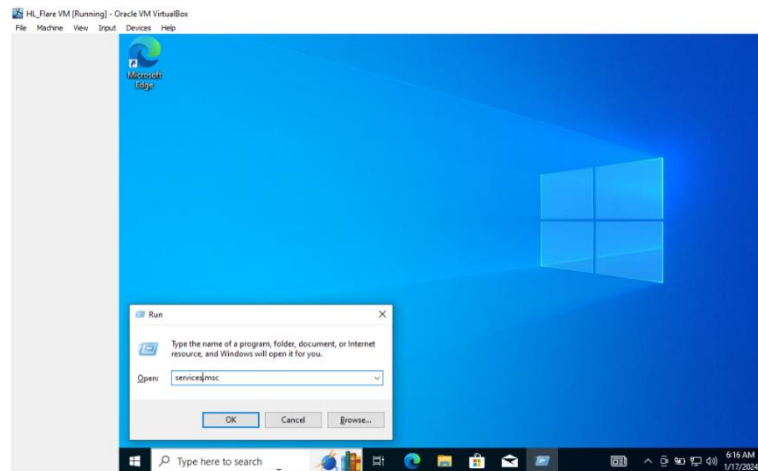


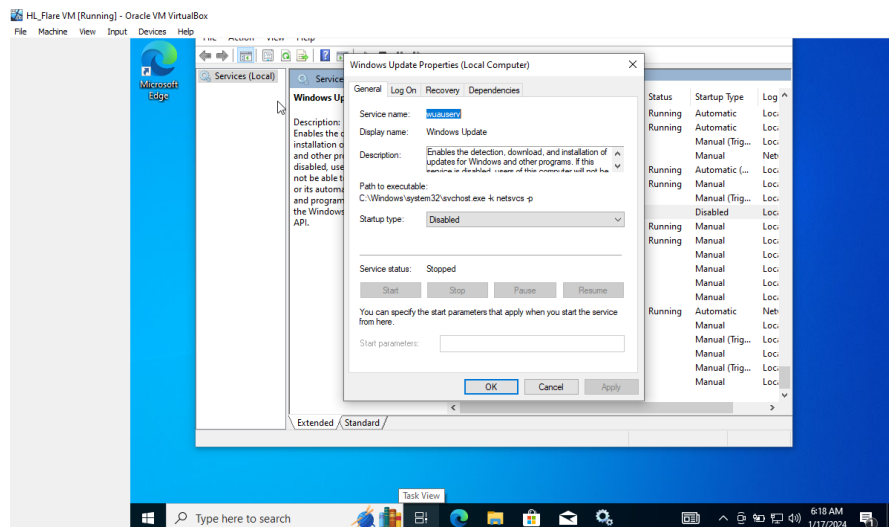
# Static Malware Analysis and Disassembly with WannaCry Ransomware

## Preparation for creating a sandbox virtual environment

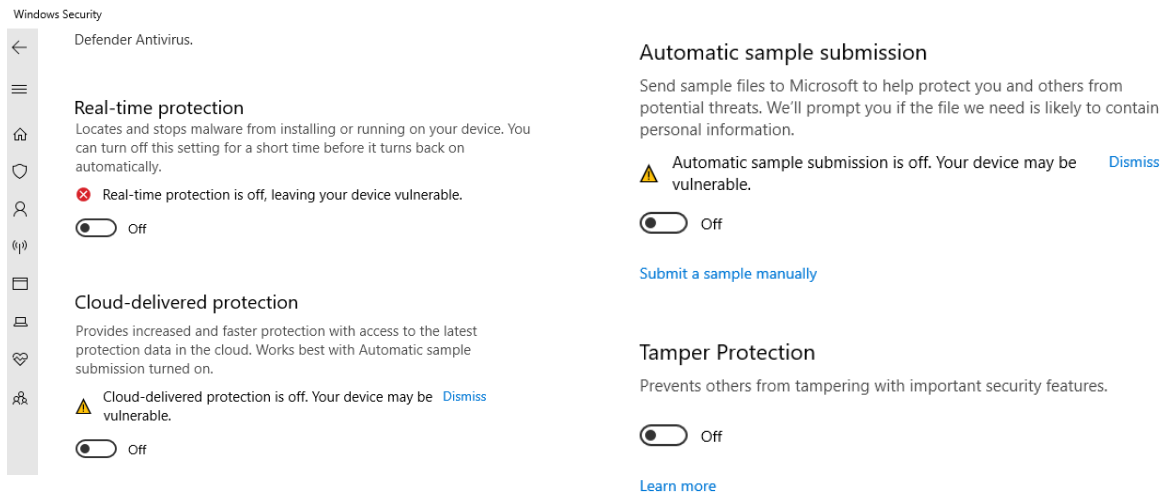
1. The first stage after installing the windows operating system on the virtualbox, some settings will be made by opening services.msc in the Run feature.



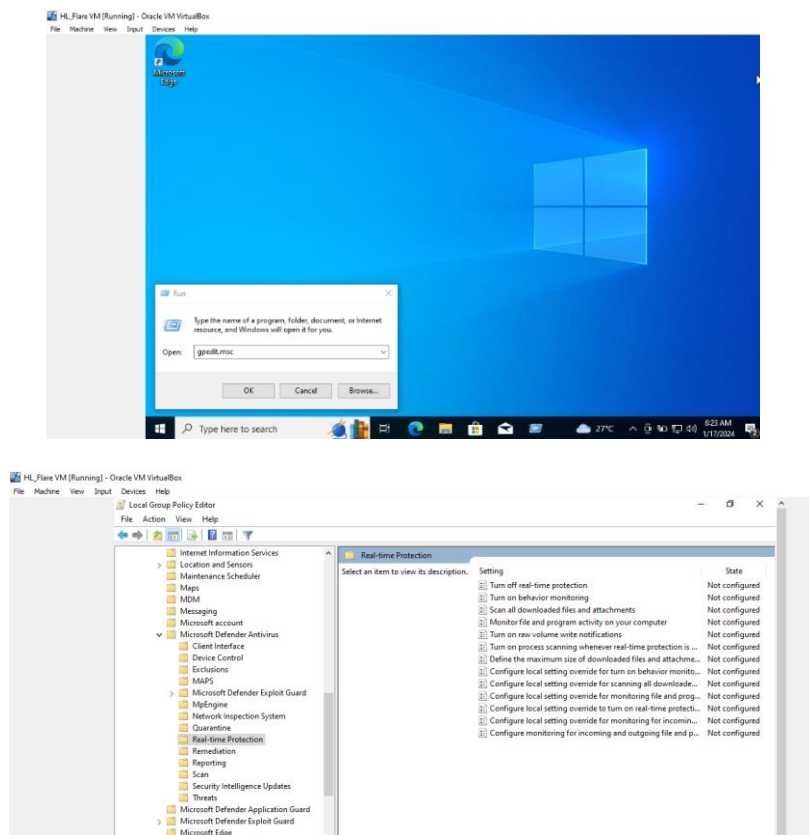
2. Then set the status type to Disabled and the services status to stopped on windows update. Then click ok.

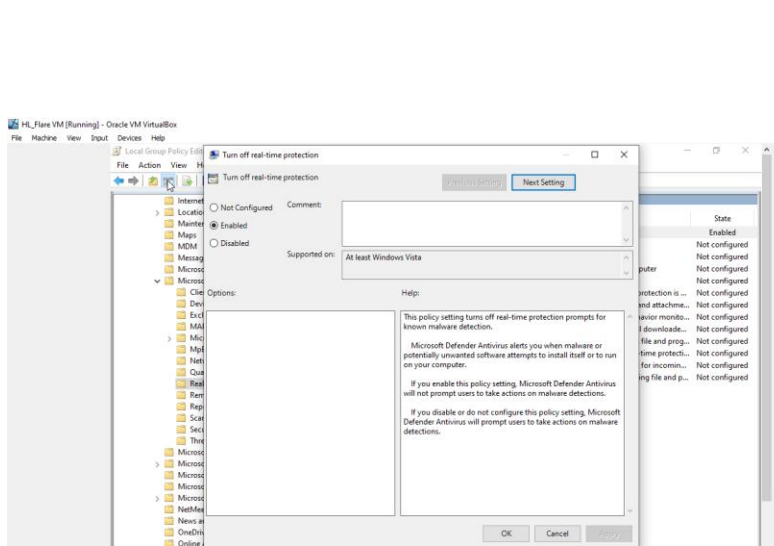


3. Next, do not activate the antivirus defender on windows security as shown below.

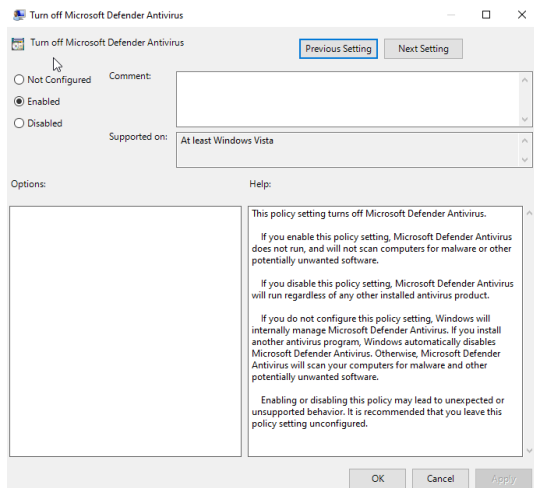


4. In the Run feature open gpedit.msc which refers to Real time Protection and select enabled on Turn off real time protection.

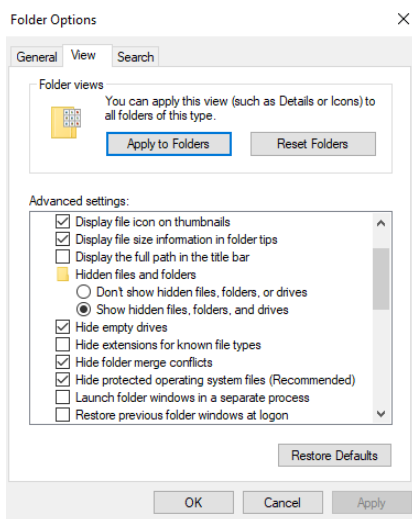




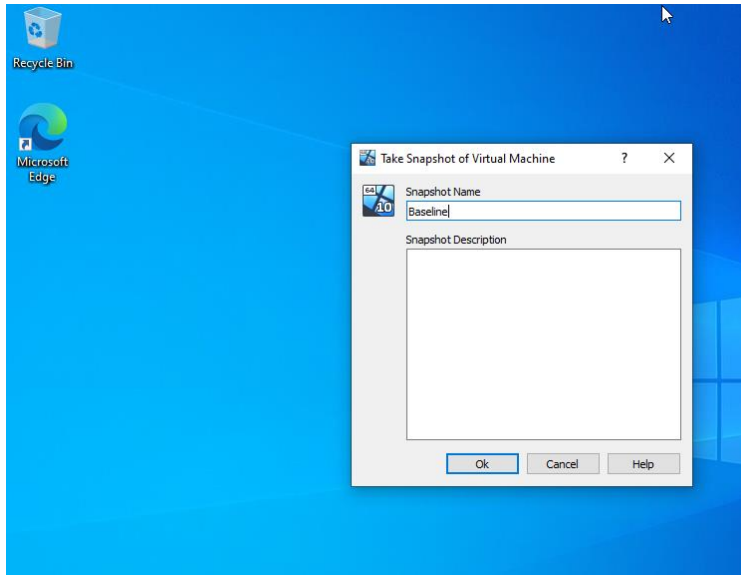
5. In the Turn off Microsoft Defender Antivirus section, select Enabled.



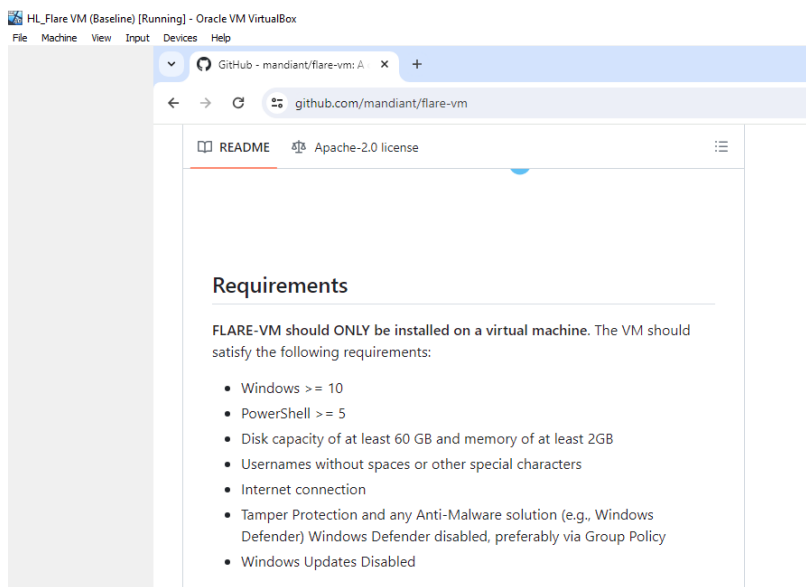
6. In the Turn off Microsoft Defender Antivirus section, select Enabled.



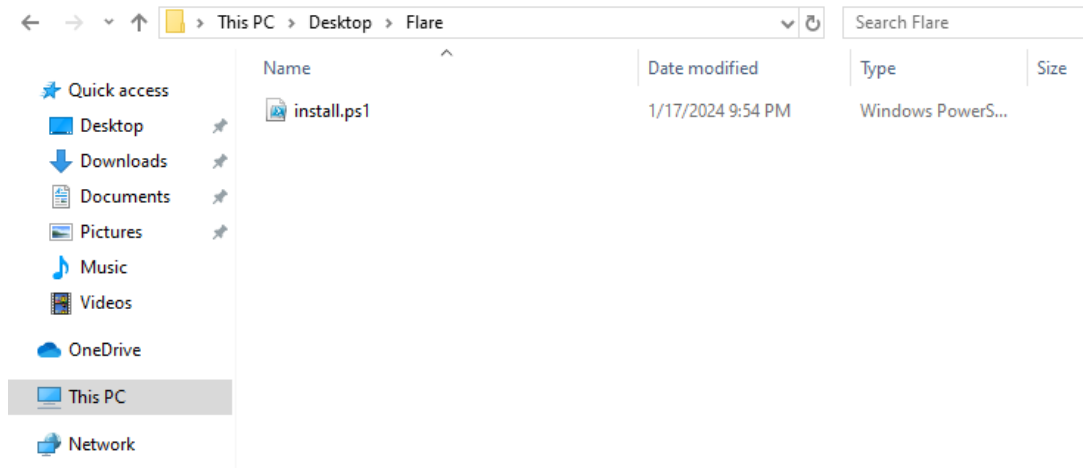
7. After making these settings. We take a snapshot so that it is stored in the virtual machine.



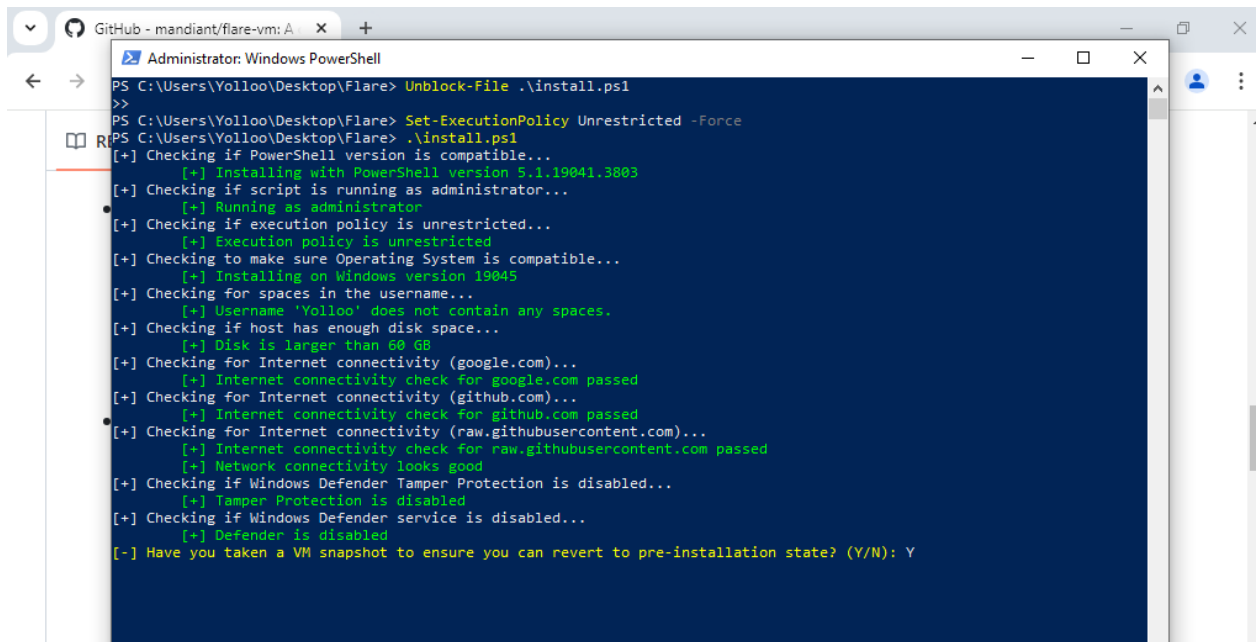
8. On google we will open the flare VM GitHub to install on the windows operating system by following some requirements as follows.



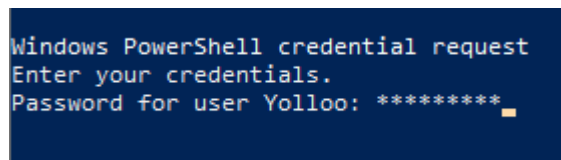
- Download install.ps1 from flare VM GitHub



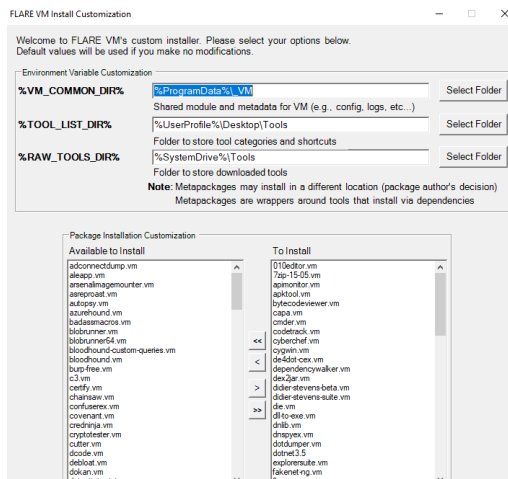
- In PowerShell windows enter the following command to install the flare VM.



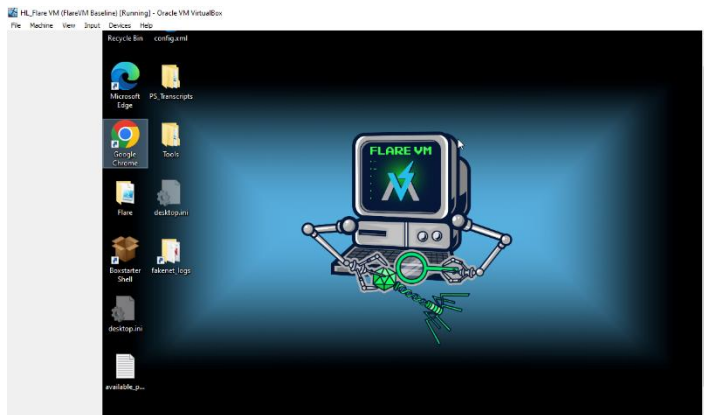
- Enter the user password to login to the flare VM.



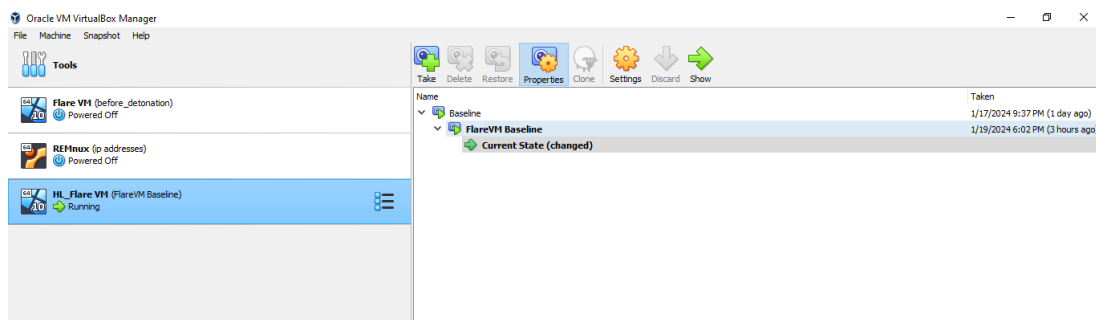
12. During the install process, Flare VM custom will appear and click ok.



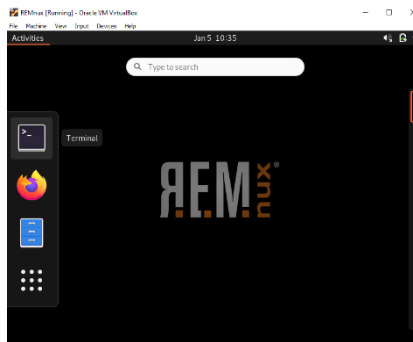
13. After the installation process is complete, the desktop will appear as follows.



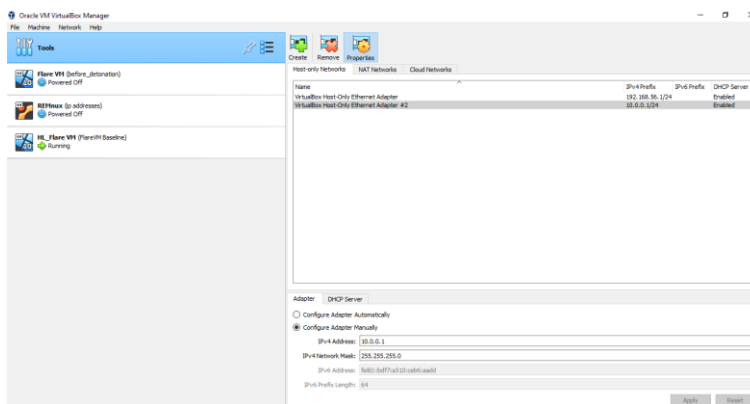
14. Take a snapshot to save the VM flare.



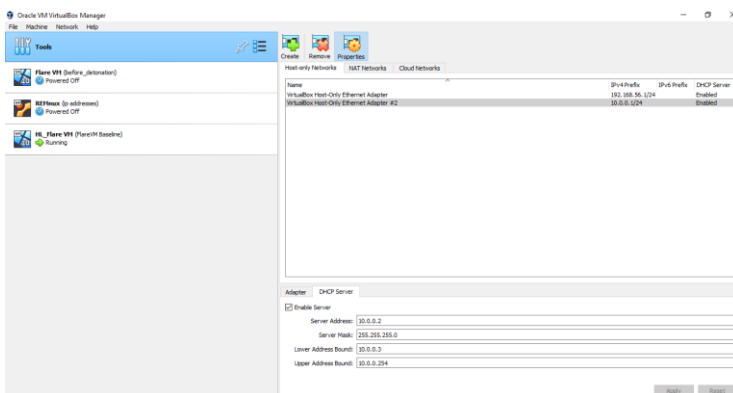
15. After downloading Remnux.ova Install Remnux on the VirtualBox.



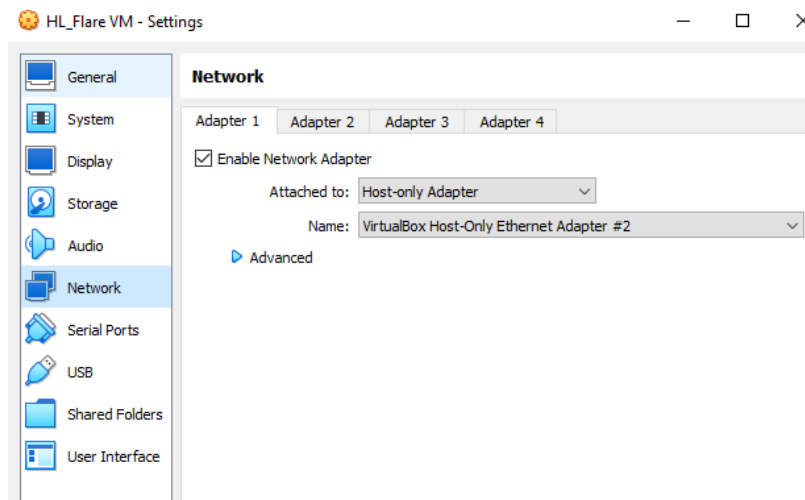
16. In Network VirtualBox add VirtualBox host only ethernet adapter 2. Then in the adapter section select configure adapter manually and enter the IP address.



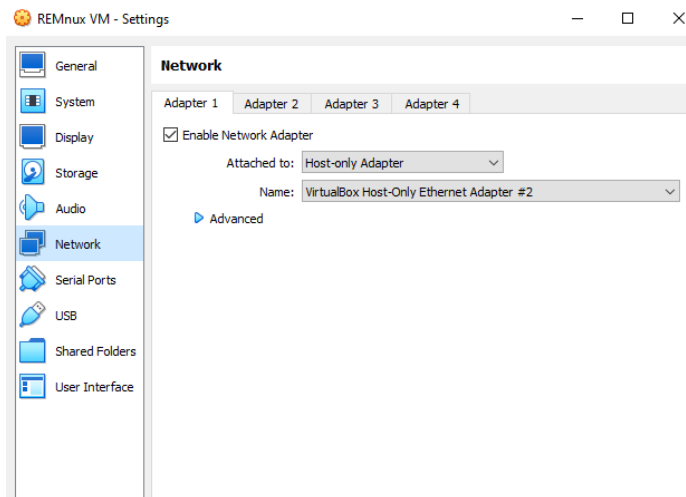
17. On the DHCP server enter the IP Address



18. On the flare VM network adapter select host only adapter with name referring to ethernet adapter 2.



19. On the Remnux VM network adapter select host only adapter and name.



20. In Remnux, check the IP address

```
remnux@remnux:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:11:97:67 brd ff:ff:ff:ff:ff:ff
```



21. Enter the following commands for network management.

```
remnux@remnux:~$ sudo vim /etc/netplan/01-netcfg.yaml
```

22. Set dhcp4 to false and addresses to 10.0.0.3/24.

```
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s17:
      dhcp4: false
      addresses: [10.0.0.3/24]
```

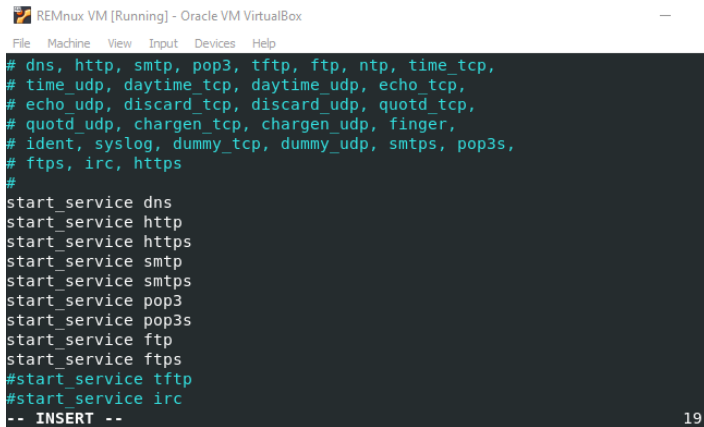
23. After making the settings. Enter the sudo netplan apply command and check the IP address again.

```
remnux@remnux:~$ sudo netplan apply
remnux@remnux:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:11:97:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.3/24 brd 10.0.0.255 scope global enp0s17
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe11:9767/64 scope link
        valid_lft forever preferred_lft forever
```

24. Use inetsim to create a controlled environment for malware analysis.

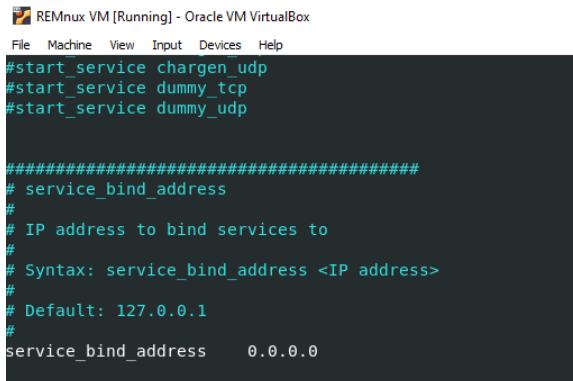
```
remnux@remnux:~$ sudo vim /etc/inetsim/inetsim.conf
```

25. Enable start service as follows.



```
REMnux VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
#start_service tftp
#start_service irc
-- INSERT --
```

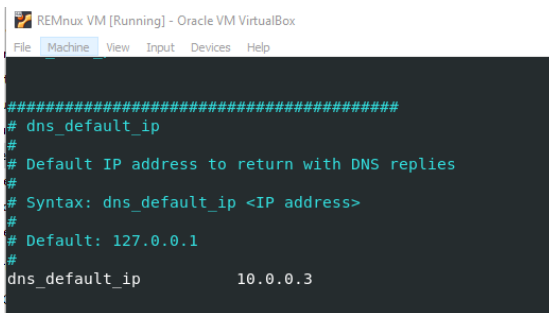
26. Set the service bind address to 0.0.0.0.



```
REMnux VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0
```

27. Set the default dns IP to 10.0.0.3.



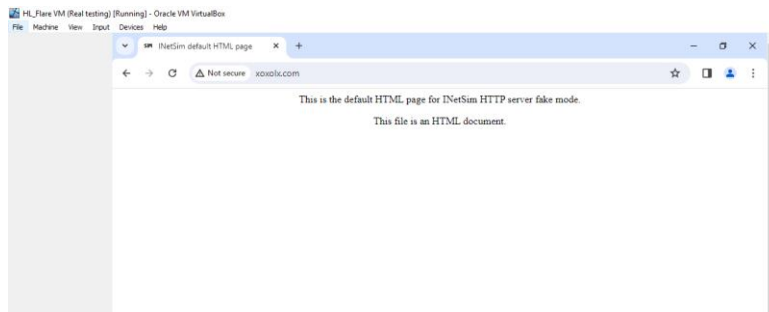
```
REMnux VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 10.0.0.3
```

## 28. Run inetsim on the Remnux VM.

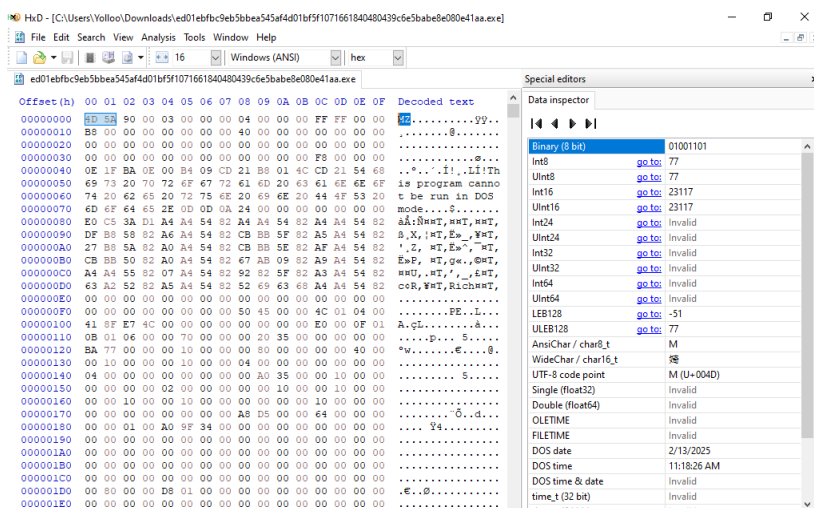
```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1516) ===
Session ID: 1516
Listening on: 10.0.0.3
Real Date/Time: 2024-01-22 05:28:33
Fake Date/Time: 2024-01-22 05:28:33 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1520)
* smtp_25_tcp - started (PID 1523)
* smtps_465_tcp - started (PID 1524)
* ftp_21_tcp - started (PID 1527)
* ftps_990_tcp - started (PID 1528)
* https_443_tcp - started (PID 1522)
* pop3_110_tcp - started (PID 1525)
* pop3s_995_tcp - started (PID 1526)
* http_80_tcp - started (PID 1521)
done.
Simulation running.
```

## 29. Then open google on flare VM and enter the domain, it will display the default inetsim which indicates that it is connected to the Remnux VM.

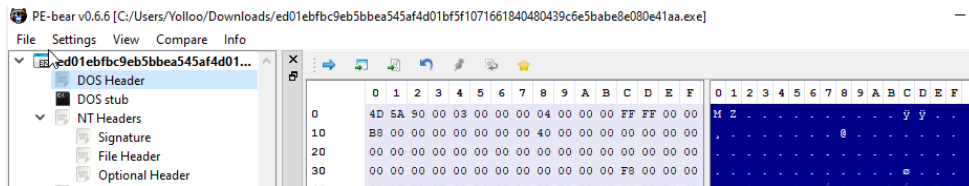


## Malware static analysis

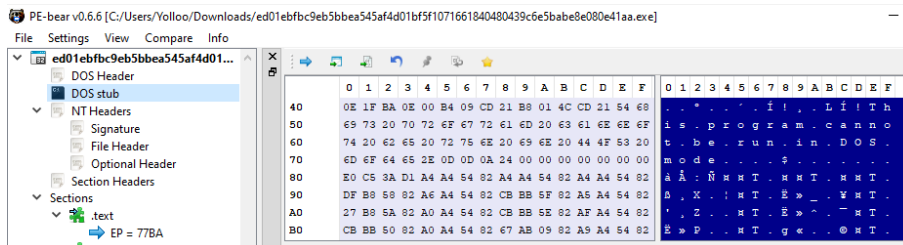
1. Determined PE file type based on hex signatures of 4D 5A with decoded text MZ. This indicates a DOS MZ executable.



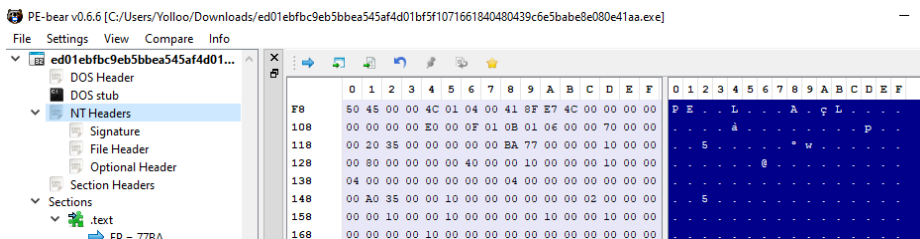
2. Using the PE bear tool which can also be used to find out the DOS Header.



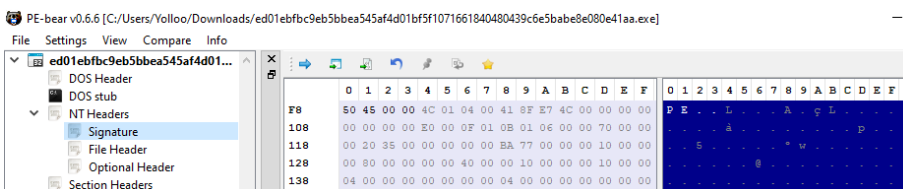
3. DOS stub is an MS-DOS program that prints an error message saying that the executable is not compatible with DOS then exits.



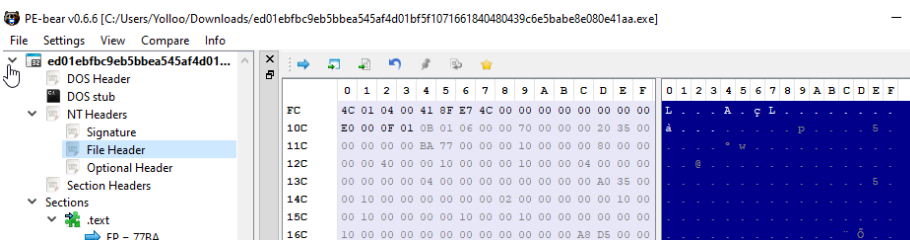
4. The NT header consists of a signature, a file header, and an optional header.



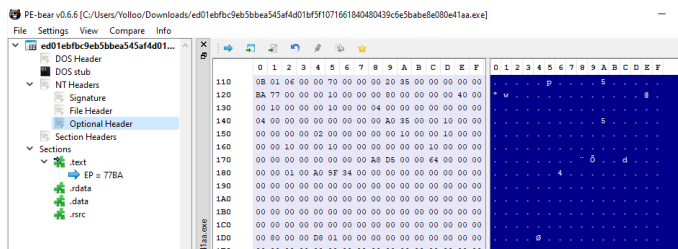
5. PE signature is a DWORD (4-bytes) that identifies the file as a PE image.



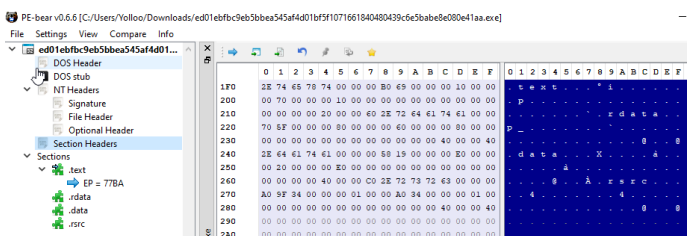
6. File Header contains important information about the PE file.



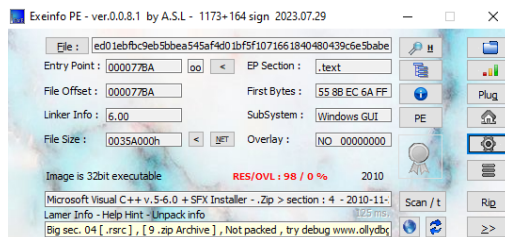
7. Optional Header is the most important part of the NT Headers. It contains a lot of information critical to the execution of the PE file, including the data directories.



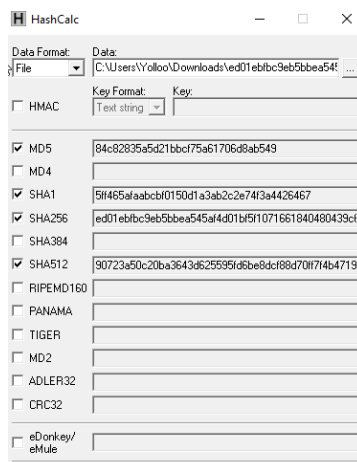
8. The Section Table contains one Section Header per row. Each Section Header contains important information about the PE file sections.



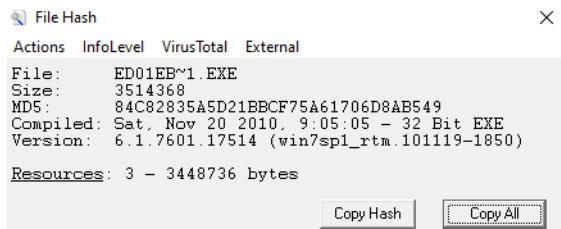
9. Detect packaged or unpacked malware samples.



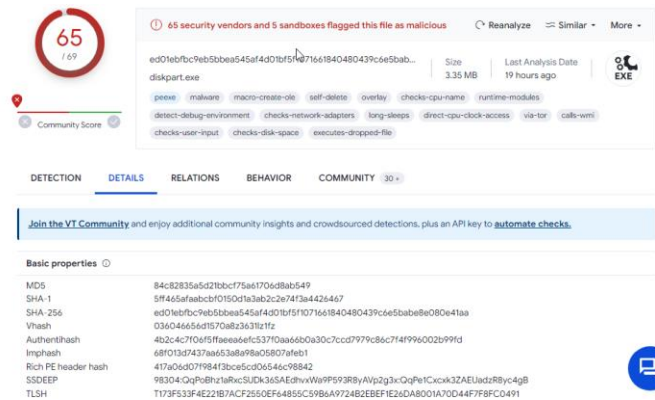
10. Finds the hash of the ransomware consisting of MD5, SHA1, SHA256, SHA512.



11. Copy the MD5 hash of the WannaCry ransomware exe file.



12. Input the copied hash into Virus Total for scanning and it will obtain a score of 65 security vendors and display other detailed information.



13. In Virus Total, we can look at the history section regarding the creation time to first submission of the ransomware.

MD5	84c82835a5d21bbc7f5a61706d8ab549
SHA-1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA-256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Vhash	036046656d1570a82363121f2
Authenthash	4b2c4c7f06f5ffaeae6efc537f0aa66b0a30c7cc97979c86c7f4f996002b99fd
Imphash	68f013d7437aa653a8a98a05807afeb1
Rich PE header hash	417a06d07f984f3bce5cd06546c98842
SSDEEP	98304:QqPoBhztalRxcSUDK36SAEdhvxWw9P593R8yAVp2g3x:QqPe1Cxxk3ZAEUadzR8yc4gB
TLSH	T173F533F4E221B7ACF2550EF64855C59B6A972482EBEF1E26DA8001A70D44F7F8FC0491
File type	Win32 EXE   executable   windows   win32   pe   peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%)   Microsoft Visual C++ compiled executable (generic) (20%)   Win6...
DetectItEasy	PE32   Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32]   Compiler: Microsoft Visual C/C++ (12.00.9782) ...
File size	3.35 MB (3514368 bytes)
PEID packer	Microsoft Visual C++
<b>History</b>	
Creation Time	2010-11-20 09:05:05 UTC
First Seen In The Wild	2016-05-16 15:27:03 UTC
First Submission	2017-05-12 07:31:10 UTC
Last Submission	2024-01-23 05:34:30 UTC
Last Analysis	2024-01-23 02:46:05 UTC

14. Showing various filenames of the WannaCry ransomware.

```
Names
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
diskpart.exe
SuperKeyPass.exe
tai lieu can sua.docx.EXE
WannaCry.EXE
Ransomware.WannaCry.exe
Volcado1.bin
WannaCry_Original_MD5.EXE
Muestra1_Volcado1.bin
recursoExtraido
Ransomware_wannacry.exe
WannaCrypt0r.exe
qq.exe
wanna-cry-sample-ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.pdf
Proforma Invoice and Bank swift-REG.P1-0086547654.exe
Muestra1.exe_R_1831_1033.bin.bin
wannaCry
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.pdf
notch_mod.exe
Endermanch@WannaCrypt0r.exe
ultra.exe
R-muestra1.bin
wannacry.exe
```

15. Extract the WannaCry ransomware string with the Floss tool into a txt file.

```
FLOSS
examples:
  extract all strings from an executable
  floss suspicious.exe

do not extract static strings
  floss --no static -- suspicious.exe

only extract stack and tight strings
  floss --only stack tight -- suspicious.exe

FLARE-VM Thu 01/25/2024 14:36:14.04
C:\Users\Yolloo\Desktop>floss C:\Users\Yolloo\Downloads\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe > flossOut.txt
INFO: floss: extracting static strings
finding decoding function features: 100% 137/137 [00:00<00:00, 292.40 functions/s, skipped 6 library functions (4%)]
INFO: floss.stackstrings: extracting stackstrings from 102 functions
INFO: floss.results: software\
extracting stackstrings: 100% 102/102 [00:03<00:00, 33.31 functions/s]
INFO: floss.tightstrings: extracting tightstrings from 13 functions...
extracting tightstrings from function 0x406880: 100% 13/13 [00:08<00:00, 1.48 functions/s]
INFO: floss.string_decoder: decoding strings
emulating function 0x403a28 (call 2/2): 100% 22/22 [00:07<00:00, 3.13 functions/s]
INFO: floss: finished execution after 80.45 seconds
INFO: floss: rendering results
```

16. The txt file displays the number of static strings and stack strings.

```
flossOut.txt - Notepad
File Edit Format View Help

+-----+-----+
| file path | C:\Users\Yolloo\Downloads\ed01ebfbc9eb5bbea545af4... |
| identified language | unknown |
| extracted strings | |
|   static strings | 43921 (206215 characters) |
|   language strings | 0 ( 0 characters) |
| stack strings | 1 |
| tight strings | 0 |
| decoded strings | 0 |
+-----+-----+
```

17. The following displays the strings from the WannaCry ransomware file. One of them is  
This program cannot be run in DOS mode.

```
flossOut.txt - Notepad
File Edit Format View Help
+-----+
| FLOSS STATIC STRINGS: ASCII (43727) |
+-----+

!This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
.rsrc
49t$
TWj
PWWh
tE9u
PWWh
SWjcf
X_^[
X_^[
^t19
QPPH
tXVP
w>wV
X_^]
```

18. In that string there are several important DLLs namely Kernel32.dll, User32.dll, Advapi32.dll, Shell32.dll, Ws2\_32.dll.

```
flossOut.txt - Notepad
File Edit Format View Help
KERNEL32.dll
wsprintfA
USER32.dll
RegCloseKey
RegQueryValueExA
RegSetValueExA
RegCreateKeyW
CryptReleaseContext
CreateServiceA
CloseServiceHandle
StartServiceA
OpenServiceA
OpenSCManagerA
ADVAPI32.dll
SHELL32.dll
OLEAUT32.dll
WS2_32.dll
```

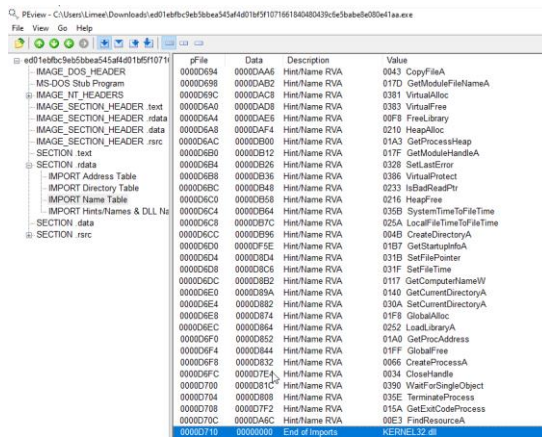
19. In Advapi32.dll there are several functions such as CreateServiceA, OpenServiceA, StartServiceA, CloseServiceHandle, CryptReleaseContext and others.

Preview - C:\Users\Linkee\Downloads\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c5e5babe8e080e41aa.exe

	pFile	Data	Description	Value
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c5e5babe8e080e41aa.exe				
IMAGE_DOS_HEADER	0000060C	0000DC2A	Hint/Name RVA	0064 CreateServiceA
MS-DOS Stub Program	00000610	0000DC52	Hint/Name RVA	01AF OpenServiceA
IMAGE_NT_HEADERS	00000614	0000DC52	Hint/Name RVA	0249 StartServiceA
IMAGE_SECTION_HEADER.text	00000618	0000DC3C	Hint/Name RVA	003E CloseServiceHandle
IMAGE_SECTION_HEADER.rdata	0000061C	0000DC14	Hint/Name RVA	00A0 CryptReleaseContext
IMAGE_SECTION_HEADER.data	00000620	0000DC04	Hint/Name RVA	01D3 RegCreateKeyW
IMAGE_SECTION_HEADER.rsrc	00000624	0000DBF2	Hint/Name RVA	0204 RegSetValueExA
SECTION.text	00000628	0000DBDE	Hint/Name RVA	01F7 RegQueryValueExA
SECTION.rdata	0000062C	0000DBD0	Hint/Name RVA	01CB RegCloseKey
IMPORT Address Table	00000630	0000DC72	Hint/Name RVA	01AD OpenSCManagerA
IMPORT Directory Table	00000634	00000000	End of Imports	ADVAPI32.dll

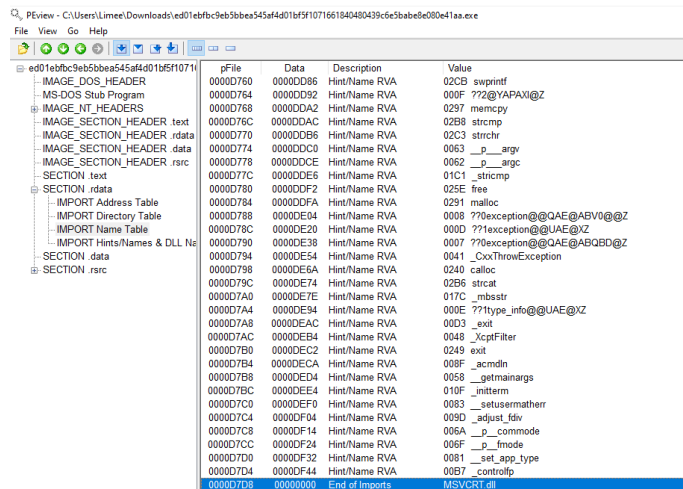


20. In kernel32.dll there are several functions such as CopyFileA, GetModuleFileNameA, VirtualAlloc, etc.



pFile	Data	Description	Value
0000D694	0000DAA6	Hint/Name RVA	0043 CopyFileA
0000D698	0000DAB2	Hint/Name RVA	0170 GetModuleFileNameA
0000D69C	0000DAC8	Hint/Name RVA	0381 VirtualAlloc
0000D6A0	0000DAD8	Hint/Name RVA	0383 VirtualFree
0000D6A4	0000DAE8	Hint/Name RVA	00F8 FreeLibrary
0000D6A8	0000DAF4	Hint/Name RVA	0210 HeapAlloc
0000D6AC	0000DB00	Hint/Name RVA	01A3 GetProcessHeap
0000D6B0	0000DB12	Hint/Name RVA	017F GetModuleHandleA
0000D6B4	0000DB26	Hint/Name RVA	0228 SetLastError
0000D6B8	0000DB36	Hint/Name RVA	0386 VirtualProtect
0000D6BC	0000DB48	Hint/Name RVA	0233 IsBadReadPtr
0000D6C0	0000DB58	Hint/Name RVA	0216 HeapFree
0000D6C4	0000DB64	Hint/Name RVA	025B SystemTimeToFileTime
0000D6C8	0000DB7C	Hint/Name RVA	025A LocalFileTimeToFileTime
0000D6CC	0000DB96	Hint/Name RVA	004B CreateDirectoryA
0000D6D0	0000DBF5E	Hint/Name RVA	01BD GetStartupInfoA
0000D6D4	0000DBD4	Hint/Name RVA	031B SetFilePointer
0000D6D8	0000DBD6	Hint/Name RVA	031F SetFileTime
0000D6DC	0000DBE2	Hint/Name RVA	0117 GetComputerNameW
0000D6E0	0000DB9A	Hint/Name RVA	0140 GetCurrentDirectoryA
0000D6E4	0000DB82	Hint/Name RVA	030A SetCurrentDirectoryA
0000D6E8	0000DB74	Hint/Name RVA	01F8 GlobalAlloc
0000D6EC	0000DB64	Hint/Name RVA	0252 LoadLibraryA
0000D6F0	0000DB52	Hint/Name RVA	0140 GetProcAddress
0000D6F4	0000DB44	Hint/Name RVA	01FF GlobalFree
0000D6F8	0000DB32	Hint/Name RVA	0066 CreateProcessA
0000D6FC	0000DB7E	Hint/Name RVA	0034 CloseHandle
0000D700	0000DB1C	Hint/Name RVA	0360 WaitForSingleObject
0000D704	0000DB08	Hint/Name RVA	035E TerminateProcess
0000D708	0000DBF2	Hint/Name RVA	015A GetExitCodeProcess
0000D70C	0000DBAC	Hint/Name RVA	00E3 FindResourceA
0000D710	00000000	End of imports	kernel32.dll

21. In MSVCRT.dll there are several functions contained in the value column.



pFile	Data	Description	Value
0000D760	0000DB86	Hint/Name RVA	02CB wprintf
0000D764	0000DD92	Hint/Name RVA	000F 772@YAPAXI@Z
0000D768	0000DDA2	Hint/Name RVA	0297 memcpy
0000D76C	0000DDAC	Hint/Name RVA	02B8 strcmp
0000D770	0000DB86	Hint/Name RVA	02C3 strchr
0000D774	0000DDC0	Hint/Name RVA	0063 _p_argv
0000D778	0000DDCE	Hint/Name RVA	0062 _p_argc
0000D77C	0000DDE6	Hint/Name RVA	01C1 _stricmp
0000D780	0000DDF2	Hint/Name RVA	025E free
0000D784	0000DDFA	Hint/Name RVA	0291 malloc
0000D788	0000DE04	Hint/Name RVA	0008 770exception@@@QAE@ABV0@@Z
0000D78C	0000DE20	Hint/Name RVA	0000 771exception@@@QAE@AZ
0000D790	0000DE38	Hint/Name RVA	0007 770exception@@@QAE@ABQBD@Z
0000D794	0000DE54	Hint/Name RVA	0041 _CxxThrowException
0000D798	0000DE6A	Hint/Name RVA	0240 calloc
0000D79C	0000DE74	Hint/Name RVA	02B6 strcat
0000D7A0	0000DE7E	Hint/Name RVA	017C _mbstr
0000D7A4	0000DE94	Hint/Name RVA	000E 771type_info@@@QAE@XZ
0000D7A8	0000DEAC	Hint/Name RVA	00D3 _exit
0000D7AC	0000DEB4	Hint/Name RVA	0048 _JcvtFilter
0000D7B0	0000DEC2	Hint/Name RVA	0249 _exit
0000D7B4	0000DECA	Hint/Name RVA	008F _acmdln
0000D7B8	0000DED4	Hint/Name RVA	0058 _getmainargs
0000D7BC	0000DEE4	Hint/Name RVA	010F _initterm
0000D7C0	0000DEF0	Hint/Name RVA	0063 _setusermatherr
0000D7C4	0000DF04	Hint/Name RVA	009D _adjust_fdw
0000D7C8	0000DF14	Hint/Name RVA	006A _p_commode
0000D7CC	0000DF24	Hint/Name RVA	006F _p_fmode
0000D7D0	0000DF32	Hint/Name RVA	0081 _set_app_type
0000D7D4	0000DF44	Hint/Name RVA	00B7 _controlfp
0000D7D8	00000000	End of imports	MSVCRT.dll

22. In User32.dll there is a function in the form of wprintfA

0000D7DC	0000DBB8	Hint/Name RVA	02D7 wprintfA
0000D7E0	00000000	End of imports	USER32.dll

# Disassembly Analysis using Ghidra

## 1. Finds the list of strings in the Ghidra.

Defined Strings - 382 items			
Location	String Value	String Representation	Data Type
00400000	MZ	"MZ"	char[2]
004000f8	PE	"PE"	char[4]
004001f0	.text	".text"	char[8]
00400218	.idata	".idata"	char[8]
00400240	.data	".data"	char[8]
00400268	.rsrc	".rsrc"	char[8]
0040ce3c	inflate 1.1.3 Copyr...	"inflate 1.1.3 Copyr..."	ds
0040d453	- unzip 0.15 Copyr...	"- unzip 0.15 Copyr..."	ds
0040d76e	CloseHandle	"CloseHandle"	ds
0040d7f4	GetExitCodeProcess	"GetExitCodeProcess"	ds
0040d80a	TerminateProcess	"TerminateProcess"	ds
0040d81e	WaitForSingleObject	"WaitForSingleObject"	ds
0040d834	CreateProcessA	"CreateProcessA"	ds
0040d846	GlobalFree	"GlobalFree"	ds
0040d854	GetProcAddress	"GetProcAddress"	ds
0040d866	LoadLibraryA	"LoadLibraryA"	ds
0040d876	GlobalAlloc	"GlobalAlloc"	ds
0040d884	GetCurrentDirectoryA	"GetCurrentDirectoryA"	ds
0040d89c	GetCurrentDirectoryA	"GetCurrentDirectoryA"	ds
0040d8b4	GetComputerNameW	"GetComputerNameW"	ds
0040d8c8	SetFileTime	"SetFileTime"	ds
0040d8d6	SetFilePointer	"SetFilePointer"	ds

Defined Strings - 382 items			
Location	String Value	String Representation	Data Type
0040db98	CreateDirectoryA	"CreateDirectoryA"	ds
0040dbaa	KERNEL32.dll	"KERNEL32.dll"	ds
0040dbba	wsprintfA	"wsprintfA"	ds
0040dbc4	USER32.dll	"USER32.dll"	ds
0040dbd2	RegCloseKey	"RegCloseKey"	ds
0040dbe0	RegQueryValueExA	"RegQueryValueExA"	ds
0040dbf4	RegSetValueExA	"RegSetValueExA"	ds
0040dc06	RegCreateKeyW	"RegCreateKeyW"	ds
0040dc16	CryptReleaseContext	"CryptReleaseCont..."	ds
0040dc2c	CreateServiceA	"CreateServiceA"	ds
0040dc3e	CloseServiceHandle	"CloseServiceHandle"	ds
0040dc54	StartServiceA	"StartServiceA"	ds
0040dc64	OpenServiceA	"OpenServiceA"	ds
0040dc74	OpenSCManagerA	"OpenSCManagerA"	ds
0040dc84	ADVAPI32.dll	"ADVAPI32.dll"	ds
0040dc92	SHELL32.dll	"SHELL32.dll"	ds
0040dc9e	OLEAUT32.dll	"OLEAUT32.dll"	ds
0040dcac	WS2_32.dll	"WS2_32.dll"	ds
0040dcba	fclose	"fclose"	ds
0040dcc4	fwrite	"fwrite"	ds
0040dccc	fread	"fread"	ds
0040dcd6	fopen	"fopen"	ds

Defined Strings - 382 items			
Location	String Value	String Representation	Data Type
0040deb94	CloseHandle	"CloseHandle"	ds
0040eba0	DeleteFileW	"DeleteFileW"	ds
0040ebac	MoveFileExW	"MoveFileExW"	ds
0040ebb8	MoveFileW	"MoveFileW"	ds
0040ebc4	ReadFile	"ReadFile"	ds
0040ebd0	WriteFile	"WriteFile"	ds
0040ebdc	CreateFileW	"CreateFileW"	ds
0040ebf8	kernel32.dll	"kernel32.dll"	ds
0040f0c4	Microsoft Enhanced RSA and AES Cry...	"Microsoft Enhanced RSA and AES Cryptographic Provider"	ds
0040f0c4	CryptGenKey	"CryptGenKey"	ds
0040f0d0	CryptDecrypt	"CryptDecrypt"	ds
0040f0e0	CryptEncrypt	"CryptEncrypt"	ds
0040f0f0	CryptDestroyKey	"CryptDestroyKey"	ds
0040f100	CryptImportKey	"CryptImportKey"	ds
0040f110	CryptAcquireContextA	"CryptAcquireContextA"	ds
0040f42c	cmd.exe /c "%s"	"cmd.exe /c \"%s\""	ds
0040f440	115p7UMHngojzPmVqHjRdfJN0j6LrLn	"115p7UMHngojzPmVqHjRdfJN0j6LrLn"	ds
0040f464	129fDPgmuZ9NvMgw519p7AA8gr...	"129fDPgmuZ9NvMgw519p7AA8gr..."	ds
0040f488	138M4WZdhvrgicQeporWt5Quy6H...	"138M4WZdhvrgicQeporWt5Quy6H..."	ds
0040f4b4	Global\Win\WinZonesCacheCounterMut...	"Global\Win\WinZonesCacheCounterMut..."	ds
0040f4d8	tasksche.exe	"tasksche.exe"	ds
0040f4e8	TaskStart	"TaskStart"	ds

## 2. In the decompiled file there is a WinMain function as the entry point of the application. Inside this function has several other functions that can be analyzed.

```
hPrevInstance = (HINSTANCE)0x0;  
hInstance = GetModuleHandleA(LPCSTR)0x0;  
exit_code = WinMain(hInstance,hPrevInstance,(LPSTR)lpCmdLine,nShowCmd);  
/* WARNING: Subroutine does not return */  
exit(exit_code);
```

## 3. In the Char\_0040f538 function there is a /i command to copy the running binary.

```
if (*args == 2) {  
    slash_i = CHAR_0040f538;  
    args = (int *)_p_argv();  
    is_argv_slash_i = strcmp((char *)(*args + 4), (char *)slash_i);  
    if ((is_argv_slash_i == 0) &&  
        (bVar1 = FUN_00401b5f((wchar_t *)0x0, CONCAT31(extraout_var,bVar1) != 0)) {  
        CopyFileA(local_210,s_tasksche.exe_0040f4d8,0);  
        DVar2 = GetFileAttributesA(s_tasksche.exe_0040f4d8);  
        if ((DVar2 != 0xffffffff) && (is_argv_slash_i = FUN_00401f5d(), is_argv_slash_i != 0)) {  
            return 0;  
        }  
    }  
}
```

CHAR_0040f538			
0040f538	bf	??	2Fh /
0040f539	69	??	69h i
0040f53a	00	??	00h
0040f53b	00	??	00h

4. In the FUN\_004010fd function there is a registry key program that generates a key name in the form of u\_Software\\.

```

undefined4 __cdecl FUN_004010fd(int param_1)
{
    size_t sVar1;
    LSTATUS LVar2;
    int iVar3;
    undefined4 *puVar4;
    undefined4 *puVar5;
    bool bVar6;
    HKEY hKey;
    BYTE local_2e0;
    undefined4 local_2df;
    undefined4 local_d8 [5];
    undefined4 local_c4 [45];
    DWORD local_10;
    int local_c;
    HKEY local_8;

    puVar4 = (undefined4 *)u_Software\0040e04c;
    puVar5 = local_d8;
    for (iVar3 = 5; iVar3 != 0; iVar3 = iVar3 + -1)
        *puVar5 = *puVar4;
    puVar4 = puVar4 + 1;

    RegCreateKeyW(hKey, (LPCWSTR)local_d8, &local_8);
    if (local_8 != (HKEY)0x0) {
        if (param_1 == 0) {
            local_10 = 0x207;
            LVar2 = RegQueryValueExA(local_8, &DAT_0040e030, (LPDWORD)
                                     &local_10);
            bVar6 = LVar2 == 0;
            if (bVar6) {
                SetCurrentDirectoryA((LPCSTR)&local_2e0);
            }
        }
        else {
            GetCurrentDirectoryA(0x207, (LPSTR)&local_2e0);
            sVar1 = strlen((char *)&local_2e0);
            LVar2 = RegSetValueExA(local_8, &DAT_0040e030, 0, 1, &loca
                                     bVar6 = LVar2 == 0;
        }
        RegCloseKey(local_8);
        if (bVar6) {
            return 1;
        }
    }
}

```

MOV	ESI, u_Software\0040e04c				
POP	ECX				
LEA	EDI, 0040e04d				
MOVSD, REP	ESI, 0040e04c				
PUSH	0x1				
XOR	EAX, 0040e04c	53 00 6f	unicode	u"Software\\"	
AND	bytd, 00 66 00	74 00 77	...		
POP	ECX	0040e060	70 eb 40 00	addr	u_.doc_0040eb70
LEA	EDI, 0040e064	64 eb 40 00	addr	u_.docx_0040eb64	
		0040e068	58 eb 40 00	addr	u_.docb_0040eb58
AND	dword, 0040e06c	4c eb 40 00	addr	u_.docm_0040eb4c	
STOSD, REP	ESI, 0040e070	40 eb 40 00	addr	u_.dot_0040eb40	
MOV	ECX, 0040e074	34 eb 40 00	addr	u_.dotm_0040eb34	
		0040e078	28 eb 40 00	addr	u_.dotx_0040eb28
		0040e07c	1c eb 40 00	addr	u_.xls_0040eb1c
		0040e080	10 eb 40 00	addr	u_.xlsx_0040eb10
		0040e084	04 eb 40 00	addr	u_.xlsm_0040eb04
		0040e088	f8 ea 40 00	addr	u_.xlsb_0040eaf8
		0040e08c	ec ea 40 00	addr	u_.xlw_0040eae4
		0040e090	e0 ea 40 00	addr	u_.xlt_0040eae0
		0040e094	d4 ea 40 00	addr	u_.xlm_0040ead4

5. Found the password WNcry@2017 to extract additional information in the form of XIA.

```

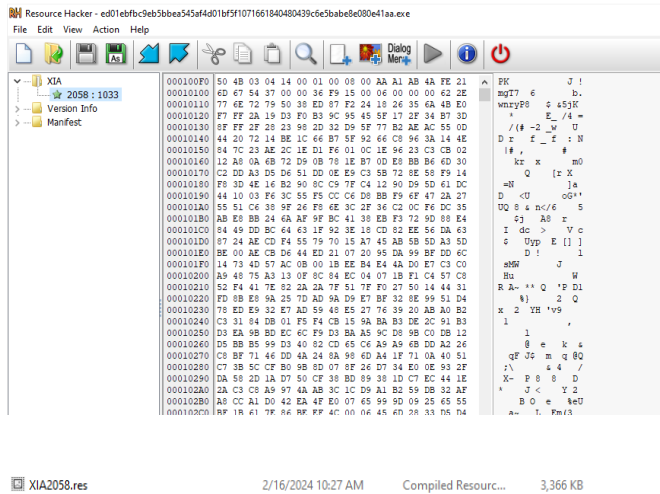
undefined4 __cdecl extract_resource(HMODULE const_0)
{
    HRSRC hResInfo;
    HGLOBAL hResData;
    LPVOID pvVar1;
    DWORD DVar2;
    int *piVar3;
    int iVar4;
    int iVar5;
    undefined4 *puVar6;
    char *pcVar7;
    undefined4 in_stack_00000008;
    int local_130;
    undefined4 local_12c [74];

    hResInfo = FindResourceA(const_0, (LPCSTR)2058, &XIA_Res_);
    if (((hResInfo != (HRSRC)0x0) &&
        (hResData = LoadResource(const_0, hResInfo), hResData)
        (pvVar1 = LockResource(hResData), pvVar1 != (LPVOID))
        DVar2 = SizeofResource(const_0, hResInfo);
        piVar3 = (int *)FUN_004075ad(pvVar1, DVar2, in_stack_00000008);

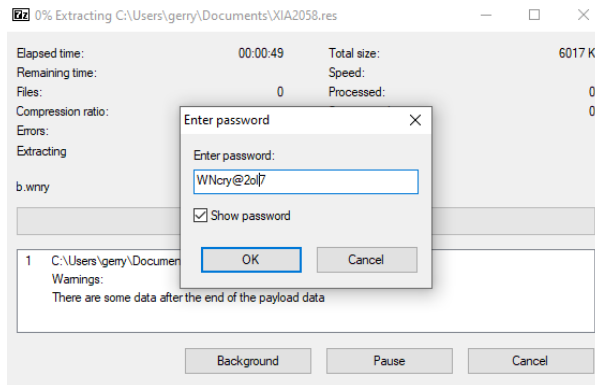
```

CALL	0040f52c	57 4e 63	ds	"WNcry@2017"	XREF[1]
PUSH	EBX	72 79 40			
CALL	0040f537	00	??	00h	

6. Compressed resources using Resource Hacker that contain XIA files.



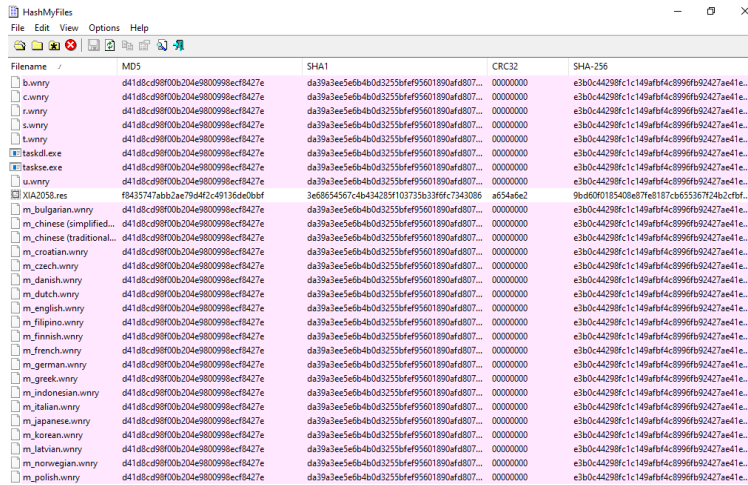
7. Enter the password WNcry@2o17 to open the XIA file.



8. The XIA file displays several files as follows.

	Name	Date modified	Type	Size
Quick access	msg	2/16/2024 10:32 AM	File folder	
Desktop	b.wnry	2/16/2024 10:30 AM	WNRY File	0 KB
Downloads	c.wnry	5/11/2017 4:11 AM	WNRY File	0 KB
Documents	r.wnry	5/10/2017 11:59 PM	WNRY File	0 KB
Pictures	s.wnry	5/9/2017 12:58 AM	WNRY File	0 KB
Gradle	t.wnry	5/11/2017 10:22 AM	WNRY File	0 KB
Music	taskdl.exe	5/11/2017 10:22 AM	Application	0 KB
Videos	taskse.exe	5/11/2017 10:22 AM	Application	0 KB
This PC	u.wnry	5/11/2017 10:22 AM	WNRY File	0 KB
Network	XIA2058.res	2/16/2024 10:27 AM	Compiled Resour...	3,366 KB

## 9. Checking the file hash on all data in XIA



Filename	MD5	SHA1	CRC32	SHA-256
b.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
c.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
l.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
l.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
l.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
taskd.exe	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
taskse.exe	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
b.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
3A2558.res	f8485747abb2ae79942c49136de06bf	3e8854567c4b434289107735b398fc734086	a654ab62	9b406018540e07e1187cb65536772462cfbf...
m_bulgarian.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_chinese (simplified...)	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_chinese (traditional...)	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_croatian.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_czech.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_danish.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_dutch.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_english.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_filipino.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_finnish.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_french.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_german.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_greek.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_indonesian.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_italian.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_japanese.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_korean.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_latvian.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_lithuanian.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...
m_polish.wnry	d418dc98f00b204a980099ecf8427e	da39a3ee5e6b404d3255fe9560190af807...	00000000	e3b0c44298fc1c149af4c8996fb92427ae41e...

## 10. Opens the b.wnry file in the form of background from WannaCry ransomware



## 11. The c.wnry file has C2 servers in the form of onion websites and the link for the Tor browser. On ghidra there are also onion addresses.

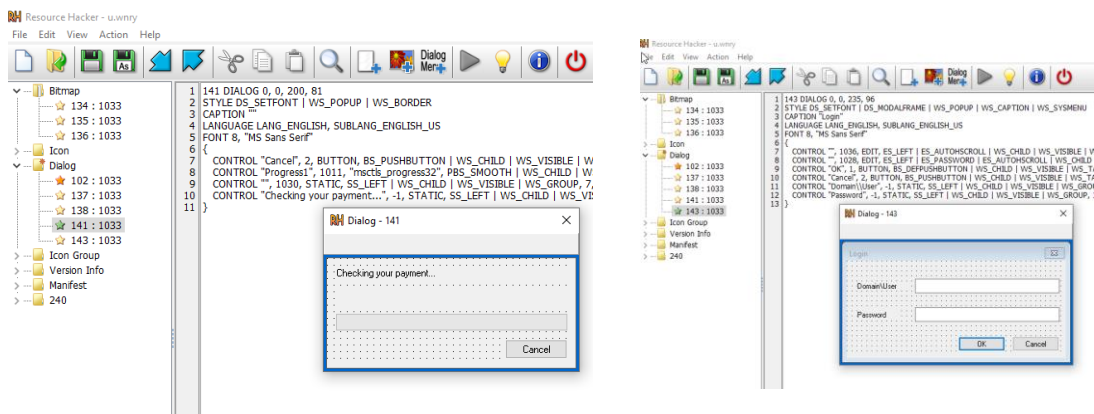
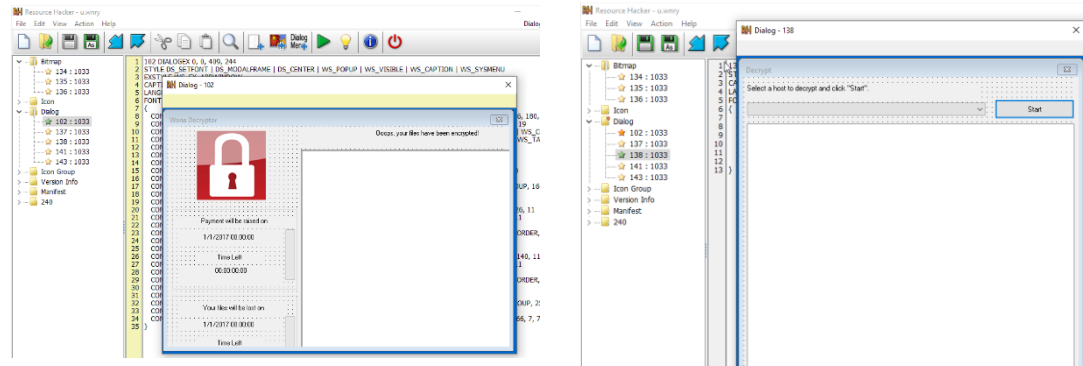
The image shows the Ghidra decompiler interface. At the top, the menu bar includes 'File', 'Edit', 'Search', 'View', 'Analysis', 'Tools', 'Window', and 'Help'. Below the menu bar is a toolbar with icons for file operations, search, and analysis. The main window is divided into two panes. The left pane shows the 'Decoded text' view, displaying a series of null bytes followed by some non-null bytes. The right pane shows the 'Data inspector' view, displaying a list of variables and their values. The 'Data inspector' view includes a 'Special editors' panel with a 'Binary (0x 00)' section. The 'Binary (0x 00)' section shows a list of variables and their values, including 'init', 'init1', 'init2', 'init3', 'init4', 'init5', 'init6', 'init7', 'init8', 'init9', 'init10', 'init11', 'init12', 'init13', 'init14', 'init15', 'init16', 'init17', 'init18', 'init19', 'init20', 'init21', 'init22', 'init23', 'init24', 'init25', 'init26', 'init27', 'init28', 'init29', 'init30', 'init31', 'init32', 'init33', 'init34', 'init35', 'init36', 'init37', 'init38', 'init39', 'init40', 'init41', 'init42', 'init43', 'init44', 'init45', 'init46', 'init47', 'init48', 'init49', 'init50', 'init51', 'init52', 'init53', 'init54', 'init55', 'init56', 'init57', 'init58', 'init59', 'init60', 'init61', 'init62', 'init63', 'init64', 'init65', 'init66', 'init67', 'init68', 'init69', 'init70', 'init71', 'init72', 'init73', 'init74', 'init75', 'init76', 'init77', 'init78', 'init79', 'init80', 'init81', 'init82', 'init83', 'init84', 'init85', 'init86', 'init87', 'init88', 'init89', 'init90', 'init91', 'init92', 'init93', 'init94', 'init95', 'init96', 'init97', 'init98', 'init99', 'init100', 'init101', 'init102', 'init103', 'init104', 'init105', 'init106', 'init107', 'init108', 'init109', 'init110', 'init111', 'init112', 'init113', 'init114', 'init115', 'init116', 'init117', 'init118', 'init119', 'init120', 'init121', 'init122', 'init123', 'init124', 'init125', 'init126', 'init127', 'init128', 'init129', 'init130', 'init131', 'init132', 'init133', 'init134', 'init135', 'init136', 'init137', 'init138', 'init139', 'init140', 'init141', 'init142', 'init143', 'init144', 'init145', 'init146', 'init147', 'init148', 'init149', 'init150', 'init151', 'init152', 'init153', 'init154', 'init155', 'init156', 'init157', 'init158', 'init159', 'init160', 'init161', 'init162', 'init163', 'init164', 'init165', 'init166', 'init167', 'init168', 'init169', 'init170', 'init171', 'init172', 'init173', 'init174', 'init175', 'init176', 'init177', 'init178', 'init179', 'init180', 'init181', 'init182', 'init183', 'init184', 'init185', 'init186', 'init187', 'init188', 'init189', 'init190', 'init191', 'init192', 'init193', 'init194', 'init195', 'init196', 'init197', 'init198', 'init199', 'init200', 'init201', 'init202', 'init203', 'init204', 'init205', 'init206', 'init207', 'init208', 'init209', 'init210', 'init211', 'init212', 'init213', 'init214', 'init215', 'init216', 'init217', 'init218', 'init219', 'init220', 'init221', 'init222', 'init223', 'init224', 'init225', 'init226', 'init227', 'init228', 'init229', 'init230', 'init231', 'init232', 'init233', 'init234', 'init235', 'init236', 'init237', 'init238', 'init239', 'init240', 'init241', 'init242', 'init243', 'init244', 'init245', 'init246', 'init247', 'init248', 'init249', 'init250', 'init251', 'init252', 'init253', 'init254', 'init255', 'init256', 'init257', 'init258', 'init259', 'init260', 'init261', 'init262', 'init263', 'init264', 'init265', 'init266', 'init267', 'init268', 'init269', 'init270', 'init271', 'init272', 'init273', 'init274', 'init275', 'init276', 'init277', 'init278', 'init279', 'init280', 'init281', 'init282', 'init283', 'init284', 'init285', 'init286', 'init287', 'init288', 'init289', 'init290', 'init291', 'init292', 'init293', 'init294', 'init295', 'init296', 'init297', 'init298', 'init299', 'init300', 'init301', 'init302', 'init303', 'init304', 'init305', 'init306', 'init307', 'init308', 'init309', 'init310', 'init311', 'init312', 'init313', 'init314', 'init315', 'init316', 'init317', 'init318', 'init319', 'init320', 'init321', 'init322', 'init323', 'init324', 'init325', 'init326', 'init327', 'init328', 'init329', 'init330', 'init331', 'init332', 'init333', 'init334', 'init335', 'init336', 'init337', 'init338', 'init339', 'init340', 'init341', 'init342', 'init343', 'init344', 'init345', 'init346', 'init347', 'init348', 'init349', 'init350', 'init351', 'init352', 'init353', 'init354', 'init355', 'init356', 'init357', 'init358', 'init359', 'init360', 'init361', 'init362', 'init363', 'init364', 'init365', 'init366', 'init367', 'init368', 'init369', 'init370', 'init371', 'init372', 'init373', 'init374', 'init375', 'init376', 'init377', 'init378', 'init379', 'init380', 'init381', 'init382', 'init383', 'init384', 'init385', 'init386', 'init387', 'init388', 'init389', 'init390', 'init391', 'init392', 'init393', 'init394', 'init395', 'init396', 'init397', 'init398', 'init399', 'init400', 'init401', 'init402', 'init403', 'init404', 'init405', 'init406', 'init407', 'init408', 'init409', 'init410', 'init411', 'init412', 'init413', 'init414', 'init415', 'init416', 'init417', 'init418', 'init419', 'init420', 'init421', 'init422', 'init423', 'init424', 'init425', 'init426', 'init427', 'init428', 'init429', 'init430', 'init431', 'init432', 'init433', 'init434', 'init435', 'init436', 'init437', 'init438', 'init439', 'init440', 'init441', 'init442', 'init443', 'init444', 'init445', 'init446', 'init447', 'init448', 'init449', 'init450', 'init451', 'init452', 'init453', 'init454', 'init455', 'init456', 'init457', 'init458', 'init459', 'init460', 'init461', 'init462', 'init463', 'init464', 'init465', 'init466', 'init467', 'init468', 'init469', 'init470', 'init471', 'init472', 'init473', 'init474', 'init475', 'init476', 'init477', 'init478', 'init479', 'init480', 'init481', 'init482', 'init483', 'init484', 'init485', 'init486', 'init487', 'init488', 'init489', 'init490', 'init491', 'init492', 'init493', 'init494', 'init495', 'init496', 'init497', 'init498', 'init499', 'init500', 'init501', 'init502', 'init503', 'init504', 'init505', 'init506', 'init507', 'init508', 'init509', 'init510', 'init511', 'init512', 'init513', 'init514', 'init515', 'init516', 'init517', 'init518', 'init519', 'init520', 'init521', 'init522', 'init523', 'init524', 'init525', 'init526', 'init527', 'init528', 'init529', 'init530', 'init531', 'init532', 'init533', 'init534', 'init535', 'init536', 'init537', 'init538', 'init539', 'init540', 'init541', 'init542', 'init543', 'init544', 'init545', 'init546', 'init547', 'init548', 'init549', 'init550', 'init551', 'init552', 'init553', 'init554', 'init555', 'init556', 'init557', 'init558', 'init559', 'init560', 'init561', 'init562', 'init563', 'init564', 'init565', 'init566', 'init567', 'init568', 'init569', 'init570', 'init571', 'init572', 'init573', 'init574', 'init575', 'init576', 'init577', 'init578', 'init579', 'init580', 'init581', 'init582', 'init583', 'init584', 'init585', 'init586', 'init587', 'init588', 'init589', 'init590', 'init591', 'init592', 'init593', 'init594', 'init595', 'init596', 'init597', 'init598', 'init599', 'init600', 'init601', 'init602', 'init603', 'init604', 'init605', 'init606', 'init607', 'init608', 'init609', 'init610', 'init611', 'init612', 'init613', 'init614', 'init615', 'init616', 'init617', 'init618', 'init619', 'init620', 'init621', 'init622', 'init623', 'init624', 'init625', 'init626', 'init627', 'init628', 'init629', 'init630', 'init631', 'init632', 'init633', 'init634', 'init635', 'init636', 'init637', 'init638', 'init639', 'init640', 'init641', 'init642', 'init643', 'init644', 'init645', 'init646', 'init647', 'init648', 'init649', 'init650', 'init651', 'init652', 'init653', 'init654', 'init655', 'init656', 'init657', 'init658', 'init659', 'init660', 'init661', 'init662', 'init663', 'init664', 'init665', 'init666', 'init667', 'init668', 'init669', 'init670', 'init671', 'init672', 'init673', 'init674', 'init675', 'init676', 'init677', 'init678', 'init679', 'init680', 'init681', 'init682', 'init683', 'init684', 'init685', 'init686', 'init687', 'init688', 'init689', 'init690', 'init691', 'init692', 'init693', 'init694', 'init695', 'init696', 'init697', 'init698', 'init699', 'init700', 'init701', 'init702', 'init703', 'init704', 'init705', 'init706', 'init707', 'init708', 'init709', 'init710', 'init711', 'init712', 'init713', 'init714', 'init715', 'init716', 'init717', 'init718', 'init719', 'init720', 'init721', 'init722', 'init723', 'init724', 'init725', 'init726', 'init727', 'init728', 'init729', 'init730', 'init731', 'init732', 'init733', 'init734', 'init735', 'init736', 'init737', 'init738', 'init739', 'init740', 'init741', 'init742', 'init743', 'init744', 'init745', 'init746', 'init747', 'init748', 'init749', 'init750', 'init751', 'init752', 'init753', 'init754', 'init755', 'init756', 'init757', 'init758', 'init759', 'init760', 'init761', 'init762', 'init763', 'init764', 'init765', 'init766', 'init767', 'init768', 'init769', 'init770', 'init771', 'init772', 'init773', 'init774', 'init775', 'init776', 'init777', 'init778', 'init779', 'init780', 'init781', 'init782', 'init783', 'init784', 'init785', 'init786', 'init787', 'init788', 'init789', 'init790', 'init791', 'init792', 'init793', 'init794', 'init795', 'init796', 'init797', 'init798', 'init799', 'init800', 'init801', 'init802', 'init803', 'init804', 'init805', 'init806', 'init807', 'init808', 'init809', 'init810', 'init811', 'init812', 'init813', 'init814', 'init815', 'init816', 'init817', 'init818', 'init819', 'init820', 'init821', 'init822', 'init823', 'init824', 'init825', 'init826', 'init827', 'init828', 'init829', 'init830', 'init831', 'init832', 'init833', 'init834', 'init835', 'init836', 'init837', 'init838', 'init839', 'init840', 'init841', 'init842', 'init843', 'init844', 'init845', 'init846', 'init847', 'init848', 'init849', 'init850', 'init851', 'init852', 'init853', 'init854', 'init855', 'init856', 'init857', 'init858', 'init859', 'init860', 'init861', 'init862', 'init863', 'init864', 'init865', 'init866', 'init867', 'init868', 'init869', 'init870', 'init871', 'init872', 'init873', 'init874', 'init875', 'init876', 'init877', 'init878', 'init879', 'init880', 'init881', 'init882', 'init883', 'init884', 'init885', 'init886', 'init887', 'init888', 'init889', 'init890', 'init891', 'init892', 'init893', 'init894', 'init895', 'init896', 'init897', 'init898', 'init899', 'init900', 'init901', 'init902', 'init903', 'init904', 'init905', 'init906', 'init907', 'init908', 'init909', 'init910', 'init911', 'init912', 'init913', 'init914', 'init915', 'init916', 'init917', 'init918', 'init919', 'init920', 'init921', 'init922', 'init923', 'init924', 'init925', 'init926', 'init927', 'init928', 'init929', 'init930', 'init931', 'init932', 'init933', 'init934', 'init935', 'init936', 'init937', 'init938', 'init939', 'init940', 'init941', 'init942', 'init943', 'init944', 'init945', 'init946', 'init947', 'init948', 'init949', 'init950', 'init951', 'init952', 'init953', 'init954', 'init955', 'init956', 'init957', 'init958', 'init959', 'init960', 'init961', 'init962', 'init963', 'init964', 'init965', 'init966', 'init967', 'init968', 'init969', 'init970', 'init971', 'init972', 'init973', 'init974', 'init975', 'init976', 'init977', 'init978', 'init979', 'init980', 'init981', 'init982', 'init983', 'init984', 'init985', 'init986', 'init987', 'init988', 'init989', 'init990', 'init991', 'init992', 'init993', 'init994', 'init995', 'init996', 'init997', 'init998', 'init999', 'init1000', 'init1001', 'init1002', 'init1003', 'init1004', 'init1005', 'init1006', 'init1007', 'init1008', 'init1009', 'init1010', 'init1011', 'init1012', 'init1013', 'init1014', 'init1015', 'init1016', 'init1017', 'init1018', 'init1019', 'init1020', 'init1021', 'init1022', 'init1023', 'init1024', 'init1025', 'init1026', 'init1027', 'init1028', 'init1029', 'init1030', 'init1031', 'init1032', 'init1033', 'init1034', 'init1035', 'init1036', 'init1037', 'init1038', 'init1039', 'init1040', 'init1041', 'init1042', 'init1043', 'init1044', 'init1045', 'init1046', 'init1047', 'init1048', 'init1049', 'init1050', 'init1051', 'init1052', 'init1053', 'init1054', 'init1055', 'init1056', 'init1057', 'init1058', 'init1059', 'init1060', 'init1061', 'init1062', 'init1063', 'init1064', 'init1065', 'init1066', 'init1067', 'init1068', 'init1069', 'init1070', 'init1071', 'init1072', 'init1073', 'init1074', 'init1075', 'init1076', 'init1077', 'init1078', 'init1079', 'init1080', 'init1081', 'init1082', 'init1083', 'init1084', 'init1085', 'init1086', 'init1087', 'init1088', 'init1089', 'init1090', 'init1091', 'init1092', 'init1093', 'init1094', 'init1095', 'init1096', 'init1097', 'init1098', 'init1099', 'init1100', 'init1101', 'init1102', 'init1103', 'init1104', 'init1105', 'init1106', 'init1107', 'init1108', 'init1109', 'init1110', 'init1111', 'init1112', 'init1113', 'init1114', 'init1115', 'init1116', 'init1117', 'init1118', 'init1119', 'init1120', 'init1121', 'init1122', 'init1123', 'init1124', 'init1125', 'init1126', 'init1127', 'init1128', 'init1129', 'init1130', 'init1131', 'init1132', 'init1133', 'init1134', 'init1135', 'init1136', 'init1137', 'init1138', 'init1139', 'init1140', 'init1141', 'init1142', 'init1143', 'init1144', 'init1145', 'init1146', 'init1147', 'init1148', 'init1149', 'init1150', 'init1151', 'init1152', 'init1153', 'init1154', 'init1155', 'init1156', 'init1157', 'init1158', 'init1159', 'init1160', 'init1161', 'init1162', 'init1163', 'init1164', 'init1165', 'init1166', 'init1167', 'init1168', 'init1169', 'init1170', 'init1171', 'init1172', 'init1173', 'init1174', 'init1175', 'init1176', 'init1177', 'init1178', 'init1179', 'init1180', 'init1181', 'init1182', 'init1183', 'init1184', 'init1185', 'init1186', 'init1187', 'init1188', 'init1189', 'init1190', 'init1191', 'init1192', 'init1193', 'init1194', 'init1195', 'init1196', 'init1197', 'init1198', 'init1199', 'init1200', 'init1201', 'init1202', 'init1203', 'init1204', 'init1205', 'init1206', 'init1207', 'init1208', 'init1209', 'init1210', 'init1211', 'init1212', 'init1213', 'init1214', 'init1215', 'init1216', 'init1217', 'init1218', 'init1219', 'init1220', 'init1221', 'init1222', 'init1223', 'init1224', 'init1225', 'init1226', 'init1227', 'init1228', 'init1229', 'init1230', 'init1231', 'init1232', 'init1233', 'init1234', 'init1235', 'init1236', 'init1237', 'init1238', 'init1239', 'init1240', 'init1241', 'init1242', 'init1243', 'init1244', 'init1245', 'init1246', 'init1247', 'init1248', 'init1249', 'init1250', 'init1251', 'init1252', 'init1253', 'init1254', 'init1255', 'init1256', 'init1257', 'init1258', 'init1259', 'init1260', 'init1261', 'init1262', 'init1263', 'init1264', 'init1265', 'init1266', 'init1267', 'init1268', 'init1269', 'init1270', 'init1271', 'init1272', 'init1273', 'init1274', 'init1275', 'init1276', 'init1277', 'init1278', 'init1279', 'init1280', 'init1281', 'init1282', 'init1283', 'init1284', 'init1285', 'init1286', 'init1287', 'init1288', 'init1289', 'init1290', 'init1291', 'init1292', 'init1293', 'init1294', 'init1295', 'init1296', 'init1297', 'init1298', 'init1299', 'init1300', 'init1301', 'init1302', 'init1303', 'init1304', 'init1305', 'init1306', 'init1307', 'init1308', 'init1309', 'init1310', 'init1311', 'init1312', 'init1313', 'init1314', 'init1315', 'init1316', 'init1317', 'init1318', 'init1319', 'init1320', 'init1321', 'init1322', 'init1323', 'init1324', 'init1325', 'init1326', 'init1327', 'init1328', 'init1329', 'init1330', 'init1331', 'init1332', 'init1333', 'init1334', 'init1335', 'init1336', 'init1337', 'init1338', 'init1339', 'init1340', 'init1341', 'init1342', 'init1343', 'init1344', 'init1345', 'init1346', 'init1347', 'init1348', 'init1349', 'init1350', 'init1351', 'init1352', 'init1353', 'init1354', 'init1355', 'init1356', 'init1357', 'init1358', 'init1359', 'init1360', 'init1361', 'init1362', 'init1363', 'init1364', 'init1365', 'init1366', 'init1367', 'init1368', 'init1369', 'init1370', 'init1371', 'init1372', 'init1373', 'init1374', 'init1375', 'init1376', 'init1377', 'init1378', 'init1379', 'init1380', 'init1381', 'init1382', 'init1383', 'init1384', 'init1385', 'init1386', 'init1387', 'init1388', 'init1389', 'init1390', 'init1391', 'init1392', 'init1393', 'init1394', 'init1395', 'init1396', 'init1397', 'init1398', 'init1399', 'init1400', 'init1401', 'init1402', 'init1403', 'init1404', 'init1405', 'init1406', 'init1407', 'init1408', 'init1409', 'init1410', 'init1411', 'init1412', 'init1413', 'init1414', 'init1415', 'init1416', 'init1417', 'init1418', 'init1419', 'init1420', 'init1421', 'init1422', 'init1423', 'init1424', 'init1425', 'init1426', 'init1427', 'init1428', 'init1429', 'init1430', 'init1431', 'init1432', 'init1433', 'init1434', 'init1435', 'init1436', 'init1437', 'init1438', 'init1439', 'init1440', 'init1441', 'init1442', 'init1443', 'init1444', 'init1445', 'init1446', 'init1447', 'init1448', 'init1449', 'init1450', 'init1451', 'init1452', 'init1453', 'init1454', 'init1455', 'init1456', 'init1457', 'init1458', 'init1459', 'init1460', 'init1461', 'init1462', 'init1463', 'init1464', 'init1465', 'init1466', 'init1467', 'init1468', 'init1469', 'init1470', 'init1471', 'init1472', 'init1473', 'init1474', 'init1475', 'init1476', 'init1477', 'init1478', 'init1479', 'init1480', 'init1481', 'init1482', 'init1483', 'init1484', 'init1485', 'init1486', 'init1487', 'init1488', 'init1489', 'init1490', 'init1491', 'init1492', 'init1493', 'init1494', 'init1495', 'init1496', 'init1497', 'init1498', 'init1499', 'init1500', 'init1501', 'init1502', 'init1503', 'init1504', 'init1505', 'init1506', 'init1507', 'init1508', 'init1509', 'init1510', 'init1511', 'init1512', 'init1513', 'init1514', 'init1515', 'init1516', 'init1517', 'init1518', 'init1519', 'init1520', 'init1521', 'init1522', 'init1523', 'init1524', 'init1525', 'init1526', 'init1527', 'init1528', 'init1529', 'init1530', 'init1531', 'init1532', 'init1533', 'init1534', 'init1535', 'init1536', 'init1537', 'init1538', 'init1539', 'init1540', 'init1541', 'init1542', 'init1543', 'init1544', 'init1545', 'init1546', 'init1547', 'init1548', 'init1549', 'init1550', 'init1551', 'init1552', 'init1553', 'init1554', 'init1555', 'init1556', 'init1557', 'init1558', 'init1559', 'init1560', 'init1561', 'init1562', 'init1563', 'init1564', 'init1565', 'init1566', 'init1567', 'init1568', 'init1569', 'init1570', 'init1571', 'init1572', 'init1573', 'init1574', 'init1575', 'init1576', 'init1577', 'init1578', 'init1579', 'init1580', 'init1581', 'init1582', 'init1583', 'init1584', 'init1585', 'init1586', 'init1587', 'init1588', 'init1589', 'init1590', 'init1591', 'init1592', 'init1593', 'init1594', 'init1595', 'init1596', 'init1597', 'init1598', 'init1599', 'init1600', 'init1601', 'init1602', 'init1603', 'init1604', 'init1605', 'init1606', 'init1607', 'init1608', 'init1609', 'init1610', 'init1611', 'init1612', 'init1613', 'init1614', 'init1615', 'init1616', 'init1617', 'init1618', 'init1619', 'init1620', 'init1621', 'init1622', 'init1623', 'init1624', 'init1625', 'init1626', 'init1627', 'init1628', 'init1629', 'init1630', 'init1631', 'init1632', 'init1633', 'init1634', 'init1635', 'init1636', 'init1637', 'init1638', 'init1639', 'init1640', 'init1641', 'init1642', 'init1643', 'init1644', 'init1645', 'init1646', 'init1647', 'init1648', 'init1649', 'init1650', 'init1651', 'init1652', 'init1653', 'init1654', 'init1655', 'init1656', 'init1657', 'init1658', 'init1659', 'init1660', 'init1661', 'init1662', 'init1663', 'init1664', 'init1665', 'init1666', 'init1667', 'init1668', 'init1669', 'init1670', 'init1671', 'init1672', 'init1673', 'init1674', 'init1675', 'init1676', 'init1677', 'init1678', 'init1679', 'init1680', 'init1681', 'init1682', 'init1683', 'init1684', 'init1685', 'init1686', 'init1687', 'init1688', 'init1689', 'init1690', 'init1691', 'init1692', 'init1693', 'init1694', 'init1695', 'init1696', 'init1697', 'init1698', 'init1699', 'init1700', 'init1701', 'init1702', 'init1703', 'init1704', 'init1705', 'init1706', 'init1707', 'init1708', 'init1709', 'init1710', 'init1711', 'init1712', 'init1713', 'init1714', 'init1715', 'init1716', 'init1717', 'init1718', 'init1719', 'init1720', 'init1721', 'init1722', 'init1723', 'init1724', 'init1725', 'init1726', 'init1727', 'init1728', 'init1729', 'init1730', 'init1731', 'init1732', 'init1733', 'init1734', 'init1735', 'init1736', 'init1737', 'init1738', 'init1739', 'init1740', 'init1741', 'init1742', 'init1743', 'init1744', 'init1745', 'init1746', 'init1747', 'init1748', 'init1749', 'init1750', 'init1751', 'init1752', 'init1753', 'init1754', 'init1755', 'init1756', 'init1757', 'init1758', 'init1759', 'init1760', 'init1761', 'init1762', 'init1763', 'init1764', 'init1765', 'init1766', 'init1767', 'init1768', 'init1769', 'init1770', 'init1771', 'init1772', 'init1773', 'init1774', 'init1775', 'init1776', 'init1777', 'init1778', 'init1779', 'init1780', 'init1781', 'init1782', 'init1783', 'init1784', 'init1785', 'init1786', 'init1787', 'init1788', 'init1789', 'init1790', 'init1791', 'init1792', 'init1793', 'init1794', 'init1795', 'init1796', 'init1797', 'init1798', 'init1799', 'init1800', 'init1801', 'init1802', 'init1803', 'init1804', 'init1805', 'init1806', 'init1807', 'init1808', 'init1809', 'init1810', 'init1811', 'init1812', 'init1813', 'init1814', 'init1815', 'init1816', 'init1817', 'init1818', 'init1819', 'init1820', 'init1821', 'init1822', 'init1823', 'init1824', 'init1825', 'init1826', 'init1827', 'init1828', 'init1829', 'init1830', 'init1831', 'init1832', 'init1833', 'init1834', 'init1835', 'init1836', 'init1837', 'init1838', 'init1839', 'init1840', 'init1841', 'init1842', 'init1843', 'init1844', 'init1845', 'init1846', 'init1847', 'init1848', 'init1849', 'init1850', 'init1851', 'init1852', 'init1853', 'init1854', 'init1855', 'init1856', 'init1857', 'init1858', 'init1859', 'init1860', 'init1861', 'init1862', 'init1863', 'init1864', 'init1865', 'init1866', 'init1867', 'init1868', 'init1869', 'init1870', 'init1871', 'init1872', 'init1873', 'init1874', 'init1875', 'init1876', 'init1877', 'init1878', 'init1879', 'init1880', 'init1881', 'init1882', 'init1883', 'init1884', 'init1885', 'init1886', 'init1887', 'init1888', 'init

```
void show_onions_and_btc_addr(void)

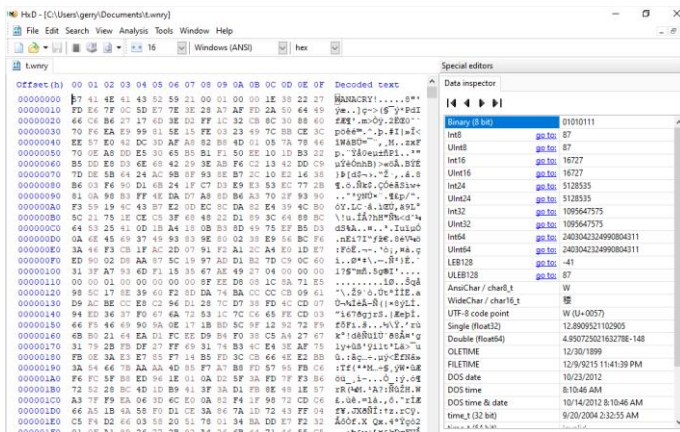
{
    bool bVar1;
    undefined3 extraout_var;
    int iVar2;
    undefined local_31c [178];
    char final_btc_addresses [602];
    char *btc_addresses [3];

    btc_addresses[0] = _"13AM4VW2dXhYgXqQepoHkHSQuyGqaEb_0040f488";
    btc_addresses[1] = _"12c9YDPgwueZ9NyWgW519p7AA5isjr6S_0040f464";
    btc_addresses[2] = _"115p7UMMngojlpHvKpR1jcRdfJNXj6Lr_0040f440";
    bVar1 = show_onion_addresses_etc(local_31c,1);
    if (CONCAT31(extraout_var,bVar1) != 0) {
        iVar2 = rand();
        strcpy(final_btc_addresses,btc_addresses[iVar2 % 3]);
        show_onion_addresses_etc(local_31c,0);
    }
    return;
}
```

## 12. Open the u.wnry file to get the wannacry ransomware dialog.

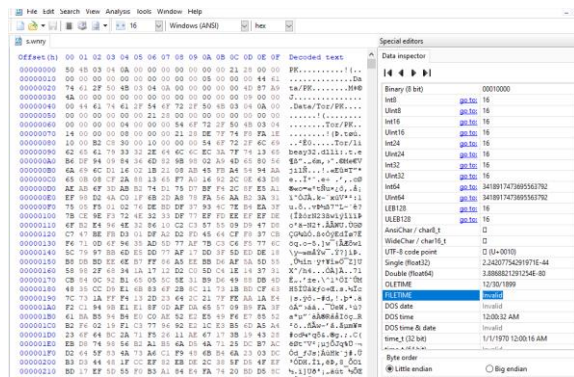


## 13. In the t.wnry file there is a WANACRY encoded file.

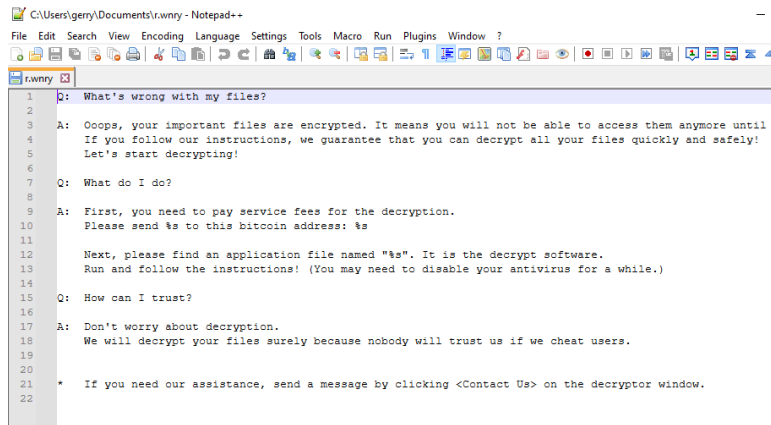




14. The s.wncry file is a compress file with PK format.



15. The r.wnry file contains text on a wannacry ransomware dialog.



16. The malware sets hidden attributes by running the createprocess command consisting of attrib+h and icacls./.

```
execute_command(s_attrib+h._0040f520,0,(LPDWORD)0x0);
execute_command(s_icacls._/grant_Everyone:F/T/C_0040f4fc,0,(LPDWORD)0x0);
```

17. The program contains taskstart as a ransomware encryption component.

```
if (is_argv_slash_i != 0) {
    local_8 = 0;
    psVar3 = (short *)something_with_file(local_6e8,s_t.wnry_0040f4f4,&local_8);
    if (((psVar3 != (short *)0x0) &&
        (args = (int *)FUN_004021bd(psVar3,local_8), args != (int *)0x0)) &&
        (pcVar4 = (code *)FUN_00402924(args,s_TaskStart_0040f4e8), pcVar4 != (code *)0x0)) {
        (*pcVar4)(0,0);
    }
}
FUN_0040137a();
```

## 18. Display the private RSA key encoded in the malware.

```

undefined4 __thiscall crypto_stuff(int param_1,int param_1_00)
{
    int iVar1;
    int in_ECX;

    iVar1 = Crypto_Context_Setup(in_ECX);
    if (iVar1 != 0) {
        if (param_1 == 0) {
            iVar1 = (*Crypt_Import_Key)(*(undefined4 *) (in_ECX + 4), &public_key_blob, 0x494, 0, 0, in_ECX);
        }
        else {
            iVar1 = FUN_004018f9(*(undefined4 *) (in_ECX + 4), in_ECX + 8, (LPCSTR)param_1);
        }
        if (iVar1 != 0) {
            return 1;
        }
    }
    FUN_004018b9(in_ECX);
    return 0;
}

```

		public_key_blob	
0040ebf8	07	??	07h
0040ebf9	02	??	02h
0040ebfa	00	??	00h
0040ebfb	00	??	00h
0040ebfc	00	??	00h
0040ebfd	a4	??	A4h
0040ebfe	00	??	00h
0040ebff	00	??	00h
0040ec00	52	??	52h R
0040ec01	53	??	53h S
0040ec02	41	??	41h A
0040ec03	32	??	32h 2
0040ec04	00	??	00h
0040ec05	08	??	08h
0040ec06	00	??	00h
0040ec07	00	??	00h

## 19. The program contains the AES key for the encrypted file.

```

Decompile: something_with_aes - (ed01ebfbc3eb5bba545af4d01bf5f107166184048043)
1
2 void __thiscall
3 something_with_aes(void *this,undefined aes_key,undefined param_2,undefined aes_key_size,
4                     undefined const_16)
5
6 {
7     undefined4 uVar1;
8     uint uVar2;
9     int iVar3;
10    char *pcVar4;
11    int iVar5;
12    uint *puVar6;
13    char *pcVar7;
14    undefined4 *puVar8;
15    int iVar9;
16    int iVar10;
17    undefined4 *puVar11;
18    undefined3 in_stack_00000005;
19    undefined3 in_stack_00000009;
20    undefined3 in_stack_0000000d;
21    undefined3 in_stack_00000011;
22    exception local_18 [20];

```

```

if (_aes_key == (byte *)0x0) {
    _param_2 = (uint *)0x0040f57c;
    exception::exception(local_18, (char *)&param_2);
    /* WARNING: Subroutine does not return */
    _CxxThrowException(local_18, (ThrowInfo *)&ThrowInfo_0040d570);
}
if (((_aes_key_size != 0x10) && (_aes_key_size != 0x18)) && (_aes_key_size != 0x20)) {
    _param_2 = (uint *)0x0040f57c;
    exception::exception(local_18, (char *)&param_2);
    /* WARNING: Subroutine does not return */
    _CxxThrowException(local_18, (ThrowInfo *)&ThrowInfo_0040d570);
}
if (((_const_16 != (byte *)0x10) && (_const_16 != (byte *)0x18)) && (_const_16 != (byte *)0x20)) {
    _param_2 = (uint *)0x0040f57c;
    exception::exception(local_18, (char *)&param_2);
    /* WARNING: Subroutine does not return */
    _CxxThrowException(local_18, (ThrowInfo *)&ThrowInfo_0040d570);
}
(Byte *)((int)this + 0x3cc) = _const_16;
(int *)((int)this + 0x3cd) = _aes_key_size;
memcpy((void *)((int)this + 0x3d0), _param_2, (size_t)_const_16);
memcpy((void *)((int)this + 0x3f0), param_2, (size_t)((int)this + 0x3cc));

```