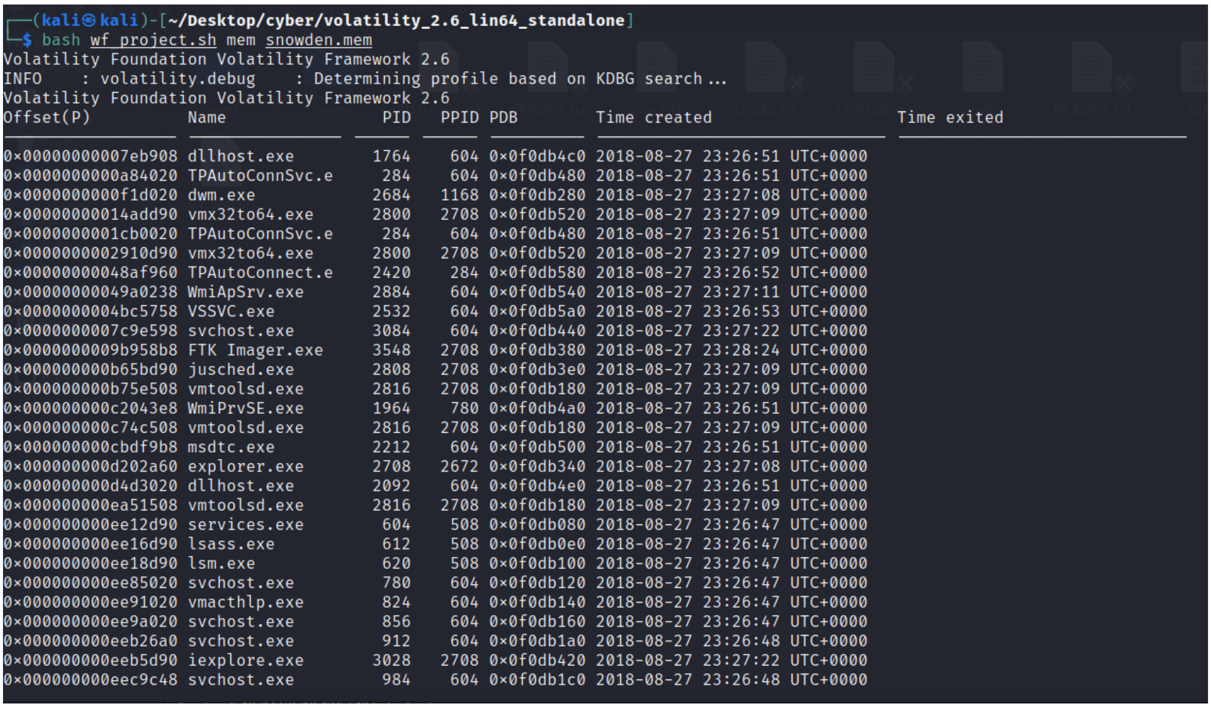
window forensics project

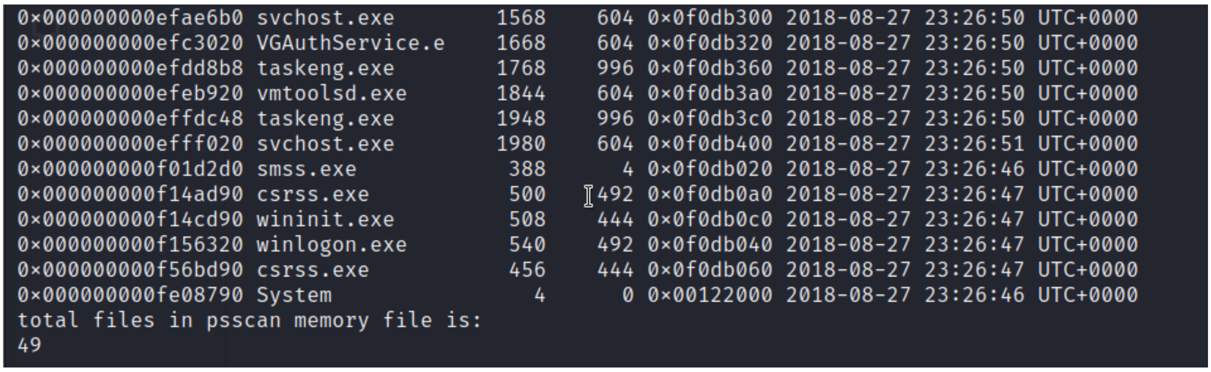
shai simchon

1.calling the MEM function while running the script.



```
┌──(kali㉿kali)-[~/Desktop/cyber/volatility_2.6_lin64_standalone]
└─$ bash wf_project.sh mem snowden.mem
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0×000000000007eb908 dllhost.exe        1764    604 0×0f0db4c0 2018-08-27 23:26:51 UTC+0000
0×0000000000a84020 TPAutoConnSvc.e      284    604 0×0f0db480 2018-08-27 23:26:51 UTC+0000
0×0000000000f1d020 dwm.exe             2684   1168 0×0f0db280 2018-08-27 23:27:08 UTC+0000
0×00000000014add90 vmx32to64.exe       2800   2708 0×0f0db520 2018-08-27 23:27:09 UTC+0000
0×0000000001cb0020 TPAutoConnSvc.e      284    604 0×0f0db480 2018-08-27 23:26:51 UTC+0000
0×0000000002910d90 vmx32to64.exe       2800   2708 0×0f0db520 2018-08-27 23:27:09 UTC+0000
0×00000000048af960 TPAutoConnect.e     2420    284 0×0f0db580 2018-08-27 23:26:52 UTC+0000
0×00000000049a0238 WmiApSrv.exe        2884    604 0×0f0db540 2018-08-27 23:27:11 UTC+0000
0×0000000004bc5758 VSSVC.exe           2532    604 0×0f0db5a0 2018-08-27 23:26:53 UTC+0000
0×0000000007c9e598 svchost.exe         3084    604 0×0f0db440 2018-08-27 23:27:22 UTC+0000
0×0000000009b958b8 FTK Imager.exe      3548   2708 0×0f0db380 2018-08-27 23:28:24 UTC+0000
0×000000000b65bd90 jusched.exe         2808   2708 0×0f0db3e0 2018-08-27 23:27:09 UTC+0000
0×000000000b75e508 vmtoolsd.exe        2816   2708 0×0f0db180 2018-08-27 23:27:09 UTC+0000
0×000000000c2043e8 WmiPrvSE.exe        1964    780 0×0f0db4a0 2018-08-27 23:26:51 UTC+0000
0×000000000c74c508 vmtoolsd.exe        2816   2708 0×0f0db180 2018-08-27 23:27:09 UTC+0000
0×000000000cbdf9b8 msdtc.exe           2212    604 0×0f0db500 2018-08-27 23:26:51 UTC+0000
0×000000000d202a60 explorer.exe        2708   2672 0×0f0db340 2018-08-27 23:27:08 UTC+0000
0×000000000d4d3020 dllhost.exe         2092    604 0×0f0db4e0 2018-08-27 23:26:51 UTC+0000
0×000000000ea51508 vmtoolsd.exe        2816   2708 0×0f0db180 2018-08-27 23:27:09 UTC+0000
0×000000000ee12d90 services.exe         604    508 0×0f0db080 2018-08-27 23:26:47 UTC+0000
0×000000000ee16d90 lsass.exe            612    508 0×0f0db0e0 2018-08-27 23:26:47 UTC+0000
0×000000000ee18d90 lsm.exe              620    508 0×0f0db100 2018-08-27 23:26:47 UTC+0000
0×000000000ee85020 svchost.exe          780    604 0×0f0db120 2018-08-27 23:26:47 UTC+0000
0×000000000ee91020 vmacthlp.exe         824    604 0×0f0db140 2018-08-27 23:26:47 UTC+0000
0×000000000ee9a020 svchost.exe          856    604 0×0f0db160 2018-08-27 23:26:47 UTC+0000
0×000000000eeb26a0 svchost.exe          912    604 0×0f0db1a0 2018-08-27 23:26:48 UTC+0000
0×000000000eeb5d90 iexplore.exe        3028   2708 0×0f0db420 2018-08-27 23:27:22 UTC+0000
0×000000000eec9c48 svchost.exe          984    604 0×0f0db1c0 2018-08-27 23:26:48 UTC+0000
```

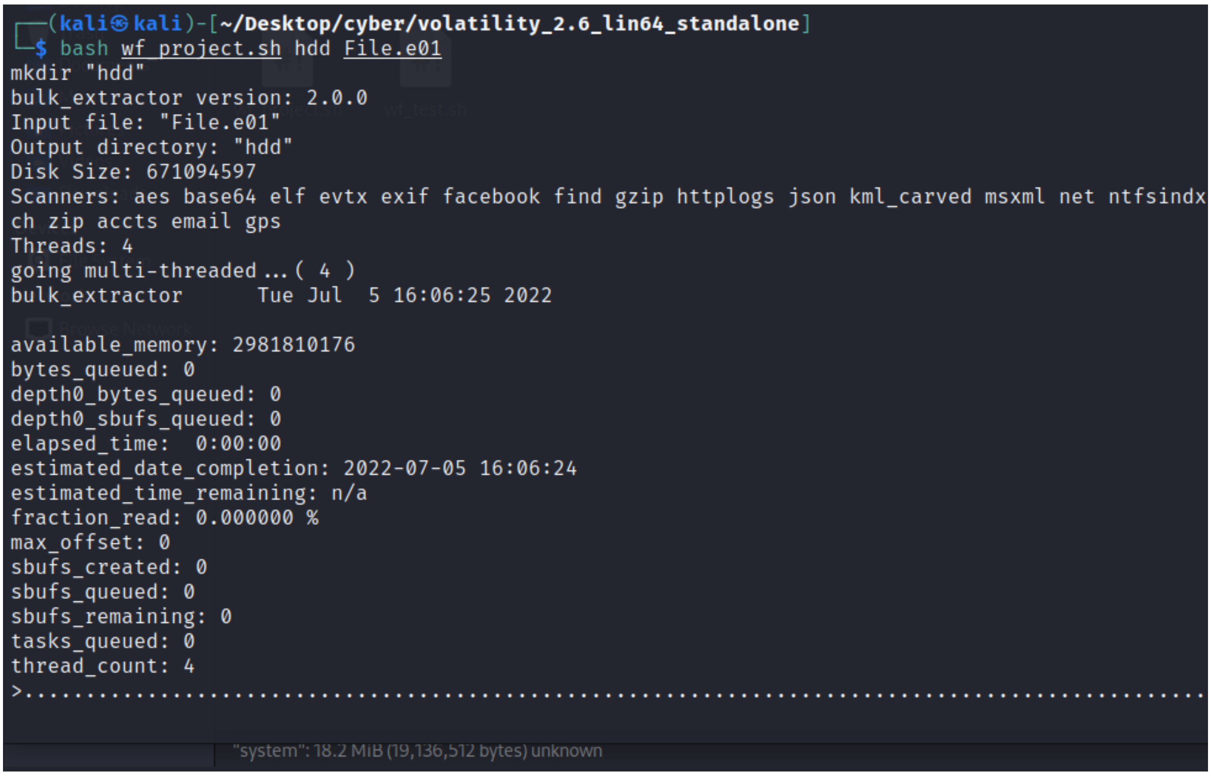
output:



```
0×000000000efae6b0 svchost.exe         1568    604 0×0f0db300 2018-08-27 23:26:50 UTC+0000
0×000000000efc3020 VGAuthService.e     1668    604 0×0f0db320 2018-08-27 23:26:50 UTC+0000
0×000000000efdd8b8 taskeng.exe         1768    996 0×0f0db360 2018-08-27 23:26:50 UTC+0000
0×000000000efeb920 vmtoolsd.exe        1844    604 0×0f0db3a0 2018-08-27 23:26:50 UTC+0000
0×000000000effdc48 taskeng.exe         1948    996 0×0f0db3c0 2018-08-27 23:26:50 UTC+0000
0×000000000efff020 svchost.exe         1980    604 0×0f0db400 2018-08-27 23:26:51 UTC+0000
0×000000000f01d2d0 smss.exe             388      4 0×0f0db020 2018-08-27 23:26:46 UTC+0000
0×000000000f14ad90 csrss.exe            500    492 0×0f0db0a0 2018-08-27 23:26:47 UTC+0000
0×000000000f14cd90 wininit.exe          508    444 0×0f0db0c0 2018-08-27 23:26:47 UTC+0000
0×000000000f156320 winlogon.exe         540    492 0×0f0db040 2018-08-27 23:26:47 UTC+0000
0×000000000f56bd90 csrss.exe            456    444 0×0f0db060 2018-08-27 23:26:47 UTC+0000
0×000000000fe08790 System                 4      0 0×00122000 2018-08-27 23:26:46 UTC+0000
total files in psscan memory file is:
49
```

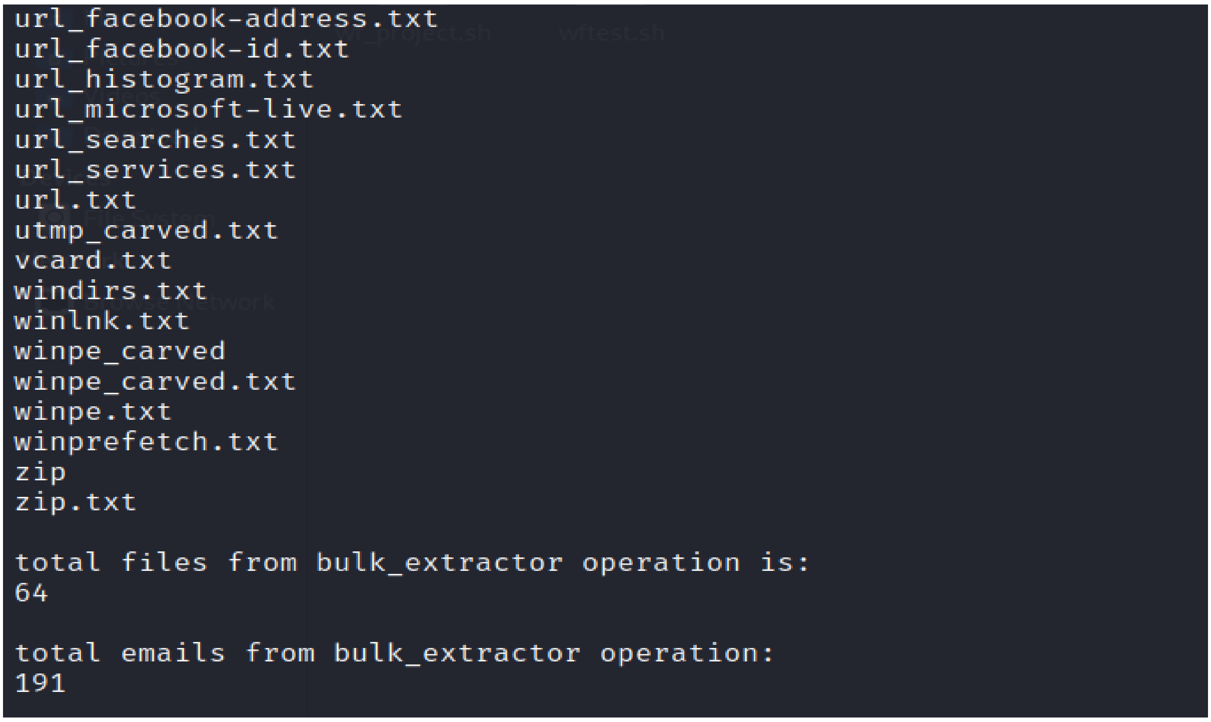
we can see that we have 49 files in this psscan.

2. calling the HDD function while running the script.



```
┌──(kali㉿kali)-[~/Desktop/cyber/volatility_2.6_lin64_standalone]
└─$ bash wf_project.sh hdd File.e01
mkdir "hdd"
bulk_extractor version: 2.0.0
Input file: "File.e01"
Output directory: "hdd"
Disk Size: 671094597
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved msxml net ntfsindx
ch zip accts email gps
Threads: 4
going multi-threaded...( 4 )
bulk_extractor      Tue Jul  5 16:06:25 2022

available_memory: 2981810176
bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time:  0:00:00
estimated_date_completion: 2022-07-05 16:06:24
estimated_time_remaining: n/a
fraction_read: 0.000000 %
max_offset: 0
sbufs_created: 0
sbufs_queued: 0
sbufs_remaining: 0
tasks_queued: 0
thread_count: 4
>...............................................................................................
```

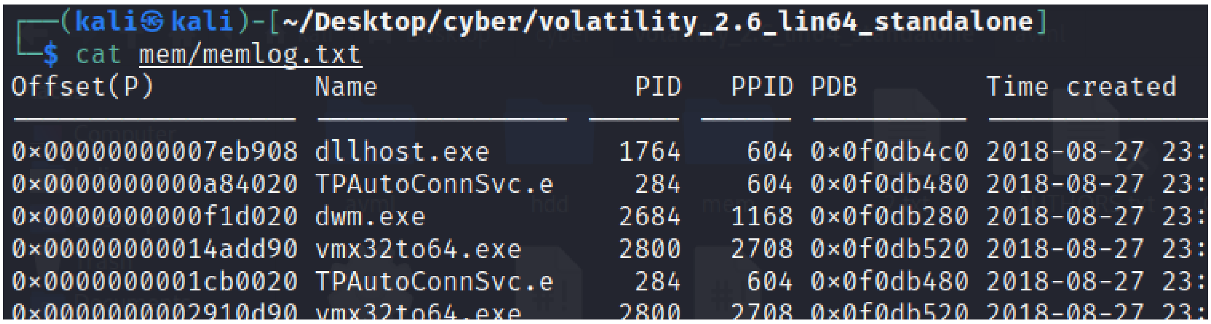
output:



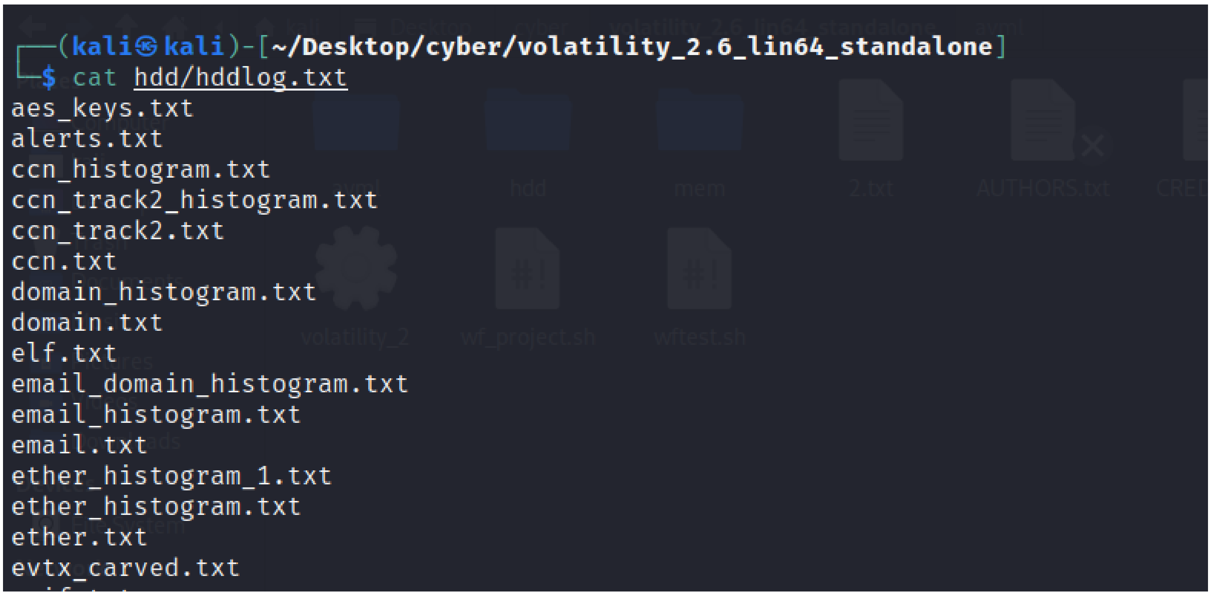
```
url_facebook-address.txt
url_facebook-id.txt
url_histogram.txt
url_microsoft-live.txt
url_searches.txt
url_services.txt
url.txt
utmp_carved.txt
vcard.txt
windirs.txt
winlnk.txt
winpe_carved
winpe_carved.txt
winpe.txt
winprefetch.txt
zip
zip.txt

total files from bulk_extractor operation is:
64

total emails from bulk_extractor operation:
191
```

We can see that we have 64 files and 191 emails from bulk extractor operation.

3. LOG script creates log text and puts it in the chosen directory that was created from the bash arguments command.



```
┌──(kali㉿kali)-[~/Desktop/cyber/volatility_2.6_lin64_standalone]
└─$ cat mem/memlog.txt
Offset(P)          Name                PID   PPID PDB        Time created
------------------ -------------------- ------ ------ ---------- ------------
0x000000000007eb908 dllhost.exe         1764    604 0x0f0db4c0 2018-08-27 23:
0x0000000000a84020 TPAutoConnSvc.e      284    604 0x0f0db480 2018-08-27 23:
0x0000000000f1d020 dwm.exe             2684   1168 0x0f0db280 2018-08-27 23:
0x00000000014add90 vmx32to64.exe       2800   2708 0x0f0db520 2018-08-27 23:
0x0000000001cb0020 TPAutoConnSvc.e      284    604 0x0f0db480 2018-08-27 23:
0x0000000002910d90 vmx32to64.exe       2800   2708 0x0f0db520 2018-08-27 23:
```



```
┌──(kali㉿kali)-[~/Desktop/cyber/volatility_2.6_lin64_standalone]
└─$ cat hdd/hddlog.txt
aes_keys.txt
alerts.txt
ccn_histogram.txt
ccn_track2_histogram.txt
ccn_track2.txt
ccn.txt
domain_histogram.txt
domain.txt
elf.txt
email_domain_histogram.txt
email_histogram.txt
email.txt
ether_histogram_1.txt
ether_histogram.txt
ether.txt
evtx_carved.txt
```