



4

Session

Network Forensics

Điều tra số trên môi trường mạng

**Tài liệu Thực hành
Pháp chứng Kỹ thuật số**

GVTH: ThS. Phan Thế Duy

Học kỳ II – Năm học 2021-2022

Tp. HCM, 4.2022

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

Bài thực hành này giúp sinh viên được làm quen, sử dụng, tăng cường kiến thức về các kỹ năng điều tra kỹ thuật số liên quan đến việc phân tích dữ liệu mạng (network forensics).

2. Giới thiệu kỹ thuật điều tra mạng

Điều tra mạng

Kỹ thuật điều tra mạng (Network Forensics) là một nhánh của khoa học điều tra số liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập. Network Forensics cũng được hiểu như Digital Forensics trong môi trường mạng. Đây là một lĩnh vực tương đối mới của khoa học pháp chứng. Về cơ bản, Network Forensics là việc chặn bắt, ghi âm và phân tích các sự kiện mạng để khám phá nguồn gốc của các cuộc tấn công hoặc sự cố của một vấn đề nào đó. Sự phát triển mỗi ngày của Internet đồng nghĩa với việc máy tính đã trở thành mạng lưới trung tâm và dữ liệu bây giờ đều khả dụng trên các chứng cứ số được lưu trên đĩa cứng máy tính. Điều tra mạng có thể được thực hiện như một cuộc điều tra độc lập hoặc kết hợp với việc phân tích pháp y máy tính (computer forensics) – thường được sử dụng để phát hiện mối liên kết giữa các thiết bị kỹ thuật số hay tái tạo lại quy trình phạm tội.

Thuật ngữ Network Forensics (điều tra mạng) được đưa ra bởi chuyên gia bảo mật máy tính Marcus Ranum vào đầu những năm 90, vay mượn từ các lĩnh vực pháp luật và tội phạm nơi mà “forensics” gắn liền với việc điều tra các hành vi phạm tội. Không giống các mảng khác của digital forensics, điều tra mạng giải quyết những thông tin dễ thay đổi và biến động. Lưu lượng mạng được truyền đi và sau đó bị mất, do đó network forensics thường là cuộc điều tra rất linh hoạt, chủ động.

Trong môi trường hiện nay, *network forensics* thường được thực hiện để phân tích sự xung đột diễn ra giữa những kẻ tấn công và người phòng thủ. Thông thường, các điều tra viên cố gắng ngăn chặn sự bùng phát sâu máy tính, điều tra hành vi vi phạm, thu thập chứng cứ cho tòa án. Các kỹ năng, kỹ thuật cần thiết cho việc phân tích pháp y mạng rất sâu rộng và nâng cao, cùng một nhà điều tra có thể được kêu gọi để khai thác bộ nhớ cache từ web proxy hay sniff thụ động lưu lượng truy cập mạng và xác định các hoạt động đáng ngờ.

Hầu hết các kỹ thuật hiện nay là giám sát thụ động, chủ yếu dựa trên lưu lượng mạng, hiệu năng CPU hoặc quá trình nhập/ xuất (Input/Output) với sự can thiệp của con người. Trong đa số các trường hợp, dấu hiệu của cuộc tấn công mới được phát hiện thủ công

hoặc trong một số trường hợp nó không bị phát hiện cho đến khi vụ việc được báo cáo. Trọng tâm của lĩnh vực pháp y mạng là để tự động hóa quá trình phát hiện tất cả các cuộc tấn công và thêm vào đó ngăn chặn các thiệt hại do vi phạm an ninh. Ý tưởng chính của network forensics là xác định tất cả các vi phạm an ninh có thể xảy ra và xây dựng các dấu hiệu vào cơ chế phát hiện và ngăn chặn để hạn chế những mất mát về sau.

Một số điểm lưu ý khi nói đến Network Forensics:

- Nó không phải là một sản phẩm (product) mà là một tiến trình (process) phức tạp (bao gồm các công cụ kỹ thuật, trí tuệ con người, luật pháp...)
- Nó không thay thế cho tường lửa, IDS, IPS,..
- Nó sử dụng các cảnh báo IDS, nhật ký của tường lửa, các gói tin...

Công cụ điều tra trên dữ liệu mạng

Một số công cụ dùng điều tra bằng chứng trên môi trường mạng:

- Wireshark, Network Miner bắt và phân tích gói tin với giao diện đồ họa
- Tshark: Nếu bạn sử dụng các hệ điều hành Linux để phân tích tập tin PCAP thì tshark là một lựa chọn không thể thiếu. Đây là một công cụ khá hiệu quả khi phân tích các tập tin PCAP trên giao diện command line. tshark cung cấp đầy đủ các chức năng như bắt gói tin, đọc và phân tích gói tin, trích xuất dữ liệu...
- Tcpdump phân tích gói tin với giao diện console
- p0f dùng để phát hiện hệ điều hành, console trên nền Linux
- netcat, debug kết nối, đóng vai trò cả client và server, console trên windows và linux
- Snort, opensource phát hiện xâm nhập
- Foremost, Scapy
- Nmap, tcpxtract, ssldump, nslookup, maxmind... và rất nhiều công cụ khác.

Network Forensics trong các cuộc thi CTF

Các thử thách Network Forensics thường yêu cầu người chơi tìm kiếm manh mối, điều tra số dựa trên tập tin ghi lại các dữ liệu truyền nhận giữa các máy tính, thiết bị, thường được lưu trữ dưới dạng file pcap (Packet Capture).

Loại dữ liệu thường gặp nhất trong các đề bài Network Forensics là dữ liệu truyền nhận giữa 2 máy tính. Tuy nhiên, các loại dữ liệu khác cũng có thể xuất hiện trong đề bài CTF

như dữ liệu truyền nhận qua thiết bị lưu trữ ngoài, kết nối các thiết bị ngoại vi hoặc thậm chí dữ liệu mạng viễn thông.

Để giải được các thử thách thuộc mảng Network Forensics, thông thường người chơi phải thực hiện các bước sau:

- Nhận diện loại dữ liệu được truyền nhận (nếu không có lưu ý đặc biệt gì từ đề bài).
- Hiểu và phân tích được các trường thông tin trong luồng dữ liệu.
- Trích xuất được các thông tin thú vị từ luồng dữ liệu.
- Một chút may mắn để tìm thấy “flag” trong các thông tin đã trích xuất.

Một số phương pháp để tìm thông tin chứng cứ trong các bài liên quan đến điều tra mạng:

- Sử dụng công cụ Wireshark/tshark để đọc và phân tích dữ liệu.
- Sử dụng công cụ NetworkMiner để trích xuất nhanh các thông tin cơ bản.
- Sử dụng các thư viện của python để phân tích thủ công một số thông tin khác.

3. Môi trường & cấu hình

- Sử dụng các thiết bị và tài liệu, khuyến cáo được cung cấp bởi GVTH, yêu cầu tác phong nghiêm túc trong quá trình thực hiện.
- Công cụ gợi ý: Wireshark, Tcpdump, tcpextract, tshark, NetworkMiner ...
- Tài liệu nên đọc: Sách “*Learning Network Forensics*” (tác giả: Samir Datt - 2016), Sách “*Digital Forensics and Incident Response*” (tác giả: Gerard Johansen - 2017).

B. THỰC HÀNH

Sinh viên thực hiện điều tra theo yêu cầu của GVHD, làm theo nhóm thực hành đã đăng ký trên lớp trong buổi thực hành.

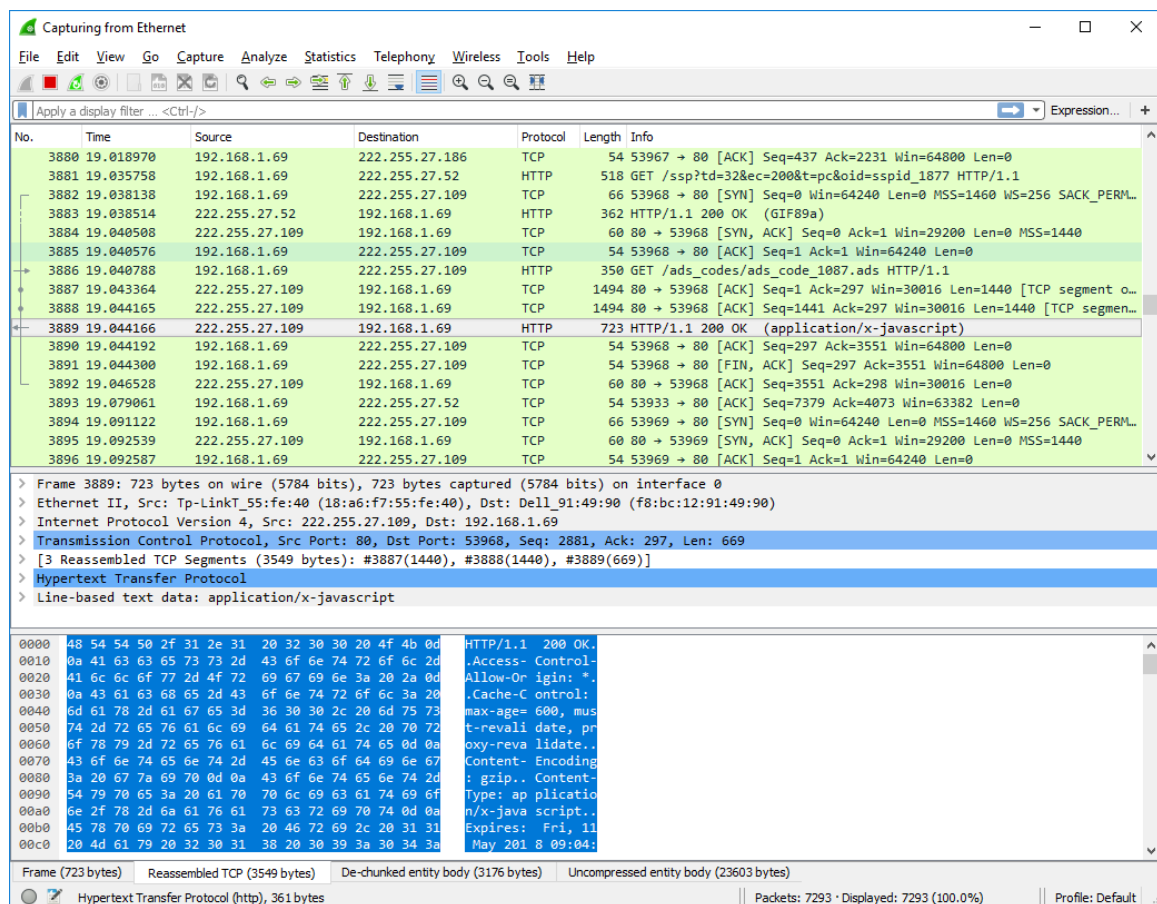
B1. Phân tích dữ liệu mạng bằng Wireshark

Giúp sinh viên nắm bắt và hiểu rõ các tính năng của công cụ phần mềm **Wireshark** khi tiến hành điều tra và tìm kiếm thông tin chứng cứ trong file pcap.

- Wireshark là một chương trình bắt và phân tích gói tin, giao thức rất mạnh, chi tiết về nó có thể tìm hiểu thêm ở những tài liệu khác. Từ việc phân tích, người điều tra có thể lấy được một số thông tin về những gì đã xảy ra trong mạng:

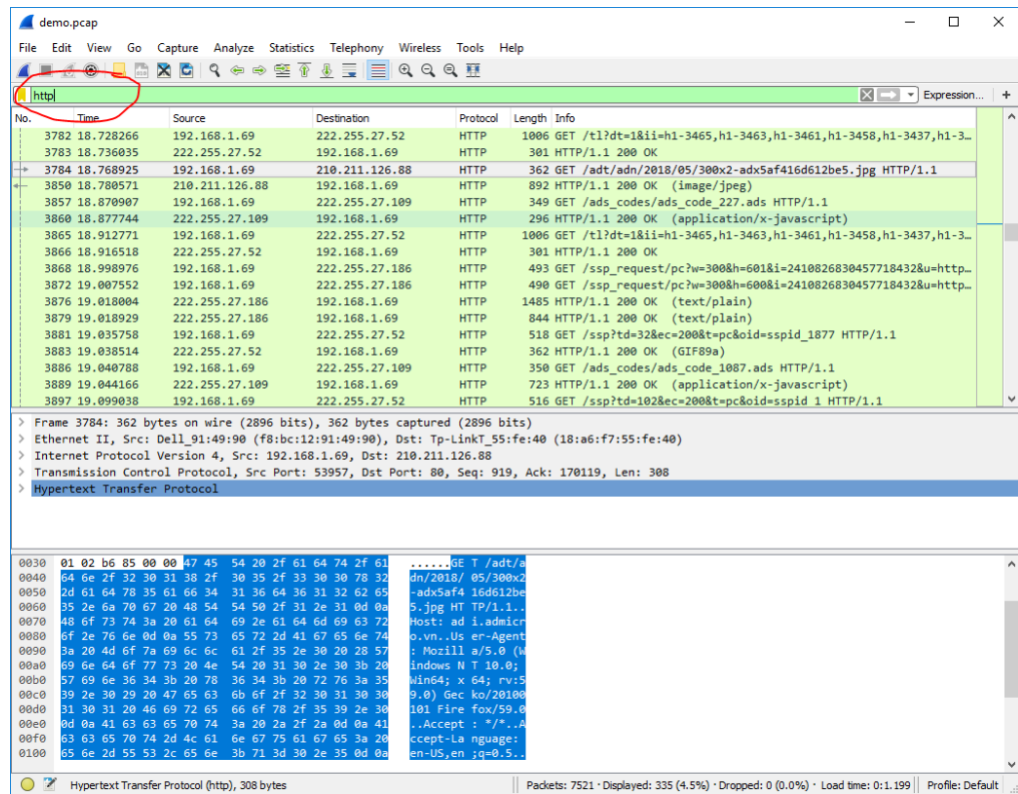
- Địa chỉ IP của kẻ tấn công và của nạn nhân
 - Thông tin về kẻ tấn công
 - Có bao nhiêu phiên TCP (TCP session) trong file dump
 - Cuộc tấn công kéo dài bao lâu
 - Dịch vụ nào trên máy nạn nhân có thể là mục tiêu tấn công? Lỗ hổng là gì?
- Thực hiện cài đặt **Wireshark**.

Liên kết tải: <https://www.wireshark.org/download.html>



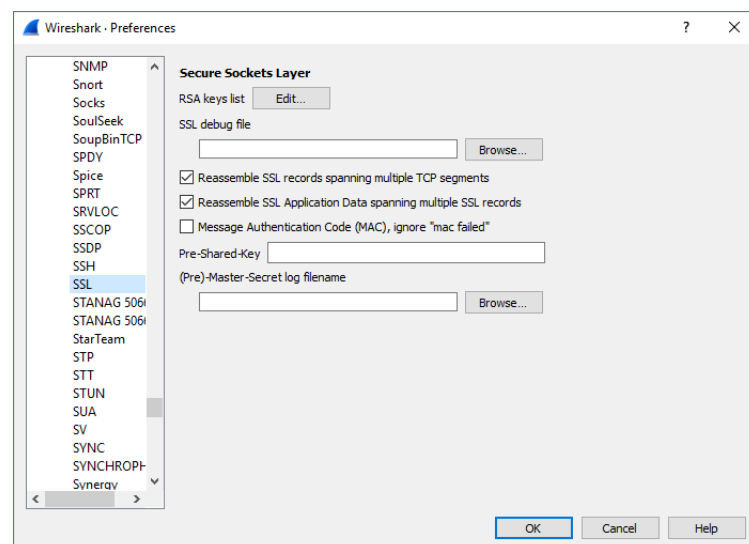
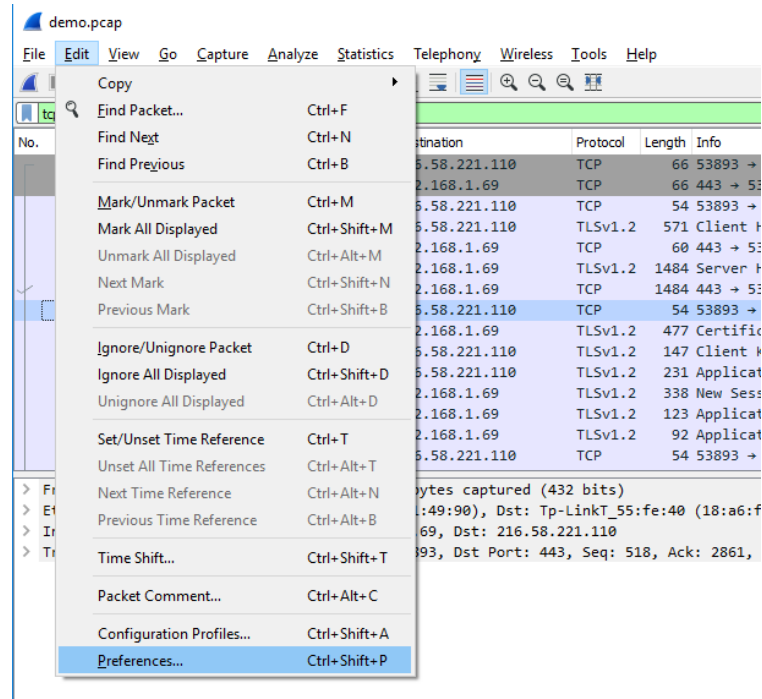
Hình 1. Giao diện công cụ Wireshark

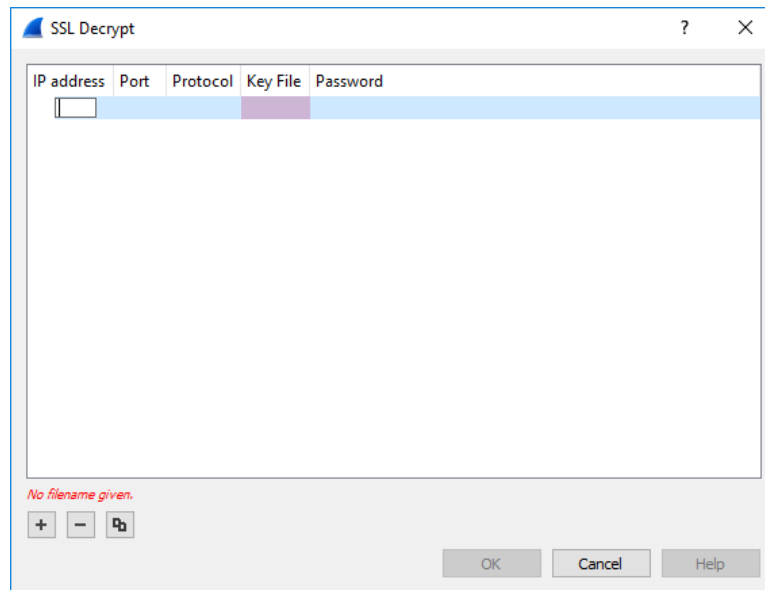
- Filter: Thông thường một file pcap nhận được sẽ chứa rất nhiều luồng dữ liệu trong đó, nếu chỉ lần lượt lướt qua từng gói tin, gần như chắc chắn bạn sẽ không thể tìm được thông tin cần thiết. Để thu hẹp số lượng gói tin cần rà soát, bạn có thể sử dụng chức năng “filter” của wireshark để lọc bớt các gói tin không cần thiết tùy vào từng tình huống gặp phải.
Để sử dụng chức năng này, bạn nhập filter mong muốn vào ô nhập “Filter” trên giao diện Wireshark. Chẳng hạn, để hiển thị riêng các gói tin HTTP, chỉ cần nhập “http”. Thậm chí bạn còn có thể lọc chi tiết hơn, chẳng hạn chỉ hiển thị các bản tin HTTP GET bằng cú pháp filter “http.request.method == GET”.



Hình 2. Chức năng Filter

- Giải mã SSL: Một chức năng khá hay khác của Wireshark là giải mã các bản tin SSL khi có Private Key. Chức năng này khá hữu ích khi gặp các loại dữ liệu SSL, đặc biệt là các phiên truy cập các trang web https. Để sử dụng chức năng này, chọn menu Edit > Preferences. Chọn tiếp Protocols > SSL. Chọn Edit và thêm entry mới. Sau khi thêm entry, các traffic SSL đến địa chỉ IP đã cấu hình sẽ được Wireshark tự động giải mã và phân tích, hiển thị theo nội dung gói tin bên trong lớp mã hóa SSL.





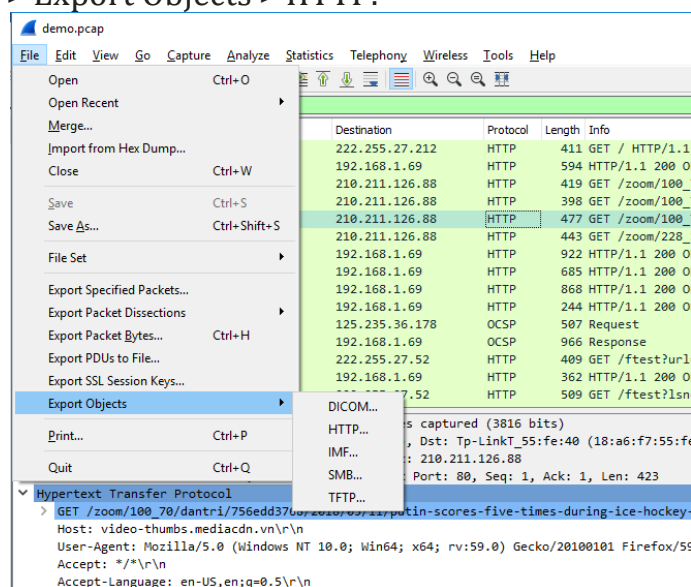
Hình 3. Chức năng giải mã SSL

- Export Packet: Sau khi đã phân tích sơ bộ được các gói tin quan trọng, nhu cầu tiếp theo là export các nội dung có trong các gói tin thành các tập tin dữ liệu. Để làm được việc này, bạn có thể sử dụng chức năng trích xuất gói tin của Wireshark.

Wireshark hỗ trợ khá nhiều phương pháp trích xuất khác nhau:

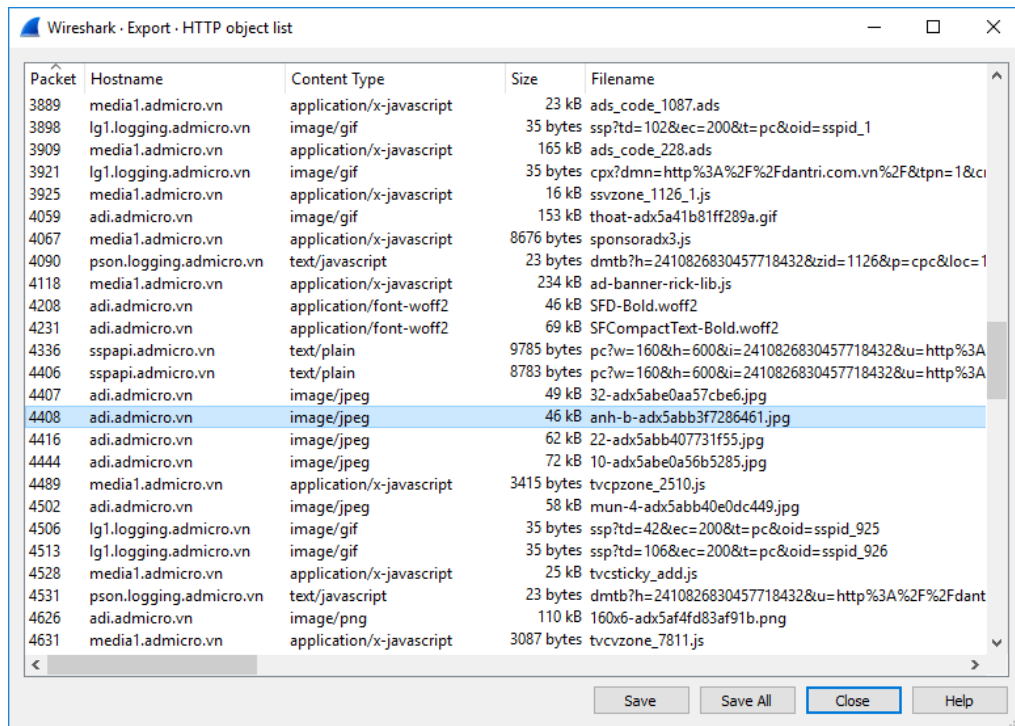
- Trích xuất các gói tin theo filter/tùy theo lựa chọn.
- Trích xuất thành dạng plain text, csv, “C” array...
- Trích xuất riêng nội dung gói tin.
- Trích xuất SSL Session Key.
- Trích xuất các object trong các gói tin (chẳng hạn như các file được truyền nhận qua HTTP...).

Chẳng hạn, để trích xuất các file được truyền nhận qua HTTP, lựa chọn menu File > Export Objects > HTTP.



Hình 4. Chức năng Export Packet

Sau đó, bạn có thể lựa chọn file muốn trích xuất hoặc trích xuất toàn bộ các file được truyền nhận.



Hình 5. Chọn tập tin muốn trích xuất từ gói tin

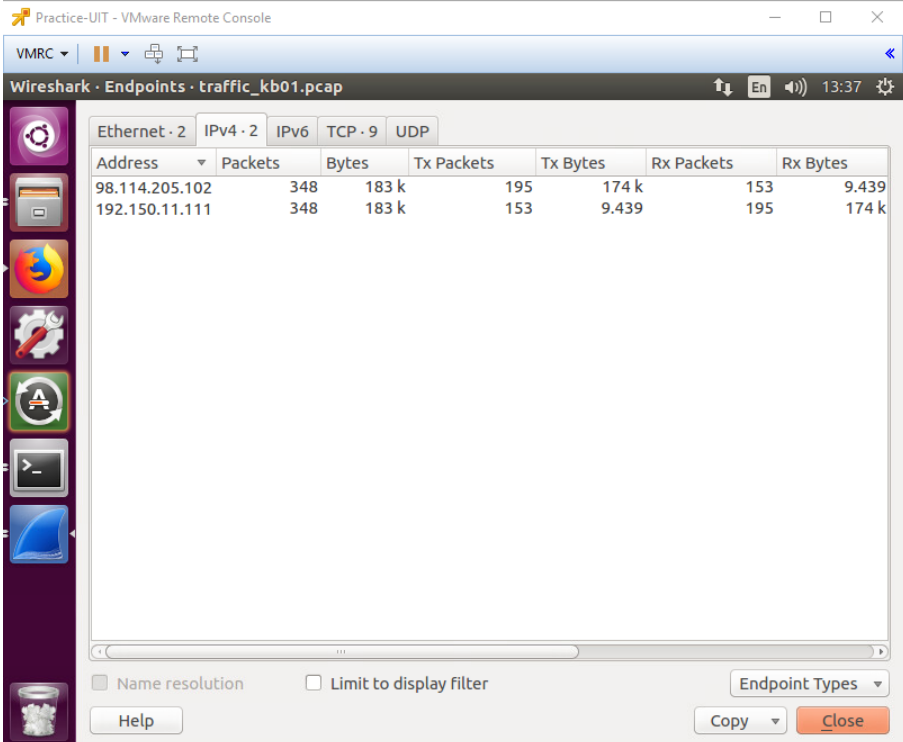
Kịch bản 01-a. Thực hiện phân tích tập tin dữ liệu mạng.

- 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:

Gợi ý:

- Mở file .pcap bằng wireshark, chúng ta có thể thấy ngay danh sách các gói tin truy cập đến máy nạn nhân. Chọn Menu Statistics/Endpoint List/IP v4 để xem danh sách các IP bắt được. Quan sát và ghi nhận kết quả.



Practice-UIT - VMware Remote Console

VMRC

Wireshark · Endpoints · traffic_kb01.pcap

Ethernet · 2 IPv4 · 2 IPv6 TCP · 9 UDP

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
98.114.205.102	348	183 k	195	174 k	153	9.439
192.150.11.111	348	183 k	153	9.439	195	174 k

☐ Name resolution ☐ Limit to display filter

Endpoint Types

Help Copy Close

Có tất cả 2 IP:

- 192.150.11.111 là IP nội bộ, chính là IP của nạn nhân
 - 98.114.205.102 là IP của kẻ tấn công
- Tìm thông tin về kẻ tấn công: Thông tin trong khung chi tiết gói tin, cho ta biết máy kẻ tấn công có địa chỉ MAC là 00:08:e2:3b:56:01(Cisco). Để tìm thêm thông tin về IP, bạn có thể dùng các công cụ geoip, whois trực tuyến hay tích hợp luôn vào wireshark. Ví dụ: có thể dùng công cụ trực tuyến cqcounter để xem thông tin: <http://cqcounter.com/whois/>

whois
IP Address / Domain Name Lookup

Site Info Who Is Trace Route RBL Check What's My IP? Web Search

Enter Domain Name or IP Address: 98.114.205.102

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° 08'53" West
Distance	7692.24 km (4779.73 miles)

Map Location

98.114.205.102 - Whois Information

- ARIN WHOIS data and services are subject to the Terms of Use
- available at: <https://www.arin.net/resources/registry/whois/tou/>
- If you see inaccuracies in the results, please report at: https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
- copyright 1997-2019, American Registry for Internet Numbers, Ltd.

- Có bao nhiêu phiên TCP (TCP session): Khi nhìn vào khung chính của wireshark bạn sẽ thấy có rất nhiều gói tin, nhưng phần lớn trong chúng là những gói tin chào hỏi, xác thực, truyền nhận dữ liệu của một phiên TCP nào đó. Để xem số phiên TCP hiện có, vào Menu Statistics -> Conversations, tab TCP. Chúng ta sẽ thấy thực tế chỉ có 5 phiên qua các cổng khác nhau:

Practice-UIT - VMware Remote Console

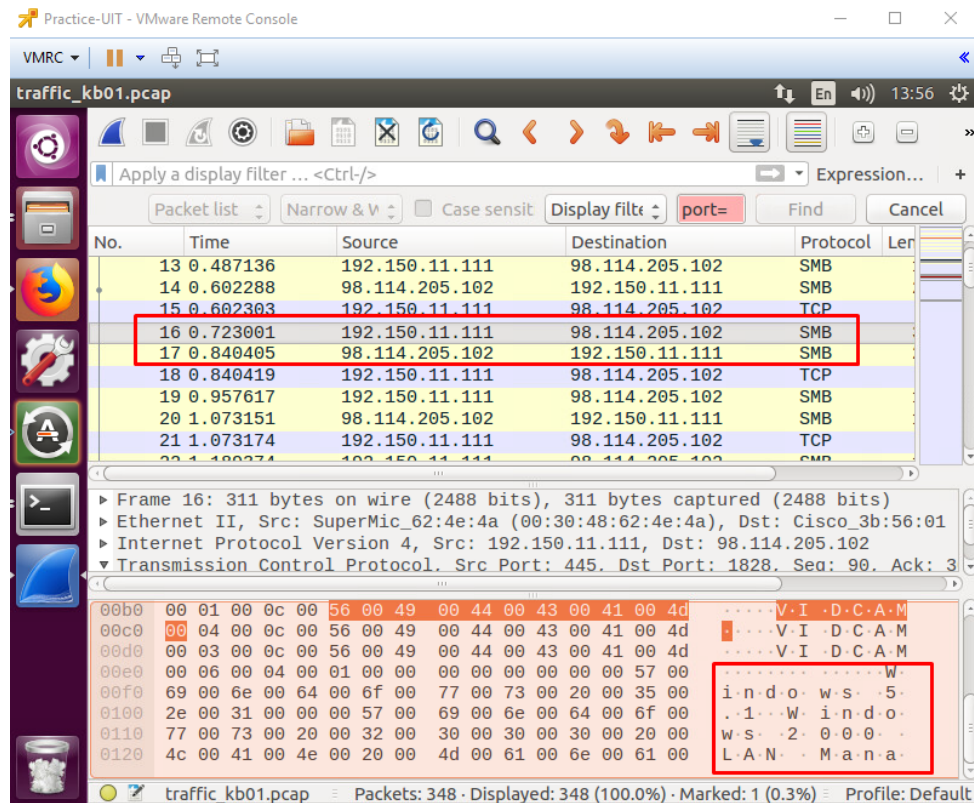
Wireshark - Conversations - traffic_kb01.pcap

Ethernet · 1		IPv4 · 1		IPv6		TCP · 5		UDP	
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Packets B → A		
98.114.205.102	1821	192.150.11.111	445	7	412	4			
98.114.205.102	1828	192.150.11.111	445	31	6.825	14			
98.114.205.102	2152	192.150.11.111	1080	271	173 k	159			
192.150.11.111	1957	98.114.205.102	1924	12	817	6			
192.150.11.111	36296	98.114.205.102	8884	27	2.069	15			

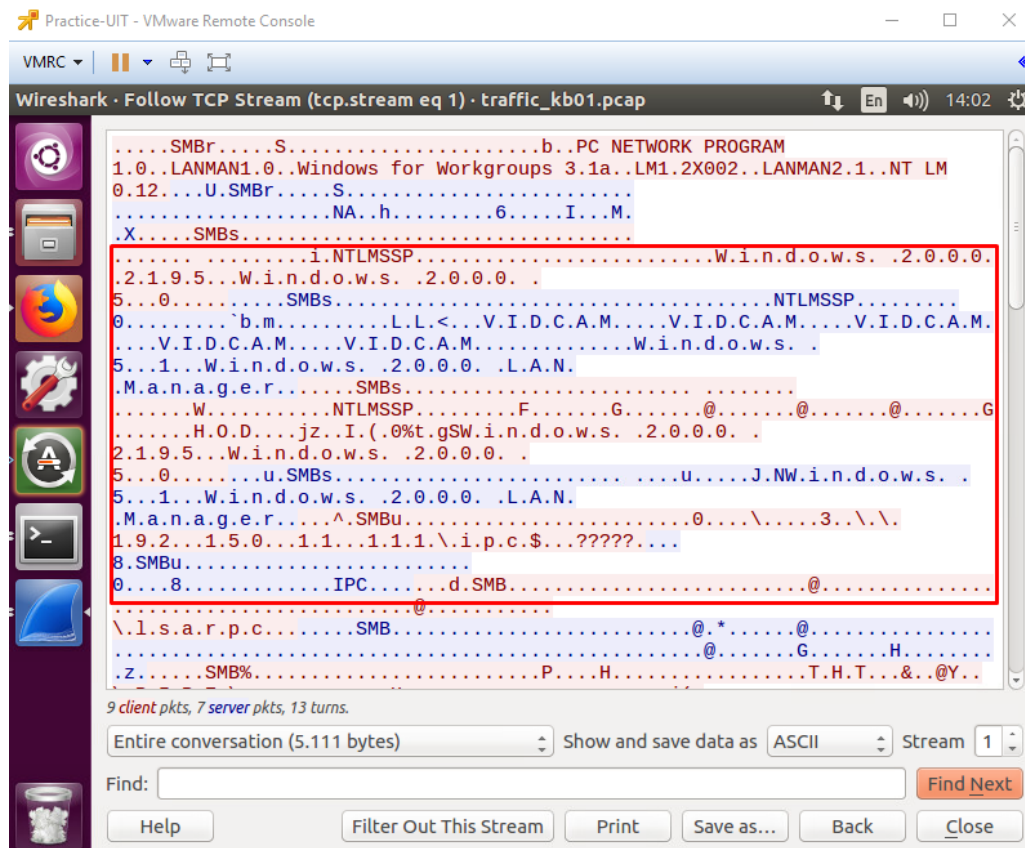
☐ Name resolution
 ☐ Limit to display filter
 ☐ Absolute start time
 Conversation Types

Help Copy Follow Stream... Graph... Close

- Xem cuộc tấn công kéo dài bao lâu
- Xác định lỗ hổng mà kẻ tấn công đã sử dụng



Chú ý cổng 445 trên máy nạn nhân. Đây là cổng chạy dịch vụ SMB (Server Message Block), cung cấp khả năng chia sẻ file giữa các máy tính hoặc máy in và máy tính. SMB từng được biết đến với việc dính một số lỗ hổng bảo mật. Ngoài ra, thông tin bắt được cũng thể hiện máy tính nạn nhân chạy hệ điều hành windows, cụ thể là windows xp hoặc windows 2000.



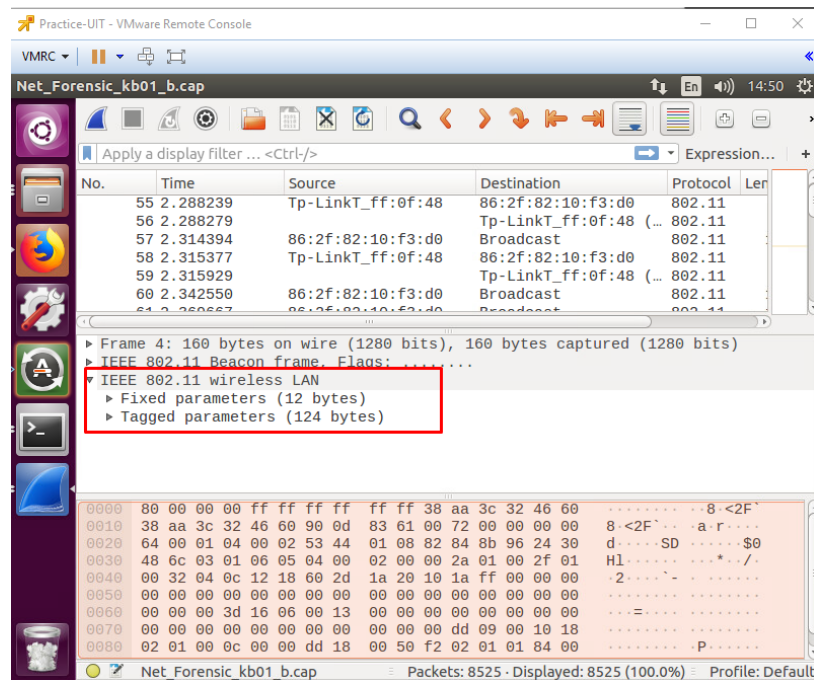
Kịch bản 01-b. Thực hiện phân tích tập tin dữ liệu mạng thu được.

- 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.

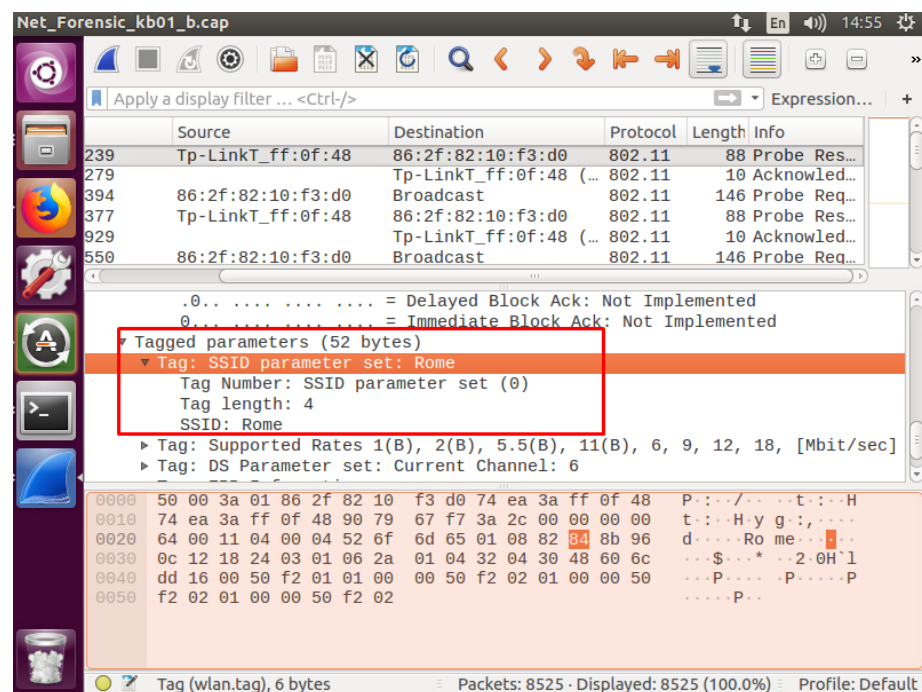
Đáp án: Flag: *be02d2a396482969e39d92b6e440f5e3*

Gợi ý:

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



- Xem SSID:



- Tiếp theo, chúng ta sẽ xem việc truyền dữ liệu mạng không dây này có được mã hóa hay không. Có thể sử dụng công cụ aircrack-ng (cài đặt để sử dụng).


```

Terminal
Apply a display filter ... <Ctrl-/>
Expression... +
Source      Destination      Protocol  Length  Info
239 Tp-LinkT_ff:0f:48 86:2f:82:10:f3:d0 802.11 88 Probe Res...
279 86:2f:82:10:f3:d0 Tp-LinkT_ff:0f:48 (... 802.11 10 Acknowled...
284 86:2f:82:10:f3:d0 Broadcast 802.11 146 Probe Res...

insecclab@uSense: ~/forensics2019/kb01
4 1:1.2-0~beta3-4 [425 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu xenial/main amd64 ieee-data all 20150531.1 [830 kB]
Fetched 1.254 kB in 7s (179 kB/s)
Selecting previously unselected package aircrack-ng.
(Reading database ... 183089 files and directories currently installed.)
Preparing to unpack .../aircrack-ng_1%3a1.2-0~beta3-4_amd64.deb ...
Unpacking aircrack-ng (1:1.2-0~beta3-4) ...
Selecting previously unselected package ieee-data.
Preparing to unpack .../ieee-data_20150531.1_all.deb ...
Unpacking ieee-data (20150531.1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up aircrack-ng (1:1.2-0~beta3-4) ...
Setting up ieee-data (20150531.1) ...
insecclab@uSense: ~/forensics2019/kb01$ aircrack-ng Net_Forensic_kb01_b.cap
Opening Net_Forensic_kb01_b.cap
Read 8525 packets.

# BSSID ESSID Encryption
1 74:EA:3A:FF:0F:48 Rome WPA (1 handshake)
2 38:AA:3C:32:46:60 SD None (192.168.43.61)

Index number of target network ?

```

Aircrack-ng là bộ công cụ dùng để pentest mạng không dây, crack wep và dò khóa wpa/wpa2-psk. Aircrack-ng có rất nhiều công cụ, một số công cụ điển hình:

- airemon-ng: dùng để chuyển card mạng của bạn từ manager sang monitor. Cách dùng: airemon-ng <start|stop|check> <interface> [channel]
- airodump-ng: dùng để bắt gói tin trong mạng wifi (lưu ý là card mạng của bạn phải ở chế độ monitor). Cách dùng: airodump-ng <options> <interface>[,<interface>,...]
- aireplay-ng: dùng để tạo ra gói tin inject gửi tới AP nhằm nhận các gói ARP phản hồi. Cách dùng: aireplay-ng <options> <replay interface>
- packetforge-ng: gửi các gói tin giả trên tới AP để nhận phản hồi. Cách dùng: packetforge-ng <mode> <options>
- airolib-ng: đây là công cụ rất hay giúp chúng ta tạo ra một cơ sở dữ liệu khóa đã được tính toán trước, làm đơn giản hóa quá trình crack key..
- aircrack-ng: crack wep hay dò khóa đều dùng nó. Cách dùng: aircrack-ng [options] <capture file(s)>

Và nhiều công cụ khác... Về các option của các công cụ này, bạn gõ **<man tên tool>** để biết chi tiết.

- Quay trở lại kịch bản, nhận thấy có một số gói tin TCP và ICMP. Sử dụng chức năng Follow TCP stream để xem thêm thông tin. Chú ý đến Hdbgarea trong file dump ra từ TCP stream. Từ khóa 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

```

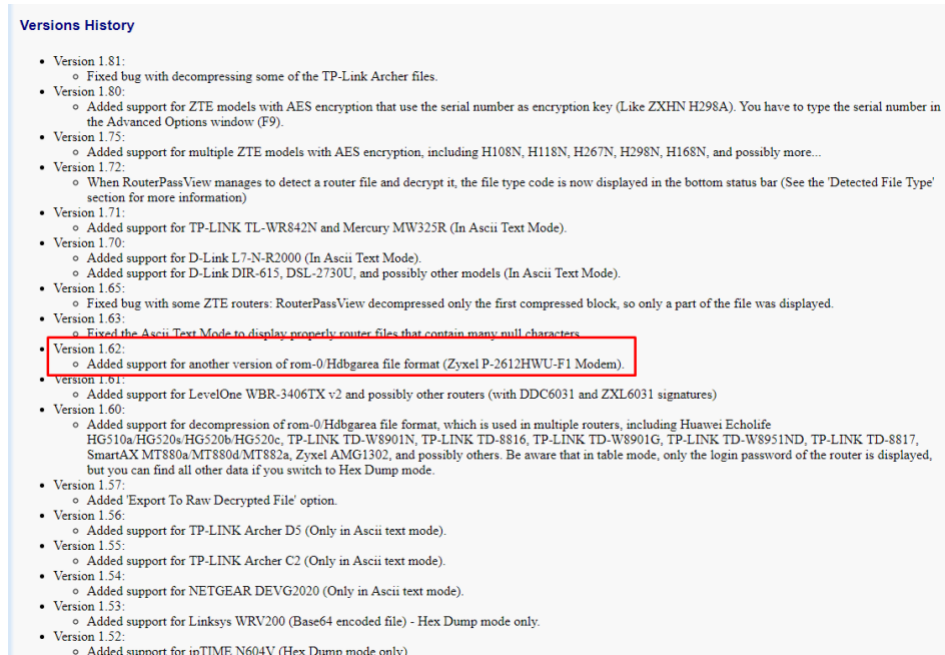
Practice-UIT - VMware Remote Console
Followstream (~/.forensics2019/kb01) - gedit
GET /rom-0 HTTP/1.1
User-Agent: Wget/1.15 (linux-gnu)
Accept: */*
Host: 46.4.232.88
Connection: Keep-Alive

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

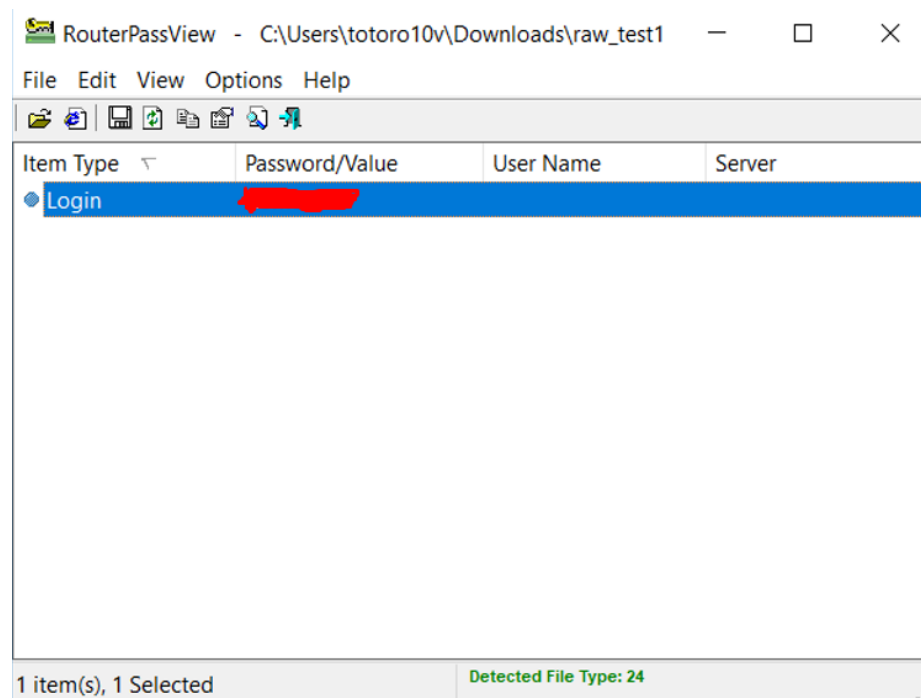
...Hdbgarea...H...
[m...a..H.m2...#...i0.N%...v.8.LF.I...p...|
...O.o...*,...i...8...#...9...
\C>0?...A...f@Y.3...H.W...
h..H.@..b...bf...!.C...I1...@..$....#...<=
o...8...+T...N...;...>...o...f...[.
(..JL.n#...4.i.X...}.V...|.Y2.Y3...d...
Lo...
,.....X...f...4.....A.
x...5.l...d.k..6#...d...?.....k...
`lG.....h...s...\.C
(.3.....x...W...8.....
S.....DS.F...@...?|.....B.m
  
```

Lưu nội dung TCP stream này sau khi đã xóa tất cả các header thành file nhị phân.

- Truy cập link trên ta xem thấy thông tin như sau:



- Do 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.



- Sau khi có mật khẩu dùng để giải mã, tiến hành giải mã tập tin pcap với công cụ airdecap-ng:

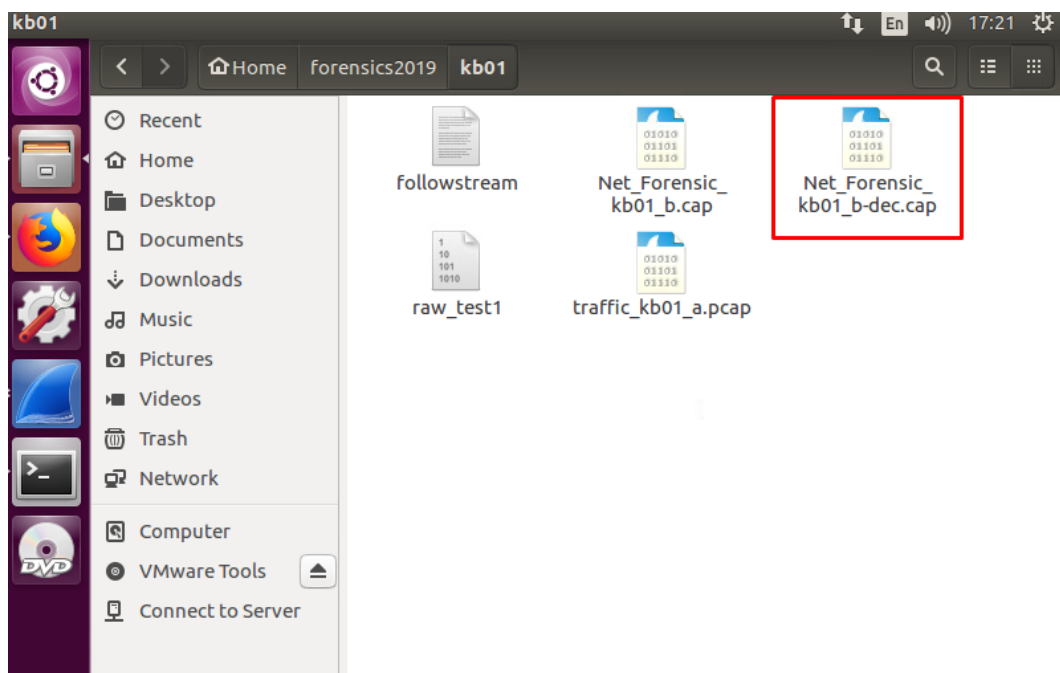
airdecap-ng -e 'Rome' -p <Mật khẩu> Net_Forensic_kb01_b.cap

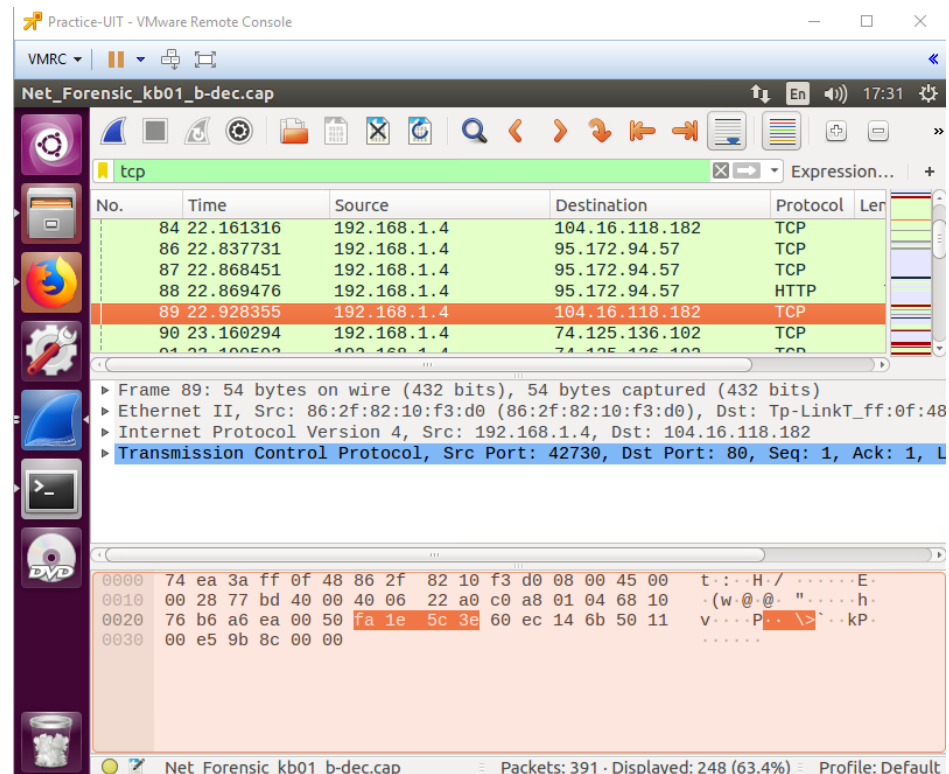
```

Terminal
insecclab@uSense: ~/forensics2019/kb01
total 1464
-rw-rw-r-- 1 insecclab insecclab 46081 Th05 20 16:05 abc
-rw-rw-r-- 1 insecclab insecclab 16775 Th05 20 16:08 bcd
-rw-rw-r-- 1 insecclab insecclab 46085 Th05 20 16:17 efg
-rw-rw-r-- 1 insecclab insecclab 16757 Th05 20 15:13 followstream
-rw-rw-r-- 1 insecclab insecclab 1010501 Th05 20 14:41 Net_Forensic_kb01_b.cap
-rw-rw-r-- 1 insecclab insecclab 16775 Th05 20 17:04 raw_test1
-rw-rw-r-- 1 insecclab insecclab 16775 Th05 20 15:47 stream.bin
-rw-r--r-- 1 root root 16775 Th05 20 16:51 thu2
-rw-r--r-- 1 root root 16775 Th05 20 16:58 thu2.bin
-rw-rw-r-- 1 insecclab insecclab 46081 Th05 20 16:55 thu3
-rw-rw-r-- 1 insecclab insecclab 189103 Th05 20 13:12 traffic_kb01_a.pcap
-rw-rw-r-- 1 insecclab insecclab 24235 Th05 20 16:30 wf.bin
insecclab@uSense:~/forensics2019/kb01$ nano ./raw_test1
insecclab@uSense:~/forensics2019/kb01$ airdecap-ng -e 'Rome' -p [REDACTED] Net_Forensic_kb01_b.cap
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
insecclab@uSense:~/forensics2019/kb01$
0030 39 08 e7 95 00 00
  
```

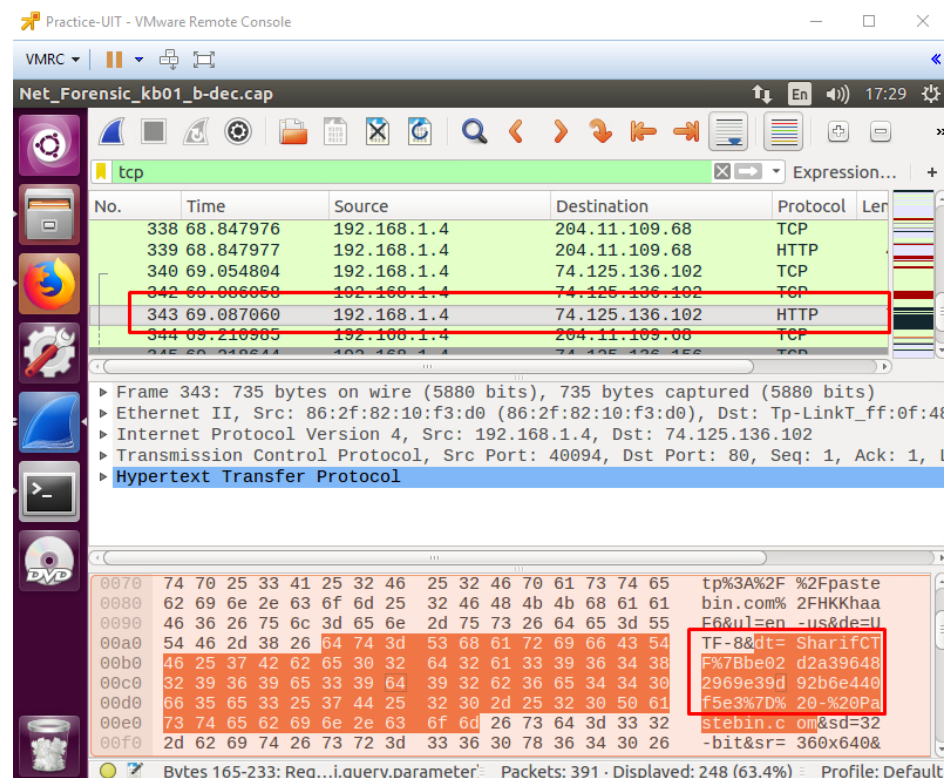
Net_Forensic_kb01_b-dec.cap Packets: 391 · Displayed: 391 (100.0%) Profile: Default

- Nội dung stream đã được giải mã:





- Phân tích một số gói HTTP thu được.



B2. Công cụ tshark

Phần này sẽ giới thiệu các chức năng của phần mềm **tshark**.

Nếu bạn sử dụng các hệ điều hành Linux để phân tích tập tin PCAP thì tshark là một lựa chọn không thể thiếu. Đây là một công cụ khá hiệu quả khi phân tích các tập tin PCAP trên giao diện command line. tshark cung cấp đầy đủ các chức năng như bắt gói tin, đọc và phân tích gói tin, trích xuất dữ liệu...

- *Bắt gói tin*

Bạn có thể sử dụng tshark để bắt các gói tin, tương tự như sử dụng Wireshark trên Windows bằng command line sau:

```
tshark -i wlan0 -w capture-output.pcap
```

Trong đó, các tùy chọn có ý nghĩa như sau:

- `-i wlan0`: bắt các gói tin từ network interface wlan0. Bạn có thể thay wlan0 bằng các interface khác cần bắt gói tin.

- `-w capture-output.pcap`: lưu trữ các gói tin bắt được thành tập tin pcap tương ứng. Bạn có thể thay capture-output.pcap thành đường dẫn tập tin pcap đầu ra mong muốn.

tshark sẽ bắt các gói tin từ interface wlan0 và lưu trữ vào tập tin capture-output.pcap và hiển thị số lượng gói tin đã bắt được trên màn hình console. Khi muốn dừng việc bắt gói tin, bạn chỉ cần gõ tổ hợp phím Ctrl+C.

Ngoài ra, bạn cũng có thể áp dụng thêm một số tùy chọn hay được sử dụng của tshark trong quá trình bắt gói tin như:

- `-c <capture packet count>`: giới hạn tối đa số lượng gói tin được bắt. tshark sẽ dừng khi bắt đủ số lượng gói tin yêu cầu.

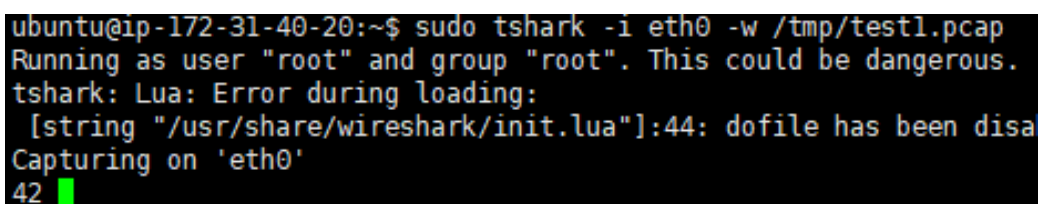
- `-b filesize:100 -a files:20`: lưu trữ gói tin bắt được ra file đầu ra riêng biệt mỗi khi đủ 100KB/1 file đầu ra, dừng khi đủ 20 file đầu ra.

- `-b duration:10 -a files:20`: lưu trữ gói tin bắt được ra file đầu ra riêng biệt mỗi 10 giây, dừng khi đủ 20 file đầu ra.

- *Đọc và phân tích tập tin pcap*

Để đọc tập tin pcap, bạn có thể sử dụng command sau:

```
tshark -r capture-output.pcap
```



```
ubuntu@ip-172-31-40-20:~$ sudo tshark -i eth0 -w /tmp/test1.pcap
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disallowed
Capturing on 'eth0'
42
```

Hình 6. Bắt gói tin bằng tshark

Trong đó, các option có ý nghĩa như sau:

– `-r capture-output.pcap`: đọc file pcap tương ứng. Bạn có thể thay `capture-output.pcap` thành đường dẫn tập tin pcap cần đọc, phân tích.

tshark sẽ đọc tập tin pcap và hiển thị từng gói tin gửi nhận có trong tập tin pcap:

```
root@ip-172-31-40-20:~# tshark -r test.pcap
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
1 0.000000000 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=1 Win=254 Len=0
2 0.705709725 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
3 0.797620878 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=53 Win=254 Len=0
4 1.211306630 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
5 1.313419031 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=105 Win=254 Len=0
6 1.715305543 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
7 1.813370200 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=157 Win=254 Len=0
8 2.219321178 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
9 2.313525169 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=209 Win=253 Len=0
10 2.723315714 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
11 2.813566066 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=261 Win=253 Len=0
12 3.227301021 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
13 3.329341408 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=313 Win=253 Len=0
14 3.731324294 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
15 4.016837662 172.31.40.20 → 172.72.58.160 TCP 106 [TCP Retransmission] 22 → 57982 [PSH, ACK] Seq=313 Ack=1 Win=277 Len=52
16 4.110496372 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=365 Win=253 Len=0
17 4.233676780 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
18 4.329492274 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=417 Win=258 Len=0
19 4.739329219 172.31.40.20 → 172.72.58.160 SSH 106 Server: Encrypted packet (len=52)
20 4.829425588 172.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=469 Win=258 Len=0
```

Hình 7. Công cụ tshark hiển thị các gói tin có trong file pcap

▪ Phân tích dữ liệu HTTP

Dữ liệu HTTP là loại dữ liệu phổ biến hiện nay. Trong ví dụ dưới đây, chúng ta sẽ thử phân tích một số gói tin HTTP với tshark.

Để liệt kê danh mục các request HTTP, sử dụng câu lệnh sau:

```
tshark -r /tmp/http.pcap -Y http.request -T fields -e frame.time -e http.host -e http.request.method -e http.user_agent
```

Kết quả hiển thị danh sách gói tin HTTP với các trường: thời gian, host, method, user agent:

```
ubuntu@ip-172-31-40-20:~$ sudo tshark -r /tmp/http.pcap -Y http.request -T fields -e frame.time -e http.host -e http.request.method -e http.user_agent
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
Jun 21, 2018 09:24:52.109649183 UTC dantri.com.vn GET Wget/1.17.1 (linux-gnu)
Jun 21, 2018 09:25:00.678806746 UTC dantri.com.vn GET Wget/1.17.1 (linux-gnu)
Jun 21, 2018 09:25:07.166671638 UTC dantri.com.vn GET curl/7.47.0
Jun 21, 2018 09:25:16.440337975 UTC dantri.com.vn GET curl/7.47.0
ubuntu@ip-172-31-40-20:~$
```

Hình 8. Hiển thị các gói tin HTTP bằng tshark

Ngoài ra, bạn có thể bổ sung thêm các thông tin khác cần hiển thị nếu muốn bằng cách thêm vào các tham số như:

- `-e http.request.uri`: hiển thị URI.

- -e ip.src: hiển thị IP nguồn.
- -e ip.dst: hiển thị IP đích.
- -e tcp.srcport: hiển thị port nguồn.
- -e tcp.dstport: hiển thị port đích.
- -e frame.time_epoch: hiển thị timestamp của gói tin.
- *Phân tích dữ liệu DNS*

Ở ví dụ dưới đây, chúng ta sẽ sử dụng tshark để phân tích các bản tin DNS.

Để liệt kê các truy vấn DNS có trong file pcap, chúng ta sử dụng command line sau:

```
tshark -r /tmp/dns.pcap -2 -R udp.dstport==53 -T fields -e frame.time -e ip.src -e ip.dst -e dns.qry.name
```

Kết quả hiển thị danh sách truy vấn DNS với các thông tin: thời gian, IP client, IP máy chủ DNS, domain truy vấn:

```
ubuntu@ip-172-31-40-20:~$ sudo tshark -r /tmp/dns.pcap -2 -R udp.dstport==53 -T fields -e frame.time -e ip.src -e ip.dst -e dns.qry.name
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
Jun 21, 2018 09:47:59.801776633 UTC      172.31.40.20      172.31.0.2      google.com
Jun 21, 2018 09:48:03.829865779 UTC      172.31.40.20      172.31.0.2      facebook.com
Jun 21, 2018 09:48:07.662853343 UTC      172.31.40.20      172.31.0.2      vnexpress.net
Jun 21, 2018 09:48:12.206017616 UTC      172.31.40.20      172.31.0.2      viettel.com.vn
Jun 21, 2018 09:48:25.862525089 UTC      172.31.40.20      172.31.0.2      dantri.com.vn
ubuntu@ip-172-31-40-20:~$
```

Hình 9. Hiển thị danh sách truy vấn DNS bằng tshark

Để liệt kê các gói tin phản hồi kết quả truy vấn từ máy chủ DNS, sử dụng câu lệnh sau:

```
tshark -r /tmp/dns.pcap -2 -R udp.srcport==53 -T fields -e frame.time -e ip.src -e ip.dst -e dns.qry.name -e dns.a
```

Kết quả hiển thị danh sách các gói tin trả lời truy vấn DNS từ máy chủ có chứa thông tin về IP của tên miền đã truy vấn:


```

ubuntu@ip-172-31-40-20:~$ sudo tshark -r /tmp/dns.pcap -2 -R udp.srcport==53 -T fields -e frame.time -e ip.s
rc -e ip.dst -e dns.qry.name -e dns.a
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser
. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivile
ged user.
Jun 21, 2018 09:47:59.803452960 UTC      172.31.0.2      172.31.40.20    google.com      74.125.68.139,74.125
.68.100,74.125.68.101,74.125.68.102,74.125.68.113,74.125.68.138
Jun 21, 2018 09:48:03.834265247 UTC      172.31.0.2      172.31.40.20    facebook.com    31.13.95.36
Jun 21, 2018 09:48:07.721244606 UTC      172.31.0.2      172.31.40.20    vnexpress.net   111.65.248.132
Jun 21, 2018 09:48:12.249748048 UTC      172.31.0.2      172.31.40.20    viettel.com.vn  203.190.170.225,203.
190.170.226
Jun 21, 2018 09:48:26.107333664 UTC      172.31.0.2      172.31.40.20    dantri.com.vn  222.255.27.212,222.2
55.27.217,222.255.27.238,103.92.32.49,222.255.27.9,222.255.27.22,222.255.27.28,222.255.27.169
ubuntu@ip-172-31-40-20:~$

```

Hình 10. Hiển thị danh sách phản hồi truy vấn DNS từ máy chủ

▪ Trích xuất tập tin từ file pcap

tshark cũng có thể được sử dụng để trích xuất các tập tin từ file pcap. Để sử dụng được tính năng trích xuất tập tin từ file pcap, bạn cần sử dụng phiên bản tshark từ 2.4 trở lên. Để cài đặt tshark 2.4, sử dụng câu lệnh sau (đối với hệ điều hành Ubuntu):

```
sudo add-apt-repository ppa:dreibh/ppasudo apt-get update && sudo apt-get install wireshark tshark
```

Hiện nay tshark hỗ trợ trích xuất các tập tin từ các giao thức sau: dicom, http, imf, smb, tftp. Chẳng hạn, để trích xuất các tập tin từ giao thức HTTP, sử dụng câu lệnh sau:

```
tshark -r /tmp/http.pcap --export-objects "http,/tmp/export"
```

Tuy nhiên, bạn có thể thay đổi tham số protocol và thư mục đầu ra tùy theo nhu cầu của mình.

```

ubuntu@ip-172-31-40-20:~$ sudo tshark -r /tmp/http.pcap --export-objects "http,/tmp/export"
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:32: dofile has been disabled due to running Wireshark as sup
1 0.000000000 27.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=1 Win=253 Len=0
2 0.285472937 172.31.40.20 → 27.72.58.160 SSH 202 Server: Encrypted packet (len=148)
3 0.386911569 27.72.58.160 → 172.31.40.20 TCP 54 58487 → 22 [ACK] Seq=1 Ack=149 Win=256 Len=0
4 0.457196441 172.31.40.20 → 27.72.58.160 SSH 106 Server: Encrypted packet (len=52)
5 0.548102870 27.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=53 Win=258 Len=0
6 0.959433645 172.31.40.20 → 27.72.58.160 SSH 106 Server: Encrypted packet (len=52)
7 1.048697882 27.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=105 Win=258 Len=0
8 1.291350862 172.31.40.20 → 27.72.58.160 SSH 122 Server: Encrypted packet (len=68)
9 1.402837661 27.72.58.160 → 172.31.40.20 TCP 54 58487 → 22 [ACK] Seq=1 Ack=217 Win=256 Len=0
10 1.463463654 172.31.40.20 → 27.72.58.160 SSH 106 Server: Encrypted packet (len=52)
11 1.564297762 27.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=157 Win=258 Len=0
12 1.967400526 172.31.40.20 → 27.72.58.160 SSH 106 Server: Encrypted packet (len=52)
13 2.064160642 27.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=209 Win=258 Len=0
14 2.297240167 172.31.40.20 → 27.72.58.160 SSH 122 Server: Encrypted packet (len=68)
15 2.403033604 27.72.58.160 → 172.31.40.20 TCP 54 58487 → 22 [ACK] Seq=1 Ack=285 Win=255 Len=0
16 2.471461480 172.31.40.20 → 27.72.58.160 SSH 106 Server: Encrypted packet (len=52)
17 2.564228223 27.72.58.160 → 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=261 Win=257 Len=0
18 2.975456548 172.31.40.20 → 27.72.58.160 SSH 106 Server: Encrypted packet (len=52)
19 3.064621941 172.31.40.20 TCP 54 57982 → 22 [ACK] Seq=1 Ack=313 Win=257 Len=0
20 3.271852536 27.72.58.160 → 172.31.40.20 SSH 90 Client: Encrypted packet (len=36)

```

Hình 11. Trích xuất các gói tin HTTP sử dụng tshark

Các tập tin được trích xuất nằm trong thư mục /tmp/export:

```
ubuntu@ip-172-31-40-20:~$ ll /tmp/export/
total 752
drwxr-xr-x 2 root root 4096 Jun 21 10:23 ./
drwxrwxrwt 9 root root 4096 Jun 21 10:24 ../
-rw-r--r-- 1 root root 155161 Jun 21 10:21 %2f
-rw-r--r-- 1 root root 155161 Jun 21 10:23 %2f(1)
-rw-r--r-- 1 root root 82590 Jun 21 10:21 vat-the-la-ro-i-xuong-rung-ha-giang-khong-phai-thiet-bi-du-bao-thoi-tiet-2018062111524804(1).htm
-rw-r--r-- 1 root root 82614 Jun 21 10:23 vat-the-la-ro-i-xuong-rung-ha-giang-khong-phai-thiet-bi-du-bao-thoi-tiet-2018062111524804(2).htm
-rw-r--r-- 1 root root 82590 Jun 21 10:23 vat-the-la-ro-i-xuong-rung-ha-giang-khong-phai-thiet-bi-du-bao-thoi-tiet-2018062111524804(3).htm
-rw-r--r-- 1 root root 82614 Jun 21 10:21 vat-the-la-ro-i-xuong-rung-ha-giang-khong-phai-thiet-bi-du-bao-thoi-tiet-2018062111524804.htm
-rw-r--r-- 1 root root 53021 Jun 21 10:23 video-page(1).htm
-rw-r--r-- 1 root root 53021 Jun 21 10:21 video-page.htm
ubuntu@ip-172-31-40-20:~$
```

Hình 12. Các tập tin HTTP được export bằng tshark

Sinh viên tự thực hiện bắt lưu lượng mạng bằng công cụ tshark.

a. Kịch bản 02: Phân tích dữ liệu mạng với tshark/Wireshark

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.

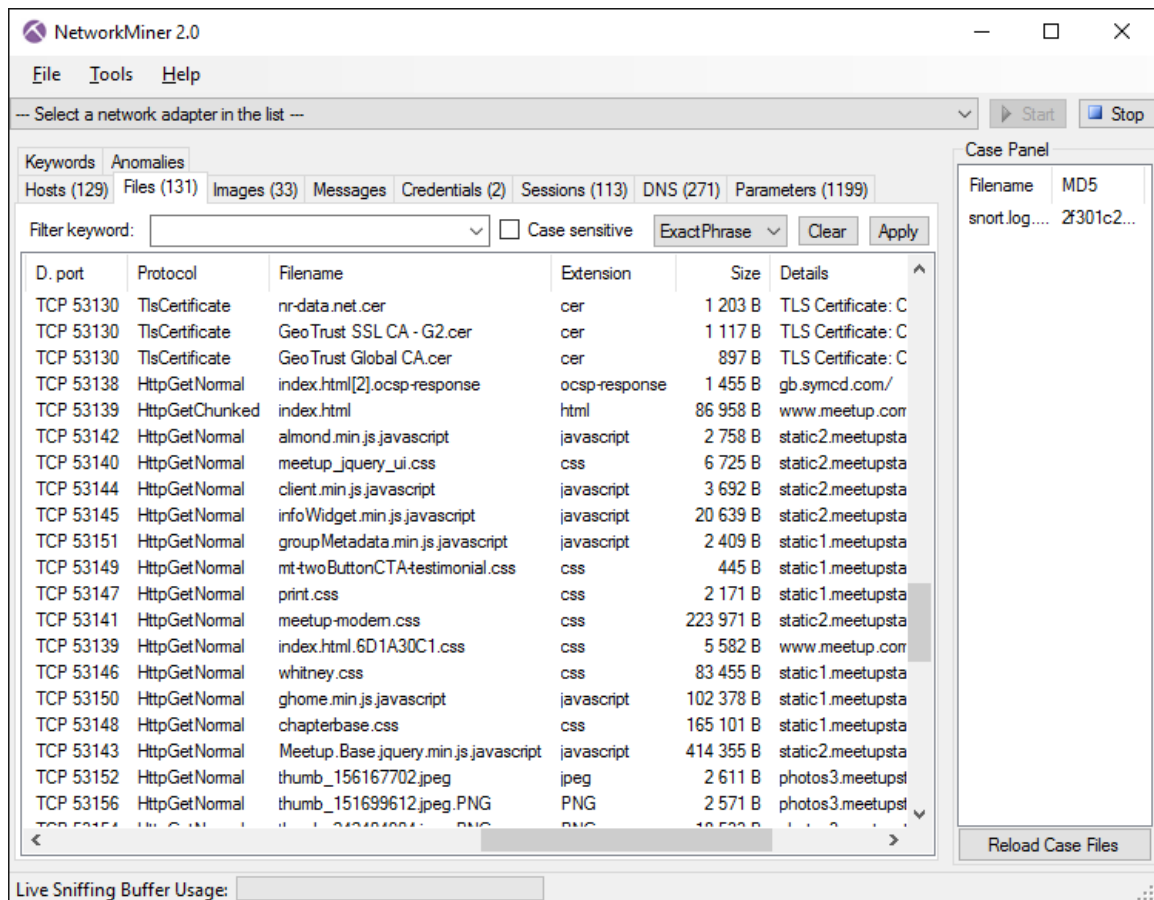
Gợi ý: Wireshark/tshark

B3. Công cụ NetworkMiner

Link tải: <https://www.netresec.com/?download=NetworkMiner>

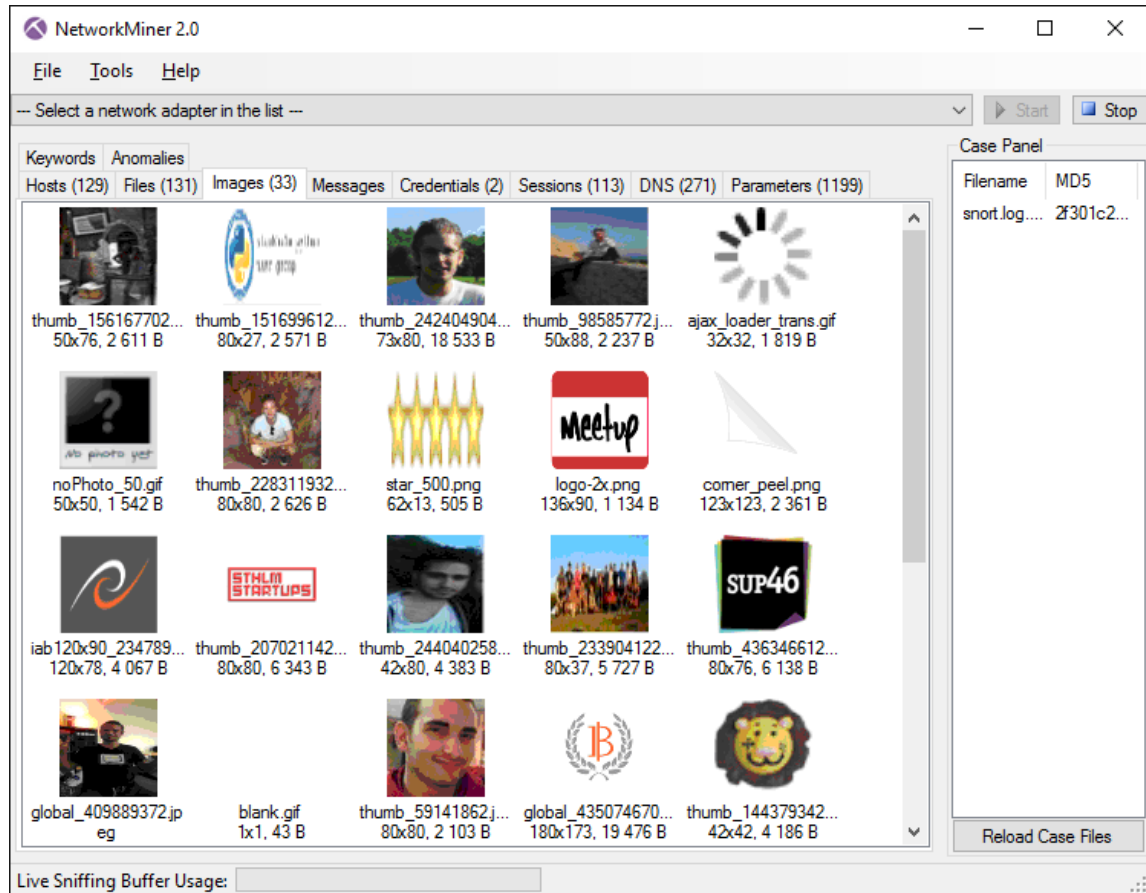
NetworkMiner là một trong những giải pháp phân tích và điều khiển mạng máy tính từ xa thông qua quyền quản trị, giúp người dùng nắm được các thông tin về tất cả các máy tính như phiên bản hệ điều hành, tên máy, tài khoản người dùng, các cổng mạng đang

được kết nối. Phần mềm này cũng giúp phát hiện các hiện tượng khả nghi và các sự cố có thể xảy ra đối với hệ thống mạng của bạn, nhằm phòng tránh và xử lý kịp thời.



NetworkMiner có khả năng trích xuất và lưu các tập tin được chuyển giao qua mạng, từ các trang Web chia sẻ trực tuyến, được thực hiện trên các giao thức FTP, TFTP, HTTP và SMB. Giao diện trực quan hiển thị đầy đủ danh sách dữ liệu thu thập được như tên Host,

Frame, Files, Images, Sessions.... Khi bạn click chọn bất cứ mục nào, tất cả chúng sẽ được hiện ra lần lượt với các thông tin chi tiết nhất và bạn có thể tải chúng về máy tính.

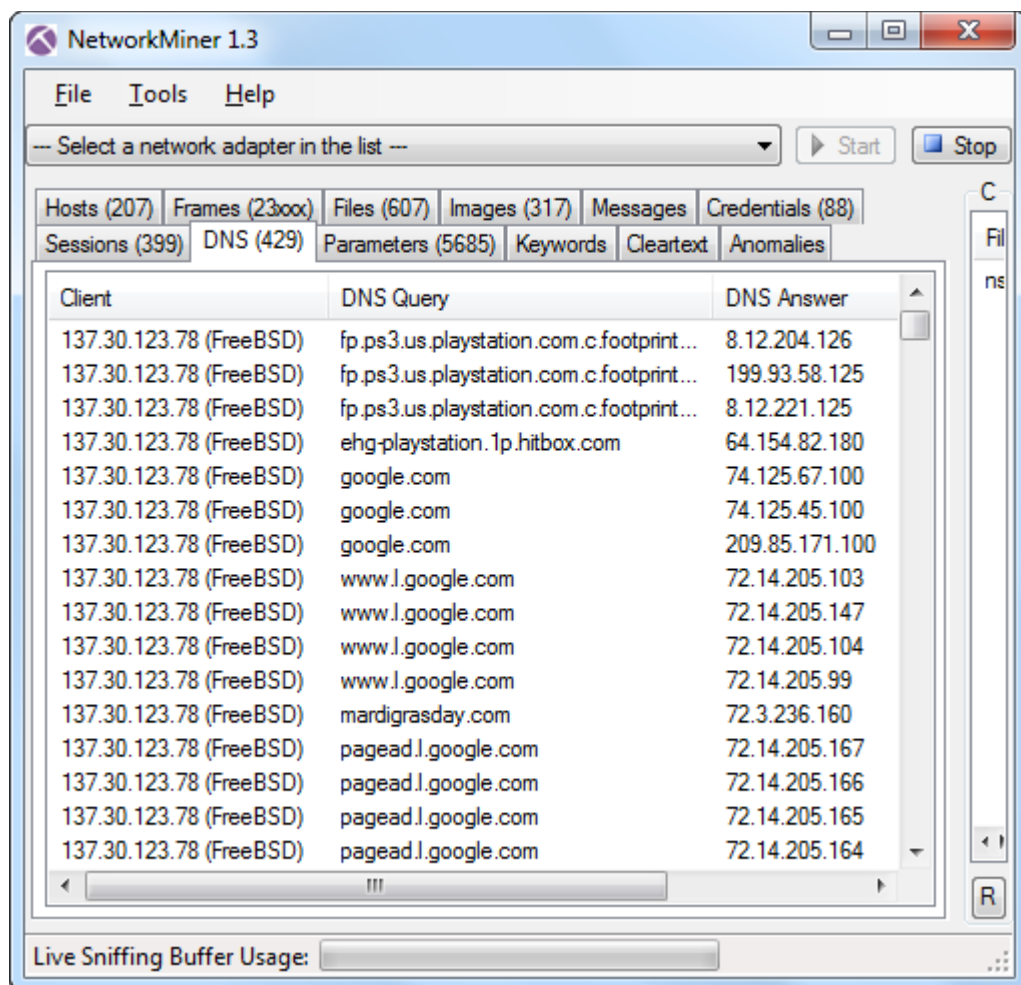


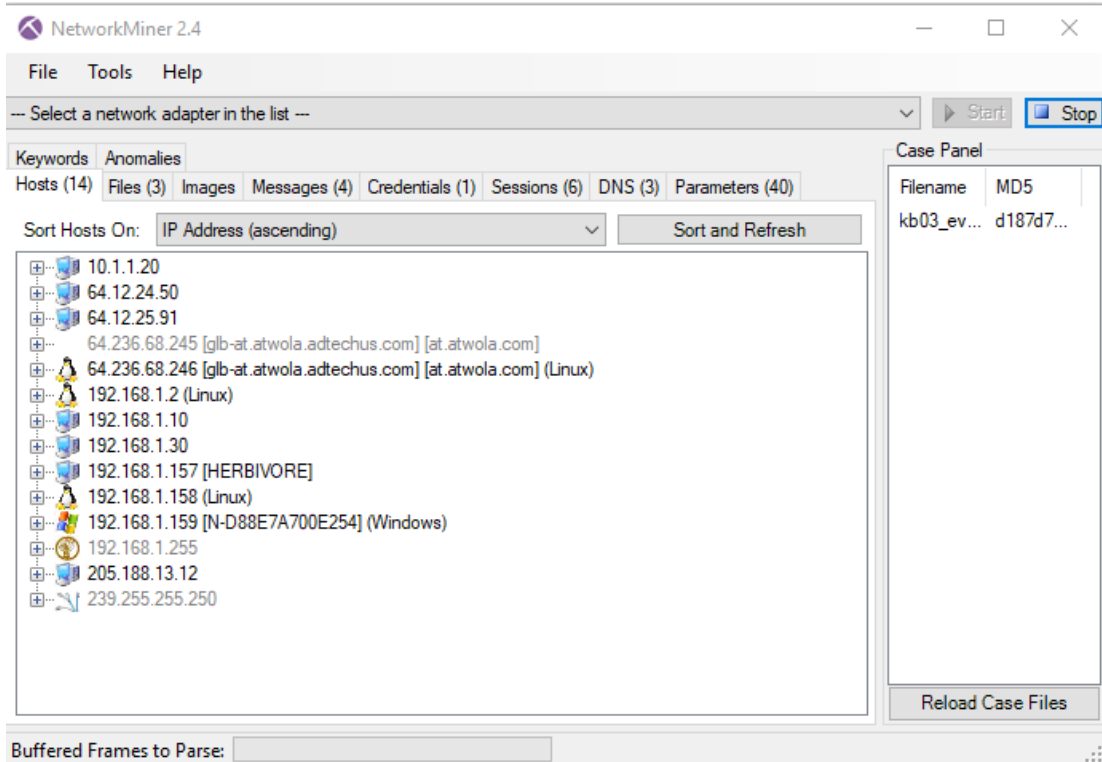
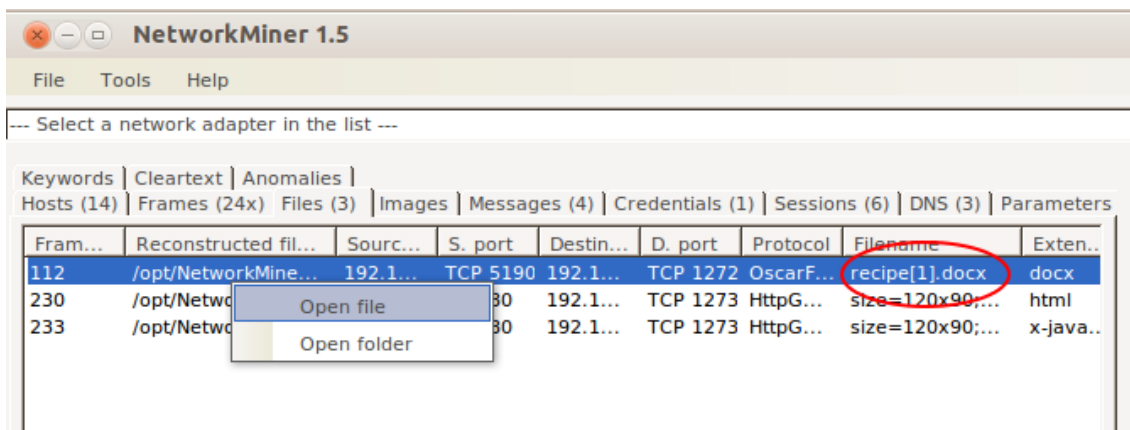
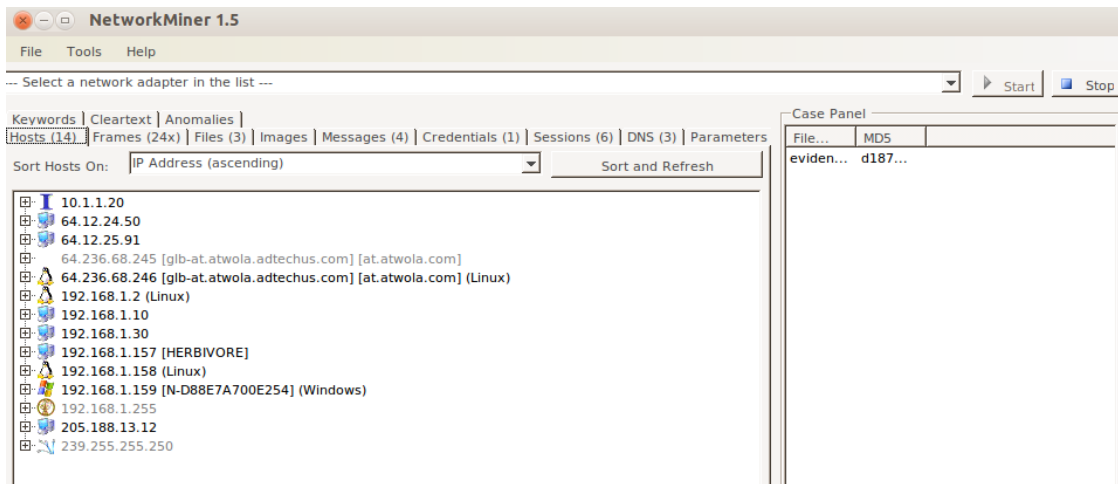
NetworkMiner còn giúp thu thập thông tin người dùng gồm tài khoản đăng nhập và mật khẩu, kể cả thông tin người dùng sử dụng cho các dịch vụ trực tuyến phổ biến như Gmail hay Facebook. Một ưu điểm của ứng dụng này là cho phép người dùng sử dụng chức

năng tìm kiếm bằng các từ khóa. Các báo cáo cũng có thể được chuyển sang các tập tin HTML, TXT, Javascript,...

Các tính năng chính của NetworkMiner:

- Thu thập dữ liệu trong hệ thống mạng
- Phát hiện các sự cố mạng
- Lưu và trích xuất các tập tin được truyền tải qua mạng
- Sử dụng chức năng tìm kiếm thông tin bằng từ khóa
- Trích xuất các báo cáo sang định dạng văn bản





Hình 13. Giao diện Network Miner các phiên bản

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 hiện 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 gửi 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.

- Dùng Wireshark để xác định các địa chỉ IP mà máy tính của Ann kết nối tới, liệt kê, phán đoán IP nghi vấn.

No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	SSL	60	Continuation Data
25	33.914966	192.168.1.158	64.12.24.50	SSL	243	Continuation Data
27	34.006599	192.168.1.158	64.12.24.50	SSL	94	Continuation Data
32	34.026804	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
33	34.026809	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
90	56.425051	192.168.1.158	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
91	57.427165	192.168.1.158	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
92	58.458768	192.168.1.158	64.12.24.50	SSL	182	Continuation Data
96	58.569716	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=457 Win=62742 Len=0
98	58.574447	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=364 Ack=495 Win=62742 Len=0
110	61.052930	192.168.1.158	192.168.1.159	TCP	62	5190 → 1272 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
112	61.054884	192.168.1.158	192.168.1.159	TCP	310	5190 → 1272 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=256
118	61.155760	192.168.1.158	192.168.1.159	TCP	60	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=0
119	61.270615	192.168.1.158	192.168.1.159	TCP	1514	5190 → 1272 [ACK] Seq=257 Ack=257 Win=6432 Len=1460
120	61.270620	192.168.1.158	192.168.1.159	TCP	1514	5190 → 1272 [ACK] Seq=1717 Ack=257 Win=6432 Len=1460
122	61.270628	192.168.1.158	192.168.1.159	TCP	1230	5190 → 1272 [PSH, ACK] Seq=3177 Ack=257 Win=6432 Len=1176

> Frame 92: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
 > Ethernet II, Src: HewlettP_45:a4:bb (00:12:79:45:a4:bb), Dst: Vmware_b0:8d:62 (00:0c:29:b0:8d:62)
 > Internet Protocol Version 4, Src: 192.168.1.158, Dst: 64.12.24.50
 > Transmission Control Protocol, Src Port: 51128, Dst Port: 443, Seq: 236, Ack: 248, Len: 128
 Secure Sockets Layer

- Sử dụng các công cụ phù hợp xem thông tin sở hữu IP của các IP nghi vấn, xác định cách mà Ann dùng để gửi thông tin ra bên ngoài.
- Xem nội dung tin nhắn mà Ann đã gửi:

```
> Frame 25: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
> Ethernet II, Src: HewlettP_45:a4:bb (00:12:79:45:a4:bb), Dst: Vmware_b0:8d:62 (00:0c:29:b0:8d:62)
> Internet Protocol Version 4, Src: 192.168.1.158, Dst: 64.12.24.50
> Transmission Control Protocol, Src Port: 51128, Dst Port: 443, Seq: 7, Ack: 1, Len: 189
  Secure Sockets Layer

0000 00 0c 29 b0 8d 62 00 12 79 45 a4 bb 00 00 45 00 --)...b...yE...E.
0010 00 e5 ab 3c 40 00 40 06 74 52 c0 a8 01 9e 40 0c ...<@. tr...@.
0020 18 32 c7 b8 01 bb 33 6b d2 c9 07 e9 60 db 50 18 .2....3k ....P.
0030 f5 3c d0 0c 00 00 2a 02 00 61 00 b7 00 04 00 06 <....>.8.....
0040 00 00 00 00 00 45 34 36 32 38 37 37 38 00 00 01 .....646 28778...
0050 00 53 65 63 35 35 38 75 73 65 72 31 00 02 00 0f .Sec558u ser1....
0060 05 01 00 04 01 01 01 02 01 01 00 83 00 00 00 00 here's t he sécre
0070 48 65 72 65 27 73 20 74 68 65 20 73 65 63 72 65 t recipe ... I ju
0080 74 20 72 65 63 69 70 65 2e 2e 2e 20 49 20 6a 75 st downl oaded it
0090 73 74 20 64 6f 77 6e 6c 6f 61 64 65 64 20 69 74 from th e file s
00a0 20 66 72 6f 6d 20 74 68 65 20 66 69 6c 65 20 73 erver. J ust copy
00b0 65 72 76 65 72 2e 20 4a 75 73 74 20 63 6f 70 79 to a th umb driv
00c0 20 74 6f 20 61 20 74 68 75 6d 62 20 64 72 69 76 e and yo u're goo
00d0 65 20 61 6e 64 20 79 6f 75 27 72 65 20 67 6f 6f d to go &gt;:-).
00e0 64 20 74 6f 20 67 6f 20 26 67 74 3b 3a 2d 29 00 ...
00f0 83 00 00
```

- Tìm nội dung công thức mà Ann đã tiết lộ.
- Tương tự, thay vì dùng Wireshark, hãy dùng công cụ NetworkMiner để thực hiện điều tra.

B4. Kịch bản tổng hợp

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 khoảng thời gian. Tìm flag, biết flag có định dạng flag{...}

Đáp án:

<https://github.com/ctfs/write-ups-2015/tree/master/csaw-ctf-2015/forensics/transfer-100>

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 trong 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 ký tự.
- Công cụ: Wireshark, tshark,...

Gợi ý: <https://github.com/ctfs/write-ups-2015/tree/master/nuit-du-hack-ctf-quals-2015/forensic/private>

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

- Mô tả: Một trong các máy chủ của CoMix Wave Films bị xâm nhập vào tuần trước, tuy nhiên không có thiệt hại đáng kể nào được ghi nhận. Mặc dù hệ thống tường lửa của công ty rất mạnh nhưng nhóm bảo mật của công ty phát hiện ra một số hoạt động đáng ngờ, có thể bị tuồn dữ liệu ra bên ngoài. Hãy điều tra liệu kẻ tấn công đã lấy được những gì từ máy chủ của công ty, giao thức sử dụng? Tìm flag.
- Tài nguyên: Nandemonaiya_kb06.pcap
- Yêu cầu – Gợi ý: <https://bitbucket.org/kscrivs/netsec-0x325-writeups/src/master/CSACTF-2019/Forensics-Kimi%20No%20Na%20Wa/>

Gợi ý:

C. THAM KHẢO

<https://www.algissalys.com/network-security/pcap-capture-view-ssid-ap-names-in-wireshark>
<https://www.aircrack-ng.org/downloads.html>

D. YÊU CẦU

Bài thực hành được chia làm 2 phần riêng biệt.

- **Class Part (CP):** Sinh viên hoàn thành trên lớp (Bắt buộc).
0% <= CP < 50%: 1đ
50% <= CP < 90 %: 5đ
90% <= CP <= 100%: 10đ
- **Home Part (HP):** Hoàn thành phần còn lại và làm báo cáo sau khi kết thúc buổi thực hành (nộp trên Course môn học theo deadline).
- Điểm Thực hành của mỗi Buổi (Session): **$S = (CP + HP)/2$**

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả gồm chi tiết những việc 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.
- Chỉ dùng duy nhất 1 loại Font chữ (Times New Roman – cỡ chữ 12)
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).
Ví dụ: [NT101.H11.1]-Session1_Group3.
- 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 Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, nộp trễ, thực hiện không nghiêm túc ... sẽ được xử lý tùy mức độ vi phạm.



HẾT