

Data Communications Laboratory Introduction to Wireshark

Your Name: Khalid Bakhshi

Your Student ID: 46392459

Documentation Task 1.

What interfaces are available on your computer? What do they appear to be? Do they all have the same IP address? Record this in your documentation.

Local Area Connection* 11	—	Ethernet	✓	default	2	—
Local Area Connection* 9	—	Ethernet	✓	default	2	—
Local Area Connection* 8	—	Ethernet	✓	default	2	—
Bluetooth Network Connection	—	Ethernet	✓	default	2	—
Addresses: 169.254.160.132, fe80::91e2:6a75:88dc:2539						
Wi-Fi	—	Ethernet	✓	default	2	—
Addresses: 10.126.70.238, fe80::b36ff0a8:8fa4:1ea0						
Local Area Connection* 2	—	Ethernet	✓	default	2	—
Addresses: 169.254.197.116, fe80::407e:5e1c:9227:c76						
Local Area Connection* 1	—	Ethernet	✓	default	2	—
Addresses: 169.254.246.118, fe80::f6b0:2b91:9032:2e7c						
Adapter for loopback traffic capture	—	BSD loopback	✓	default	2	—
Addresses: ::1, 127.0.0.1						
Ethernet	—	Ethernet	✓	default	2	—
Addresses: 169.254.251.104, fe80::d18f:739e:1364:1687						
Event Tracing for Windows (ETW) reader	—	DLT_ETW	—	default	—	—

They all have different IP addresses because they are different networks. The network that my personal computer is connected to is the wifi network

Documentation Task 2.

Record the IP address and MAC (Ethernet) address for the Ethernet interface of the computer you are using

IP address is IPv4: 10.126.70.238

Physical Address is: 34-6F-24-57-7F-57

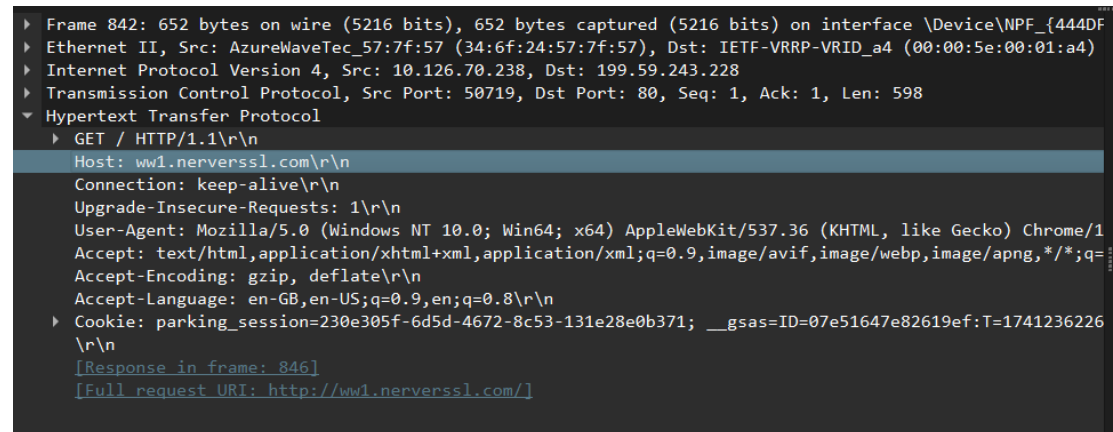
Documentation Task 3.

1. How many HTTP packets were received by your machine?

1018 http packets were received by my machine

2. Which one contains the main source code for the web page? Could you tell this from the main capture window? How? *Hint: make sure the HTTP section is selected in the packet in the middle pane.*

The column in the main capture window (top pane) shows details like 652 GET / HTTP/1.1.



```
▶ Frame 842: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \Device\NPF_{444DF...}
▶ Ethernet II, Src: AzureWaveTec_57:7f:57 (34:6f:24:57:7f:57), Dst: IETF-VRRP-VRID_a4 (00:00:5e:00:01:a4)
▶ Internet Protocol Version 4, Src: 10.126.70.238, Dst: 199.59.243.228
▶ Transmission Control Protocol, Src Port: 50719, Dst Port: 80, Seq: 1, Ack: 1, Len: 598
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: ww1.nerverssl.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1...
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=...
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    Cookie: parking_session=230e305f-6d5d-4672-8c53-131e28e0b371; __gsas=ID=07e51647e82619ef:T=1741236226...
  ▶ [Response in frame: 846]
  ▶ [Full request URI: http://ww1.nerverssl.com/]
```

Was unable to get line based text data

Documentation Task 4.

1. Draw a diagram showing (in outline, don't worry about details such as how many bytes are used and fields in each packet) how the the IP, TCP and HTTP packets are contained within the Ethernet frame

Ethernet II → Shows **MAC** addresses.

Internet Protocol (IP) → Shows **Source & Destination IP**.

Transmission Control Protocol (TCP) → Shows **Port Numbers** and sequence numbers

Hypertext Transfer Protocol (HTTP) → Shows the **actual web request or response**.

Documentation Task 5.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message.

1. How many bytes long is the packet?

344	27.545078	10.126.70.238	23.221.133.91	HTTP	495 GET / HTTP/1.1
-----	-----------	---------------	---------------	------	--------------------

It is 495 bytes long

2. What is the 48-bit MAC address of your computer?

34-6F-24-57-7F-57

3. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of `www.bom.gov.au` ? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong.]

It leads to a local router. My computer does not know the MAC address of `www.bom.gov.au` because it communicates with routers and network devices that handle the traffic for the website.

4. What is the hexadecimal (shown by 0xnnnn) value for the two-byte “Type field” in the Ethernet header?

0x0800

5. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? *Hint: count the number of bytes in the raw packet pane at the bottom of the Wireshark window.*

54-56

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

6. What is the value of the Ethernet source address? Is this the address of your computer, or of `www.bom.gov.au` ? What device has this as its Ethernet address?

```
Ethernet II, Src: AzureWaveTec_57:7f:57 (34:6f:24:57:7f:57), Dst: IETF-VRRP-VRID_a4 (00:00:5e:00:01:a4)
  Destination: IETF-VRRP-VRID_a4 (00:00:5e:00:01:a4)
    ..0. .... = LG bit: Globally unique address (factory default)
    ...0. .... = IG bit: Individual address (unicast)
  Source: AzureWaveTec_57:7f:57 (34:6f:24:57:7f:57)
    ..0. .... = LG bit: Globally unique address (factory default)
    ...0. .... = IG bit: Individual address (unicast)
```

7. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

The destination address of the ethernet frame is the router. No this isn't the the ethernet address of my computer.

8. What is the hexadecimal value for the two-byte “Type field” in the Ethernet header?
IPv4 (0x800)
9. Is the OK in the HTTP message actually contained in the HTTP packet shown to you by Wireshark when you filter for HTTP packets? If not, where is it?