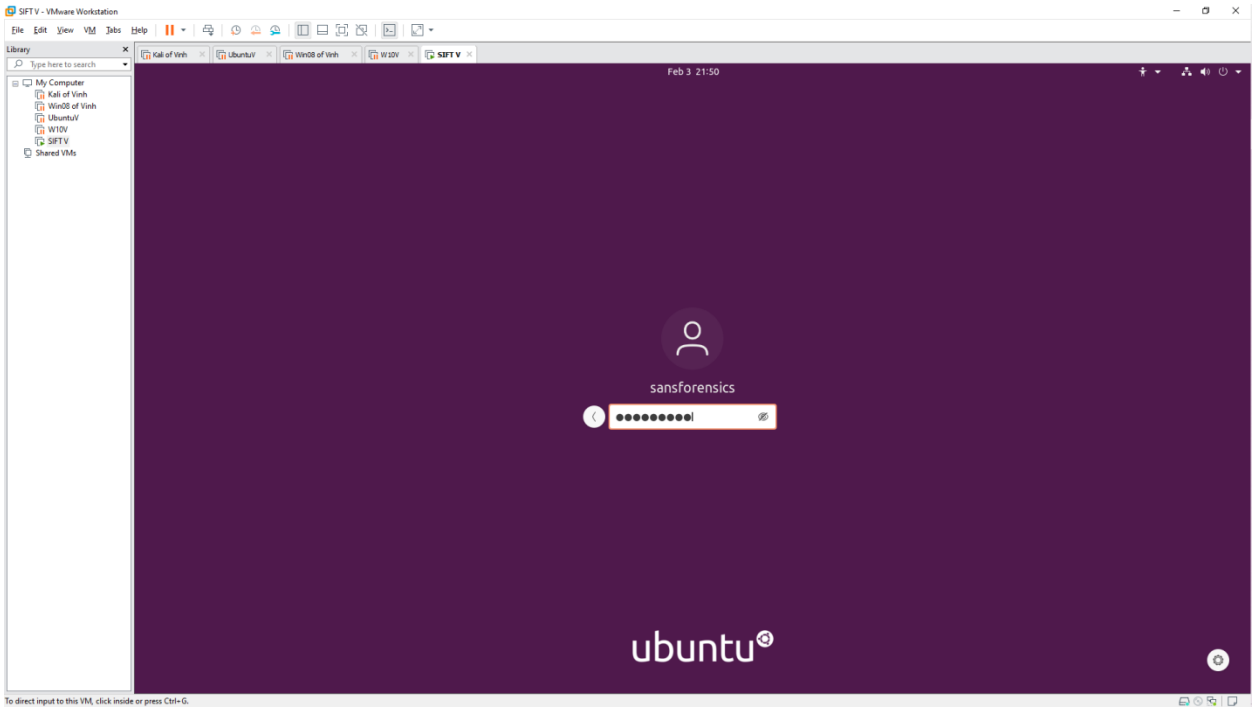
LAB 1: Public AV Scanner and Sandbox

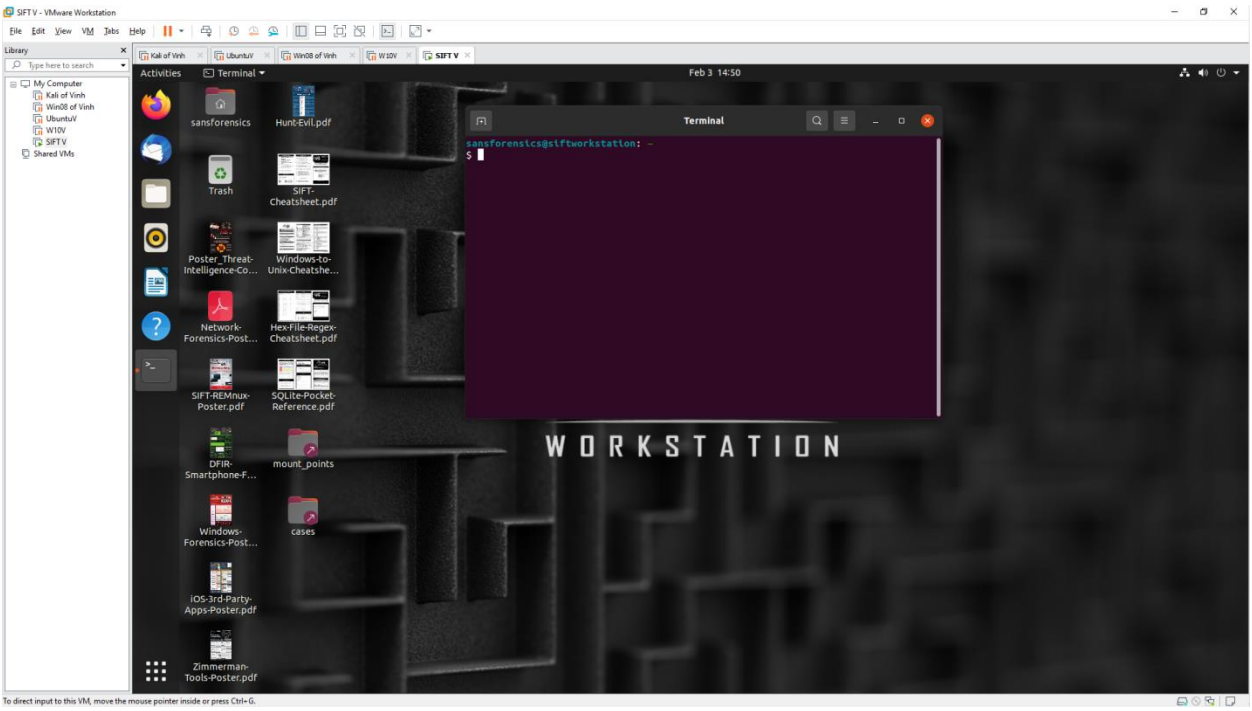
Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 4/2/2023

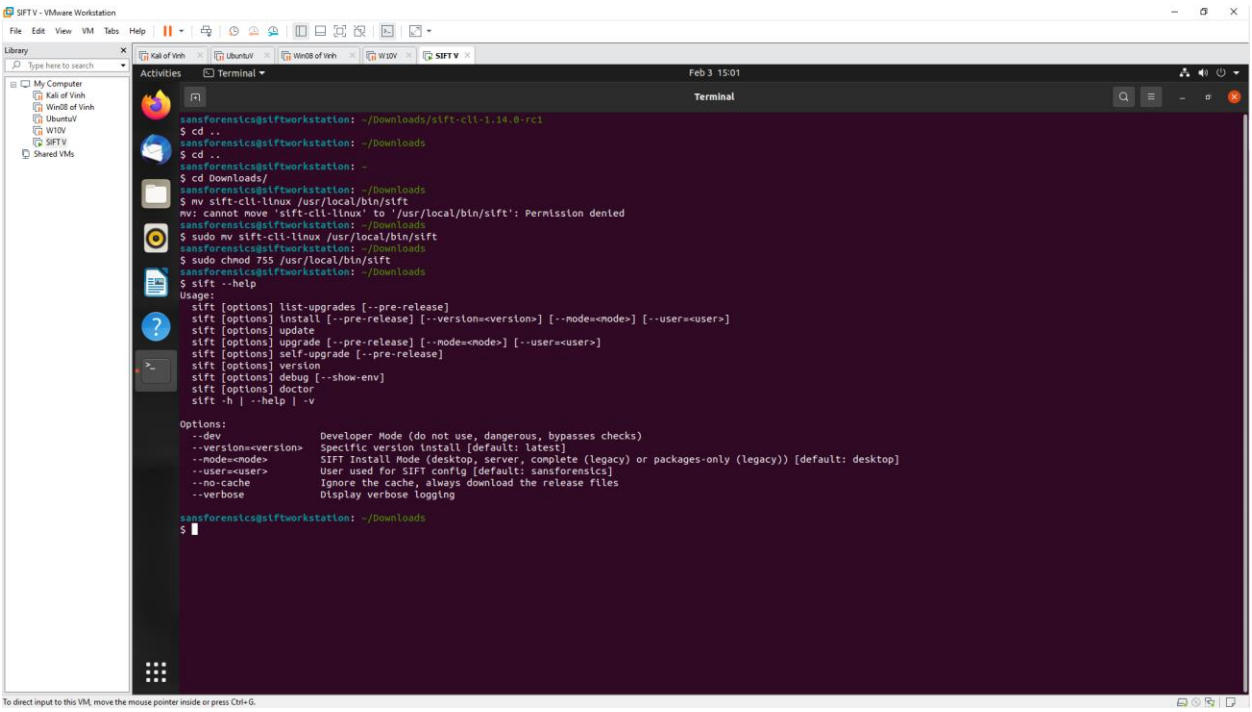
Purpose

Setup Sandbox, install SIFT Workstation, use tools to scan malware

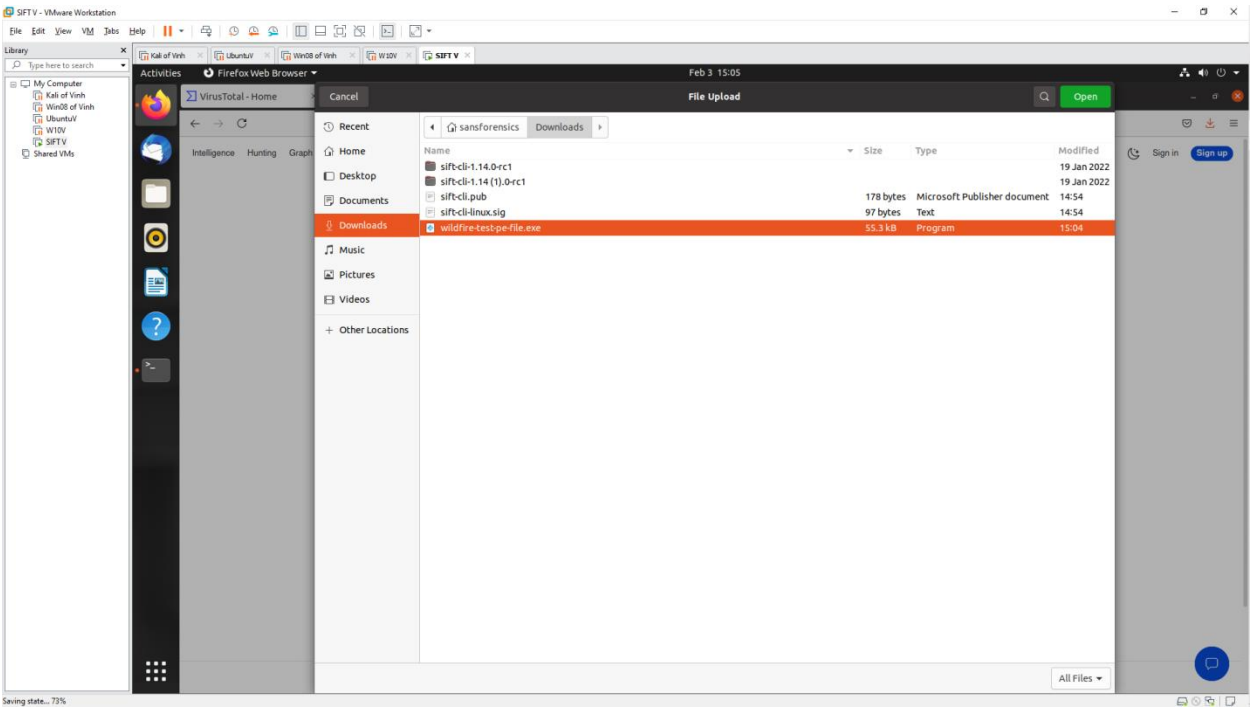
Install SIFT



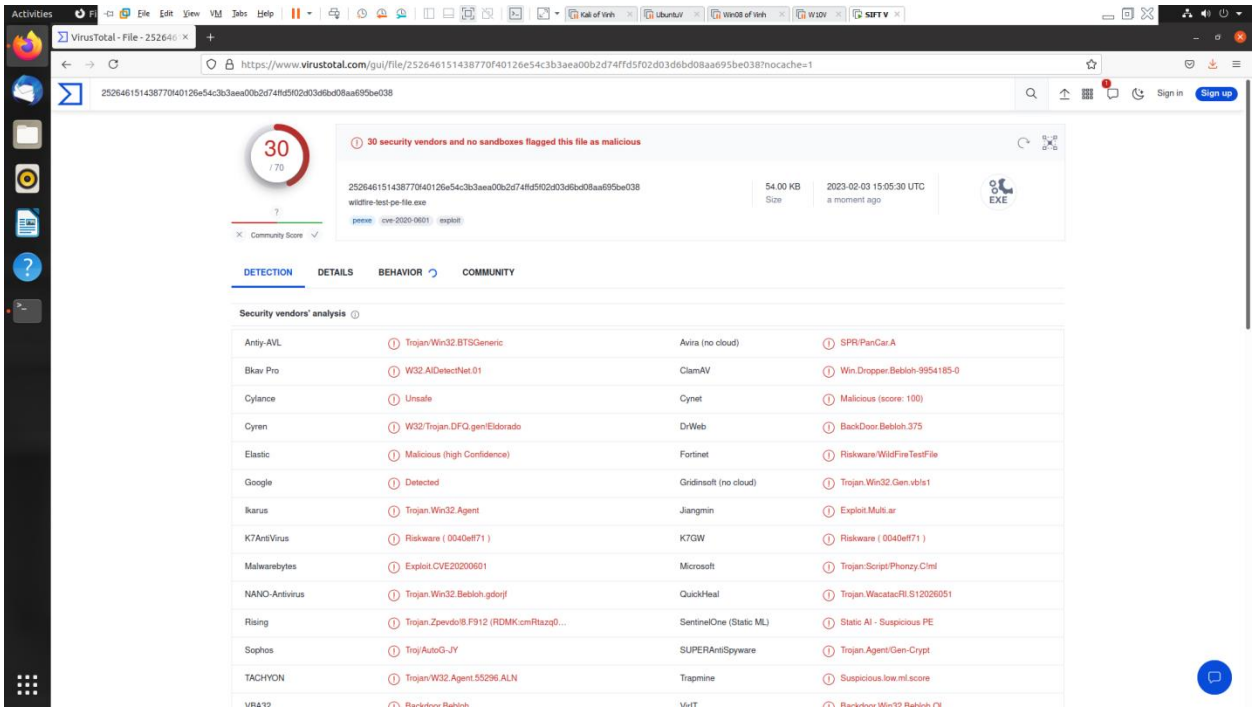


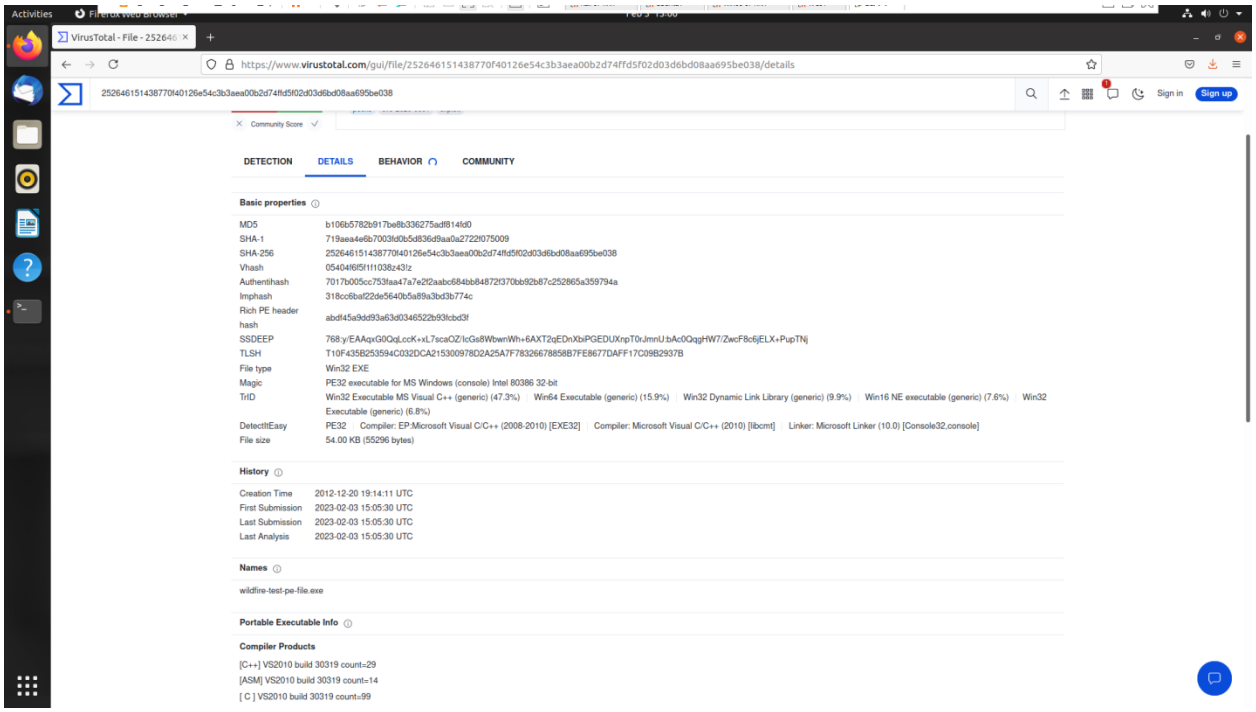


Download a sample malware

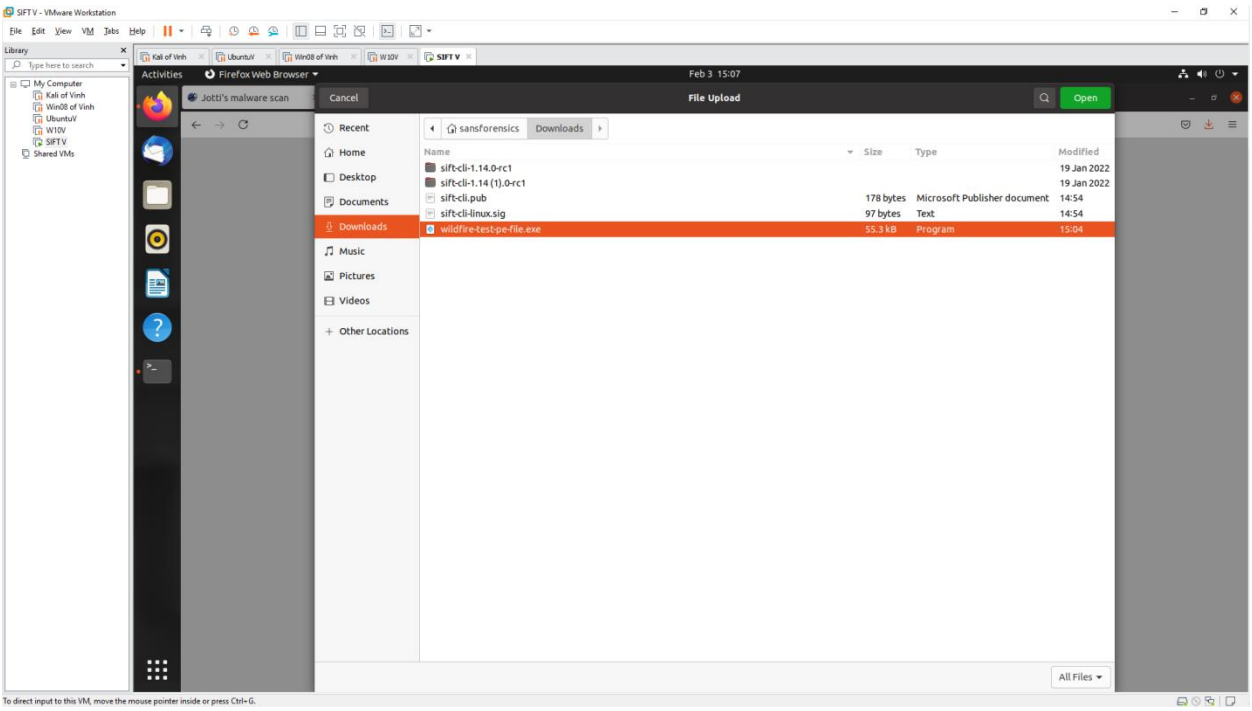


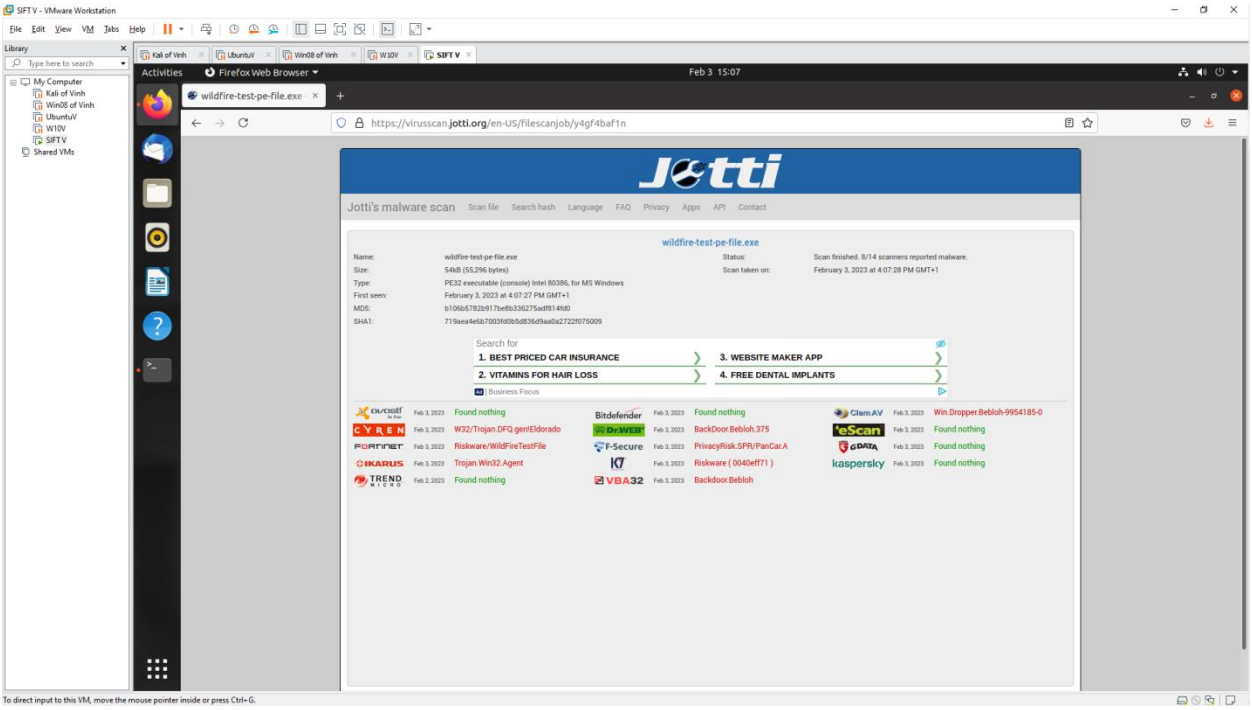
Upload to virustotal



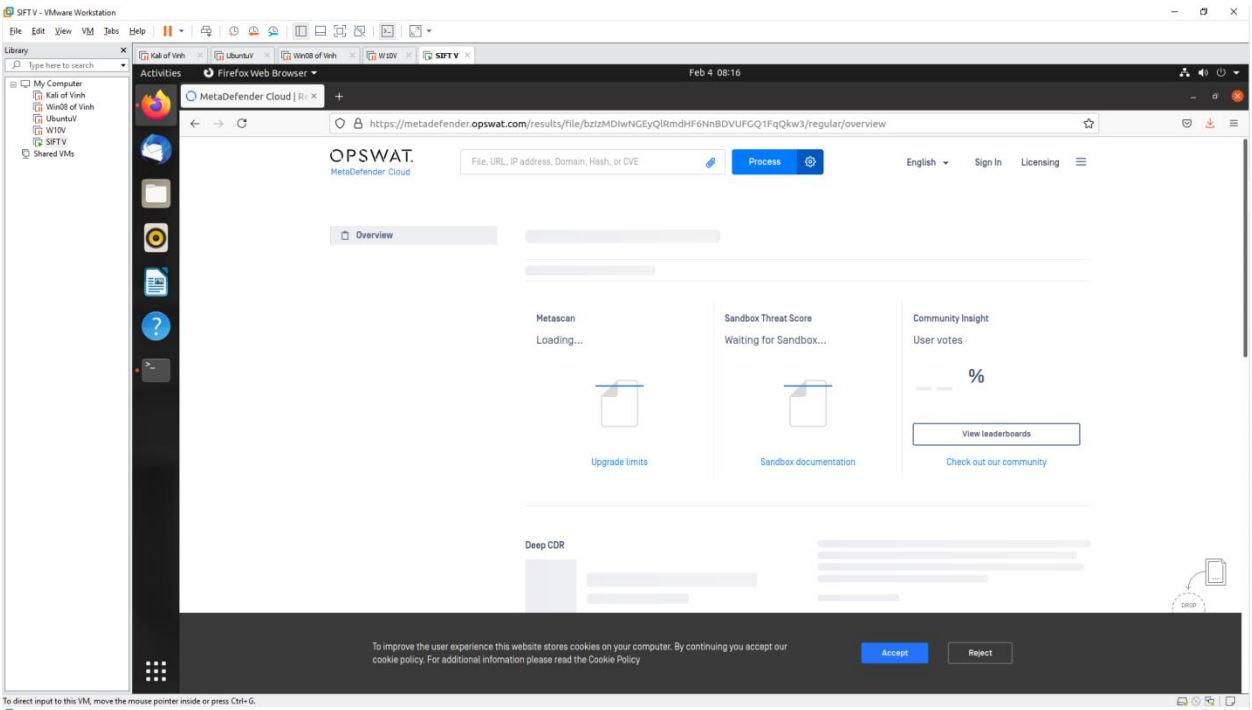


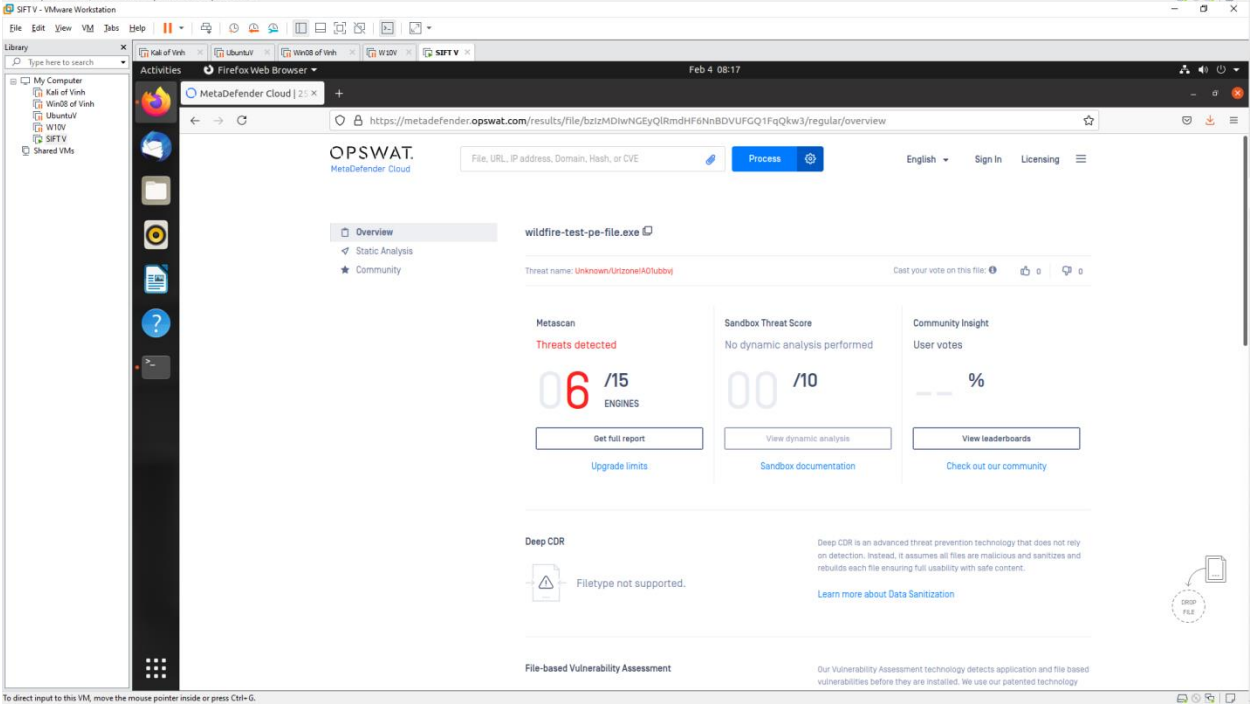
Upload Jotti

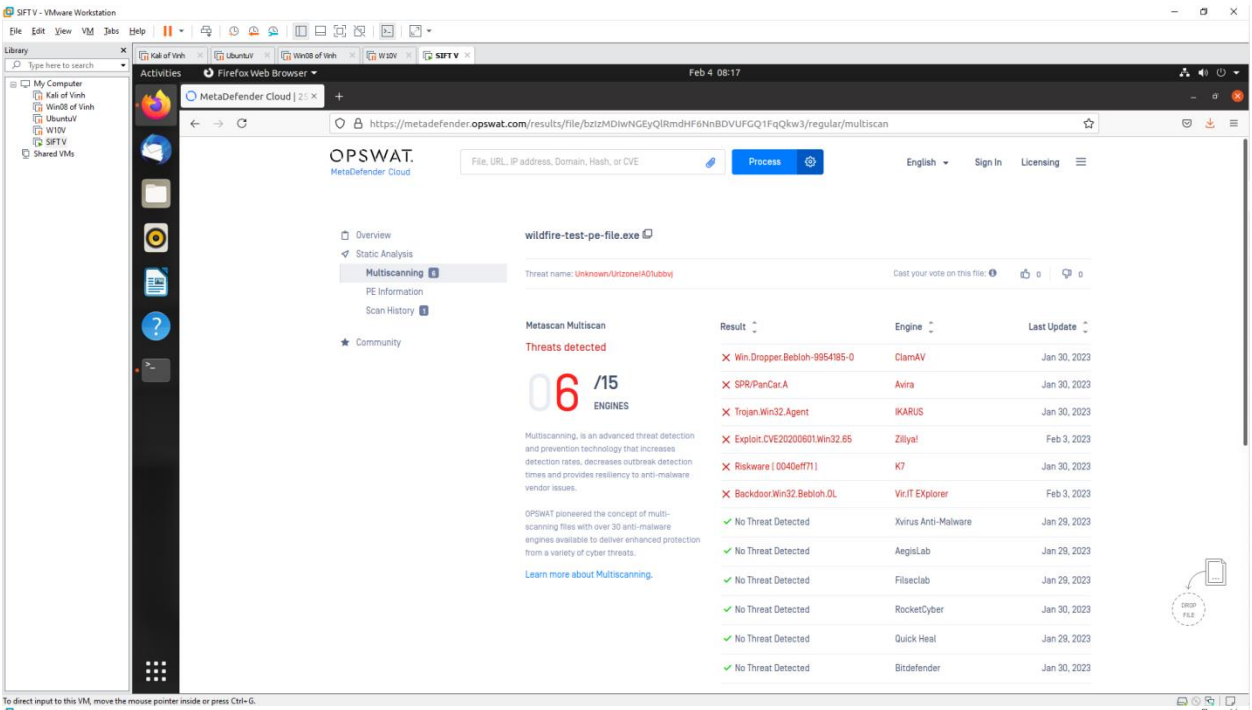


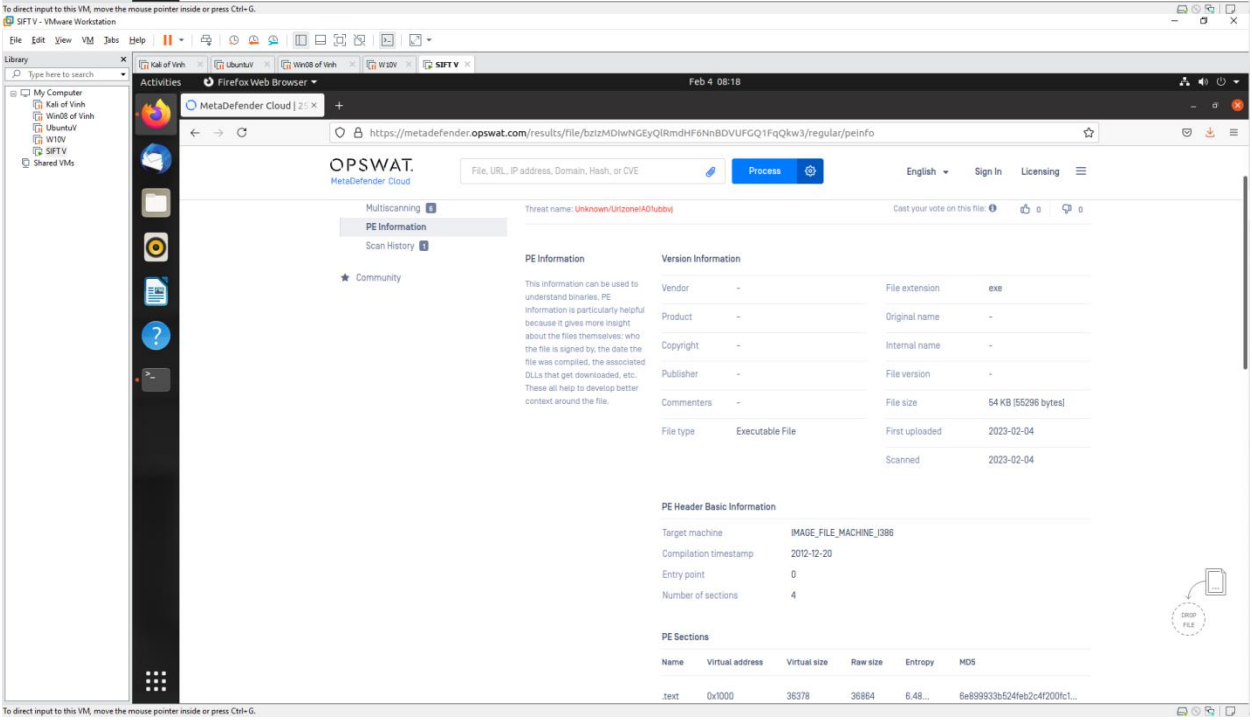


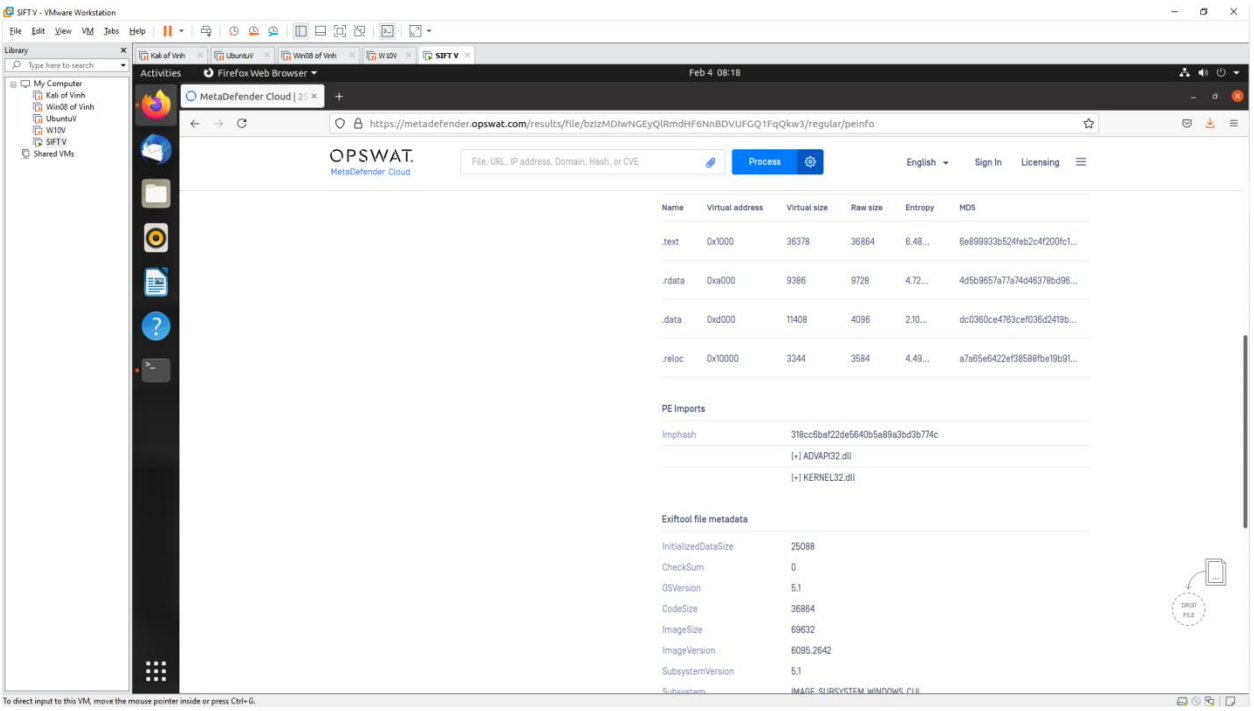
MetaDefender


SIFT V - VMware Workstation
Activities
Firefox Web Browser
Feb 4 08:16
MetaDefender Cloud
https://metadefender.opswat.com/results/file/bzizMDIwNGEyQlRmdHF6NnBDVUFGQ1FqQkw3/regular/overview
OPSWAT.
MetaDefender Cloud
File, URL, IP address, Domain, Hash, or CVE
Process
English
Sign In
Licensing
Overview
Metascan
Loading...
Upgrade limits
Sandbox Threat Score
Waiting for Sandbox...
Sandbox documentation
Community Insight
User votes
%
View leaderboards
Check out our community
Deep CDR
To improve the user experience this website stores cookies on your computer. By continuing you accept our cookie policy. For additional infomation please read the Cookie Policy
Accept
Reject
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


SIFT V - VMware Workstation
Activities
Firefox Web Browser
Feb 4 08:17
MetaDefender Cloud
https://metadefender.opswat.com/results/file/bzizMDIwNGEyQlRmdHF6NnBDVUFGQ1FqQkw3/regular/overview
OPSWAT.
MetaDefender Cloud
File, URL, IP address, Domain, Hash, or CVE
Process
English
Sign In
Licensing
Overview
Static Analysis
Community
wildfire-test-pe-file.exe
Threat name: Unknown/Urizone!A0lubbvj
Cast your vote on this file:
Metascan
Threats detected
06 /15
ENGINES
Get full report
Upgrade limits
Sandbox Threat Score
No dynamic analysis performed
00 /10
View dynamic analysis
Sandbox documentation
Community Insight
User votes
%
View leaderboards
Check out our community
Deep CDR
Filetype not supported.
Deep CDR is an advanced threat prevention technology that does not rely on detection. Instead, it assumes all files are malicious and sanitizes and rebuilds each file ensuring full usability with safe content.
Learn more about Data Sanitization
File-based Vulnerability Assessment
Our Vulnerability Assessment technology detects application and file based vulnerabilities before they are installed. We use our patented technology
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


SIFT V - VMware Workstation
Activities
Firefox Web Browser
Feb 4 08:17
MetaDefender Cloud
https://metadefender.opswat.com/results/file/bzizMDIwNGEyQlRmdHF6NnBDVUFGQ1FqQkw3/regular/multiscan
OPSWAT.
MetaDefender Cloud
File, URL, IP address, Domain, Hash, or CVE
Process
English
Sign In
Licensing
Overview
Static Analysis
Multiscanning
PE Information
Scan History
Community
wildfire-test-pe-file.exe
Threat name: Unknown/Urizone!A01ubbvj
Cast your vote on this file:
Metascan Multiscan
Threats detected
06 /15
ENGINES
Multiscanning, is an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues.
OPSWAT pioneered the concept of multi-scanning files with over 30 anti-malware engines available to deliver enhanced protection from a variety of cyber threats.
Learn more about Multiscanning.
Result
Engine
Last Update
Win.Dropper.Bebloh-9954185-0 ClamAV Jan 30, 2023
SPR/PanCar.A Avira Jan 30, 2023
Trojan.Win32.Agent IKARUS Jan 30, 2023
Exploit.CVE2020601.Win32.65 Zillya! Feb 3, 2023
Riskware [0040eff71] K7 Jan 30, 2023
Backdoor.Win32.Bebloh.OL Vir.IT EXplorer Feb 3, 2023
No Threat Detected Xvirus Anti-Malware Jan 29, 2023
No Threat Detected AegisLab Jan 29, 2023
No Threat Detected Filseclab Jan 29, 2023
No Threat Detected RocketCyber Jan 30, 2023
No Threat Detected Quick Heal Jan 29, 2023
No Threat Detected Bitdefender Jan 30, 2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

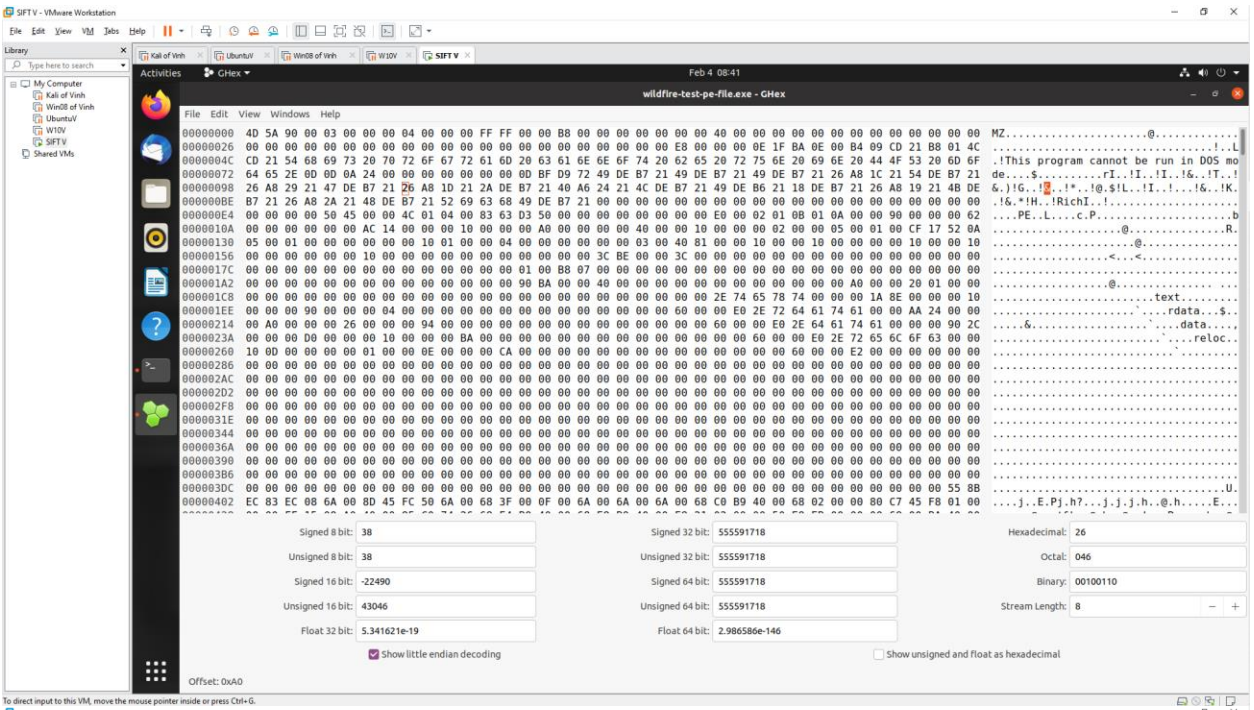

SIFT V - VMware Workstation
Activities
Firefox Web Browser
Feb 4 08:18
MetaDefender Cloud
https://metadefender.opswat.com/results/file/bzizMDIwNGEyQlRmdHF6NnBDVUFGQ1FqQkw3/regular/peinfo
OPSWAT.
MetaDefender Cloud
File, URL, IP address, Domain, Hash, or CVE
Process
English
Sign In
Licensing
Multiscanning
PE Information
Scan History
Community
Threat name: Unknown/Urizone!A01ubbvj
Cast your vote on this file:
PE Information
This information can be used to understand binaries. PE information is particularly helpful because it gives more insight about the files themselves: who the file is signed by, the date the file was compiled, the associated DLLs that get downloaded, etc. These all help to develop better context around the file.
Version Information
Vendor -
Product -
Copyright -
Publisher -
Commenters -
File type Executable File
File extension exe
Original name -
Internal name -
File version -
File size 54 KB [55296 bytes]
First uploaded 2023-02-04
Scanned 2023-02-04
PE Header Basic Information
Target machine IMAGE_FILE_MACHINE_I386
Compilation timestamp 2012-12-20
Entry point 0
Number of sections 4
PE Sections
Name Virtual address Virtual size Raw size Entropy MD5
.text 0x1000 36378 36864 6.48... 6e899933b524feb2c4f200fc1...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

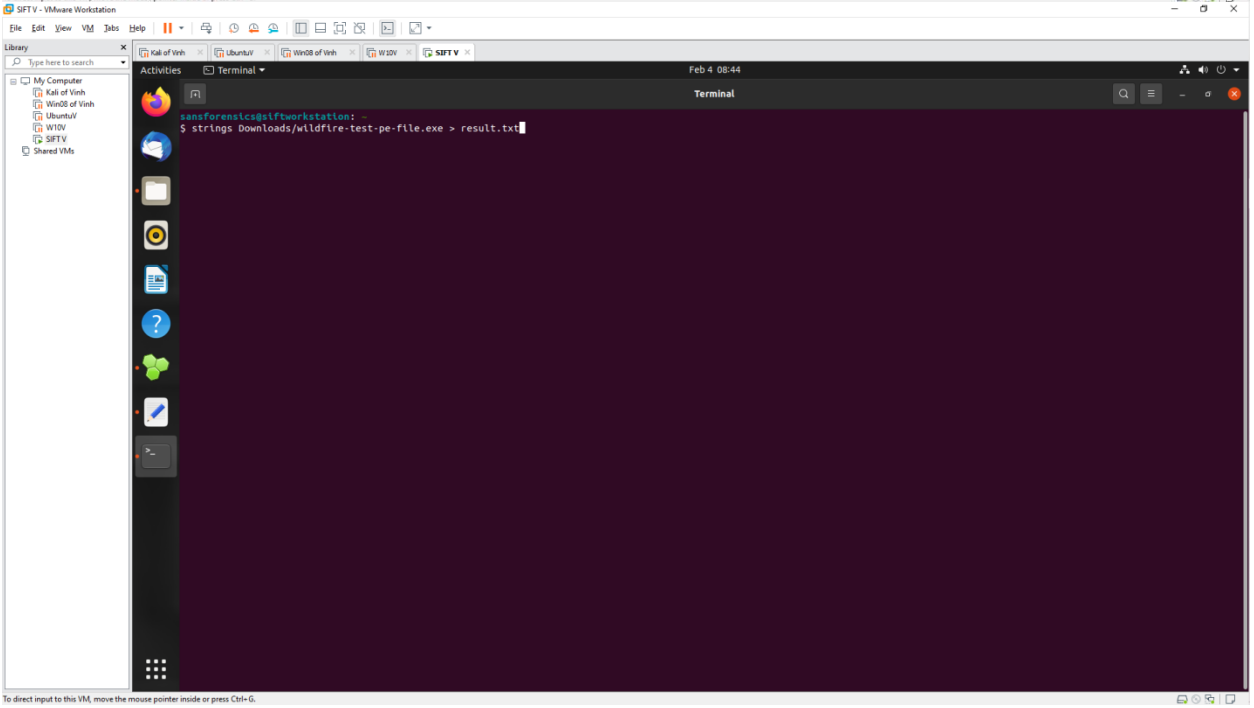


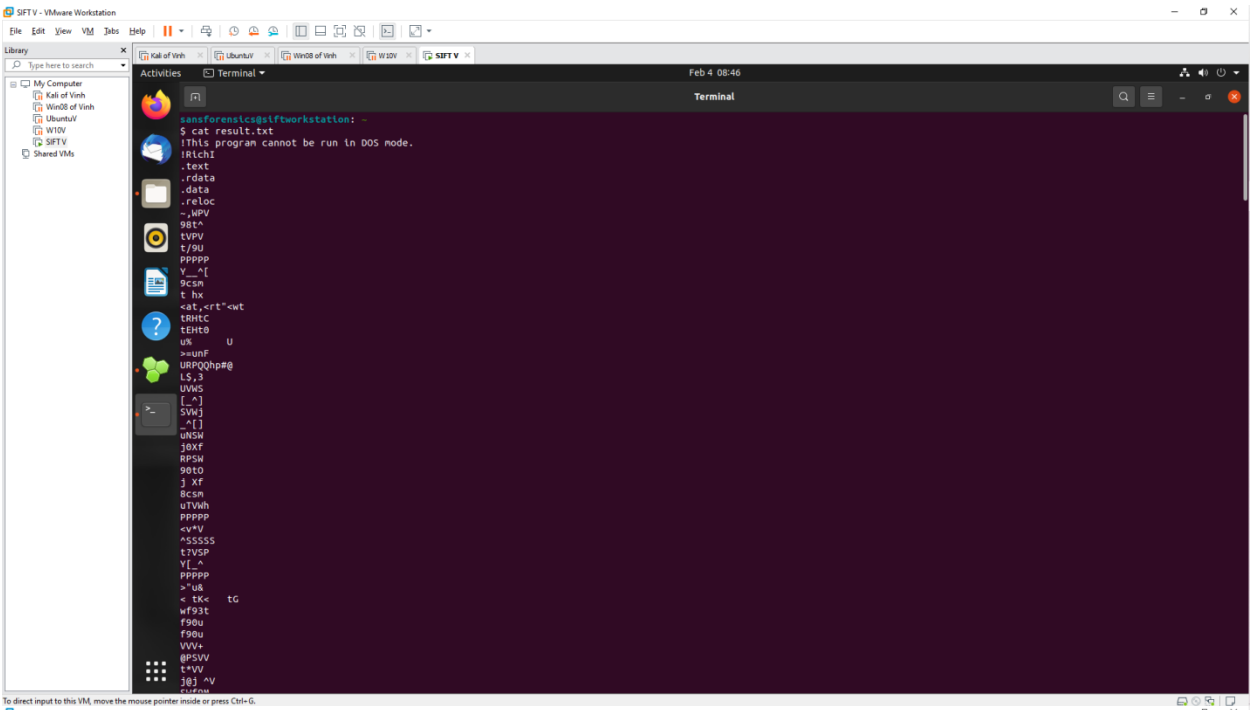
Conclusion

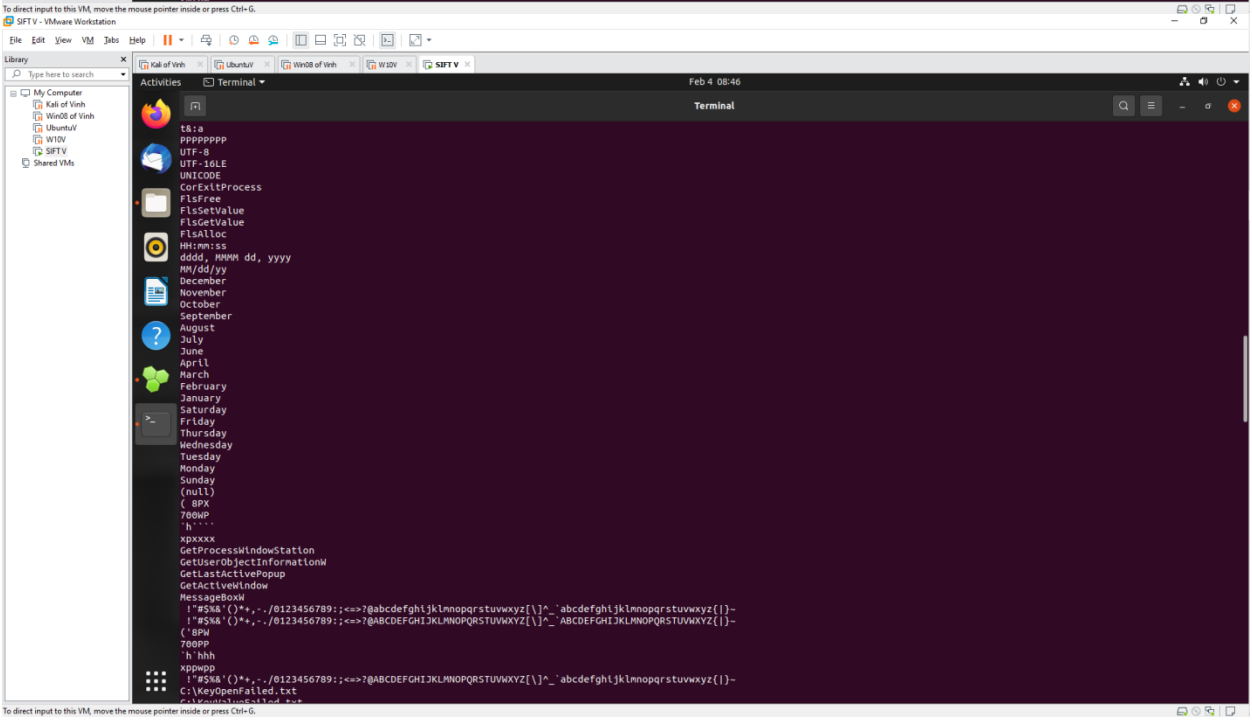
- Virustotal is the website used to scan Malware most effectively when it gives the most results, history of malware. Meanwhile, Jotti gives more results than MetaDefender but the specific information of MetaDefender is clearer than Jotti

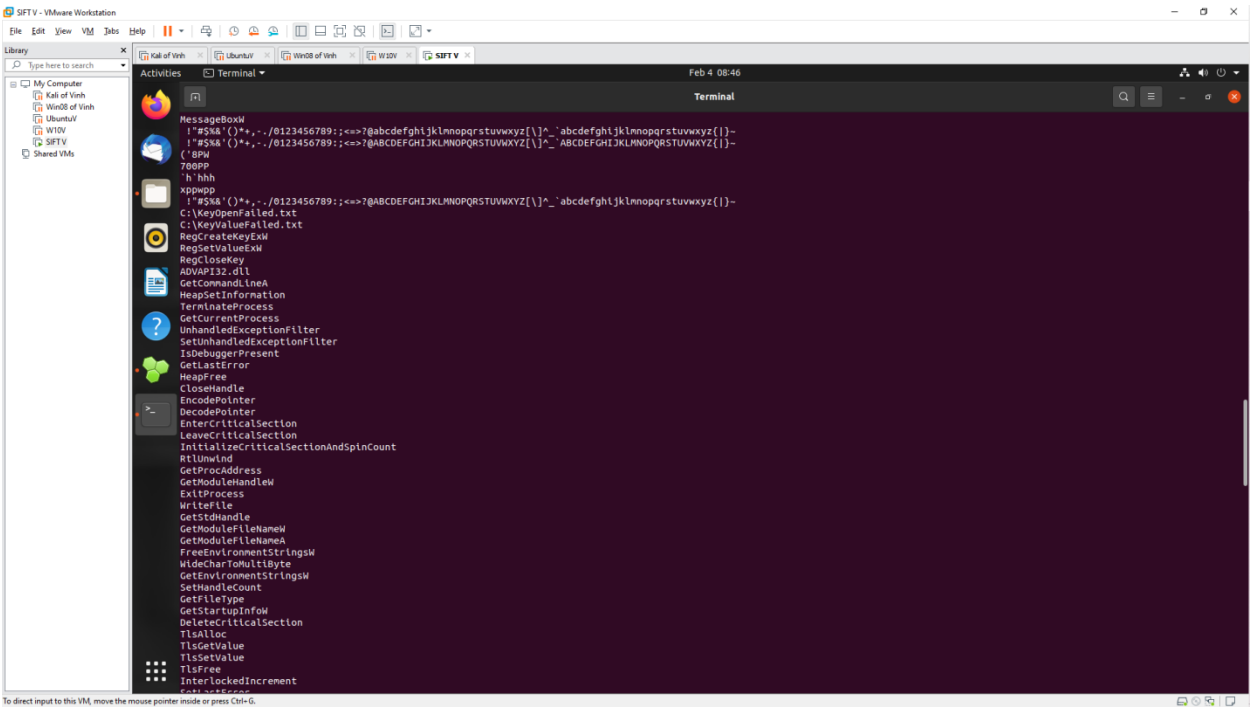
Use tools on SIFT Workstation


SIFT V - VMware Workstation
wildfire-test-pe-file.exe - GHex
Signed 8 bit: 38
Unsigned 8 bit: 38
Signed 16 bit: -22490
Unsigned 16 bit: 43046
Float 32 bit: 5.341621e-19
Signed 32 bit: 555591718
Unsigned 32 bit: 555591718
Signed 64 bit: 555591718
Unsigned 64 bit: 555591718
Float 64 bit: 2.986586e-146
Hexadecimal: 26
Octal: 046
Binary: 00100110
Stream Length: 8
Show little endian decoding
Show unsigned and float as hexadecimal
Offset: 0xA0


SIFT V - VMware Workstation
Terminal
sansforensics@siftworkstation: ~
$ strings Downloads/wildfire-test-pe-file.exe > result.txt


SIFT V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
Feb 4 08:46
Terminal
sansforensics@siftworkstation: ~
$ cat result.txt
!This program cannot be run in DOS mode.
!RLchI
.text
.rdata
.data
.reloc
~,WPV
98t^
tVPV
t/9u
PPPPP
Y__^[
9csm
t hx
<at,<rt"<wt
tRHtC
tEHt0
u% U
>=unF
URPQQhp#@
L$,3
UVWS
[_^]
SVWj
_^[]
uNSW
j0Xf
RPSW
90tO
j Xf
8csm
uTVWh
PPPPP
<v*V
^SSSSS
t?VSP
Y[_^
PPPPP
>"u&
< tK< tG
wf93t
f90u
f90u
VVV+
@PSVV
t*VV
j@j ^V
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


SIFT V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
Feb 4 08:46
Terminal
t&:a
PPPPPPPP
UTF-8
UTF-16LE
UNICODE
CorExitProcess
FlsFree
FlsSetValue
FlsGetValue
FlsAlloc
HH:mm:ss
dddd, MMMM dd, yyyy
MM/dd/yy
December
November
October
September
August
July
June
April
March
February
January
Saturday
Friday
Thursday
Wednesday
Tuesday
Monday
Sunday
(null)
(8PX
700WP
`h````
xpxxxx
GetProcessWindowStation
GetUserObjectInformationW
GetLastActivePopup
GetActiveWindow
MessageBoxW
!"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
('8PH
700PP
`h`hhh
xppwpp
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
C:\KeyOpenFailed.txt
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


SIFT V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali of Vinh
Win08 of Vinh
UbuntuV
W10V
SIFT V
Shared VMs
Kali of Vinh
UbuntuV
Win08 of Vinh
W10V
SIFT V
Activities
Terminal
Feb 4 08:46
Terminal
MessageBoxW
!"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
('BPW
700PP
`h`hhh
xppwpp
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
C:\KeyOpenFailed.txt
C:\KeyValueFailed.txt
RegCreateKeyExW
RegSetValueExW
RegCloseKey
ADVAPI32.dll
GetCommandLineA
HeapSetInformation
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
SetUnhandledExceptionFilter
IsDebuggerPresent
GetLastError
HeapFree
CloseHandle
EncodePointer
DecodePointer
EnterCriticalSection
LeaveCriticalSection
InitializeCriticalSectionAndSpinCount
RtlUnwind
GetProcAddress
GetModuleHandleW
ExitProcess
WriteFile
GetStdHandle
GetModuleFileNameW
GetModuleFileNameA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStringsW
SetHandleCount
GetFileType
GetStartupInfoW
DeleteCriticalSection
TlsAlloc
TlsGetValue
TlsSetValue
TlsFree
InterlockedIncrement
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.