Adithya Rao Kalathur
Reg No: 200953015 Section: CCE-A
Roll no: 04 Group number: Group-1
Adithya Rao Kalathur

Camlin Page

FISAC - 1

Analysis of Cellular Network using Mobile App and Sniffer

a) Write the steps to generate and capture the mobile data packets (http) using any sniffer tool.

Answer:

To generate and capture mobile data packets we will use PCAPdroid app. PCAPdroid is a privacy-friendly programme which helps you track and analyse the connections established by the other apps in your device. It also allows you to export a PCAP dump of the traffic, analyse HTTP, decrypt TLS communication & much more. PCAPdroid replicates a VPN to record network traffic without requiring root access. It processes data locally on the device rather than using a remote VPN server.

To capture a packet we need to open the app first and then press ready to capture the packets.

The app also shows the stats of the data like bytes sent, Bytes received, Packet sent, Packet received, active connections etc.

It also has a log area which shows when the packet loop was started, when packet loop was stopped etc.

Once we are done capturing the packet we need to press the stop button & once the stop button is pressed a PCAP file is created. The PCAP file can be transferred to a laptop/PC where we can use software like wireshark to analyze the captured packet. The steps to analyze the packets using wireshark are -

1) Capture packets: Start a packet capture in wireshark and select the network interface that you want to capture traffic on.

2) Filter Packets: use a display filter to only show HTTP traffic in the packet list. you can do this by typing "http" into the filter bar at the top of the wireshark window.

3) Analyze packet details: Click on a HTTP packet to view it's details in the packet details pane, The HTTP packet will be broken down into several sub-protocols such as TCP, IP, and HTTP.

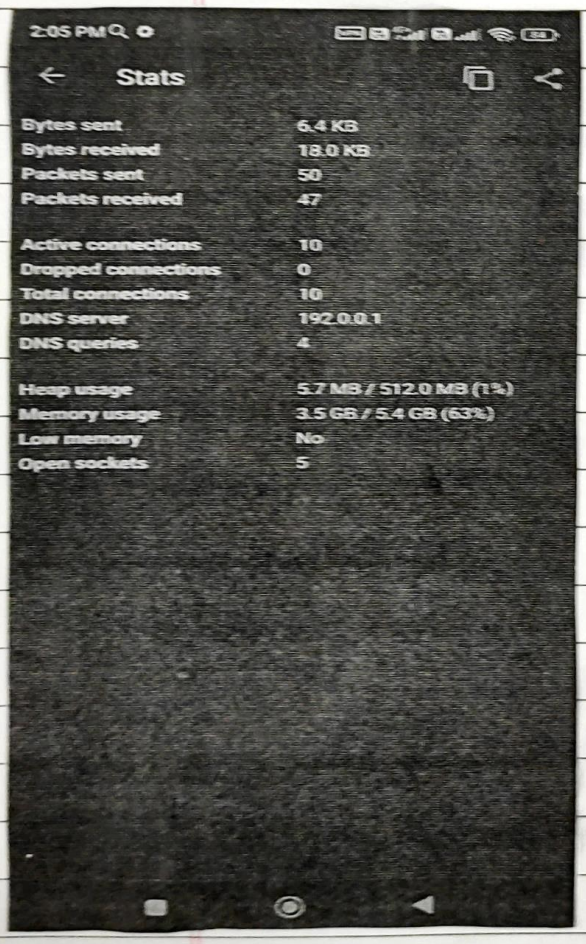
4) View HTTP headers: Expand the HTTP portion of the packet details pane to view the HTTP headers. This will give you details about the HTTP request & response, such as the URL requested, status codes, & cookies.

5) Follow HTTP Streams: If you want to view the entire conversation between the client & the server, you can follow the HTTP stream. To do this, right-click on an HTTP packet & select "Follow -> HTTP stream" This will show you the entire HTTP conversation in a separate window.

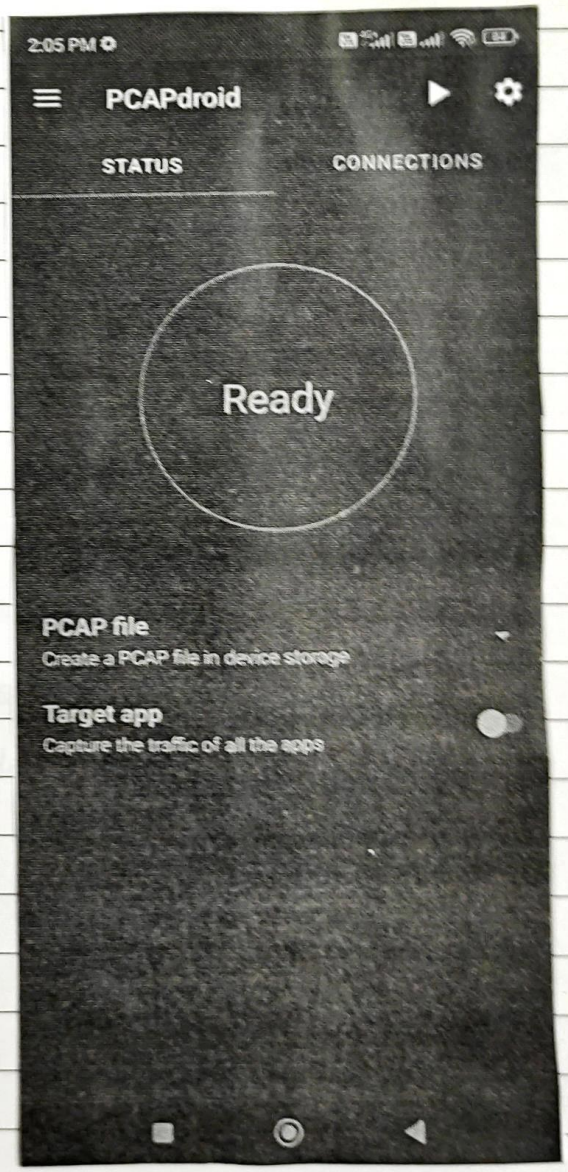
6) Decode HTTP content: wireshark can decode HTTP content, such as HTML, images & other files. If you want to see the actual content

of an HTTP request or response, right click on the packet & select "Follow -> HTTP Stream", then select the "Save As" button to save the content as a file.

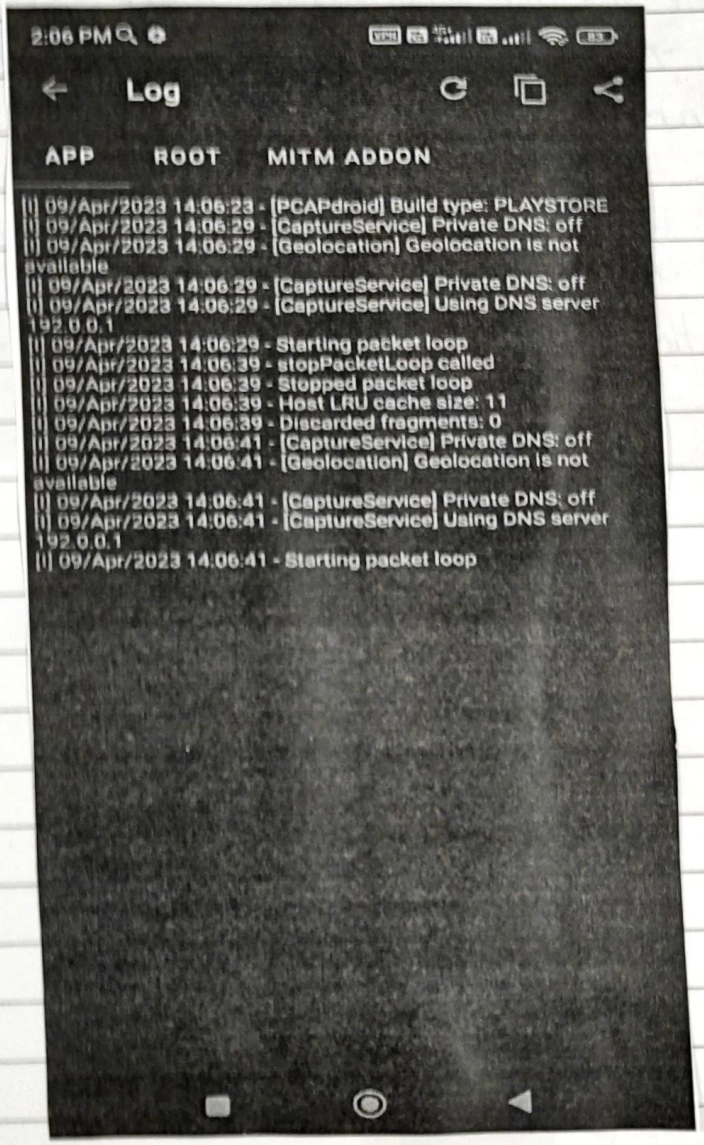
7) Analyze HTTP performance: Wireshark can also help you to analyze HTTP performance by showing you metrics such as response time & transfer rate. To see these metrics, go to "Statistics -> HTTP -> Packet Counter", & select the desired metric.



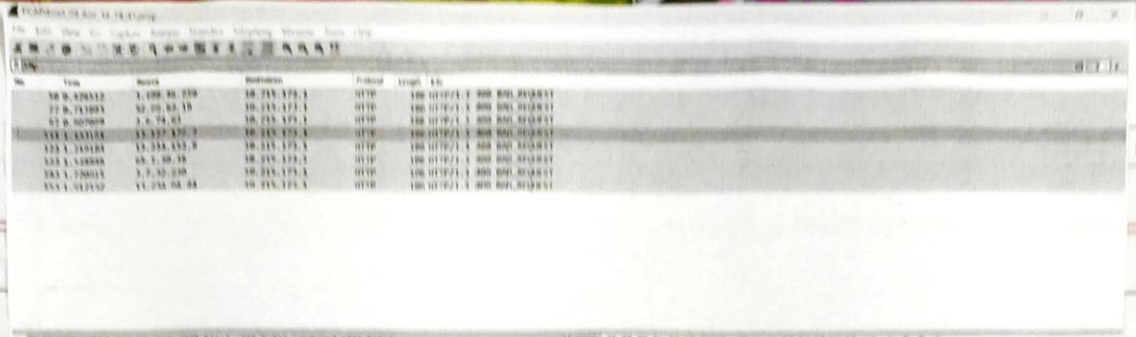
Statistics Tab

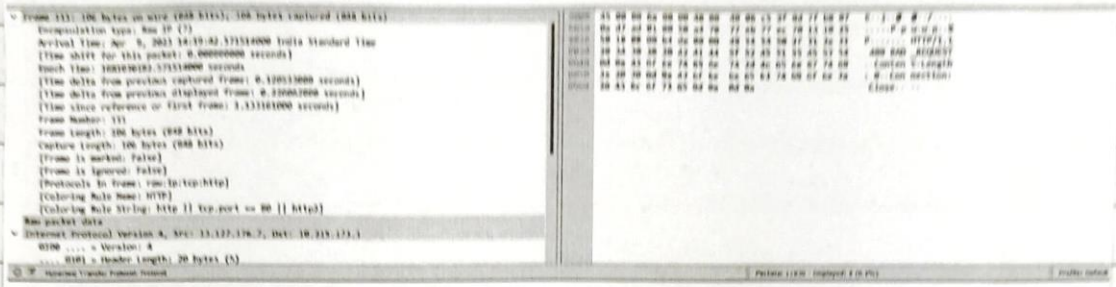


Status Tab of PCAPdroid



Log tab of Pcapdroid





Pcap file in wireshark

Wireshark · Packet Counter · PCAPdroid_09_Apr_14_19_41.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	10				0.0003	100%	0.0100	0.427
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	8				0.0002	80.00%	0.0100	0.427
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	8				0.0002	100.00%	0.0100	0.427
400 Bad Request	8				0.0002	100.00%	0.0100	0.427
3xx: Redirection	0				0.0000	0.00%	-	-
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	2				0.0001	20.00%	0.0100	32.711
SEARCH	2				0.0001	100.00%	0.0100	32.711

Display filter: Apply

Copy Save as... Close

wireshark packet contents

```
Frame 50: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
    Encapsulation type: Raw IP (7)
    Arrival Time: Apr  9, 2023 14:19:41.864865000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1681030181.864865000 seconds
    [Time delta from previous captured frame: 0.021655000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.426512000 seconds]
    Frame Number: 50
    Frame Length: 106 bytes (848 bits)
    Capture Length: 106 bytes (848 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Raw packet data
```

b) Study the mobile App and write a detail note on fechures of the tool with specific terms Ex: Signal strength, channel, data & rate, latency (Follow of the content should be proper with screenshots).

Answer:

The Android app call Signal Monitor is a specialist tool for monitoring GSM, UMTS, & LTE network conditions. This network monitor is helpful if you wish to examine change dynamics of the strength level of nearby base transceiver stations (BTS); create statistics on cell usage; examine the speed of the incoming & outgoing connection; make a cell ID log; display BTS locations (after importing a special CLF file); & verify the speed of the connection.

3 tabs make up the user interface: overview, strength chart, & speed chart. Swiping or clicking on tab titles will choose them. Statistics, log & Database Managers are accessible through the menu. A background service measures the parameters of the network. By selecting the button in the application's top bar, you can start or stop it. While background service is active, an icon is displayed in the notification area.

Overview tab:

The first tab contains information about cellular network, connection speed, the serving cell, & neighbouring cells. It provides information about -

- State of radio unit;
- name of current mobile operator;

- Mobile country code (MCC);
- Mobile network code (MNC);
- current network type (GPRS/EDGE/UMTS/HSPA/HSDPA/HSUPA/LTE);
- roaring indicator;
- Speed of incoming & outgoing connection;
- Cell identifier (CID);
- Location Area Code (LAC) - for GSM/UMTS networks;
- Tracking Area Code (TAC) - for LTE networks;
- Radio Network controller (RNC) - for UMTS networks
- Received signal strength indication (RSSI);
- Reference Signals Received power (RSRP) - for LTE networks.

Each cell identifier is given a colour by the application. Charts in other app tabs use this colour. A coloured bar shows the signal strength. Signal intensity varies between -113dBM (low power) & -50 dBM (high power) in GSM & UMTS networks, & between -140 dBM & -50 dBM in LTE networks. In GPRS & UMTS networks, the app provides information about nearby cells. Nevertheless due to firmware restrictions, certain devices are unable to display this information.

Strength chart tab:

It displays the changes of received signal strength (RSSI). Line colours correspond to the colors of cell IDs in the previous tabs. The chart updates every second chart can be saved as PNG or file in SD card folder specified in the app preferences.

P.T.O.

Camlin Page

Speed chart tab:

This tab contains charts of upload & download speed. The speed is measured for GSM / UMTS / LTE networks. If Wi-Fi is on the charts will be empty because no data is transmitted via cellular network. The image of charts can be saved as PNG files in a folder specified in the app preferences.

Log tab:

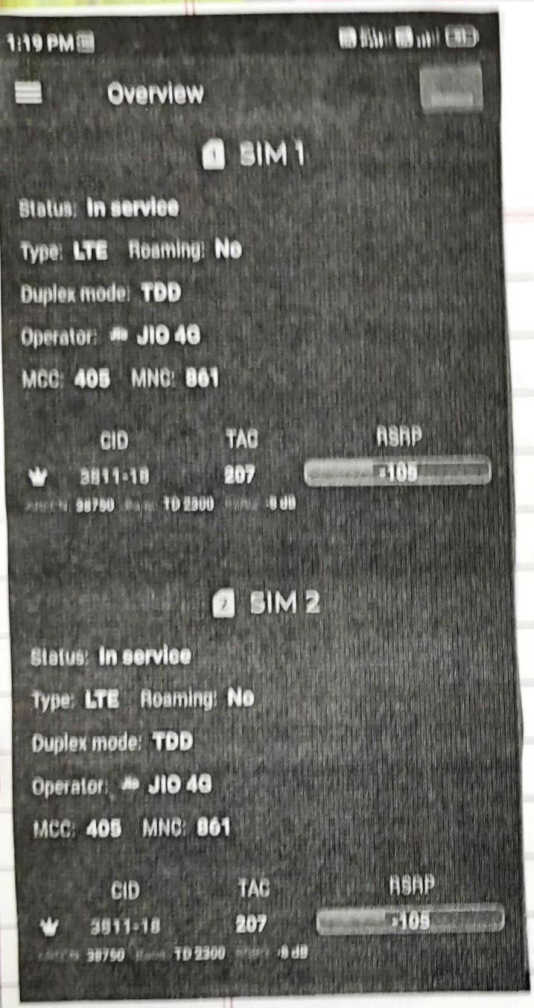
Log displays the data about serving cells used by the phone. It also contains entries about radio unit states changes. Log entries can be saved as CSV file in a folder specified in the app preferences

Statistics tab:

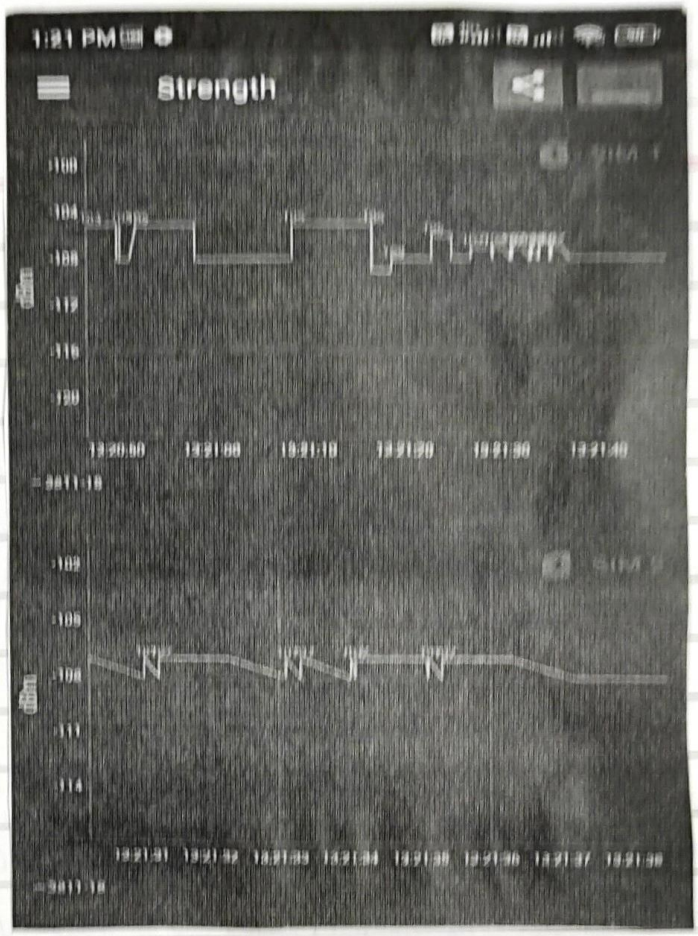
This window displays a statistics of all usage. The period of time can be set in preferences. Color of diagram sector corresponds to the color of cell ID in the overview tab.

DB Manager tab:

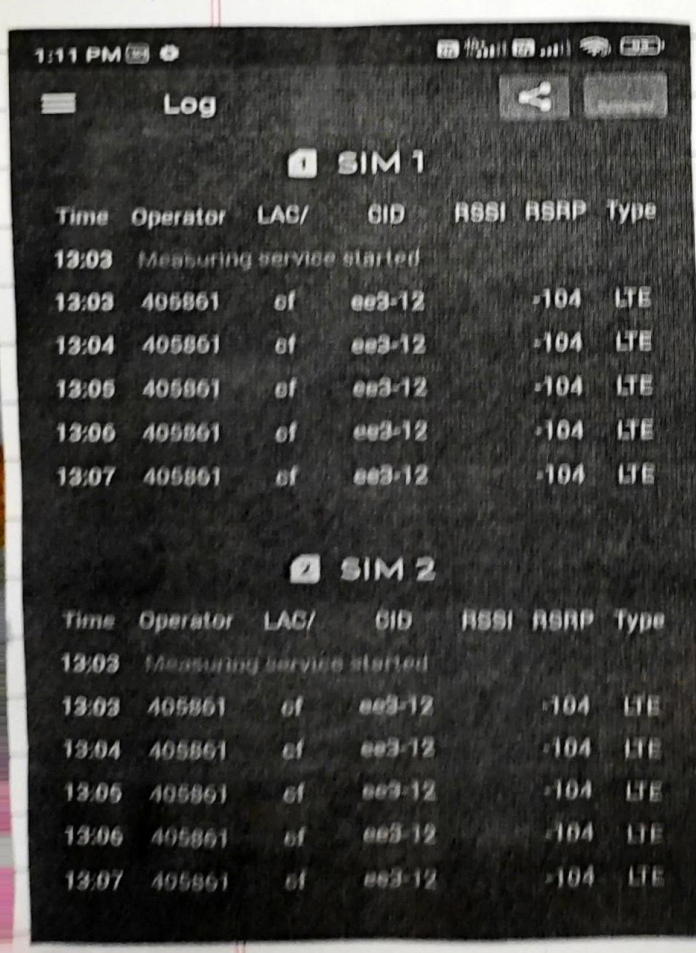
Database Manager allows to control information about signal strength measurements & cell locations data



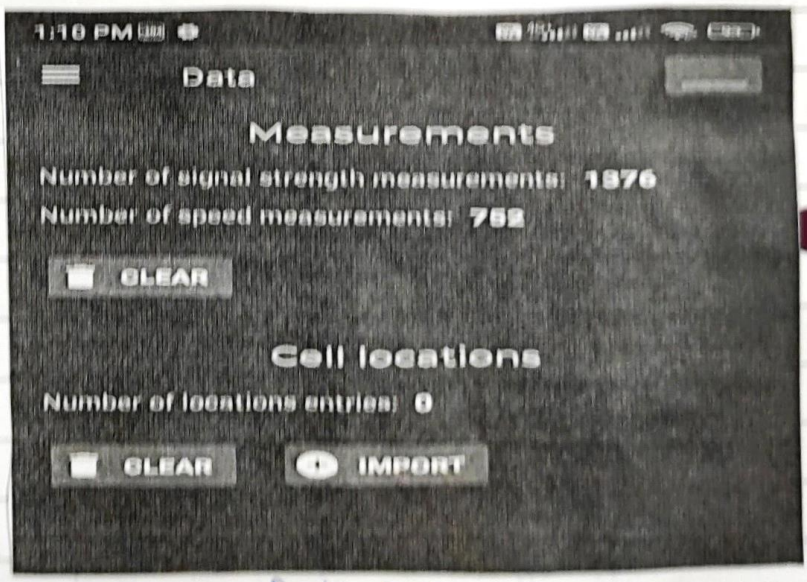
Overview Tab



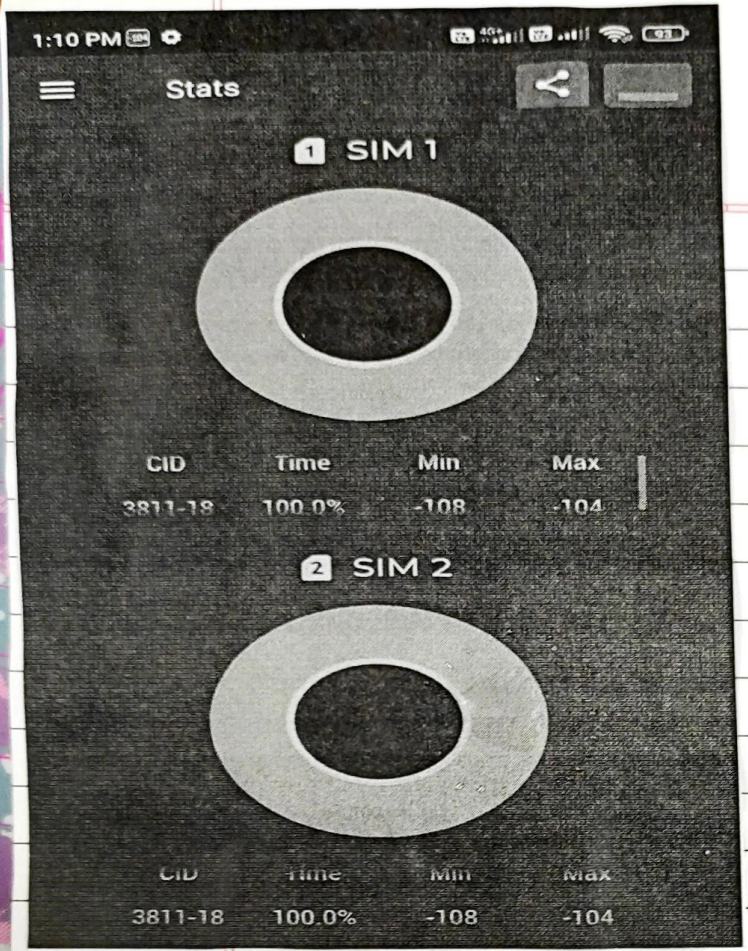
Strength tab



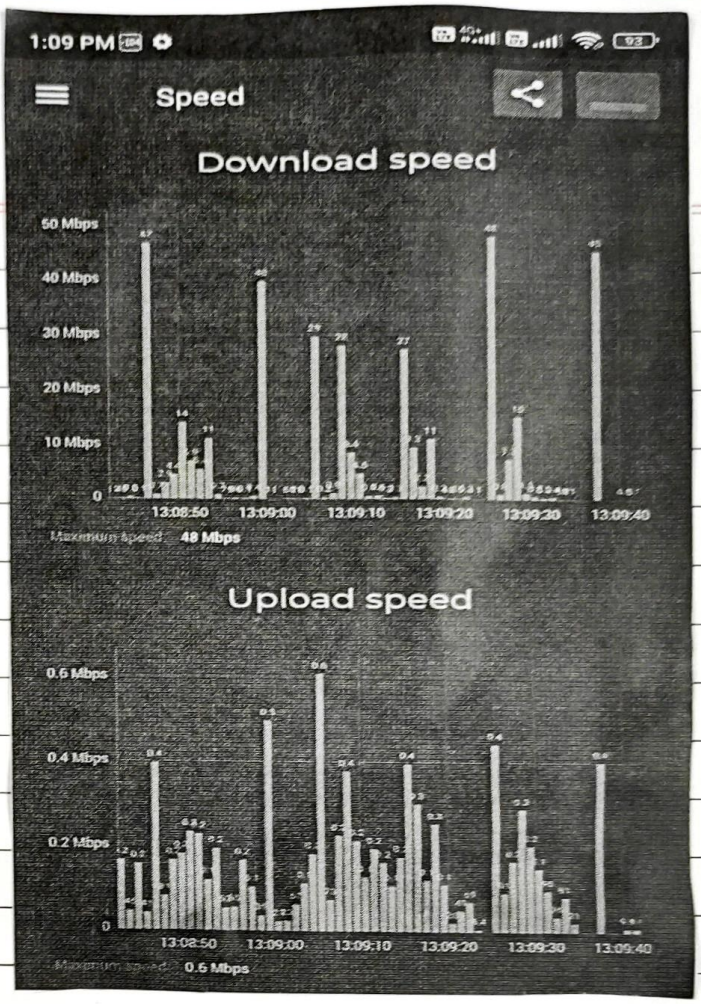
Log tab



Data tab



Status tab of cell signal monitor



Speed tab of cell signal monitor