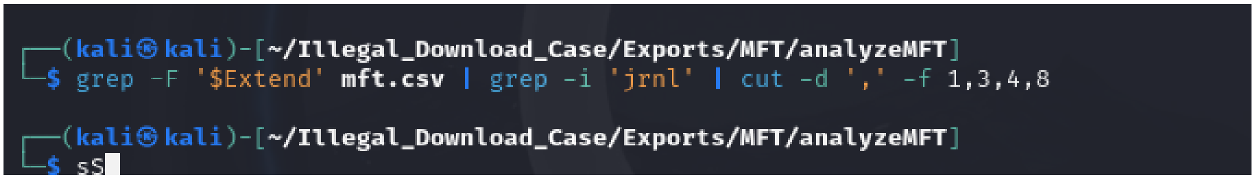
Daniella Boulos, Julianna Russo, Tyler Kaminer — Oct 5, 2024

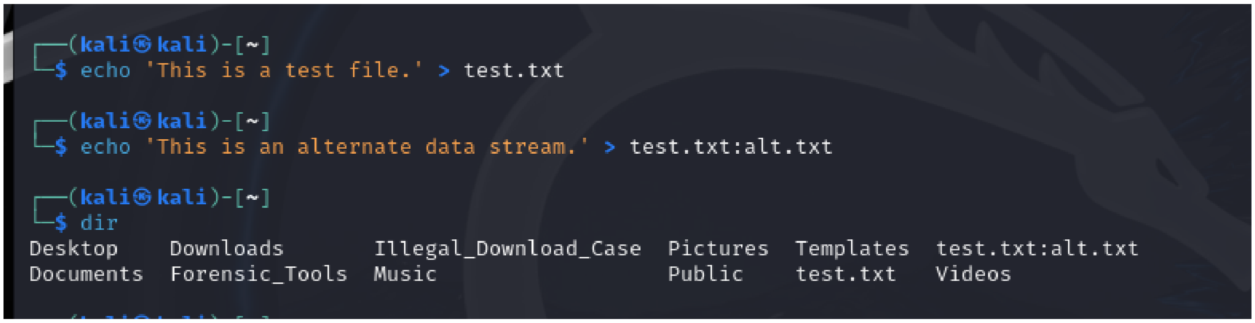
NIST Case: USN Journal Timeline — Computer Forensics

Location of the USN Journal

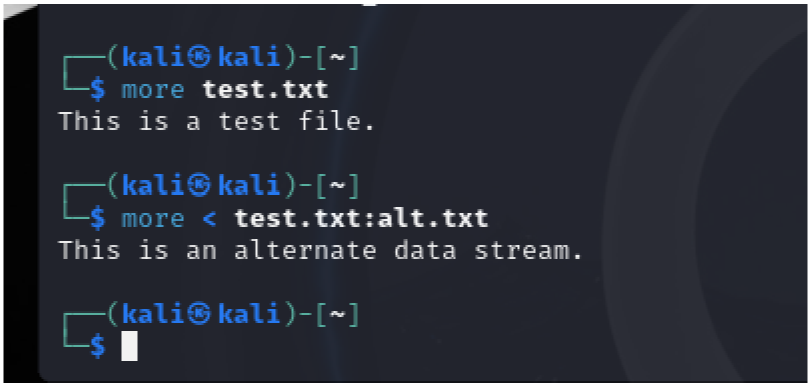


```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ grep -F '$Extend' mft.csv | grep -i 'jrnl' | cut -d ',' -f 1,3,4,8

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ sS
```

How to create an alternate data stream

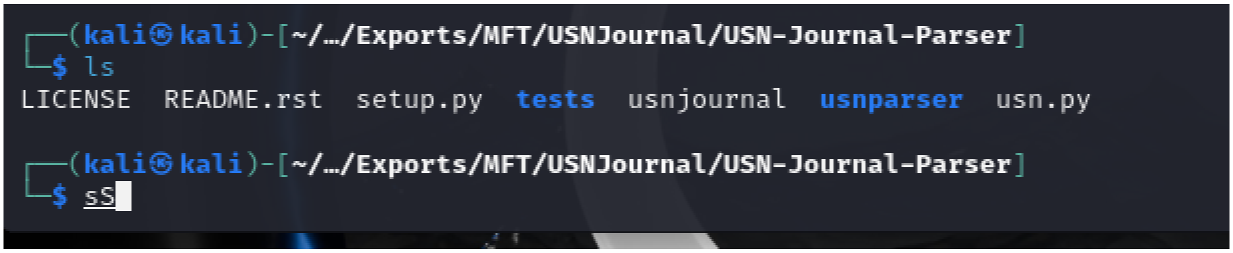


```
┌──(kali㉿kali)-[~]
└─$ echo 'This is a test file.' > test.txt

┌──(kali㉿kali)-[~]
└─$ echo 'This is an alternate data stream.' > test.txt:alt.txt

┌──(kali㉿kali)-[~]
└─$ dir
Desktop     Downloads       Illegal_Download_Case  Pictures  Templates  test.txt:alt.txt
Documents   Forensic_Tools  Music                  Public    test.txt   Videos
```



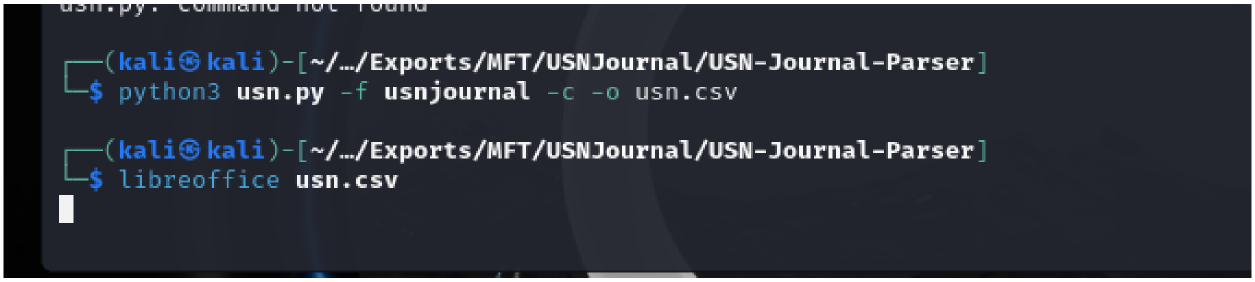
```
┌──(kali㉿kali)-[~]
└─$ more test.txt
This is a test file.

┌──(kali㉿kali)-[~]
└─$ more < test.txt:alt.txt
This is an alternate data stream.

┌──(kali㉿kali)-[~]
└─$ 
```

USN Record Carver to obtain the USN Journal entries

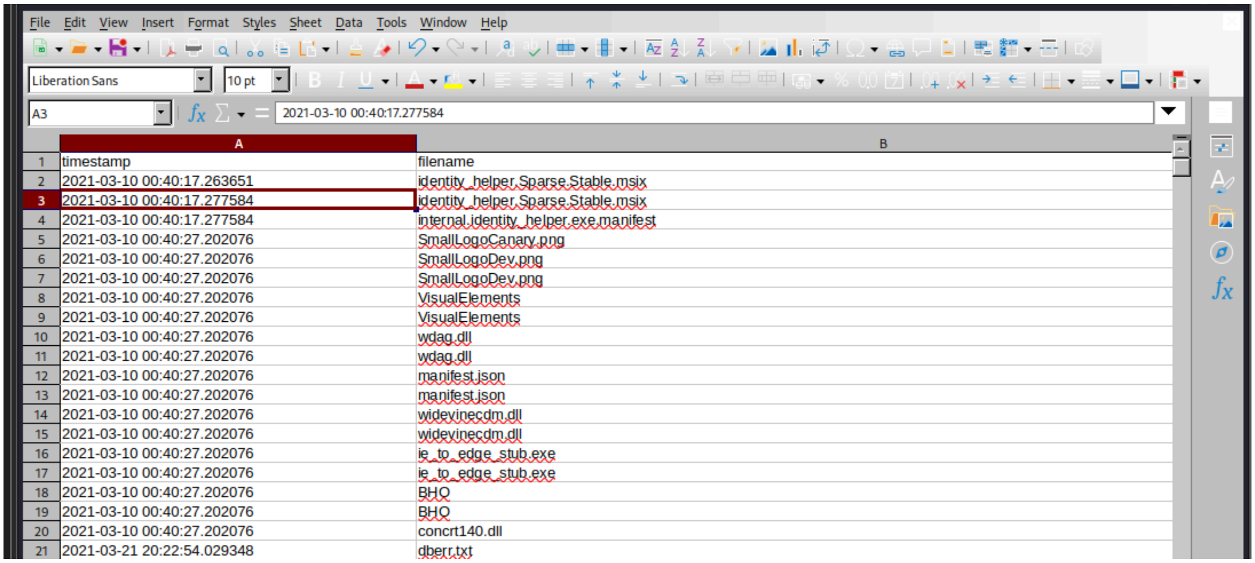


```
┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ ls
LICENSE  README.rst  setup.py  tests  usnjournal  usnparser  usn.py

┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ sS
```

Use USN Journal Parser to parse the USN Journal entries



```
usn.py: command not found

┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ python3 usn.py -f usnjournal -c -o usn.csv

┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ libreoffice usn.csv
```

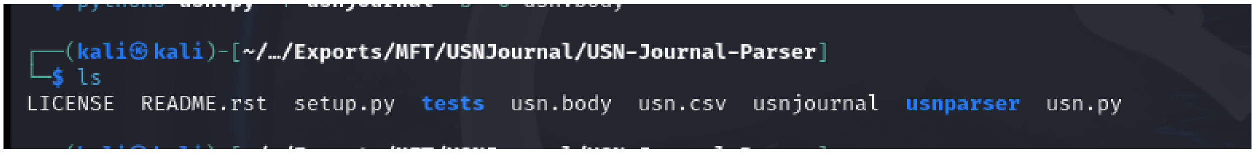


File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
A3

2021-03-10 00:40:17.277584

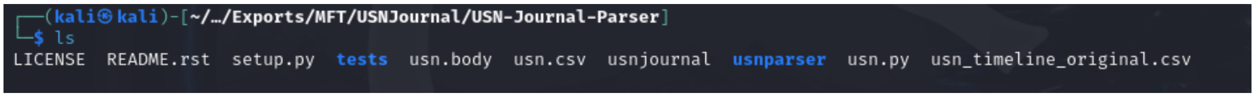
	A	B
1	timestamp	filename
2	2021-03-10 00:40:17.263651	identity_helper.Sparse.Stable.msix
3	2021-03-10 00:40:17.277584	identity_helper.Sparse.Stable.msix
4	2021-03-10 00:40:17.277584	internal.identity_helper.exe.manifest
5	2021-03-10 00:40:27.202076	SmallLogoCanary.png
6	2021-03-10 00:40:27.202076	SmallLogoDev.png
7	2021-03-10 00:40:27.202076	SmallLogoDev.png
8	2021-03-10 00:40:27.202076	VisualElements
9	2021-03-10 00:40:27.202076	VisualElements
10	2021-03-10 00:40:27.202076	wdag.dll
11	2021-03-10 00:40:27.202076	wdag.dll
12	2021-03-10 00:40:27.202076	manifest.json
13	2021-03-10 00:40:27.202076	manifest.json
14	2021-03-10 00:40:27.202076	widevinecdm.dll
15	2021-03-10 00:40:27.202076	widevinecdm.dll
16	2021-03-10 00:40:27.202076	ie_to_edge_stub.exe
17	2021-03-10 00:40:27.202076	ie_to_edge_stub.exe
18	2021-03-10 00:40:27.202076	BHO
19	2021-03-10 00:40:27.202076	BHO
20	2021-03-10 00:40:27.202076	concrt140.dll
21	2021-03-21 20:22:54.029348	dberr.txt

Use usn.py to generate a body file



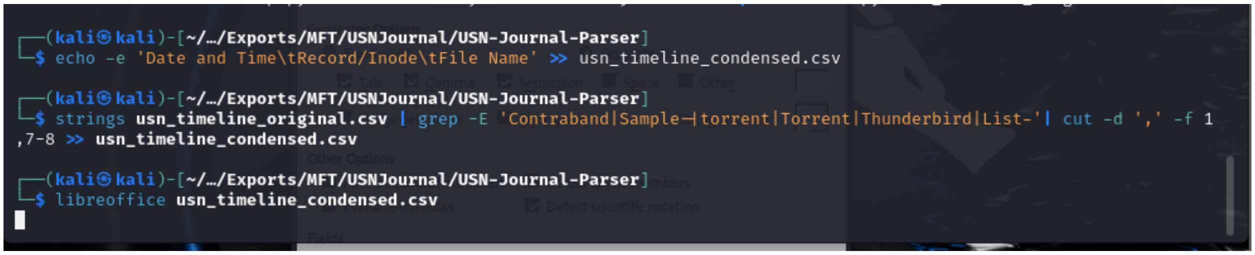
```
└─$ python3 usn.py -f usnjournal -b -o usn.body

┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ ls
LICENSE  README.rst  setup.py  tests  usn.body  usn.csv  usnjournal  usnparser  usn.py
```

Use mactime to generate a timeline from the USN Journal records

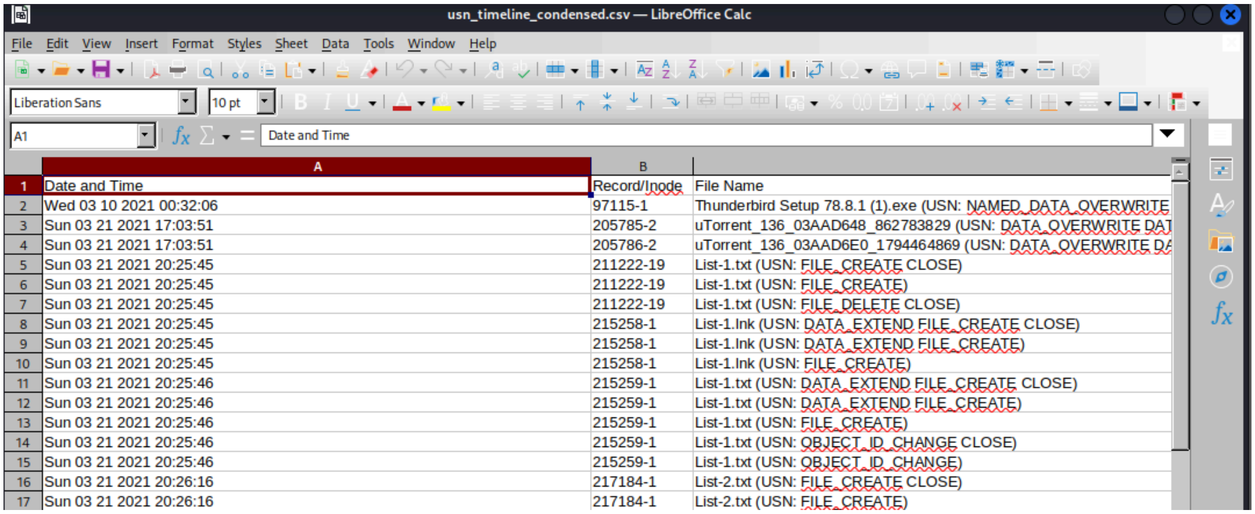


```
┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ ls
LICENSE  README.rst  setup.py  tests  usn.body  usn.csv  usnjournal  usnparser  usn.py  usn_timeline_original.csv
```

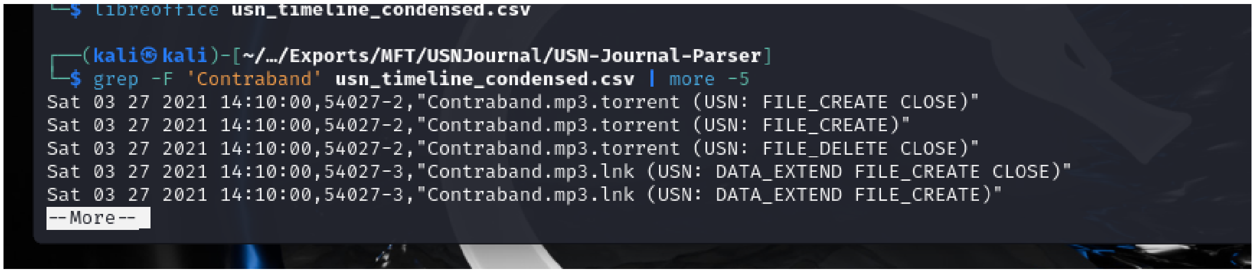
Analyze the timeline for files of interest



```
┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ echo -e 'Date and Time\tRecord/Inode\tFile Name' >> usn_timeline_condensed.csv

┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ strings usn_timeline_original.csv | grep -E 'Contraband|Sample-|torrent|Torrent|Thunderbird|List-'| cut -d ',' -f 1
,7-8 >> usn_timeline_condensed.csv

┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ libreoffice usn_timeline_condensed.csv
```


usn_timeline_condensed.csv — LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
A1
Date and Time

	A	B	
1	Date and Time	Record/Inode	File Name
2	Wed 03 10 2021 00:32:06	97115-1	Thunderbird Setup 78.8.1 (1).exe (USN: NAMED_DATA_OVERWRITE
3	Sun 03 21 2021 17:03:51	205785-2	uTorrent_136_03AAD648_862783829 (USN: DATA_OVERWRITE DAT
4	Sun 03 21 2021 17:03:51	205786-2	uTorrent_136_03AAD6E0_1794464869 (USN: DATA_OVERWRITE DA
5	Sun 03 21 2021 20:25:45	211222-19	List-1.txt (USN: FILE_CREATE CLOSE)
6	Sun 03 21 2021 20:25:45	211222-19	List-1.txt (USN: FILE_CREATE)
7	Sun 03 21 2021 20:25:45	211222-19	List-1.txt (USN: FILE_DELETE CLOSE)
8	Sun 03 21 2021 20:25:45	215258-1	List-1.lnk (USN: DATA_EXTEND FILE_CREATE CLOSE)
9	Sun 03 21 2021 20:25:45	215258-1	List-1.lnk (USN: DATA_EXTEND FILE_CREATE)
10	Sun 03 21 2021 20:25:45	215258-1	List-1.lnk (USN: FILE_CREATE)
11	Sun 03 21 2021 20:25:46	215259-1	List-1.txt (USN: DATA_EXTEND FILE_CREATE CLOSE)
12	Sun 03 21 2021 20:25:46	215259-1	List-1.txt (USN: DATA_EXTEND FILE_CREATE)
13	Sun 03 21 2021 20:25:46	215259-1	List-1.txt (USN: FILE_CREATE)
14	Sun 03 21 2021 20:25:46	215259-1	List-1.txt (USN: OBJECT_ID_CHANGE CLOSE)
15	Sun 03 21 2021 20:25:46	215259-1	List-1.txt (USN: OBJECT_ID_CHANGE)
16	Sun 03 21 2021 20:26:16	217184-1	List-2.txt (USN: FILE_CREATE CLOSE)
17	Sun 03 21 2021 20:26:16	217184-1	List-2.txt (USN: FILE_CREATE)



```
└─$ libreoffice usn_timeline_condensed.csv

┌──(kali㉿kali)-[~/…/Exports/MFT/USNJournal/USN-Journal-Parser]
└─$ grep -F 'Contraband' usn_timeline_condensed.csv | more -5
Sat 03 27 2021 14:10:00,54027-2,"Contraband.mp3.torrent (USN: FILE_CREATE CLOSE)"
Sat 03 27 2021 14:10:00,54027-2,"Contraband.mp3.torrent (USN: FILE_CREATE)"
Sat 03 27 2021 14:10:00,54027-2,"Contraband.mp3.torrent (USN: FILE_DELETE CLOSE)"
Sat 03 27 2021 14:10:00,54027-3,"Contraband.mp3.lnk (USN: DATA_EXTEND FILE_CREATE CLOSE)"
Sat 03 27 2021 14:10:00,54027-3,"Contraband.mp3.lnk (USN: DATA_EXTEND FILE_CREATE)"
--More--
```