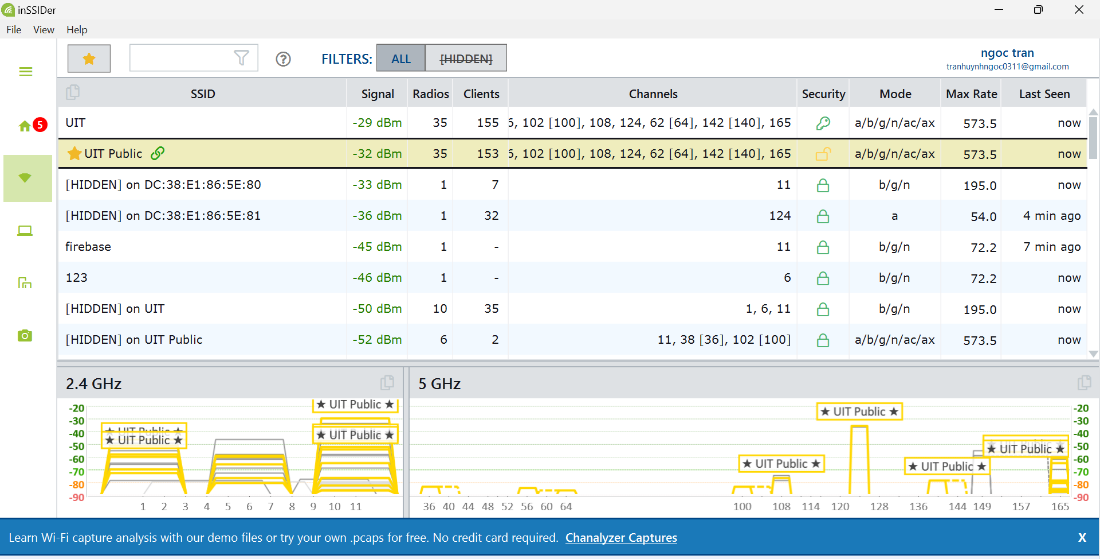
21520641 Cao Thị Kim Cẩm

21522384 Trần Huỳnh Ngọc

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

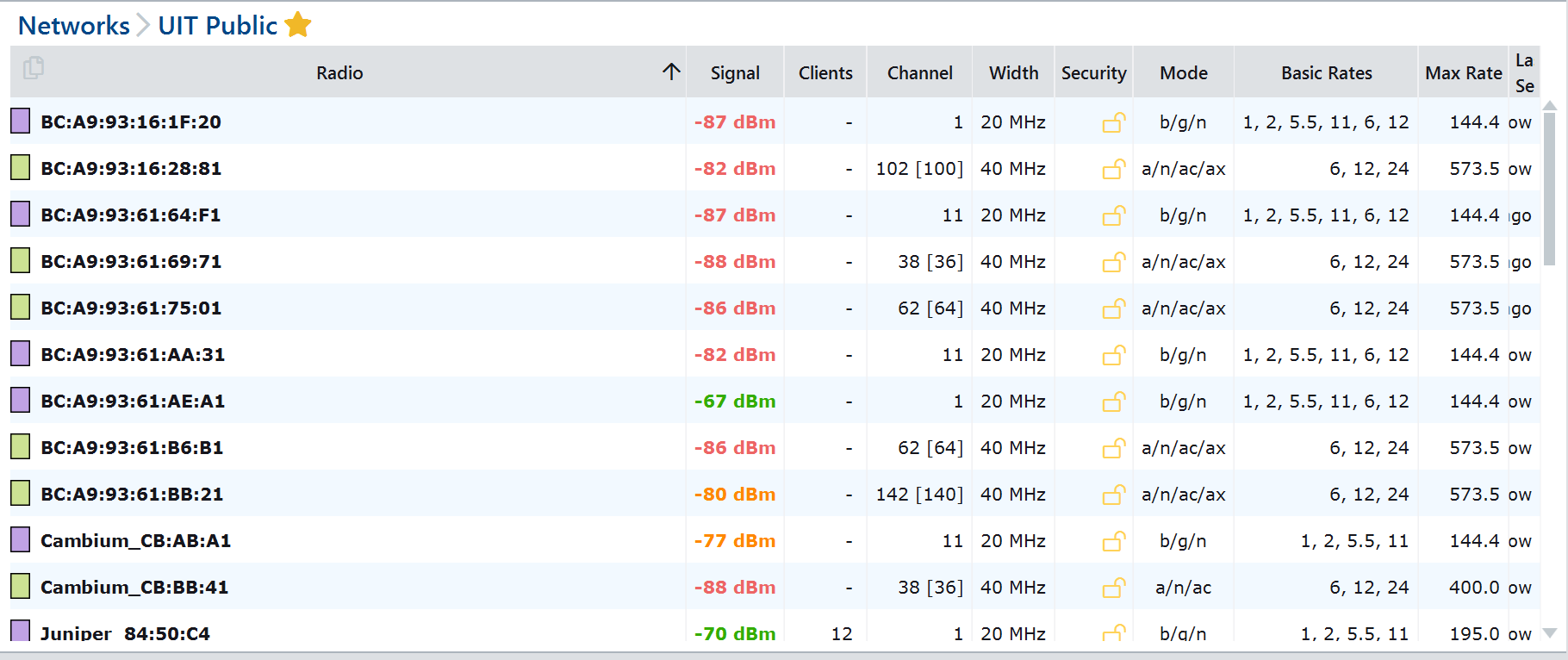
Công cụ cài đặt: inSSIDer



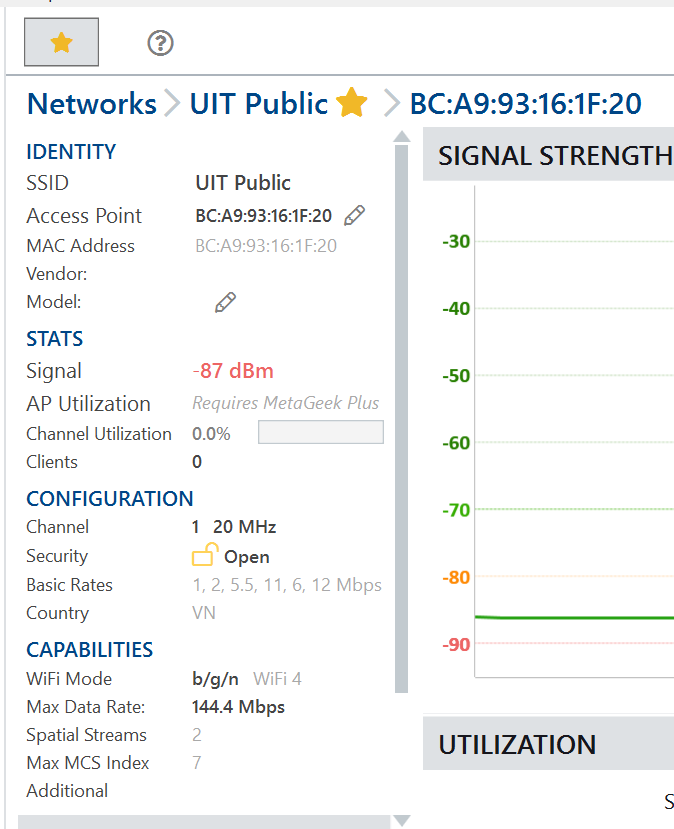


Theo như hình, bắt được các mạng sau:

* UIT public: được phát ra từ nhiều access point như:

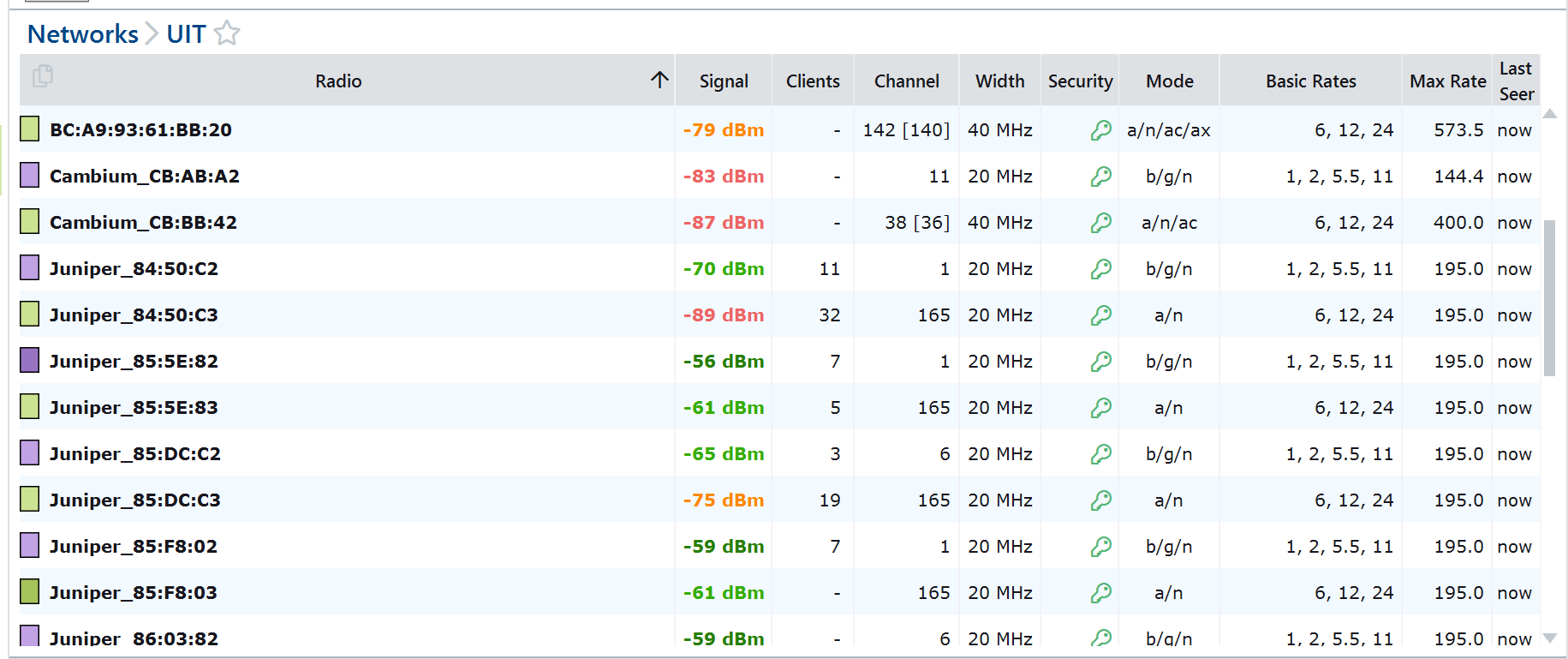


* Xem chi tiết một AP thì các thông tin như: địa chỉ mac của AP đó, SSID, tốc độ truyền,...

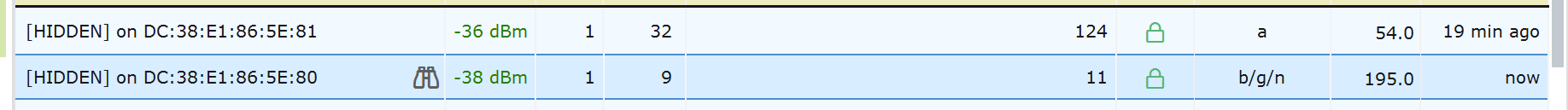


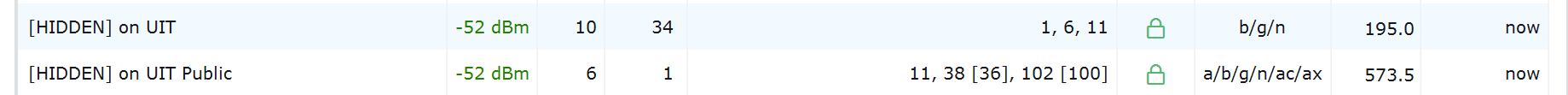
* Mạng UIT cũng được phát ra từ nhiều access point như:

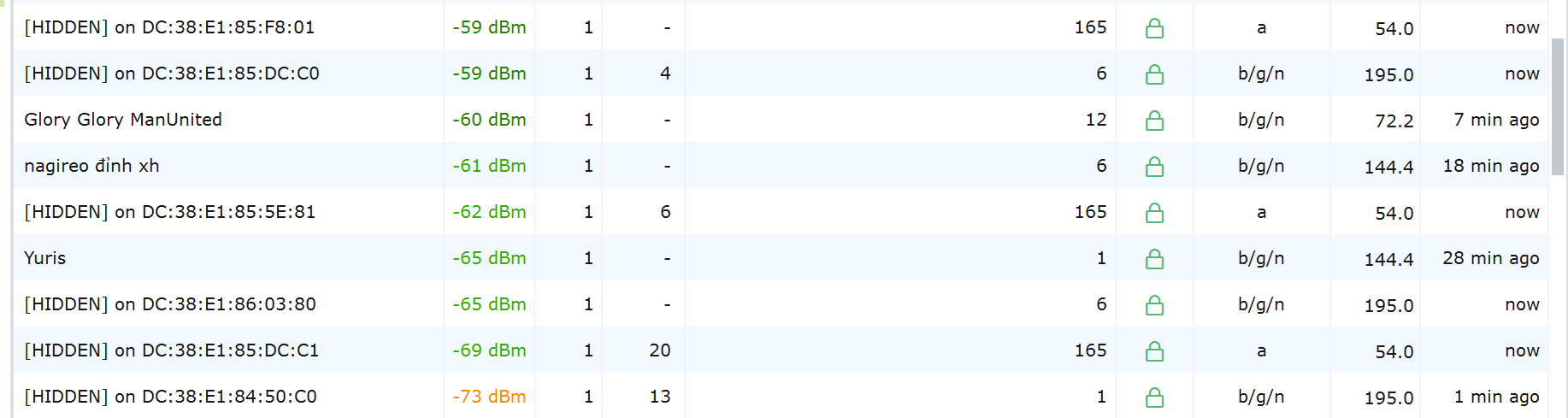




- Mạng hidden là mạng mà SSID không được hiển thị công khai, khi sử dụng inSSIDer ta bắt được các được các mạng hidden sau:





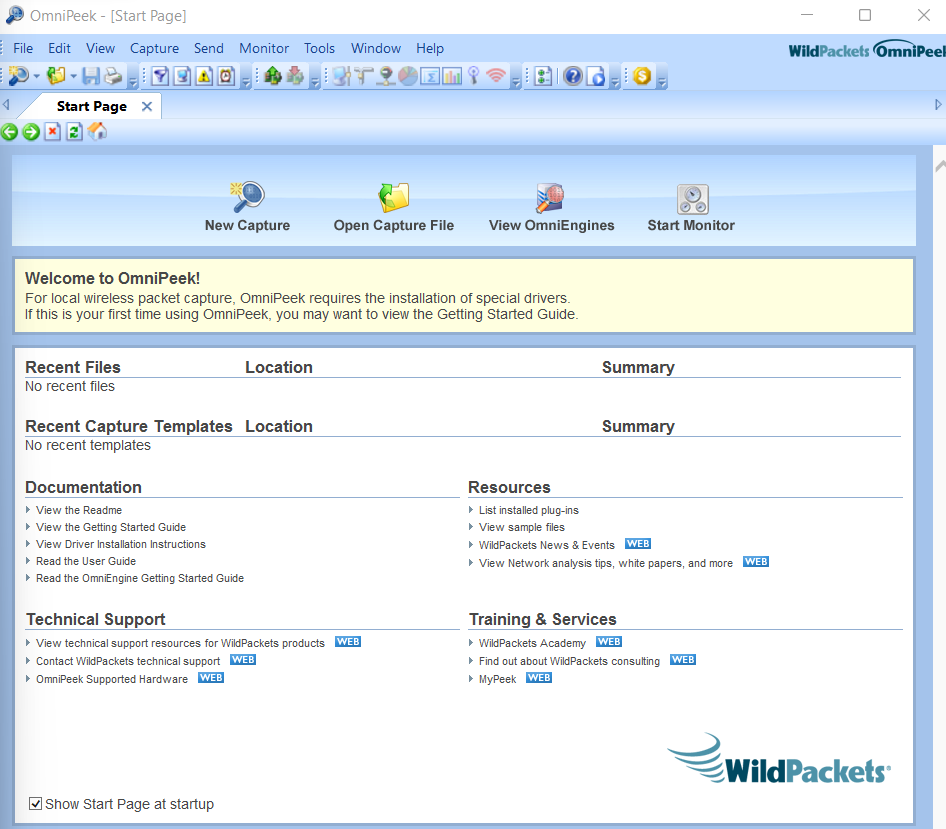


Ngoài ra, còn có các mạng do cá nhân phát ra như:

|  |  |  |
| --- | --- | --- |
| SSID | MAC address | Chú thích |
| 123 | 56:C5:43:9A:62:A9 | Bảo mật WPA2 – tốc độ 72.2 Mbps |
| bananaa | 5E:D2:7C:29:52:E6 | Bảo mật WPA2 - tốc độ 866.7 Mbps |
| firebase | 06:7B:D8:B7:37:C0 | Bảo mật WPA2 – tốc độ 72.2 Mbps |
| GloryGlory ManUnited | 9E:17:AF:37:DB:65 | Bảo mật WPA2 – tốc độ 72.2 Mbps |

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

Đầu tiên, tải và cài đặt OmniPeek.



Chọn New Capture và lựa chọn card mạng của máy thật:

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, số

Mô tả được tạo tự động

Sau khi nhấn OK, sẽ thấy như sau:

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, màn hình

Mô tả được tạo tự động

Chọn Start Capture để tiến hành bắt gói tin. Thống kê lưu lượng sẽ được cập nhật lên dashboarch từ khi Start Capture.

Sau đó chọn Stop Capture để kết thúc việc bắt gói. Có thể thêm, xoá, hoặc tiếp tục quá trình bắt gói.

Một số kết quả của quá trình bắt gói: (Do ở đây em sử dụng version bị giới hạn nên chỉ bắt được 2000 gói tin)

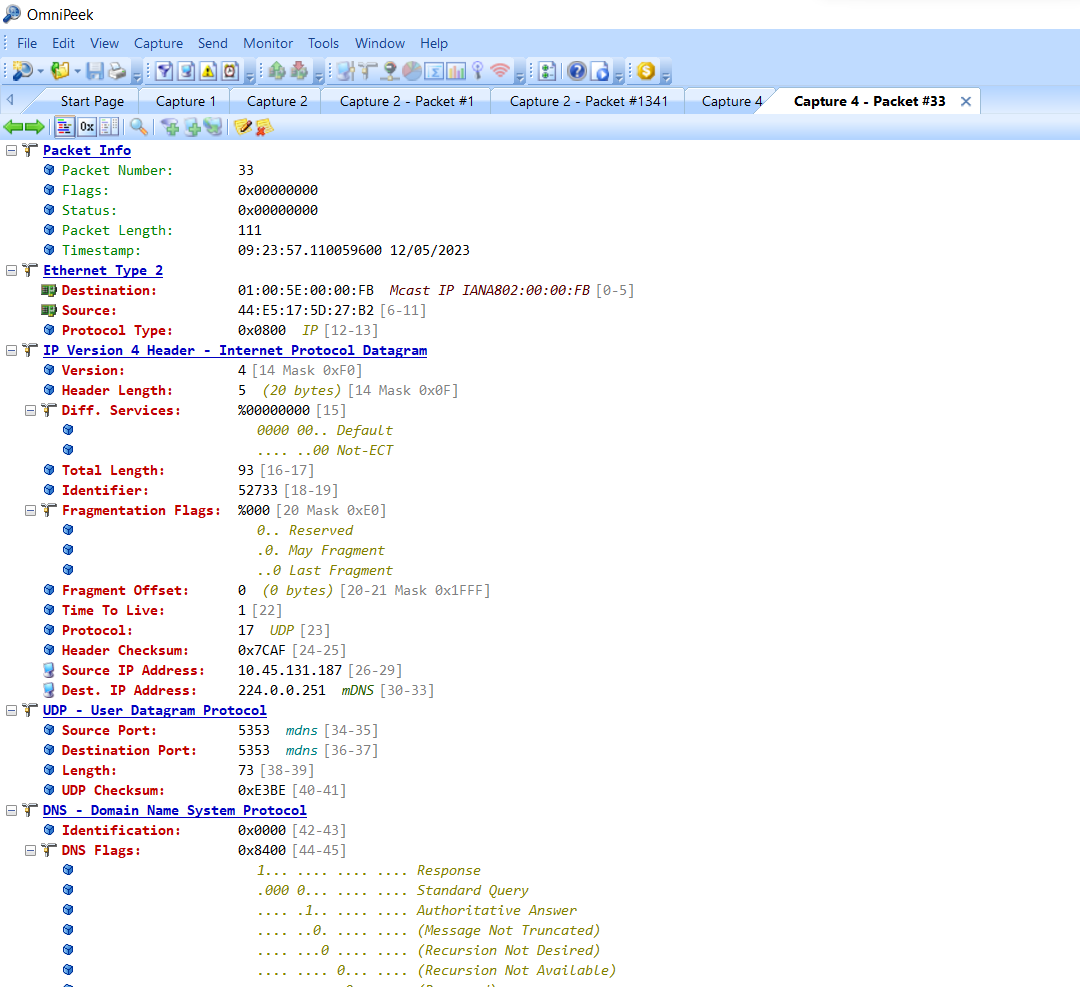
Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Ảnh có chứa văn bản, phần mềm, số, Biểu tượng máy tính

Mô tả được tạo tự động

Có thể phân tích chi tiết gói tin, bằng cách chọn gói tin, và chọn decode packet.



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

* Airbase-ng: dùng để tạo điểm truy cập giả để đánh lừa người khác kết nối vào để tấn công vào máy những người truy cập tới thay vì tân công vào chính access point
* Aireplay-ng: chèn các gói tin vào mạng để tạo lưu lượng truy cập
* Airmon-ng: bật chế độ monitor cho card mạng không dây để bắt hết các hết gói tin có trong mạng đó
* Aircrack-ng: dùng để bẻ khóa các giao thức bảo mật mạng như WEP, WPA, WPA-2
* Airgraph-ng: tạo đồ thị có dữ liệu từ airodump-ng
* Airtun-ng: tạo giao diện đường hầm ảo với 2 công dụng chính là giám sát tất cả lưu lượng truy cập được mã hóa và đưa lưu lượng truy cập tùy ý vào mạng (hay là làm tăng lưu lượng mạng lên)
* Airdecap-ng: giải mã tệp pcap được mã hóa WEP, WPA
* Airdecloack-ng: loại bỏ tệp WEP trong tệp pcap
* Airodump-ng: dùng để bắt thu thập thông tin trong mạng không dây qua việc bắt các gói tin đó, bên cạnh đó nó còn có thể ghi lại tọa độ cũa các điểm truy cập được phát hiện
* Airolib-ng: dùng để tạo và quản lý các bảng băm
* Tkiptin-ng: chèn các gói tin vào mạng WPA, TKIP bằng QoS
* Airdrop-ng: dùng để hủy xác thực người dùng

## **Câu 5: Trình bày các biện pháp tấn công mạng wifi**

* Đổi SSID mặc định sau khi cấu hình WLAN
* Cài đặt password và bật (enable) tường lửa bảo vệ cho router truy cập
* Bật (enable) lọc địa chỉ MAC trên điểm truy cập hoặc router của bạn
* Bật (enable) mã hoá trên điểm truy cập và thay đổi mật khẩu thường xuyên
* Sử dụng che đậy SSID để chắc chắn rằng thông báo mạng không dây mặc định từ việc quảng bá ID tới tất cả mọi thiết bị.
* Đặt 1 fileware hoặc một bộ lọc gói giữa AP và mạng nội bộ doanh nghiệp
* Kiểm tra thiết bị không dây về những vấn đề cấu hình và thiết lập thường xuyên
* Triển khai một công nghệ khác cho mã hoá các traffic, như IPSEC trên mạng không dây
* Chọn bảo mật mạng không dây WPA thay vì WEP
* Triển khai mô hình WPA2 ở bất cứ nơi nào mà có thể
* Đặt một AP mạng không dây trong một khu vực bảo mật
* Giữ cho drivers trên thiết bị mạng không dây được cật nhât
* Sử dụng 1 server tập trung cho xác thực