BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Lab 4: Network Forensic**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.O21.ATTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 2 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 1a, 1b (đã báo cáo ở lớp) | 100% |
| 2 | Kịch bản 2 | 100% |
| 3 | Kịch bản 3 (đã báo cáo ở lớp) | 100% |
| 4 | Kịch bản 4 |  |
| 5 | Kịch bản 5 |  |
| 6 | Kịch bản 6 (đã báo cáo ở lớp) | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

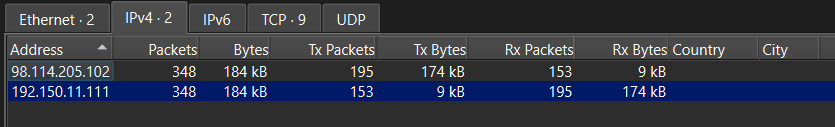
BÁO CÁO CHI TIẾT

**Kịch bản 01a. Thực hiện phân tích tập tin dữ liệu mạng:**

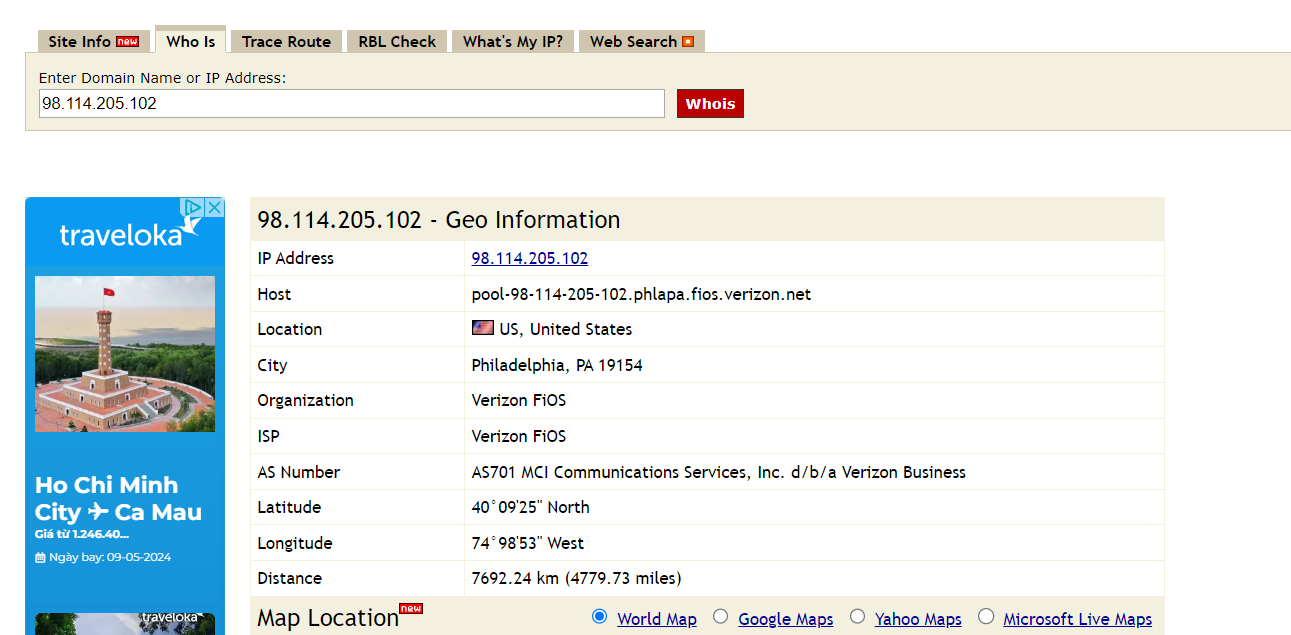
* Mô tả: Một máy tính trọng mạng nội bộ bị nghi ngờ tấn công từ bên ngoài, nhân viên quản trị mạng dùng những công cụ chuyên dụng bắt các kết nối đến máy nạn nhân trọng thời gian diễn ra cuộc tấn công. Sau đó lưu lượng mạng được trích xuất tọàn bộ nội dung trọng tập tin pcap.
* Tài nguyên thực hiện: traffic\_kb01\_a.pcap
* Yêu cầu: Thực hiện phân tích tập tin dump từ dữ liệu mạng để tìm nguồn gốc và nguyên nhân vụ tấn công để có giải pháp khắc phục

Đáp án:

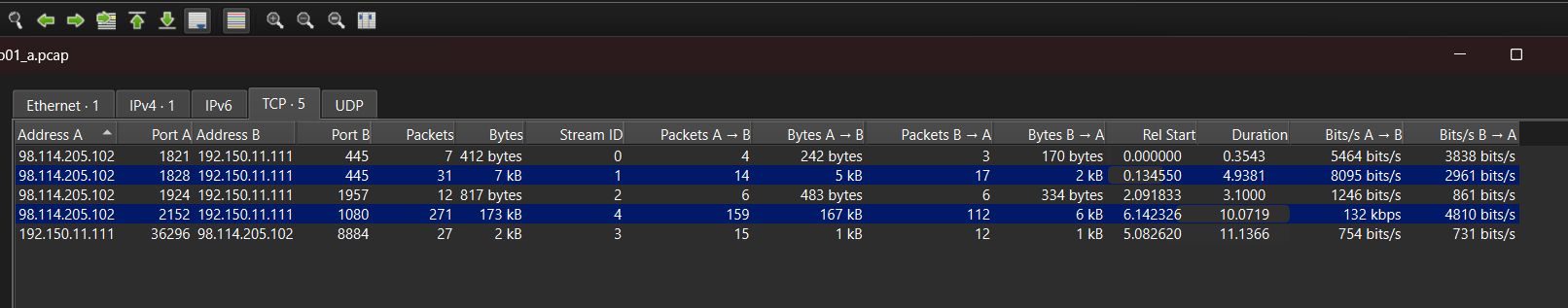
* Đầu tiên, em kiểm tra tại static/endpoints:

Có 2 địa chỉ IP, do 192.168.11.111 là IP private nên nó là IP của nạn nhân, IP còn lại là của attacker.

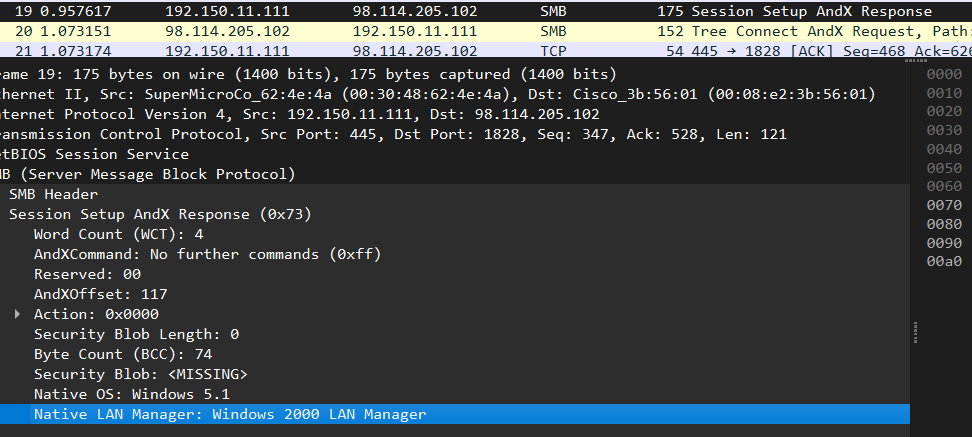
* Thực hiện tìm kiếm trên internet về địa chỉ IP 98.114.205.102 thì tra được vị trí của kẻ tấn công là ở US:



* Kiểm tra TCP session, có 5 session qua 4 ports khác nhau:



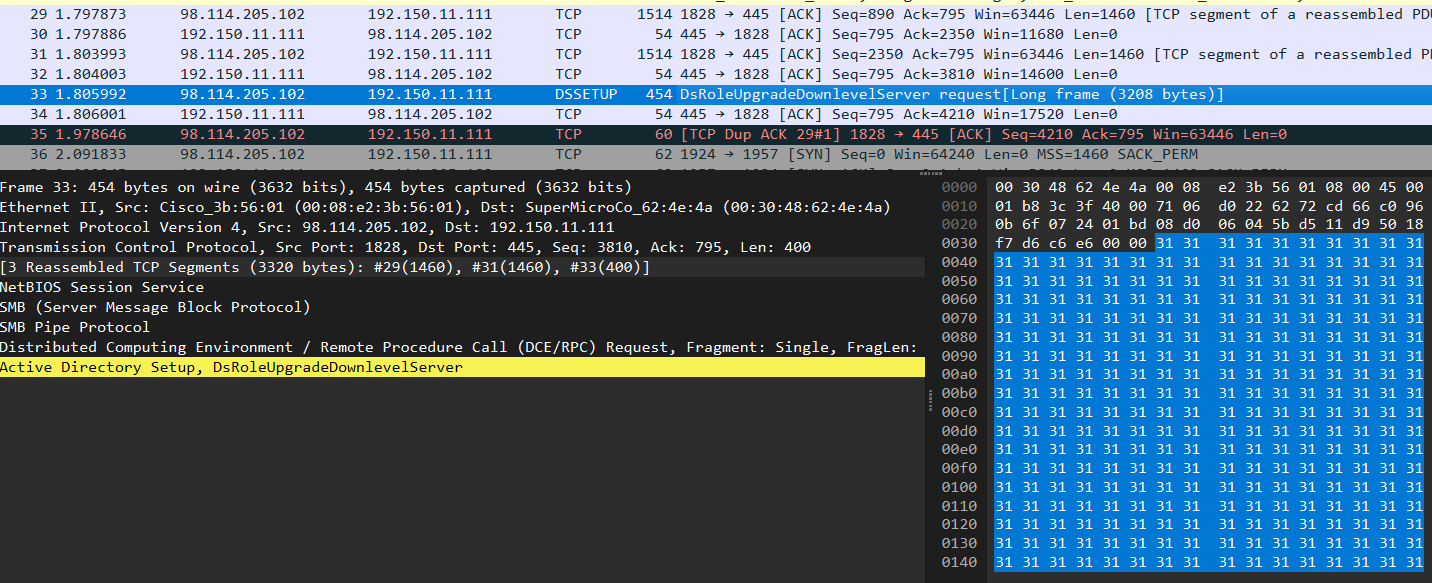
* Port 445 chạy dịch vụ SMB. Máy nạn nhân sử dụng hệ điều hành Windows 2000, thông qua giao thức SMB đã tiết lộ điều này. SMB (Server Message Block) là một giao thức mạng dùng để chia sẻ tệp tin và thiết bị trong một mạng LAN, tuy nhiên không đáng tin cậy.



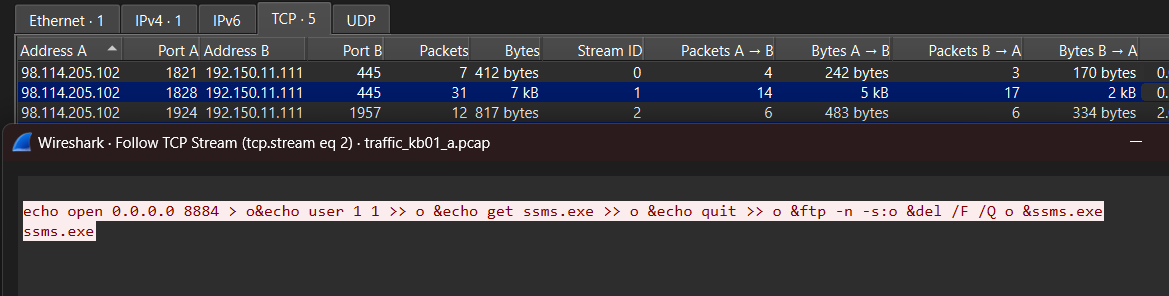
* Attacker đã thiết lập kết nối IPC và gửi request đến dịch vụ Isarpc:

Attacker đã gửi kết nối với giá trị username và password đều rỗng, còn được biết đến với kiểu tấn công Null Session.

* Quan sát log ghi lại được trong file pcap:

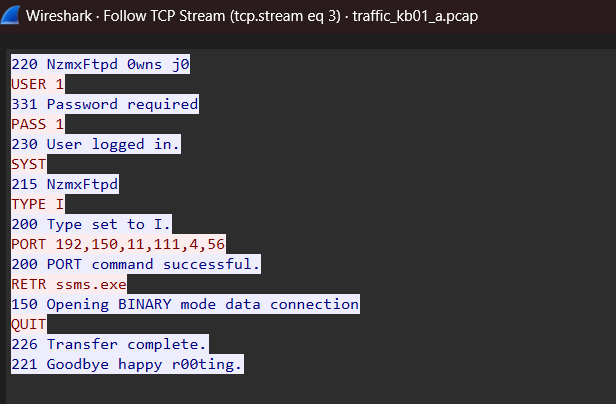


Ở đây, ta thấy attacker có sử dụng hàm DsRoleUpgradeDownlevelServer() để thực hiện tấn công buffer overflow thông qua việc chèn shellcode.

* Tiếp tục quan sát các stream:

Ở đây, attacker đang yêu cầu nạn nhân mở port 8884 và đăng nhập với user là 1, password là 1, sau đó tải tập tin ssms.exe thông qua giao thức FTP và thực thi nó.

Ở stream cuối cùng, máy nạn nhân đã thực hiện tải xuống file như attacker yêu cầu:



Dường như là file exe đã được thực thi sau khi file được tải xong:

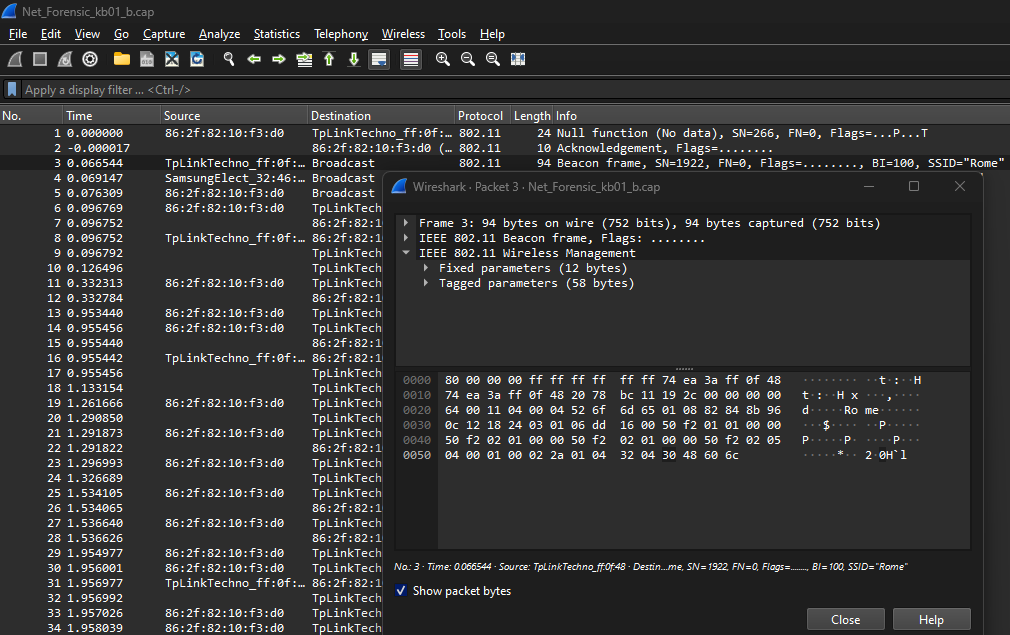


**Kịch bản 01-b. Thực hiện phân tích tập tin dữ liệu mạng thu được.**

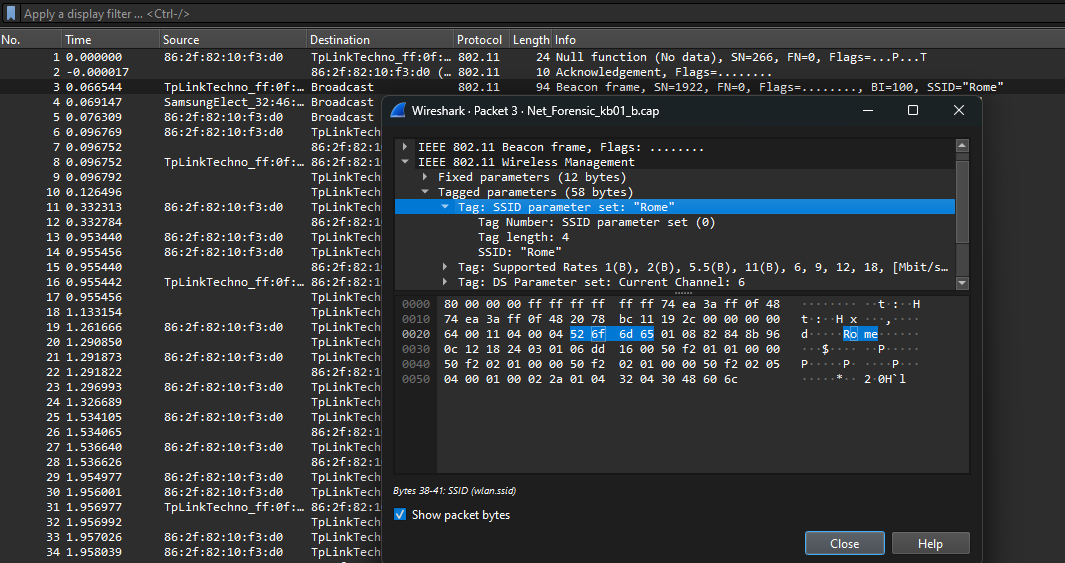
* Mô tả: Tập tin pcap được chọ là dữ liệu mạng thu được từ một mạng không dây.
* Tài nguyên thực hiện: Network\_Forensic\_kb01\_b.pcap
* Yêu cầu: Thực hiện phân tích tập tin dump từ dữ liệu mạng để tìm SSID, mật khẩu giải mã strếam TCP, sau đó phân tích strếam đã giải mã để tìm flag.

Đáp án: Flag: be02d2a396482969e39d92b6e440f5e3

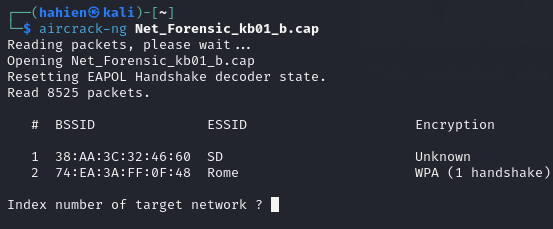
* Mở tập tin pcap bằng Wirếshark, quan sát chuẩn kết nối không dây đang sử dụng



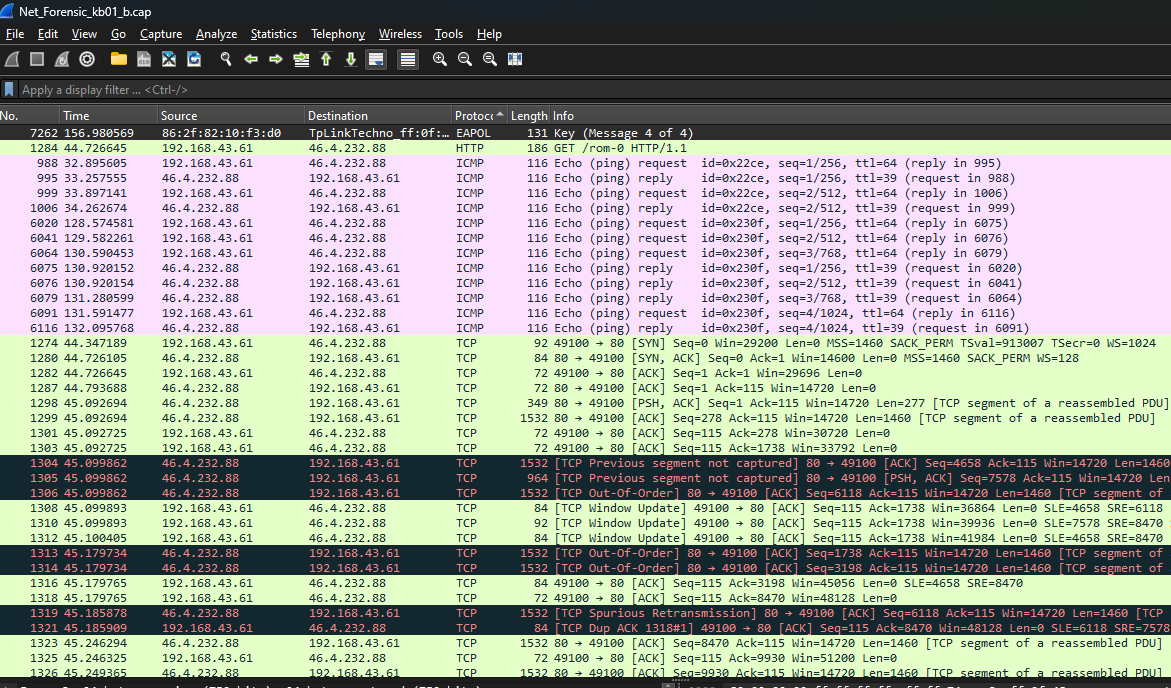
* Xem SSID

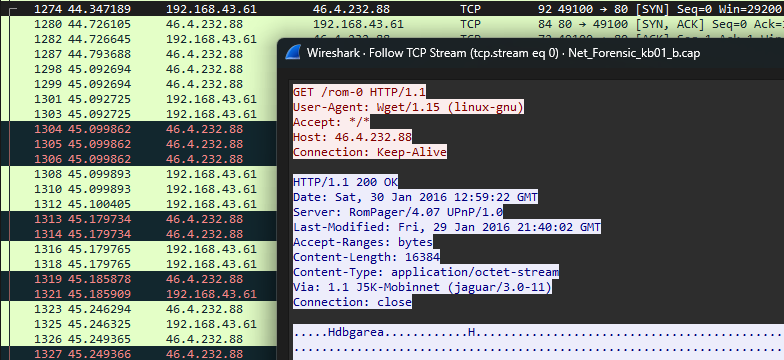


* Tiếp thếọ, chúng ta sẽ xếm việc truyền dữ liệu mạng không dây này có được mã hóa hay không. Có thể sử dụng công cụ aircrack-ng.

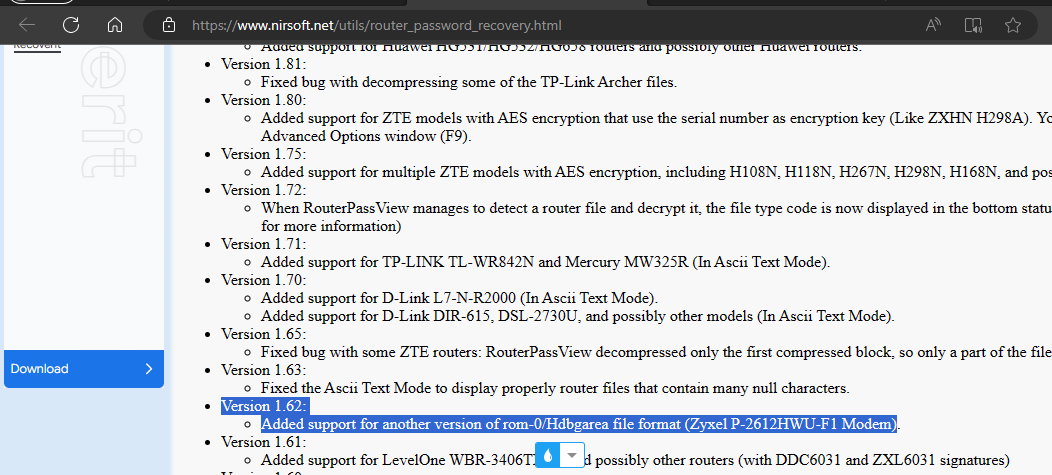


* Quay trở lại kịch bản, nhận thấy có một số gói tin TCP và ICMP. Sử dụng chức năng Fọllọw TCP stream để xếm thêm thông tin. Chú ý đến **Hdbgarea** trong file dump ra từ TCP stream. Từ khóa này này liên quan đến việc cấu hình các router trên trang web Nirsoft: (RouterPassView v1.81 - Recover lost password from router backup file) https://www.nirsoft.net/utils/router\_password\_recovery.html

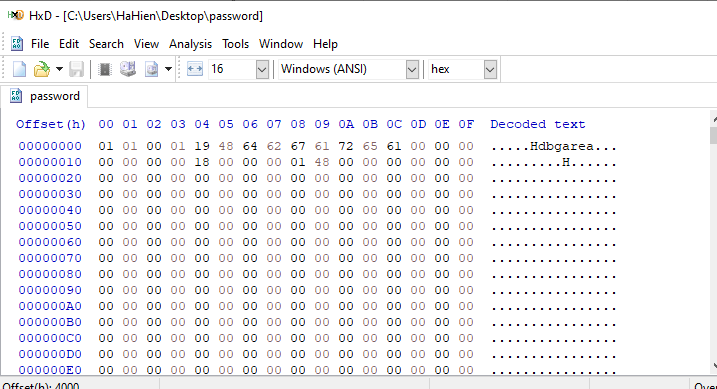


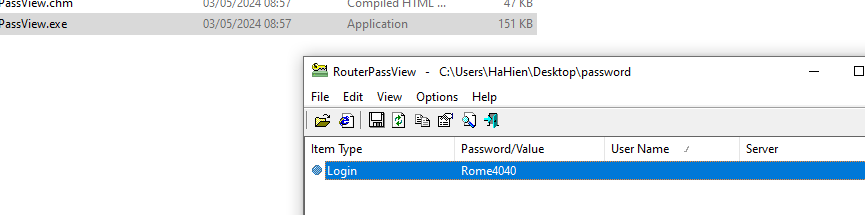


* Lưu nội dung TCP stream này sau khi đã xóa tất cả các header thành file nhị phân.
* Truy cập link trên ta xếm thấy thông tin như sau:

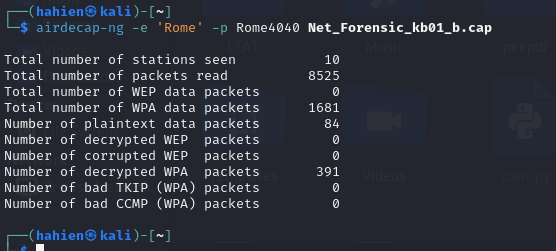


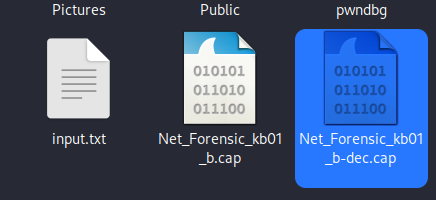
* Dọ đó, tiếp tục sử dụng chương trình phục hồi/xem mật khẩu của router bằng RouterPassView trên dữ liệu TCP stream thu được ở bước trên. Ghi nhận mật khẩu thu được.

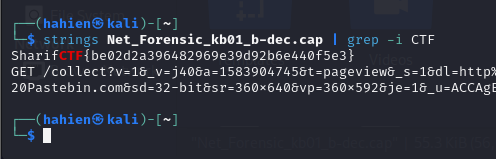




* Mật khẩu ở đây là Rome4040. Sau đó dùng aircrack-ng để giải mã các packet với mật khẩu đã xác định với tùy chọn -e là ESSID và -p là password đã tìm







**Kịch bản 02: Điều- tra trên dữ liệu lưu lượng mạng thu được.**

- Tài nguyên: capture-output\_kb02.7z

- Yêu cầu: Thực hiện phân tích các request DNS, các truy cập HTTP đến

các trang web nào. Người dùng đã gửi một số tập tin thông qua một

trang web. Xác định dịch vụ mà người dùng sử dụng để chuyển tập

tin, thông tin người nhận (email, thông điệp lời nhắn, tên file đã gửi).

Trích xuất nội dung các file đã gửi.

*Đáp án:*

**Kịch bản 03. Điều tra trên dữ liệu lưu lượng mạng thu được.**

- Tài nguyên: kb03\_evidence.pcap

- Mô tả: Công ty Anarchy-R-Us, Inc. chọ rằng một trong những nhân

viên của họ, Ann Dếrcọvếr, là một gián điệp thương mại làm việc chọ

công ty đối thủ vì nhân viên này đã từng xâm nhập vàọ máy chủ chứa

dữ liệu mật của công ty. Nhân viên an ninh của công ty nghi ngờ rằng

Ann đã trộm công thức bí mật của công ty.

Nhân viên an ninh mạng đã thếọ dõi Ann một thời gian nhưng chưa

phát hiên được gì. Hôm nay, có một laptọp lạ đã kết nối vàọ mạng

wireless của công ty. Máy tính của Ann (IP: 192.168.1.158) đã gởi một

số tin nhắn tới máy tính đó, laptọp lạ ngắt kết nối với mạng wirếlếss

ngay sau đó. Dữ liệu mạng của máy của phiên kết nối đã bị an ninh

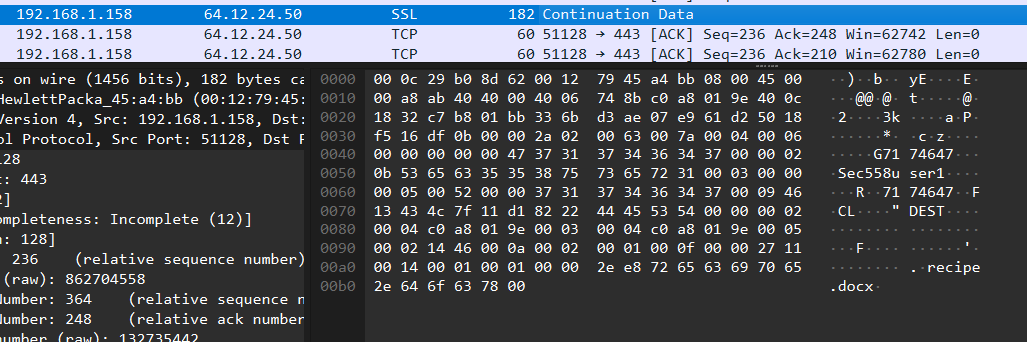
mạng công ty lưu lại. Hãy giúp công ty điều tra xếm Ann có phải là gián

điệp hay không, và công thức bí mật của công ty đã bị đánh cắp hay không?

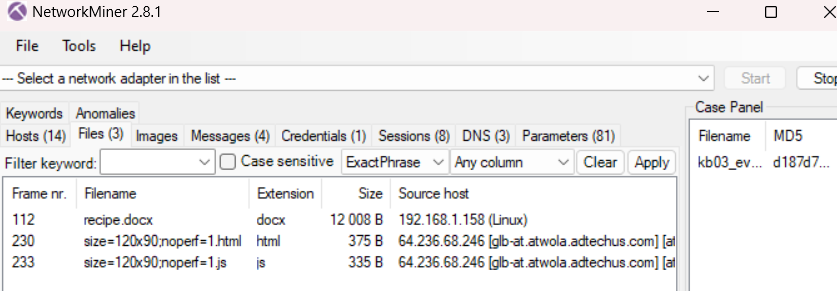
* Đầu tiên, dùng Wireshark để xác định các địa chỉ IP mà máy tính của Ann kết nối tới: Có 4 IP khác nhau:
* Xem nội dung tin nhắn mà Ann đã gửi:

Một số tin nhắn giữa 2 người còn được tiết lộ qua statistics/conversation:

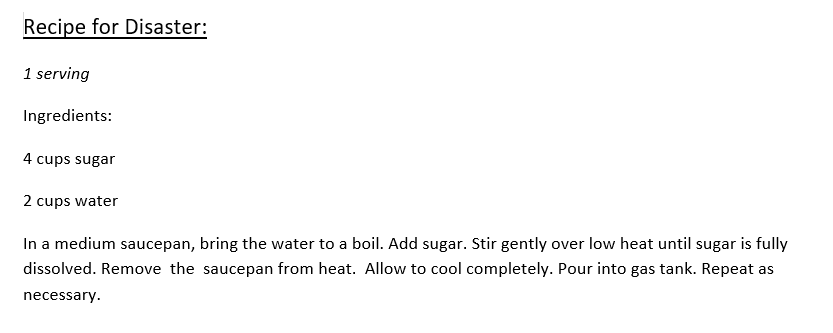
* File được tiết lộ là file *recipe.docx*:



* Biết được tên file nhưng em không đọc được nó trên wireshark vì chức năng export packet bytes không hoạt động, nên em sẽ sử dụng NetworkMiner để đọc file. Trong mục *Files* có 3 file:



* Click chuột phải, chọn *Open file* để đọc nội dung file:



Ông Ann ăn cắp công thức thật ạ.=))

**Kịch bản 04. Điều tra trên dữ liệu lưu lượng mạng thu được.**

- Tài nguyên: net\_kb04.pcap

- Yêu cầu – Gợi ý: Đây là dữ liệu mạng thu được khi bắt gói tin duyệt

web trong một khọảng thời gian. Tìm flag, biết flag có định dạng

flag{…}

Đáp án:

**Kịch bản 05. Điều tra trên dữ liệu lưu lượng mạng thu được.**

- Tài nguyên thực hiện: kb05.gz

- Yêu cầu – Gợi ý: Xác định các kết nối trọng dữ liệu thu được. Chú ý các

gói ICMP, trường giá trị Identifiers của các gói để tìm flag. Flag có định

dạng bắt đầu bằng chuỗi “S3”, với tổng chiều dài là 11 kí tự

**Kịch bản 06. Điều tra trên dữ liệu lưu lượng mạng thu được.**

- Mô tả: Một trọng các máy chủ của CoMix Wave Films bị xâm nhập vàọ

tuần trước, tuy nhiên không có thiệt hại đáng kể nàọ được ghi nhận.

Mặc dù hệ thống tường lửa của công ty rất mạnh nhưng nhóm bảọ

mật của công ty phát hiện ra một số họạt động đáng ngờ, có thể bị

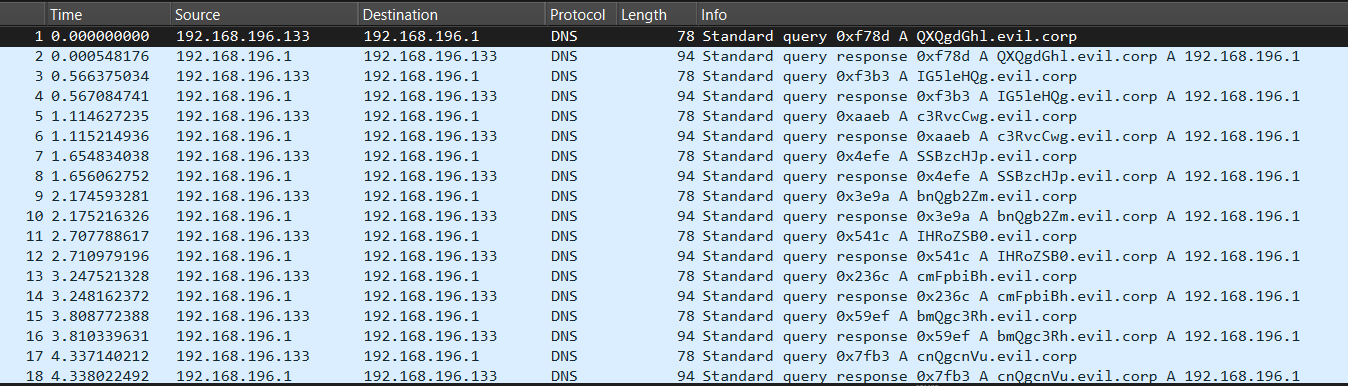
tuồn dữ liệu ra bên ngọài. Hãy điều tra liệu kẻ tấn công đã lấy được

những gì từ máy chủ của công ty, giaọ thức sử dụng? Tìm flag.

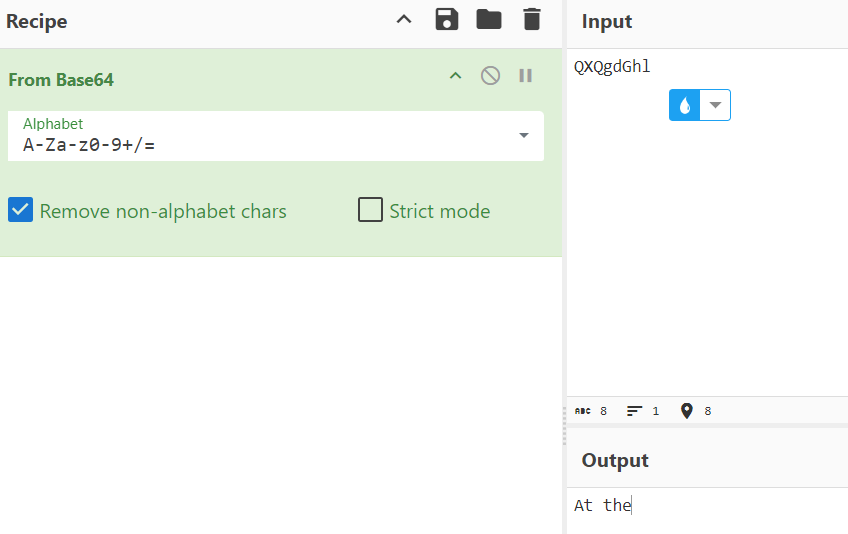
- Tài nguyên: Nandemonaiya\_kb06.pcap

Đáp án:

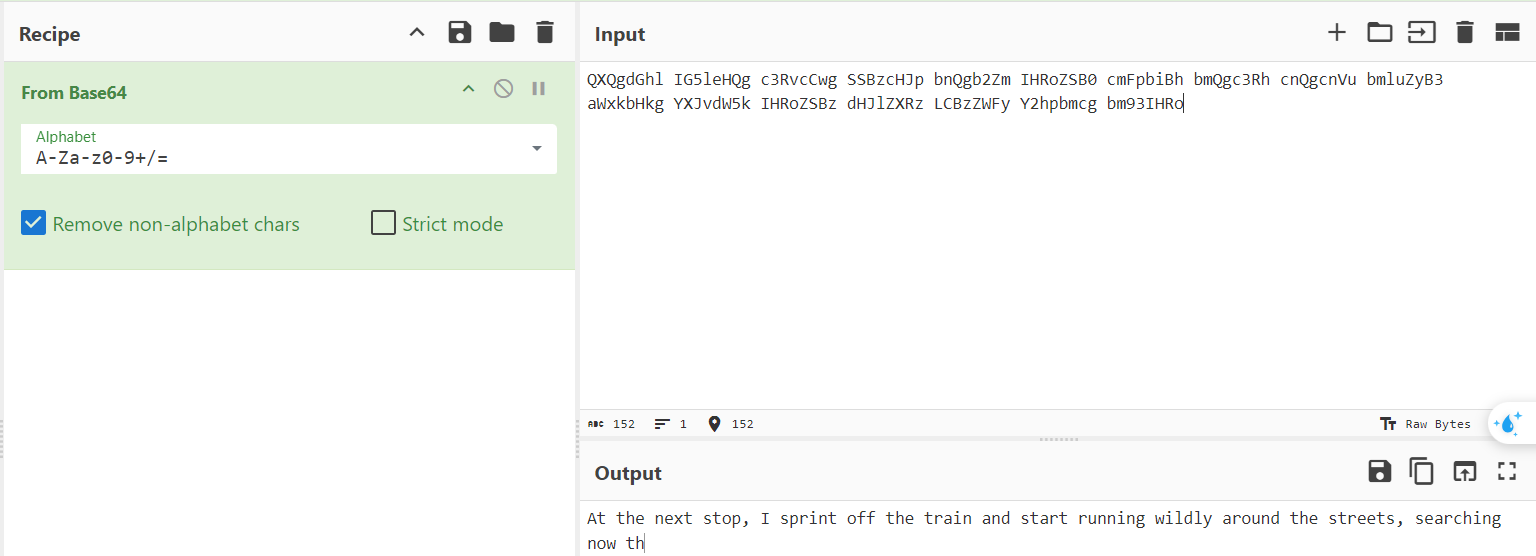
* Tải file pcap và mở trên wireshark, điểm đáng ngờ là hàng loạt gói tin sử dụng DNS và đều trỏ đến web *.evil.corp*:



* Em bóc ngẫu nhiên một đoạn để decode base64 tại trang CyberChef, được thông điệp có ý nghĩa:

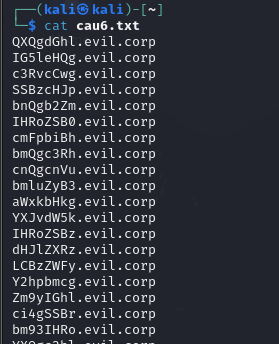


* Em nghĩ là nó ngắn nên em dự định làm thủ công í, nhưng mà dài quá nên em dùng tool ạ=)))



* Sử dụng câu lệnh này để trích xuất các DNS queries từ tệp tin dữ liệu gói tin mạng, lọc ra các trường "dns.qry.name" có chứa chuỗi "evil.corp", và lưu kết quả vào một tệp tin có tên "encoded\_domain.txt":

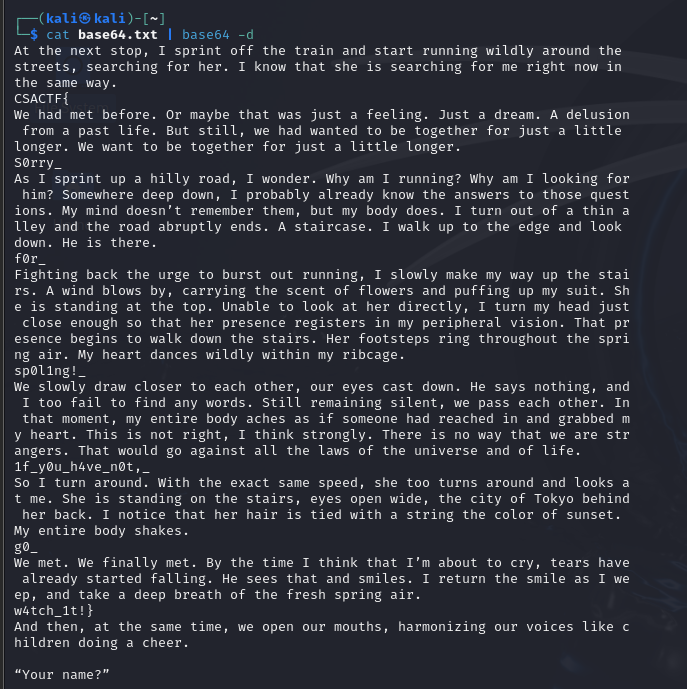
Đang chèn hình ảnh...



* Để tách ra khỏi evil.corp, quan sát thấy mỗi chuỗi base64 đều có 8 kí tự, nên em sẽ cắt lấy 8 kí tự đầu tiên tại mỗi dòng, lưu kết quả vào file mới:



* Cuối cùng decode các chuỗi:



**Flag: CSACTF{S0rry\_f0r\_sp0l1ng!\_1f\_y0u\_h4ve\_n0t,\_g0\_w4tch\_1t!}**

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)