

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

Student:

Andre Hardy

Email:

ahardy754@email.porterchester.edu

Time on Task:

2 hours, 22 minutes

Progress:

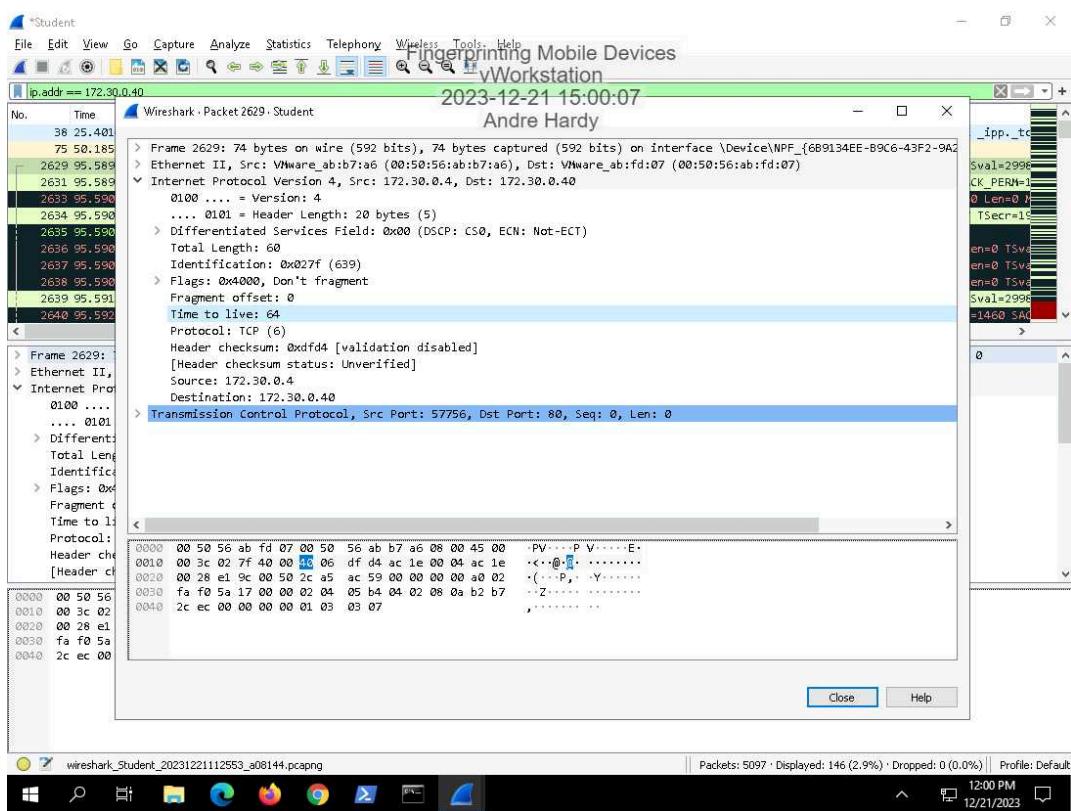
100%

Report Generated: Sunday, December 24, 2023 at 3:42 PM

Section 1: Hands-On Demonstration

Part 1: Perform Passive Fingerprinting with Wireshark

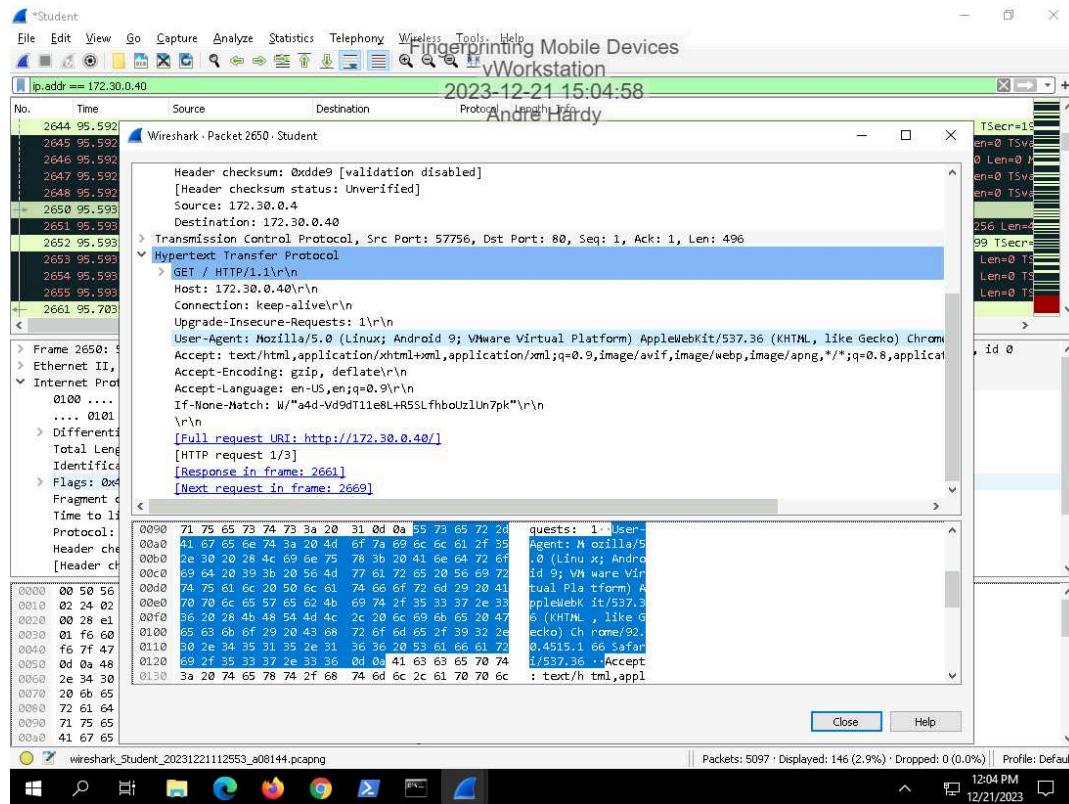
14. Make a screen capture showing the Time to live field.



Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

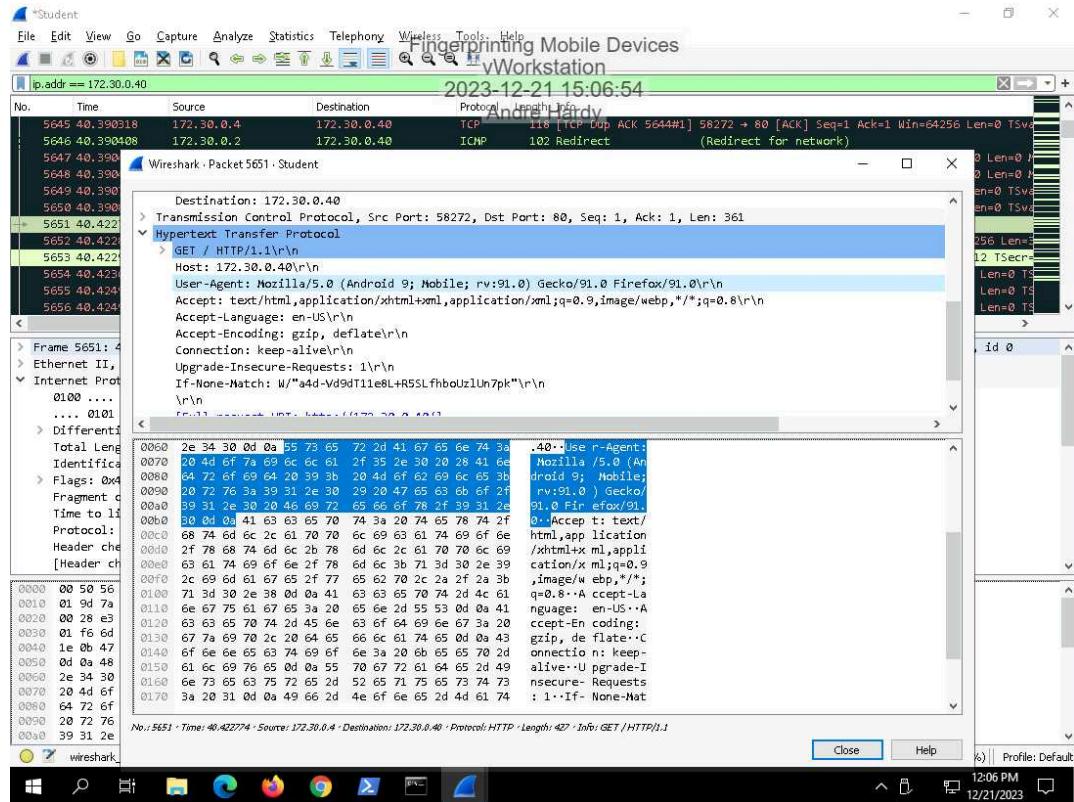
18. Make a screen capture showing the User-Agent string for the Chrome browser session.



Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

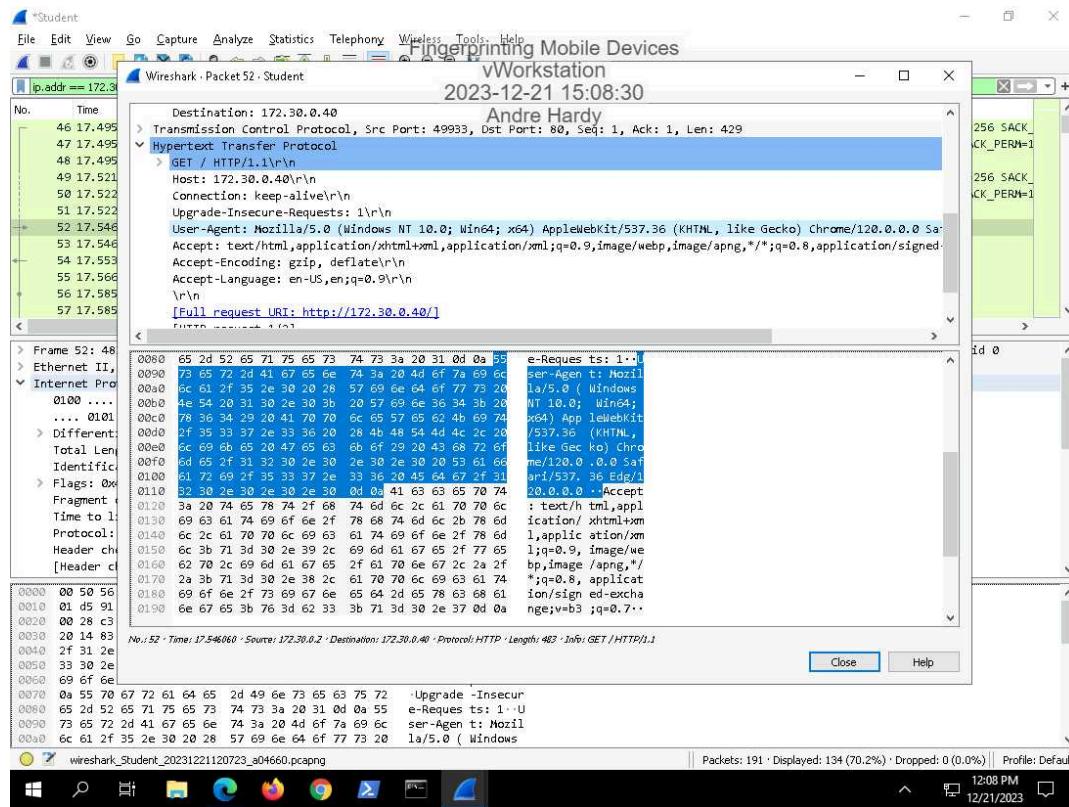
23. Make a screen capture showing the User-Agent string for the Firefox browser session.



Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

29. Make a screen capture showing the User-Agent string for the Edge browser session from the vWorkstation.



30. Compare the three User-Agent strings. How do they differ? How are they similar?

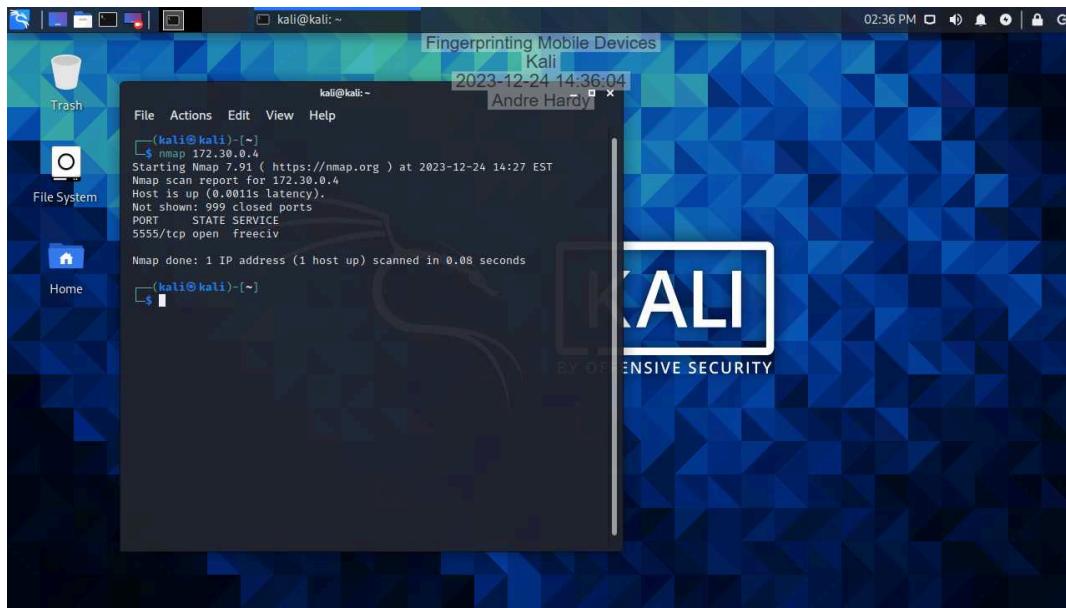
Each include the different operating system and web browser; however, they all follow the same format and convention.

Part 2: Perform Active Fingerprinting with Nmap

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

5. Make a screen capture showing the results of the default Nmap scan.

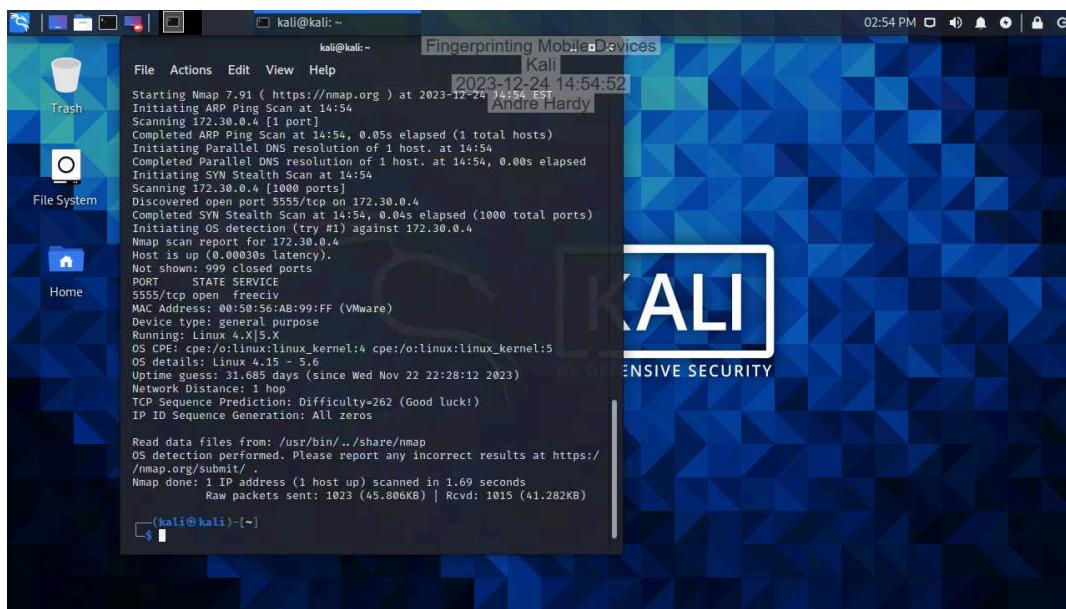


A screenshot of a Kali Linux desktop environment. In the center, a terminal window titled "Fingerprinting Mobile Devices" displays the output of a default Nmap scan. The terminal shows the command \$ nmap 172.30.0.4, the start time 2023-12-24 14:36:04, and the host information for 172.30.0.4. It lists one open port, 5555/tcp, which is identified as freeciv. The scan completed in 0.08 seconds. The desktop background features the Kali logo.

```
(kali㉿kali)-[~]
$ nmap 172.30.0.4
Starting Nmap 7.91 ( https://nmap.org ) at 2023-12-24 14:27 EST
Nmap scan report for 172.30.0.4
Host is up (0.001s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
5555/tcp  open  freeciv

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

7. Make a screen capture showing the results of the -O -v Nmap scan.



A screenshot of a Kali Linux desktop environment. In the center, a terminal window titled "Fingerprinting Mobile Devices" displays the output of a detailed Nmap scan using the -O and -v options. The terminal shows the command \$ nmap -O -v 172.30.0.4, the start time 2023-12-24 14:54:52, and the host information for 172.30.0.4. The output provides extensive details about the target host, including OS detection (Linux 4.15.0-kvm), MAC address (00:50:56:AB:99:FF), device type (general purpose), kernel version (4.15.0-kvm), uptime (31.685 days since Nov 22 2023), network distance (1 hop), TCP sequence prediction (Difficulty=262), and IP ID sequence generation (All zeros). The scan also includes a note about reading data files from /usr/bin/../share/nmap and reporting incorrect results at https://nmap.org/submit/. The scan completed in 1.69 seconds with 1023 raw packets sent and 1015 received. The desktop background features the Kali logo.

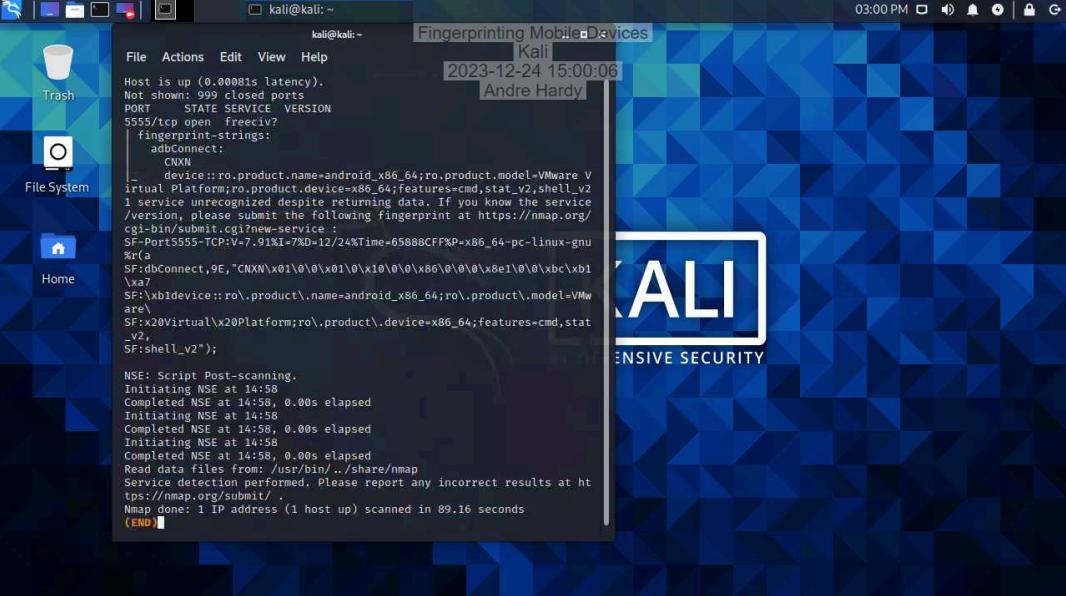
```
(kali㉿kali)-[~]
$ nmap -O -v 172.30.0.4
Starting Nmap 7.91 ( https://nmap.org ) at 2023-12-24 14:54:52 EST
Initiating ARP Ping Scan at 14:54
Scanning 172.30.0.4 [1 port]
Completed ARP Ping Scan at 14:54, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:54
Completed Parallel DNS resolution of 1 host. at 14:54, 0.00s elapsed
Initiating SYN Stealth Scan at 14:54
Scanning 172.30.0.4 [1000 ports]
Discovered open port 5555/tcp on 172.30.0.4
Completed SYN Stealth Scan at 14:54, 0.04s elapsed (1000 total ports)
Initiating OS detection (try #1) against 172.30.0.4
Nmap scan report for 172.30.0.4
Host is up (0.00030s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
5555/tcp  open  freeciv
MAC Address: 00:50:56:AB:99:FF (VMware)
Device type: general-purpose
Running: Linux 4.15.0-kvm
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 31.685 days (since Wed Nov 22 22:28:12 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.282KB)
```

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

11. Make a screen capture showing the product name in the Nmap output.



The screenshot shows a Kali Linux desktop environment with a terminal window titled "Fingerprinting Mobile Devices". The terminal displays the results of an Nmap scan. The output includes:

```
kali@kali: ~
[+] Fingerprinting Mobile Devices [Kali]
[+] 2023-12-24 15:00:06 [Andre Hardy]
Host is up (0.00081s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
5555/tcp   open  freeicc?
fingerprint-strings:
  |_  CNXN
    |_ device::ro.product.name=android_x86_64;ro.product.model=VMware V
      irtual Platform;ro.product.device=x86_64;features=cmd,stat_v2,shell_v2
      1 service unrecognized despite returning data. If you know the service
      /version, please submit the following fingerprint at https://nmap.org/
      cgi-bin/submit.cgi?new-service :
SF-Port5555-TCP:V=7.91%l=7%D=12/24%Tme=65888CFF%P=x86_64-pc-linux-gnu
%r(a
SF:doConnect,9E,"CNXN\x01\x00\x01\x00\x10\x00\x86\0\0\x8e\0\xbc\xb1
\xa7
SF:\xb1device::ro\.product\.name=android_x86_64;ro\.product\.model=VMw
are\
SF:x20Virtual\x20Platform;ro\.product\.device=x86_64;features=cmd,stat
_v2,
SF:shell_v2";
NSE: Script Post-scanning.
Initiating NSE at 14:58
Completed NSE at 14:58, 0.00s elapsed
Initiating NSE at 14:58
Completed NSE at 14:58, 0.00s elapsed
Initiating NSE at 14:58
Completed NSE at 14:58, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 89.16 seconds
(END)
```

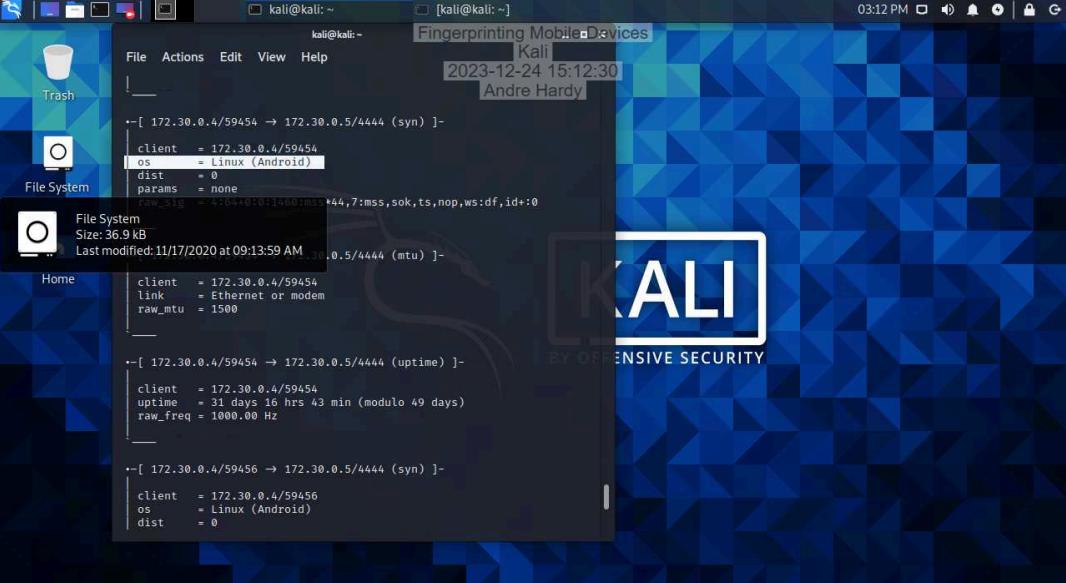
Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

Section 2: Applied Learning

Part 1: Perform Passive Fingerprinting with p0f

7. Make a screen capture showing the p0f result identifying 172.30.0.4 as Linux (Android).



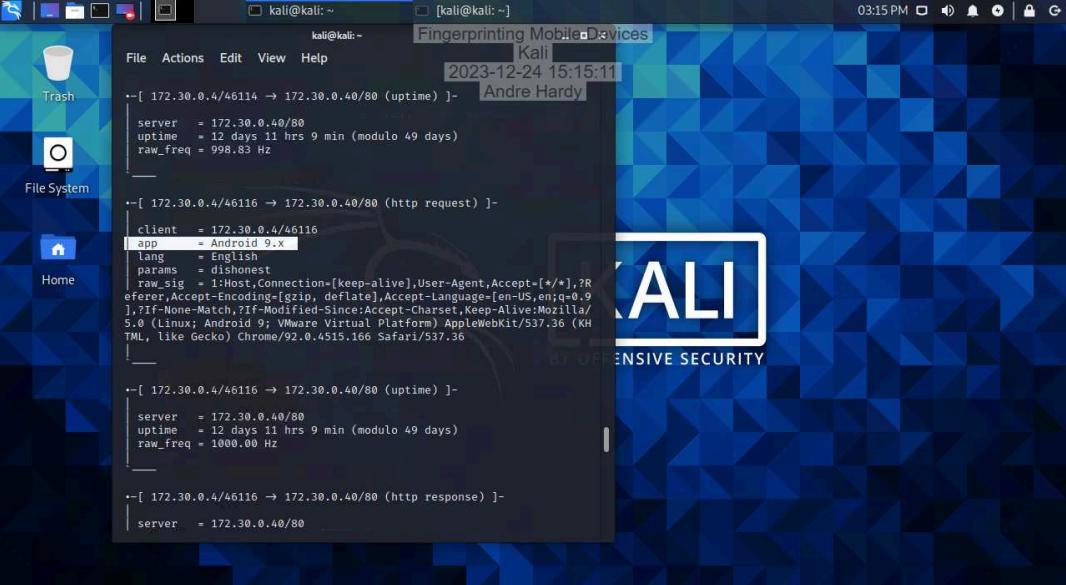
```
kali@kali: ~ [kali@kali: ~] Fingerprinting Mobile Devices Kali 2023-12-24 15:12:30 Andre Hardy
File Actions Edit View Help
--[ 172.30.0.4/59454 → 172.30.0.5/4444 (syn) ]-
client = 172.30.0.4/59454
os = Linux (Android)
dist = 0
params = none
raw_sig = 41:64+0:0:1460:ms>44,7:mss,sok,ts,nop,ws:df,id*:0

File System
Size: 36.9 kB
Last modified: 11/17/2020 at 09:13:59 AM
--[ 172.30.0.4/59454 → 172.30.0.5/4444 (mtu) ]-
client = 172.30.0.4/59454
link = Ethernet or modem
raw_mtu = 1500

--[ 172.30.0.4/59454 → 172.30.0.5/4444 (uptime) ]-
client = 172.30.0.4/59454
uptime = 31 days 16 hrs 43 min (modulo 49 days)
raw_freq = 1000.00 Hz

--[ 172.30.0.4/59456 → 172.30.0.5/4444 (syn) ]-
client = 172.30.0.4/59456
os = Linux (Android)
dist = 0
```

14. Make a screen capture showing the p0f result identifying 172.30.0.4 as Android 9.x.



```
kali@kali: ~ [kali@kali: ~] Fingerprinting Mobile Devices Kali 2023-12-24 15:15:11 Andre Hardy
File Actions Edit View Help
--[ 172.30.0.4/46114 → 172.30.0.40/80 (uptime) ]-
server = 172.30.0.40/80
uptime = 12 days 11 hrs 9 min (modulo 49 days)
raw_freq = 998.83 Hz

--[ 172.30.0.4/46116 → 172.30.0.40/80 (http request) ]-
client = 172.30.0.4/46116
app = Android 9.x
lang = English
params = dishonest
raw_sig = 1:Host,Connection=[keep-alive],User-Agent,Accept=[/*,*],?Referer,Accept-Encoding=[gzip, deflate],Accept-Language=[en-US,en;q=0.9],?If-None-Match,?If-Modified-Since:Accept-Charset,Keep-Alive:Mozilla/5.0 (Linux; Android 9; VMware Virtual Platform) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.166 Safari/537.36
|_

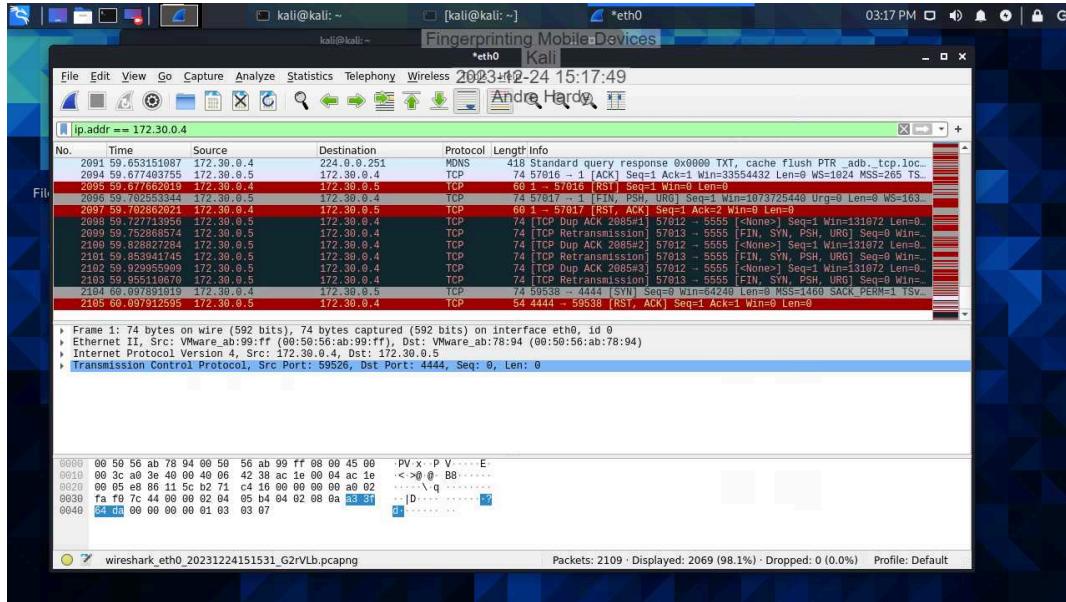
--[ 172.30.0.4/46116 → 172.30.0.40/80 (uptime) ]-
server = 172.30.0.40/80
uptime = 12 days 11 hrs 9 min (modulo 49 days)
raw_freq = 1000.00 Hz

--[ 172.30.0.4/46116 → 172.30.0.40/80 (http response) ]-
server = 172.30.0.40/80
```

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

19. Make a screen capture showing the traffic generated by Nmap in Wireshark.



24. Compare the Wireshark results from the p0f scan to the Nmap scan.

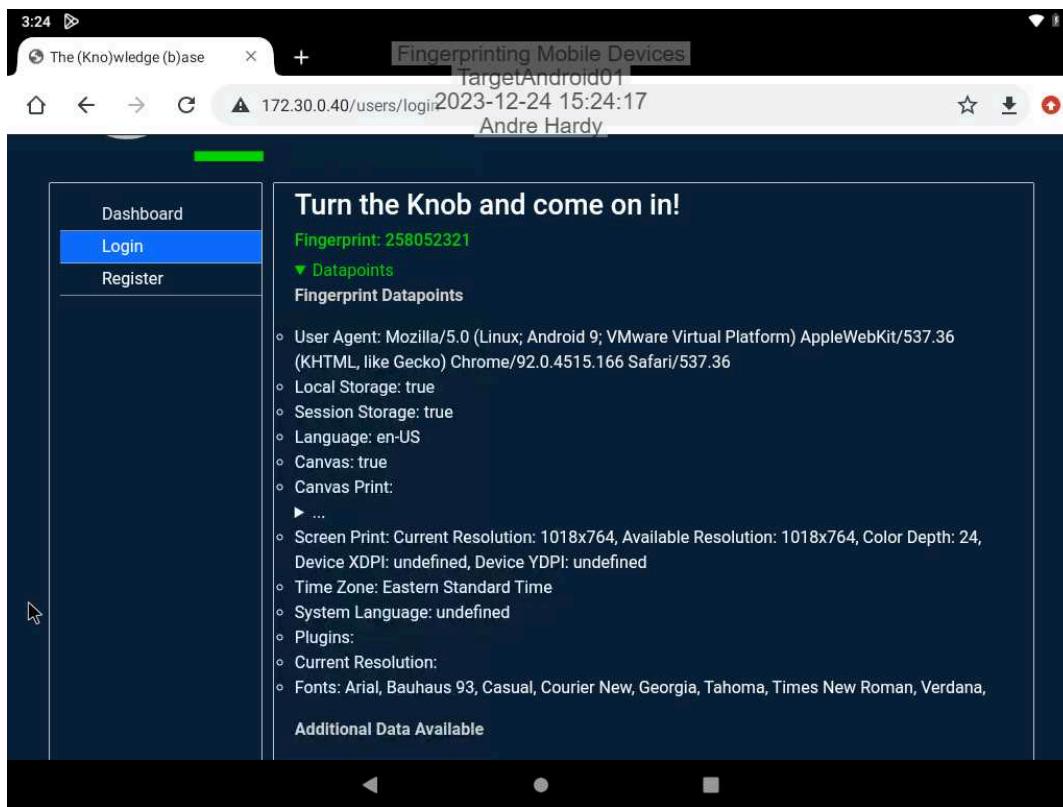
The results from the p0f scan only produced around 250 lines of traffic compared to the 2,000 lines produced by Nmap.

Part 2: Perform Active Fingerprinting with ClientJS

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

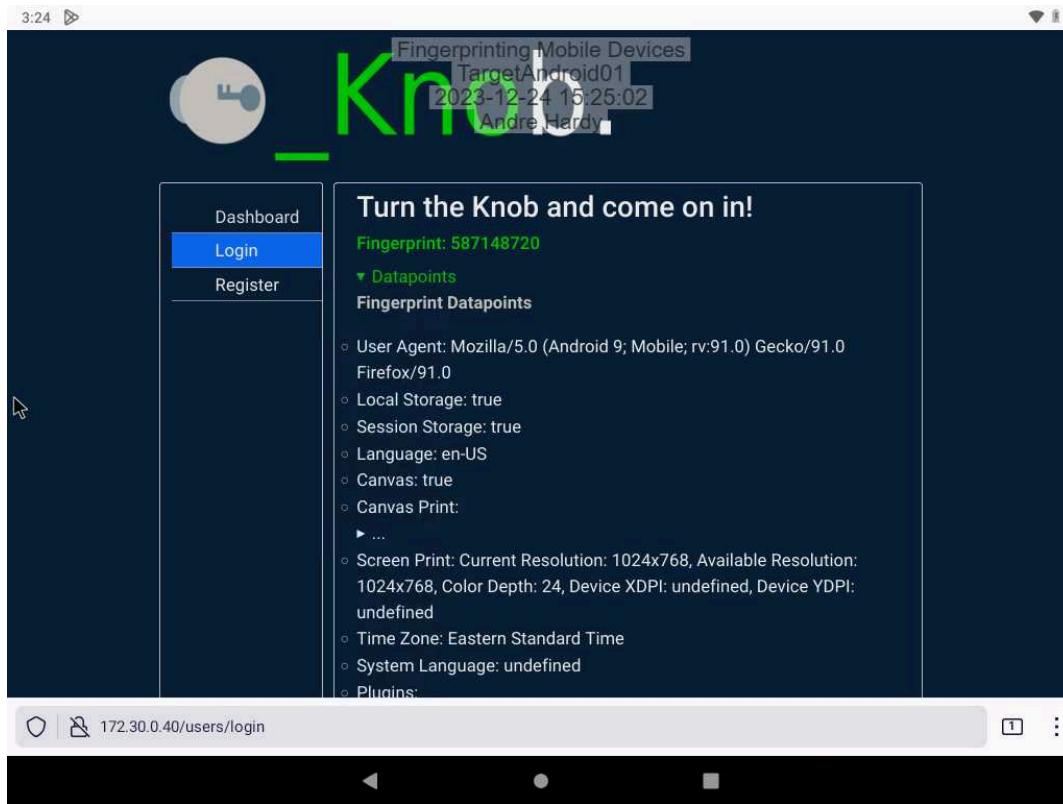
4. Make a screen capture showing the Chrome fingerprint on TargetAndroid01.



Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

9. Make a screen capture showing the Firefox fingerprint on TargetAndroid01.



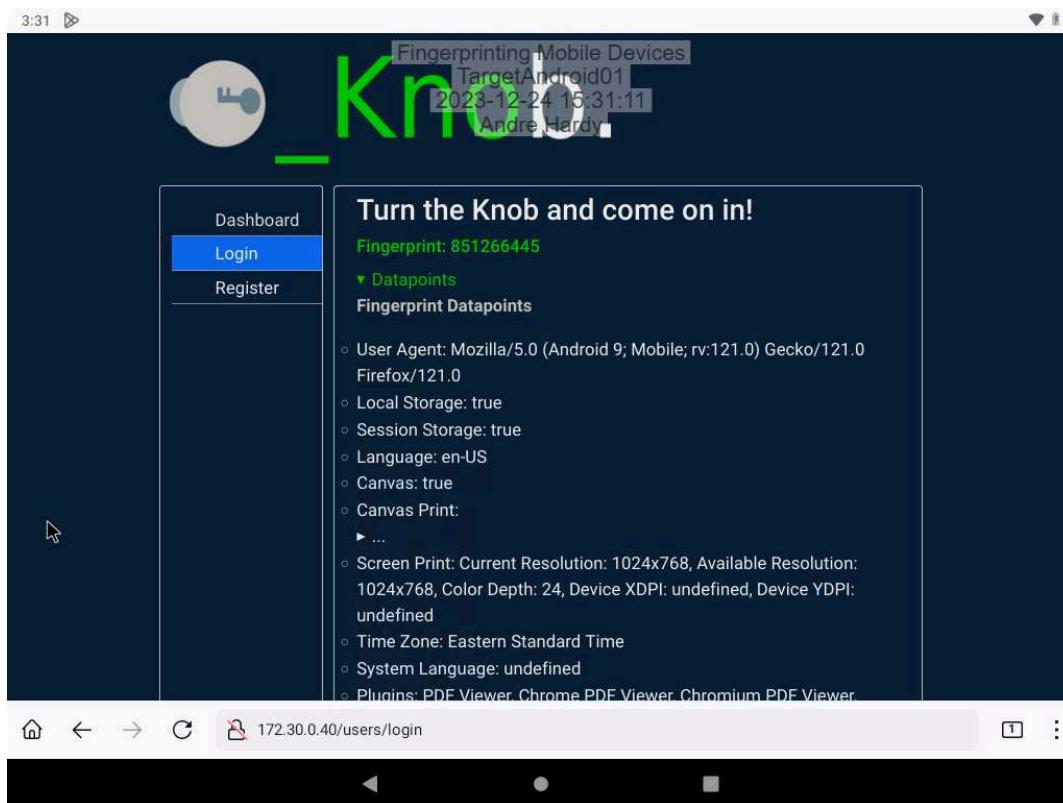
10. Identify the differences between the Datapoints values generated for Chrome and the Datapoints values generated for Firefox.

I do not see any differences

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

16. Make a screen capture showing the updated Firefox fingerprint on TargetAndroid01.



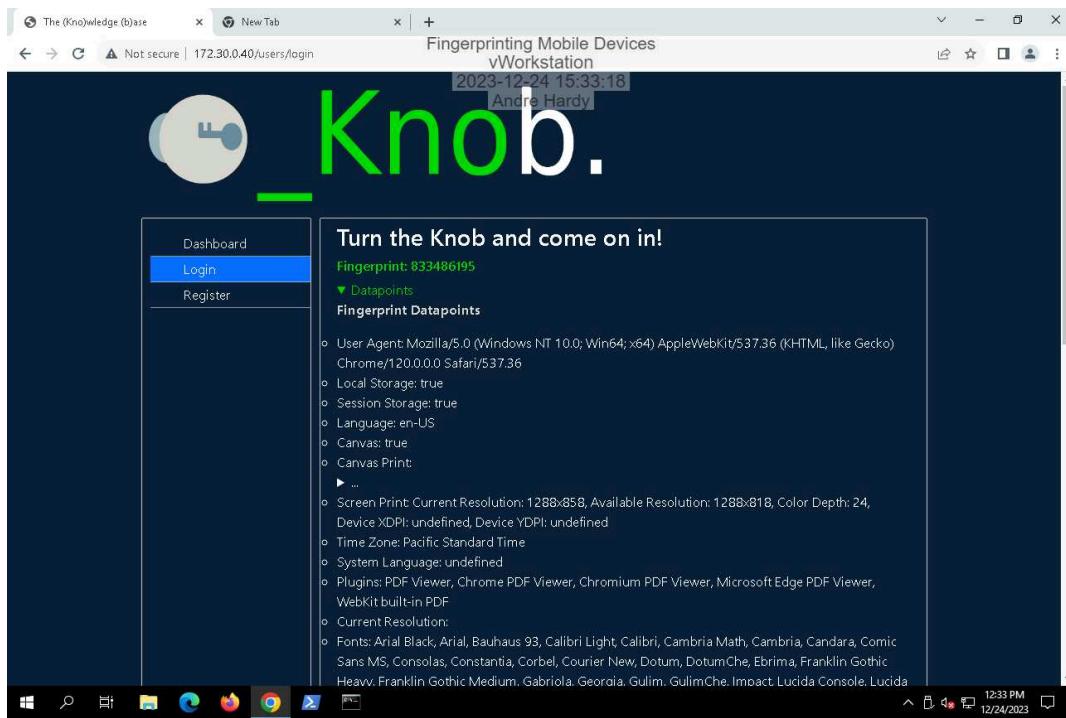
17. Identify the differences between the Datapoints values for Firefox before and after the update.

I do not see any differences

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

20. Make a screen capture showing the Chrome fingerprint on the vWorkstation.



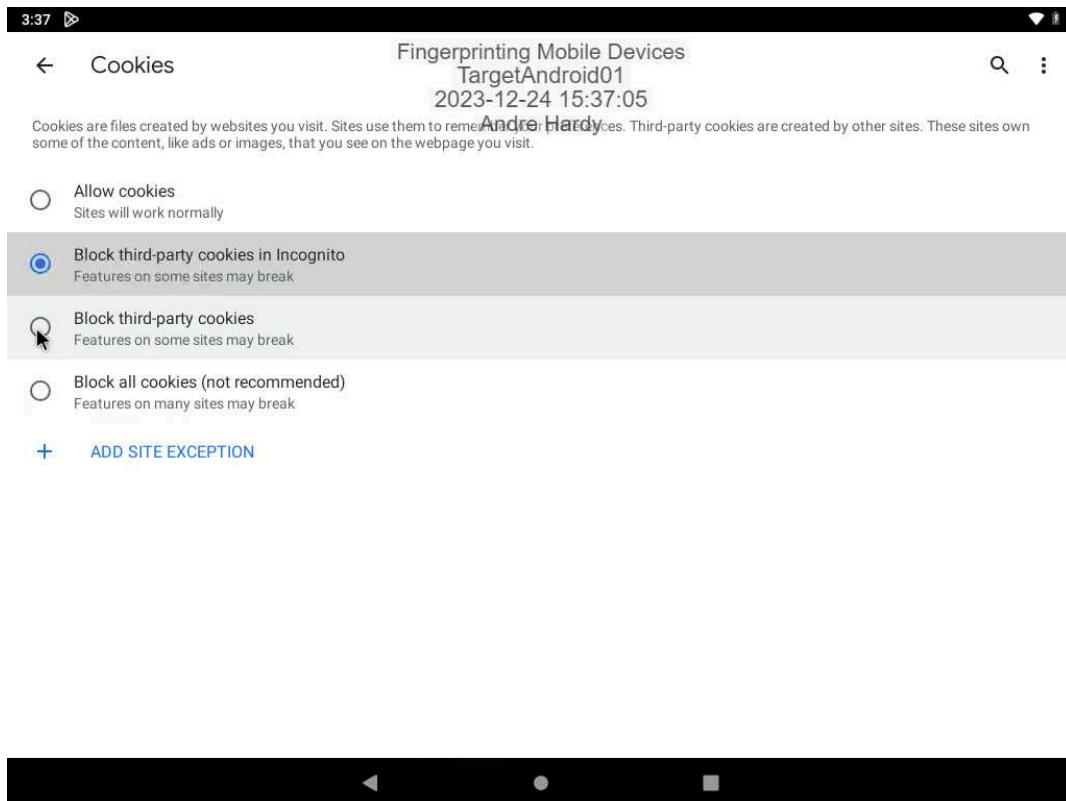
21. Identify the differences between the Datapoints values on the vWorkstation and TargetAndroid01.

It appears to have collected the same data points

Section 3: Challenge and Analysis

Part 1: Disable Third-Party Cookies

Make a screen capture showing the cookie settings in Chrome on TargetAndroid01.



What would happen if you switched to a different option for allowing versus blocking cookies, and how would it hinder attempts to track your activities online? Would there be any drawbacks?

There would be drawbacks to security in terms of fingerprinting your device and allow easier tracking of your device.

Part 2: Test Your Browser's Tracking Protection

Fingerprinting Mobile Devices

Wireless and Mobile Device Security, Second Edition - Lab 05

Make a screen capture showing the **Cover Your Tracks assessment results**.

The screenshot shows a mobile web browser interface. At the top, there are two tabs: "The (Kno)wledge (b)ase" and "Cover Your Tracks". The main content area displays the results of a fingerprinting test. The title "Fingerprinting Mobile Devices" is at the top, followed by "TargetAndroid01" and the date "2023-12-24 15:39:59". Below this, a message from Andre Hardy encourages using a tracker blocker like Privacy Badger or a browser with built-in fingerprinting protection. A section titled "WHAT IS A BIT OF INFORMATION?" explains that a "bit" is a basic unit of information for computers, often represented as "1" or "0". It notes that while individual metrics may seem like a small amount of information, when combined with other metrics, they can uniquely identify a browser. The results are measured in "bits of identifying information", which is a combined summary of all these metrics. A note at the bottom credits Fingerprint2 and Aloodo for portions of the test. The browser's address bar shows the URL <https://coveryourtracks.eff.org>. The bottom of the screen shows the Android navigation bar.

Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 27256.14 browsers have the same fingerprint as yours**.

Currently, we estimate that your browser has a fingerprint that conveys **14.73 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here](#).

Detailed Results

Here's some more granular information we gathered about your browser. Your report includes examples of several different kinds of metrics:

WEB HEADERS

Whenever you connect to a website (in our case, "<https://coveryourtracks.eff.org>"), your device sends a request that includes HTTP headers. These headers contain information like your device's timezone, language, privacy