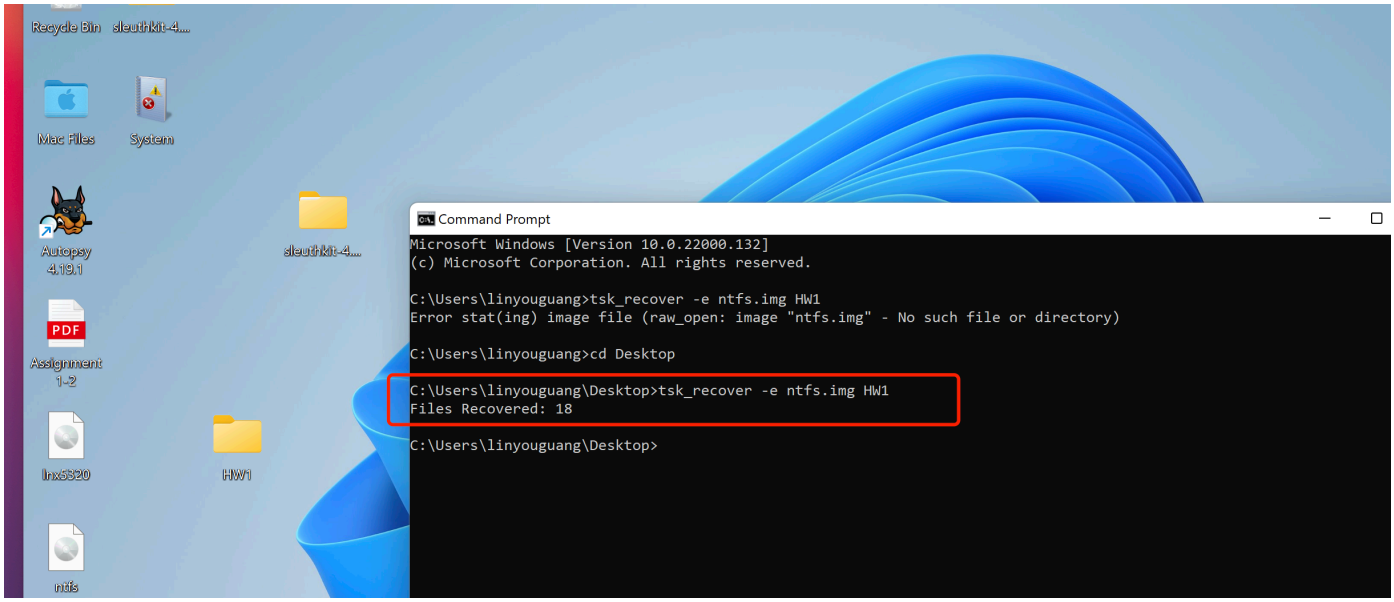
IERG5320, Fall 2021 Assignment1

- Name : Youguang Lin - Student ID : 1155169171

Q1.1

Firstly, I use command "tsk_recover -e ntfs.img HW1" to revocer the img files.

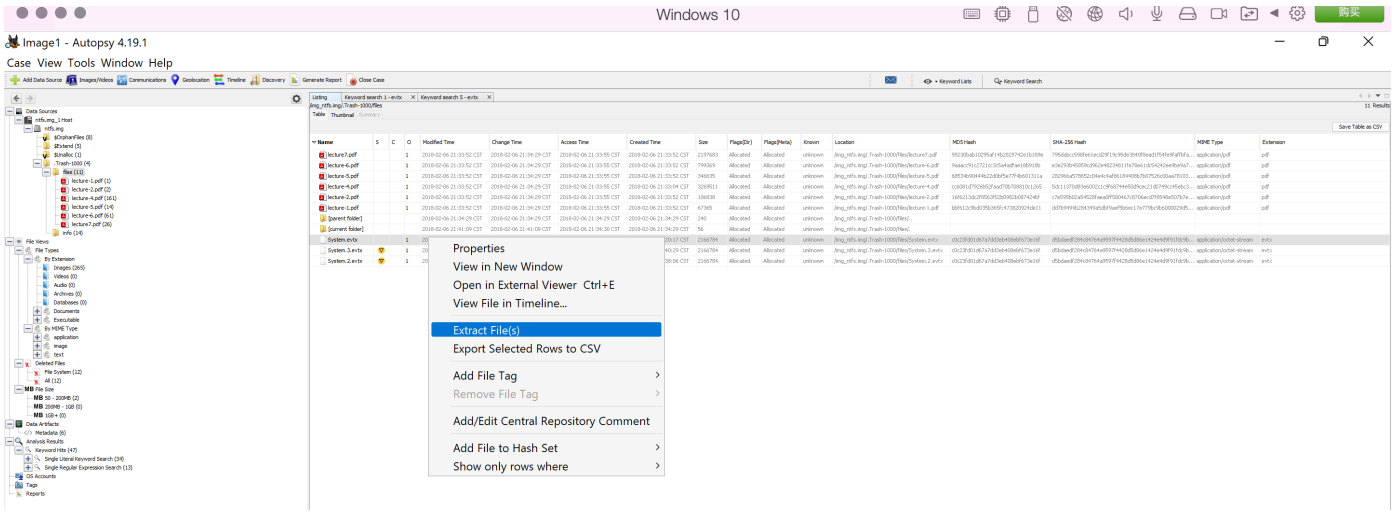


Then I use command "exiftool .\System.evtx" to check the Windows event log file with its meta information, which includes filename, file size and the last modified date and time.

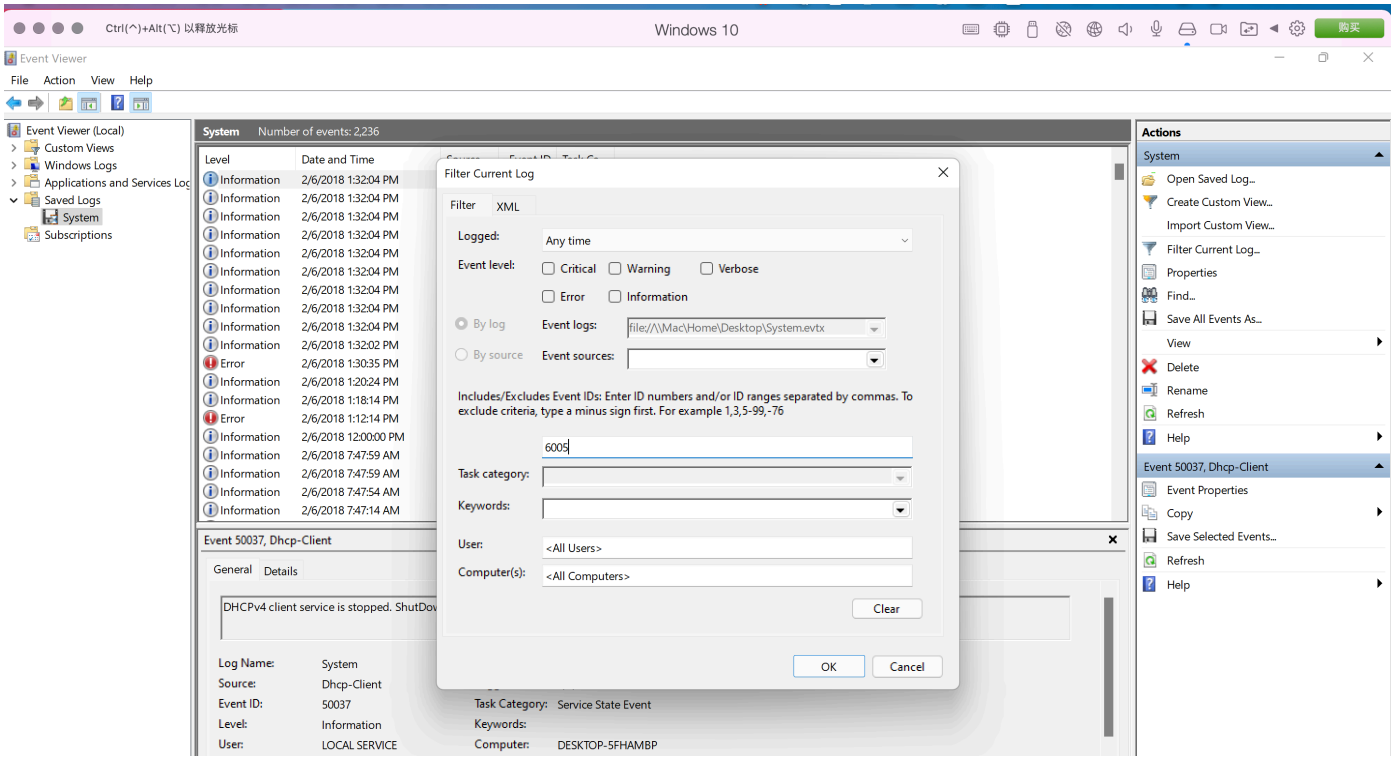
```
C:\Users\linyouguang\Desktop\HW1\.Trash-1000>cd files

C:\Users\linyouguang\Desktop\HW1\.Trash-1000\files>exiftool .\System.evtx
ExifTool Version Number         : 12.34
File Name                       : System.evtx
Directory                       : .
File Size                       : 2.1 MiB
File Modification Date/Time     : 2021:11:02 19:53:11+08:00
File Access Date/Time           : 2021:11:02 19:53:12+08:00
File Creation Date/Time         : 2021:11:02 19:53:11+08:00
File Permissions                : -rw-rw-rw-
Error                           : Unknown file type

C:\Users\linyouguang\Desktop\HW1\.Trash-1000\files>
```

Q1.2

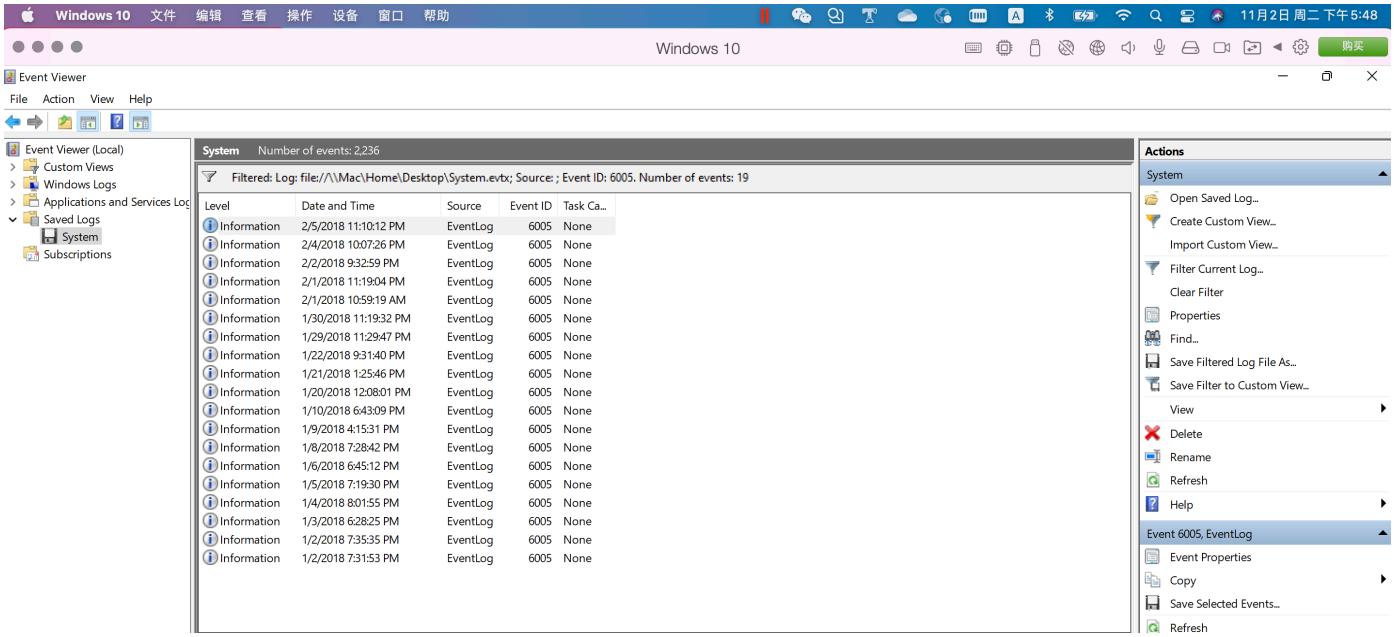
Then I use sluethkit tool to extract the system.ectx to my disk.



Then I open this file on Window and filter the log by their Id. 6005 is the ID when Windows starts.



Finally, you can see the result.

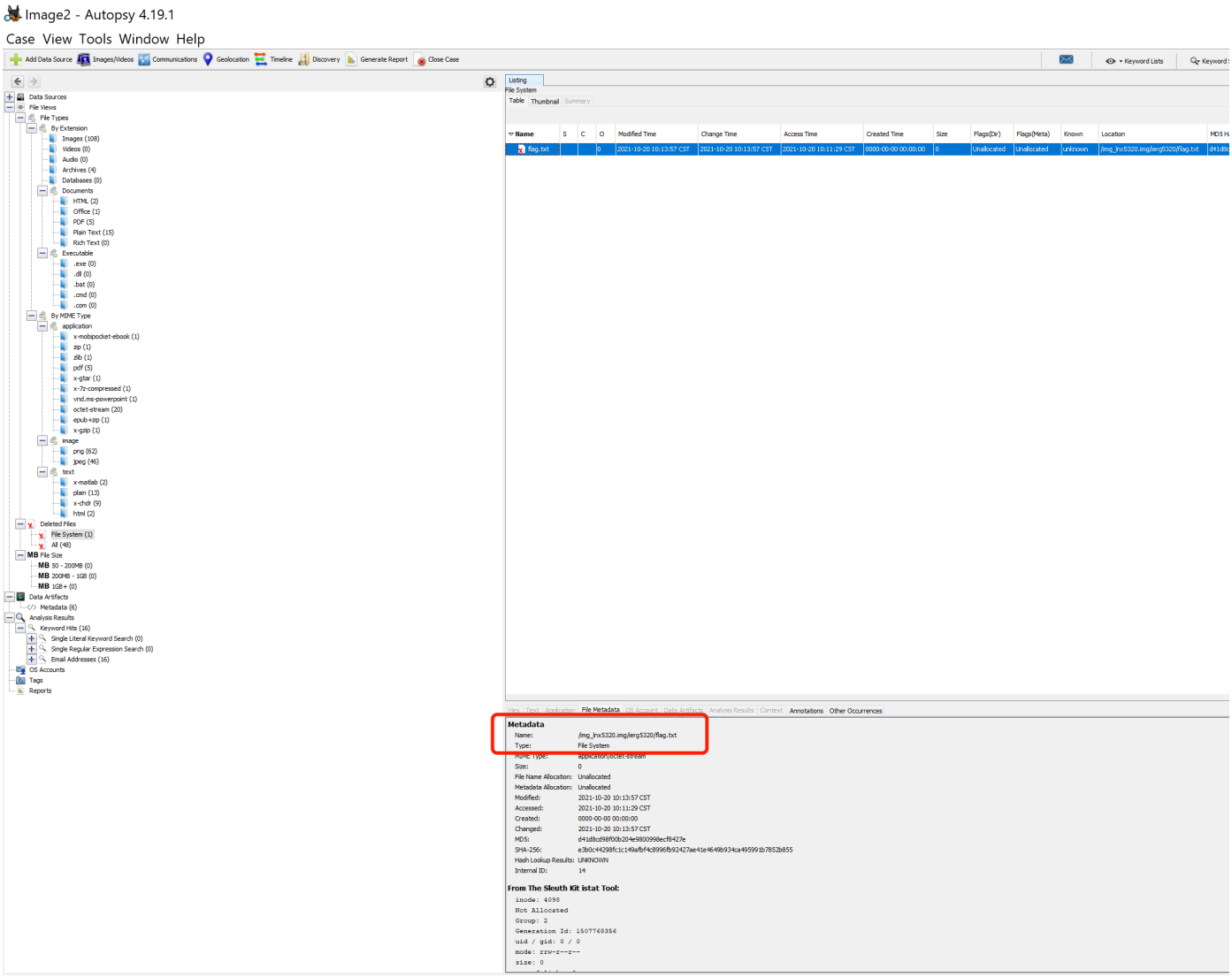


Question 2.1

First recover the delete file and get file name ---- ierg5320.

```
PS C:\Users\linyouguang\Desktop> tsk_recover -e .\lnx5320.img HW2
Files Recovered: 1
PS C:\Users\linyouguang\Desktop> cd HW2
PS C:\Users\linyouguang\Desktop\HW2> ls


    Directory: C:\Users\linyouguang\Desktop\HW2


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         11/3/2021   7:54 PM                ierg5320


PS C:\Users\linyouguang\Desktop\HW2>
```

We can also see the file name by using autopsy.



Question 2.2

See what really happens on an Ext3 file system.

```
PS C:\Users\linyouguang\Desktop> ils -r .\lnx5320.img
class|host|device|start_time
ils|unknown||1635926692
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
4098|f|0|0|1634696037|1634695889|1634696037|0|644|0|0
PS C:\Users\linyouguang\Desktop> istat .\lnx5320.img 4098
inode: 4098
Not Allocated
Group: 2
Generation Id: 1507768356
uid / gid: 0 / 0
mode: rrw-r--r--
size: 0
num of links: 0

Inode Times:
Accessed:       2021-10-20 10:11:29 (China Standard Time)
File Modified:  2021-10-20 10:13:57 (China Standard Time)
Inode Modified: 2021-10-20 10:13:57 (China Standard Time)
Deleted:        2021-10-20 10:13:57 (China Standard Time)

Direct Blocks:
PS C:\Users\linyouguang\Desktop>
```

Look the stats of block group 2:

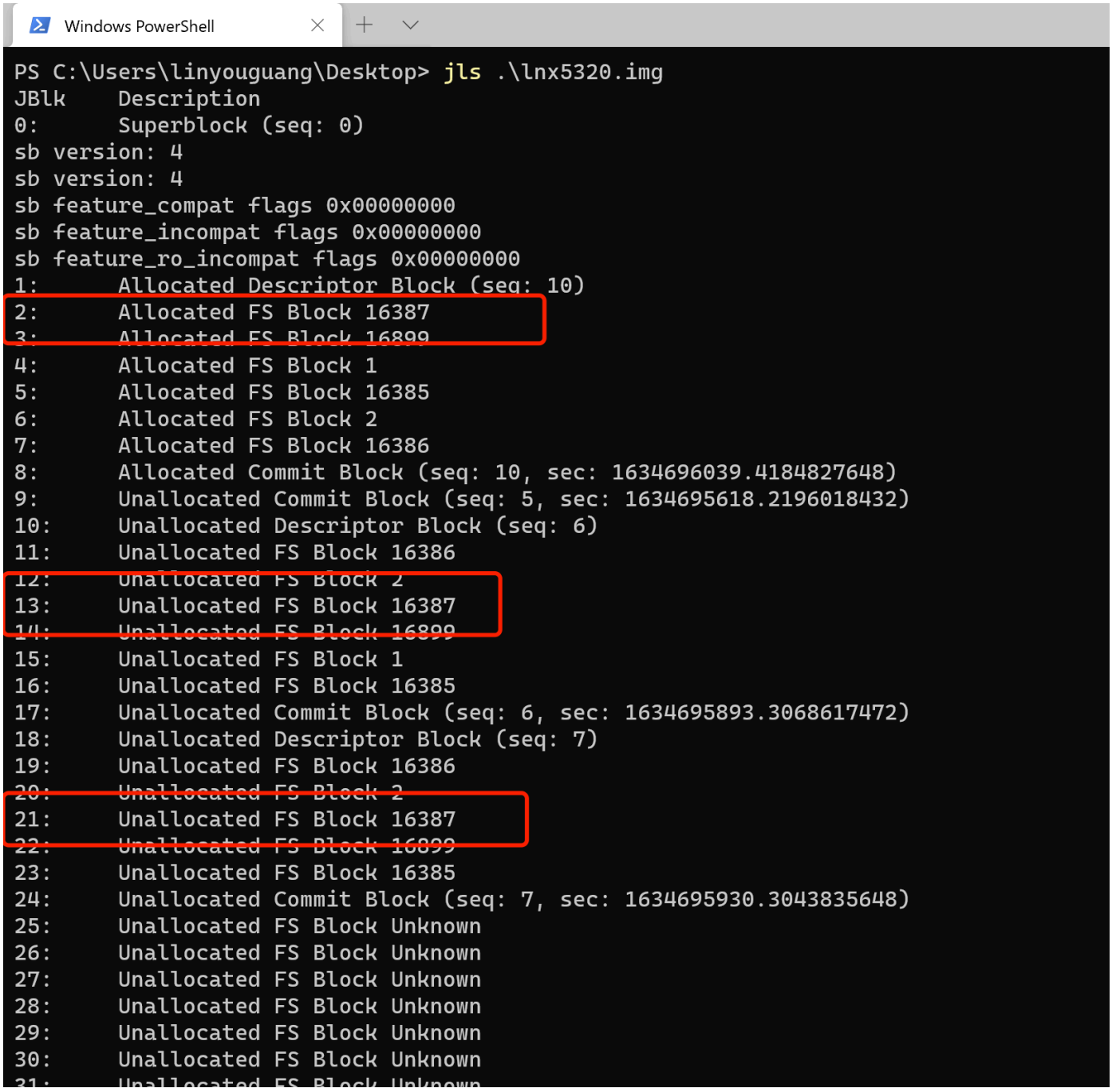
```
PS C:\Users\linyouguang\Desktop> fsstat .\lnx5320.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name: LNXExt3
Volume ID: b018e4395ef976b8ac426fb8cddcd373

Last Written at: 2021-10-20 10:13:49 (China Standard Time)
Last Checked at: 2021-10-20 09:58:28 (China Standard Time)

Last Mounted at: 2021-10-20 10:13:49 (China Standard Time)
Unmounted properly
Last mounted on: /mnt

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Needs Recovery,
Read Only Compat Features: Sparse Super, Large File,

Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 16385
Root Directory: 2
Free Inodes: 16370

CONTENT INFORMATION
--------------------------------------------
Block Range: 0 - 65535
Block Size: 1024
Reserved Blocks Before Block Groups: 1
Free Blocks: 56008

BLOCK GROUP INFORMATION
--------------------------------------------
Number of Block Groups: 8
```

Take a look closely to the information of group 2

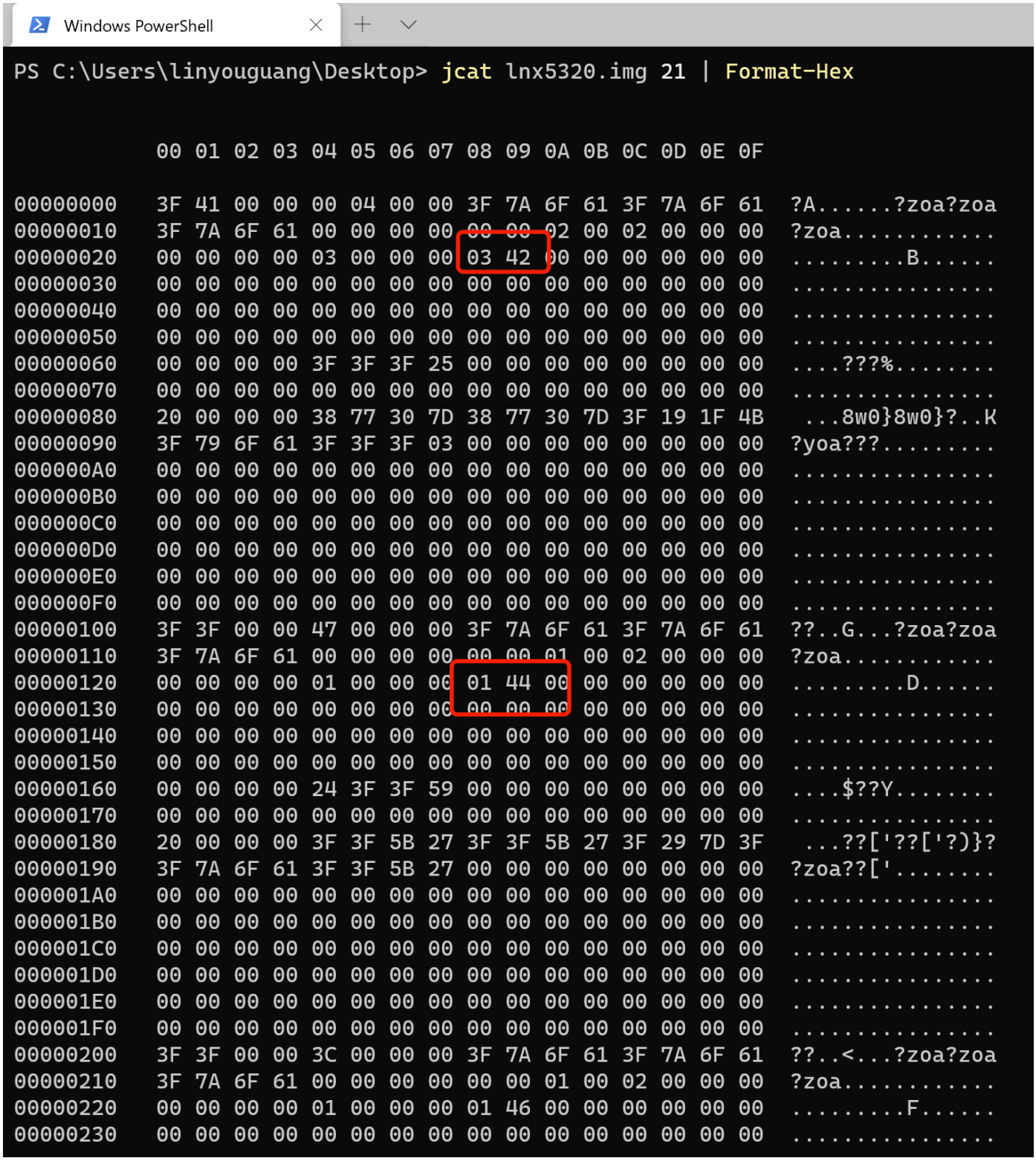
```
Group: 2:
  Inode Range: 4097 - 6144
  Block Range: 16385 - 24576
  Layout:
    Data bitmap: 16385 - 16385
    Inode bitmap: 16386 - 16386
    Inode Table: 16387 - 16898
    Data Blocks: 16387 - 16386, 16899 - 0
  Free Inodes: 2046 (0%)
  Free Blocks: 7676 (0%)
  Total Directories: 1
```

We can see that for this group there are 2048 nodes (Inode range: 4097 - 6144) and the inode table has a size of 512 blocks (Inode Table: 16387 - 16898). Each block of the inode table has 4 nodes (2048 diveded by 512), thus inode 4098 it's the 2nd entry in the table and its content is located in the first block of the inode table.

Checking the output from jls, we find out that there are serveral references to 16387(the first block of the inode table). The output shows that block 2 of the journal contains information regarding an operation on the inode table of group 2 and since the journal at least records copies of the metadata (default journal mode is ordered) that has been modified; we can look for a copy of inode 4098 within the journal. There are cases that checking each instance of a particular block in the journal must be analyzed, but in this case we just want to recover the earliest one.



We found there are three rows contain 16387, this is the start of the Inode Table of group 2. Because we want to recover the final one. The first entry, I think it is to create the file because it is the action of allocate. So the unallocated means delete. I use jcat to extract the copy of inode 4098. I use hex format.



According to the i-node data structure, I found three single indirect pointer。

In linux, it use Little Endian. For the first one, i can see the 0342, so it is 4203 in hex, i convert it into decimal is 16899 block. That is the 4097 inode. But I want to find 4098.

```
PS C:\Users\linyouguang\Desktop> istat .\lnx5320.img 4097
inode: 4097
Allocated
Group: 2
Generation Id: 635149009
uid / gid: 0 / 0
mode: drwxr-xr-x
size: 1024
num of links: 2

Inode Times:
Accessed:       2021-10-20 10:13:53 (China Standard Time)
File Modified:  2021-10-20 10:13:57 (China Standard Time)
Inode Modified: 2021-10-20 10:13:57 (China Standard Time)

Direct Blocks:
16899
PS C:\Users\linyouguang\Desktop>
```

Then the third one is 0146. It is the 4601 in hex and 17921 in decimal. Then, we check its block. It's the dummy.txt. It is not the inode I want to find.

```
C:\Users\linyouguang\Desktop>ffind -a lnx5320.img 4098
* /ierg5320/flag.txt

C:\Users\linyouguang\Desktop>fls -r lnx5320.img
d/d 11: lost+found
d/d 4097:       ierg5320
+ r/r * 4098:   flag.txt
+ r/r 4099:     dummy.txt
V/V 16385:      $OrphanFiles

C:\Users\linyouguang\Desktop>
```

```
PS C:\Users\linyouguang\Desktop> istat .\lnx5320.img 4099
inode: 4099
Allocated
Group: 2
Generation Id: 3056517178
uid / gid: 0 / 0
mode: rrw-r--r--
size: 60
num of links: 1

Inode Times:
Accessed:       2021-10-20 10:12:04 (China Standard Time)
File Modified:  2021-10-20 10:12:04 (China Standard Time)
Inode Modified: 2021-10-20 10:12:04 (China Standard Time)

Direct Blocks:
17921
PS C:\Users\linyouguang\Desktop>
```

Then is the seond one. It is 4401 in hex and 17409 in decimal. Then we use blkcat to see the content in this block. And I found it.

```
000003C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000003D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000003E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000003F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................



PS C:\Users\linyouguang\Desktop> blkcat .\lnx5320.img 17409
find me if you can, dear IERG5320 students. Token is 20211020 10:11:43
PS C:\Users\linyouguang\Desktop>
```

It is funny!

We can also get all the unallocate into a file and find the possible answer. I use blkls to get the unallocate data. And found the result in the blkls.


Inx5320.blkls - Notepad
File Edit Format View Help
find me if you can, dear IERG5320 students. Token is 20211020 10:11:43