Before You Begin

Welcome! The Virtual Security Cloud Labs are your opportunity to gain valuable hands-on experience with professional-grade tools and techniques as you work through the guided lab exercises provided in the on-screen lab manual. The use of virtualization enables you to perform all of the tasks in the lab manual in a live environment without putting your personal device or institution's assets at risk.

Before you begin the guided lab exercises, please review the following preparation checklist.

1. **Run the** System Checker. The System Checker will confirm that your browser and network connection are ready to support virtual labs.

2. **Review the** Common Lab Tasks document. This document provides an overview of the virtual lab environment and outlines several of the recurring tasks you may need to complete your lab exercise.

3. **When you've finished, use the Disconnect button to end your session and create a StateSave**. To end your lab session and save your work, click the Disconnect button in the upper-right corner of the Lab View toolbar. When prompted, assign a name for your StateSave (we recommend using the Section, Part, and Step number where you stopped) and click Continue. Please note that a StateSave will preserve any changes written to disk in your lab session. A StateSave will not preserve any open windows or active processes, similar to restarting your computer.
   If you close your browser window without disconnecting, your lab session will automatically end after 5 minutes.

4. Technical Support **is here to help!** Our technical support team is available 24/7 to help troubleshoot common issues.
   Please note that the 24/7 support team is Level 1 only, and cannot assist with questions about lab content or the array of software used in the labs. If you believe you've identified an error in the lab guide or a problem with the lab environment, your ticket will be escalated to the Jones & Bartlett Learning product team for review. In the meantime, we recommend resetting the lab (Options > Reset) or reaching out to your instructor for assistance.

Introduction

It is critical that security administrators have a clear understanding of the type and volume of traffic that is considered “normal” on their networks. They must also have the ability to detect anomalous traffic which could indicate a past or ongoing attack. Two tools that can prove very useful are packet capturing tools and traffic analyzers. Wireshark is a popular tool for capturing network traffic in promiscuous mode. Wireshark is analogous to the TCP Dump tool found on Linux. Wireshark is able to filter though large amounts of data quickly and help an administrator understand a full “conversation” between systems at the packet level. NetWitness is a popular tool from RSA that can read saved TCP Dump and Wireshark packet captures. Tools like Wireshark are used to capture data packets over time (continuously or overnight). The data it captures can then be imported via a .pcap file to NetWitness Investigator where it cleanly parses and displays the data for analysis by the administrator.

One of the most important tools needed for information systems security practitioners is a packet capture and protocol analysis tool. Wireshark is a freeware tool providing basic packet capture and protocol decoding capabilities. NetWitness Investigator provides security practitioners with a deep packet inspection tool used for examining everything from the data link layer up to the application layer.

In this lab, you will use common applications to generate traffic and transfer files between the machines in this lab. You will capture data using Wireshark and review the captured traffic at the packet level. Then, you will use NetWitness Investigator, a free tool that provides security practitioners with a means of analyzing a complete packet capture, to review the same traffic at a consolidated level.

Learning Objectives

Upon completing this lab, you will be able to:

1. Use Wireshark to capture live IP, ICMP, TCP, and UDP traffic from Telnet, FTP, TFTP, and SSH sessions

2. Use Wireshark and NetWitness Investigator as a protocol analysis tool

3. Analyze the packet capture data in both Wireshark and NetWitness Investigator and be able to identify the traffic generated in the lab

4. Examine captured packet traces to view clear text and ciphertext

Lab Overview

Each section of this lab is assigned at your instructor's discretion. Please consult your instructor to confirm which sections you are required to complete for your lab assignment.

SECTION 1 of this lab has three parts, which should be completed in the order specified.

1. In the first part of the lab, you will generate common network traffic using protocols such as Telnet, Secure Shell (SSH), File Transfer Protocol (FTP), and Remote Desktop Protocol (RDP).

2. In the second part of the lab, you will use Wireshark to analyze the data captured in Part 1 of this lab.

3. In the third part of the lab, you will use NetWitness Investigator to analyze the same Wireshark packet capture you saved in Part 2.

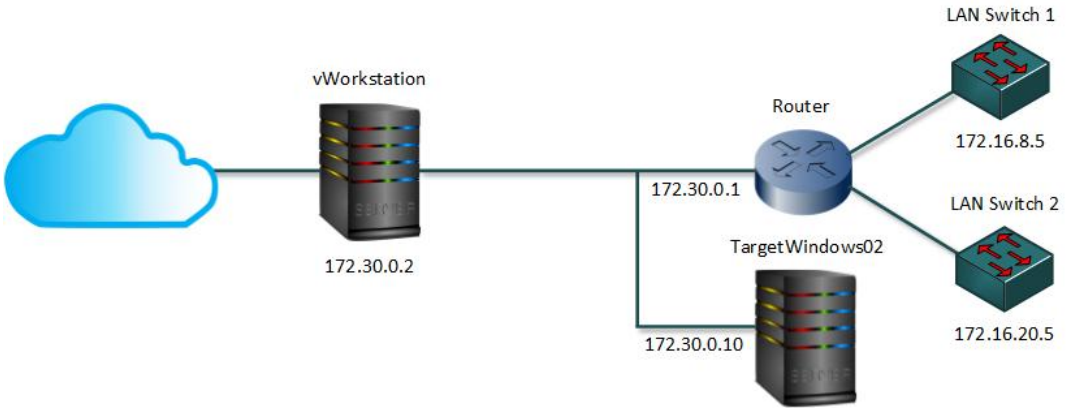
SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods**.**

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab. You will answer questions and complete challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work, similar to what you will encounter in a real-world situation.

Topology

This lab contains the following virtual devices. Please refer to the network topology diagram below.

- vWorkstation (Windows Server 2016)
- TargetWindows02 (Windows Server 2016)
- Cisco Router (Cisco IOS Emulator)
- LAN Switch 1 (Cisco IOS Emulator)
- LAN Switch 2 (Cisco IOS Emulator)



Tools and Software

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

- NetWitness Investigator
- PuTTY
- Tftpd64
- Wireshark

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1:

1. Lab Report file including screen captures of the following;

- *yourname*_tftp.txt in the Tftpd64 directory;
- the FileZilla window displaying the successful file transfer;
- captured file transfer in the Wireshark window;
- password information for the *yourname*_S1_Collection;

2. Files downloaded from the virtual environment:

- *yourname*_S1_PacketCapture.pcap;

3. Any additional information as directed by the lab:

- none;

4. Lab Assessment (worksheet or quiz - see instructor for guidance)

SECTION 2:

1. Lab Report file including screen captures of the following:

- *yourname*_S2_tftp.txt in the Tftpd64 directory;
- the FileZilla window displaying the successful file transfer;
- captured file transfer in the Wireshark window;
- NetWitness session detail for the *yourname*_S2_tftp.txt file transfer;

2. Files downloaded from the virtual environment:

- *yourname*_S2_PacketCapture.pcap;
- *yourname*_S2_Collection.xml;

3. Any additional information as directed by the lab:

- the Wireshark frame number of the transferred file.

SECTION 3:

1. Analysis and Discussion
2. Tools and Commands
3. Challenge Exercise

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverable(s).

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

Part 1: Generate Network Traffic

Note: In the next steps, you will start a Wireshark packet capture and open and close several common tools to generate traffic and transfer files between machines in this lab. Wireshark will continue running in the background until you manually stop the capture process later in this lab. You will analyze the captured packets in the second part of this 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 TargetWindows02.

   If prompted, **type** the following credentials and **click OK**.

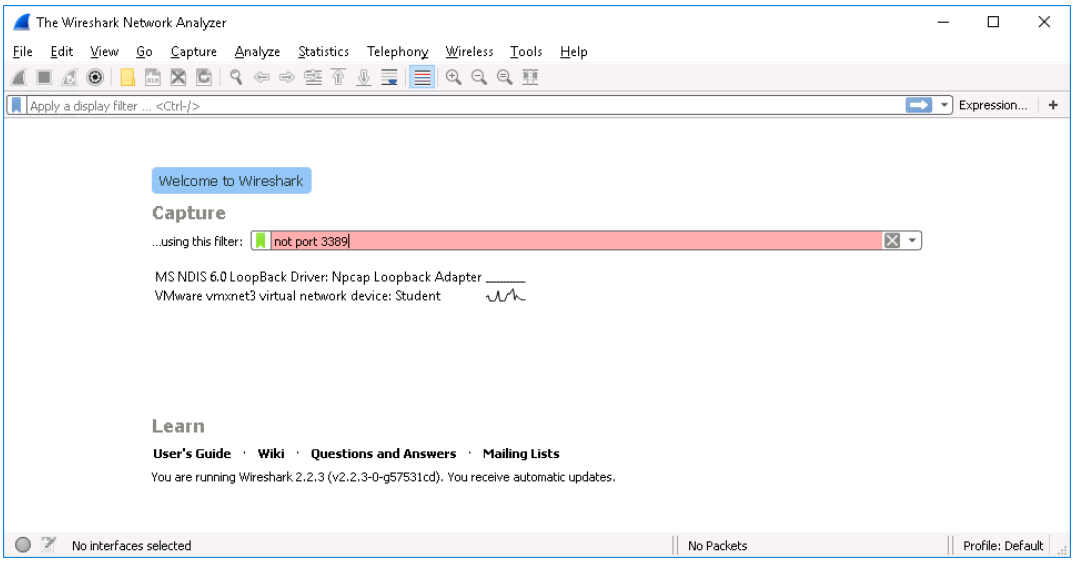
   - Username: **`Administrator`**
   - Password: **`P@ssw0rd!`**

   The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

3. From the TargetWindows02 taskbar, **click** the **Wireshark icon** (a blue shark fin) to open the

Wireshark application.

Wireshark is a protocol analyzer tool (sometimes called a “packet sniffer”). It is used to capture IP traffic from a variety of sources. The main screen of Wireshark includes details about the current capture configuration. From this screen, analysts can select recently used filters from the drop-down menu, or type a custom filter command to quickly sort the captured data.



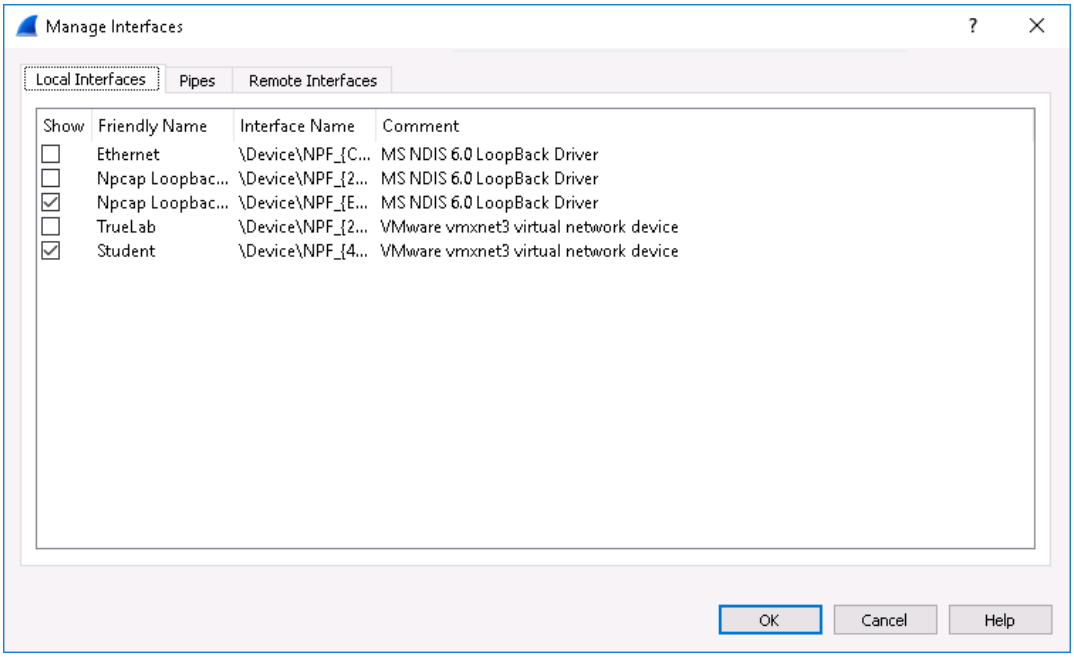
Wireshark main screen

4. From the Wireshark menu bar, **click Capture** and **select Options** to open the Capture Interfaces window.

5. In the Capture Interfaces window, **click** the **Manage Interfaces button** to open the Manage Interfaces dialog box.

6. In the Manage Interfaces dialog box, **verify** that the **Student** and **Npcap Loopback Adapter interfaces** are selected, as shown in the following figure.

   The student interface is the lab environment that you are working in. Selecting this interface ensures that Wireshark can analyze traffic from areas of the network that are visible to students.

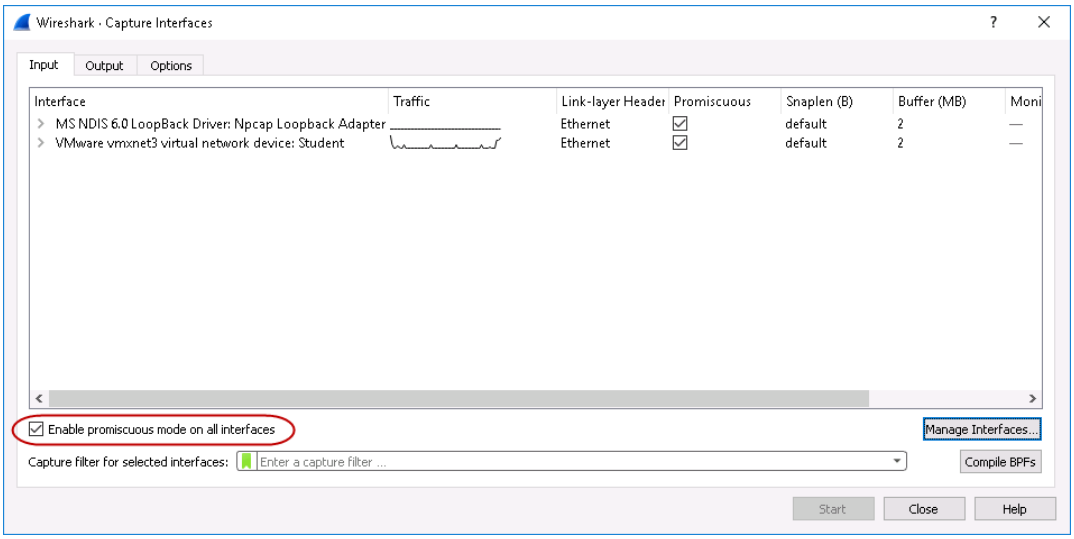


Student interface

7. **Click OK** to close the Manage Interfaces dialog box.

8. In the Capture Interfaces window, **verify** that the **Enable promiscuous mode on all interfaces checkbox** is selected.

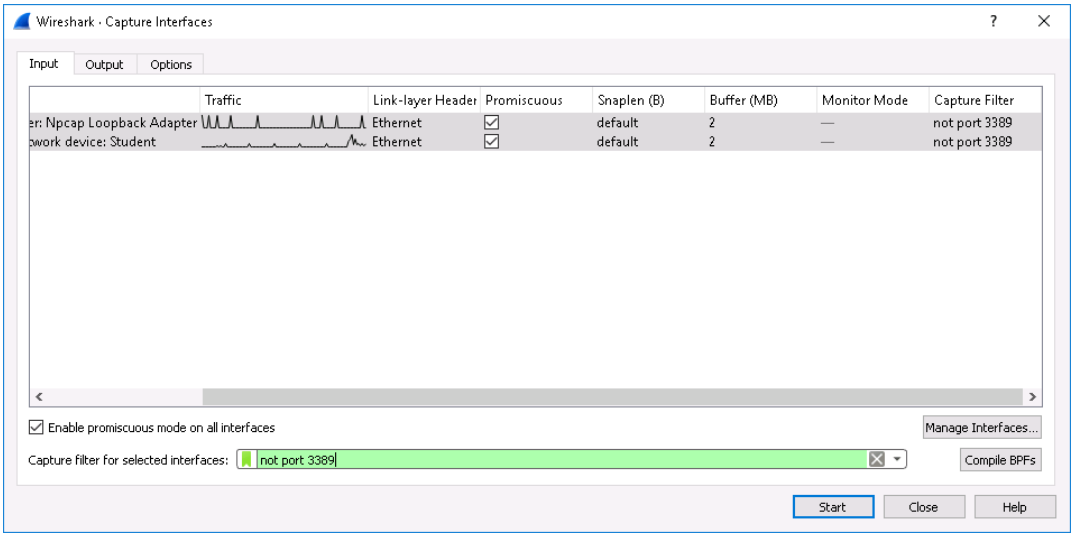
   Promiscuous mode allows Wireshark, or any other application, to capture packets destined to any host on the same subnet or virtual LAN (VLAN). Without this option selected, Wireshark would only capture packets to and from the TargetWindows02 machine.



Verify promiscuous mode

9. In the Capture Interfaces window, **hold down Ctrl** and **click** the **Student** and **Npcap Loopback Adapter interfaces** to select both interfaces.

10. In the Capture filter for selected interface box, **type** `not port 3389` to filter out the packets that are generated between the vWorkstation and TargetWindows02 systems as part of the RDP connection.



Select interfaces

11. **Click Start** to close the Capture Interfaces window and begin the packet capture.

Note: In the next steps, you will generate traffic for Wireshark to capture.

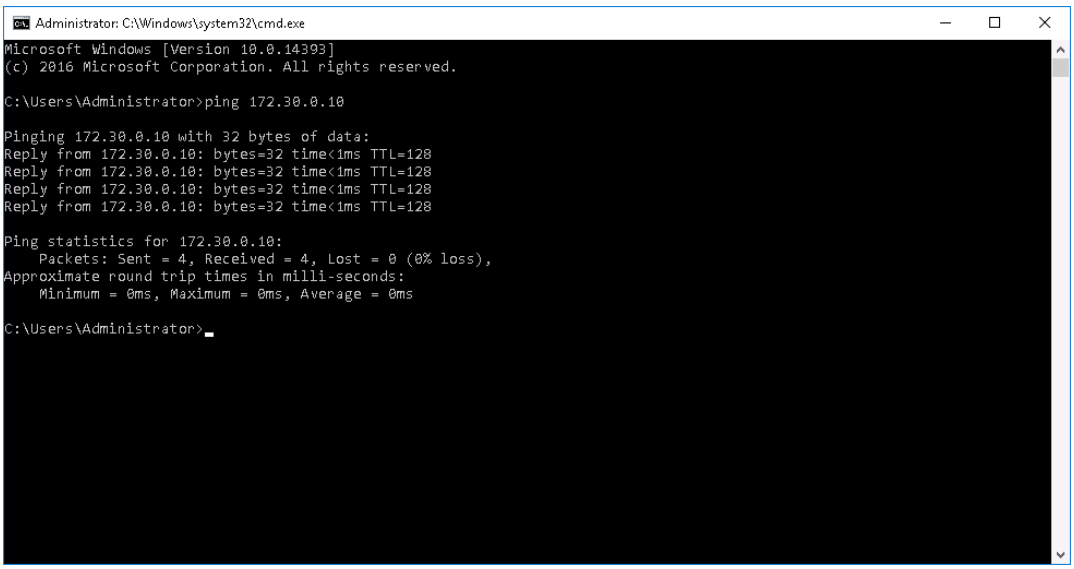
12. **Minimize** the **remote TargetWindows02 connection** to return to the vWorkstation desktop.

13. On the vWorkstation taskbar, **right-click** the **Windows Start icon** and **select Run** from the menu.

14. In the Run dialog box, **type** `cmd` and **click OK** to open a command prompt window.

15. At the command prompt, **type** `ping 172.30.0.10` (the IP address of the TargetWindows02 machine) and **press Enter** to ping the TargetWindows02 machine.

    You will see four successful replies from 172.30.0.10.



Ping TargetWindows02

16. At the command prompt, **type** `exit` and **press Enter** to close the command prompt window.

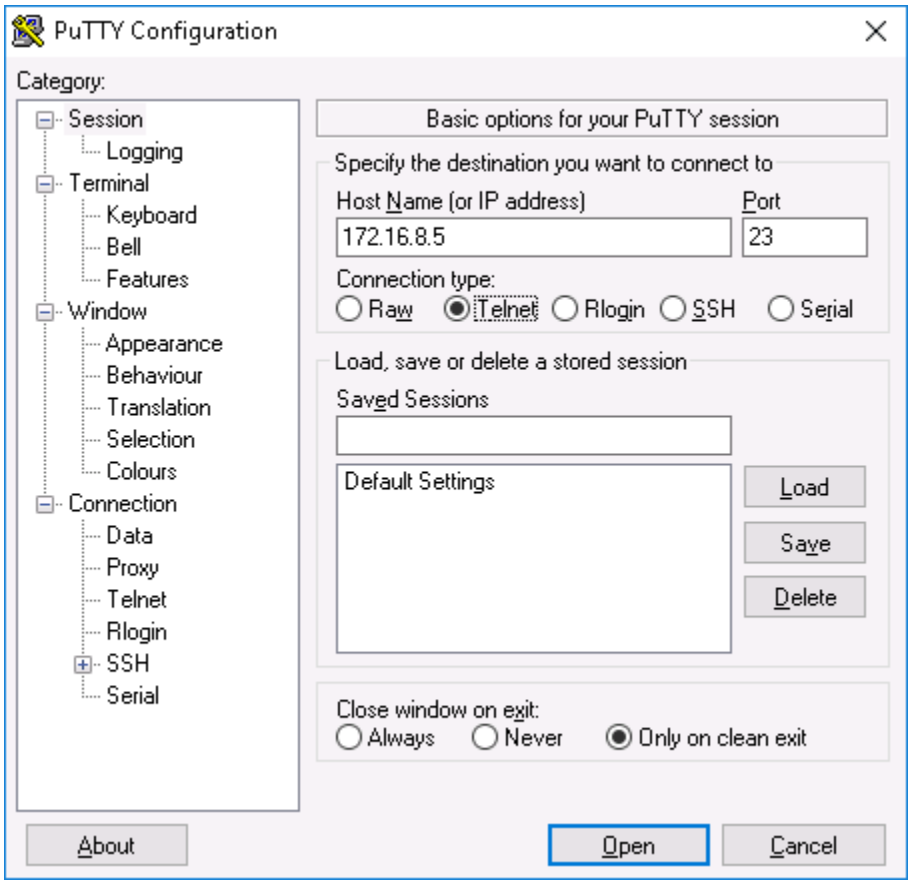
17. **Restore** the **remote TargetWindows02 connection**.

18. **Minimize** the **Wireshark window**.

19. On the TargetWindows02 desktop, **double-click** the **putty icon** to start the PuTTY application.

20. In the Host Name (or IP address) box, **type** `172.16.8.5` (the IP address for LAN Switch 1).

21. In the Connection type section, **click** the **Telnet radio button**, then **click Open** to launch a terminal console on the host machine using an unsecure Telnet connection.

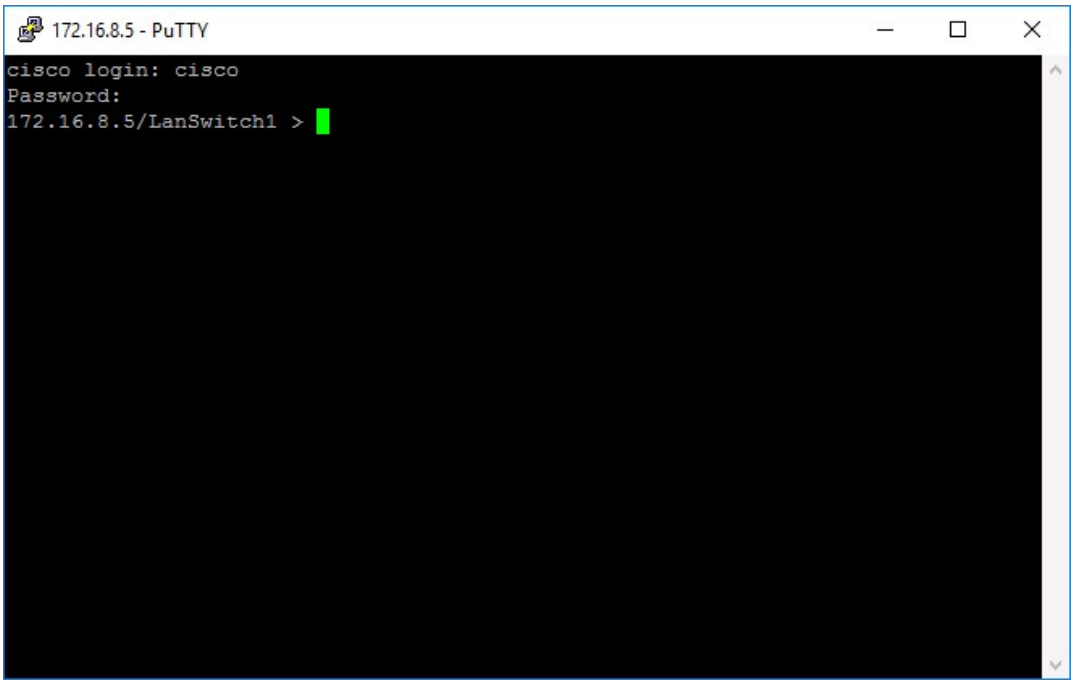


Configure PuTTY for Telnet

22. At the login prompt, **type** the following credentials, and **press Enter** after each entry:

    - Login: **`cisco`**
    - Password: **`cisco`**

Once successfully logged in, the command prompt, 172.16.8.5/LanSwitch1>, is displayed.



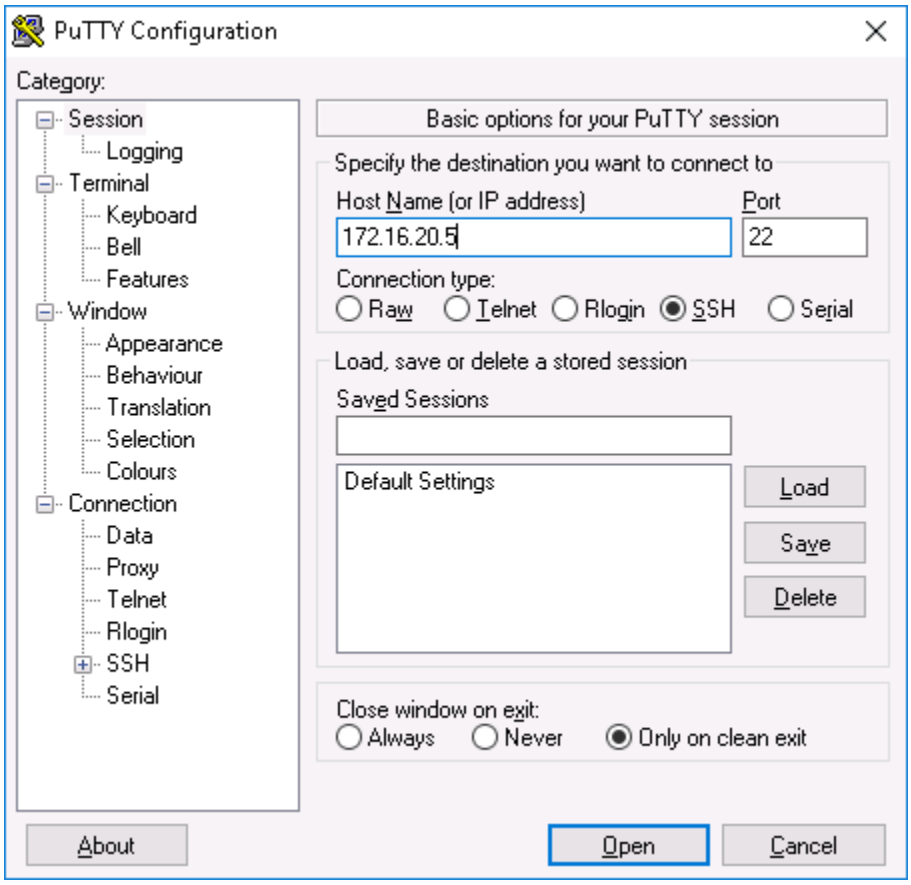
Unsecure login

23. In the terminal console window, **type** `quit` and **press Enter** to close the terminal console session to LAN Switch 1.

24. On the TargetWindows02 desktop, **double-click** the **putty icon** to start the PuTTY application again.

25. In the Host Name (or IP address) box, **type** `172.16.20.5`, the IP address for LAN Switch 2.

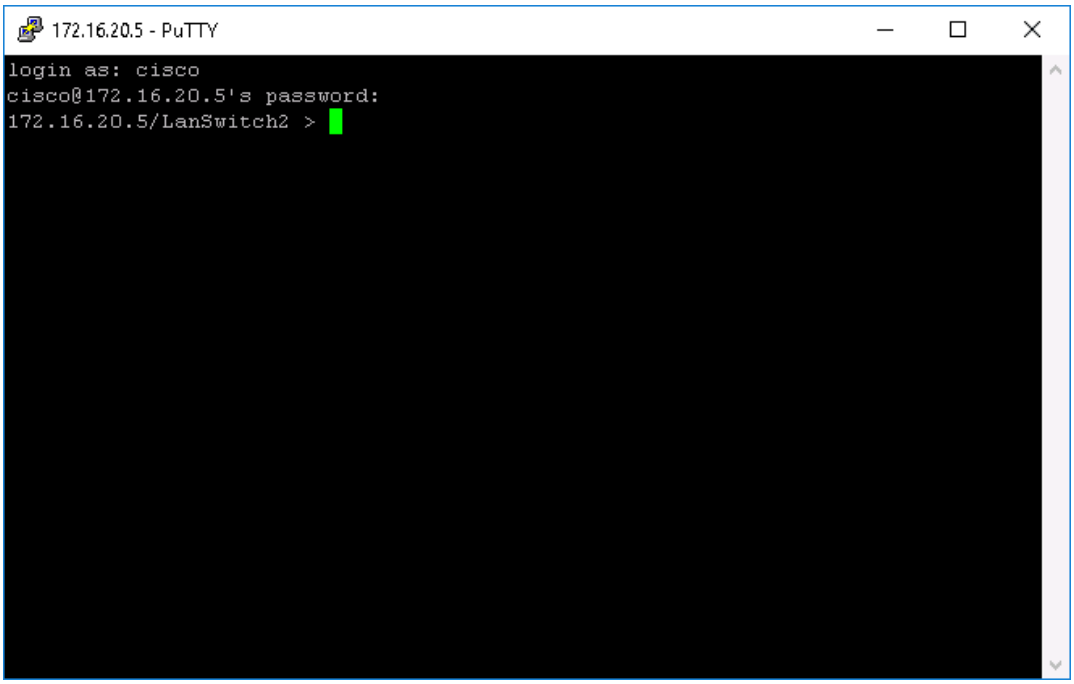
26. In the Connection type section, **click** the **SSH radio button**, then **click Open** to launch a terminal console on the host machine using the Secure Shell (SSH) protocol.



Configure PuTTY for SSH

27. At the login prompt, **type** the following credentials and **press Enter** after each entry:

    - Login: **`cisco`**
    - Password: **`cisco`**



Secure login

28. In the terminal console window, **type** `quit` and **press Enter** to close the terminal console session to LAN Switch 2.

29. On the TargetWindows02 desktop, **double-click** the **Tftpd64 icon** to launch the Tftpd64 application.

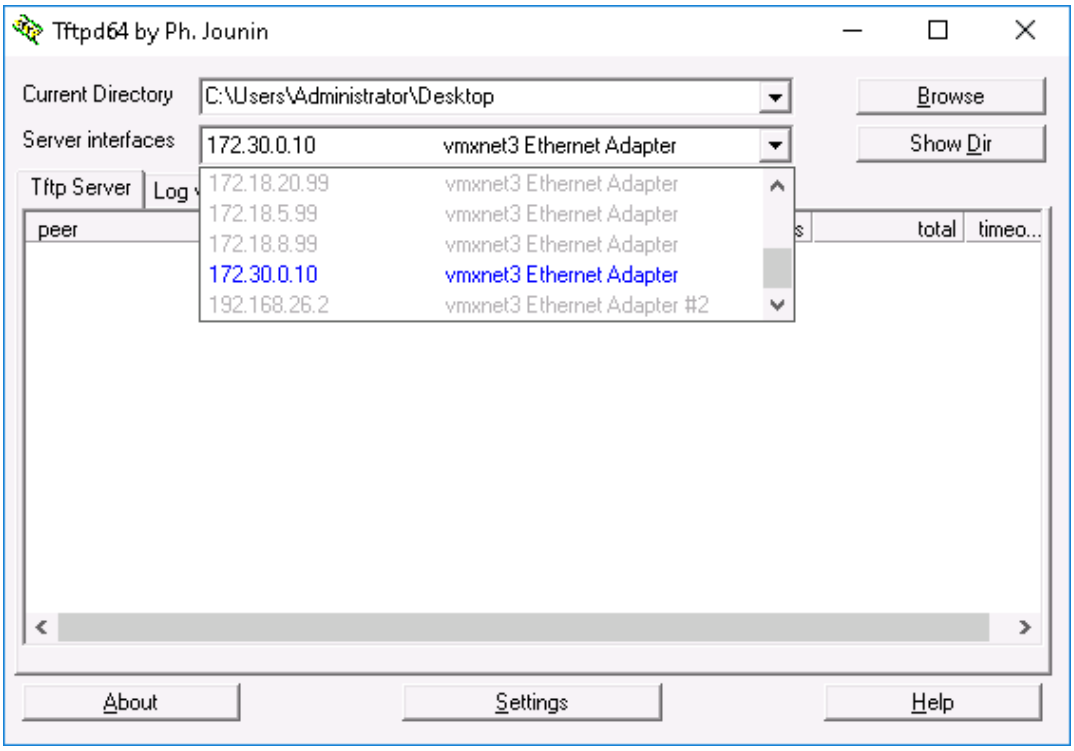
    The Tftpd64 application uses TFTP (Trivial File Transfer Protocol) to send (put) or receive (get) files between computers.

30. In the Tftpd64 window, **click** the **Browse button**, then **scroll** to the top of the **Browse for Folder** list, **select Desktop**, and **click OK**. This will change the Current Directory field to C:\Users\Administrator\Desktop.

31. From the Server interfaces drop-down menu, **select 172.30.0.10** (the IP address for TargetWindows02) to establish TargetWindows02 as a TFTP server.

    The local TFTP server will now listen on UDP port 69 on the 172.30.0.10 interface for a file

transfer. In the next steps, you will transfer a file to the directory shown in the Current Directory box using TFTP.



Start the TFTP64 Server

32. **Minimize** the **remote TargetWindows02 connection** to return to the vWorkstation desktop.

    If necessary, **minimize** the **Connections folder**.

33. On the vWorkstation desktop, **right-click** anywhere and **select New > Text Document** from the context menu.

34. With *New Text Document* highlighted, **type** ***yourname*_tftp**, replacing *yourname* with your own name, and **press Enter** to name the new file.

35. On the vWorkstation desktop, **double-click** the ***yourname*_tftp file** you just created to open it in Notepad.

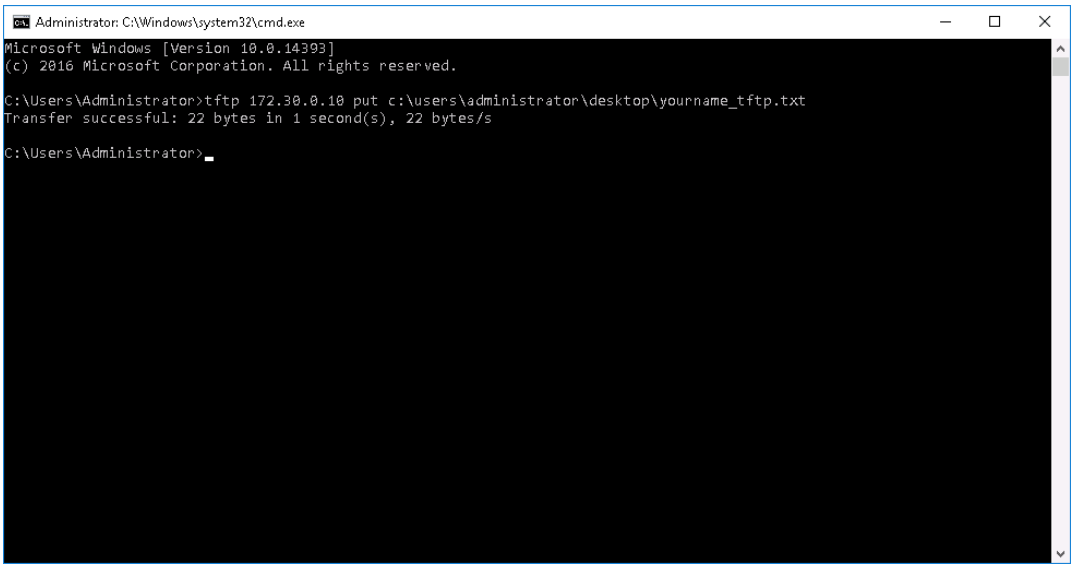
36. In the Notepad window, **type** `This is a test of TFTP`, then **select File > Exit** from the Notepad menu and **click Save** when prompted.

37. On the vWorkstation taskbar, **right-click** the **Windows Start icon** and **select Run** from the menu.

38. In the Run dialog box, **type** `cmd` and **click OK** to open a command prompt window.

39. At the command prompt, **type** `tftp 172.30.0.10 put c:\users\administrator\desktop\`***`yourname`***`_tftp.txt` and **press Enter** to transfer the file to the TargetWindows02 desktop.

    You will see confirmation of a successful TFTP file transfer of the TFTP.txt from the vWorkstation desktop to TargetWindows02.

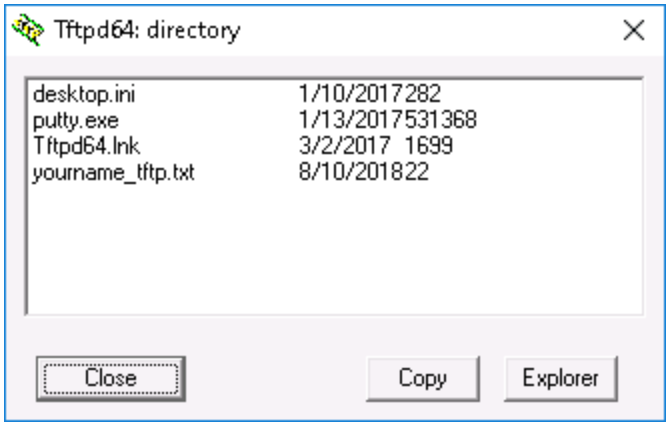


TFTP file transfer confirmation

40. At the command prompt, **type** `exit` and **press Enter** to close the command prompt window.

41. **Restore** the **remote TargetWindows02 connection**.

42. In the Tftpd64 window, **click** the **Show Dir button** to confirm the file transfer.



Successful TFTP transfer

43. **Make a screen capture** showing ***yourname*_tftp.txt in the Tftpd64 directory** and **paste** it into your Lab Report file.

44. **Click Close** to close the directory window.

45. **Close** the **Tftpd64 window**.

46. On the TargetWindows02 desktop, **double-click** the **FileZilla Server Interface icon** to launch the FileZilla Server application.

47. **Minimize** the **remote TargetWindows02 connection** to return to the vWorkstation.

48. On the vWorkstation taskbar, **click** the **FileZilla icon** to launch the FileZilla Client application.

49. **Maximize** the **FileZilla Client window**.

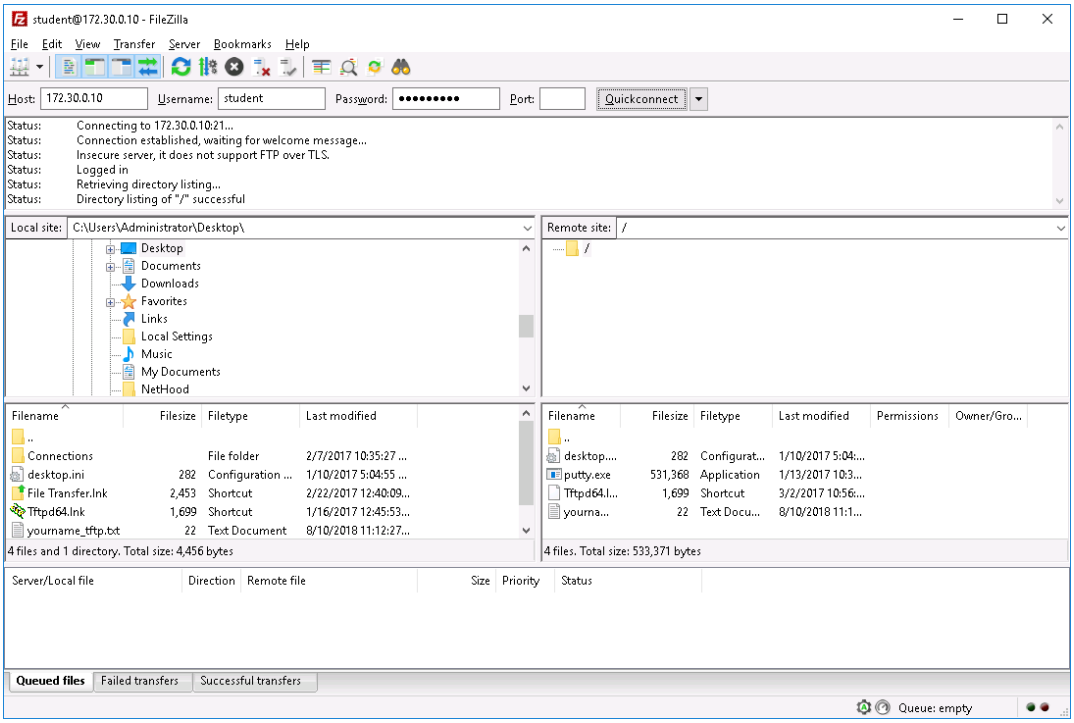
50. In the FileZilla Quickconnect bar, **type** the following details, then **click** the **Quickconnect button** to connect to the FileZilla Server application on TargetWindows02.

    - Host: **`172.30.0.10`**
    - Username: **`student`**
    - Password: **`P@ssw0rd!`**
    - Port: **`21`**

51. In the center pane of the FileZilla window, **navigate** to the **Desktop** in both the Local site and the Remote site panes:

    - Local site: (**C:\Users\Administrator\Desktop**)
    - Remote site: (***/***)

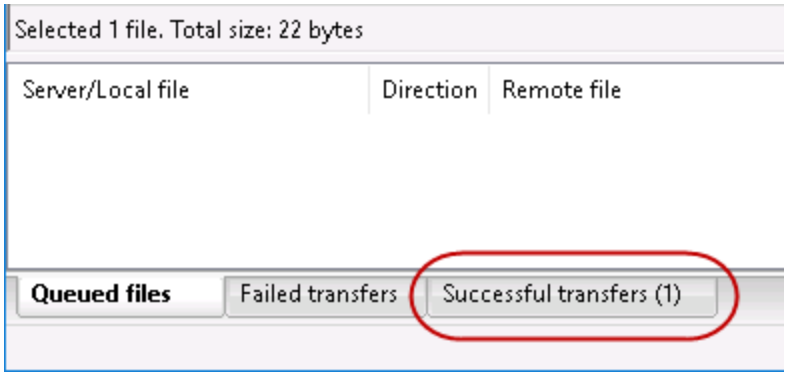
    You can drag the borders between any of the FileZilla frames to adjust the view to ensure that you can see the entire filename and ensure that you are selecting the correct file. When the download process is complete, use the scrollbar in the Local pane to see the new file.



Connect to TargetWindows02 using the FileZilla

52. In the Remote site pane, **right-click** the **yourname_tftp.txt file** and **select Download** from the context menu to transfer the file from the TargetWindows02 desktop to the vWorkstation desktop. When prompted with a notification that the target file already exists, **select Overwrite** and **click OK**.

    When a file is successfully transferred, FileZilla will display a blue success pop-up and the bottom of the FileZilla window will indicate the transfer has taken place.



FTP file transfer

53. **Make a screen capture** showing **the FileZilla window displaying the successful file transfer** and **paste** it into your Lab Report file.

54. **Close** the **FileZilla Client window**.

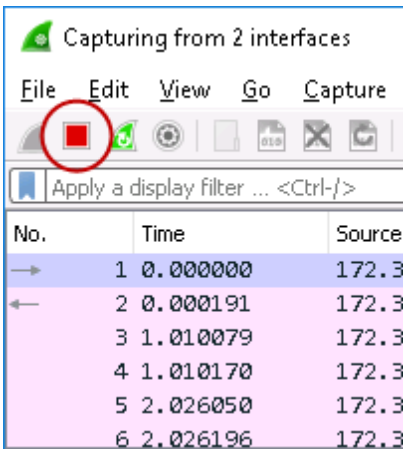
55. **Restore** the **remote TargetWindows02 connection**.

56. **Close** the **FileZilla Server window**.

57. On the TargetWindows02 taskbar, **click** the **Wireshark icon** to restore the Wireshark

application.

58. On the Wireshark toolbar, **click** the red **Stop icon** to stop the packet capture process.



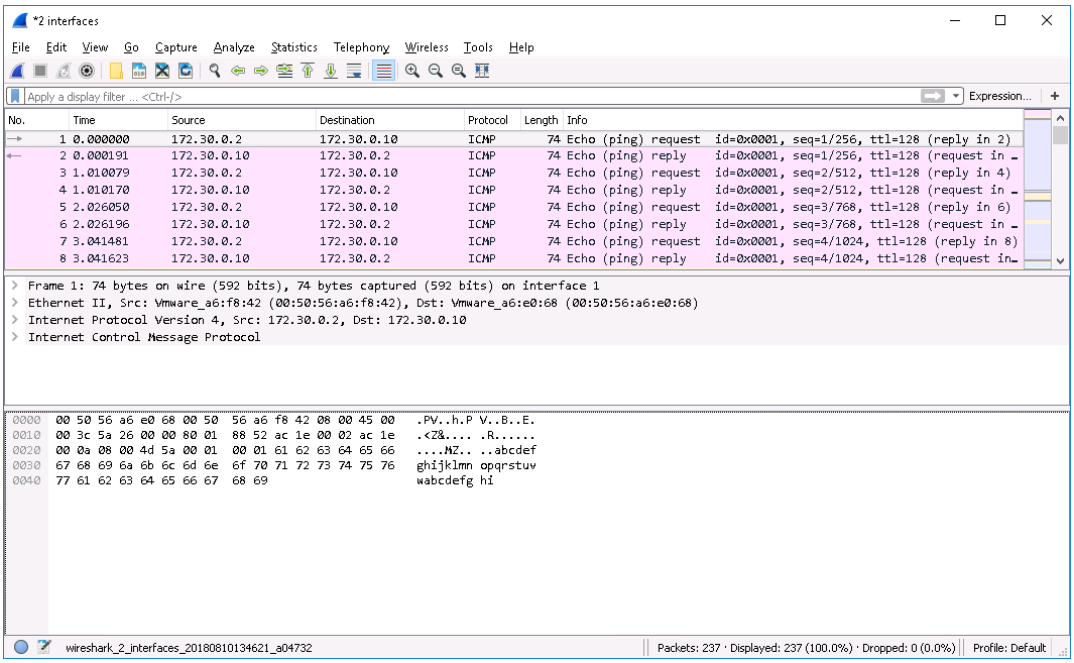
Stop the packet capture

Part 2: Analyze Traffic using Wireshark

Note: While it is possible to scroll through all of the packets captured by Wireshark to find what you are looking for, it is far easier to use display filters. Display filters enable you to find only the traffic you wish to analyze. In the next steps, you will use display filters to analyze the traffic generated in the first part of this lab.

Because this data was captured live during Part 1 of the lab, you will notice that your display does not match the images in this part of the lab. This is normal, and you will still be able to complete the steps.

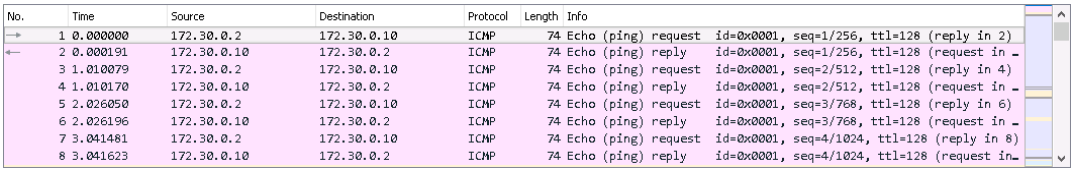
1. If necessary, **maximize** the **Wireshark window**.



Wireshark window

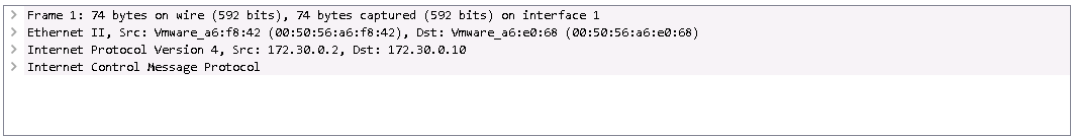
Exploring Wireshark The Wireshark window opens with the detailed information about the packets captured in three panes. Use your mouse to drag the borders of any pane up or down to change its size.

- The top pane of the Wireshark window contains all of the packets that Wireshark has captured, in time order, and provides a summary of the contents of the packet in a format close to English. Keep in mind that the content will be different depending on where you capture packets in the network. Also remember that the "source" and "destination" are relative to where a packet is captured. This area of the Wireshark window is referred to as the *frame summary*.



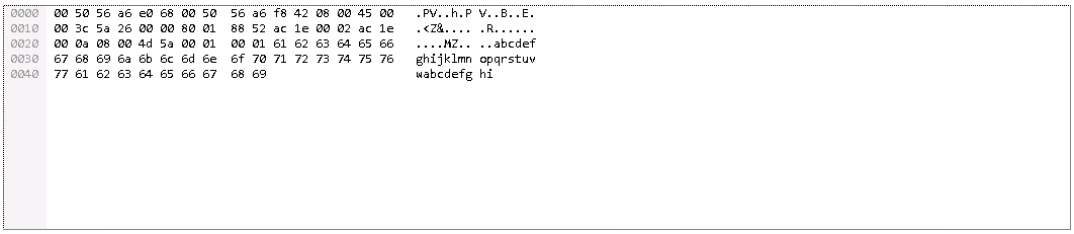
Frame summary pane

- The middle pane of the Wireshark window is used to display the packet structure and contents of fields within the packet. This area of the Wireshark window is referred to as the *frame detail*.



Frame detail pane

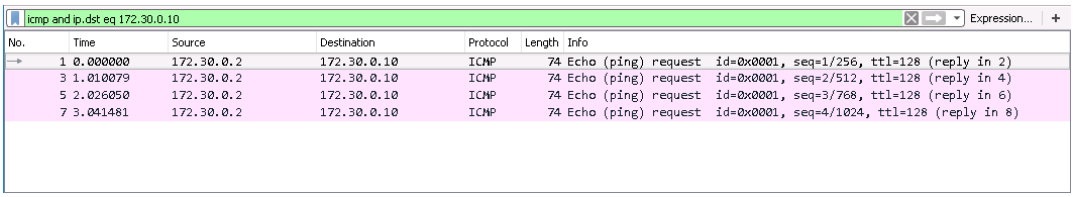
- The bottom pane of the Wireshark window displays the hex data. All of the information in the packet is displayed in hexadecimal on the left and in decimal, in characters when possible, on the right. This can be a useful feature, especially if passwords you are looking for are unencrypted. This area of the Wireshark window is referred to as the *hex pane*.



Hex pane

2. In the Filter box on the Wireshark toolbar, **type** `icmp and ip.dst eq 172.30.0.10` and **press Enter**.

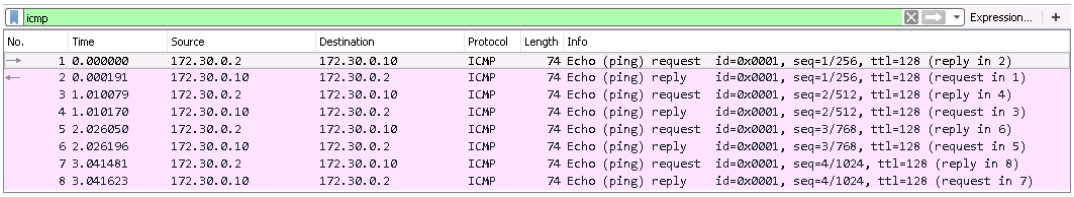
   Wireshark will filter all packets to show only those packets that meet that criteria: all ICMP (ping) packets that were destined for 172.30.0.10. Notice that we only see half of the conversation (the echo request).



Filtered traffic

3. In the Filter box, **type `icmp`** (replacing the previous filter) and **press Enter**.

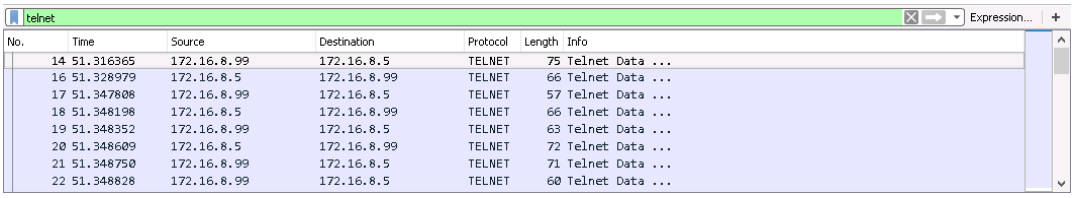
   Wireshark will once again filter all of the packets captured to view the complete conversation (ping requests and replies) between the vWorkstation (172.30.0.2) and the TargetWindows02 (172.30.0.10) systems.



Complete ICMP conversation

4. In the Filter box, **type `telnet`** and **press Enter**.

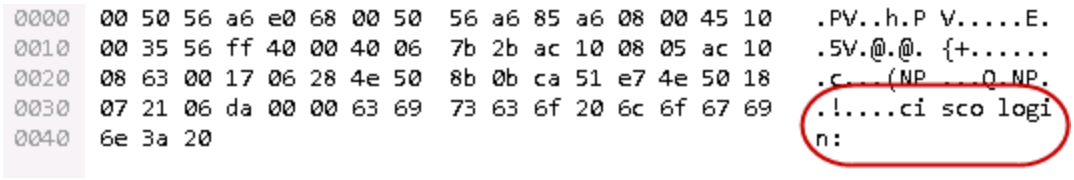
   Wireshark will display your Telnet (unsecure) PuTTY session between TargetWindows02 and 172.16.8.5 (LAN Switch 1), when you logged in as user *cisco* with a password of *cisco*.



Telnet traffic

5. **Click** the **first frame** to select it, then **use** the **down arrow** to scroll down through the rest of the frames packet-by-packet, paying attention to the right-most side of the hex pane.

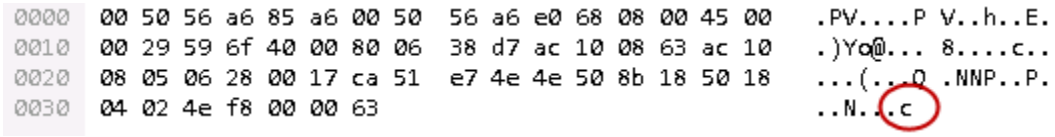
   You will notice mostly indiscernible text. Continue until you will come across a packet that clearly reads *login*.



Captured login prompt

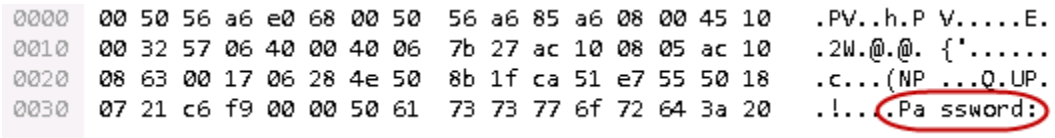
6. **Use** the **down arrow** to move to the next frame.

   Note the last letter in the hex pane for this frame is a *c*. The next frame down also ends in a letter *c* because the packets are grouped in pairs. The next pair of frames ends in a letter *i*, the next pair in a letter *s*, the next pair ends in *c*, and then a pair ending in the letter *o*. Wireshark has captured the Telnet user name, *cisco*, in clear text, character by character.



Username sent in clear text

7. **Use** the **down arrow** to select new frames until you see the word *Password* in the hex pane.



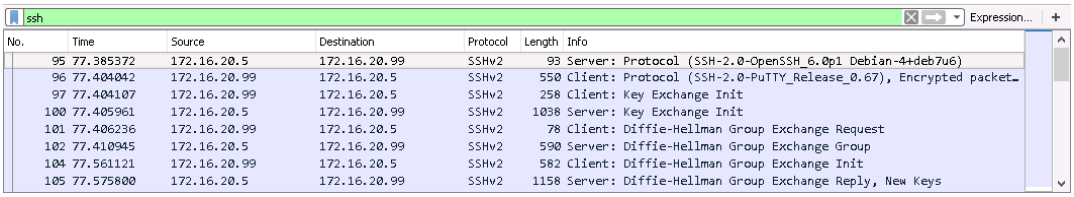
Captured password prompt

8. **Repeat step 6** to identify the password, *cisco*, for the Telnet session.

   Wireshark is able to capture the password in clear text because Telnet is an unsecure connection.

9. In the Filter box, **type** **ssh** and **press Enter**.

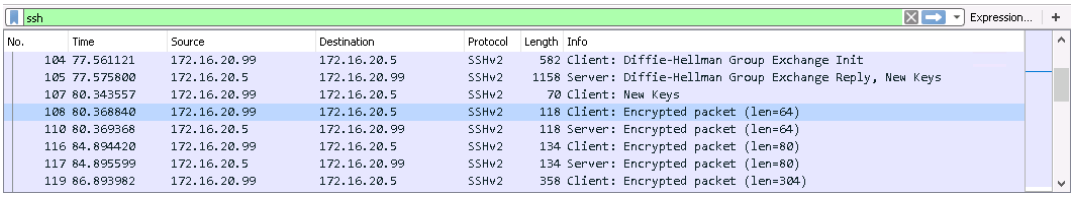
   Wireshark will filter out everything except the SSH (secure) PuTTY session between TargetWindows02 and 172.16.20.5 (LAN Switch 2). Notice that the first part of the conversation is the exchange of keys.



SSH key exchange

10. **Click** the **first frame** to select it, then **use** the **down arrow** to view the rest of the packets related to the SSH session.

    The rest of the SSH conversation is encrypted so the username and password are not visible. SSH encrypts the data transmission between the SSH client and the SSH host to maintain confidentiality.



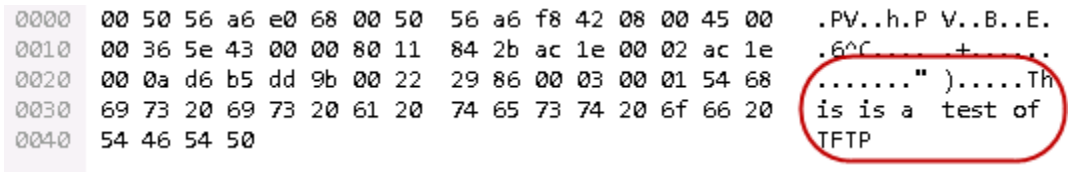
Encrypted traffic

11. In the Filter box, **type** `tftp` and **press Enter**.

    Wireshark will filter out everything except the TFTP session between TargetWindows02 and the vWorkstation.

12. **Click** the **first frame** to select it, then **use** the **down arrow** to scroll through the frames, paying attention to the right side of the hex pane, until you locate the contents of the transferred TFTP.txt file.

Without encryption, anything can be stolen off a network by a promiscuous packet analyzer like Wireshark.



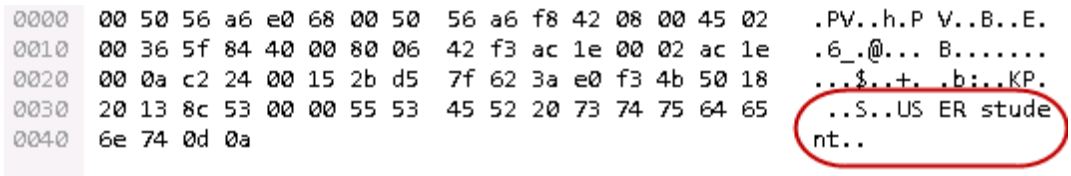
Captured contents of a text file

Note: While the threat posed by tools like Wireshark might be cause for alarm to network security analysts, Wireshark's ability to capture traffic is greatly hampered by switched networks. Switches only forward packets destined to and from an attached system (as well as broadcast packets). Thus, it is impossible for a system in promiscuous mode to "sniff" all traffic on a given network without first compromising the switching hardware in some way.

13. In the Filter box, **type** `ftp` and **press Enter**.

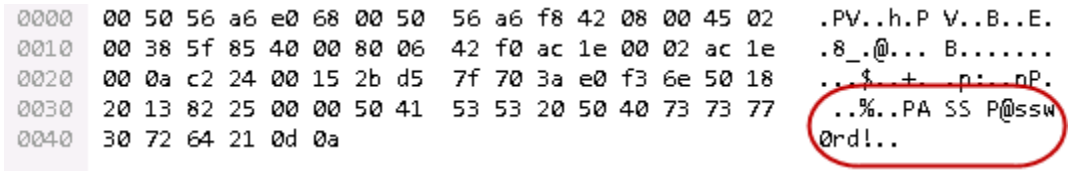
    Wireshark will filter out everything except the FTP session between TargetWindows02 and the vWorkstation.

14. **Click** the **first frame** to select it, then **use** the **down arrow** to scroll through the frames, paying attention to the right side of the hex pane, until you locate the first packet containing information about the FTP session (the username: *student*).



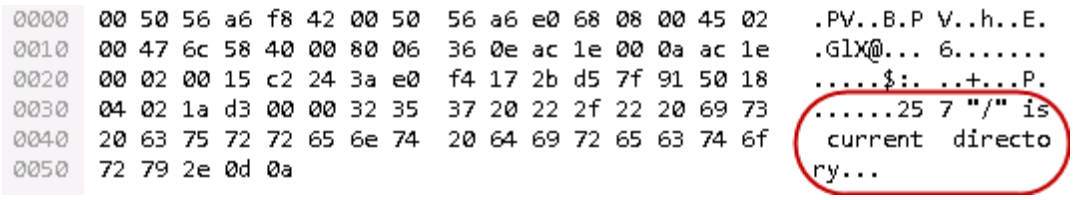
Captured username

15. **Use** the **down arrow** to locate the password for the FTP session.



Captured password

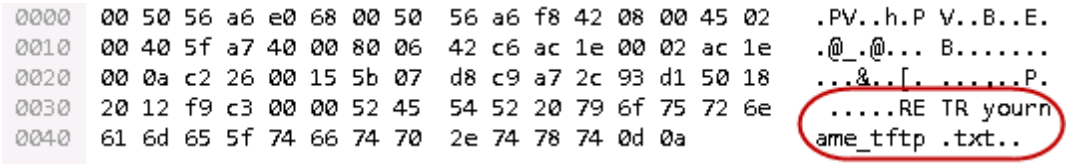
16. **Use** the **down arrow** to locate the TargetWindows02 directory for the FTP session.



Captured directory path

17. **Use** the **down arrow** to locate the name of the file transferred during the FTP session.

    While Wireshark could not capture the contents of the transferred file, almost everything else was easily visible in clear text. Despite this lack of security, FTP is still an extremely popular method of sharing and transferring files over the Internet.

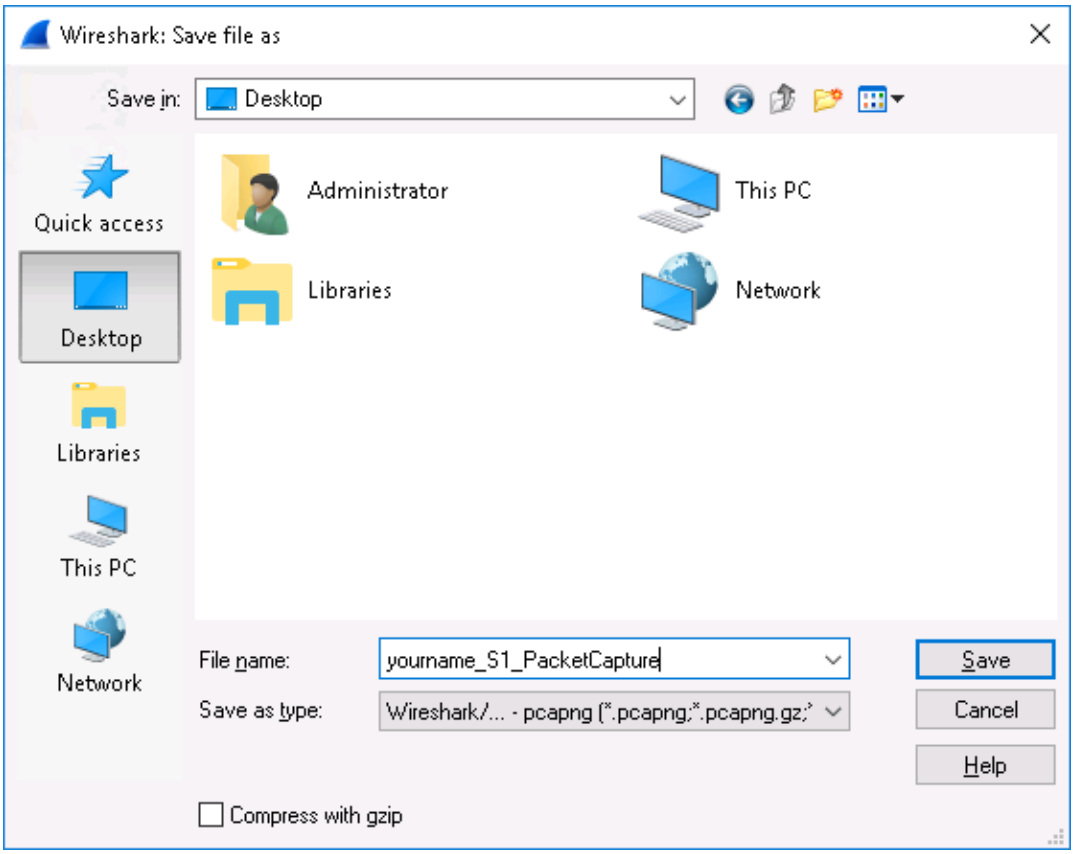


Captured file transfer

18. **Make a screen capture** showing the **captured file transfer in the entire Wireshark window** and **paste** it into your Lab Report file.

19. From the Wireshark menu bar, **click File**, then **select Save As** to open the Save As dialog box.

20. In the Save As dialog box, **click** the **Desktop icon**, **select Wireshark/tcpdump/…-pcap** in the Save as type box, **type** ***yourname*_S1_PacketCapture**, replacing *yourname* with your own name, and **click Save** to save the capture file to the TargetWindows02 desktop.



File Name and Type

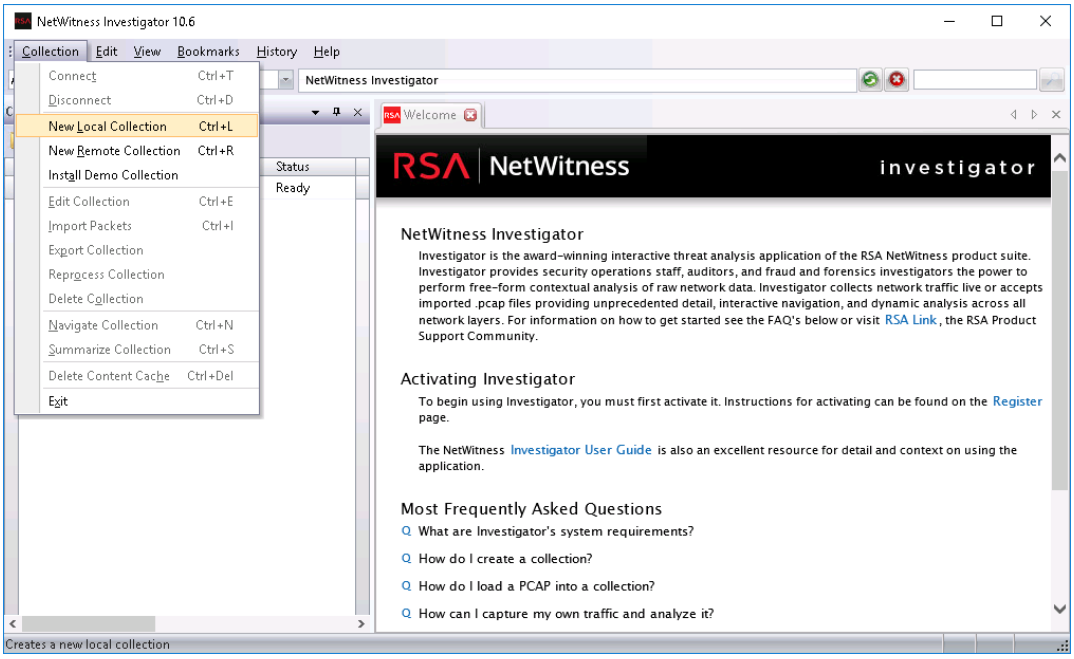
21. **Close** the **Wireshark window**.

Part 3: Analyze Traffic using NetWitness Investigator

Note: In the next steps, you will use NetWitness Investigator to analyze the Wireshark packet capture file you saved in Part 2 of this lab. Before analyzing packets in NetWitness Investigator, you must first create a collection and then import a packet capture (*.pcap) file.

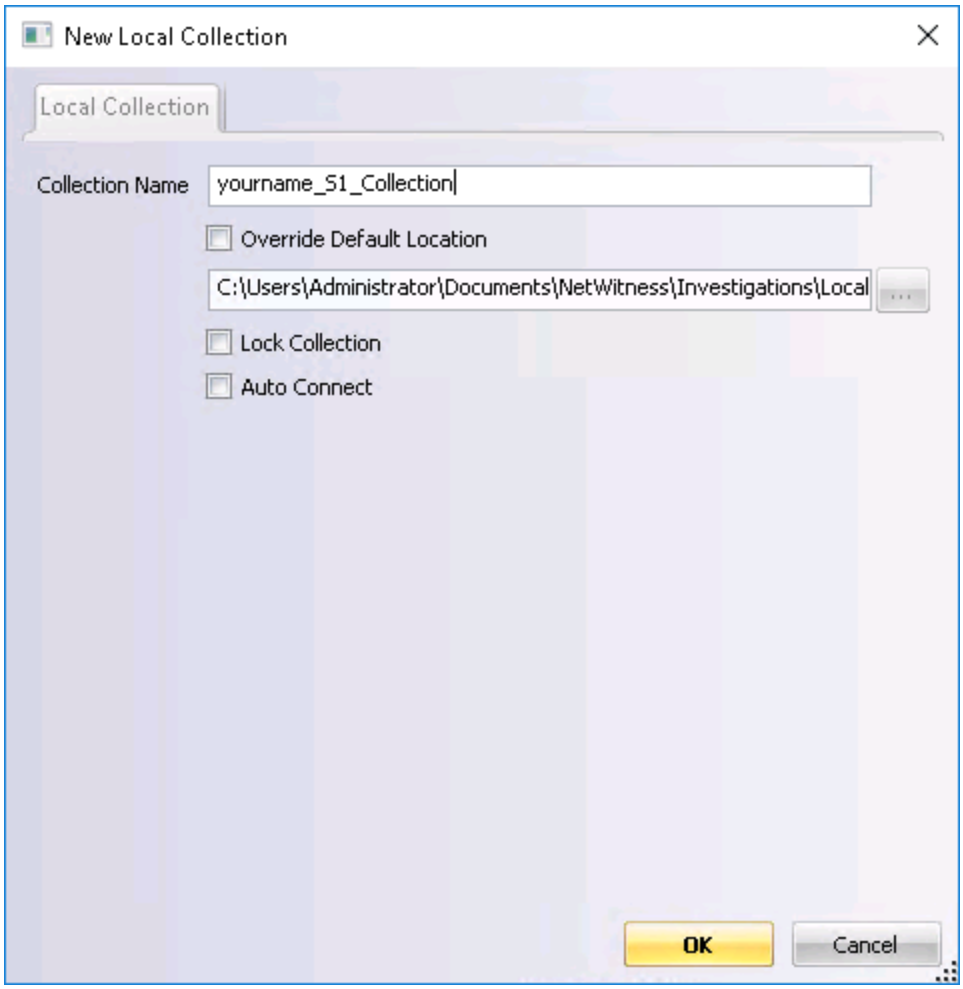
1. From the TargetWindows02 taskbar, **click** the **RSA icon** to open the NetWitness Investigator application.

2. From the NetWitness Investigator menu, **click Collection > New Local Collection**.



Create a new collection

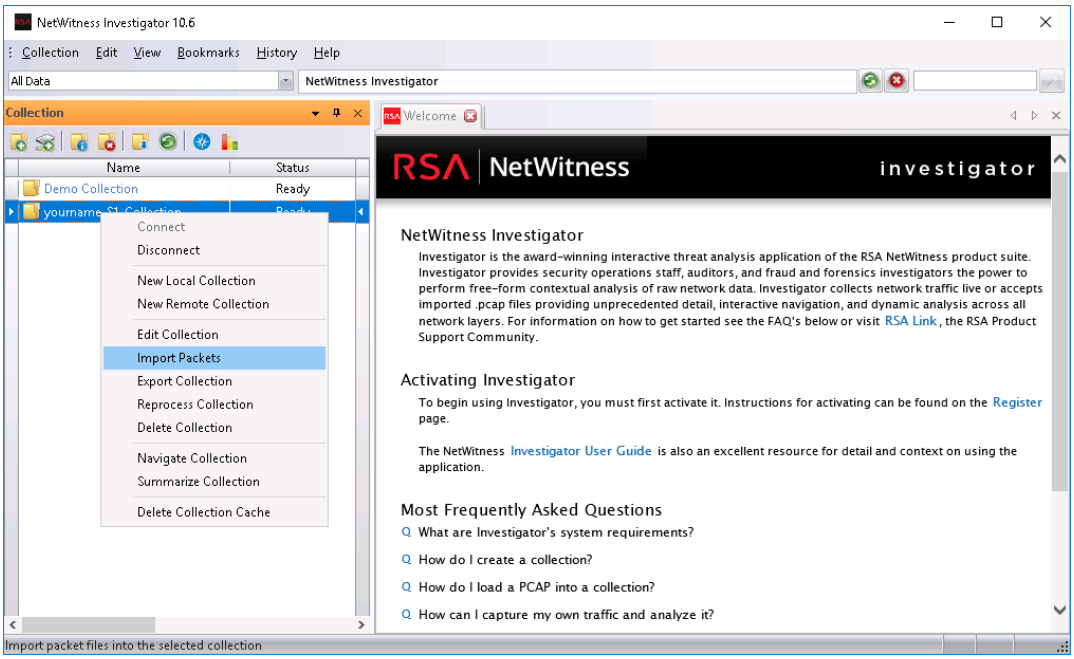
3. In the Collection Name box, **type** ***yourname*_S1_Collection**, replacing *yourname* with your own name, then **click OK** to save the new collection.



Name the collection

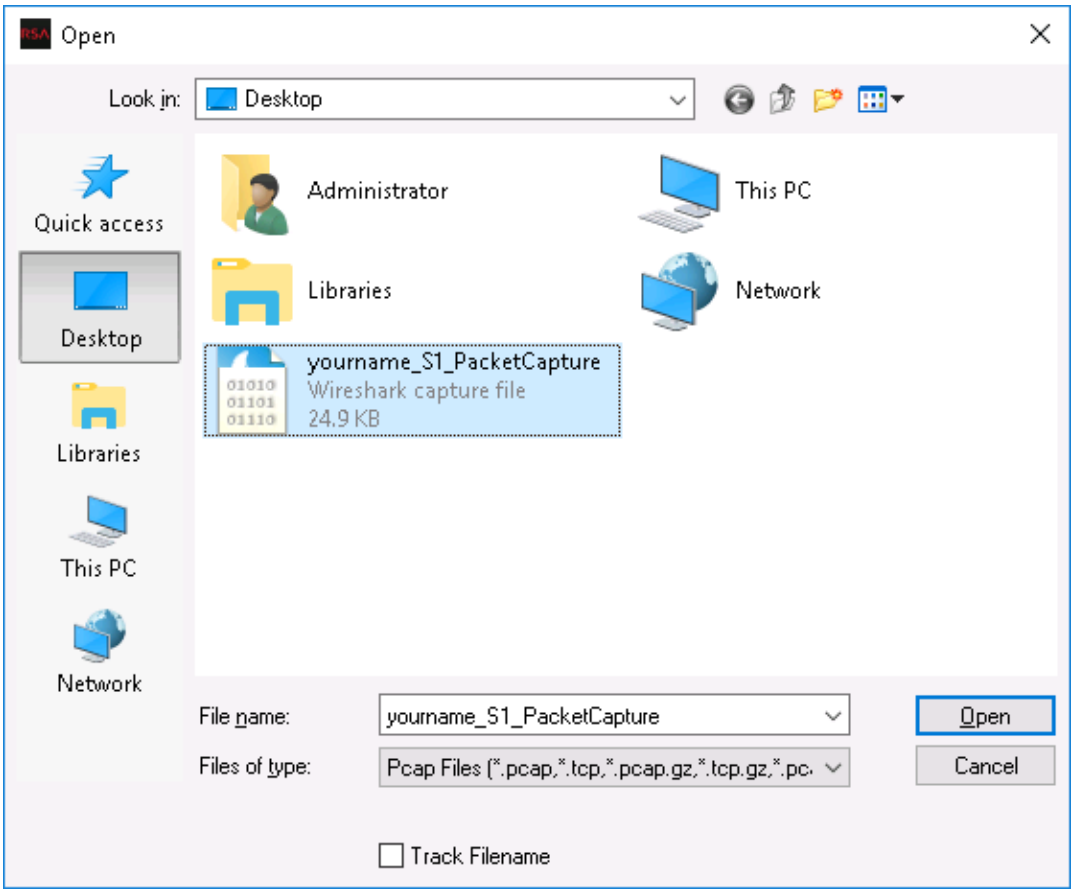
4. In the left pane, **double-click** the ***yourname*_S1_Collection** to activate it and change the status to *Ready*.

5. In the left pane, **right-click** the ***yourname*_S1_Collection** and **select Import Packets** from the context menu.



Import a PCAP file

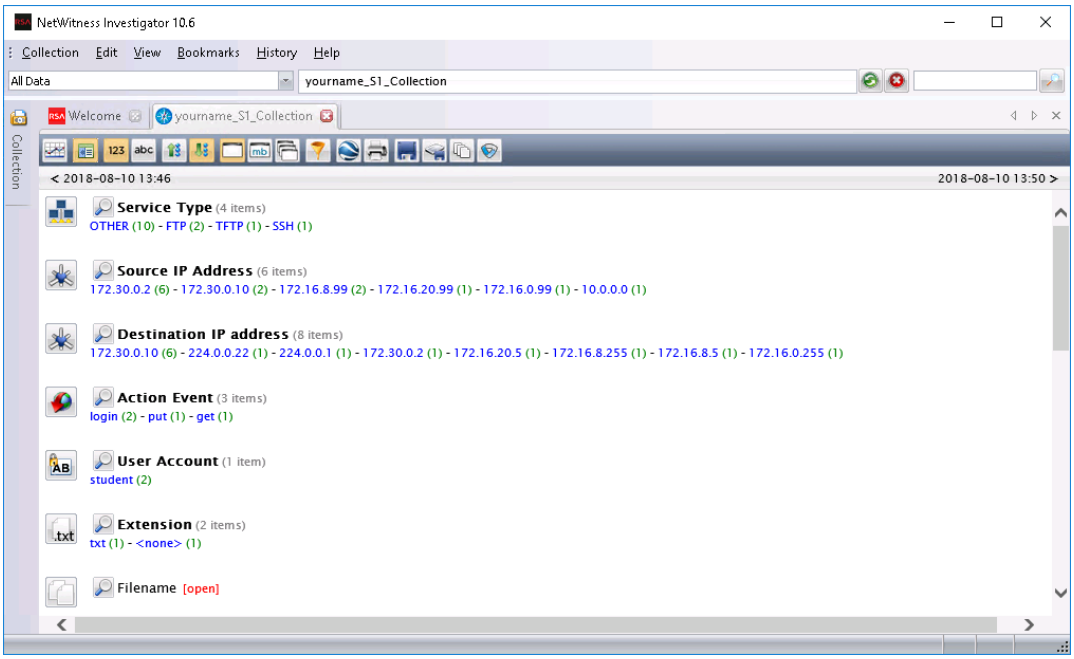
6. In the Open dialog box, **select** the ***yourname*_S1_PacketCapture.pcap file** you saved earlier in this lab, then **click Open**.



Select the PCAP file to import

7. When the file has finished importing, **double-click** the ***yourname*_S1_Collection** to open it in NetWitness Investigator.

Note: 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 anomalous patterns become more apparent.



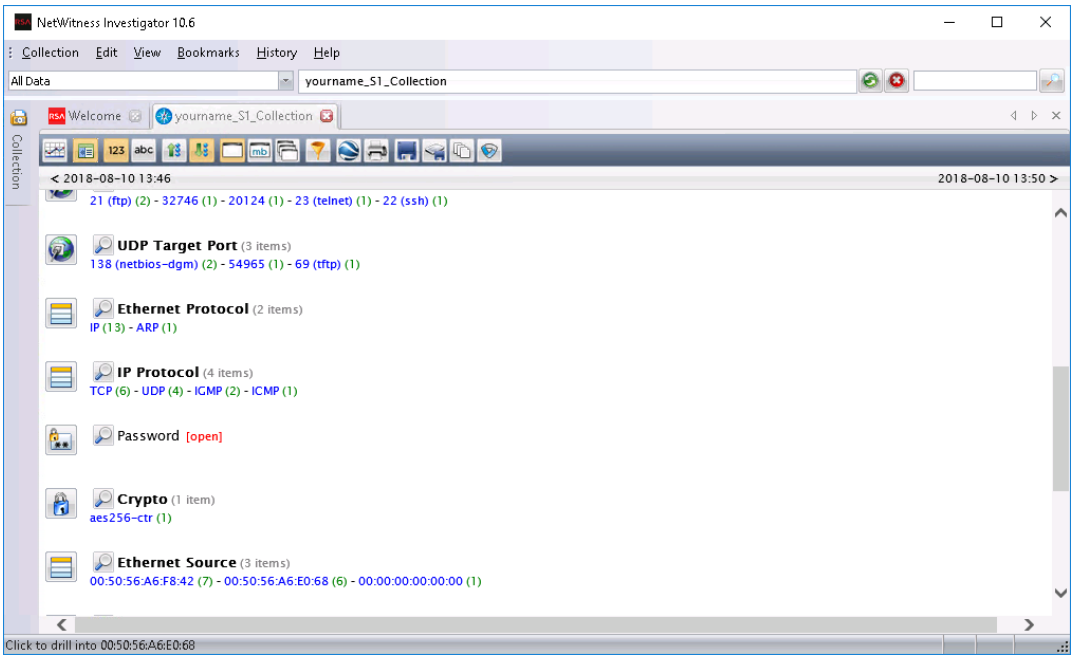
NetWitness Investigator collection summary

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.

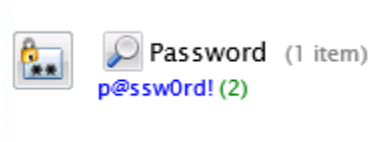
User Account	User names seen on the network.
Extension	Types of files seen on the network.
Filename	Names of files seen on the network. **Click [open]** to view.
TCP Destination Port	TCP Ports accessed.
UDP Target Port	UDP Ports accessed.
Password	Cleartext passwords seen on the network. **Click [open]** to view.

8. In the NetWitness Investigator window, **use the scrollbar** to review the contents of the collection and **locate** the **Password category**.



NetWitness Investigator collection

9. Under the Password category, **click** the **[open] link** to open the report.



Captured password

10. Under the Password category, **click** the **(2) link** to view the session details related to password captures.

11. **Make a screen capture** showing the **password information for the *yourname*_ Collection** and **paste** it into your Lab Report file.

12. **Close** the **NetWitness Investigator window**.

Note: This completes Section 1 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

13. From the TargetWindows02 desktop, **select any deliverable files** you saved in the course of this lab and **copy** them to the Windows clipboard.

    - ***yourname*_S1_PacketCapture.pcap**

14. **Minimize** the **remote TargetWindows02 connection**.

15. On the vWorkstation desktop, **right-click** and **select Paste** to paste the copied files to the desktop.

    If necessary, **close** the **Connection folder**.

16. On the vWorkstation desktop, **drag** the deliverable files into the File Transfer folder to complete the download to your local computer.

Section 2: Applied Learning

Note: SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods.

Please confirm with your instructor that you have been assigned Section 2 before proceeding.

1. On your local computer, **create** the **Lab Report file**.
   Frequently performed tasks, such as how to create the Lab Report file, make screen captures, and download files from the lab, are explained in the Common Lab Tasks document. You should review these tasks before starting the lab.

2. If you already completed Section 1 of this lab, you will need to reset the virtual environment before beginning Section 2. To reset the virtual environment, complete one of the following options.
   a. **Click Options > Reset Lab** to restore all virtual machines to their base state. This will take several minutes to complete. If you do not see the vWorkstation desktop after five minutes, **click Options > Reload Lab** to reload your lab connection.

   b. **Click Disconnect**, then **select Discard Changes** to end your lab session without creating a StateSave. If you previously created a StateSave, delete the StateSave at the launch page, then start a new lab session.

3. **Proceed** with **Part 1**.

Part 1: Generate Network Traffic

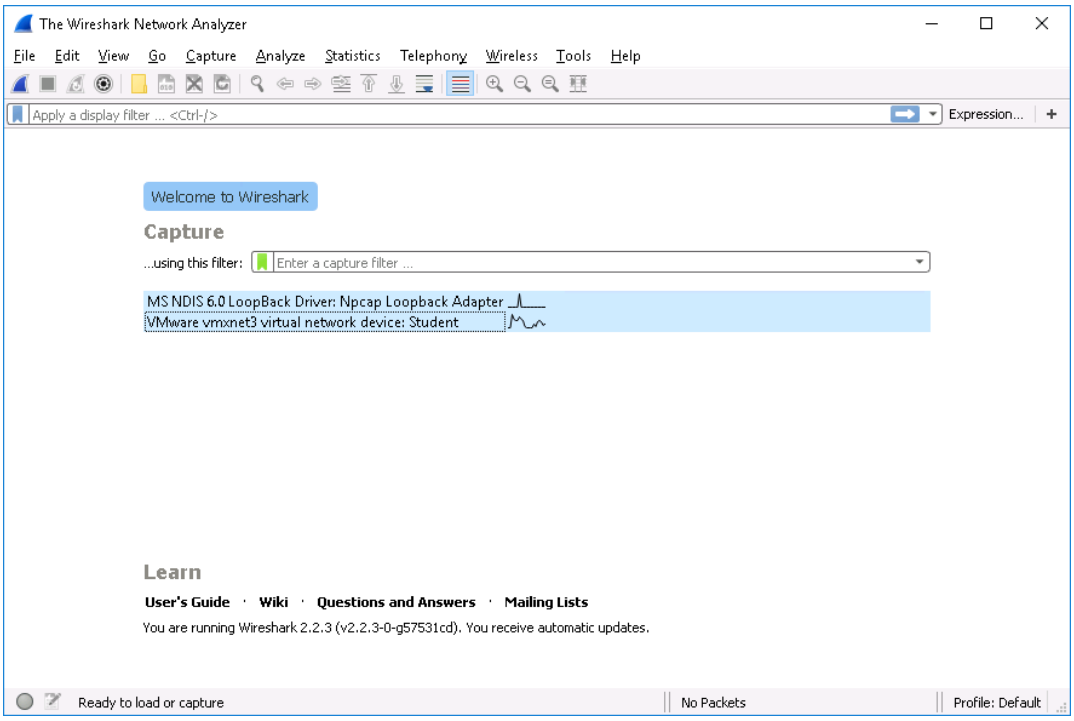
Note: In the next steps, you will start a Wireshark packet capture and open and close several common tools to generate traffic and transfer files between machines in this lab. Wireshark will continue running in the background until you manually stop the capture process later in this lab. You will analyze the captured packets in the second part of this lab.

1. **Open a remote connection** to the **TargetWindows02 machine**.

2. **Launch** the **Wireshark application**.

   Wireshark is a protocol analyzer tool (sometimes called a “packet sniffer”). It is used to capture IP traffic from a variety of sources. The main screen of Wireshark includes details about the current capture configuration. From this screen, analysts can select common filters from the drop-down menu, or type a custom filter command to quickly sort the captured data.

3. On the main screen, **select** the **Student** and **Npcap Loopback Adapter capture interfaces**.



Verify interface selection

The student interface is the lab environment that you are working in. Selecting this interface ensures that Wireshark can analyze traffic from areas of the network that are visible to students.

4. **Apply a filter** to filter out RDP traffic generated between the vWorkstation and TargetWindows02 systems, then **start** the packet capture.

Note: In the next steps, you will generate traffic for Wireshark to capture.

5. **Minimize** the **remote TargetWindows02 connection**.

6. On the vWorkstation, **launch** a **Command Prompt window**.

7. In the command prompt window, **ping** the **TargetWindows02 machine**, then **close** the **command prompt window**.

8. **Restore** the **remote TargetWindows02 connection**.

9. **Minimize** the **Wireshark window**.

10. **Launch** the **PuTTY application**.

11. **Open** a **Telnet** connection to **LAN Switch 1**.

12. At the login prompt, **use the following credentials** to connect to LAN Switch 1, then **close** the **PuTTY session**.

    - Login: **`cisco`**
    - Password: **`cisco`**

13. **Launch** the **PuTTY application** again and **open a SSH connection** to **LAN Switch 2**.

14. At the login prompt, **use the following credentials** to connect to LAN Switch 2, then **close** the **PuTTY session**.

    - Login: **`cisco`**
    - Password: **`cisco`**

15. **Launch** the **Tftpd64 application**, **change** the **current directory** to the Administrator desktop,

and **set 172.30.0.10** as the server interface.

The local TFTP server will now listen on UDP port 69 on the 172.30.0.10 interface for a file transfer. In the next steps, you will transfer a file to this machine using TFTP.

16. **Minimize** the **remote TargetWindows02 connection**.

17. On the vWorkstation desktop, **create a new text document** named ***yourname*_S2_tftp**, replacing *yourname* with your own name.

18. **Open** the ***yourname*_S2_tftp file**, add **This is a test for Section 2 TFTP** to the body of the file, then **close Notepad**, saving the file when prompted.

19. **Launch** a **command prompt window**.

20. At the command prompt, **execute the command** to transfer *yourname*_S2_tftp.txt to TargetWindows02 using tftp, then **close** the **command prompt window**.

    You will see a successful TFTP file transfer of *yourname*_S2_tftp.txt from the vWorkstation desktop to TargetWindows02.

21. **Restore** the **remote TargetWindows02 connection**.

22. In the Tftpd64 window, **click** the **Show Dir button** to confirm the file transfer was successful.

23. **Make a screen capture** showing ***yourname*_S2_tftp.txt in the Tftpd64 directory** and **paste** it into your Lab Report file.

24. **Close** the **directory window** and the **Tftpd64 window**.

25. **Launch FileZilla Server**, then **minimize** the **remote TargetWindows02 connection**.

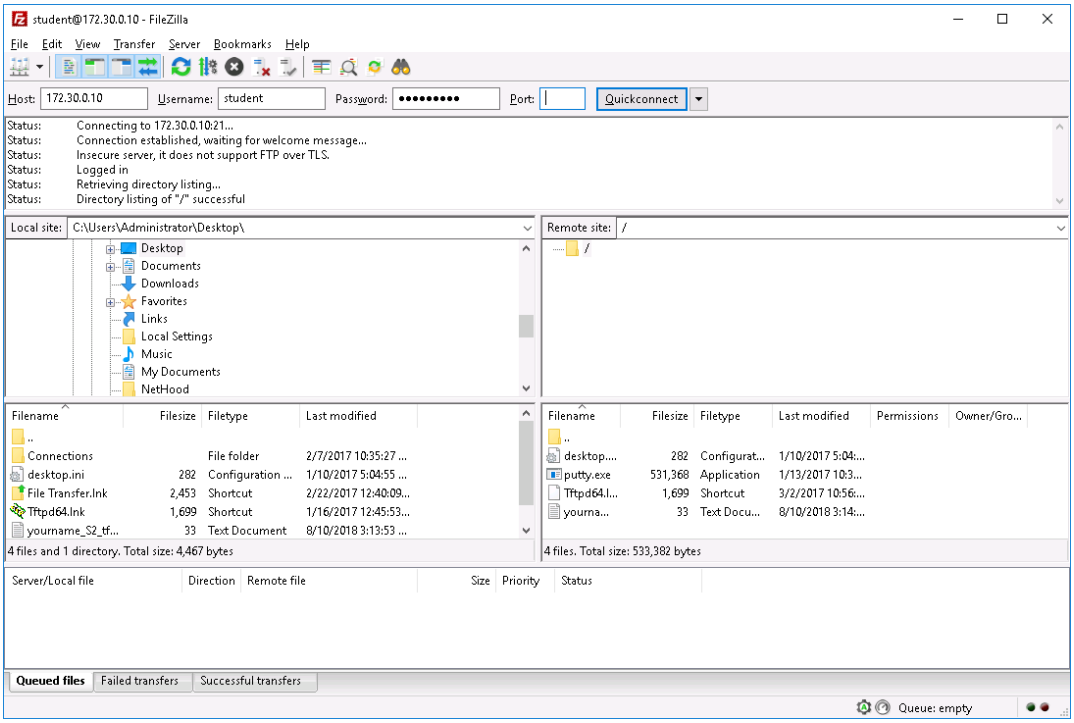
26. From the vWorkstation taskbar, **launch** the **FileZilla Client application**.

27. In the FileZilla QuickConnect bar, **enter** the following details and **connect** to the FileZilla Server on TargetWindows02.

    - Host: **`172.30.0.10`**
    - Username: **`student`**
    - Password: **`P@ssw0rd!`**
    - Port: **`21`**

28. In the center pane of the FileZilla window, **navigate** to the **Desktop** in both the Local site and the Remote site panes:

    - Local site: (**C:\Users\Administrator\Desktop**)
    - Remote site: (***/***)



Connect to TargetWindows02 using FileZilla

29. **Transfer** the ***yourname*_S2_tftp.txt file** from the TargetWindows02 desktop to the vWorkstation desktop, overwriting the existing file.

When a file is successfully transferred, FileZilla will display a blue success pop-up and the bottom of the FileZilla window will indicate the transfer has taken place.

30. **Make a screen capture** showing **the FileZilla window displaying the successful file transfer** and **paste** it into your Lab Report file.

31. **Close** the **FileZilla Client window** and **restore** the **remote TargetWindows02 connection**.

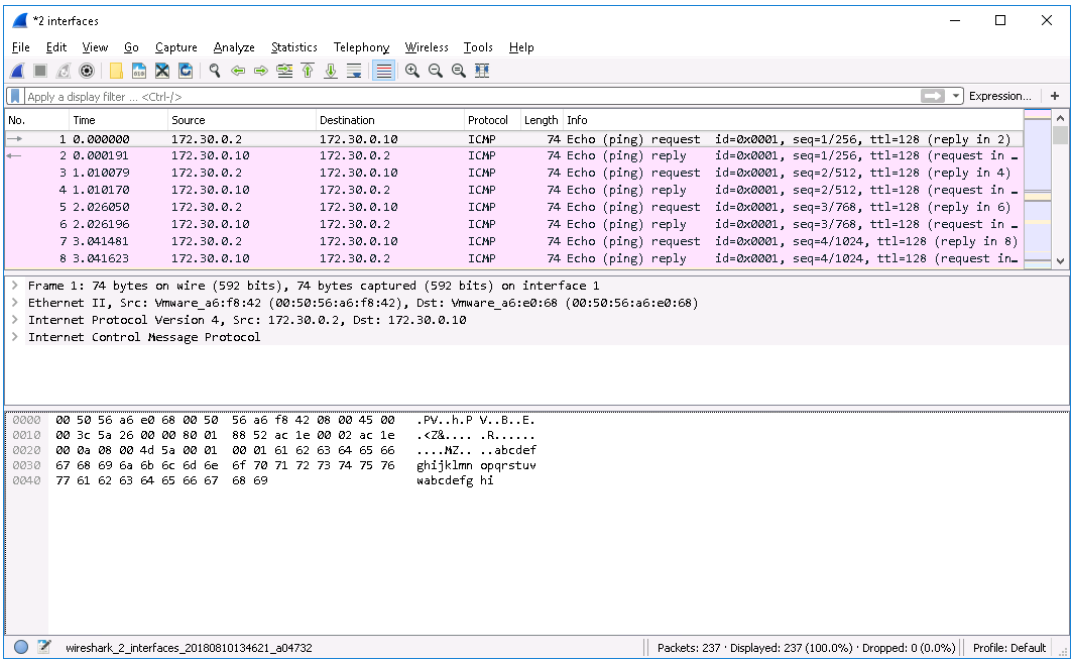
32. **Close** the **FileZilla Server window**, then **restore** the **Wireshark window** and **stop** the **packet capture** process.

Part 2: Analyze Traffic using Wireshark

Note: While it is possible to scroll through all of the packets captured by Wireshark to find what you are looking for, it is far easier to use display filters. Display filters enable you to find only the traffic you wish to analyze. In the next steps, you will use display filters to analyze the traffic generated in the first part of this lab.

Because this data was captured live during Part 1 of the lab, you will notice that your display may not match the images in this part of the lab. This is normal; you will still be able to complete the steps.

1. If necessary, **maximize** the **Wireshark window**.

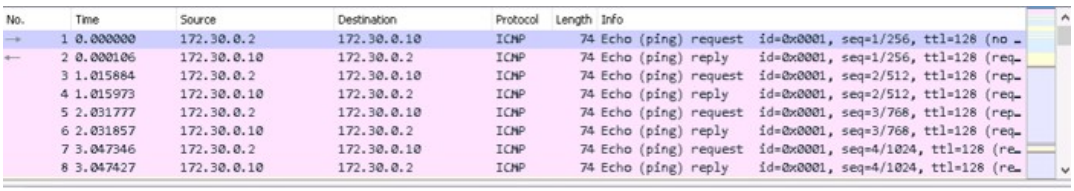


Wireshark window

Exploring Wireshark

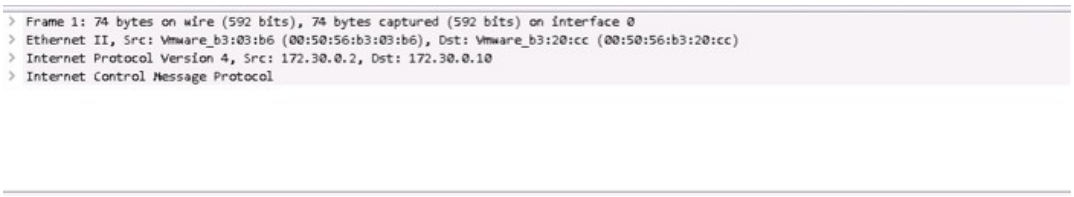
The Wireshark window opens with the detailed information about the packets captured in three panes. Use your mouse to drag the borders of any pane up or down to change its size.

- The top pane of the Wireshark window contains all of the packets that Wireshark has captured, in time order, and provides a summary of the contents of the packet in a format close to English. Keep in mind that the content will be different depending on where you capture packets in the network. Also remember that the "source" and "destination" are relative to where a packet is captured. This area of the Wireshark window is referred to as the *frame summary*.



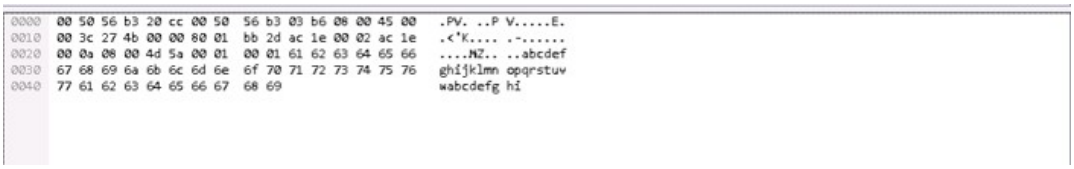
Frame summary pane

- The middle pane of the Wireshark window is used to display the packet structure and contents of fields within the packet. This area of the Wireshark window is referred to as the *frame detail*.



Frame detail pane

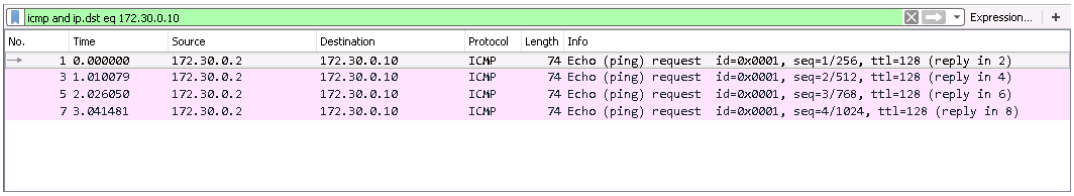
- The bottom pane of the Wireshark window displays the hex. All of the information in the packet is displayed in hexadecimal on the left and in decimal, in characters when possible, on the right. This can be a useful feature, especially if passwords you are looking for are unencrypted. This area of the Wireshark window is referred to as the *hex pane*.



Hex pane

2. **Add a filter** to display only ICMP packets destined for 172.30.0.10.

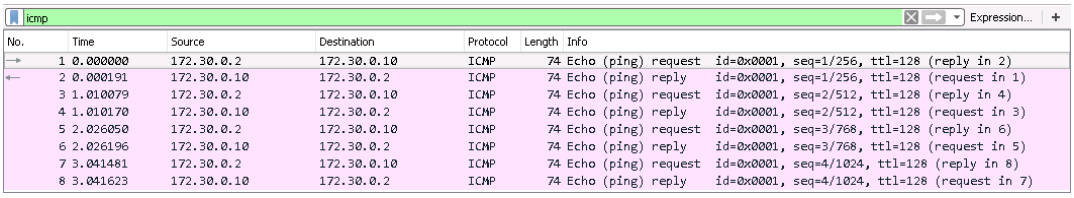
   Notice that we only see half of the conversation (the echo request).



Filtered traffic

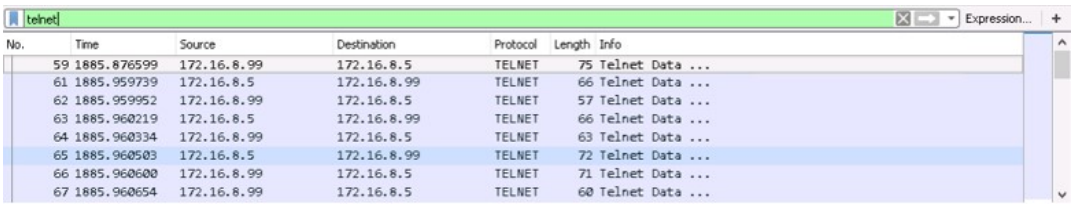
3. **Add a filter** to display only **ICMP** packets.

   Wireshark will once again filter all of the packets captured to view the complete conversation (ping requests and replies) between the vWorkstation (172.30.0.2) and the TargetWindows01 (172.30.0.10) machine.



Complete ICMP conversation

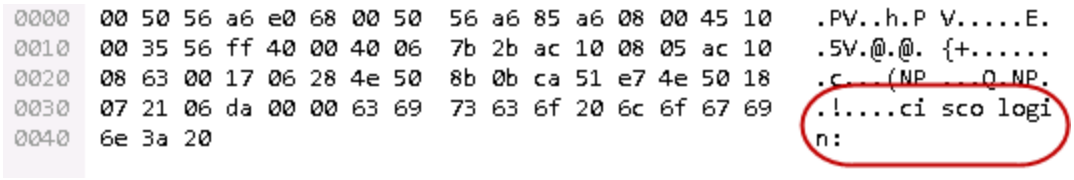
4. **Add a filter** to display only **Telnet** packets from the unsecure PuTTY session between TargetWindows02 and LAN Switch 1.



Telnet traffic

5. **Select** the **first frame**, then **use** the **down arrow** to scroll down through the rest of the frames packet-by-packet, paying attention to the right-most side of the hex pane.

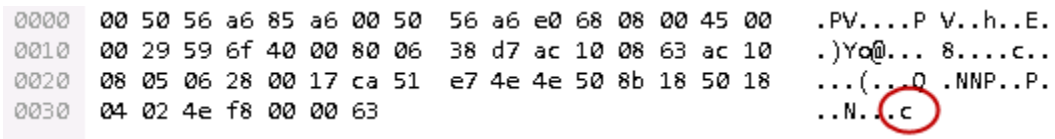
   You will notice mostly indiscernible text. Continue until you will come across a packet that clearly reads *login*.



Captured login prompt

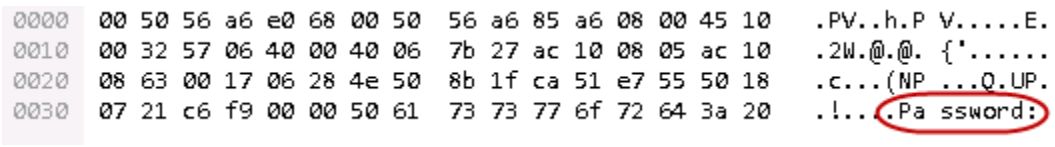
6. **Use** the **down arrow** to move to the next frame.

   Note the last letter in the hex pane for this frame is a *c*. The next frame down also ends in a letter *c* because the packets are grouped in pairs. The next pair of frames ends in a letter *i*, the next pair in a letter *s*, the next pair ends in *c*, and then a pair ending in the letter *o*. Wireshark has captured the Telnet user name, *cisco*, in clear text, character by character.



Username sent in cleartext

7. **Use** the **down arrow** to scroll down until you see the word *Password* in the hex pane.



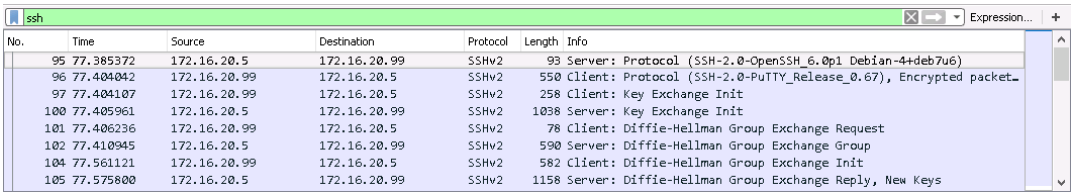
Captured password prompt

8. **Repeat step 7** to identify the password, *cisco*, for the Telnet session.

   Wireshark is able to capture the password in clear text because Telnet is an unsecure connection.

9. **Add a filter** to display only **SSH** packets from the secure PuTTY session between TargetWindows02 and LAN Switch 2.

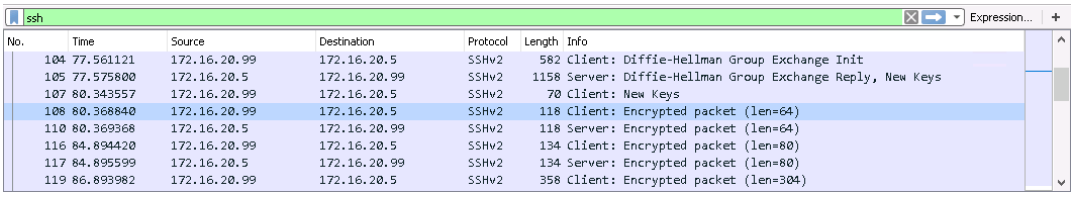
   Notice that the first part of the conversation is the exchange of keys.



SSH key exchange

10. **Use** the **down arrow** to view the rest of the packets related to the SSH session.

    The rest of the SSH conversation is encrypted so the username and password are not visible. SSH encrypts the data transmission between the SSH client and the SSH host to maintain confidentiality.

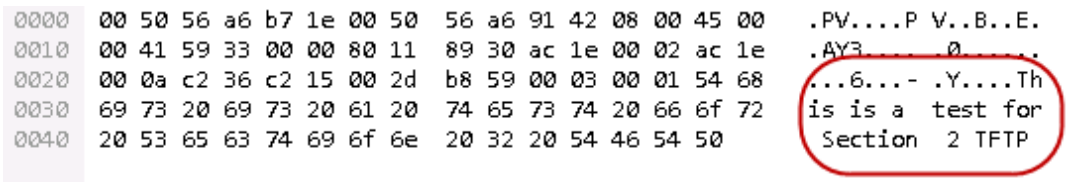


Encrypted traffic

11. **Add a filter** to display only **TFTP** packets from the TFTP session between TargetWindows02 and the vWorkstation.

12. **Select** the **first frame**, then **use** the **down arrow** to scroll through the frames, paying attention to the right side of the hex pane, until you locate the contents of the transferred TFTP.txt file.

    Without encryption, anything can be stolen off a network by a promiscuous packet analyzer like Wireshark.



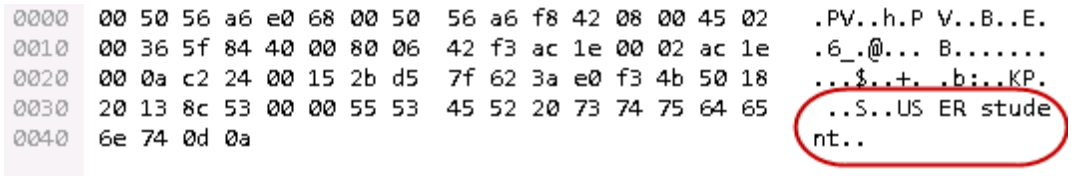
Captured contents of a text file

Note: While the threat posed by tools like Wireshark might be cause for alarm to network security analysts, Wireshark's ability to capture traffic is greatly hampered by switched networks. Switches only forward packets destined to and from an attached system (as well as broadcast packets). Thus, it is impossible for a system in promiscuous mode to "sniff" all traffic on a given network without first compromising the switching hardware in some way.

13. **Add a filter** to display only **FTP** packets from FTP session between TargetWindows02 and the

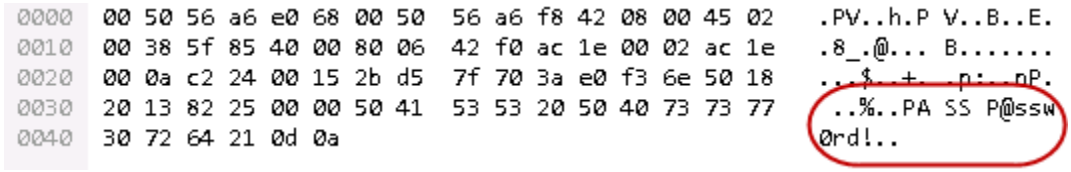
vWorkstation.

14. **Select** the **first frame**, then **use** the **down arrow** to scroll through the frames, paying attention to the right side of the hex pane, until you locate the first packet containing information about the FTP session (the username: *student*).



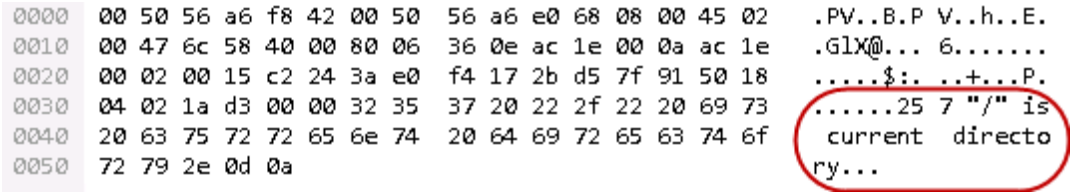
Captured username

15. **Locate** the **password** for the FTP session.



Captured password

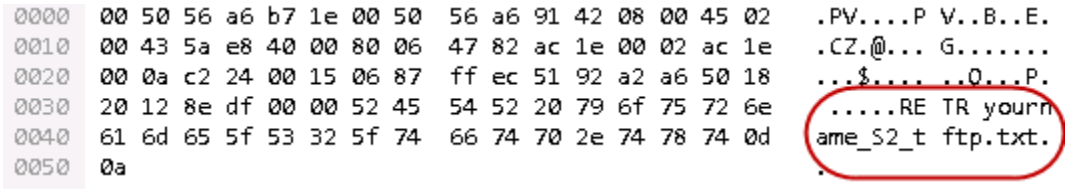
16. **Locate** the **TargetWindows02 directory** for the FTP session.



Captured directory path

17. **Locate** the **name of the file** transferred during the FTP session.

    While Wireshark could not capture the contents of the transferred file, almost everything else was easily visible in clear text. Despite this lack of security, FTP is still an extremely popular method of sharing and transferring files over the Internet.



Captured file transfer

18. **Make a screen capture** showing the **captured file transfer in the entire Wireshark window** and **paste** it into your Lab Report file.

19. In the Lab Report file, **identify the frame number** in which the name of the file transferred is displayed.

20. **Save the capture file** to the TargetWindows02 desktop as ***yourname*_S2_PacketCapture.pcap**, replacing *yourname* with your own name.

21. **Close** the **Wireshark window**.

Part 3: Analyze Traffic using NetWitness Investigator

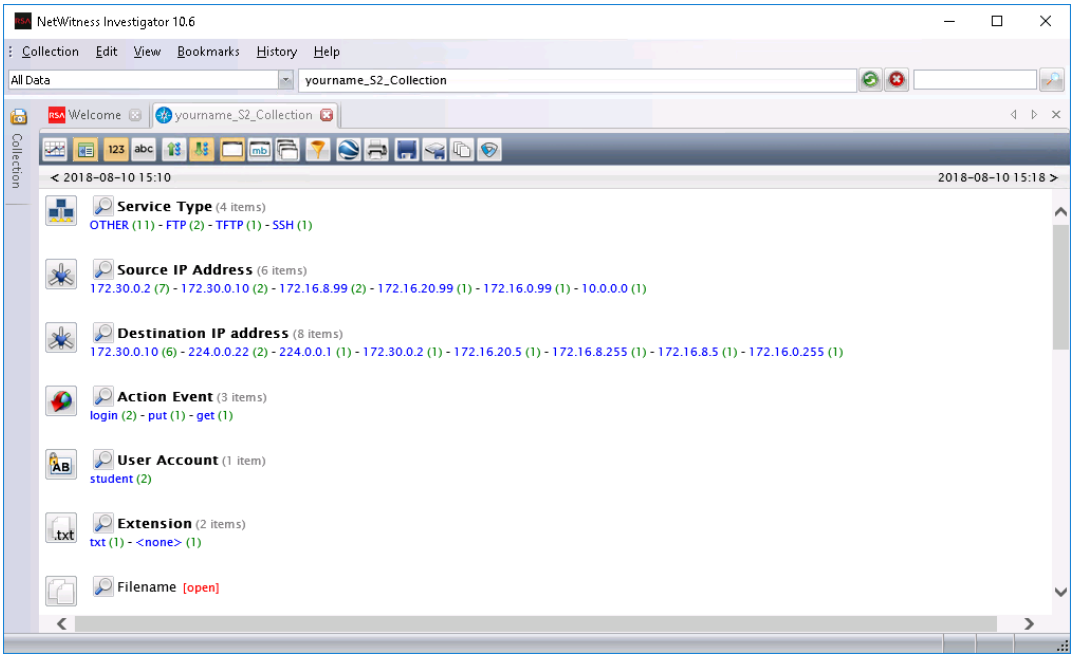
Note: In the next steps, you will use NetWitness Investigator to analyze the Wireshark packet capture file you saved in Part 2 of this lab. Before analyzing packets in NetWitness Investigator, you must first create a collection and then import a packet capture (*.pcap) file.

1. **Launch NetWitness Investigator**.

2. **Create** a **new Local Collection** titled ***yourname*_S2_Collection** (replacing *yourname* with your own name), then **import** the ***yourname*_S2_PacketCapture.pcap file**.

3. **Open** the ***yourname*_S2_Collection**.

Note: 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.



NetWitness Investigator collection summary

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	Cleartext passwords seen on the network. **Click [open]** to view.

4. **Locate** the **yourname_S2_tftp.txt file** that was transferred earlier in this lab and **display** the **session detail** related to the file.

5. **Make a screen capture** showing the **session detail for the yourname_S2_tftp.txt file transfer** and **paste** it into your Lab Report file.

6. **Close** the ***yourname* Collection tab** and **select Collection > Export Collection** from the NetWitness Investigator menu.

7. **Export** the file to the desktop as ***yourname*_S2_Collection.xml**.

8. **Close NetWitness Investigator**.

Note: This completes Section 2 of this lab. In the next steps, you will use the File Transfer folder to move any files from the vWorkstation to your local system that are to be submitted as part of your lab deliverables. Refer to the instructions in the Common Lab Tasks document for more information on how to use this function.

9. From the TargetWindows02 desktop, **select any deliverable files** you saved in the course of this lab and **copy** them to the Windows clipboard.

    - ***yourname*_S2_PacketCapture.pcap**
    - ***yourname*_S2_Collection.xml**

10. **Minimize** the **remote TargetWindows02 connection**.

11. On the vWorkstation desktop, **right-click** and **select Paste** to paste the copied files to the desktop.

    If necessary, **close** the **Connections folder**.

12. On the vWorkstation desktop, **drag** the deliverable files into the File Transfer folder to complete the download to your local computer.

Section 3: Lab Challenge and Analysis

Note: The following questions are provided to allow you the opportunity for independent, unguided research, similar to what you will encounter in a real situation. Some questions will challenge you to find command line syntax for tasks you performed in the lab, others may ask you to extend your learning from the lab. Use screen captures where possible to illustrate your answers.

Part 1: Analysis and Discussion

Review the *yourname* Collection that you created in the lab. In your Lab Report file, identify every IP address found in the collection. Describe any unexpected findings in the report.

Part 2: Tools and Commands

In the lab, launch the FileZilla Server on the TargetWindows02 machine, and then switch to the vWorkstation to launch Filezilla Client. Use FileZilla to attempt an FTP connection with any other IP address in the virtual environment. Document the IP addresses used, your results, and how you obtained the addresses.

Part 3: Challenge Exercise

In this lab, you generated common network traffic. You then analyzed that traffic at the packet level (using Wireshark) and at a consolidated level (using NetWitness). To better understand the utility of NetWitness, use what you have learned in this lab to generate a simulated brute force password attack on the switch interface at 172.16.8.5.

a. Start a packet capture in Wireshark.
b. Open FileZilla Client on the vWorkstation desktop and attempt to connect to the server at 172.16.8.5 using all of the incorrect user names and passwords described in the following table.

User Names and Passwords	
User Name	Passwords
admin	password, letmein, root, boss, l33t
Administrator	password, letmein, root, boss, l33t
cisco	password, letmein, root, boss, l33t

c. Save the Wireshark capture file as *yourname*_ChallengeCapture.pcap**,** replacing *yourname* with your own name.
d. Import the *yourname*_ChallengeCapture.pcap file into NetWitness Investigator.
e. In your Lab Report file, briefly summarize your analysis of how the brute force password attack is recognizable in NetWitness Investigator. Use screen captures as appropriate to illustrate your findings.