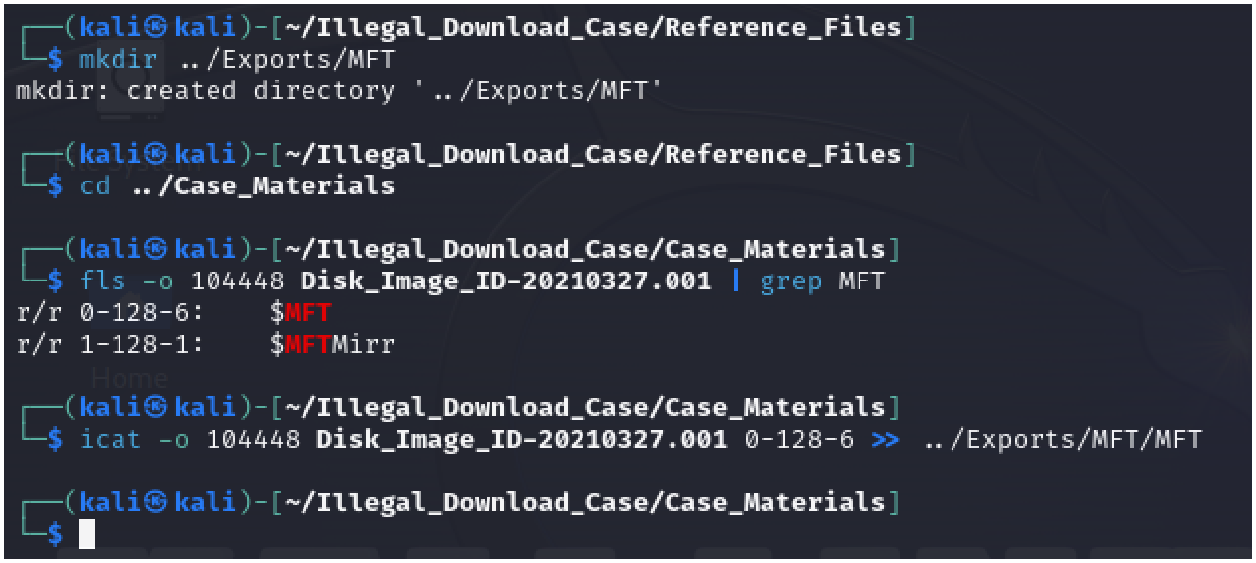
Daniella Boulos, Julianna Russo, Tyler Kaminer
NIST Case: MFT Timeline

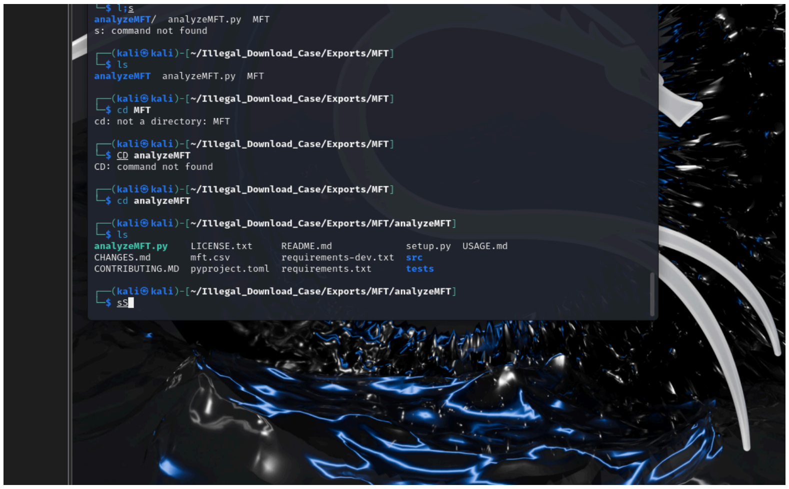
Sept 29, 2024
Computer Forensics

Extracting MFT



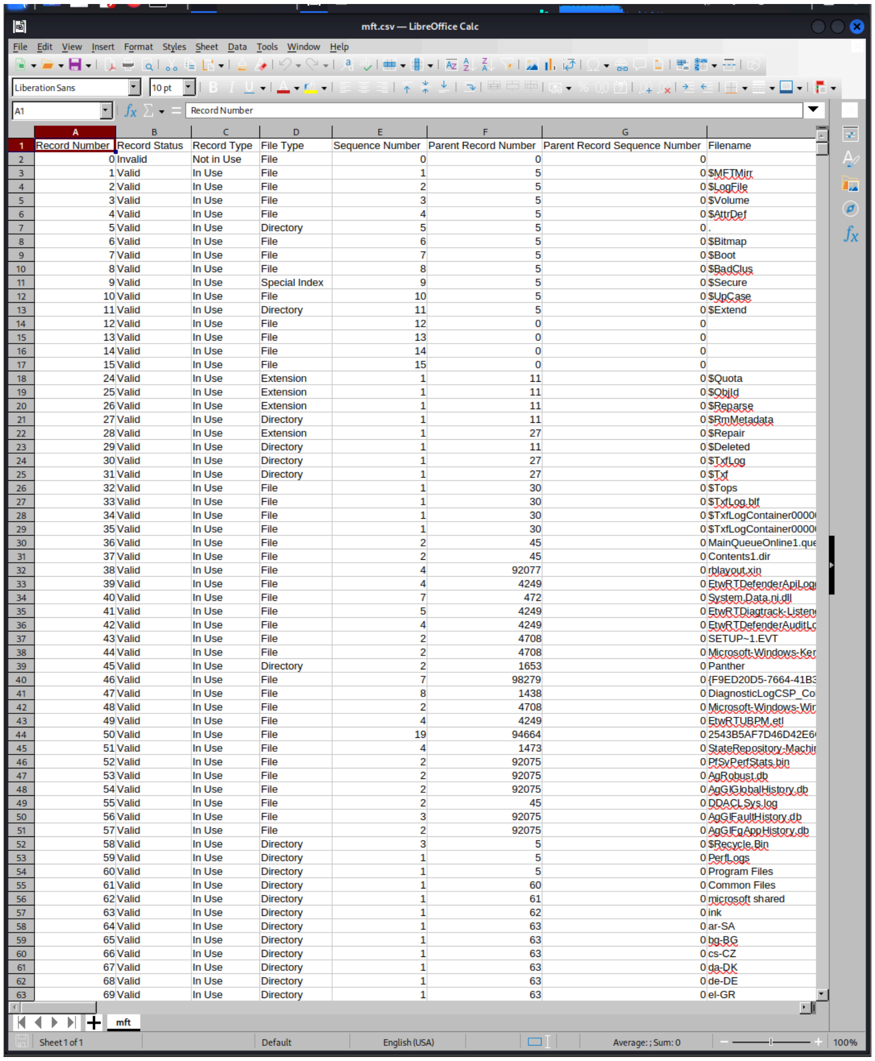
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ mkdir ../Exports/MFT
mkdir: created directory '../Exports/MFT'

┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ cd ../Case_Materials

┌──(kali㉿kali)-[~/Illegal_Download_Case/Case_Materials]
└─$ fls -o 104448 Disk_Image_ID-20210327.001 | grep MFT
r/r 0-128-6:    $MFT
r/r 1-128-1:    $MFTMirr

┌──(kali㉿kali)-[~/Illegal_Download_Case/Case_Materials]
└─$ icat -o 104448 Disk_Image_ID-20210327.001 0-128-6 >> ../Exports/MFT/MFT

┌──(kali㉿kali)-[~/Illegal_Download_Case/Case_Materials]
└─$ 
```

Parsing the MFT



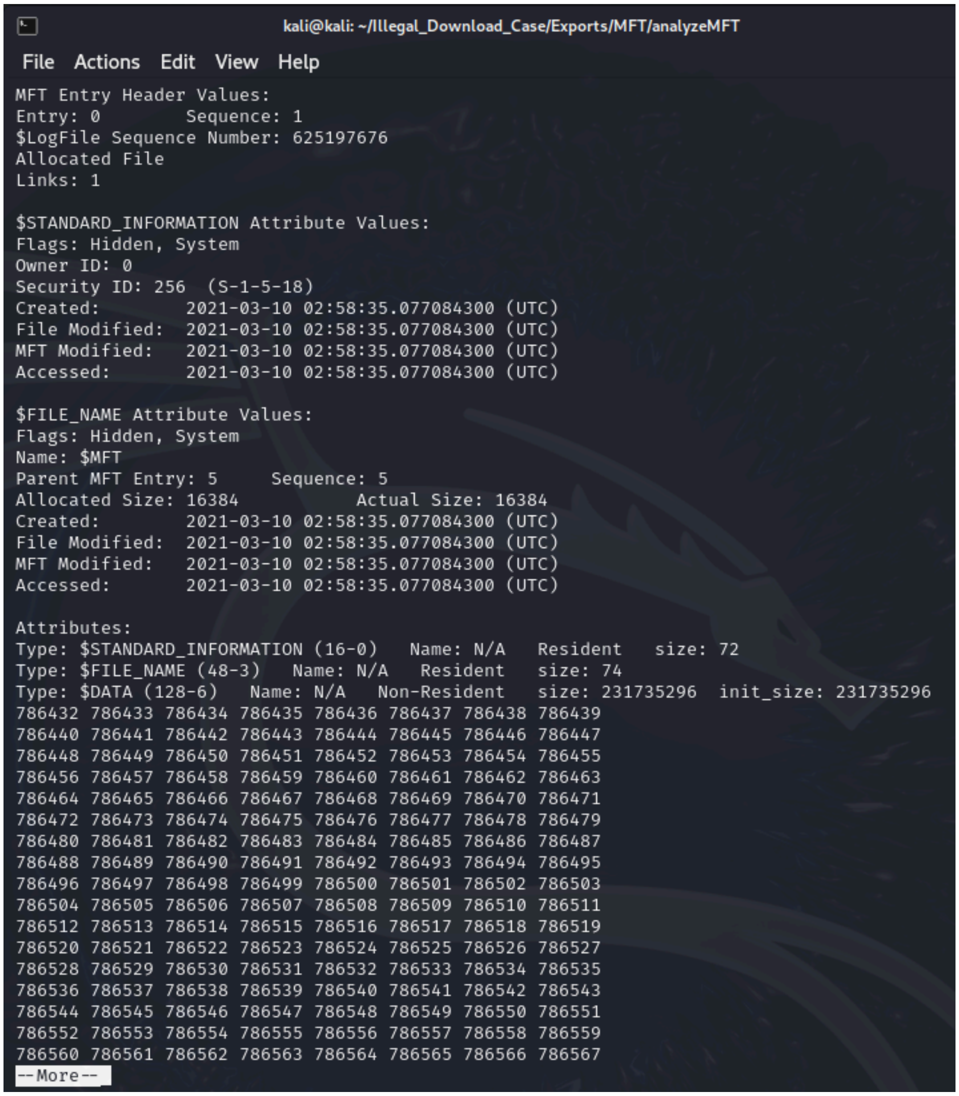
```
└─$ l;s
analyzeMFT/  analyzeMFT.py  MFT
s: command not found

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT]
└─$ ls
analyzeMFT  analyzeMFT.py  MFT

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT]
└─$ cd MFT
cd: not a directory: MFT

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT]
└─$ CD analyzeMFT
CD: command not found

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

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ ls
analyzeMFT.py    LICENSE.txt     README.md              setup.py  USAGE.md
CHANGES.md       mft.csv         requirements-dev.txt   src
CONTRIBUTING.MD  pyproject.toml  requirements.txt       tests

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

Opening mft.csv



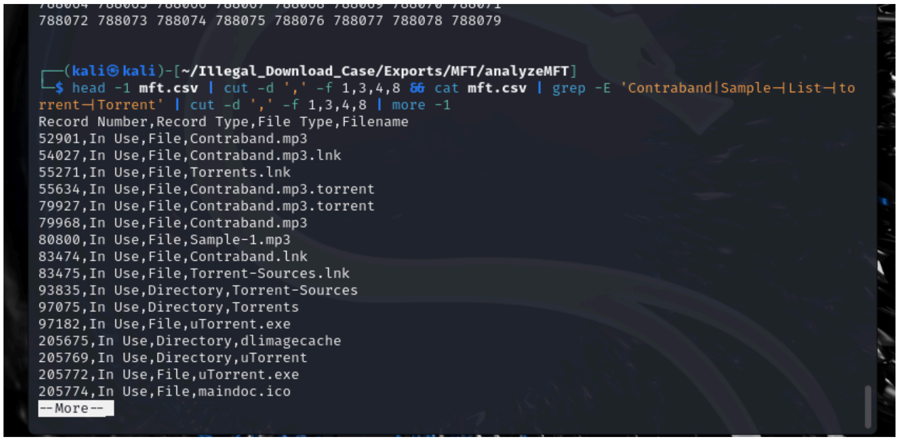
1	Record Number	Record Status	Record Type	File Type	Sequence Number	Parent Record Number	Parent Record Sequence Number	Filename
2	0	Invalid	Not in Use	File	0	0	0	
3	1	Valid	In Use	File	1	5	0	$MFTMirr
4	2	Valid	In Use	File	2	5	0	$LogFile
5	3	Valid	In Use	File	3	5	0	$Volume
6	4	Valid	In Use	File	4	5	0	$AttrDef
7	5	Valid	In Use	Directory	5	5	0	.
8	6	Valid	In Use	File	6	5	0	$Bitmap
9	7	Valid	In Use	File	7	5	0	$Boot
10	8	Valid	In Use	File	8	5	0	$BadClus
11	9	Valid	In Use	Special Index	9	5	0	$Secure
12	10	Valid	In Use	File	10	5	0	$UpCase
13	11	Valid	In Use	Directory	11	5	0	$Extend
14	12	Valid	In Use	File	12	0	0	
15	13	Valid	In Use	File	13	0	0	
16	14	Valid	In Use	File	14	0	0	
17	15	Valid	In Use	File	15	0	0	
18	24	Valid	In Use	Extension	1	11	0	$Quota
19	25	Valid	In Use	Extension	1	11	0	$ObjId
20	26	Valid	In Use	Extension	1	11	0	$Reparse
21	27	Valid	In Use	Directory	1	11	0	$RmMetadata
22	28	Valid	In Use	Extension	1	27	0	$Repair
23	29	Valid	In Use	Directory	1	11	0	$Deleted
24	30	Valid	In Use	Directory	1	27	0	$TxfLog
25	31	Valid	In Use	Directory	1	27	0	$Txf
26	32	Valid	In Use	File	1	30	0	$Tops
27	33	Valid	In Use	File	1	30	0	$TxfLog.blf
28	34	Valid	In Use	File	1	30	0	$TxfLogContainer0000
29	35	Valid	In Use	File	1	30	0	$TxfLogContainer0000
30	36	Valid	In Use	File	2	45	0	MainQueueOnline1.que
31	37	Valid	In Use	File	2	45	0	Contents1.dir
32	38	Valid	In Use	File	4	92077	0	rblayout.xin
33	39	Valid	In Use	File	4	4249	0	EtwRTDefenderApiLog
34	40	Valid	In Use	File	7	472	0	System.Data.ni.dll
35	41	Valid	In Use	File	5	4249	0	EtwRTDiagtrack-Listen
36	42	Valid	In Use	File	4	4249	0	EtwRTDefenderAuditLo
37	43	Valid	In Use	File	2	4708	0	SETUP~1.EVT
38	44	Valid	In Use	File	2	4708	0	Microsoft-Windows-Ker
39	45	Valid	In Use	Directory	2	1653	0	Panther
40	46	Valid	In Use	File	7	98279	0	{F9ED20D5-7664-41B3
41	47	Valid	In Use	File	8	1438	0	DiagnosticLogCSP_Co
42	48	Valid	In Use	File	2	4708	0	Microsoft-Windows-Wir
43	49	Valid	In Use	File	4	4249	0	EtwRTUBPM.etl
44	50	Valid	In Use	File	19	94664	0	2543B5AF7D46D42E6
45	51	Valid	In Use	File	4	1473	0	StateRepository-Machi
46	52	Valid	In Use	File	2	92075	0	PfSvPerfStats.bin
47	53	Valid	In Use	File	2	92075	0	AgRobust.db
48	54	Valid	In Use	File	2	92075	0	AgGlGlobalHistory.db
49	55	Valid	In Use	File	2	45	0	DDACLSys.log
50	56	Valid	In Use	File	3	92075	0	AgGlFaultHistory.db
51	57	Valid	In Use	File	2	92075	0	AgGlFgAppHistory.db
52	58	Valid	In Use	Directory	3	5	0	$Recycle.Bin
53	59	Valid	In Use	Directory	1	5	0	PerfLogs
54	60	Valid	In Use	Directory	1	5	0	Program Files
55	61	Valid	In Use	Directory	1	60	0	Common Files
56	62	Valid	In Use	Directory	1	61	0	microsoft shared
57	63	Valid	In Use	Directory	1	62	0	ink
58	64	Valid	In Use	Directory	1	63	0	ar-SA
59	65	Valid	In Use	Directory	1	63	0	bg-BG
60	66	Valid	In Use	Directory	1	63	0	cs-CZ
61	67	Valid	In Use	Directory	1	63	0	da-DK
62	68	Valid	In Use	Directory	1	63	0	de-DE
63	69	Valid	In Use	Directory	1	63	0	el-GR

Using istat

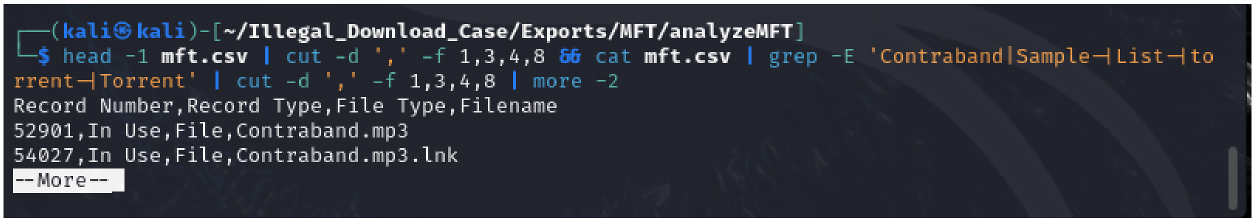

kali@kali: ~/Illegal_Download_Case/Exports/MFT/analyzeMFT
File Actions Edit View Help

```
MFT Entry Header Values:
Entry: 0        Sequence: 1
$LogFile Sequence Number: 625197676
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-18)
Created:        2021-03-10 02:58:35.077084300 (UTC)
File Modified:  2021-03-10 02:58:35.077084300 (UTC)
MFT Modified:   2021-03-10 02:58:35.077084300 (UTC)
Accessed:       2021-03-10 02:58:35.077084300 (UTC)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 16384           Actual Size: 16384
Created:        2021-03-10 02:58:35.077084300 (UTC)
File Modified:  2021-03-10 02:58:35.077084300 (UTC)
MFT Modified:   2021-03-10 02:58:35.077084300 (UTC)
Accessed:       2021-03-10 02:58:35.077084300 (UTC)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-3)   Name: N/A   Resident   size: 74
Type: $DATA (128-6)   Name: N/A   Non-Resident   size: 231735296  init_size: 231735296
786432 786433 786434 786435 786436 786437 786438 786439
786440 786441 786442 786443 786444 786445 786446 786447
786448 786449 786450 786451 786452 786453 786454 786455
786456 786457 786458 786459 786460 786461 786462 786463
786464 786465 786466 786467 786468 786469 786470 786471
786472 786473 786474 786475 786476 786477 786478 786479
786480 786481 786482 786483 786484 786485 786486 786487
786488 786489 786490 786491 786492 786493 786494 786495
786496 786497 786498 786499 786500 786501 786502 786503
786504 786505 786506 786507 786508 786509 786510 786511
786512 786513 786514 786515 786516 786517 786518 786519
786520 786521 786522 786523 786524 786525 786526 786527
786528 786529 786530 786531 786532 786533 786534 786535
786536 786537 786538 786539 786540 786541 786542 786543
786544 786545 786546 786547 786548 786549 786550 786551
786552 786553 786554 786555 786556 786557 786558 786559
786560 786561 786562 786563 786564 786565 786566 786567
--More--
```

Searching for files of interest in the $MFT

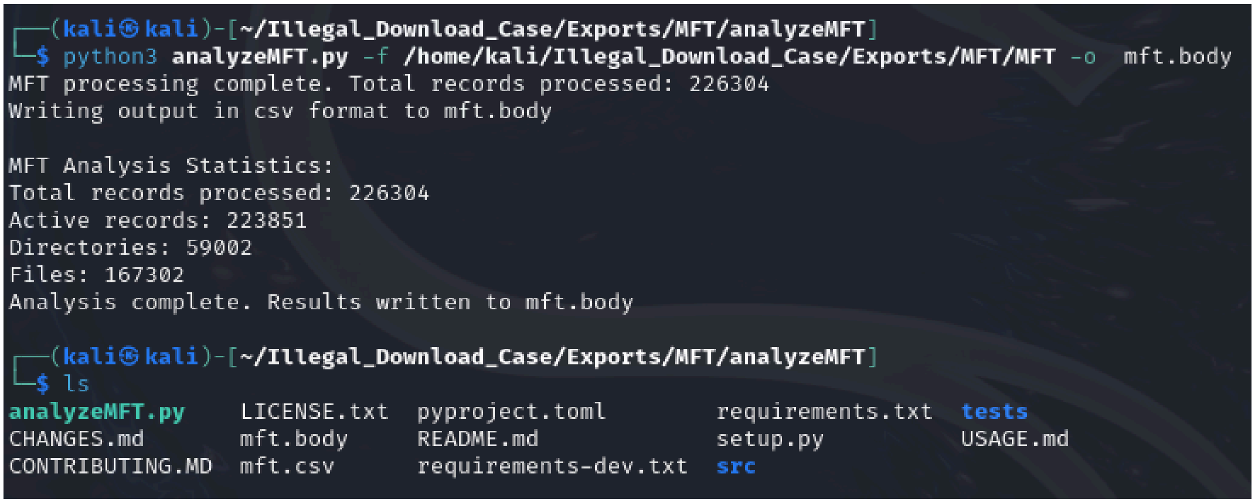


```
788064 788065 788066 788067 788068 788069 788070 788071
788072 788073 788074 788075 788076 788077 788078 788079

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ head -1 mft.csv | cut -d ',' -f 1,3,4,8 && cat mft.csv | grep -E 'Contraband|Sample-|List-|to
rrent-|Torrent' | cut -d ',' -f 1,3,4,8 | more -1
Record Number,Record Type,File Type,Filename
52901,In Use,File,Contraband.mp3
54027,In Use,File,Contraband.mp3.lnk
55271,In Use,File,Torrents.lnk
55634,In Use,File,Contraband.mp3.torrent
79927,In Use,File,Contraband.mp3.torrent
79968,In Use,File,Contraband.mp3
80800,In Use,File,Sample-1.mp3
83474,In Use,File,Contraband.lnk
83475,In Use,File,Torrent-Sources.lnk
93835,In Use,Directory,Torrent-Sources
97075,In Use,Directory,Torrents
97182,In Use,File,uTorrent.exe
205675,In Use,Directory,dlimagecache
205769,In Use,Directory,uTorrent
205772,In Use,File,uTorrent.exe
205774,In Use,File,maindoc.ico
--More--
```



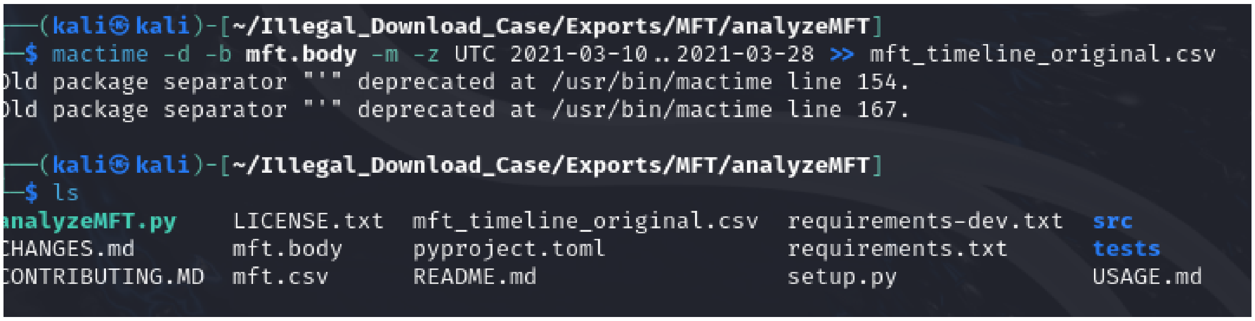
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ head -1 mft.csv | cut -d ',' -f 1,3,4,8 && cat mft.csv | grep -E 'Contraband|Sample-|List-|to
rrent-|Torrent' | cut -d ',' -f 1,3,4,8 | more -2
Record Number,Record Type,File Type,Filename
52901,In Use,File,Contraband.mp3
54027,In Use,File,Contraband.mp3.lnk
--More--
```

Generate a body file



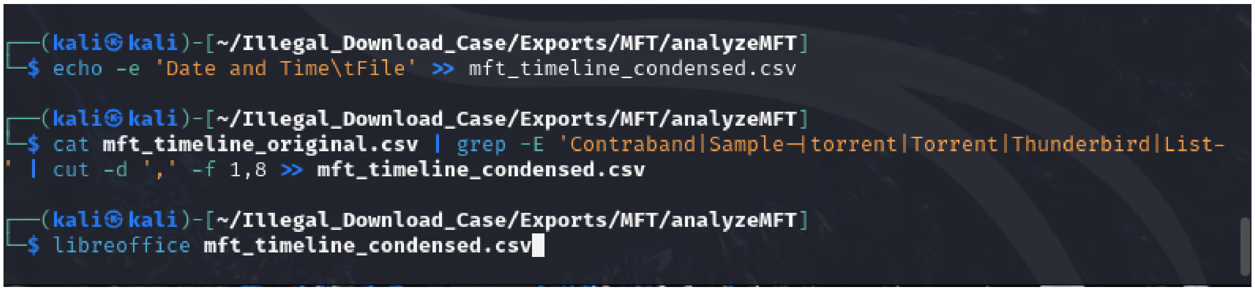
```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ python3 analyzeMFT.py -f /home/kali/Illegal_Download_Case/Exports/MFT/MFT -o  mft.body
MFT processing complete. Total records processed: 226304
Writing output in csv format to mft.body

MFT Analysis Statistics:
Total records processed: 226304
Active records: 223851
Directories: 59002
Files: 167302
Analysis complete. Results written to mft.body

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ ls
analyzeMFT.py    LICENSE.txt  pyproject.toml        requirements.txt  tests
CHANGES.md       mft.body     README.md             setup.py          USAGE.md
CONTRIBUTING.MD  mft.csv      requirements-dev.txt  src
```

Generate timeline of MFT entries



```
──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
─$ mactime -d -b mft.body -m -z UTC 2021-03-10..2021-03-28 >> mft_timeline_original.csv
Old package separator "'" deprecated at /usr/bin/mactime line 154.
Old package separator "'" deprecated at /usr/bin/mactime line 167.

──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
─$ ls
analyzeMFT.py    LICENSE.txt  mft_timeline_original.csv  requirements-dev.txt  src
CHANGES.md       mft.body     pyproject.toml             requirements.txt      tests
CONTRIBUTING.MD  mft.csv      README.md                  setup.py              USAGE.md
```

Analyze timeline



```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ echo -e 'Date and Time\tFile' >> mft_timeline_condensed.csv

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ cat mft_timeline_original.csv | grep -E 'Contraband|Sample-|torrent|Torrent|Thunderbird|List-
' | cut -d ',' -f 1,8 >> mft_timeline_condensed.csv

┌──(kali㉿kali)-[~/Illegal_Download_Case/Exports/MFT/analyzeMFT]
└─$ libreoffice mft_timeline_condensed.csv
```

Analyze timeline for files of interest in terminal