Mission Name

Indicators of Compromise

History Context

EUPHEA - Principal & Chancellor's office at Shanghai. The investigation leads to The Principal and the Chancellor. Ethan must place the bug.

Technical High-Level Overview

Player must locate how a binary was downloaded and executed.

Short Description

In previous missions, you had to check Ethan´s bug but this, you´re going to investigate how Ethan downloaded the bug into the system. Your goal will be to identify the binary hidden by Ethan. This binary has something inside it.

Mission Description

Previously was the first time that you go to connect to a live Windows machine to investigate how Ethan placed the bug into the system. This time, you will face an offline evidence to check your capabilities in terms of finding indicators of compromise. Your goal will be to identify the binary hidden by Ethan. This binary has something inside it.

Location

EUPHEA FACULTY | THE PRINCIPAL'S QUARTERS

Tools

- Autopsy: https://www.autopsy.com/download/
- https://github.com/markmckinnon/Autopsy-Plugins
- Imount - pip3 install imagemounter
- Floss - https://github.com/fireeye/flare-floss
- Firepwd - https://github.com/lclevy/firepwd
- Keepass: sudo apt-get install keepass2
- Wine32
- Dislocker: sudo apt install dislocker

Questions

From which domain was downloaded the suspicious binary?

- Windows1.update

From which IP address was downloaded the suspicious binary?

- 192.168.211.164

Which windows binary performed the downloading of the suspicious binary?

- Powershell

Hints

1. Analyse all execution artifacts, specially Prefetch.
2. Check passwords on all applications, including browsers
3. Check encrypted partitions.

Write Up

Player should use Autopsy to mount the image provided:

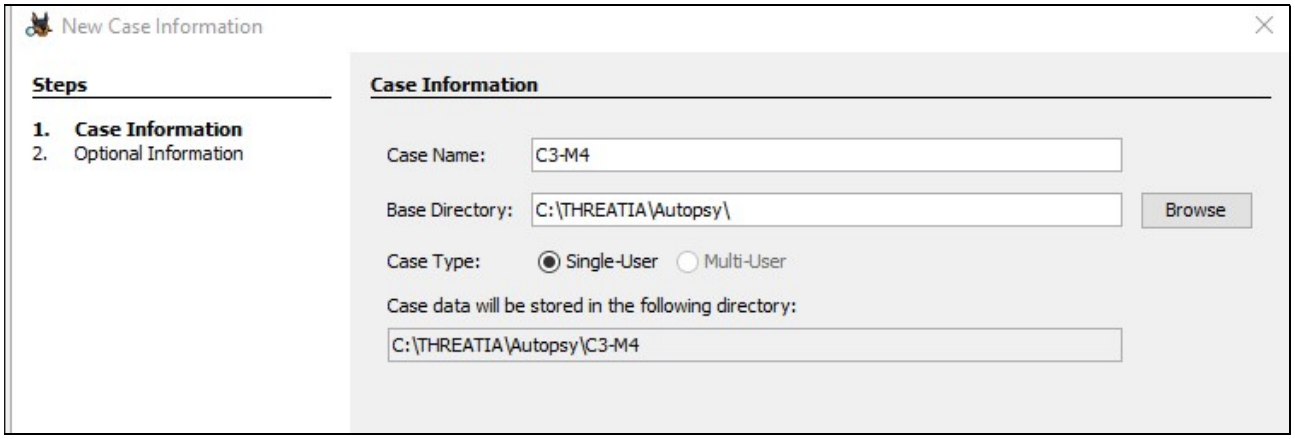


Figure 1

Fill all the necessary information to create the case:

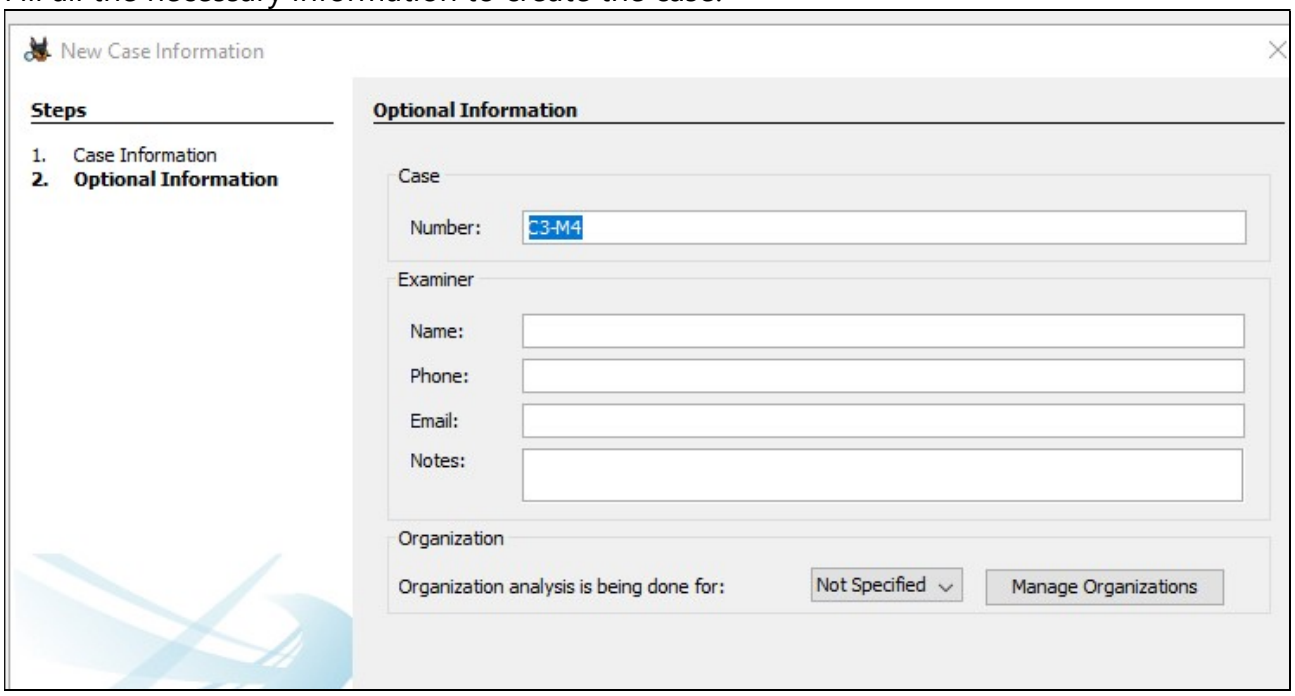


Figure 2

Select the source of the information to analyse:

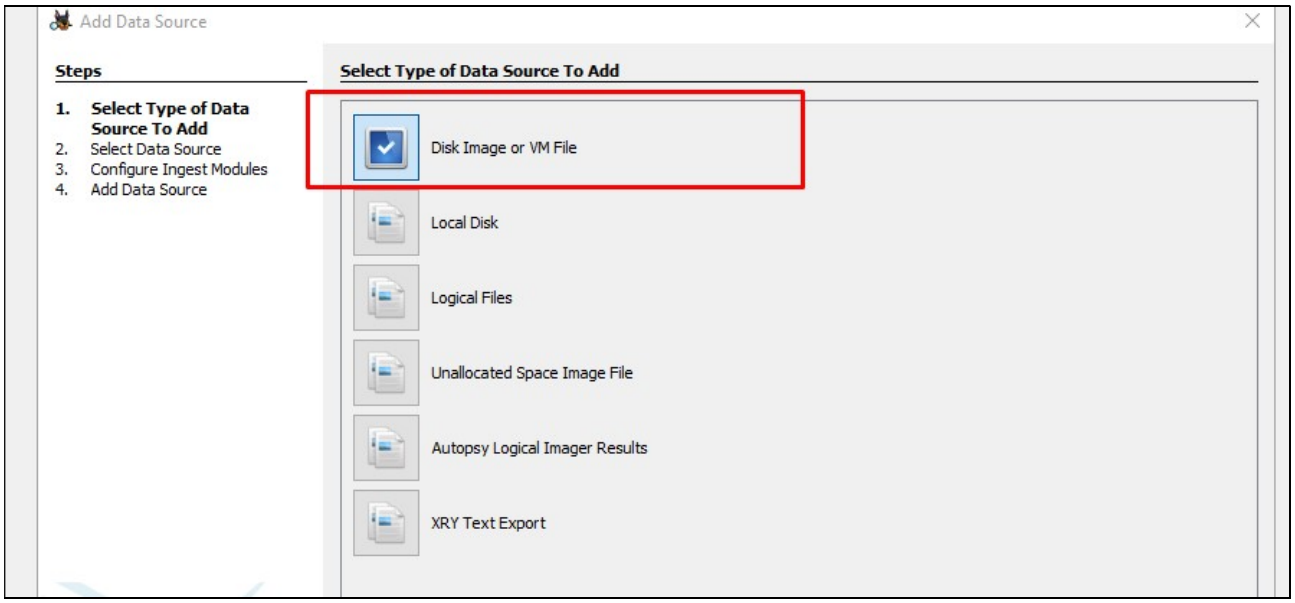


Figure 3

Once Autopsy requires you, to select ingest modules, player must select Windows Internals as the following image:

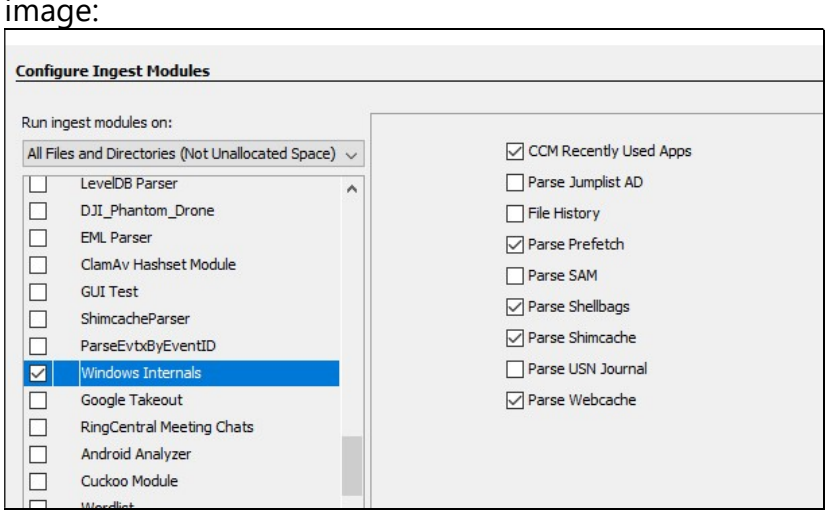


Figure 4

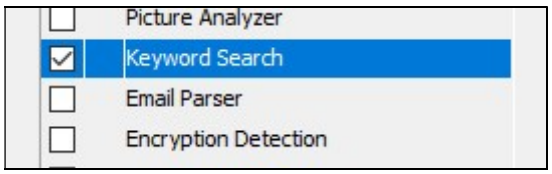


Figure 5

When Autopsy finishes, there will be these options:

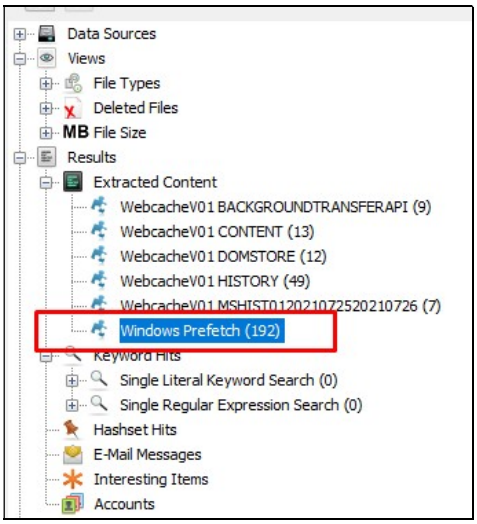
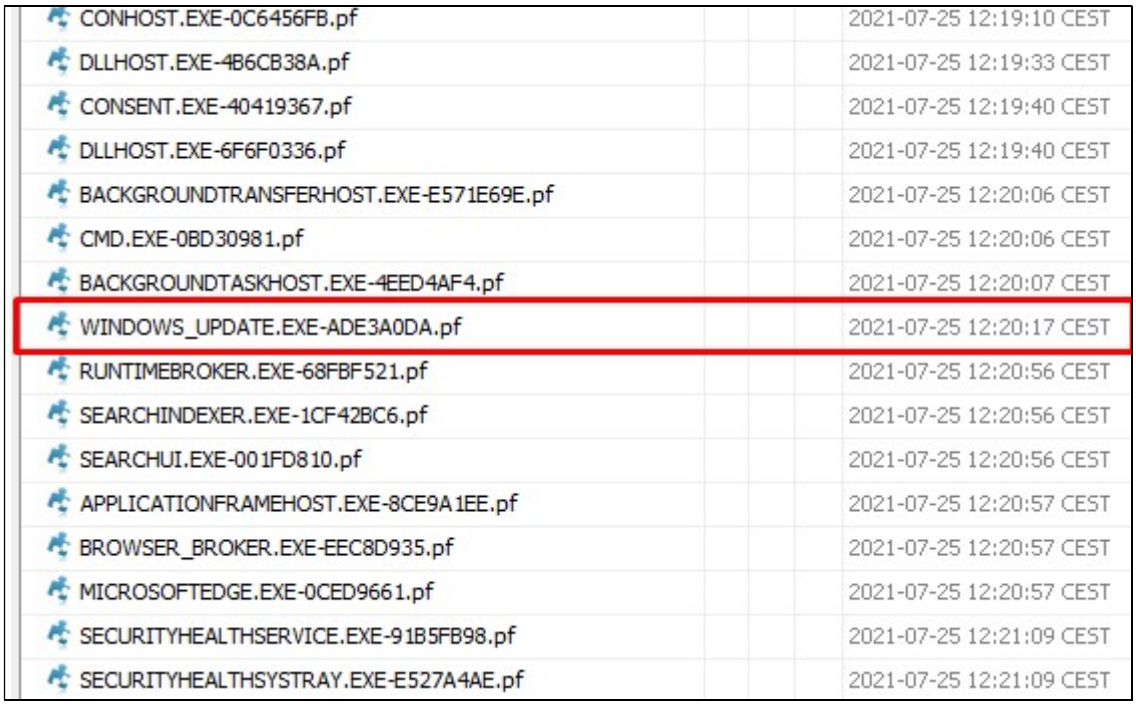


Figure 6

Select Prefetch folder and sort columns by first execution:

Figure 7

As you can see in Autopsy Prefetch, this app would be our target:



CONHOST.EXE-0C6456FB.pf	2021-07-25 12:19:10 CEST
DLLHOST.EXE-4B6CB38A.pf	2021-07-25 12:19:33 CEST
CONSENT.EXE-40419367.pf	2021-07-25 12:19:40 CEST
DLLHOST.EXE-6F6F0336.pf	2021-07-25 12:19:40 CEST
BACKGROUNDTRANSFERHOST.EXE-E571E69E.pf	2021-07-25 12:20:06 CEST
CMD.EXE-0BD30981.pf	2021-07-25 12:20:06 CEST
BACKGROUNDTASKHOST.EXE-4EED4AF4.pf	2021-07-25 12:20:07 CEST
WINDOWS_UPDATE.EXE-ADE3A0DA.pf	2021-07-25 12:20:17 CEST
RUNTIMEBROKER.EXE-68FBF521.pf	2021-07-25 12:20:56 CEST
SEARCHINDEXER.EXE-1CF42BC6.pf	2021-07-25 12:20:56 CEST
SEARCHUI.EXE-001FD810.pf	2021-07-25 12:20:56 CEST
APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf	2021-07-25 12:20:57 CEST
BROWSER_BROKER.EXE-EEC8D935.pf	2021-07-25 12:20:57 CEST
MICROSOFTEDGE.EXE-0CED9661.pf	2021-07-25 12:20:57 CEST
SECURITYHEALTHSERVICE.EXE-91B5FB98.pf	2021-07-25 12:21:09 CEST
SECURITYHEALTHSYSTRAY.EXE-E527A4AE.pf	2021-07-25 12:21:09 CEST

Figure 8

fetch File Name	WINDOWS_UPDATE.EXE-ADE3A0DA.pf
ual File Name	WINDOWS_UPDATE.EXE
gram Number Runs	0
Execution DTTM 1	2021-07-25 12:20:17
Execution DTTM 2	2021-07-25 12:19:10
Execution DTTM 3	0000-00-00 00:00:00
Execution DTTM 4	0000-00-00 00:00:00
Execution DTTM 5	0000-00-00 00:00:00
Execution DTTM 6	0000-00-00 00:00:00
Execution DTTM 7	0000-00-00 00:00:00
Execution DTTM 8	0000-00-00 00:00:00
irce File Path	/img_image.E01/vol_vol6/Windows/Prefetch/WINDOWS_UPDATE.EXE-ADE3A0DA.pf
ifact ID	-9223372036854775620

Figure 9

Perform a search to locate the binary:

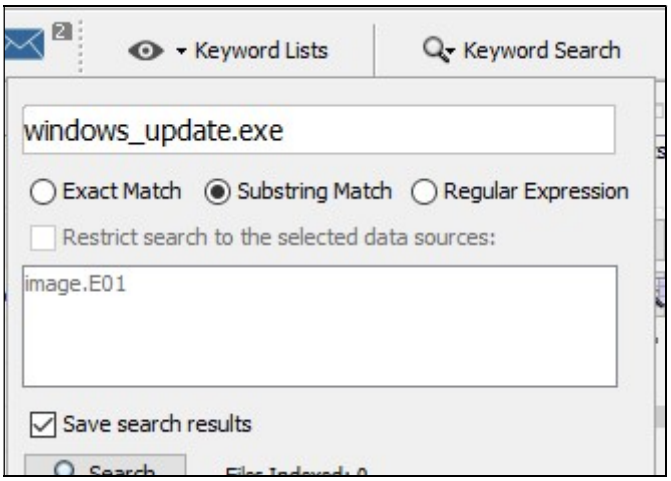

Keyword Lists
Keyword Search
windows_update.exe
Exact Match
Substring Match
Regular Expression
Restrict search to the selected data sources:
image.E01
Save search results

Figure 10

The binary is located at E:

Figure 11

Bitlocker encryption enabled:

```
C:\Windows\System32\BitLockerWizard.exe
-8O7H
Microsoft-Windows-Security-Auditing%
Security
DESKTOP-8O75370$
WORKGROUP
SYSTEM
NT AUTHORITY
Advapi
Negotiate
C:\Windows\System32\services.exe
%%1833
%%1843
%%1842
Microsoft-Windows-Security-Auditing%
Security
xUS3
SYSTEM
NT AUTHORITY
SeAssignPrimaryTokenPrivilege
                                SeTcbPrivilege
                                SeSecurityPrivilege
                                SeTakeOwnershipPrivilege
                                SeLoadDriverPrivilege
                                SeBackupPrivilege
                                SeRestorePrivilege
```

Figure 12

Launch imount to mount the evidence:

sudo imount /mnt/hgfs/C3-M4/evidence/image.E01

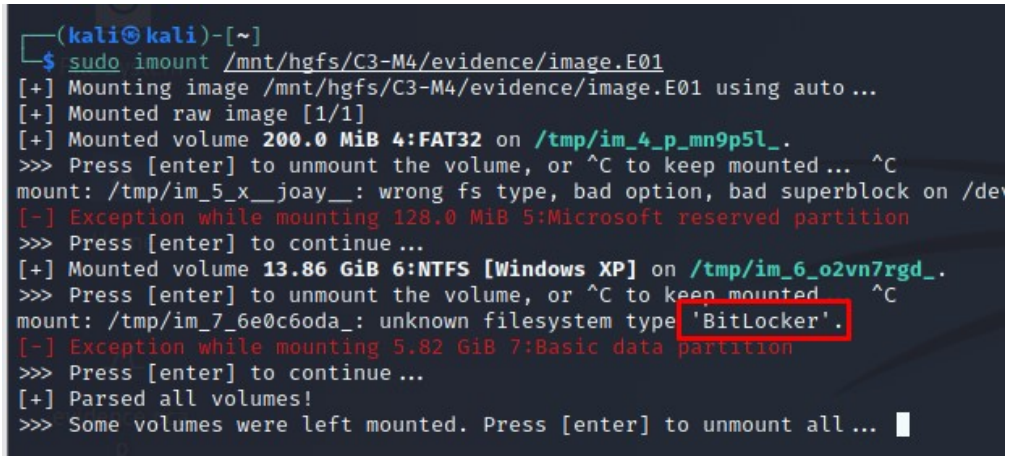


Figure 13

Leave imount, not close.Install FIREPWD

- Git clone https://github.com/lclevy/firepwd.git
- Cd firepwd
- Pip3 install -r requirements

- python3 firepwd.py --dir /tmp/im_6_yz465rea_/Users/skytech/AppData/Roaming/Mozilla/Firefox/Profiles/17qj41m9.default-release/

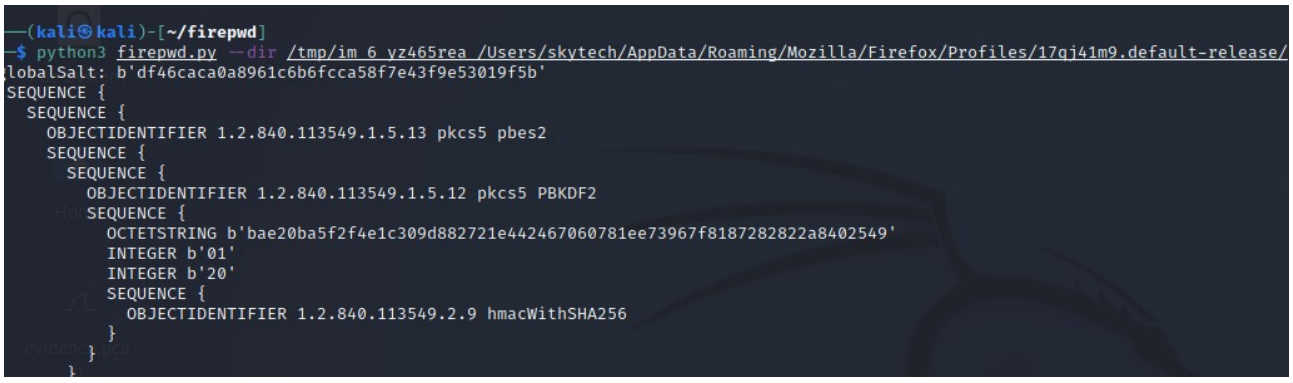


Figure 14

```
    }
    OCTETSTRING b'6f3199544e79d4cd1398f15a79101114d4e820dcc91a6363eb5f035e1d33c9f9'
  }
clearText b'f7925ea1f7c84fd5233176b3c4e668700d46d6e94c9273d008080808080808080808'
decrypting login/password pairs
https://account.protonmail.com:b'skytech',b'Ethanwascheckingifyouarethebest!'
https://account.protonmail.com:b'skytech-hq',b'Ethanwascheckingifyouarethebest!'
```

Figure 15

We have located cached password on Firefox. Next step would be to check Keepass:

- sudo apt-get install keepass2

Open it, and locate database on the image mounted:

- /tmp/im_6_yz465rea_/Users/skytech/MyDocuments/Database.kdbx

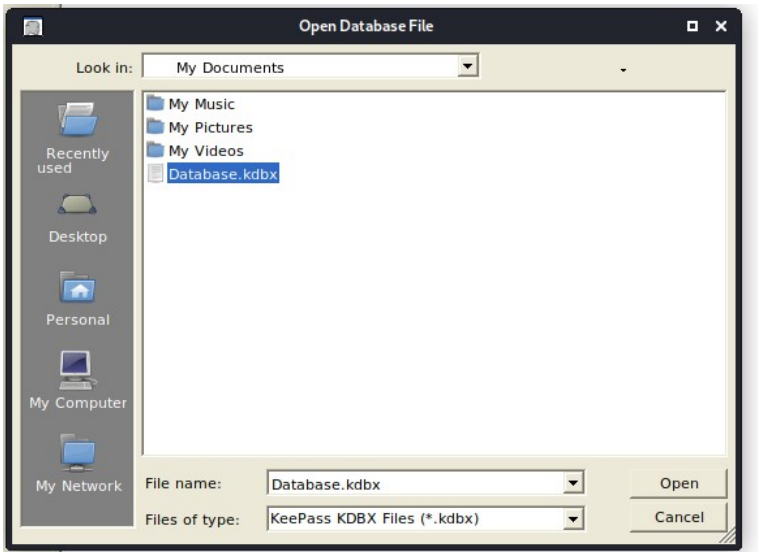


Figure 16

Use password extracted from Firefox: **Ethanwascheckingifyouarethebest!**

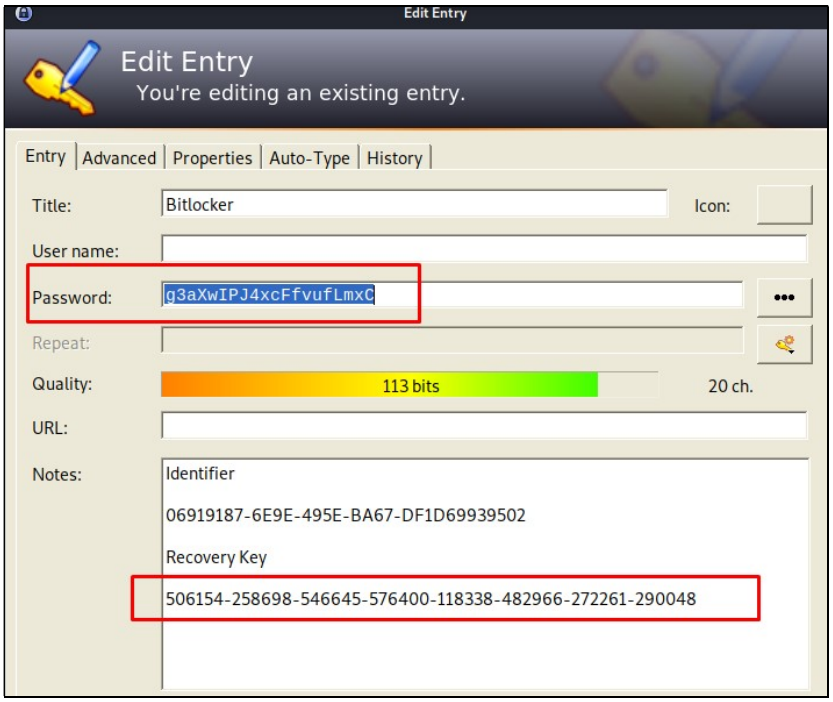


Figure 17

- sudo ewfmount /mnt/hgfs/C3-M4/evidence/image.E01 /mnt/fcroot

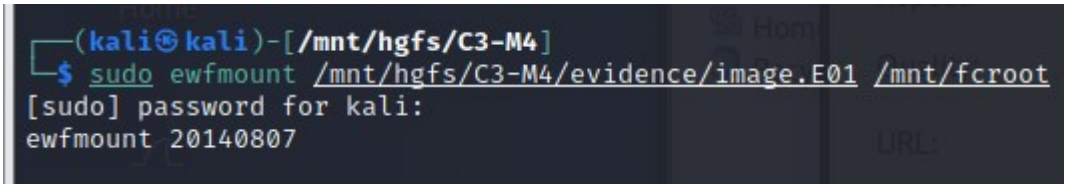
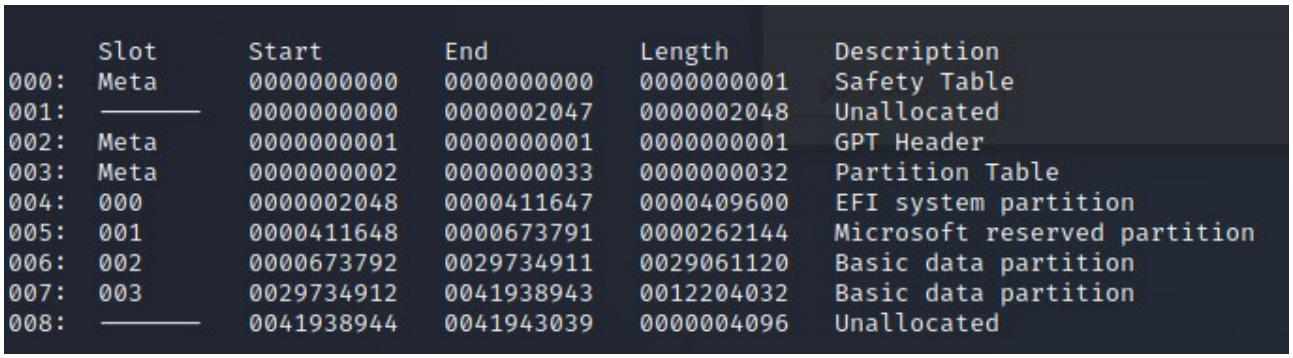


Figure 18

```
sudo mmls /mnt/fcroot/ewf1
```



	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Safety Table
001:	————	0000000000	0000002047	0000002048	Unallocated
002:	Meta	0000000001	0000000001	0000000001	GPT Header
003:	Meta	0000000002	0000000033	0000000032	Partition Table
004:	000	0000002048	0000411647	0000409600	EFI system partition
005:	001	0000411648	0000673791	0000262144	Microsoft reserved partition
006:	002	0000673792	0029734911	0029061120	Basic data partition
007:	003	0029734912	0041938943	0012204032	Basic data partition
008:	————	0041938944	0041943039	0000004096	Unallocated

Figure 19

```
sudo apt install dislocker
sudo mkdir -p /media/bitlocker_decrypt
sudo mkdir -p /media/bitlocker_mount
sudo dislocker /mnt/fcroot/ewf1 -O 15224274944 -u /media/bitlocker_decrypt
```

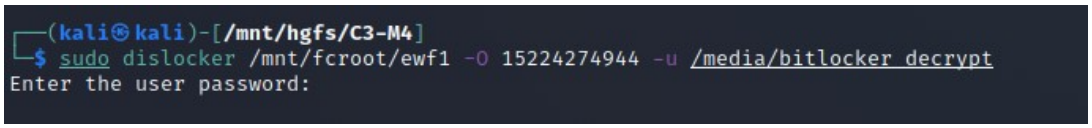


Figure 20

Insert password: g3aXwIPJ4xcFfvufLmxC

```
sudo mount -o loop /media/bitlocker_decrypt/dislocker-file /media/bitlocker_mount
```

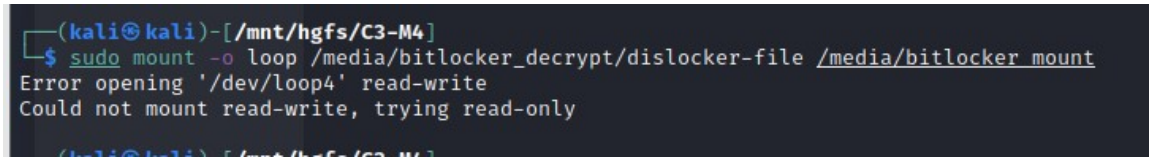


Figure 21

```
cd /media/bitlocker_mount
```

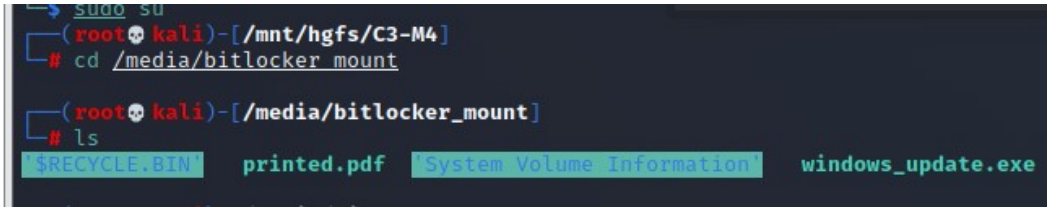


Figure 22

```
wine windows_update.exe
```

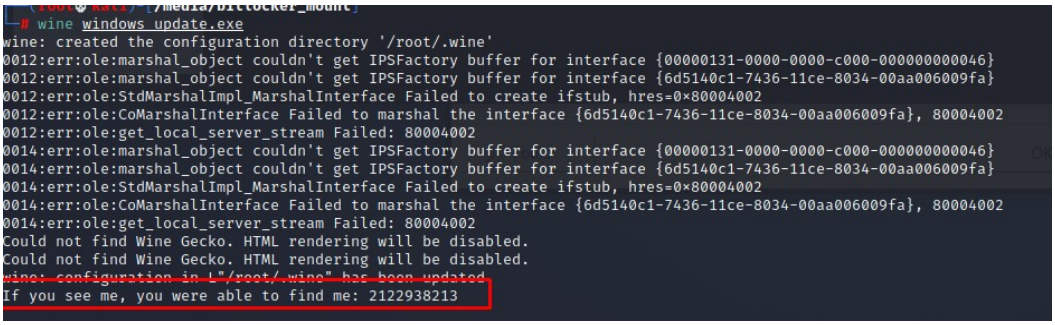


Figure 23

Flag Information

flag{2122938213}