BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 3: Network Forensics

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.P21.ANTT.1

STT	Họ và tên	MSSV	Email
1	Trần Huỳnh Tiến	22521476	22521476@gm.uit.edu.vn
2	Nguyễn Ngọc Xuân Tùng	22521619	22521619@gm.uit.edu.vn
3	Đào Xuân Vinh	22521666	22521666@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 1a	100%
2	Kịch bản 1b	100%
3	Kịch bản 2	100%
4	Kịch bản 3	100%

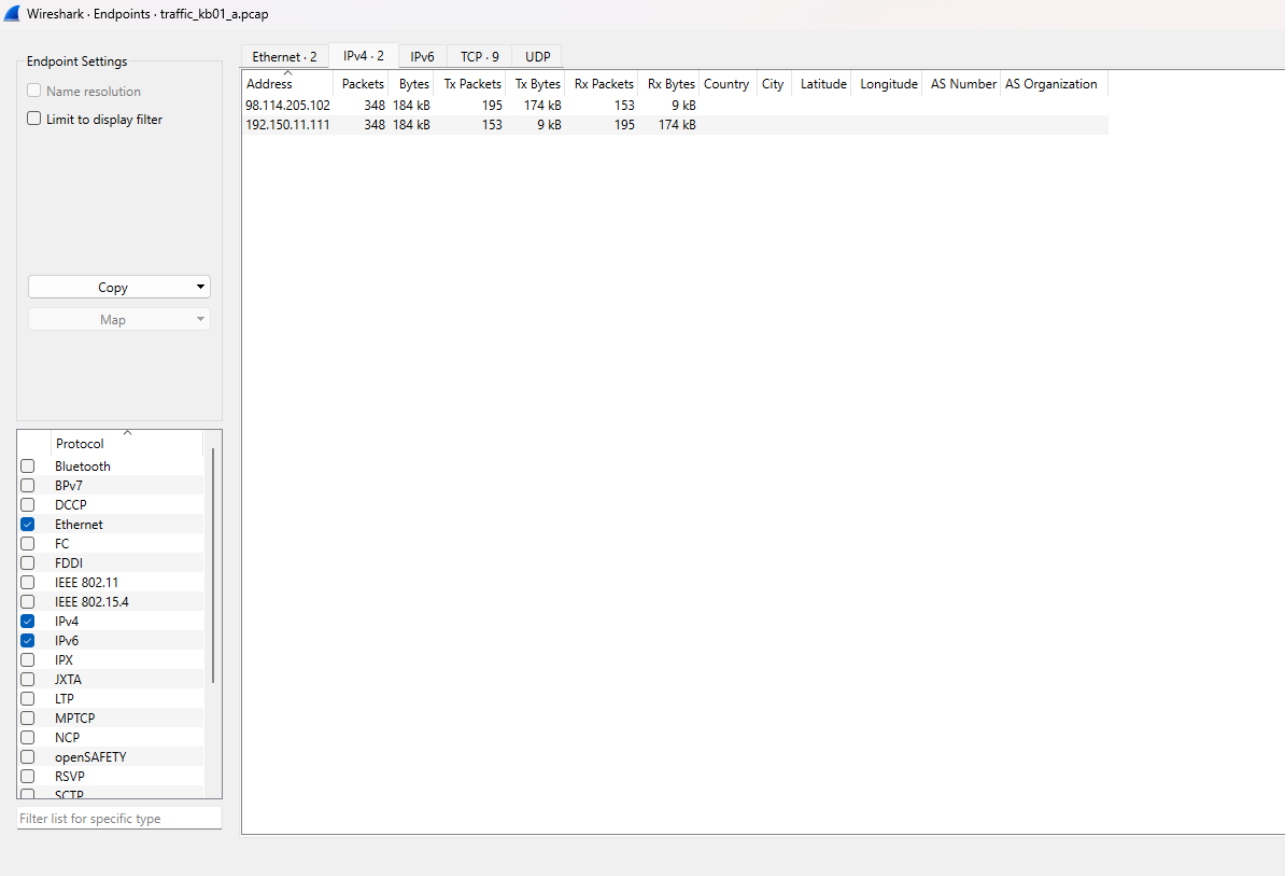
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Kịch bản 01-a. 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 toàn 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

- Mở Enpoint List/IPv4 của file pcap ta thấy được ip của máy tấn công và ip nạn nhân lần lượt là 98.114.205.102 và 192.150.11.111

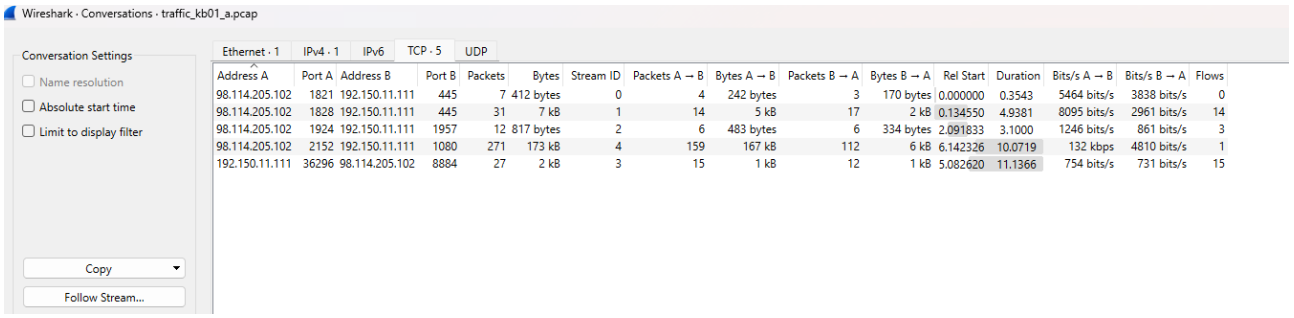


- Tra cứu ip trên whois

98.114.205.102 - Geo Information

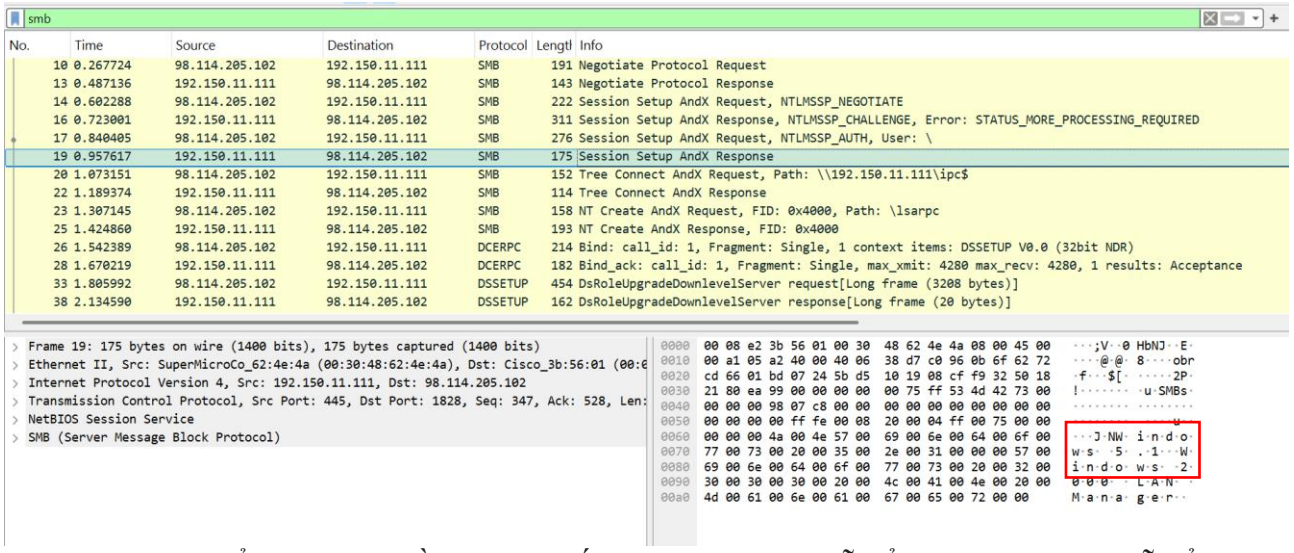
IP Address	98.114.205.102
Host	pool-98-114-205-102.phlapa.fios.verizon.net
Location	US, United States
City	Philadelphia, PA 19154
Organization	Verizon FiOS
ISP	Verizon FiOS
AS Number	AS701 MCI Communications Services, Inc. d/b/a Verizon Business
Latitude	40°09'25" North
Longitude	74°98'53" West
Distance	7692.24 km (4779.73 miles)

- Trong phần Conversations/TPC ta thấy được 5 phiên diễn ra giữa 2 máy. Trong đó từ gói đầu tiên được attacker gửi đi đến gói cuối cùng từ máy nạn nhân gửi đi là 11.1366s



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	Flows
98.114.205.102	1821	192.150.11.111	445	7	412 bytes	0	4	242 bytes	3	170 bytes	0.000000	0.3543	5464 bits/s	3838 bits/s	0
98.114.205.102	1828	192.150.11.111	445	31	7 kB	1	14	5 kB	17	2 kB	0.134550	4.9381	8095 bits/s	2961 bits/s	14
98.114.205.102	1924	192.150.11.111	1957	12	817 bytes	2	6	483 bytes	6	334 bytes	2.091833	3.1000	1246 bits/s	861 bits/s	3
98.114.205.102	2152	192.150.11.111	1080	271	173 kB	4	159	167 kB	112	6 kB	6.142326	10.0719	132 kbps	4810 bits/s	1
192.150.11.111	36296	98.114.205.102	8884	27	2 kB	3	15	1 kB	12	1 kB	5.082620	11.1366	754 bits/s	731 bits/s	15

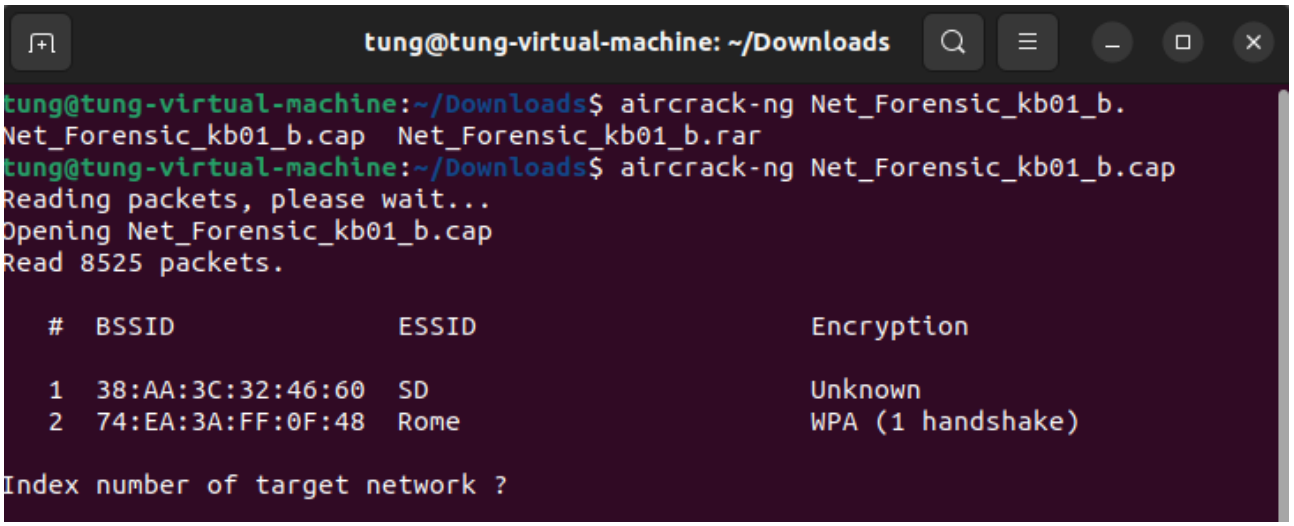
- Attacker đã truy cập các port sau trong máy nạn nhân:
  - 445: SMB - Windows File Sharing
  - 7: Echo Protocol - có thể dùng để kiểm tra máy đích có hoạt động hay không
  - 1957: Dịch vụ không rõ ràng
  - 2152: Dịch vụ không rõ ràng
  - 36296: Dịch vụ không rõ rang
- Kiểm tra gói tin giao thức SMB thì thấy nạn nhân dùng hệ điều hành Windows



➔ Vậy có thể nhận định rằng đây là tấn công khai thác lỗ hổng EternalBlue (lỗ hổng trong giao thức SMB), các port có dịch vụ không rõ ràng là các port được mở trên máy và bị attacker lợi dụng để giao tiếp giữa 2 máy.

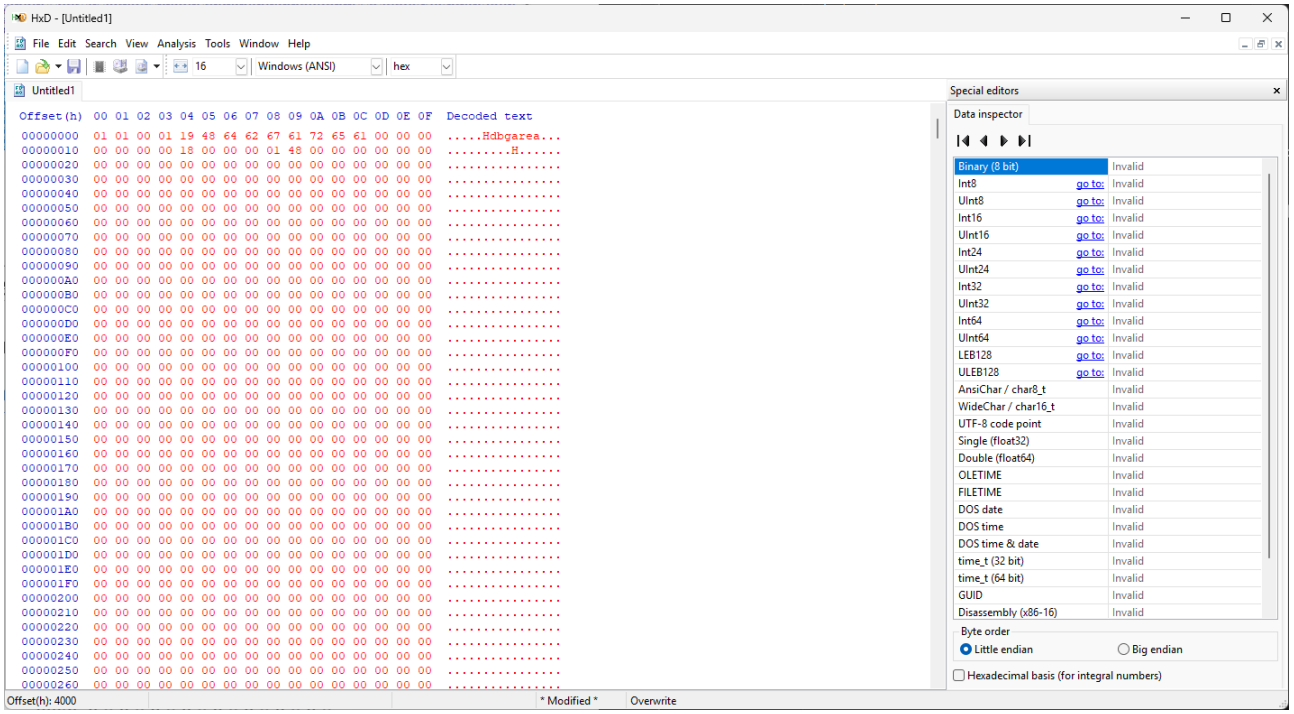
Kịch bản 01-b. Thực hiện phân tích tập tin dữ liệu mạng thu được.
- Mô tả: Tập tin pcap được cho là dữ liệu mạng thu được từ một mạng không dây.
- Tài nguyên thực hiện: Network_Forensic_kb01_b.pcap
- Yêu cầu: Thực hiện phân tích tập tin dump từ dữ liệu mạng để tìm SSID, mật khẩu giải mã strếam TCP, sau đó phân tích strếam đã giải mã để tìm flag.

Dùng aircrack-ng để xem các thông tin cơ bản

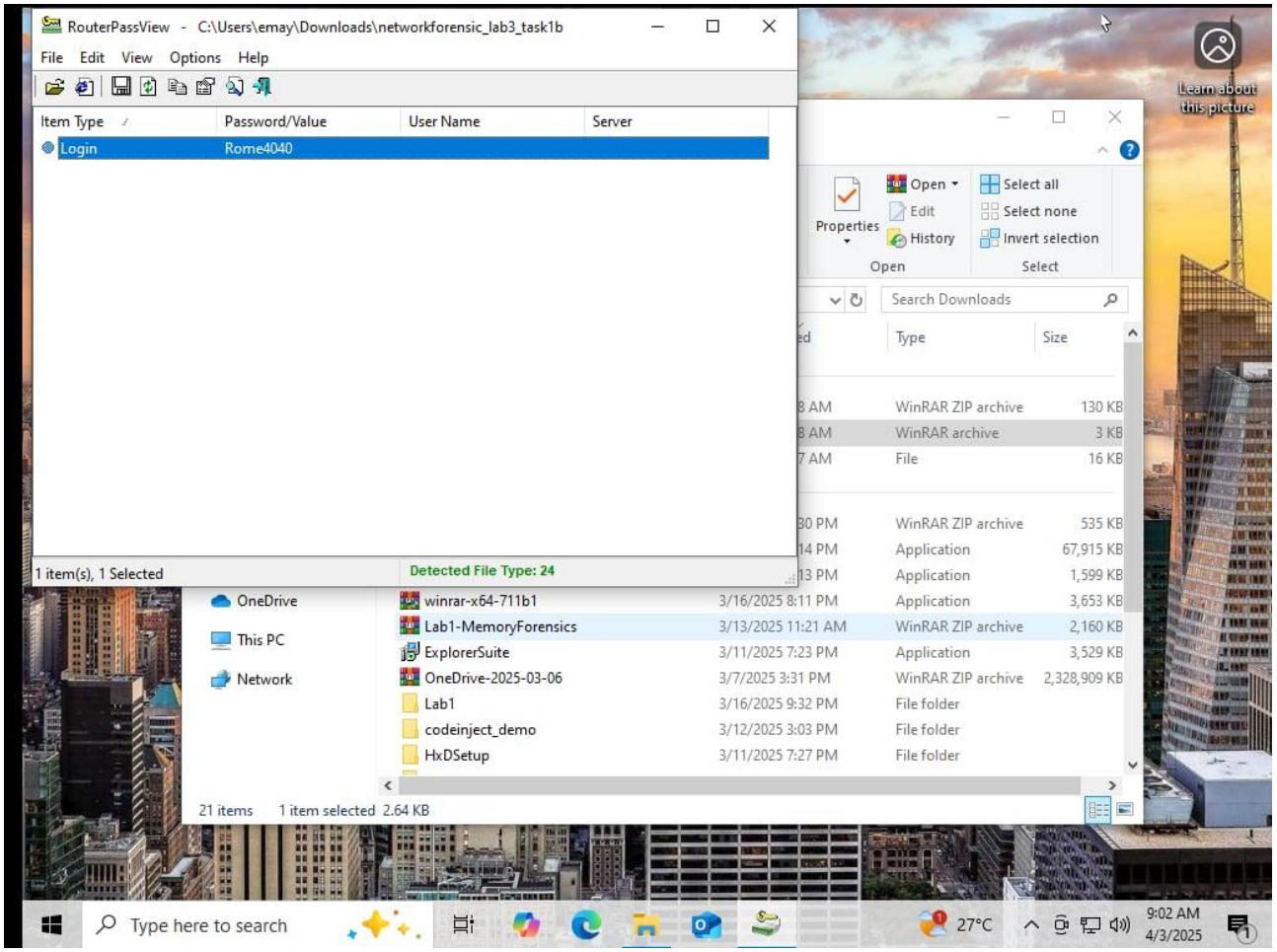


Dùng wireshark lọc cái gói tin TCP → chọn 1 gói tin TCP bất kỳ → vào TCP Stream để xem đầy đủ thông tin được gửi đi thấy "Hdbgarea" là đoạn mở đầu trong file cấu hình của RouterPassView

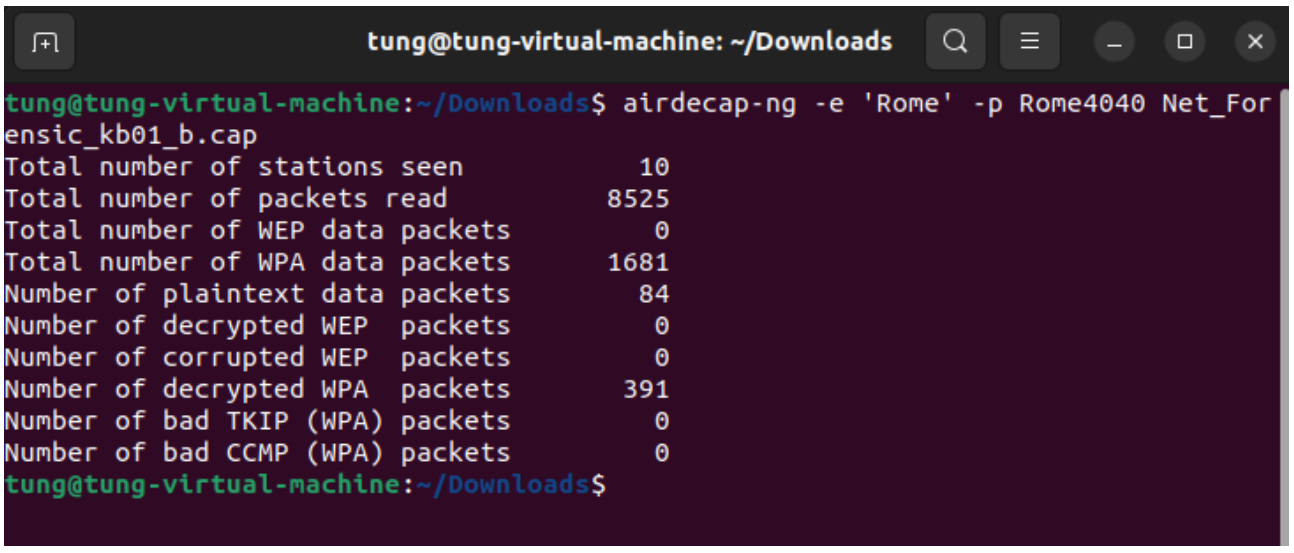
Để thực hiện recover password bằng Router Pass View → từ nội dung request chuyển sang dạng raw (bỏ phần header) → copy toàn bộ nội dung còn lại bỏ vào HxD → save lại dưới dạng file hex



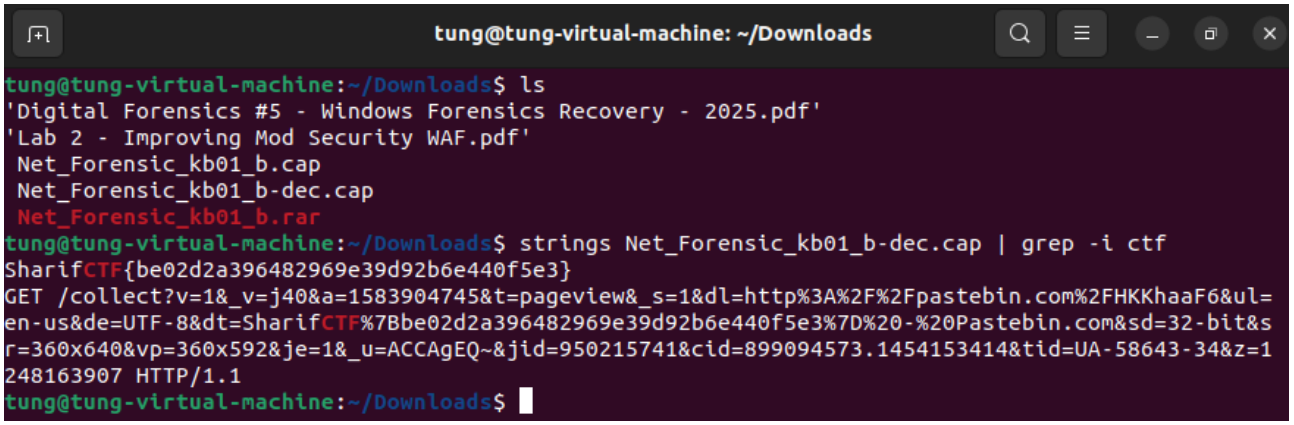
Đưa vào Router Pass View để recover password nhận được password là **Rome404**



Sau khi đã có password dùng aircrack-ng để decrypt packets



Tới đây có thể dùng lệnh strings | grep hoặc phân tích file pcap-decrypted để tìm flag



Flag: SharifCTF{be02d2a396482969e39d92b6e440f5e3}

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.

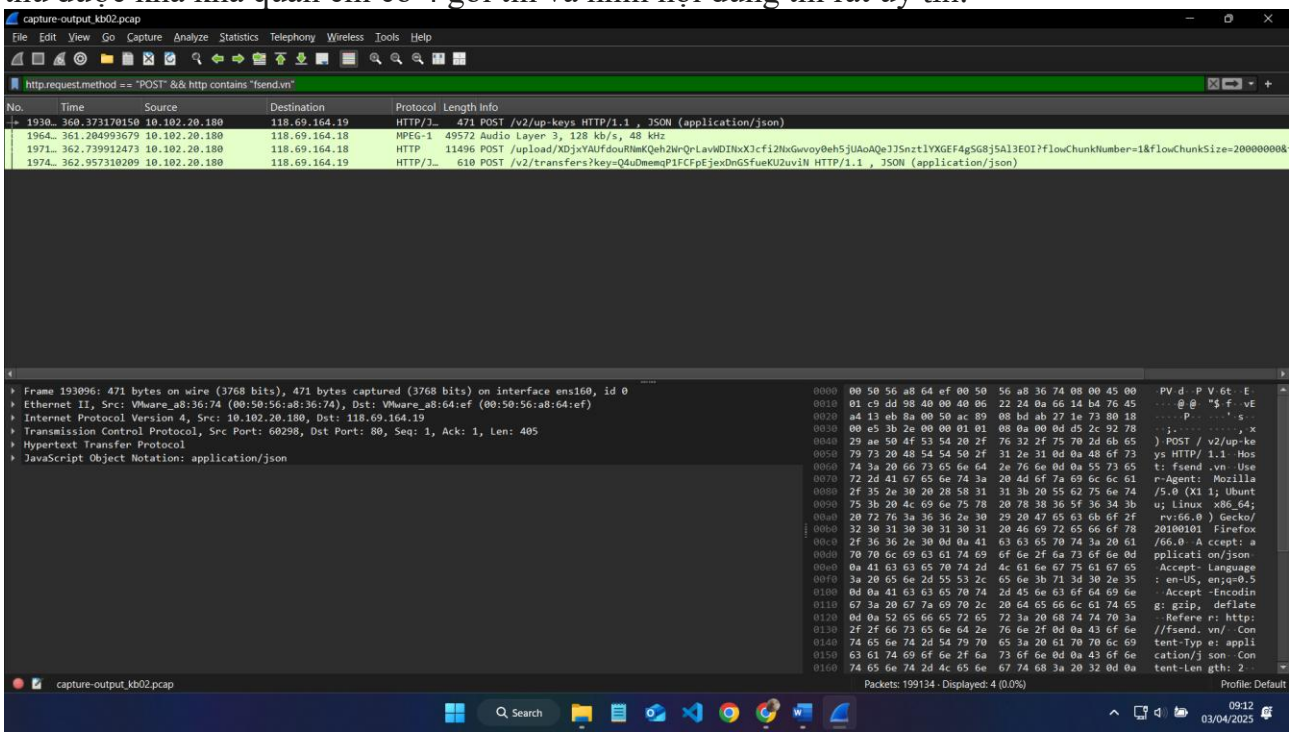
Đầu tiên, ta sẽ phân tích các request HTTP để kiểm tra xem người dùng đã truy cập đến các trang nào, với sự trợ giúp của ChatGPT, ta có được câu lệnh sau sử dụng công cụ tshark:
tshark -r capture-output_kb02.pcap -Y "http.request" -T fields -e http.host -e http.request.uri | sort | uniq -c

```
F:\Downloads\Compressed\capture-output_kb02>tshark -r capture-output_kb02.pcap -Y
"http.request" -T fields -e http.host -e http.request.uri | sort | uniq -c
    370 10.102.20.169:8080      /ping
    146 10.102.20.169:8080      /v2-beta/publish
     28 239.255.255.250:1900    *
      1 connectivity-check.ubuntu.com   /
      1 fsend.vn        /img/slides/slide-2.png
      1 fsend.vn        /img/slides/slide-3.png
      1 fsend.vn        /Roboto-Bold.c0f1e4a4fdfb8048c72e.woff2
      1 fsend.vn        /Roboto-Light.3c37aa69cd77e6a53a06.woff2
      1 fsend.vn        /Roboto-Regular.5136cbe62a63604402f2.woff2
      1 fsend.vn        /v2/services
      1 fsend.vn        /v2/transfers?key=Q4uDmemqP1FCFpEjexDnGSfueKU2uviN
      1 fsend.vn        /v2/up-keys
      2 fsend.vn        /v2/up-keys/Q4uDmemqP1FCFpEjexDnGSfueKU2uviN/upload
      1 linkmaker.itunes.apple.com      /assets/shared/badges/vi-vn/appstore-lrg.svg
     18 ocsp.comodoca.com       /
     30 ocsp.digicert.com       /
      3 ocsp.godaddy.com        /
      5 ocsp.int-x3.letsencrypt.org     /
     21 ocsp.pki.goog   /GTSGIAG3
      2 ocsp.sca1b.amazontrust.com      /
```

2 ocsp.sectigo.com /
2 ocsp.trustwave.com /
2 ocsp2.globalsign.com /gsalphasha2g2
1 ocsp2.globalsign.com /gsorganizationvalsha2g2
1 status.geotrust.com /
1 status.rapidssl.com /
1 tuoitre.vn /
2 up.fshare.vn /upload/dZFL+bxh+3-P3-GAqMhhaORkNJcYxR6ITPZLZBzywLUWX2twgbTa7ZHOtsPUJ45wPUUYvqUceOhozr46?flowChunkNumber=1&flowChunkSize=20000000&flowCurrentChunkSize=4698321&flowTotalSize=4698321&flowIdentifier=4698321-Anh-Oi-O-Lai-Chi-Pu-Dat-Gmp3&flowFilename=Anh-Oi-O-Lai-Chi-Pu-Dat-G.mp3&flowRelativePath=Anh-Oi-O-Lai-Chi-Pu-Dat-G.mp3&flowTotalChunks=1
2 up.fshare.vn /upload/XDjxYAUfdouRNmKQeh2WrQrLavWDINxXJcfi2NxGwvoy0eh5jUAoAQeJJSnztlYXGEF4gSG8j5Al3EOI?flowChunkNumber=1&flowChunkSize=20000000&flowCurrentChunkSize=90429&flowTotalSize=90429&flowIdentifier=90429-imagejpg&flowFilename=image.jpg&flowRelativePath=image.jpg&flowTotalChunks=1

Kết quả thu được là khá nhiều, tuy nhiên, có thể để ý thấy có các domain mà trong đó, request tới 2 domain “fsend.vn” và “fshare.vn” có vẻ như chính là các request upload, thậm chí với request tới domain “fshare.vn” còn kèm cả tên file các thứ.
Chuyển sang công cụ Wireshark để phân tích sâu hơn về các request này.
Với filter để tìm các gói HTTP request tới các domain trên, ta có filter:
http.request.method == "POST" && http contains "fsend.vn"

Ở filter này, ta sẽ tìm các HTTP request có giao thức POST, và domain “fsend.vn”, kết quả thu được khá khả quan chỉ có 4 gói tin và nhìn nội dung thì rất uy tín:



Follow ngay gói đầu tiên, ta có được hầu như đầy đủ thông tin mà ta cần tìm, các file được gửi bao gồm 1 file mp3 và 1 file ảnh:

Anh-Oi-O-Lai-Chi-Pu-Dat-G.mp3

```
{"file_name":"Anh-Oi-O-Lai-Chi-Pu-Dat-G.mp3","file_size":4698321}
HTTP/1.1 200 OK
Server: Fshare
Date: Tue, 21 May 2019 02:56:15 GMT
Content-Type: application/json; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Encoding: gzip
```

image.jpg

```
{"file_name":"image.jpg","file_size":90429}
HTTP/1.1 200 OK
Server: Fshare
Date: Tue, 21 May 2019 02:56:17 GMT
Content-Type: application/json; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Encoding: gzip
```

Ngoài ra, ta còn thu thập được thông tin gửi đi:

```
{"recipients":["duypt@uit.edu.vn"],"message":"Khong o lai dau :v","title":null,"password_lock":null}
HTTP/1.1 201 Created
Server: Fshare
Date: Tue, 21 May 2019 02:56:19 GMT
Content-Type: application/json; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
```

Email người nhận: duypt@uit.edu.vn
Message: “Khong o lai dau :v”
Title: null (bỏ trống)

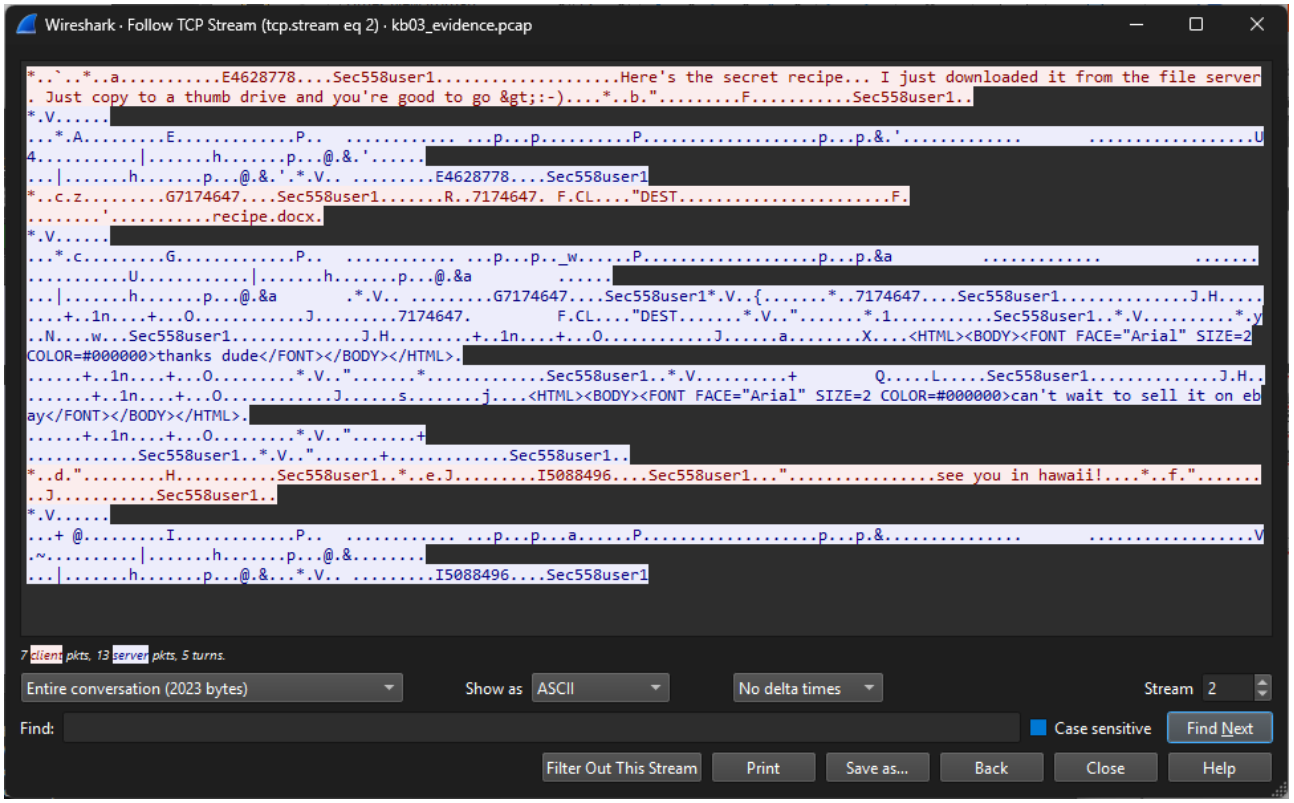
Tuy nhiên, khi tiến hành việc trích xuất nội dung các file đã gửi, thì Wireshark bị đơ, dẫn tới không thể nào trích xuất được.

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 trọng những nhân viên của họ, Ann Dercover là một gián điệp thương mại làm việc chọ công ty đối thủ vì nhân viên này đã từng xâm nhập vào 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.

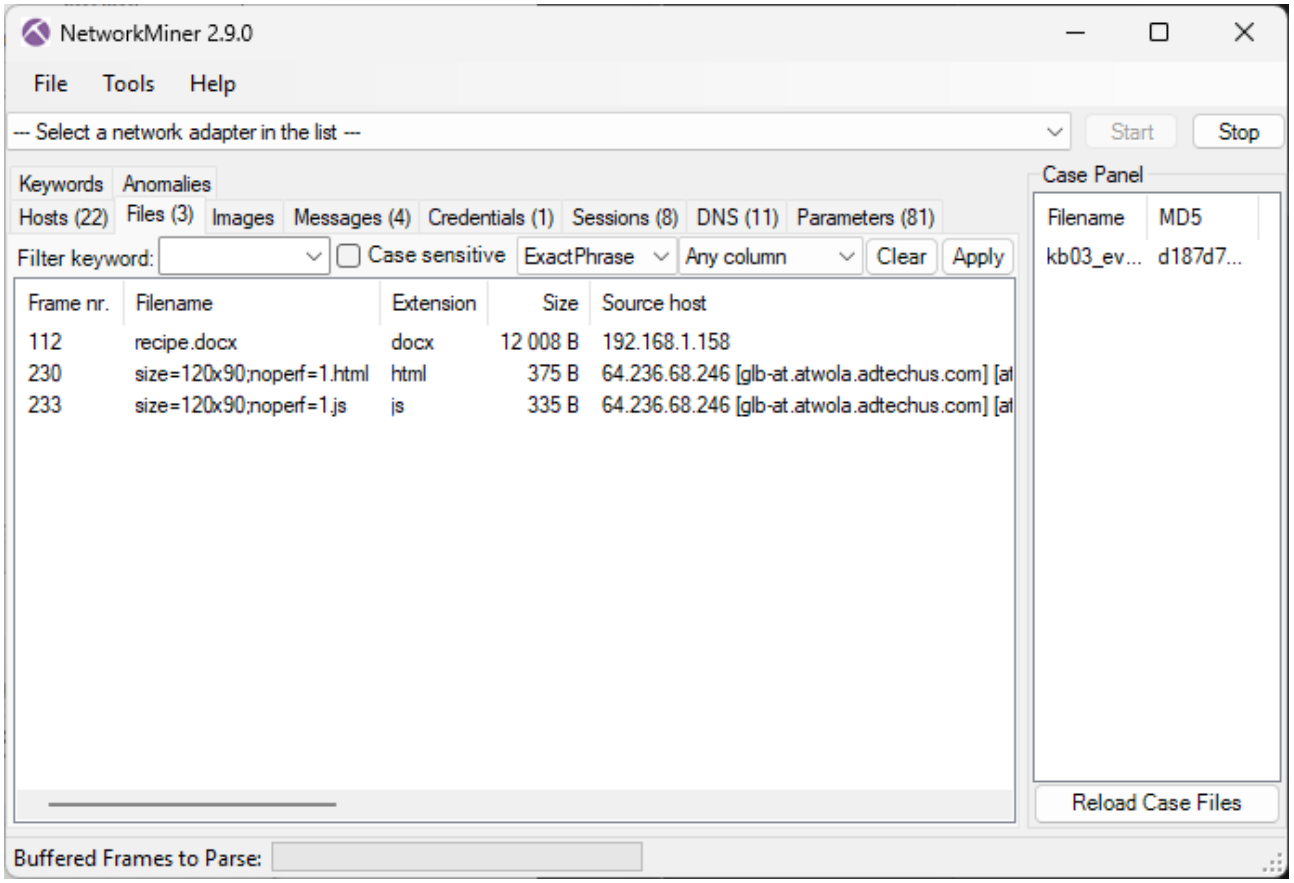
Nhân viên an ninh mạng đã theo dõi Ann một thời gian nhưng chưa phát hiên được gì. Hôm nay, có một laptop lạ đã kết nối vào mạng wireless của công ty. Máy tính của Ann (IP: 192.168.1.158) đã gởi một số tin nhắn tới máy tính đó, laptop lạ ngắt kết nối với mạng wireless ngay sau đó. Dữ liệu mạng của máy 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?

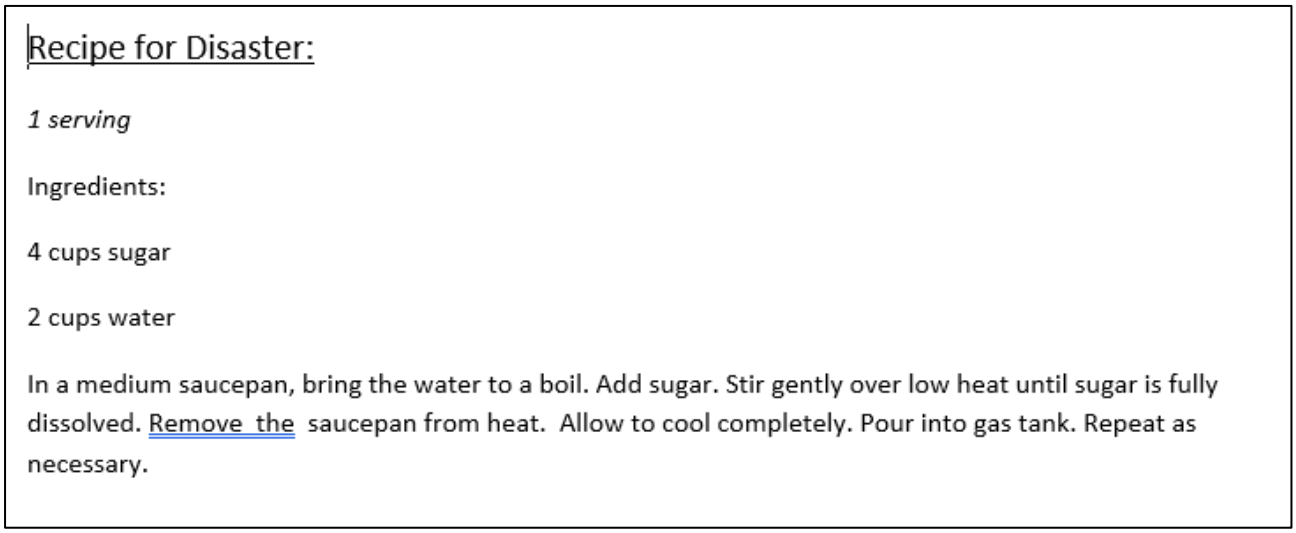
Dựa vào thông tin được cung cấp filter ip 192.168.1.158 → follow TCP Stream 1 gói tin SSL



Xem được một số nội dung khả nghi đặc biệt là file recipe.docx → Dùng NetworkMiner để phân tích và xem thông tin chi tiết hơn



Thấy được file recipe.docx có source host là IP của Ann → Xem nội dung file



Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Có thể thấy Ann đã trộm công thức bí mật của công ty

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