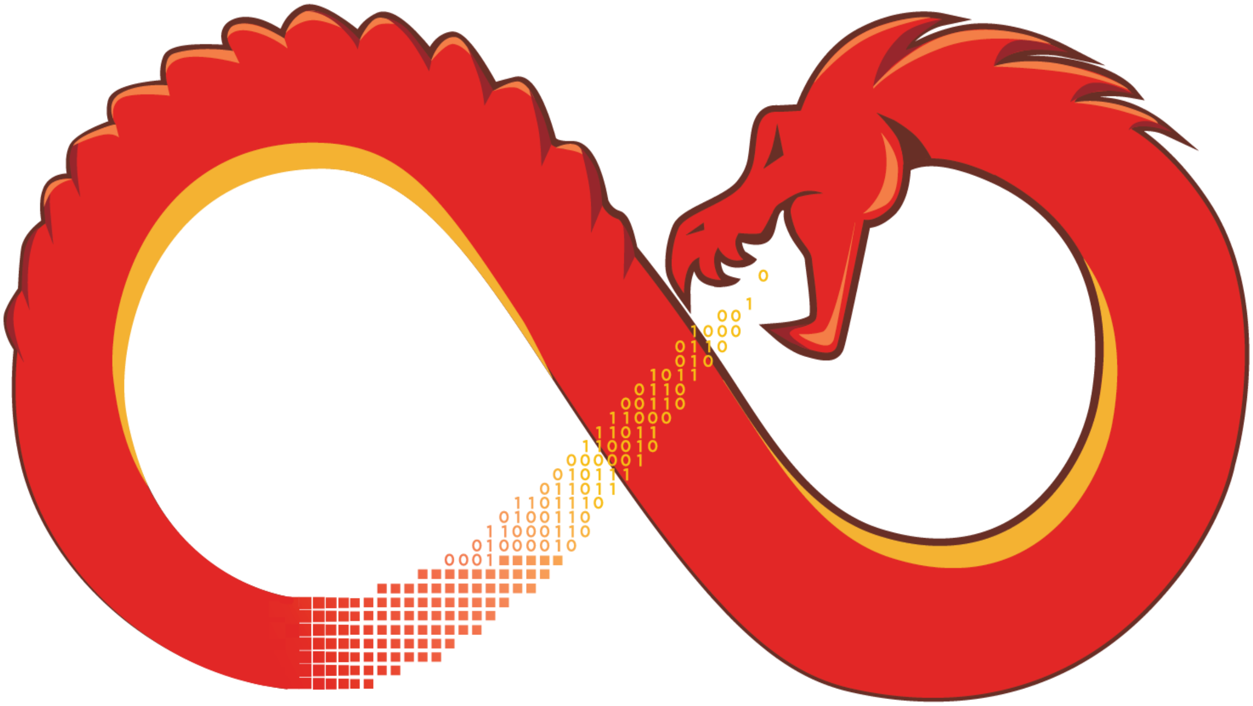


GHIDRA

NOTE This software or Reverse Engineering Framework can be obtained from the official NSA github.com repository at the following secure address:
https://github.com/NationalSecurityAgency/ghidra

GHIDRA

Ghidra Software Reverse Engineering Framework

Ghidra is a software reverse engineering (SRE) framework created and maintained by the National Security Agency Research Directorate. This framework includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows, macOS, and Linux. Capabilities include disassembly, assembly, decompilation, graphing, and scripting, along with hundreds of other features. Ghidra supports a wide variety of processor instruction sets and executable formats and can be run in both user-interactive and automated modes. Users may also develop their own Ghidra extension components and/or scripts using Java or Python.

In support of NSA's Cybersecurity mission, Ghidra was built to solve scaling and teaming problems on complex SRE efforts, and to provide a customizable and extensible SRE research platform. NSA has applied Ghidra SRE capabilities to a variety of problems that involve analyzing malicious code and generating deep insights for SRE analysts who seek a better understanding of potential vulnerabilities in networks and systems.

As we can see, Ghidra is a highly flexible and adaptable framework for cybersecurity and digital forensics experts. This walkthrough will show you precisely how to open Ghidra, create a project and decompile the MeMz Virus.

WHAT IS MeMZ?

MEMZ is a custom-made trojan for Microsoft Windows, originally created for the popular YouTuber Danooct1's Viewer-Made Malware series as a parody of a script kiddie's idea of dangerous malware. It has gained fame and notoriety due to its highly complex and unique payloads, many of which are based around internet memes. MEMZ is mainly thought of as a joke trojan.It is available as an executable .exe file and a batch version. The batch version works like a self-extracting archive, which just extracts and runs the .exe out of itself. The MEMZ trojan is a leetspeek-style misspelling of the word "Memes". This is why most parts of this trojan contain leetspeek and random web searches, Nyan Cat, and references to Materialisimo's video "MLG Antivirus". The creator of this trojan, Leurak, makes a few Joke Programs, like the Illuminati Joke Program, and the Earthquake joke program. This trojan has gotten recognition ever since Danooct1 uploaded his review, for which it was originally made. Joel from Vinesauce used it in his "Windows 10 Destruction" stream, where he showcases MEMZ near the ending of the first livestream. He also thanks Danooct1 for helping with acquiring the trojan.

Contrary to popular belief, MEMZ isn't especially destructive, nor will it render computers inoperable forever. Users with basic knowledge on how to use the PC's recovery mode can easily return their computer to normal in a few minutes at most. The source code of MEMZ used to be found on Leurak's GitHub, but sometime after January 14th, 2020, the Github repository was removed. The README.md file lists the dependencies, but the build procedure is – most likely intentionally – not described outright. It is currently unknown if MEMZ or other variants of this trojan has entered the wild; Microsoft's own help desk has several questions related to MEMZ from confused (or inexperienced users) who ran the trojan without reading the warnings first, but as of 2018 there is no evidence that the trojan has been propagated through any traditional method. To prevent malicious users from deliberately spreading the trojan, currently, only versions 4 (which has the disclaimer and non-destructive version bundled with the destructive version) and up are available to download.

Step 1: The first step in this process is to simply run the Ghidra executable file that you downloaded from the official GitHub repository. Upon running the program, you should receive a window like the below screenshot:

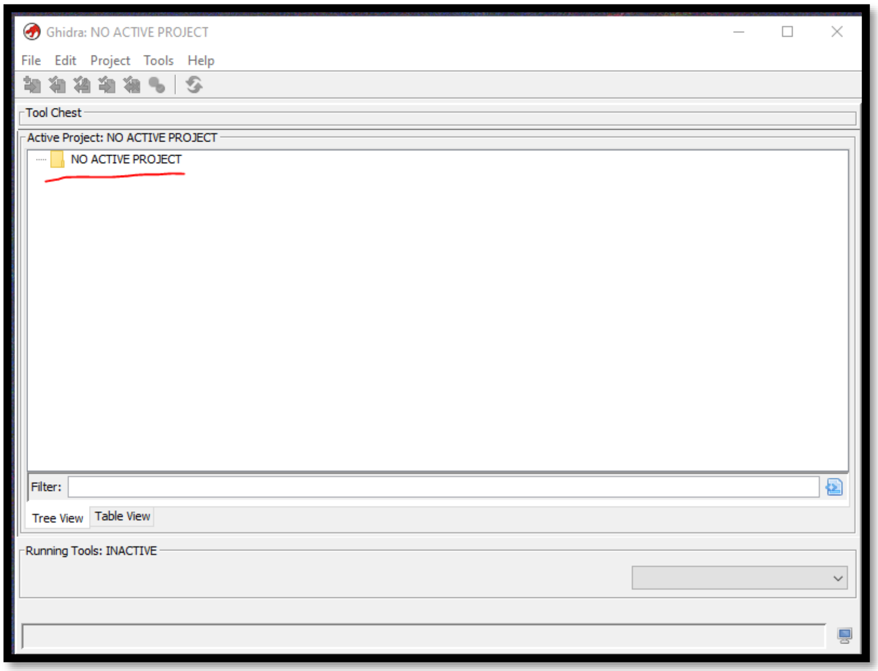
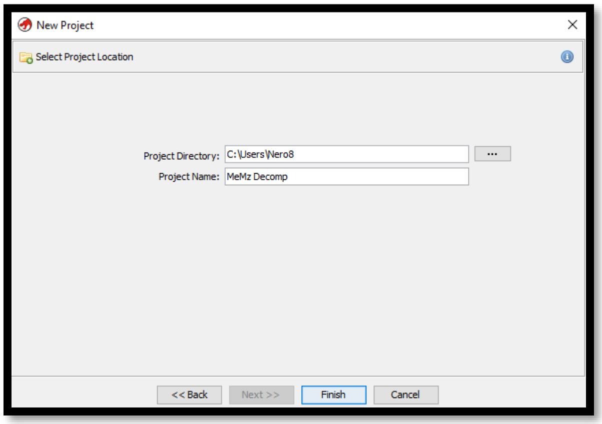


Figure 1.0: You can see in this screenshot, that there are no current active projects associated with this current session. We will change that in step 2.

STEP 2:

- Click File dropdown
- Select "New Project"
- Ensure "Non-Shared Project" is selected and click Next
- Identify your Project Directory (This is not as intricate as it looks, just identify a directory)
- Create a Name for your project (Mine is identified as MeMz Decomp)



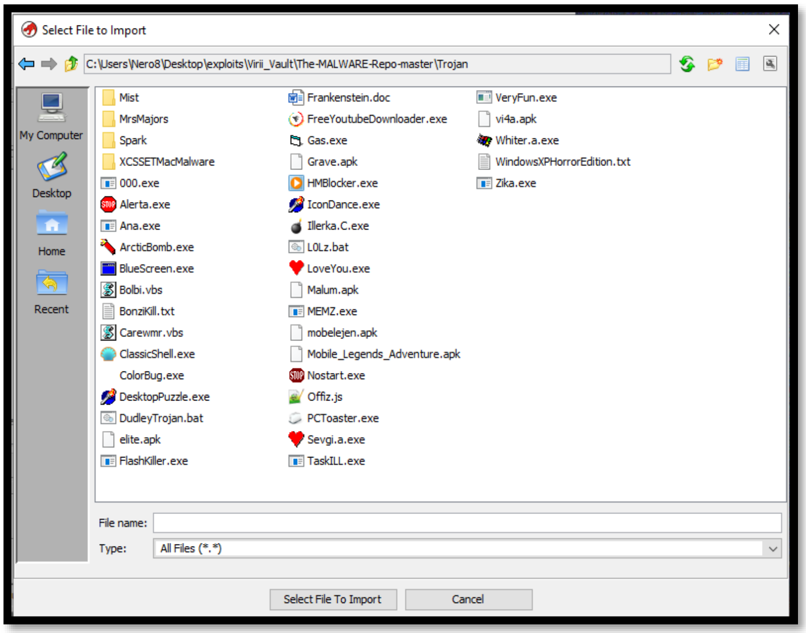
Project Directory: C:\Users\Nero8
Project Name: MeMz Decomp

- At this point, go ahead and click Finish

- Now we have created our project (Great, but not done yet)

STEP 3: In this step, we will focus on importing our file in question. For this example, I am using an active version of the MeMz virus.

- Click File dropdown
- Select “Import File”
- Utilize the built-in file explorer to identify the file you will be conducting forensics on



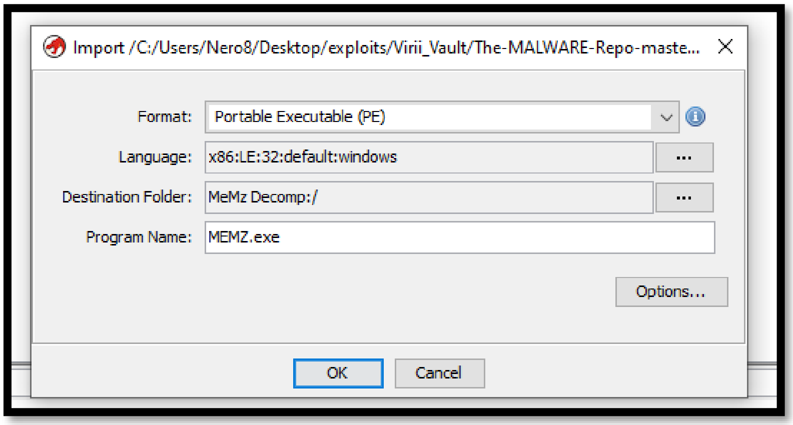
Select File to Import

C:\Users\Nero8\Desktop\exploits\Virii_Vault\The-MALWARE-Repo-master\Trojan

File name:

Type: All Files (*.*)

- Once you have identified you file, go ahead and click select.
- The next box to pop up will be the identification of the file: See Below:



Import /C:/Users/Nero8/Desktop/exploits/Virii_Vault/The-MALWARE-Repo-maste...

Format: Portable Executable (PE)

Language: x86:LE:32:default:windows

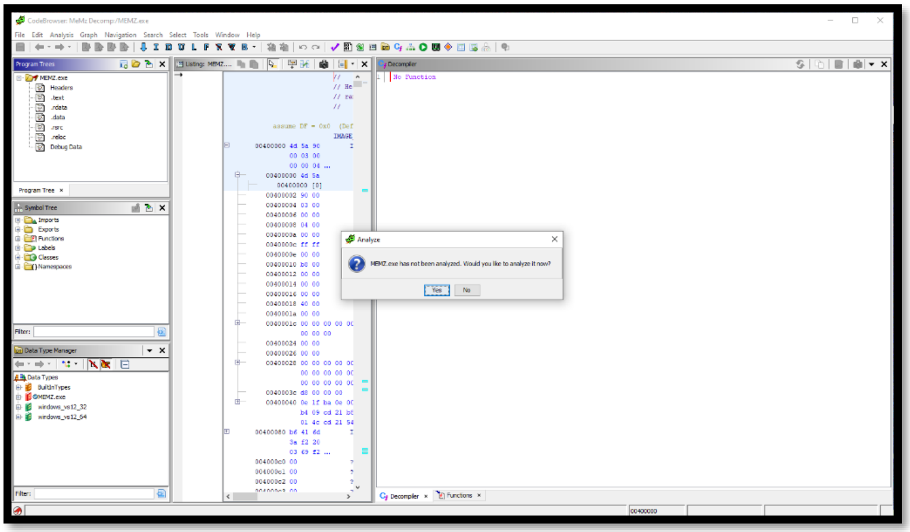
Destination Folder: MeMz Decomp:/

Program Name: MEMZ.exe

- Here the program itself is attempting to identify the type and architecture of the given file.
- Once you have done this (Most often Ghidra will be successful in identification) select OK.
- After import of the file is complete, you will receive an Import Results Summary. Select OK

STEP 4: In this, the final step of the import and decompilation process, we will simply open the file and request a full deconstruction of the file.

- Double Click the file in your project



CodeBrowser: MeMz Decomp:/MEMZ.exe

Analyze

MEMZ.exe has not been analyzed. Would you like to analyze it now?

Yes No

-
- Go ahead and click YES to run a full analysis of the file
- Once you do this, Ghidra will begin the De-Compilation process and the result will be a somewhat open book for you to scan through.

WHERE CAN YOU START?

1. Look through the Functions
2. Scan for clear text data
3. If you see and C# data, give it a google and see what it's doing

This is all for now. Once we get a clear understanding of the platform itself, we will move into more intense operations within Ghidra for Reverse Engineering and Digital Forensics. Please let me know if you have questions on this platform with respect to this short walkthrough and I will do my best to assist.