

Digital Forensics Experiments Report

Exp. 1

DD Command is one of the most basic and traditional command used to make a bit by bit copy of the drive/image.

We can mention the input file and the output file for copying the image.

dd if = /media/naman/h of = /mnt/f bs = 512

dd if = /mnt/f/image1.png of = /mnt/f/image2.png bs = 512

dd command can also be used for copying files.

Here bs = block size i.e. the amount of bytes it copies each time until all blocks are copied.

```
naman@LAPTOP-DL075JBE:/mnt/
naman@LAPTOP-DL075JBE:/mnt/e$ dd if=image1.png of=image3.png bs=512
25325+0 records in
25325+0 records out
12966400 bytes (13 MB, 12 MiB) copied, 40.516 s, 320 kB/s
naman@LAPTOP-DL075JBE:/mnt/e$
naman@LAPTOP-DL075JBE:/mnt/e$ dd -h
dd: invalid option -- 'h'
Try 'dd --help' for more information.
naman@LAPTOP-DL075JBE:/mnt/e$ dd --h
Usage: dd [OPERAND]...
or: dd OPTION
Copy a file, converting and formatting according to the operands.

bs=BYTES      read and write up to BYTES bytes at a time (default: 512);
               overrides ibs and obs
cbs=BYTES     convert BYTES bytes at a time
conv=CONVS    convert the file as per the comma separated symbol list
count=N       copy only N input blocks
ibs=BYTES     read up to BYTES bytes at a time (default: 512)
if=FILE       read from FILE instead of stdin
iflag=FLAGS   read as per the comma separated symbol list
obs=BYTES     write BYTES bytes at a time (default: 512)
of=FILE       write to FILE instead of stdout
oflag=FLAGS   write as per the comma separated symbol list
seek=N       skip N obs-sized blocks at start of output
skip=N        skip N ibs-sized blocks at start of input
status=LEVEL  The LEVEL of information to print to stderr;
               'none' suppresses everything but error messages,
               'noxfen' suppresses the final transfer statistics,
               'progress' shows periodic transfer statistics

N and BYTES may be followed by the following multiplicative suffixes:
c=1, m=2, b=512, kB=1000, K=1024, MB=1000*1000, M=1024*1024, XM=M,
GB=1000*1000*1000, G=1024*1024*1024, and so on for T, P, E, Z, Y.
Binary prefixes can be used, too: KiB=K, MiB=M, and so on.

Each CONV symbol may be:

ascii      from EBCDIC to ASCII
ebcdic     from ASCII to EBCDIC
lbn        from ASCII to alternate EBCDIC
block      pad newline-terminated records with spaces to cbs-size
unblock    replace trailing spaces in cbs-size records with newline
```

```
naman@LAPTOP-DL075JBE:/mnt/e$ ls
image1.png  dfr1f.dd  image3.png  output2  output6  'System Volume Information'
image2.png  fdisk.001  L0_Graphic.dd  output3_Fri_Oct_28_11_32_27_2020  output7_Fri_Oct_28_22_36_31_2020  Windows10log.txt
dfr10.dd   image1.png  nps-2009-canon2-gen1.E01  output4_Fri_Oct_28_13_45_15_2020  output8_Fri_Oct_28_23_23_2020
dfr11.dd   image2.png  output5
```

Exp. 2

DD Command for Data Carving.

DD can be used for data carving also. All we need to do is to specify a skip & count offset to tell it to start from the position we want to carve the data and how much to carve.

```
naman@LAPTOP-DL075JBE: /mnt/e
count_bytes treat 'count=N' as a byte count (iflag only)
skip_bytes treat 'skip=N' as a byte count (iflag only)
seek_bytes treat 'seek=N' as a byte count (oflag only)

Sending a USR1 signal to a running 'dd' process makes it
print I/O statistics to standard error and then resume copying.

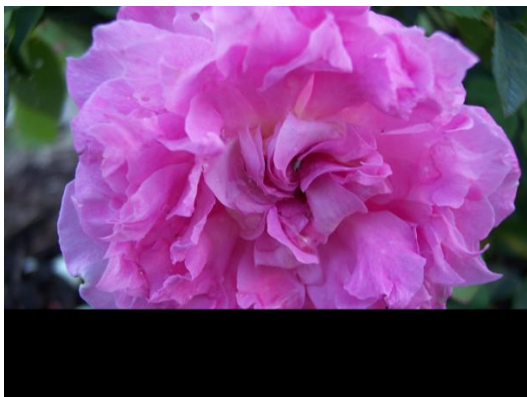
Options are:
--help      display this help and exit
--version   output version information and exit

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/dd>
or available locally via: info '(coreutils) dd invocation'
naman@LAPTOP-DL075JBE: /mnt/e$ dd if=L0_Graphic.dd of=image1.png bs=512 skip=10000 count=25325
25325+0 records in
25325+0 records out
12966400 bytes (13 MB, 12 MiB) copied, 34.1163 s, 380 kB/s
naman@LAPTOP-DL075JBE: /mnt/e$ dd if=L0_Graphic.dd of=image2.png bs=512 skip=10000 count=20000
20000+0 records in
20000+0 records out
10240000 bytes (10 MB, 9.8 MiB) copied, 30.3863 s, 337 kB/s
naman@LAPTOP-DL075JBE: /mnt/e$ ls
fdisk.001          seminar.pptx
image1.png         'System Volume Information'
image2.png         Windows.old
L0_Graphic.dd      Windows.oldupgrade
nps-2009-canon2-gen1.E01
naman@LAPTOP-DL075JBE: /mnt/e$
```

\$ dd if= L0_Graphic.dd of= image2.png bs= 512 count= 25325



\$ dd if= L0_Graphic.dd of= image2.png bs= 512 count= 20000



Exp. 3

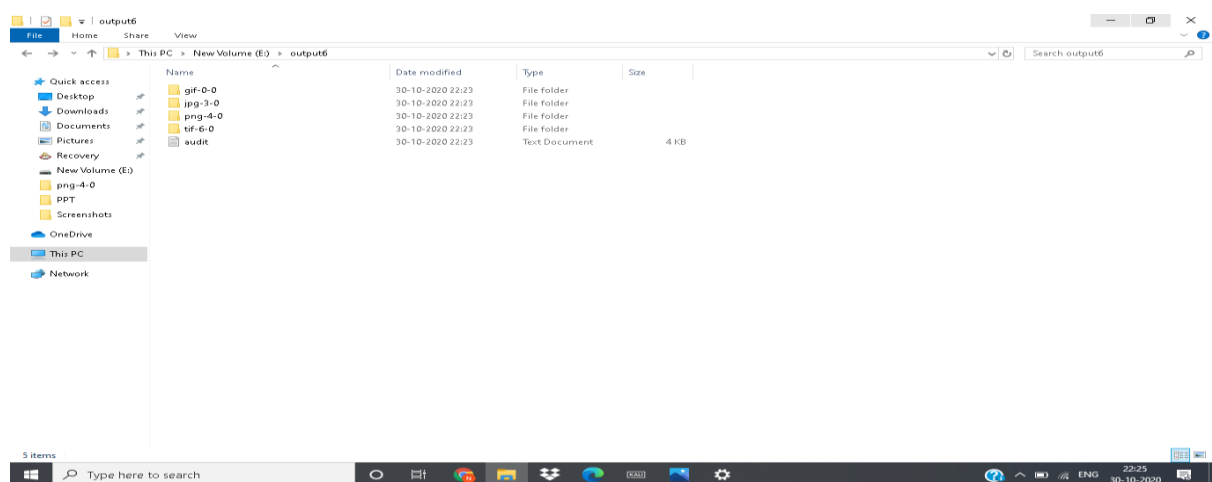
Scalpel is an open-source tool used for data carving. It has a config file which contains all the predefined headers which we need to uncomment in order to carve files of those formats.

1. Sudo apt-get install scalpel.
2. Nano /etc/scalpel/scalpel.config > Uncomment #jpg,#tif,#gif,#png
3. Scalpel -o output6 L0_Graphic.dd
(-o offset specifies the output file)

```
naman@LAPTOP-DL0753BE:/mnt/e$ scalpel -o output6 L0_Graphic.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/mnt/e/L0_Graphic.dd"

Image file pass 1/2.
L0_Graphic.dd: 100.0% |*****| 61.8
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built. Workload:
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 1 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x45\x78\x60\x66" and footer "\xff\xd9" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x4a\x46\x40\x46" and footer "\xff\xd9" --> 1 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 55 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 0 files
tif with header "\x49\x49\x2a\x00" and footer "" --> 1 files
tif with header "\x4d\x4d\x00\x2a" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
L0_Graphic.dd: 100.0% |*****| 61.8
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 58, elapsed = 10 seconds.
naman@LAPTOP-DL0753BE:/mnt/e$
```



audit - Notepad									
[scalpel version 1.60 audit fileStarted at Fri Oct 30 22:23:08 2020Command line:scalpel -o output6 L0_Graphic.dd Output directory: /mnt/e/output6Configuration file: /etc/scalpel/scalpel.confOpening target "H"The following files were carved:File									
File	Start	Chop	Length	Extracted From					
00000001.jpg	29133824	NO	60716	L0_Graphic.dd00000005.png	23742804	NO	12444764	L0_Graphic.dd	
00000004.png	23679912	NO	1250856	L0_Graphic.dd00000003.png	23630804	NO	1255584	L0_Graphic.dd	
00000002.png	23883373	NO	12883395	L0_Graphic.dd00000006.png	34614526	NO	1572242	L0_Graphic.dd	
00000007.png	34667068	NO	1519700	L0_Graphic.dd00000008.png	34690282	NO	1496486	L0_Graphic.dd	
00000009.png	34794612	NO	1392156	L0_Graphic.dd00000010.png	34965167	NO	1221601	L0_Graphic.dd	
00000011.png	34968798	NO	1217970	L0_Graphic.dd00000012.png	34982899	NO	1203869	L0_Graphic.dd	
00000013.png	35048484	NO	1138364	L0_Graphic.dd00000014.png	35084267	NO	1102501	L0_Graphic.dd	
00000015.png	35112553	NO	1074215	L0_Graphic.dd00000016.png	35119343	NO	1067425	L0_Graphic.dd	
00000017.png	35133963	NO	1052805	L0_Graphic.dd00000018.png	35134174	NO	1052594	L0_Graphic.dd	
00000019.png	35341795	NO	844973	L0_Graphic.dd00000020.png	35405847	NO	780921	L0_Graphic.dd	
00000021.png	35622690	NO	564078	L0_Graphic.dd00000022.png	35636746	NO	550022	L0_Graphic.dd	
00000023.png	35765286	NO	421482	L0_Graphic.dd00000024.png	35766394	NO	420374	L0_Graphic.dd	
00000025.png	36031286	NO	155482	L0_Graphic.dd00000026.png	36147955	NO	38013	L0_Graphic.dd	
00000027.png	36307134	NO	570691	L0_Graphic.dd00000028.png	36369735	NO	508090	L0_Graphic.dd	
00000029.png	36423869	NO	453956	L0_Graphic.dd00000030.png	36433898	NO	443927	L0_Graphic.dd	
00000031.png	36444800	NO	433025	L0_Graphic.dd00000032.png	36591165	NO	286660	L0_Graphic.dd	
00000033.png	36741140	NO	136685	L0_Graphic.dd00000034.png	36817373	NO	60452	L0_Graphic.dd	
00000035.png	37187510	NO	69368	L0_Graphic.dd00000036.png	37291603	NO	168852	L0_Graphic.dd	
00000037.png	37519180	NO	13552	L0_Graphic.dd00000038.png	37614117	NO	9609	L0_Graphic.dd	
00000039.png	37647399	NO	59231	L0_Graphic.dd00000040.png	38005887	NO	1055323	L0_Graphic.dd	
00000041.png	38049051	NO	1012159	L0_Graphic.dd00000042.png	38154581	NO	906629	L0_Graphic.dd	
00000043.png	38208068	NO	85142	L0_Graphic.dd00000044.png	38221277	NO	839933	L0_Graphic.dd	
00000045.png	38263092	NO	798118	L0_Graphic.dd00000046.png	38501888	NO	559322	L0_Graphic.dd	
00000047.png	38527437	NO	533773	L0_Graphic.dd00000048.png	38529837	NO	531373	L0_Graphic.dd	
00000049.png	38619511	NO	441699	L0_Graphic.dd00000050.png	38824894	NO	236316	L0_Graphic.dd	
00000051.png	38857480	NO	203730	L0_Graphic.dd00000052.png	38866596	NO	194614	L0_Graphic.dd	
00000053.png	38869987	NO	191223	L0_Graphic.dd00000054.png	38901164	NO	160046	L0_Graphic.dd	
00000055.png	38957671	NO	103539	L0_Graphic.dd00000056.png	39000796	NO	60414	L0_Graphic.dd	
00000057.tif	44547072	YES	20222465	L0_Graphic.dd00000000.gif	64636416	NO	36579	L0_Graphic.dd	
Completed at Fri Oct 30 22:23:17 2020									

Foremost :

It's also an open source tool for file carving like scalpel. It differs in it's output file an execution command offset.

\$ foremost -T jpeg,png,tif -o output8 -i L_0Graphic.dd

```

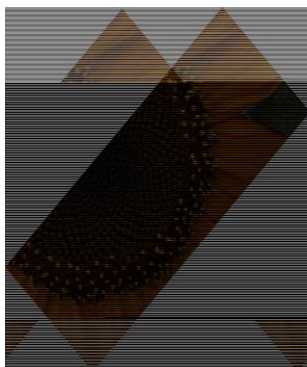
hamaan@LAPTOP-DL875JBE:/mnt/e$ foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w|-d] [-t <type>] [-s <blocks>] [-k <size>]
[-b <size>] [-c <file>] [-o <dir>] [-i <file>]

-v - display copyright information and exit
-t - specify file type. (-t jpeg,pdf ...)
-d - turn on indirect block detection (for UNIX file-systems)
-i - specify input file (default is stdin)
-a - Write all headers, perform no error detection (corrupted files)
-w - Only write the audit file, do not write any detected files to the disk
-o - set output directory (defaults to output)
-c - set configuration file to use (defaults to foremost.conf)
-q - enables quick mode. Search are performed on 512 byte boundaries.
-Q - enables quiet mode. Suppress output messages.
-v - verbose mode. Logs all messages to screen
hamaan@LAPTOP-DL875JBE:/mnt/e$ foremost -T jpeg,png,tif -o output7 -i nps-2009-canon2-gen1.E01
Processing: nps-2009-canon2-gen1.E01
[*]
hamaan@LAPTOP-DL875JBE:/mnt/e$ ls
00000001.jpg  dfrif.dd  L0_Graphic.dd  00000005.png  00000008.png  00000011.png  00000013.png  00000015.png  00000017.png  00000019.png  00000021.png  00000023.png  00000025.png  00000027.png  00000029.png  00000031.png  00000033.png  00000035.png  00000037.png  00000039.png  00000041.png  00000043.png  00000045.png  00000047.png  00000049.png  00000051.png  00000053.png  00000055.png  00000057.tif
00000004.png  fdisk.001  nps-2009-canon2-gen1.E01  00000003.png  00000006.png  00000010.png  00000012.png  00000014.png  00000016.png  00000018.png  00000020.png  00000022.png  00000024.png  00000026.png  00000028.png  00000030.png  00000032.png  00000034.png  00000036.png  00000038.png  00000040.png  00000042.png  00000044.png  00000046.png  00000048.png  00000050.png  00000052.png  00000054.png  00000056.png
dfrif0.dd  image1.png  00000007.png  00000009.png  00000011.png  00000013.png  00000015.png  00000017.png  00000019.png  00000021.png  00000023.png  00000025.png  00000027.png  00000029.png  00000031.png  00000033.png  00000035.png  00000037.png  00000039.png  00000041.png  00000043.png  00000045.png  00000047.png  00000049.png  00000051.png  00000053.png  00000055.png  00000057.tif
dfrif1.dd  image2.png  00000002.png  00000004.png  00000006.png  00000008.png  00000010.png  00000012.png  00000014.png  00000016.png  00000018.png  00000020.png  00000022.png  00000024.png  00000026.png  00000028.png  00000030.png  00000032.png  00000034.png  00000036.png  00000038.png  00000040.png  00000042.png  00000044.png  00000046.png  00000048.png  00000050.png  00000052.png  00000054.png
hamaan@LAPTOP-DL875JBE:/mnt/e$ foremost -T jpeg,png,tif -o output8 -i L_0Graphic.dd
Processing: L0_Graphic.dd
[*]
hamaan@LAPTOP-DL875JBE:/mnt/e$

```

audit - Notepad									
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick MikusAudit FileForemost started at Fri Oct 30 22:39:23 2020Invocation: foremost -T jpeg,png,tif -o output8 -i L0_Graphic.dd Output directory: /mnt/e/output8_Fri_Oct_30_22_39_23_2020Configuration file: /etc/foremost.conf									
Size	File	Offset	Comment	0:	00056902.jpg	59 KB	29133824	1:	00126243.gif
00010000.png	12 MB	5120000	(2580 x 1932)	Finish: Fri Oct 30 22:39:28 20203 FILES EXTRACTED	jpg:= 1gif:= 1png:= 1				
Foremost finished at Fri Oct 30 22:39:28 2020									

Outputs of Both :



The MFT Table is an important part of NTFS file system and contains the entry of each and every file on the drive which is crucial for any digital investigation. Each entry contains important attributes of the file like type, size, date/time of creation, date/time of most recent modification etc. are stored in MFT.

-
- The screenshot displays the AccessData FTK Imager 4.5.0.3 application window. The interface is divided into several panels:
- Evidence Tree:** Shows the file system structure of the mounted image. The root is 'New Volume [NTFS]' with a subdirectory 'root'. Under 'root', there are several folders including '\$BadClus', '\$Extend', '\$RECYCLE.BIN', '\$Secure', '\$UpCase', 'EDRAW', 'Evernote', 'flask', 'FTK Imager', 'Getting Started', 'obs-studio', 'sharding.svg', 'sign_original.jpg', and 'System Volume Information'.
 - File List:** A table listing files and directories within the selected volume. The columns are Name, Size, Type, and Date Modified. The file 'SMFT' is highlighted.
 - Properties:** A panel showing details for the selected file 'SMFT'. It includes fields for Name, File Class, File Size, Physical Size, Start Cluster, Date Accessed, Date Created, Date Modified, Encrypted, and Compressed.
 - Hex View:** A panel showing the raw data of the selected file 'SMFT' in hexadecimal and ASCII format.
- The File List table contains the following data:
- | Name | Size | Type | Date Modified |
|---------------------------------|--------|-------------------|---------------------|
| TypingMaster10 | 1 | Directory | 04-02-2020 18:05:06 |
| volatility3-master | 1 | Directory | 14-10-2020 10:36:54 |
| volatility_2.6_win64_standalone | 1 | Directory | 14-10-2020 04:26:44 |
| \$AttrDef | 3 | Regular File | 18-02-2015 15:49:26 |
| \$BadClus | 0 | Regular File | 18-02-2015 15:49:26 |
| \$Bitmap | 4,538 | Regular File | 18-02-2015 15:49:26 |
| \$Boot | 8 | Regular File | 18-02-2015 15:49:26 |
| \$ISO | 16 | NTFS Index All... | 27-10-2020 08:26:57 |
| \$LogFile | 65,536 | Regular File | 18-02-2015 15:49:26 |
| SMFT | 15,360 | Regular File | 18-02-2015 15:49:26 |
| SMFTMirr | 4 | Regular File | 18-02-2015 15:49:26 |
| \$Secure | 1 | Regular File | 18-02-2015 15:49:26 |
| STXF_DATA | 1 | NTFS Logged ... | 27-10-2020 08:26:57 |
- The Properties panel for 'SMFT' shows:
- Name: SMFT
 - File Class: Regular File
 - File Size: 15,728,640
 - Physical Size: 15,728,640
 - Start Cluster: 786,432
 - Date Accessed: 18-02-2015 15:49:26
 - Date Created: 18-02-2015 15:49:26
 - Date Modified: 18-02-2015 15:49:26
 - Encrypted: False
 - Compressed: False
- The Hex View panel shows the raw data of the file 'SMFT' in hexadecimal and ASCII format. The data starts with '000000' and continues with various hexadecimal values and their corresponding ASCII characters.

Drag a column header here to group by that column

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Rt
No image data	\$Extend	.	✓	□	2015-02-18 15:...		2015-02-18 15:...		2015-02-18 15:49:...		2
	\$RECYCLE.BIN	.	✓	□	2015-05-23 17:...		2017-07-14 23:...	2015-05-23 17:...	2017-07-14 23:58:...	2015-05-23 17:32:...	2
	EDRAW	.	✓	□	2019-04-22 10:...		2020-02-04 17:...	2020-02-04 17:...	2020-02-04 17:49:...	2019-04-22 10:41:...	2
	Evernote	.	✓	□	2019-05-23 12:...	2020-02-04 17:...	2020-02-04 17:...	2020-02-04 17:...	2020-02-04 17:49:...	2020-02-04 17:49:...	2
	flask	.	✓	□	2020-07-27 12:...		2020-07-27 12:...	2020-07-27 12:...	2020-07-27 12:30:...	2020-07-27 12:29:...	2
	FTK Imager	.	✓	□	2020-10-26 15:...		2020-10-26 15:...	2020-10-26 15:...	2020-10-26 15:29:...	2020-10-26 15:29:...	2
	Getting Started	.	✓	✓	2019-04-22 07:...		2020-10-27 08:...	2019-04-22 07:...	2020-10-27 08:26:...	2019-04-22 07:46:...	2
	obs-studio	.	✓	□	2020-09-24 07:...		2020-09-24 07:...	2020-09-24 07:25:...	2020-09-24 07:24:...		2

Properties: Copied, Has ADS, Is deleted, Is directory, Possible Timestamped

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Overview Details

Type: StandardInformation, Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, Content offset: 0x18, Resident: True

Flags: Hidden[System, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x0, Quota Charged: 0x0, Update Sequence #: 0x19EB0

Created On: 2015-02-18 15:49:26.6883576
Content Modified On: 2020-10-27 08:26:57.7293889
Record Modified On: 2020-10-27 08:26:57.7293889
Last Accessed On: 2020-10-27 08:26:57.7293889

File name: (Length: 0x1)
Flags: Hidden[System]IsDirectory, Name Type: DosWindows, Reparse Value: 0x0,

In the MFT file, We can see entries of all the files in F:/ drive even the deleted ones.(above image)

Now we analyse a deleted folder named “Getting Started” which contained some videos. We can see it’s entry in the MFT although it’s deleted. We can extract information/metadata about it.

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Rt
No image data	\$Extend	.	✓	□	2015-02-18 15:...		2015-02-18 15:...		2015-02-18 15:49:...		2
	\$RECYCLE.BIN	.	✓	□	2015-05-23 17:...		2017-07-14 23:...	2015-05-23 17:...	2017-07-14 23:58:...	2015-05-23 17:32:...	2
	EDRAW	.	✓	□	2019-04-22 10:...		2020-02-04 17:...	2020-02-04 17:...	2020-02-04 17:49:...	2019-04-22 10:41:...	2
	Evernote	.	✓	□	2019-05-23 12:...	2020-02-04 17:...	2020-02-04 17:...	2020-02-04 17:...	2020-02-04 17:49:...	2020-02-04 17:49:...	2
	flask	.	✓	□	2020-07-27 12:...		2020-07-27 12:...	2020-07-27 12:...	2020-07-27 12:30:...	2020-07-27 12:29:...	2
	FTK Imager	.	✓	□	2020-10-26 15:...		2020-10-26 15:...	2020-10-26 15:...	2020-10-26 15:29:...	2020-10-26 15:29:...	2
	Getting Started	.	✓	✓	2019-04-22 07:...		2020-10-27 08:...	2019-04-22 07:...	2020-10-27 08:26:...	2019-04-22 07:46:...	2
	obs-studio	.	✓	□	2020-09-24 07:...		2020-09-24 07:...	2020-09-24 07:25:...	2020-09-24 07:24:...		2

Properties: Copied, Has ADS, Is deleted, Is directory, Possible Timestamped

Current offset: 242 (0xF2) Bytes selected: 29 (0x1D)

Overview Details

Type: StandardInformation, Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, Content offset: 0x18, Resident: True

Flags: None, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x1D, Quota Charged: 0x0, Update Sequence #: 0x18D688

Created On: 2019-04-22 07:46:49.2965393
Content Modified On: 2020-10-27 08:26:23.7076403
Record Modified On: 2020-10-27 08:26:23.7076403
Last Accessed On: 2020-10-27 08:26:23.7076403

File name: Getting Started (Length: 0xF)
Flags: IsDirectory, Name Type: Posix, Reparse Value: 0x0, Physical Size: 0x0, Logical Size: 0x0
Parent Mft Record: Entry/seq: 0x5-0x5

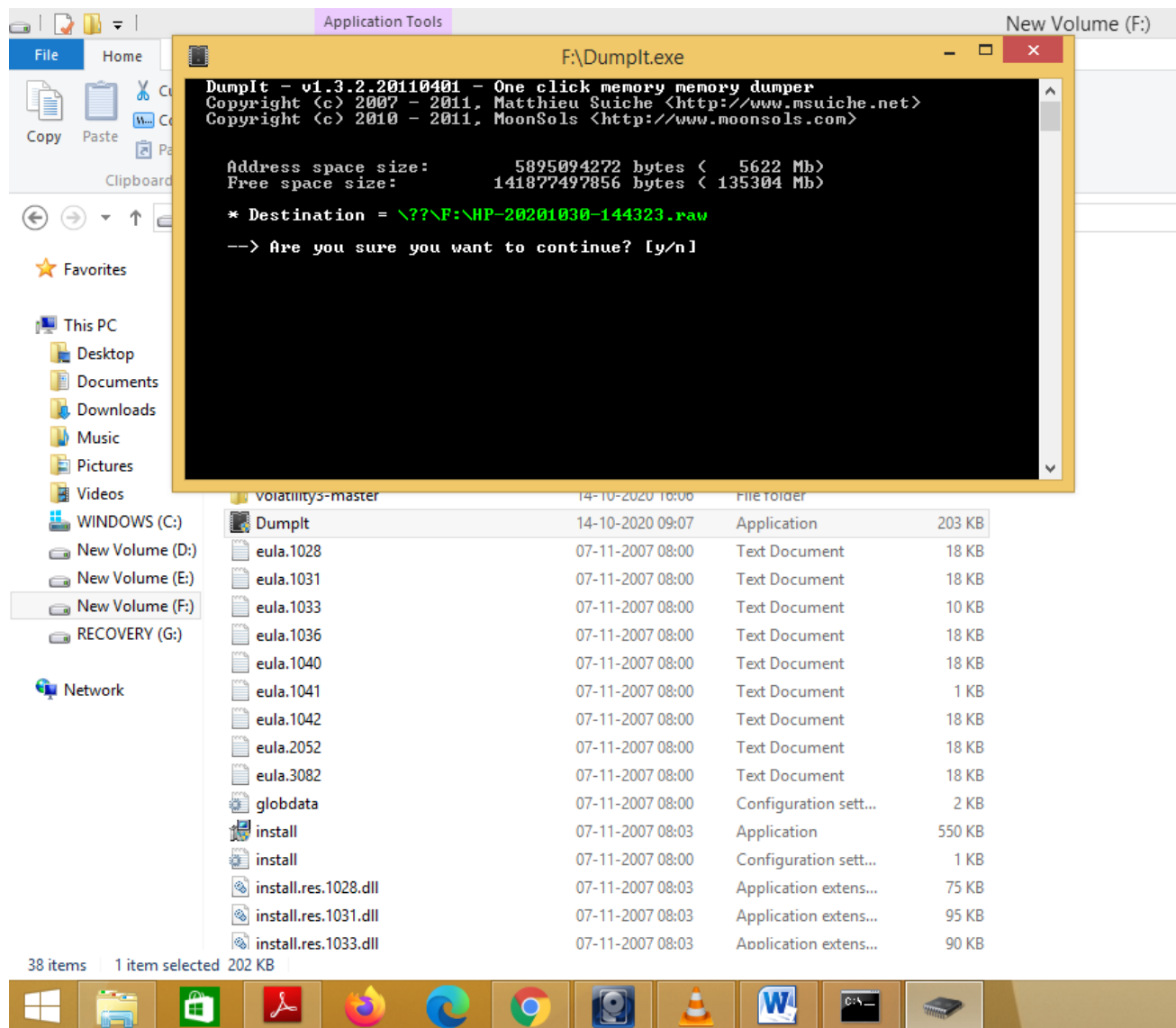
Created On: 2019-04-22 07:46:49.2965393
Content Modified On: 2019-04-22 07:46:49.2965393
Record Modified On: 2019-04-22 07:46:49.2965393
Last Accessed On: 2019-04-22 07:46:49.2965393

We clearly see that the entries in **SI attribute(0x10)** have changed but the entries in **FN attribute(0x30)** have not changed and remain as it is. Also the name of the folder is stored in MFT entry.

Exp. 5 Using DumpIt.exe we capture the RAM image. We can then use it for forensic analysis using Volatility tool.

Dumpit is a free tool which is easy to use.

1. Download Dumpit.exe from Github
2. Open Dumpit.exe
3. Check the destination folder.
4. Type y to make the image.



Exp.6 Volatility 3 as it's name suggests is a volatile memory (RAM) Analysis tool. It's written in python. It takes as input the RAM image and has different command to show different details like Basic active process listing, terminated processes scan etc.

The major commands are :

1. Python vol.py -f HP-20201014-033903.raw windows.psscan.PsScan

This cmd shows Basic active process listing along with scanning for hidden or terminated pr

C:\Windows\system32\cmd.exe

```
C:\volatility3-master>python vol.py -f HP-20201014-033903.raw windows.psscan.PsScan
Volatility 3 Framework 1.2.1-beta.1
Progress: 0.00
```

ID	PPID	ImageFileName	Offset	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	Dumped
0	0	System	0x0	0	0	0	N/A	00000000	00000000	False
4	0	smss.exe	0x0	1	0	0	N/A	00000000	00000000	False
8	4	svchost.exe	0x0	1	0	0	N/A	00000000	00000000	False
12	8	taskhost.exe	0x0	1	0	0	N/A	00000000	00000000	False
16	12	WmiProcSE.exe	0x0	1	0	0	N/A	00000000	00000000	False
20	16	chrome.exe	0x0	1	0	0	N/A	00000000	00000000	False
24	20	SearchProtocol	0x0	1	0	0	N/A	00000000	00000000	False
28	24	Teams.exe	0x0	1	0	0	N/A	00000000	00000000	False
32	28	explorer.exe	0x0	1	0	0	N/A	00000000	00000000	False
36	32	tiworker.exe	0x0	1	0	0	N/A	00000000	00000000	False
40	36	igfxEM.exe	0x0	1	0	0	N/A	00000000	00000000	False
44	40	Teams.exe	0x0	1	0	0	N/A	00000000	00000000	False
48	44	TouchpointAnal	0x0	1	0	0	N/A	00000000	00000000	False
52	48	taskeng.exe	0x0	1	0	0	N/A	00000000	00000000	False
56	52	HPSupportSolut	0x0	1	0	0	N/A	00000000	00000000	False
60	56	SearchFilterHo	0x0	1	0	0	N/A	00000000	00000000	False
64	60	OPBHOBroker.ex	0x0	1	0	0	N/A	00000000	00000000	False
68	64	audiodg.exe	0x0	1	0	0	N/A	00000000	00000000	False
72	68	Teams.exe	0x0	1	0	0	N/A	00000000	00000000	False
76	72	igfxHK.exe	0x0	1	0	0	N/A	00000000	00000000	False
80	80	MSOSYNC.EXE	0x0	1	0	0	N/A	00000000	00000000	False
84	84	MpCmdRun.exe	0x0	1	0	0	N/A	00000000	00000000	False
88	88	IAStorDataMgr\$	0x0	1	0	0	N/A	00000000	00000000	False
92	92	OPBHOBrokerDsk	0x0	1	0	0	N/A	00000000	00000000	False
96	96	SynTPEnh.exe	0x0	1	0	0	N/A	00000000	00000000	False
100	100	chrome.exe	0x0	1	0	0	N/A	00000000	00000000	False
104	104	RAVBg64.exe	0x0	1	0	0	N/A	00000000	00000000	False
108	108	Dumplt.exe	0x0	1	0	0	N/A	00000000	00000000	False
112	112	chrome.exe	0x0	1	0	0	N/A	00000000	00000000	False
116	116	HPSF.exe	0x0	1	0	0	N/A	00000000	00000000	False
120	120	csrss.exe	0x0	1	0	0	N/A	00000000	00000000	False
124	124	Teams.exe	0x0	1	0	0	N/A	00000000	00000000	False
128	128	dwm.exe	0x0	1	0	0	N/A	00000000	00000000	False
132	132	Teams.exe	0x0	1	0	0	N/A	00000000	00000000	False
136	136	RuntimeBroker.	0x0	1	0	0	N/A	00000000	00000000	False
140	140	WmiProcSE.exe	0x0	1	0	0	N/A	00000000	00000000	False
144	144	winlogon.exe	0x0	1	0	0	N/A	00000000	00000000	False
148	148	MicrosoftEdgeU	0x0	1	0	0	N/A	00000000	00000000	False
152	152	taskhost.exe	0x0	1	0	0	N/A	00000000	00000000	False
156	156	svchost.exe	0x0	1	0	0	N/A	00000000	00000000	False
160	160	TrustedInstall	0x0	1	0	0	N/A	00000000	00000000	False
164	164	chrome.exe	0x0	1	0	0	N/A	00000000	00000000	False
168	168	MALLABStartupA	0x0	1	0	0	N/A	00000000	00000000	False
172	172	SynTPEnh.exe	0x0	1	0	0	N/A	00000000	00000000	False
176	176	SynTPEnh.exe	0x0	1	0	0	N/A	00000000	00000000	False
180	180	wininit.exe	0x0	1	0	0	N/A	00000000	00000000	False
184	184	opvapp.exe	0x0	1	0	0	N/A	00000000	00000000	False
188	188	Teams.exe	0x0	1	0	0	N/A	00000000	00000000	False
192	192	smss.exe	0x0	1	0	0	N/A	00000000	00000000	False
196	196	svchost.exe	0x0	1	0	0	N/A	00000000	00000000	False
200	200	conhost.exe	0x0	1	0	0	N/A	00000000	00000000	False
204	204	Teams.exe	0x0	1	0	0	N/A	00000000	00000000	False

As here we can see, PID = Process ID, PPID = Parent PID, No. of thread by each process, start time, end time, Session Id.

System has PPID = 0, as it's the first process to start.

System has Session ID = N/A because the System starts before sessions are established.

2. Python vol.py -f HP-20201014-033903.raw windows.pslist.PsList

This shows basic active process listing.

C:\Windows\system32\cmd.exe

F:\volatility3-master>python vol.py -f HP-20201014-033903.raw windows.pslist.PsList

Volatility 3 Framework 1.2.1-beta.1

Progress: 0.00

PID	PPID	ImageFileName	Offset(U)	Scanning primary2	using Threads	PdbSignatureScanner	Handles	SessionId	Wow64	CreateTime	ExitTime	Dumped
4	0	System	0xe001e3e998c0	140	-	N/A	False	2020-10-13 14:20:37.000000	N/A	False		
336	4	smss.exe	0xe001e7e21380	2	-	N/A	False	2020-10-13 14:20:37.000000	N/A	False		
484	432	csrss.exe	0xe001e97e9380	9	-	0	False	2020-10-13 14:20:45.000000	N/A	False		
544	432	wininit.exe	0xe001e7d11080	1	-	0	False	2020-10-13 14:20:45.000000	N/A	False		
608	544	services.exe	0xe001e84428c0	5	-	0	False	2020-10-13 14:20:46.000000	N/A	False		
616	544	lsass.exe	0xe001e8470480	5	-	0	False	2020-10-13 14:20:46.000000	N/A	False		
756	608	svchost.exe	0xe001e84ac8c0	10	-	0	False	2020-10-13 14:20:49.000000	N/A	False		
788	608	svchost.exe	0xe001e84a88c0	9	-	0	False	2020-10-13 14:20:49.000000	N/A	False		
904	608	OmniServ.exe	0xe001ec32f8c0	5	-	0	False	2020-10-13 14:20:49.000000	N/A	False		
956	608	svchost.exe	0xe001ec37c180	23	-	0	False	2020-10-13 14:20:51.000000	N/A	False		
984	608	svchost.exe	0xe001e7f33180	50	-	0	False	2020-10-13 14:20:51.000000	N/A	False		
1008	608	svchost.exe	0xe001ec3c78c0	22	-	0	False	2020-10-13 14:20:51.000000	N/A	False		
376	608	igfxCUIService	0xe001ebdb8840	5	-	0	False	2020-10-13 14:20:52.000000	N/A	False		
500	608	svchost.exe	0xe001ebdb5080	20	-	0	False	2020-10-13 14:20:52.000000	N/A	False		
848	608	RtkAudioServic	0xe001ebfa3580	4	-	0	False	2020-10-13 14:20:54.000000	N/A	False		
1068	608	svchost.exe	0xe001ec43d8c0	18	-	0	False	2020-10-13 14:20:54.000000	N/A	False		
1200	500	wlanext.exe	0xe001ec4ad8c0	7	-	0	False	2020-10-13 14:20:55.000000	N/A	False		
1212	1200	conhost.exe	0xe001ec4a8500	1	-	0	False	2020-10-13 14:20:55.000000	N/A	False		
1316	608	spoolsv.exe	0xe001ec4cb340	14	-	0	False	2020-10-13 14:20:56.000000	N/A	False		
1340	608	svchost.exe	0xe001ec5328c0	22	-	0	False	2020-10-13 14:20:56.000000	N/A	False		
1500	608	armsvc.exe	0xe001ec5d88c0	2	-	0	True	2020-10-13 14:20:57.000000	N/A	False		
1536	608	ALERTSR64.exe	0xe001ebcda8c0	2	-	0	False	2020-10-13 14:20:58.000000	N/A	False		
1552	608	svchost.exe	0xe001ec5da8c0	6	-	0	False	2020-10-13 14:20:58.000000	N/A	False		
1568	608	HealthMon.exe	0xe001ec6a52c0	2	-	0	True	2020-10-13 14:20:58.000000	N/A	False		
1620	608	mDNSResponder.	0xe001ec58b8c0	2	-	0	False	2020-10-13 14:20:59.000000	N/A	False		
1636	608	BTDevMgr.exe	0xe001ec66c2c0	2	-	0	False	2020-10-13 14:20:59.000000	N/A	False		
1660	608	svchost.exe	0xe001ec70d8c0	13	-	0	False	2020-10-13 14:20:59.000000	N/A	False		
1696	608	HPWMISUC.exe	0xe001ec6ee380	2	-	0	True	2020-10-13 14:20:59.000000	N/A	False		
1728	608	mongod.exe	0xe001ec7098c0	30	-	0	False	2020-10-13 14:20:59.000000	N/A	False		
1788	608	mosquitto.exe	0xe001ec6fd8c0	1	-	0	False	2020-10-13 14:21:01.000000	N/A	False		
1804	608	mysqld.exe	0xe001ec84c8c0	3	-	0	False	2020-10-13 14:21:01.000000	N/A	False		
1824	1804	mysqld.exe	0xe001ec7308c0	39	-	0	False	2020-10-13 14:21:02.000000	N/A	False		
1836	1824	conhost.exe	0xe001ec72d8c0	2	-	0	False	2020-10-13 14:21:02.000000	N/A	False		
1876	608	RichVideo64.ex	0xe001ec7338c0	2	-	0	False	2020-10-13 14:21:02.000000	N/A	False		
1952	608	SynTPEnhServic	0xe001ec73c8c0	2	-	0	False	2020-10-13 14:21:03.000000	N/A	False		
1976	608	svchost.exe	0xe001ec88d8c0	2	-	0	False	2020-10-13 14:21:03.000000	N/A	False		
2036	608	Lavasoft.WCAss	0xe001ec7428c0	9	-	0	False	2020-10-13 14:21:03.000000	N/A	False		
2056	608	MsMpEng.exe	0xe001ec73f8c0	24	-	0	False	2020-10-13 14:21:07.000000	N/A	False		
2984	608	NisSrv.exe	0xe001eccad8c0	8	-	0	False	2020-10-13 14:22:36.000000	N/A	False		
1672	608	svchost.exe	0xe001ec660540	6	-	0	False	2020-10-13 14:22:36.000000	N/A	False		
2600	608	svchost.exe	0xe001e7b5c080	3	-	0	False	2020-10-13 14:22:36.000000	N/A	False		
1648	1952	SynTPEnh.exe	0xe001e7c158c0	0	-	1	False	2020-10-13 14:22:43.000000	2020-10-13 14:41:58.000000			
1704	608	PresentationFo	0xe001ecb09080	4	-	0	False	2020-10-13 14:22:43.000000	N/A	False		
3532	608	svchost.exe	0xe001ec7208c0	9	-	0	False	2020-10-13 14:22:48.000000	N/A	False		
3664	608	SearchIndexer.	0xe001eca04080	11	-	0	False	2020-10-13 14:22:49.000000	N/A	False		
3868	608	HPSupportSolut	0xe001e44a8080	8	-	0	False	2020-10-13 14:24:37.000000	N/A	False		
5056	608	TouchpointAnal	0xe001e44298c0	11	-	0	False	2020-10-13 14:24:48.000000	N/A	False		
2384	608	IAStorDataMgrS	0xe001e4702080	6	-	0	True	2020-10-13 14:25:13.000000	N/A	False		
3556	984	HPSF.exe	0xe001e47d38c0	0	-	1	False	2020-10-13 14:26:44.000000	2020-10-13 14:27:15.000000			
4740	4764	chrome.exe	0xe001e508c4c0	0	-	1	False	2020-10-13 14:28:24.000000	2020-10-13 14:40:36.000000			
316	984	taskhost.exe	0xe001e7b50740	10	-	0	False	2020-10-13 14:35:56.000000	N/A	False		
3556	984	HPSF.exe	0xe001e47d38c0	0	-	1	False	2020-10-13 14:26:44.000000	2020-10-13 14:27:15.000000			

Here we can see some processes (hidden processes) as compared to last one.

3. Python vol.py -f HP-20201014-033903.raw windows.pstree.PsTree

This shows processes in parent-child tree format.

Here we can see parent processes and child processes clearly with starts as levels o f=f the child tree.

System is the parent process.

Services is a parent process which has so many children.

C:\Windows\system32\cmd.exe										
F:\volatility3-master>python vol.py -f HP-20201014-033903.raw windows.pstree.PsTree										
Volatility 3 Framework 1.2.1-beta.1										
Progress: 0.00										
PID	PPID	ImageFileName	Offset(U)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	
4	0	System	0xe001e51634c0	140	-	N/A	False	2020-10-13 14:20:37.000000	N/A	
* 336	4	smss.exe	0xe001e51634c0	2	-	0	False	2020-10-13 14:20:37.000000	N/A	
484	432	csrss.exe	0xe001e51634c0	9	-	0	False	2020-10-13 14:20:45.000000	N/A	
544	432	wininit.exe	0xe001e51634c0	1	-	0	False	2020-10-13 14:20:45.000000	N/A	
* 608	544	services.exe	0xe001e51634c0	5	-	0	False	2020-10-13 14:20:46.000000	N/A	
** 1536	608	AERTSr64.exe	0xe001e51634c0	2	-	0	False	2020-10-13 14:20:58.000000	N/A	
** 904	608	OmniServ.exe	0xe001e51634c0	5	-	0	False	2020-10-13 14:20:49.000000	N/A	
** 2056	608	MsMpEng.exe	0xe001e51634c0	24	-	0	False	2020-10-13 14:21:07.000000	N/A	
** 1672	608	svchost.exe	0xe001e51634c0	6	-	0	False	2020-10-13 14:22:36.000000	N/A	
** 5000	608	TrustedInstall	0xe001e51634c0	6	-	0	False	2020-10-14 03:37:37.000000	N/A	
** 1804	608	mysqld.exe	0xe001e51634c0	3	-	0	False	2020-10-13 14:21:01.000000	N/A	
*** 1824	1804	mysqld.exe	0xe001e51634c0	39	-	0	False	2020-10-13 14:21:02.000000	N/A	N/A
**** 1836	1824	conhost.exe	0xe001e51634c0	2	-	0	False	2020-10-13 14:21:02.000000	N/A	N/A
** 1552	608	svchost.exe	0xe001e51634c0	6	-	0	False	2020-10-13 14:20:58.000000	N/A	
** 788	608	svchost.exe	0xe001e51634c0	9	-	0	False	2020-10-13 14:20:49.000000	N/A	
** 3868	608	HPSupportSolut	0xe001e51634c0	8	-	0	False	2020-10-13 14:24:37.000000	N/A	
** 1568	608	HealthMon.exe	0xe001e51634c0	2	-	0	True	2020-10-13 14:20:58.000000	N/A	
** 1696	608	HPWMISUC.exe	0xe001e51634c0	2	-	0	True	2020-10-13 14:20:59.000000	N/A	
** 1952	608	SynTPEnhServic	0xe001e51634c0	2	-	0	False	2020-10-13 14:21:03.000000	N/A	
*** 1648	1952	SynTPEnh.exe	0xe001e51634c0	0	-	1	False	2020-10-13 14:22:43.000000		2020-
*** 2488	1952	SynTPEnh.exe	0xe001e51634c0	8	-	2	False	2020-10-14 03:34:35.000000		N/A
**** 1124	2488	SynTPEnh.exe	0xe001e51634c0	0	-	2	False	2020-10-14 03:34:35.000000		2020-
***** 4320	1124	SynTPHelper.ex	0xe001e51634c0	1	-	2	False	2020-10-14 03:34:35.000000		N/A
*** 5568	1952	SynTPEnh.exe	0xe001e51634c0	0	-	1	False	2020-10-13 14:41:58.000000		2020-
** 1316	608	spoolsv.exe	0xe001e51634c0	14	-	0	False	2020-10-13 14:20:56.000000	N/A	
** 1788	608	mosquitto.exe	0xe001e51634c0	1	-	0	False	2020-10-13 14:21:01.000000	N/A	
** 2984	608	NisSrv.exe	0xe001e51634c0	8	-	0	False	2020-10-13 14:22:36.000000	N/A	
** 2600	608	svchost.exe	0xe001e51634c0	3	-	0	False	2020-10-13 14:22:36.000000	N/A	
** 1704	608	PresentationFo	0xe001e51634c0	4	-	0	False	2020-10-13 14:22:43.000000	N/A	
** 1068	608	svchost.exe	0xe001e51634c0	18	-	0	False	2020-10-13 14:20:54.000000	N/A	
** 5684	608	svchost.exe	0xe001e51634c0	5	-	0	False	2020-10-14 03:36:52.000000	N/A	
** 1976	608	svchost.exe	0xe001e51634c0	2	-	0	False	2020-10-13 14:21:03.000000	N/A	
** 1340	608	svchost.exe	0xe001e51634c0	22	-	0	False	2020-10-13 14:20:56.000000	N/A	
** 956	608	svchost.exe	0xe001e51634c0	23	-	0	False	2020-10-13 14:20:51.000000	N/A	
*** 3624	956	audiody.exe	0xe001e51634c0	4	-	0	False	2020-10-14 03:35:48.000000		N/A
** 1728	608	mongod.exe	0xe001e51634c0	30	-	0	False	2020-10-13 14:20:59.000000	N/A	
** 5056	608	TouchpointAnal	0xe001e51634c0	11	-	0	False	2020-10-13 14:24:48.000000	N/A	
** 3532	608	svchost.exe	0xe001e51634c0	9	-	0	False	2020-10-13 14:22:48.000000	N/A	
** 848	608	RtkAudioServic	0xe001e51634c0	4	-	0	False	2020-10-13 14:20:54.000000	N/A	
*** 5740	848	RAUBg64.exe	0xe001e51634c0	4	-	2	False	2020-10-14 03:34:34.000000		N/A
** 3664	608	SearchIndexer.	0xe001e51634c0	11	-	0	False	2020-10-13 14:22:49.000000	N/A	
*** 2872	3664	SearchFilterHo	0xe001e51634c0	1	-	0	False	2020-10-14 03:37:09.000000		N/A
**** 212	3664	SearchProtocol	0xe001e51634c0	4	-	0	False	2020-10-14 03:37:09.000000	N/A	
** 2384	608	IAStorDataMgrS	0xe001e51634c0	6	-	0	True	2020-10-13 14:25:13.000000	N/A	
** 1620	608	mDNSResponder.	0xe001e51634c0	2	-	0	False	2020-10-13 14:20:59.000000	N/A	
** 1876	608	RichVideo64.ex	0xe001e51634c0	2	-	0	False	2020-10-13 14:21:02.000000	N/A	
** 984	608	svchost.exe	0xe001e51634c0	50	-	0	False	2020-10-13 14:20:51.000000	N/A	
*** 3556	984	HPSPF.exe	0xe001e51634c0	0	-	1	False	2020-10-13 14:26:44.000000		2020-
*** 5412	984	taskhostex.exe	0xe001e51634c0	9	-	2	False	2020-10-14 03:34:35.000000		N/A
*** 5444	984	taskeng.exe	0xe001e51634c0	3	-	0	False	2020-10-14 03:34:35.000000		N/A
**** 3152	5444	MATLABStartupA	0xe001e51634c0	1	-	0	False	2020-10-14 03:34:35.000000		N/A
** 1704	608	PresentationFo	0xe001e51634c0	4	-	0	False	2020-10-13 14:22:43.000000	N/A	

- Python vol.py -f HP-20201014-033903.raw windows.dllicst.DllList -pid 5940
Shows list of all processes used by the process with -pid mentioned.
Here the output shows the list of DLLs used by Microsoft Teams.exe pid = 5940.

C:\Windows\system32\cmd.exe									
PID	Process Base	Size	Name	Path	LoadTime	Dumped			
5940	Teams.exe	0x7ff6d4b0000	0x58b1000	Teams.exe	C:\Users\home\AppData\Local\Microsoft\Teams\current\Teams.exe	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6ce0000	0x1ad000	ntdll.dll	C:\Windows\SYSTEM32\ntdll.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6050000	0x13f000	KERNEL32.DLL	C:\Windows\system32\KERNEL32.DLL	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4240000	0x115000	KERNELBASE.dll	C:\Windows\system32\KERNELBASE.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6b00000	0x31c000	ffmpeg.dll	C:\Users\home\AppData\Local\Microsoft\Teams\current\ffmpeg.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf1600000	0x27b000	COMCTL32.dll	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9600.1	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf43d0000	0xaa000	ADVAPI32.dll	C:\Windows\system32\ADVAPI32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf63b0000	0x14d000	GDI32.dll	C:\Windows\system32\GDI32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6500000	0xc7000	OLEAUT32.dll	C:\Windows\system32\OLEAUT32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4360000	0x7000	PSAPI.DLL	C:\Windows\system32\PSAPI.DLL	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4840000	0x152e000	SHELL32.dll	C:\Windows\system32\SHELL32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4480000	0x177000	USER32.dll	C:\Windows\system32\USER32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec8e0000	0x4ac000	WININET.dll	C:\Windows\SYSTEM32\WININET.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec8ba0000	0x22000	WINMM.dll	C:\Windows\SYSTEM32\WINMM.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6190000	0x5a000	WS2_32.dll	C:\Windows\system32\WS2_32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf68a0000	0x195000	ole32.dll	C:\Windows\system32\ole32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf2060000	0x2a000	IPHLAPI.DLL	C:\Windows\SYSTEM32\IPHLAPI.DLL	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfecf50000	0x6a000	OLEACC.dll	C:\Windows\SYSTEM32\OLEACC.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6b00000	0xd000	msdmo.dll	C:\Windows\SYSTEM32\msdmo.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf2ff0000	0xd000	HID.DLL	C:\Windows\SYSTEM32\HID.DLL	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6b00000	0xb6000	COMDLG32.dll	C:\Windows\system32\COMDLG32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec440000	0x189000	dbghep.dll	C:\Windows\SYSTEM32\dbghep.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec3a0000	0xa000	VERSION.dll	C:\Windows\SYSTEM32\VERSION.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4370000	0x54000	SHLWAPI.dll	C:\Windows\system32\SHLWAPI.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf43d0000	0x21000	USERENV.dll	C:\Windows\system32\USERENV.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec00000	0x17f000	PROPSYS.dll	C:\Windows\SYSTEM32\PROPSYS.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6b00000	0x16000	USP10.dll	C:\Windows\SYSTEM32\USP10.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfecf0000	0x1ec000	DWrite.dll	C:\Windows\SYSTEM32\DWrite.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf65f0000	0x36000	IMM32.dll	C:\Windows\system32\IMM32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf1b70000	0x21000	dumapi.dll	C:\Windows\SYSTEM32\dumapi.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf2020000	0x12000	WTSAPI32.dll	C:\Windows\SYSTEM32\WTSAPI32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec6a0000	0x82000	WINSPOOL.DRV	C:\Windows\SYSTEM32\WINSPOOL.DRV	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfecb0000	0xc9000	WINHTTP.dll	C:\Windows\SYSTEM32\WINHTTP.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf1ac0000	0x87000	dxgi.dll	C:\Windows\SYSTEM32\dxgi.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf48c10000	0x221000	d3d9.dll	C:\Windows\SYSTEM32\d3d9.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4920000	0x24000	dxva2.dll	C:\Windows\SYSTEM32\dxva2.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf1de0000	0x233000	d3d11.dll	C:\Windows\SYSTEM32\d3d11.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec90000	0x85000	ver.dll	C:\Windows\SYSTEM32\ver.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4060000	0x1df000	CRYPT32.dll	C:\Windows\system32\CRYPT32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfed0e0000	0x18a000	urlmon.dll	C:\Windows\SYSTEM32\urlmon.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf2090000	0xc000	Secur32.dll	C:\Windows\SYSTEM32\Secur32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4310000	0x25000	ncrypt.dll	C:\Windows\SYSTEM32\ncrypt.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec2d0000	0x1a000	dhcpcsvc.DLL	C:\Windows\SYSTEM32\dhcpcsvc.DLL	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfed70000	0x135000	UIAutomationCore.DLL	C:\Windows\SYSTEM32\UIAutomationCore.DLL	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf20a0000	0x7000	MSIMC32.dll	C:\Windows\SYSTEM32\MSIMC32.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf2a70000	0x129000	UxTheme.dll	C:\Windows\SYSTEM32\UxTheme.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6c30000	0xaa000	msvcrt.dll	C:\Windows\system32\msvcrt.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf4670000	0x50000	sechost.dll	C:\Windows\SYSTEM32\sechost.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6920000	0x140000	RPCRT4.dll	C:\Windows\system32\RPCRT4.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf65d0000	0x211000	combase.dll	C:\Windows\system32\combase.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfec0e0000	0x2cc000	iertutil.dll	C:\Windows\SYSTEM32\iertutil.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcfecb70000	0x2a000	WINMMBASE.dll	C:\Windows\SYSTEM32\WINMMBASE.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf6c20000	0x9000	NSI.dll	C:\Windows\system32\NSI.dll	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf1bb0000	0xa000	WINNSI.DLL	C:\Windows\SYSTEM32\WINNSI.DLL	2020-10-14 03:35:40.000000	False	False	False
5940	Teams.exe	0x7ffcf1bb0000	0xa000	WINNSI.DLL	C:\Windows\SYSTEM32\WINNSI.DLL	2020-10-14 03:35:40.000000	False	False	False

C:\Windows\system32\cmd.exe									
5940	Teams.exe	0x7ffcfef00000	0x0000	WDDemoPI.DLL	C:\Windows\system32\WDDemoPI.DLL	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf5f00000	0xb6000	clbcatq.dll	C:\Windows\SYSTEM32\clbcatq.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcfef10000	0x32000	ntarta.dll	C:\Windows\SYSTEM32\ntarta.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf6b10000	0x15000	napinsp.dll	C:\Windows\system32\napinsp.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf6b00000	0x15000	napinsp.dll	C:\Windows\system32\napinsp.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf3440000	0x4000	DNSAPI.dll	C:\Windows\SYSTEM32\DNSAPI.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf6b00000	0x0000	winmm.dll	C:\Windows\SYSTEM32\winmm.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf6000000	0x26000	ndnsNSP.dll	C:\Program Files\Bonjour\ndnsNSP.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf4000000	0x14000	schhlp.dll	C:\Windows\system32\schhlp.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf6e00000	0x0000	rasadhlp.dll	C:\Windows\SYSTEM32\rasadhlp.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf2000000	0x6b000	fupacInt.dll	C:\Windows\System32\FupacInt.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf6c00000	0x0000	CRUIP.dll	C:\Windows\SYSTEM32\CRUIP.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf3200000	0x36000	rasadhlp.dll	C:\Windows\system32\rasadhlp.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf3f00000	0x0000	atlchunk.dll	C:\Windows\SYSTEM32\atlchunk.dll	2020-10-14 03:35:43.000000	False	False	False
5940	Teams.exe	0x7ffcf2170000	0x0000	LINKINFO.dll	C:\Windows\SYSTEM32\LINKINFO.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf6d00000	0x1da000	SETUPAPI.dll	C:\Windows\system32\SETUPAPI.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf6b90000	0xba000	ntshrui.dll	C:\Windows\SYSTEM32\ntshrui.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf3a00000	0x26000	svchll.dll	C:\Windows\SYSTEM32\svchll.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf6f10000	0x22000	escapi.dll	C:\Windows\SYSTEM32\escapi.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf4700000	0x7000	IconCodecService.dll	C:\Windows\system32\IconCodecService.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf3600000	0x1af000	WindowsCodecs.dll	C:\Windows\SYSTEM32\WindowsCodecs.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf3a00000	0x2f000	explorerFrame.dll	C:\Windows\system32\explorerFrame.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf6f00000	0x40000	User.dll	C:\Windows\system32\User.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf1be0000	0xc1c000	DUI70.dll	C:\Windows\system32\DUI70.dll	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf6ae0000	0x22000	adal-win.node	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\adal-win	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf6900000	0x1c7000	adal.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\adal	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf2500000	0x1f000	keytar.node	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\keytar	2020-10-14 03:35:44.000000	False	False	False
5940	Teams.exe	0x7ffcf2a00000	0x0000	DPAPI.dll	C:\Windows\SYSTEM32\DPAPI.dll	2020-10-14 03:35:45.000000	False	False	False
5940	Teams.exe	0x7ffcf3f00000	0x24000	gpapi.dll	C:\Windows\SYSTEM32\gpapi.dll	2020-10-14 03:35:46.000000	False	False	False
5940	Teams.exe	0x7ffcf6000000	0x33000	cryptnet.dll	C:\Windows\system32\cryptnet.dll	2020-10-14 03:35:46.000000	False	False	False
5940	Teams.exe	0x7ffcf4610000	0x5c000	WLDAP32.dll	C:\Windows\system32\WLDAP32.dll	2020-10-14 03:35:46.000000	False	False	False
5940	Teams.exe	0x7ffcf9020000	0x0000	ondemandconnroutehelper.dll	C:\Windows\SYSTEM32\ondemandconnroutehelper.dll	2020-10-14 03:35:46.000000	False	False	False
5940	Teams.exe	0x7ffcf3210000	0x6e000	channel.dll	C:\Windows\system32\channel.dll	2020-10-14 03:35:47.000000	False	False	False
5940	Teams.exe	0x7ffcf3f40000	0x1d000	ncryptsp.dll	C:\Windows\system32\ncryptsp.dll	2020-10-14 03:35:47.000000	False	False	False
5940	Teams.exe	0x7ffcf6e60000	0x3e000	wdmaud.drv	C:\Windows\SYSTEM32\wdmaud.drv	2020-10-14 03:35:48.000000	False	False	False
5940	Teams.exe	0x7ffcf6b00000	0x0000	ksuser.dll	C:\Windows\SYSTEM32\ksuser.dll	2020-10-14 03:35:48.000000	False	False	False
5940	Teams.exe	0x7ffcf2050000	0x0000	WUI.dll	C:\Windows\SYSTEM32\WUI.dll	2020-10-14 03:35:48.000000	False	False	False
5940	Teams.exe	0x7ffcf47a0000	0x0000	msacn32.drv	C:\Windows\SYSTEM32\msacn32.drv	2020-10-14 03:35:48.000000	False	False	False
5940	Teams.exe	0x7ffcf2b00000	0x1c000	MSACM32.dll	C:\Windows\SYSTEM32\MSACM32.dll	2020-10-14 03:35:48.000000	False	False	False
5940	Teams.exe	0x7ffcf4200000	0x0000	midimap.dll	C:\Windows\SYSTEM32\midimap.dll	2020-10-14 03:35:48.000000	False	False	False
5940	Teams.exe	0x7ffcf3d50000	0x79000	exe.dll	C:\Windows\SYSTEM32\exe.dll	2020-10-14 03:36:10.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x1d000	sharing-indicator.node	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\sharing-indicator	2020-10-14 03:36:10.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False	False	False
5940	Teams.exe	0x7ffcf2300000	0x25000	RtmControl.dll	\\?C:\Users\home\AppData\Local\Microsoft\Teams\current\Resources\app.asar.unpacked\node_modules\linclor	2020-10-14 03:36:26.000000	False		

5. Python vol.py -f HP-20201014-033903.raw windows.netscan.NetScan

Gives Network Info like open & closed ports, processes using them, IP address, port ID etc.

C:\Windows\system32\cmd.exe										
F:\volatility3-master>python vol.py -f HP-20201014-033903.raw windows.netscan.NetScan										
Volatility 3 Framework 1.2.1-beta.1										
Progress: 0.00										
Offset	Proto	LocalAddr	LocalPort	Scanning primary2	ForeignAddr	ForeignPort	SignatureScanner	State	PID	Owner
Created										
0x17276c50	TCPv4	0.0.0.0	49159	0.0.0.0	0	LISTENING	608	services.exe	-	-
0x172bfec0	UDPv4	192.168.1.6	41072	*	0		4	System	2020-10-14	03:34:59.000000
0x1733d520	UDPv4	0.0.0.0	0	*	0		4048	Teams.exe	2020-10-14	03:36:41.000000
0x1733d520	UDPv6	::	0	*	0		4048	Teams.exe	2020-10-14	03:36:41.000000
0x173447e0	UDPv6	:::1	16528	*	0		3532	svchost.exe	2020-10-14	03:36:33.000000
0x1736c010	UDPv4	127.0.0.1	16608	*	0		3532	svchost.exe	2020-10-14	03:36:33.000000
0x173f4ae0	TCPv4	192.168.1.6	49493	40.70.184.83	443	CLOSED	-	-	-	-
0x2fcd700	TCPv4	192.168.1.6	49438	74.125.24.188	5228	ESTABLISHED	-	-	-	N/A
0x2fda4d70	UDPv4	0.0.0.0	0	*	0		1068	svchost.exe	2020-10-14	03:35:26.000000
0x2fdded00	TCPv4	192.168.1.6	49475	142.250.67.174	80	CLOSED	-	-	-	-
0x2fed6d00	UDPv4	0.0.0.0	0	*	0		5056	TouchpointAnal	2020-10-13	14:24:59.000000
0x3580eec0	UDPv4	0.0.0.0	0	*	0		5056	TouchpointAnal	2020-10-13	14:24:59.000000
0x3580eec0	UDPv6	::	0	*	0		5056	TouchpointAnal	2020-10-13	14:24:59.000000
0x3584f180	TCPv4	192.168.1.6	49498	52.114.6.176	443	ESTABLISHED	-	-	-	N/A
0x35929d00	TCPv4	192.168.1.6	49436	13.233.76.15	443	CLOSED	-	-	-	N/A
0x37cde010	TCPv4	192.168.1.6	49464	52.114.16.94	443	ESTABLISHED	-	-	-	N/A
0x4a4b3d00	TCPv4	192.168.1.6	49499	52.107.17.92	443	ESTABLISHED	-	-	-	N/A
0x4a66d5d0	UDPv4	0.0.0.0	0	*	0		5688	chrome.exe	2020-10-14	03:36:09.000000
0x4a66d5d0	UDPv6	::	0	*	0		5688	chrome.exe	2020-10-14	03:36:09.000000
0x4a6d48f0	UDPv4	0.0.0.0	0	*	0		5688	chrome.exe	2020-10-14	03:36:09.000000
0x4a70e930	UDPv4	0.0.0.0	0	*	0		4048	Teams.exe	2020-10-14	03:36:41.000000
0x4a70e930	UDPv6	::	0	*	0		4048	Teams.exe	2020-10-14	03:36:41.000000
0x51b97da0	UDPv4	192.168.1.6	41072	*	0		3532	svchost.exe	2020-10-14	03:36:33.000000
0x72610570	UDPv4	0.0.0.0	0	*	0		4048	Teams.exe	2020-10-14	03:36:38.000000
0x759fd760	TCPv4	192.168.1.6	49448	151.139.128.14	80	CLOSED	-	-	-	-
0x76c28800	UDPv4	192.168.1.6	41072	*	0		4	System	2020-10-14	03:34:59.000000
0x7bhb1010	TCPv4	192.168.1.6	49449	117.239.189.11	80	CLOSED	-	-	-	N/A
0x98aeb270	UDPv4	0.0.0.0	0	*	0		1068	svchost.exe	2020-10-14	03:40:28.000000
0x996fe6a0	UDPv6	fe80::ac56:3c92:7a59:c0ee	49266	*	0		1620	mDNSResponder	2020-10-14	03:35:01.000000
0x103942010	UDPv4	192.168.1.6	41072	*	0		0	svchost.exe	2020-10-14	03:35:26.000000
0x10395ed00	TCPv4	192.168.1.6	49497	52.114.6.176	443	ESTABLISHED	-	-	-	N/A
0x10399dec0	UDPv4	0.0.0.0	0	*	0		4048	Teams.exe	2020-10-14	03:36:38.000000
0x10399dec0	UDPv6	::	0	*	0		4048	Teams.exe	2020-10-14	03:36:38.000000
0x1039cd010	UDPv6	:::1	16528	*	0		3532	svchost.exe	2020-10-14	03:36:33.000000
0x1039db440	UDPv4	0.0.0.0	0	*	0		1068	svchost.exe	2020-10-14	03:40:28.000000
0x1039db440	UDPv6	::	0	*	0		1068	svchost.exe	2020-10-14	03:40:28.000000
0x1039de260	UDPv4	0.0.0.0	0	*	0		2600	svchost.exe	2020-10-13	14:22:37.000000
0x1039de260	UDPv6	::	0	*	0		2600	svchost.exe	2020-10-13	14:22:37.000000
0x1039de970	UDPv4	0.0.0.0	0	*	0		2600	svchost.exe	2020-10-13	14:22:37.000000
0x103d31c30	TCPv4	0.0.0.0	49153	0.0.0.0	0	LISTENING	956	svchost.exe	-	-
0x1058776b0	UDPv4	0.0.0.0	0	*	0		5940	Teams.exe	2020-10-14	03:39:15.000000
0x1058776b0	UDPv6	::	0	*	0		5940	Teams.exe	2020-10-14	03:39:15.000000
0x1058ee010	UDPv6	fe80::ac56:3c92:7a59:c0ee	49266	*	0		0	svchost.exe	2020-10-14	03:36:33.000000
0x10596c430	UDPv6	fe80::ac56:3c92:7a59:c0ee	49266	*	0		956	svchost.exe	2020-10-14	03:40:28.000000
0x1073d5930	TCPv4	192.168.1.6	49413	40.119.211.203	443	ESTABLISHED	-	-	-	N/A
0x10b483870	TCPv4	0.0.0.0	49153	0.0.0.0	0	LISTENING	956	svchost.exe	-	-
0x10b483870	TCPv6	::	49153	::	0	LISTENING	956	svchost.exe	-	-
0x1132a6ed0	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	788	svchost.exe	-	-
0x1133694c0	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	788	svchost.exe	-	-
0x1133694c0	TCPv6	::	135	::	0	LISTENING	788	svchost.exe	-	-
0x11b7fe1b0	TCPv4	0.0.0.0	49152	0.0.0.0	0	LISTENING	544	wininit.exe	-	-