ForeignerForensics - Writeup

An actual forensics-forensics challenge.

Participants are given two sets of forensic images, which have been compressed super hard :

1. A .E01 forensic image of the suspect's computer. (5.71 GB)
2. A .E01 forensic image for the suspect's encrypted USB. (30MB)

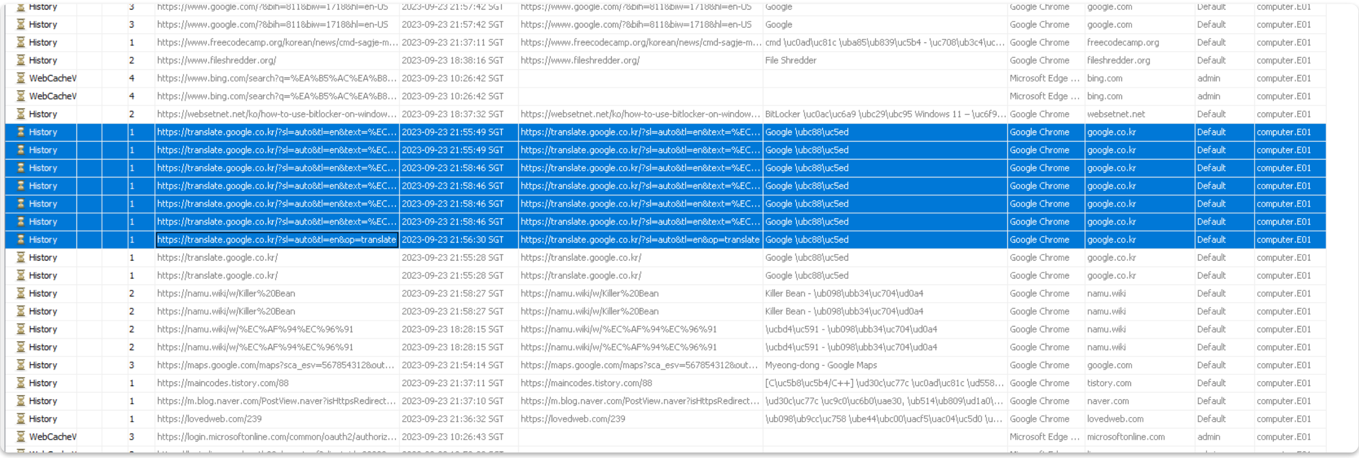
To demonstrate how this challenge can be solved, I will be using Autopsy. Magnet

Step 1 : Find stuff

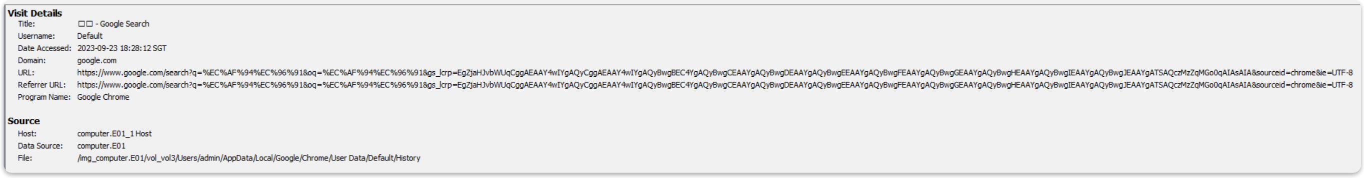
Start by analyzing the first disk, as it's not encrypted. There are a whole lot of irrelevant files in the forensic image, but we should focus on the suspect's web history.

There are a lot of instances where the suspect went to the forum page reddit. The suspect has also made several searches in korean related to file deletion.

More notably, there are quite a few times where google translate appeared in the suspect's searches. We can see the full URL of the google translate search:



History			3	https://www.google.com/?&bih=811&biw=1718&hl=en-US	2023-09-23 21:57:42 SGT	https://www.google.com/?&bih=811&biw=1718&hl=en-US	Google	Google Chrome	google.com	Default	computer.E01
History			3	https://www.google.com/?&bih=811&biw=1718&hl=en-US	2023-09-23 21:57:42 SGT	https://www.google.com/?&bih=811&biw=1718&hl=en-US	Google	Google Chrome	google.com	Default	computer.E01
History			1	https://www.freecodecamp.org/korean/news/cmd-sagje-m...	2023-09-23 21:37:11 SGT	https://www.freecodecamp.org/korean/news/cmd-sagje-m...	cmd \uc0ad\uc81c \uba85\ub839\uc5b4 - \uc708\ub3c4\uc...	Google Chrome	freecodecamp.org	Default	computer.E01
History			2	https://www.fileshredder.org/	2023-09-23 18:38:16 SGT	https://www.fileshredder.org/	File Shredder	Google Chrome	fileshredder.org	Default	computer.E01
WebCacheV			4	https://www.bing.com/search?q=%EA%B5%AC%EA%B8...	2023-09-23 10:26:42 SGT			Microsoft Edge ...	bing.com	admin	computer.E01
WebCacheV			4	https://www.bing.com/search?q=%EA%B5%AC%EA%B8...	2023-09-23 10:26:42 SGT			Microsoft Edge ...	bing.com	admin	computer.E01
History			2	https://websetnet.net/ko/how-to-use-bitlocker-on-window...	2023-09-23 18:37:32 SGT	https://websetnet.net/ko/how-to-use-bitlocker-on-window...	BitLocker \uc0ac\uc6a9 \ubc29\ubc95 Windows 11 – \uc6f9...	Google Chrome	websetnet.net	Default	computer.E01
History			1	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	2023-09-23 21:55:49 SGT	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	2023-09-23 21:55:49 SGT	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	2023-09-23 21:58:46 SGT	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	2023-09-23 21:58:46 SGT	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	2023-09-23 21:58:46 SGT	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	2023-09-23 21:58:46 SGT	https://translate.google.co.kr/?sl=auto&tl=en&text=%EC...	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/?sl=auto&tl=en&op=translate	2023-09-23 21:56:30 SGT	https://translate.google.co.kr/?sl=auto&tl=en&op=translate	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/	2023-09-23 21:55:28 SGT	https://translate.google.co.kr/	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			1	https://translate.google.co.kr/	2023-09-23 21:55:28 SGT	https://translate.google.co.kr/	Google \ubc88\uc5ed	Google Chrome	google.co.kr	Default	computer.E01
History			2	https://namu.wiki/w/Killer%20Bean	2023-09-23 21:58:27 SGT	https://namu.wiki/w/Killer%20Bean	Killer Bean - \ub098\ubb34\uc704\ud0a4	Google Chrome	namu.wiki	Default	computer.E01
History			2	https://namu.wiki/w/Killer%20Bean	2023-09-23 21:58:27 SGT	https://namu.wiki/w/Killer%20Bean	Killer Bean - \ub098\ubb34\uc704\ud0a4	Google Chrome	namu.wiki	Default	computer.E01
History			2	https://namu.wiki/w/%EC%AF%94%EC%96%91	2023-09-23 18:28:15 SGT	https://namu.wiki/w/%EC%AF%94%EC%96%91	\ucbd4\uc591 - \ub098\ubb34\uc704\ud0a4	Google Chrome	namu.wiki	Default	computer.E01
History			2	https://namu.wiki/w/%EC%AF%94%EC%96%91	2023-09-23 18:28:15 SGT	https://namu.wiki/w/%EC%AF%94%EC%96%91	\ucbd4\uc591 - \ub098\ubb34\uc704\ud0a4	Google Chrome	namu.wiki	Default	computer.E01
History			3	https://maps.google.com/maps?sca_esv=567854312&out...	2023-09-23 21:54:14 SGT	https://maps.google.com/maps?sca_esv=567854312&out...	Myeong-dong - Google Maps	Google Chrome	google.com	Default	computer.E01
History			1	https://maincodes.tistory.com/88	2023-09-23 21:37:11 SGT	https://maincodes.tistory.com/88	[C\uc5b8\uc5b4/C++] \ud30c\uc77c \uc0ad\uc81c \ud558...	Google Chrome	tistory.com	Default	computer.E01
History			1	https://m.blog.naver.com/PostView.naver?isHttpsRedirect...	2023-09-23 21:37:10 SGT	https://m.blog.naver.com/PostView.naver?isHttpsRedirect...	\ud30c\uc77c \uc9c0\uc6b0\uae30, \ub514\ub809\ud1a0\...	Google Chrome	naver.com	Default	computer.E01
History			1	https://lovedweb.com/239	2023-09-23 21:36:32 SGT	https://lovedweb.com/239	\ub098\ub9cc\uc758 \ube44\ubc00\uacf5\uac04\uc5d0 \u...	Google Chrome	lovedweb.com	Default	computer.E01
WebCacheV			3	https://login.microsoftonline.com/common/oauth2/authoriz...	2023-09-23 10:26:43 SGT			Microsoft Edge ...	microsoftonline.com	admin	computer.E01



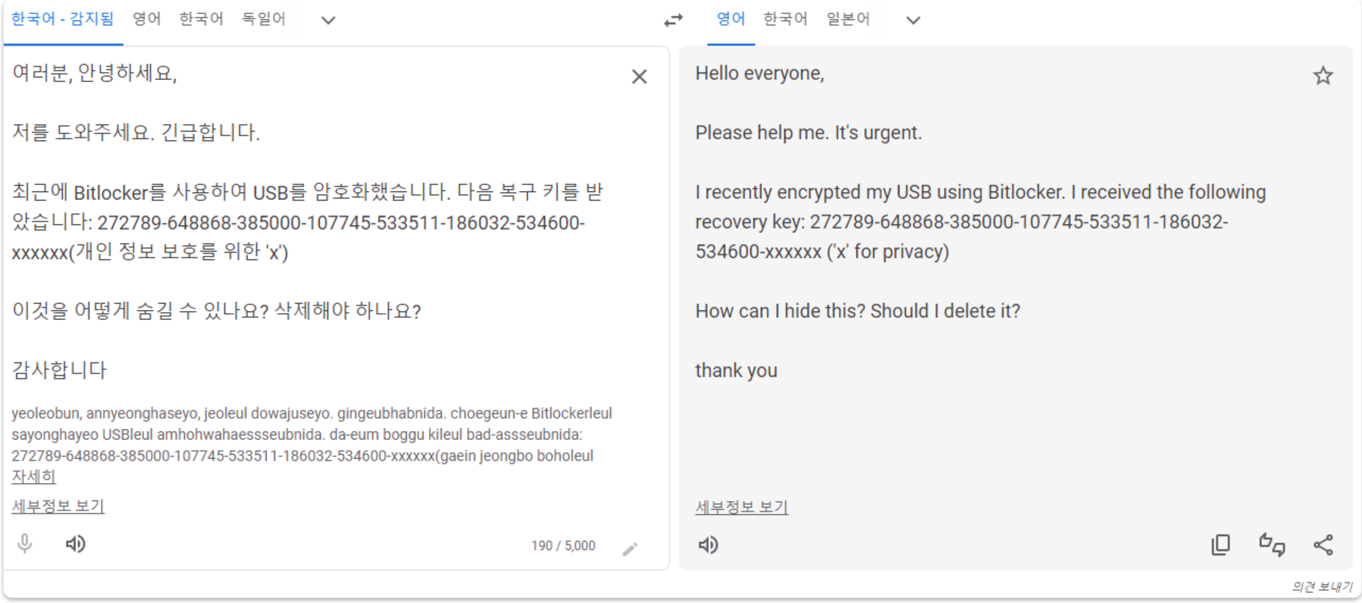
Visit Details

Title: □□ - Google Search
Username: Default
Date Accessed: 2023-09-23 18:28:12 SGT
Domain: google.com
URL: https://www.google.com/search?q=%EC%AF%94%EC%96%91&oq=%EC%AF%94%EC%96%91&gs_lcrp=EgZjaHJvbWUqCggAEAAY4wIYgAQyCggAEAAY4wIYgAQyBwgBEC4YgAQyBwgCEAAYgAQyBwgDEAAYgAQyBwgEEAAYgAQyBwgFEAAYgAQyBwgGEAAYgAQyBwgHEAAYgAQyBwgIEAAYgAQyBwgJEAAYgATSAQczMzZqMGo0qAIAsAIA&sourceid=chrome&ie=UTF-8
Referrer URL: https://www.google.com/search?q=%EC%AF%94%EC%96%91&oq=%EC%AF%94%EC%96%91&gs_lcrp=EgZjaHJvbWUqCggAEAAY4wIYgAQyCggAEAAY4wIYgAQyBwgBEC4YgAQyBwgCEAAYgAQyBwgDEAAYgAQyBwgEEAAYgAQyBwgFEAAYgAQyBwgGEAAYgAQyBwgHEAAYgAQyBwgIEAAYgAQyBwgJEAAYgATSAQczMzZqMGo0qAIAsAIA&sourceid=chrome&ie=UTF-8
Program Name: Google Chrome

Source

Host: computer.E01_1 Host
Data Source: computer.E01
File: /img_computer.E01/vol_vol3/Users/admin/AppData/Local/Google/Chrome/User Data/Default/History

Going to the link actually shows us what the suspect was trying to translate from korean to english. Appears to be asking some people for help regarding a bitlocker encrypted USB.



여러분, 안녕하세요,

저를 도와주세요. 긴급합니다.

최근에 Bitlocker를 사용하여 USB를 암호화했습니다. 다음 복구 키를 받았습니다: 272789-648868-385000-107745-533511-186032-534600-xxxxxx(개인 정보 보호를 위한 'x')

이것을 어떻게 숨길 수 있나요? 삭제해야 하나요?

감사합니다

yeoleobun, annyeonghaseyo, jeoleul dowajuseyo. gingeubhabnida. choegeun-e Bitlockerleul sayonghayeo USBleul amhohwahaessseubnida. da-eum boggu kileul bad-assseubnida: 272789-648868-385000-107745-533511-186032-534600-xxxxxx(gaein jeongbo boholeul 자세히

Hello everyone,

Please help me. It's urgent.

I recently encrypted my USB using Bitlocker. I received the following recovery key: 272789-648868-385000-107745-533511-186032-534600-xxxxxx ('x' for privacy)

How can I hide this? Should I delete it?

thank you

The suspect revealed pretty much his entire bitlocker recovery code, except for the last 6 digits. This calls for bruteforcing!! Pretty useful link : https://github.com/e-ago/bitcracker

Step 2 : Extract hashes, make a wordlist

We can generate a wordlist based on what we know. this can be done using john :

```
 john --mask=272789-648868-385000-107745-533511-186032-534600[-]?d?d?d?d?d?d --stdout
> bitlocker_wordlist.txt
```

Or you can use the Crunch wordlist generator. Same thing.

We should also extract the bitlocker hash from the image of the encrypted drive. Now the problem is that the bitcracker tool mentioned above only accepts .img and .vhd formats for the extraction of hashes. This is up to the participant to figure out, I managed to do it pretty easily.

After conversion, we can run this command,

```
 bitlocker2john -i usb.vhd
```

which will yield the following output :

```
 User Password hash:
$bitlocker$0$16$7548c4905f71bcf0a40279f007d8a697$1048576$12$50ce905509eed90103000000$60$
49836926f0c0a51df2fb1d56f13e30662697bea218bbf477be889dfdf2fb5bd7e53176a7d26a984a13cf5f3a
3d45fb7044e2c97cb2eeef1c8e9a91b7
Hash type: User Password with MAC verification (slower solution, no false positives)
$bitlocker$1$16$7548c4905f71bcf0a40279f007d8a697$1048576$12$50ce905509eed90103000000$60$
49836926f0c0a51df2fb1d56f13e30662697bea218bbf477be889dfdf2fb5bd7e53176a7d26a984a13cf5f3a
```

```
3d45fb7044e2c97cb2eeef1c8e9a91b7
Hash type: Recovery Password fast attack
$bitlocker$2$16$cde282e850b667d65817a05584f07fa1$1048576$12$50ce905509eed90106000000$60$
1a150ce5e07e291d50db3d07f977fe3666b49cdb5280f4625440a34263915c9b82d76126b46a7928296ef637
0fe33feb209306da2d57dce9422417a6
Hash type: Recovery Password with MAC verification (slower solution, no false positives)
$bitlocker$3$16$cde282e850b667d65817a05584f07fa1$1048576$12$50ce905509eed90106000000$60$
1a150ce5e07e291d50db3d07f977fe3666b49cdb5280f4625440a34263915c9b82d76126b46a7928296ef637
0fe33feb209306da2d57dce9422417a6
```

We can ignore the User Password hashes, as we have no idea what the suspect set his bitlocker password as. Recovery Password fast attack might work, but we should proceed with Recovery Password with MAC verification for a smaller risk of false positives.

Step 3 : Crack

```
john --format=bitlocker-opencl --wordlist=bitlocker_wordlist.txt bitlocker.hash
```

You will eventually get the correct key : 272789-648868-385000-107745-533511-186032-534600-394768

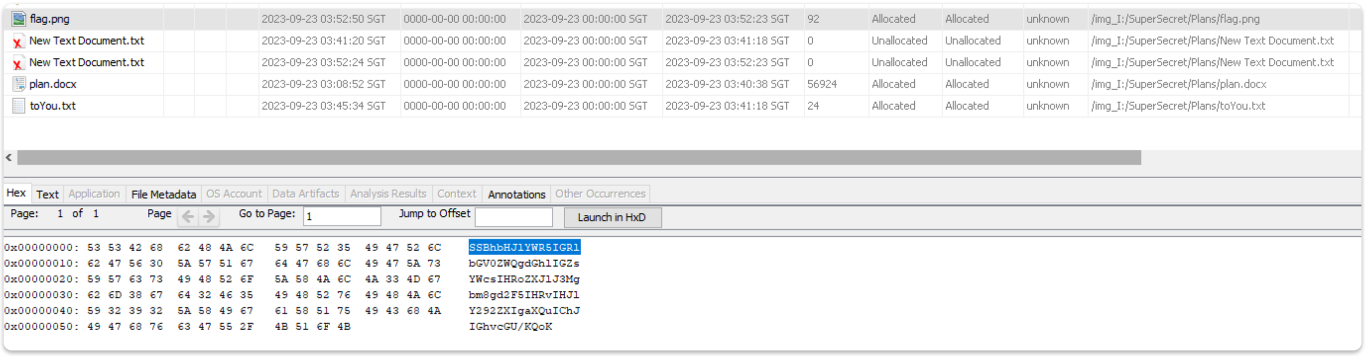
Brute forcing shouldn't take too long, because we are only missing 6 digits.

Step 4 : Examine the decrypted USB

It is now up to the participants to figure out a way to decrypt the encrypted USB and examine its contents.

What I did was use Arsenal Image Mounter, mount the encrypted E01 as an external drive, and decrypt it. Then I used autopsy and selected the mounted virtual disk as an evidence source.

There are quite a few red herrings left in the USB drive, but when we look at flag.png, we see some base64 encoded text :

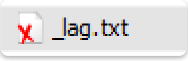


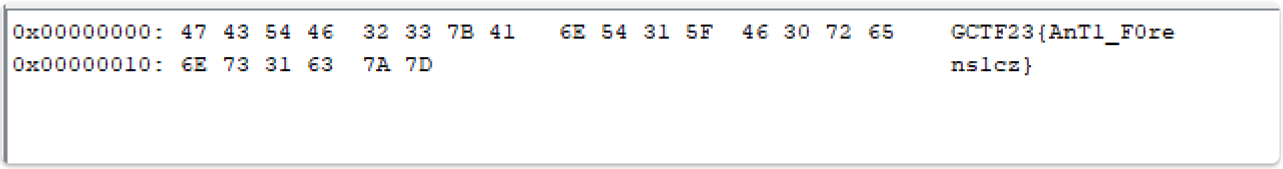
flag.png				2023-09-23 03:52:50 SGT	0000-00-00 00:00:00	2023-09-23 00:00:00 SGT	2023-09-23 03:52:23 SGT	92	Allocated	Allocated	unknown	/img_I:/SuperSecret/Plans/flag.png
New Text Document.txt				2023-09-23 03:41:20 SGT	0000-00-00 00:00:00	2023-09-23 00:00:00 SGT	2023-09-23 03:41:18 SGT	0	Unallocated	Unallocated	unknown	/img_I:/SuperSecret/Plans/New Text Document.txt
New Text Document.txt				2023-09-23 03:52:24 SGT	0000-00-00 00:00:00	2023-09-23 00:00:00 SGT	2023-09-23 03:52:23 SGT	0	Unallocated	Unallocated	unknown	/img_I:/SuperSecret/Plans/New Text Document.txt
plan.docx				2023-09-23 03:08:52 SGT	0000-00-00 00:00:00	2023-09-23 00:00:00 SGT	2023-09-23 03:40:38 SGT	56924	Allocated	Allocated	unknown	/img_I:/SuperSecret/Plans/plan.docx
toYou.txt				2023-09-23 03:45:34 SGT	0000-00-00 00:00:00	2023-09-23 00:00:00 SGT	2023-09-23 03:41:18 SGT	24	Allocated	Allocated	unknown	/img_I:/SuperSecret/Plans/toYou.txt

```
0x00000000: 53 53 42 68  62 48 4A 6C  59 57 52 35  49 47 52 6C    SSBhbHJ1YWR5IGRl
0x00000010: 62 47 56 30  5A 57 51 67  64 47 68 6C  49 47 5A 73    bGV0ZWQgdGhlIGZs
0x00000020: 59 57 63 73  49 48 52 6F  5A 58 4A 6C  4A 33 4D 67    YWcsIHRoZXJlJ3Mg
0x00000030: 62 6D 38 67  64 32 46 35  49 48 52 76  49 48 4A 6C    bm8gd2F5IHRvIHJl
0x00000040: 59 32 39 32  5A 58 49 67  61 58 51 75  49 43 68 4A    Y292ZXIgaXQuIChJ
0x00000050: 49 47 68 76  63 47 55 2F  4B 51 6F 4B                 IGhvcGU/KQoK
```

Decoded, it says the following : I already deleted the flag, there's no way to recover it. (I hope?)

Pretty good hint to look at what your favored forensics tool carved out from the USB image. The flag is actually in a deleted file :


_lag.txt



```
0x00000000: 47 43 54 46  32 33 7B 41   6E 54 31 5F  46 30 72 65    GCTF23{AnT1_F0re
0x00000010: 6E 73 31 63  7A 7D                                     ns1cz}
```

Flag : GCTF23{AnT1_F0rens1cz}

Note : In Autopsy, the deleted file is straight up there in the root directory of the image. Wasn't intentional, but oh well.