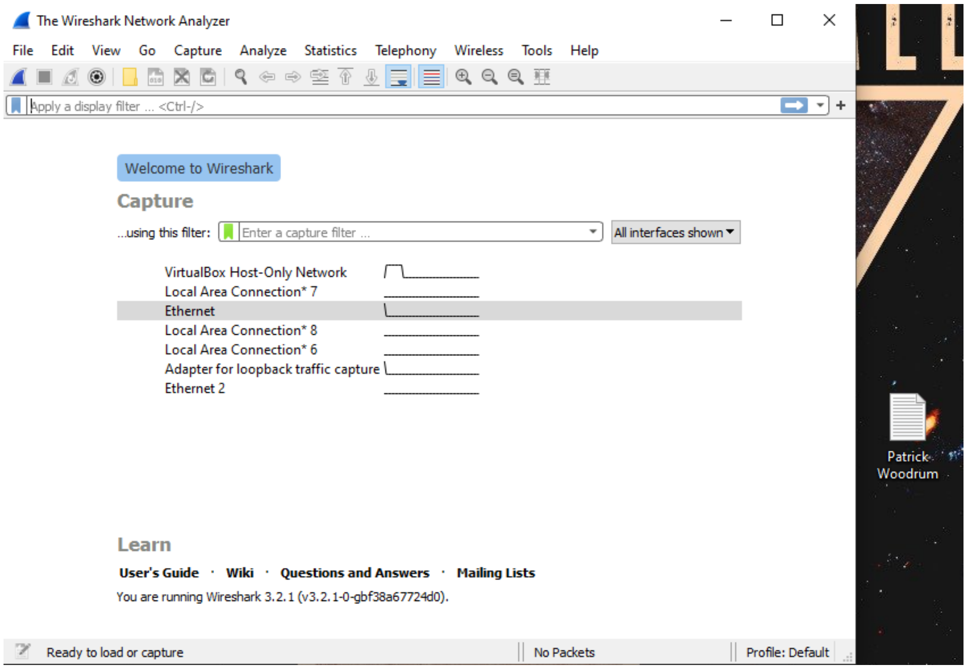
CPSC 3600 HW1

Lab Task 1

1.1 - Install Wireshark

After navigating to http://www.wireshark.org, the program was successfully installed and set up.



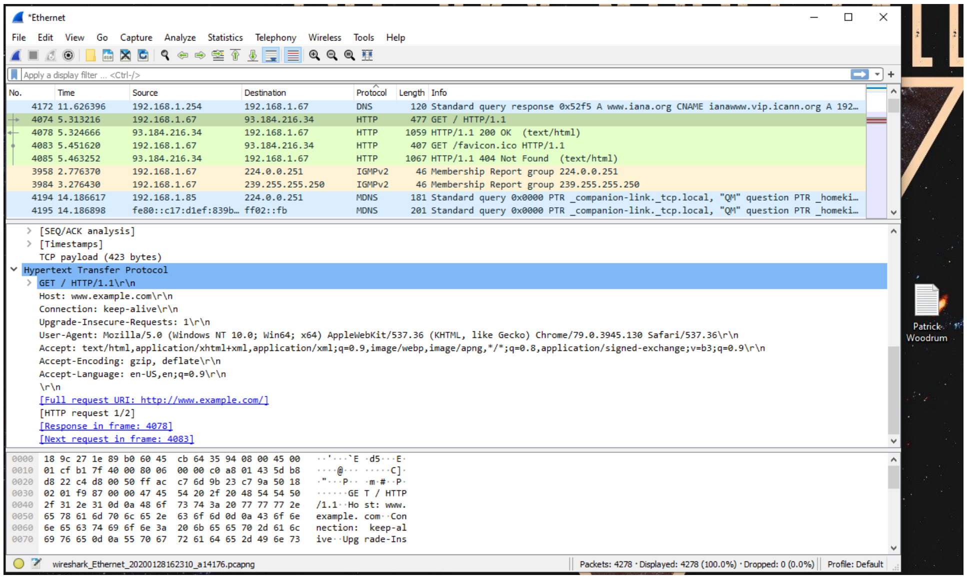
VirtualBox Host-Only Network
Local Area Connection* 7
Ethernet
Local Area Connection* 8
Local Area Connection* 6
Adapter for loopback traffic capture
Ethernet 2

You are running Wireshark 3.2.1 (v3.2.1-0-gbf38a67724d0).

Ready to load or capture | No Packets | Profile: Default

1.2 - Trace HTTP

Wireshark was then set up using the capture filter through my ethernet port. I cleared my browsing cache on Google Chrome to be sure everything ran smoothly. Following this, I navigated to www.example.com with the capture turned on and received the following information after finding the HTTP Protocol.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Patrick Woodrum

No.	Time	Source	Destination	Protocol	Length	Info
4172	11.626396	192.168.1.254	192.168.1.67	DNS	120	Standard query response 0x52f5 A www.iana.org CNAME ianawww.vip.icann.org A 192…
4074	5.313216	192.168.1.67	93.184.216.34	HTTP	477	GET / HTTP/1.1
4078	5.324666	93.184.216.34	192.168.1.67	HTTP	1059	HTTP/1.1 200 OK (text/html)
4083	5.451620	192.168.1.67	93.184.216.34	HTTP	407	GET /favicon.ico HTTP/1.1
4085	5.463252	93.184.216.34	192.168.1.67	HTTP	1067	HTTP/1.1 404 Not Found (text/html)
3958	2.776370	192.168.1.67	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
3984	3.276430	192.168.1.67	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
4194	14.186617	192.168.1.85	224.0.0.251	MDNS	181	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homeki…
4195	14.186898	fe80::c17:d1ef:839b…	ff02::fb	MDNS	201	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homeki…

```
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (423 bytes)
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.example.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/79.0.3945.130 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://www.example.com/]
    [HTTP request 1/2]
    [Response in frame: 4078]
    [Next request in frame: 4083]
```

```
0000  18 9c 27 1e 89 b0 60 45  cb 64 35 94 08 00 45 00   ··'···`E ·d5···E·
0010  01 cf b1 7f 40 00 80 06  00 00 c0 a8 01 43 5d b8   ····@··· ·····C]·
0020  d8 22 c4 d8 00 50 ff ac  c7 6d 9b 23 c7 9a 50 18   ·"···P·· ·m·#··P·
0030  02 01 f9 87 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1··Ho st: www.
0050  65 78 61 6d 70 6c 65 2e  63 6f 6d 0d 0a 43 6f 6e   example. com··Con
0060  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0070  69 76 65 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   ive··Upg rade-Ins
```

wireshark_Ethernet_20200128162310_a14176.pcapng | Packets: 4278 · Displayed: 4278 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

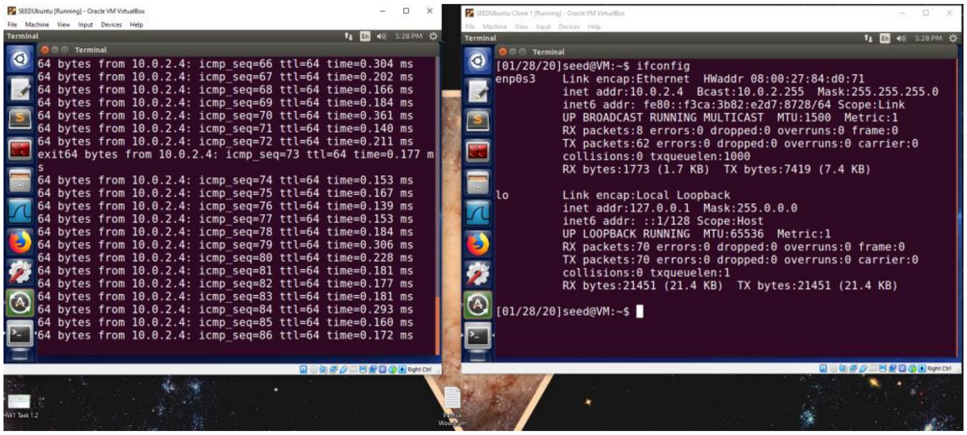
1.3 - Trace Decode

1. The full URL of the object requested by the browser is http://www.example.com/
2. My browser is using HTTP Request Version: HTTP/1.1 and the destination web server is using HTTP/1.1 as well.
3. This HTTP connection is persistent. This is known via the "Connection: keep-alive\r\n" line. All HTTP requests are labelled as keep-alive and are therefore persistent.
4. The browser used to send the request is Google Chrome version 79.0.3945.130. This is found beside "User-Agent".
5. The web browser was running on Windows 10 64-bit and is shown under User-Agent as (Windows NT 10.0; Win64; x64).
6. The kind of web server that answered the request was ECS (agb/5338)\r\n and was found beside "Server:" in the HTTP response packet
7. The server produced a 404 Not Found error when requesting from the server but the file data was successfully transferred as the HTML type, found under the first line after using the dropdown arrow for "Line-based text data: text/html"

<u>Lab Task 2</u>

2.1 - Deploy Two Virtual Machines

After successfully cloning my first VM, I booted both at the same time and used ifconfig and the ping command to see each respective address and to test the connection between the two.


SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
5:28 PM
Terminal
Right Ctrl
HW1 Task 1.2
Patrick Woodrum
SEEDUbuntu Clone 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
5:28 PM
Terminal
Right Ctrl

```
64 bytes from 10.0.2.4: icmp_seq=66 ttl=64 time=0.304 ms
64 bytes from 10.0.2.4: icmp_seq=67 ttl=64 time=0.202 ms
64 bytes from 10.0.2.4: icmp_seq=68 ttl=64 time=0.166 ms
64 bytes from 10.0.2.4: icmp_seq=69 ttl=64 time=0.184 ms
64 bytes from 10.0.2.4: icmp_seq=70 ttl=64 time=0.361 ms
64 bytes from 10.0.2.4: icmp_seq=71 ttl=64 time=0.140 ms
64 bytes from 10.0.2.4: icmp_seq=72 ttl=64 time=0.211 ms
exit64 bytes from 10.0.2.4: icmp_seq=73 ttl=64 time=0.177 m
s
64 bytes from 10.0.2.4: icmp_seq=74 ttl=64 time=0.153 ms
64 bytes from 10.0.2.4: icmp_seq=75 ttl=64 time=0.167 ms
64 bytes from 10.0.2.4: icmp_seq=76 ttl=64 time=0.139 ms
64 bytes from 10.0.2.4: icmp_seq=77 ttl=64 time=0.153 ms
64 bytes from 10.0.2.4: icmp_seq=78 ttl=64 time=0.184 ms
64 bytes from 10.0.2.4: icmp_seq=79 ttl=64 time=0.306 ms
64 bytes from 10.0.2.4: icmp_seq=80 ttl=64 time=0.228 ms
64 bytes from 10.0.2.4: icmp_seq=81 ttl=64 time=0.181 ms
64 bytes from 10.0.2.4: icmp_seq=82 ttl=64 time=0.177 ms
64 bytes from 10.0.2.4: icmp_seq=83 ttl=64 time=0.181 ms
64 bytes from 10.0.2.4: icmp_seq=84 ttl=64 time=0.293 ms
64 bytes from 10.0.2.4: icmp_seq=85 ttl=64 time=0.160 ms
64 bytes from 10.0.2.4: icmp_seq=86 ttl=64 time=0.172 ms
```

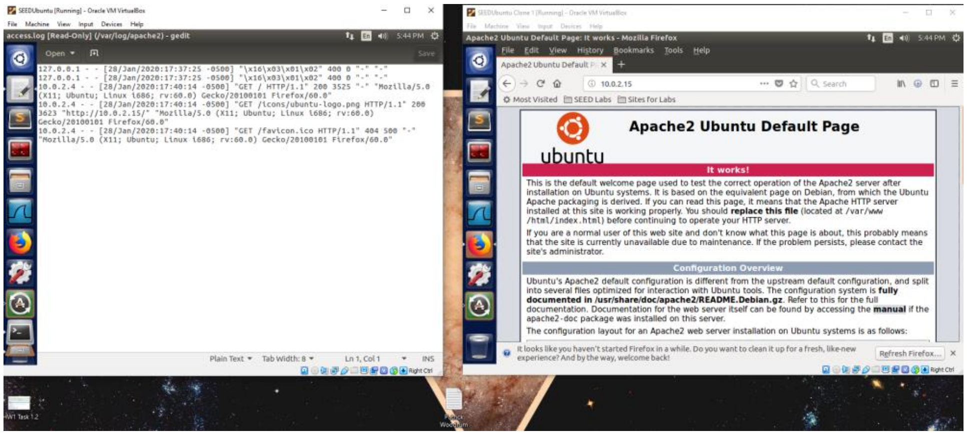
```
[01/28/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:84:d0:71
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::f3ca:3b82:e2d7:8728/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1773 (1.7 KB)  TX bytes:7419 (7.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21451 (21.4 KB)  TX bytes:21451 (21.4 KB)

[01/28/20]seed@VM:~$ 
```

2.2 - Apache Web Server

1. My Apache web server is listening on port 80. This was found in the ports.conf file in the installation directory for Apache2.
2. Upon entering https://localhost:80, the browser presented me with a “Secure Connection Failed” error message stating that “the page cannot be shown because the authenticity of the received data could not be verified.” Based on this result, it appears that the default server configuration does not support HTTPS protocol.
3. After finding the ip address of VM A to be 10.0.2.15, I successfully accessed the server on VM B. Following this, I navigated to /var/log/apache2/access.log and opened the access log to see that VM B did in fact make a connection using the ip address 10.0.2.4.


SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
access.log [Read-Only] (/var/log/apache2) - gedit
5:44 PM
Open
Save
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
Right Ctrl
HW1 Task 1.2
SEEDUbuntu Clone 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apache2 Ubuntu Default Page: It works - Mozilla Firefox
5:44 PM
File Edit View History Bookmarks Tools Help
Apache2 Ubuntu Default P
10.0.2.15
Search
Most Visited
SEED Labs
Sites for Labs
Refresh Firefox...
Right Ctrl

```
127.0.0.1 - - [28/Jan/2020:17:37:25 -0500] "\x16\x03\x01\x02" 400 0 "-" "-"
127.0.0.1 - - [28/Jan/2020:17:37:25 -0500] "\x16\x03\x01\x02" 400 0 "-" "-"
10.0.2.4 - - [28/Jan/2020:17:40:14 -0500] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0
(X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
10.0.2.4 - - [28/Jan/2020:17:40:14 -0500] "GET /icons/ubuntu-logo.png HTTP/1.1" 200
3623 "http://10.0.2.15/" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0)
Gecko/20100101 Firefox/60.0"
10.0.2.4 - - [28/Jan/2020:17:40:14 -0500] "GET /favicon.ico HTTP/1.1" 404 500 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
```

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!