**Name:** Hemant Jain

**Lab Progress Report Due Date:** 03/15/2021

**Current Week Since Start Date:** Week 8 (03/16/2021– 03/22/2021)

**Reporting Week:** From Mar 09, 2021 to Mar 15, 2021

**Summary about the TestOut Module-8 Learning:**

From the TestOut LabSim, I learnt about the Wireless Threats. Continuing the coursework, I came across the various wireless network hardware components namely like Wireless Access Point(WAP), Wireless Interface, Wireless bridge, Wireless LAN Controller(WLC), Lightweight Access Point(LWAP). Learnt the simulating and troubleshooting steps to follow to configure the wireless network. Two key roles of wireless antennas are Absorbing incoming radio signals and radiating outgoing radio signals. Learnt which are the types of antennas used in the networking configurations.

Learnt about using the wireless attack tools and how to crack the wifi encryption using the Aircrack-ng. Detecting rogue hosts which are the unauthorized access points added into the network was one of the modules and configuring the rogue host protection to prevent the threats was follow-up assignments.

Read about the WiFi Attacks like Rogue Access Points(AP), Evil twin attack, Initialization vector(IV) attack, Jamming attack, Disassociation/deauthentication attacks, Bluetooth attacks, RFID/NFC attacks with eavesdropping, man-in-the-middle, Denial of Service(DOS), Cloning and spoofing.

In last sub-module, demonstrated the hardening of a wireless network, Configuring a wireless network intrusion prevention system, and configuring a captive portal along side. Security Configuration actions is the first step in making your network more secured and prone to attacks. Enabling MAC address filtering can prevent the unauthorized connection to the WAP.

**In-class Lab Homework:**

**Week 8 Lab Pt 1 Web Privacy and Anonymity**

**Part-1: Check Out Your Data**

Question: What types of information had this online service collected about you?

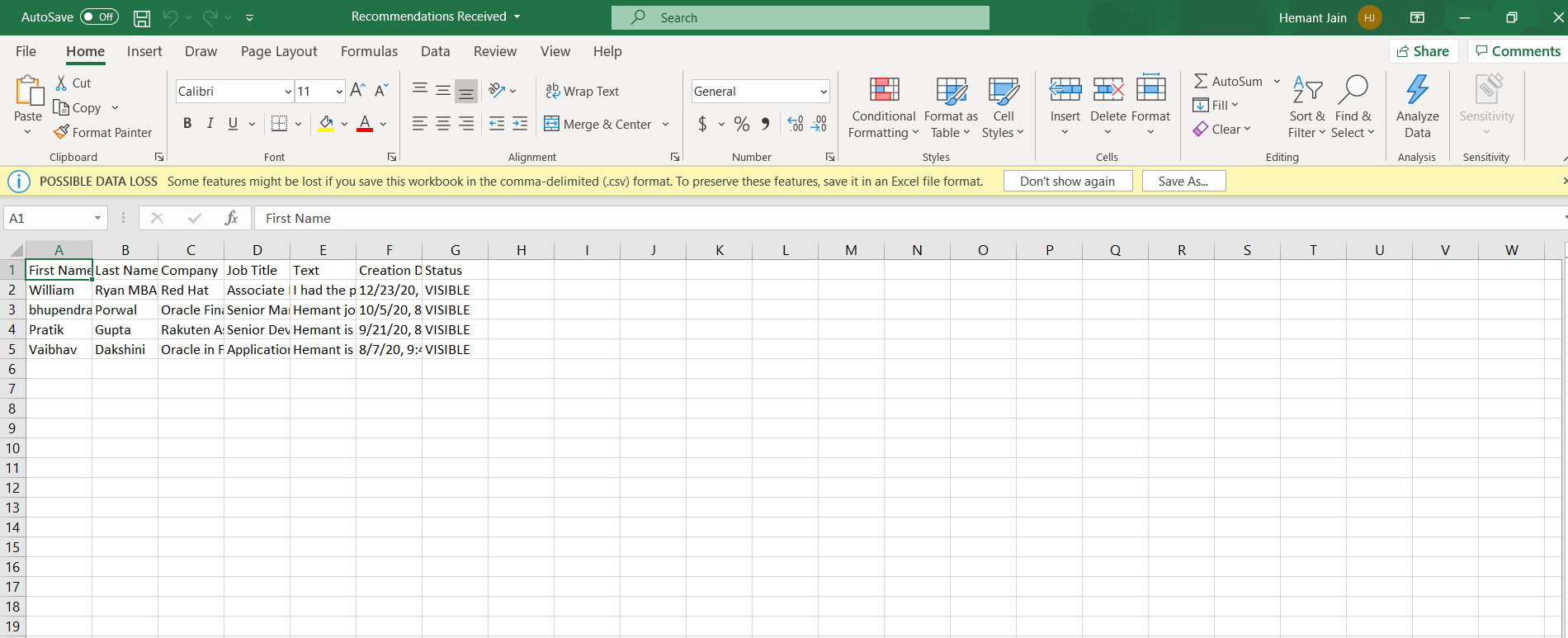
Answer: I collected my LinkedIn Feed Invitations, Connection Request, Profiles, Recommendation Received, Articles data from LinkedIn.

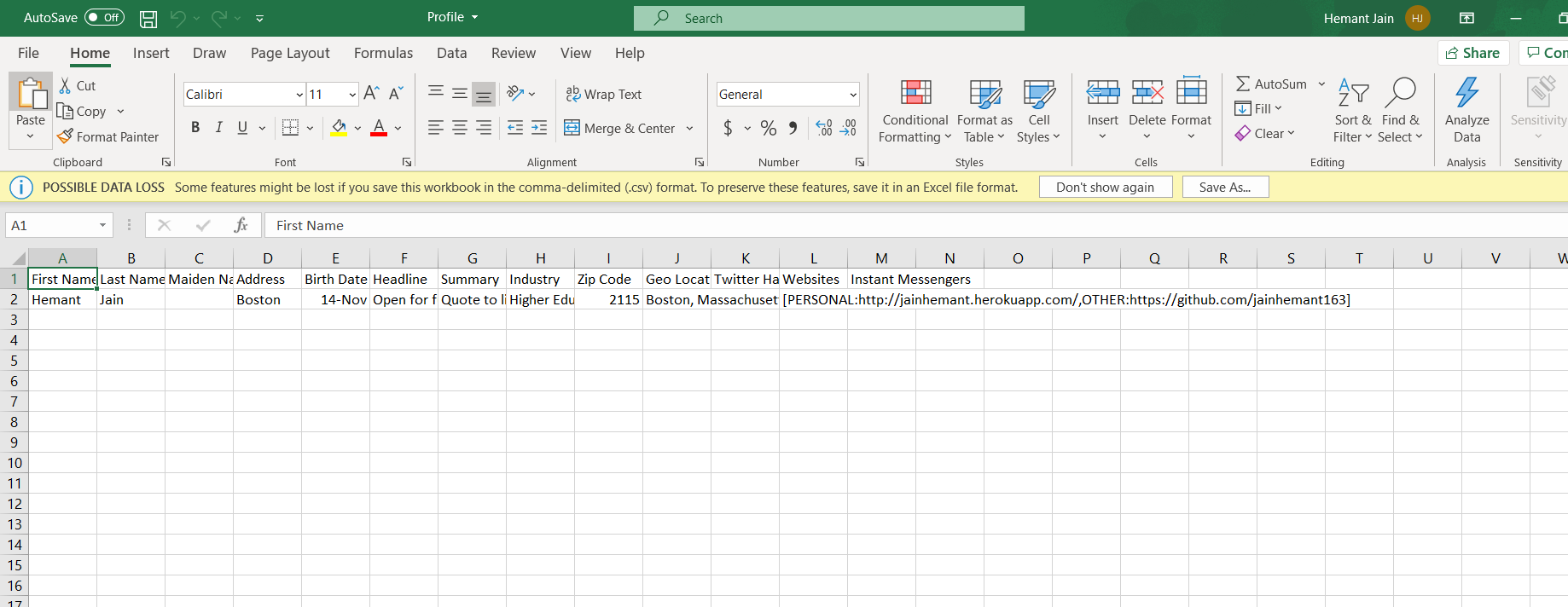
I tried using the Facebook but was unable to find out the button where I can download the facebook data for the offline analysis.

Question: Did anything you found in the data about yourself surprise you?

Answer: Nothing much interesting, as it showed up all the nominal and normal usage and data actions I performed while being active on the platform.

Question: Submit to Canvas as screenshot of the files you obtained from the online service. Don't submit a screenshot of the contents of these files.

Answer: 

**Part-2 : Blocking Web Trackers**

Question: What is the name of the third-party tracker you read about, and what kinds of information is its company collecting about you?

Answer:

**Part 3: Browser Fingerprinting**

Question: Is your browser blocking tracking ads? No



Question: Is your browser blocking invisible trackers? No

Question: Does your browser unblock 3rd parties that promise to honor Do Not Track? No

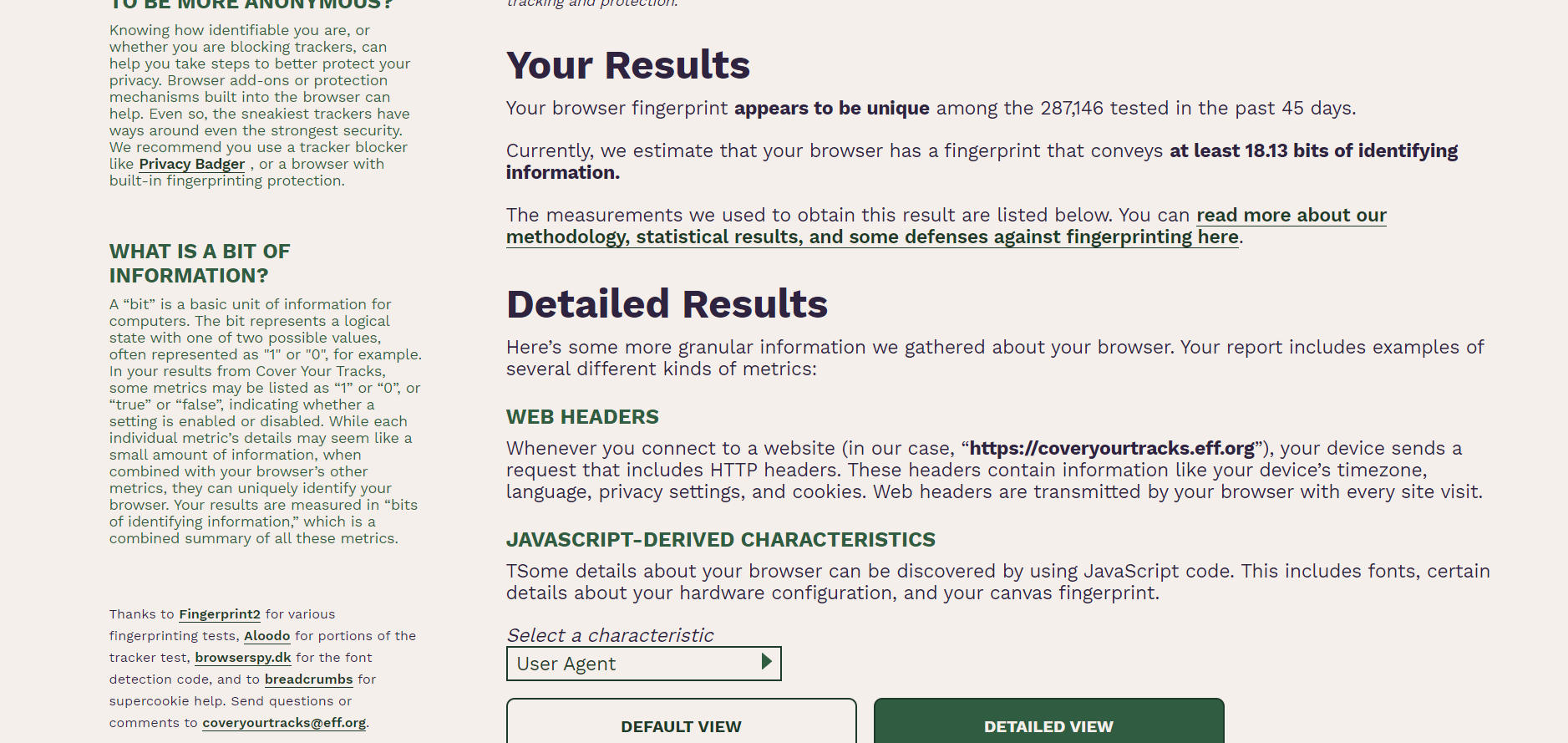
Question: Does your browser protect against fingerprinting?

It says : Your browser has a unique fingerprint

**Question:** How many bits of information does Panopticlick report for your browser?

Answer: Your browser fingerprint appears to be unique among the 287,146 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys at least 18.13 bits of identifying information.



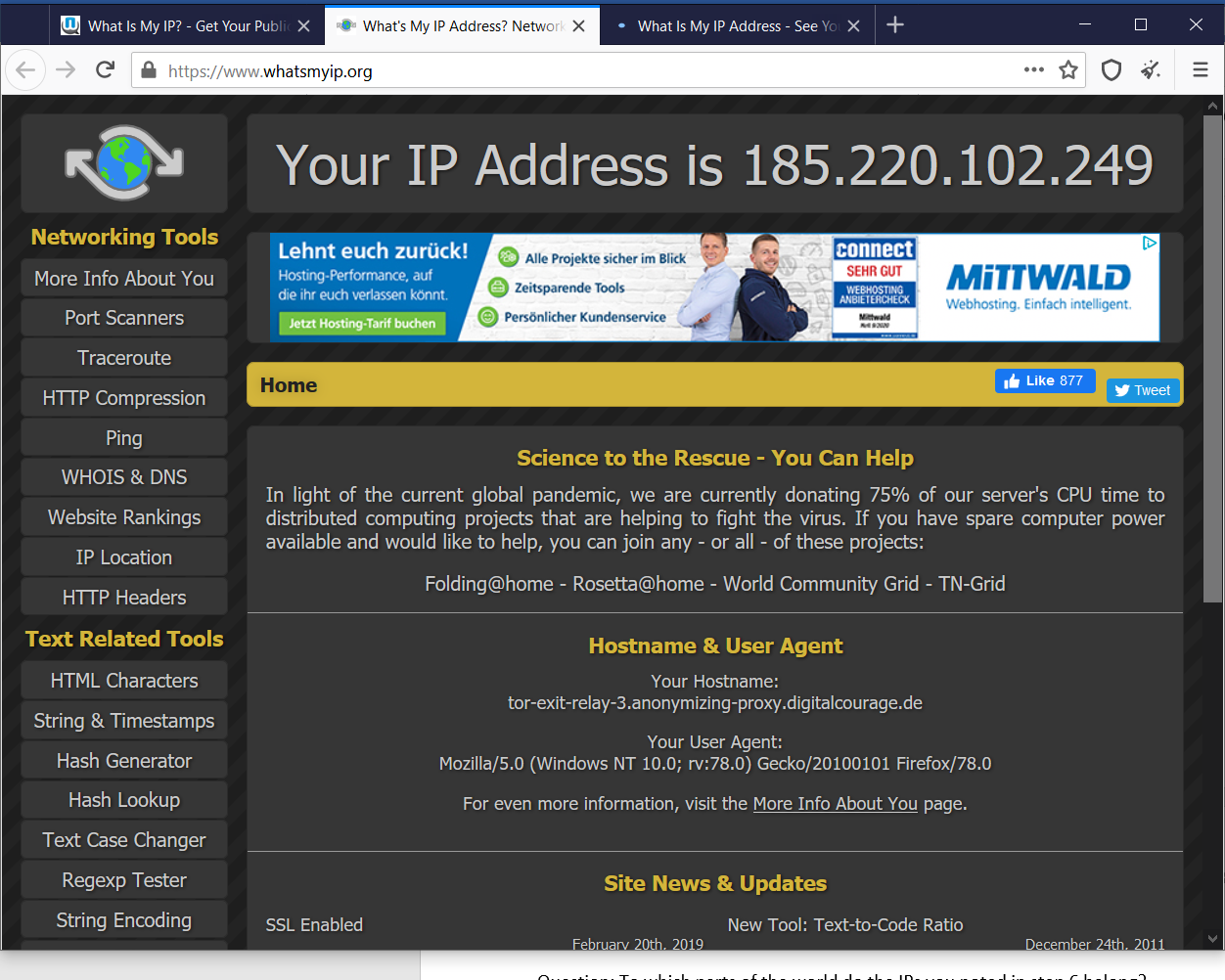
**Part 4: Anonymous Web Browsing**

Question: If your true IP address can still be seen by web servers, what does your browser\’s privacy mode do?

Answer: Despite your browser history remaining hidden, incognito mode does not improve your security in any other way – your IP address will remain visible and the websites you visit will still be able to store data about your actions – if you accept the use of cookies, they will still be stored on your computer, and be able to gather information about your browsing habits etc. To reiterate – the incognito mode in a web browser is primarily used to hide your browsing history – It is not a complex security feature that can protect you from malicious attacks or attempts to retrieve your personal data.

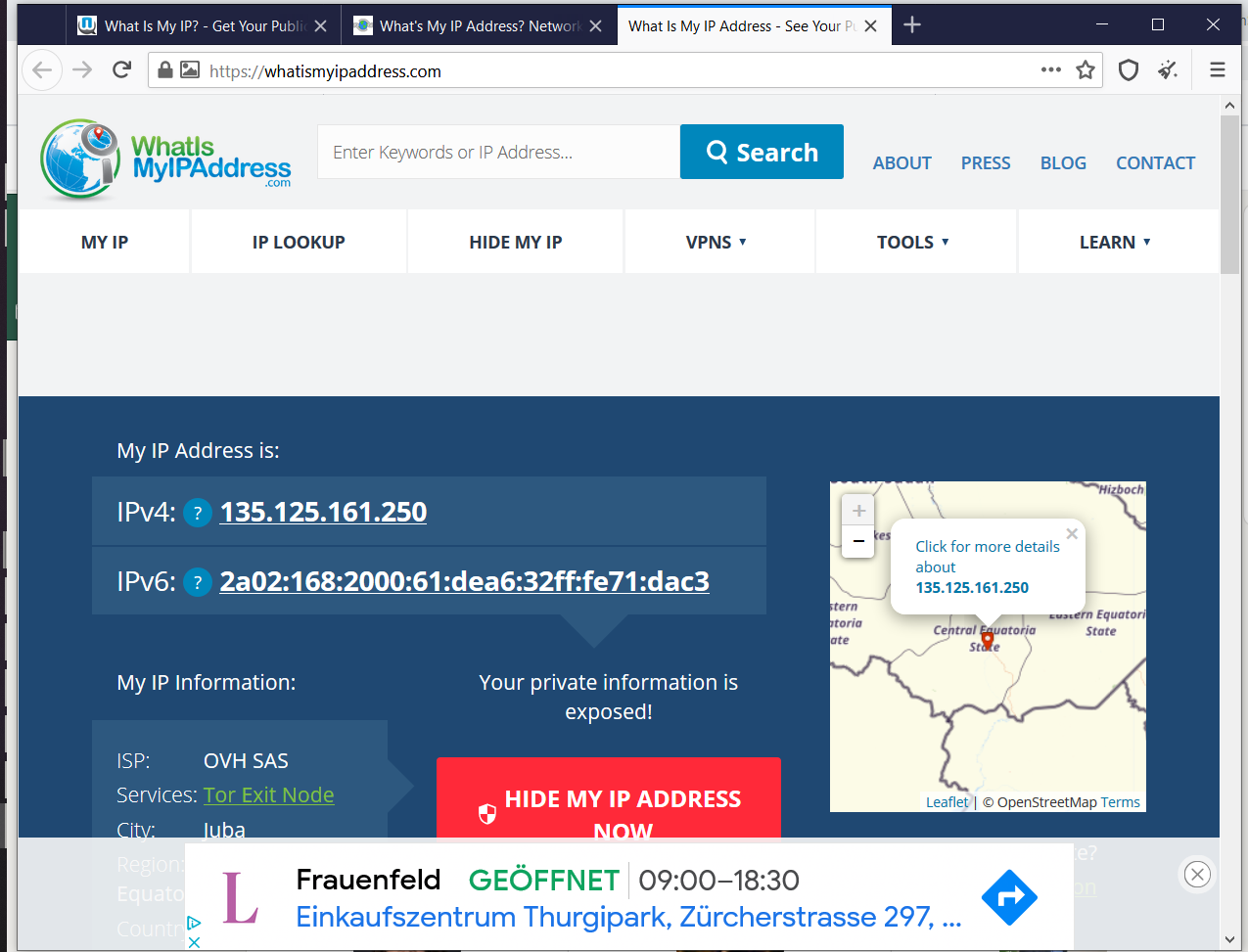
Tor Browser verify that your IP address has changed:

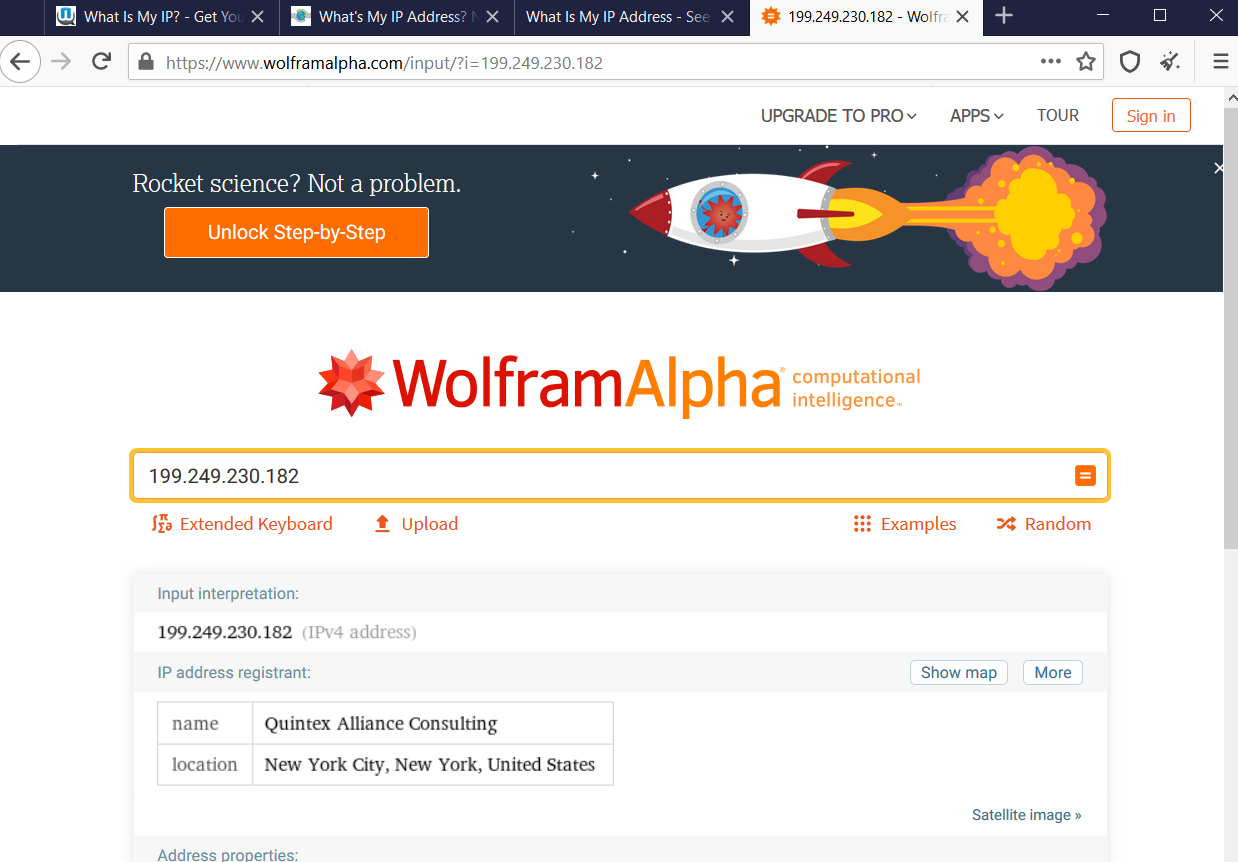


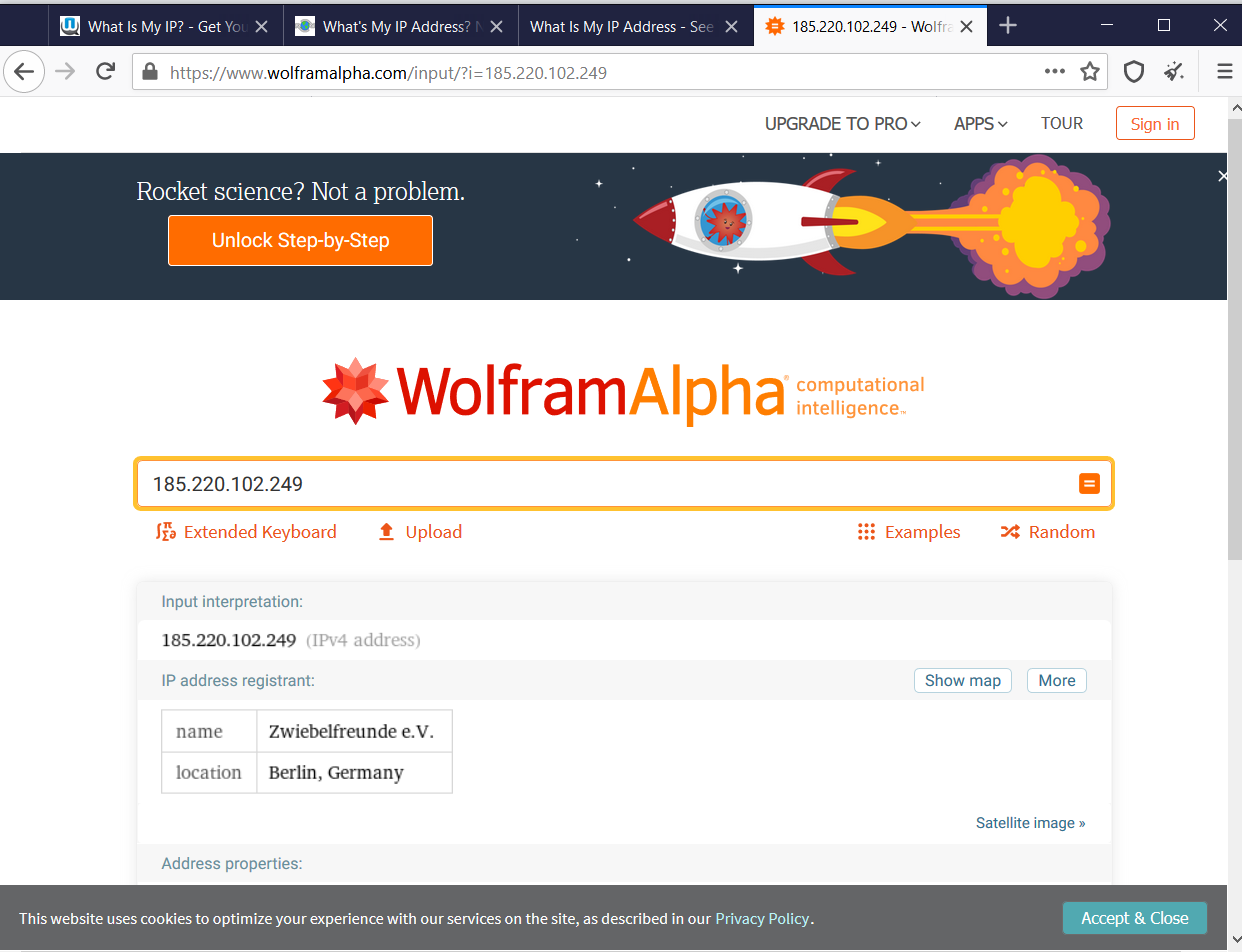
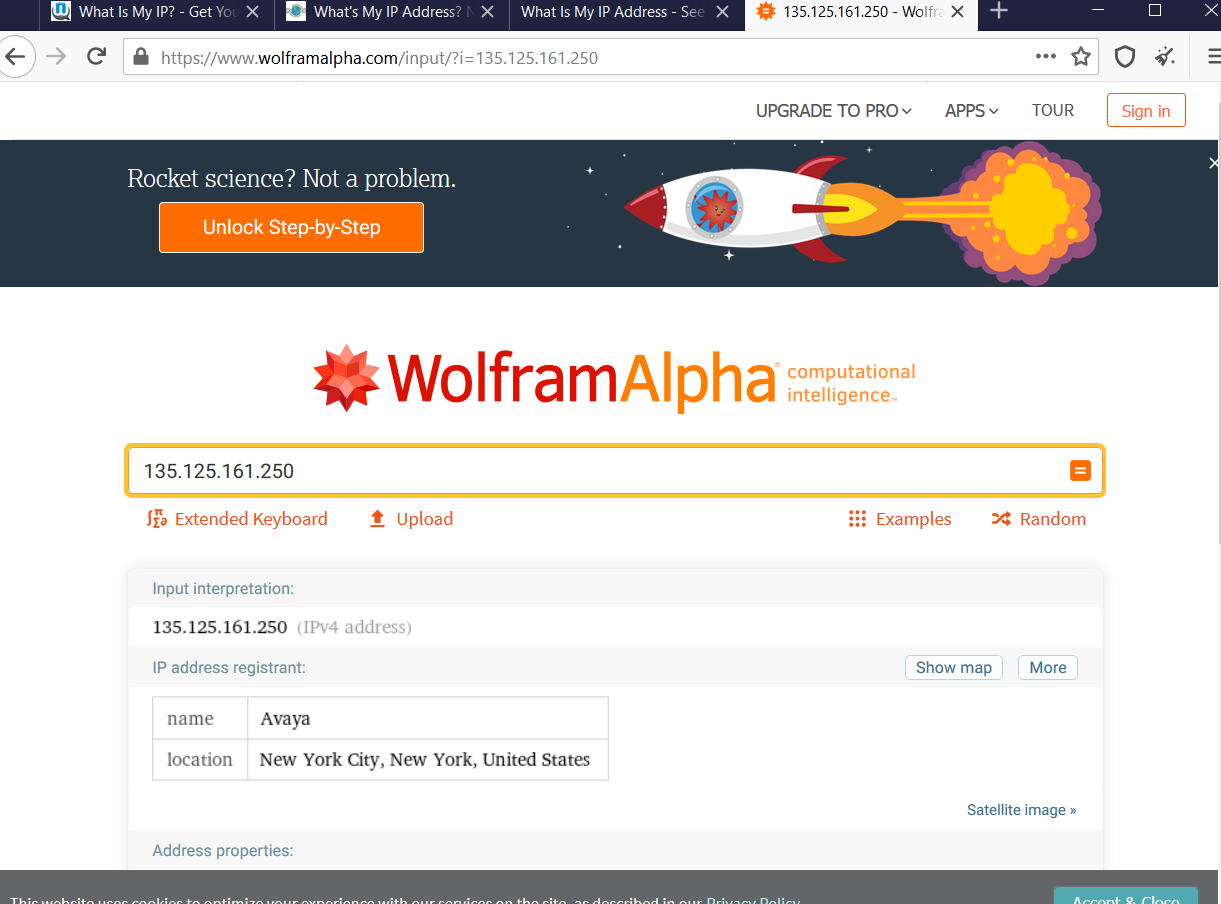


Question: To which parts of the world do the IPs you noted in step 6 belong?

Boston, MA, United States





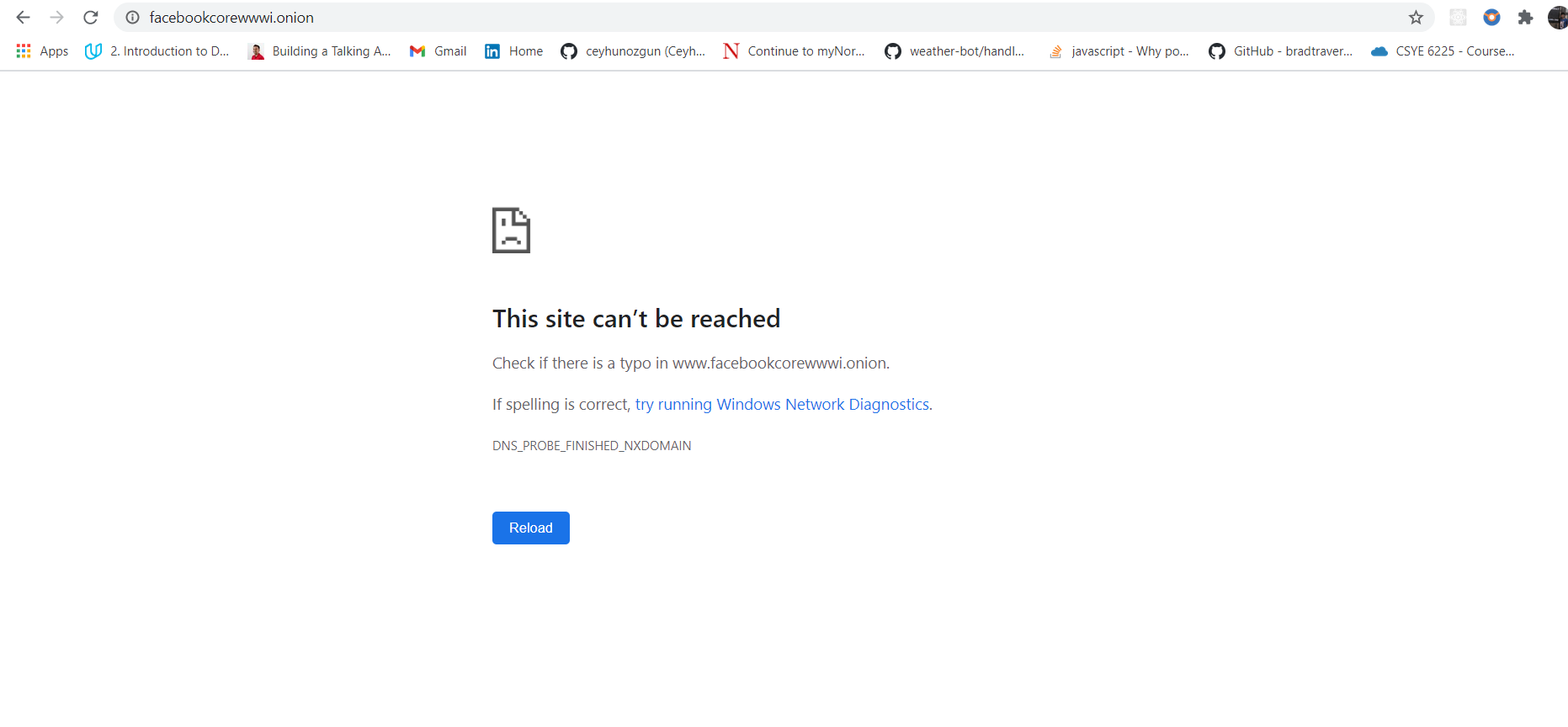
Question: What error message do you receive?

# This site can’t be reached

Check if there is a typo in www.facebookcorewwwi.onion.

* If spelling is correct, [try running Windows Network Diagnostics](javascript:diagnoseErrors()).

DNS\_PROBE\_FINISHED\_NXDOMAIN



Question: What do you think about the experience of accessing TOR services?

I do feel it is good browser if I want to search very secret content using TOR services.

Sometimes it takes longer time than expected to serve our URL and chances of getting phished are higher. Tor is useful for anyone who wants to keep their internet activities out of the hands of advertisers, ISPs, and websites. That includes people getting around censorship restrictions in their country, people looking to hide their IP address, or anyone else who doesn’t want their browsing habits linked to them.

The Tor network can also host websites that are only accessible by other Tor users. In other words, you’ve now entered the world of the Dark Web, or sites that aren’t indexed by the regular crawlers you use to search for cute animals, things to buy, and trivia answers. You can find everything from free textbooks to drugs on the Dark Web—and worse—so long as you know the special URL that takes you to these sites.

Reference Link: <https://lifehacker.com/what-is-tor-and-should-i-use-it-1527891029>

**Week 8 Lab Pt. 2: Wireless Monitoring Tools**

**Project 1: Using a Wireless Monitor Tool**

Question: Does the amount of available in form at ion from Wi-Fi networks to which you are not connected surprise you?

Answer: Yes, I see many unknown devices connected to our WiFi network.

Question: Under SSID, is there a service set identifier for each network? Why would an SSID not appear?

Answer: No, If the desired network SSID is not displayed on the screen, check the following points.

Make sure that the wireless access point/router is powered on.

Move your machine to an area with no items which obstruct the wireless network signal, such as metal doors or walls, or closer to the wireless access point/router.

Temporarily place your machine within about 1 m (3.3 feet) from the wireless access point when you are configuring the wireless settings.

If your wireless access point/router is using MAC address filtering, confirm the MAC address of this machine is allowed in the filter.

Question: Does disabling the broadcast of the SSID name give any enhanced level of security? Why not?

Answer:

1. Disabling SSID broadcast will not hide your network completely

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

1. Third-party software can easily trace a hidden network

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

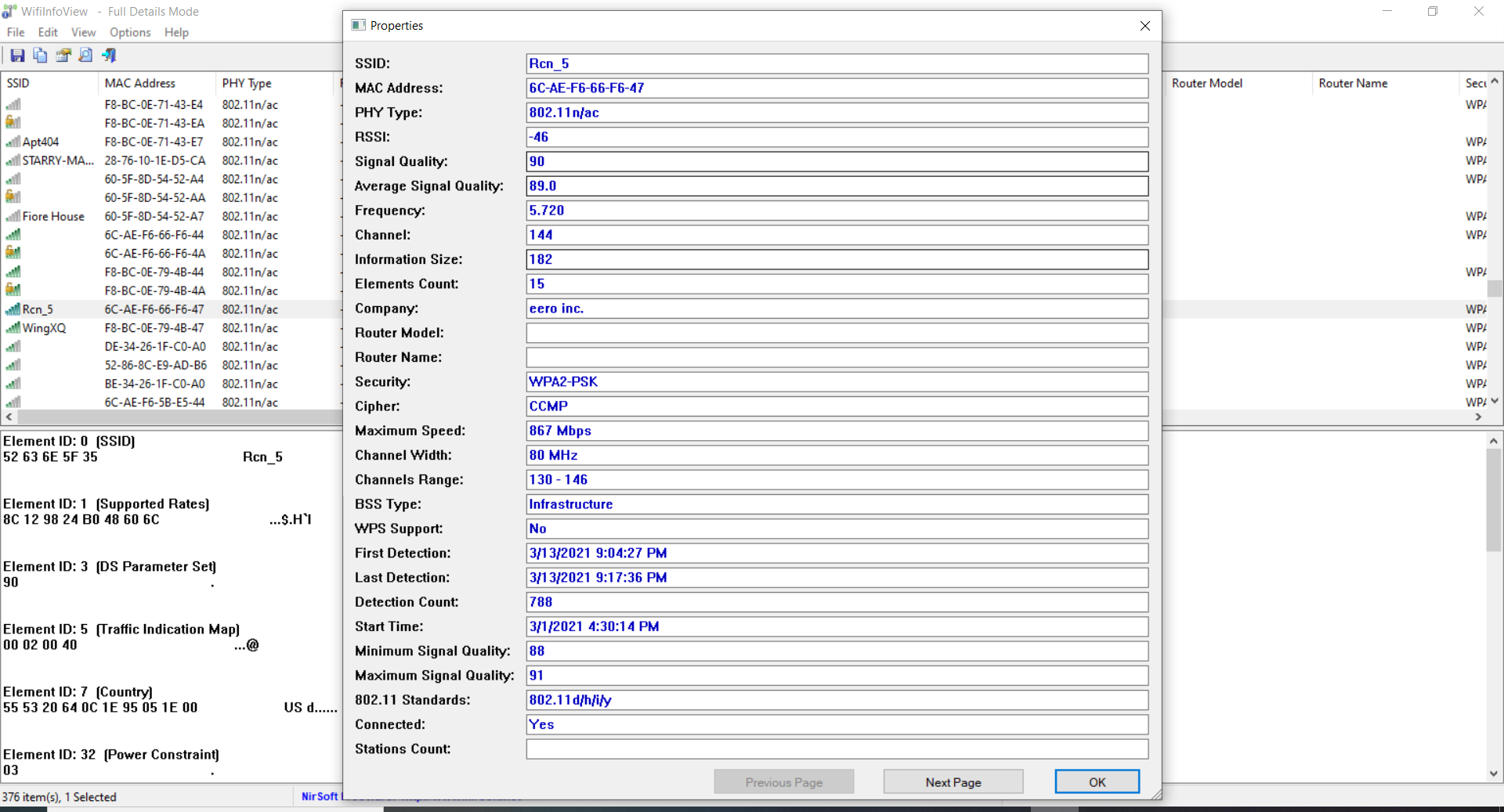
1. ou might attract unwanted attention

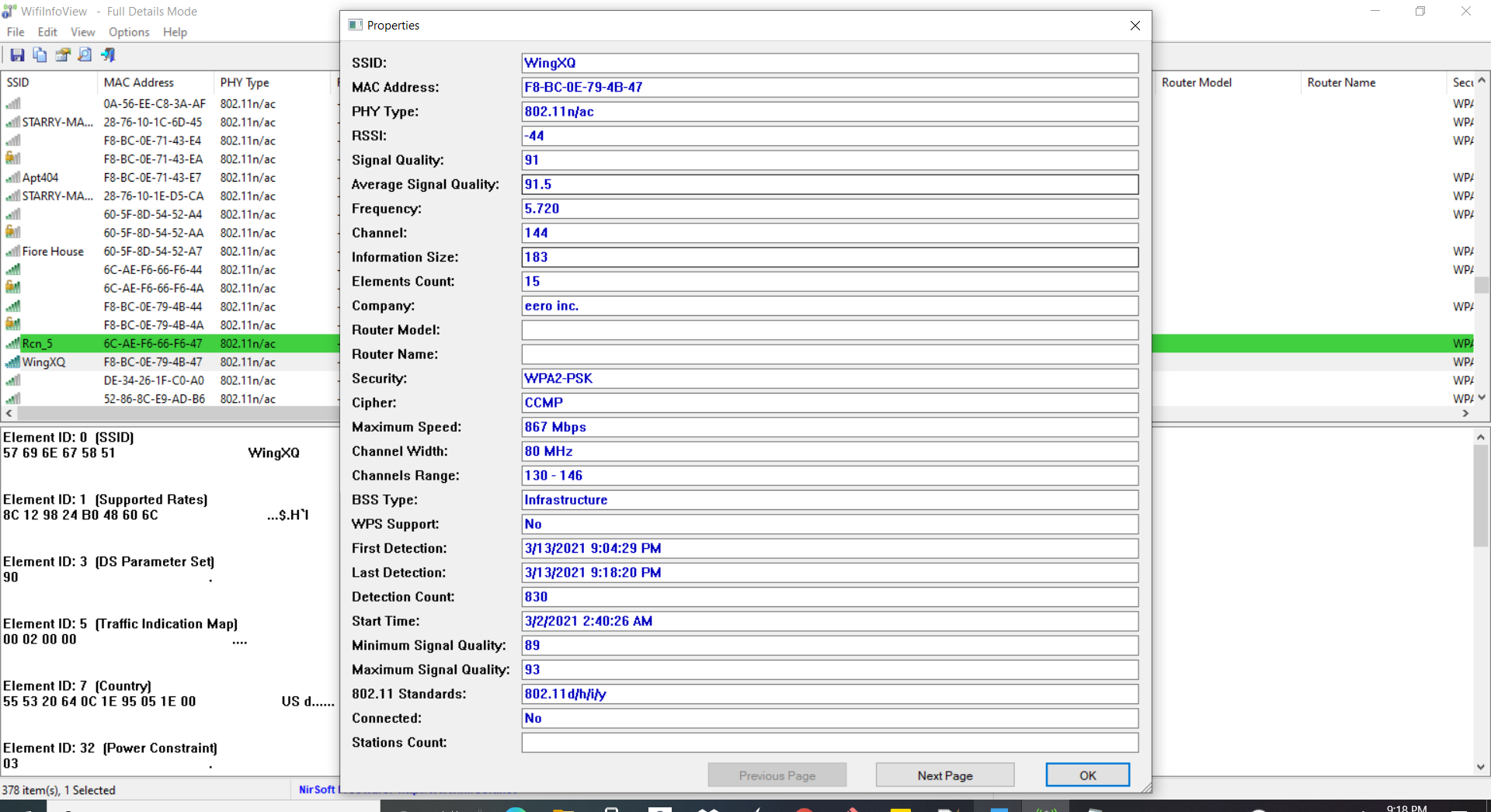
Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so.

Question: . Note the value under the column MAC Address. How could a threat actor use this information?

Answer:

Hacker can use the users open MAC Address for MAC Spoofing or Man-in-the-Middle Attacks.





**Question:** Scroll to the Security and Cipher columns . What security are the networks using?

Answer: Security : WPA2-PSK Cipher: CCMP

**Question:** Scroll to WPS Support . How many networks have WPS turned on? Is this secure?

Answer: None

Question: What additional information do you find useful? What information would a threat actor find useful?

Answer: This all-additional parameter could acts as helpful for the threat in the network : RSSI, Signal Quality, Average Signal Quality, Frequency, Information Size, Maximum Speed, Channel Range, First Detection, Detection Count, Country.

**Project 2: Viewing WLAN Security Information with Vistumbler**

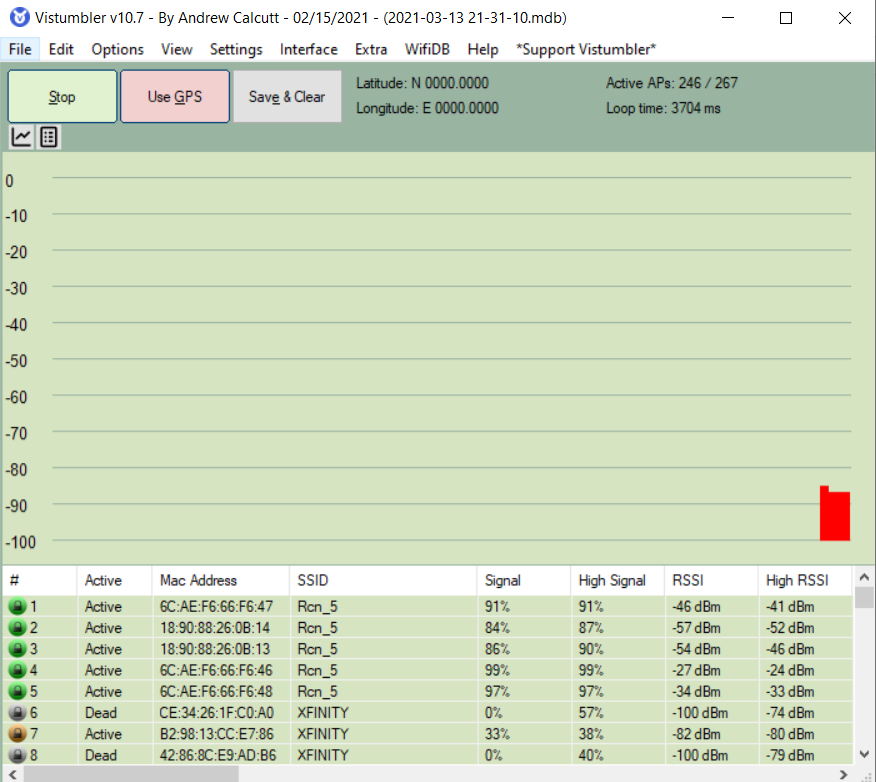
Question: Click one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes. What information is displayed on this graph?

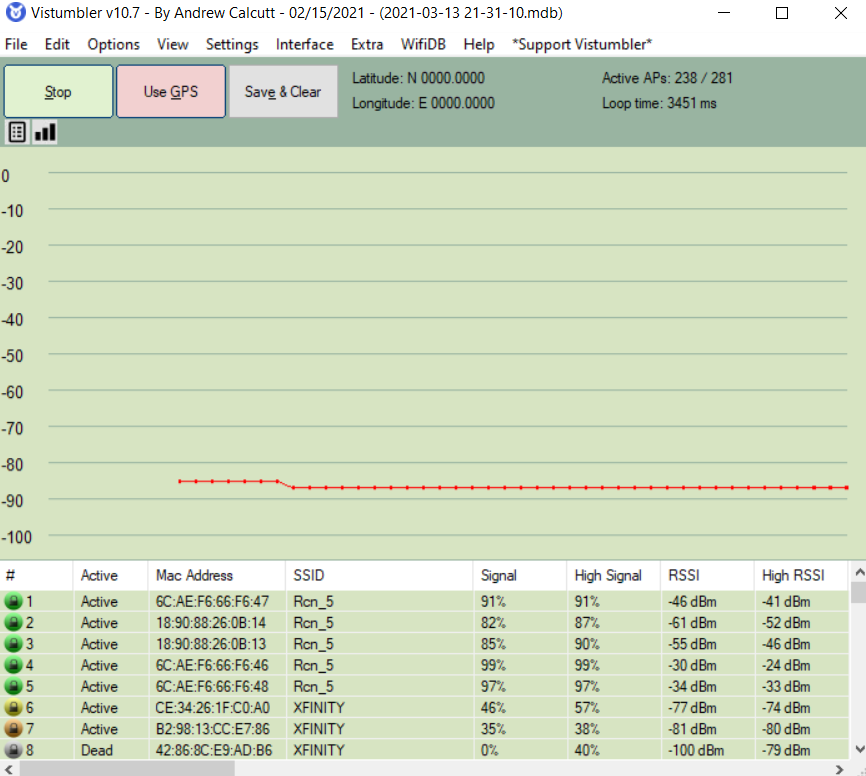
Answer:



Question: . Click another one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes. What information is displayed on this graph? How is this different from the previous graph?

Answer:

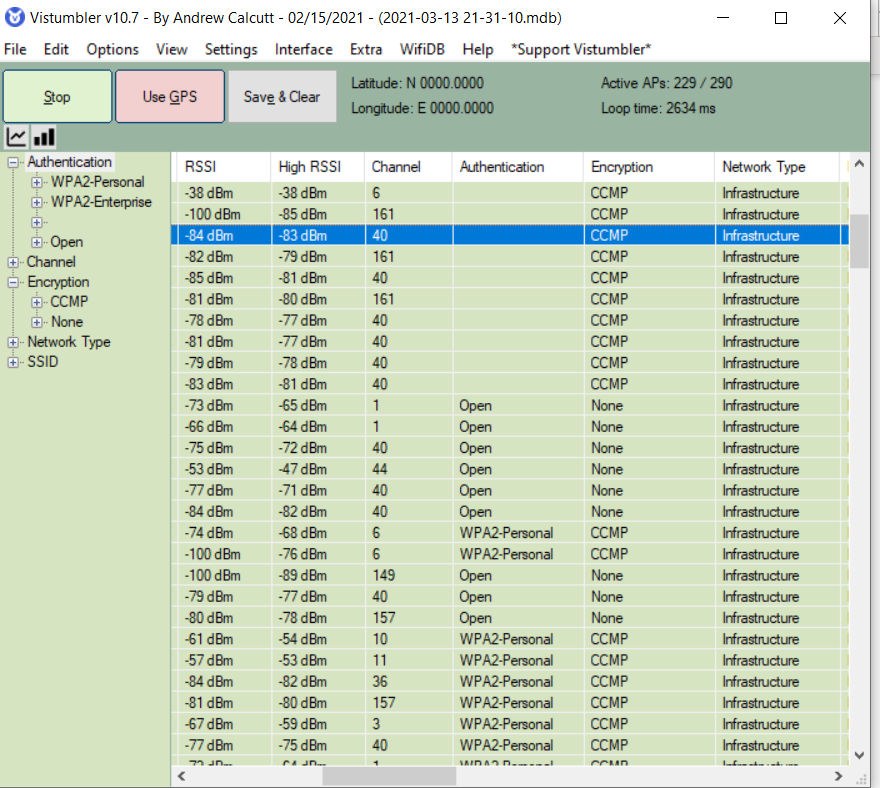




Question: Use the horizontal scroll bar to move to the right. Note the columns Authentication , Encryption , Manufacturer , and Radio Type. How would this information be useful to an attacker?

Answer:

Using the Authentication column, we can easily know which machine is open and not authenticated against the new connection are required. And the Encryption column lets you whether the encryption of data is done before transmission of sender messages.



Question: Record the total number of different WLANs that you can detect, along with the number of encryption types. Which type is most common?

Answer:

WPA2-Personal

Question: How does Vistumbler compare with WiFilnfoView? Which is easier to use? Which tool gives more information?

Answer: Anytime I would recommend Vistumbler over WiFiInfoView which gives out more detailed information as compared to few user outputs from WiFiInfoView.

**Project 3: Configuring Access Points**

Question: Under Broadcast Network Name (SSID), click the down arrow next to Enabled. What other option is available? Would it be an advantage to change this setting? Why or why not?

Answer: The other option available is Disabled.

**Disabling SSID broadcast** will make your Wi-FI **network name** invisible to other users. However, this only hides the **name**, not the **network** itself. You cannot disguise the router's activity, so it can still be attacked by hackers. With your **network** invisible to wireless devices, connecting becomes a bit more complicated.

Enable and Disable

b. Would it be an advantage to change this setting? Why or why not?

Answer: The Broadcast name SSID just shows who you are online, so disabling it is like keeping yourself safe from other networks finding out who you really are and enabling it will let them know who you are.

8. Under Frequency (Channel) note that the default is Auto. What does this mean?

Answer: This means that it will automatically pick the best suited channel signal it can find

9. Click the down arrow on Auto. When would you want to change the channel on which the wireless signal is broadcast?

Answer: You will see a set of channels that you can manually select and if you set your router toa specific channel you can use that.,

10. Under Channel BandWidth click the down arrow on 20 MHz. Answer the following questions:

a. What is the other option?

Answer: 40MHzb.

b. Why would you choose this option?

Answer: I will choose this option because it will increase the range on how many signals can be reached

c. What are the advantages and disadvantages of changing the channel bandwidth?

Answer: Advantages of increasing the bandwidth will help reach across further signal. Disadvantage will be that the further the signal the slower the connection.

11. Under Security Policy there is a single configuration option Security Mode. Note the default setting. Answer the following questions:

a. Is this a good option default option?

Answer: Yes, because it will require a password to login.

b. What does WPA2-PSK mean?

Answer: Wi-Fi protected Access 2- Pre-shared Key. In other words, it usually asks the user to enter a password but remembers the tiny details for logging in

12. Click the down arrow on WPA2-PSK. Answer the following questions:

a. What are the other options?

Answer: Disable, WPA, WPA-PSK, WPA2-PSK Mixes, WPA2 Mixed

b. What do they mean?

Answer: They are a set of different security protocols that either require a password or just username some require both and others require a lot more detail.13. Under WPA note the option WPA Encryption. Click the down arrow on AES. What are the other options available and what do they mean?

Answer: TKIP=AES Temporary Key Integrity Protocol + Advanced Encryption Standard these are encryptions for Wi-Fi(s).14. Under WPA passphrase how long is the default passphrase? Is that sufficient?

Answer: 11 letters and it’s considered okay the longer it is the more it feels secure.

16. Note the option under Internet Access Only. When would you select this option?

Answer: When you have private LAN network.

17. Note the option under Wireless Client Isolation. Why is this not enabled by default?

Answer: It is not enabled by default because it restricts the guests to commutate with another on the network and only give them internet access

18. Under Security Policy note that the Security Mode is set to Disable by default. Why would a guest network’s security be turned off by default? (Hint: If it were turned on what would the guests need before they could use the network?)

Answer: They don’t need the password to access the network because if they did then you will have to give them the password to your network which isn’t safe.

21. Under Access Control what is the LAN Client Filter Function? Does it provide strong security if it were enabled?

Answer: If it was enabled, it would limit the amount of services you get from the internet and you won’t be able to get to some sites cause the IP will be filtered out.

22. Answer the following questions:

a. How easy is this user interface to navigate?

Answer: It is straight forward if you know what you are doing and for someone who doesn’t know might be confusing.

b. Does it provide enough information for a user to set up the security settings on this system?

Answer:

Yes, it’s enough but reckon it might need some more information to understand what

each set of settings mean.

b. Does it provide enough information for a user to set up the security settings on this system?

Answer:

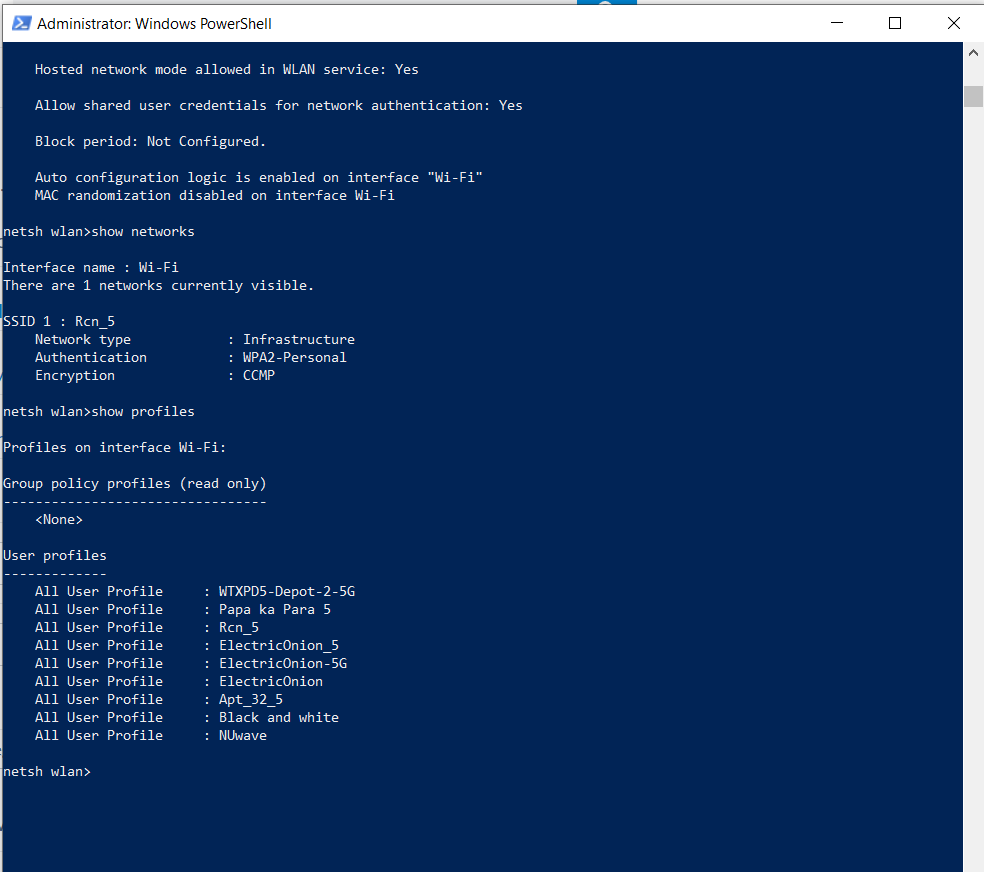
Yes, it’s enough but reckon it might need some more information to understand what

each set of settings mean.

b. Does it provide enough information for a user to set up the security settings on this system? Answer: Yes, it’s enough but reckon it might need some more information to understand what each set of settings mean.

**Project 4: Using Microsoft Windows Netsh Commands**





15. Question: Does the network that you previously blocked appear in the list ?

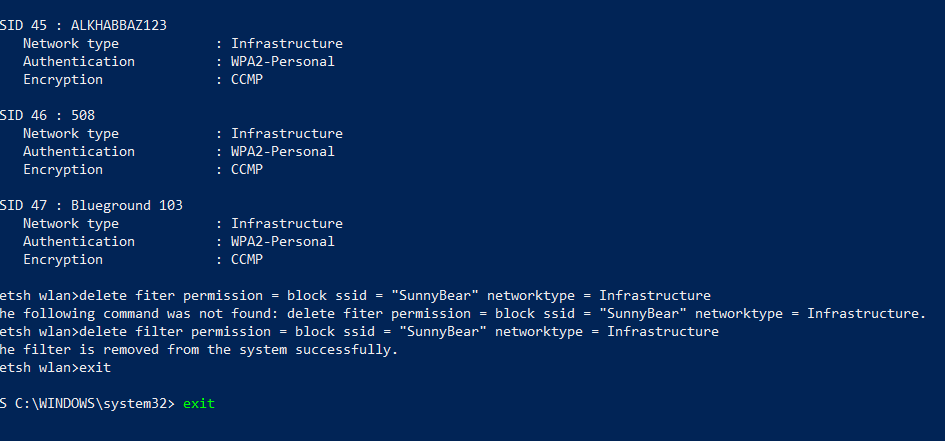
Answer: No

16. Question: Click the wireless icon in your system tray . Does the network appear in this list?

Answer: Yes

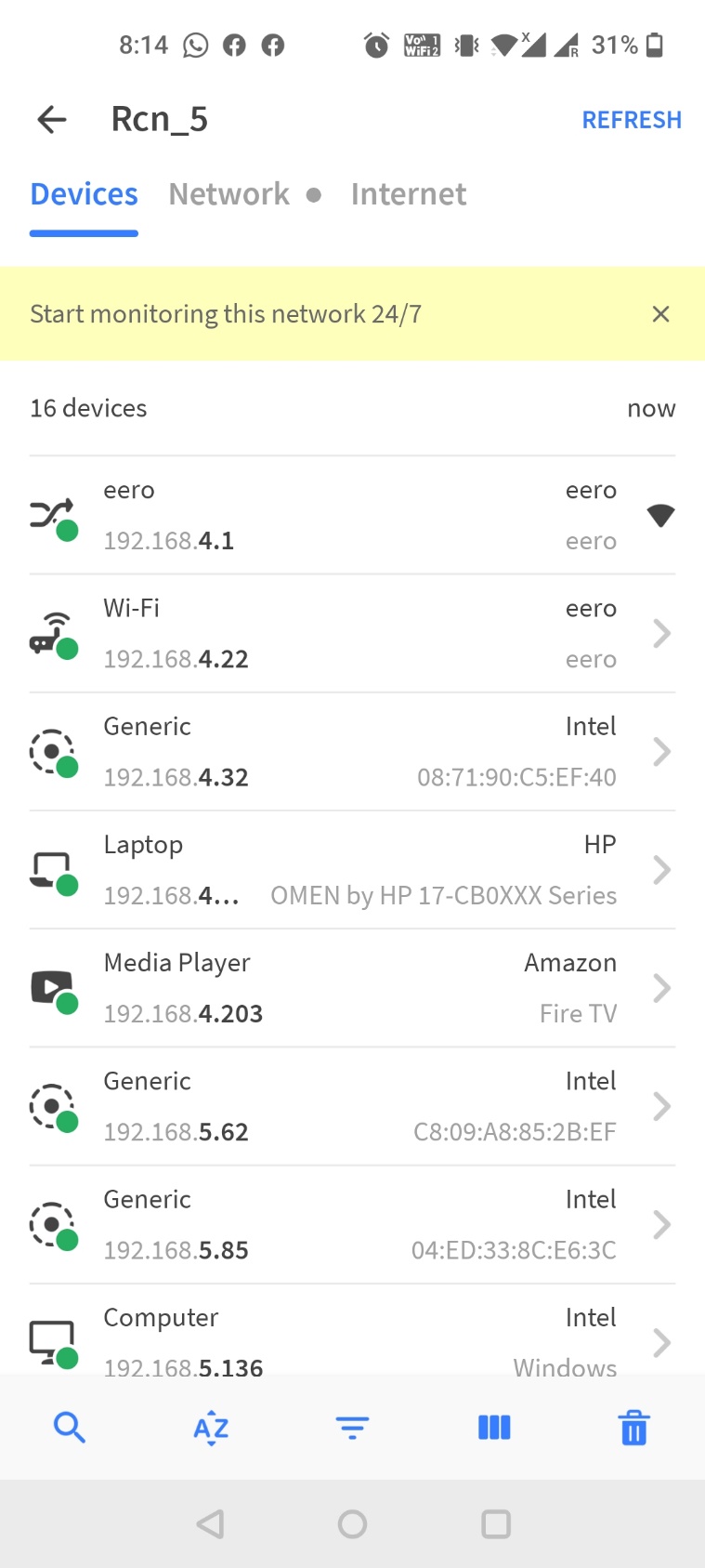
17. Question: If necessary, click the wireless icon in your system tray again. What appears next to the name of this blocked network? Click the name of the network. What does it say?

Answer: It shows up as Secured with a cross mark on the wifi logo in the side-tab.

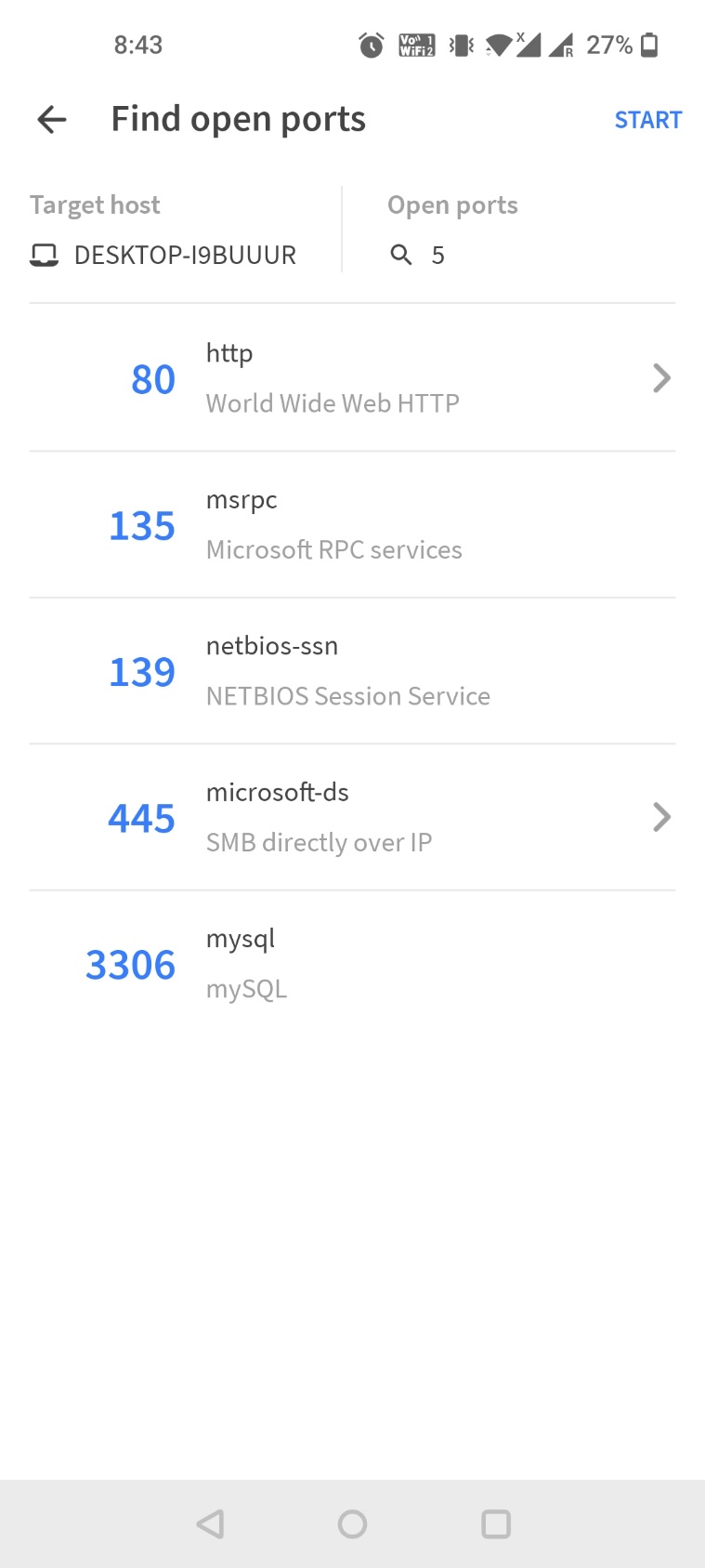
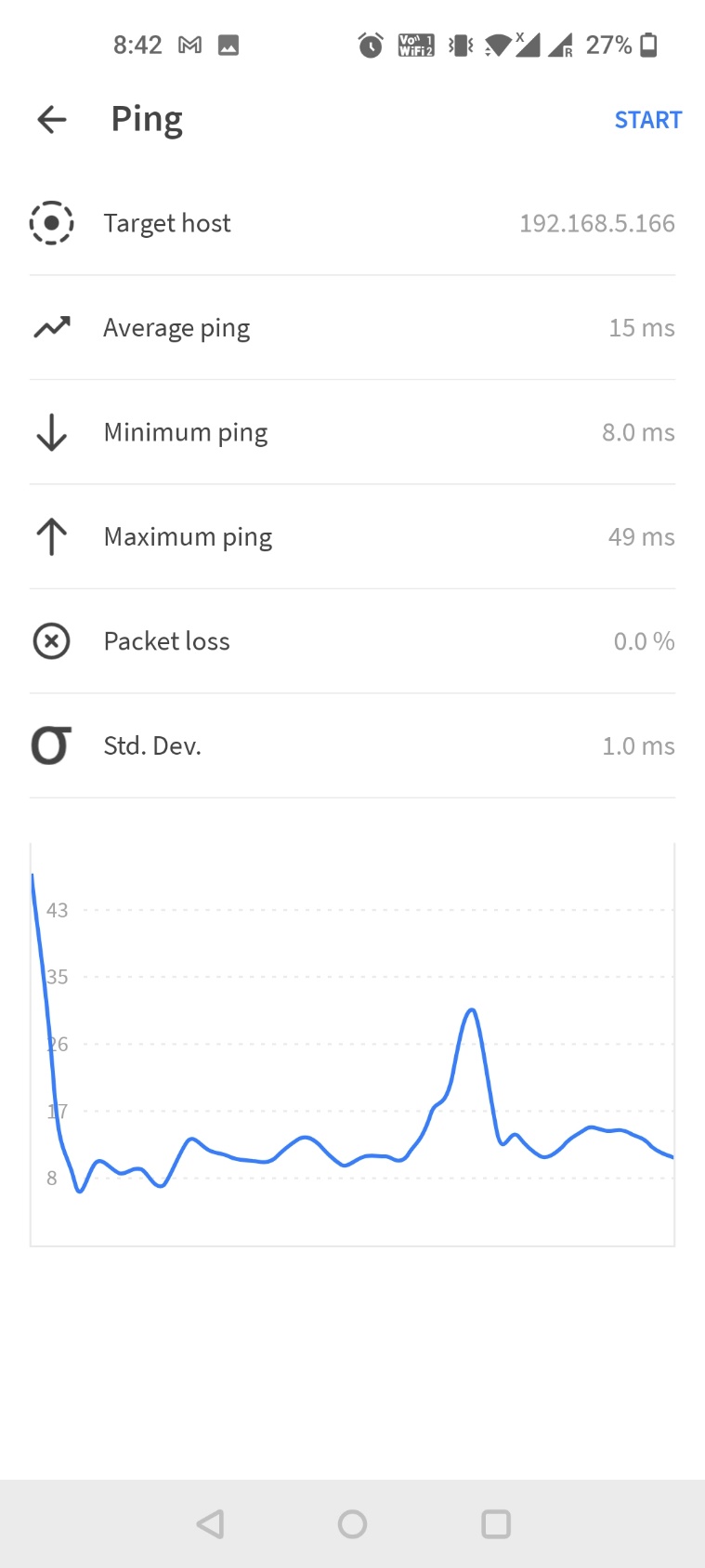
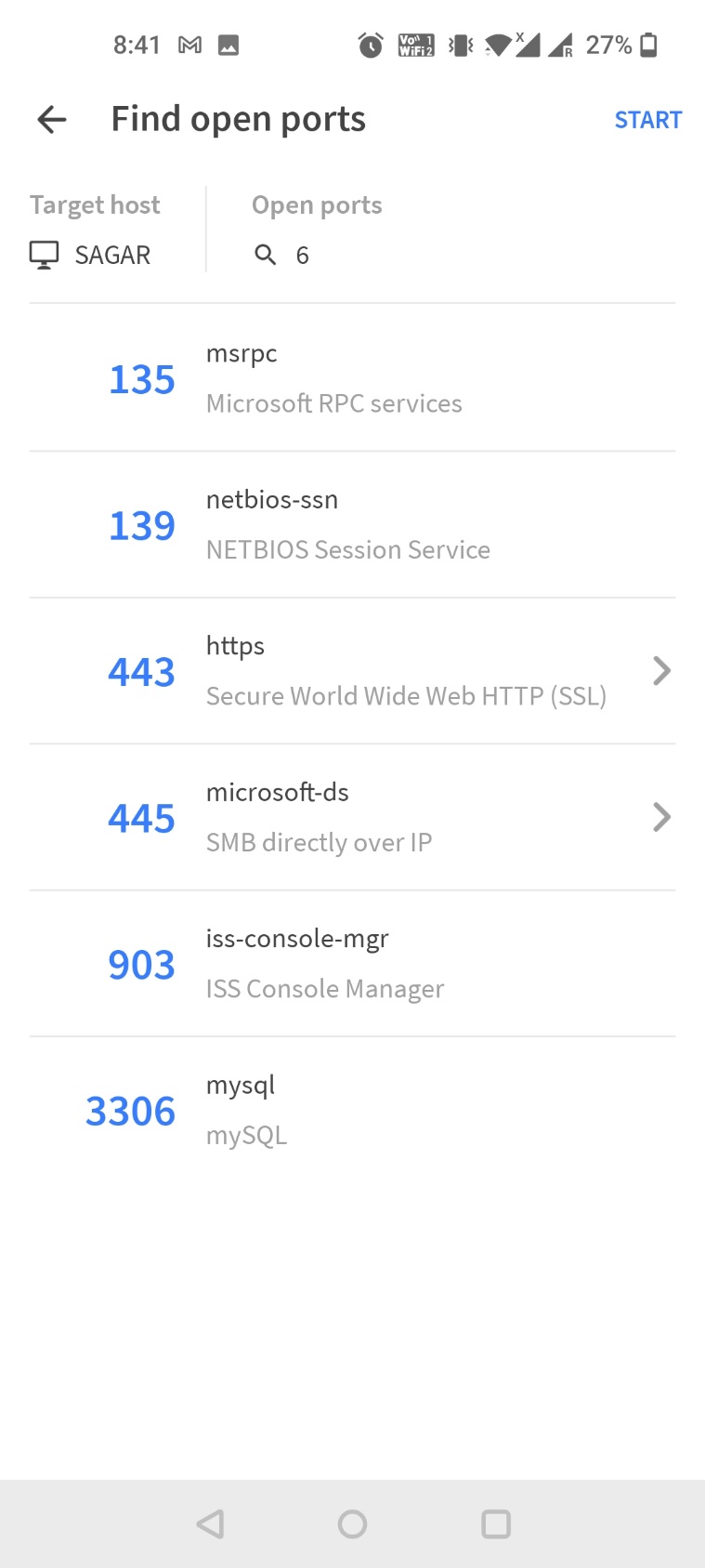
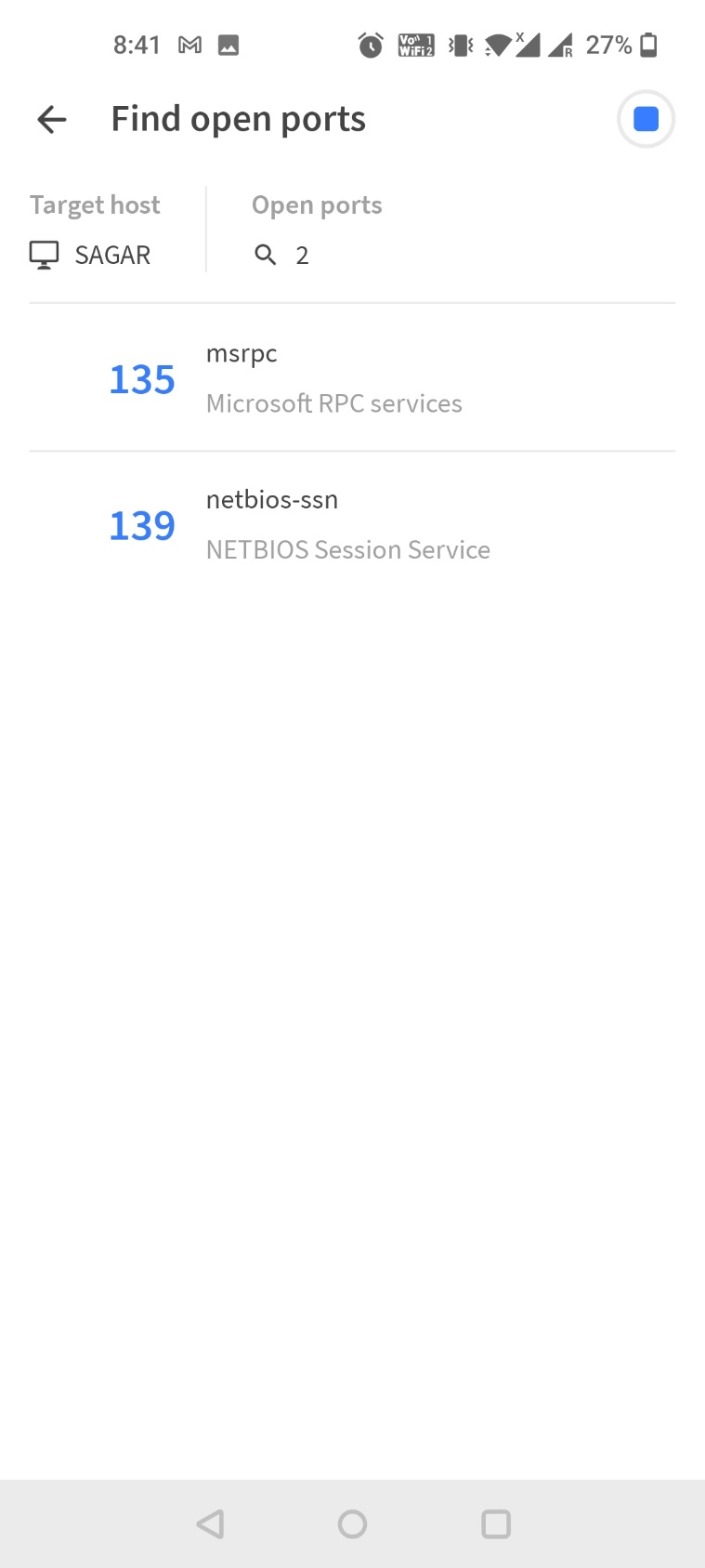
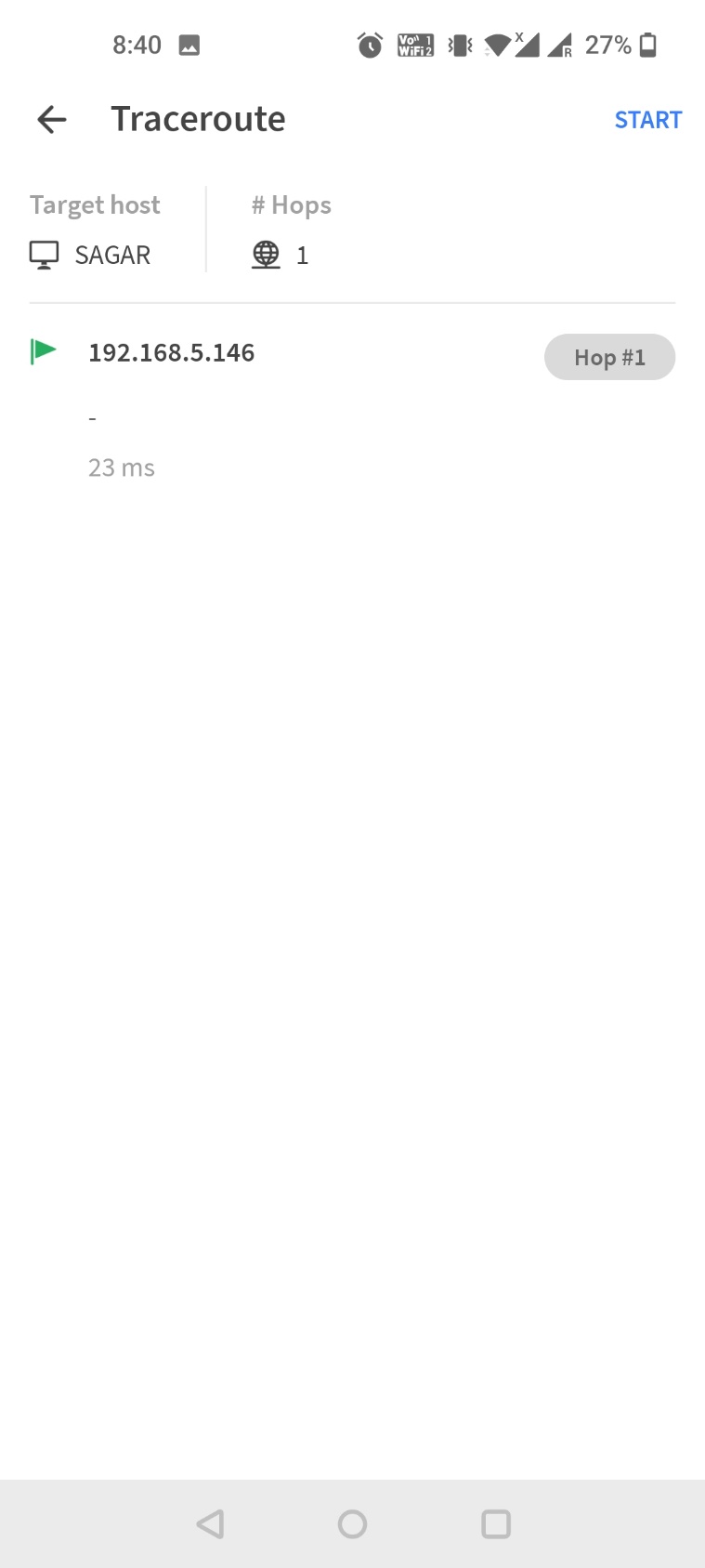
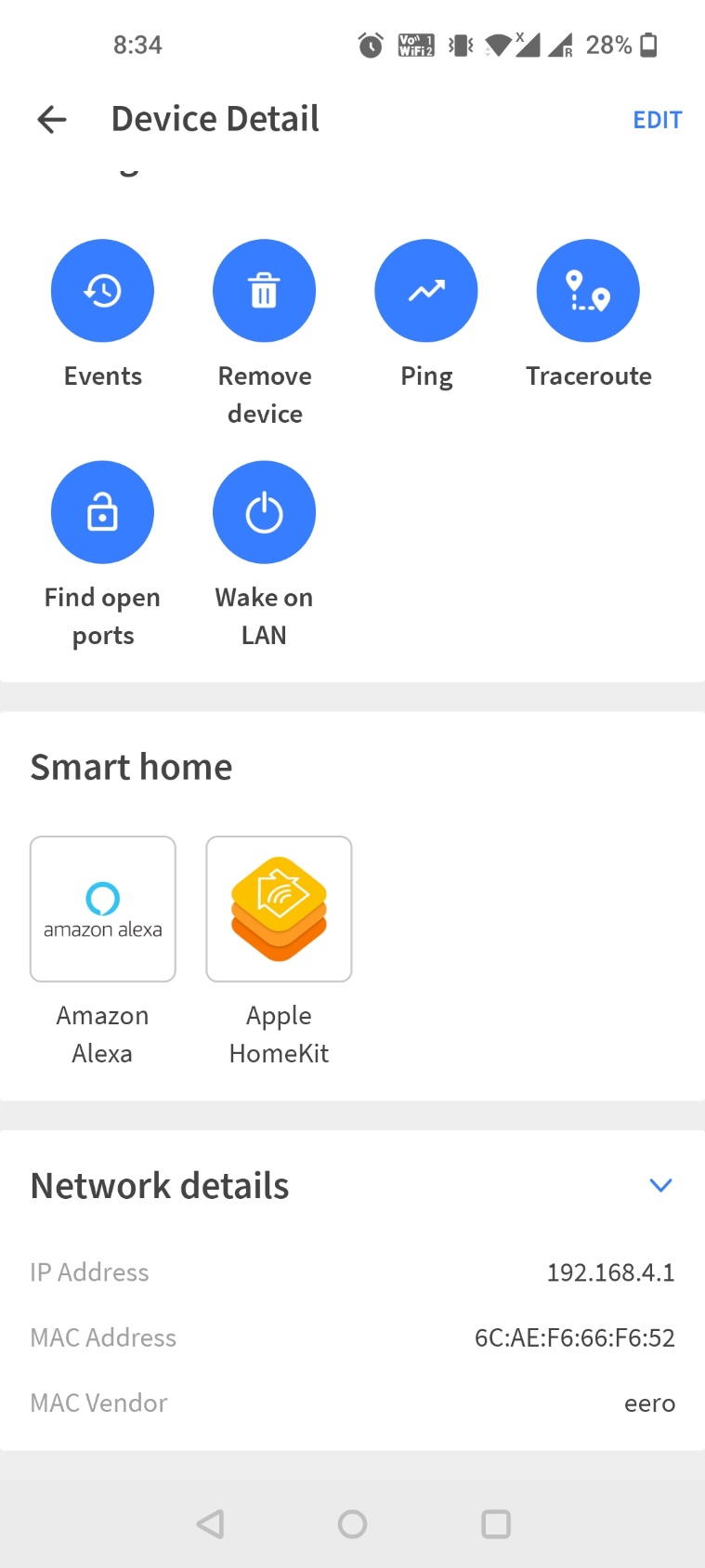


**Week 8 Lab Pt 3 – Use Fing to Scan a Wireless Network**

Fing is the Best Free Network IP Scanner for Securing Your Home Network. It is 100% free to scan IPs with Fing, and there are no ads. A beautifully designed network scanning app that is intuitive AND nice to look at it. It includes many features beyond network IP scanning and alerts. It always gives you the best network IP information that is available. It helps you identify intruders that are connected to your network

****

****

****

**Progress Embedded Image of Progress Report from LabSim:**

