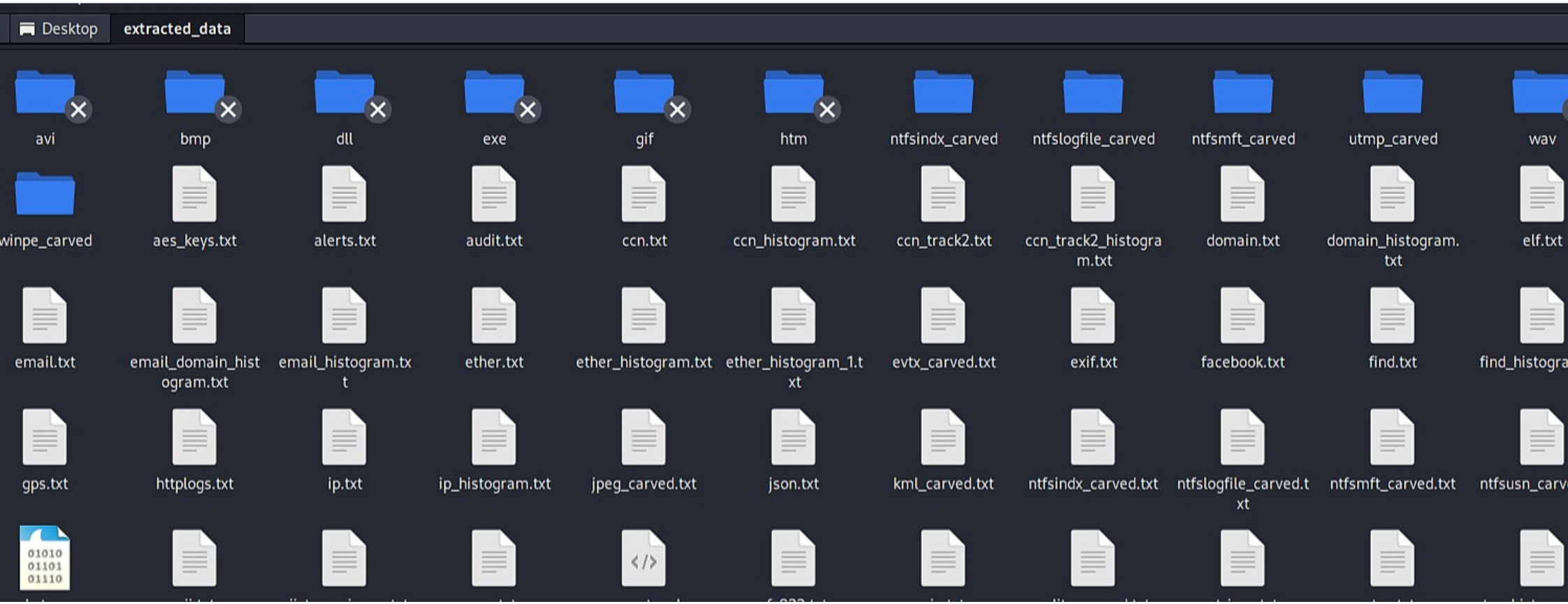
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo ./pro.sh
[sudo] password for kali:

Checking if Foremost is installed ...
It is already installed

Checking if Bulk-extractor is installed ...
It is already installed

Checking if Bulk-extractor-dbgsym is installed ...
It is already installed

Checking if Strings is installed ...
It is already installed

Checking if Tree is installed ...
It is already installed

Checking if Zip is installed ...
It is already installed

Checking if Volatility is installed ...
It is already installed

All neccessary tools have been installed


Enter a file name:

memdump.mem

File path: /home/kali/Desktop/memdump.mem


Running Foremost ...
Processing: memdump.mem
|******|

Running Bulk Extractor ...
bulk_extractor version: 2.0.0
Input file: "memdump.mem"
Output directory: "extracted_data"
Disk Size: 536870912
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved msxml net ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard_carved windirs winlnk winpe winprefetch zip accts email gps
Threads: 4
```


analysis_resu
lts.zip
analysis_repo
rt.txt
extracted_dat
a


Desktop
extracted_data
avi
bmp
dll
exe
gif
htm
ntfsindx_carved
ntfslogfile_carved
ntfsmft_carved
utmp_carved
wav
winpe_carved
aes_keys.txt
alerts.txt
audit.txt
ccn.txt
ccn_histogram.txt
ccn_track2.txt
ccn_track2_histogram.txt
domain.txt
domain_histogram.txt
elf.txt
email.txt
email_domain_histogram.txt
email_histogram.txt
ether.txt
ether_histogram.txt
ether_histogram_1.txt
evtx_carved.txt
exif.txt
facebook.txt
find.txt
gps.txt
httplogs.txt
ip.txt
ip_histogram.txt
jpeg_carved.txt
json.txt
kml_carved.txt
ntfsindx_carved.txt
ntfslogfile_carved.txt
ntfsmft_carved.txt
01010
01101
01110

analysis_report.txt

```
Analysis Report
---------------
Analysis Time: Tue Jun 20 09:53:33 PM IDT 2023
Number of Found Files: 3368
List of Extracted Files:
extracted_data/ccn_track2.txt
extracted_data/domain.txt
extracted_data/facebook.txt
extracted_data/jpeg_carved.txt
extracted_data/ip.txt
extracted_data/wav/00178840.wav
extracted_data/wav/00396280.wav
extracted_data/wav/00184216.wav
extracted_data/unrar_carved.txt
extracted_data/ccn.txt
extracted_data/url_searches.txt
```

```
0×e1035b60 0×02ac3b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0×e102e008 0×02a7d008 [no name]

Analysis Time: Tue Jun 20 09:26:17 PM IDT 2023


Number of Found Files: 3368

  adding: extracted_data/ (stored 0%)
  adding: extracted_data/ccn_track2.txt (stored 0%)
  adding: extracted_data/domain.txt (deflated 86%)
  adding: extracted_data/facebook.txt (stored 0%)
  adding: extracted_data/jpeg_carved.txt (stored 0%)
  adding: extracted_data/ip.txt (deflated 91%)
  adding: extracted_data/wav/ (stored 0%)
  adding: extracted_data/wav/00178840.wav (deflated 59%)
  adding: extracted_data/wav/00396280.wav (deflated 78%)
  adding: extracted_data/wav/00184216.wav (deflated 41%)
  adding: extracted_data/unrar_carved.txt (stored 0%)
  adding: extracted_data/ccn.txt (stored 0%)
  adding: extracted_data/url_searches.txt (stored 0%)
  adding: extracted_data/url_facebook-address.txt (stored 0%)
  adding: extracted_data/utmp_carved/ (stored 0%)
  adding: extracted_data/utmp_carved/000/ (stored 0%)
  adding: extracted_data/utmp_carved/000/212192944utmp (deflated 96%)
  adding: extracted_data/dll/ (stored 0%)
  adding: extracted_data/dll/00167576.dll (deflated 36%)
  adding: extracted_data/dll/00156928.dll (deflated 76%)
  adding: extracted_data/dll/00128888.dll (deflated 96%)
```

```
  adding: extracted_data/ntfslogfile_carved/000/202813440.LogFile-RCRD_corrupted (deflated 80%)
  adding: extracted_data/ntfslogfile_carved/000/150499328.LogFile-RCRD_corrupted (deflated 85%)
  adding: extracted_data/ntfslogfile_carved/000/124370944.LogFile-RCRD_corrupted (deflated 84%)
  adding: extracted_data/ntfslogfile_carved/000/220880896.LogFile-RCRD_corrupted (deflated 85%)
  adding: extracted_data/ntfslogfile_carved/000/150032384.LogFile-RCRD_corrupted (deflated 86%)
  adding: extracted_data/ntfslogfile_carved/000/219901952.LogFile-RCRD_corrupted (deflated 89%)
  adding: extracted_data/rfc822.txt (deflated 78%)
  adding: extracted_data/url.txt (deflated 88%)
  adding: extracted_data/json.txt (stored 0%)
  adding: extracted_data/alerts.txt (deflated 22%)
  adding: extracted_data/find_histogram.txt (stored 0%)
  adding: extracted_data/sqlite_carved.txt (stored 0%)
  adding: extracted_data/url_microsoft-live.txt (stored 0%)
  adding: extracted_data/ntfsusn_carved.txt (stored 0%)
  adding: extracted_data/avi/ (stored 0%)
  adding: extracted_data/avi/00184132.avi (deflated 50%)
  adding: extracted_data/windirs.txt (deflated 93%)
  adding: extracted_data/ether_histogram_1.txt (deflated 16%)
  adding: extracted_data/httplogs.txt (stored 0%)
  adding: analysis_report.txt (deflated 90%)

Extraction and Report generation completed. Results saved in analysis_results.zip.
```

Running processes:

```
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x823c89c8 System                    4      0     53      240 ------      0
0x822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000
0x822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000
0x82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0x82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0x81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0x823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
0x821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0x82295650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0x821dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 UTC+0000
0x81eb17b8 spoolsv.exe            1512    652     14      113      0      0 2012-07-22 02:42:36 UTC+0000
0x81e7bda0 reader_sl.exe          1640   1484      5       39      0      0 2012-07-22 02:42:36 UTC+0000
0x820e8da0 alg.exe                 788    652      7      104      0      0 2012-07-22 02:43:01 UTC+0000
0x821fcda0 wuauclt.exe            1136   1004      8      173      0      0 2012-07-22 02:43:46 UTC+0000
0x8205bda0 wuauclt.exe            1588   1004      5      132      0      0 2012-07-22 02:44:01 UTC+0000
```

Network connections:

```
Volatility Foundation Volatility Framework 2.5
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x81e87620 172.16.112.128:1038      41.168.5.140:8080        1484
```

Registry information:

```
Volatility Foundation Volatility Framework 2.5
Virtual    Physical   Name
---------- ---------- ----
0xe18e5b60 0x093f8b60 \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a19b60 0x0a5a9b60 \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
0xe18398d0 0x08a838d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe18614d0 0x08e624d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe183bb60 0x08e2db60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe17f2b60 0x08519b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1570510 0x07669510 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1571008 0x0777f008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe15709b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe15719e8 0x0777f9e8 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ba008 0x02e4b008 [no name]
0xe1035b60 0x02ac3b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02a7d008 [no name]
```

```
depth0_bytes_queued: 33554432
depth0_sbufs_queued: 2
elapsed_time:  0:00:47
estimated_date_completion: 2023-06-20 21:24:22
estimated_time_remaining:  0:00:00
fraction_read: 100.000000 %
max_offset: 520093696
sbufs_created: 1680380
sbufs_queued: 2
sbufs_remaining: 1
tasks_queued: 0
thread-1: 520093696: accts (16777216 bytes)
thread-3: 520093696: email (16777216 bytes)
thread_count: 4
```

```
Phase 2. Shutting down scanners
Computing final histograms and shutting down ...
Phase 3. Generating stats and printing final usage information
All Threads Finished!
Elapsed time: 48.44 sec.
Total MB processed: 536
Overall performance: 11.08 MBytes/sec 2.771 (MBytes/sec/thread)
sbufs created:   1680380
sbufs unaccounted: 0
Time producer spent waiting for scanners to process data:         0:00:38 (38.09 seconds)
Time consumer scanners spent waiting for data from producer:      0:00:03 (3.86 seconds)
Average time each consumer spent waiting for data from producer:  0:00:00 (0.00 seconds)
*** More time spent waiting for workers. You need a faster CPU or more cores for improved performance.
Total email features found: 123

Running Volatility Imageinfo...
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search ...

Running Volatility PSlist...
Volatility Foundation Volatility Framework 2.5

Running Strings ...

Network data Found [Path: extracted_data/aes_keys.txt ] [Size 4.0K]

memdump.mem can be analyzed in Volatility.
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search ...

Memory profile: WinXPSP2x86
```

```
Running Bulk Extractor ...
bulk_extractor version: 2.0.0
Input file: "memdump.mem"
Output directory: "extracted_data"
Disk Size: 536870912
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved msxml net ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard_carved windirs winlnk winpe winprefetch zip accts email gps
Threads: 4
going multi-threaded ... ( 4 )
bulk_extractor      Tue Jun 20 21:23:35 2023

available_memory: 1325850624
bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time:  0:00:00
estimated_date_completion: 2023-06-20 21:23:34
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
>.....................................................................................................................................................................................

bulk_extractor      Tue Jun 20 21:23:36 2023

available_memory: 1263632384
bytes_queued: 817889280
depth0_bytes_queued: 817889280
depth0_sbufs_queued: 39
elapsed_time:  0:00:01
estimated_date_completion: 2023-06-20 21:23:51
estimated_time_remaining:  0:00:15
fraction_read: 6.250000 %
max_offset: 0
sbufs_created: 98341
sbufs_queued: 39
sbufs_remaining: 3
tasks_queued: 35
thread-1: 0: net (20971520 bytes)
thread-2: 0: rar (20971520 bytes)
thread-3: 0: aes (20971520 bytes)
thread-4: 0: winprefetch (20971520 bytes)
```