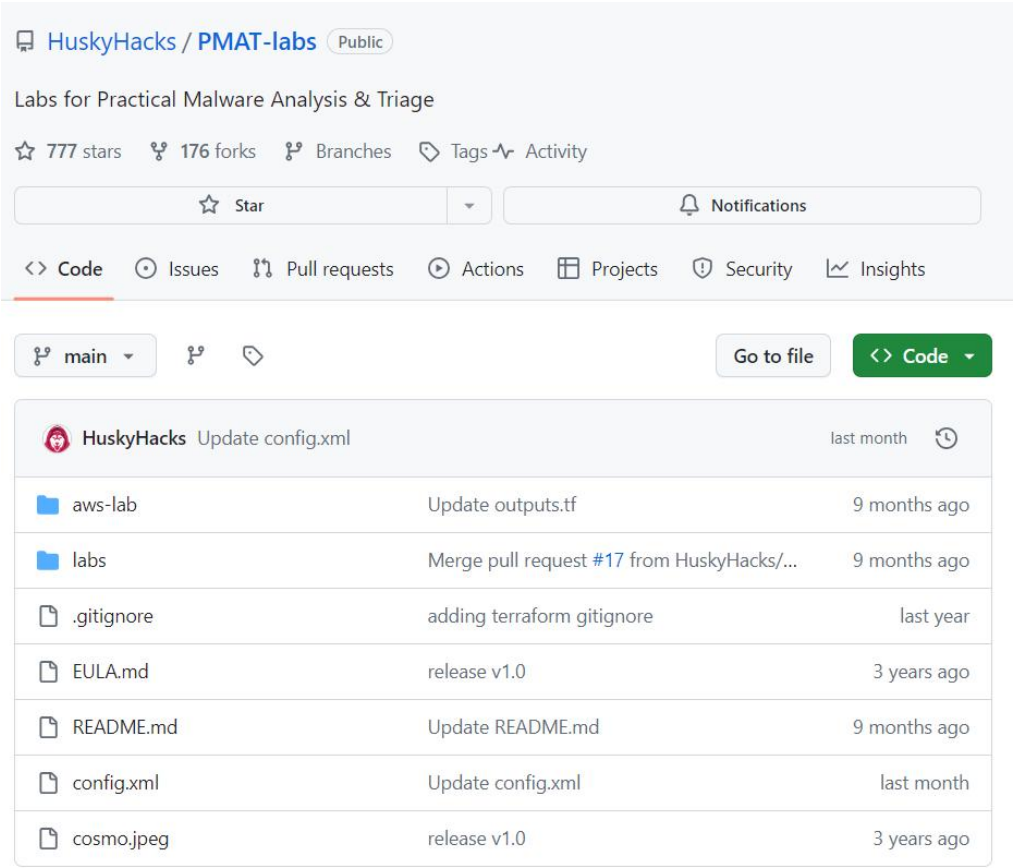
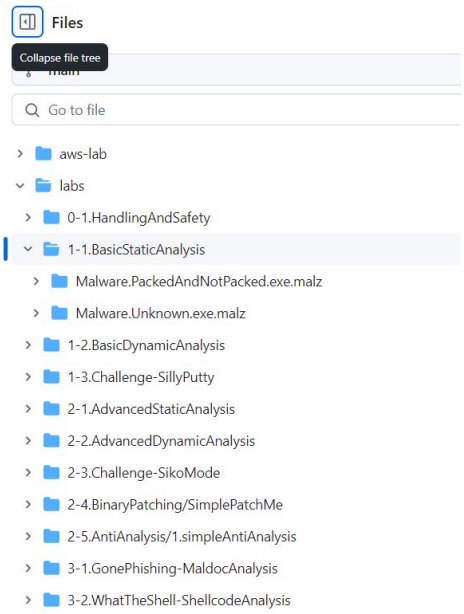
Performing Reverse Engineering by Downloading Sample Malware and RE through Ghidra

Download Malware Sample

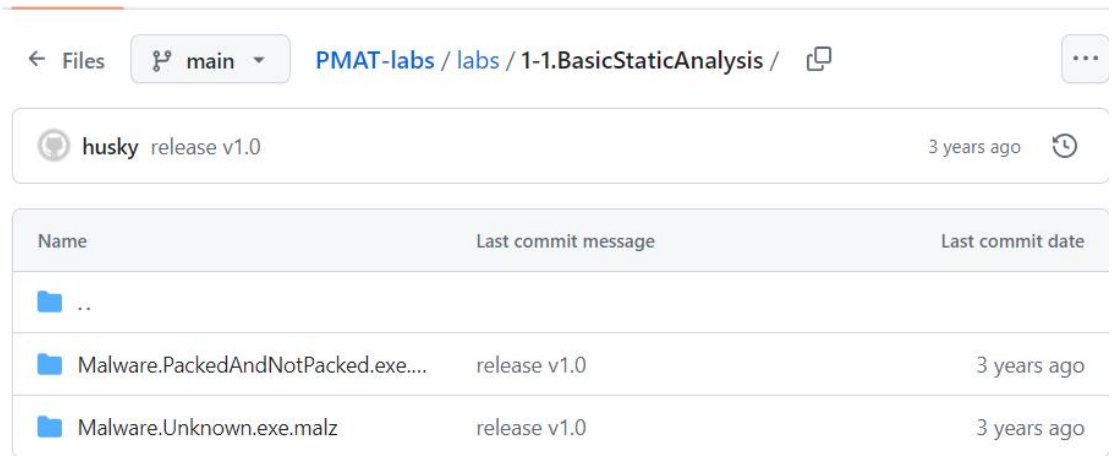
Step 1: we will download the malware sample from Git-hub

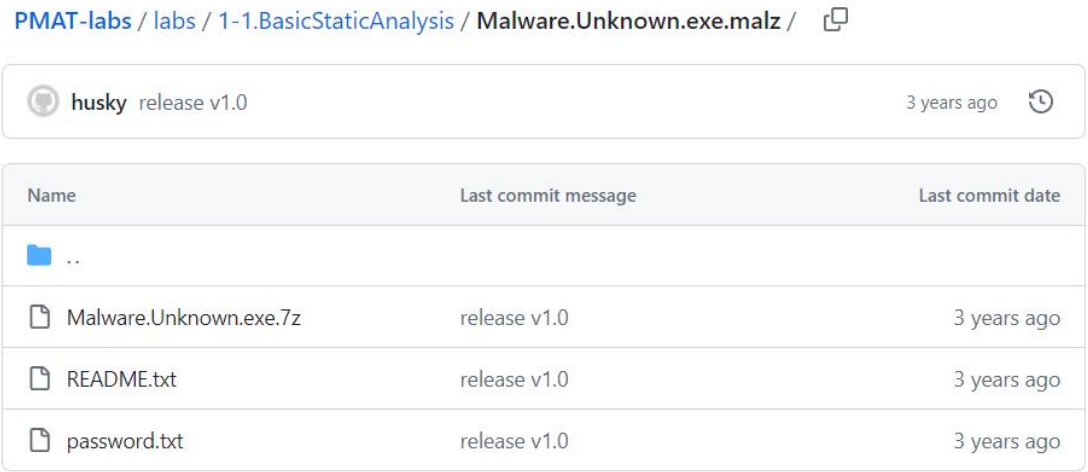


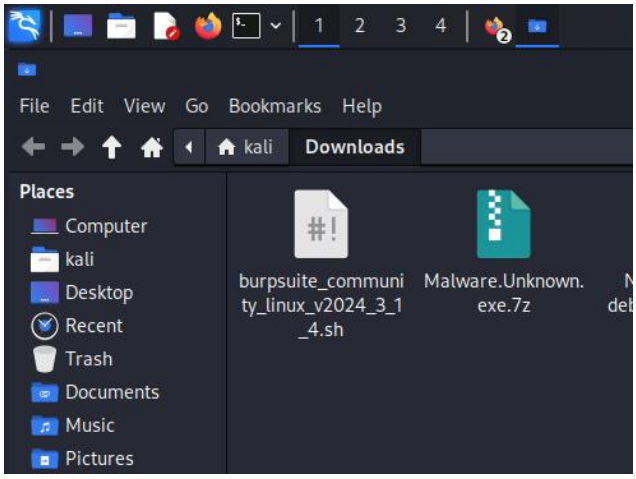
Step 2: After that go to the labs tab and open 1-1 BasicStaticAnalysis



Step 3: Click on the Malware.Unknown.exe.malz and download it







Step 4: Now after downloading the sample malware extract the file using the password " infected"

Here is the extracted file

Virus Total

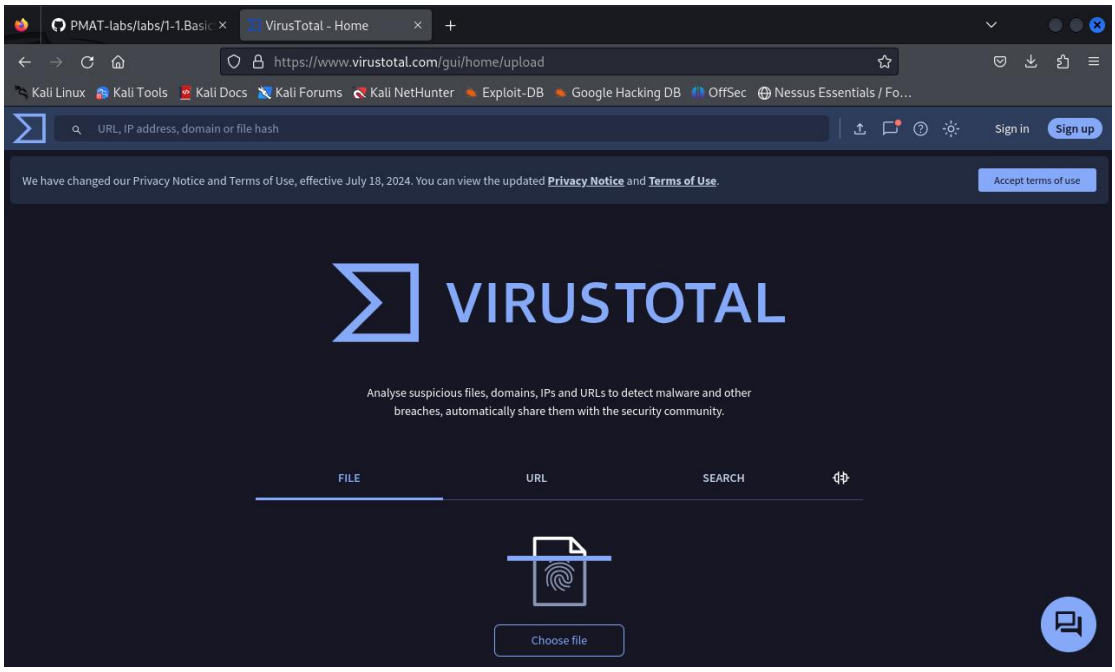
Step 1: What is Virus Total?

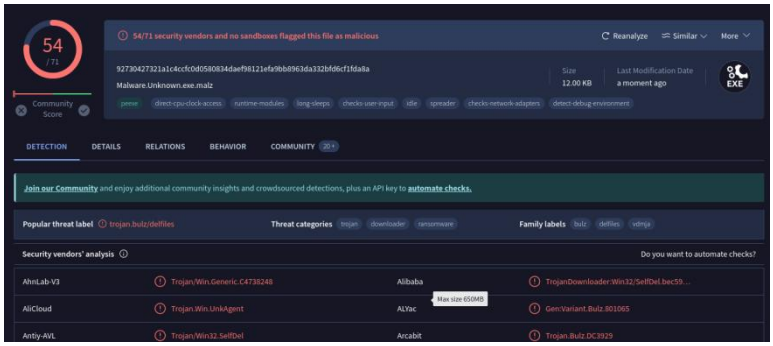
Virus Total is an online service that examines suspicious files and URLs to identify various types of malware and malicious content using multiple antivirus engines and website scanners. It also offers an API that enables users to access the data generated by VirusTotal.

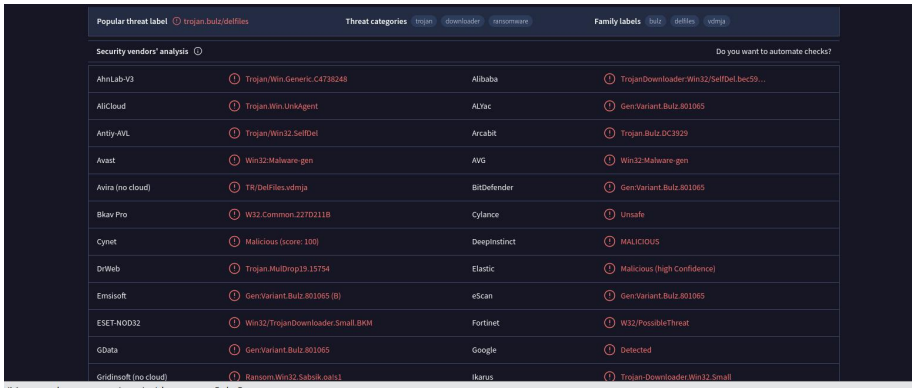
Step 2: Use the md5sum command to find the hash

```
┌──(kali㉿192)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿192)-[~]
└─$ cd Downloads

┌──(kali㉿192)-[~/Downloads]
└─$ ls
Malware.Unknown.exe.7z            ZAP_2_15_0_unix.sh
Malware.Unknown.exe.malz          burpsuite_community_linux_v2024_3_1_4.sh
Nessus-10.7.3-debian10_amd64.deb  zenmap-7.95-1.noarch.rpm

┌──(kali㉿192)-[~/Downloads]
└─$ md5sum Malware.Unknown.exe.7z
ffcb385056fdac305c8e7d7568d01aae  Malware.Unknown.exe.7z

┌──(kali㉿192)-[~/Downloads]
└─$
```

Step 3: Open the Virus Total



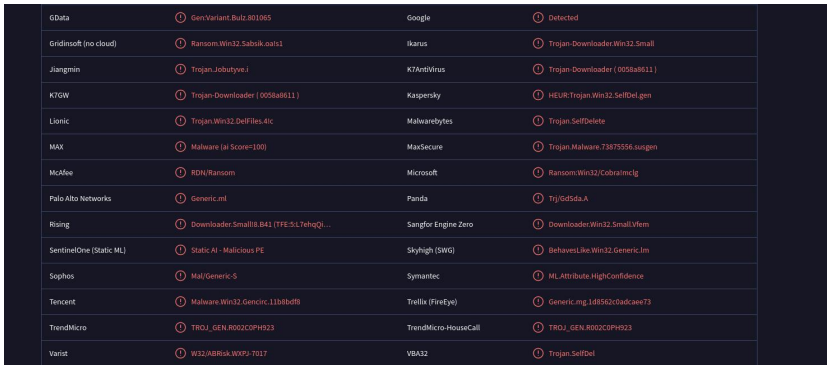




Popular threat label: trojan.bulz/delfiles
Threat categories: trojan, downloader, ransomware
Family labels: bulz, delfiles, vdmja

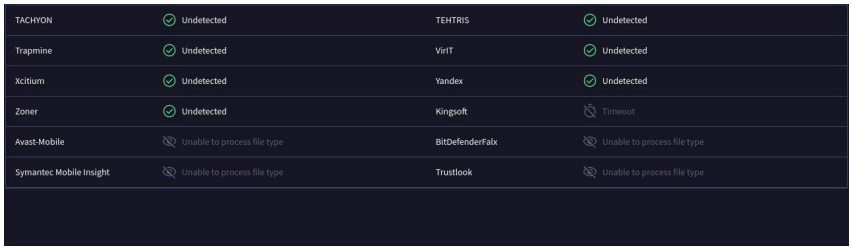
Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Trojan/Win.Generic.C4738248	Alibaba	TrojanDownloader:Win32/SelfDel.bec59...
AliCloud	Trojan.Win.UnkAgent	ALYac	Gen:Variant.Bulz.801065
Antiy-AVL	Trojan/Win32.SelfDel	Arcabit	Trojan.Bulz.DC3929
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/DelFiles.vdmja	BitDefender	Gen:Variant.Bulz.801065
Bkav Pro	W32.Common.227D211B	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.MulDrop19.15754	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Bulz.801065 (B)	eScan	Gen:Variant.Bulz.801065
ESET-NOD32	Win32/TrojanDownloader.Small.BKM	Fortinet	W32/PossibleThreat
GData	Gen:Variant.Bulz.801065	Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Sabsik.oa!s1	Ikarus	Trojan-Downloader.Win32.Small



GData	Gen:Variant.Bulz.801065	Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Sabsik.oa!s1	Ikarus	Trojan-Downloader.Win32.Small
Jiangmin	Trojan.Jobutyve.i	K7AntiVirus	Trojan-Downloader (0058a8611)
K7GW	Trojan-Downloader (0058a8611)	Kaspersky	HEUR:Trojan.Win32.SelfDel.gen
Lionic	Trojan.Win32.DelFiles.4!c	Malwarebytes	Trojan.SelfDelete
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.73875556.susgen
McAfee	RDN/Ransom	Microsoft	Ransom:Win32/CobraImcIg
Palo Alto Networks	Generic.ml	Panda	Trj/GdSda.A
Rising	Downloader.Small!8.B41 (TFE:5:L7ehqQi...	Sangfor Engine Zero	Downloader.Win32.Small.Vfem
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	BehavesLike.Win32.Generic.lm
Sophos	Mal/Generic-S	Symantec	ML.Attribute.HighConfidence
Tencent	Malware.Win32.Gencirc.11b8bdf8	Trellix (FireEye)	Generic.mg.1d8562c0adcaee73
TrendMicro	TROJ_GEN.R002C0PH923	TrendMicro-HouseCall	TROJ_GEN.R002C0PH923
Varist	W32/ABRisk.WXPJ-7017	VBA32	Trojan.SelfDel

Lionic	Trojan.Win32.DelFiles.4!c	Malwarebytes	Trojan.SelfDelete
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.73875556.susgen
McAfee	RDN/Ransom	Microsoft	Ransom:Win32/CobraImcIg
Palo Alto Networks	Generic.ml	Panda	Trj/GdSda.A
Rising	Downloader.Small!8.B41 (TFE:5:L7ehqQi...	Sangfor Engine Zero	Downloader.Win32.Small.Vfem
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	BehavesLike.Win32.Generic.lm
Sophos	Mal/Generic-S	Symantec	ML.Attribute.HighConfidence
Tencent	Malware.Win32.Gencirc.11b8bdf8	Trellix (FireEye)	Generic.mg.1d8562c0adcaee73
TrendMicro	TROJ_GEN.R002C0PH923	TrendMicro-HouseCall	TROJ_GEN.R002C0PH923
Varist	W32/ABRisk.WXPJ-7017	VBA32	Trojan.SelfDel
VIPRE	Gen:Variant.Bulz.801065	ViRobot	Trojan.Win32.Z.Agent.12288.EBS
Webroot	W32.Trojan.TR.DelFiles.vdmja	WithSecure	Trojan.TR/DelFiles.vdmja
Zillya	Downloader.Small.Win32.140841	ZoneAlarm by Check Point	HEUR:Trojan.Win32.SelfDel.gen



TACHYON	Undetected	TEHTRIS	Undetected
Trapmine	Undetected	VirIT	Undetected
Xcitium	Undetected	Yandex	Undetected
Zoner	Undetected	Kingsoft	Timeout
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

String/Floss

Strings/Floss is a command line tool that extracts strings from a file. Find and explore all the strings in the malware sample.

Step 1: Use the command

Strings “and write the file name”

```
┌──(kali㉿192)-[~/Downloads]
└─$ strings Malware.Unknown.exe.7z
g1Y{
(DAM
BmR!
h@&2
Z,%%_
D←C1
E!Wgs
+GmW
Ix<t
y$_A
Et>p
Gk65=
1IrJ
T] Go+2
W,htE
?JA^
&Kt&
l><7L
mm&U [s7{
"&<f
9~OH
!$G{
0|NE
Q/-u
9E[GPG
sec#3
MG_6
Mo[('H`
BTNd
Q<`ah
bhF#j
sDrl
"#\ay
-EA5b
c@A
H:'_x
<p],
6Ka5
bpA
x(V2u
```

Readpe

This is a powerful command that is used for

- Listing the headers in the PE file
- Listing the sections in the PE file
- Listing the imported and exported functions

View all the headers, sections, imported and exported functions.

Step 2: Use command readpe and “ write file name”

```
┌──(kali㉿192)-[~/Downloads]
└─$ readpe Malware.Unknown.exe.7z
Command 'readpe' not found, but can be installed with:
sudo apt install readpe
Do you want to install it? (N/y)y
sudo apt install readpe
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libpe1
The following NEW packages will be installed:
  libpe1 readpe
0 upgraded, 2 newly installed, 0 to remove and 417 not upgraded.
Need to get 182 kB of archives.
After this operation, 1412 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libpe1 amd64 0.82-3 [33.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 readpe amd64 0.82-3 [149 kB]
Fetched 182 kB in 2s (103 kB/s)
Selecting previously unselected package libpe1.
(Reading database ... 200017 files and directories currently installed.)
Preparing to unpack .../libpe1_0.82-3_amd64.deb ...
Unpacking libpe1 (0.82-3) ...
Selecting previously unselected package readpe.
Preparing to unpack .../readpe_0.82-3_amd64.deb ...
Unpacking readpe (0.82-3) ...
Setting up libpe1 (0.82-3) ...
Setting up readpe (0.82-3) ...
Processing triggers for libc-bin (2.37-12) ...
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...

┌──(kali㉿192)-[~/Downloads]
└─$ readpe Malware.Unknown.exe.7z
```

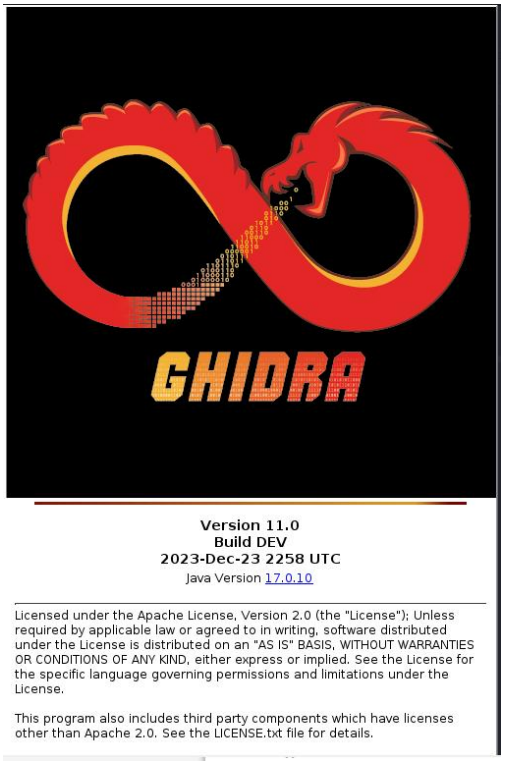
Step 3: When we run the command readpe it will show the following interface

```
└─$ readpe Malware.Unknown.exe.malz
DOS Header
    Magic number:                   0x5a4d (MZ)
    Bytes in last page:             144
    Pages in file:                  3
    Relocations:                    0
    Size of header in paragraphs:   4
    Minimum extra paragraphs:       0
    Maximum extra paragraphs:       65535
    Initial (relative) SS value:    0
    Initial SP value:               0xb8
    Initial IP value:               0
    Initial (relative) CS value:    0
    Address of relocation table:    0x40
    Overlay number:                 0
    OEM identifier:                 0
    OEM information:                0
    PE header offset:               0xf8
COFF/File header
    Machine:                        0x14c IMAGE_FILE_MACHINE_I386
    Number of sections:             5
    Date/time stamp:                1630779072 (Sat, 04 Sep 2021 18:11:12 UTC)
    Symbol Table offset:            0
    Number of symbols:              0
    Size of optional header:        0xe0
    Characteristics:                0x102
    Characteristics names
        IMAGE_FILE_EXECUTABLE_IMAGE
        IMAGE_FILE_32BIT_MACHINE

Optional/Image header
    Magic number:                   0x10b (PE32)
    Linker major version:           14
    Linker minor version:           28
    Size of .text section:          0x1600
    Size of .data section:          0x1800
    Size of .bss section:           0
    Entrypoint:                     0x15f1
    Address of .text section:       0x1000
    Address of .data section:       0x3000
    ImageBase:                      0x400000
    Alignment of sections:          0x1000
    Alignment factor:               0x200
    Major version of required OS:   6
    Minor version of required OS:   0
```

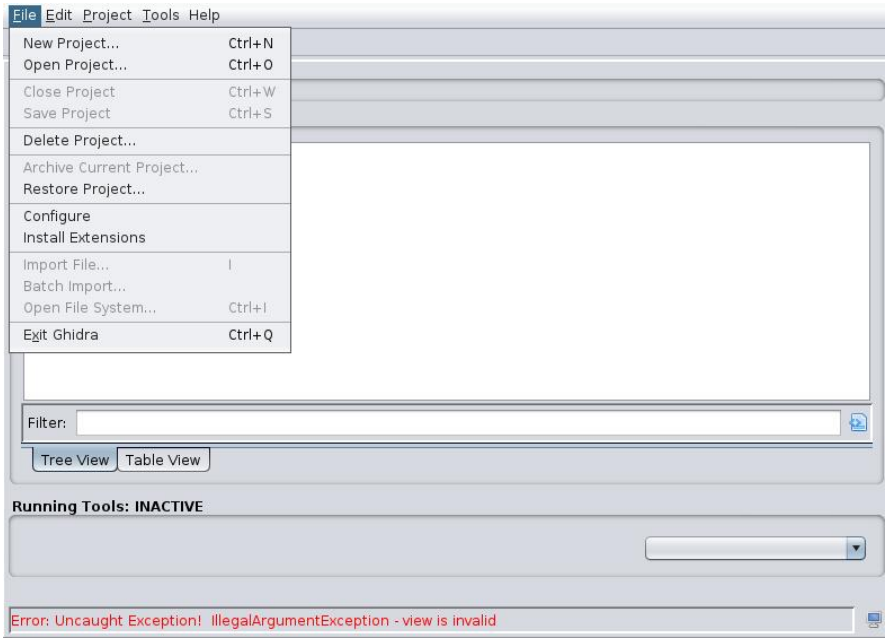
Ghidra

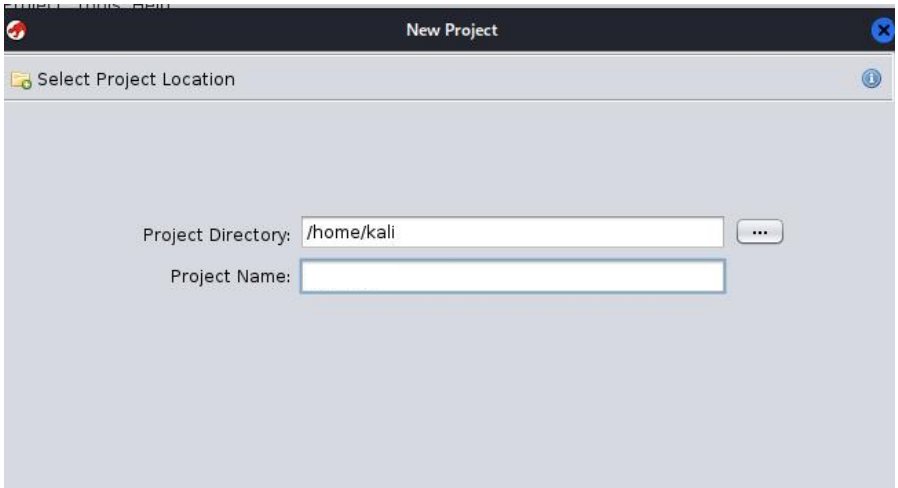
Ghidra is a reverse engineering tool developed by the NSA and released in 2019. It has become particularly popular among malware analysts due to its functionality as a disassembly tool. Ghidra converts low-level machine code into high-level code, making it an invaluable resource for analyzing malware.

Step 1: As Ghidra is already installed we will run it using ghidra command

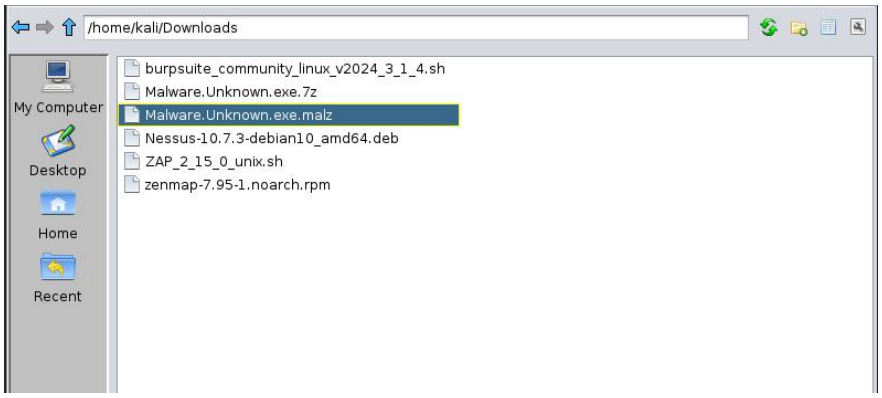


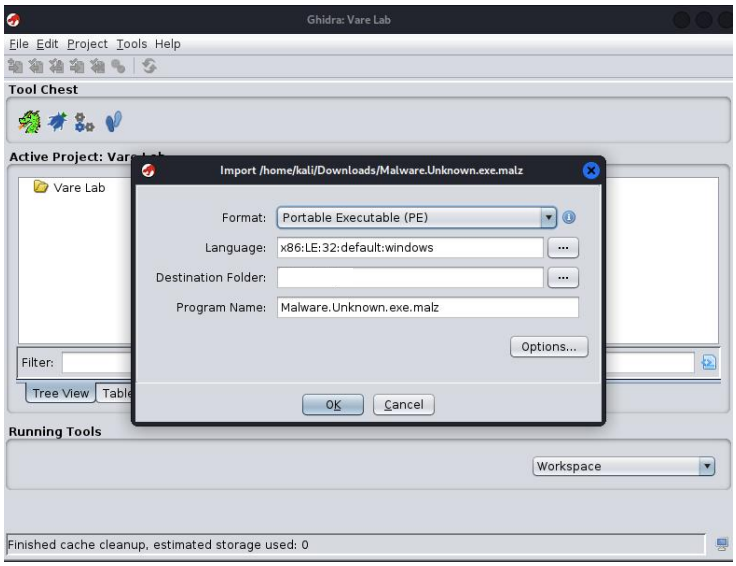
Step 2: we will make a new project in ghidra and name the project and click on finish



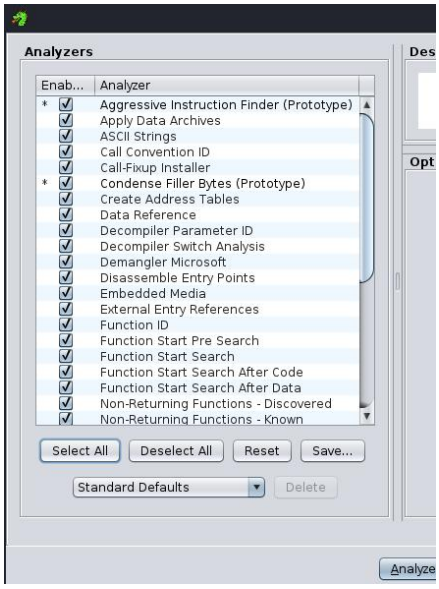


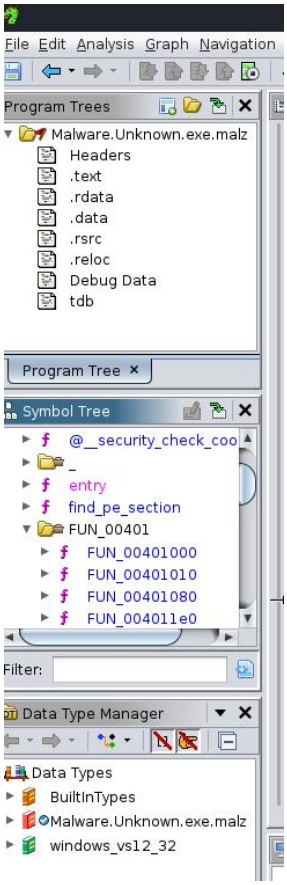
Step 3: click on the import and import the malware sample extracted file





Step 4: Click on the vare Lab file and select the extracted file and select and we will click on analyze





Explore the function tab 1 by 1