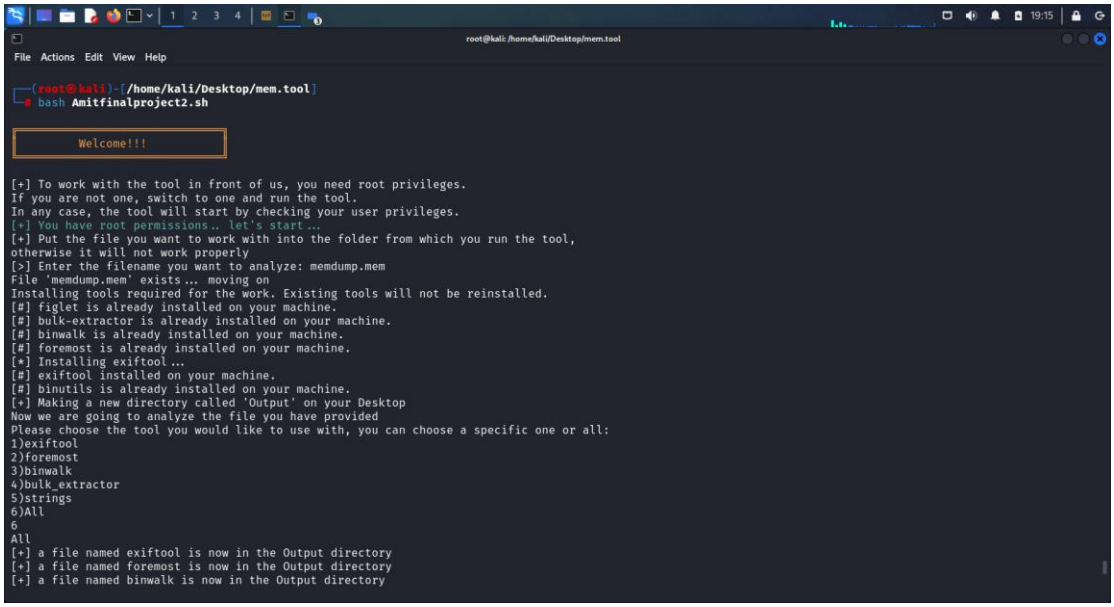
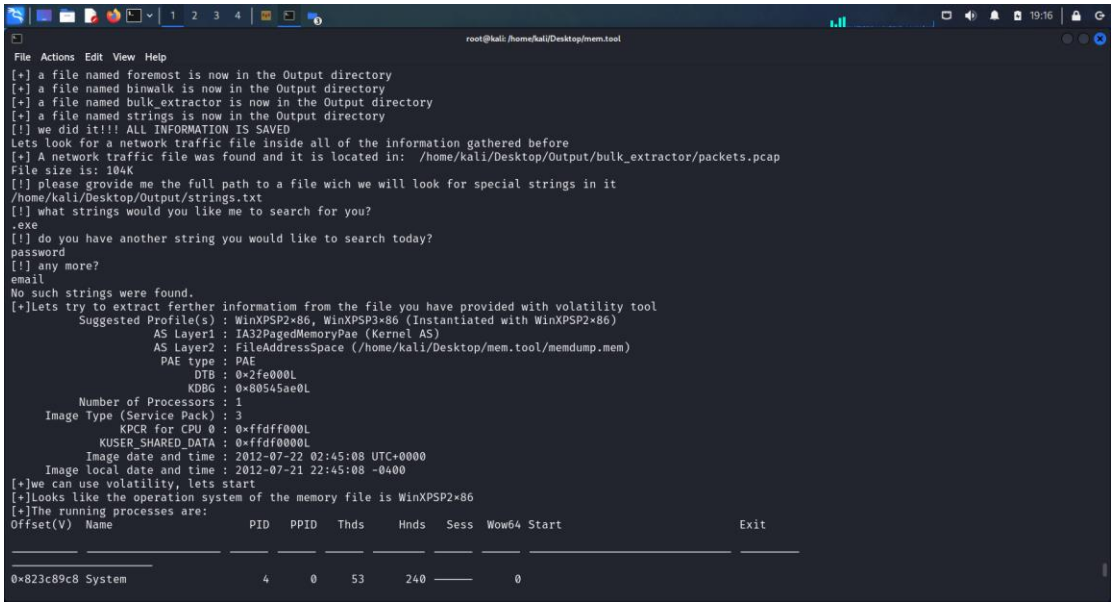
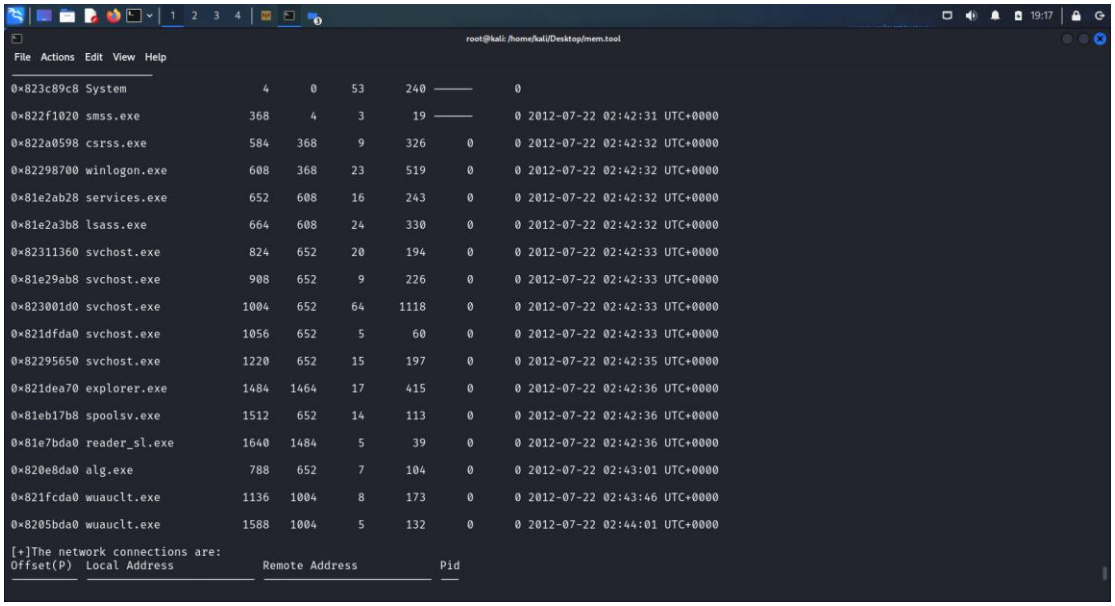
DIGITAL FORENSICS ANALYZER PROJECT- AMIT PERSKY

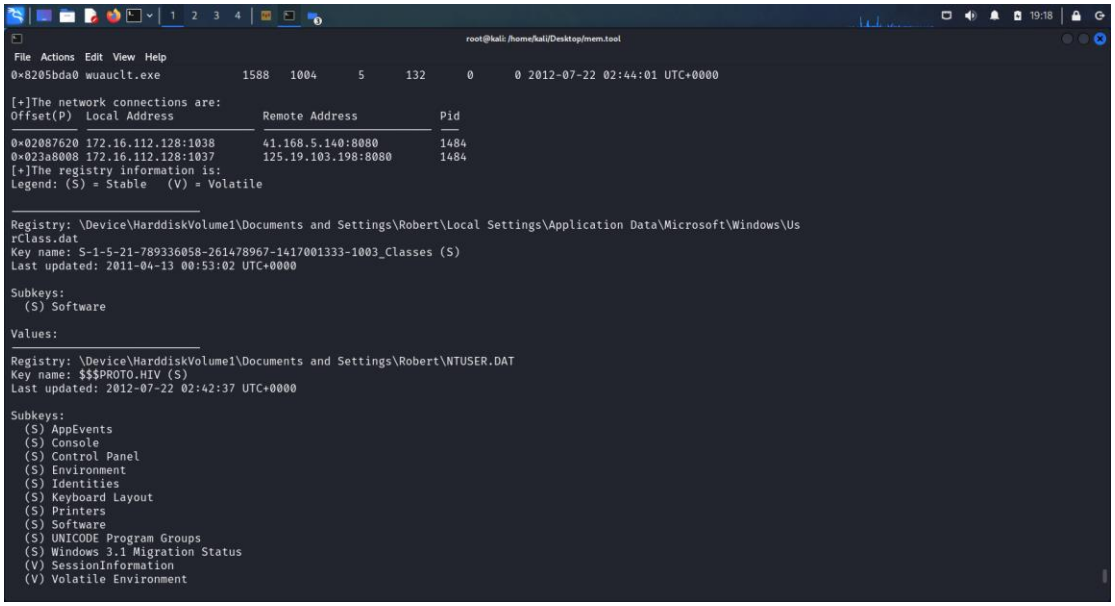
This project involved the creation of a comprehensive program for digital forensic analysis. Focused on automated hard disk drive (HDD) and memory investigations, it was designed to identify, extract, and display crucial data elements like network traffic or human-readable information. Additionally, the program integrates with the Volatility software for in-depth memory analysis and outputs detailed reports. It also features a dedicated function to install necessary forensic tools, ensuring smooth operation.

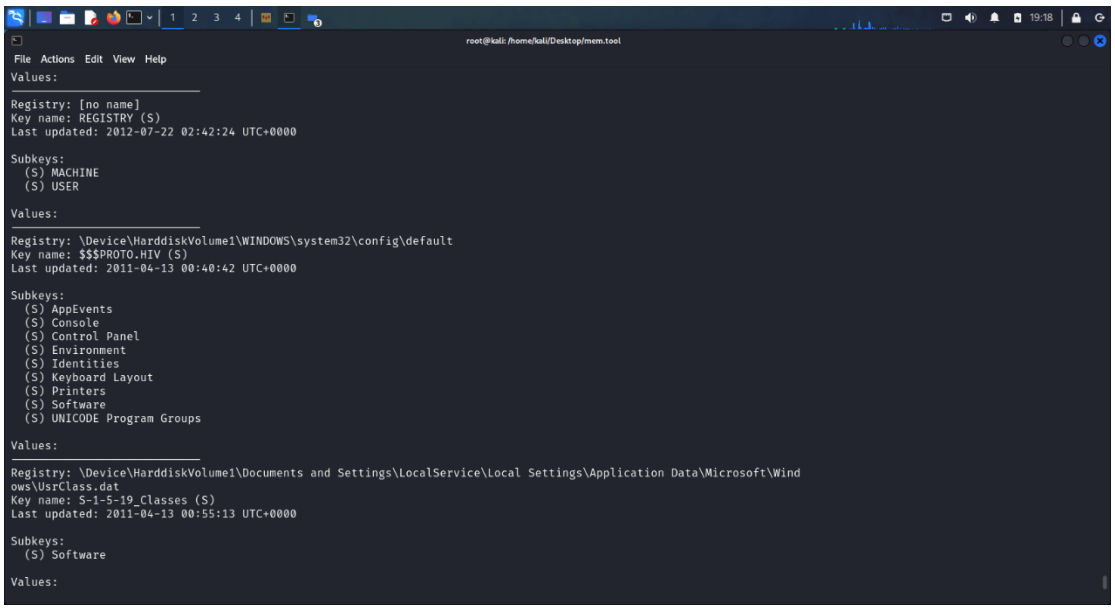
Output of my script:

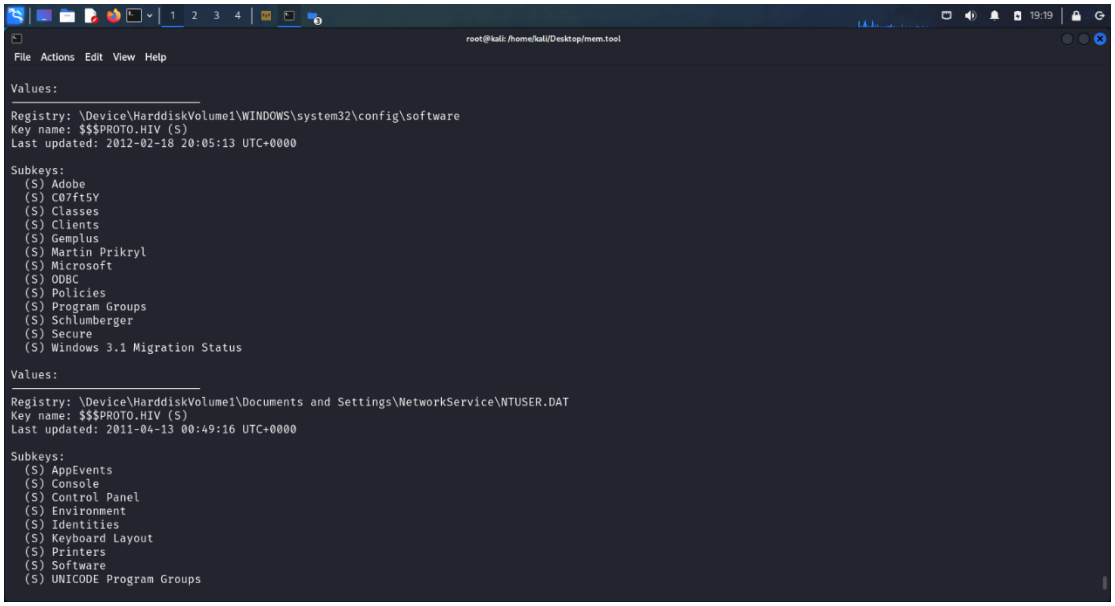


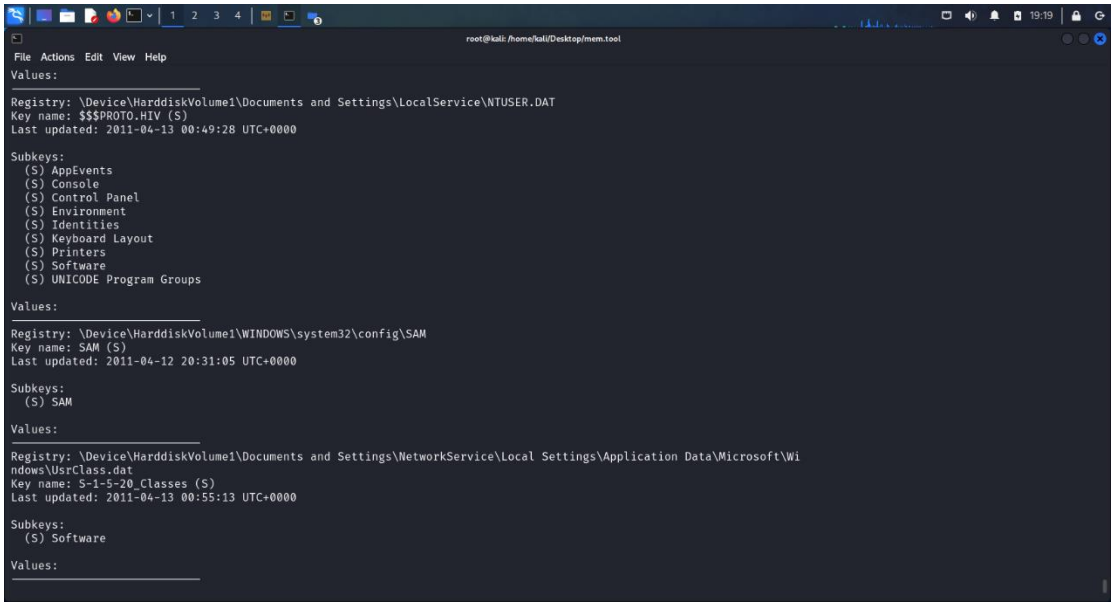


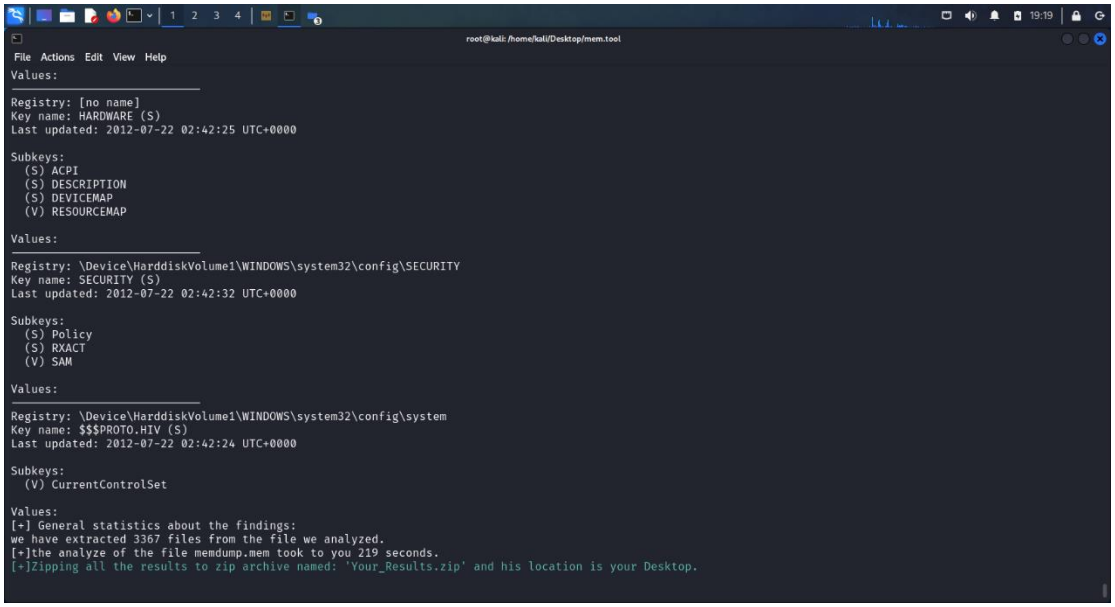

root@kali: /home/kali/Desktop/mem.tool
File Actions Edit View Help
0×823c89c8 System 4 0 53 240 ——— 0
0×822f1020 smss.exe 368 4 3 19 ——— 0 2012-07-22 02:42:31 UTC+0000
0×822a0598 csrss.exe 584 368 9 326 0 0 2012-07-22 02:42:32 UTC+0000
0×82298700 winlogon.exe 608 368 23 519 0 0 2012-07-22 02:42:32 UTC+0000
0×81e2ab28 services.exe 652 608 16 243 0 0 2012-07-22 02:42:32 UTC+0000
0×81e2a3b8 lsass.exe 664 608 24 330 0 0 2012-07-22 02:42:32 UTC+0000
0×82311360 svchost.exe 824 652 20 194 0 0 2012-07-22 02:42:33 UTC+0000
0×81e29ab8 svchost.exe 908 652 9 226 0 0 2012-07-22 02:42:33 UTC+0000
0×823001d0 svchost.exe 1004 652 64 1118 0 0 2012-07-22 02:42:33 UTC+0000
0×821dfda0 svchost.exe 1056 652 5 60 0 0 2012-07-22 02:42:33 UTC+0000
0×82295650 svchost.exe 1220 652 15 197 0 0 2012-07-22 02:42:35 UTC+0000
0×821dea70 explorer.exe 1484 1464 17 415 0 0 2012-07-22 02:42:36 UTC+0000
0×81eb17b8 spoolsv.exe 1512 652 14 113 0 0 2012-07-22 02:42:36 UTC+0000
0×81e7bda0 reader_sl.exe 1640 1484 5 39 0 0 2012-07-22 02:42:36 UTC+0000
0×820e8da0 alg.exe 788 652 7 104 0 0 2012-07-22 02:43:01 UTC+0000
0×821fcda0 wuauclt.exe 1136 1004 8 173 0 0 2012-07-22 02:43:46 UTC+0000
0×8205bda0 wuauclt.exe 1588 1004 5 132 0 0 2012-07-22 02:44:01 UTC+0000
[+]The network connections are:
Offset(P) Local Address Remote Address Pid


root@kali: /home/kali/Desktop/mem.tool
File Actions Edit View Help
0×8205bda0 wuauclt.exe 1588 1004 5 132 0 0 2012-07-22 02:44:01 UTC+0000
[+]The network connections are:
Offset(P) Local Address Remote Address Pid
0×02087620 172.16.112.128:1038 41.168.5.140:8080 1484
0×023a8008 172.16.112.128:1037 125.19.103.198:8080 1484
[+]The registry information is:
Legend: (S) = Stable (V) = Volatile
Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-21-789336058-261478967-1417001333-1003_Classes (S)
Last updated: 2011-04-13 00:53:02 UTC+0000
Subkeys:
(S) Software
Values:
Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2012-07-22 02:42:37 UTC+0000
Subkeys:
(S) AppEvents
(S) Console
(S) Control Panel
(S) Environment
(S) Identities
(S) Keyboard Layout
(S) Printers
(S) Software
(S) UNICODE Program Groups
(S) Windows 3.1 Migration Status
(V) SessionInformation
(V) Volatile Environment


root@kali: /home/kali/Desktop/mem.tool
File Actions Edit View Help
Values:
Registry: [no name]
Key name: REGISTRY (S)
Last updated: 2012-07-22 02:42:24 UTC+0000
Subkeys:
(S) MACHINE
(S) USER
Values:
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: $$$PROTO.HIV (S)
Last updated: 2011-04-13 00:40:42 UTC+0000
Subkeys:
(S) AppEvents
(S) Console
(S) Control Panel
(S) Environment
(S) Identities
(S) Keyboard Layout
(S) Printers
(S) Software
(S) UNICODE Program Groups
Values:
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-19_Classes (S)
Last updated: 2011-04-13 00:55:13 UTC+0000
Subkeys:
(S) Software
Values:


root@kali: /home/kali/Desktop/mem.tool
File Actions Edit View Help
Values:
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: $$$PROTO.HIV (S)
Last updated: 2012-02-18 20:05:13 UTC+0000
Subkeys:
(S) Adobe
(S) C07ft5Y
(S) Classes
(S) Clients
(S) Gemplus
(S) Martin Prikryl
(S) Microsoft
(S) ODBC
(S) Policies
(S) Program Groups
(S) Schlumberger
(S) Secure
(S) Windows 3.1 Migration Status
Values:
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2011-04-13 00:49:16 UTC+0000
Subkeys:
(S) AppEvents
(S) Console
(S) Control Panel
(S) Environment
(S) Identities
(S) Keyboard Layout
(S) Printers
(S) Software
(S) UNICODE Program Groups


root@kali: /home/kali/Desktop/mem.tool
File Actions Edit View Help
Values:
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2011-04-13 00:49:28 UTC+0000
Subkeys:
(S) AppEvents
(S) Console
(S) Control Panel
(S) Environment
(S) Identities
(S) Keyboard Layout
(S) Printers
(S) Software
(S) UNICODE Program Groups
Values:
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
Key name: SAM (S)
Last updated: 2011-04-12 20:31:05 UTC+0000
Subkeys:
(S) SAM
Values:
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Wi
ndows\UsrClass.dat
Key name: S-1-5-20_Classes (S)
Last updated: 2011-04-13 00:55:13 UTC+0000
Subkeys:
(S) Software
Values:


root@kali: /home/kali/Desktop/mem.tool
File Actions Edit View Help
Values:
Registry: [no name]
Key name: HARDWARE (S)
Last updated: 2012-07-22 02:42:25 UTC+0000
Subkeys:
(S) ACPI
(S) DESCRIPTION
(S) DEVICEMAP
(V) RESOURCEMAP
Values:
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
Key name: SECURITY (S)
Last updated: 2012-07-22 02:42:32 UTC+0000
Subkeys:
(S) Policy
(S) RXACT
(V) SAM
Values:
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: $$$PROTO.HIV (S)
Last updated: 2012-07-22 02:42:24 UTC+0000
Subkeys:
(V) CurrentControlSet
Values:
[+] General statistics about the findings:
we have extracted 3367 files from the file we analyzed.
[+]the analyze of the file memdump.mem took to you 219 seconds.
[+]Zipping all the results to zip archive named: 'Your_Results.zip' and his location is your Desktop.

Explanation of output according to the project structure:

1. Automate HDD and Memory Analysis:

1.1 Check the current user; exit if not 'root'

```
[+] To work with the tool in front of us, you need root privileges.
If you are not one, switch to one and run the tool.
In any case, the tool will start by checking your user privileges.
[+] You have root permissions.. let's start ...
```

As we can see the tool explains how to use it but also says that it will be tested. In our case, we have root permission, so the tool starts working.

1.2 Allow the user to specify the filename; check if the file exists

```
[+] Put the file you want to work with into the folder from which you run the tool,
otherwise it will not work properly
[>] Enter the filename you want to analyze: memdump.mem
File 'memdump.mem' exists ... moving on
```

The tool explains the procedure regarding the file you want to analyze, then checks and confirms that the file is indeed found, and the tool progresses.

1.3 Create a function to install the forensics tools if missing.. If the applications are installed already , we dont installing them.

```
Installing tools required for the work. Existing tools will not be reinstalled.
[#] figlet is already installed on your machine.
[#] bulk-extractor is already installed on your machine.
[#] binwalk is already installed on your machine.
[#] foremost is already installed on your machine.
[*] Installing exiftool ...
[#] exiftool installed on your machine.
[#] binutils is already installed on your machine.
[+] Making a new directory called 'Output' on your Desktop
```

The tool installs the carvers, or does not install if they exist. In addition, the tool prepares a folder for the results.

1.4 Use different carvers to automatically extract data..

1.5 Data should be saved into a directory... > Saved to the Dir Output on your Desktop

```
Now we are going to analyze the file you have provided
Please choose the tool you would like to use with, you can choose a specific one or all:
1)exiftool
2)foremost
3)binwalk
4)bulk_extractor
5)strings
6)All
6
All
[+] a file named exiftool is now in the Output directory
[+] a file named foremost is now in the Output directory
[+] a file named binwalk is now in the Output directory
```

```
[+] a file named foremost is now in the Output directory
[+] a file named binwalk is now in the Output directory
[+] a file named bulk_extractor is now in the Output directory
[+] a file named strings is now in the Output directory
[!] we did it!!! ALL INFORMATION IS SAVED
```

As you can see, the tool uses several carvers in order to extract information from the selected file. and then saves the results into a folder we have already created on the desktop.

1.6 Attempt to extract network traffic; if found, display to the user the location and size.

```
Lets look for a network traffic file inside all of the information gathered before
[+] A network traffic file was found and it is located in:  /home/kali/Desktop/Output/bulk_extractor/packets.pcap
File size is: 104K
```

The tool tells the user that it has found such a file and indicates the location and the weight of the file.

1.7 Check for human-readable (exe files, passwords, usernames, etc.).

```
[!] please grovide me the full path to a file wich we will look for special strings in it
/home/kali/Desktop/Output/strings.txt
[!] what strings would you like me to search for you?
.exe
[!] do you have another string you would like to search today?
password
[!] any more?
email
No such strings were found.
```

The tool asks the user for a path to the file he wants to check in order to find readable expressions, the tool performs a search but does not find any.

2. Memory Analysis with Volatility:

2.1 Check if the file can be analyzed in Volatility; if yes, run Volatility

```
[+]Lets try to extract ferther informatiom from the file you have provided with volatility tool
          Suggested Profile(s) : WinXPSP2×86, WinXPSP3×86 (Instantiated with WinXPSP2×86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/mem.tool/memdump.mem)
                      PAE type : PAE
                           DTB : 0×2fe000L
                          KDBG : 0×80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0×ffdff000L
             KUSER_SHARED_DATA : 0×ffdf0000L
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400
[+]we can use volatility, lets start
```

The tool uses one function of the VOLATILITY tool to check that the thing works, the tool issues an output and gives an indication to the user that VOLATILITY can be used

2.2 Find the memory profile and save it into a variable

```
[+]Looks like the operation system of the memory file is WinXPSP2×86
```

The tool gives the user the file profile and the operating system it came from.

2.3 Display the running processes

```
[+]The running processes are:
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
0×81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0×82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0×81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0×823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
0×821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0×82295650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0×821dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 UTC+0000
0×81eb17b8 spoolsv.exe            1512    652     14      113      0      0 2012-07-22 02:42:36 UTC+0000
0×81e7bda0 reader_sl.exe          1640   1484      5       39      0      0 2012-07-22 02:42:36 UTC+0000
0×820e8da0 alg.exe                 788    652      7      104      0      0 2012-07-22 02:43:01 UTC+0000
0×821fcda0 wuauclt.exe            1136   1004      8      173      0      0 2012-07-22 02:43:46 UTC+0000
0×8205bda0 wuauclt.exe            1588   1004      5      132      0      0 2012-07-22 02:44:01 UTC+0000
```

The tool gives the user the processes that are running on the computer.

2.4 Display network connections

```
[+]The network connections are:
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0×02087620 172.16.112.128:1038      41.168.5.140:8080         1484
0×023a8008 172.16.112.128:1037      125.19.103.198:8080       1484
```

The tool gives the user the internet connections the computer was connected to.

2.5 Attempt to extract registry information

```
[+]The registry information is:
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\Microsoft\Windows\Us
rClass.dat
Key name: S-1-5-21-789336058-261478967-1417001333-1003_Classes (S)
Last updated: 2011-04-13 00:53:02 UTC+0000

Subkeys:
  (S) Software

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2012-07-22 02:42:37 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups
  (S) Windows 3.1 Migration Status
  (V) SessionInformation
  (V) Volatile Environment
```

```
Values:
----------------------------
Registry: [no name]
Key name: REGISTRY (S)
Last updated: 2012-07-22 02:42:24 UTC+0000

Subkeys:
  (S) MACHINE
  (S) USER

Values:
----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: $$$PROTO.HIV (S)
Last updated: 2011-04-13 00:40:42 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Wind
ows\UsrClass.dat
Key name: S-1-5-19_Classes (S)
Last updated: 2011-04-13 00:55:13 UTC+0000

Subkeys:
  (S) Software

Values:
```

```
Values:
-------------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: $$$PROTO.HIV (S)
Last updated: 2012-02-18 20:05:13 UTC+0000

Subkeys:
  (S) Adobe
  (S) C07ft5Y
  (S) Classes
  (S) Clients
  (S) Gemplus
  (S) Martin Prikryl
  (S) Microsoft
  (S) ODBC
  (S) Policies
  (S) Program Groups
  (S) Schlumberger
  (S) Secure
  (S) Windows 3.1 Migration Status

Values:
-------------------------------

Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2011-04-13 00:49:16 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups
```

```
Values:
-------------------------------

Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: $$$PROTO.HIV (S)
Last updated: 2011-04-13 00:49:28 UTC+0000

Subkeys:
  (S) AppEvents
  (S) Console
  (S) Control Panel
  (S) Environment
  (S) Identities
  (S) Keyboard Layout
  (S) Printers
  (S) Software
  (S) UNICODE Program Groups

Values:
-------------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
Key name: SAM (S)
Last updated: 2011-04-12 20:31:05 UTC+0000

Subkeys:
  (S) SAM

Values:
-------------------------------

Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: S-1-5-20_Classes (S)
Last updated: 2011-04-13 00:55:13 UTC+0000

Subkeys:
  (S) Software

Values:
-------------------------------
```

```
Values:
-------------------------------

Registry: [no name]
Key name: HARDWARE (S)
Last updated: 2012-07-22 02:42:25 UTC+0000

Subkeys:
  (S) ACPI
  (S) DESCRIPTION
  (S) DEVICEMAP
  (V) RESOURCEMAP

Values:
-------------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
Key name: SECURITY (S)
Last updated: 2012-07-22 02:42:32 UTC+0000

Subkeys:
  (S) Policy
  (S) RXACT
  (V) SAM

Values:
-------------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: $$$PROTO.HIV (S)
Last updated: 2012-07-22 02:42:24 UTC+0000

Subkeys:
  (V) CurrentControlSet

Values:
```

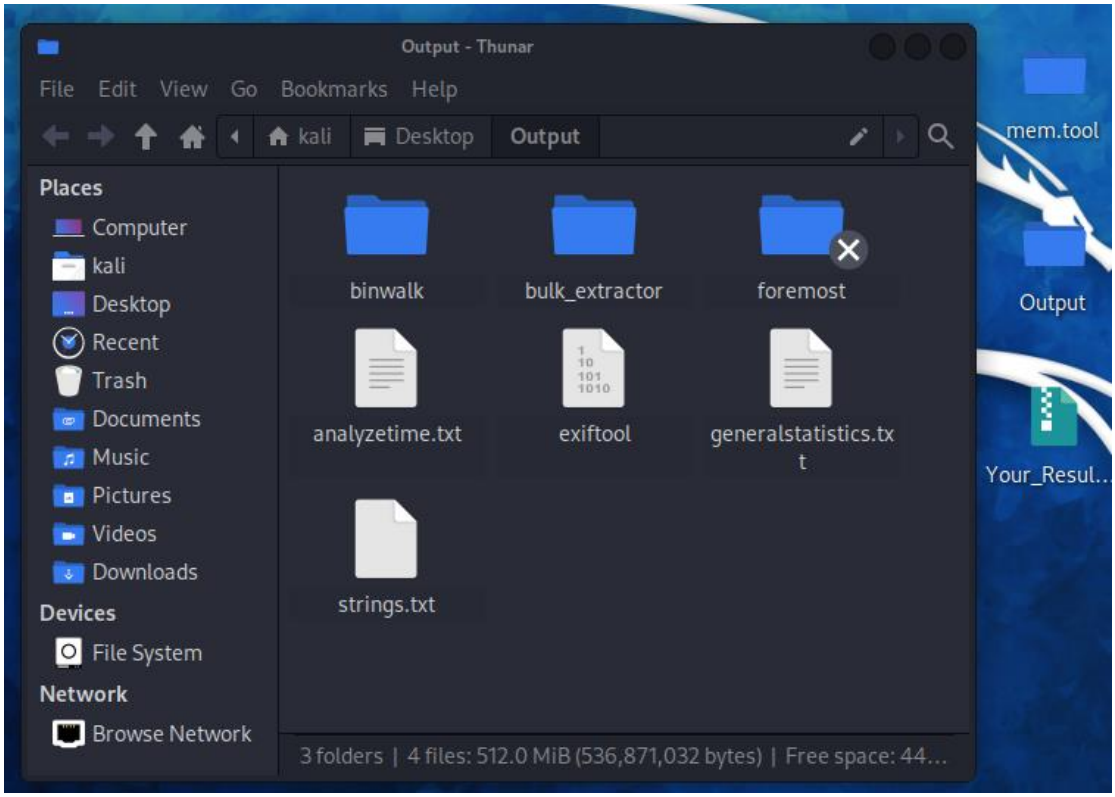
The tool gives the user the details about the registry files

3. Results

3.1 Display general statistics (time of analysis, number of found files, etc.)

3.2 Save all the results into a report (name, files extracted, etc.).

```
[+] General statistics about the findings:
we have extracted 3367 files from the file we analyzed.
[+]the analyze of the file memdump.mem took to you 219 seconds.
```



The tool gives the user details about what he has done and also saves the results properly

3.3 Zip the extracted files and the report file

```
[+]Zipping all the results to zip archive named: 'Your_Results.zip' and his location is your Desktop.
```

The tool takes all the results we got, and puts them in a zip file.