


2) TRYHACKME “Disk Analysis & Autopsy”

Learn > Disk Analysis & Autopsy



Disk Analysis & Autopsy

Ready for a challenge? Use Autopsy to investigate artifacts from a disk image.

📶 Medium ⌚ 45 min

🖨 Start AttackBox ▼ Help ▼ 📌 Save Room

👍 779 🗨 Options ▼

Room progress (0%)

🐶 Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status
Adding:
Users\FH454\AppData\Roaming\Mozilla\Firefox\Profiles\o9uppw5z.default-release\storage\default\https+++en.softonic.com\ldb

*This process may take some time for large data sources.

< Back Next > Finish **Cancel** Help

Q1. What is the MD5 hash of the E01 image?

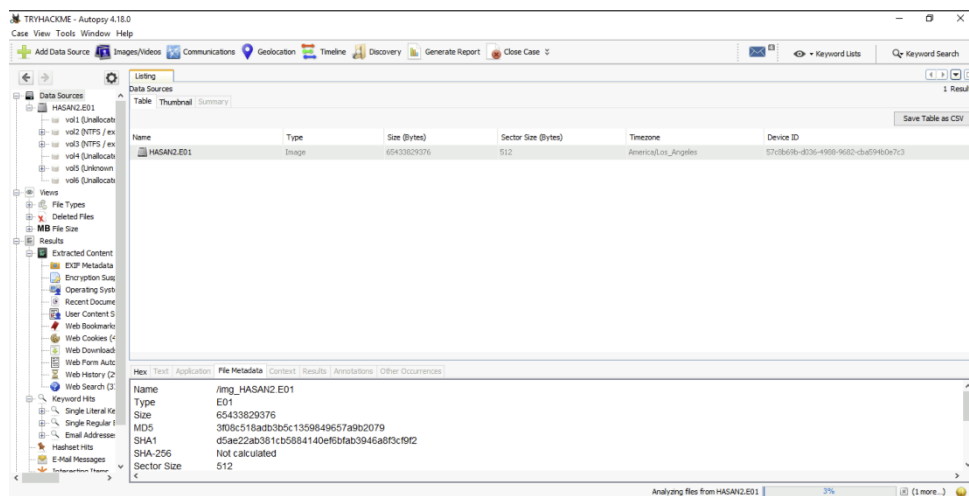
E01 이미지의 MD5 해시는 무엇인가?

Answer the questions below

What is the MD5 hash of the E01 image?

Answer format: *****

Submit



Autopsy에서 이미지를 추가하면 그 파일의 메타데이터를 자동으로 읽어온다. Data Source에서 해당 E01 이미지를 클릭하고, 밑에 메타데이터를 살펴보면 MD5 해시 값을 확인할 수 있다.

3f08c518adb3b5c1359849657a9b2079

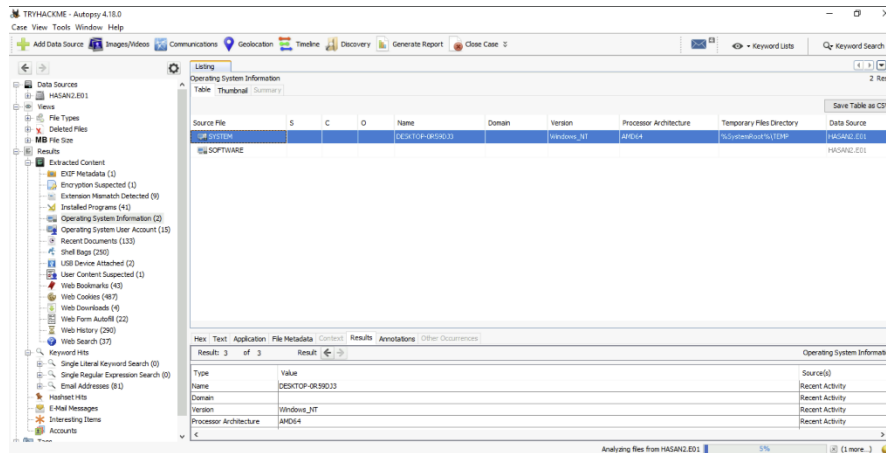
Q2. What is the computer account name?

컴퓨터 계정 이름은 무엇인가?

What is the computer account name?

Answer format: *****

Submit



SYSTEM 레지스트리 하이드에서 컴퓨터 이름 등의 시스템 설정을 가져오기 때문에, Autopsy가 SYSTEM 하이드를 자동 분석해서 보여준다. Operating System Information 창에서 SYSTEM을 클릭한 후, 밑에 파일 메타데이터에서 Name칸을 보면 확인할 수 있다.

DESKTOP-OR59DJ3

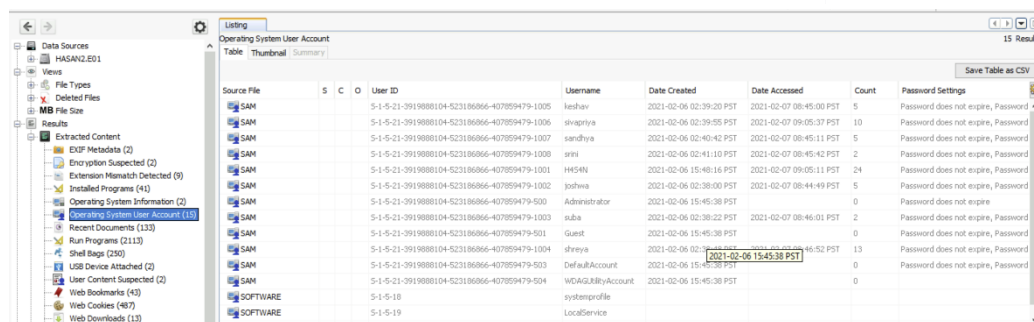
Q3. List all user accounts (in alphabetical order)

모든 사용자 계정을 나열해라. (알파벳순)

List all the user accounts. (alphabetical order)

Answer format: *****

Submit



Autopsy는 SAM 레지스트리에서 사용자 계정 목록을 추출하여 자동으로 표시한다. 따라서, Operating System User Account 창을 들어가보면 확인이 가능하다.

H4S4N,joshwa,keshav,sandhya,shreya,sivapriya,srini,suba

Q4. Who was the last user to log in?

컴퓨터에 마지막으로 로그인한 사용자는?

Who was the last user to log into the computer?

Answer format: *****

Submit

Listing									
Operating System User Account									
Table Thumbnail Summary									
Source File	S	C	O	User ID	Username	Date Created	Date Accessed	Count	Password Settings
SAM				5-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-06 02:39:55 PST	2021-02-07 09:05:37 PST	10	Password does not expire, Password
SAM				5-1-5-21-3919888104-523186866-407859479-1001	H454N	2021-02-06 15:48:16 PST	2021-02-07 09:05:11 PST	24	Password does not expire, Password
SAM				5-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-06 02:38:48 PST	2021-02-07 08:46:52 PST	13	Password does not expire, Password
SAM				5-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-06 02:38:22 PST	2021-02-07 08:46:01 PST	2	Password does not expire, Password
SAM				5-1-5-21-3919888104-523186866-407859479-1008	sriini	2021-02-06 02:41:10 PST	2021-02-07 08:45:42 PST	2	Password does not expire, Password
SAM				5-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-06 02:40:42 PST	2021-02-07 08:45:11 PST	5	Password does not expire, Password
SAM				5-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-06 02:39:20 PST	2021-02-07 08:45:00 PST	5	Password does not expire, Password

아까 위에 창에서 Date Accessed 열로 나열하면, 가장 최근에 로그인한 계정을 확인할 수 있다.

sivapriya

Q5. What was the IP address of the computer?

컴퓨터 IP 주소는 무엇인가?

What was the IP address of the computer?

Answer format: *****

Submit

Listing									
File Metadata									
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dx)
[current folder]				2021-02-07 00:12:59 PST	2021-02-07 00:12:59 PST	2021-02-07 09:05:30 PST	2021-02-06 23:49:11 PST	56	Allocated
[parent folder]				2021-02-06 23:49:11 PST	2021-02-07 09:02:23 PST	2021-02-07 09:02:23 PST	2019-12-07 01:14:52 PST	56	Allocated
Report				2021-02-07 00:12:52 PST	2021-02-07 00:12:52 PST	2021-02-07 00:12:53 PST	2021-02-06 23:49:13 PST	240	Allocated
sounds				2021-02-07 00:12:53 PST	2021-02-07 00:12:53 PST	2021-02-07 00:12:53 PST	2021-02-06 23:49:14 PST	560	Allocated
CLMAnual.dlm				2004-02-17 04:01:50 PST	2021-02-07 00:12:59 PST	2004-01-15 06:54:39 PST	2005-11-12 06:13:33 PST	11749	Allocated
hwid.dat				2021-02-07 00:14:19 PST	2021-02-07 00:14:19 PST	2021-02-07 00:14:19 PST	2021-02-06 23:49:30 PST	4	Allocated
runin.bsp				2021-02-07 00:12:32 PST	2021-02-07 00:12:32 PST	2021-02-07 00:12:59 PST	2021-02-06 23:49:17 PST	6134	Allocated
runin.dat				2021-02-07 00:12:32 PST	2021-02-07 00:12:32 PST	2021-02-07 00:12:59 PST	2021-02-06 23:49:17 PST	33968	Allocated
runin.ini				2021-02-07 00:13:03 PST	2021-02-07 00:13:03 PST	2021-02-07 00:12:59 PST	2021-02-06 23:49:17 PST	10163	Allocated
runin.jpg				2021-02-07 00:12:32 PST	2021-02-07 00:12:32 PST	2021-02-07 00:12:59 PST	2021-02-06 23:49:17 PST	18938	Allocated
labasec.dat				2003-04-27 07:31:03 PST	2021-02-07 00:12:53 PST	2021-02-07 00:13:25 PST	2005-11-12 06:13:33 PST	2324	Allocated

해당 이미지를 확인해보니, Look@LAN 창이 있는 것을 확인할 수 있다. 이는 네트워크 상태 확인 도구로, 이 도구를 통해 설정 파일인 irunin.ini에 IP 주소가 저장되어 있는 것을 확인할 수 있다. Data Source 창에서 Program File(x86) 창 안에 Look@LAN 안에서 해당 설정 파일을 확인할 수 있다.

192.168.130.216

Q6. What was the MAC address?

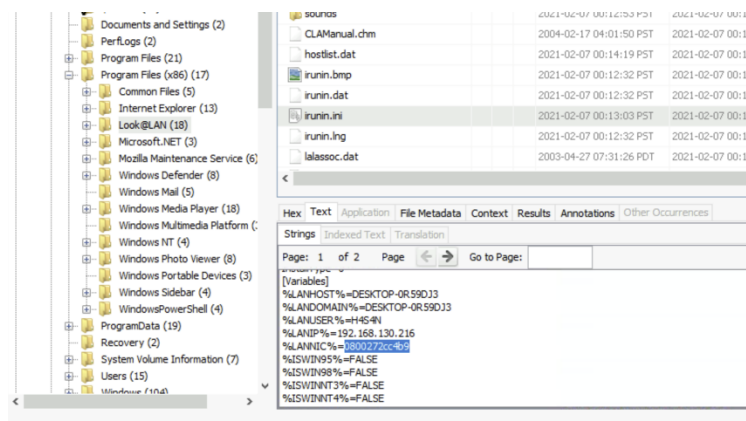
컴퓨터의 MAC 주소는 무엇인가?

What was the MAC address of the computer? (XX-XX-XX-XX-XX-XX)

Answer format: *****

Submit

Hint



위에 창에서 IP를 찾을 수 있었는데, 그 바로 밑에 MAC 주소 또한 발견할 수 있다.

08-00-27-c4-b9

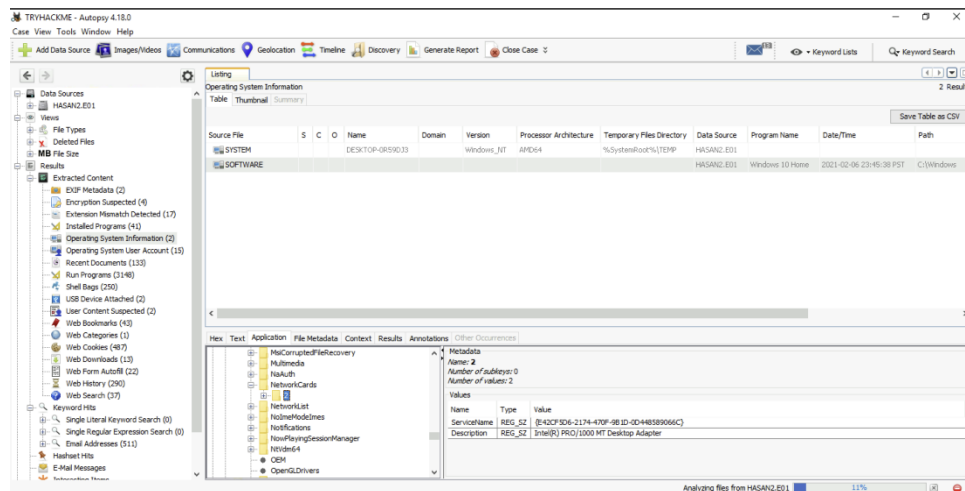
Q7. What is the name of the network card on this computer?

컴퓨터의 네트워크 카드 이름은 무엇인가?

What is the name of the network card on this computer?

Answer format: *****/*****

Submit



Windows는 설치된 네트워크 카드 정보를 SOFTWARE 레지스트리에 기록한다. 해당 경로를 따라가면, 카드 이름 확인이 가능하다. Operating System Information 창에서 SOFTWARE 레지스트리를 클릭한 후, Microsoft/Windows NT/NetworkCards에 들어가 2를 클릭하면, Description 창에서 네트워크 카드 이름이 확인 가능하다.

Intel(R) PRO/1000 MT Desktop Adapter

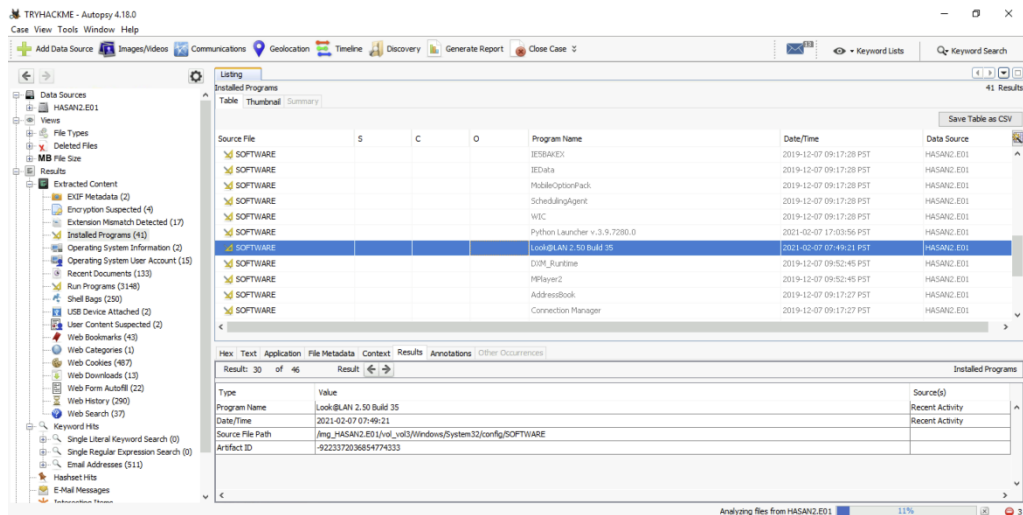
Q8. What is the name of the network monitoring tool?

네트워크 모니터링 도구의 이름이 무엇인가?

What is the name of the network monitoring tool?

Answer format: *****

Submit



아까 위에서 Look@LAN 도구를 발견하였는데, 이는 Installed Program 창에서도 발견이 가능하다. Autopsy가 설치된 프로그램 목록을 SOFTWARE 하이브에서 추출해 자동으로 분석해준다.

Look@LAN

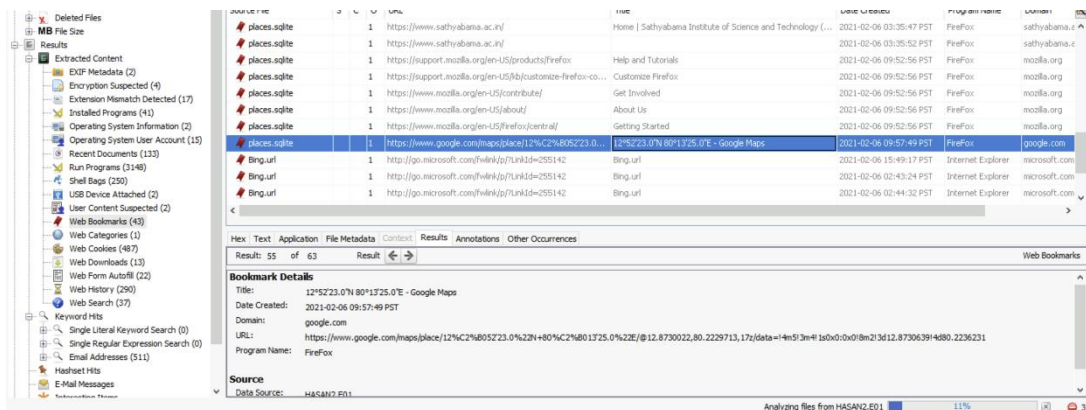
Q9. A user bookmarked a Google Maps location. What are the coordinates of the location?

사용자가 Google Maps 위치를 북마크를 했다. 그 위치의 좌표는 무엇인가?

A user bookmarked a Google Maps location. What are the coordinates of the location?

Answer format: ***** *

Submit



Autospy는 브라우저 데이터 분석 모듈로부터 북마크 항목을 가져와서 정리해준다. Web Bookmarks 창으로 가면, 좌표가 포함된 Google Maps 링크를 확인할 수 있다.

12°52'23.0"N 80°13'25.0"E

Q10. A user has his full name printed on his desktop wallpaper.

What is the user's full name?

사용자가 데스크톱 배경화면에 풀네임을 새겨놓았다.

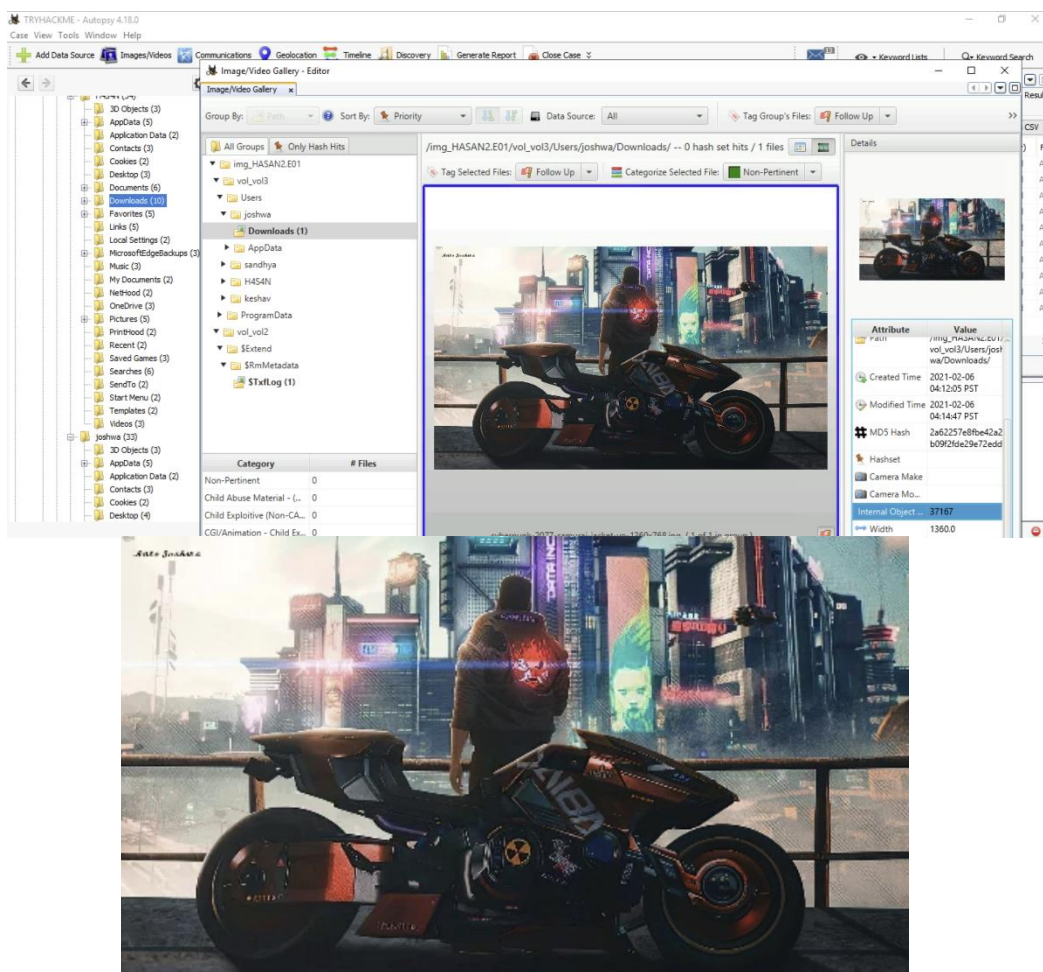
사용자의 전체 이름은 무엇인가?

A user has his full name printed on his desktop wallpaper.

What is the user's full name?

Answer format: **** *

Submit



맨 위에 Images/Videos 창을 클릭한 후, Program Files/Users/joshwa를 클릭하고, Downloads 폴더에 들어가보면, 사용자의 배경화면을 확인할 수 있다. 배경화면을 살펴보니, 왼쪽 윗편에 사용자의 풀네임이 새겨져 있는 것을 확인할 수 있다.

Anto Joshwa

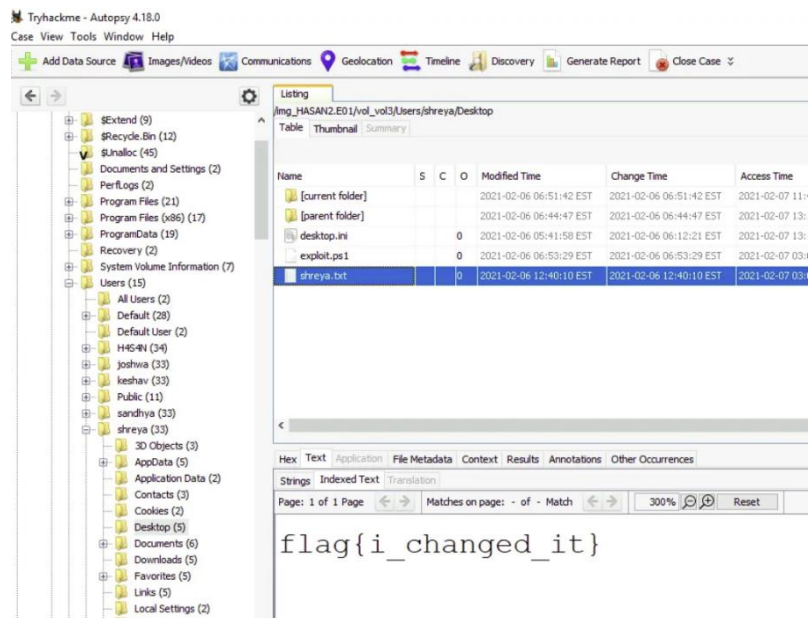
Q11. A user had a file on her desktop. It had a flag but she changed the flag using PowerShell. What was the first flag?

한 사용자가 데스크톱에 파일을 가지고 있었다. 파일에 플래그가 있었다. PowerShell을 사용하여 플래그를 변경하였는데, 바뀌기 전 첫 번째 플래그는 무엇인가?

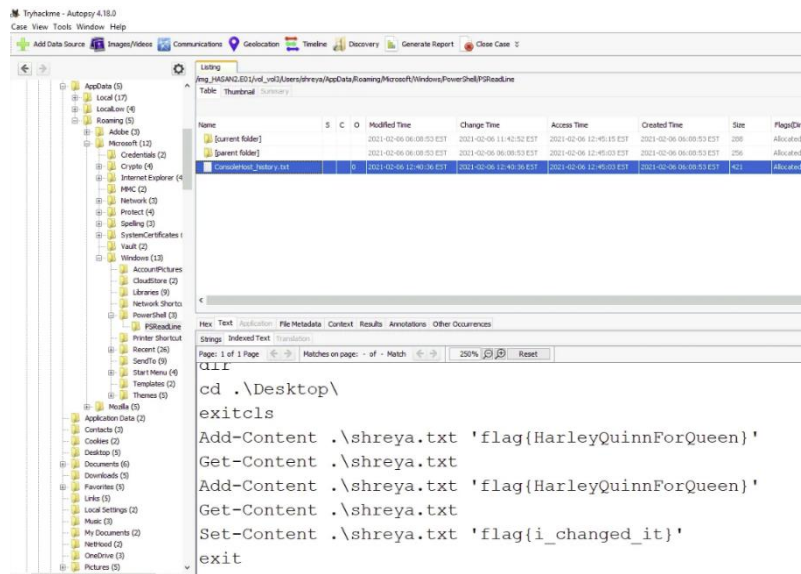
A user had a file on her desktop. It had a flag but she changed the flag using PowerShell. What was the first flag?

Answer format: ****{*****}

Submit



Users 창을 뒤져보니, Shreya라는 사용자가 플래그를 가지고 있는 것을 확인하였다. 이는 바뀐 플래그 값이므로, 이제 이전에 있었던 플래그를 찾아보도록 하겠다.



해당 Shreya 사용자의 AppData 창에서 Roaming/Microsoft/Windows/Powershell/PSReadLine/ConsoleHost_history.txt 에 들어가보면, i_changed_it 플래그 이전에 플래그 값을 확인할 수 있다. 이는 PowerShell 명령어 기록이 저장된 파일로, 사용자가 어떤 명령어를 입력했는지 시간순으로 확인이 가능하다.

flag{HarleyQuinnForQueen}

Q12. The same user found an exploit to escalate privileges on the computer.

What was the message to the device owner?

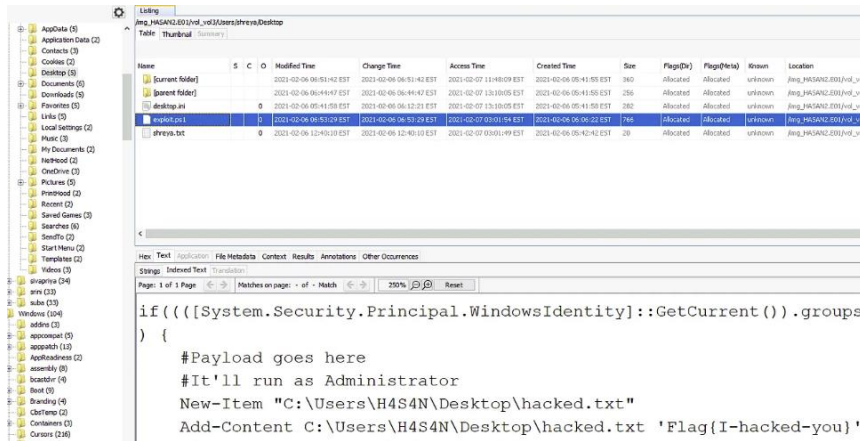
같은 사용자가 컴퓨터에서 권한을 상승시키는 익스플로잇을 발견했다.

장치 소유자에게 보낸 메시지는 무엇인가?

The same user found an exploit to escalate privileges on the computer. What was the message to the device owner?

Answer format: ****{*****}

Submit



Shreya의 데스크톱 폴더로 이동하면, 컴퓨터의 권한을 상승시키는 exploit PowerShell 스크립트를 확인할 수 있다. 또한, 스크립트가 실행되면 생성되는 텍스트 파일도 추가적으로 확인할 수 있는데 여기에 I hacked you 라는 메시지를 확인할 수 있다.

flag{I-hacked-you}

Q13. 2 hack tools focused on passwords were found in the system.

What are the names of these tools? (alphabetical order)

비밀번호에 초점을 맞춘 두 개의 해킹 도구가 시스템에서 발견되었다.

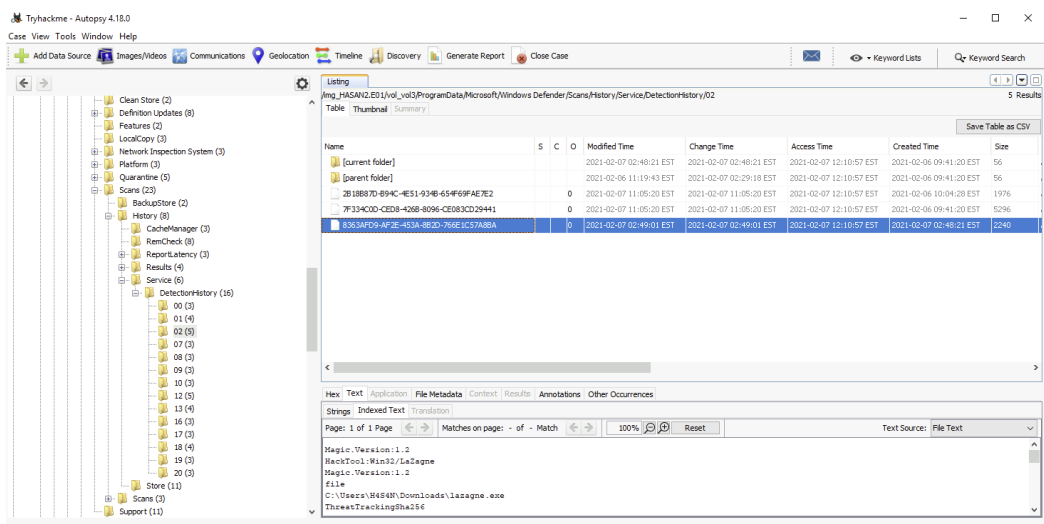
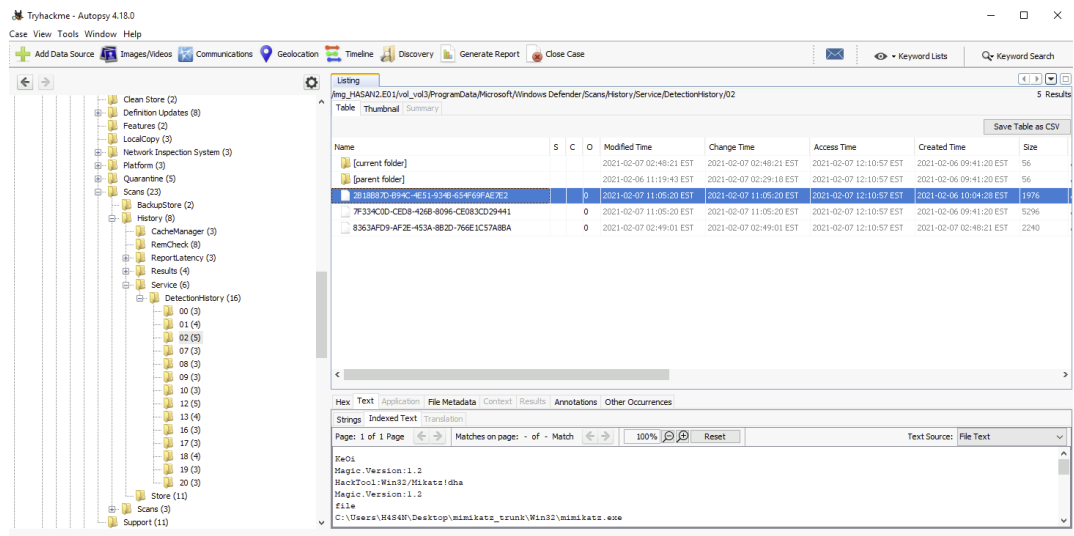
이 도구의 이름은 무엇인가? (알파벳순)

2 hack tools focused on passwords were found in the system. What are the names of these tools? (alphabetical order)

Answer format: ***** , *****

Submit

Hint



이런 해킹 툴들은 Windows Defender가 감지를 하는데, 이 감지 기록을 Autopsy가 일반 파일처럼 읽어낼 수 있다. Data Source 창에서 Microsoft/Windows Defender/Scans/History/Service/DetectionHistory로 들어가면, 해당 기록을 살펴볼 수 있고, 2개의 해킹 툴을 발견할 수 있다.

Lazagne,Mimikatz

What is the name of the author?

There is a YARA file on the computer. Inspect the file. What is the name of the author?

Submit

[illegible]

.yar 확장자를 가진 파일을 검색하고, 해당 파일의 위치를 확인한 후, 이를 참고하여, 해당 파일을 확인해보니, 작성자의 이름을 확인할 수 있었다.

Benjamin DELPY (gentilkiwi)

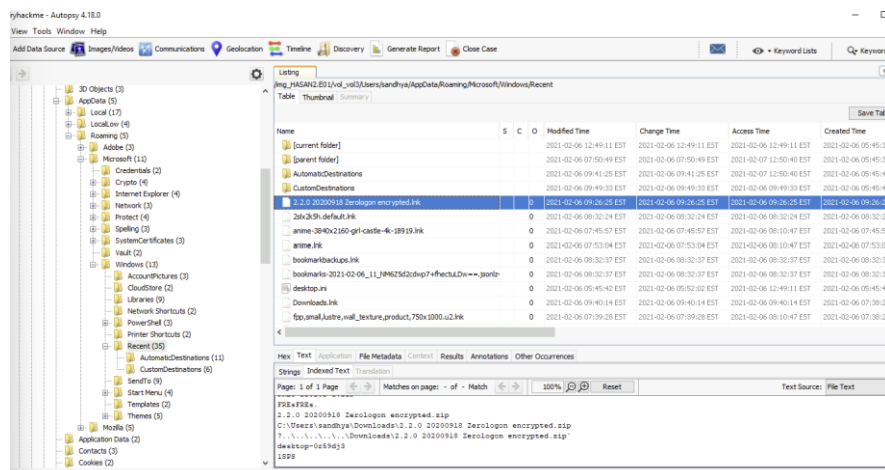
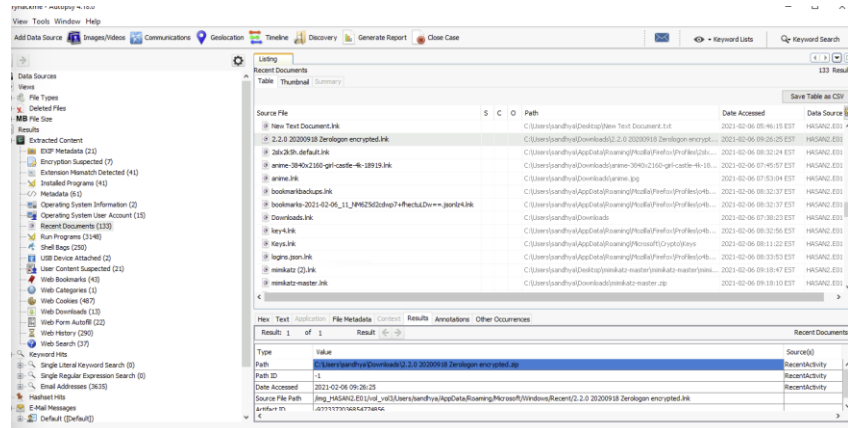
Q15. One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the filename of the archive that you found? (include the spaces in your answer)

사용자 중 한 명이 MS-NRPC 기반 익스플로잇으로 도메인 컨트롤러를 익스플로잇하려고 했다. 찾은 아카이브의 파일 이름은 무엇인가? (답변에 공백을 포함해라)

One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the filename of the archive that you found? (include the spaces in your answer)

Answer format: * * * * *

Submit



Recent Document 창을 살펴보면, Zerologon을 악용하는 익스플로잇이 다운로드되어 있는 것을 확인할 수 있다. 밑에 다운로드된 경로를 확인하여, 해당 경로로 이동해보면, sandhya가 다운로드한 해당 파일의 이름을 확인할 수 있다.

2.2.0 20200918 Zerologon encrypted.zip