SuSeC Cyber Security Contest

Forensics : Little

Description : A little boy is playing around in his grandfather's attic, where he finds a magical box. Help him discover what is in the box.
ATTENTION: The flag that you are going to capture for this task does not contain the word "SUSEC{", but you have to add this word to the beginning of the discovered flag before submitting it.

Attachment : little.img.txz

Solutions :

First we need to download the attachment file and extract it content. Once extracted we got an “**img**” file named “**little.img**”.

We can see it file type with “**file**” command.

```
kali@kali:~$ file little.img
little.img: DOS/MBR boot sector, code offset 0x3c+2, OEM-ID "mkfs.fat", sectors/cluster 4, reserved sectors 2048, root entries 512, sectors 8192 (volumes <=32 MB), Media descriptor 0xf8, sectors/FAT 5, sectors/track 32, heads 64, serial number 0xe318769f, unlabeled, FAT (12 bit)
```

Using “**strings**” we can deduce our flag is separate in three files.

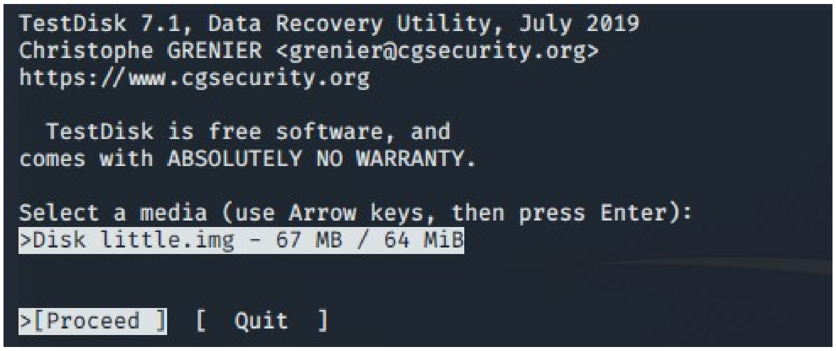
```
kali@kali:~$ strings little.img | grep "firstf"
196424  firstf.ogg
kali@kali:~$ strings little.img | grep "secondf"
secondf.png
kali@kali:~$ strings little.img | grep "thirdf"
thirdf.mp4
thirdf.mp4
```

Our goal is to extract those three files from the “**img**” file.

Running “**testdisk**” utility against the file for see if we can retrieve some files. First run the tools.

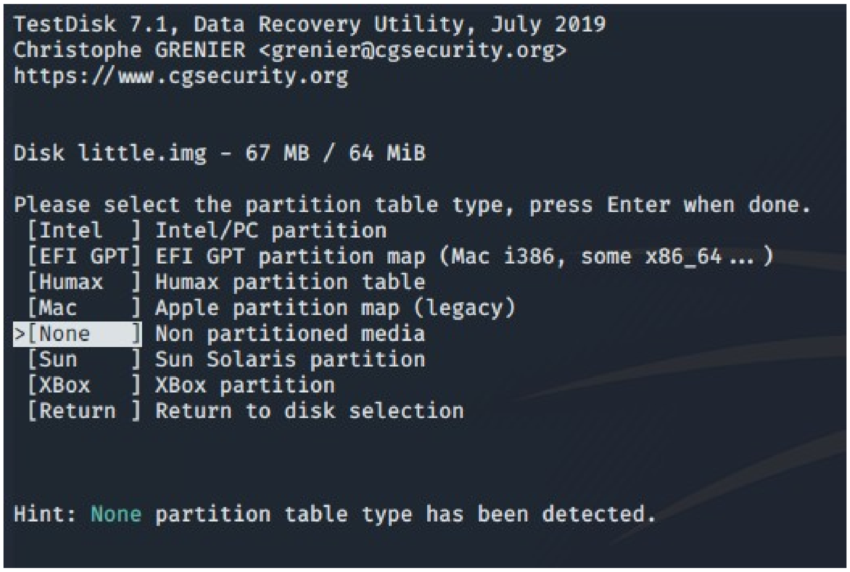
```
kali@kali:~$ sudo testdisk little.img
```

Choose the disk and press on “**Proceed**”.



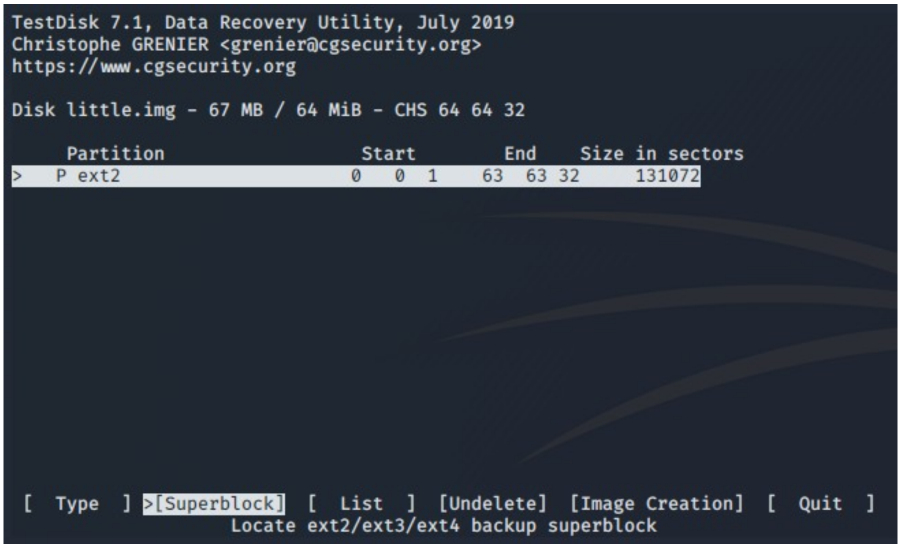
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

  TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk little.img - 67 MB / 64 MiB


>[Proceed ]  [  Quit  ]
```

As said the hint, choose the “**None**” partition table.



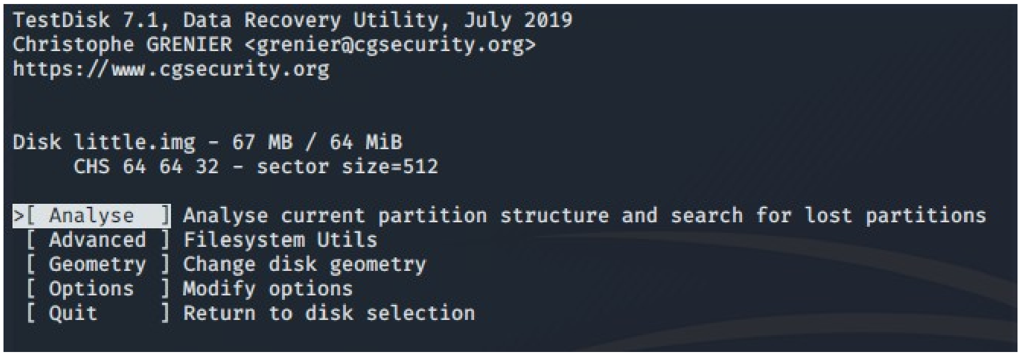
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk little.img - 67 MB / 64 MiB

Please select the partition table type, press Enter when done.
 [Intel  ] Intel/PC partition
 [EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
 [Humax  ] Humax partition table
 [Mac    ] Apple partition map (legacy)
>[None   ] Non partitioned media
 [Sun    ] Sun Solaris partition
 [XBox   ] XBox partition
 [Return ] Return to disk selection



Hint: None partition table type has been detected.
```

On this page, press “**Q**” for quit.



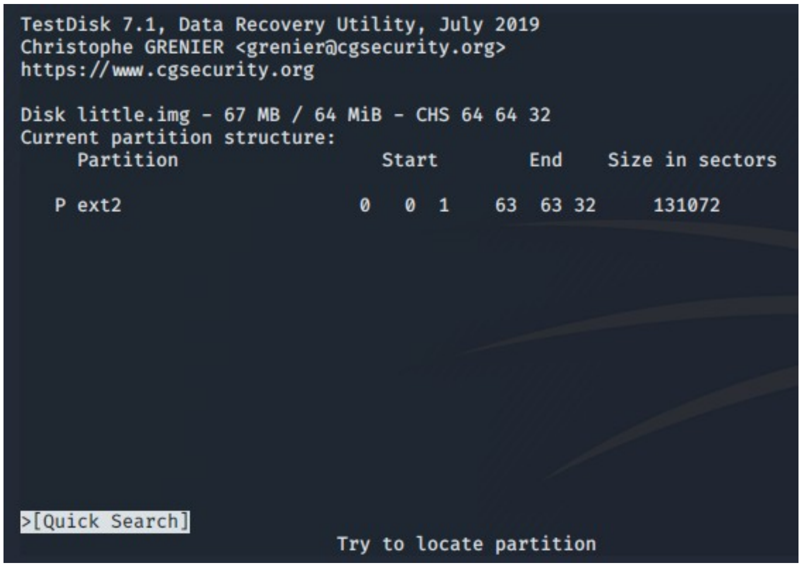
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk little.img - 67 MB / 64 MiB - CHS 64 64 32

     Partition                  Start        End    Size in sectors
>    P ext2                     0   0  1    63  63 32      131072


 [  Type  ] >[Superblock]  [  List  ]  [Undelete]  [Image Creation]  [  Quit  ]
                    Locate ext2/ext3/ext4 backup superblock
```

Choose “**Analyse**”, for analyse the partition structure.



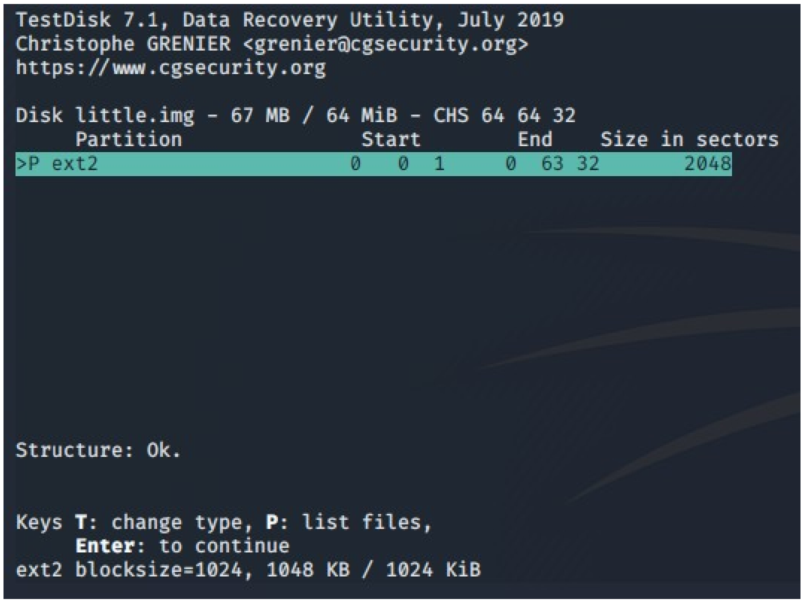
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk little.img - 67 MB / 64 MiB
     CHS 64 64 32 - sector size=512

>[ Analyse  ] Analyse current partition structure and search for lost partitions
 [ Advanced ] Filesystem Utils
 [ Geometry ] Change disk geometry
 [ Options  ] Modify options
 [ Quit     ] Return to disk selection
```

Then “**Quick Search**”.



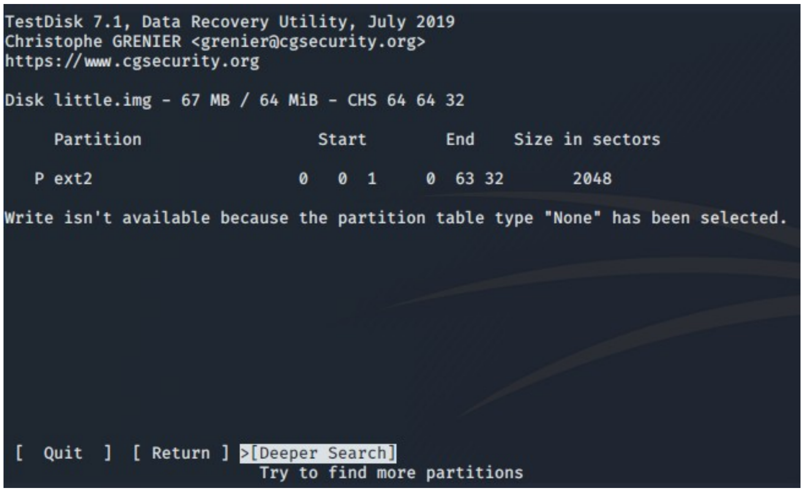
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk little.img - 67 MB / 64 MiB - CHS 64 64 32
Current partition structure:
     Partition                  Start        End    Size in sectors

   P ext2                     0   0  1    63  63 32     131072










>[Quick Search]
                            Try to locate partition
```

We found one partition. On this page press “**Q**” for quit.



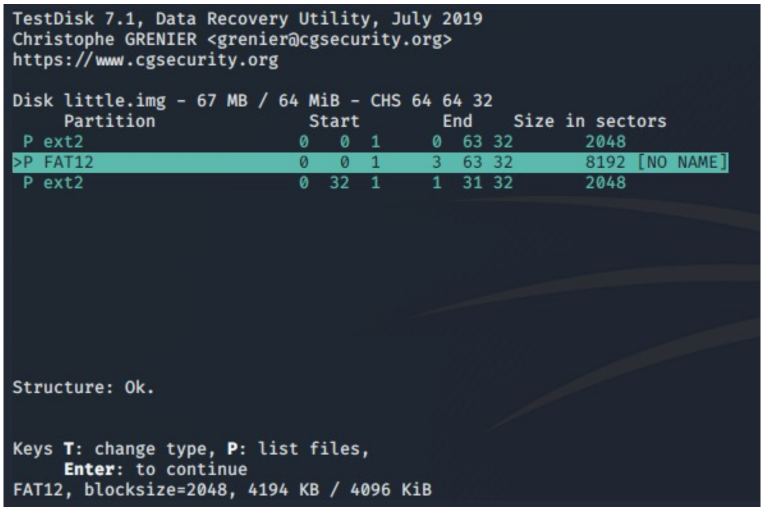
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk little.img - 67 MB / 64 MiB - CHS 64 64 32
     Partition                  Start        End    Size in sectors
>P ext2                       0   0  1     0  63 32          2048












Structure: Ok.


Keys T: change type, P: list files,
     Enter: to continue
ext2 blocksize=1024, 1048 KB / 1024 KiB
```

Choose “**Deep Search**”.



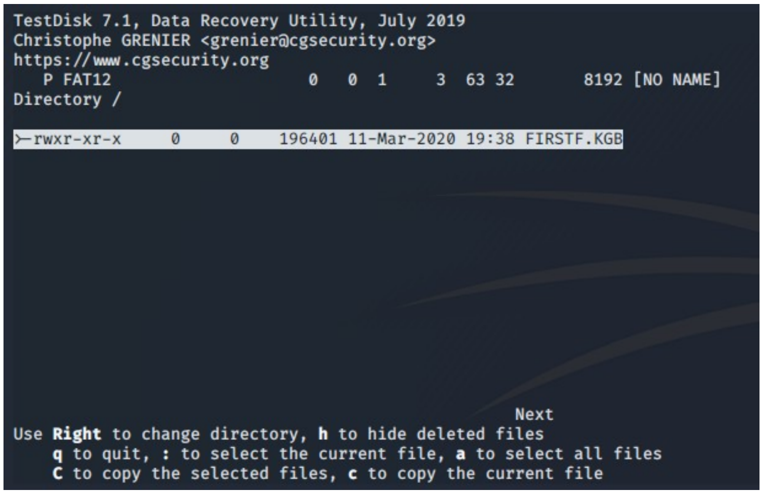
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk little.img - 67 MB / 64 MiB - CHS 64 64 32

     Partition                  Start        End    Size in sectors

   P ext2                     0   0  1     0  63 32       2048

Write isn't available because the partition table type "None" has been selected.







 [  Quit  ]  [ Return ] >[Deeper Search]
                          Try to find more partitions
```

Now we find three partitions.



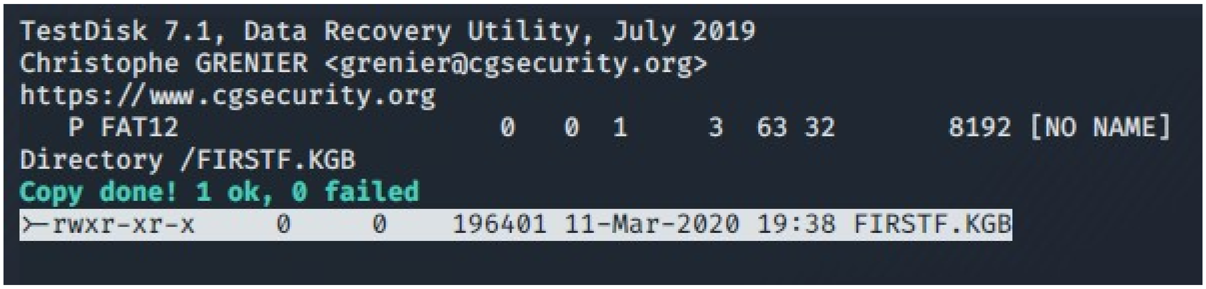
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk little.img - 67 MB / 64 MiB - CHS 64 64 32
     Partition                  Start        End    Size in sectors
 P ext2                       0   0  1     0  63 32       2048
>P FAT12                      0   0  1     3  63 32       8192 [NO NAME]
 P ext2                       0  32  1     1  31 32       2048










Structure: Ok.


Keys T: change type, P: list files,
     Enter: to continue
FAT12, blocksize=2048, 4194 KB / 4096 KiB
```

The third “**ext2**” is broken. The first “**ext2**” contain “**secondf.png**” and the “**FAT12**” partition contain “**FIRSTF.KGB**”. Choose the “**FAT12**” partition and press “**P**” for list files.



```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
   P FAT12                      0   0  1     3  63 32       8192 [NO NAME]
Directory /

>-rwxr-xr-x     0     0    196401 11-Mar-2020 19:38 FIRSTF.KGB















                                                   Next
Use Right to change directory, h to hide deleted files
    q to quit, : to select the current file, a to select all files
    C to copy the selected files, c to copy the current file
```

Now press on “**C/c**” chose the directory location where copy the file, and press “**C/c**” again.



```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
   P FAT12                    0   0  1     3  63 32       8192 [NO NAME]
Directory /FIRSTF.KGB
Copy done! 1 ok, 0 failed
>-rwxr-xr-x     0      0    196401 11-Mar-2020 19:38 FIRSTF.KGB
```

You can now press “**Q**” and repeat the same operation for extract “**second.png**” from the first “**ext2**” partition. But having trouble doing it, there is another way to do it, using “**binwalk**” we will see it later.

Now as we have our “**FIRSTF.KGB**” I looked on google what is this type of extension, and I see I can extract is content using “**kgb**” tool on linux.

First install the tools.

```
kali@kali:~$ sudo apt-get install kgb
```

Then extract the content of the “**kgb**” file.

```
kali@kali:~$ kgb FIRSTF.KGB
Extracting archive KGB_arch -3 FIRSTF.KGB ...
    191KB firstf.ogg: extracted
191KB -> 191KB w 0.51s. (99.99% czas: 386 KB/s)
```

As we can see we extracted an “**ogg**” audio file. Listen it and it give the first part of the flag.

First flag : c0me_wi4h_f4t_m4n_

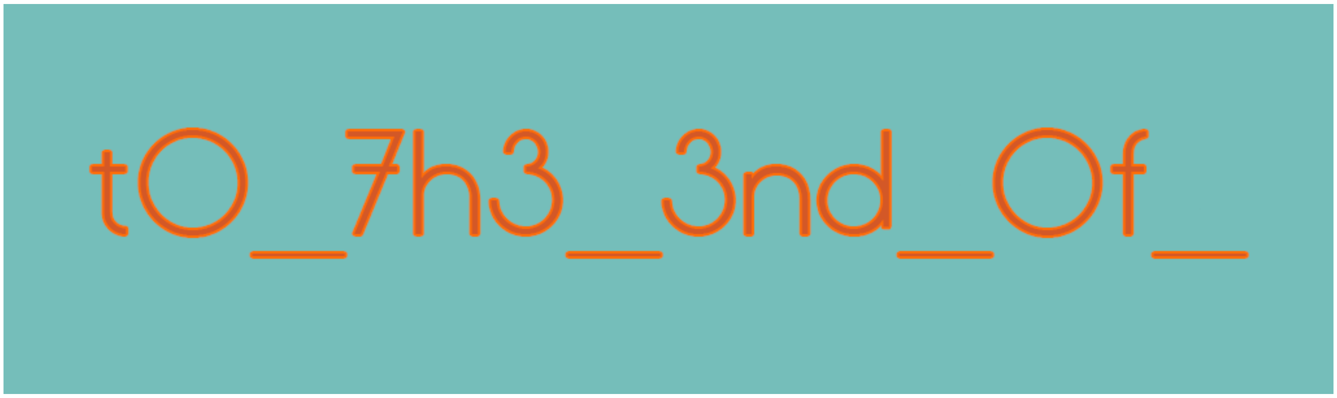
Now let’s get our second flag part. Using “**binwalk**” extract the content of “**little.img**”.

```
kali@kali:~$ binwalk -e little.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Linux EXT filesystem, blocks count: 1024, image size: 1048576, rev 1.0, ext2
filesystem data, UUID=e0676215-9cc7-abbd-f840-953aacffacff
1072128       0x105C00        KGB archive
66601544      0x3F84248       Unix path: /home/susec/your_searching_/name_is/littleBoy.img
66863688      0x3FC4248       Unix path: /home/susec/your_searching_/name_is/littleBoy.img
```

Going to the extracted directory and we can find the second flag part.

```
kali@kali:~/_little.img.extracted/ext-root$ ls -la
total 28
drwxr-xr-x 2 kali kali  4096 Mar 16 15:13 .
drwxr-xr-x 3 kali kali  4096 Mar 16 15:13 ..
-rw-r--r-- 1 kali kali 20133 Mar 16 15:13 secondf.png
```

Open the picture and you can see the Second flag part.



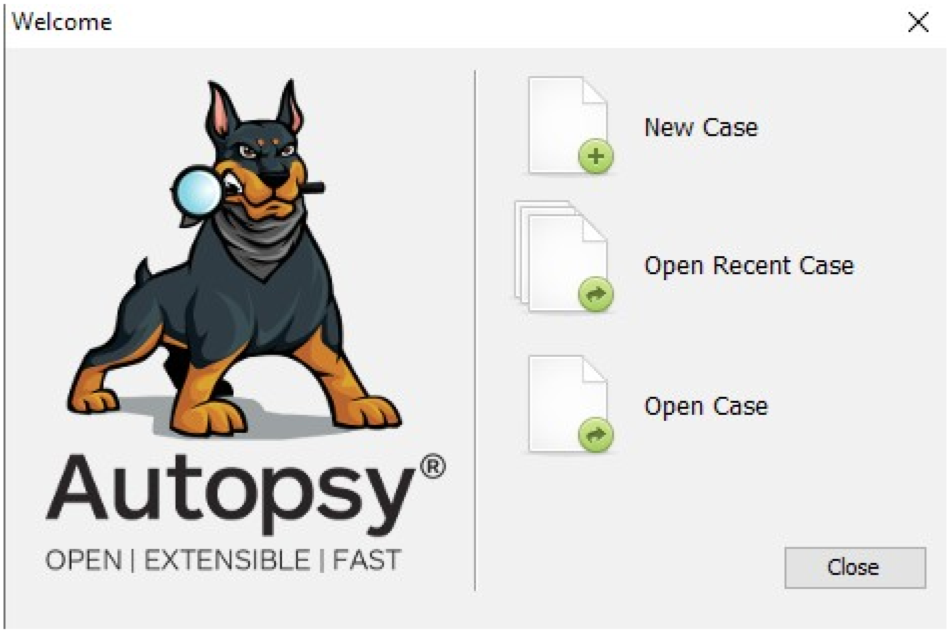
t0_7h3_3nd_0f_

Second Flag : t0_7h3_3nd_0f_

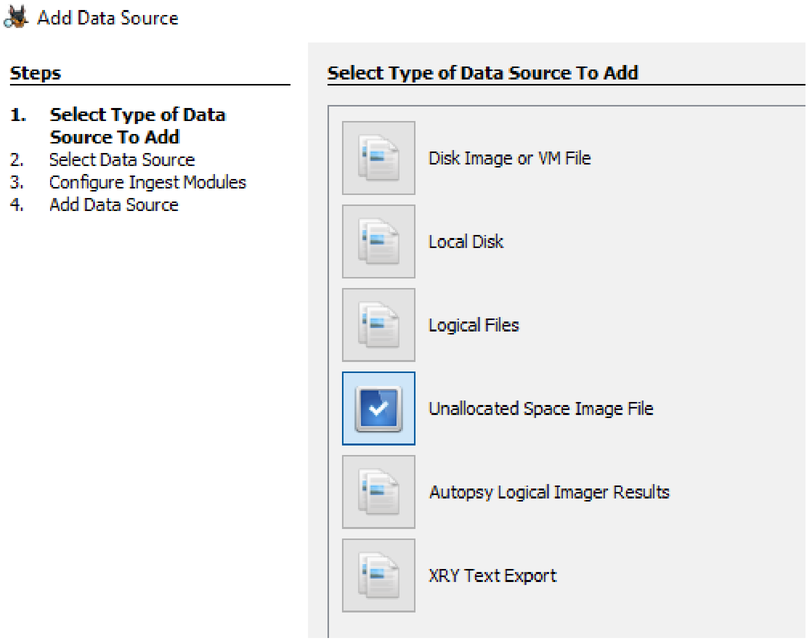
Now we need to find the last part of the flag, “**thirdf.mp4**”. To do it I used “**Autopsy**” tool version 4.14.0 for windows.

Source : https://www.autopsy.com/download/

Run the tool and create a new case.



Then add a new Data source and choose the type “**Unallocated Space Image File**”. Then load your “**little.img”** file.



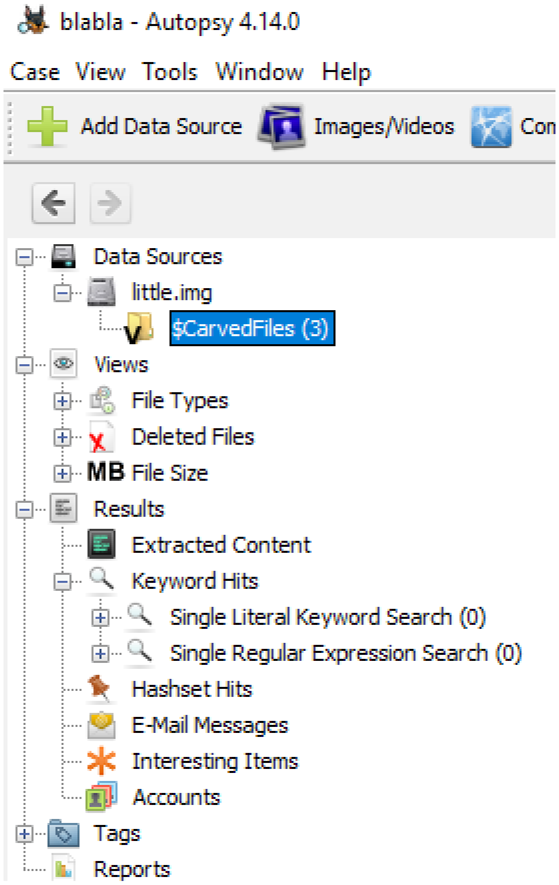
Add Data Source

Steps

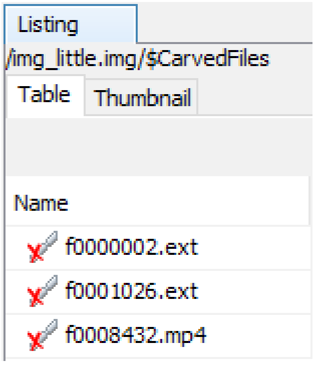
1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

Once the file loaded, on the left panel inside “**Data sources > little.img**” select “**$CarvedFiles (3)**” folder.



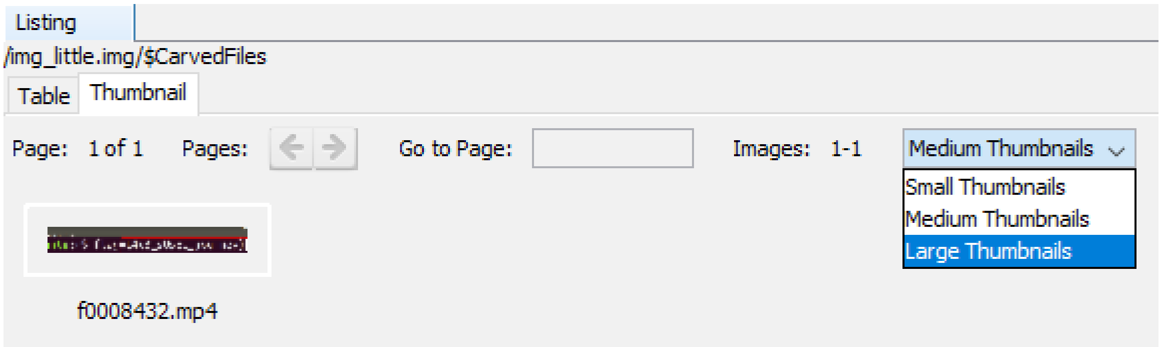
Then we can see on the listing panel on the right, into the “**Table**” tab, we can see our “**mp4**” file.



/img_little.img/$CarvedFiles

Name
f0000002.ext
f0001026.ext
f0008432.mp4

Maybe we can recover the file, I don’t know, personally I don’t try harded this step and going into the “**Thumbnail**” tab. Setting the images in “**Large Thumbnails**” mode.

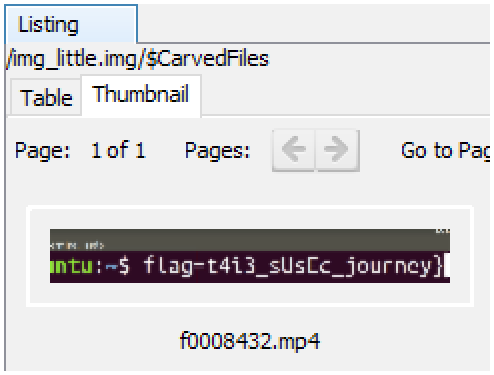


/img_little.img/$CarvedFiles

Page: 1 of 1 Pages: Go to Page: Images: 1-1 Medium Thumbnails

f0008432.mp4

Then we can see our third flag part.



/img_little.img/$CarvedFiles

Page: 1 of 1 Pages: Go to Pag

```
ntu:~$ flag-t4i3_sUsEc_journey}
```

f0008432.mp4

Third Flag : t4i3_sUsEc_journey}

Full Flag : SUSEC{c0me_wi4h_f4t_m4n_t0_7h3_3nd_0f_t4i3_sUsEc_journey}