Analysis

Of Virus File

Virus Analysis Report

Report On file calc.exe & sys-logs.dll

Date: 2022/03/26

Time: 10:12 am

CHARCHIT SUBEDI

CONTENT **PAGE NO.**

INTRODUCTION TO COMPUTER VIRUS

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are said to be "infected" with a computer virus.

Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage. A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.

Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and to spread the virus. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit (e.g., with ransomware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for damage and denial of service, or simply because they wish to explore cybersecurity issues, artificial life and evolutionary algorithms.

Computer viruses cause billions of dollars' worth of economic damage each year.

In response, an industry of antivirus software has cropped up, selling or freely distributing virus protection to users of various operating systems.

INTRODUCTION TO VIRUS TOTAL

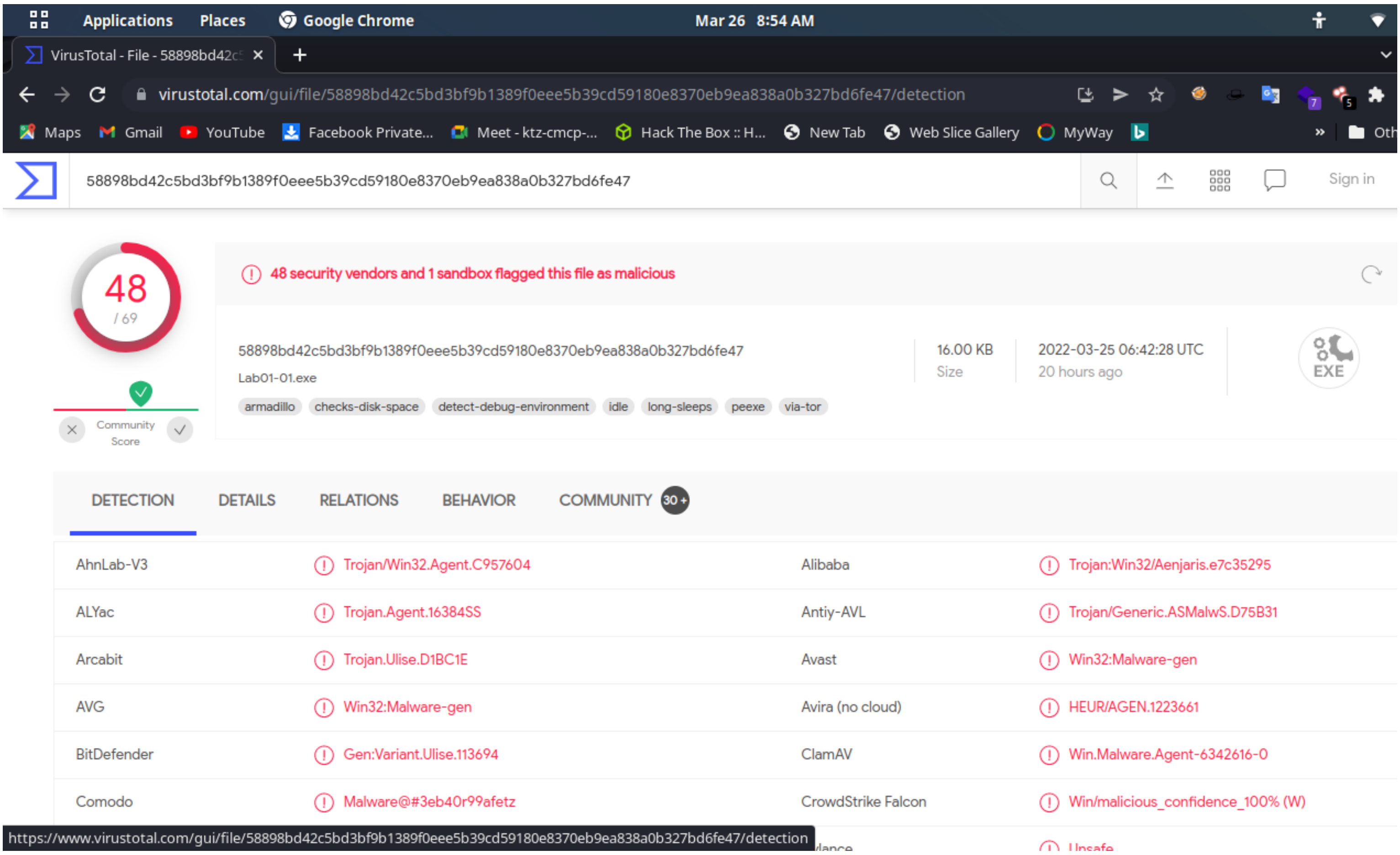
VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google in September 2012. The company's ownership switched in January 2018 to Chronicle, a subsidiary of Google.

VirusTotal aggregates many antivirus products and online scan engines called Contributors. In November, 2018, the Cyber National Mission Force, a unit subordinate to the U.S. Cyber Command became a Contributor. The aggregated data from these Contributors allows a user to check for viruses that the user's own antivirus software may have missed, or to verify against any false positives. Files up to 650 MB can be uploaded to the website, or sent via email (max. 32MB). Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software and, by extension, VirusTotal's own capability. Users can also scan suspect URLs and search through the VirusTotal dataset. VirusTotal uses the Cuckoo sandbox for dynamic analysis of malware. VirusTotal was selected by PC World as one of the best 100 products of 2007.

INTRODUCTION TO CUTTER TOOLS

Cutter is an open-source graphical user interface for the radare2 reverse engineering framework. Cutter is a complete framework for reverse-engineering and analyzing binaries; composed of a set of small utilities that can be used together or independently from the GUI. Built around a disassembler for computer software which generates assembly language source code from machine-executable code, it supports a variety of executable formats for different processor architectures and operating systems.

ANALYSIS OF CALC.EXE



58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47

48 security vendors and 1 sandbox flagged this file as malicious

58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Lab01-01.exe

16.00 KB
Size

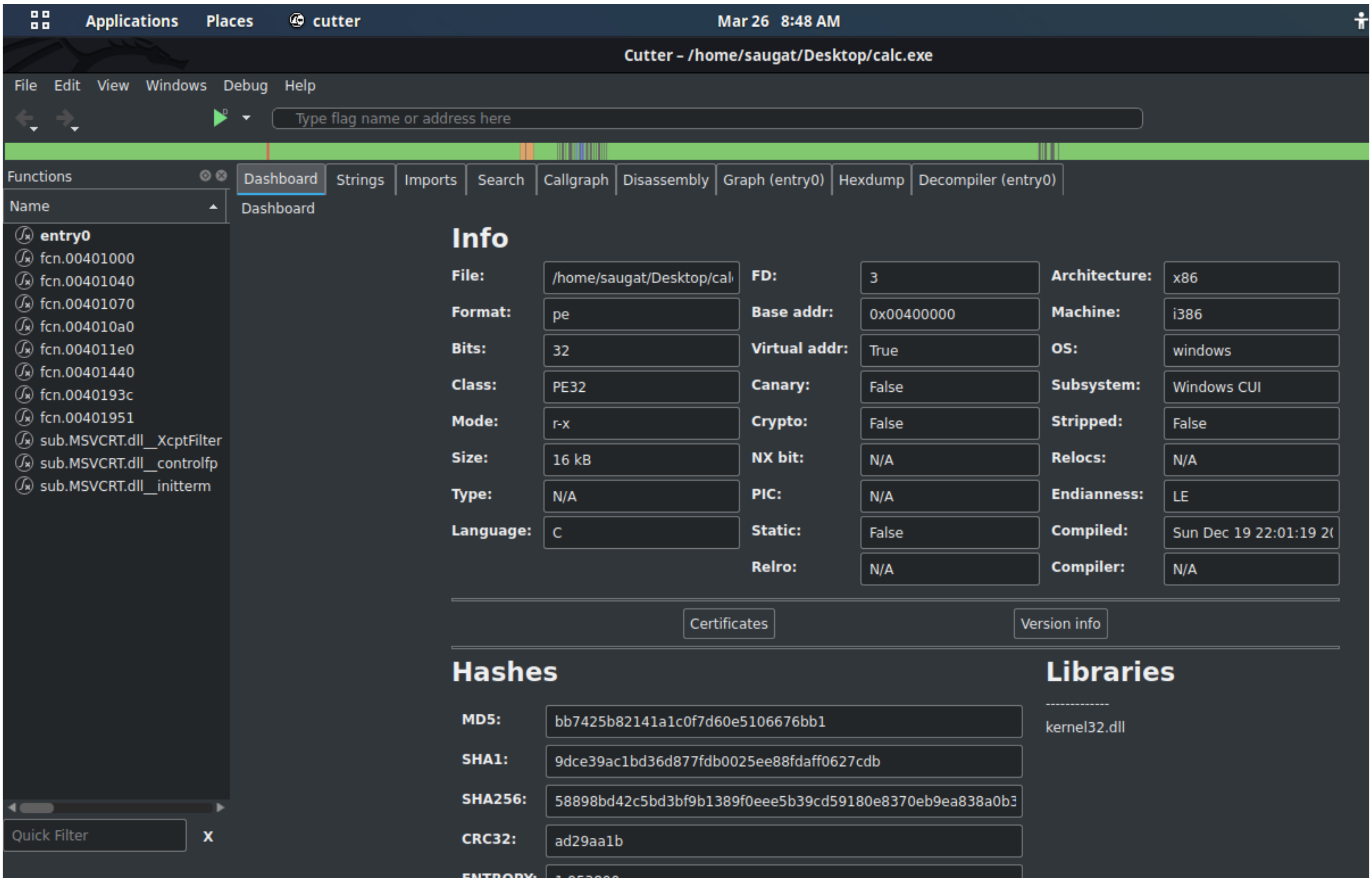
2022-03-25 06:42:28 UTC
20 hours ago

armadillo checks-disk-space detect-debug-environment idle long-sleeps peexe via-tor

AhnLab-V3	Trojan/Win32.Agent.C957604	Alibaba	Trojan:Win32/Aenjaris.e7c35295
ALYac	Trojan.Agent.16384SS	Antiy-AVL	Trojan/Generic.ASMalwS.D75B31
Arcabit	Trojan.Ulise.D1BC1E	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	HEUR/AGEN.1223661
BitDefender	Gen:Variant.Ulise.113694	ClamAV	Win.Malware.Agent-6342616-0
Comodo	Malware@#3eb40r99afetz	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
		lance	Unsafe

https://www.virustotal.com/gui/file/58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47/detection

From the above screenshot, we can see that we have scanned the calc.exe file from www.virustotal.com . In the above scanned result the file is detected by 48 antivirus out of 69. Some of the antiviruse said that it is Trojan, some have said that it is malware. Let’s do Reverse Engineering of the software with the help of cutter tool.



entry0
fcn.00401000
fcn.00401040
fcn.00401070
fcn.004010a0
fcn.004011e0
fcn.00401440
fcn.0040193c
fcn.00401951
sub.MSVCRT.dll__XcptFilter
sub.MSVCRT.dll__controlfp
sub.MSVCRT.dll__initterm

Dashboard

Info

File:	/home/saugat/Desktop/cal	FD:	3	Architecture:	x86
Format:	pe	Base addr:	0x00400000	Machine:	i386
Bits:	32	Virtual addr:	True	OS:	windows
Class:	PE32	Canary:	False	Subsystem:	Windows CUI
Mode:	r-x	Crypto:	False	Stripped:	False
Size:	16 kB	NX bit:	N/A	Relocs:	N/A
Type:	N/A	PIC:	N/A	Endianness:	LE
Language:	C	Static:	False	Compiled:	Sun Dec 19 22:01:19 2(
		Relro:	N/A	Compiler:	N/A

Hashes

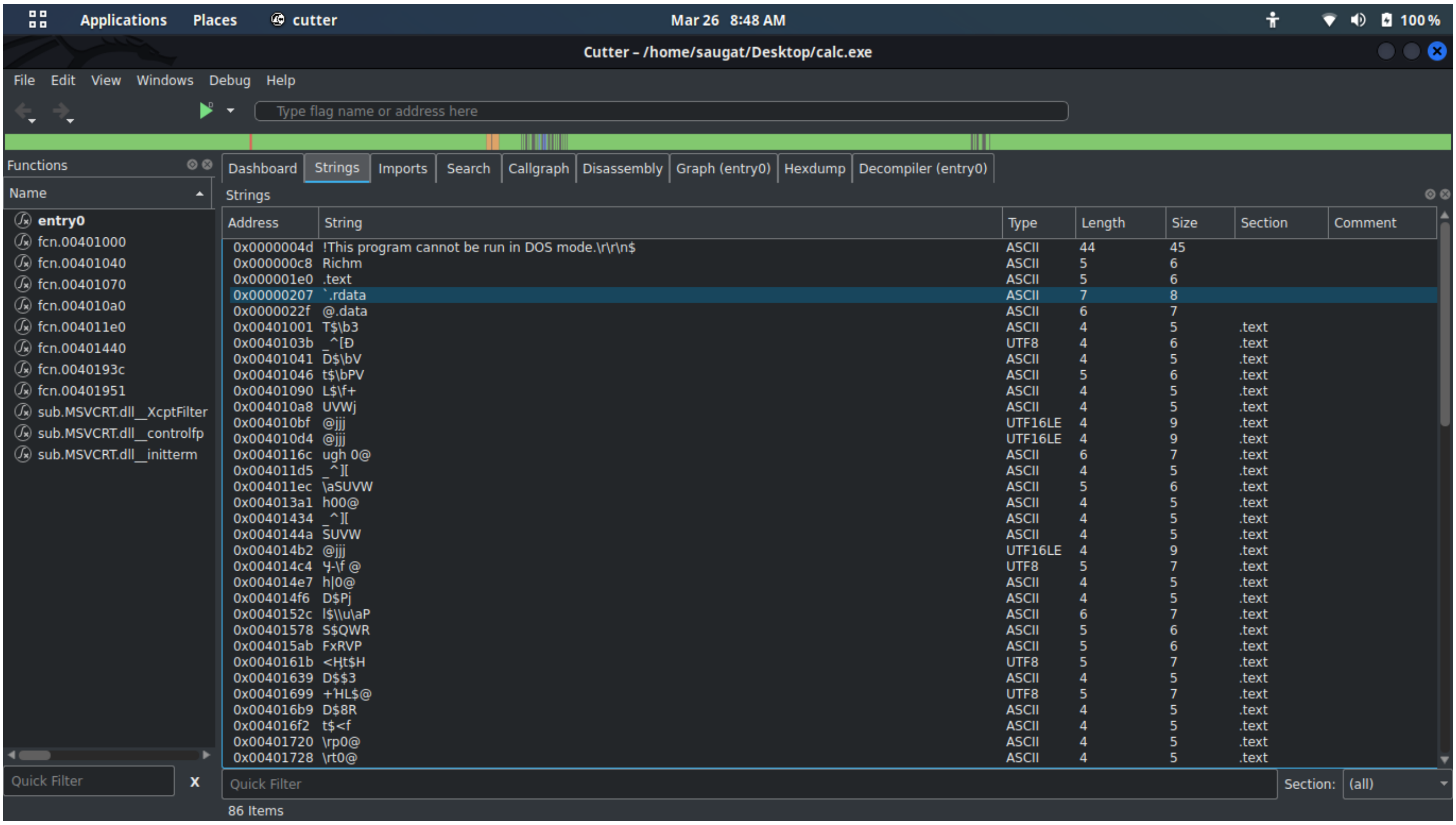
MD5:	bb7425b82141a1c0f7d60e5106676bb1
SHA1:	9dce39ac1bd36d877fdb0025ee88fdaff0627cdb
SHA256:	58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b3
CRC32:	ad29aa1b

Libraries

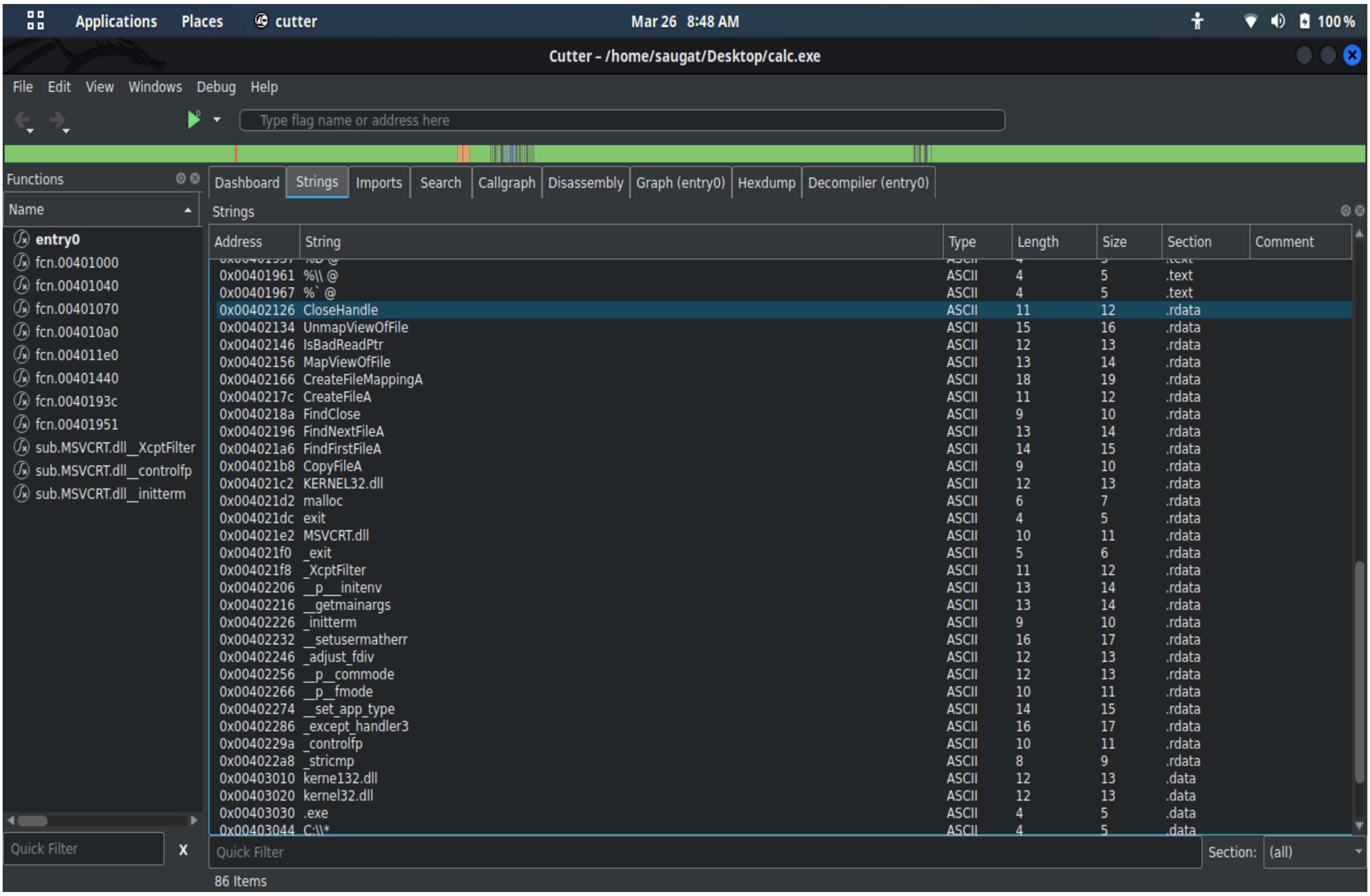
----
kernel32.dll

In the above screenshot we can see the dashboard of cutter tool. In the dashboard we can see the information of calc.exe file where, the main information are listed below :

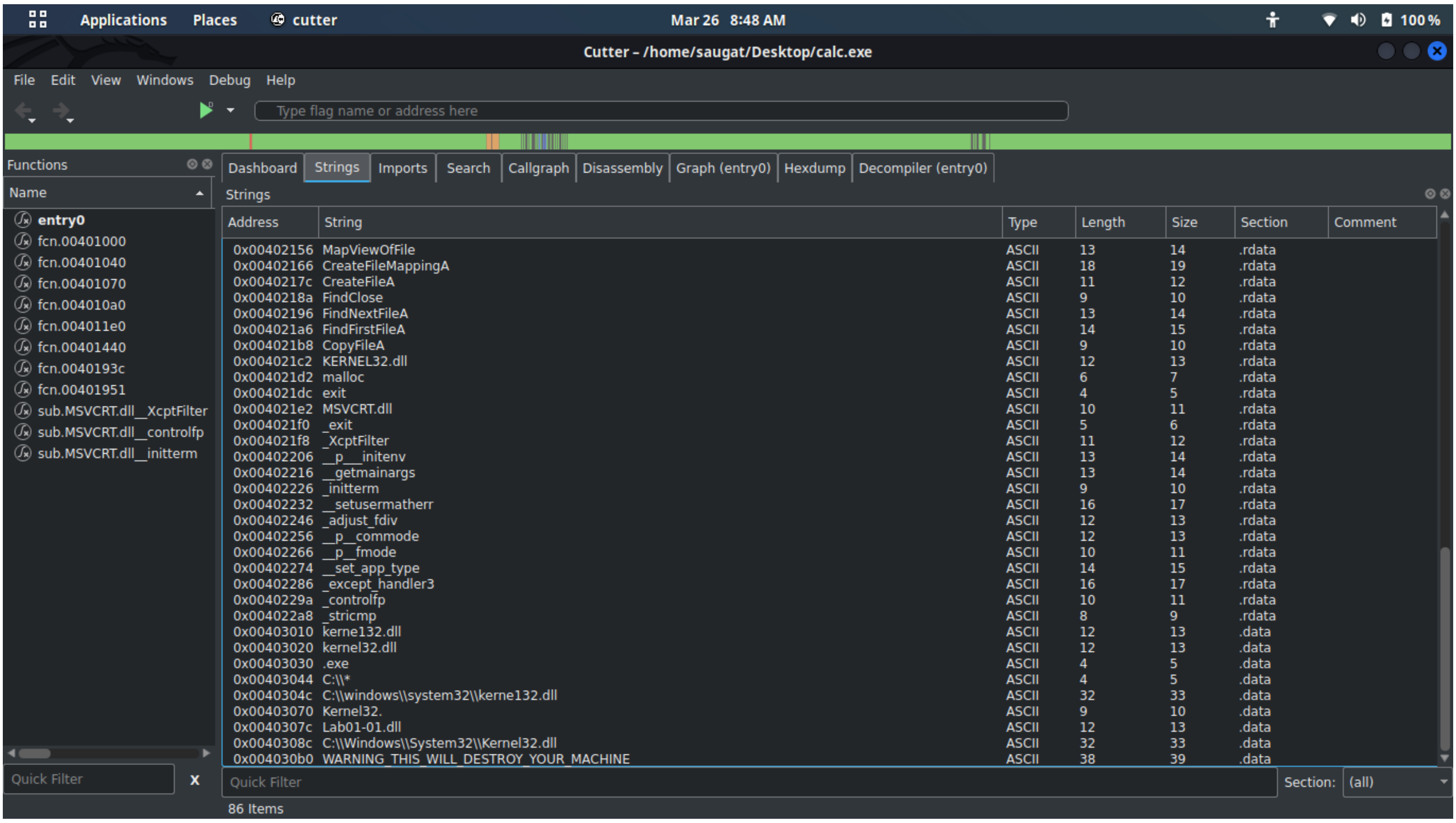
i. It is created from “c” programming language.
ii. It’s architecture is X86 which support only 32bit operating system.
iii. It support only Window operating system.



Address	String	Type	Length	Size	Section	Comment
0x0000004d	!This program cannot be run in DOS mode.\r\r\n$	ASCII	44	45		
0x000000c8	Richm	ASCII	5	6		
0x000001e0	.text	ASCII	5	6		
0x00000207	`.rdata	ASCII	7	8		
0x0000022f	@.data	ASCII	6	7		
0x00401001	T$\b3	ASCII	4	5	.text	
0x0040103b	_^[Đ	UTF8	4	6	.text	
0x00401041	D$\bV	ASCII	4	5	.text	
0x00401046	t$\bPV	ASCII	5	6	.text	
0x00401090	L$\f+	ASCII	4	5	.text	
0x004010a8	UVWj	ASCII	4	5	.text	
0x004010bf	@jjj	UTF16LE	4	9	.text	
0x004010d4	@jjj	UTF16LE	4	9	.text	
0x0040116c	ugh 0@	ASCII	6	7	.text	
0x004011d5	_^][	ASCII	4	5	.text	
0x004011ec	\aSUVW	ASCII	5	6	.text	
0x004013a1	h00@	ASCII	4	5	.text	
0x00401434	_^][	ASCII	4	5	.text	
0x0040144a	SUVW	ASCII	4	5	.text	
0x004014b2	@jjj	UTF16LE	4	9	.text	
0x004014c4	Ӌ-\f @	UTF8	5	7	.text	
0x004014e7	h|0@	ASCII	4	5	.text	
0x004014f6	D$Pj	ASCII	4	5	.text	
0x0040152c	l$\\u\aP	ASCII	6	7	.text	
0x00401578	S$QWR	ASCII	5	6	.text	
0x004015ab	FxRVP	ASCII	5	6	.text	
0x0040161b	<Ḩt$H	UTF8	5	7	.text	
0x00401639	D$$3	ASCII	4	5	.text	
0x00401699	+ʹHL$@	UTF8	5	7	.text	
0x004016b9	D$8R	ASCII	4	5	.text	
0x004016f2	t$<f	ASCII	4	5	.text	
0x00401720	\rp0@	ASCII	4	5	.text	
0x00401728	\rt0@	ASCII	4	5	.text	



Address	String	Type	Length	Size	Section	Comment
0x00401961	%\\ @	ASCII	4	5	.text	
0x00401967	%` @	ASCII	4	5	.text	
0x00402126	CloseHandle	ASCII	11	12	.rdata	
0x00402134	UnmapViewOfFile	ASCII	15	16	.rdata	
0x00402146	IsBadReadPtr	ASCII	12	13	.rdata	
0x00402156	MapViewOfFile	ASCII	13	14	.rdata	
0x00402166	CreateFileMappingA	ASCII	18	19	.rdata	
0x0040217c	CreateFileA	ASCII	11	12	.rdata	
0x0040218a	FindClose	ASCII	9	10	.rdata	
0x00402196	FindNextFileA	ASCII	13	14	.rdata	
0x004021a6	FindFirstFileA	ASCII	14	15	.rdata	
0x004021b8	CopyFileA	ASCII	9	10	.rdata	
0x004021c2	KERNEL32.dll	ASCII	12	13	.rdata	
0x004021d2	malloc	ASCII	6	7	.rdata	
0x004021dc	exit	ASCII	4	5	.rdata	
0x004021e2	MSVCRT.dll	ASCII	10	11	.rdata	
0x004021f0	_exit	ASCII	5	6	.rdata	
0x004021f8	_XcptFilter	ASCII	11	12	.rdata	
0x00402206	__p__initenv	ASCII	13	14	.rdata	
0x00402216	__getmainargs	ASCII	13	14	.rdata	
0x00402226	_initterm	ASCII	9	10	.rdata	
0x00402232	__setusermatherr	ASCII	16	17	.rdata	
0x00402246	_adjust_fdiv	ASCII	12	13	.rdata	
0x00402256	__p__commode	ASCII	12	13	.rdata	
0x00402266	__p__fmode	ASCII	10	11	.rdata	
0x00402274	__set_app_type	ASCII	14	15	.rdata	
0x00402286	_except_handler3	ASCII	16	17	.rdata	
0x0040229a	_controlfp	ASCII	10	11	.rdata	
0x004022a8	_stricmp	ASCII	8	9	.rdata	
0x00403010	kerne132.dll	ASCII	12	13	.data	
0x00403020	kernel32.dll	ASCII	12	13	.data	
0x00403030	.exe	ASCII	4	5	.data	
0x00403044	C:\*	ASCII	4	5	.data	



Address	String	Type	Length	Size	Section	Comment
0x00402156	MapViewOfFile	ASCII	13	14	.rdata	
0x00402166	CreateFileMappingA	ASCII	18	19	.rdata	
0x0040217c	CreateFileA	ASCII	11	12	.rdata	
0x0040218a	FindClose	ASCII	9	10	.rdata	
0x00402196	FindNextFileA	ASCII	13	14	.rdata	
0x004021a6	FindFirstFileA	ASCII	14	15	.rdata	
0x004021b8	CopyFileA	ASCII	9	10	.rdata	
0x004021c2	KERNEL32.dll	ASCII	12	13	.rdata	
0x004021d2	malloc	ASCII	6	7	.rdata	
0x004021dc	exit	ASCII	4	5	.rdata	
0x004021e2	MSVCRT.dll	ASCII	10	11	.rdata	
0x004021f0	_exit	ASCII	5	6	.rdata	
0x004021f8	_XcptFilter	ASCII	11	12	.rdata	
0x00402206	__p___initenv	ASCII	13	14	.rdata	
0x00402216	__getmainargs	ASCII	13	14	.rdata	
0x00402226	_initterm	ASCII	9	10	.rdata	
0x00402232	__setusermatherr	ASCII	16	17	.rdata	
0x00402246	_adjust_fdiv	ASCII	12	13	.rdata	
0x00402256	__p__commode	ASCII	12	13	.rdata	
0x00402266	__p__fmode	ASCII	10	11	.rdata	
0x00402274	__set_app_type	ASCII	14	15	.rdata	
0x00402286	_except_handler3	ASCII	16	17	.rdata	
0x0040229a	_controlfp	ASCII	10	11	.rdata	
0x004022a8	_stricmp	ASCII	8	9	.rdata	
0x00403010	kerne132.dll	ASCII	12	13	.data	
0x00403020	kernel32.dll	ASCII	12	13	.data	
0x00403030	.exe	ASCII	4	5	.data	
0x00403044	C:*	ASCII	4	5	.data	
0x0040304c	C:\\windows\\system32\\kerne132.dll	ASCII	32	33	.data	
0x00403070	Kernel32.	ASCII	9	10	.data	
0x0040307c	Lab01-01.dll	ASCII	12	13	.data	
0x0040308c	C:\\Windows\\System32\\Kernel32.dll	ASCII	32	33	.data	
0x004030b0	WARNING_THIS_WILL_DESTROY_YOUR_MACHINE	ASCII	38	39	.data	

In the above screenshot we can see that, We are in string section, Let's explain main string's

i. This program will not run in DOS (disk operating system) .

ii. CloseHandle : The CloseHandle function closes an open object handle.

iii. Unmap view office : Unmaps a mapped view of a file from the calling process's address space.

iv. IsBadReadptr : Verifies that the calling process has read access to the specified range of memory.

v. MapViewOffice : This function maps a view of a file into the address space of the calling process.

vi. CreateFileMappingA : Creates or opens a named or unnamed file mapping object for a specified file.

vii. CReateFileA : Creates or opens a file or I/O device. The most commonly used I/O devices are as follows: file, file stream, directory, physical disk, volume, console buffer, tape drive, communications resource, mailslot, and pipe. The function returns a handle that can be used to access the file or device for various types of I/O depending on the file or device and the flags and attributes specified.

viii. CopyfileA : Copies an existing file to a new file. The CopyFileEx function provides two additional capabilities. CopyFileEx can call a specified callback function each time a portion of the copy operation is completed, and CopyFileEx can be canceled during the copy operation.

ix. FindClose : Closes a file search handle opened by the FindFirstFile, FindFirstFileEx, FindFirstFileNameW, FindFirstFileNameTransactedW, FindFirstFileTransacted, FindFirstStreamTransactedW, or FindFirstStreamW functions.

x. FindNextFileA : Continues a file search from a previous call to the FindFirstFile, FindFirstFileEx, or FindFirstFileTransacted functions.

xi. FindFirstFileA : Searches a directory for a file or subdirectory with a name that matches a specific name (or partial name if wildcards are used).

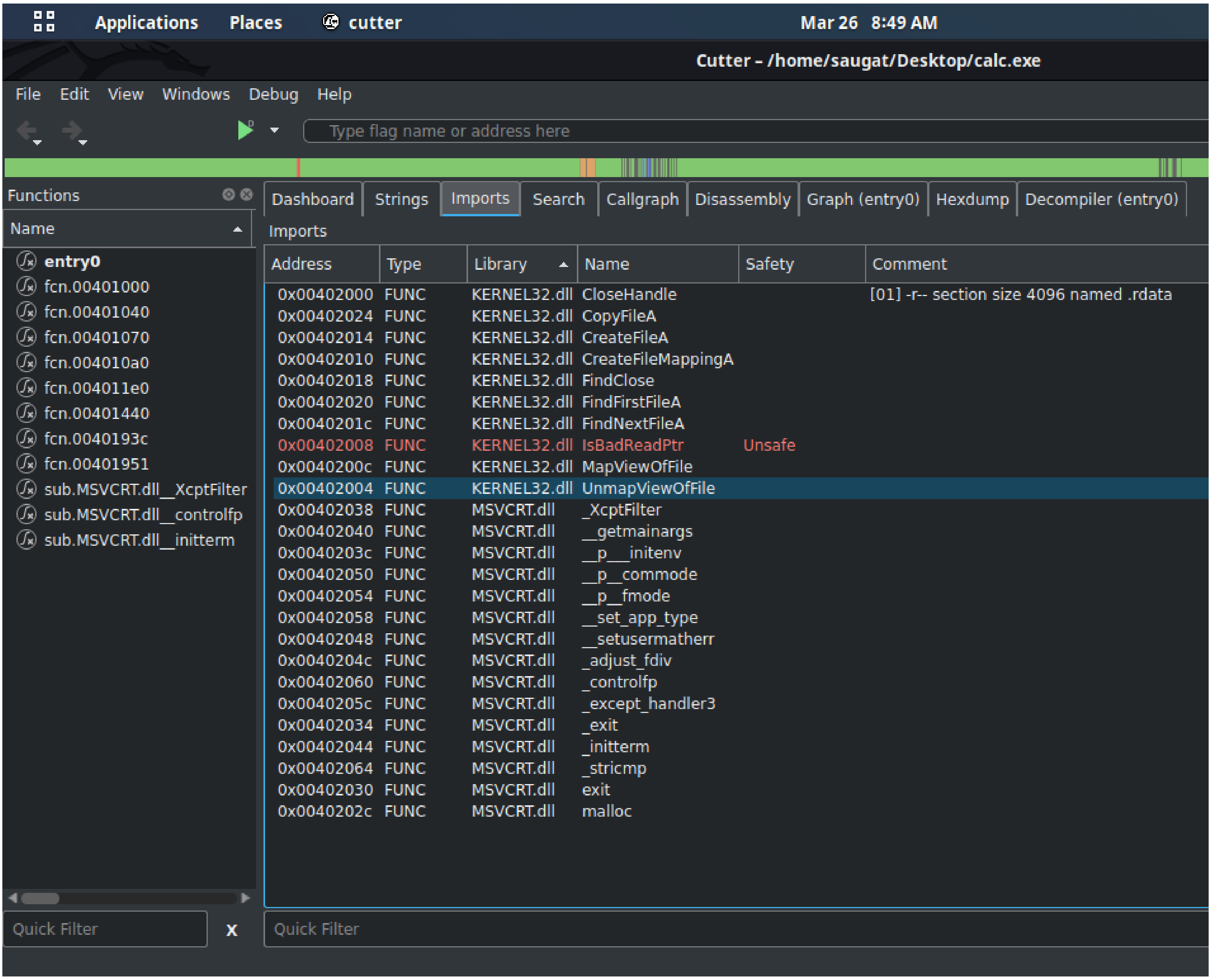
xii. Kernal32.dll : KERNEL32. DLL exposes to applications most of the Win32 base APIs, such as memory management, input/output (I/O) operations, process and thread creation, and synchronization functions.

xiii. Malloc : The name "malloc" stands for memory allocation. The malloc() function reserves a block of memory of the specified number of bytes. And, it returns a pointer of void which can be casted into pointers of any form.

xiv. MSVCRT.dll : MSVCRT. DLL is the C standard library for the Visual C++ (MSVC) compiler from version 4.2 to 6.0. It provides programs compiled by these versions of MSVC with most of the standard C library functions. These include string manipulation, memory allocation, C-style input/output calls, and others.

xv. XcptFilter : This method is called by the exception-filter expression of the try-except Statement. The method consults the _XcptActTab[] table to identify the exception and determine the appropriate action. _XcptActTab[] is a constant and is defined as shown in the following table. The exception numbers are defined in winnt.h and the signal numbers are defined in signal.h.

xvi. _setusermather : Specifies a user-supplied rountine to handle math errors, instead of the _matherr routine.



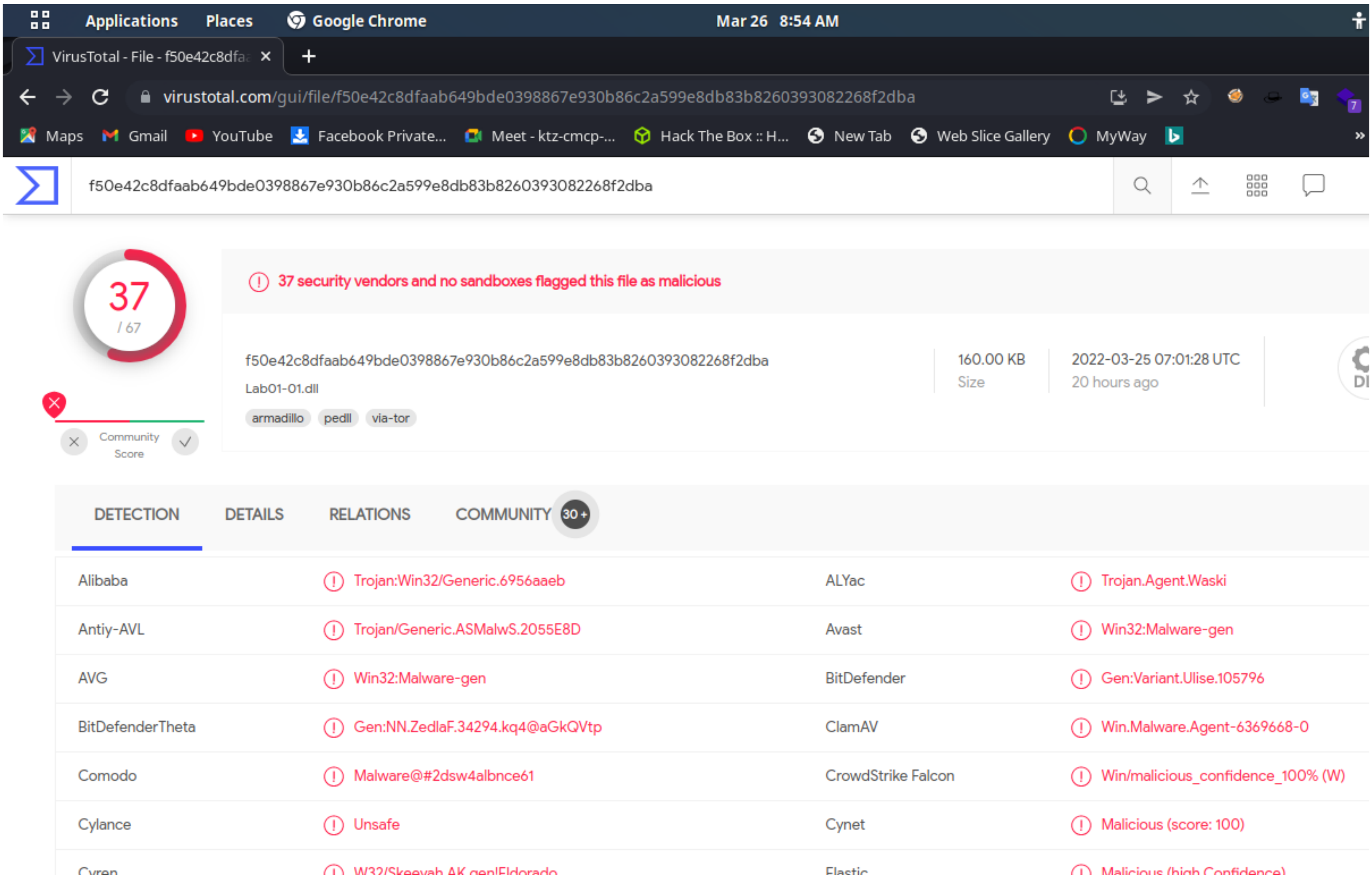
Name
entry0
fcn.00401000
fcn.00401040
fcn.00401070
fcn.004010a0
fcn.004011e0
fcn.00401440
fcn.0040193c
fcn.00401951
sub.MSVCRT.dll__XcptFilter
sub.MSVCRT.dll__controlfp
sub.MSVCRT.dll__initterm

Imports

Address	Type	Library	Name	Safety	Comment
0x00402000	FUNC	KERNEL32.dll	CloseHandle		[01] -r-- section size 4096 named .rdata
0x00402024	FUNC	KERNEL32.dll	CopyFileA		
0x00402014	FUNC	KERNEL32.dll	CreateFileA		
0x00402010	FUNC	KERNEL32.dll	CreateFileMappingA		
0x00402018	FUNC	KERNEL32.dll	FindClose		
0x00402020	FUNC	KERNEL32.dll	FindFirstFileA		
0x0040201c	FUNC	KERNEL32.dll	FindNextFileA		
0x00402008	FUNC	KERNEL32.dll	IsBadReadPtr	Unsafe	
0x0040200c	FUNC	KERNEL32.dll	MapViewOfFile		
0x00402004	FUNC	KERNEL32.dll	UnmapViewOfFile		
0x00402038	FUNC	MSVCRT.dll	_XcptFilter		
0x00402040	FUNC	MSVCRT.dll	__getmainargs		
0x0040203c	FUNC	MSVCRT.dll	__p__initenv		
0x00402050	FUNC	MSVCRT.dll	__p__commode		
0x00402054	FUNC	MSVCRT.dll	__p__fmode		
0x00402058	FUNC	MSVCRT.dll	__set_app_type		
0x00402048	FUNC	MSVCRT.dll	__setusermatherr		
0x0040204c	FUNC	MSVCRT.dll	_adjust_fdiv		
0x00402060	FUNC	MSVCRT.dll	_controlfp		
0x0040205c	FUNC	MSVCRT.dll	_except_handler3		
0x00402034	FUNC	MSVCRT.dll	_exit		
0x00402044	FUNC	MSVCRT.dll	_initterm		
0x00402064	FUNC	MSVCRT.dll	_stricmp		
0x00402030	FUNC	MSVCRT.dll	exit		
0x0040202c	FUNC	MSVCRT.dll	malloc		

This is the Import section . where we can see the Kernal32.dll isbadreadptr is unsafe / the main file of virus.

ANALYSIS OF SYS-LOGS.DLL



37 security vendors and no sandboxes flagged this file as malicious

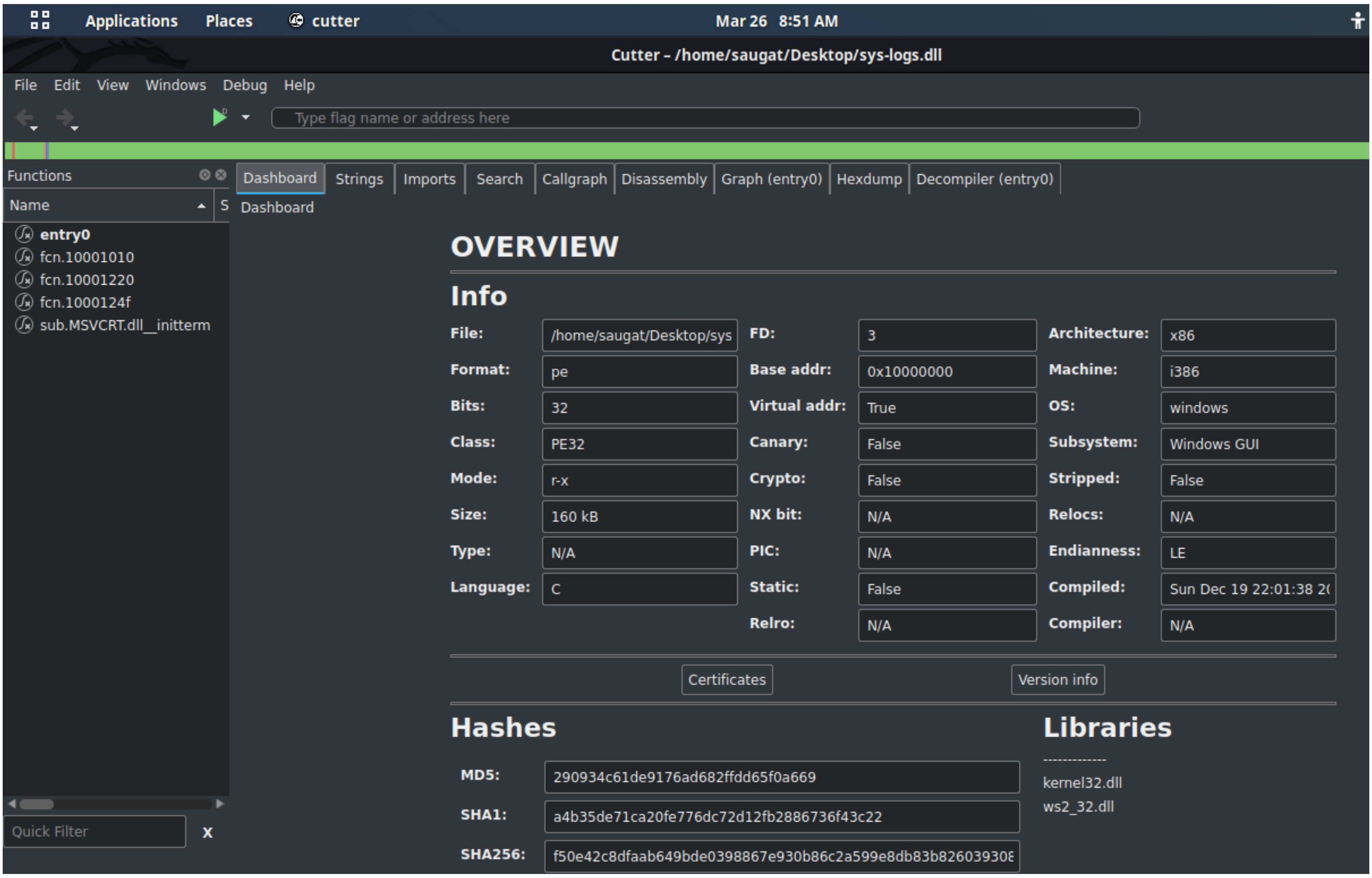
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
Lab01-01.dll
armadillo pedll via-tor

160.00 KB
Size

2022-03-25 07:01:28 UTC
20 hours ago

Alibaba	Trojan:Win32/Generic.6956aaeb	ALYac	Trojan.Agent.Waski
Antiy-AVL	Trojan/Generic.ASMalwS.2055E8D	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	BitDefender	Gen:Variant.Ulise.105796
BitDefenderTheta	Gen:NN.ZedlaF.34294.kq4@aGkQVtp	ClamAV	Win.Malware.Agent-6369668-0
Comodo	Malware@#2dsw4albnce61	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Skeeyah.AK.gen!Eldorado	Elastic	Malicious (high Confidence)

From the above screenshot, we can see that we have scanned the sys-logs.dll file from www.virustotal.com . In the above scanned result the file is detected by 37 antivirus out of 67. Some of the antiviruse said that it is Trojan, some have said that it is malware. Let's do Reverse Engineering of the software with the help of cutter tool.



OVERVIEW

Info

File:	/home/saugat/Desktop/sys	FD:	3	Architecture:	x86
Format:	pe	Base addr:	0x10000000	Machine:	i386
Bits:	32	Virtual addr:	True	OS:	windows
Class:	PE32	Canary:	False	Subsystem:	Windows GUI
Mode:	r-x	Crypto:	False	Stripped:	False
Size:	160 kB	NX bit:	N/A	Relocs:	N/A
Type:	N/A	PIC:	N/A	Endianness:	LE
Language:	C	Static:	False	Compiled:	Sun Dec 19 22:01:38 2
		Relro:	N/A	Compiler:	N/A

Hashes

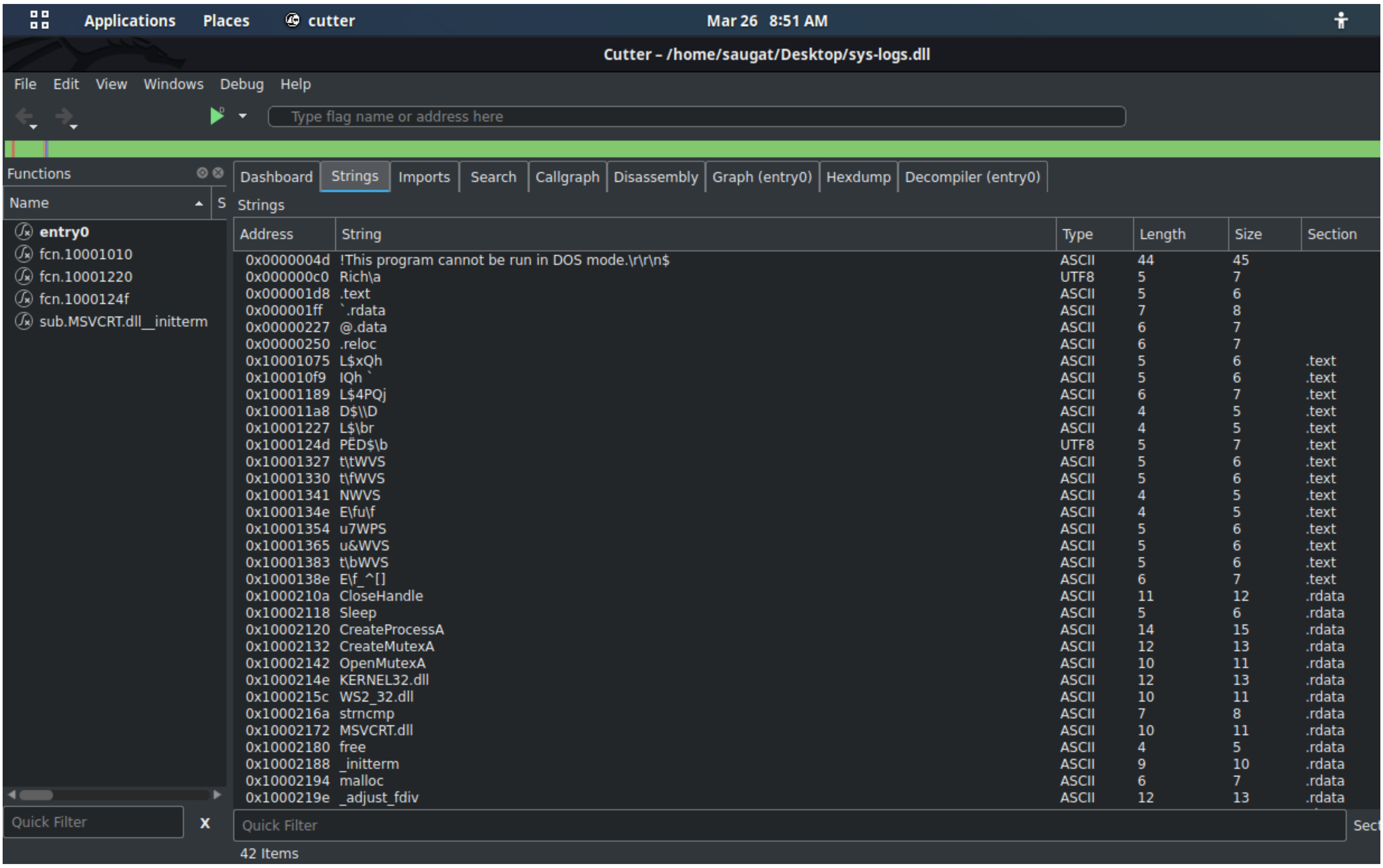
MD5:	290934c61de9176ad682ffdd65f0a669
SHA1:	a4b35de71ca20fe776dc72d12fb2886736f43c22
SHA256:	f50e42c8dfaab649bde0398867e930b86c2a599e8db83b826039308

Libraries

----
kernel32.dll
ws2_32.dll

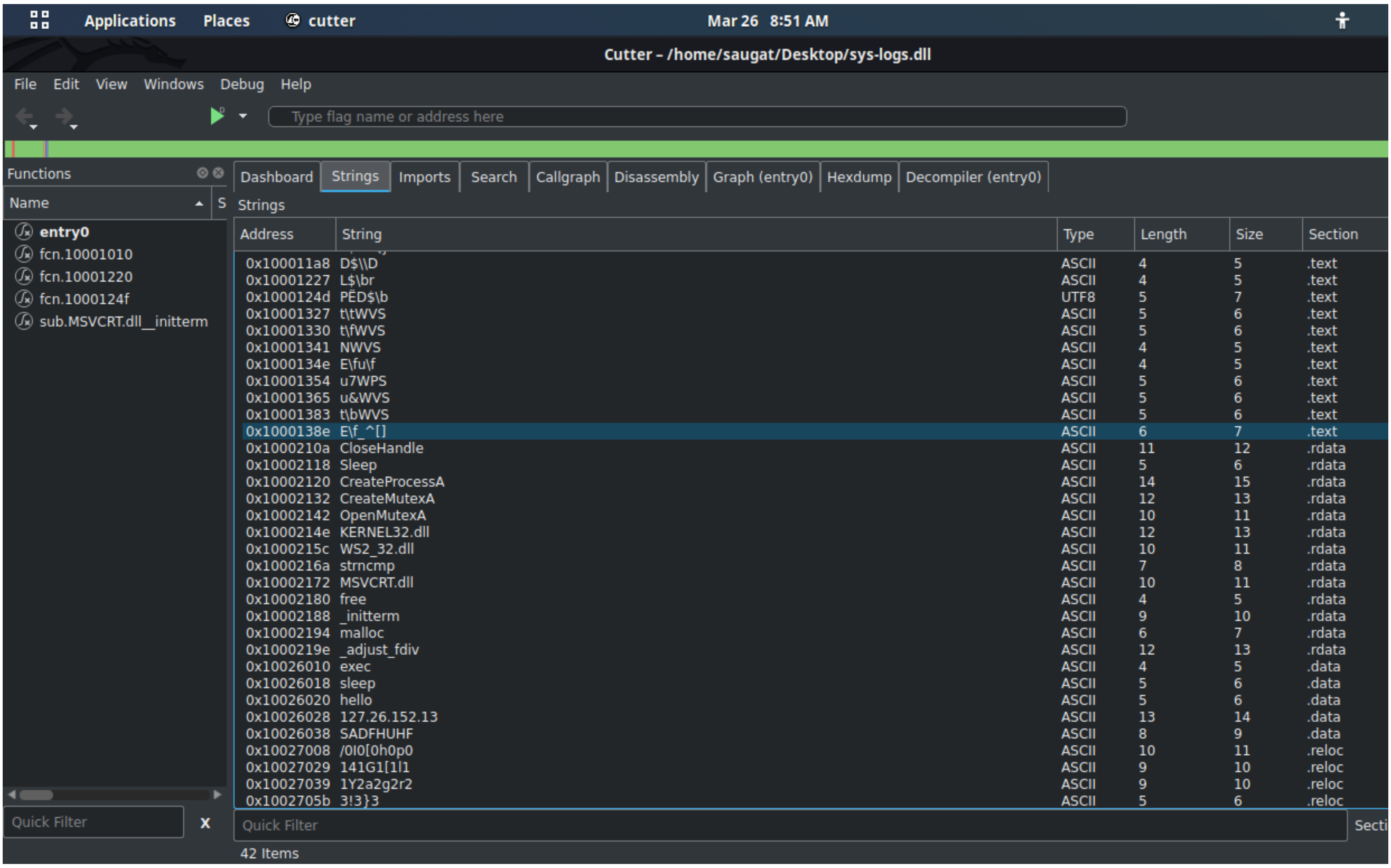
In the above screenshot we can see the dashboard of cutter tool. In the dashboard we can see the information of sys-logs.dll file where, the main information are listed below :

i. It is created from “c” programming language.
ii. It’s architecture is X86 which support only 32bit operating system.
iii. It support only Window operating system.
iv. It’s subsystem is Window GUI .
v. It’s libraries are Kernal32.dll and ws_32.dll



Address	String	Type	Length	Size	Section
0x0000004d	!This program cannot be run in DOS mode.\r\r\n$	ASCII	44	45	
0x000000c0	Rich\a	UTF8	5	7	
0x000001d8	.text	ASCII	5	6	
0x000001ff	`.rdata	ASCII	7	8	
0x00000227	@.data	ASCII	6	7	
0x00000250	.reloc	ASCII	6	7	
0x10001075	L$xQh	ASCII	5	6	.text
0x100010f9	IQh `	ASCII	5	6	.text
0x10001189	L$4PQj	ASCII	6	7	.text
0x100011a8	D$\\D	ASCII	4	5	.text
0x10001227	L$\br	ASCII	4	5	.text
0x1000124d	PËD$\b	UTF8	5	7	.text
0x10001327	t\tWVS	ASCII	5	6	.text
0x10001330	t\fWVS	ASCII	5	6	.text
0x10001341	NWVS	ASCII	4	5	.text
0x1000134e	E\fu\f	ASCII	4	5	.text
0x10001354	u7WPS	ASCII	5	6	.text
0x10001365	u&WVS	ASCII	5	6	.text
0x10001383	t\bWVS	ASCII	5	6	.text
0x1000138e	E\f_^[]	ASCII	6	7	.text
0x1000210a	CloseHandle	ASCII	11	12	.rdata
0x10002118	Sleep	ASCII	5	6	.rdata
0x10002120	CreateProcessA	ASCII	14	15	.rdata
0x10002132	CreateMutexA	ASCII	12	13	.rdata
0x10002142	OpenMutexA	ASCII	10	11	.rdata
0x1000214e	KERNEL32.dll	ASCII	12	13	.rdata
0x1000215c	WS2_32.dll	ASCII	10	11	.rdata
0x1000216a	strncmp	ASCII	7	8	.rdata
0x10002172	MSVCRT.dll	ASCII	10	11	.rdata
0x10002180	free	ASCII	4	5	.rdata
0x10002188	_initterm	ASCII	9	10	.rdata
0x10002194	malloc	ASCII	6	7	.rdata
0x1000219e	_adjust_fdiv	ASCII	12	13	.rdata

42 Items



Address	String	Type	Length	Size	Section
0x100011a8	D$\\D	ASCII	4	5	.text
0x10001227	L$\br	ASCII	4	5	.text
0x1000124d	PËD$\b	UTF8	5	7	.text
0x10001327	t\tWVS	ASCII	5	6	.text
0x10001330	t\fWVS	ASCII	5	6	.text
0x10001341	NWVS	ASCII	4	5	.text
0x1000134e	E\fu\f	ASCII	4	5	.text
0x10001354	u7WPS	ASCII	5	6	.text
0x10001365	u&WVS	ASCII	5	6	.text
0x10001383	t\bWVS	ASCII	5	6	.text
0x1000138e	E\f_^[]	ASCII	6	7	.text
0x1000210a	CloseHandle	ASCII	11	12	.rdata
0x10002118	Sleep	ASCII	5	6	.rdata
0x10002120	CreateProcessA	ASCII	14	15	.rdata
0x10002132	CreateMutexA	ASCII	12	13	.rdata
0x10002142	OpenMutexA	ASCII	10	11	.rdata
0x1000214e	KERNEL32.dll	ASCII	12	13	.rdata
0x1000215c	WS2_32.dll	ASCII	10	11	.rdata
0x1000216a	strncmp	ASCII	7	8	.rdata
0x10002172	MSVCRT.dll	ASCII	10	11	.rdata
0x10002180	free	ASCII	4	5	.rdata
0x10002188	_initterm	ASCII	9	10	.rdata
0x10002194	malloc	ASCII	6	7	.rdata
0x1000219e	_adjust_fdiv	ASCII	12	13	.rdata
0x10026010	exec	ASCII	4	5	.data
0x10026018	sleep	ASCII	5	6	.data
0x10026020	hello	ASCII	5	6	.data
0x10026028	127.26.152.13	ASCII	13	14	.data
0x10026038	SADFHUHF	ASCII	8	9	.data
0x10027008	/0I0[0h0p0	ASCII	10	11	.reloc
0x10027029	141G1[1l1	ASCII	9	10	.reloc
0x10027039	1Y2a2g2r2	ASCII	9	10	.reloc
0x1002705b	3!3}3	ASCII	5	6	.reloc

42 Items

In the above screenshot we can see that, We are in string section, Let's explain main string's

i. This program will not run in DOS (disk operating system) .

ii. CloseHandle : The CloseHandle function closes an open object handle.

iii. Sleep : sleep() function is used in order to wait for a current thread for a specified time. slepp() function will sleep given thread specified time for the current executable. Of course, the CPU and other processes will run without a problem.

iv. CreateProcessA : Creates a new process and its primary thread. The new process runs in the security context of the calling process. If the calling process is impersonating another user, the new process uses the token for the calling process, not the impersonation token. To run the new process in the security context of the user represented by the impersonation token, use the CreateProcessAsUser or CreateProcessWithLogonW function.

v. CreateMutexA : Creates or opens a named or unnamed mutex object. To specify an access mask for the object, use the CreateMutexEx function

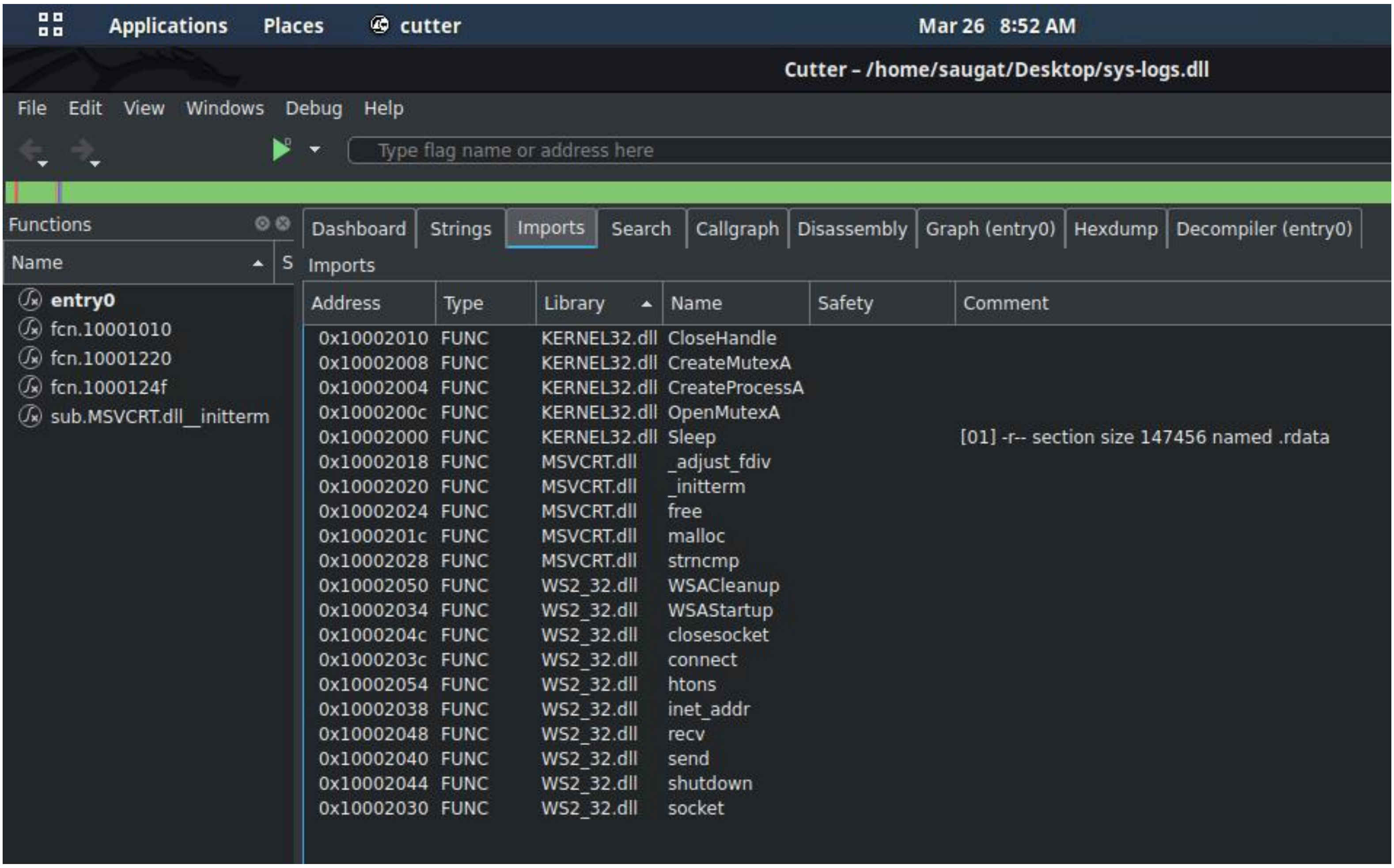
vi. Kernal32.dll : KERNEL32. DLL exposes to applications most of the Win32 base APIs, such as memory management, input/output (I/O) operations, process and thread creation, and synchronization functions.

vii. Strncmp : Compares up to num characters of the C string str1 to those of the C string str2. This function starts comparing the first character of each string. If they are equal to each other, it continues with the following pairs until the characters differ, until a terminating null-character is reached, or until num characters match in both strings, whichever happens first.

viii. **MSVCRT.dll** : MSVCRT. DLL is the C standard library for the Visual C++ (MSVC) compiler from version 4.2 to 6.0. It provides programs compiled by these versions of MSVC with most of the standard C library functions. These include string manipulation, memory allocation, C-style input/output calls, and others.

ix. **FREE :** The free() function in C library allows you to release or deallocate the memory blocks which are previously allocated by calloc(), malloc() or realloc() functions. It frees up the memory blocks and returns the memory to heap.

x. **_exec :** In computing, exec is a functionality of an operating system that runs an executable file in the context of an already existing process, replacing the previous executable. This act is also referred to as an overlay.



- entry0
- fcn.10001010
- fcn.10001220
- fcn.1000124f
- sub.MSVCRT.dll__initterm

Imports

Address	Type	Library	Name	Safety	Comment
0x10002010	FUNC	KERNEL32.dll	CloseHandle		
0x10002008	FUNC	KERNEL32.dll	CreateMutexA		
0x10002004	FUNC	KERNEL32.dll	CreateProcessA		
0x1000200c	FUNC	KERNEL32.dll	OpenMutexA		
0x10002000	FUNC	KERNEL32.dll	Sleep		[01] -r-- section size 147456 named .rdata
0x10002018	FUNC	MSVCRT.dll	_adjust_fdiv		
0x10002020	FUNC	MSVCRT.dll	_initterm		
0x10002024	FUNC	MSVCRT.dll	free		
0x1000201c	FUNC	MSVCRT.dll	malloc		
0x10002028	FUNC	MSVCRT.dll	strncmp		
0x10002050	FUNC	WS2_32.dll	WSACleanup		
0x10002034	FUNC	WS2_32.dll	WSAStartup		
0x1000204c	FUNC	WS2_32.dll	closesocket		
0x1000203c	FUNC	WS2_32.dll	connect		
0x10002054	FUNC	WS2_32.dll	htons		
0x10002038	FUNC	WS2_32.dll	inet_addr		
0x10002048	FUNC	WS2_32.dll	recv		
0x10002040	FUNC	WS2_32.dll	send		
0x10002044	FUNC	WS2_32.dll	shutdown		
0x10002030	FUNC	WS2_32.dll	socket		

This is the Import section . where we can see what types of files are being imported by the sys-logs.dll . It will close handle ,CreateMutex A , CreateprocessA , sleep, closesocket, connect,receive,send,shutdown the computer.

CONCLUSION

Hence, From the above report we Know that Any software can be affected by Virus and malware. We should always use Geniun Products / software. If we are not able to use Geniun software then once we have to properly check that software in Virustotal.