

CS 3873: Net-Centric Computing

Lab 1: Preparation and Warm-up

Student Name: ___Adrian Freeman___

Student Number: ___3661616___

[Mandatory] Declaration: "I warrant that this is my own work."

Signed by _Adrian Freeman_

(You can type in your name as your signature.)

From the UNB Undergraduate Calendar, available at the website:

<http://www.unb.ca/academics/calendar/undergraduate/current/regulations/universitywideacademicregulations/viii-academicoffences/index.html>.

"Plagiarism includes:

1. quoting verbatim or almost verbatim from any source, regardless of format, without acknowledgement;
2. adopting someone else's line of thought, argument, arrangement, or supporting evidence (such as, statistics, bibliographies, etc.) without indicating such dependence;
3. submitting someone else's work, in whatever form (essay, film, workbook, artwork, computer materials, etc.) without acknowledgement;
4. knowingly representing as one's own work any idea of another."

Penalties for plagiarism and other academic offences can be found at the above website.

Report for Lab Exercise 1: Preparation and Warm-up

LAB ACTIVITIES:

In this lab, we learnt how to capture packet traces with Wireshark and how to use Wireshark to examine the details of captured packets.

ANSWERS TO LAB QUESTIONS:

The following gives you one example on how to draft your answer to the lab questions.

5. Examine the trace which contains live packet data exchanged between your machine and the Web server (the host providing the webpage to your machine).
 - a. Even though the only action you took was to download a webpage, there were evidently many other protocols running on your computer that are unseen by the user. We'll learn much more about these protocols as we progress through the text! In the trace you can see many protocols listed. Choose three of these protocols from your list and use Google or go to the IETF site to find out what they are being used to support.

ICMPv6: Supports error reporting and diagnostics for IPv6, helping with network connectivity and route discovery.

ARP: Maps IP addresses to MAC addresses in IPv4 networks, enabling devices to communicate within a local network.

TLSv1.2: Encrypts data for secure communication over the internet, widely used in HTTPS and other secure protocols.

- b. Pasted at the end to improve readability of document (wouldn't it be easier to just submit the .txt file?

6. Based on the above trace, answer the following questions.
- Select the first HTTP message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer to the HTTP server. When you select the HTTP GET message, the Ethernet or Ethernet II frame, IPv4 datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window. How long did it take from when the HTTP GET message was sent until the first HTTP response was received?

No.	Time	Source	Destination	Protocol	Length	Info
13	0.883422899	10.0.0.109	128.119.245.12	HTTP	516	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
15	0.956649604	128.119.245.12	10.0.0.109	HTTP	540	HTTP/1.1 200 OK (text/html)

↑

It took $(0.956649604 - 0.883422899 = 0.073226705)$ seconds to receive the HTTP response

- In the trace you will find IPv4 addresses within the packets. Find an example packet in the trace where the IPv4 address associated with your machine is present. Compare this address with the IPv4 address you can find by using the following command: `ipconfig /all` on Windows, or `ifconfig` on MacOS or Linux. If you use Windows VM for the above capture, make sure you run the command on the terminal within the VM. Running this command also gives a 48-bit physical address for the network interface. This is the MAC (medium access control) address (not discussed in class yet) of your machine. Can you find the MAC address of the packet in the trace? Is it the same as the physical address returned by the above command? If you use your personal computer, you can mask selected digits of your MAC address and IPv4 address in your answers to protect your private information.

```

(adrian@desktop-kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.109 netmask 255.255.255.0 broadcast 10.0.0.255
    inet6 2607:fea8:e923:2c00:2ef0:5dff:fe81:c702 prefixlen 64 scopeid 0x0
<global>
    inet6 2607:fea8:e923:2c00::106c prefixlen 128 scopeid 0x0<global>
    inet6 fe80::2ef0:5dff:fe81:c702 prefixlen 64 scopeid 0x20<link>
    inet6 2607:fea8:e923:2c00:f965:c7f9:8963:999d prefixlen 64 scopeid 0x0
<global>
    ether 2c:f0:5d:81:c7:02 txqueuelen 1000 (Ethernet)
  > Frame 13: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) c
  > Ethernet II, Src: MicroStarINT-81:c7:02 (2c:f0:5d:81:c7:02), Dst: Vantiva
  > Internet Protocol Version 4, Src: 10.0.0.109, Dst: 128.119.245.12
  > Transmission Control Protocol, Src Port: 58860, Dst Port: 80, Seq: 1, Ack
  > Hypertext Transfer Protocol
  
```

The MAC and IPv4 addresses are the same in my ifconfig and the trace.

No.	Time	Source	Destination	Protocol	Length	Info
13	0.883422899	10.0.0.109	128.119.245.12	HTTP	516	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 13: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) on interface eth0, id 0

Section number: 1

Interface id: 0 (eth0)

Interface name: eth0

Encapsulation type: Ethernet (1)

Arrival Time: Sep 13, 2024 16:18:11.114645998 ADT

UTC Arrival Time: Sep 13, 2024 19:18:11.114645998 UTC

Epoch Arrival Time: 1726255091.114645998

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000107200 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.883422899 seconds]

Frame Number: 13

Frame Length: 516 bytes (4128 bits)

Capture Length: 516 bytes (4128 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02), Dst: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)

Destination: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)

Address: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)

....0. = LG bit: Globally unique address (factory default)

....0. = IG bit: Individual address (unicast)

Source: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02)

Address: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02)

....0. = LG bit: Globally unique address (factory default)

....0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.0.109, Dst: 128.119.245.12

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 502

Identification: 0xbf1d (48925)

010. = Flags: 0x2, Don't fragment

0... = Reserved bit: Not set

.1.. = Don't fragment: Set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0xf9f3 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.0.0.109

Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 58860, Dst Port: 80, Seq: 1, Ack: 1, Len: 462

Source Port: 58860

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

..0. = RST: Absent

...0 = FIN: Absent

.... 1... = Data: Present

.... .1.. = ACK: Present

.... ..1. = SYN-ACK: Present

.... ...1 = SYN: Present

[Completeness Flags: ..DASS]

[TCP Segment Len: 462]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2764171843

[Next Sequence Number: 463 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1183115203

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 ... = Acknowledgment: Set

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

[TCP Flags:AP...]

Window: 251

[Calculated window size: 32128]

[Window size scaling factor: 128]

Checksum: 0x81d9 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[Time since first frame in this TCP stream: 0.055403906 seconds]

[Time since previous frame in this TCP stream: 0.000107200 seconds]

[SEQ/ACK analysis]

[iRTT: 0.055296706 seconds]

[Bytes in flight: 462]

[Bytes sent since last PSH flag: 462]

TCP payload (462 bytes)

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]

[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 15]
[Next request in frame: 17]

No.	Time	Source	Destination	Protocol	Length	Info
15	0.956649604	128.119.245.12	10.0.0.109	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 15: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface eth0, id 0

Section number: 1

Interface id: 0 (eth0)

Interface name: eth0

Encapsulation type: Ethernet (1)

Arrival Time: Sep 13, 2024 16:18:11.187872703 ADT

UTC Arrival Time: Sep 13, 2024 19:18:11.187872703 UTC

Epoch Arrival Time: 1726255091.187872703

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.016896964 seconds]

[Time delta from previous displayed frame: 0.073226705 seconds]

[Time since reference or first frame: 0.956649604 seconds]

Frame Number: 15

Frame Length: 540 bytes (4320 bits)
 Capture Length: 540 bytes (4320 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
 [Coloring Rule Name: HTTP]
 [Coloring Rule String: http || tcp.port == 80 || http2]
 Ethernet II, Src: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e), Dst: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02)
 Destination: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02)
 Address: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
 Source: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)
 Address: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
 Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.109
 0100 = Version: 4
0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 526
 Identification: 0x6a0b (27147)
 010. = Flags: 0x2, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 44
 Protocol: TCP (6)
 Header Checksum: 0x62ee [validation disabled]
 [Header checksum status: Unverified]

Source Address: 128.119.245.12

Destination Address: 10.0.0.109

Transmission Control Protocol, Src Port: 80, Dst Port: 58860, Seq: 1, Ack: 463, Len: 486

Source Port: 80

Destination Port: 58860

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

..0. = RST: Absent

...0 = FIN: Absent

.... 1... = Data: Present

.... .1.. = ACK: Present

.... ..1. = SYN-ACK: Present

.... ...1 = SYN: Present

[Completeness Flags: ..DASS]

[TCP Segment Len: 486]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1183115203

[Next Sequence Number: 487 (relative sequence number)]

Acknowledgment Number: 463 (relative ack number)

Acknowledgment number (raw): 2764172305

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

000. = Reserved: Not set

...0 = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 1... = Push: Set

....0.. = Reset: Not set

....0. = Syn: Not set

....0 = Fin: Not set

[TCP Flags:AP...]

Window: 237

[Calculated window size: 30336]

[Window size scaling factor: 128]
Checksum: 0xeca7 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.128630611 seconds]
[Time since previous frame in this TCP stream: 0.016896964 seconds]
[SEQ/ACK analysis]
[iRTT: 0.055296706 seconds]
[Bytes in flight: 486]
[Bytes sent since last PSH flag: 486]
TCP payload (486 bytes)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 13 Sep 2024 19:18:11 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Fri, 13 Sep 2024 05:59:01 GMT\r\n
ETag: "80-621f9eb7e378d"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.073226705 seconds]

[Request in frame: 13]

[Next request in frame: 17]

[Next response in frame: 18]

[Request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>]

File Data: 128 bytes

Line-based text data: text/html (4 lines)