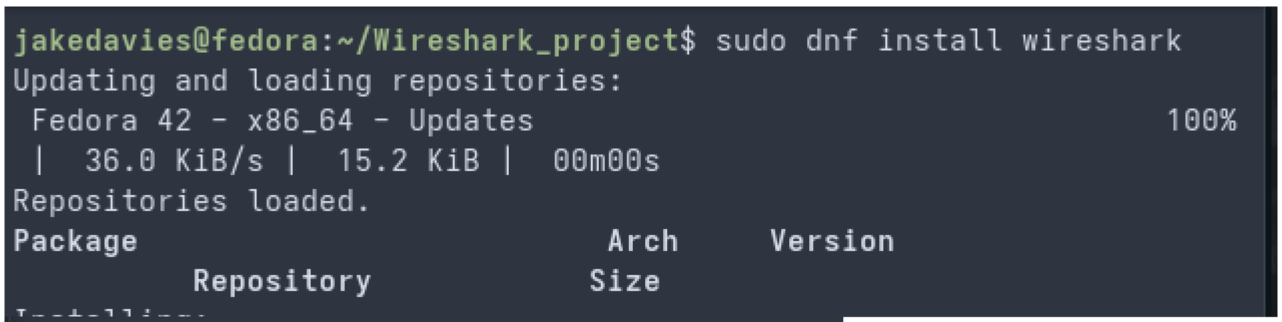
SOC Intrusion Detection - Wireshark

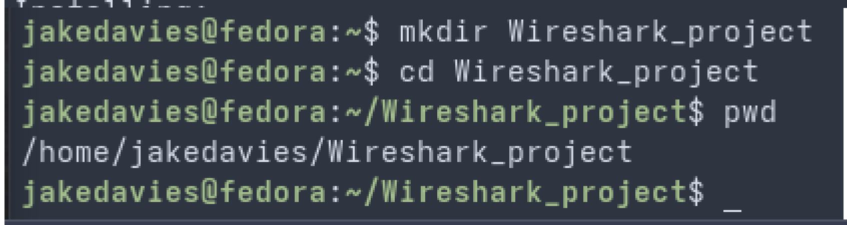
In this Project i am to show that i can use WireShark to monitor my laptops Traffic on a basic level.

Step 1: Setup

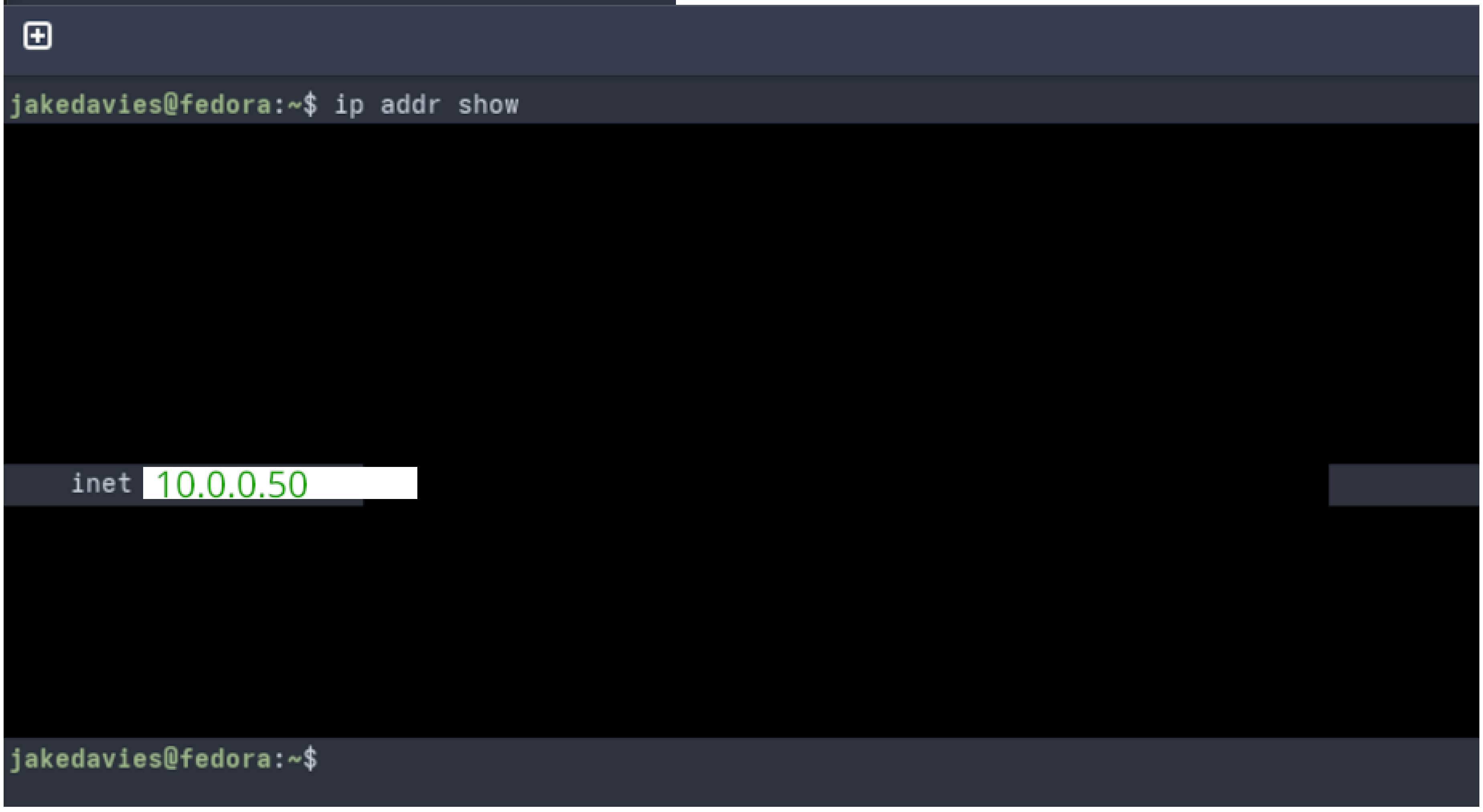
Created folder with `mkdir ~/Wireshark_project` . Installed Wireshark. Confirmed laptop's private IP through Bash. For This project i will be radacting my IP for security reasons.



```
jakedavies@fedora:~/Wireshark_project$ sudo dnf install wireshark
Updating and loading repositories:
 Fedora 42 - x86_64 - Updates                                 100%
 |  36.0 KiB/s |  15.2 KiB |  00m00s
Repositories loaded.
Package                          Arch     Version
          Repository             Size
Installing:
```



```
jakedavies@fedora:~$ mkdir Wireshark_project
jakedavies@fedora:~$ cd Wireshark_project
jakedavies@fedora:~/Wireshark_project$ pwd
/home/jakedavies/Wireshark_project
jakedavies@fedora:~/Wireshark_project$ _
```

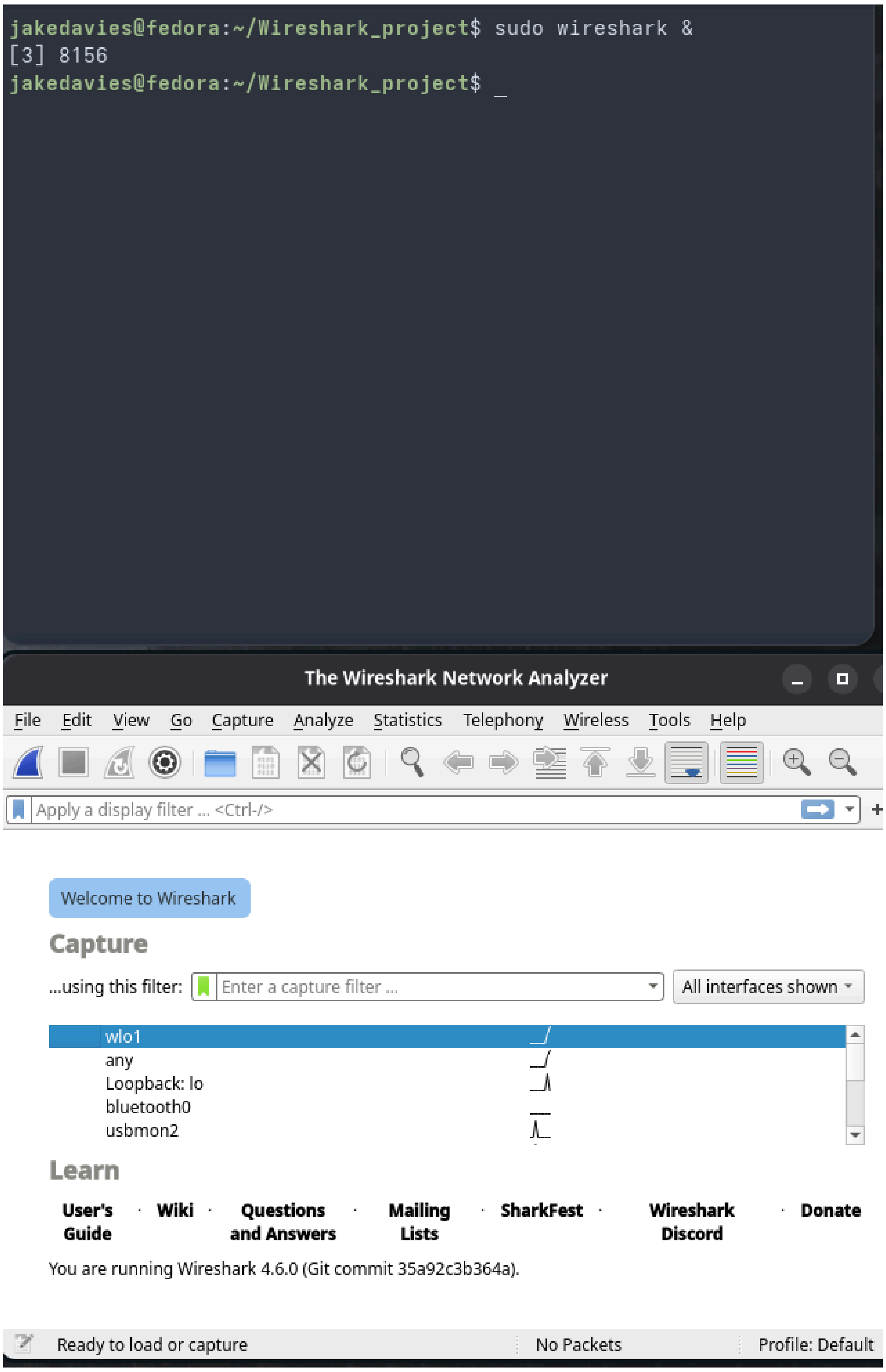


```
jakedavies@fedora:~$ ip addr show
[redacted]
    inet 10.0.0.50
[redacted]
jakedavies@fedora:~$
```

I Ran **ip addr show** and under the **wlol** section i saw my laptops IP (For this i will place a fake IP of **10.0.0.50**).

Step 2: Capture Traffic

Started Wireshark with `sudo wireshark &` . Selected `wlo1` , applied filter `ip.addr == 10.0.0.50 && http for laptop traffic filter to HTTP unsecure websites.

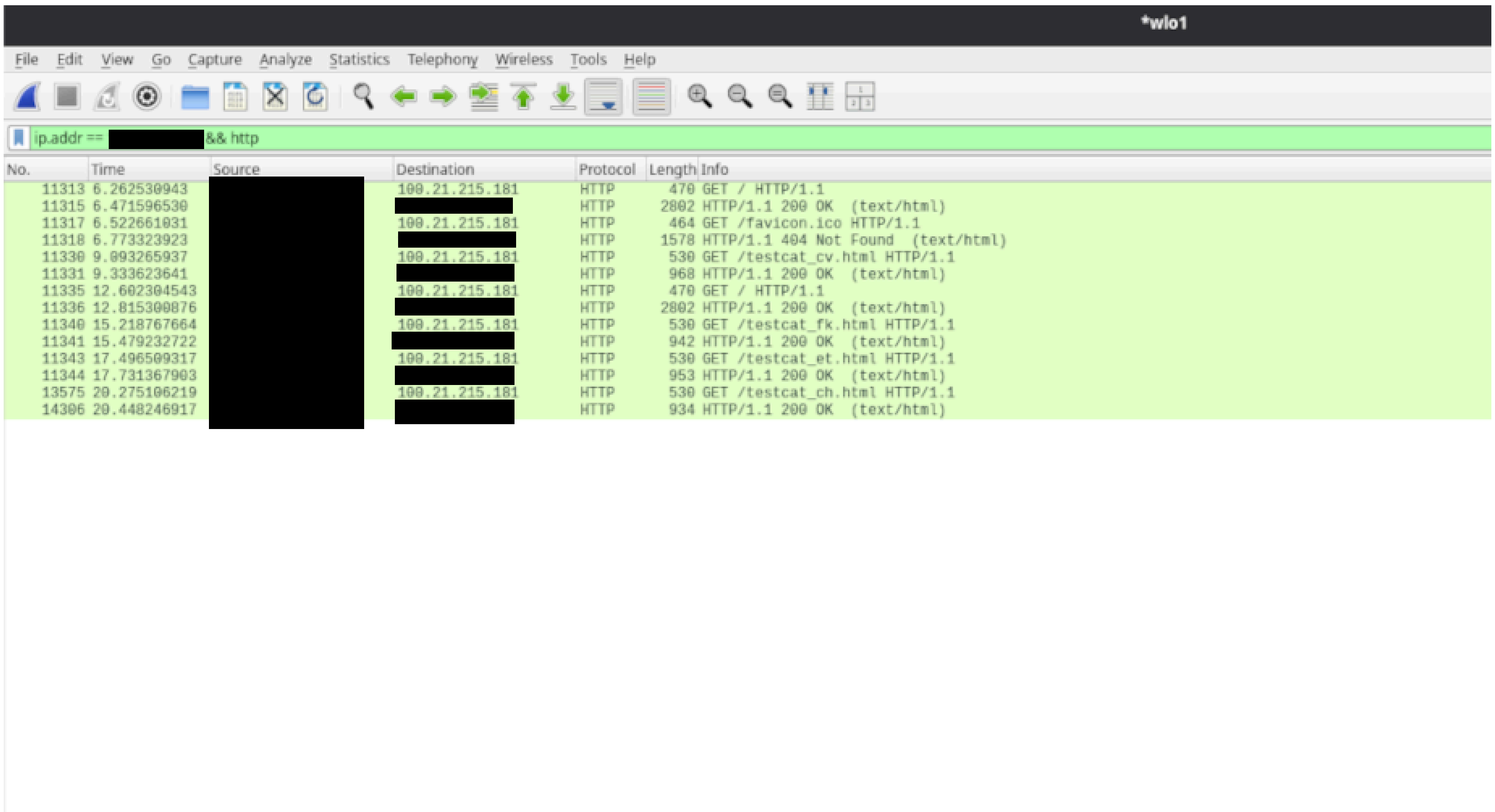


```
jakedavies@fedora:~/Wireshark_project$ sudo wireshark &
[3] 8156
jakedavies@fedora:~/Wireshark_project$ _
```

wlo1
any
Loopback: lo
bluetooth0
usbmon2

You are running Wireshark 4.6.0 (Git commit 35a92c3b364a).

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


*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == [redacted] && http

No.	Time	Source	Destination	Protocol	Length	Info
11313	6.262530943	[redacted]	100.21.215.181	HTTP	470	GET / HTTP/1.1
11315	6.471596530	[redacted]	[redacted]	HTTP	2802	HTTP/1.1 200 OK (text/html)
11317	6.522661031	[redacted]	100.21.215.181	HTTP	464	GET /favicon.ico HTTP/1.1
11318	6.773323923	[redacted]	[redacted]	HTTP	1578	HTTP/1.1 404 Not Found (text/html)
11330	9.093265937	[redacted]	100.21.215.181	HTTP	530	GET /testcat_cv.html HTTP/1.1
11331	9.333623641	[redacted]	[redacted]	HTTP	968	HTTP/1.1 200 OK (text/html)
11335	12.602304543	[redacted]	100.21.215.181	HTTP	470	GET / HTTP/1.1
11336	12.815300876	[redacted]	[redacted]	HTTP	2802	HTTP/1.1 200 OK (text/html)
11340	15.218767664	[redacted]	100.21.215.181	HTTP	530	GET /testcat_fk.html HTTP/1.1
11341	15.479232722	[redacted]	[redacted]	HTTP	942	HTTP/1.1 200 OK (text/html)
11343	17.496509317	[redacted]	100.21.215.181	HTTP	530	GET /testcat_et.html HTTP/1.1
11344	17.731367903	[redacted]	[redacted]	HTTP	953	HTTP/1.1 200 OK (text/html)
13575	20.275106219	[redacted]	100.21.215.181	HTTP	530	GET /testcat_ch.html HTTP/1.1
14306	20.448246917	[redacted]	[redacted]	HTTP	934	HTTP/1.1 200 OK (text/html)

So on this step i initially ran wire shark from the terminal with the command sudo wireshark &

I found out that the Sudo command allows you to run commands as the root. To allow this it authorizes you with a hidden password.

The & in the command Runs wireshark in the background.

When in the wireshark GUI i saw different interface options. For learning i just focused on wlol.
This is because my IP was under the wlol section on Bash

In the filter bar at the top i type in ip.addr == [Redacted] && HTTP. I did this for two reasons.

1. To filter out any unwanted noise &
2. To Refine my search directly for unsecured HTTP packets.

As i can see there are 3 collumns i am paying attention to.

1. Destination, this shows the destinations IP in which my Laptop is accessing.
2. Protocol, This confirms that the website i have visited is indeed a unsecured HTTP website. For this example i used: http://www.testingmcafeesites.com/testcat_cv.html
3. Info, this shows the packets : `GET /testcat_cv.html` , & `200 OK (text/html)`

GET /testcat_cv.html means that my browser asked for this page &

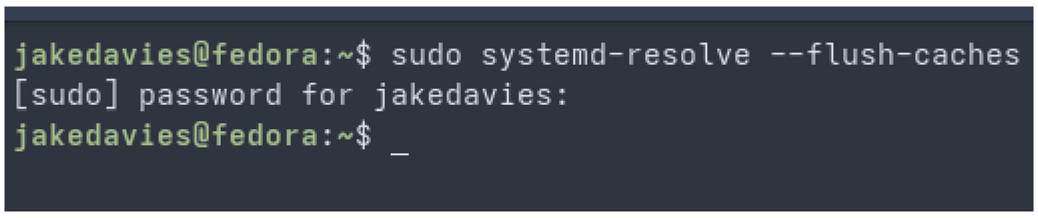
200 OK (text/html) means the server responded and provided the page.

Skills I Learned:

- Use terminal to check network
- Start Wireshark safely
- Capture real internet traffic
- Filter packets on a basic level
- Hide private info (OPSEC)

Step 3 - DNS, How names become IP's

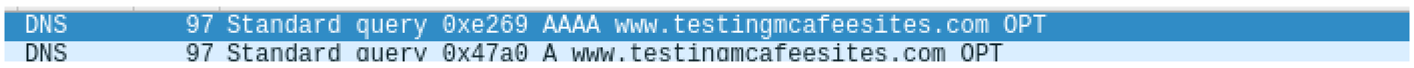
First step was to clear my DNS cache with i new command i learnt:
[sudo systemd-resolve --flush-cache]



```
jakedavies@fedora:~$ sudo systemd-resolve --flush-caches
[sudo] password for jakedavies:
jakedavies@fedora:~$ _
```

Next i filtered my IP again with this time a DNS line:

ip.addr == 10.0.0.50 && dns



```
DNS        97 Standard query 0xe269 AAAA www.testingmcafeesites.com OPT
DNS        97 Standard query 0x47a0 A www.testingmcafeesites.com OPT
```

the results came back were:

18935 4.483135582 192.168.1.126 8.8.8.8 DNS 97 Standard query 0xe269 AAAA www.testingmcafeesites.com OPT

In short my laptop asked **Google DNS** (**8.8.8.8**): “What’s the **IP address** of www.testingmcafeesites.com