

Lab 4 – Observing Network Traffic

Write down the name of the equipment used in this lab:

Computer Name	
---------------	--

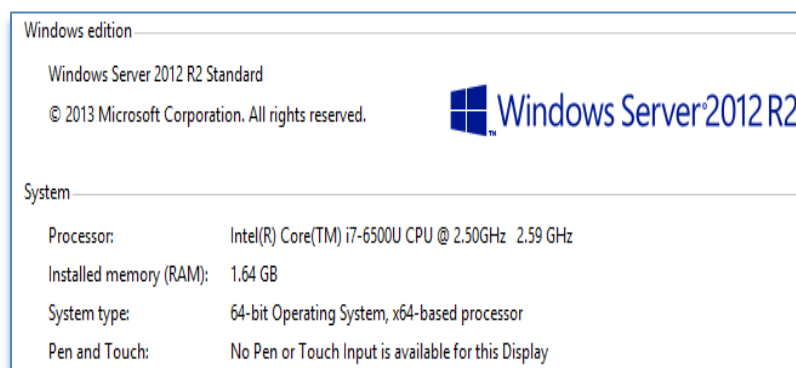
In this lab, we will be using Wireshark, a software-based protocol analyser to troubleshoot network problems by observing network traffic. This software will help students visualize packet content and network dialog. We will observe the dialog of some protocols such as ARP, ICMP, DHCP, and HTTP. Hopefully this lab will help you gain more understanding of a protocol analyzer and its value as a diagnostic tool.

A. Installing the latest version of Wireshark

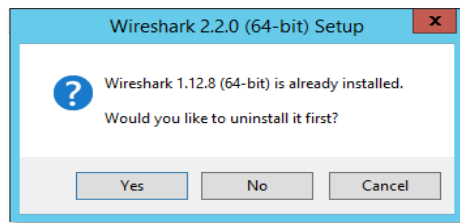
Login to a computer by clicking the CSIS student icon by using the following password: **STF@II2016**
Run the Oracle VM Virtualbox program, double-click on Windows Server 2012 VM and login to the server (username: administrator, password: Id0ntf0rget). Go to View and click *Switch to Fullscreen* or simply press [RightCtrl] + F to switch to fullscreen. You can go back to the windowed mode any time by pressing [RightCtrl] + F.

Wireshark (formerly Ethereal) is a free, open-source, network protocol analyzer that runs on Windows, Linux/Unix, and Mac computers. Wireshark's main website, at www.wireshark.org.

- a. Go to <https://www.wireshark.org/#download>
- b. Download the appropriate version (e.g. Windows 32bit).
 - When in doubt, you can use control panel -> System and Security -> System to give you a hint on which version to use. Example



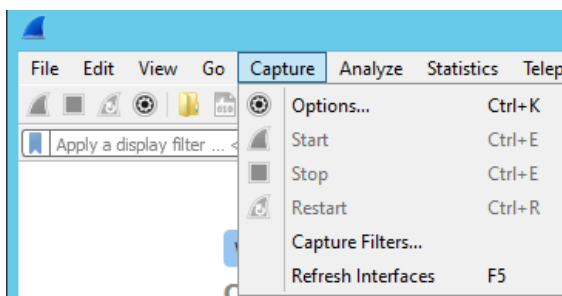
- c. Install Wireshark. Yes, uninstall the previous version if it asks.



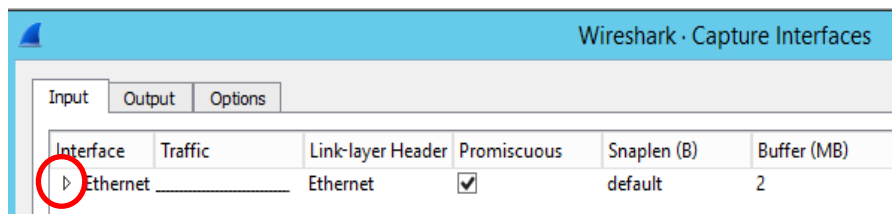
- d. Leave the default selected features. Continuously click next/install ... until it actually installs it. Relax, you will not be asked for your credit card.

B. Network Protocol Analyzer

1. Run the “wireshark” program
2. Go to the Capture menu and select Option. You should see a list of the capture interfaces.



(Q.1) Click on the arrow next to “Ethernet”. Record the IPv4 address listed.

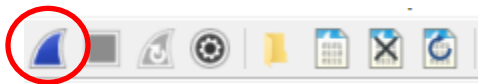



(Q.2). Underneath the interface list, there is a check box for “Enable promiscuous mode on all interfaces”. To capture network traffic between your computer and a destination computer (which is what we will do in this lab), which mode should be used?

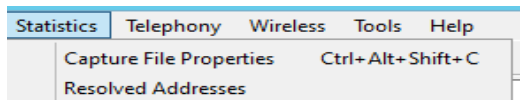
Promiscuous mode:

- if you are thinking something outside of networking concept, that’s not it.
- When enabled, it captures packets even if not it does not concern your machine.
- If you are using wifi, you need to install AirPcap adapter. Otherwise, it would still run in promiscuous mode.

3. Click start to start capturing. Another way to start capturing is to click on the blue shark fin icon near the top left corner.



4. Click on the notepad/pencil icon on the bottom left corner  (or from the Statistics menu, Capture File Properties)



Must be running. Otherwise, “Capture File Properties” is disabled

(Q.3). From the capture properties:

- a. Take a screenshot of the information under statistics (hint: just scroll down)
- b. After 2 minutes or so, take another screenshot. (Purpose: To show that there is a continuous packet being sent)

C. Observing ping

Ping (packet internet gopher) is the utility used to verify that TCP/IP is installed, bound to the NIC, configured correctly, and communicating with the network. Ping sends echo request and reply messages to devices on the network.

1. **ping target_address**, where target_address can be an IP address or a domain name.
2. Close any web browsers that are open to avoid capturing unrelated network traffic.
3. Prepare a PING command.
 - a. ping google.ca (don't press enter yet. Leave the Command Prompt window open)
4. From Wireshark, click "Start" to start capturing from the active interface. No need to save previous results.
5. Switch to the command prompt window and press enter (to execute the ping command)
6. After all the reply/output is displayed, Switch back to Wireshark and stop the capture. **Go to File > Save As >** enter a name and save it on your desktop. You can use it later if you need to look at the capture again.
7. Examine the capture messages. Too many info?
Try filtering ICMP (Internet Control Message Protocol)



ICMP (Internet Control Message Protocol)

- ICMP - a Network layer core protocol that reports on the success or failure of data delivery
- ICMP can indicate when:
 - Part of a network is congested
 - Data fails to reach its destination
 - Data has been discarded when the TTL has expired
- ICMP announces transmission failures to sender but does not correct errors it detects

(Q.4). What protocol was used by the ping utility?

The TYPES defined are:

TYPE	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect Message
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request (No Longer Used)
16	Information Reply (No Longer Used)
17	Address Mask Request
18	Address Mask Reply

Possible ICMP types

(Q.5). Select one of (ping) request entries. Indicate the no. , source ip, and destination ip

Take a screenshot

Example

No.	Time	Source	Destination	Protocol	Length	Info
→ 86	12.013096	192.168.0.16	216.58.216.163	ICMP	74	Echo (ping) request id=0x0001, seq=1179/39684, ttl=128 reply in 87)

(Q.6). Below, you will find Internet Control Message Protocol details. Expand, look at the type value, and take a screenshot. The response frame # should match your Q.5 screenshot

Example

Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x48c0 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 1179 (0x049b)
Sequence number (LE): 39684 (0x9b04)
[Response frame: 87]
Data (32 bytes)
Data: 61626364656666768696a6b6c6d6e6f707172737475767761...
[Length: 32]

Big-endian (BE) and little-endian (LE) are terms to describe how the bytes are stored in computer memory.

8. Now prepare a new ping to a domain name (don't hit enter yet): **ping cbc.ca**
9. In Wireshark, click the blue shark-fin icon to start capturing.
10. Go back to command prompt and press enter to execute the ping. Once the ping stops, stop the Wireshark capture and save it for future reference.

(Q.7). *When pinging cbc.ca, what protocol was used before fulfilling your Echo (ping) request? cbc.ca's ip address: _____*

Hints:

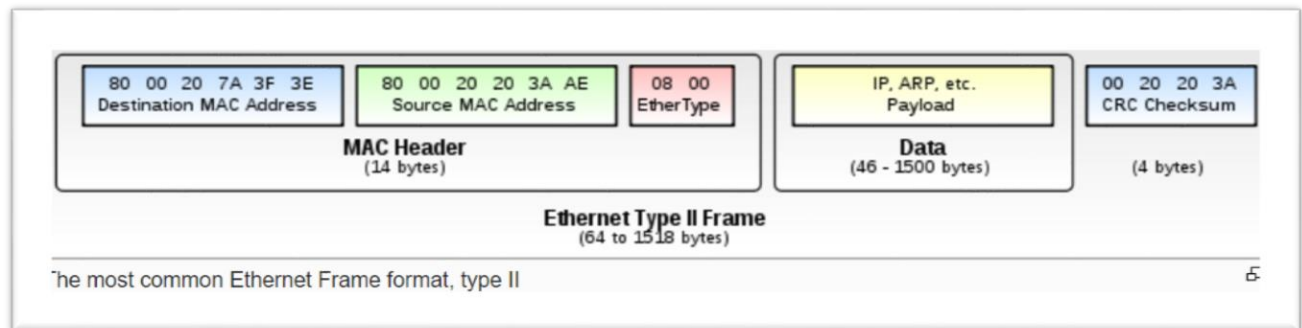
- a. remove the any filtering
- b. Try to find cbc.ca under the column info

11. Now capture and observe ping to the following address: **ping -n 10 192.168.xx.255**
IP addresses that end with .255 is said to be "broadcast"
-n 10 means "expect 10 replies"

(Q.8) Take a screenshot of the reply. Observe the IP addresses that replied.

D. Observing Ethernet Traffic

In this exercise, you'll study Ethernet frames containing the dialogue of an HTTP session - that is, surfing to a web site.



Source: https://en.wikipedia.org/wiki/Ethernet_frame

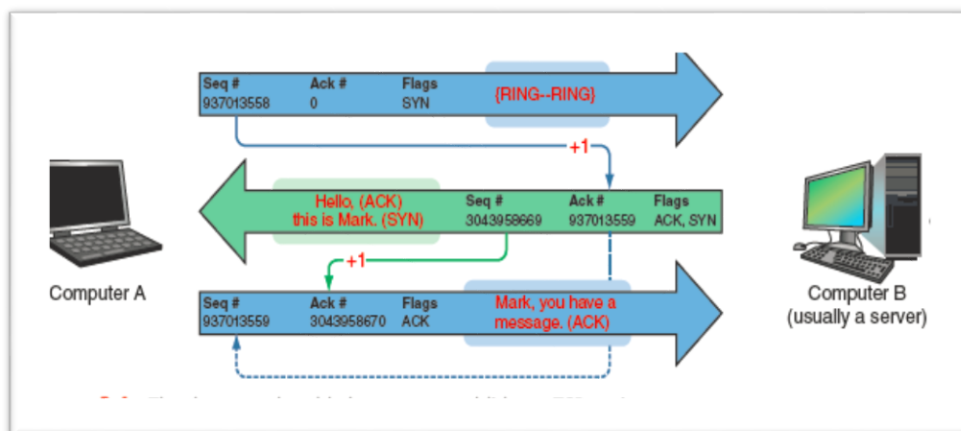
EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN ^[4]
0x22F3	IETF TRILL Protocol
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q) and Shortest Path Bridging IEEE 802.1aq ^[5]
0x8137	IPX
0x8204	QNX Qnet

EtherType uses 2 octets
 1 octet => 1 byte
 1 byte = 4 bits
 4 bits = 1 Hexadecimal

1. Close all browsers and open a new Firefox browser.
2. Start Wireshark capture
3. On Firefox, surf to <http://www.oldmasterq.com/comics/1487/>
4. Stop the packet capture and save a copy to the desktop.

TCP Three-Way Handshake

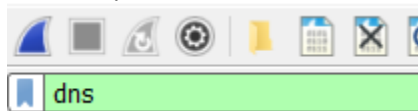
- Three transmission sent before data transmission:
 - Step 1 - request for a connection (SYN)
 - Step 2 - response to the request (SYN/ACK)
 - Step 3 - connection established (ACK)
- After the three initial messages, the payload or data is sent
- Sequence numbers will be increased by the number of bits included in each received segment
 - Confirms the correct length of message was received



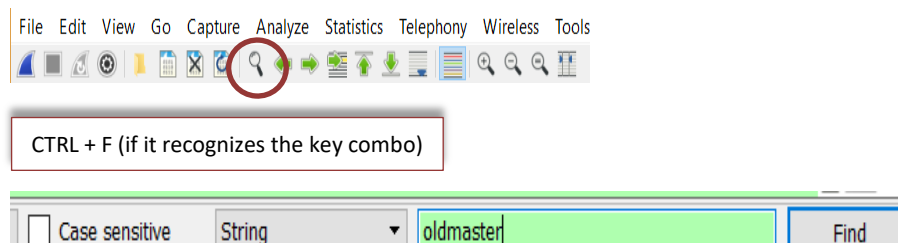
5. In Wireshark capture, try to see if you can find the DNS query for **www.oldmasterq.com**. That marks the beginning of this packet trace.

If there are too many protocols captured and displayed, you can use filter to assist you.

- a) limit the protocol to dns



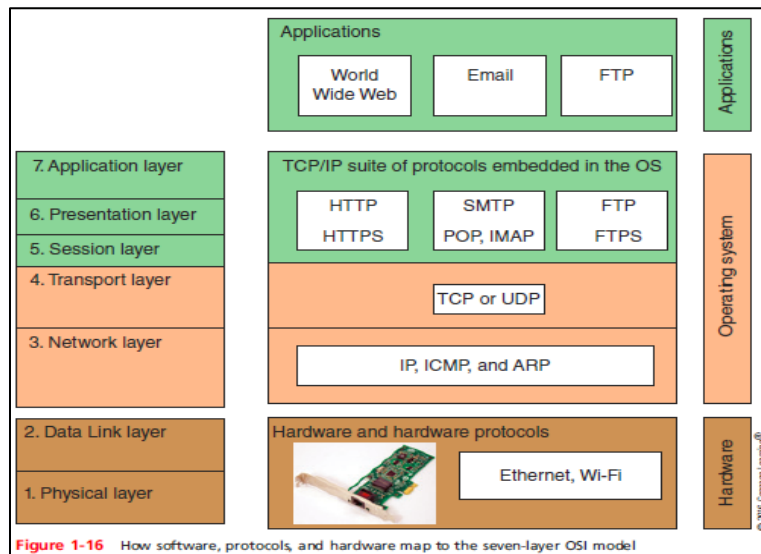
- b) you can further limit it by finding a specific string/text. Try using "Find a packet"



6. Next see if you can find the TCP three-way hand-shake. The handshake is performed before TCP transmits actual data (before the first HTTP get).
7. Let's filter out some of the messages. Type: **"http" in the filter box.**
8. The HTTP get message is the request you sent to the web server. The HTTP response usually contains status/error code, such as "200 OK", "302 Found", etc.
9. Click on one of the HTTP get message (e.g. GET / HTTP/1.1). Expand the Ethernet II information in the packet details area that is the middle of the Wireshark window.

(Q.9). Select an HTTP get message. In the middle pane of the Wireshark window, there should be 5 sections of information available. The sections correspond to layers in OSI model (e.g. Frame & Ethernet II section = layer 2/Data Link layer). Name all sections and state which layer(s) they belong to.

Guides



OSI Model				
	Layer	Protocol data unit (PDU)	Function ^[3]	Examples
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access	HTTP, NFS, FTP, Telnet, SMTP, SSH ^[4]
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption	S/MIME, TLS
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, SCP, PAP
	4. Transport	Segment (TCP) / Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	TCP, UDP, NBF
Media layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control	IPv4, IPv6, ICMP, IPsec, CLNP, DDP
	2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer	IEEE 802.2, L2TP, LLDP, IEEE 802 MAC layers (Ethernet, IEEE 802.11, etc.), PPP, ATM, MPLS
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	DOCSIS, DSL, IEEE 802 physical layers (Ethernet, IEEE 802.11, etc.), ISDN, RS-232

(Q.10). *In the HTTP Get message's Ethernet II information:*

- What is the MAC address of your computer (take a screenshot)
- What is the destination MAC address in the Ethernet frame? (take a screenshot)
 - What device does this MAC address refer to?

Hints

- a) Something to think about: would it possible for your machine to know the MAC of another computer? (no need to type your answer – just speculate)
- b) Using `ipconfig /all`, try to verify your default gateway's IP
 - a. Try `arp -a` or `arp -a IP_ADDRESS_OF_YOUR_GATEWAY`
 - i. See if you find something interesting

E. Observing DHCP

When a computer is configured to obtain an IP address automatically, it gets its IP address from the DHCP server.

1. Start a new capture in Wireshark.
2. In the command prompt, type:
 - `ipconfig /release`
 - `ipconfig /renew`
3. Stop the Wireshark capture and save as necessary.
4. Pause – relax – smile – breath - ... ok. Back to work
5. To see only the DHCP packets, **filter for “bootp” (without the quotes)**. DHCP evolved from an older protocol called BOOTP or bootstrap protocol.
6. You should see 5 messages: DHCP Release, DHCP Discover, DHCP Offer, DHCP Request, and DHCP Ack.

(Q.11). *Take a screenshot as proof ☺*

7. DHCP Release message is sent by your computer to the DHCP server to let the server know that the computer is releasing its IP address/ending the lease. After receiving this message, the IP address will become available to be assigned to other computer.
8. **Examine the DHCP Discover message** (expand Ethernet II). This is the first packet sent when the computer doesn't have any IP address

(Q.12). *Who sent the Discover message? And who was the recipient? What do you think is the purpose of this message?*

Hints:

- a. Examine the destination carefully. Look at the “description” beside the word destination.
- b. Something to think about – if you are lost in a forest, what would you do to find help? (no need to type your answer)

9. Examine the DHCP Offer message (expand Ethernet II & bootstrap protocol).

(Q.13). *Who sent the Offer message? And who was the recipient? What do you think is the purpose of this message? What is the IP lease time? What other information is included in this message?*

10. Examine the DHCP Request message.

(Q.14). *Who sent the HTTP Request message? And who was the recipient? What do you think is the purpose of this message?*

Hints

- a. expand Ethernet II & bootstrap protocol.
- b. Look at Options 53, 61, 50, and 54
- c. Something to think about – Imagine, each PC is a potential buyer and DHCP server is the seller. The buyer doesn't know if there are other buyers looking for the same product (e.g. IP address). When a seller informs the potential buyers (PC/Laptop/etc..) that he has the product (e.g. IP address), what would be the logical response of the buyer? (no need to type the answer – think about it).

11. Examine the DHCP ACK message.

(Q.15). *Who sent the ACK message? And who was the recipient? What do you think is the purpose of this message?*

Hints

- Look at the source and destination
- Compare the Bootstrap Protocol returned by DHCP offer and DHCP ACK

(Q.16). *Does DHCP use TCP or UDP?*

Guide

TCP (Transmission Control Protocol)

- Connection-oriented protocol - TCP ensures that a connection or session is established by using a three-step process called a three-way handshake

UDP (User Datagram Protocol)

- UDP provides no error checking or sequencing
 - Makes UDP more efficient than TCP
- Useful for live audio or video transmissions over the Internet

F. End of the lab

★ You need to get the lab instructor to check your work. Show all the capture files you saved.

After your work is inspected and marked, shutdown the server gracefully. Select “Other (planned)” and continue. Logoff the Windows 7 computer after you have saved all your files on an external USB/cloud storage. **All changes made to the computer will be erased.**

Deliverables

- Submit a report named **Lab4.pdf or Lab4.docx** that describes what you did in the lab including the answer to all the questions
- Submit to D2L before the due date (posted in D2L).