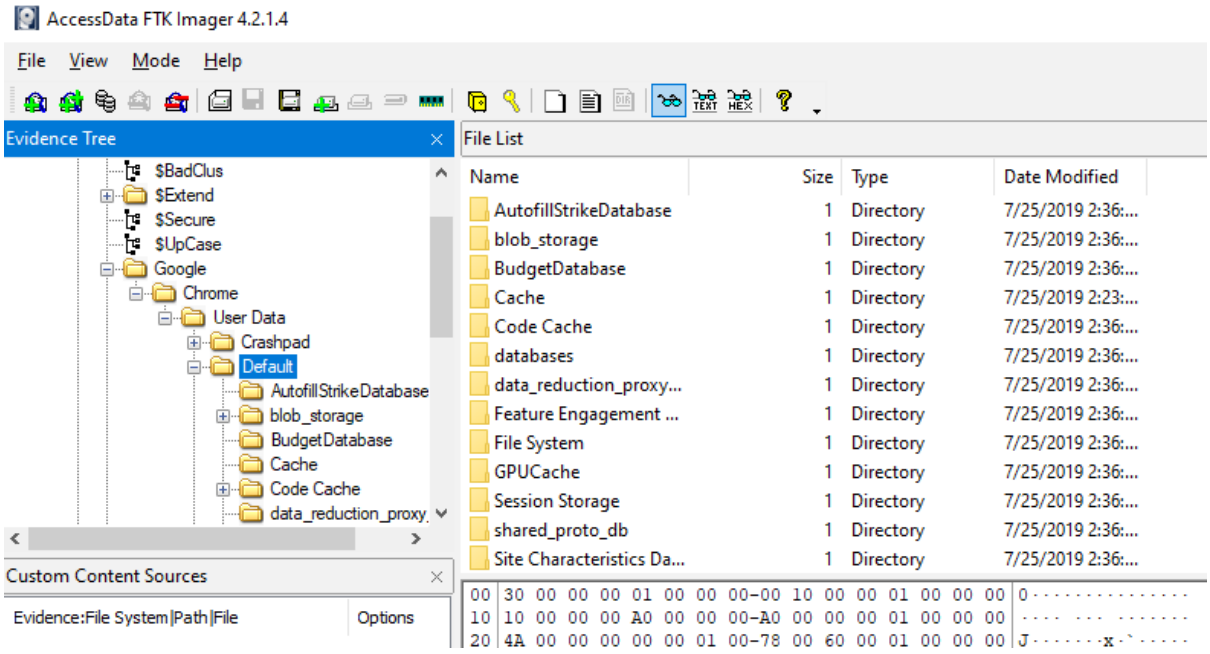
Challenge 10

FLAG: “I AM BACK.jpg”

Checked in Linux “file ‘Cloud Memories.E01’ and know it’s an Encase image file.

Used FTK Imager to add the image as evidence item. Saw a chrome profile.



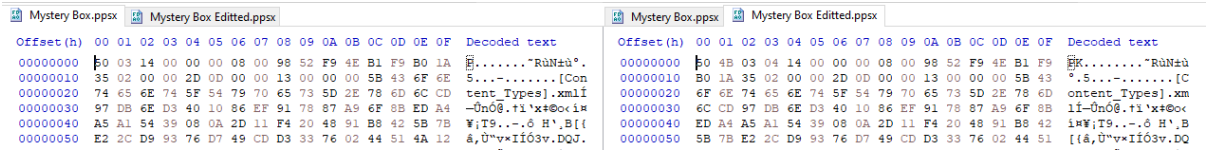
Since the txt mentioned that the hints are in his browser, I used Hindsight to analyse the web artifacts and extract out a list of urls. This url https://mega.nz/#F!K0FjIlBK!86xtcPjjd0HGNHx6BirlBw stood out, since it’s a file hosting service.

Hindsight Internet History Forensics (v2.4.0)				
Type	Timestamp (US/Pacif	URL	Title / Name / Status	Data / Value /
url	2019-07-23 20:38:15.970	https://www.google.com/search?rlz=1C1CHBF_enSG859SG859&ei=d	modern encryption standards - Google Sea	
url	2019-07-23 20:38:18.982	https://en.wikipedia.org/wiki/Cryptography_standards	Cryptography standards - Wikipedia	
preference	2019-07-23 20:38:36.807	https://blog.storagecraft.com:443,*	media_engagement [in Prefe	{u'last_modifi
url	2019-07-23 20:38:47.269	https://www.google.com/search?rlz=1C1CHBF_enSG859SG859&ei=q	file encryption software - Google Search	
url	2019-07-23 20:39:08.658	https://www.google.com/search?q=hyperlinks+pictures&oq=hyperli	hyperlinks pictures	
preference	2019-07-23 20:39:40.920	https://www.pcmag.com:443,*	site_engagement [in Prefere	{u'last_modifi
preference	2019-07-23 20:40:11.362	https://www.techrepublic.com:443,*	media_engagement [in Prefe	{u'last_modifi
preference	2019-07-23 20:40:17.965	https://lifehacker.com:443,*	media_engagement [in Prefe	{u'last_modifi
preference	2019-07-23 20:40:20.667	https://www.pcmag.com:443,*	media_engagement [in Prefe	{u'last_modifi
url	2019-07-23 20:40:27.099	https://www.google.com/search?rlz=1C1CHBF_enSG859SG859&ei=x	SHA 512 - Google Search	
url	2019-07-23 20:40:32.365	https://en.wikipedia.org/wiki/Secure_Hash_Algorithms	Secure Hash Algorithms - Wikipedia	
url	2019-07-23 20:40:44.650	https://www.google.com/search?rlz=1C1CHBF_enSG859SG859&ei=K	aes encryption - Google Search	
url	2019-07-23 20:40:47.476	https://en.wikipedia.org/wiki/Advanced_Encryption_Standard	Advanced Encryption Standard - Wikipedia	
url	2019-07-23 20:40:50.658	https://searchsecurity.techtarget.com/definition/Advanced-Encrypt	What is Advanced Encryption Standard (AE	
preference	2019-07-23 20:40:53.660	https://searchsecurity.techtarget.com:443,*	media_engagement [in Prefe	{u'last_modifi
url	2019-07-23 20:41:17.277	https://mega.nz/#F!K0FjIIBK!86xtcPjjd0HGNHx6BirlBw	MEGA	
url	2019-07-23 20:41:18.018	https://mega.nz/#F!K0FjIIBK!86xtcPjjd0HGNHx6BirlBw	MEGA	
preference	2019-07-23 20:41:35.942	https://mega.nz:443,*	site_engagement [in Prefere	{u'last_modifi
url	2019-07-23 20:47:31.926	https://www.google.com/search?q=tifa+final+fantasy+7&rlz=1C1CHE	tifa final fantasy 7 - Google Search	
url	2019-07-23 20:47:37.210	https://finalfantasy.fandom.com/wiki/Tifa_Lockhart	Tifa Lockhart | Final Fantasy Wiki | FANDOM	
url	2019-07-23 20:47:44.083	https://www.polygon.com/e3/2019/6/10/18660611/final-fantasy-7-r	Final Fantasy 7 Remake: First look at Tifa in	
preference	2019-07-23 20:47:47.732	https://finalfantasy.fandom.com:443,*	site_engagement [in Prefere	{u'last_modifi
url	2019-07-23 20:47:52.051	https://www.polygon.com/e3/2019/6/10/18660611/final-fantasy-7-r	Final Fantasy 7 Remake: First look at Tifa in	
preference	2019-07-23 20:47:53.902	https://www.polygon.com:443,*	media_engagement [in Prefe	{u'last_modifi
url	2019-07-23 20:47:58.582	https://www.google.com/search?rlz=1C1CHBF_enSG859SG859&ei=1	aerith final fantasy - Google Search	
url	2019-07-23 20:48:02.983	https://finalfantasy.fandom.com/wiki/Aerith_Gainsborough	Aerith Gainsborough | Final Fantasy Wiki |	
url	2019-07-23 20:48:06.330	https://en.wikipedia.org/wiki/Aerith_Gainsborough	Aerith Gainsborough - Wikipedia	
cache (gpu)	2019-07-23 20:48:10.937	Chrome/75.0.3770.142----:JDD0SeTco7k66PYSM0zJXCNSQOo=	Normal (data cached)	

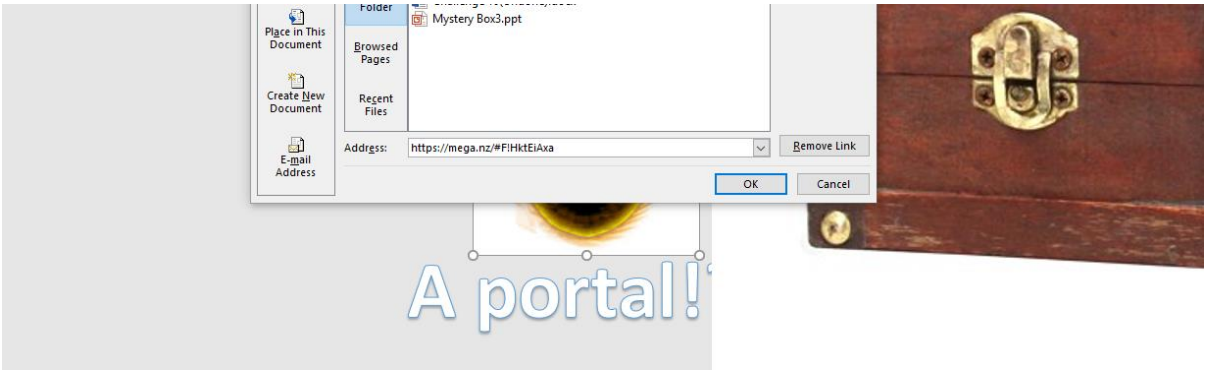
Downloaded the Mystery.ppsx and tried opening with Powerpoint, not possible. May be it's not a ppsx file?

Used binwalk –e Mystery.ppsx to extract the files within it. From the content inside, I found a treasure chest and a portal image. The xml files also suggested that this is a ppt/pptx/ppsx file.

Went to create sample ppsx files and downloaded some online. Using HxD, I notice that the file header is different, [Content_Types].xml should start at 0x100E but it starts at 0x100C, and the header should contain "PK" (50 4B 03 04). I tried my luck by replacing the first two bytes with "50 4B 03 04", pushing the [Content_Types].xml to start at 0x100E. Opening the ppsx works.



Navigating the ppsx seems to only display the treasure chest with "Huh? What is this?". I remember seeing a portal image and "A portal!?" text when going through the extracted materials. I opened it as a ppt instead and found the portal image and text hidden below the treasure chest. Remembering that the user tried searching for hyperlinking image, I checked the hyperlink of the portal and found another Mega link "https://mega.nz/#F!HktEiAxa".



This mega link requires a decryption key that can only be known if we login to Cloud's mega account. Went to look through the img file but find no login credentials, checked Login Data file as well. So it's pretty impossible to find his credential and I think that there's a key which is hidden somewhere.

Went to do more research and found out that the ppsx file is actually in OOXML. Initial idea about being a ppsx file is not wrong, but the main idea is that it can be renamed to a zip file.

Opening up the zip file, I checked the [Content_Types].xml and found the decryption key: _36vglVUGFG5wapRBbTzIA

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <Types xmlns="http://schemas.openxmlformats.org/package/2006/content-types">
  <!-- Hi! This is young Cloud. In case I lose my memory in the future, this is my cloud key. You get it? Cloud... Cloud Key...? No? Ok nevermind.. Mega key:
  _36vglVUGFG5wapRBbTzIA -->
    <Default ContentType="image/jpeg" Extension="jpeg"/>
    <Default ContentType="image/png" Extension="png"/>
    <Default ContentType="application/vnd.openxmlformats-package.relationships+xml" Extension="rels"/>
```

This time it's a Hidden Box.7zip file. Downloaded and extracted out "Hidden Box", "MY Memories.mem" and a "README". Read the hint from the README.

Checked "Hidden Box" with file command on linux, then run binwalk with it. No information.

"My Memories.mem" is a memory dump. Maybe this is a memory analysis.

Search for tools to analyse My Memories.mem and found Volatility. Rename the memory dump to mem.mem. Run a command to scan the processes. Volatility_2.6_win64_standalone –profile=Win7SP0x64 psscan –f mem.mem

```
C:\Users\NTUIntern\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone --profile=Win7SP
0x64 psscan -f mem.mem
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB               Time created                   Time exited
------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------
0x000000003da8a570 sppsvc.exe         3824    480 0x000000001b654000 2019-07-24 07:02:32 UTC+0000
0x000000003da9d060 WmiApSrv.exe       3144    480 0x00000000226b1000 2019-07-24 07:02:55 UTC+0000
0x000000003dc39b30 SearchProtocol     2360   2880 0x0000000032347000 2019-07-24 07:03:53 UTC+0000
0x000000003de11b30 taskhost.exe       2340    480 0x000000000630d000 2019-07-24 07:01:24 UTC+0000
0x000000003de41b30 dwm.exe            2492    848 0x0000000037aa6000 2019-07-24 07:01:25 UTC+0000
0x000000003de6a630 explorer.exe       2516   2480 0x000000003763f000 2019-07-24 07:01:25 UTC+0000
0x000000003dee3820 vmtoolsd.exe       2604   2516 0x0000000032176000 2019-07-24 07:01:26 UTC+0000
0x000000003df1e250 FTK Imager.exe     1372   2516 0x000000003a1d0000 2019-07-24 07:04:27 UTC+0000
0x000000003dfa55e0 chrome.exe         2988   2516 0x0000000013746000 2019-07-24 07:01:33 UTC+0000   2019-07-24 07:03:34 UTC+0000
0x000000003dfc0b30 VeraCrypt.exe       580   2516 0x0000000007648000 2019-07-24 07:03:35 UTC+0000
0x000000003dfc3700 SearchFilterHo     3760   2880 0x0000000030392000 2019-07-24 07:03:53 UTC+0000
0x000000003e027b30 WmiPrvSE.exe       1856    640 0x000000000d751000 2019-07-24 07:00:32 UTC+0000
0x000000003e03ab30 msdtc.exe          2024    480 0x000000000c4f9000 2019-07-24 07:00:32 UTC+0000
0x000000003e04db30 VSSVC.exe          1864    480 0x000000000b33f000 2019-07-24 07:00:33 UTC+0000   2019-07-24 07:03:34 UTC+0000
```

Noticed VeraCrypt.exe, which is a disk encryption software. Went to look through the beginner tutorial, which mentioned about encryption and hash algorithm, which reminds me of the web history which Cloud searched about, AES and SHA-512. The tutorial also mentioned the possibility to set an exact volume size. This reminds me of the size of "Hidden Box" which is 5*1024*1024 bytes. "Hidden Box" is very likely an encrypted VeraCrypt volume. Now I have to look for the password.

Tried reading the keyboard buffer using Volatility in the memory dump.

Volatility_2.6_win64_standalone –profile=Win7SP0x64 bioskbd –f mem.mem

Nothing from there.

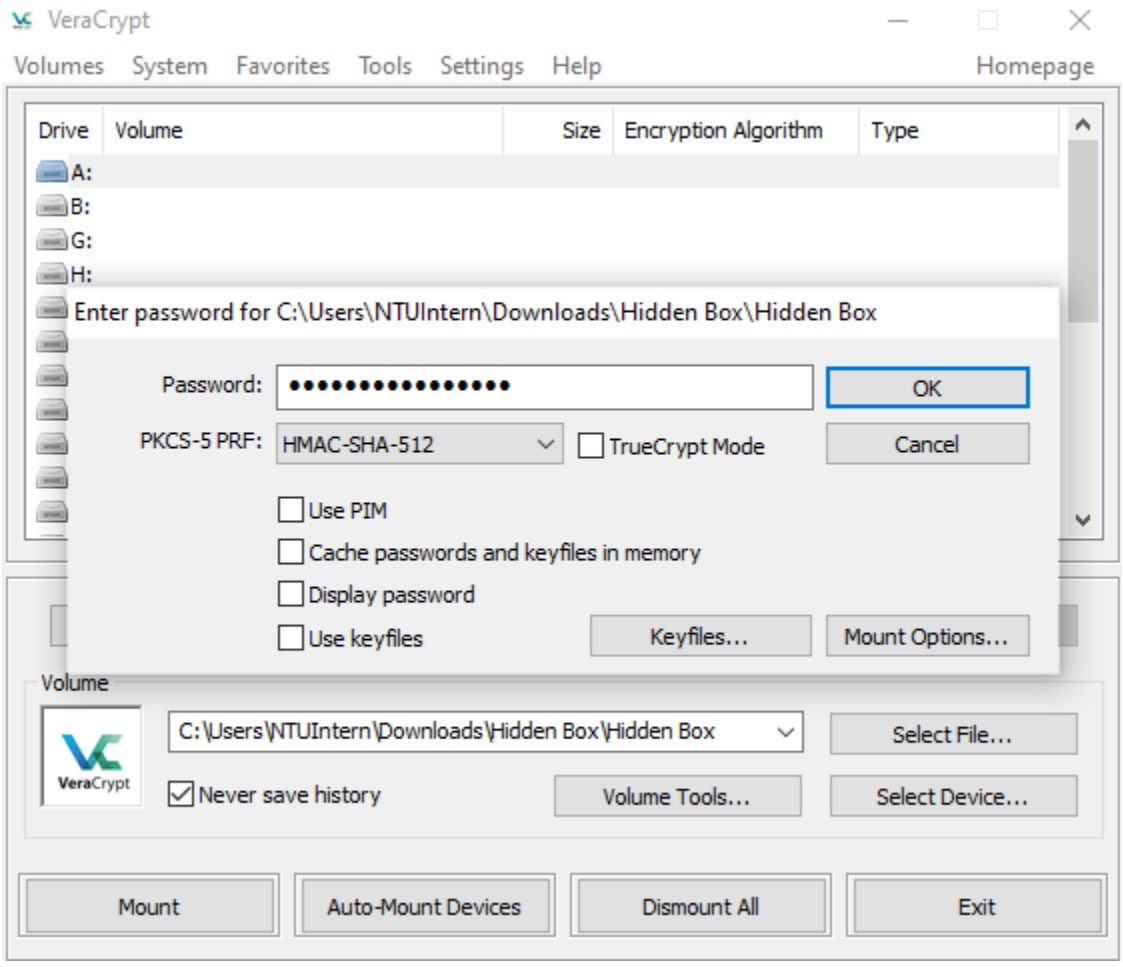
Remembering the hint mentioning that the box can be opened in a short period of time, he probably copied and paste his password from somewhere. Tried reading the clipboard.

Volatility_2.6_win64_standalone –profile=Win7SP0x64 clipboard –f mem.mem

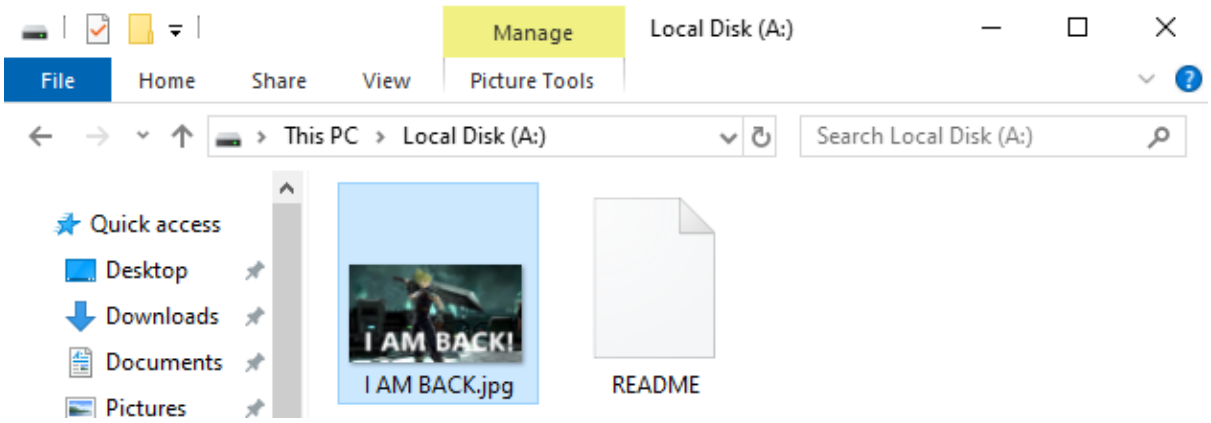
```
C:\Users\NTUIntern\Downloads\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone --profile=Win7SP
0x64 clipboard -f mem.mem
Volatility Foundation Volatility Framework 2.6
Session    WindowStation Format                        Handle Object             Data
---------- ------------- ------------------ ---------------- ------------------ ----------------------------------------------------
         1 WinSta0       0xc009L                     0x601af 0xfffff900c061c660
         1 WinSta0       CF_TEXT              0x5700790000c0b2 ------------------
         1 WinSta0       0x0L                   0x200000000000 ------------------
         1 WinSta0       CF_UNICODETEXT               0x1d0221 0xfffff900c06b1120 T!faL0ckhar71997
         1 WinSta0       CF_TEXT                       0xc013 ------------------
         1 WinSta0       0xa0125L             0x200000000001 ------------------
         1 WinSta0       CF_LOCALE                   0x200157 0xfffff900c063e5a0
         1 ------------- ------------------           0xa0125 0xfffff900c3a987e0
```

I found the password! T!faL0ckhar71997

Using the knowledge that Cloud used SHA-512 as the hash from Chrome history..



I opened the Hidden Box and obtained the photo flag.


Manage
Local Disk (A:)
File
Home
Share
View
Picture Tools
This PC
Local Disk (A:)
Search Local Disk (A:)
Quick access
Desktop
Downloads
Documents
Pictures
I AM BACK!
I AM BACK.jpg
README