NI

Save as type: Wireshark/tcpdump/... - pcap (*.pcap;*.pcap.g

□ Compress with gzip

Figure 11 Wireshark Save As Dialog Box

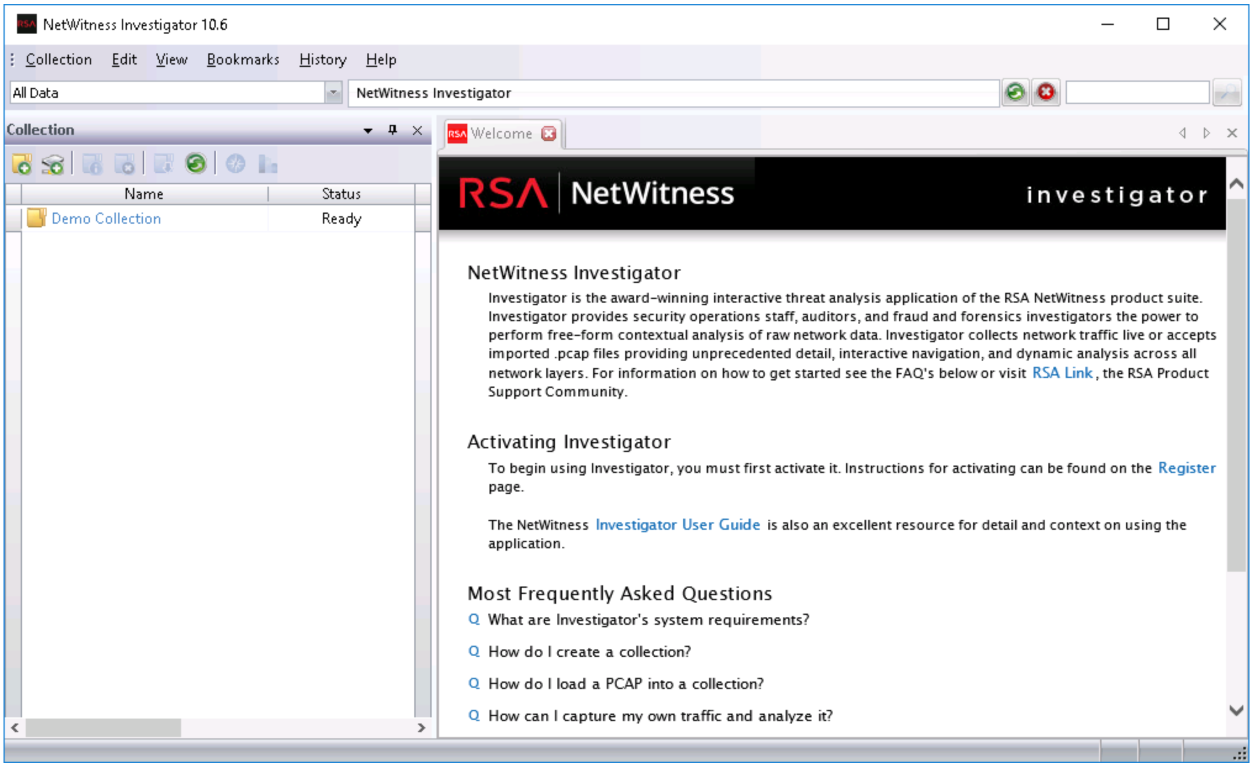
22. **Click "Save"** to save the new **DemoCapture4NI** file in the preferred format for NetWitness Investigator.

23. From the Wireshark menu bar, **click "File > Quit"** to close Wireshark.

Part 2: Compare with NetWitness Investigator

Note: In this part of the lab, you will use NetWitness Investigator to analyze the same packet capture file you reviewed in Part 1 of this lab. Because Wireshark is available for free, it is often used for packet capture and for initial analysis. NetWitness Investigator, on the other hand, requires the purchase of a license for use, so it is often used only by more senior, more skilled, and better trained security analysts for specific types of analysis. Often, investigators, or even clients, with little training can capture needed information with the no-cost Wireshark while a more in-depth security-focused analysis is later done with NetWitness Investigator.

1. On the TargetWindows02 taskbar, **click** the **RSA** icon (RSA) to launch the NetWitness application.


NetWitness Investigator 10.6

NetWitness Investigator

Investigator is the award-winning interactive threat analysis application of the RSA NetWitness product suite. Investigator provides security operations staff, auditors, and fraud and forensics investigators the power to perform free-form contextual analysis of raw network data. Investigator collects network traffic live or accepts imported .pcap files providing unprecedented detail, interactive navigation, and dynamic analysis across all network layers. For information on how to get started see the FAQ's below or visit RSA Link, the RSA Product Support Community.

Activating Investigator

To begin using Investigator, you must first activate it. Instructions for activating can be found on the Register page.

The NetWitness Investigator User Guide is also an excellent resource for detail and context on using the application.

Most Frequently Asked Questions

- What are Investigator's system requirements?
- How do I create a collection?
- How do I load a PCAP into a collection?
- How can I capture my own traffic and analyze it?

Name	Status
Demo Collection	Ready

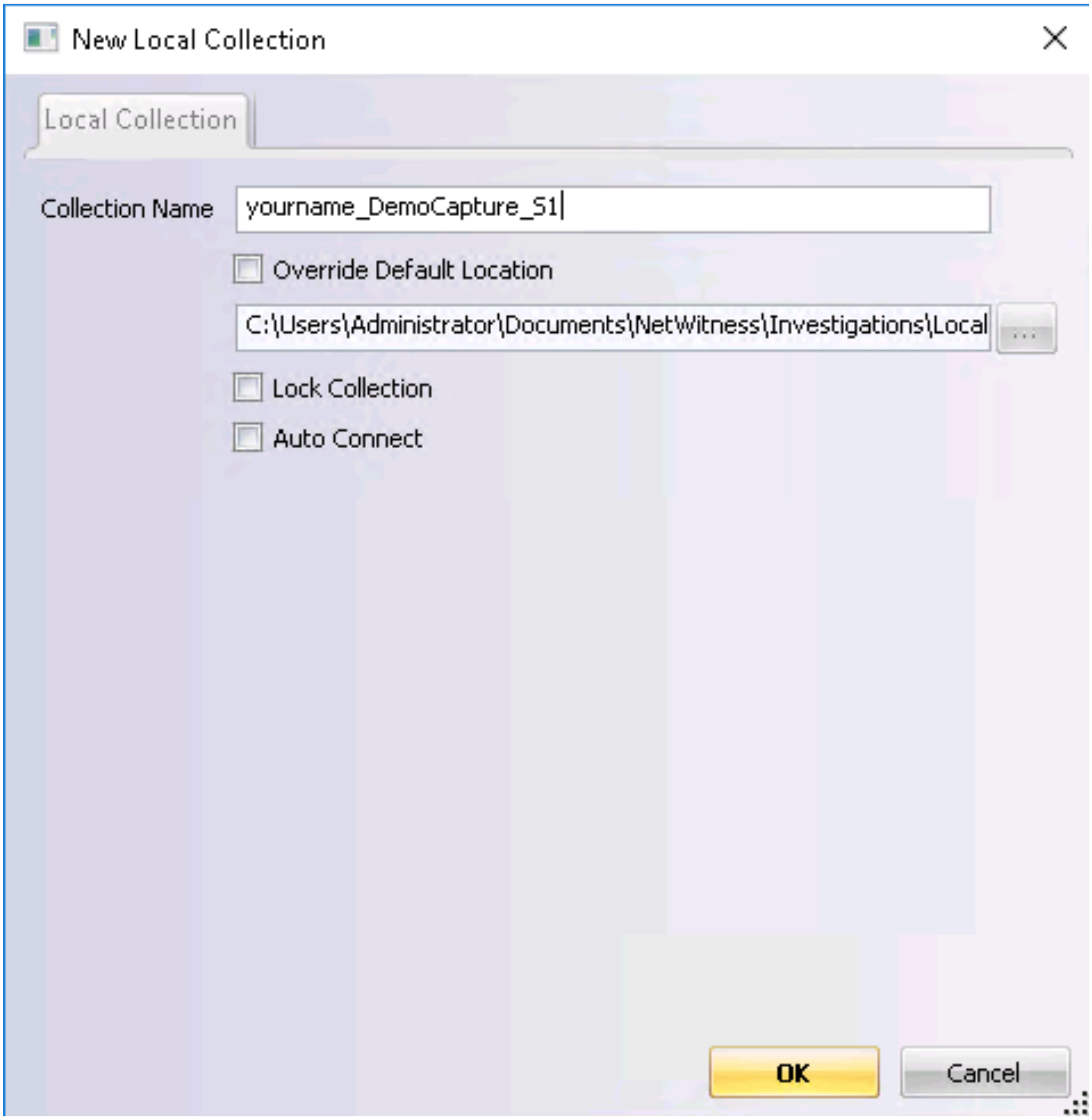
Figure 12 NetWitness Investigator Application

Note: The welcome screen in NetWitness Investigator displays a list of frequently asked questions and links to NetWitness Community, User Guide, and Customer Portal. You are encouraged, though not required, to review this material from your own computer. Remember, the virtual lab does not have access to the Internet by design, so the Internet links will not work in this lab environment.

2. On the **NetWitness Investigator** menu, **select "Collection > New Local Collection"** to open the **New Local Collection** dialog box.

3. In the **Collection Name** box, type ***yourname*_DemoCapture_S1**, replacing *yourname* with your own name, and **click OK** to name the new collection.

   Similar to creating a new file folder, creating a new local collection within NetWitness Investigator provides a place to put the packets from the DemoCapture file. This collection, DemoCapture, will appear in the left pane, the Collection pane of NetWitness Investigator.



Collection Name: yourname_DemoCapture_S1

□ Override Default Location

C:\Users\Administrator\Documents\NetWitness\Investigations\Local

□ Lock Collection

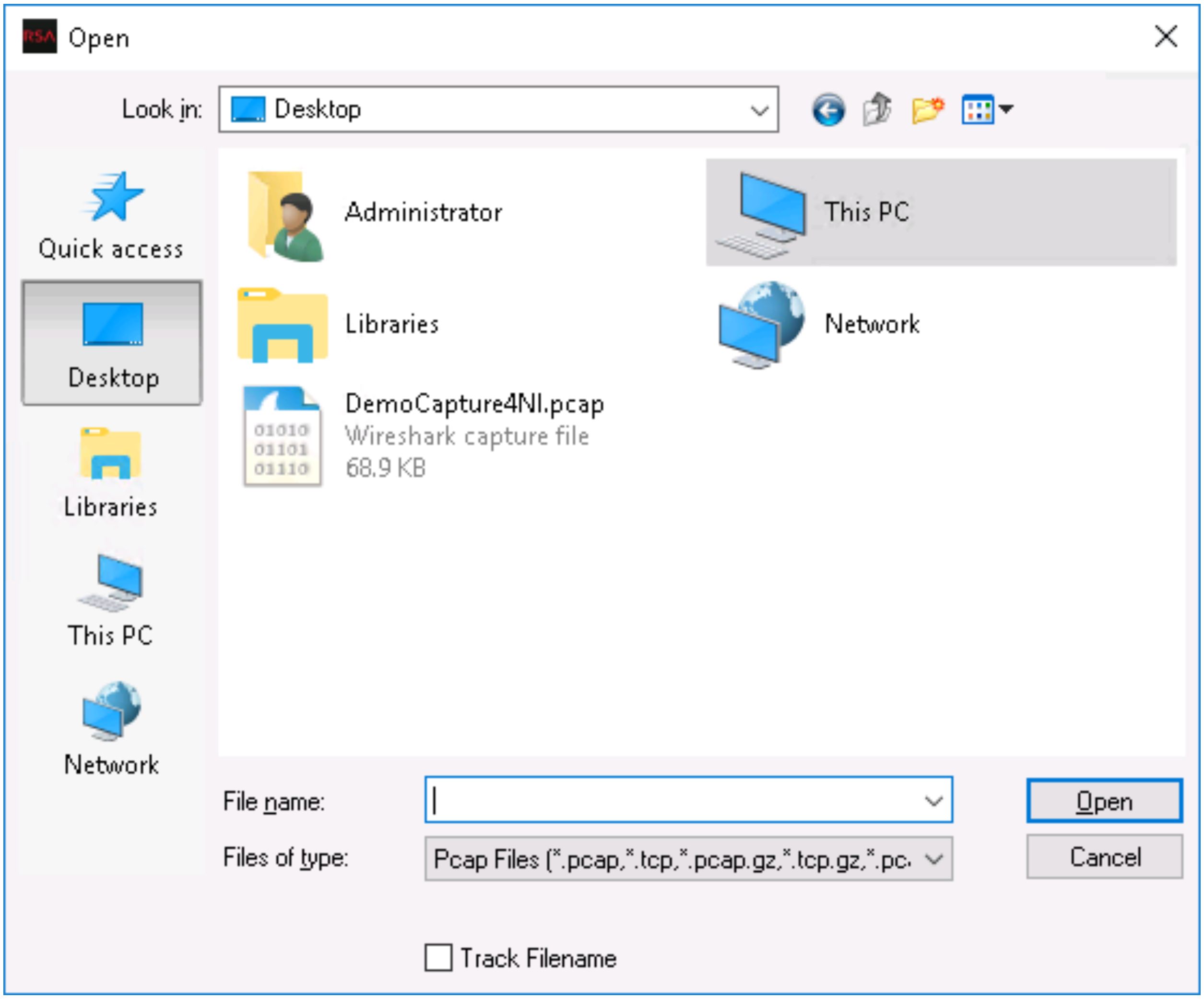
□ Auto Connect

Figure 13 New Local Collection Window

4. In the **Collection** pane, **double-click** the ***yourname*_DemoCapture_S1** collection you just created to activate it and change the status to **Ready**.

5. In the **Collection** pane, right-click the ***yourname*_DemoCollection_S1** and **select Import Packets** from the context menu.

6. In the **Open** dialog box, click the **Desktop** button, then **double-click** the **DemoCapture4NI** file that you saved in **Part 1** to begin the import process.



Look in: Desktop

File name:

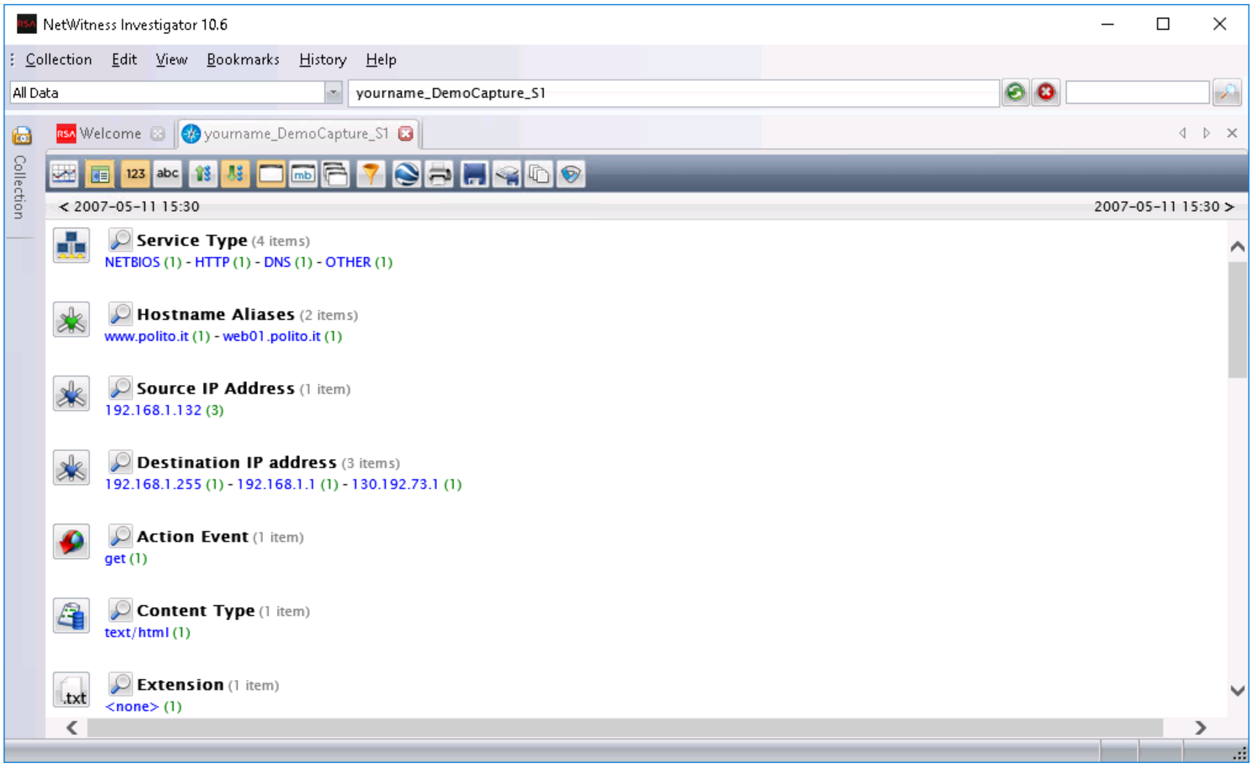
Files of type: Pcap Files (*.pcap,*.tcp,*.pcap.gz,*.tcp.gz,*.pc

Figure 14 Open Dialog Box

7. The **Collection** pane will display a progress report while the import progress is underway. When the import is finished, the new collection will again display a status of **Ready**.

8. When the file has finished importing, **double-click** the ***yourname*_DemoCapture_S1 collection** to open it in NetWitness Investigator.

   The packets from the capture file have been analyzed by NetWitness and all of the reports generated by NetWitness are displayed in the right pane. Use the scrollbar as necessary to view the complete list of reports.


NetWitness Investigator 10.6
Collection Edit View Bookmarks History Help
All Data
Welcome
Collection

yourname_DemoCapture_S1

< 2007-05-11 15:30 2007-05-11 15:30 >

Service Type (4 items)
NETBIOS (1) - HTTP (1) - DNS (1) - OTHER (1)

Hostname Aliases (2 items)
www.polito.it (1) - web01.polito.it (1)

Source IP Address (1 item)
192.168.1.132 (3)

Destination IP address (3 items)
192.168.1.255 (1) - 192.168.1.1 (1) - 130.192.73.1 (1)

Action Event (1 item)
get (1)

Content Type (1 item)
text/html (1)

Extension (1 item)
<none> (1)

Figure 22 NetWitness Reports from the DemoCapture Collection

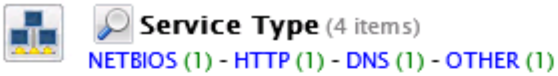
The following table describes the categories that NetWitness Investigator recognizes.

NetWitness Investigator Collection Categories	
SECTION TITLE	**DESCRIPTION**
Service Type	Types of traffic seen on the network.
Source IP Address	Who sent traffic?
Destination IP Address	Who received traffic?
Action Event	Commands seen in the traffic flow.
User Account	User names seen on the network.
Extension	Types of files seen on the network.
Filename	Names of files seen on the network. **Click [open]** to view.
TCP Destination Port	TCP Ports accessed.
UDP Target Port	UDP Ports accessed.
Password	Clear text passwords seen on the network. **Click [open]** to view.

Note: While you will not find any of the low-level wireless information, such as command and control, in NetWitness Investigator that you found in Wireshark, you will find that the kind of sophisticated analysis that requires some work to accomplish within Wireshark is automated by NetWitness Investigator. For instance, the Layer 2 MAC addresses, which in this case are Ethernet, and the Layer 3 IP addresses are available in both Wireshark and NetWitness, but you will not find the transmitter and receiver addresses in NetWitness. What you will find, easily, in NetWitness is information about the geographic location of the transmitter and receiver which, when plotted on Google Earth, can aid an investigation.

You should also notice that where both tools provide the same information, such as the DNS request, the two tools differ in how that information is displayed.

9. Under the **Service Type** category, **click** the **green (1)** link next to the **DNS** link to drill down and get further information about the DNS request.



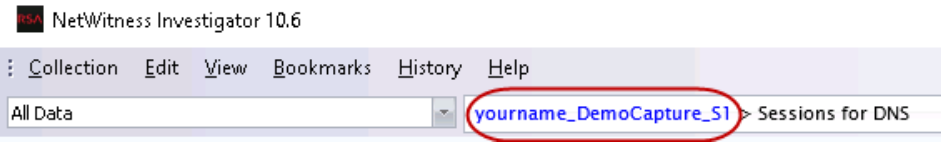
Service Type (4 items)
NETBIOS (1) - HTTP (1) - DNS (1) - OTHER (1)

The **(1)** link that follows the DNS label indicates that there is only one DNS request in this packet capture file. In the next steps, you will investigate this DNS request and compare the results against the Wireshark findings.

10. **Make a screen capture** of the DNS query showing the **Hostname Alias, the Source IP Address, and the Destination IP Address** fields and **paste** it into your Lab Report file.

11. In the Lab Report file, **compare in 200 words** the information provided by NetWitness to the screen capture you made with Wireshark (Part 1, Step#20).

12. From the NetWitness Investigator navigation bar, **click** the ***yourname*_DemoCapture_S1 link** to return to the high-level analysis of the entire packet capture file.

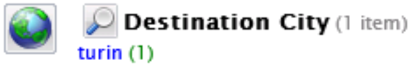


13. In the NetWitness Investigator window, use the scrollbar to **locate** the **Ethernet Source** and **Ethernet Destination** categories. **Compare in 200 words** the information you can get from these categories with the Frame Control information captured by Wireshark (See Figure 6 in Part 1).

14. From the NetWitness navigation bar, **click** the ***yourname*_DemoCapture_S1** link to return to the high-level analysis of the entire packet capture file.

15. In the NetWitness Investigator window, use the scrollbar to **locate** the **Destination City** category.

16. Under the **Destination City** category, **click** the **green (1)** link next to the **Turin** link to reveal additional details from this report.



Destination City (1 item)
turin (1)

From the data, you can determine that the transaction originated in Turin, Italy, and was an HTTP get request in which a website was retrieved. NetWitness has done a lot of analysis of the higher-level transaction without revealing the lower level frame or packet detail to the user.

Note: Although it is accurate to say that the Top-Level Domain (TLD) ".it" belongs to Italy, there is no assurance that the website is physically located in Italy, only that a domain name is registered with the appropriate registrar for the .it TLD. Only by physically finding the server hosting the website using geolocation technology such as IP-geolocation or triangulation using PINGs is it possible to determine the actual physical location of the server.

17. From the NetWitness Investigator menu bar, **click Collection** and **select Exit** to close the **NetWitness Investigator** window.

18. **Close** the remote **TargetWindows02** connection.

19. **Close** the lab environment.

Note: Having investigated the same capture file with both tools, Wireshark and NetWitness Investigator, you are now better equipped to determine which tool is appropriate for specific tasks. You might also realize that using both tools together might be required to show a complete picture for a forensic investigation.

Also, remember, that in any forensic investigation, special care must be taken to protect the chain of custody for any evidence used in legal proceedings. It is important to realize that capture files are just digital files and can easily be manipulated and edited and should be handled as would any volatile digital evidence. Maintaining chain of custody is particularly important to ensure the recovered evidence is admissible in a court of law.

Part 3: Challenge Question

After research on the Wireshark tool, discuss its current limitation (in 200 words).