Windows Forensics

Project By Stas Kolbeshkin

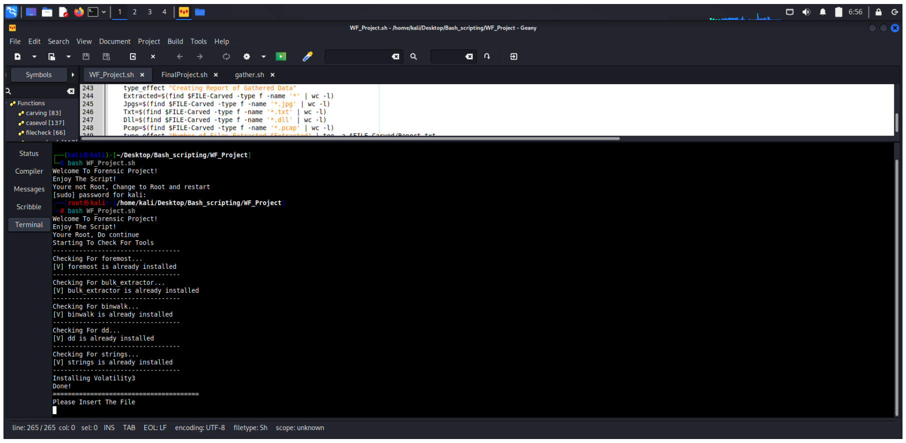
Course ID 7736/31

As part of the studying I was tasked to summarize my knowledge which acquired by attending the classes into automated script of collecting data from various files using various programs.

The project himself have been found enriching by himself, if its founding various versions of OS cannot be reached by some programs or some of the features cannot be accomplished in some of them, all of this knowledge of gathering different pieces of information combined with previous knowledge acquired help me understand more the role of the Cyber Security proffesion.

With the help of our Teacher Doron Zohar I accomplished another step into the amazing word of Cyber security!

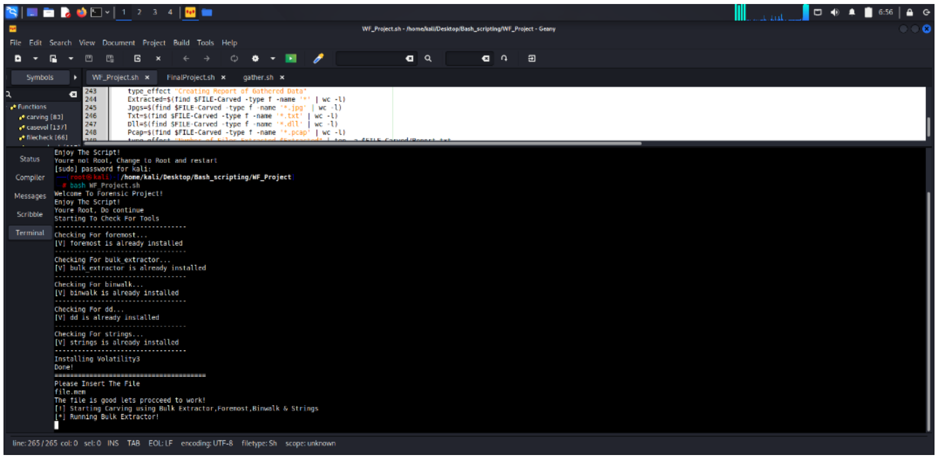
Here are a few pictures of the project!



```
    type_effect "Creating Report of Gathered Data"
    Extracted=$(find $FILE-Carved -type f -name '*' | wc -l)
    Jpgs=$(find $FILE-Carved -type f -name '*.jpg' | wc -l)
    Txt=$(find $FILE-Carved -type f -name '*.txt' | wc -l)
    Dll=$(find $FILE-Carved -type f -name '*.dll' | wc -l)
    Pcap=$(find $FILE-Carved -type f -name '*.pcap' | wc -l)
```

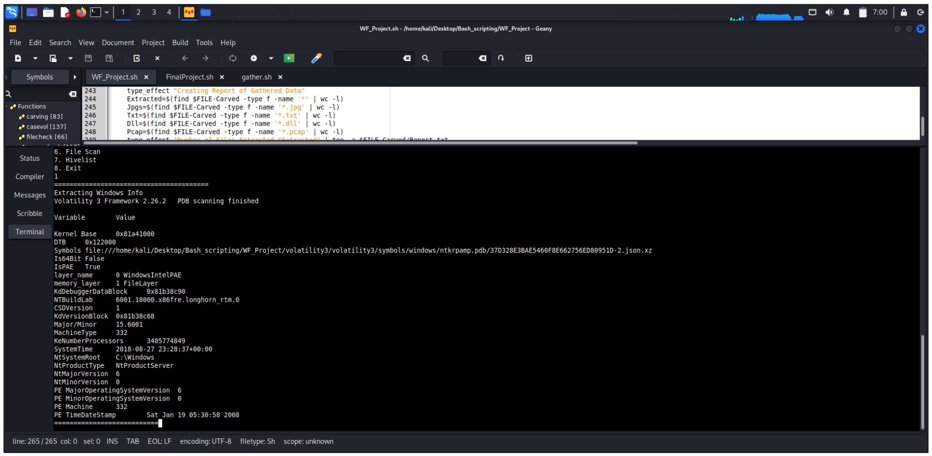
```
┌──(kali㉿kali)-[~/Desktop/Bash_scripting/WF_Project]
└─$ bash WF_Project.sh
Welcome To Forensic Project!
Enjoy The Script!
Youre not Root, Change to Root and restart
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop/Bash_scripting/WF_Project]
└─# bash WF_Project.sh
Welcome To Forensic Project!
Enjoy The Script!
Youre Root, Do continue
Starting To Check For Tools
----------------------------------
Checking For foremost...
[V] foremost is already installed
----------------------------------
Checking For bulk_extractor...
[V] bulk_extractor is already installed
----------------------------------
Checking For binwalk...
[V] binwalk is already installed
----------------------------------
Checking For dd...
[V] dd is already installed
----------------------------------
Checking For strings...
[V] strings is already installed
----------------------------------
Installing Volatility3
Done!
======================================
Please Insert The File
```

line: 265 / 265 col: 0 sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: unknown


WF_Project.sh - /home/kali/Desktop/Bash_scripting/WF_Project - Geany
File Edit Search View Document Project Build Tools Help
Symbols
WF_Project.sh
FinalProject.sh
gather.sh
Functions
carving [83]
casevol [137]
filecheck [66]
Status
Compiler
Messages
Scribble
Terminal
line: 265 / 265 col: 0 sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: unknown

```
    type_effect "Creating Report of Gathered Data"
    Extracted=$(find $FILE-Carved -type f -name '*' | wc -l)
    Jpgs=$(find $FILE-Carved -type f -name '*.jpg' | wc -l)
    Txt=$(find $FILE-Carved -type f -name '*.txt' | wc -l)
    Dll=$(find $FILE-Carved -type f -name '*.dll' | wc -l)
    Pcap=$(find $FILE-Carved -type f -name '*.pcap' | wc -l)
```

```
Enjoy The Script!
Youre not Root, Change to Root and restart
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop/Bash_scripting/WF_Project]
└─# bash WF_Project.sh
Welcome To Forensic Project!
Enjoy The Script!
Youre Root, Do continue
Starting To Check For Tools
---------------------------------
Checking For foremost...
[V] foremost is already installed
---------------------------------
Checking For bulk_extractor...
[V] bulk_extractor is already installed
---------------------------------
Checking For binwalk...
[V] binwalk is already installed
---------------------------------
Checking For dd...
[V] dd is already installed
---------------------------------
Checking For strings...
[V] strings is already installed
---------------------------------
Installing Volatility3
Done!
========================================
Please Insert The File
file.mem
The file is good lets procceed to work!
[!] Starting Carving using Bulk Extractor,Foremost,Binwalk & Strings
[*] Running Bulk Extractor!
```

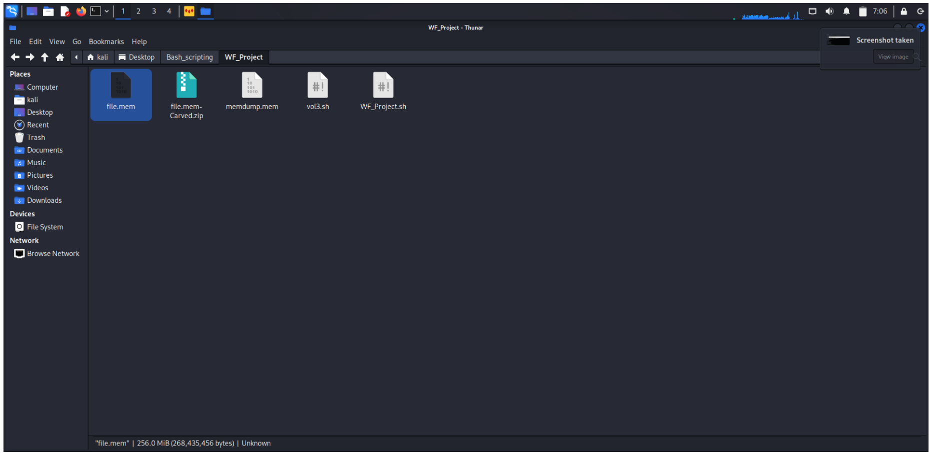

WF_Project.sh - /home/kali/Desktop/Bash_scripting/WF_Project - Geany
File Edit Search View Document Project Build Tools Help
Symbols
WF_Project.sh
FinalProject.sh
gather.sh
Functions
carving [83]
casevol [137]
filecheck [66]
Status
Compiler
Messages
Scribble
Terminal
line: 265 / 265 col: 0 sel: 0 INS TAB EOL: LF encoding: UTF-8 filetype: Sh scope: unknown

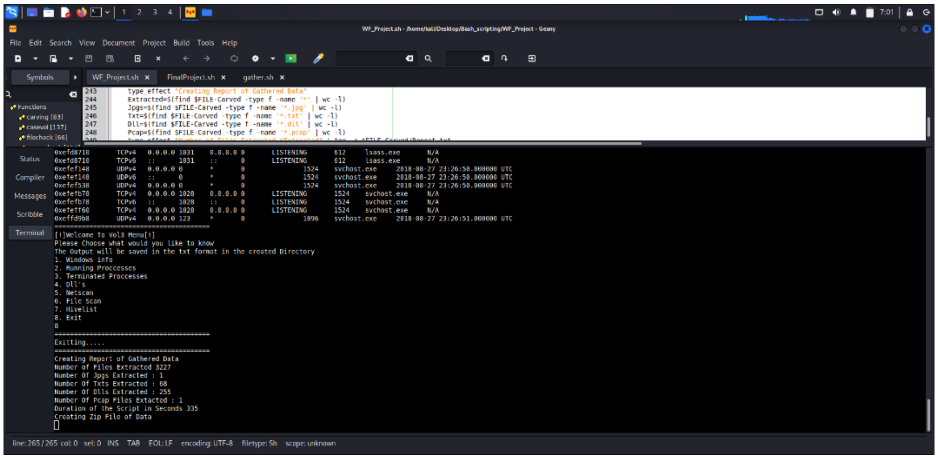
```
    type_effect "Creating Report of Gathered Data"
    Extracted=$(find $FILE-Carved -type f -name '*' | wc -l)
    Jpgs=$(find $FILE-Carved -type f -name '*.jpg' | wc -l)
    Txt=$(find $FILE-Carved -type f -name '*.txt' | wc -l)
    Dll=$(find $FILE-Carved -type f -name '*.dll' | wc -l)
    Pcap=$(find $FILE-Carved -type f -name '*.pcap' | wc -l)
```

```
6. File Scan
7. Hivelist
8. Exit
1
========================================
Extracting Windows Info
Volatility 3 Framework 2.26.2   PDB scanning finished

Variable        Value

Kernel Base     0x81a41000
DTB     0x122000
Symbols file:///home/kali/Desktop/Bash_scripting/WF_Project/volatility3/volatility3/symbols/windows/ntkrpamp.pdb/37D328E3BAE5460F8E662756ED80951D-2.json.xz
Is64Bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x81b38c90
NTBuildLab      6001.18000.x86fre.longhorn_rtm.0
CSDVersion      1
KdVersionBlock  0x81b38c68
Major/Minor     15.6001
MachineType     332
KeNumberProcessors      3405774849
SystemTime      2018-08-27 23:28:37+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductServer
NtMajorVersion  6
NtMinorVersion  0
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  0
PE Machine      332
PE TimeDateStamp        Sat Jan 19 05:30:58 2008
==========================
```





```
    type_effect "Creating Report of Gathered Data"
    Extracted=$(find $FILE-Carved -type f -name '*' | wc -l)
    Jpgs=$(find $FILE-Carved -type f -name '*.jpg' | wc -l)
    Txt=$(find $FILE-Carved -type f -name '*.txt' | wc -l)
    Dll=$(find $FILE-Carved -type f -name '*.dll' | wc -l)
    Pcap=$(find $FILE-Carved -type f -name '*.pcap' | wc -l)
```

```
0xefd8710       TCPv4   0.0.0.0 1031    0.0.0.0 0       LISTENING       612     lsass.exe       N/A
0xefd8710       TCPv6   ::      1031    ::      0       LISTENING       612     lsass.exe       N/A
0xefef148       UDPv4   0.0.0.0 0       *       0               1524    svchost.exe     2018-08-27 23:26:50.000000 UTC
0xefef148       UDPv6   ::      0       *       0               1524    svchost.exe     2018-08-27 23:26:50.000000 UTC
0xefef538       UDPv4   0.0.0.0 0       *       0               1524    svchost.exe     2018-08-27 23:26:50.000000 UTC
0xefefb78       TCPv4   0.0.0.0 1028    0.0.0.0 0       LISTENING       1524    svchost.exe     N/A
0xefefb78       TCPv6   ::      1028    ::      0       LISTENING       1524    svchost.exe     N/A
0xefeff60       TCPv4   0.0.0.0 1028    0.0.0.0 0       LISTENING       1524    svchost.exe     N/A
0xeffd9b8       UDPv4   0.0.0.0 123     *       0               1096    svchost.exe     2018-08-27 23:26:51.000000 UTC
========================================
[!]Welcome To Vol3 Menu[!]
Please Choose what would you like to know
The Output will be saved in the txt format in the created Directory
1. Windows info
2. Running Proccesses
3. Terminated Proccesses
4. Dll's
5. Netscan
6. File Scan
7. Hivelist
8. Exit
8
========================================
Exitting.....
========================================
Creating Report of Gathered Data
Number of Files Extracted 3227
Number Of Jpgs Extracted : 1
Number Of Txts Extracted : 68
Number Of Dlls Extracted : 255
Number Of Pcap Files Extacted : 1
Duration of the Script in Seconds 335
Creating Zip File of Data
```