Configuration Manual

MSc Research Project
Programme Name

Ian Ngugi Wamunyu
Student ID: X20110448

School of Computing
National College of Ireland

Supervisor: DR Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. …… Ian Ngugi Wamunyu ……

Student ID: …… X20110448……..……

Programme: … MSc Cyber Security …… **Year:** ……2023……..

Module: …… Research Project ……..……

Lecturer: …… Dr Imran Khan ……..……

Submission Due Date: ……18/09/2023……..……

Project Title: …… Comparative Analysis of Malware Investigative Tools ……

Word Count: ……921…… **Page Count:** ……14……..……..……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Ian Ngugi Wamunyu……

Date: ……18/09/2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Ian Ngugi Wamunyu
X20110488

1 INTRODUCTION

This is a configuration manual for a comparative analysis of malware investigation tools. The manual is divided into section 2 machine configurations, section 3 installation Section 4 Malware analysis and section 5 references.

2 CONFIGURATION

2.1 Hardware configuration

Host machine	
Computer	HP
RAM	16GB
Memory	1TB
Operating system	Windows 11
Virtual Machine (Virtual Box)	
Operating system	Windows 10
RAM	8GB
Memory	80GB

Table 1. Hardware Configuration

2.2 Software Configuration

Malware Analysis Tools

Name	**Category**	**Program**	**Operating System**
Virtual box	Virtual machine	Open Source	Cross-platform
Ninite (multiple basic system applications		Open Source	Windows
Virus Total	Static tools	Open Source	Cross-platform
PEStudio		Open Source	Windows
ProMonitor	Dynamic tools	Open Source	Windows
Regshot		Open Source	Windows
Volatility	Memory tools	Open Source	Cross-platform
GRR Rapid Response		Open Source	Cross-platform
Radare2	Code tools	Open Source	Cross-platform
Ghidra		Open Source	Cross-platform

Table 3. Software resources

3 Installation

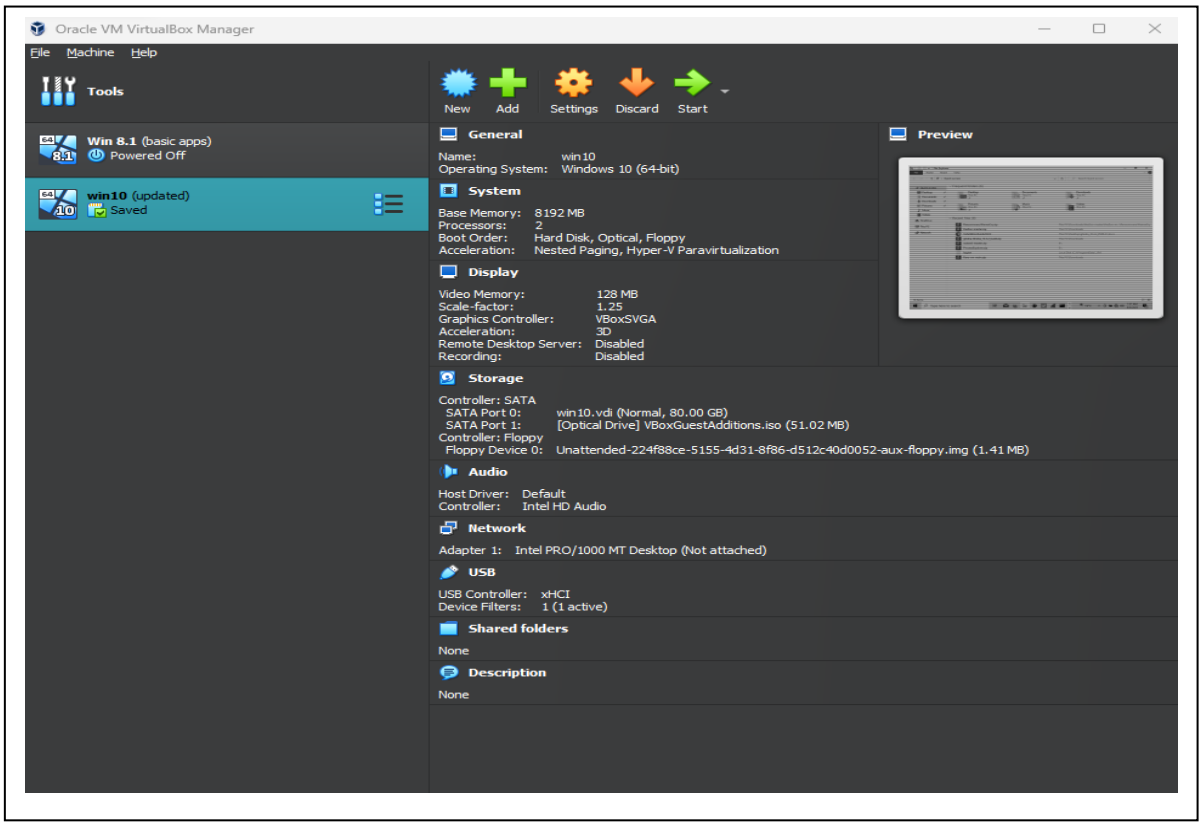


Fig. 1. Oracle VM VirtualBox Manager

Figure 1 shows the VirtualBox sandbox setup: Operating system-windows 10 (64bit), memory-8GB, processors -2, graphics controller-VBoxSVGA, storage-80GB, shared folders disabled, network-adapter 1(NAT network) and(not-attached) while conducting analysis.

Fig2 shows the use of ninite software to download multiple basic applications to mimic a normal computing environment(Swieskowski and Kuzins, no date).

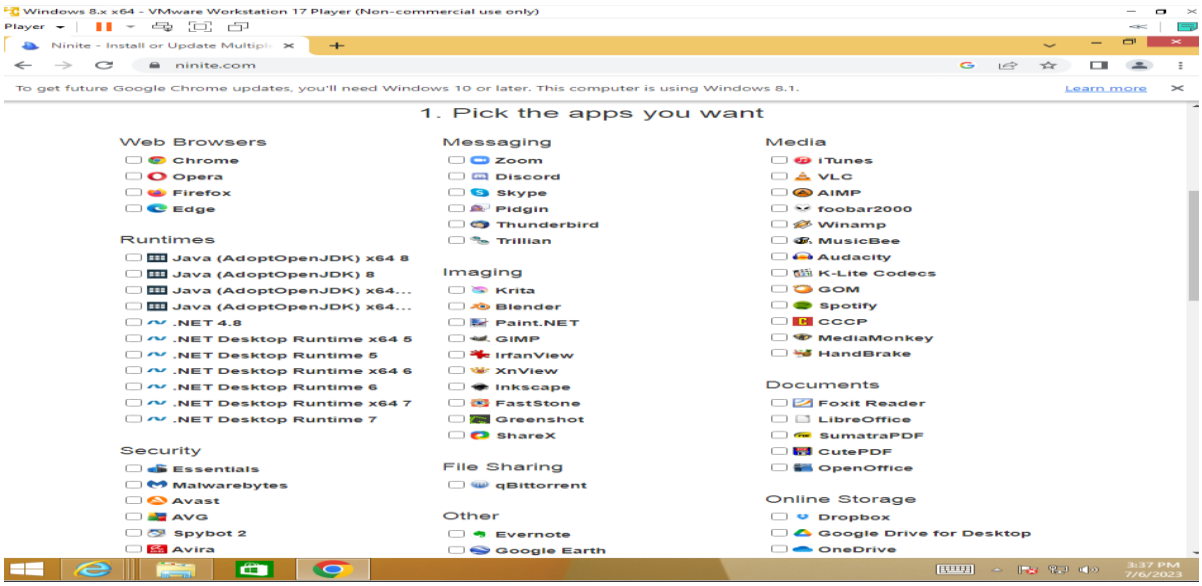


Fig. 2. Basic application setups

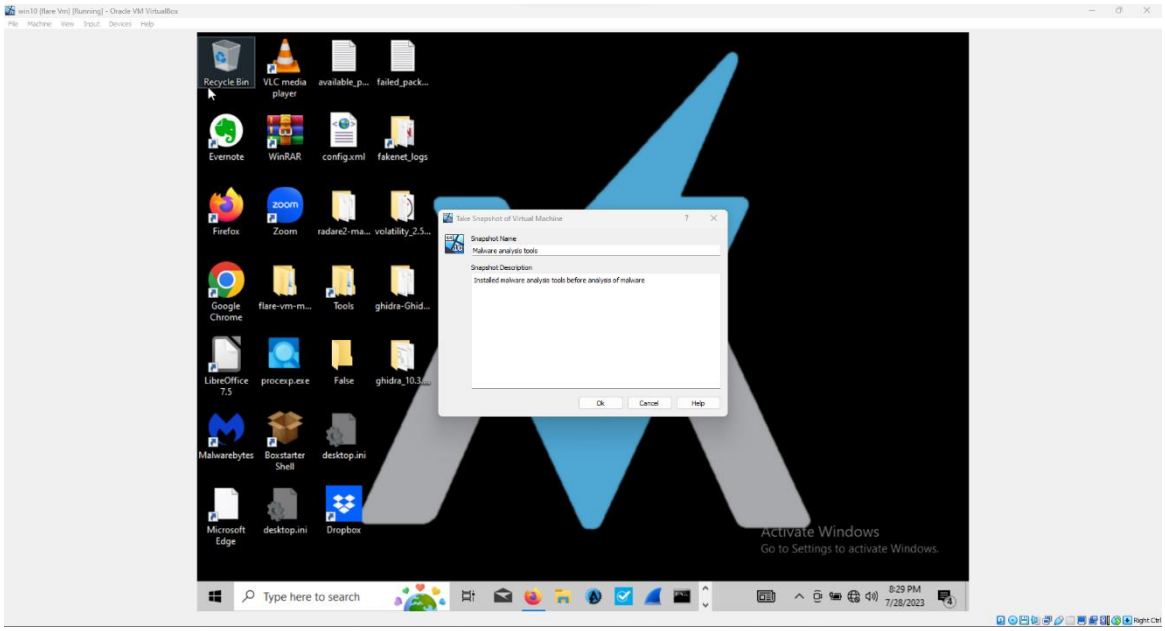
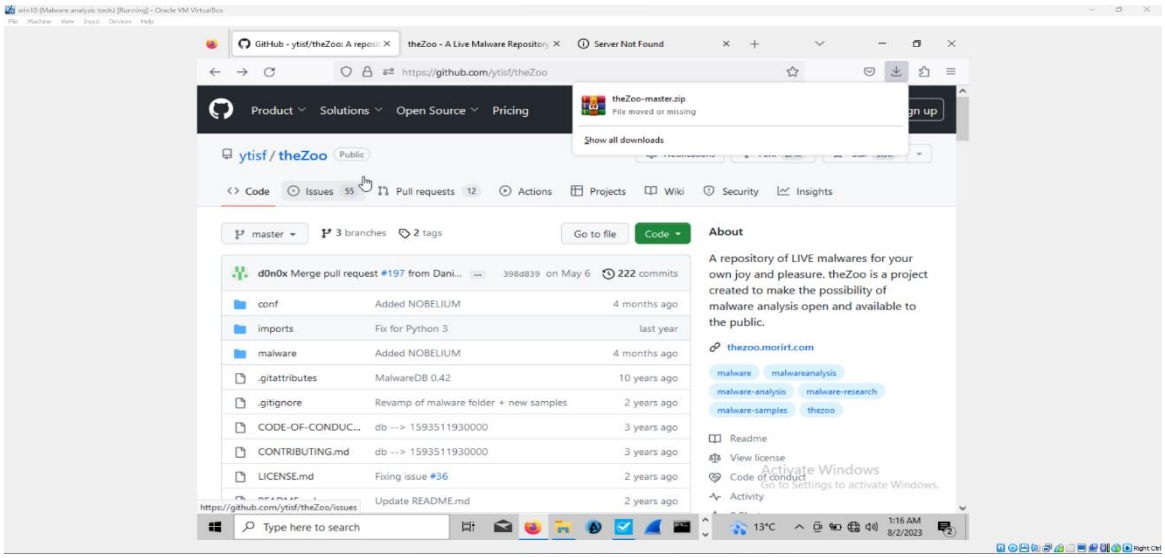


Fig. 3. Malware analysis tools setup

Figure 3 illustrates a virtual machine snapshot. This will enable the user to revert to the previous state after malware analysis.



4. Malware dataset

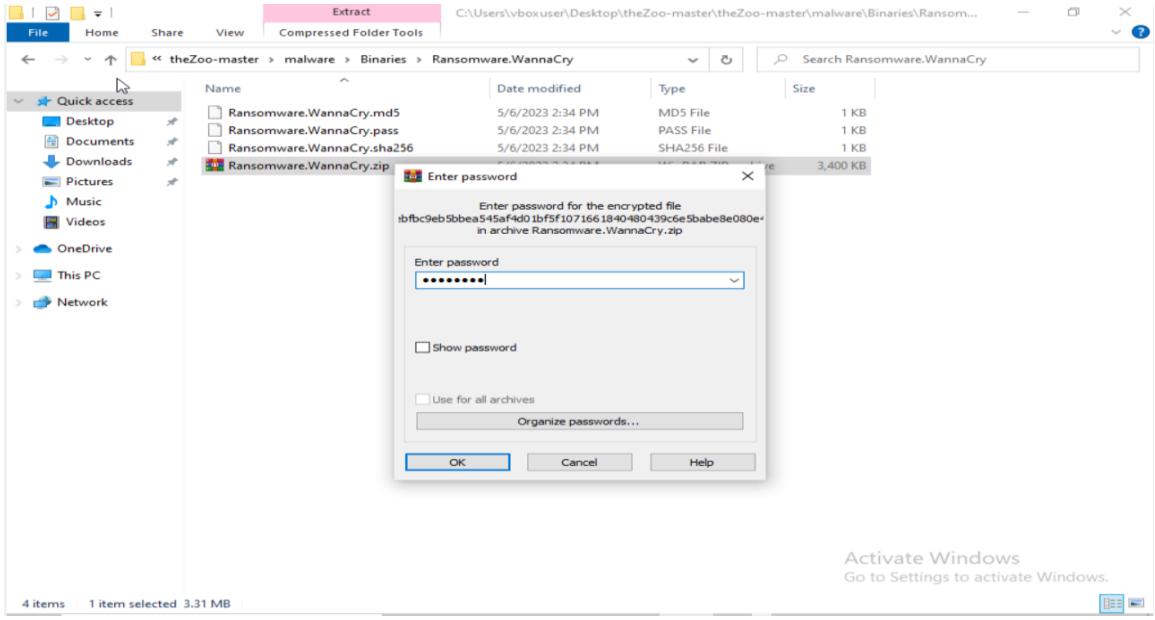


Fig. 5. Ransomware WannaCry

Both fig 4 & 5 shows WannaCry portable executable from theZoo malware repository database (Nativ and Shalev, no date)

It is important to note that the executable is compressed, and password protected to safeguard a user's system if clicked on accidentally. The password can be found in the artefact file include under *theZoo/malware/Binaries/Ransomware.WannaCry/Ransomware.Wanacry.pass* directory**.**

4 Malware Analysis

4.1 Virus total

Figure 6 and 7 shows the portable executable submitted to Virus Total via *https://www.virustotal.com/gui/home/upload*(virus Total, 2023)
This tool shows results for 65 out of 69 antivirus software.

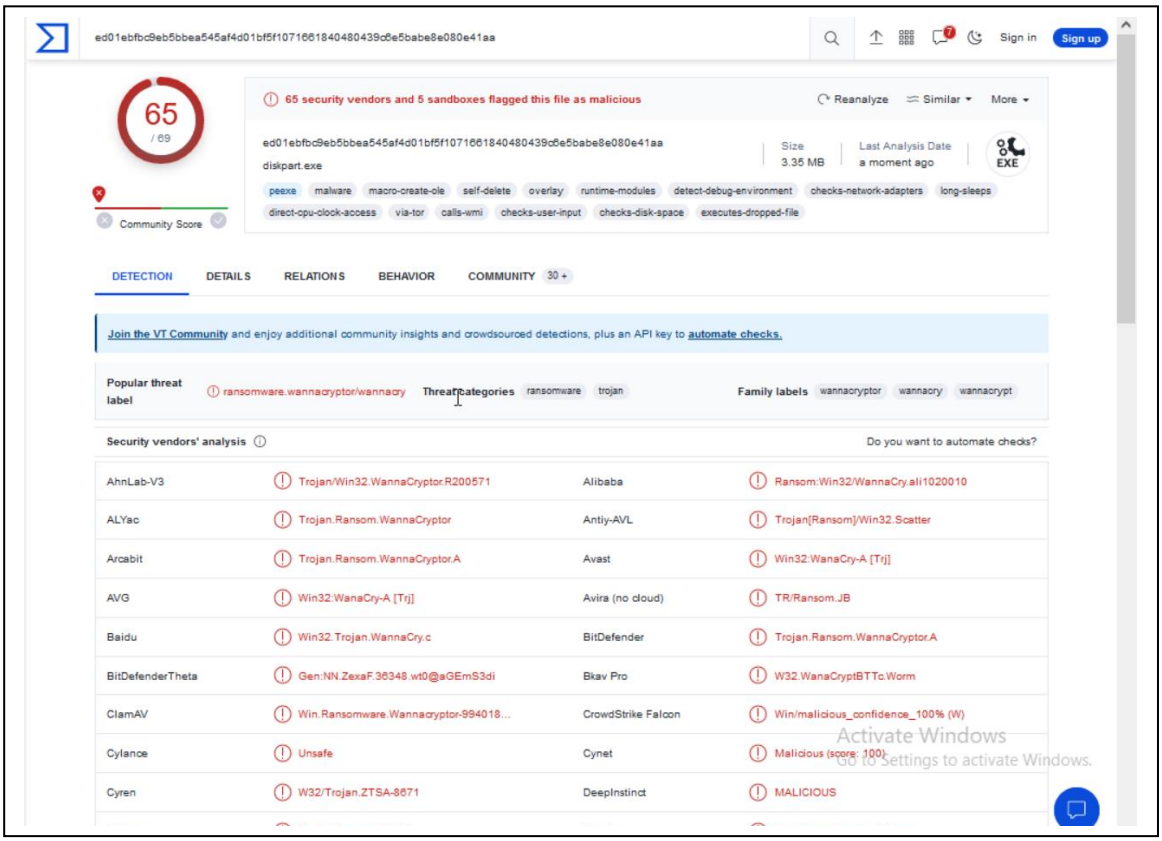


Fig. 6 Virus total analysis

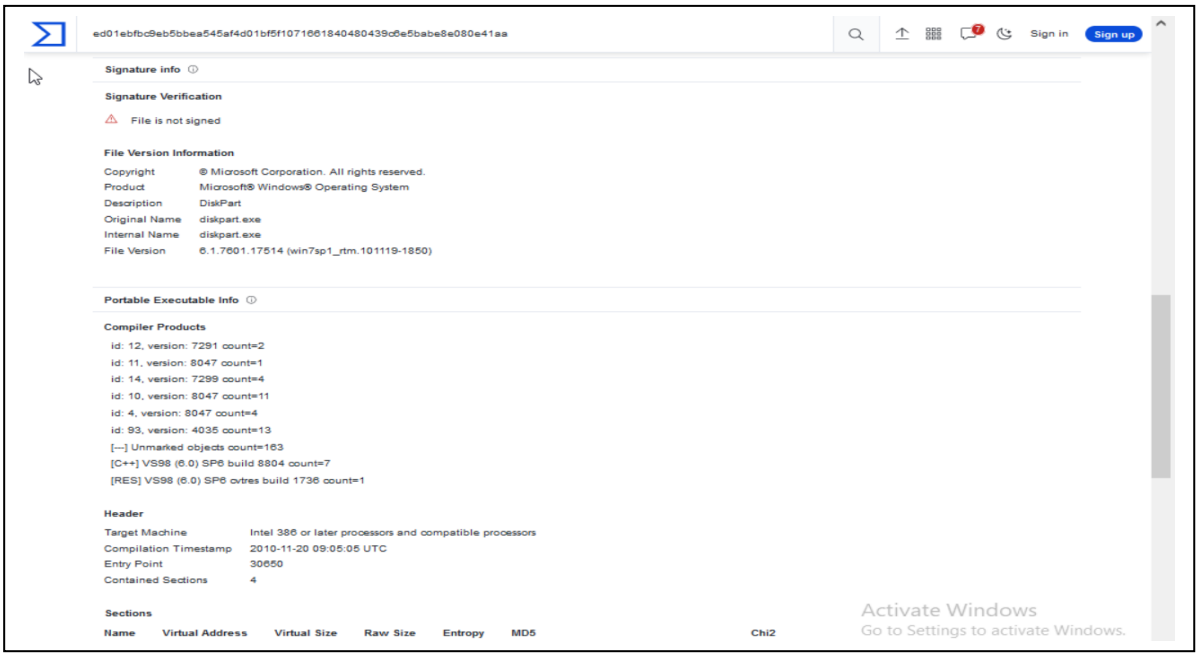

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Sign in
Sign up
Signature info
Signature Verification
File is not signed
File Version Information
Copyright © Microsoft Corporation. All rights reserved.
Product Microsoft® Windows® Operating System
Description DiskPart
Original Name diskpart.exe
Internal Name diskpart.exe
File Version 6.1.7601.17514 (win7sp1_rtm.101119-1850)
Portable Executable Info
Compiler Products
id: 12, version: 7291 count=2
id: 11, version: 8047 count=1
id: 14, version: 7299 count=4
id: 10, version: 8047 count=11
id: 4, version: 8047 count=4
id: 93, version: 4035 count=13
[---] Unmarked objects count=163
[C++] VS98 (6.0) SP6 build 8804 count=7
[RES] VS98 (6.0) SP6 cvtres build 1736 count=1
Header
Target Machine Intel 386 or later processors and compatible processors
Compilation Timestamp 2010-11-20 09:05:05 UTC
Entry Point 30650
Contained Sections 4
Sections
Name Virtual Address Virtual Size Raw Size Entropy MD5 Chi2
Activate Windows
Go to Settings to activate Windows.

Fig. 7 Virus total analysis

4.2 PEstudio(Ochsenmeier, 2023)

This tool provides a direct link to the virus total (65/69) score. To fully maximise the potential of this tool, the user should open it with administrative privilege.

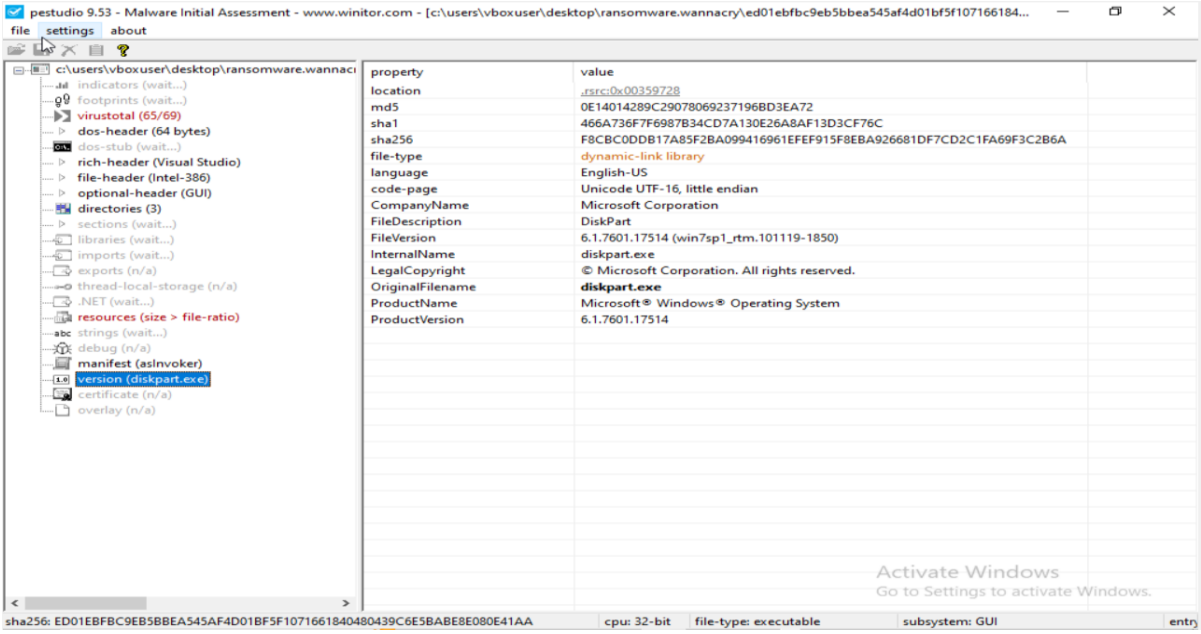


Fig. 8 PE studio analysis

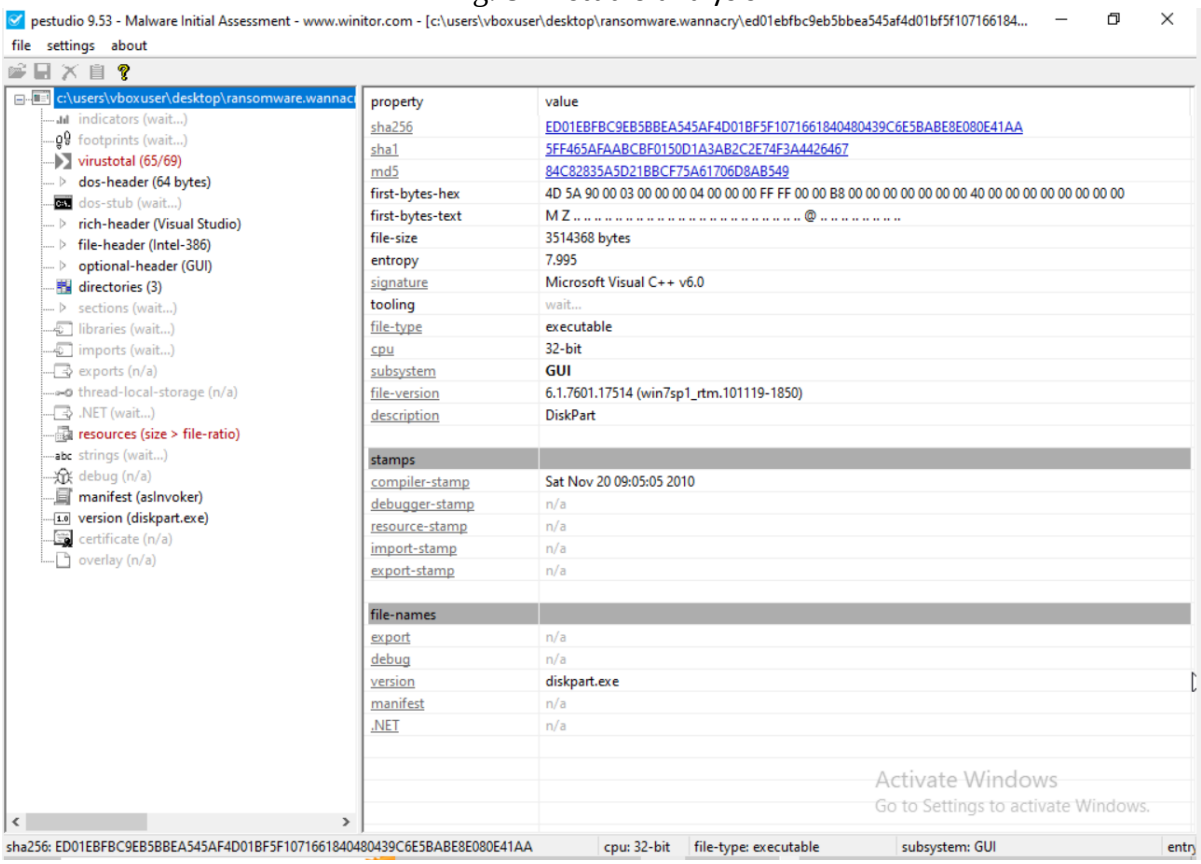


Fig. 8 PE studio analysis

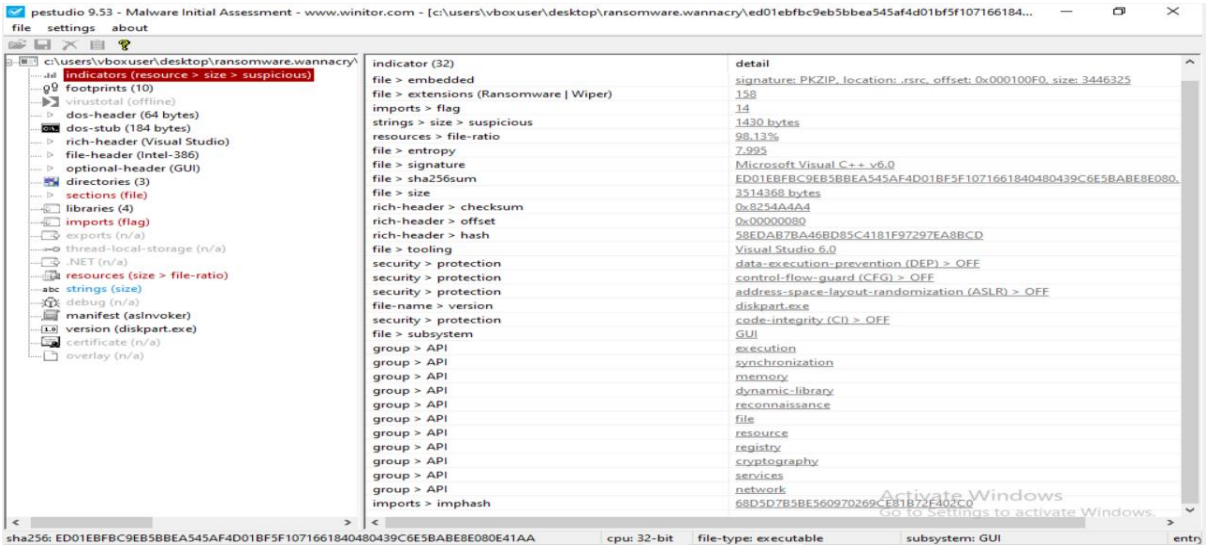


Fig. 9 PEstudio

4.3 ProMonitor(Russinovich, 2023)

Process monitor is like Windows task manager and focuses on program activity. Fig 10 shows the executable's operations, path, results, and details. Fig 11 shows WannaCry's process tree and every child's process from it.

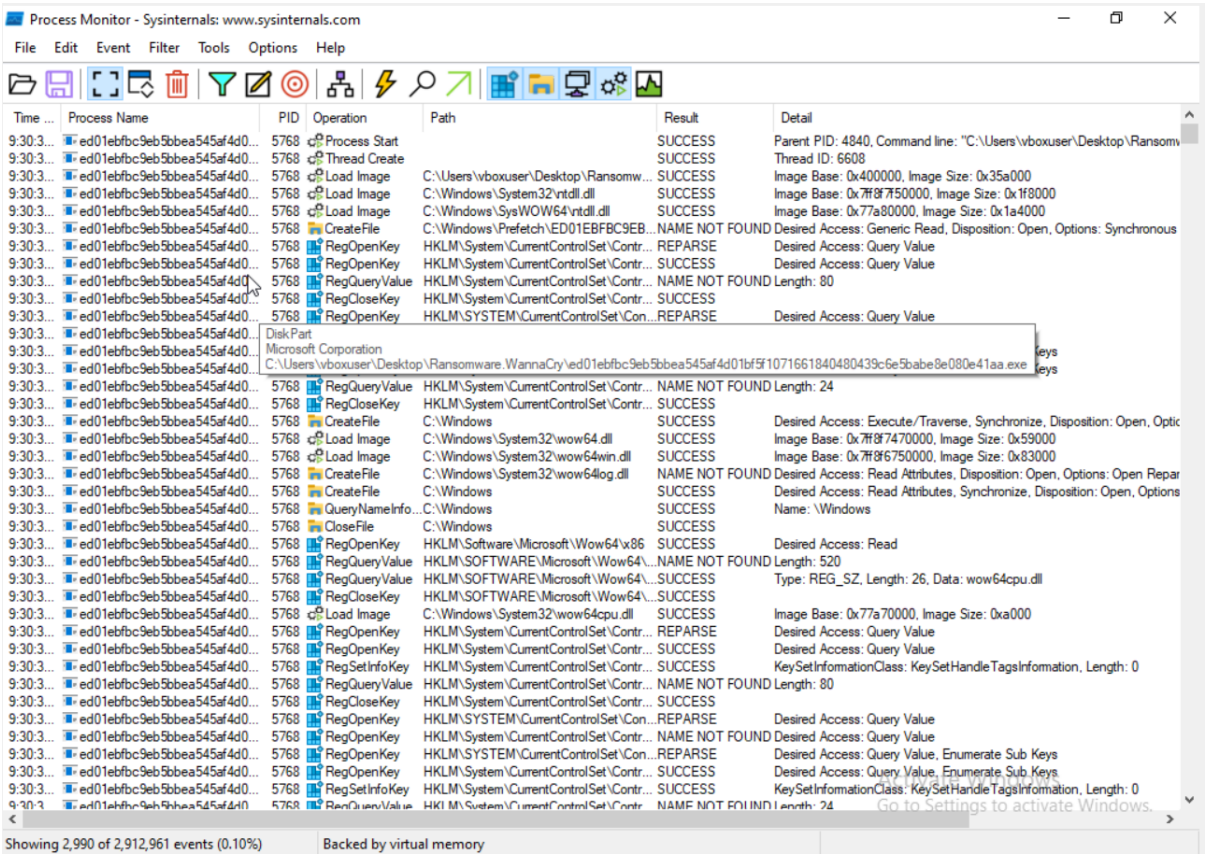


Fig. 10 ProMonitor

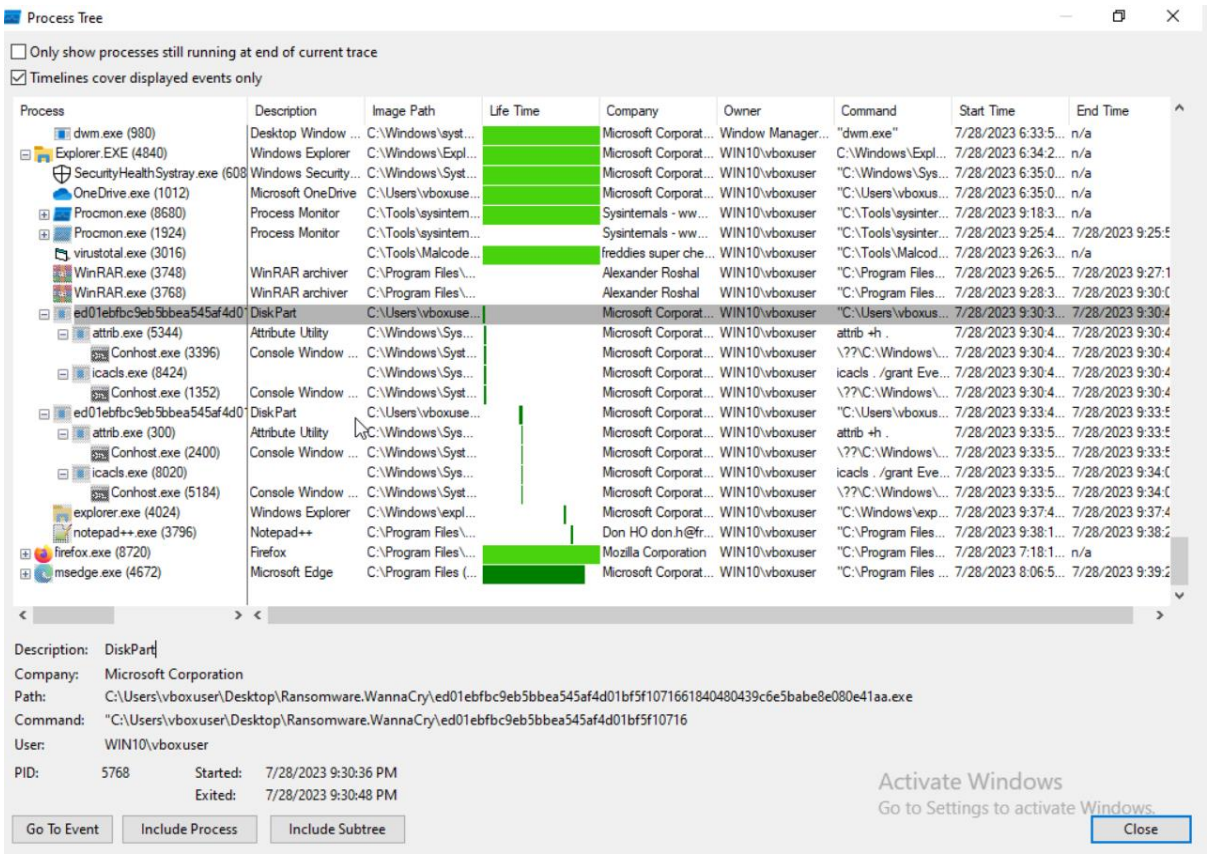


Fig. 11 ProMonitor

4.4 Regshot(TiANWEi, 2023)

The 1st snapshot is taken before executing the malicious program. The 2nd snapshot as shown in Fig 12 is taken after executing WannaCry.

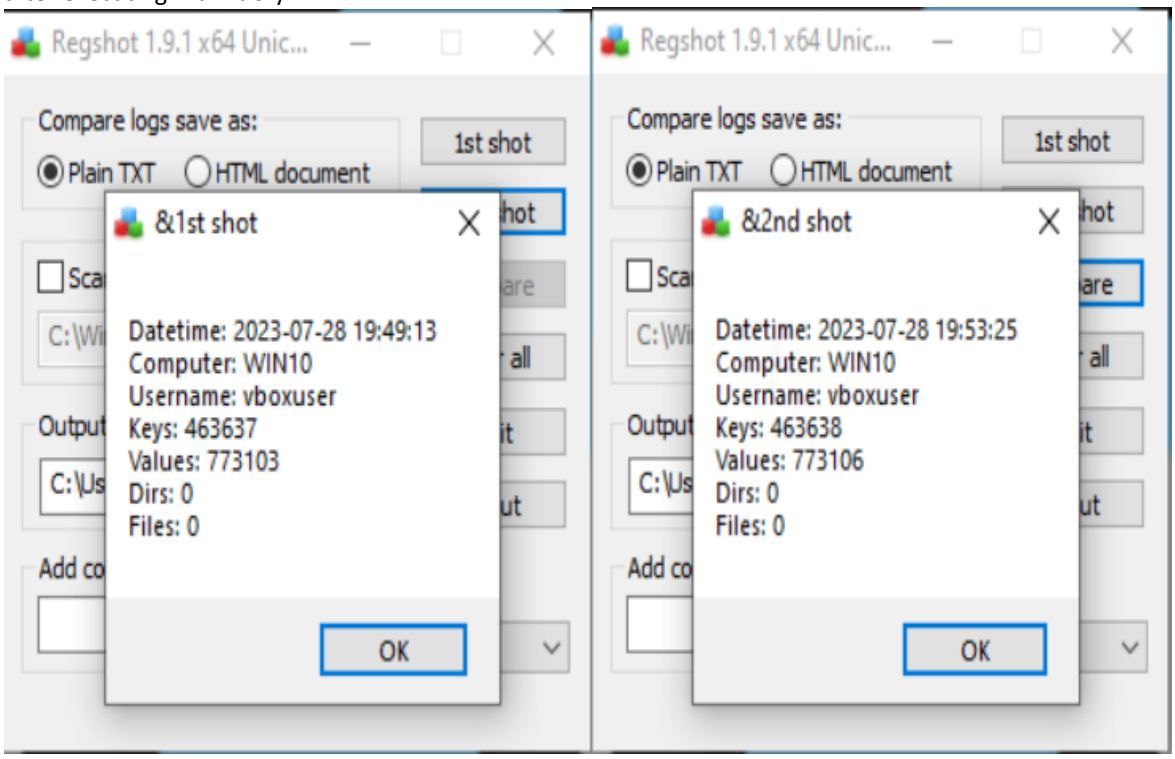


Fig. 12 Regshot

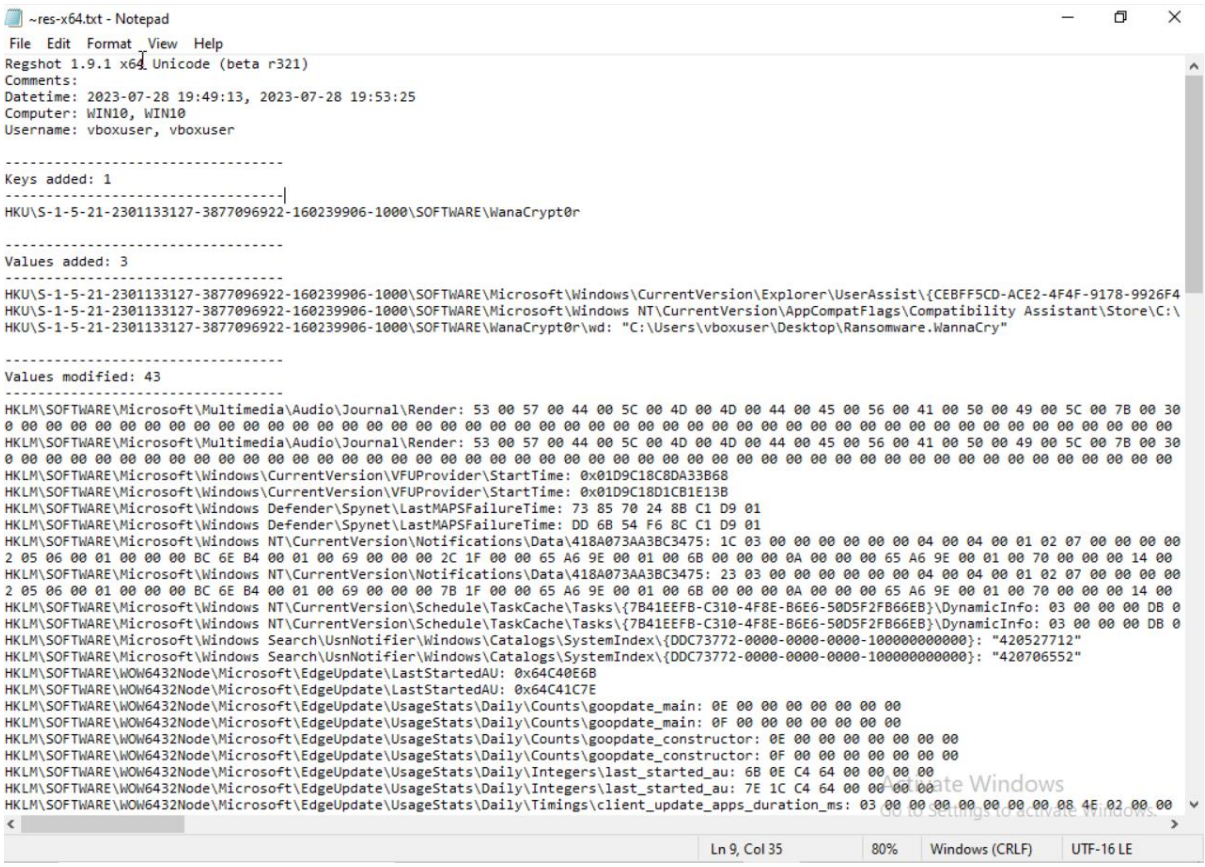


Fig. 13 Regshot

Figure 13 shows Keys added, values added and values modified with detail.

4.5 Ghidra(*Ghidra*, no date)

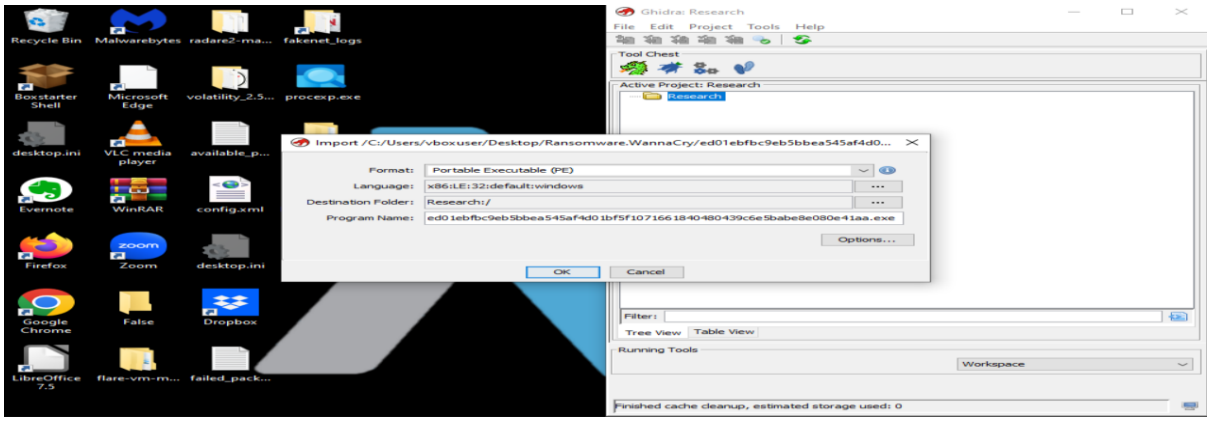


Fig. 14 Ghidra

This tool requires a user to install java jdk from (*Download the Latest Java LTS Free*, no date) Before installing it.

Fig.15Ghidra

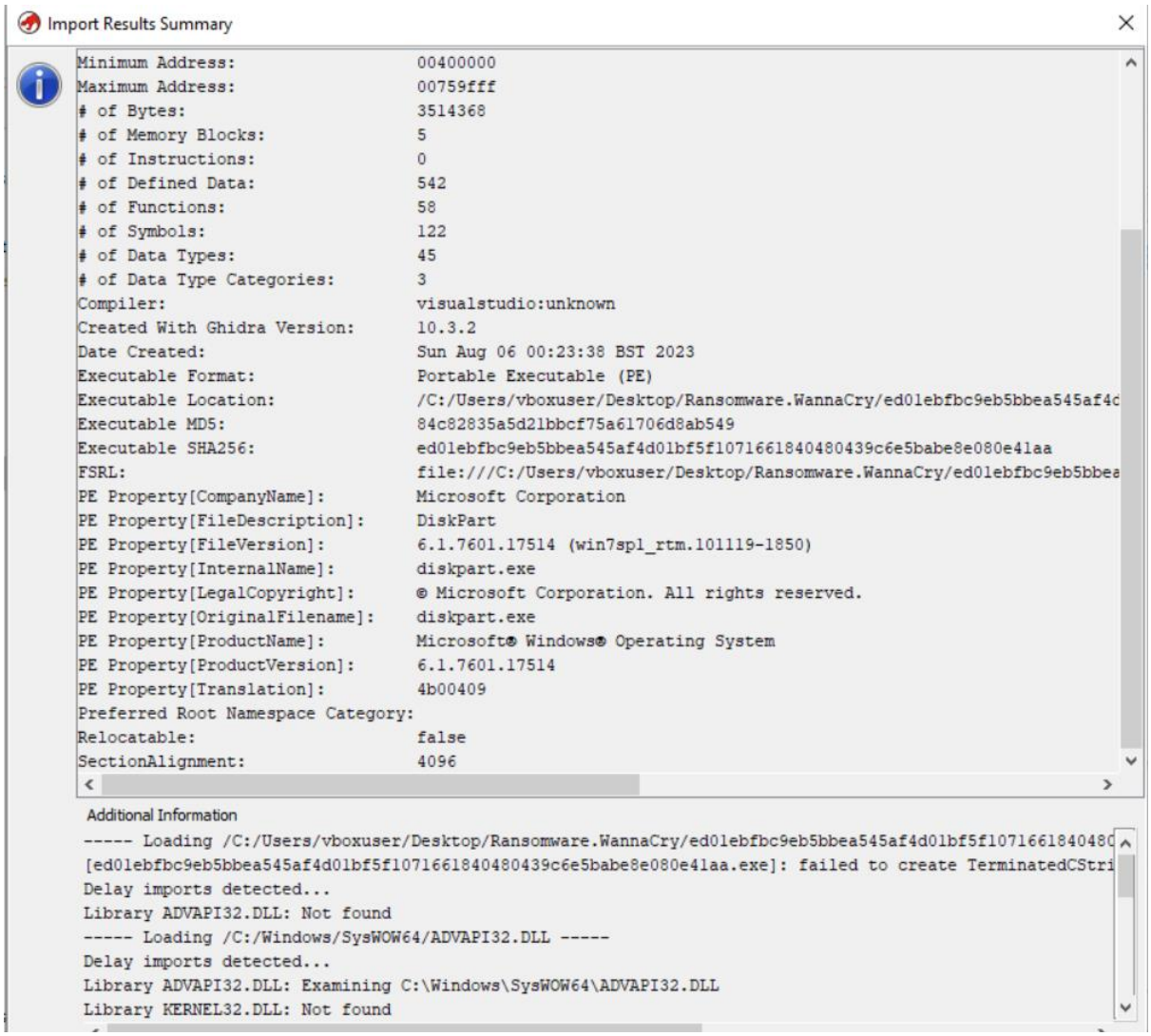


Fig. 16 Ghidra

This tool provides a detailed static analysis and then processes to provide code analysis.

References

Download the Latest Java LTS Free (no date). Available at: https://www.oracle.com/ie/java/technologies/downloads/ (Accessed: 14 August 2023).

Ghidra (no date). Available at: https://ghidra-sre.org/ (Accessed: 12 August 2023).

Nativ, Y. and Shalev, S. (no date) *theZoo - A Live Malware Repository*, *theZoo aka Malware DB*. Available at: https://thezoo.morirt.com/ (Accessed: 9 August 2023).

Ochsenmeier, M. (2023) *Winitor*. Available at: https://www.winitor.com/download (Accessed: 12 August 2023).

Russinovich, M. (2023) *Process Monitor - Sysinternals*. Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon (Accessed: 12 August 2023).

Swieskowski, P. and Kuzins, S. (no date) *Ninite - Install or Update Multiple Apps at Once*. Available at: https://ninite.com/ (Accessed: 13 August 2023).

TiANWEi (2023) 'Seabreg/Regshot'. Seabreg. Available at: https://github.com/Seabreg/Regshot (Accessed: 13 August 2023).

virus total (2023) *VirusTotal - Home*. Available at: https://www.virustotal.com/gui/home/upload (Accessed: 12 August 2023).