



***Universidad Autónoma de Chiapas.
Facultad de Negocios C-IV***

**Licenciatura en Ingeniería en Desarrollo y Tecnologías
de Software**

Optativa Computo Forense

Orozco Cárdenas José Eduardo

7.- "D"

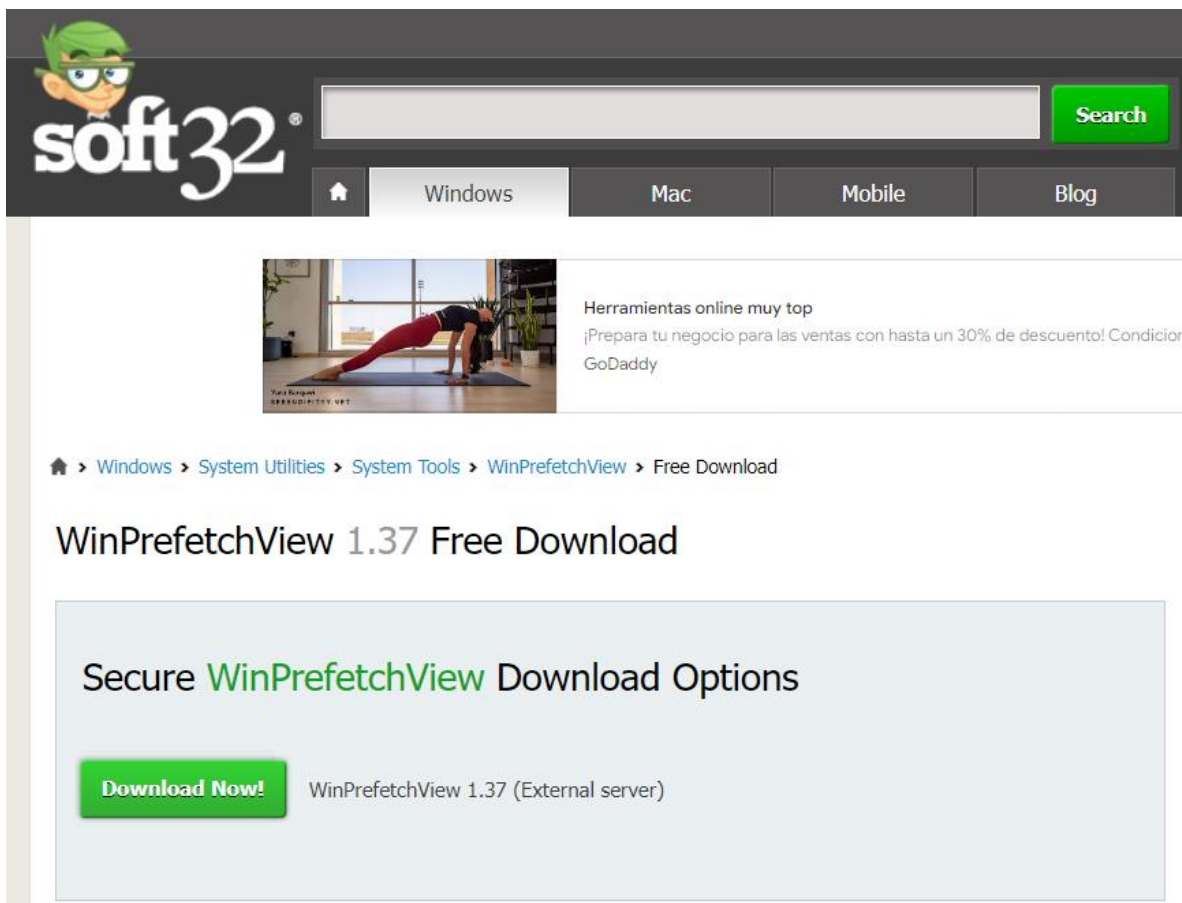
Profesor Rene Servando Rivera Roblero

Practica Análisis Forense

Tapachula, Chiapas, México a 09 de septiembre de 2023

Windows

1. Descargamos el software WINPREFETCHVIEW



The screenshot shows the soft32.com website. The header includes the soft32 logo, a search bar, and navigation links for Windows, Mac, Mobile, and Blog. A banner for 'Herramientas online muy top' is visible. The breadcrumb trail reads: Home > Windows > System Utilities > System Tools > WinPrefetchView > Free Download. The main heading is 'WinPrefetchView 1.37 Free Download'. Below it, a section titled 'Secure WinPrefetchView Download Options' contains a green 'Download Now!' button and the text 'WinPrefetchView 1.37 (External server)'.

2. Buscamos el .zip y lo descomprimos, para después descomprimir y buscar el .exe



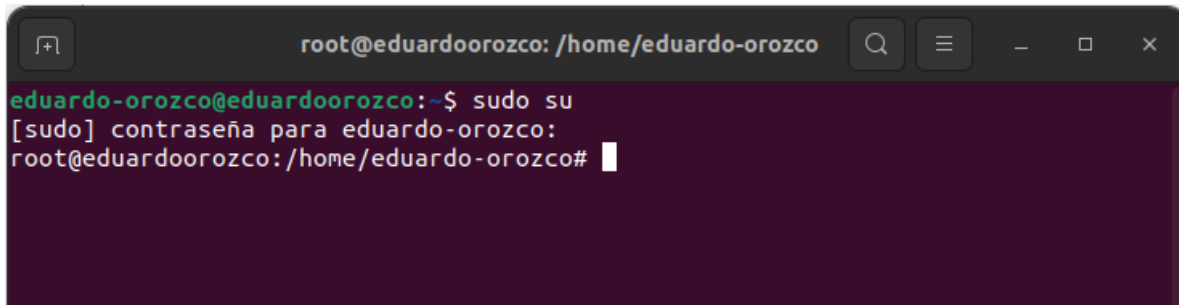
3. Después de ejecutar nos abre la venta con el reporte

WinPrefetchView							
File Edit View Options Help							
Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time
0.DAT-24906F61.pf	22/9/2023 21:45:57	22/9/2023 21:45:57	21,860	0.DAT	C:\Users\joseg\AppData\Local\NVIDIA\NV...	1	22/9/2023 21:45:57
9FDC-4231-122F-086F...	23/9/2023 10:35:00	23/9/2023 10:35:00	4,484	9FDC-4231-122F-0...	C:\WINDOWS\SYSTEMTEMP\9FDC-4231-12...	1	23/9/2023 10:35:00
AM_DELTA_PATCH_1.3...	22/9/2023 22:39:08	22/9/2023 22:39:08	1,835	AM_DELTA_PATCH...	C:\WINDOWS\SOFTWAREDISTRIBUTION\D...	1	22/9/2023 22:39:08
AM_DELTA_PATCH_1.3...	23/9/2023 10:48:09	23/9/2023 10:48:09	1,860	AM_DELTA_PATCH...	C:\WINDOWS\SOFTWAREDISTRIBUTION\D...	1	23/9/2023 10:48:09
AM_DELTA_PATCH_1.3...	23/9/2023 20:45:22	23/9/2023 20:45:22	1,829	AM_DELTA_PATCH...	C:\WINDOWS\SOFTWAREDISTRIBUTION\D...	1	23/9/2023 20:45:22
APP_W.EXE-2E9907EA...	19/5/2023 04:49:51	19/5/2023 05:26:19	160,016	APP_W.EXE	D:\joseg\DOCUMENTS\Python\dist\App...	17	19/5/2023 04:49:51
APPLICATIONFRAME...	2/4/2023 08:58:16	28/7/2023 23:04:39	20,681	APPLICATIONFRA...	C:\WINDOWS\SYSTEM32\APPLICATIONFR...	28	28/7/2023 23:04:39
APPLICATIONFRAME...	31/7/2023 11:16:34	13/9/2023 22:30:04	21,000	APPLICATIONFRA...	C:\WINDOWS\SYSTEM32\APPLICATIONFR...	27	13/9/2023 22:30:04
APPVSHNOTIFY.EXE-F...	21/9/2023 23:38:18	21/9/2023 23:38:18	4,662	APPVSHNOTIFY.EXE	C:\PROGRAM FILES\COMMON FILES\MICR...	2	21/9/2023 23:38:18
ARDUINO IDE.EXE-032...	3/5/2023 18:29:07	23/6/2023 21:00:03	56,006	ARDUINO IDE.EXE	C:\PROGRAM FILES\ARDUINO IDE\ARDUIN...	47	23/6/2023 21:00:03
Filename	Full Path	Device Path	Index				
SMFT	C:\Windows\SysWOW64\oleaut32.dll	\\VOLUME{01d803dd94c0d44d-3694d6...	36				
0.DAT	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	18				
300_YING_XIONG.TRA...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	54				
7_DAYS_TO_DIE.TRA...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	55				
7FAN_ALL_HEROES.TRA...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	56				
9_MONKEYS_OF_SHA...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	57				
A_PLAQUE_TALE_INN...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	58				
A_PLAQUE_TALE_REQ...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	59				
A_WAY_OUT.TRANSL...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	60				
ACE_COMBAT_7_SKIE...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	61				
ACE_COMBAT ASSAU...	C:\Users\joseg\AppData\Local\NVIDI...	\\VOLUME{01d803dd94c0d44d-3694d6...	62				
379 Files, 1 Selected				NirSoft Freeware. https://www.nirsoft.net			

Automáticamente, nos aparece un análisis que ha hecho el programa en nuestro equipo y de todo lo que está sucediendo en el momento y los programas que se están utilizando.

Linux

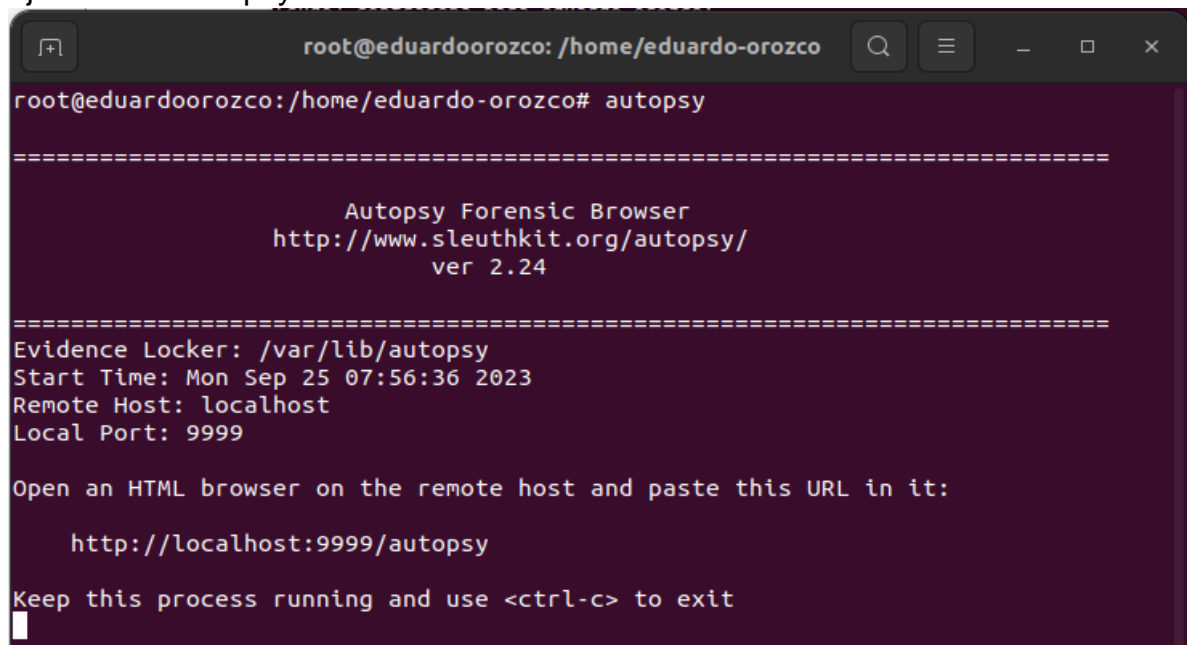
1. Iniciamos sesión como super usuario



```
root@eduardoorozco: /home/eduardo-orozco
eduardo-orozco@eduardoorozco:~$ sudo su
[sudo] contraseña para eduardo-orozco:
root@eduardoorozco: /home/eduardo-orozco#
```

2. ejecutamos el comando: `sudo apt-get install autopsy`
este comando nos instalará la herramienta necesaria

3. ejecutamos autopsy en el bash



```
root@eduardoorozco: /home/eduardo-orozco# autopsy

=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====

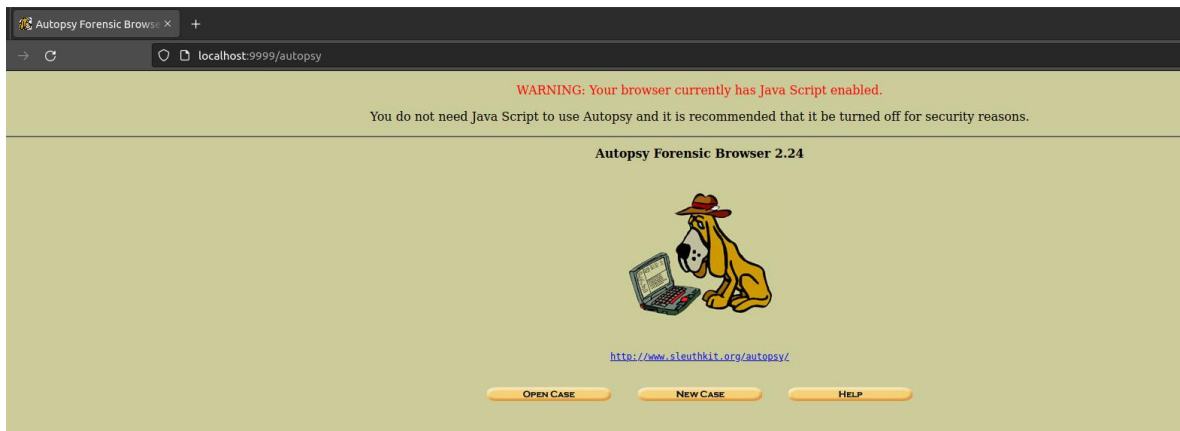
Evidence Locker: /var/lib/autopsy
Start Time: Mon Sep 25 07:56:36 2023
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

4. Ingresamos al link del localhost que nos lleva a la página de la herramienta



5. creamos un nuevo caso

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	<input type="text" value="eduardo"/>	b.	<input type="text"/>
c.	<input type="text"/>	d.	<input type="text"/>
e.	<input type="text"/>	f.	<input type="text"/>
g.	<input type="text"/>	h.	<input type="text"/>
i.	<input type="text"/>	j.	<input type="text"/>

NEW CASE CANCEL HELP

6. Añadimos un host

Creating Case: case4

Case directory (/var/lib/autopsy/case4/) created
Configuration file (/var/lib/autopsy/case4/case.aut) created

We must now create a host for this case.

Please select your name from the list: eduardo ▾

ADD HOST

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

host1

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

ADD HOST

CANCEL

HELP

7. En una terminal creamos una nueva carpeta llamada autopsy

```
eduardo-oro...@eduardoorozco: ~/Documentos
eduardo-oro...@eduardoorozco:~$ cd Documentos
eduardo-oro...@eduardoorozco:~/Documentos$ ls
autopsy desarrollo-movil-y-web nuevo OZ
eduardo-oro...@eduardoorozco:~/Documentos$ mkdir autopsy
```

una vez creada entramos como super user

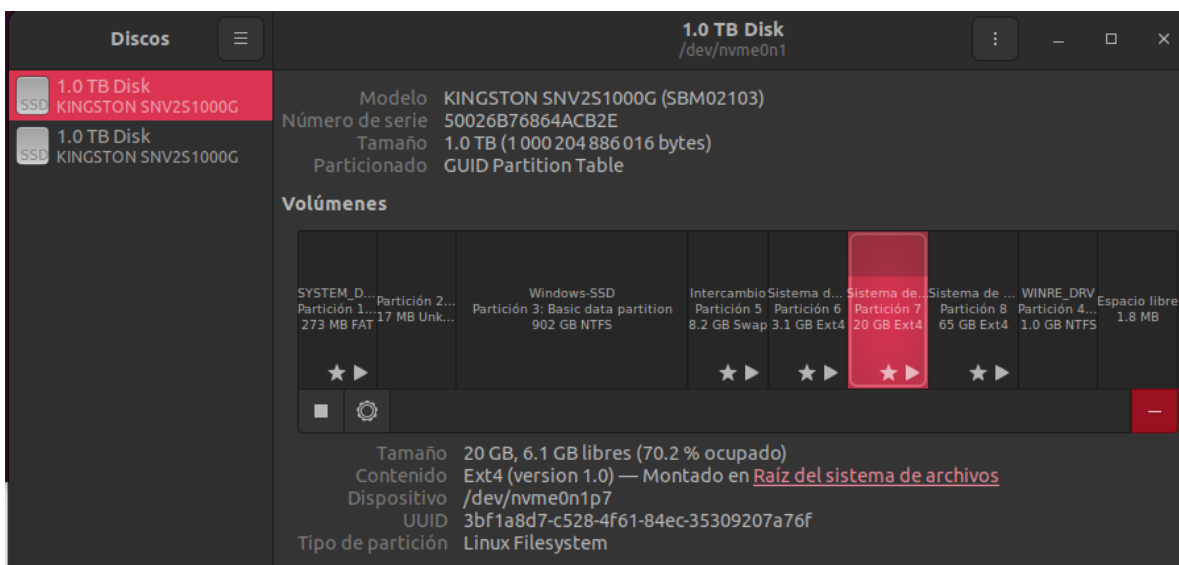
8. entramos a la carpeta creada

```
root@eduardoorozco: /home/eduardo-oro.../Documentos/...
root@eduardoorozco:/home/eduardo-oro.../Documentos# ls
autopsy desarrollo-movil-y-web nuevo OZ
root@eduardoorozco:/home/eduardo-oro.../Documentos# cd autopsy
root@eduardoorozco:/home/eduardo-oro.../Documentos/autopsy#
```

9. creamos una imagen

```
root@eduardoorozco:/home/eduardo-oro.../Documentos/autopsy# touch forense.img
root@eduardoorozco:/home/eduardo-oro.../Documentos/autopsy# ls
edu.img forense.img lales.img
root@eduardoorozco:/home/eduardo-oro.../Documentos/autopsy# S
```

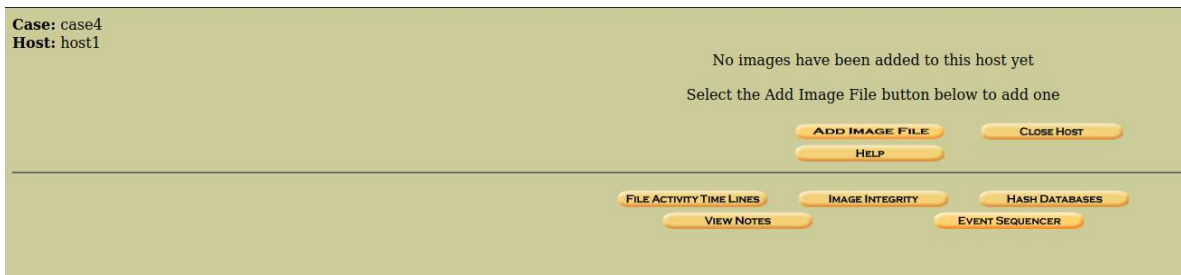
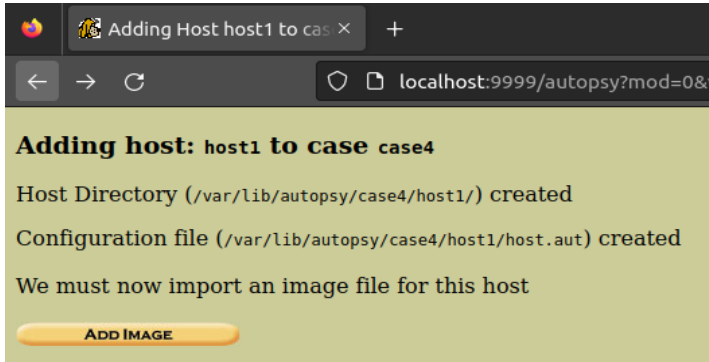
10. ahora buscamos en nuestro administrador de discos el nombre la partición a la que haremos la copia



11. Ejecutamos el comando y nos crea una copia de la partición

```
root@eduardoorozco: /home/eduardo-orozco/Documentos/autopsy
root@eduardoorozco: /home/eduardo-orozco/Documentos/autopsy# dd if=/dev/nvme0n1p7 of=/home/eduardo-orozco/Documentos/autopsy/forense.img
39999488+0 registros leídos
39999488+0 registros escritos
20479737856 bytes (20 GB, 19 GiB) copied, 99.7992 s, 205 MB/s
root@eduardoorozco: /home/eduardo-orozco/Documentos/autopsy#
```

12. agregamos la imagen a la página



Local Name: images/forense.img

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☒ Ignore the hash value for this image.
☐ Calculate the hash value for this image.
☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ext4)
 Mount Point: File System Type:

Testing partitions
 Linking image(s) into evidence locker
 Image file added with ID img1
 Volume image (0 to 0 - ext - /1/) added with ID vol1

damos en ok

13. Ahora analizamos la partición

Select a volume to analyze or add a new image file.

CASE GALLERY		HOST GALLERY		HOST MANAGER	
mount	name	fs type			
<input checked="" type="radio"/> /1/	forense.img-0-0	ext	details		

14. Revisamos el análisis generado

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

?

X

Directory Seek

Enter the name of a directory that you want to view.
/1/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Current Directory: /1/

ADD NOTE

GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
Error Parsing File (Invalid Characters?): V/V 1250929: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0									
	d / d	../	2023-09-20 00:08:11 (CST)	2023-09-25 01:44:54 (CST)	2023-09-20 00:08:11 (CST)	4096	0	0	2
	d / d	../	2023-09-20 00:08:11 (CST)	2023-09-25 01:44:54 (CST)	2023-09-20 00:08:11 (CST)	4096	0	0	2
	l / l	bin	2023-09-04 14:35:55 (CST)	2023-09-25 01:44:51 (CST)	2023-09-04 14:35:55 (CST)	7	0	0	12
	d / d	boot/	2023-09-04 14:35:54 (CST)	2023-09-25 01:44:52 (CST)	2023-09-04 14:35:54 (CST)	4096	0	0	784897
	d / d	cdrom/	2023-09-04 14:38:15 (CST)	2023-09-04 14:38:15 (CST)	2023-09-04 14:38:15 (CST)	4096	0	0	1064567
	d / d	dev/	2022-08-09 06:48:12 (CDT)	2023-09-04 14:43:05 (CST)	2023-09-04 14:38:09 (CST)	4096	0	0	261633
	d / d	etc/	2023-09-21 06:20:28 (CST)	2023-09-21 14:18:06 (CST)	2023-09-21 06:20:28 (CST)	12288	0	0	1046529
	d / d	home/	2023-09-04 14:35:54 (CST)	2023-09-25 01:44:52 (CST)	2023-09-04 14:35:54 (CST)	4096	0	0	654081
	l / l	lib	2023-09-04 14:35:55 (CST)	2023-09-25 01:44:51 (CST)	2023-09-04 14:35:55 (CST)	7	0	0	13
	l / l	lib32	2023-09-04 14:35:55 (CST)	2023-09-21 06:20:22 (CST)	2023-09-04 14:35:55 (CST)	9	0	0	14
	l / l	lib64	2023-09-04 14:35:55 (CST)	2023-09-25 01:44:51 (CST)	2023-09-04 14:35:55 (CST)	9	0	0	15
	l / l	libx32	2023-09-04 14:35:55 (CST)	2023-09-21 06:20:18 (CST)	2023-09-04 14:35:55 (CST)	10	0	0	16
	l / l	lost+found/	2023-09-04 14:35:55 (CST)	2023-09-04 14:35:55 (CST)	2023-09-04 14:35:55 (CST)	4096	0	0	11

File Browsing Mode