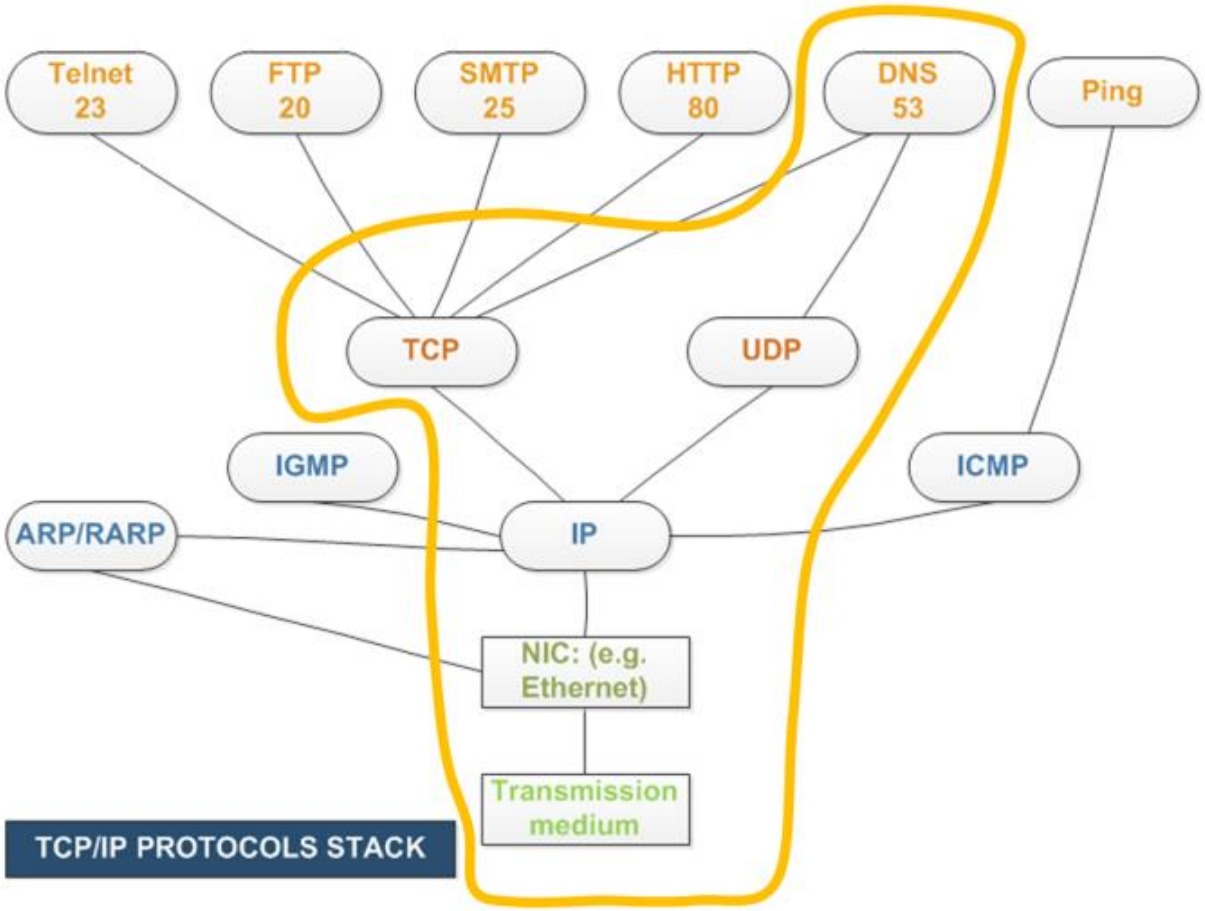
Lab 1: Server Discovery and Application Layer Protocols Analysis



Introduction to Computer Security (EECS 3482)
Khalil Abuosba, Ph.D.
Winter 2019

The purpose of this lab is to introduce to strategies and tools that are utilized in discovering servers and networks. The lab also demonstrates several application layer protocol interactions. sample application layer services. Using packet capturing software, you will be demonstrating the basic concepts of the OSI, Specifically HTTP, FTP, SSL, Telnet, and SSH protocols are demonstrated based on the stack.

General Information and Policies

- Solutions must to be submitted on through the blackboard system.
- Ideal reports include screen snapshots of all of the exercises.

Objectives

- *Map the theoretical context of the material learned in class to their implementation in the real world.*
- *Dissect popular network services using protocols analysis software.*
- *Differentiate between network services based on the TCP/IP Reference Model.*
- *Demonstrate secure application layer protocols.*
- *Observe differences between Telnet and SSH.*
- *Discover server type, name and IPs*
- *Observe HTTP headers and HTTP error codes.*

Keywords

IP, , promiscuous mode, HTTP, FTP, SSH, Telnet, http 200, http 301, http 302, IPv4, IPv6

Readings and Resources:

- Review the "Introduction to Wireshark" video. http://wiresharkdownloads.riverbed.com/video/wireshark/introduction-to-wireshark/

- Read pages 1-3 of Chapter-1 (The WireShark User's Guide).
- Review Week-1 and Week-2 Lecture notes.
- HTTP Status Codes: https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html
- Read about the functionalities of the keywords above.

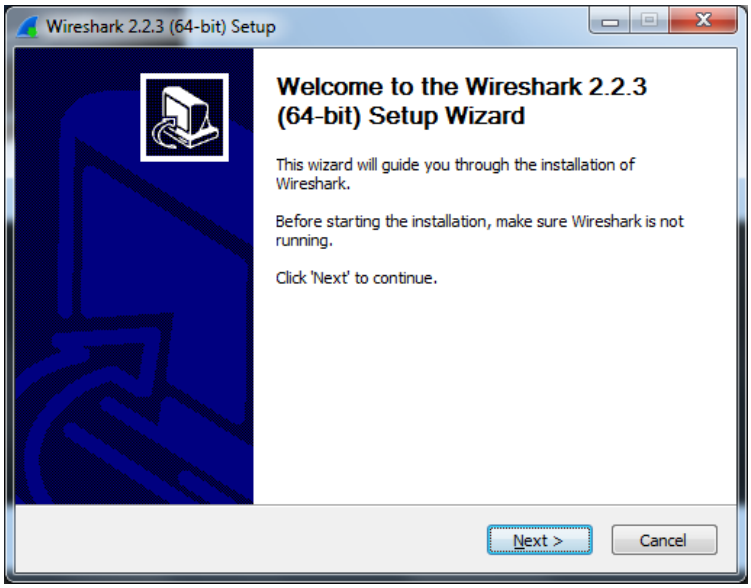
Deliverables

- A report that documents solutions to the questions listed in Part1 supported by screen snapshots.
- Wireshark Data Files.

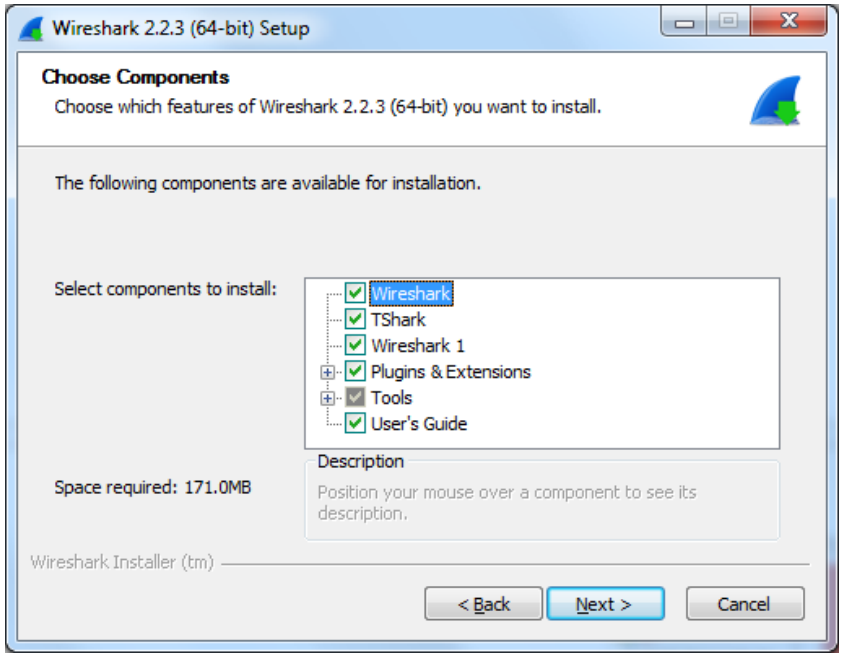
Pre-lab**: WireShark Software Installation**

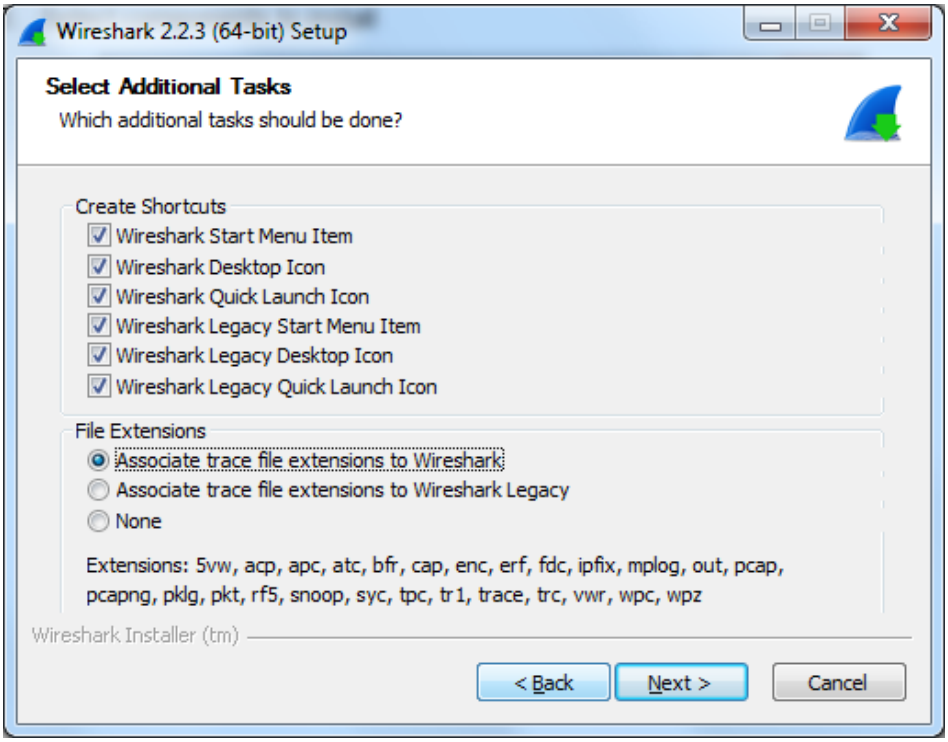
a. WireShark Installation

1. **Download Wireshark: https://www.wireshark.org/#download**
2. **Double click on the WireShark Installer Software**

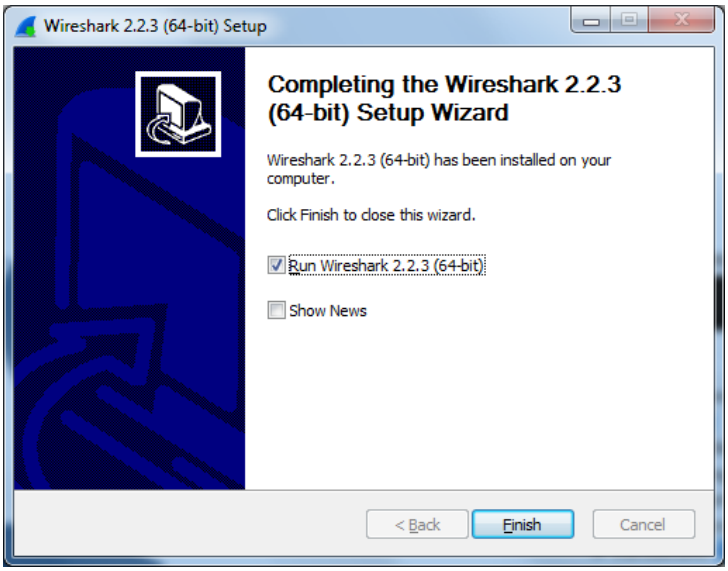


3. **Select components to be installed**





4. **Select ➔ WinPcap 4.1.3**
5. **Select ➔ Install USBCap..**
6. **Select ➔ Automatically start WinPcap driver at boot time.**


Wireshark 2.2.3 (64-bit) Setup
Completing the Wireshark 2.2.3 (64-bit) Setup Wizard
Wireshark 2.2.3 (64-bit) has been installed on your computer.
Click Finish to close this wizard.
Run Wireshark 2.2.3 (64-bit)
Show News
< Back
Finish
Cancel

1. Start a browser session.
   1.1 Retrieve the resource: www.network-tools.com.

   a. Select Express and specify the server as www.yorku.ca ➔ Click Go
      i. What is the IP address of the server? _____

      ii. Open a browser session and paste the IP address in the address bar of the browser, document the output using a screen snapshot.

      iii. What is the source of the server that performed resolution of whois utility? _____

      iv. What is the network name?

      v. What is the Organization's name?

      vi. From the Tools menu, select Nslookup and specify www.yorku.ca for the host name and select All for Query Type.

         1. What type of records does the server has (A or AAAA)?
         2. What is the IP address of the server?
         3. Attempt to browse the home page of the server using its IP address and document the output using a screen snapshot.
         4. What is the 1st domain server's name?
         5. What is the 2nd domain server's name?

      vii. From the Tools menu, select Nslookup and specify www.iis.se for the host name and select All for Query Type.
         1. What type of records does the server has?
         2. What is/are the IP address of the server?
         3. Attempt to browse the home page of the server using its IP addresses IPv4 and IPv6 and document the output using a screen snapshot.
         4. Reattempt to brows the home page using [IPv6], you should include the IPv6 in the brackets in the address bar of the browser.
         5. What is the 1st domain server's name?
         6. What is the 2nd domain server's name?
         7. Test connectivity to the server using the Ping utility and IPv6.

      viii. Using the resource https://tools.keycdn.com/geo,
         1. find the geographical location of the server www.yorku.ca by name and by IPv4.

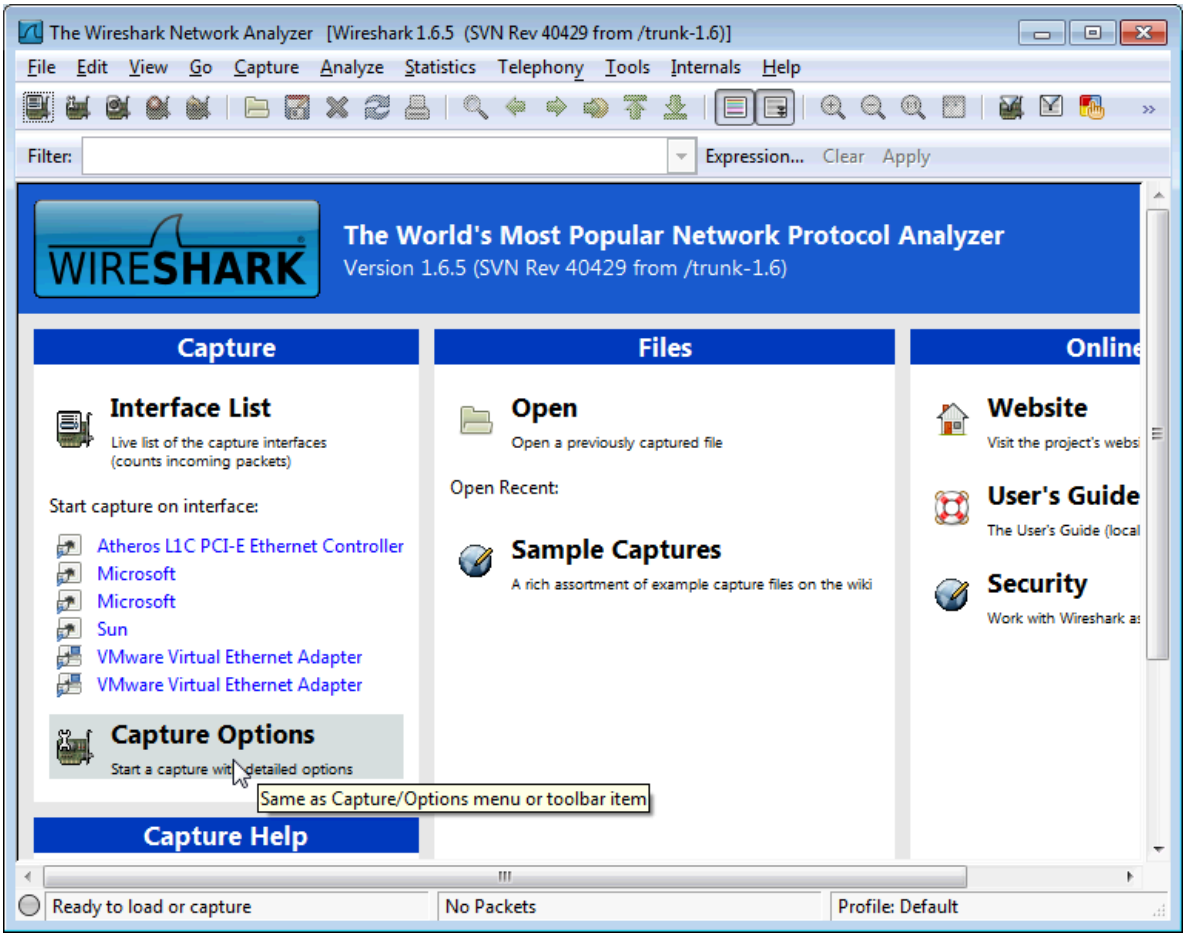
a. What is the host name?
b. What is AS number of the network?
c. What are the city, country, content, and latitude/longitude coordinates values.

2. Find the geographical location of the server www.iis.se by the server name, IPv4, and IPv6.
   a. What is the host name?
   b. What is AS number of the network?
   c. What are the city, country, content, and latitude/longitude coordinates values?

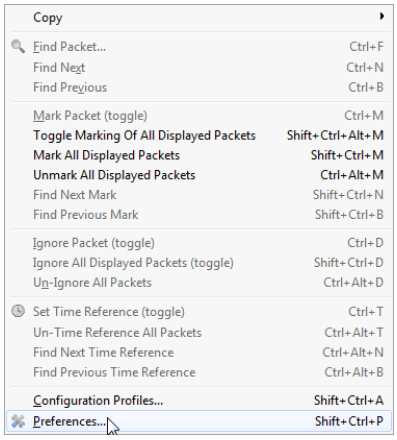
ix. Using the resource https://network-tools.com/, select HTTP Headers and specify the server name yorku.ca as the server name.
   1. What is the HTTP protocol version running on the server?
   2. What type of web server is running on the server?
   3. What type of operating system is running on the server?
   4. Has the server reported any error messages? If so, search the code and attempt to interpret its meaning?

x. Using the resource https://network-tools.com/, select HTTP Headers and specify the server name www.iis.se as the server name.
   1. What is the HTTP protocol version running on the server?
   2. What type of web server is running on the server?
   3. What type of operating system is running on the server?
   4. Has the server reported any error messages? If so, search the code and attempt to interpret its meaning?
   5. Re-attempt requesting the headers using https://www.iis.se instead of www.iis.se; has the server reported any messages; if so, what is the message code?

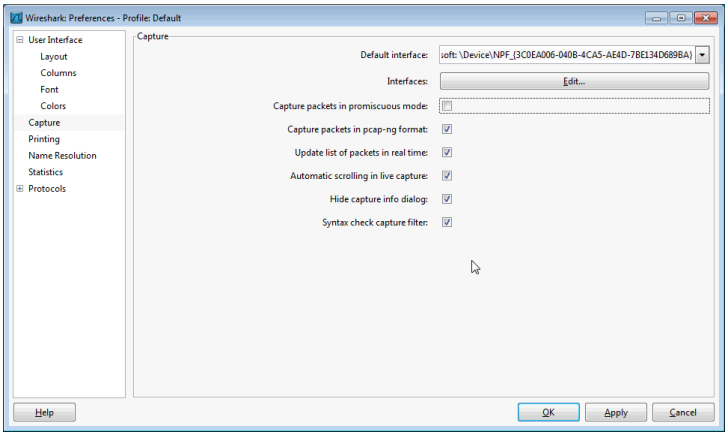
Part 2: Packet Analysis



- From the Edit menu, select Edit □□Preference:

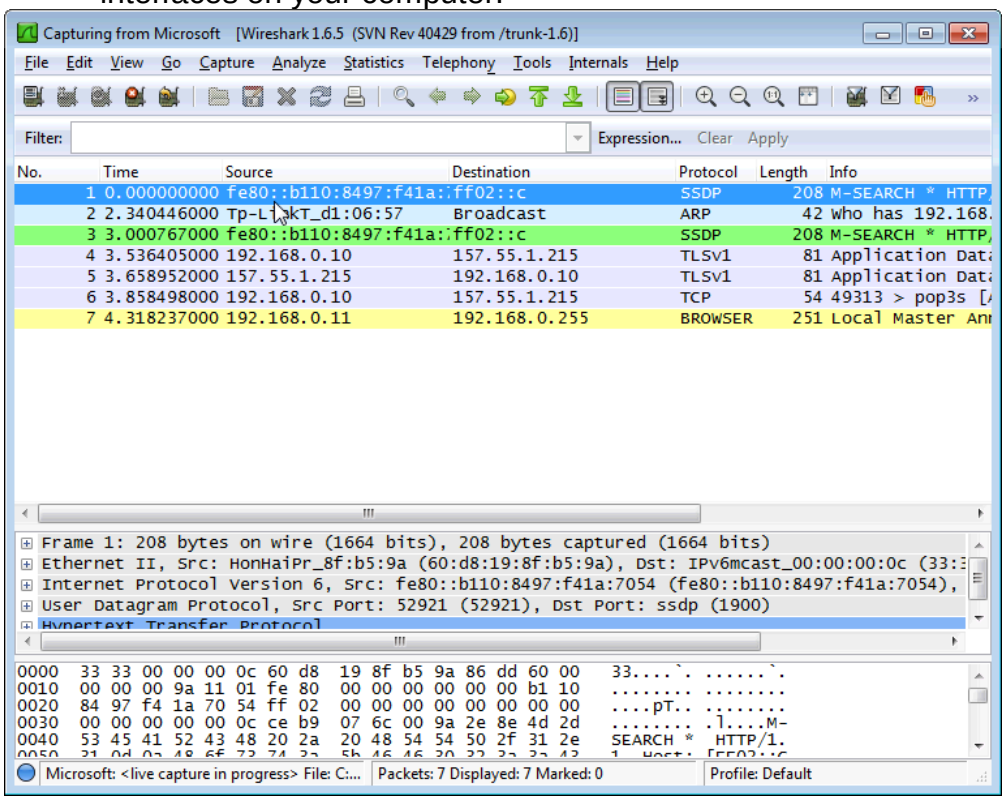


- From User Interface tab, select Capture □Deselect the ``Capture packets in promiscuous mode`` option



- Click Apply.
- What is promiscuous mode?

  - Click on ``Interfaces List`` and Start the capturing service for all physical interfaces on your computer.



  - Document your steps to be included in your lab report.

Part 2: HTTP Demonstration: Download the PuTTY for Telnet using Hypertext Transfer Protocol

This section demonstrates a method for downloading a file using the Hypertext Transfer Protocol.

1.1 Open your Internet browser and request the Putty download page using the following URL:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

1.2 Make sure that your WireShark is running and from the Capture Menu click Restart.

1.3 Switch to Putty Homepage using Alt-key and Tab-key.

1.4 From the Putty Homepage, click on puttytel.exe hyperlink in order to down load the file using Hypertext Transfer Protocol.

1.5 On the WireShark Capture menu, click stop

1.6 Save the captured segment in a file and name it http-puttytel.pcap

1.7 On the Putty Homepage, hover with mouse on the puttytel.exe hyperlink and right-click the mouse and select Properties. From the dialog box obtain the URL for the hyperlink (or copy link address and paste into a notepad file).

1.8 From the hyper link extract the URI for the putty server:_____

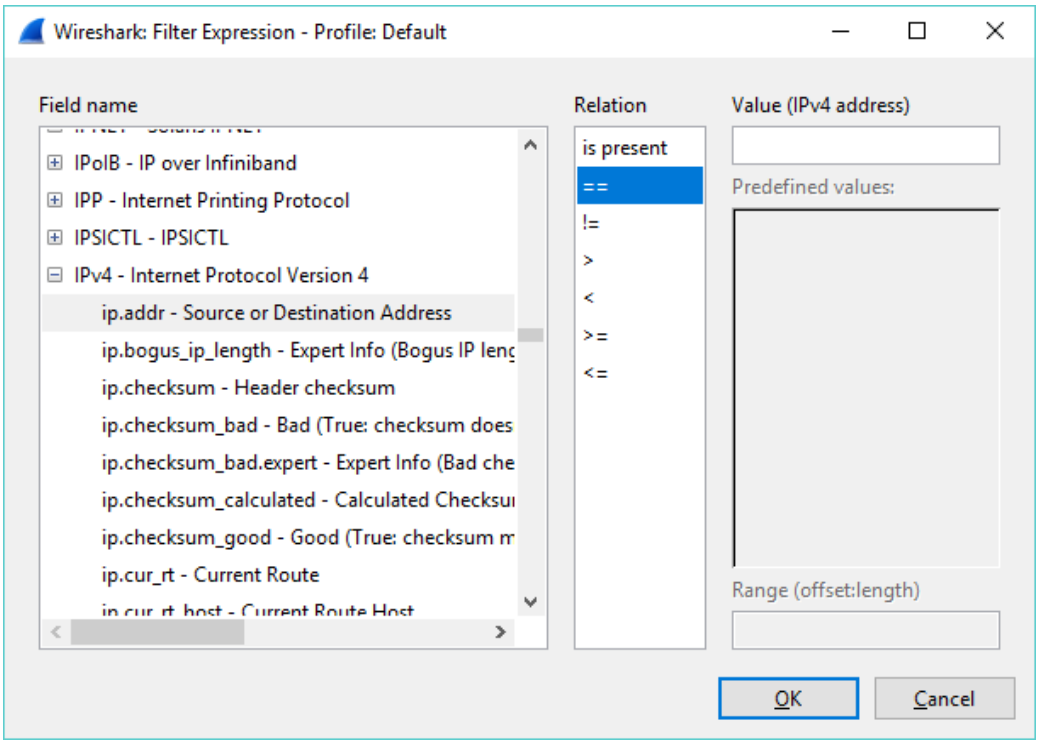
1.9 Ping the extracted URL.

1.10 Identify the IP address of the pinged server: _____

1.11 Identify the port number of the server: _____

1.12 Using the filter dialog box, extract the frames that includes the IP address that you have identified in step 1.10 (above):

- Click on Expression.
- Specify field name as IPv4 – Internet Protocol Version 4
- Select ip.addr as Source or Destination Address
- Specify relation as "= ="
- Identify the IPv4 address that matches step 1.10



Part 2: FTP Demonstration: Download the PuTTY for Telnet utility using File Transfer Protocol

This section demonstrates a method for downloading the file puttytel.exe using the File Transfer Protocol.

1.13 Open your Internet browser and request the Putty download page using the following URL:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

1.14 Make sure that your WireShark is running and from the Capture Menu click Restart.

1.15 Switch to Putty Homepage using Alt-key and Tab-key.

1.16 From the Putty Homepage, click on (or by FTP) hyperlink and download the file puttytel.exe

1.17 On the WireShark Capture menu, click stop.

1.18 Save the captured segments in the file: ftp-puttytel.pcap

1.19 On the Putty Homepage: Right-click the mouse on the on puttytel.exe hyperlink and select Properties. From the dialog box obtain the URL for the hyperlink.

1.20 From the hyper link extract the URL for the putty server:

1.21 Ping the extracted URL.

1.22 Identify the assigned IP address of the pinged server: _____

1.23 Display the segment of frames for that particular IP using the WireShark captured data

1.24 Demonstrate the port number of the server

1.25 Identify the IP address of the server using Wireshar