Wardriving Project

Group #6: Vineetha, Dickson, Maurice Ayozie

Tim Fielder

November 20 2024

Group Members

We are group 6, consisting of:

- **Maurice Ayozie**: Driver
- **Dickson Houmbie**: War Driver
- **Vineetha Jasti**: Navigator

UTPB

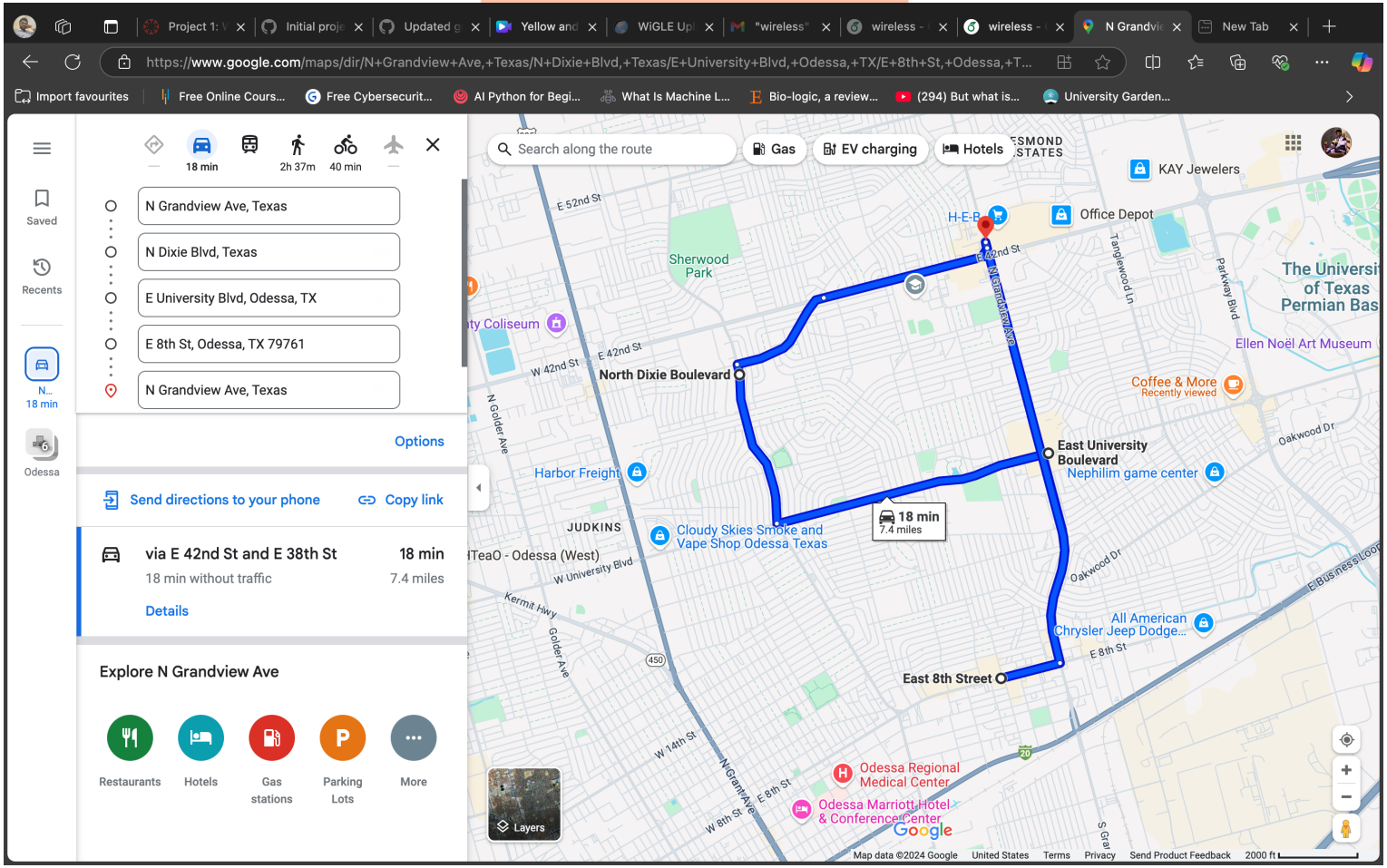
Geographic Location

Our group covered the area bounded by:

- N Grandview Ave to N Dixie Blvd
- E Uni Blvd to E 8th St

UTPB

Map of Area


https://www.google.com/maps/dir/N+Grandview+Ave,+Texas/N+Dixie+Blvd,+Texas/E+University+Blvd,+Odessa,+TX/E+8th+St,+Odessa,+T...
18 min
2h 37m
40 min
N Grandview Ave, Texas
N Dixie Blvd, Texas
E University Blvd, Odessa, TX
E 8th St, Odessa, TX 79761
N Grandview Ave, Texas
Options
Send directions to your phone
Copy link
via E 42nd St and E 38th St
18 min
18 min without traffic
7.4 miles
Details
Explore N Grandview Ave
Restaurants
Hotels
Gas stations
Parking Lots
More
Search along the route
Gas
EV charging
Hotels
KAY Jewelers
Office Depot
H-E-B
Sherwood Park
North Dixie Boulevard
East University Boulevard
Nephilim game center
Ellen Noël Art Museum
Coffee & More
Harbor Freight
Cloudy Skies Smoke and Vape Shop Odessa Texas
JUDKINS
18 min
7.4 miles
All American Chrysler Jeep Dodge...
East 8th Street
Odessa Regional Medical Center
Odessa Marriott Hotel & Conference Center
Layers
Map data ©2024 Google
United States
Terms
Privacy
Send Product Feedback
2000 ft

Description of Area

The area is composed of commercial places, Park , two elementry Schools, one middle school and Residential homes.

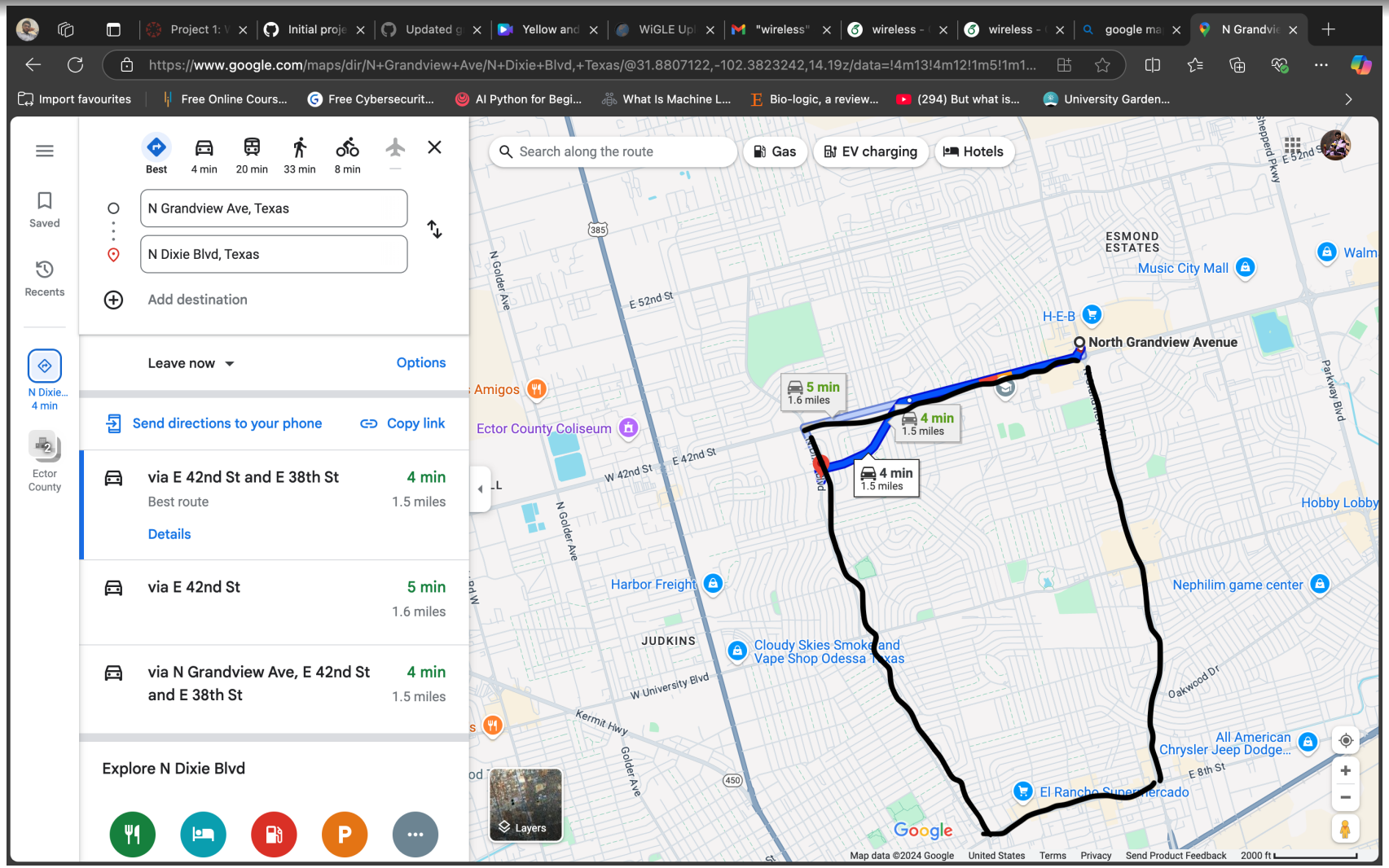
UTPB

Data

We found a total of 9197 access points, falling into the following broad categories:

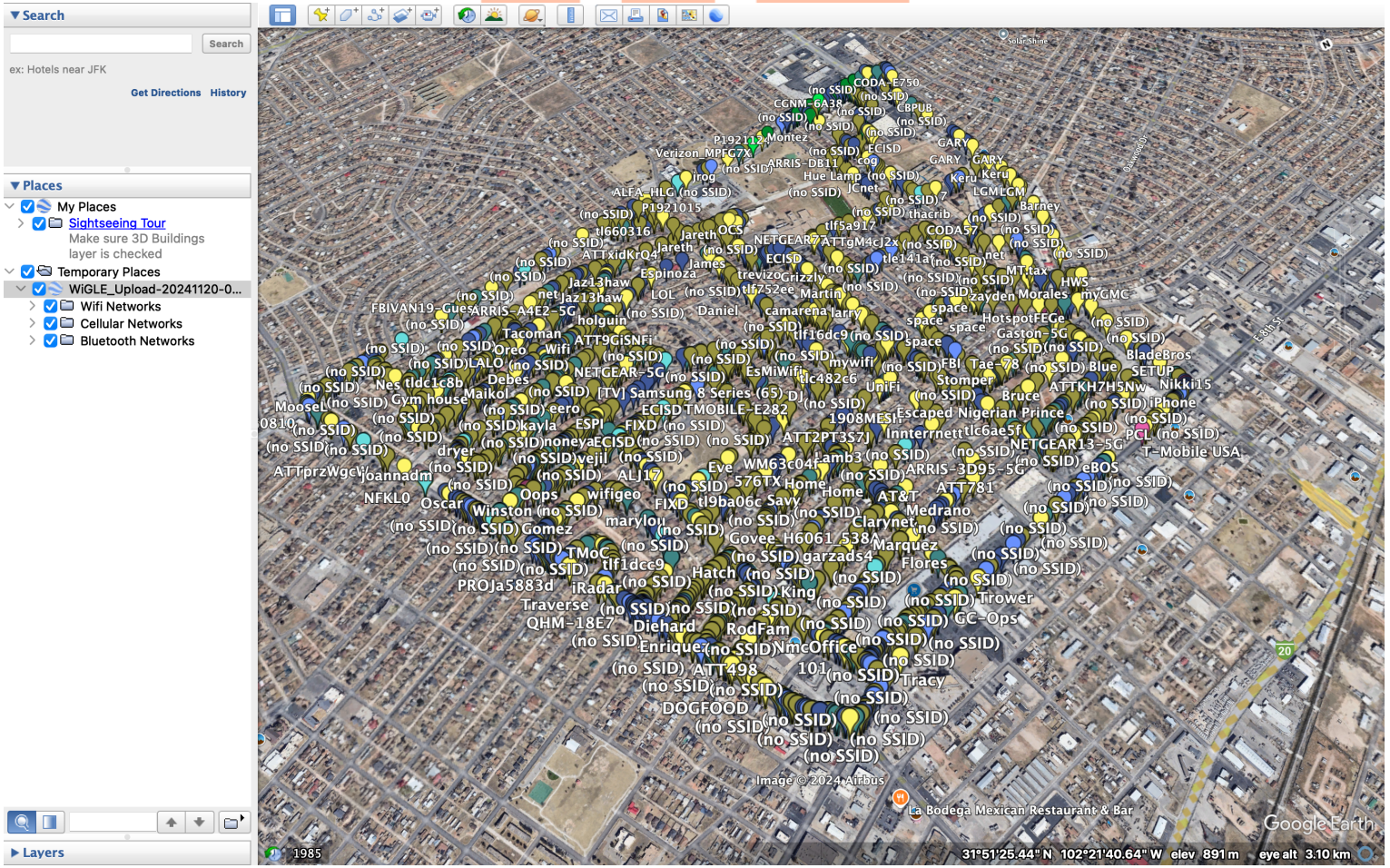
- Open: 2039
- WEP: 58
- WPA: 1
- WPA2: 5602
- WPA3: 820
- Unknown: 677

Map of APs

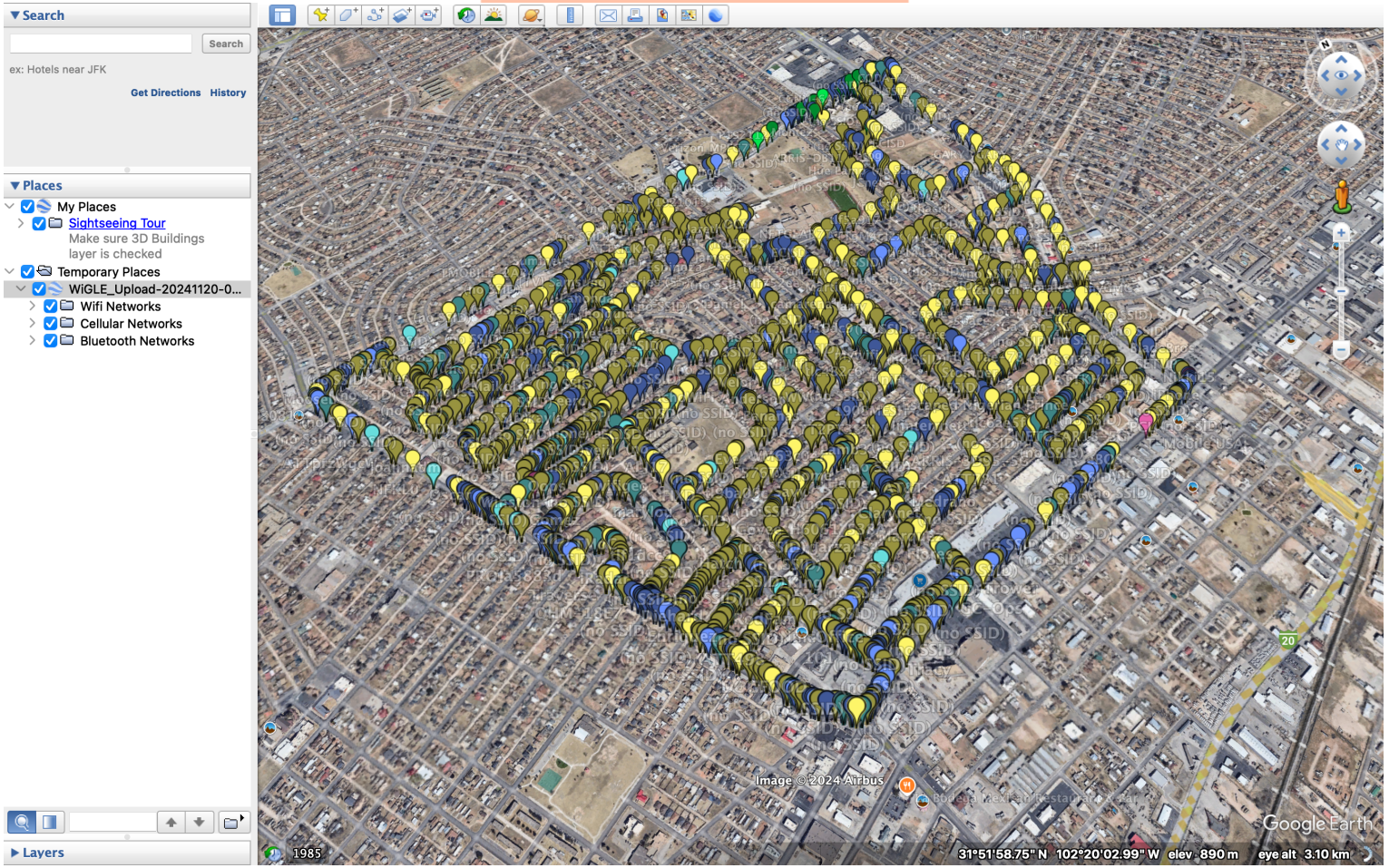

https://www.google.com/maps/dir/N+Grandview+Ave/N+Dixie+Blvd,+Texas/@31.8807122,-102.3823242,14.19z/data=!4m13!4m12!1m5!1m1...
Best
4 min
20 min
33 min
8 min
N Grandview Ave, Texas
N Dixie Blvd, Texas
Add destination
Leave now
Options
Send directions to your phone
Copy link
via E 42nd St and E 38th St
4 min
Best route
1.5 miles
Details
via E 42nd St
5 min
1.6 miles
via N Grandview Ave, E 42nd St and E 38th St
4 min
1.5 miles
Explore N Dixie Blvd
Search along the route
Gas
EV charging
Hotels
ESMOND ESTATES
Music City Mall
H-E-B
North Grandview Avenue
5 min
1.6 miles
4 min
1.5 miles
4 min
1.5 miles
Amigos
Ector County Coliseum
Harbor Freight
JUDKINS
Cloudy Skies Smoke and Vape Shop Odessa Texas
Nephilim game center
Hobby Lobby
All American Chrysler Jeep Dodge...
El Rancho Supermercado
Layers
Map data ©2024 Google
United States
Terms
Privacy
Send Product Feedback
2000 ft

All APs

These are all of the AP of our data which includes some unknown, Open,WEP and WPA/2/3



All APs


Search
Search
ex: Hotels near JFK
Get Directions
History
Places
My Places
Sightseeing Tour
Make sure 3D Buildings layer is checked
Temporary Places
WiGLE_Upload-20241120-0...
Wifi Networks
Cellular Networks
Bluetooth Networks
Layers
Image © 2024 Airbus
Google Earth
1985
31°51'58.75" N 102°20'02.99" W elev 890 m eye alt 3.10 km

Relevant Findings

- The majority of networks (approximately 75 percent) use WPA2, which indicates that most network administrators in the area are using industry-standard encryption. This is a positive trend in terms of security.
- About 11 percent of networks have adopted WPA3, reflecting a gradual move towards more secure technologies. However, further adoption is needed to enhance security across the board.
- The presence of 58 WEP networks and 1 WPA network highlights potential vulnerabilities in the area. These networks are susceptible to being compromised and may represent outdated systems.
- A significant proportion of networks fall into "Unknown" or "Other" categories. This suggests either incomplete data or the use of non-standard or unrecognized security measures.

What can someone do with this information?

- Unauthorized Network Access: Hackers can gain access to unsecured or poorly secured networks, allowing them to use the internet connection without permission
  - Data Theft: Once inside the network, attackers can access connected devices to steal sensitive information such as personal files, financial data, and login credentials
- Installing Malware: Hackers can install malware on devices connected to the compromised network, which can lead to further data breaches or control over the devices
  - Identity Theft: By accessing personal information, attackers can commit identity theft, using the stolen data to open accounts, make purchases, or engage in other fraudulent activities
- Brute-Force or Crack Encryption:
  - Illegal Activities: Attackers might use the compromised network to carry out illegal activities, making it difficult to trace the actions back to them
- Sniff Unencrypted Data
  - Hackers can use tools like Wireshark to capture transmitted data, revealing sensitive information like login credentials..
  - Perform Man-in-the-Middle (MITM) Attacks by Intercepting and

Questions