JW4158-Info8590-22S-Portfolio-1

John White

6714158

INFO8590

Table of Contents

Lab 1- Introduction To Packet Tracer

Description

The purpose of this lab was to serve as an introduction to Packet Tracer. We did this by enrolling in Cisco's Packet Tracer course and following the instructions in Chapter 2 to build a simple network in Packet Tracer in which multiple end users can contact a remote server via the internet. This configuration can be viewed in Figure 1-1.

Preparation

Visit https://www.netacad.com/courses/packet-tracer and enroll in the Packet Tracer course. Download Packet Tracer and install it. Go to Chapter 2 and download the exercise titled "Create a Simple Network". The file will be called 2.1.1-packet-tracer-create-a-simple-network.pka. Copy the configuration for the wireless router, Cloud-PT, and Server-PT that is already in the .pka file and follow the instructions in the file as well. Once this is done, the network should be built and both the PC and the Desktop should be able to contact the Server-PT.

Observations

During this lab, the largest problem that I ran into was related to Cisco's Skills for All website[1] which is required to access the Packet Tracer course as well as the Packet Tracer download. The website would function normally until I logged in, after which the page would load indefinitely. I tried to clear my cache, use another browser, use another computer, and use another account but the solution that worked for me was to go to someone else's house and use their internet. The router at my house may have an unusual configuration that is not recognized by some of Cisco's servers, but the true cause is unclear to me at this time.

Other than that, the configurations and instructions provided should be sufficient given that they are followed correctly. I personally found it helpful to go into Options > Preferences and under the Interface tab, enable "Show Device Model Labels" and "Always Show Port Labels in Logical Workspace". An experienced user of Packet Tracer may want to keep these disabled to reduce clutter on the screen. As a new user, I find these labels helpful to keep track of things.

Screenshots

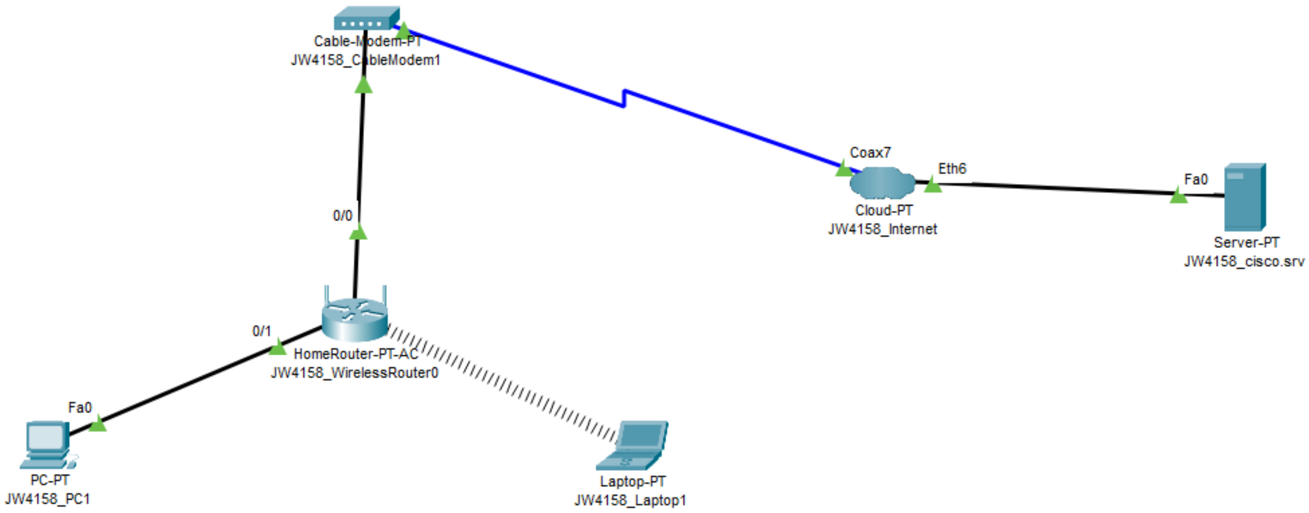


Figure 1-1 - Configuration diagram of the completed network.

Reflection

After completing the brief introduction to Packet Tracer, it is fair to say that this software is very useful and easy to understand for beginners, especially considering the fact that it is free. Packet Tracer allows the user to simulate a network environment by adding virtual network devices to a diagram and connecting them using cables. These virtual devices function like real computers and the user can also customize the hardware of these machines and configure their software. This allows for the fast and cheap creation of network simulations or network diagrams, as well as the sharing of these configurations in a single file, making Packet Tracer extremely useful for educational or design purposes. Packet Tracer could also be used to rapidly test changes made to a network in order to find out if the configuration is valid or not. When a connection between devices is being made, Packet Tracer shows the traffic as it is occurring and can even be paused or be made to travel at different speeds. This offers a level of flexibility that is very useful for a beginner and is not possible using real network setups.

The physical mode is very useful in Packet Tracer as well. For each network device, the user can view the device in Physical mode which shows the ethernet ports, network cards, cabling, etc. of the device. Physically experimenting with this networking hardware in real life would be extremely time-consuming and also incredibly expensive. This allows people to experiment with physical hardware for free which is great. It also allows the users to get familiar with the technical names of all of the different network devices and hardware.

Lab 2- Inspecting TCP/IP Traffic

Description

The purpose of this lab was to give us a brief introduction to the use of Wireshark and to get us to understand what kind of information can be gathered with it. We did this by connecting to the Apache Foundation website[2] while using Wireshark to monitor the traffic on our network.

Preparation

Go to https://wireshark.org/download.html. Download and install Wireshark. Ensure that your current web browser is configured so that it does not automatically correct HTTP addresses to HTTPS or we will not be able to view the information we desire in Wireshark. This can be done by using Microsoft Edge. Using Microsoft Edge, navigate to edge://flags. Search for the flag "Automatic HTTPS" and disable it. We are now ready to begin the lab.

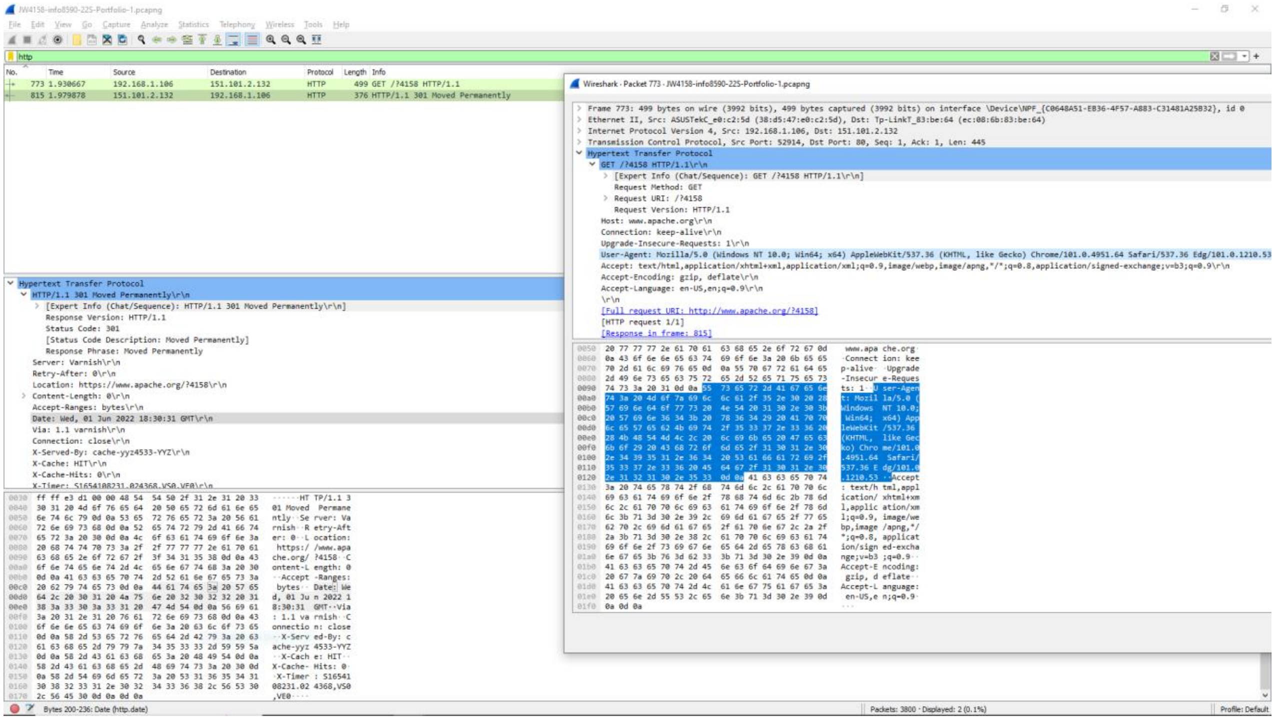
Observations

To conduct the lab, begin capturing traffic on your network using Wireshark. Using your web browser, navigate to http://apache.org/?4158. Once the website finishes loading, stop the Wireshark capture. We can now go through the data. To view the 2 packets we captured, filter the packets by http using the bar at the top in Wireshark. The first packet is the one that we sent to apache.org and the 2nd packet is the data that was sent back to us.

If the HTTP packets can not be found and you are sure that Wireshark is capturing on the right network, a likely problem is that we are visiting the website via HTTPS instead of HTTP. Wireshark automatically filters out HTTPS traffic by default and even if we could view it, it would be encrypted so we could not view the data easily. Some browsers may not be able to disable this feature so keep this in mind when carrying out this lab.

After reviewing all of the packets filtered by DNS, I noticed some web traffic that had URLs that I did not recognize. After looking these up, I think they may be related to adware on my computer that I had not noticed. This is outside the scope of this lab but I thought it would be worthy to note here.

Screenshots

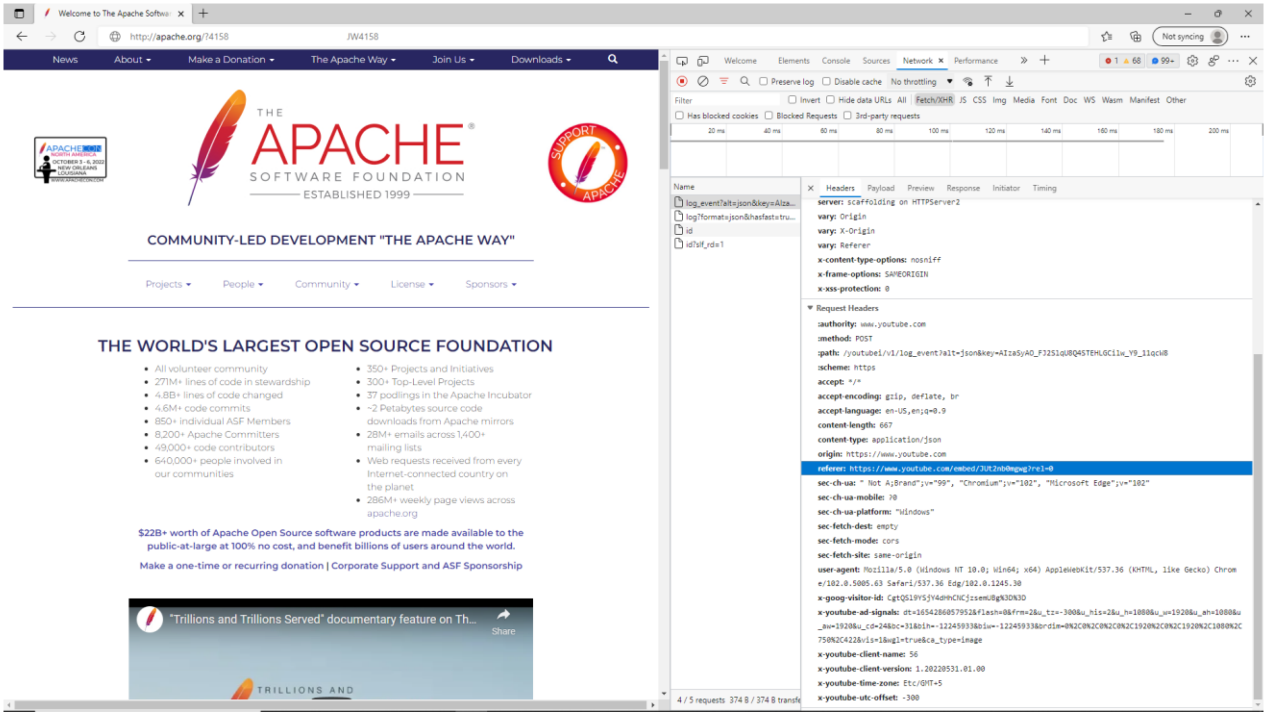

JW4158-info8590-22S-Portfolio-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 773 · JW4158-info8590-22S-Portfolio-1.pcapng
Bytes 200-236: Date (http.date)
Packets: 3800 · Displayed: 2 (0.1%)
Profile: Default

```
No.   Time        Source          Destination     Protocol  Length  Info
773   1.930667    192.168.1.106   151.101.2.132   HTTP      499     GET /?4158 HTTP/1.1
815   1.979878    151.101.2.132   192.168.1.106   HTTP      376     HTTP/1.1 301 Moved Permanently
```

```
Hypertext Transfer Protocol
  HTTP/1.1 301 Moved Permanently\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
    Response Version: HTTP/1.1
    Status Code: 301
    [Status Code Description: Moved Permanently]
    Response Phrase: Moved Permanently
  Server: Varnish\r\n
  Retry-After: 0\r\n
  Location: https://www.apache.org/?4158\r\n
  Content-Length: 0\r\n
  Accept-Ranges: bytes\r\n
  Date: Wed, 01 Jun 2022 18:30:31 GMT\r\n
  Via: 1.1 varnish\r\n
  Connection: close\r\n
  X-Served-By: cache-yyz4533-YYZ\r\n
  X-Cache: HIT\r\n
  X-Cache-Hits: 0\r\n
  X-Timer: S1654108231.024368,VS0,VE0\r\n
```

```
Frame 773: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits) on interface \Device\NPF_{C0648A51-EB36-4F57-A883-C31481A25B32}, id 0
Ethernet II, Src: ASUSTekC_e0:c2:5d (38:d5:47:e0:c2:5d), Dst: Tp-LinkT_83:be:64 (ec:08:6b:83:be:64)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 151.101.2.132
Transmission Control Protocol, Src Port: 52914, Dst Port: 80, Seq: 1, Ack: 1, Len: 445
Hypertext Transfer Protocol
  GET /?4158 HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /?4158 HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /?4158
    Request Version: HTTP/1.1
  Host: www.apache.org\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/101.0.4951.64 Safari/537.36 Edg/101.0.1210.53
  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.apache.org/?4158]
  [HTTP request 1/1]
  [Response in frame: 815]
```

Figure 2-1 – Date and time as reported by the webserver (highlighted in grey on the left) and the User Agent as reported by the webserver (highlighted in blue on the right).


Welcome to The Apache Softwa
http://apache.org/?4158
JW4158
News
About
Make a Donation
The Apache Way
Join Us
Downloads
APACHECON NORTH AMERICA OCTOBER 3 - 6, 2022 NEW ORLEANS LOUISIANA
THE APACHE SOFTWARE FOUNDATION ESTABLISHED 1999
SUPPORT APACHE
Projects
People
Community
License
Sponsors
"Trillions and Trillions Served" documentary feature on Th...
Share
TRILLIONS AND
Welcome Elements Console Sources Network Performance
Preserve log Disable cache No throttling
Filter Invert Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other
Has blocked cookies Blocked Requests 3rd-party requests
Name
log_event?alt=json&key=AIza...
log?format=json&hasfast=tru...
id
id?slf_rd=1
4 / 5 requests 374 B / 374 B transfe
Headers Payload Preview Response Initiator Timing

COMMUNITY-LED DEVELOPMENT "THE APACHE WAY"

THE WORLD'S LARGEST OPEN SOURCE FOUNDATION

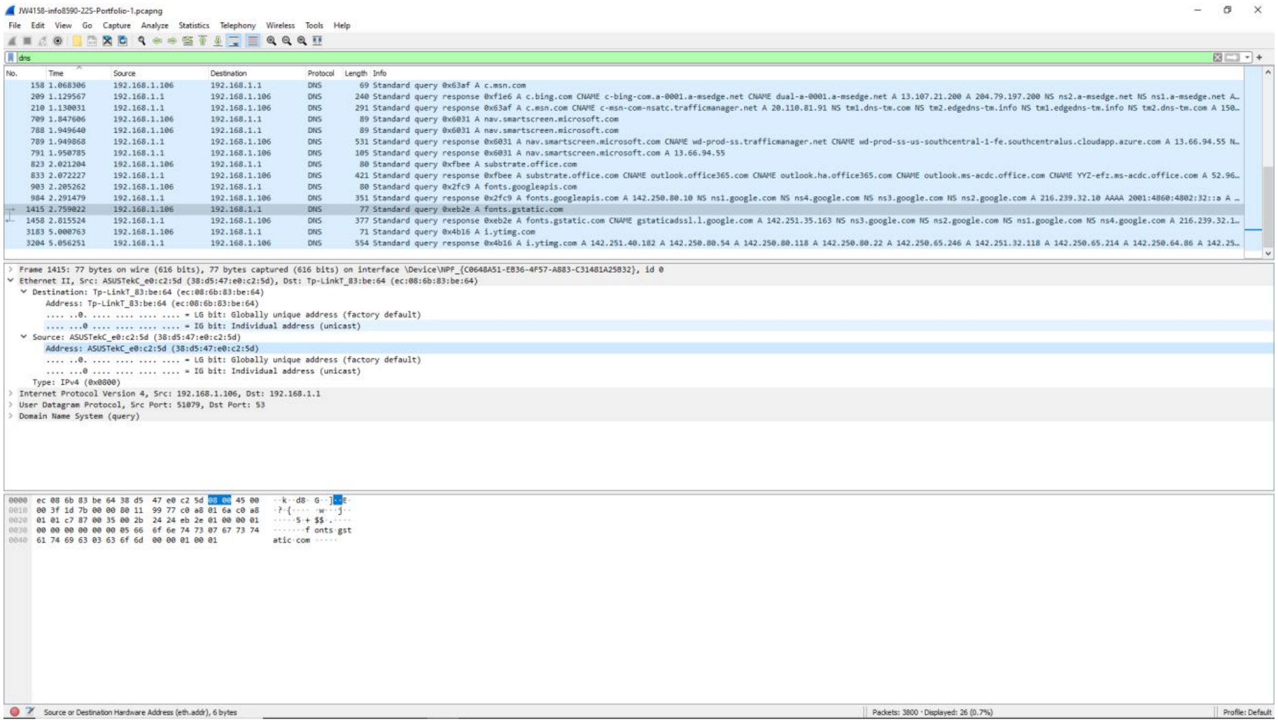
- All volunteer community
- 271M+ lines of code in stewardship
- 4.8B+ lines of code changed
- 4.6M+ code commits
- 850+ individual ASF Members
- 8,200+ Apache Committers
- 49,000+ code contributors
- 640,000+ people involved in our communities
- 350+ Projects and Initiatives
- 300+ Top-Level Projects
- 37 podlings in the Apache Incubator
- ~2 Petabytes source code downloads from Apache mirrors
- 28M+ emails across 1,400+ mailing lists
- Web requests received from every Internet-connected country on the planet
- 286M+ weekly page views across apache.org

$22B+ worth of Apache Open Source software products are made available to the public-at-large at 100% no cost, and benefit billions of users around the world.

Make a one-time or recurring donation | Corporate Support and ASF Sponsorship

```
server: scaffolding on HTTPServer2
vary: Origin
vary: X-Origin
vary: Referer
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 0
Request Headers
:authority: www.youtube.com
:method: POST
:path: /youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8
:scheme: https
accept: */*
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
content-length: 667
content-type: application/json
origin: https://www.youtube.com
referer: https://www.youtube.com/embed/JUt2nb0mgwg?rel=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="102", "Microsoft Edge";v="102"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-dest: empty
sec-fetch-mode: cors
sec-fetch-site: same-origin
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36 Edg/102.0.1245.30
x-goog-visitor-id: CgtQSl9YSjY4dHhCNCjzsemUBg%3D%3D
x-youtube-ad-signals: dt=1654286057952&flash=0&frm=2&u_tz=-300&u_his=2&u_h=1080&u_w=1920&u_ah=1080&u_aw=1920&u_cd=24&bc=31&bih=-12245933&biw=-12245933&brdim=0%2C0%2C0%2C0%2C1920%2C0%2C1920%2C1080%2C750%2C422&vis=1&wgl=true&ca_type=image
x-youtube-client-name: 56
x-youtube-client-version: 1.20220531.01.00
x-youtube-time-zone: Etc/GMT+5
x-youtube-utc-offset: -300
```

Figure 2-2 – The website Referer can be found via our web browser, but this information cannot be found on wire shark.



JW4158-info8590-22S-Portfolio-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.     Time        Source          Destination     Protocol Length Info
    158 1.068306    192.168.1.106   192.168.1.1     DNS       69 Standard query 0x63af A c.msn.com
    209 1.129567    192.168.1.1     192.168.1.106   DNS      240 Standard query response 0xf1e6 A c.bing.com CNAME c-bing-com.a-0001.a-msedge.net CNAME dual-a-0001.a-msedge.net A 13.107.21.200 A 204.79.197.200 NS ns2.a-msedge.net NS ns1.a-msedge.net A…
    210 1.130031    192.168.1.1     192.168.1.106   DNS      291 Standard query response 0x63af A c.msn.com CNAME c-msn-com-nsatc.trafficmanager.net A 20.110.81.91 NS tm1.dns-tm.com NS tm2.edgedns-tm.info NS tm1.edgedns-tm.info NS tm2.dns-tm.com A 150…
    709 1.847606    192.168.1.106   192.168.1.1     DNS       89 Standard query 0x6031 A nav.smartscreen.microsoft.com
    788 1.949640    192.168.1.106   192.168.1.1     DNS       89 Standard query 0x6031 A nav.smartscreen.microsoft.com
    789 1.949868    192.168.1.1     192.168.1.106   DNS      531 Standard query response 0x6031 A nav.smartscreen.microsoft.com CNAME wd-prod-ss.trafficmanager.net CNAME wd-prod-ss-us-southcentral-1-fe.southcentralus.cloudapp.azure.com A 13.66.94.55 N…
    791 1.950785    192.168.1.1     192.168.1.106   DNS      105 Standard query response 0x6031 A nav.smartscreen.microsoft.com A 13.66.94.55
    823 2.021204    192.168.1.106   192.168.1.1     DNS       80 Standard query 0xfbee A substrate.office.com
    833 2.072227    192.168.1.1     192.168.1.106   DNS      421 Standard query response 0xfbee A substrate.office.com CNAME outlook.office365.com CNAME outlook.ha.office365.com CNAME outlook.ms-acdc.office.com CNAME YYZ-efz.ms-acdc.office.com A 52.96…
    903 2.205262    192.168.1.106   192.168.1.1     DNS       80 Standard query 0x2fc9 A fonts.googleapis.com
    984 2.291479    192.168.1.1     192.168.1.106   DNS      351 Standard query response 0x2fc9 A fonts.googleapis.com A 142.250.80.10 NS ns1.google.com NS ns4.google.com NS ns3.google.com NS ns2.google.com A 216.239.32.10 AAAA 2001:4860:4802:32::a A …
   1415 2.759022    192.168.1.106   192.168.1.1     DNS       77 Standard query 0xeb2e A fonts.gstatic.com
   1458 2.815524    192.168.1.1     192.168.1.106   DNS      377 Standard query response 0xeb2e A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 142.251.35.163 NS ns3.google.com NS ns2.google.com NS ns1.google.com NS ns4.google.com A 216.239.32.1…
   3183 5.000763    192.168.1.106   192.168.1.1     DNS       71 Standard query 0x4b16 A i.ytimg.com
   3204 5.056251    192.168.1.1     192.168.1.106   DNS      554 Standard query response 0x4b16 A i.ytimg.com A 142.251.40.182 A 142.250.80.54 A 142.250.80.118 A 142.250.80.22 A 142.250.65.246 A 142.251.32.118 A 142.250.65.214 A 142.250.64.86 A 142.25…
```

```
> Frame 1415: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{C0648A51-EB36-4F57-A883-C31481A25B32}, id 0
v Ethernet II, Src: ASUSTekC_e0:c2:5d (38:d5:47:e0:c2:5d), Dst: Tp-LinkT_83:be:64 (ec:08:6b:83:be:64)
  v Destination: Tp-LinkT_83:be:64 (ec:08:6b:83:be:64)
      Address: Tp-LinkT_83:be:64 (ec:08:6b:83:be:64)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: ASUSTekC_e0:c2:5d (38:d5:47:e0:c2:5d)
      Address: ASUSTekC_e0:c2:5d (38:d5:47:e0:c2:5d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 51079, Dst Port: 53
> Domain Name System (query)
```

```
0000  ec 08 6b 83 be 64 38 d5  47 e0 c2 5d 08 00 45 00   ··k··d8· G··]··E·
0010  00 3f 1d 7b 00 00 80 11  99 77 c0 a8 01 6a c0 a8   ·?·{···· ·w···j··
0020  01 01 c7 87 00 35 00 2b  24 24 eb 2e 01 00 00 01   ·····5·+ $$·.····
0030  00 00 00 00 00 00 05 66  6f 6e 74 73 07 67 73 74   ·······f onts·gst
0040  61 74 69 63 03 63 6f 6d  00 00 01 00 01            atic·com ·····
```

Source or Destination Hardware Address (eth.addr), 6 bytes | Packets: 3800 · Displayed: 26 (0.7%) | Profile: Default

Figure 2-3 – The IP address and MAC address of the user’s network card can be easily viewed by someone monitoring the network using Wireshark if they filter for DNS traffic.

<u>Reflection</u>

If we review the data that we gathered from those 2 packets, we can come to a number of interesting conclusions. In Figure 2-1, we can see that the first packet we captured (the outgoing packet) contains the User-Agent data. This can be used to determine the web browser that was being used (in our case, Microsoft Edge, visible at the end of the string) as well as the operating system we used (Windows x64). To find the date and time as reported by the webserver, we must view the data that was sent back to our computer from Apache.org. This is the 2nd packet and in our case we can see that the server reports it was contacted at 18:30:31 GMT on June 1, 2022. It is not possible for us to view the Referer using Wireshark because that information was not sent on our network. There is a Referer visible via our web browser as shown in Figure 2-2 because there was a referral made between YouTube and Apache but our network was not involved.

If one was to visit a coffee shop and connect to the free Wi-Fi there, another user on the network could view important information about your device if they captured DNS traffic from your device using Wireshark. DNS means Domain Name Service and consists of multiple servers that officiate which devices and networks are assigned which IP addresses. This is required for internet access. Because all devices have many applications that require the internet, your device is constantly contacting DNS servers in order to acquire or renew it’s IP address. By looking at this traffic, we can easily see the source of the traffic to find the IP address of the user, or we can look at MAC address of the user’s network card. This can be seen in Figure 2-3.

This information could be used to attack the user's device directly rather than just for monitoring purposes, making this information dangerous to reveal. I believe the solution to this problem is to control the traffic that can come into your device with a firewall. Because the information needs to be accessible by DNS servers, there is no way for us to encrypt it so our best bet is to block the traffic from the malicious user. By configuring the firewall on our device so that it allows DNS traffic in and out while blocking by default the traffic that we don't explicitly allow through, we can allow our device to maintain it's DNS connection without putting our security at risk.

References

1. Cisco. (2022, Jun. 1). Skills for All website. – https://skillsforall.com
2. Apache Foundation. (2022, Jun. 1). Apache Foundation website - http://Apache.org