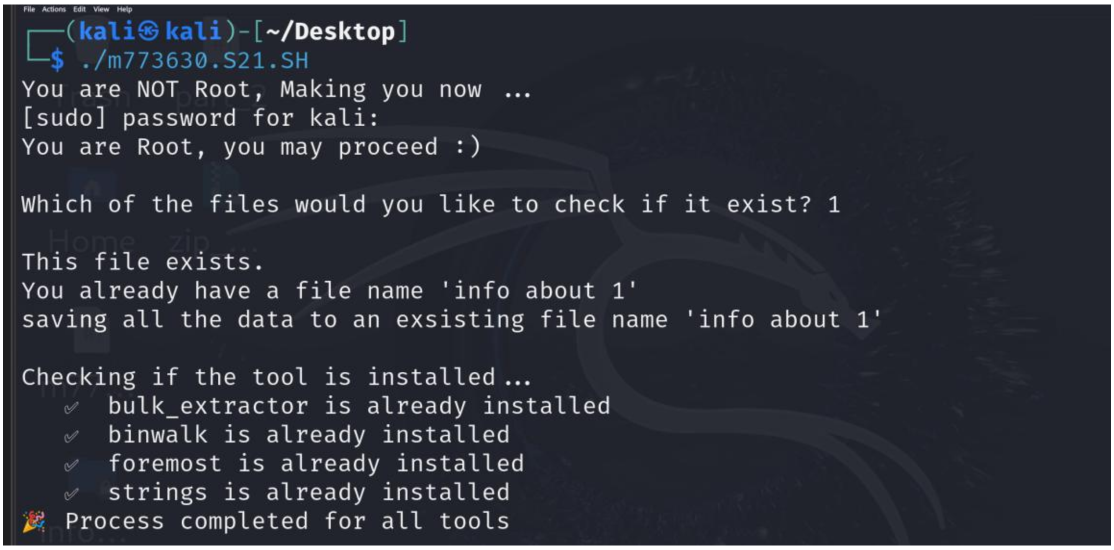
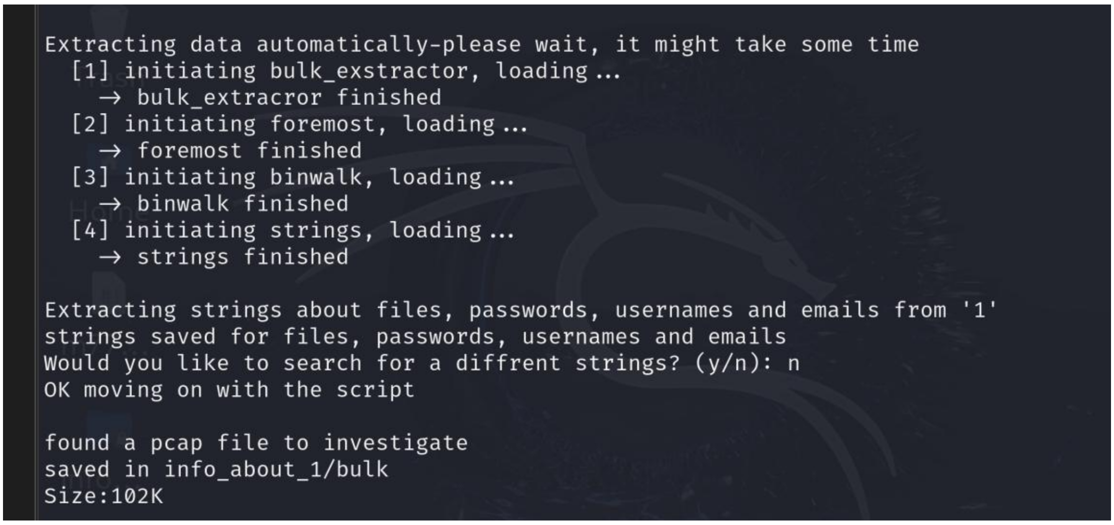
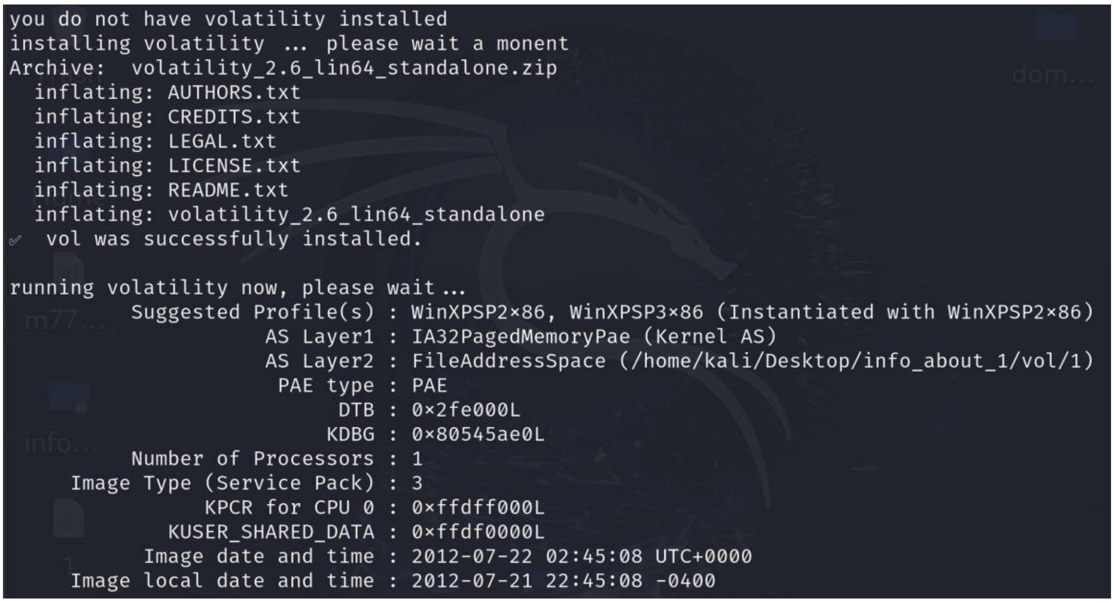


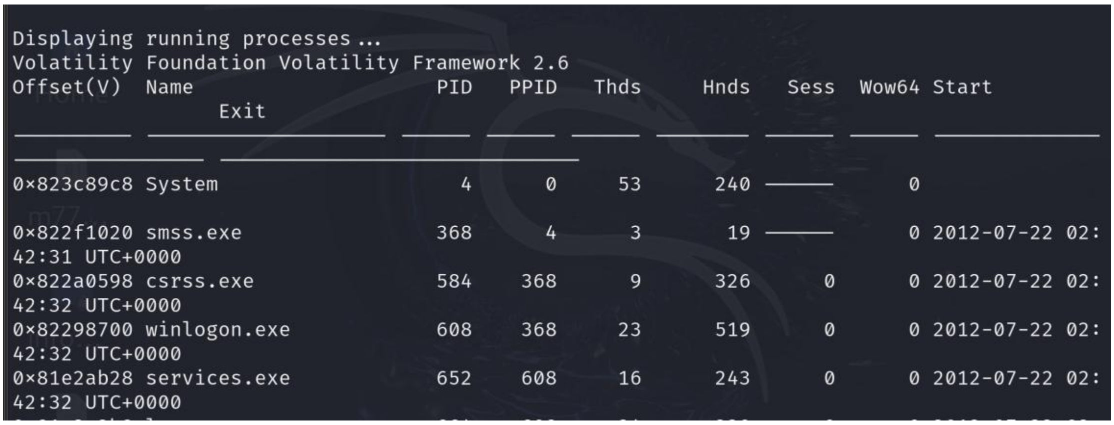
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ./m773630.S21.SH
You are NOT Root, Making you now ...
[sudo] password for kali:
You are Root, you may proceed :)

Which of the files would you like to check if it exist? 1

This file exists.
You already have a file name 'info about 1'
saving all the data to an exsisting file name 'info about 1'

Checking if the tool is installed...
   ✓  bulk_extractor is already installed
   ✓  binwalk is already installed
   ✓  foremost is already installed
   ✓  strings is already installed
🎉 Process completed for all tools
```



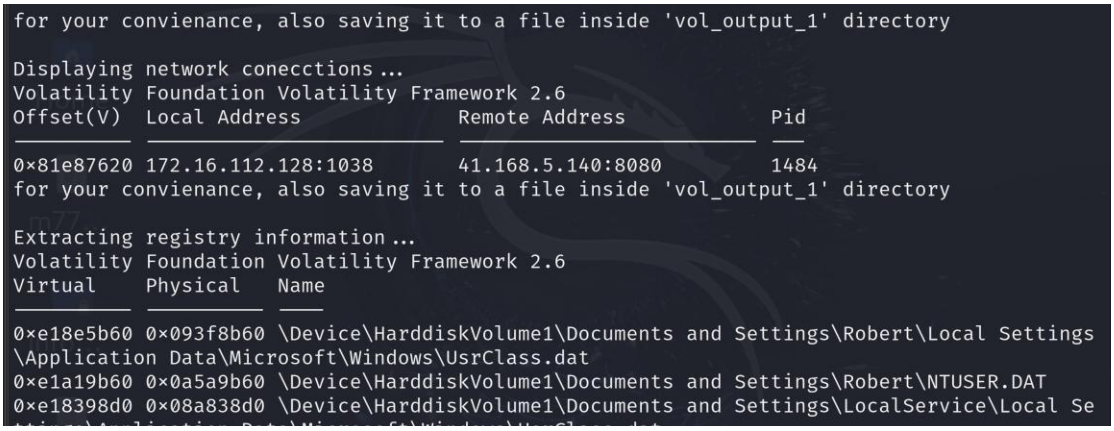
```
Extracting data automatically-please wait, it might take some time
  [1] initiating bulk_exstractor, loading...
    → bulk_extracror finished
  [2] initiating foremost, loading...
    → foremost finished
  [3] initiating binwalk, loading...
    → binwalk finished
  [4] initiating strings, loading...
    → strings finished

Extracting strings about files, passwords, usernames and emails from '1'
strings saved for files, passwords, usernames and emails
Would you like to search for a diffrent strings? (y/n): n
OK moving on with the script

found a pcap file to investigate
saved in info_about_1/bulk
Size:102K
```



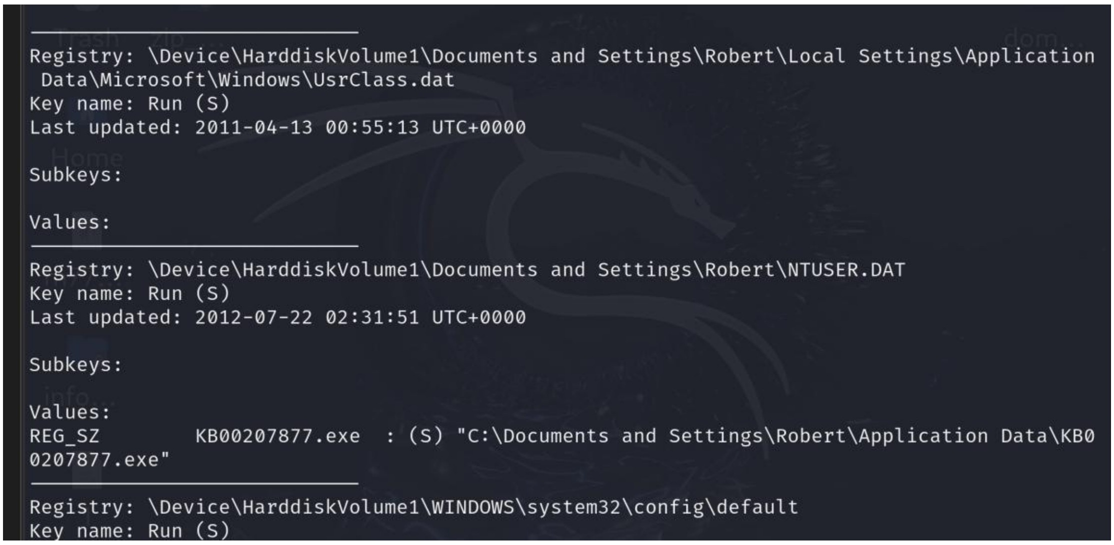
```
you do not have volatility installed
installing volatility ... please wait a monent
Archive:  volatility_2.6_lin64_standalone.zip
  inflating: AUTHORS.txt
  inflating: CREDITS.txt
  inflating: LEGAL.txt
  inflating: LICENSE.txt
  inflating: README.txt
  inflating: volatility_2.6_lin64_standalone
✓  vol was successfully installed.

running volatility now, please wait...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/info_about_1/vol/1)
                      PAE type : PAE
                           DTB : 0x2fe000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400
```



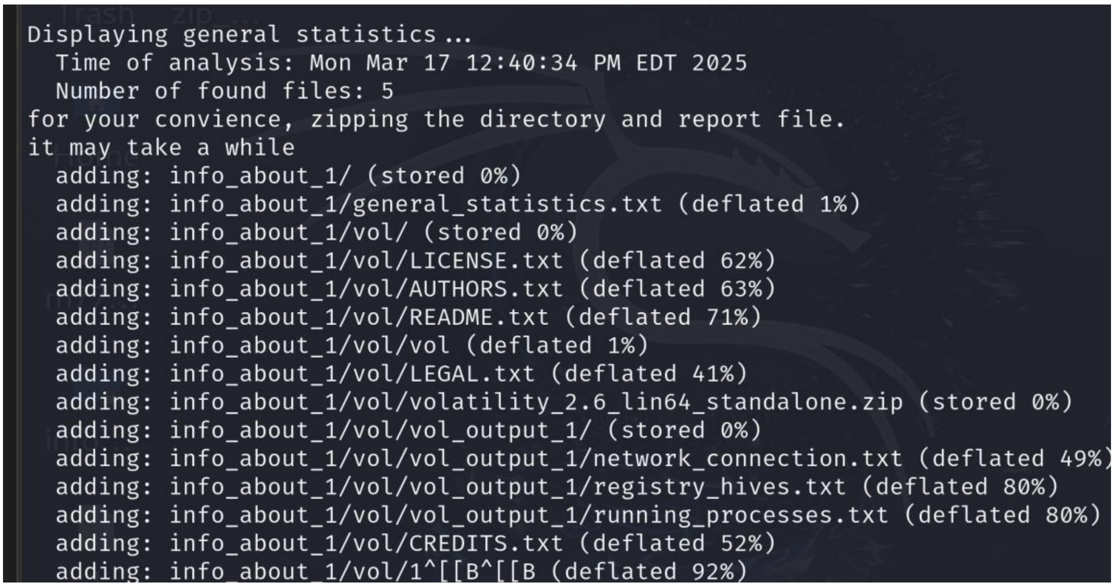
```
Displaying running processes ...
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
                 Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
------------------------------ ------------------------------

0×823c89c8 System                    4      0     53      240 ------      0

0×822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:
42:31 UTC+0000
0×822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:
42:32 UTC+0000
0×82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:
42:32 UTC+0000
0×81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:
42:32 UTC+0000
```



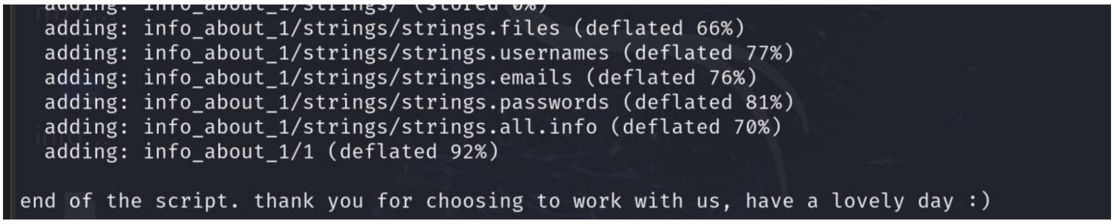
```
for your convienance, also saving it to a file inside 'vol_output_1' directory

Displaying network conecctions ...
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---

0×81e87620 172.16.112.128:1038       41.168.5.140:8080         1484
for your convienance, also saving it to a file inside 'vol_output_1' directory

Extracting registry information ...
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----

0×e18e5b60 0×093f8b60 \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings
\Application Data\Microsoft\Windows\UsrClass.dat
0×e1a19b60 0×0a5a9b60 \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
0×e18398d0 0×08a838d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Se
ttings\Application Data\Microsoft\Windows\UsrClass.dat
```



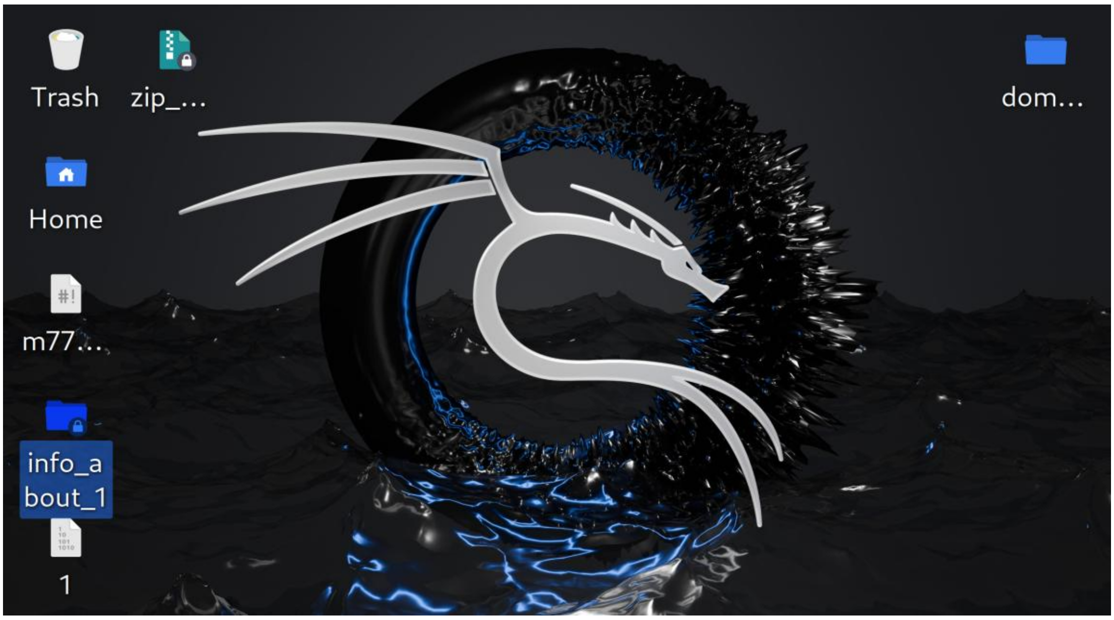
```
 ----------------------------
 Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application
  Data\Microsoft\Windows\UsrClass.dat
 Key name: Run (S)
 Last updated: 2011-04-13 00:55:13 UTC+0000

 Subkeys:

 Values:
 ----------------------------
 Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
 Key name: Run (S)
 Last updated: 2012-07-22 02:31:51 UTC+0000

 Subkeys:

 Values:
 REG_SZ        KB00207877.exe  : (S) "C:\Documents and Settings\Robert\Application Data\KB0
 0207877.exe"
 ----------------------------
 Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
 Key name: Run (S)
```



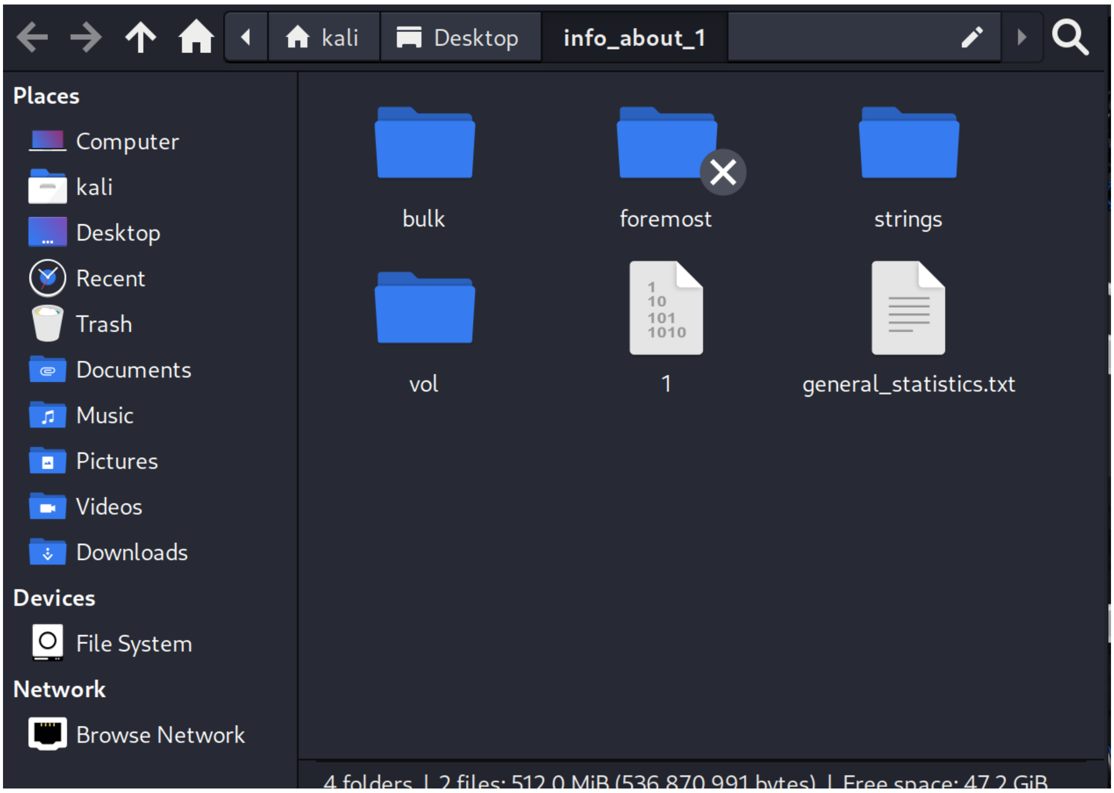
```
Displaying general statistics...
  Time of analysis: Mon Mar 17 12:40:34 PM EDT 2025
  Number of found files: 5
for your convience, zipping the directory and report file.
it may take a while
  adding: info_about_1/ (stored 0%)
  adding: info_about_1/general_statistics.txt (deflated 1%)
  adding: info_about_1/vol/ (stored 0%)
  adding: info_about_1/vol/LICENSE.txt (deflated 62%)
  adding: info_about_1/vol/AUTHORS.txt (deflated 63%)
  adding: info_about_1/vol/README.txt (deflated 71%)
  adding: info_about_1/vol/vol (deflated 1%)
  adding: info_about_1/vol/LEGAL.txt (deflated 41%)
  adding: info_about_1/vol/volatility_2.6_lin64_standalone.zip (stored 0%)
  adding: info_about_1/vol/vol_output_1/ (stored 0%)
  adding: info_about_1/vol/vol_output_1/network_connection.txt (deflated 49%)
  adding: info_about_1/vol/vol_output_1/registry_hives.txt (deflated 80%)
  adding: info_about_1/vol/vol_output_1/running_processes.txt (deflated 80%)
  adding: info_about_1/vol/CREDITS.txt (deflated 52%)
  adding: info_about_1/vol/1^[[B^[[B (deflated 92%)
```



```
  adding: info_about_1/strings/ (stored 0%)
  adding: info_about_1/strings/strings.files (deflated 66%)
  adding: info_about_1/strings/strings.usernames (deflated 77%)
  adding: info_about_1/strings/strings.emails (deflated 76%)
  adding: info_about_1/strings/strings.passwords (deflated 81%)
  adding: info_about_1/strings/strings.all.info (deflated 70%)
  adding: info_about_1/1 (deflated 92%)

end of the script. thank you for choosing to work with us, have a lovely day :)
```

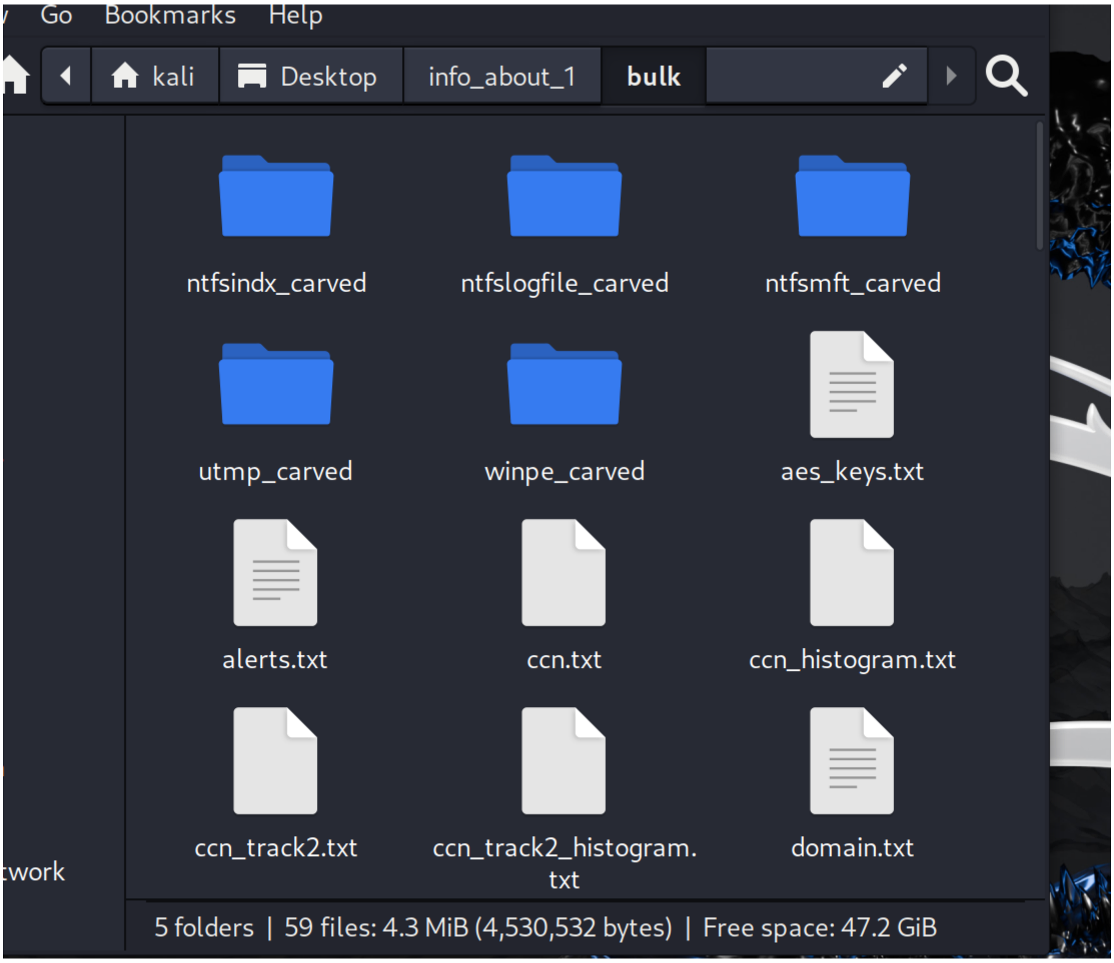


שומר את המידע בתיקייה בשם הMEMDUMP שחקרתי . אני חקרתי קובץ בשם 1

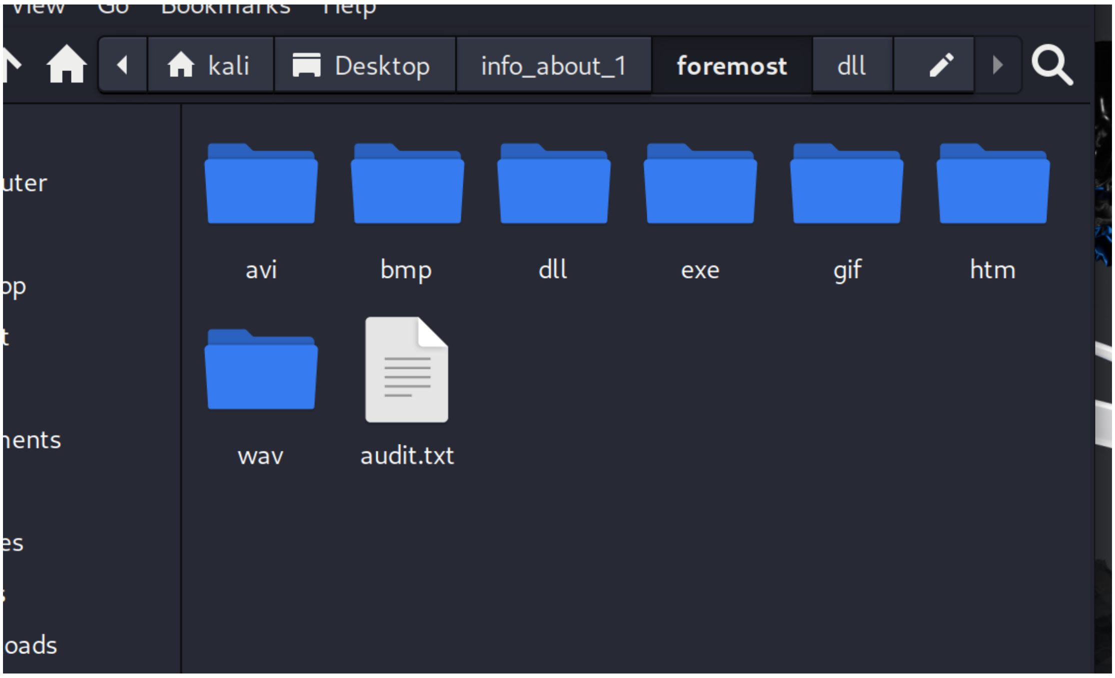


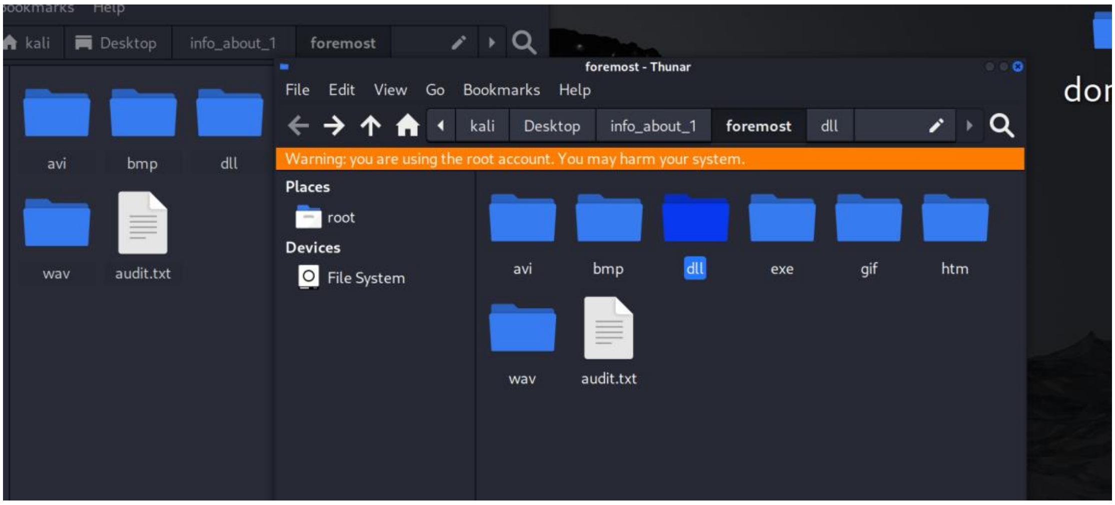
4 folders | 2 files: 512.0 MiB (536,870,991 bytes) | Free space: 47.2 GiB

הסקריפט פותח תיקיות על פי הנתונים שהוציא



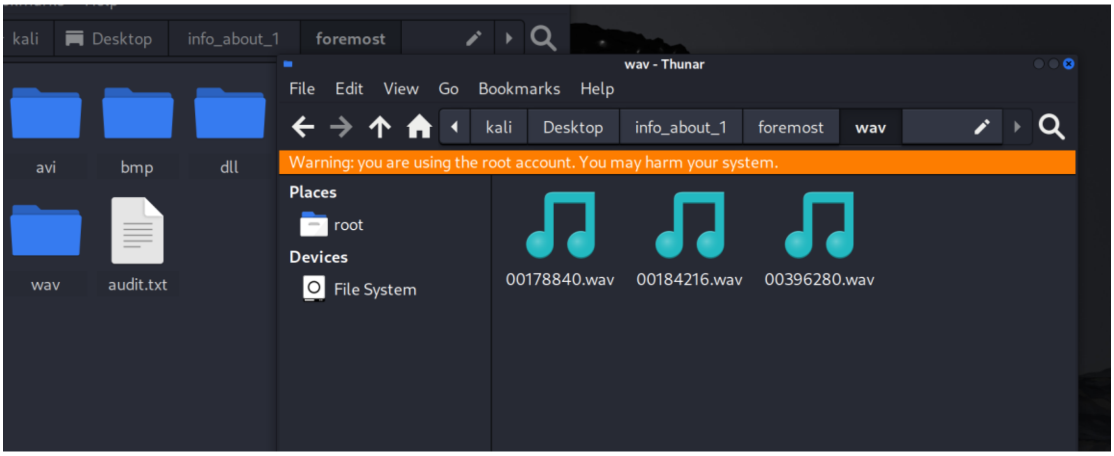
5 folders | 59 files: 4.3 MiB (4,530,532 bytes) | Free space: 47.2 GiB



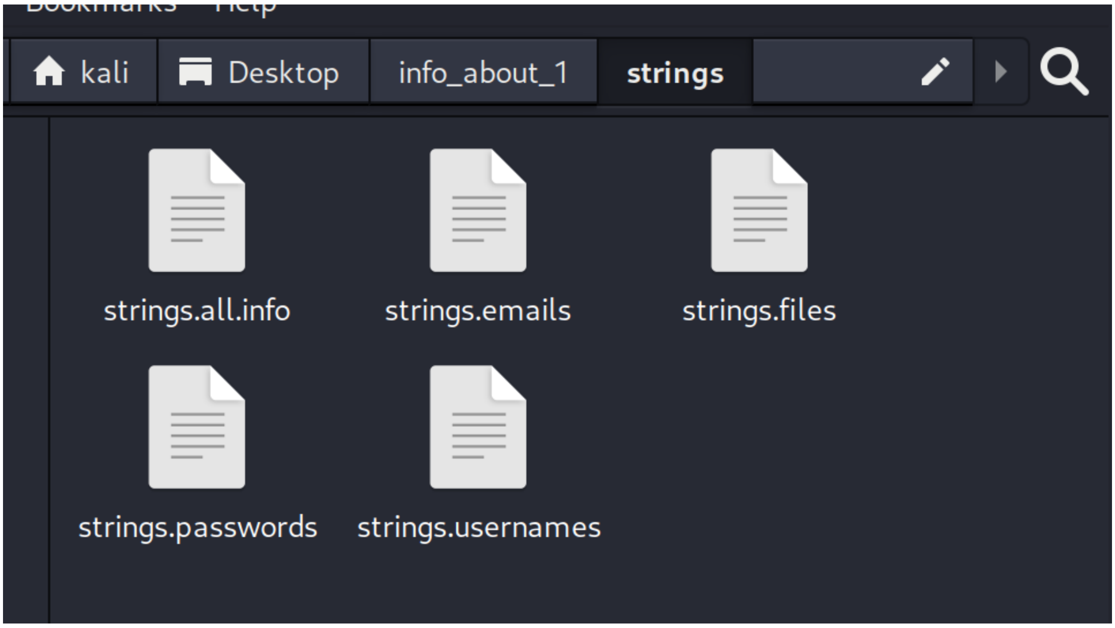


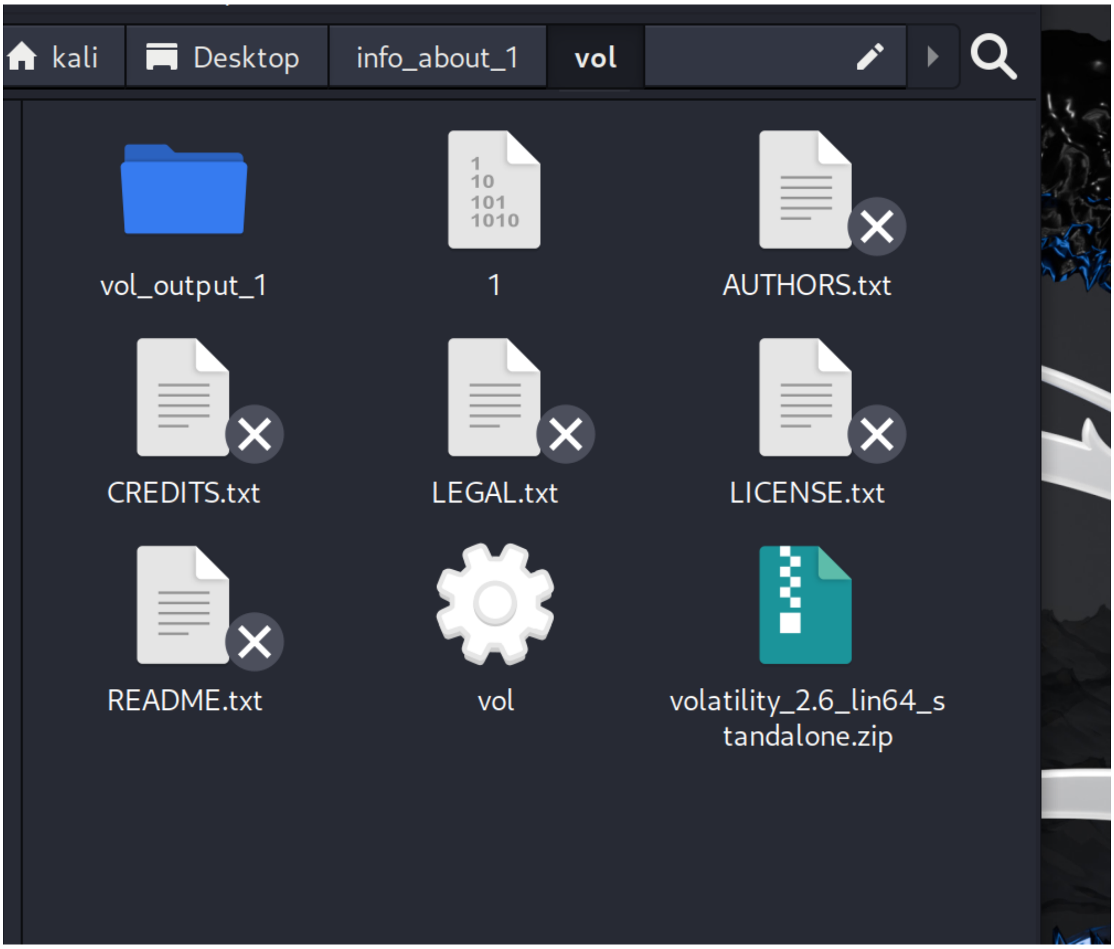
Warning: you are using the root account. You may harm your system.

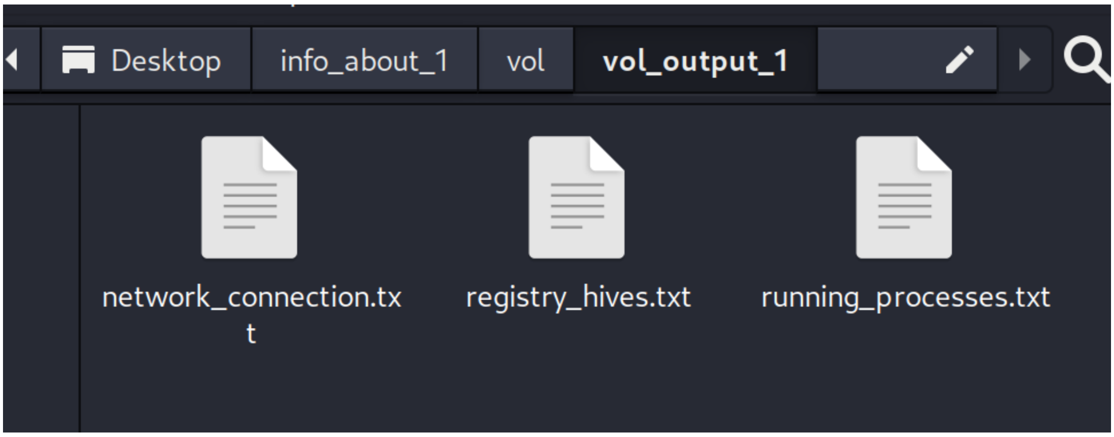
פורמוסט נפתח רק אם אני רות ולכן יש איקס בכניסה לתיקייה



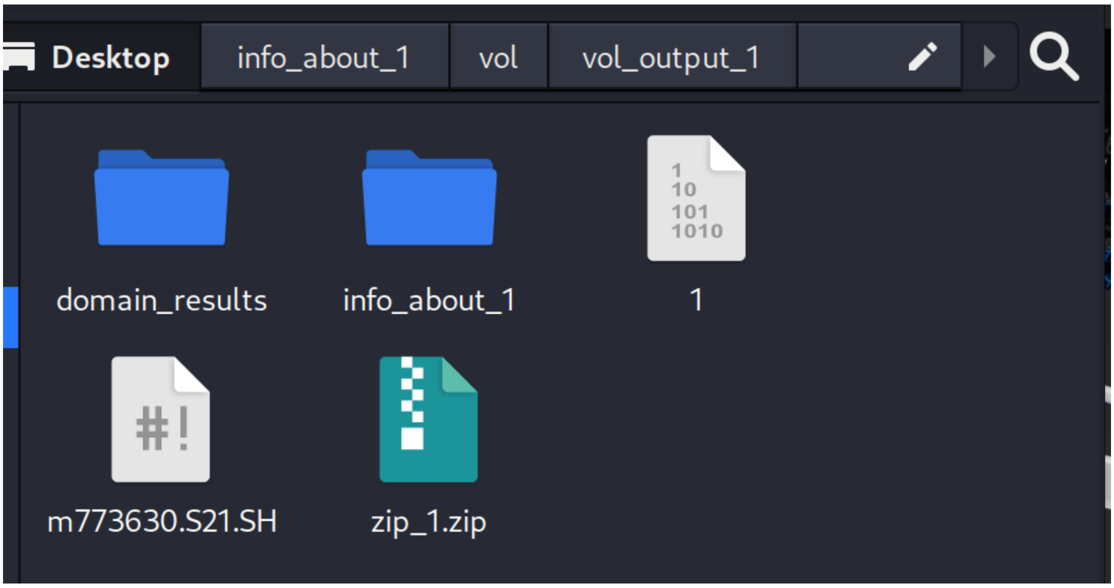
Warning: you are using the root account. You may harm your system.


Bookmarks
Help
kali
Desktop
info_about_1
strings
strings.all.info
strings.emails
strings.files
strings.passwords
strings.usernames


kali
Desktop
info_about_1
vol
vol_output_1
1
AUTHORS.txt
CREDITS.txt
LEGAL.txt
LICENSE.txt
README.txt
vol
volatility_2.6_lin64_standalone.zip



וזה תמונה מהדסקטופ שיצר לי גם קובץ זיפ לתיקייה



Desktop
info_about_1
vol
vol_output_1
domain_results
info_about_1
1
m773630.S21.SH
zip_1.zip