Lê Ngọc Kiều Anh - 22520047

Nhóm có 3 bạn:

Phùng Việt Bắc - 22520089

Trần Phước Đại - 22520284

**BÀI TẬP AN TOÀN MẠNG MÁY TÍNH BUỔI 13**

**Câu 1. Cài đặt 2 công cụ khám phá mạng không dây. Phân tích các mạng trong phạm vi mạng xung quanh.**

1. ***Công cụ inSSIDer:***

**Quét các mạng Wi-Fi xung quanh:**

inSSIDer sẽ hiển thị danh sách các mạng Wi-Fi trong phạm vi, bao gồm:

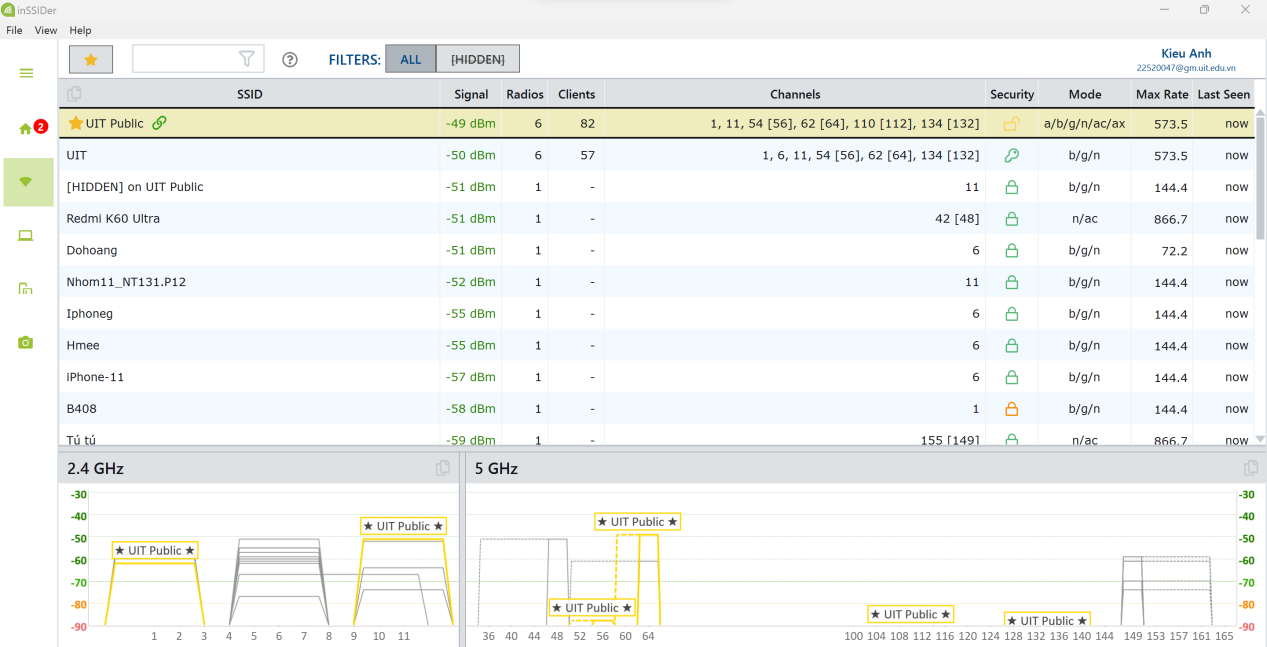
**SSID:** Tên của mạng WiFi

**BSSID:** Địa chỉ MAC của Access Point (AP)

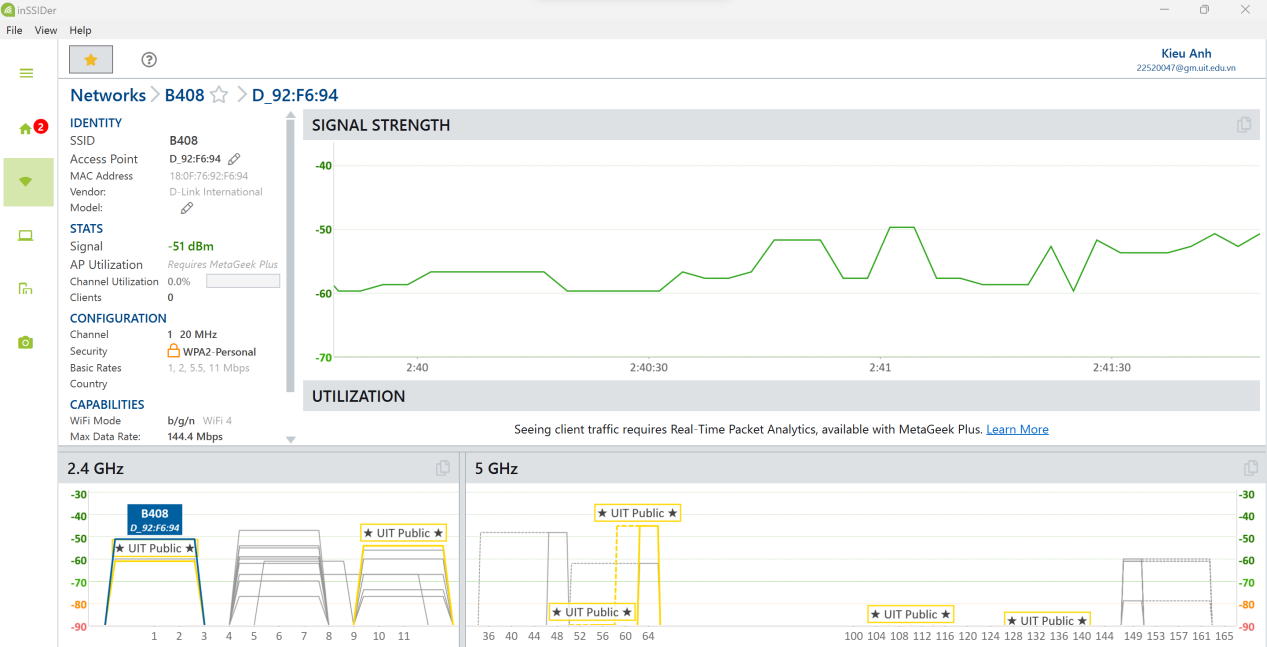
**RSSI:** Cường độ tín hiệu (dBm)

**Channel:** Kênh hoạt động của từng mạng

**Security:** Loại mã hóa (WEP, WPA/WPA2)

****

**Phân tích 1 mạng trong các mạng đã quét:** chọn mạng B408

****

1. Thông tin cơ bản của mạng B408

- SSID: Tên mạng WiFi là B408

- Access Point (AP): Địa chỉ MAC là D:92:F6:94

2. Thống kê tín hiệu và cấu hình

Cường độ tín hiệu (Signal):

- Giá trị -51 dBm: Tín hiệu này khá mạnh. Cường độ tín hiệu tốt thường nằm trong khoảng từ -30 dBm đến -50 dBm.

- AP Utilization: Không có thông tin về việc sử dụng AP (0% Channel Utilization).

Channel:

- Mạng này đang sử dụng Channel 1 (20 MHz) trong băng tần 2.4 GHz.

- Bảo mật (Security): Mạng này sử dụng mã hóa WPA2-Personal, đảm bảo mức độ bảo mật cao.

3. Đánh giá tổng thể mạng WiFi xung quanh (2.4 GHz và 5 GHz)

***Băng tần 2.4 GHz***

Các kênh được sử dụng:

- B408 đang sử dụng kênh 1.

- Các mạng khác như UIT Public đang sử dụng kênh 6 và 11.

Cường độ tín hiệu:

- B408 có tín hiệu mạnh nhất ở -51 dBm.

- UIT Public cũng có tín hiệu tương đối mạnh nhưng kênh của chúng không trùng với mạng B408.

***Băng tần 5 GHz***

- UIT Public hoạt động trên nhiều kênh khác nhau như 36, 52, 60, 64, 136, 149, nhưng không có sự xung đột đáng kể với B408 vì B408 chỉ hoạt động trên 2.4 GHz.

- Mật độ sử dụng ở băng tần 5 GHz thấp hơn, cải thiện hiệu suất và giảm nhiễu.

1. ***Công cụ Netsurveyor:***

**Quét các mạng Wi-Fi xung quanh:**

Sau khi quét xong, các mạng Wi-Fi sẽ hiển thị với các thông tin chi tiết như:

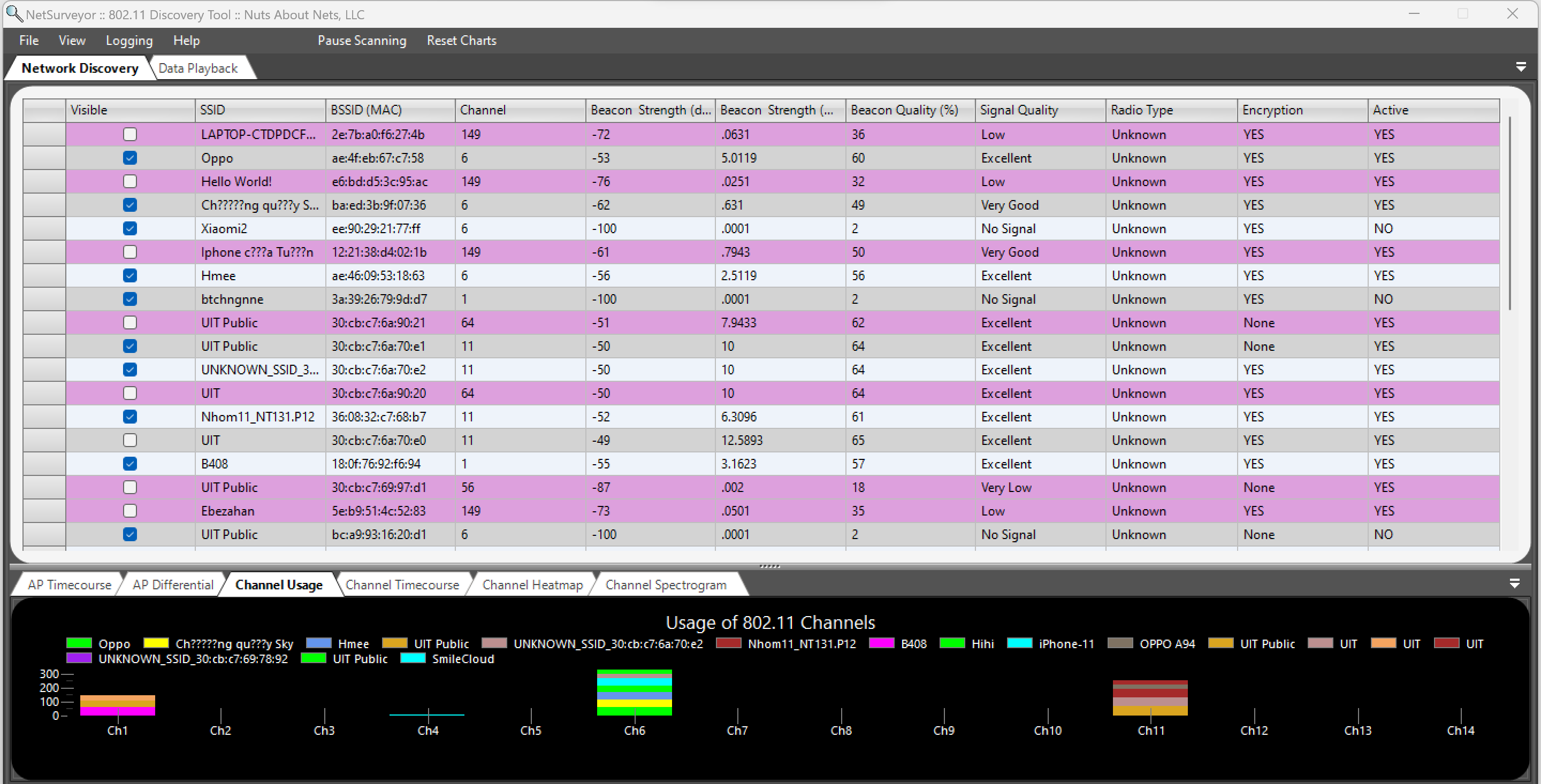
**SSID** (Tên mạng).

**Channel** (Kênh sóng Wi-Fi).

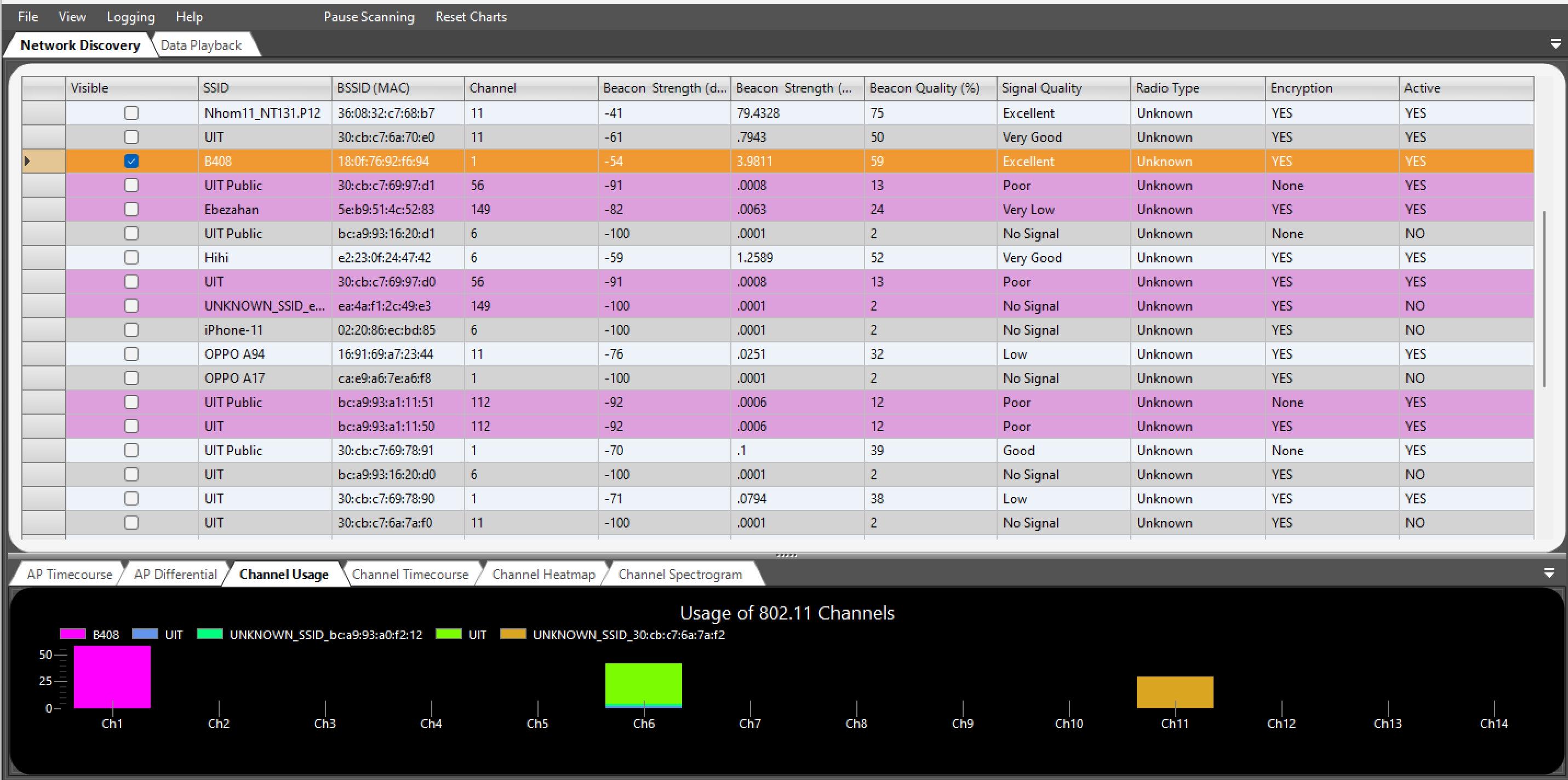
**Signal Strength** (Cường độ tín hiệu).

**Encryption** (Loại mã hóa, ví dụ WPA2).

**MAC Address** (Địa chỉ MAC của Access Point)

****

**Phân tích 1 mạng trong các mạng đã quét:** chọn mạng B408

****

**Bảng Network Discovery với các thông tin:**

**Visible:** Hiển thị dấu chọn cho các mạng đang được quét và giám sát.

Ví dụ: SSID "B408" đã được chọn.

**SSID:** Tên của các mạng Wi-Fi được phát hiện.

Ví dụ: "UIT", "B408", "Nhom11\_NT31.P12", "OPPO A94".

**BSSID (MAC):** Địa chỉ MAC của từng Access Point (AP).

Ví dụ: "18:0f:76:92:6f:94" là BSSID của mạng "B408".

**Channel:** Kênh mà từng mạng đang sử dụng.

Ví dụ:

"Nhom11\_NT31.P12" và "UIT" sử dụng kênh 11.

"UIT Public" sử dụng kênh 56 và 112.

"B408" sử dụng kênh 1.

**Beacon Strength (dBm):** Độ mạnh của tín hiệu beacon từ Access Point, đơn vị tính bằng dBm. Các giá trị âm càng gần 0 thì tín hiệu càng mạnh.

Ví dụ:

"Nhom11\_NT31.P12": -41 dBm (tín hiệu mạnh).

"B408": -54 dBm (tốt).

"UIT Public" trên kênh 112: -92 dBm (rất yếu).

**Beacon Quality (%):** Chất lượng tín hiệu được tính theo phần trăm.

Ví dụ:

"Nhom11\_NT31.P12" có chất lượng tín hiệu 75%.

"B408" có 59%.

**Signal Quality:** Đánh giá chất lượng tín hiệu theo thang mô tả: Excellent, Very Good, Poor, Low, hoặc No Signal.

Ví dụ:

"Nhom11\_NT31.P12" có chất lượng tín hiệu Excellent.

"UIT Public" có tín hiệu Poor hoặc No Signal.

**Radio Type:** Loại sóng vô tuyến, tuy nhiên trong hình ảnh này đều hiển thị là Unknown.

**Encryption:** Cho biết mạng có được mã hóa bảo mật không.

Ví dụ:

"UIT Public" ở kênh 56 không có mã hóa (None).

"B408" và "UIT" có mã hóa (YES).

**Active:**

Cho biết mạng có đang hoạt động hay không.

Ví dụ:

Một số mạng như "OPPO A94" và "UNKNOWN\_SSID\_e…" có trạng thái NO.

**Biểu đồ Channel Usage sử dụng các kênh tần số 802.11:**

**Ch1:** Kênh 1 đang có mạng "B408" chiếm dụng với tín hiệu mạnh (màu hồng và nổi bật).

**Ch6:** Kênh 6 có mạng "UNKNOWN\_SSID\_bca:93:a0:f2:12" chiếm dụng (màu xanh lá cây).

**Ch11:** Kênh 11 có nhiều mạng cùng chia sẻ: "UIT" và "Nhom11\_NT31.P12" (màu vàng).

**Phân tích:**

- Kênh 1, 6, và 11 là các kênh phổ biến trên băng tần 2.4 GHz.

- Kênh 11 có dấu hiệu bị quá tải khi nhiều mạng cùng hoạt động.

- Kênh 1 (B408) có tín hiệu tốt nhất và ít xung đột.

**Câu 2. Cài đặt công cụ phân tích mạng như Pilot, OmniPeek,…nêu cách sử dụng.**

**Câu 3. Cho biết công dụng các tool trong bộ Aircrack-ng Suite.**

|  |  |  |
| --- | --- | --- |
| **Công cụ** | **Chức năng** | **Nhóm chức năng** |
| **Airbase-ng** | Thu thập WPA/WPA2 handshake và hoạt động như một điểm truy cập giả lập (ad-hoc AP). | Tấn công và giả lập AP |
| **Aircrack-ng** | Công cụ crack mật khẩu WEP và WPA/WPA2-PSK. | Cracking mật khẩu |
| **Airdecap-ng** | Giải mã WEP/WPA/WPA2 và loại bỏ phần header không dây từ các gói tin WiFi. | Giải mã gói tin |
| **Airdecloak-ng** | Xóa WEP cloaking từ file pcap. | Xử lý gói tin |
| **Airdriver-ng** | Cung cấp thông tin trạng thái về các driver không dây trên hệ thống. | Quản lý driver |
| **Airdrop-ng** | Thực hiện deauthentication các client có mục tiêu dựa trên quy tắc. | Tấn công ngắt kết nối |
| **Aireplay-ng** | Tạo lưu lượng, xác thực giả mạo, replay gói tin, và injection yêu cầu ARP. | Tấn công injection |
| **Airgraph-ng** | Tạo mối quan hệ giữa client và AP từ dữ liệu của Airodump-ng. | Phân tích và hiển thị dữ liệu |
| **Airodump-ng** | Bắt gói tin thô của 802.11 và thu thập IVs WEP. | Bắt gói tin và giám sát |
| **Airolib-ng** | Lưu trữ và quản lý danh sách ESSID và mật khẩu dùng để crack WPA/WPA2. | Quản lý dữ liệu crack |
| **Airserv-ng** | Cho phép nhiều chương trình sử dụng card WiFi độc lập qua kết nối TCP client-server. | Quản lý card mạng |
| **Airmon-ng** | Chuyển card mạng không dây sang chế độ monitor và ngược lại. | Chế độ monitor |
| **Airtun-ng** | Chèn lưu lượng vào mạng WPA TKIP và phục hồi MIC key từ lưu lượng WiFi. | Tấn công và chèn lưu lượng |
| **Easside-ng** | Giao tiếp với AP mã hóa WEP mà không cần biết key. | Khai thác WEP |
| **Packetforge-ng** | Tạo các gói tin được mã hóa để sử dụng trong việc injection. | Tạo gói tin |
| **Tkiptun-ng** | Tạo đường hầm ảo để theo dõi và chèn lưu lượng vào mạng được mã hóa. | Tấn công TKIP |
| **Wesside-ng** | Kết hợp nhiều kỹ thuật để thu thập key WEP nhanh chóng. | Khai thác WEP |

**Câu 4. Mô tả các bước thực hiện việc crack mật khẩu mạng wifi với bộ công cụ mạng Aircrack-ng.**

**- Bước 1. Bật chế độ monitor cho card mạng**

Sử dụng Airmon-ng để chuyển card WiFi sang chế độ monitor:

***airmon-ng start wlan0***

**- Bước 2. Quét và thu thập thông tin mạng**

Dùng Airodump-ng để quét và thu thập thông tin mạng WiFi:

***airodump-ng wlan0mon***

Ghi lại thông tin về BSSID và kênh của mạng mục tiêu.

**- Bước 3. Thu thập gói tin**

Dùng Airodump-ng để thu thập gói tin của AP mục tiêu:

***airodump-ng -c [channel] --bssid [BSSID] -w [output\_file] wlan0mon***

**- Bước 4. Tạo lưu lượng để ép client gửi gói tin**

Sử dụng Aireplay-ng để ép client gửi gói tin hoặc deauth client:

***aireplay-ng --deauth 0 -a [BSSID] wlan0mon***

**- Bước 5. Crack mật khẩu với Aircrack-ng**

Sau khi thu thập đủ gói tin, dùng Aircrack-ng để crack mật khẩu:

***aircrack-ng -w [wordlist.txt] [capture\_ file.cap]***

**Câu 5. Trình bày các biện pháp phòng chống tấn công mạng wifi.**

* Sử dụng mã hóa mạnh: Dùng chuẩn WPA3 hoặc tối thiểu là WPA2 với mật khẩu mạnh và phức tạp.
* Thay đổi SSID mặc định: Đặt tên SSID mới để tránh bị tấn công do các cấu hình mặc định.
* Bật tính năng MAC Filtering: Chỉ cho phép các thiết bị có MAC được phép kết nối vào mạng.
* Tắt WPS (Wi-Fi Protected Setup): WPS dễ bị tấn công brute force và cần tắt để tăng bảo mật.
* Cập nhật firmware thường xuyên: Luôn cập nhật firmware cho router và thiết bị để khắc phục các lỗ hổng bảo mật.
* Giám sát lưu lượng mạng: Sử dụng công cụ để theo dõi lưu lượng và phát hiện các hoạt động bất thường.
* Dùng VPN: Mã hóa dữ liệu khi truy cập mạng để tránh bị đánh cắp thông tin.
* Phân chia mạng:Sử dụng VLAN hoặc guest network để cô lập các thiết bị không tin cậy.
* Tắt tính năng không cần thiết: Vô hiệu hóa các tính năng như remote management, UPnP nếu không cần thiết.