



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 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

- Mở Endpoint 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

Wireshark - Endpoints - traffic_kb01_a.pcap

Endpoint Settings

- ☐ Name resolution
- ☐ Limit to display filter

Copy

Map

Protocol

- ☐ Bluetooth
- ☐ BPv7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA
- ☐ LTP
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP
- ☐ SCTP

Filter list for specific type

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
98.114.205.102	348	184 kB	195	174 kB	153	9 kB						
192.150.11.111	348	184 kB	153	9 kB	195	174 kB						

- Tra cứu ip trên whois

98.114.205.102 - Geo Information

IP Address	98.114.205.102
Host	pool-98-114-205-102.phlpa.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)

Map Location new

☒ World Map
 ☐ Google Maps
 ☐ Yahoo Maps
 ☐ Microsoft Live Maps

- 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

Wireshark - Conversations - traffic_kb01.pcap

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Limit to display filter

Copy

Follow Stream...

Ethernet · 1IPv4 · 1IPv6TCP · 5UDP

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 ràng
- Kiểm tra gói tin giao thức SMB thì thấy nạn nhân dùng hệ điều hành Windows

No.	Time	Source	Destination	Protocol	Length	Info
10	0.267724	98.114.205.102	192.150.11.111	SMB	191	Negotiate Protocol Request
13	0.487136	192.150.11.111	98.114.205.102	SMB	143	Negotiate Protocol Response
14	0.602288	98.114.205.102	192.150.11.111	SMB	222	Session Setup AndX Request, NTLMSSP_NEGOTIATE
16	0.723001	192.150.11.111	98.114.205.102	SMB	311	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
17	0.840405	98.114.205.102	192.150.11.111	SMB	276	Session Setup AndX Request, NTLMSSP_AUTH, User: \
19	0.957617	192.150.11.111	98.114.205.102	SMB	175	Session Setup AndX Response
20	1.073151	98.114.205.102	192.150.11.111	SMB	152	Tree Connect AndX Request, Path: \\192.150.11.111\ipc\$
22	1.189374	192.150.11.111	98.114.205.102	SMB	114	Tree Connect AndX Response
23	1.307145	98.114.205.102	192.150.11.111	SMB	158	NT Create AndX Request, FID: 0x4000, Path: \lsarpc
25	1.424860	192.150.11.111	98.114.205.102	SMB	193	NT Create AndX Response, FID: 0x4000
26	1.542389	98.114.205.102	192.150.11.111	DCERPC	214	Bind: call_id: 1, Fragment: Single, 1 context items: DSSETUP V0.0 (32bit NDR)
28	1.670219	192.150.11.111	98.114.205.102	DCERPC	182	Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance
33	1.805992	98.114.205.102	192.150.11.111	DSSETUP	454	DsRoleUpgradeDownlevelServer request[Long frame (3208 bytes)]
38	2.134590	192.150.11.111	98.114.205.102	DSSETUP	162	DsRoleUpgradeDownlevelServer response[Long frame (20 bytes)]

> Frame 19: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits)	0000 00 08 e2 3b 56 01 00 30 48 62 4e 4a 08 00 45 00 ...jV..0 HbNj..E
> Ethernet II, Src: SuperMicroCo_62:4e:4a (00:30:48:62:4e:4a), Dst: Cisco_3b:56:01 (00:00:03:00:00:01)	0010 00 a1 05 a2 40 00 00 38 d7 c0 96 0b 6f 62 72 ...@..8...obr
> Internet Protocol Version 4, Src: 192.150.11.111, Dst: 98.114.205.102	0020 cd 66 01 bd 07 24 5b d5 10 19 08 cf f9 32 50 18 ...f...\$[...2P
> Transmission Control Protocol, Src Port: 445, Dst Port: 1828, Seq: 347, Ack: 528, Len: 175	0030 21 80 ea 99 00 00 00 00 00 75 ff 53 4d 42 73 00 !...\$...u.SMBs
> NetBIOS Session Service	0040 00 00 00 98 07 c8 00 00 00 00 00 00 00 00 00 ...000000000000
> SMB (Server Message Block Protocol)	0050 00 00 00 00 ff fe 00 00 20 00 04 ff 00 75 00 00 ...000000000000
	0060 00 00 00 4a 00 4e 57 00 69 00 6a 00 64 00 6f 00 ...000000000000
	0070 77 00 73 00 20 00 35 00 2e 00 31 00 00 00 57 00 ...000000000000
	0080 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 32 00 ...000000000000
	0090 30 00 30 00 30 00 20 00 4c 00 41 00 4e 00 20 00 ...0000LAN
	00a0 4d 00 61 00 6e 00 61 00 67 00 65 00 72 00 00 00 ...Managern

➔ 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 stream TCP, sau đó phân tích stream đã giải mã để tìm flag.

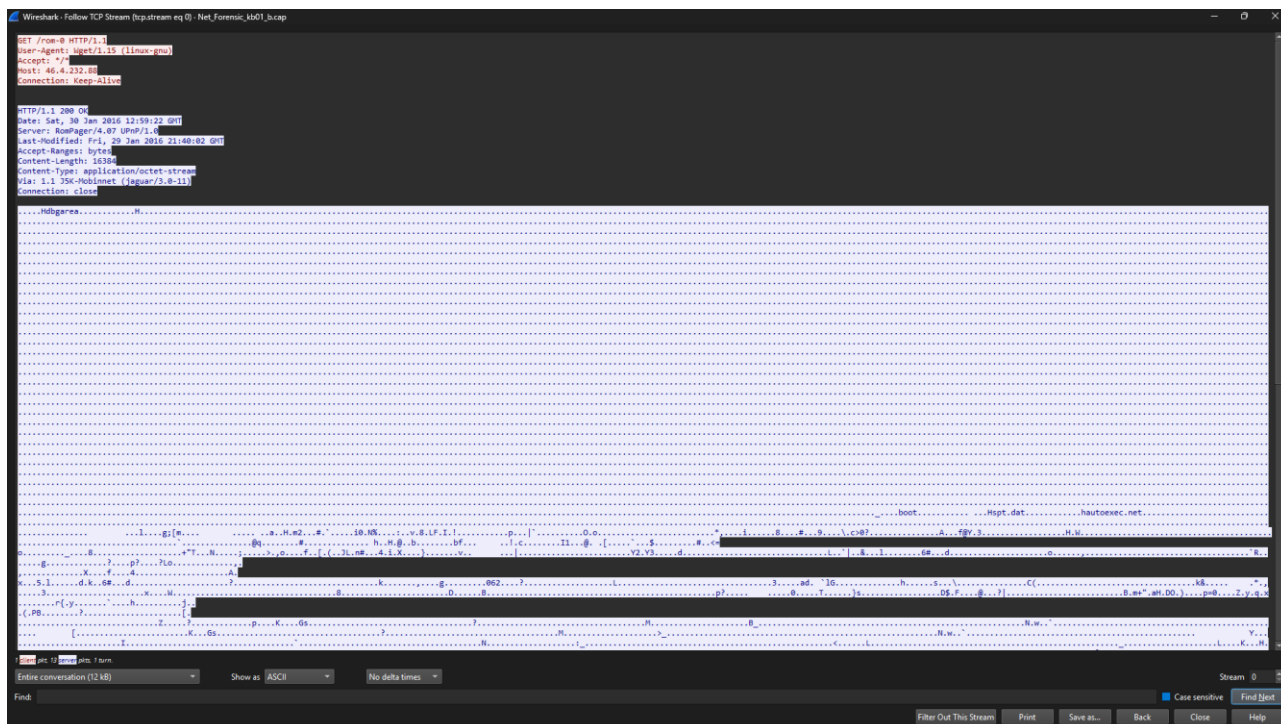
Dùng aircrack-ng để xem các thông tin cơ bản

```
tung@tung-virtual-machine: ~/Downloads
tung@tung-virtual-machine:~/Downloads$ aircrack-ng Net_Forensic_kb01_b.
Net_Forensic_kb01_b.cap Net_Forensic_kb01_b.rar
tung@tung-virtual-machine:~/Downloads$ aircrack-ng Net_Forensic_kb01_b.cap
Reading packets, please wait...
Opening Net_Forensic_kb01_b.cap
Read 8525 packets.

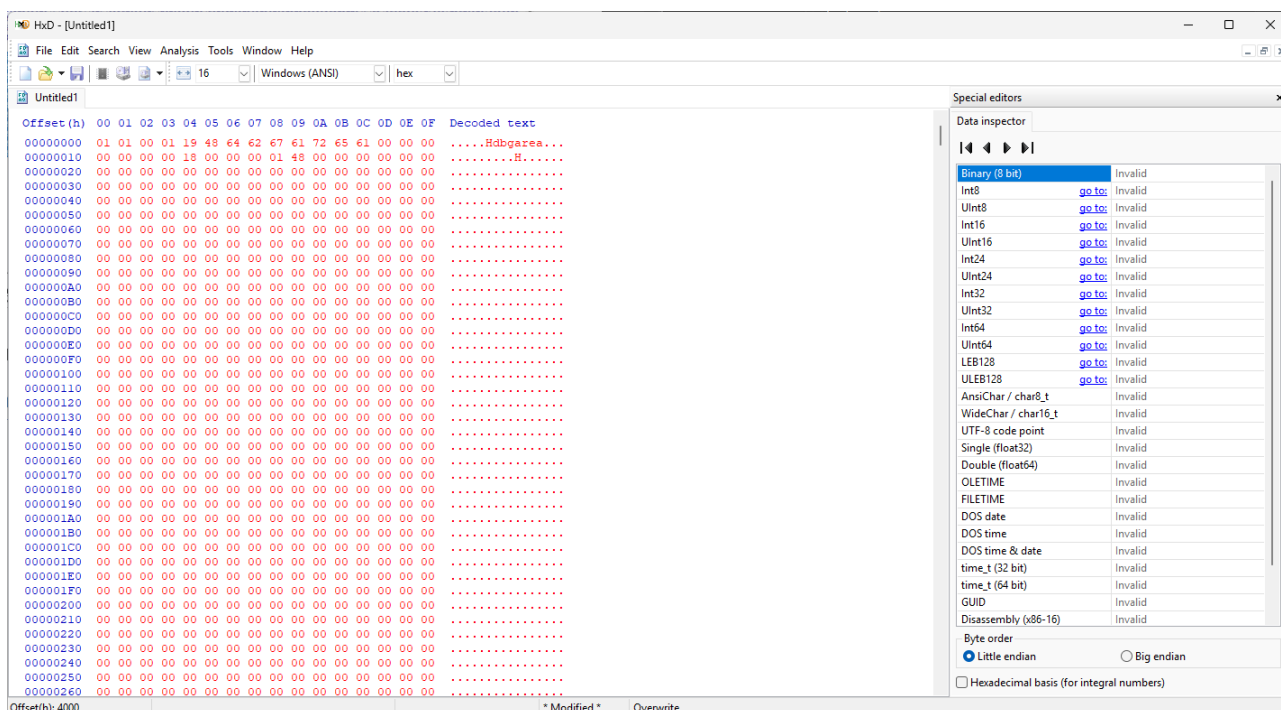
# BSSID ESSID Encryption
1 38:AA:3C:32:46:60 SD Unknown
2 74:EA:3A:FF:0F:48 Rome WPA (1 handshake)

Index number of target network ?
```

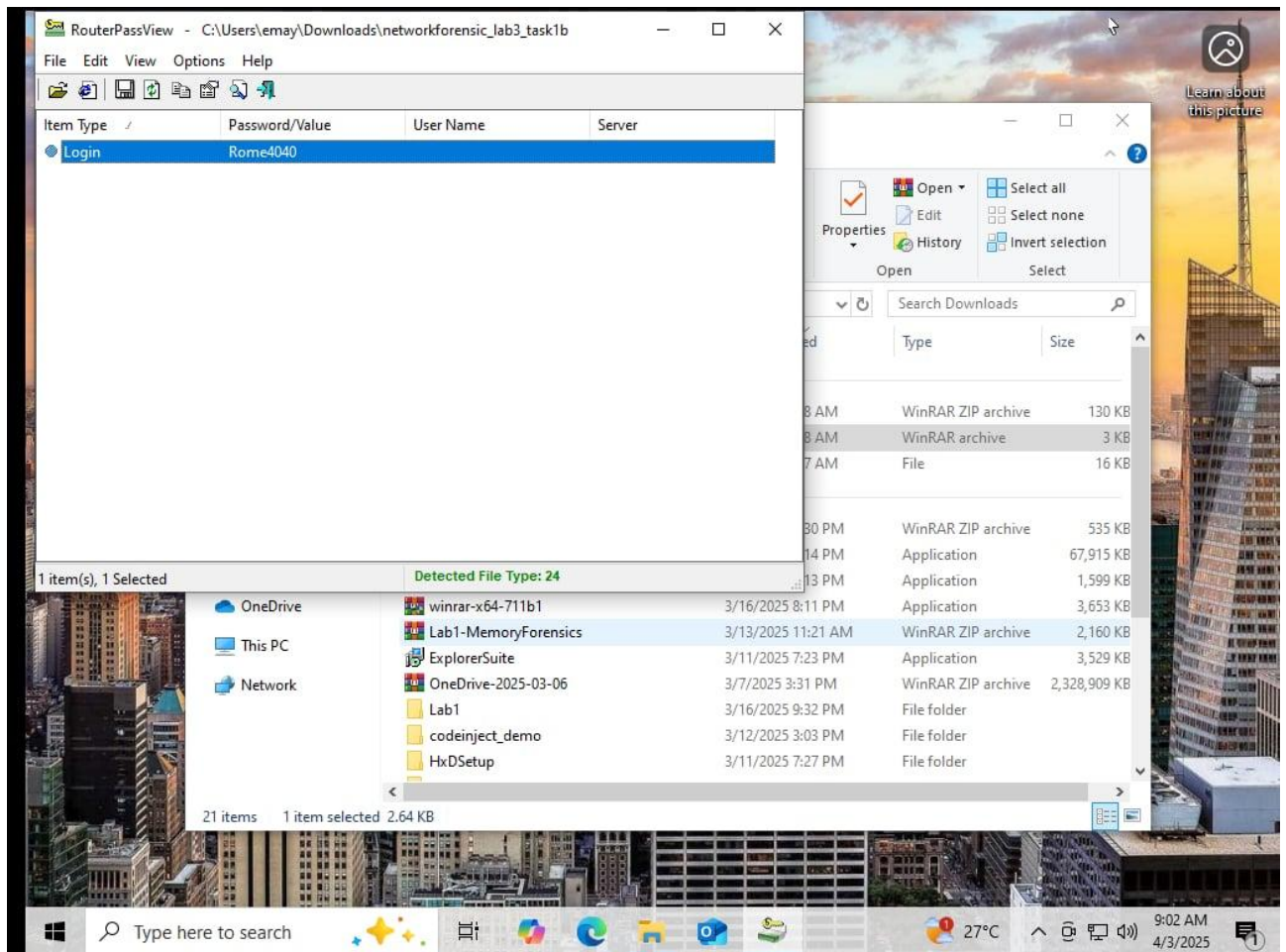
Dùng wireshark lọc cái gói tin TCP ➔ chọn 1 gói tin TCP bất kỳ ➔ vào TCP Stream để xem đầy đủ thông tin được gửi đi thấy “Hdbgarea” là đoạn mở đầu trong file cấu hình của RouterPassView



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

```
tung@tung-virtual-machine: ~/Downloads
tung@tung-virtual-machine:~/Downloads$ airdecap-ng -e 'Rome' -p Rome4040 Net_For
ensic_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
tung@tung-virtual-machine:~/Downloads$
```

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

```
tung@tung-virtual-machine: ~/Downloads
tung@tung-virtual-machine:~/Downloads$ ls
'Digital Forensics #5 - Windows Forensics Recovery - 2025.pdf'
'Lab 2 - Improving Mod Security WAF.pdf'
Net_Forensic_kb01_b.cap
Net_Forensic_kb01_b-dec.cap
Net_Forensic_kb01_b.rar
tung@tung-virtual-machine:~/Downloads$ strings Net_Forensic_kb01_b-dec.cap | grep -i ctf
SharifCTF{be02d2a396482969e39d92b6e440f5e3}
GET /collect?v=1&v=j40&a=1583904745&t=pageview&s=1&dl=http%3A%2F%2Fpastebin.com%2FHKKhaf6&ul=en-us&de=UTF-8&dt=SharifCTF%7Bbe02d2a396482969e39d92b6e440f5e3%7D%20-%20Pastebin.com&sd=32-bit&sr=360x640&vp=360x592&je=1&_u=ACCAgEQ~&jid=950215741&cid=899094573.1454153414&tid=UA-58643-34&z=1248163907 HTTP/1.1
tung@tung-virtual-machine:~/Downloads$
```

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.c0f1e4a4fdffb8048c72e.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 obsp.comodoca.com /
30 obsp.digicert.com /
3 obsp.godaddy.com /
5 obsp.int-x3.letsencrypt.org /
21 obsp.pki.goog /GTSIGAG3
2 obsp.sca1b.amazontrust.com /
```

```

2 obsp.sectigo.com /
2 obsp.trustwave.com /
2 obsp2.globalsign.com /gsalpatha2g2
1 obsp2.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&flowT
otalSize=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/XDjxYAUfdouRNmKQeh2WrQrLavWDINxXJcfi2NxGwvoy0eh5jUAoAQeJJSnztly
XGEF4gSG8j5Al3EOI?flowChunkNumber=1&flowChunkSize=20000000&flowCurrentChu
nkSize=90429&flowTotalSize=90429&flowIdentifier=90429-
image.jpg&flowFilename=image.jpg&flowRelativePath=image.jpg&flowTotalChunks=1**

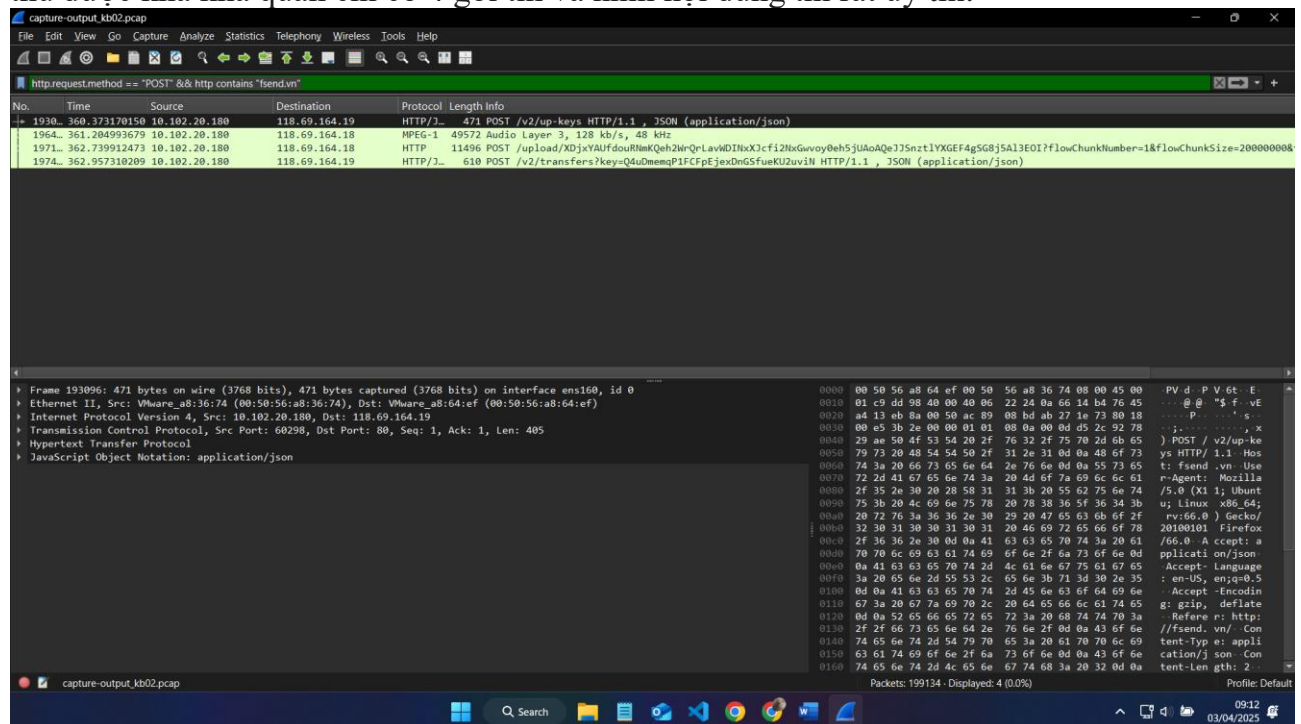
Kết quả thu được là khá nhiều, tuy nhiên, có thể dễ dàng thấy có các domain mà trong đó, request tới 2 domain “fsend.vn” và “fshare.vn” có vẻ như chính là các request upload, thậm chí với request tới domain “fshare.vn” còn kèm cả tên file các thứ.

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”

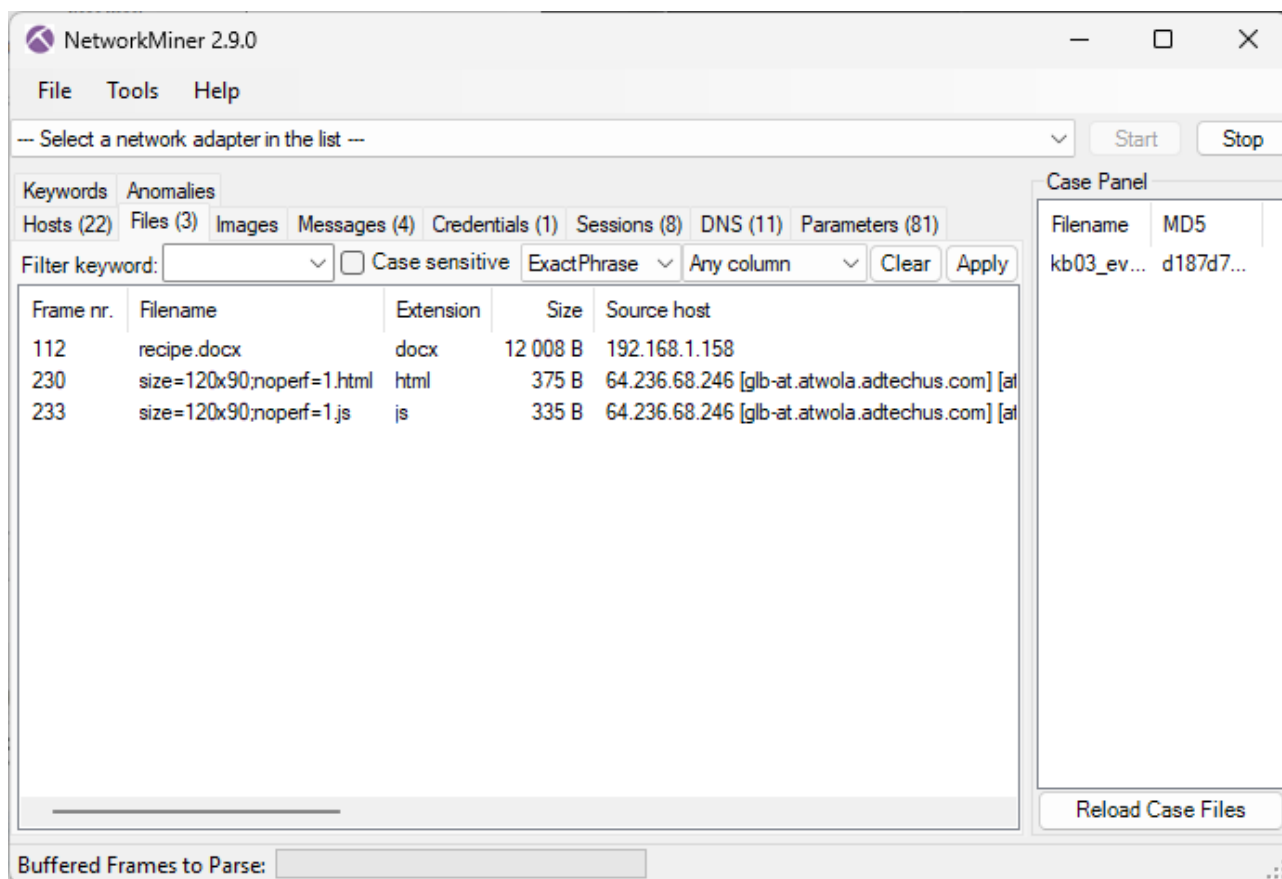
Title: null (bỏ trống)

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. 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.



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, trể, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT