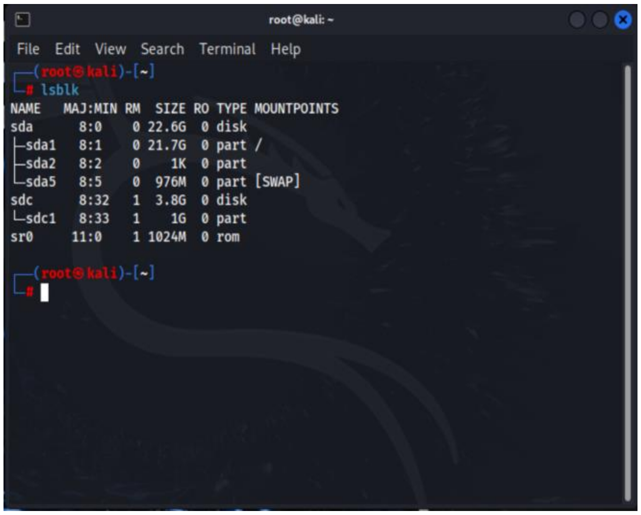
The Command Line Interface (CLI) is an editing environment that is text-based. It uses specified text (known as commands) to interact with the computer and perform numerous operations, including installing and working with programs. In Module2, we will be using **Terminal**, a CLI tool in Linux.

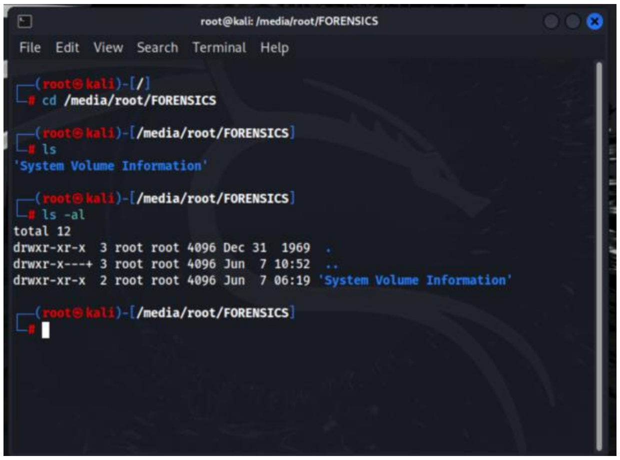
Why use Command Line Interface (CLI) over Graphical User Interface (GUI)?
When you first start working with CLI, the first question that pops up is why the ugly looking terminal, over the beautifully crafted GUI. The main reason is the CLI uses less RAM space and interacts with the operating system directly, which though ugly looking, makes it more powerful and faster than using GUI.

In Linux, one of the main tools for CLI is **Terminal**. In Windows, we have **Cmd** and **Powershell**. This instruction guide will go through basic commands that you will need to operate Terminal for the Module2. If you are interested, any online tutorials will teach you more.

Linux commands	**Functions**
• lsblk	To list information about all available or the specified block devices 
• ls • ls -al	Displays information about files in the current directory. ls -al gives us more information, including hidden files which start

```
┌──(root㉿kali)-[~]
└─# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 22.6G  0 disk
├─sda1   8:1    0 21.7G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0  976M  0 part [SWAP]
sdc      8:32   1  3.8G  0 disk
└─sdc1   8:33   1    1G  0 part
sr0     11:0    1 1024M  0 rom

┌──(root㉿kali)-[~]
└─# █
```

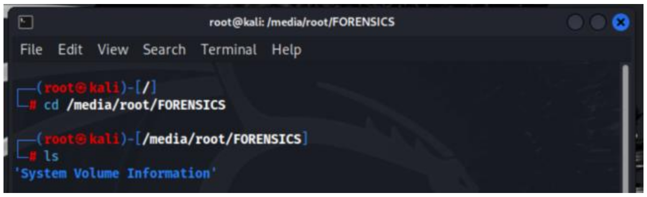
with a ‘.’



```
┌──(root㉿kali)-[/]
└─# cd /media/root/FORENSICS

┌──(root㉿kali)-[/media/root/FORENSICS]
└─# ls
'System Volume Information'

┌──(root㉿kali)-[/media/root/FORENSICS]
└─# ls -al
total 12
drwxr-xr-x  3 root root 4096 Dec 31  1969  .
drwxr-x---+ 3 root root 4096 Jun  7 10:52  ..
drwxr-xr-x  2 root root 4096 Jun  7 06:19 'System Volume Information'

┌──(root㉿kali)-[/media/root/FORENSICS]
└─# 
```

- cd

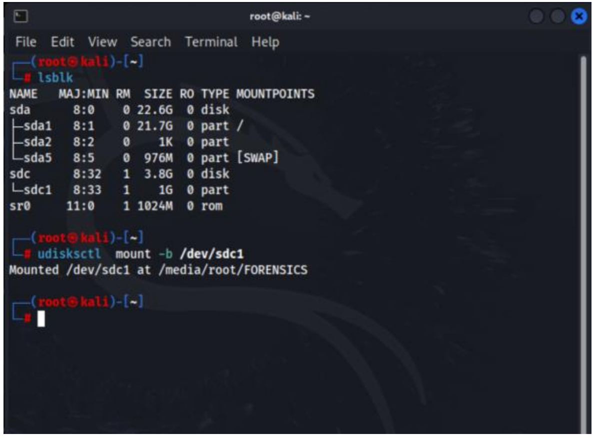
To navigate between different folders.



```
┌──(root㉿kali)-[/]
└─# cd /media/root/FORENSICS

┌──(root㉿kali)-[/media/root/FORENSICS]
└─# ls
'System Volume Information'
```

- udisksctl mount -b

To mount a disk (making it available for OS to use).

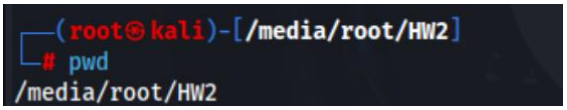


```
┌──(root㉿kali)-[~]
└─# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 22.6G  0 disk
├─sda1   8:1    0 21.7G  0 part /
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0  976M  0 part [SWAP]
sdc      8:32   1  3.8G  0 disk
└─sdc1   8:33   1    1G  0 part
sr0     11:0    1 1024M  0 rom

┌──(root㉿kali)-[~]
└─# udisksctl  mount -b /dev/sdc1
Mounted /dev/sdc1 at /media/root/FORENSICS

┌──(root㉿kali)-[~]
└─# 
```

- pwd

Stands for "print working directory." It outputs the full path of the current working directory. Displays the current working directory.

<table>
<tr>
<td></td>
<td>



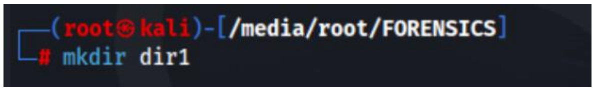
```
┌──(root㉿kali)-[/media/root/HW2]
└─# pwd
/media/root/HW2
```

</td>
</tr>
<tr>
<td>

- mkdir

</td>
<td>

Creates a directory (folder).



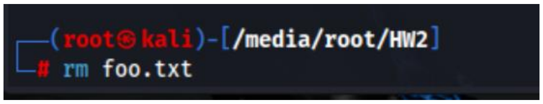
```
┌──(root㉿kali)-[/media/root/FORENSICS]
└─# mkdir dir1
```

</td>
</tr>
<tr>
<td>

- rm

</td>
<td>

Deletes files.



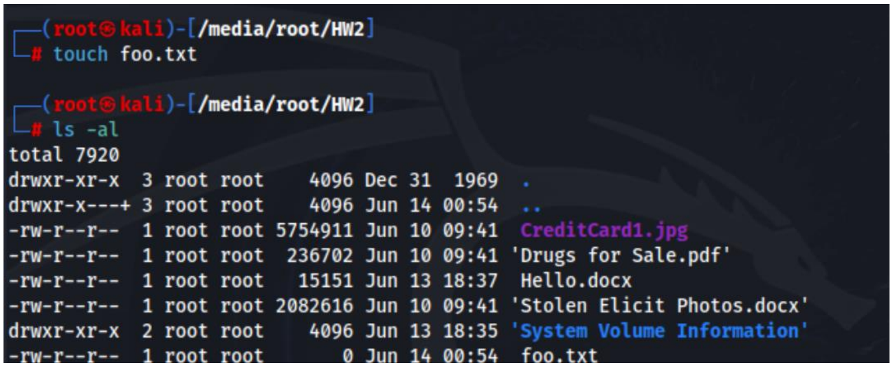
```
┌──(root㉿kali)-[/media/root/HW2]
└─# rm foo.txt
```

</td>
</tr>
<tr>
<td>

- touch

</td>
<td>

Create empty files.



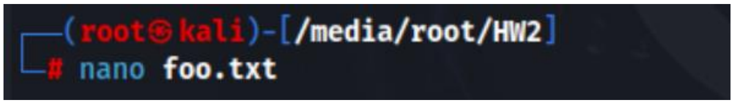
```
┌──(root㉿kali)-[/media/root/HW2]
└─# touch foo.txt

┌──(root㉿kali)-[/media/root/HW2]
└─# ls -al
total 7920
drwxr-xr-x  3 root root    4096 Dec 31  1969  .
drwxr-x---+ 3 root root    4096 Jun 14 00:54  ..
-rw-r--r--  1 root root 5754911 Jun 10 09:41  CreditCard1.jpg
-rw-r--r--  1 root root  236702 Jun 10 09:41 'Drugs for Sale.pdf'
-rw-r--r--  1 root root   15151 Jun 13 18:37  Hello.docx
-rw-r--r--  1 root root 2082616 Jun 10 09:41 'Stolen Elicit Photos.docx'
drwxr-xr-x  2 root root    4096 Jun 13 18:35 'System Volume Information'
-rw-r--r--  1 root root       0 Jun 14 00:54  foo.txt
```

</td>
</tr>
<tr>
<td>

- nano

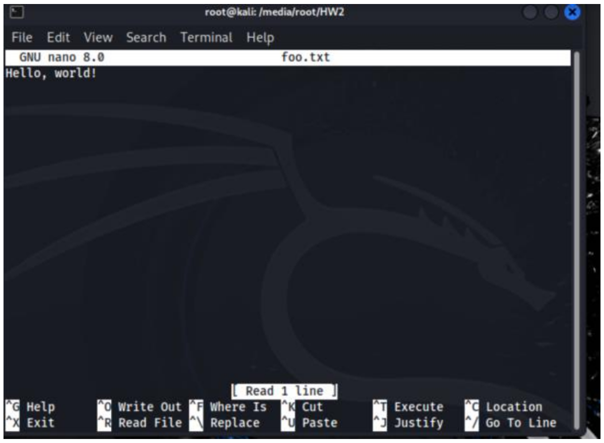
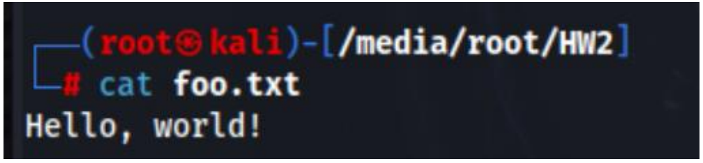
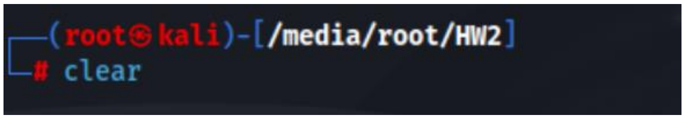
</td>
<td>

Text editor for files. Creates a new file if the filename doesn’t exist. Use Ctrl + X to close.



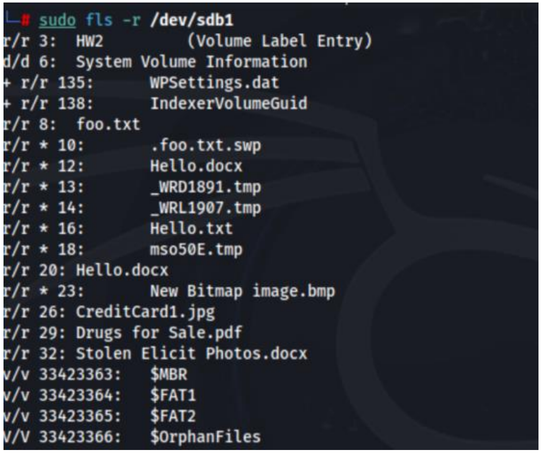
```
┌──(root㉿kali)-[/media/root/HW2]
└─# nano foo.txt
```

</td>
</tr>
</table>

	 root@kali: /media/root/HW2 File Edit View Search Terminal Help GNU nano 8.0 foo.txt Hello, world! [Read 1 line] ^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line
- cat	Display file contents on terminal.  ┌──(root㉿kali)-[/media/root/HW2] └─# cat foo.txt Hello, world!
- clear	Clear terminal.  ┌──(root㉿kali)-[/media/root/HW2] └─# clear
- sudo	sudo stands for "superuser do" and is commonly used to perform tasks that require administrative privileges.

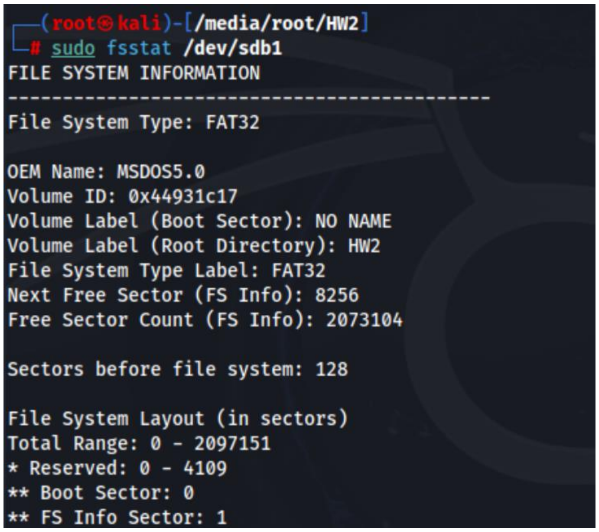
a. fls
b. fsstat
c. icat
d. istat

fls is a command-line tool from The Sleuth Kit (TSK), used for listing files and directories in an image file or device



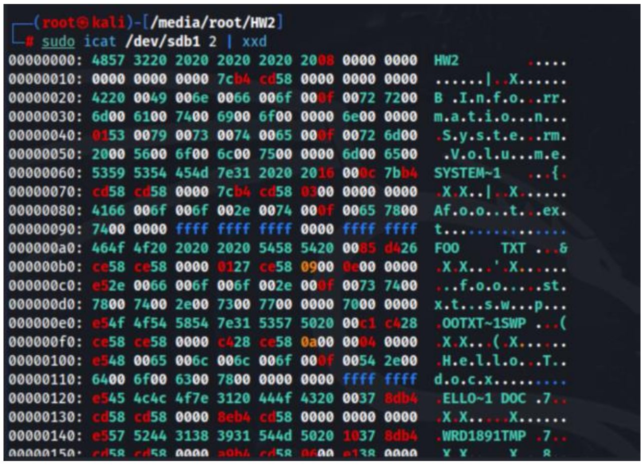
```
└─# sudo fls -r /dev/sdb1
r/r 3:  HW2         (Volume Label Entry)
d/d 6:  System Volume Information
+ r/r 135:      WPSettings.dat
+ r/r 138:      IndexerVolumeGuid
r/r 8:  foo.txt
r/r * 10:       .foo.txt.swp
r/r * 12:       Hello.docx
r/r * 13:       _WRD1891.tmp
r/r * 14:       _WRL1907.tmp
r/r * 16:       Hello.txt
r/r * 18:       mso50E.tmp
r/r 20: Hello.docx
r/r * 23:       New Bitmap image.bmp
r/r 26: CreditCard1.jpg
r/r 29: Drugs for Sale.pdf
r/r 32: Stolen Elicit Photos.docx
v/v 33423363:   $MBR
v/v 33423364:   $FAT1
v/v 33423365:   $FAT2
V/V 33423366:   $OrphanFiles
```

fsstat is another tool from The Sleuth Kit that provides detailed information about a file system in an image or device. It displays metadata and statistical information about the file system.



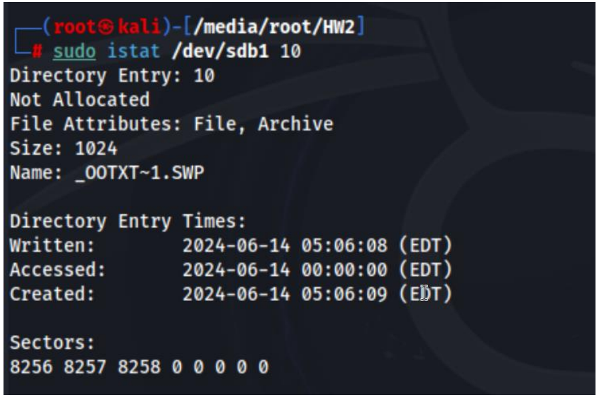
```
┌──(root㉿kali)-[/media/root/HW2]
└─# sudo fsstat /dev/sdb1
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x44931c17
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): HW2
File System Type Label: FAT32
Next Free Sector (FS Info): 8256
Free Sector Count (FS Info): 2073104

Sectors before file system: 128

File System Layout (in sectors)
Total Range: 0 - 2097151
* Reserved: 0 - 4109
** Boot Sector: 0
** FS Info Sector: 1
```

icat is used to recover files or data blocks from an image.



```
┌──(root㉿kali)-[/media/root/HW2]
└─# sudo icat /dev/sdb1 2 | xxd
00000000: 4857 3220 2020 2020 2020 2008 0000 0000  HW2        .....
00000010: 0000 0000 0000 7cb4 cd58 0000 0000 0000  ......|..X......
00000020: 4220 0049 006e 0066 006f 000f 0072 7200  B .I.n.f.o...rr.
00000030: 6d00 6100 7400 6900 6f00 0000 6e00 0000  m.a.t.i.o...n...
00000040: 0153 0079 0073 0074 0065 000f 0072 6d00  .S.y.s.t.e...rm.
00000050: 2000 5600 6f00 6c00 7500 0000 6d00 6500   .V.o.l.u...m.e.
00000060: 5359 5354 454d 7e31 2020 2016 000c 7bb4  SYSTEM~1    ...{.
00000070: cd58 cd58 0000 7cb4 cd58 0300 0000 0000  .X.X..|..X......
00000080: 4166 006f 006f 002e 0074 000f 0065 7800  Af.o.o...t...ex.
00000090: 7400 0000 ffff ffff ffff 0000 ffff ffff  t...............
000000a0: 464f 4f20 2020 2020 5458 5420 0085 d426  FOO     TXT ...&
000000b0: ce58 ce58 0000 0127 ce58 0900 0e00 0000  .X.X...'.X......
000000c0: e52e 0066 006f 006f 002e 000f 0073 7400  ...f.o.o.....st.
000000d0: 7800 7400 2e00 7300 7700 0000 7000 0000  x.t...s.w...p...
000000e0: e54f 4f54 5854 7e31 5357 5020 00c1 c428  .OOTXT~1SWP ...(
000000f0: ce58 ce58 0000 c428 ce58 0a00 0004 0000  .X.X...(.X......
00000100: e548 0065 006c 006c 006f 000f 0054 2e00  .H.e.l.l.o...T..
00000110: 6400 6f00 6300 7800 0000 0000 ffff ffff  d.o.c.x.........
00000120: e545 4c4c 4f7e 3120 444f 4320 0037 8db4  .ELLO~1 DOC .7..
00000130: cd58 cd58 0000 8eb4 cd58 0000 0000 0000  .X.X.....X......
00000140: e557 5244 3138 3931 544d 5020 1037 8db4  .WRD1891TMP .7..
00000150: cd58 cd58 0000 a9b4 cd58 0600 e138 0000  .X.X.....X...8..
```

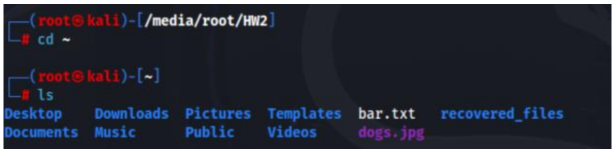
istat displays detailed information about an inode, such as its size, file type, and allocated blocks.



```
┌──(root㉿kali)-[/media/root/HW2]
└─# sudo istat /dev/sdb1 10
Directory Entry: 10
Not Allocated
File Attributes: File, Archive
Size: 1024
Name: _OOTXT~1.SWP

Directory Entry Times:
Written:        2024-06-14 05:06:08 (EDT)
Accessed:       2024-06-14 00:00:00 (EDT)
Created:        2024-06-14 05:06:09 (EDT)

Sectors:
8256 8257 8258 0 0 0 0 0
```

- ~/

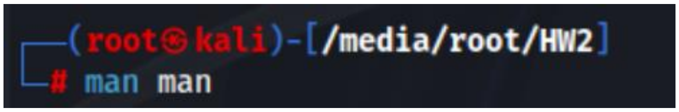
Shortcut to reach home directory of the File System.



```
┌──(root㉿kali)-[/media/root/HW2]
└─# cd ~

┌──(root㉿kali)-[~]
└─# ls
Desktop    Downloads  Pictures  Templates  bar.txt   recovered_files
Documents  Music      Public    Videos     dogs.jpg
```

- man

Access manual for all Linux commands.



```
┌──(root㉿kali)-[/media/root/HW2]
└─# man man
```