WannaCry Malware Analysis

Lucian-Mihai Lungu

Introduction

Overview of WannaCry ransomware

Impact and significance of the malware

Objectives of the analysis

Agenda:

- Static Analysis
- Dynamic Analysis
- Registry Artifacts
- Ghidra Decompilation

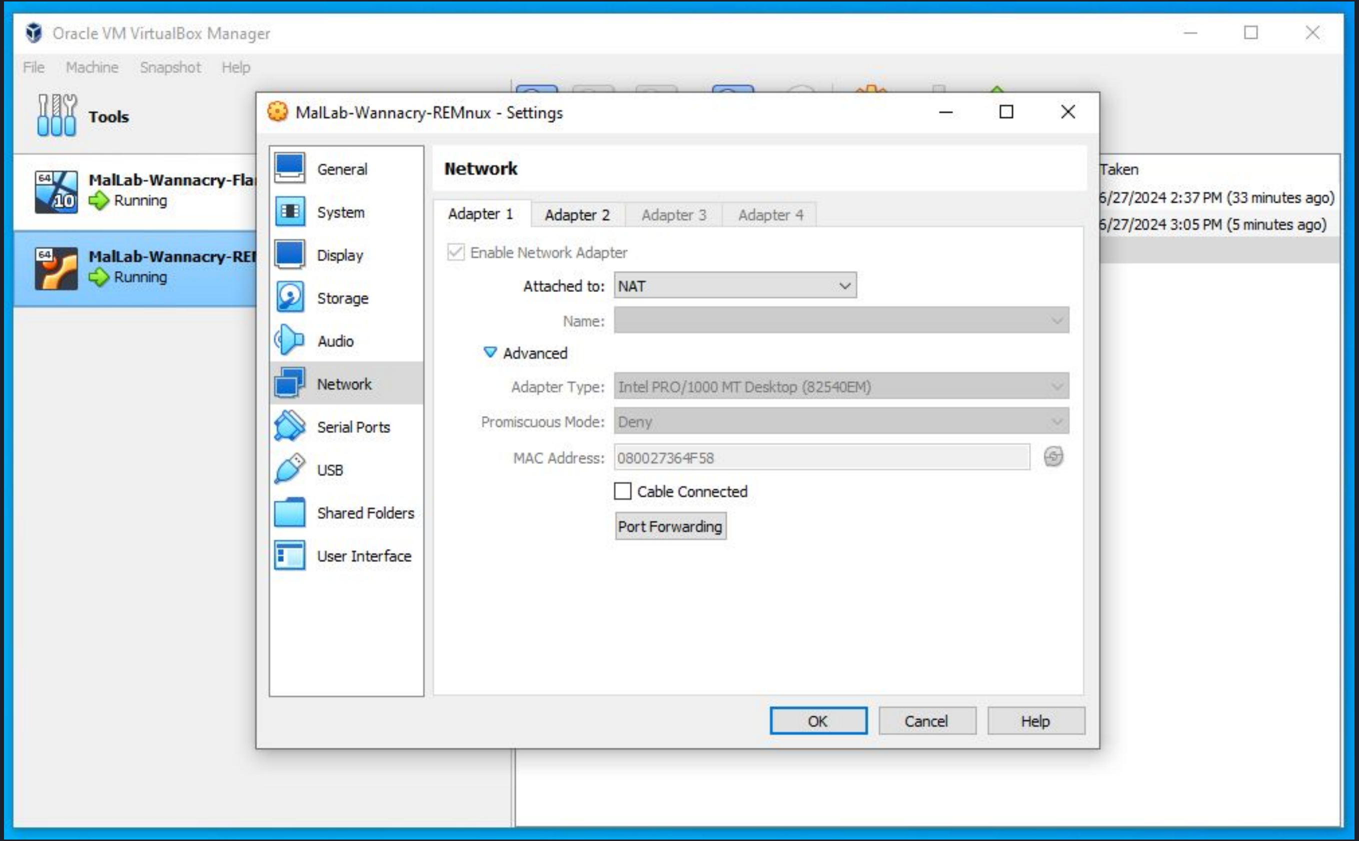
Environmental Setup

Lab Stack:

- Flare VM: Windows-based malware analysis platform
- REMnux: Linux distribution for malware analysis

Configuration:

- Ensure VMs are not on the home network
- Set up a dedicated, isolated subnet



MalLab-Wannacry-REMnux - Settings

Network

☑ Enable Network Adapter

Attached to: NAT

Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027364F58

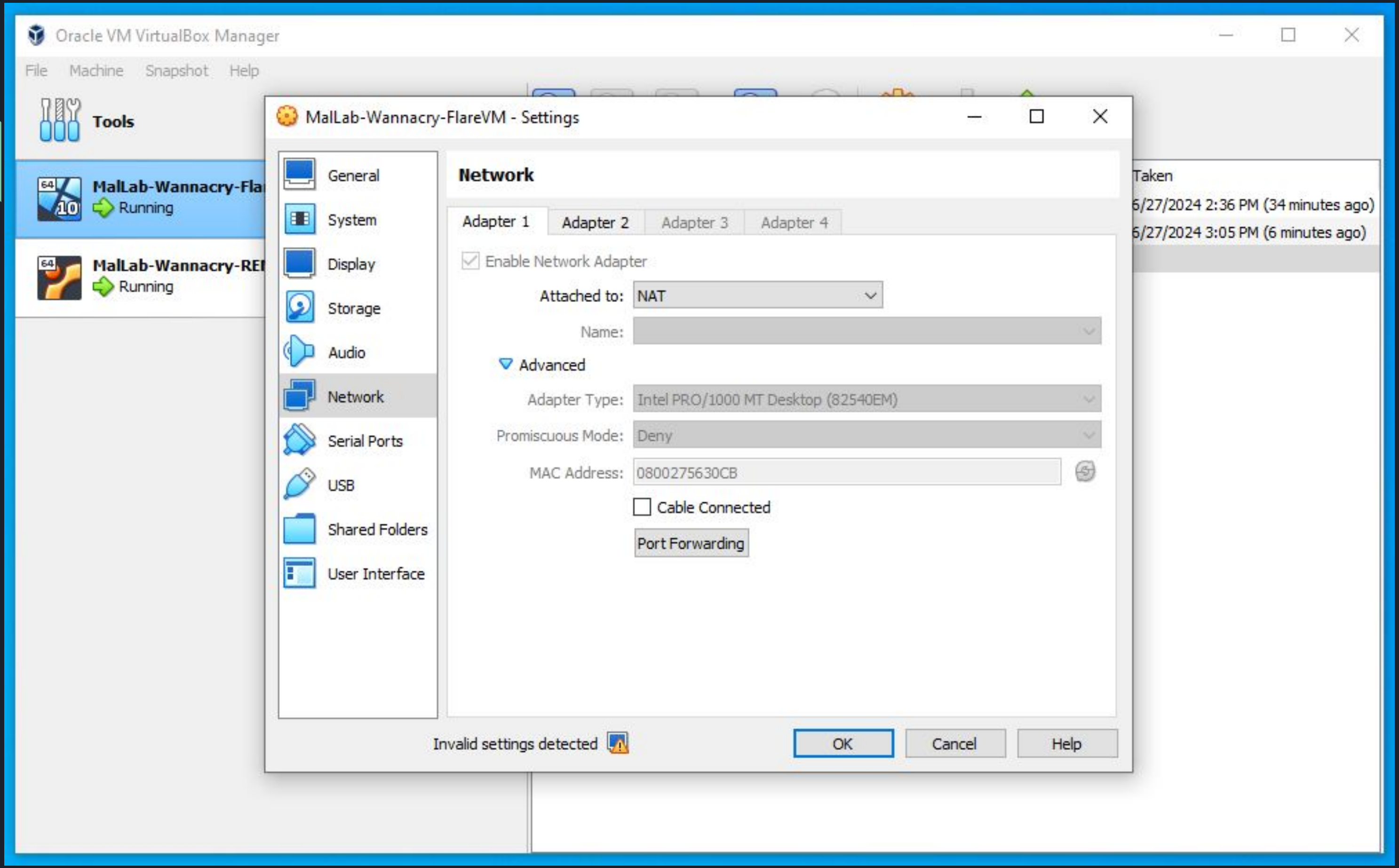
□ Cable Connected

6/27/2024 2:37 PM (33 minutes ago)

6/27/2024 3:05 PM (5 minutes ago)

Network Isolation Checks

- Verify VMs cannot access the internet or home network
- Ping tests to confirm isolation



Oracle VM VirtualBox Manager

MalLab-Wannacry-FlareVM - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: NAT

Name:

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 0800275630CB

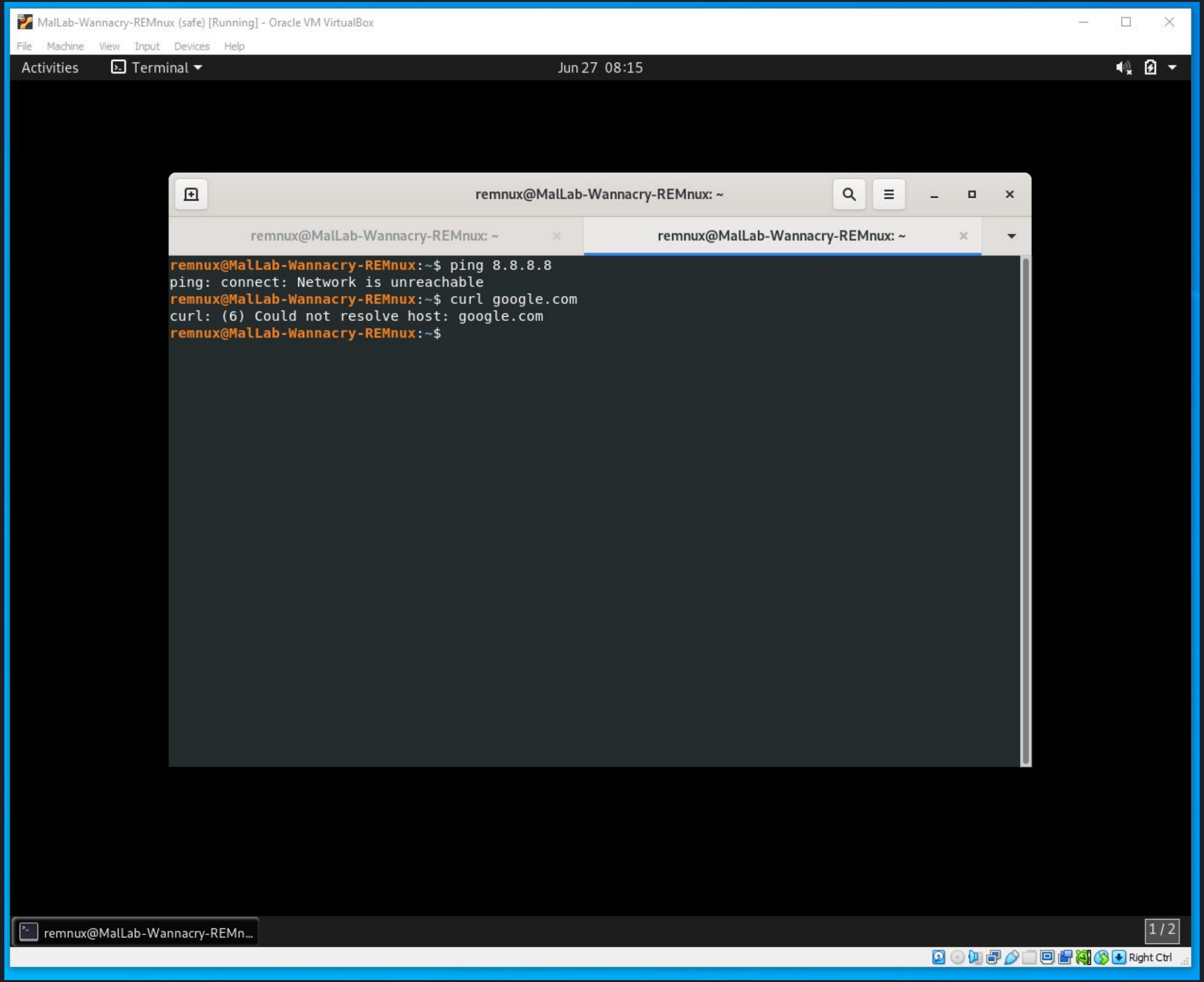
□ Cable Connected

Invalid settings detected

Taken

6/27/2024 2:36 PM (34 minutes ago)

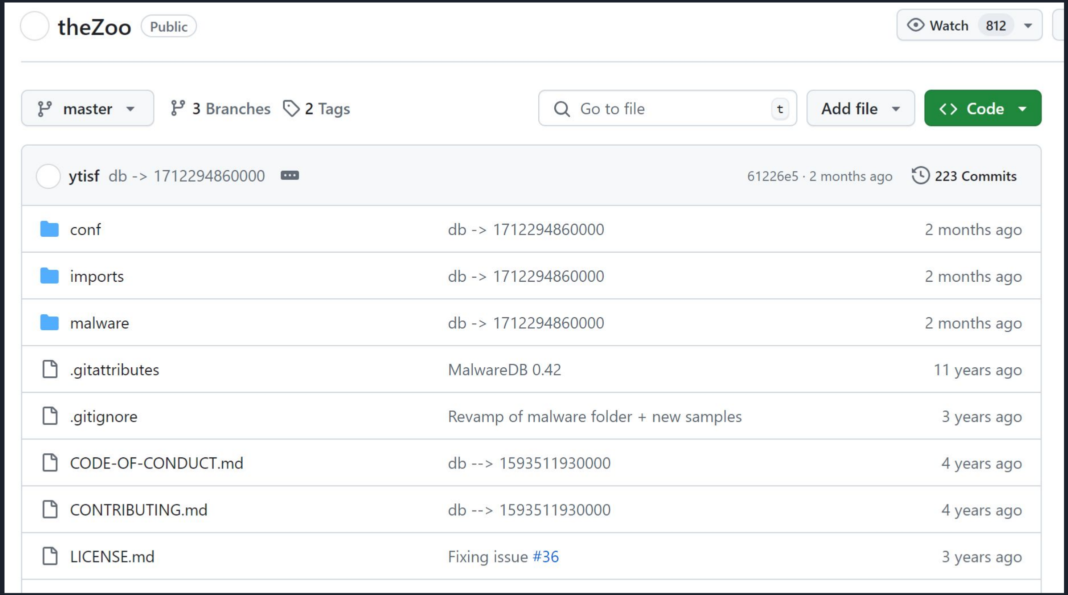
6/27/2024 3:05 PM (6 minutes ago)


MalLab-Wannacry-REMnux (safe) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Jun 27 08:15
remnux@MalLab-Wannacry-REMnux: ~
remnux@MalLab-Wannacry-REMnux: ~
remnux@MalLab-Wannacry-REMnux: ~
remnux@MalLab-Wannacry-REMn...
1 / 2
Right Ctrl

```
remnux@MalLab-Wannacry-REMnux:~$ ping 8.8.8.8
ping: connect: Network is unreachable
remnux@MalLab-Wannacry-REMnux:~$ curl google.com
curl: (6) Could not resolve host: google.com
remnux@MalLab-Wannacry-REMnux:~$
```

Sourcing Binaries

- Obtaining WannaCry sample from theMalwareZoo.zip
- Download path and file details



ytisf db -> 1712294860000 61226e5 · 2 months ago 223 Commits

conf	db -> 1712294860000	2 months ago
imports	db -> 1712294860000	2 months ago
malware	db -> 1712294860000	2 months ago
.gitattributes	MalwareDB 0.42	11 years ago
.gitignore	Revamp of malware folder + new samples	3 years ago
CODE-OF-CONDUCT.md	db --> 1593511930000	4 years ago
CONTRIBUTING.md	db --> 1593511930000	4 years ago
LICENSE.md	Fixing issue #36	3 years ago

Basic Static Analysis

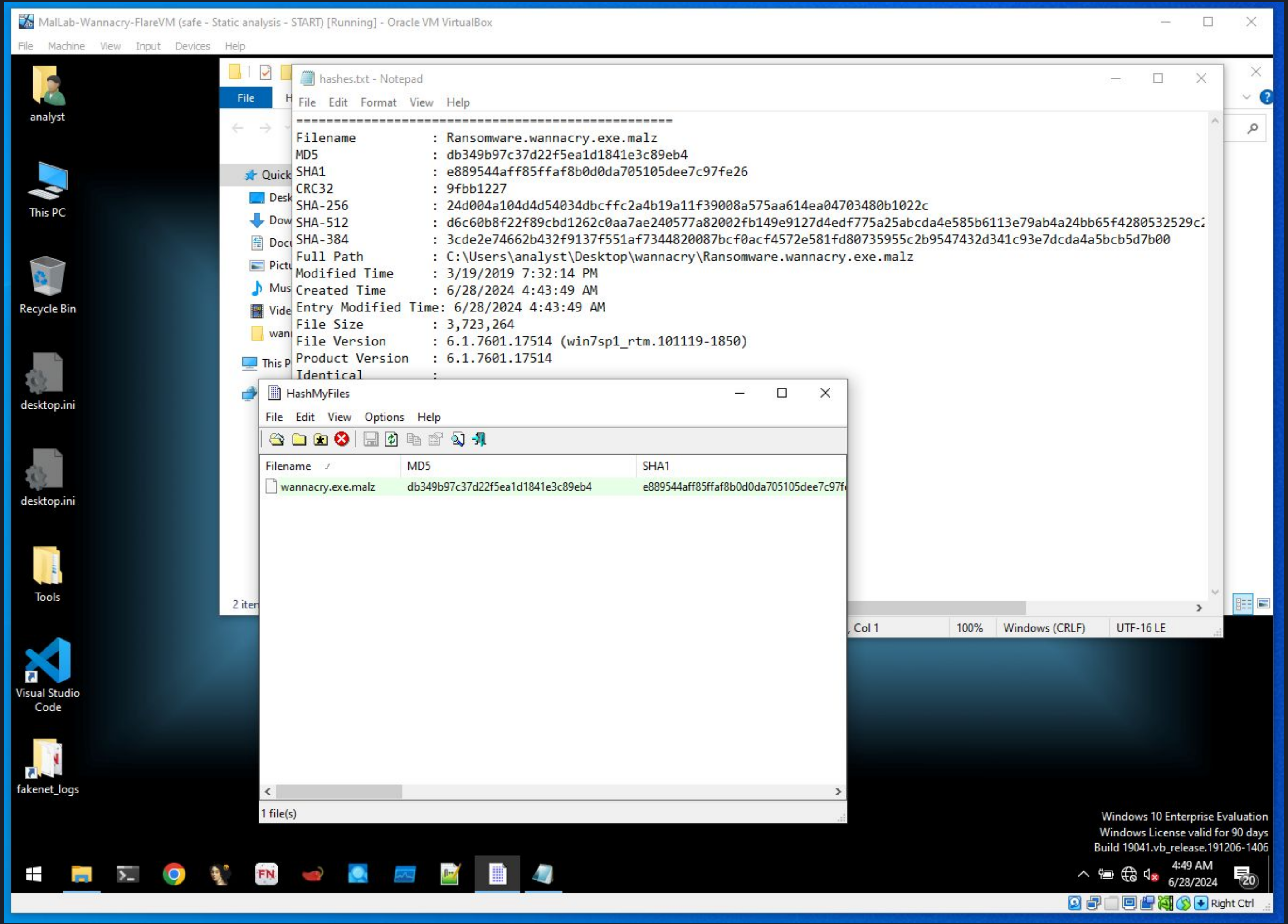
Hash Calculation:

- Using HashMyFiles and REMnux commands
- VirusTotal check for hash verification

Tool: Floss

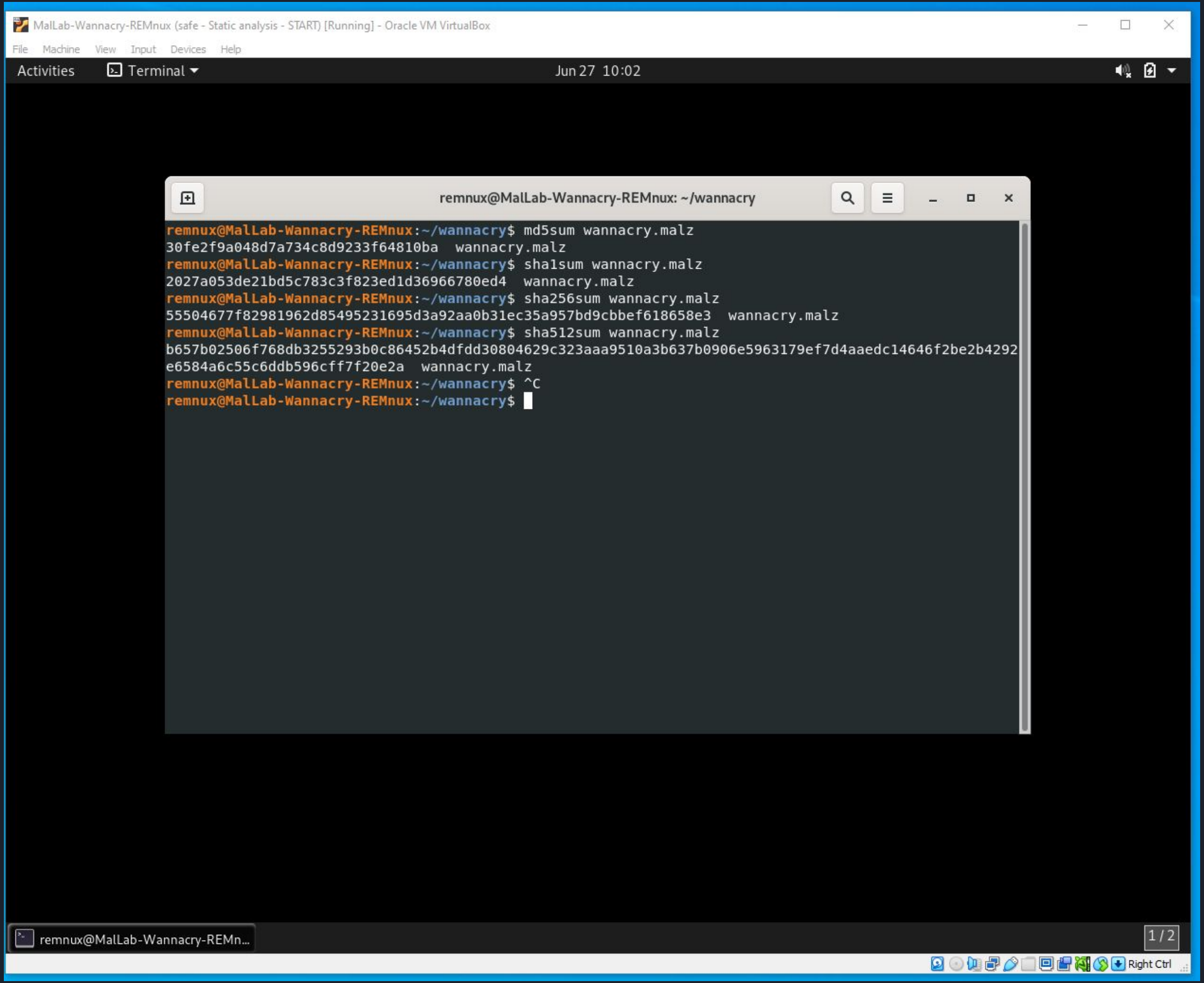
- Extracting text strings from the binary
- Key findings (API calls, URLs, executable names)

Unpacking binaries to find additional executables



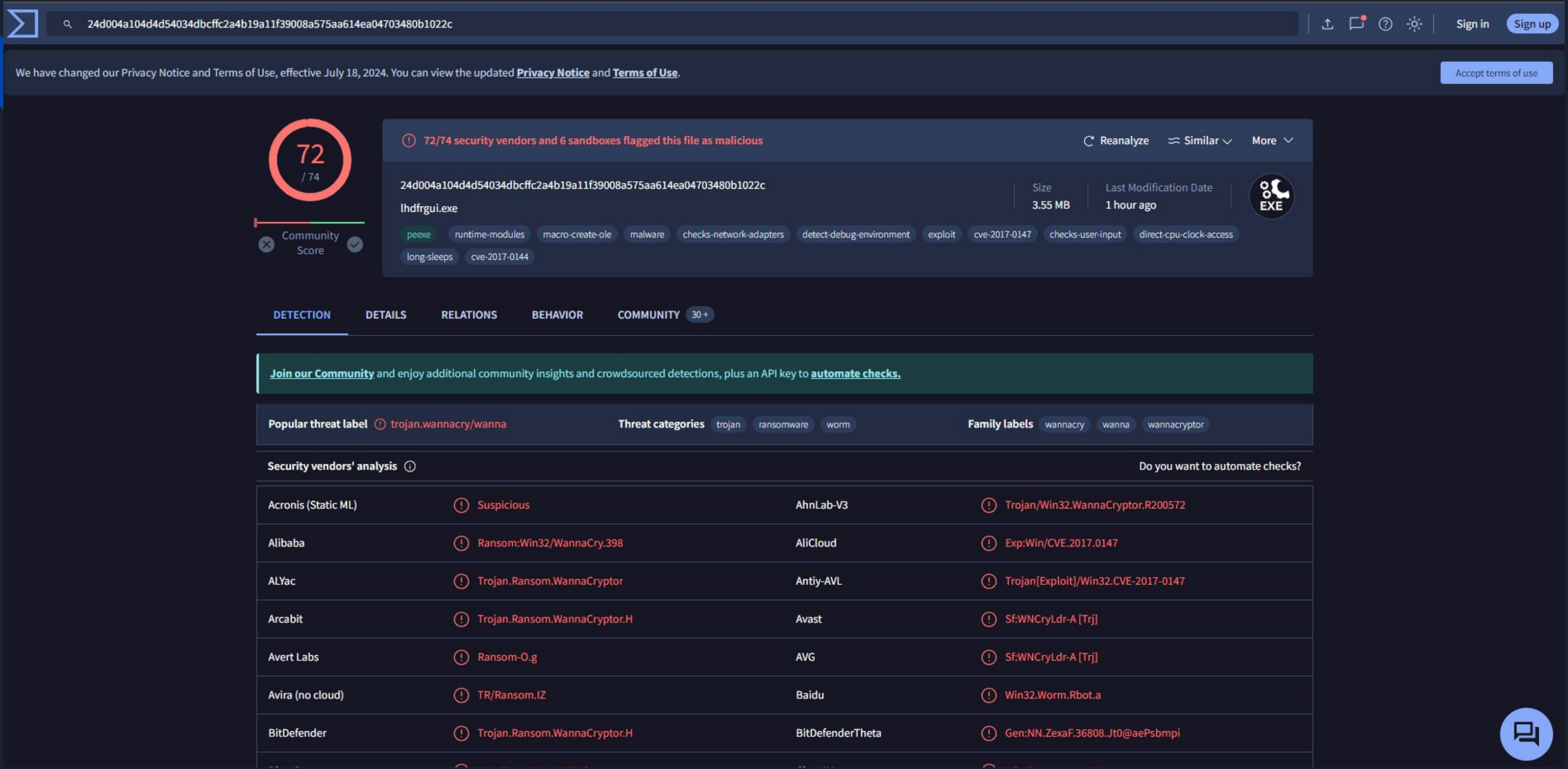
```
==================================================
Filename          : Ransomware.wannacry.exe.malz
MD5               : db349b97c37d22f5ea1d1841e3c89eb4
SHA1              : e889544aff85ffaf8b0d0da705105dee7c97fe26
CRC32             : 9fbb1227
SHA-256           : 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
SHA-512           : d6c60b8f22f89cbd1262c0aa7ae240577a82002fb149e9127d4edf775a25abcda4e585b6113e79ab4a24bb65f4280532529c2
SHA-384           : 3cde2e74662b432f9137f551af7344820087bcf0acf4572e581fd80735955c2b9547432d341c93e7dcda4a5bcb5d7b00
Full Path         : C:\Users\analyst\Desktop\wannacry\Ransomware.wannacry.exe.malz
Modified Time     : 3/19/2019 7:32:14 PM
Created Time      : 6/28/2024 4:43:49 AM
Entry Modified Time: 6/28/2024 4:43:49 AM
File Size         : 3,723,264
File Version      : 6.1.7601.17514 (win7sp1_rtm.101119-1850)
Product Version   : 6.1.7601.17514
Identical         :
```

Filename	MD5	SHA1
wannacry.exe.malz	db349b97c37d22f5ea1d1841e3c89eb4	e889544aff85ffaf8b0d0da705105dee7c97f



MalLab-Wannacry-REMnux (safe - Static analysis - START) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Jun 27 10:02
remnux@MalLab-Wannacry-REMnux: ~/wannacry
remnux@MalLab-Wannacry-REMn...
1 / 2
Right Ctrl

```
remnux@MalLab-Wannacry-REMnux:~/wannacry$ md5sum wannacry.malz
30fe2f9a048d7a734c8d9233f64810ba  wannacry.malz
remnux@MalLab-Wannacry-REMnux:~/wannacry$ sha1sum wannacry.malz
2027a053de21bd5c783c3f823ed1d36966780ed4  wannacry.malz
remnux@MalLab-Wannacry-REMnux:~/wannacry$ sha256sum wannacry.malz
55504677f82981962d85495231695d3a92aa0b31ec35a957bd9cbbef618658e3  wannacry.malz
remnux@MalLab-Wannacry-REMnux:~/wannacry$ sha512sum wannacry.malz
b657b02506f768db3255293b0c86452b4dfdd30804629c323aaa9510a3b637b0906e5963179ef7d4aaedc14646f2be2b4292
e6584a6c55c6ddb596cff7f20e2a  wannacry.malz
remnux@MalLab-Wannacry-REMnux:~/wannacry$ ^C
remnux@MalLab-Wannacry-REMnux:~/wannacry$ 
```



24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated **Privacy Notice** and **Terms of Use**.

72 / 74

Community Score

72/74 security vendors and 6 sandboxes flagged this file as malicious

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
lhdfrgui.exe

Size 3.55 MB

Last Modification Date 1 hour ago

peexe runtime-modules macro-create-ole malware checks-network-adapters detect-debug-environment exploit cve-2017-0147 checks-user-input direct-cpu-clock-access long-sleeps cve-2017-0144

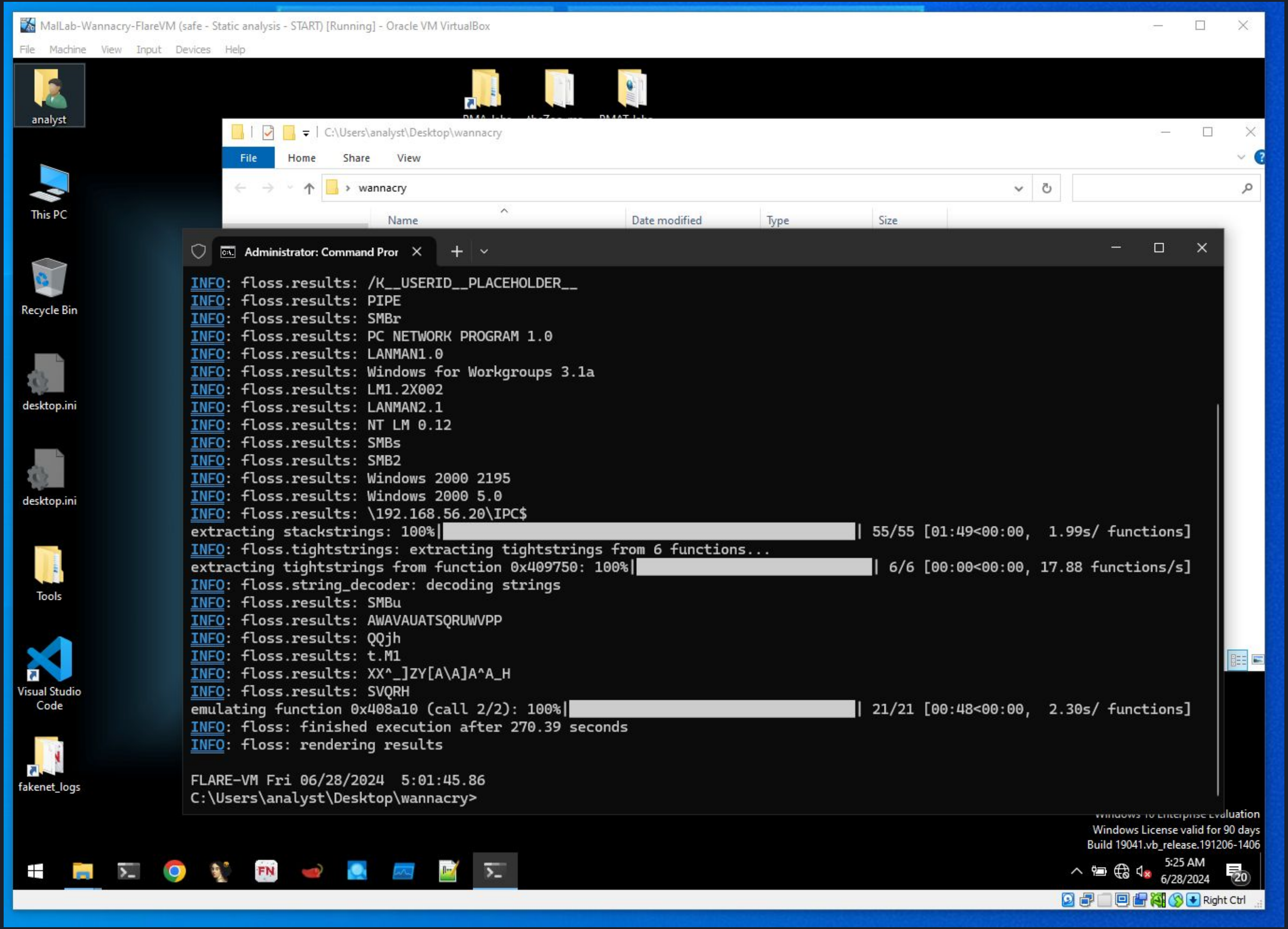
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Popular threat label trojan.wannacry/wanna **Threat categories** trojan ransomware worm **Family labels** wannacry wanna wannacryptor

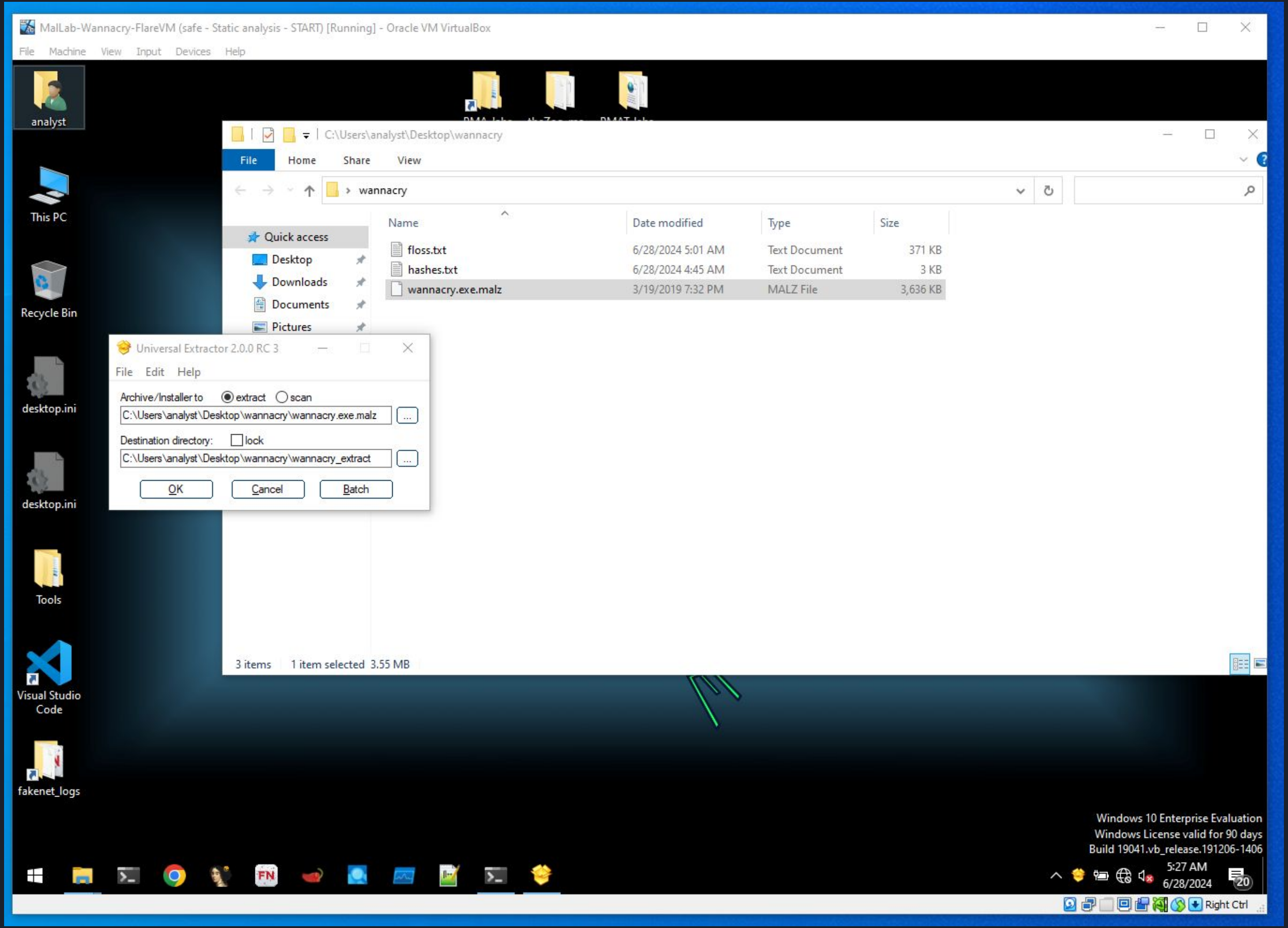
Security vendors' analysis ⓘ

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.WannaCryptor.R200572
Alibaba	Ransom:Win32/WannaCry.398	AliCloud	Exp:Win/CVE.2017.0147
ALYac	Trojan.Ransom.WannaCryptor	Antiy-AVL	Trojan[Exploit]/Win32.CVE-2017-0147
Arcabit	Trojan.Ransom.WannaCryptor.H	Avast	Sf:WNCryLdr-A [Trj]
Avert Labs	Ransom-O.g	AVG	Sf:WNCryLdr-A [Trj]
Avira (no cloud)	TR/Ransom.IZ	Baidu	Win32.Worm.Rbot.a
BitDefender	Trojan.Ransom.WannaCryptor.H	BitDefenderTheta	Gen:NN.ZexaF.36808.Jt0@aePsbmpi


MalLab-Wannacry-FlareVM (safe - Static analysis - START) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
analyst
This PC
Recycle Bin
desktop.ini
desktop.ini
Tools
Visual Studio Code
fakenet_logs
C:\Users\analyst\Desktop\wannacry
File Home Share View
wannacry
Name Date modified Type Size
Administrator: Command Pror
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406
5:25 AM
6/28/2024
Right Ctrl

```
INFO: floss.results: /K__USERID__PLACEHOLDER__
INFO: floss.results: PIPE
INFO: floss.results: SMBr
INFO: floss.results: PC NETWORK PROGRAM 1.0
INFO: floss.results: LANMAN1.0
INFO: floss.results: Windows for Workgroups 3.1a
INFO: floss.results: LM1.2X002
INFO: floss.results: LANMAN2.1
INFO: floss.results: NT LM 0.12
INFO: floss.results: SMBs
INFO: floss.results: SMB2
INFO: floss.results: Windows 2000 2195
INFO: floss.results: Windows 2000 5.0
INFO: floss.results: \192.168.56.20\IPC$
extracting stackstrings: 100%|████████████████████████████████████████| 55/55 [01:49<00:00,  1.99s/ functions]
INFO: floss.tightstrings: extracting tightstrings from 6 functions...
extracting tightstrings from function 0x409750: 100%|██████████████████████| 6/6 [00:00<00:00, 17.88 functions/s]
INFO: floss.string_decoder: decoding strings
INFO: floss.results: SMBu
INFO: floss.results: AWAVAUATSQRUWVPP
INFO: floss.results: QQjh
INFO: floss.results: t.M1
INFO: floss.results: XX^_]ZY[A\A]A^A_H
INFO: floss.results: SVQRH
emulating function 0x408a10 (call 2/2): 100%|████████████████████████████| 21/21 [00:48<00:00,  2.30s/ functions]
INFO: floss: finished execution after 270.39 seconds
INFO: floss: rendering results

FLARE-VM Fri 06/28/2024  5:01:45.86
C:\Users\analyst\Desktop\wannacry>
```



MalLab-Wannacry-FlareVM (safe - Static analysis - START) [Running] - Oracle VM VirtualBox

C:\Users\analyst\Desktop\wannacry

Name	Date modified	Type	Size
floss.txt	6/28/2024 5:01 AM	Text Document	371 KB
hashes.txt	6/28/2024 4:45 AM	Text Document	3 KB
wannacry.exe.malz	3/19/2019 7:32 PM	MALZ File	3,636 KB

3 items   1 item selected 3.55 MB

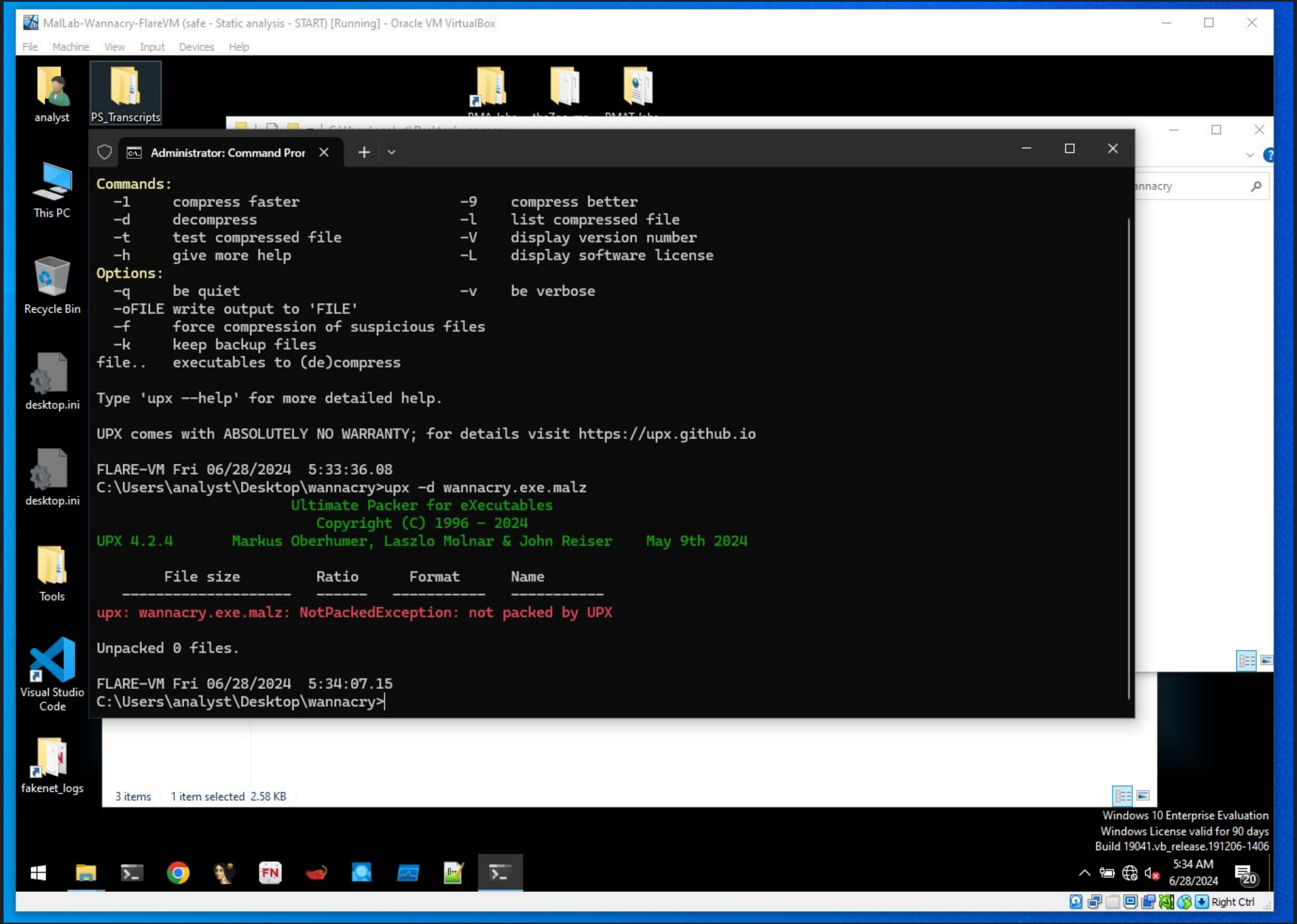
Universal Extractor 2.0.0 RC 3

Archive/Installer to ● extract ○ scan

C:\Users\analyst\Desktop\wannacry\wannacry.exe.malz

Destination directory: □ lock

C:\Users\analyst\Desktop\wannacry\wannacry_extract


MalLab-Wannacry-FlareVM (safe - Static analysis - START) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
analyst
PS_Transcripts
This PC
Recycle Bin
desktop.ini
desktop.ini
Tools
Visual Studio Code
fakenet_logs
Administrator: Command Pror
3 items
1 item selected 2.58 KB
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406
5:34 AM
6/28/2024
Right Ctrl

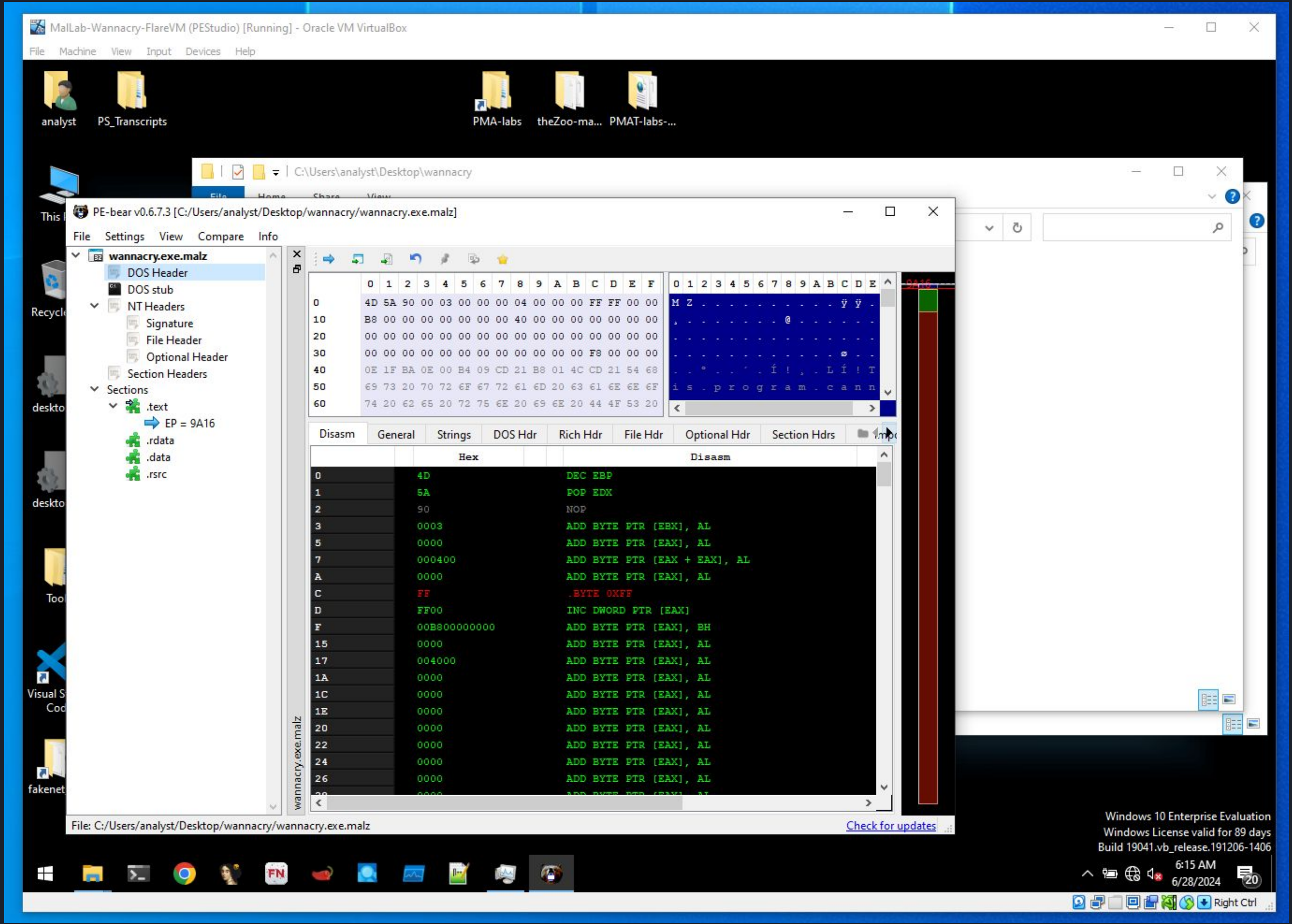
```
Commands:
  -1     compress faster                   -9    compress better
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give more help                    -L    display software license
Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  -k     keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io

FLARE-VM Fri 06/28/2024  5:33:36.08
C:\Users\analyst\Desktop\wannacry>upx -d wannacry.exe.malz
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.4       Markus Oberhumer, Laszlo Molnar & John Reiser    May 9th 2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: wannacry.exe.malz: NotPackedException: not packed by UPX

Unpacked 0 files.

FLARE-VM Fri 06/28/2024  5:34:07.15
C:\Users\analyst\Desktop\wannacry>
```

PE Analysis

Using PEStudio or PE View to analyze binary headers

Inspecting imported functions and data sections

Indicators and API calls related to internet activity



MalLab-Wannacry-FlareVM (PEStudio) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
analyst
PS_Transcripts
PMA-labs
theZoo-ma...
PMAT-labs-...
C:\Users\analyst\Desktop\wannacry
PE-bear v0.6.7.3 [C:/Users/analyst/Desktop/wannacry/wannacry.exe.malz]
File Settings View Compare Info
Disasm General Strings DOS Hdr Rich Hdr File Hdr Optional Hdr Section Hdrs
Check for updates
Windows 10 Enterprise Evaluation
Windows License valid for 89 days
Build 19041.vb_release.191206-1406
6:15 AM
6/28/2024
Right Ctrl

```
wannacry.exe.malz
    DOS Header
    DOS stub
    NT Headers
        Signature
        File Header
        Optional Header
    Section Headers
    Sections
        .text
            EP = 9A16
        .rdata
        .data
        .rsrc
```

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
0     4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   M Z . . . . . . . . . . ÿ ÿ .
10    B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ¸ . . . . . . . @ . . . . . .
20    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . .
30    00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00   . . . . . . . . . . . . ø . .
40    0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   . . º . . ´ . Í ! ¸ . L Í ! T
50    69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   i s . p r o g r a m . c a n n
60    74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
```

```
      Hex              Disasm
0     4D               DEC EBP
1     5A               POP EDX
2     90               NOP
3     0003             ADD BYTE PTR [EBX], AL
5     0000             ADD BYTE PTR [EAX], AL
7     000400           ADD BYTE PTR [EAX + EAX], AL
A     0000             ADD BYTE PTR [EAX], AL
C     FF               .BYTE 0XFF
D     FF00             INC DWORD PTR [EAX]
F     00B800000000     ADD BYTE PTR [EAX], BH
15    0000             ADD BYTE PTR [EAX], AL
17    004000           ADD BYTE PTR [EAX], AL
1A    0000             ADD BYTE PTR [EAX], AL
1C    0000             ADD BYTE PTR [EAX], AL
1E    0000             ADD BYTE PTR [EAX], AL
20    0000             ADD BYTE PTR [EAX], AL
22    0000             ADD BYTE PTR [EAX], AL
24    0000             ADD BYTE PTR [EAX], AL
26    0000             ADD BYTE PTR [EAX], AL
```

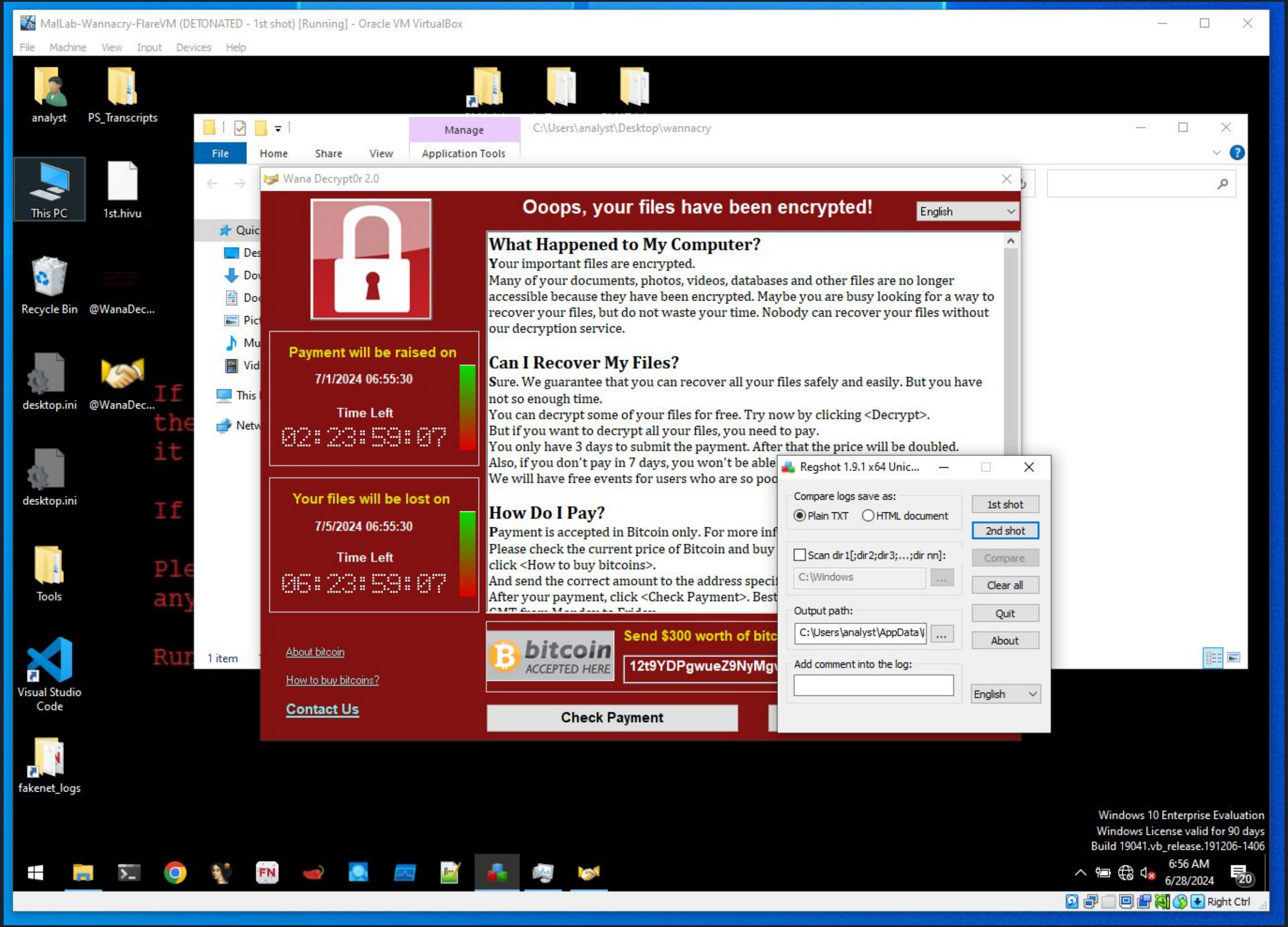
File: C:/Users/analyst/Desktop/wannacry/wannacry.exe.malz

Basic Dynamic Analysis

Executing the malware in a controlled environment

Immediate effects (file encryption, system changes)

Network traffic analysis using Wireshark and FakeNet-NG/inetSim


MalLab-Wannacry-FlareVM (DETONATED - 1st shot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
analyst
PS_Transcripts
This PC
1st.hivu
Recycle Bin
@WanaDec...
desktop.ini
@WanaDec...
desktop.ini
Tools
Visual Studio Code
fakenet_logs
Manage
C:\Users\analyst\Desktop\wannacry
File Home Share View Application Tools
Quic
Des
Dov
Doc
Pict
Mu
Vid
This
Netw
1 item
If
the
it
If
Ple
any
Rur

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able

We will have free events for users who are so poo

How Do I Pay?

Payment is accepted in Bitcoin only. For more inf

Please check the current price of Bitcoin and buy

click <How to buy bitcoins>.

And send the correct amount to the address speci

After your payment, click <Check Payment>. Best

Payment will be raised on

7/1/2024 06:55:30

Time Left

02:23:59:07

Your files will be lost on

7/5/2024 06:55:30

Time Left

06:23:59:07

Send $300 worth of bitc

12t9YDPgwueZ9NyMg

Regshot 1.9.1 x64 Unic...

Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\Windows

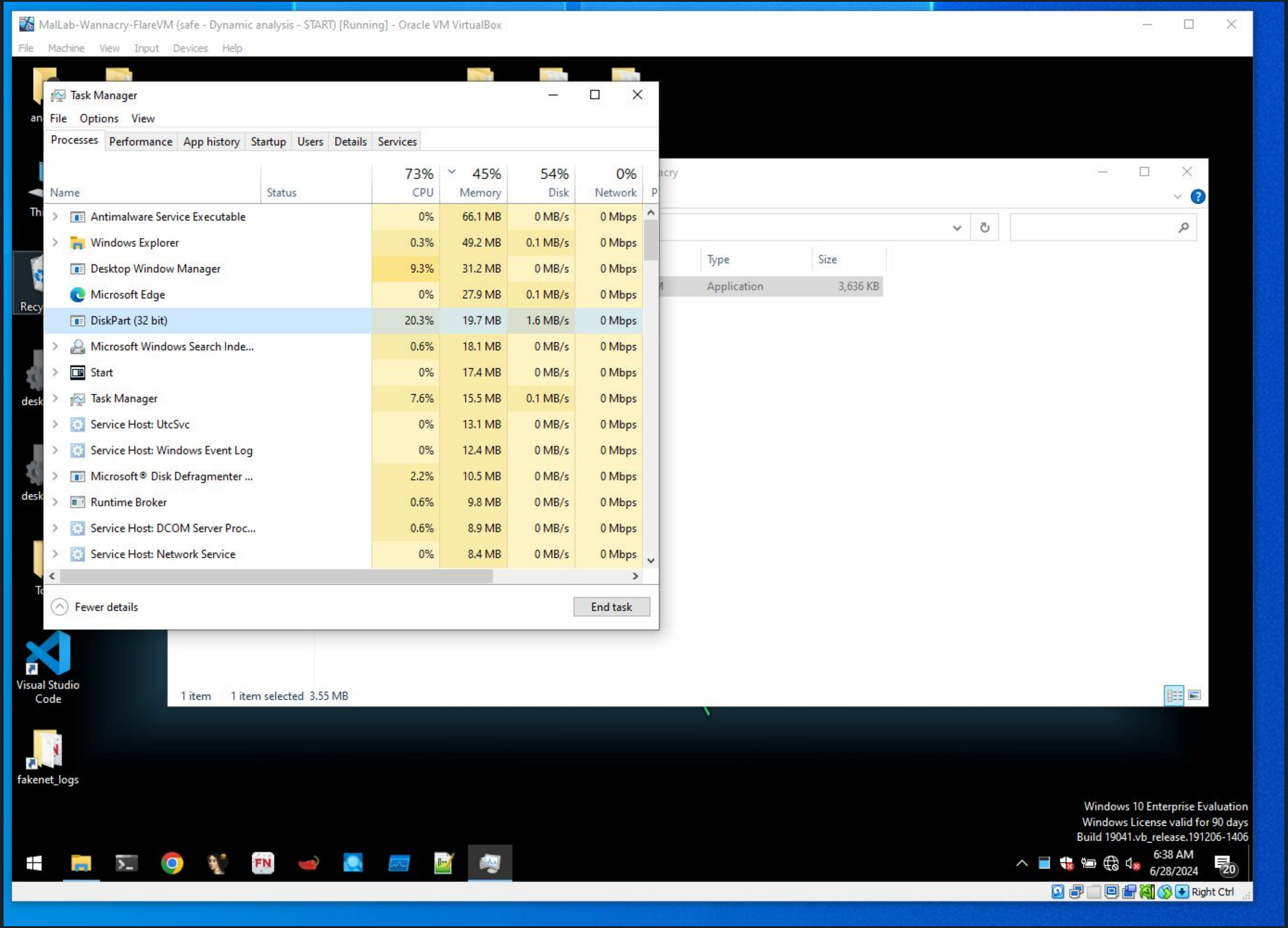
Output path:

C:\Users\analyst\AppData\

Add comment into the log:

Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406

6:56 AM
6/28/2024



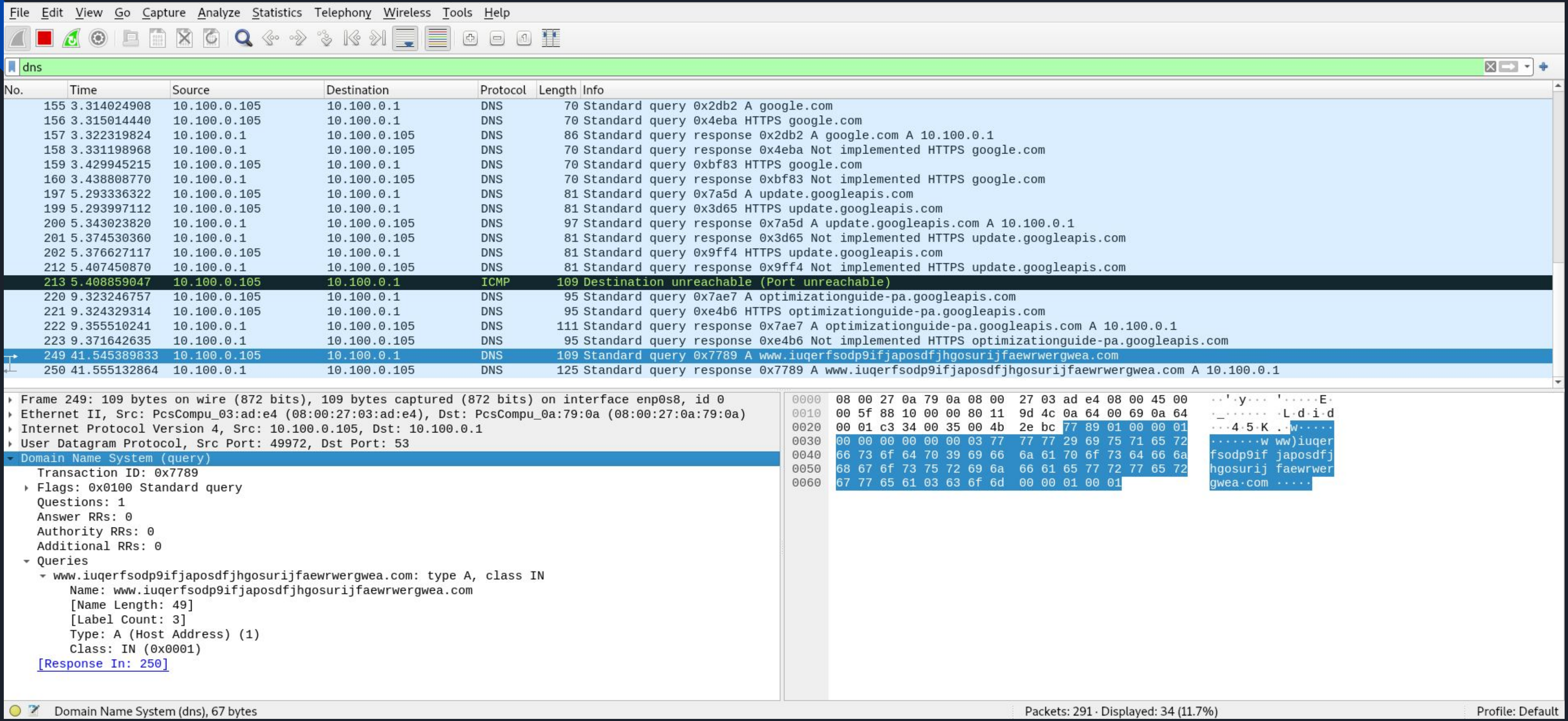
Name	Status	73% CPU	45% Memory	54% Disk	0% Network
Antimalware Service Executable		0%	66.1 MB	0 MB/s	0 Mbps
Windows Explorer		0.3%	49.2 MB	0.1 MB/s	0 Mbps
Desktop Window Manager		9.3%	31.2 MB	0 MB/s	0 Mbps
Microsoft Edge		0%	27.9 MB	0.1 MB/s	0 Mbps
DiskPart (32 bit)		20.3%	19.7 MB	1.6 MB/s	0 Mbps
Microsoft Windows Search Inde...		0.6%	18.1 MB	0 MB/s	0 Mbps
Start		0%	17.4 MB	0 MB/s	0 Mbps
Task Manager		7.6%	15.5 MB	0.1 MB/s	0 Mbps
Service Host: UtcSvc		0%	13.1 MB	0 MB/s	0 Mbps
Service Host: Windows Event Log		0%	12.4 MB	0 MB/s	0 Mbps
Microsoft® Disk Defragmenter ...		2.2%	10.5 MB	0 MB/s	0 Mbps
Runtime Broker		0.6%	9.8 MB	0 MB/s	0 Mbps
Service Host: DCOM Server Proc...		0.6%	8.9 MB	0 MB/s	0 Mbps
Service Host: Network Service		0%	8.4 MB	0 MB/s	0 Mbps

Type	Size
Application	3,636 KB

1 item 1 item selected 3.55 MB

Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406

6:38 AM
6/28/2024



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.  Time          Source        Destination   Protocol Length Info
 155 3.314024908   10.100.0.105  10.100.0.1    DNS        70 Standard query 0x2db2 A google.com
 156 3.315014440   10.100.0.105  10.100.0.1    DNS        70 Standard query 0x4eba HTTPS google.com
 157 3.322319824   10.100.0.1    10.100.0.105  DNS        86 Standard query response 0x2db2 A google.com A 10.100.0.1
 158 3.331198968   10.100.0.1    10.100.0.105  DNS        70 Standard query response 0x4eba Not implemented HTTPS google.com
 159 3.429945215   10.100.0.105  10.100.0.1    DNS        70 Standard query 0xbf83 HTTPS google.com
 160 3.438808770   10.100.0.1    10.100.0.105  DNS        70 Standard query response 0xbf83 Not implemented HTTPS google.com
 197 5.293336322   10.100.0.105  10.100.0.1    DNS        81 Standard query 0x7a5d A update.googleapis.com
 199 5.293997112   10.100.0.105  10.100.0.1    DNS        81 Standard query 0x3d65 HTTPS update.googleapis.com
 200 5.343023820   10.100.0.1    10.100.0.105  DNS        97 Standard query response 0x7a5d A update.googleapis.com A 10.100.0.1
 201 5.374530360   10.100.0.1    10.100.0.105  DNS        81 Standard query response 0x3d65 Not implemented HTTPS update.googleapis.com
 202 5.376627117   10.100.0.105  10.100.0.1    DNS        81 Standard query 0x9ff4 HTTPS update.googleapis.com
 212 5.407450870   10.100.0.1    10.100.0.105  DNS        81 Standard query response 0x9ff4 Not implemented HTTPS update.googleapis.com
 213 5.408859047   10.100.0.105  10.100.0.1    ICMP      109 Destination unreachable (Port unreachable)
 220 9.323246757   10.100.0.105  10.100.0.1    DNS        95 Standard query 0x7ae7 A optimizationguide-pa.googleapis.com
 221 9.324329314   10.100.0.105  10.100.0.1    DNS        95 Standard query 0xe4b6 HTTPS optimizationguide-pa.googleapis.com
 222 9.355510241   10.100.0.1    10.100.0.105  DNS       111 Standard query response 0x7ae7 A optimizationguide-pa.googleapis.com A 10.100.0.1
 223 9.371642635   10.100.0.1    10.100.0.105  DNS        95 Standard query response 0xe4b6 Not implemented HTTPS optimizationguide-pa.googleapis.com
 249 41.545389833  10.100.0.105  10.100.0.1    DNS       109 Standard query 0x7789 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
 250 41.555132864  10.100.0.1    10.100.0.105  DNS       125 Standard query response 0x7789 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 10.100.0.1
```

```
▸ Frame 249: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface enp0s8, id 0
▸ Ethernet II, Src: PcsCompu_03:ad:e4 (08:00:27:03:ad:e4), Dst: PcsCompu_0a:79:0a (08:00:27:0a:79:0a)
▸ Internet Protocol Version 4, Src: 10.100.0.105, Dst: 10.100.0.1
▸ User Datagram Protocol, Src Port: 49972, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x7789
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN
        Name: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
        [Name Length: 49]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 250]
```

```
0000  08 00 27 0a 79 0a 08 00  27 03 ad e4 08 00 45 00   ··'·y··· '·····E·
0010  00 5f 88 10 00 00 80 11  9d 4c 0a 64 00 69 0a 64   ·_······ ·L·d·i·d
0020  00 01 c3 34 00 35 00 4b  2e bc 77 89 01 00 00 01   ···4·5·K .·w·····
0030  00 00 00 00 00 00 03 77  77 77 29 69 75 71 65 72   ·······w ww)iuqer
0040  66 73 6f 64 70 39 69 66  6a 61 70 6f 73 64 66 6a   fsodp9if japosdfj
0050  68 67 6f 73 75 72 69 6a  66 61 65 77 72 77 65 72   hgosurij faewrwer
0060  67 77 65 61 03 63 6f 6d  00 00 01 00 01            gwea·com ·····
```

Domain Name System (dns), 67 bytes

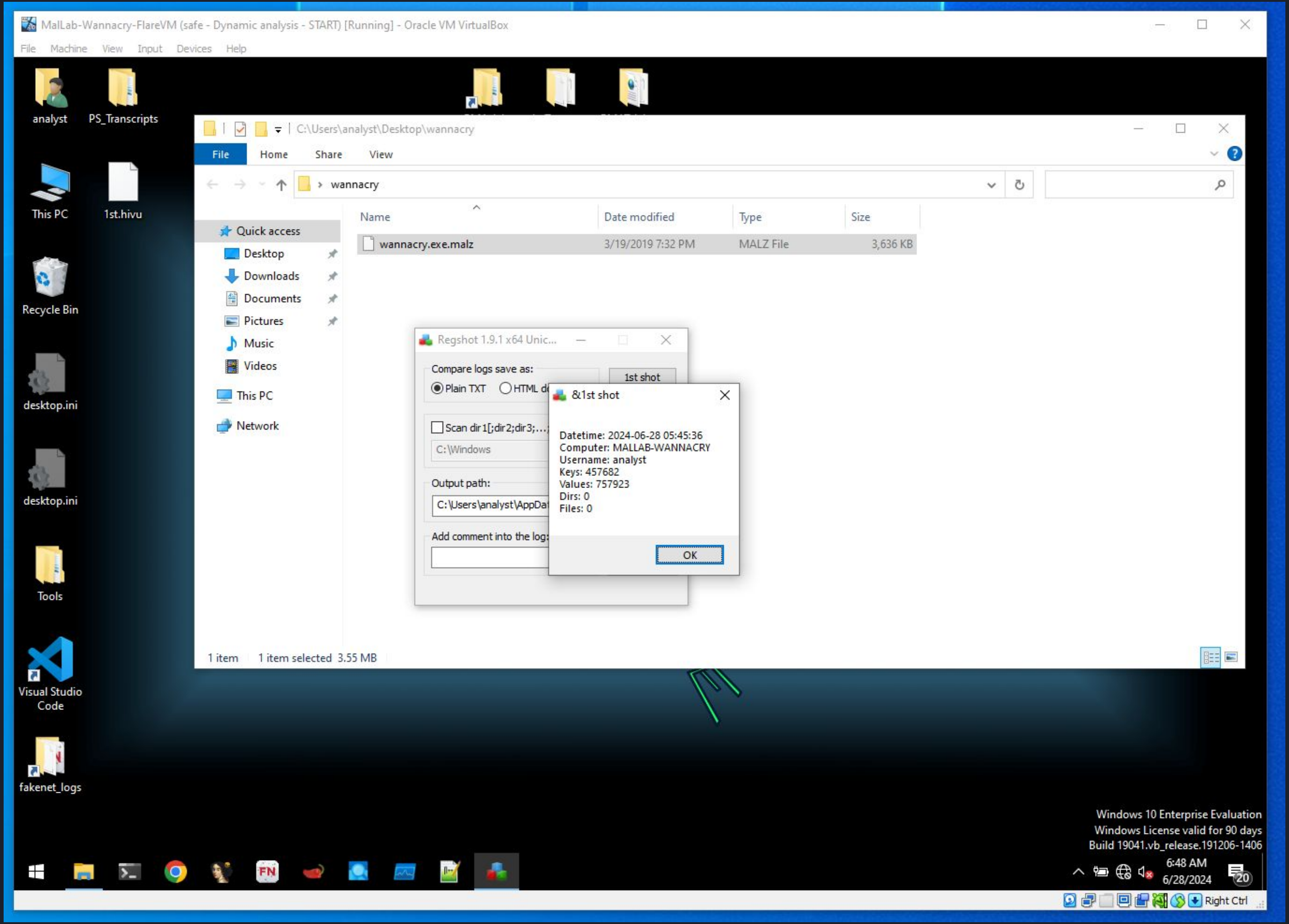
Packets: 291 · Displayed: 34 (11.7%)

Profile: Default

Registry and File System Changes

Using Regshot to compare registry snapshots

Identifying persistence mechanisms (e.g., hidden directories, registry keys)


MalLab-Wannacry-FlareVM (safe - Dynamic analysis - START) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
analyst
PS_Transcripts
This PC
1st.hivu
Recycle Bin
desktop.ini
desktop.ini
Tools
Visual Studio Code
fakenet_logs
C:\Users\analyst\Desktop\wannacry
File Home Share View
wannacry
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network
Name
Date modified
Type
Size
1 item 1 item selected 3.55 MB
Regshot 1.9.1 x64 Unic...
1st shot
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406
6:48 AM
6/28/2024
Right Ctrl

Name	Date modified	Type	Size
wannacry.exe.malz	3/19/2019 7:32 PM	MALZ File	3,636 KB

Compare logs save as:
● Plain TXT ○ HTML d

□ Scan dir1[;dir2;dir3;...
C:\Windows

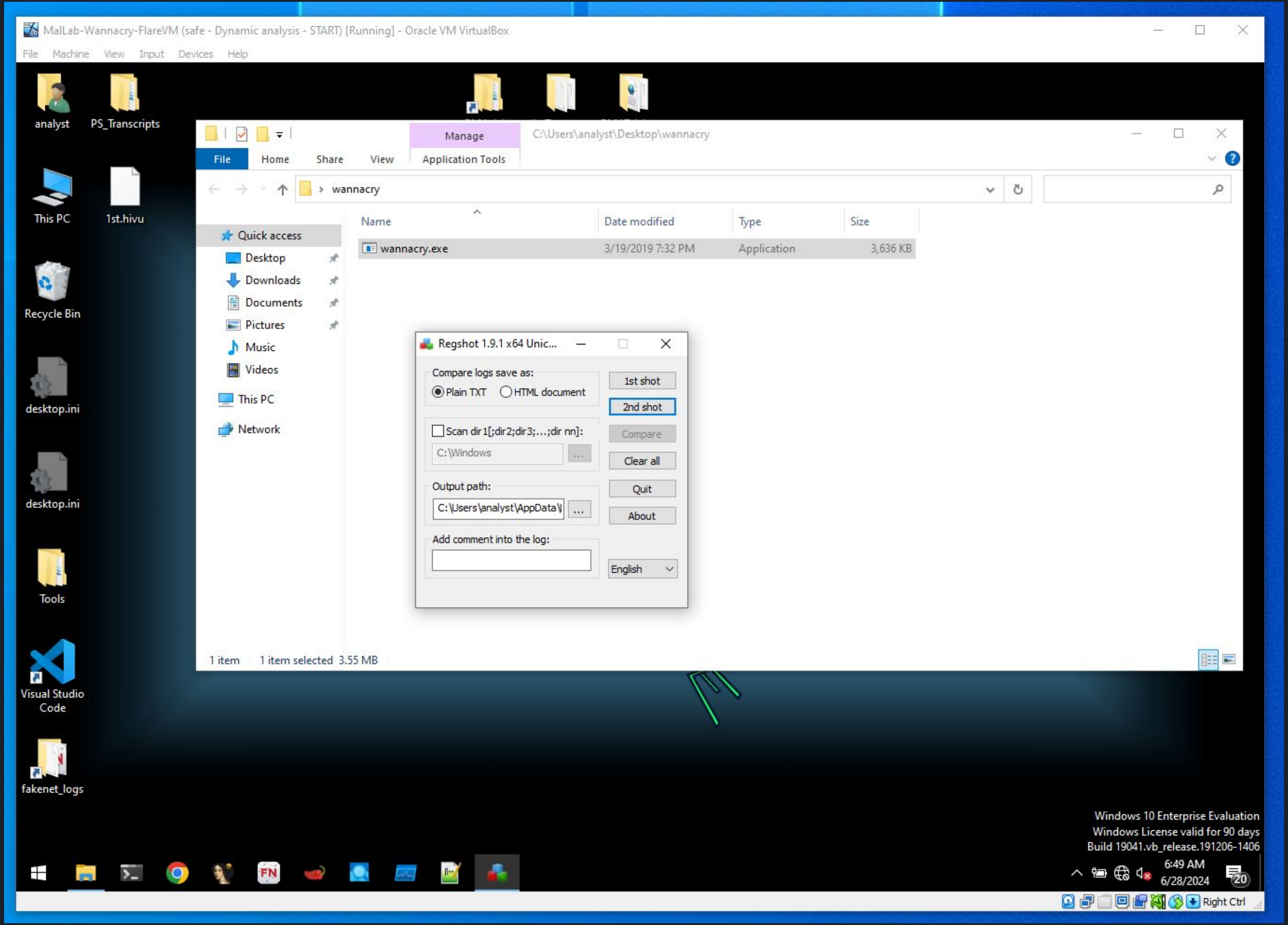
Output path:
C:\Users\analyst\AppDat

Add comment into the log:

&1st shot

```
Datetime: 2024-06-28 05:45:36
Computer: MALLAB-WANNACRY
Username: analyst
Keys: 457682
Values: 757923
Dirs: 0
Files: 0
```

OK



MalLab-Wannacry-FlareVM (safe - Dynamic analysis - START) [Running] - Oracle VM VirtualBox

C:\Users\analyst\Desktop\wannacry

Name	Date modified	Type	Size
wannacry.exe	3/19/2019 7:32 PM	Application	3,636 KB

1 item 1 item selected 3.55 MB

Regshot 1.9.1 x64 Unic...

Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]: C:\Windows

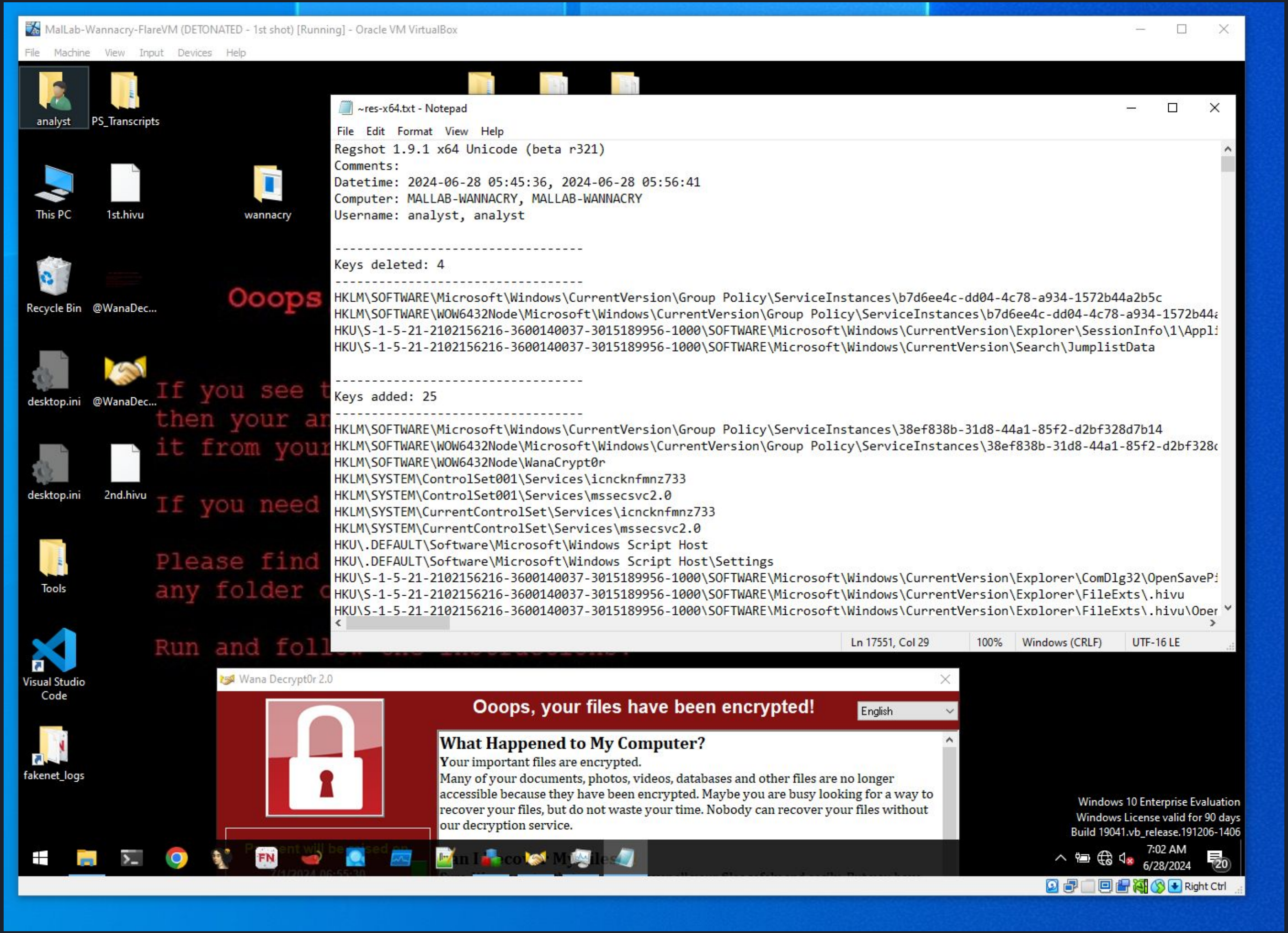
Output path: C:\Users\analyst\AppData\

Add comment into the log:

English

Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406

6:49 AM
6/28/2024



```
Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2024-06-28 05:45:36, 2024-06-28 05:56:41
Computer: MALLAB-WANNACRY, MALLAB-WANNACRY
Username: analyst, analyst

----------------------------------
Keys deleted: 4
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\b7d6ee4c-dd04-4c78-a934-1572b44a2b5c
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\b7d6ee4c-dd04-4c78-a934-1572b44a
HKU\S-1-5-21-2102156216-3600140037-3015189956-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Appli
HKU\S-1-5-21-2102156216-3600140037-3015189956-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData

----------------------------------
Keys added: 25
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\38ef838b-31d8-44a1-85f2-d2bf328d7b14
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\38ef838b-31d8-44a1-85f2-d2bf328d
HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r
HKLM\SYSTEM\ControlSet001\Services\icncknfmnz733
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0
HKLM\SYSTEM\CurrentControlSet\Services\icncknfmnz733
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0
HKU\.DEFAULT\Software\Microsoft\Windows Script Host
HKU\.DEFAULT\Software\Microsoft\Windows Script Host\Settings
HKU\S-1-5-21-2102156216-3600140037-3015189956-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePi
HKU\S-1-5-21-2102156216-3600140037-3015189956-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu
HKU\S-1-5-21-2102156216-3600140037-3015189956-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu\Oper
```

Ooops

If you see t
then your ar
it from your

If you need

Please find
any folder c

Run and foll

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

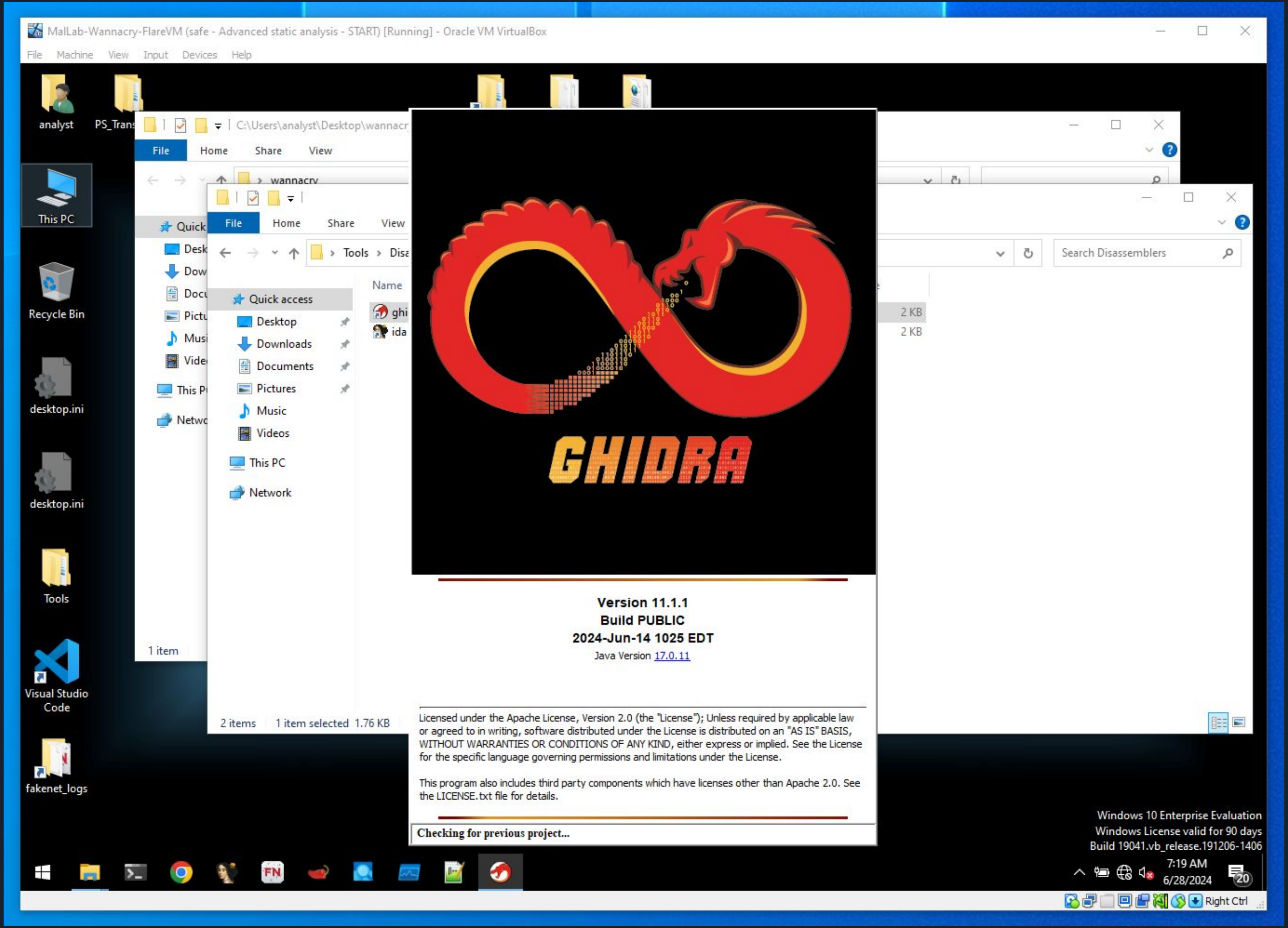
Advanced Static Analysis with Ghidra

Importing the WannaCry binary into Ghidra

Decompiling and examining high-level code

Key function analysis (network communication, file encryption)

Identifying the kill-switch URL handling code

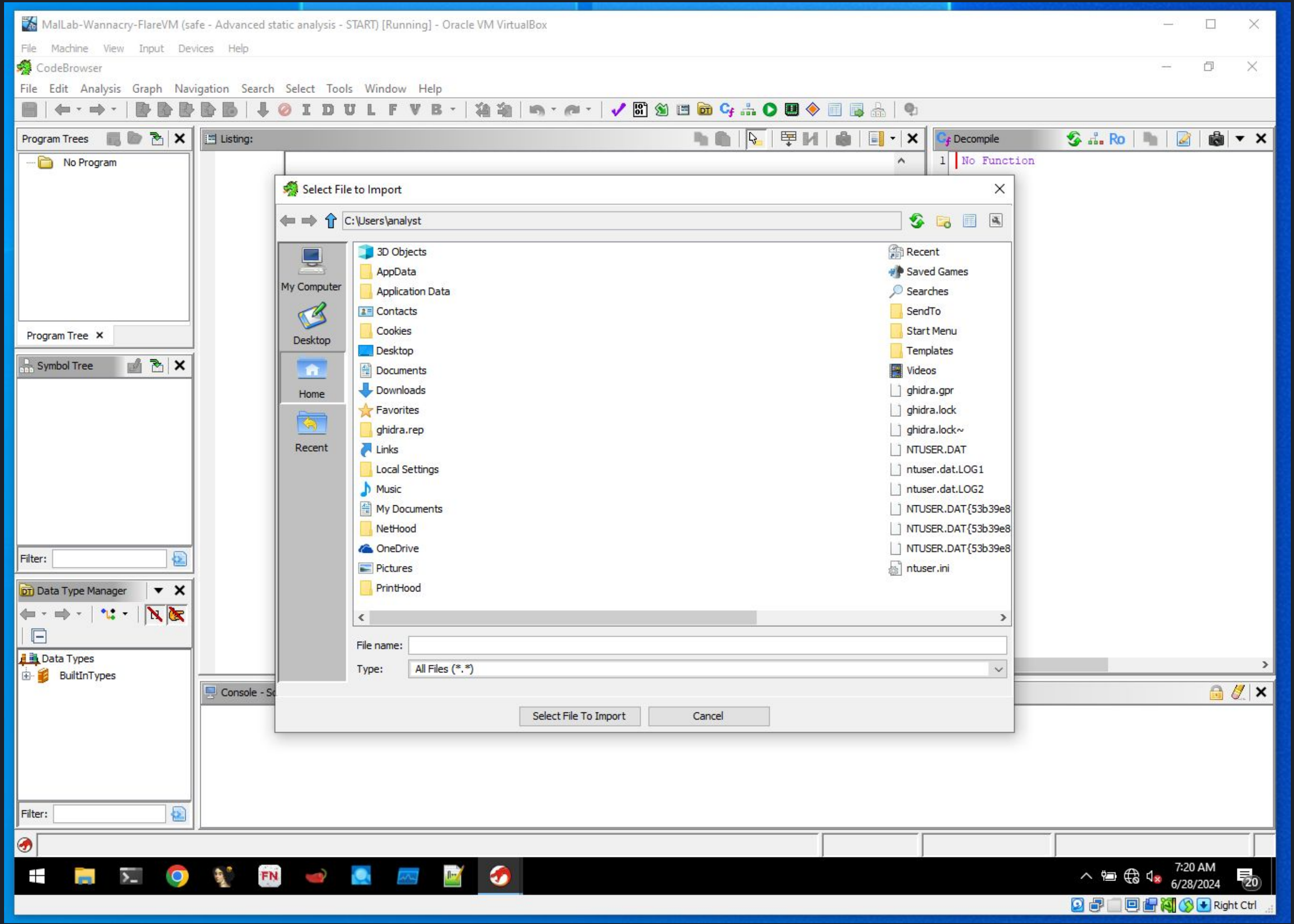


Version 11.1.1
Build PUBLIC
2024-Jun-14 1025 EDT
Java Version 17.0.11

Licensed under the Apache License, Version 2.0 (the "License"); Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This program also includes third party components which have licenses other than Apache 2.0. See the LICENSE.txt file for details.

Checking for previous project...



MalLab-Wannacry-FlareVM (safe - Advanced static analysis - START) [Running] - Oracle VM VirtualBox

CodeBrowser

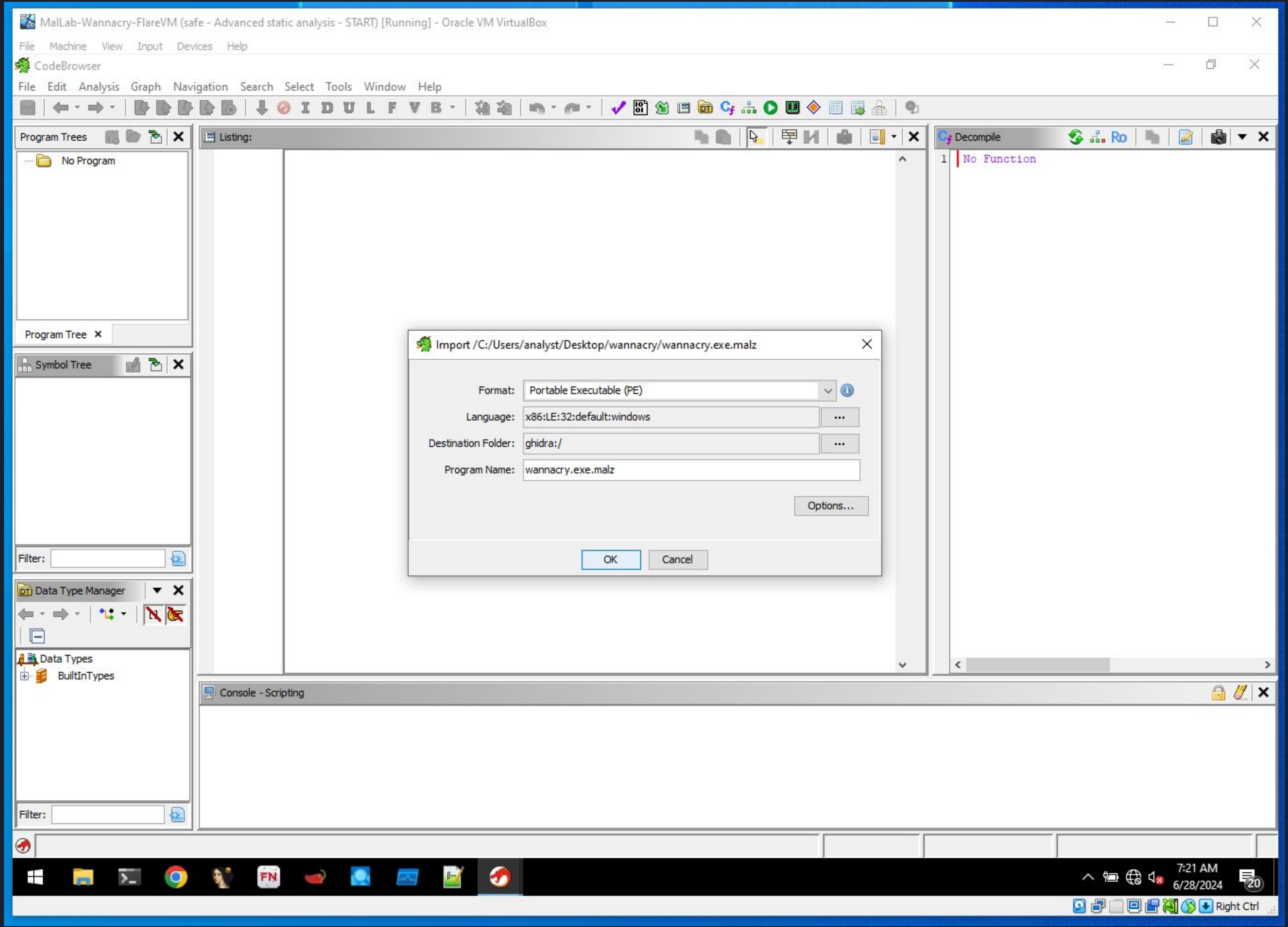
Select File to Import

C:\Users\analyst

```
3D Objects          Recent
AppData             Saved Games
Application Data    Searches
Contacts            SendTo
Cookies             Start Menu
Desktop             Templates
Documents           Videos
Downloads           ghidra.gpr
Favorites           ghidra.lock
ghidra.rep          ghidra.lock~
Links               NTUSER.DAT
Local Settings      ntuser.dat.LOG1
Music               ntuser.dat.LOG2
My Documents        NTUSER.DAT{53b39e8
NetHood             NTUSER.DAT{53b39e8
OneDrive            NTUSER.DAT{53b39e8
Pictures            ntuser.ini
PrintHood
```

File name:

Type: All Files (*.*)


MalLab-Wannacry-FlareVM (safe - Advanced static analysis - START) [Running] - Oracle VM VirtualBox

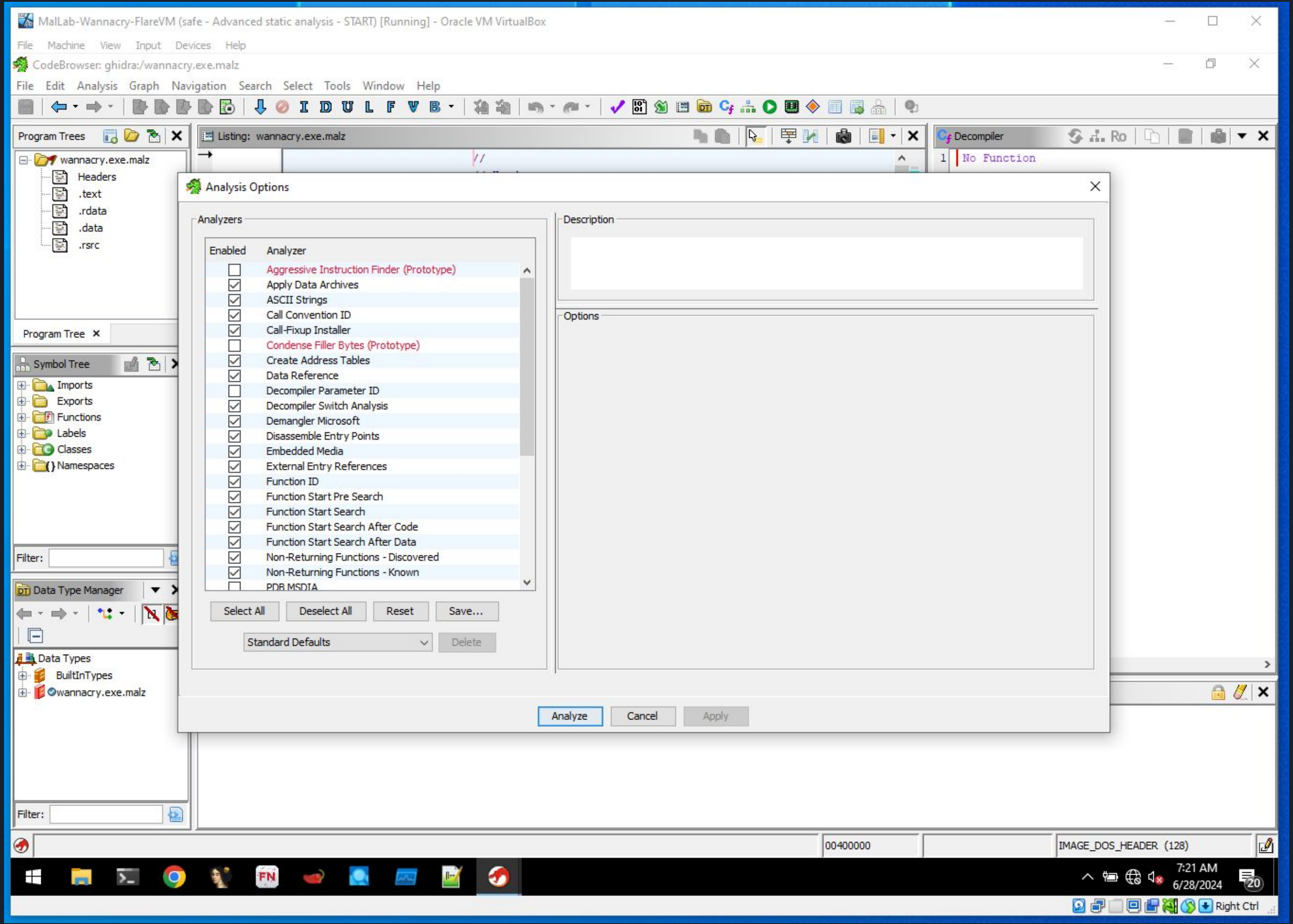
Import /C:/Users/analyst/Desktop/wannacry/wannacry.exe.malz

Format: Portable Executable (PE)

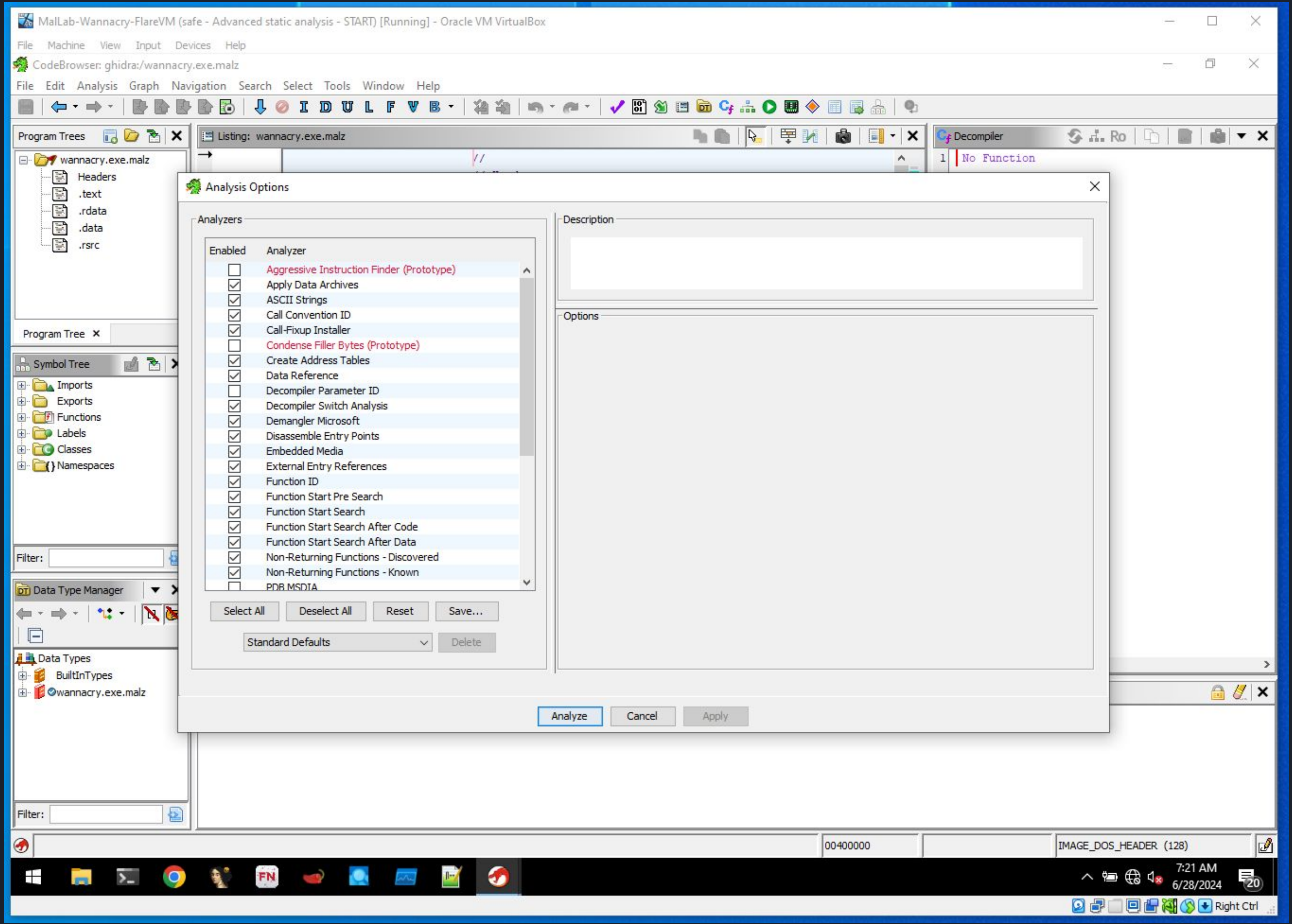
Language: x86:LE:32:default:windows

Destination Folder: ghidra:/

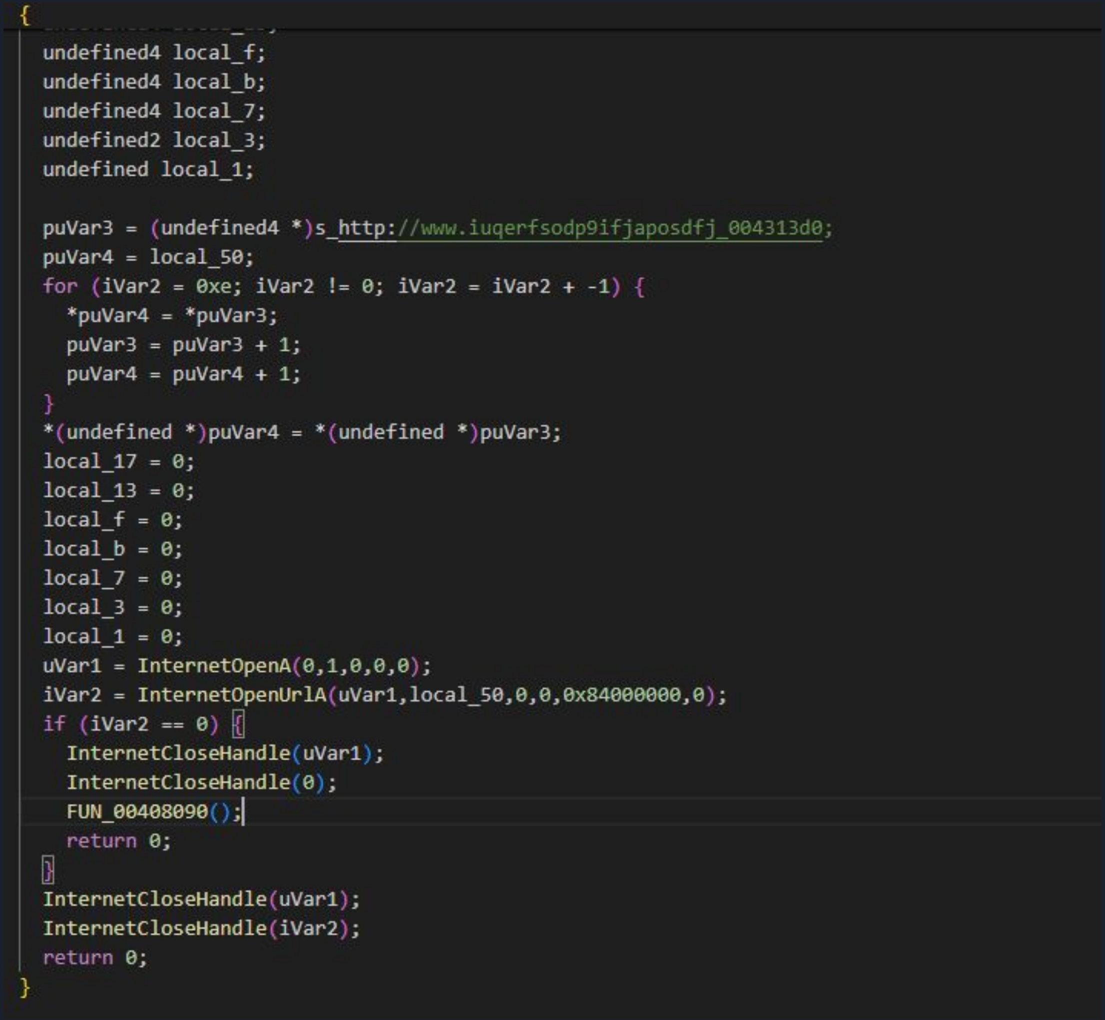
Program Name: wannacry.exe.malz



Enabled	Analyzer
☐	Aggressive Instruction Finder (Prototype)
☑	Apply Data Archives
☑	ASCII Strings
☑	Call Convention ID
☑	Call-Fixup Installer
☐	Condense Filler Bytes (Prototype)
☑	Create Address Tables
☑	Data Reference
☐	Decompiler Parameter ID
☑	Decompiler Switch Analysis
☑	Demangler Microsoft
☑	Disassemble Entry Points
☑	Embedded Media
☑	External Entry References
☑	Function ID
☑	Function Start Pre Search
☑	Function Start Search
☑	Function Start Search After Code
☑	Function Start Search After Data
☑	Non-Returning Functions - Discovered
☑	Non-Returning Functions - Known
☐	PDB MSDIA



Enabled	Analyzer
☐	Aggressive Instruction Finder (Prototype)
☑	Apply Data Archives
☑	ASCII Strings
☑	Call Convention ID
☑	Call-Fixup Installer
☐	Condense Filler Bytes (Prototype)
☑	Create Address Tables
☑	Data Reference
☐	Decompiler Parameter ID
☑	Decompiler Switch Analysis
☑	Demangler Microsoft
☑	Disassemble Entry Points
☑	Embedded Media
☑	External Entry References
☑	Function ID
☑	Function Start Pre Search
☑	Function Start Search
☑	Function Start Search After Code
☑	Function Start Search After Data
☑	Non-Returning Functions - Discovered
☑	Non-Returning Functions - Known
☐	PDB MSDIA



```
{
  undefined4 local_f;
  undefined4 local_b;
  undefined4 local_7;
  undefined2 local_3;
  undefined local_1;

  puVar3 = (undefined4 *)s_http://www.iuqerfsodp9ifjaposdfj_004313d0;
  puVar4 = local_50;
  for (iVar2 = 0xe; iVar2 != 0; iVar2 = iVar2 + -1) {
    *puVar4 = *puVar3;
    puVar3 = puVar3 + 1;
    puVar4 = puVar4 + 1;
  }
  *(undefined *)puVar4 = *(undefined *)puVar3;
  local_17 = 0;
  local_13 = 0;
  local_f = 0;
  local_b = 0;
  local_7 = 0;
  local_3 = 0;
  local_1 = 0;
  uVar1 = InternetOpenA(0,1,0,0,0);
  iVar2 = InternetOpenUrlA(uVar1,local_50,0,0,0x84000000,0);
  if (iVar2 == 0) {
    InternetCloseHandle(uVar1);
    InternetCloseHandle(0);
    FUN_00408090();
    return 0;
  }
  InternetCloseHandle(uVar1);
  InternetCloseHandle(iVar2);
  return 0;
}
```

Questions & Answers

Open the floor for questions