Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

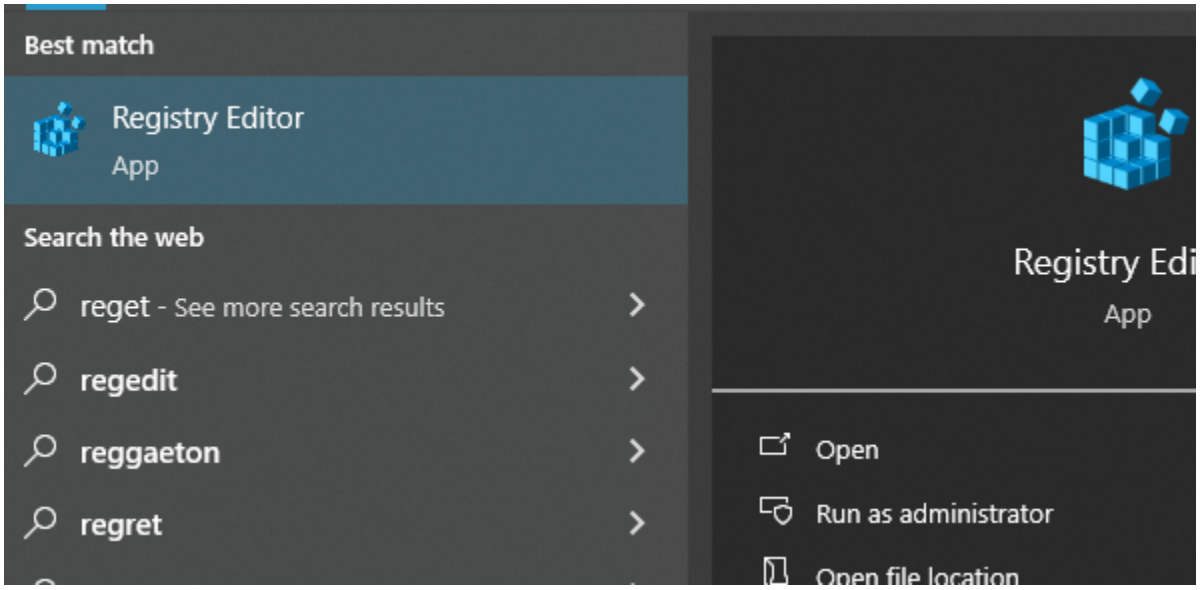
Title : Malware and Forensics

Lab : 10

Chapter : 23 (Digital Forensics)

Lab 10
Exercise : 23. 01

Step 1 :
A.



Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem

ACPI
AppID
AppReadiness
Arbiters
Audio
BackupRestore
BGFX
BitLocker
BitlockerStatus
Bluetooth
cfgAdll
CI
Class
CloudDomainJoin

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisableDeleteNo...	REG_DWORD	0x00000000 (0)
FilterSupportedF...	REG_DWORD	0x00000000 (0)
LongPathsEnabl...	REG_DWORD	0x00000001 (1)
NtfsAllowExten...	REG_DWORD	0x00000000 (0)
NtfsBugcheckO...	REG_DWORD	0x00000000 (0)
NtfsDisable8dot...	REG_DWORD	0x00000002 (2)
NtfsDisableCom...	REG_DWORD	0x00000000 (0)
NtfsDisableEncr...	REG_DWORD	0x00000000 (0)
NtfsDisableLast...	REG_DWORD	0x80000000 (2147483648)
NtfsDisableLfsD...	REG_DWORD	0x00000000 (0)
NtfsDisableVols...	REG_DWORD	0x00000000 (0)

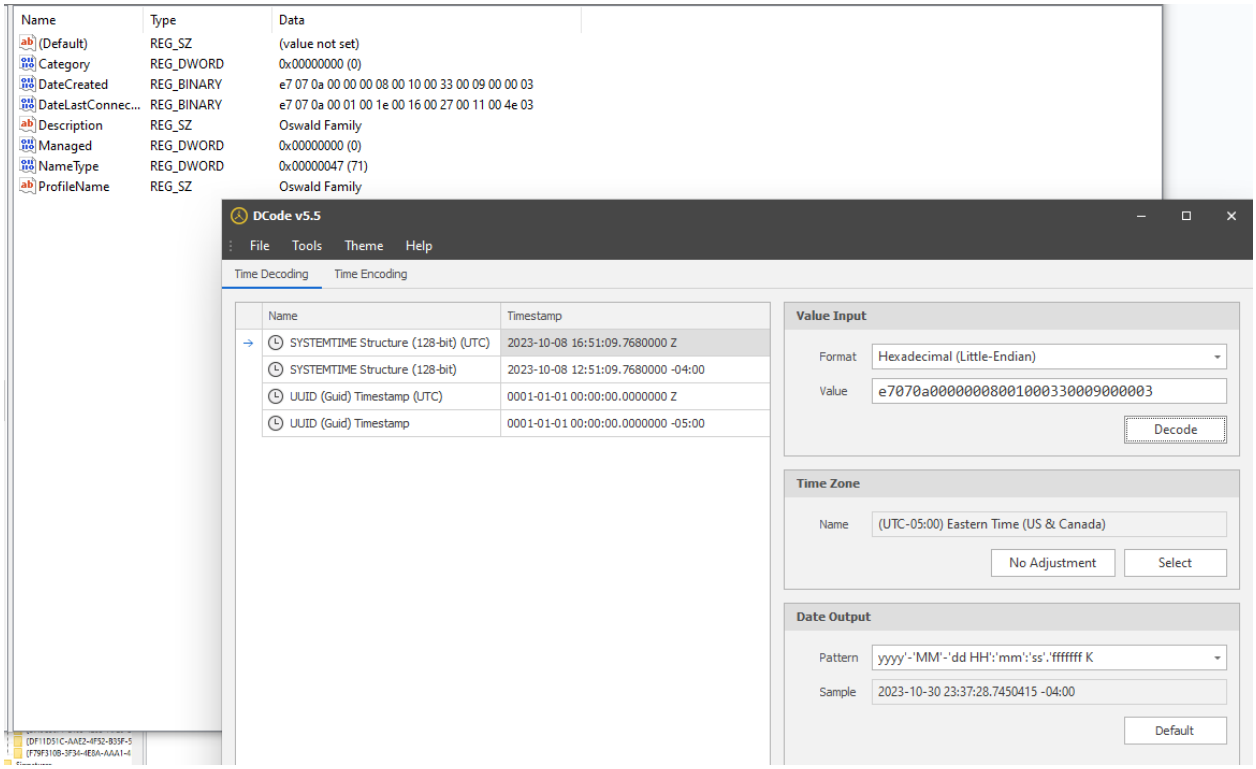
B.

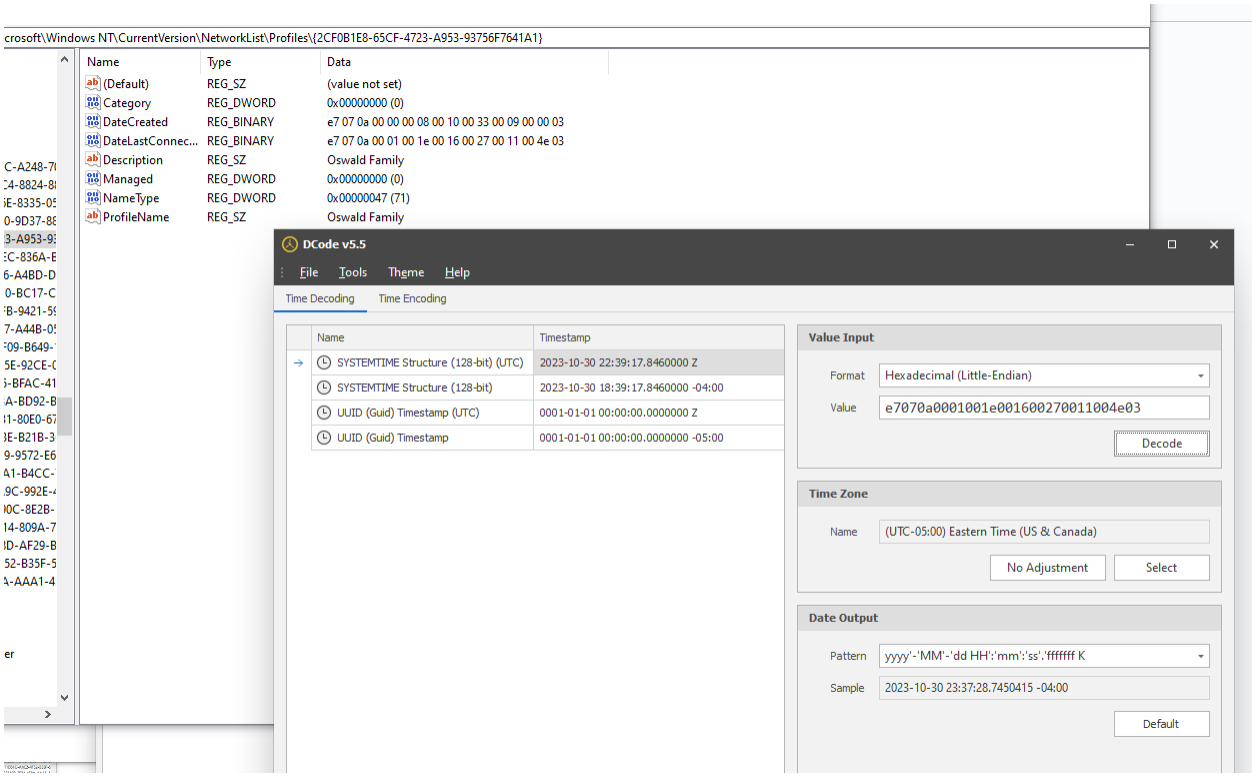
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{1A697866-3C35-461C-A248-70D6EC737D6E}

FirewallSync
NewNetworks
Nla
Permissions
Policies
Profiles
{1A697866-3C35-461C-A248-7(
{214A5BBC-67F4-47C4-8824-8
{23055E6A-8D65-4C6E-8335-0
{2C139C79-11F9-4220-9D37-8
{2CF0B1E8-65CF-4723-A953-9
{3ACBF2A8-5071-40EC-836A-E
{3BD41E34-3F03-4126-A4BD-D
{53ED57D3-8B07-4210-BC17-C
{5D16A736-30A3-47FB-9421-5
{6081AD4E-6275-4837-A44B-0
{6ADCAB8E-0C1C-4F09-B649-
{76CE7AD8-DEF5-4C5E-92CE-(
{8392684B-14EE-4995-BFAC-41
{895EEE56-81C8-4CBA-BD92-B
{8F9E2EEA-038A-4A31-80E0-67
{B37630C4-5DD8-443E-B21B-3
{B5B25022-92D1-4549-9572-E6
{BA53DFC4-6140-4BA1-B4CC-
{BFDE9A5A-2F2C-4A9C-992E-
{C8CD113A-A1A7-490C-8E2B-
{CC72A55D-90F3-4E14-809A-7
{DA6C36F1-E403-428D-AF29-B
{DF11D51C-AAE2-4F52-B35F-5
{F79F310B-3F34-4E8A-AAA1-4
Signatures
NolmeModelmes

Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	e7 07 01 00 05 00 06 00 0b 00 06 00 0f 00 2c 01
DateLastConnec...	REG_BINARY	e7 07 01 00 05 00 06 00 0b 00 06 00 0f 00 2e 01
Description	REG_SZ	SRIHER CAMPUS WIFI 1
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD	0x00000047 (71)
ProfileName	REG_SZ	SRIHER CAMPUS WIFI 1

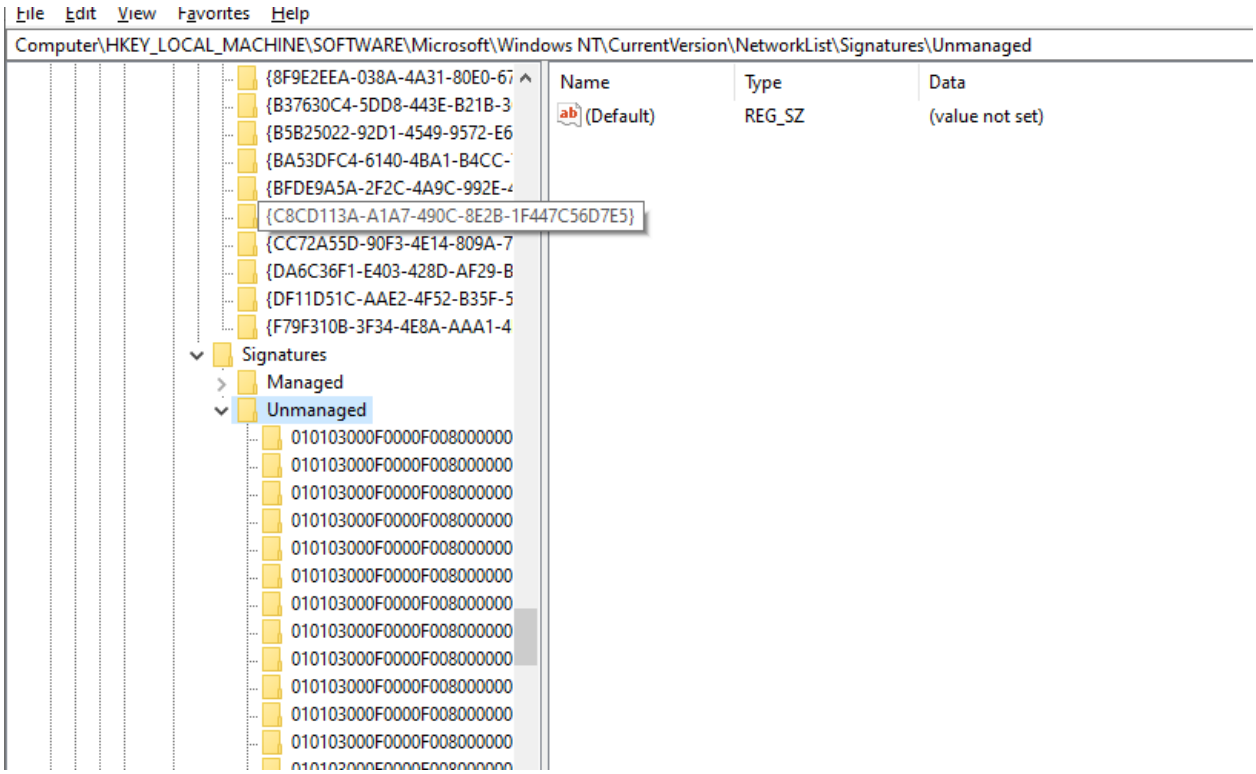
C.


Name Type Data
(Default) REG_SZ (value not set)
Category REG_DWORD 0x00000000 (0)
DateCreated REG_BINARY e7 07 0a 00 00 00 08 00 10 00 33 00 09 00 00 03
DateLastConnec... REG_BINARY e7 07 0a 00 01 00 1e 00 16 00 27 00 11 00 4e 03
Description REG_SZ Oswald Family
Managed REG_DWORD 0x00000000 (0)
NameType REG_DWORD 0x00000047 (71)
ProfileName REG_SZ Oswald Family
DCode v5.5
File Tools Theme Help
Time Decoding Time Encoding
Name Timestamp
SYSTEMTIME Structure (128-bit) (UTC) 2023-10-08 16:51:09.7680000 Z
SYSTEMTIME Structure (128-bit) 2023-10-08 12:51:09.7680000 -04:00
UUID (Guid) Timestamp (UTC) 0001-01-01 00:00:00.0000000 Z
UUID (Guid) Timestamp 0001-01-01 00:00:00.0000000 -05:00
Value Input
Format Hexadecimal (Little-Endian)
Value e7070a0000000800100033000900000 3
Decode
Time Zone
Name (UTC-05:00) Eastern Time (US & Canada)
No Adjustment Select
Date Output
Pattern yyyy'-'MM'-'dd HH':'mm':'ss'.'fffffff K
Sample 2023-10-30 23:37:28.7450415 -04:00
Default

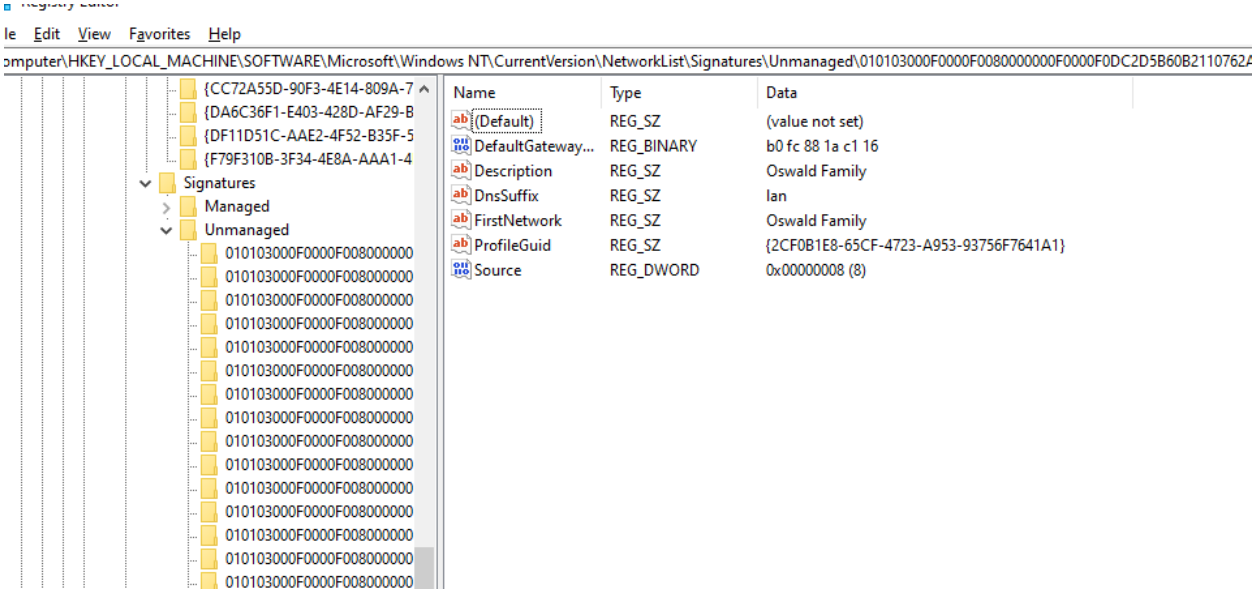

crosoft\Windows NT\CurrentVersion\NetworkList\Profiles\{2CF0B1E8-65CF-4723-A953-93756F7641A1}
Name Type Data
(Default) REG_SZ (value not set)
Category REG_DWORD 0x00000000 (0)
DateCreated REG_BINARY e7 07 0a 00 00 00 08 00 10 00 33 00 09 00 00 03
DateLastConnec... REG_BINARY e7 07 0a 00 01 00 1e 00 16 00 27 00 11 00 4e 03
Description REG_SZ Oswald Family
Managed REG_DWORD 0x00000000 (0)
NameType REG_DWORD 0x00000047 (71)
ProfileName REG_SZ Oswald Family
DCode v5.5
File Tools Theme Help
Time Decoding Time Encoding
Name Timestamp
SYSTEMTIME Structure (128-bit) (UTC) 2023-10-30 22:39:17.8460000 Z
SYSTEMTIME Structure (128-bit) 2023-10-30 18:39:17.8460000 -04:00
UUID (Guid) Timestamp (UTC) 0001-01-01 00:00:00.0000000 Z
UUID (Guid) Timestamp 0001-01-01 00:00:00.0000000 -05:00
Value Input
Format Hexadecimal (Little-Endian)
Value e7070a0001001e00160027001 1004e03
Decode
Time Zone
Name (UTC-05:00) Eastern Time (US & Canada)
No Adjustment Select
Date Output
Pattern yyyy'-'MM'-'dd HH':'mm':'ss'.'fffffff K
Sample 2023-10-30 23:37:28.7450415 -04:00
Default

D.
These wifi connections and information like last connected are very useful to understand about and store evidence on particular ssid, if we come to find it has any issues or caused any incident, it will be great practice for collecting evidence and reverse engineering the problem.

Step 2 :
A.

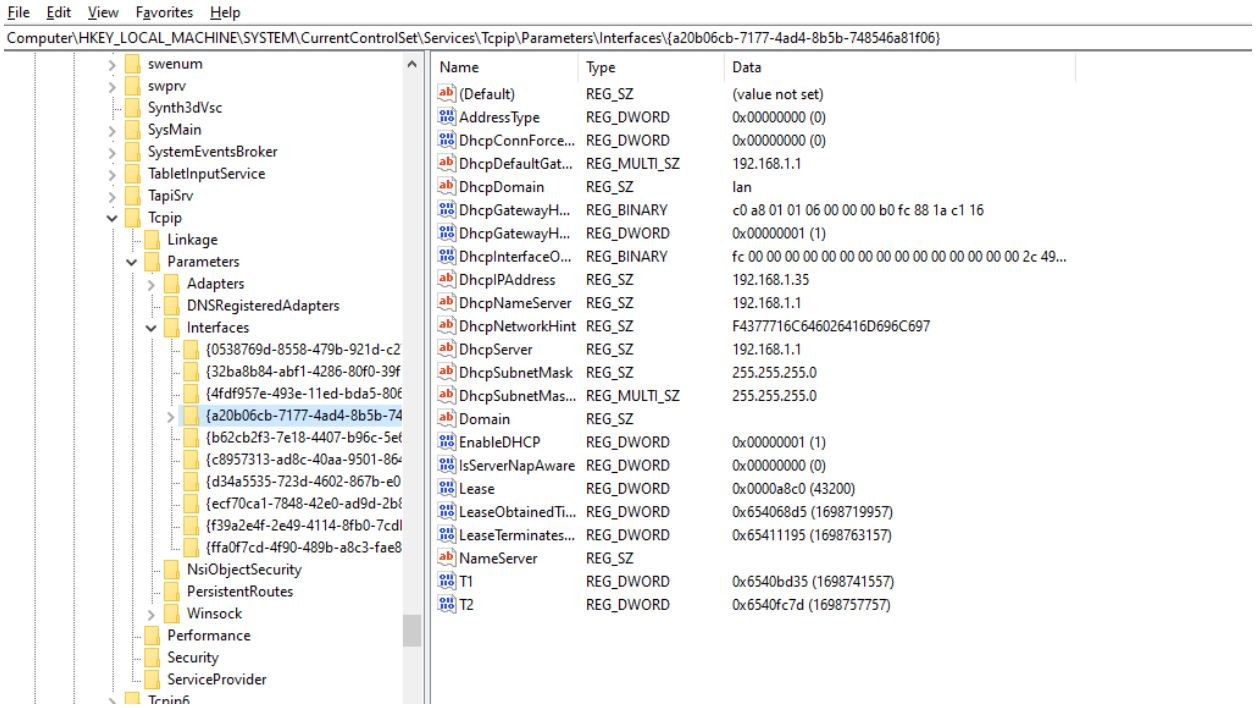


B.

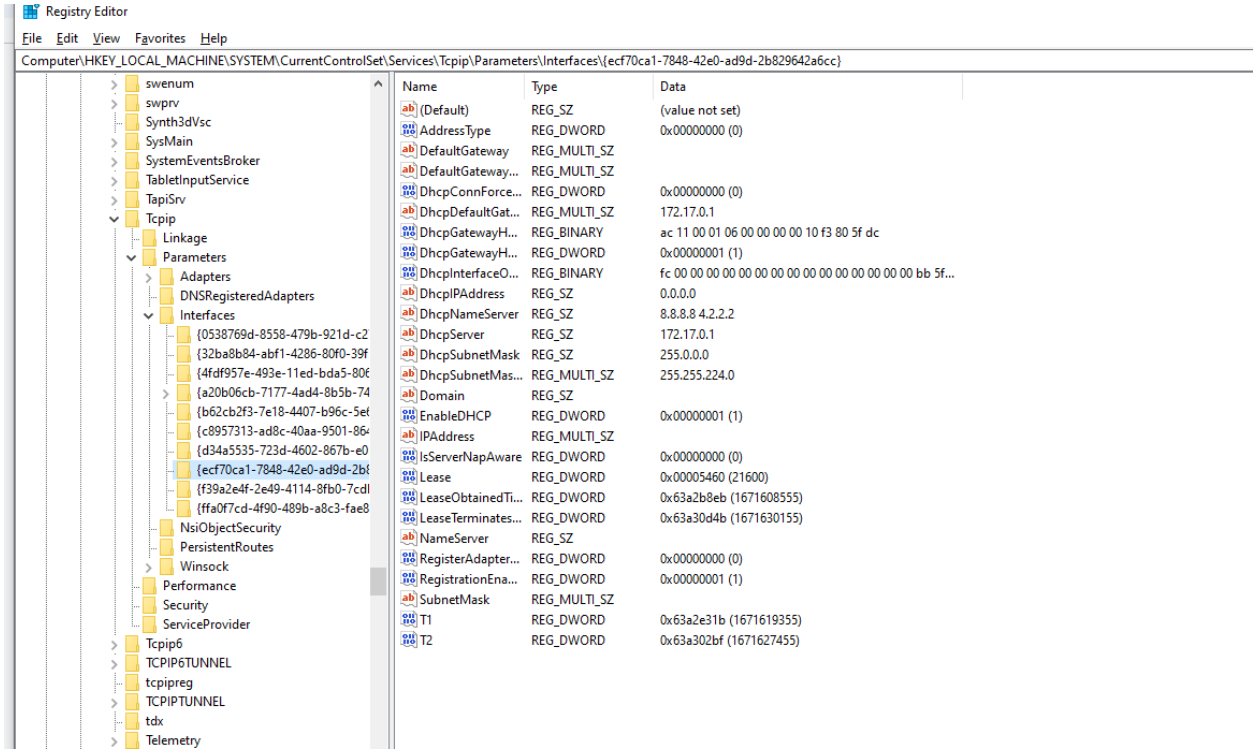


C.
It will be a evidence for mentioning of this device and ensuring that this device is the device that affected and participated in the incident. This evidence will be strong as mac address are unique for each device.

Step 3 :
A.



B.

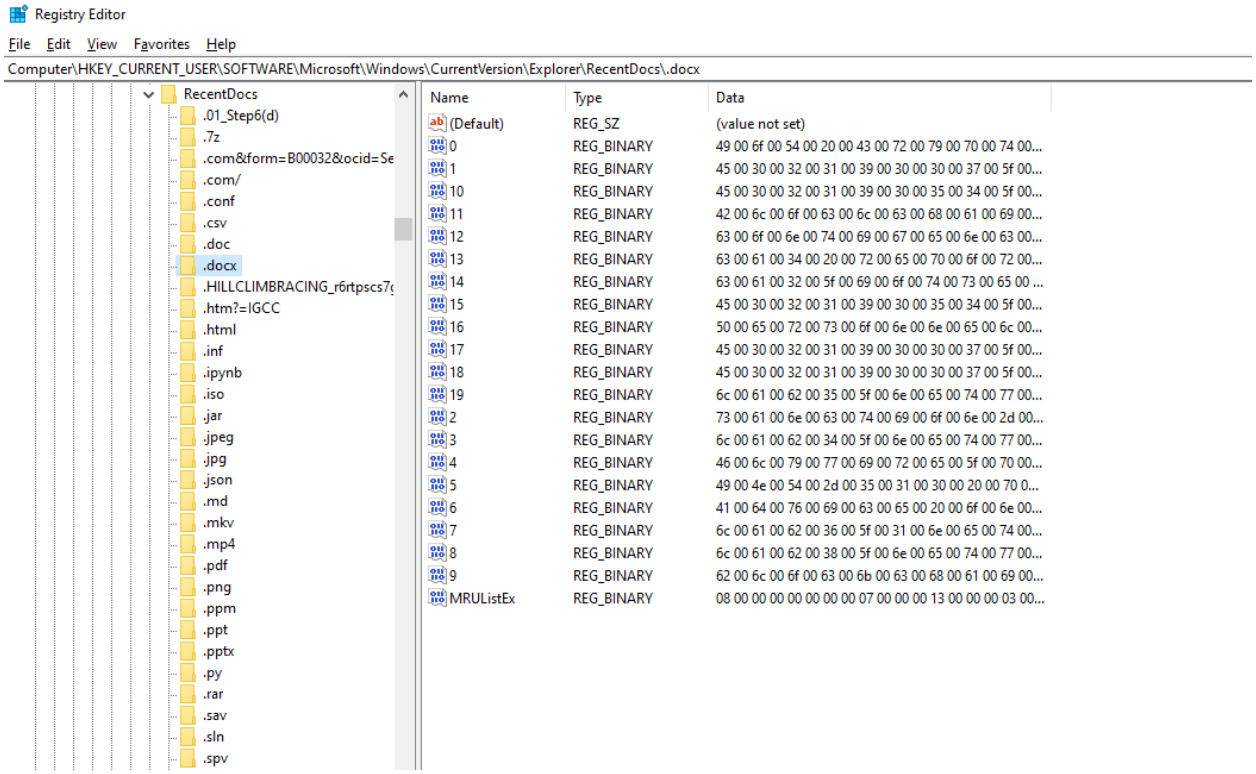


C.

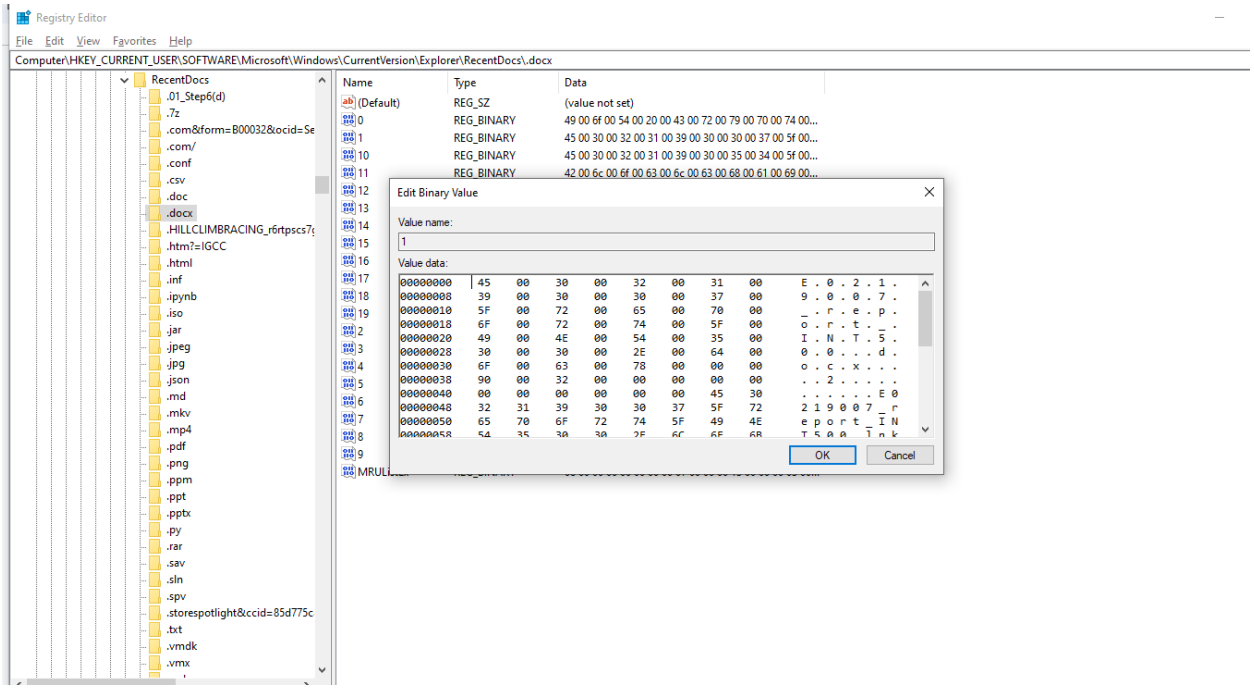
This collects all the network information and it would be helpful for collecting evidence on network related incidents.

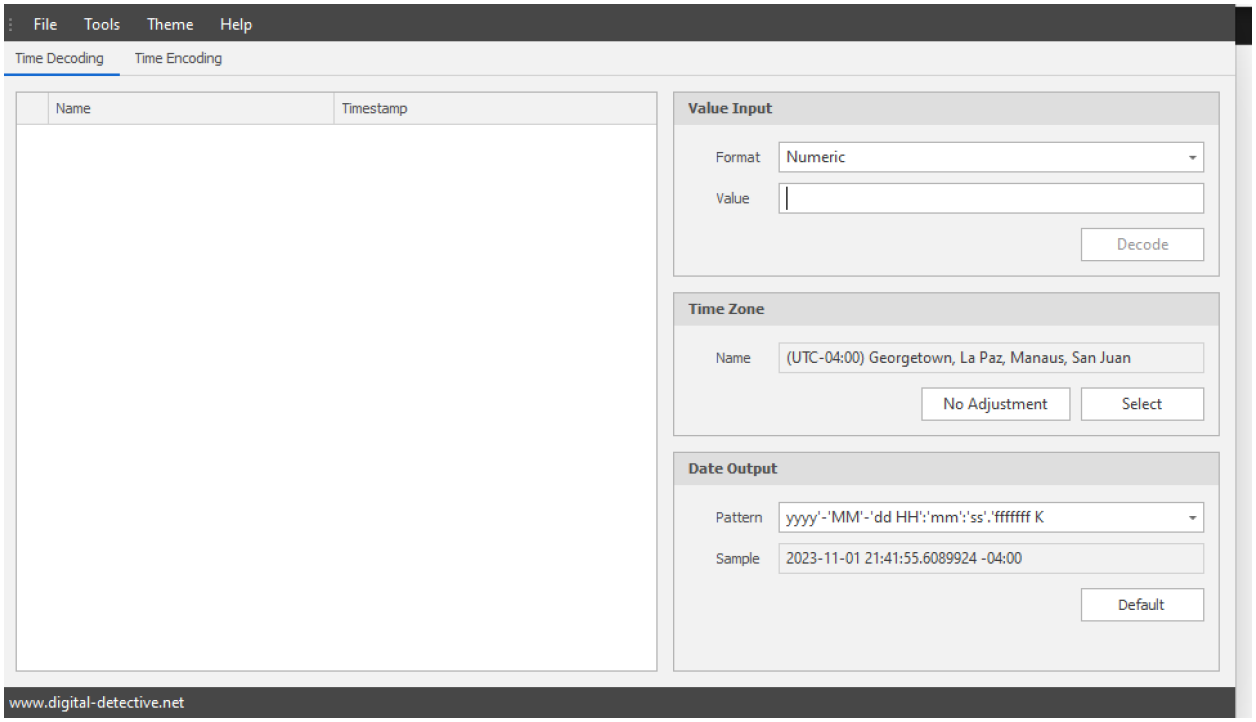
Step 4 :

A.

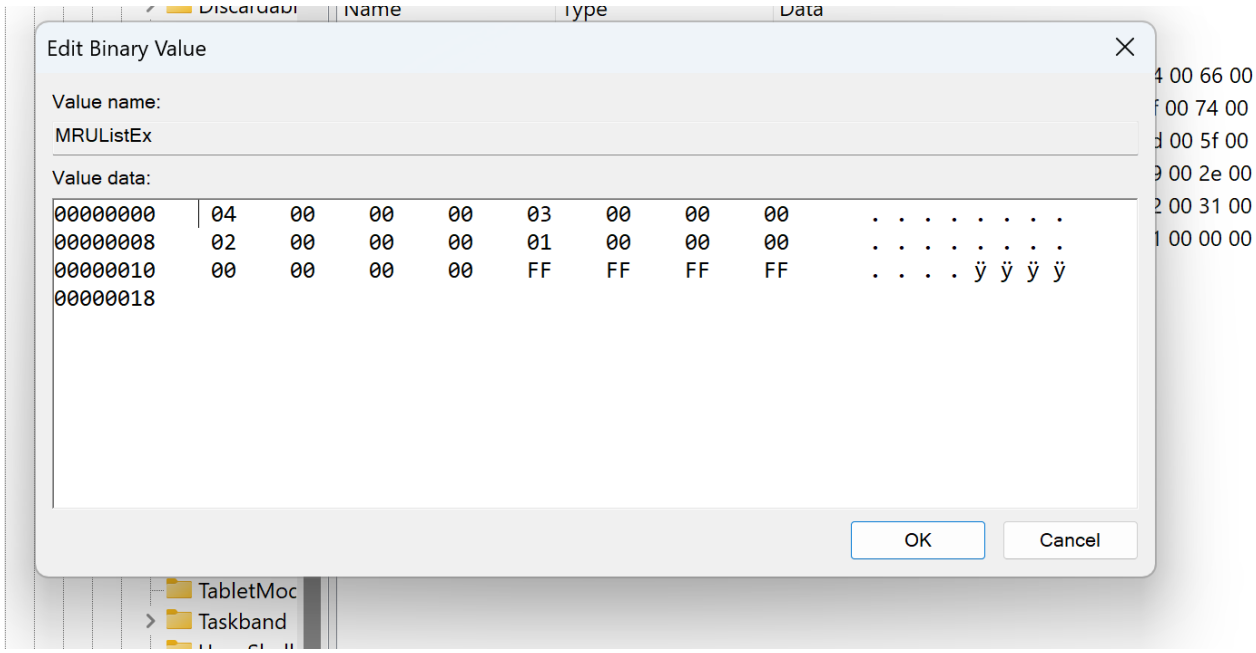

Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
RecentDocs
.01_Step6(d)
.7z
.com&form=B00032&ocid=Se
.com/
.conf
.csv
.doc
.docx
.HILLCLIMBRACING_r6rtpscs7
.htm?=IGCC
.html
.inf
.ipynb
.iso
.jar
.jpeg
.jpg
.json
.md
.mkv
.mp4
.pdf
.png
.ppm
.ppt
.pptx
.py
.rar
.sav
.sln
.spv
Name Type Data
(Default) REG_SZ (value not set)
0 REG_BINARY 49 00 6f 00 54 00 20 00 43 00 72 00 79 00 70 00 74 00...
1 REG_BINARY 45 00 30 00 32 00 31 00 39 00 30 00 30 00 37 00 5f 00...
10 REG_BINARY 45 00 30 00 32 00 31 00 39 00 30 00 35 00 34 00 5f 00...
11 REG_BINARY 42 00 6c 00 6f 00 63 00 6c 00 63 00 68 00 61 00 69 00...
12 REG_BINARY 63 00 6f 00 6e 00 74 00 69 00 67 00 65 00 6e 00 63 00...
13 REG_BINARY 63 00 61 00 34 00 20 00 72 00 65 00 70 00 6f 00 72 00...
14 REG_BINARY 63 00 61 00 32 00 5f 00 69 00 6f 00 74 00 73 00 65 00 ...
15 REG_BINARY 45 00 30 00 32 00 31 00 39 00 30 00 35 00 34 00 5f 00...
16 REG_BINARY 50 00 65 00 72 00 73 00 6f 00 6e 00 6e 00 65 00 6c 00...
17 REG_BINARY 45 00 30 00 32 00 31 00 39 00 30 00 30 00 37 00 5f 00...
18 REG_BINARY 45 00 30 00 32 00 31 00 39 00 30 00 30 00 37 00 5f 00...
19 REG_BINARY 6c 00 61 00 62 00 35 00 5f 00 6e 00 65 00 74 00 77 00...
2 REG_BINARY 73 00 61 00 6e 00 63 00 74 00 69 00 6f 00 6e 00 2d 00...
3 REG_BINARY 6c 00 61 00 62 00 34 00 5f 00 6e 00 65 00 74 00 77 00...
4 REG_BINARY 46 00 6c 00 79 00 77 00 69 00 72 00 65 00 5f 00 70 00...
5 REG_BINARY 49 00 4e 00 54 00 2d 00 35 00 31 00 30 00 20 00 70 0...
6 REG_BINARY 41 00 64 00 76 00 69 00 63 00 65 00 20 00 6f 00 6e 00...
7 REG_BINARY 6c 00 61 00 62 00 36 00 5f 00 31 00 6e 00 65 00 74 00...
8 REG_BINARY 6c 00 61 00 62 00 38 00 5f 00 6e 00 65 00 74 00 77 00...
9 REG_BINARY 62 00 6c 00 6f 00 63 00 6b 00 63 00 68 00 61 00 69 00...
MRUListEx REG_BINARY 08 00 00 00 00 00 00 00 07 00 00 00 13 00 00 00 03 00...

B.


Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx
Edit Binary Value
Value name:
1
Value data:
00000000 45 00 30 00 32 00 31 00 E . 0 . 2 . 1 .
00000008 39 00 30 00 30 00 37 00 9 . 0 . 0 . 7 .
00000010 5F 00 72 00 65 00 70 00 _ . r . e . p .
00000018 6F 00 72 00 74 00 5F 00 o . r . t . _ .
00000020 49 00 4E 00 54 00 35 00 I . N . T . 5 .
00000028 30 00 30 00 2E 00 64 00 0 . 0 . . . d .
00000030 6F 00 63 00 78 00 00 00 o . c . x . . .
00000038 90 00 32 00 00 00 00 00 . . 2 . . . . .
00000040 00 00 00 00 00 00 45 30 . . . . . E 0
00000048 32 31 39 30 30 37 5F 72 2 1 9 0 0 7 _ r
00000050 65 70 6F 72 74 5F 49 4E e p o r t _ I N
OK
Cancel

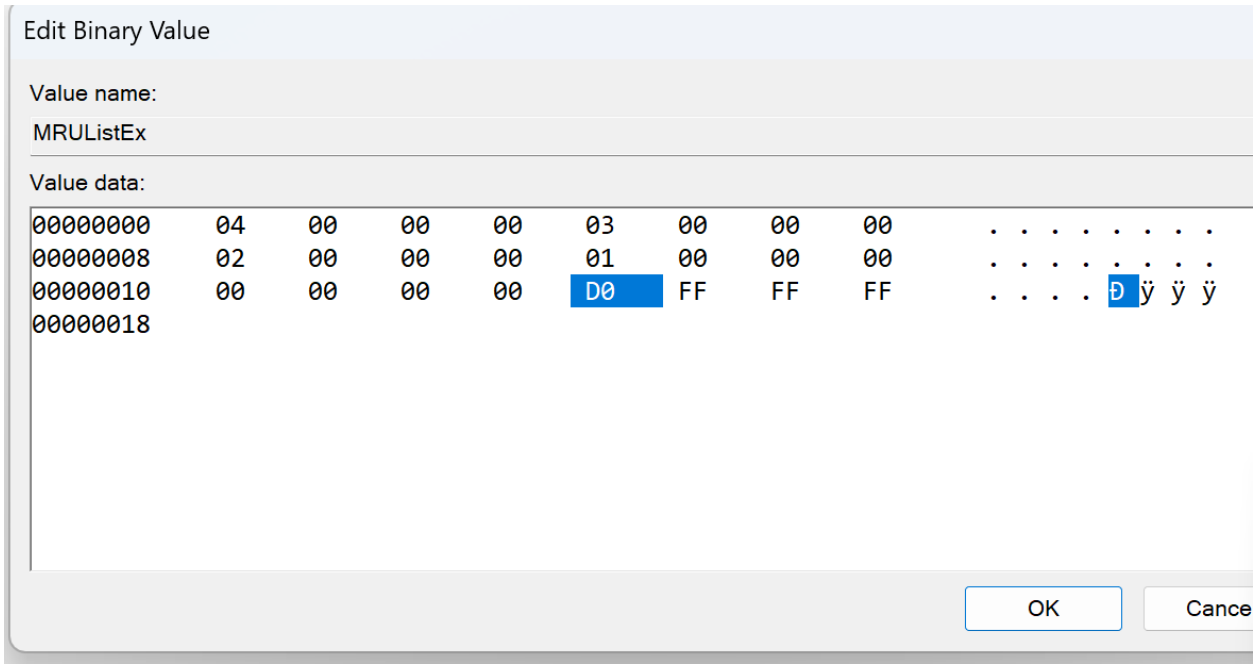

File
Tools
Theme
Help
Time Decoding
Time Encoding
Name
Timestamp
Value Input
Format
Numeric
Value
Decode
Time Zone
Name
(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
No Adjustment
Select
Date Output
Pattern
yyyy'-'MM'-'dd HH':'mm':'ss'.'fffffff K
Sample
2023-11-01 21:41:55.6089924 -04:00
Default
www.digital-detective.net

C.

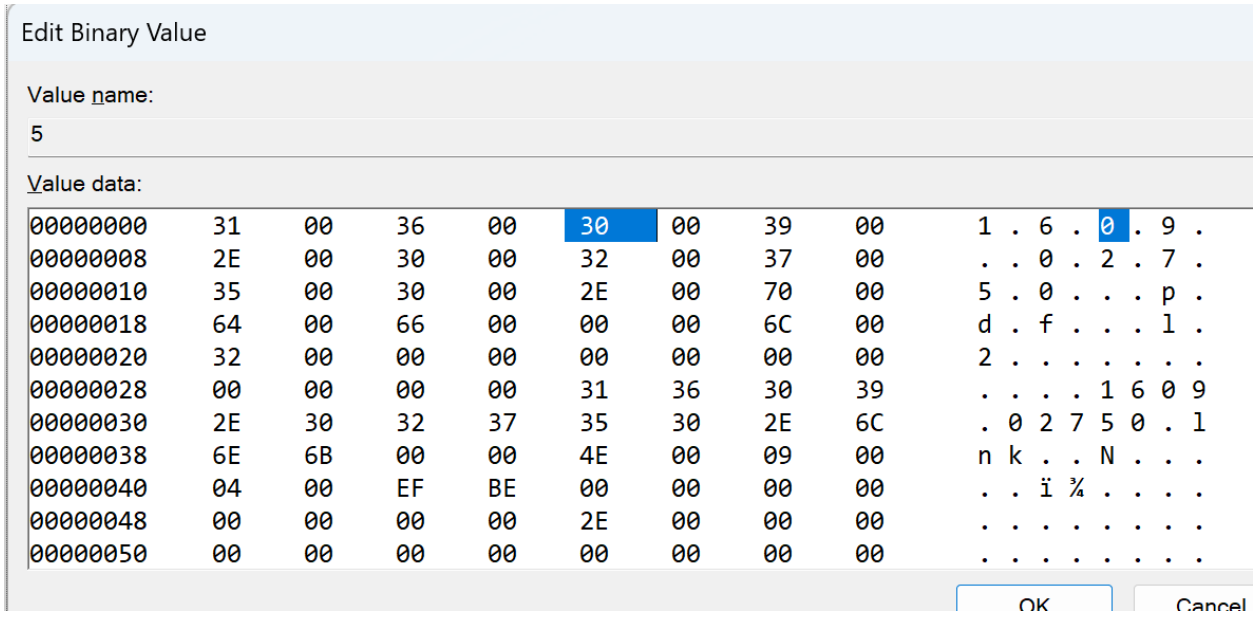

Edit Binary Value
Value name:
MRUListEx
Value data:
00000000 04 00 00 00 03 00 00 00 . . . . . .
00000008 02 00 00 00 01 00 00 00 . . . . . .
00000010 00 00 00 00 FF FF FF FF . . . . ÿ ÿ ÿ ÿ
00000018
OK
Cancel
TabletMoc
Taskband

D.

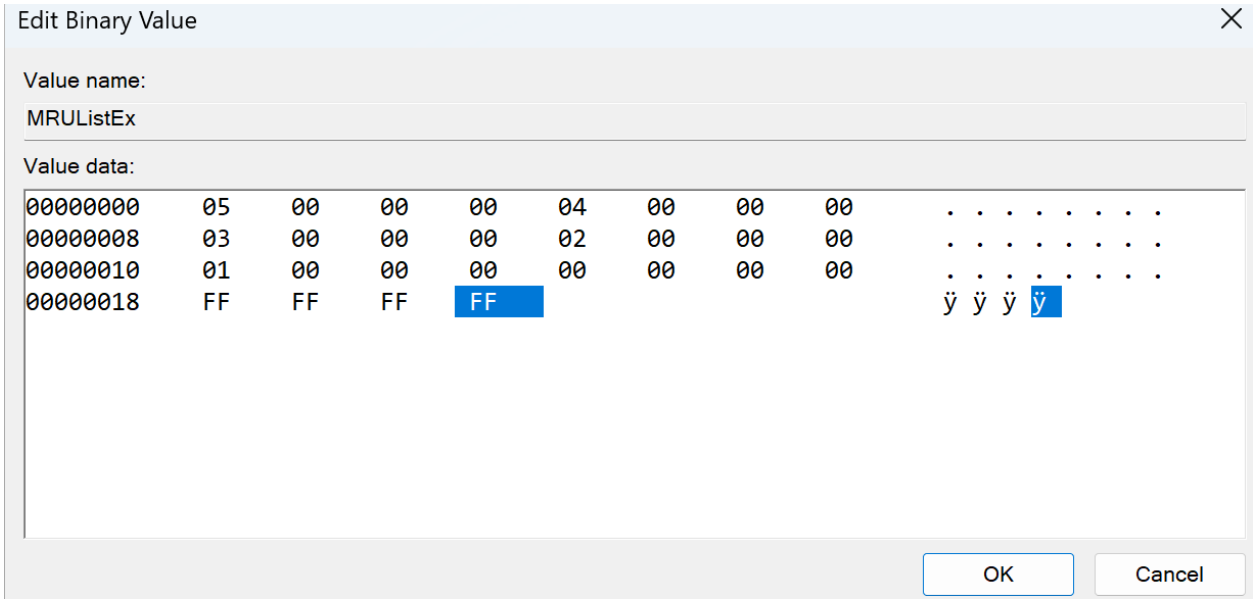
Recent file i worked on



E.



FF is 30 :

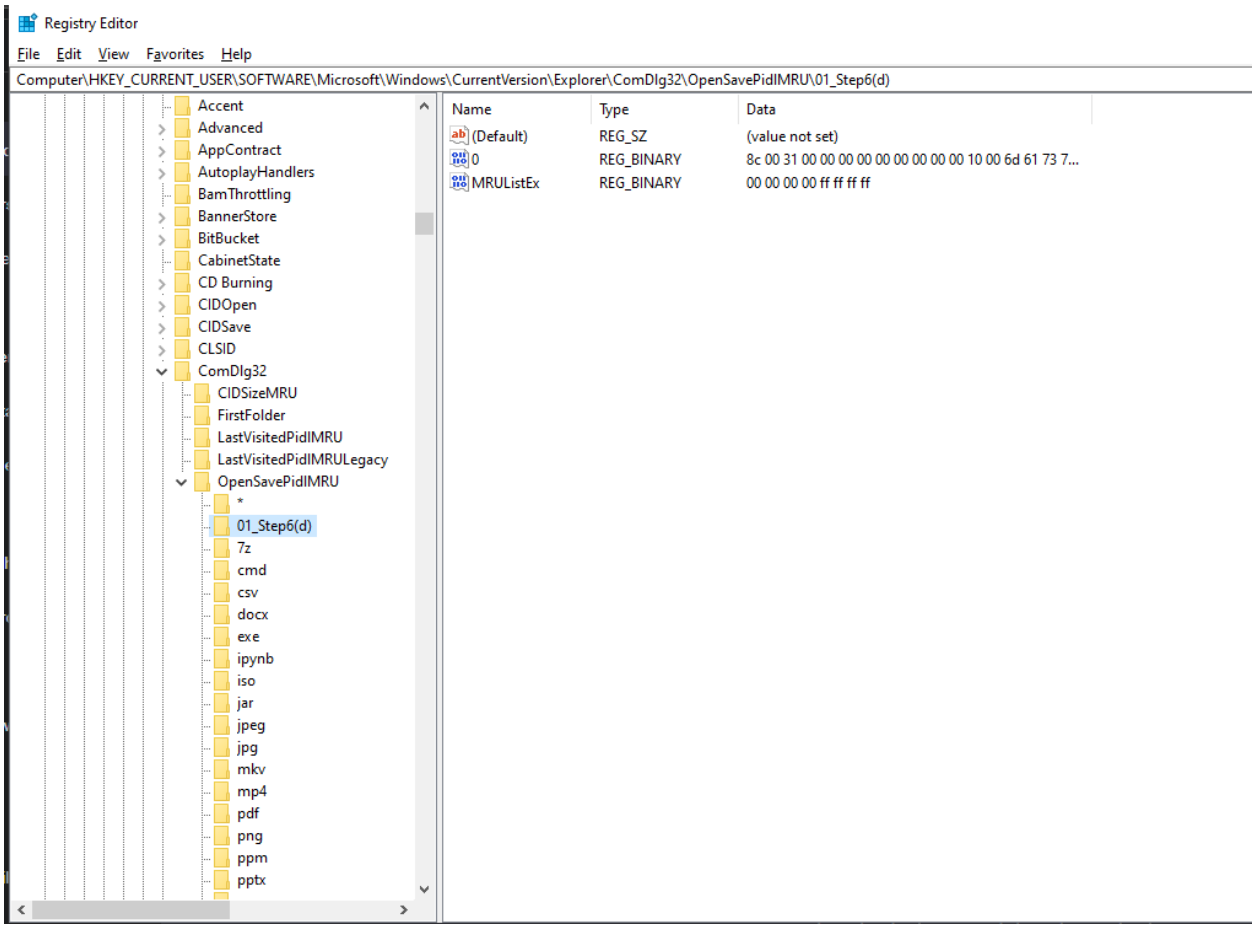


F.

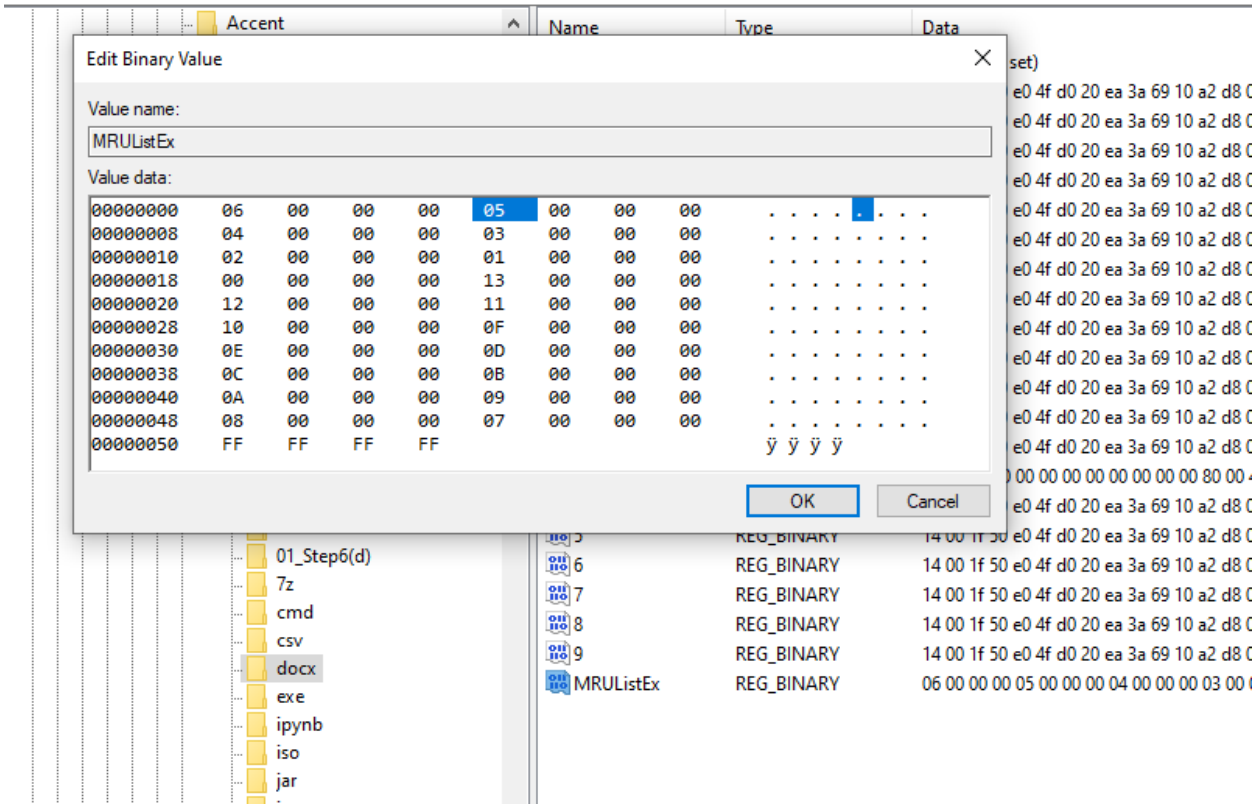
We can track down which file ran and which file was modified by the attacker in case he accessed the file. It will be helpful for us to know which recent file has been ran.

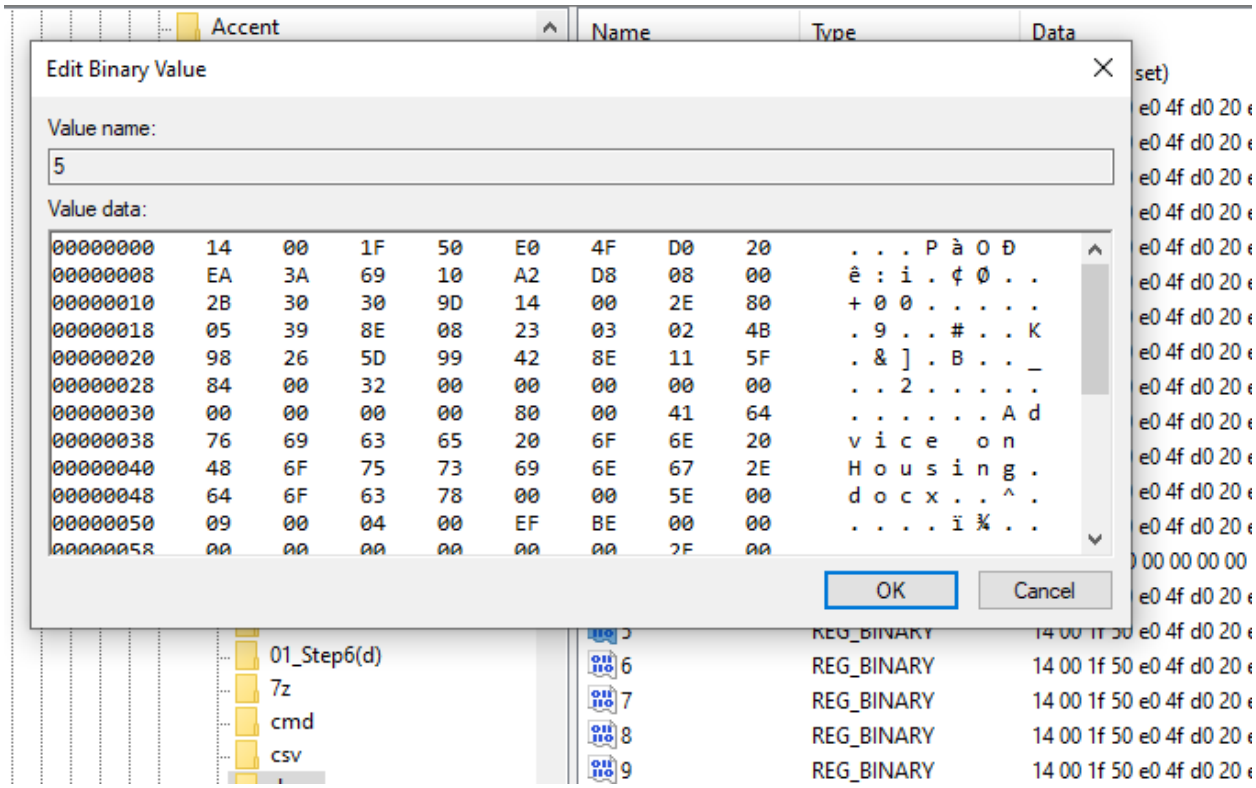
Step 5 :

A.


Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\01_Step6(d)
Accent
Advanced
AppContract
AutoplayHandlers
BamThrottling
BannerStore
BitBucket
CabinetState
CD Burning
CIDOpen
CIDSave
CLSID
ComDlg32
CIDSizeMRU
FirstFolder
LastVisitedPidlMRU
LastVisitedPidlMRULegacy
OpenSavePidlMRU
*
01_Step6(d)
7z
cmd
csv
docx
exe
ipynb
iso
jar
jpeg
jpg
mkv
mp4
pdf
png
ppm
pptx
Name
Type
Data
(Default)
REG_SZ
(value not set)
0
REG_BINARY
8c 00 31 00 00 00 00 00 00 00 00 00 10 00 6d 61 73 7...
MRUListEx
REG_BINARY
00 00 00 00 ff ff ff ff

B.

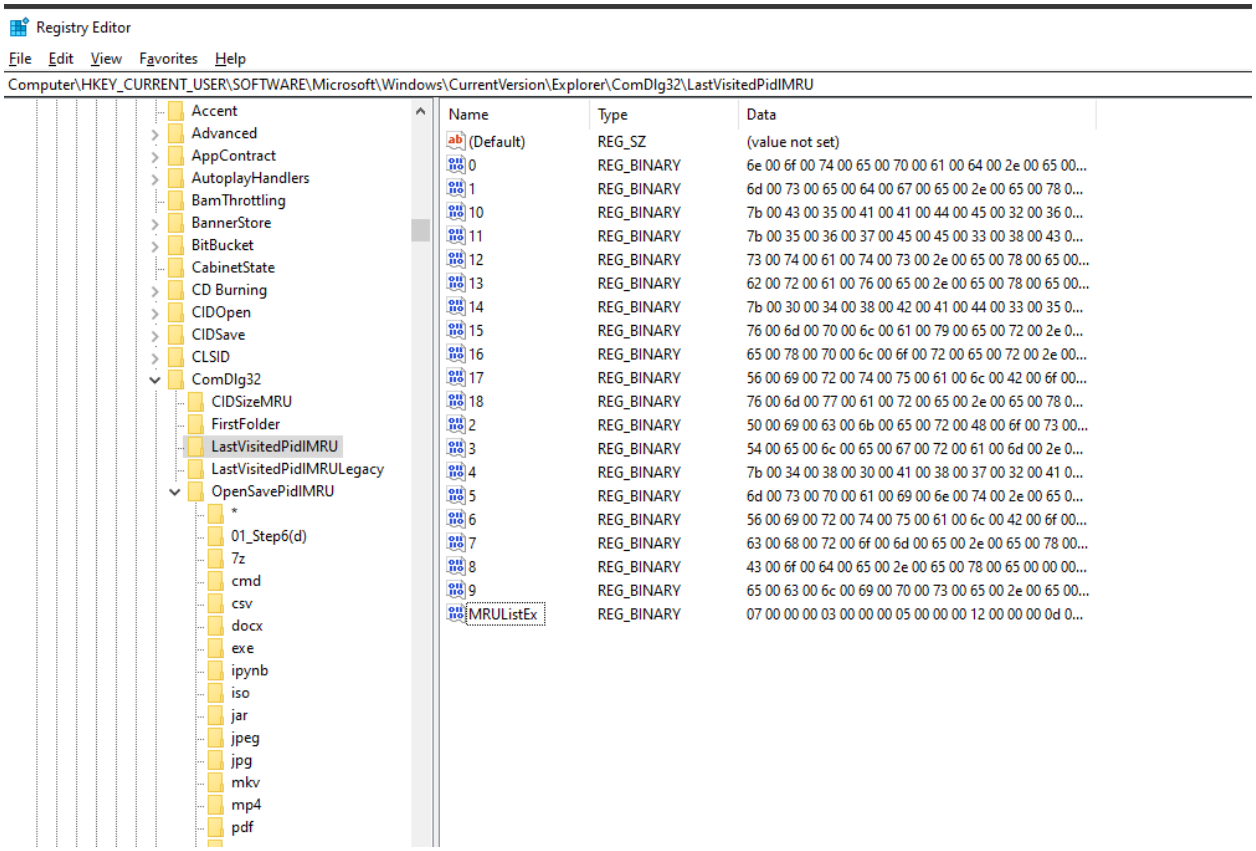




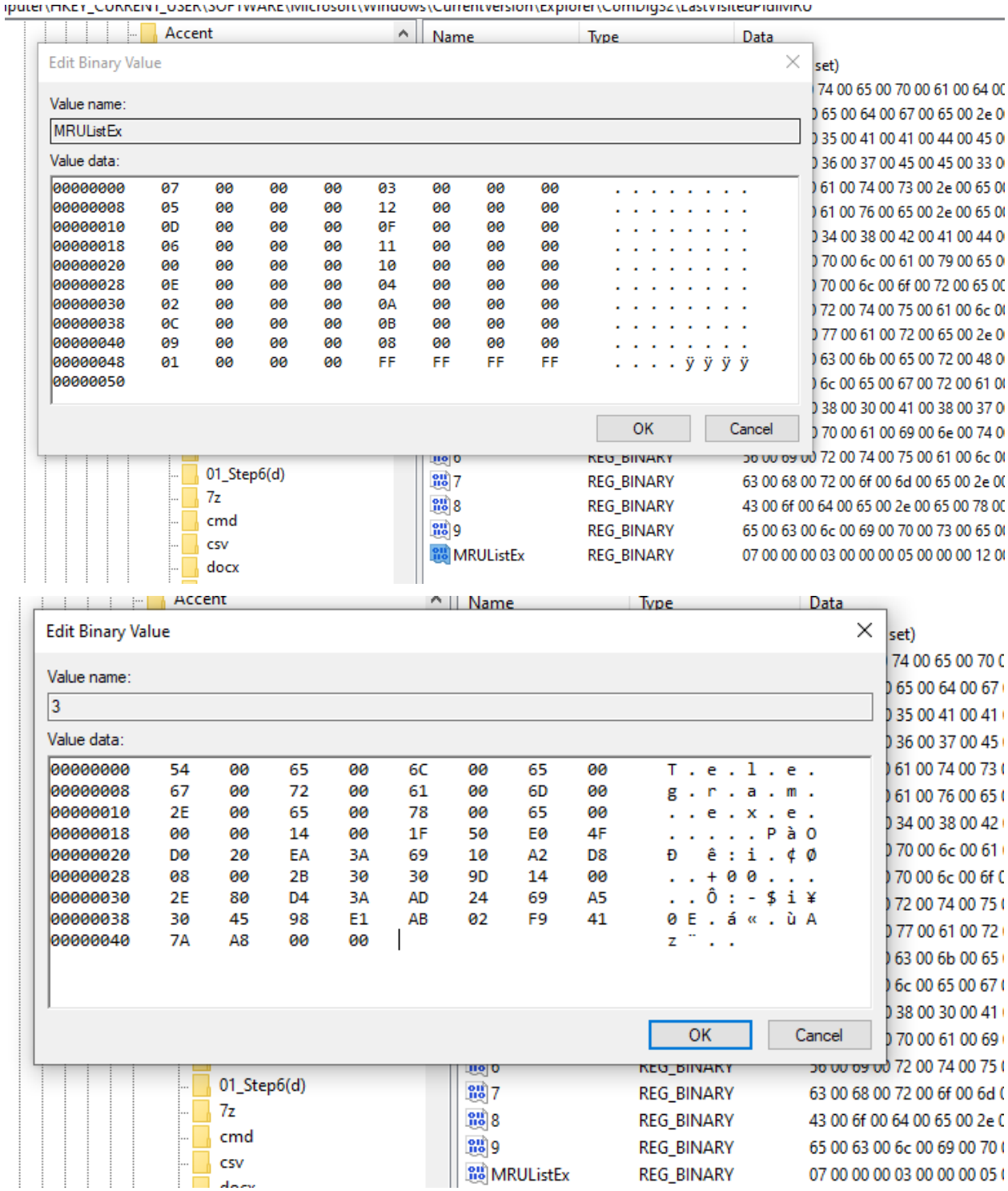
This is the recent file opened.

C.
This is highly useful for collecting evidence for recently modified or affected file. While collecting the evidence for analysing recent docs which is critical.

Step 6 :
A.



B.

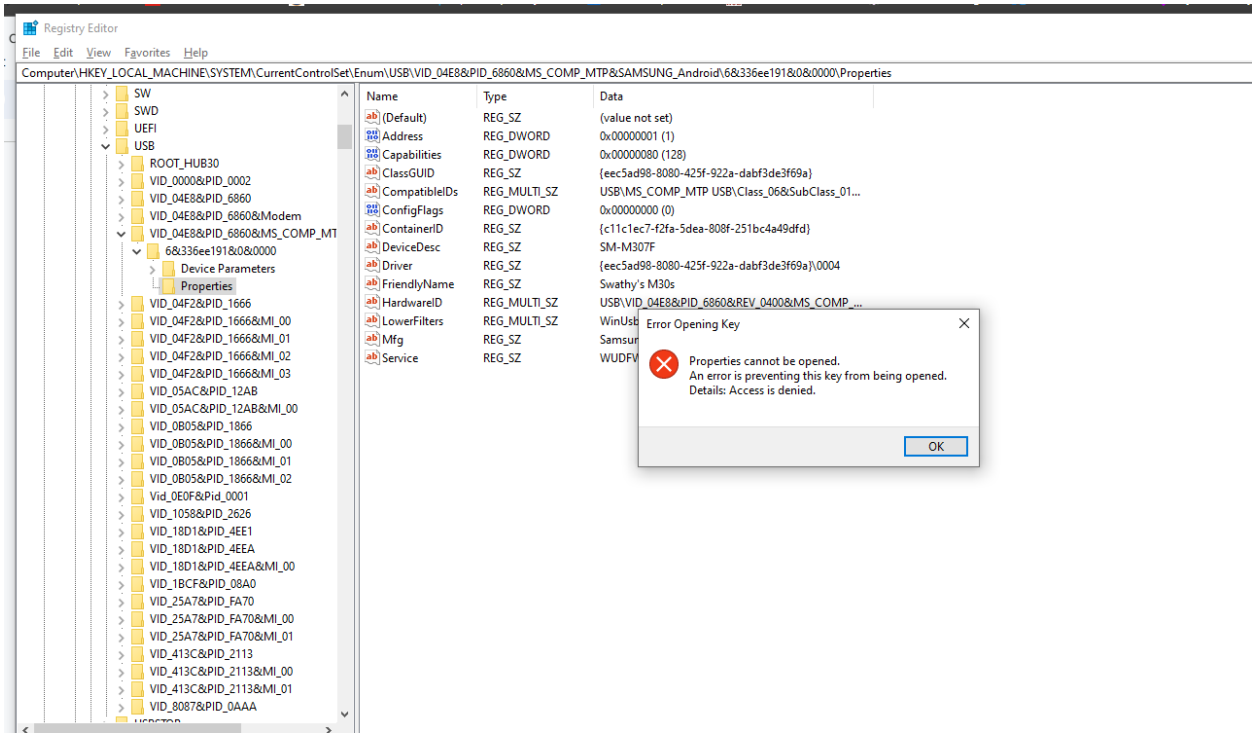


C.

We can find evidence like whether the file is copied or transferred to another location, which means stealing of the file or data is happened. We can record this incident in this way.

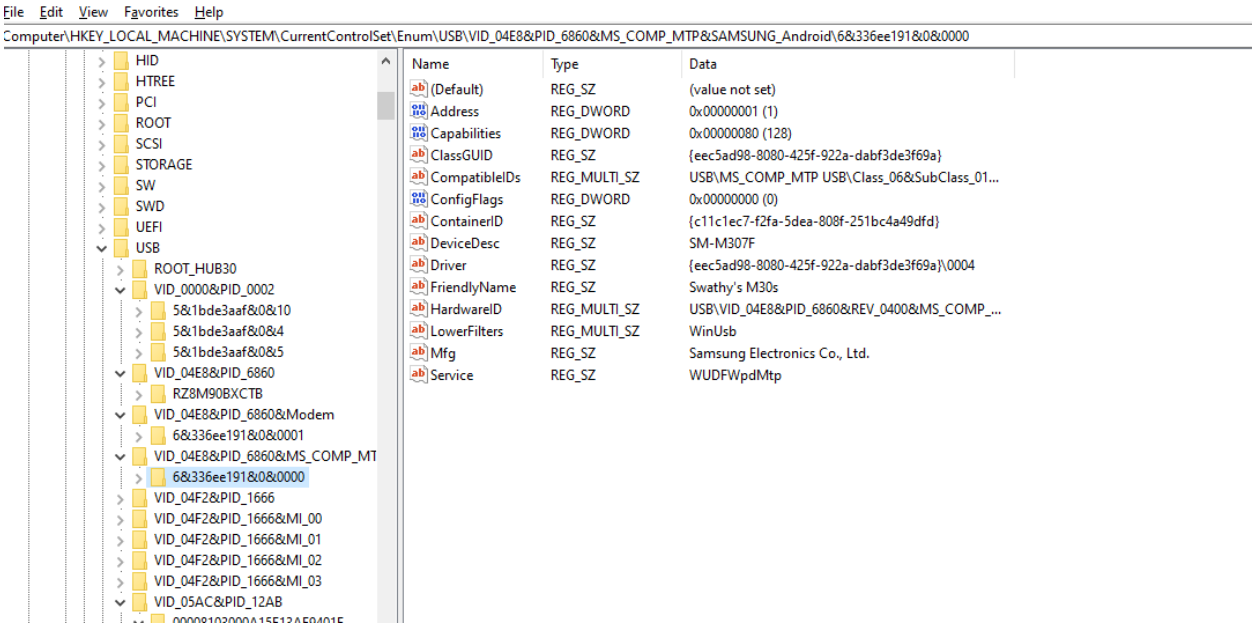
Step 7 :

A.



B.

This device is plugged into my system

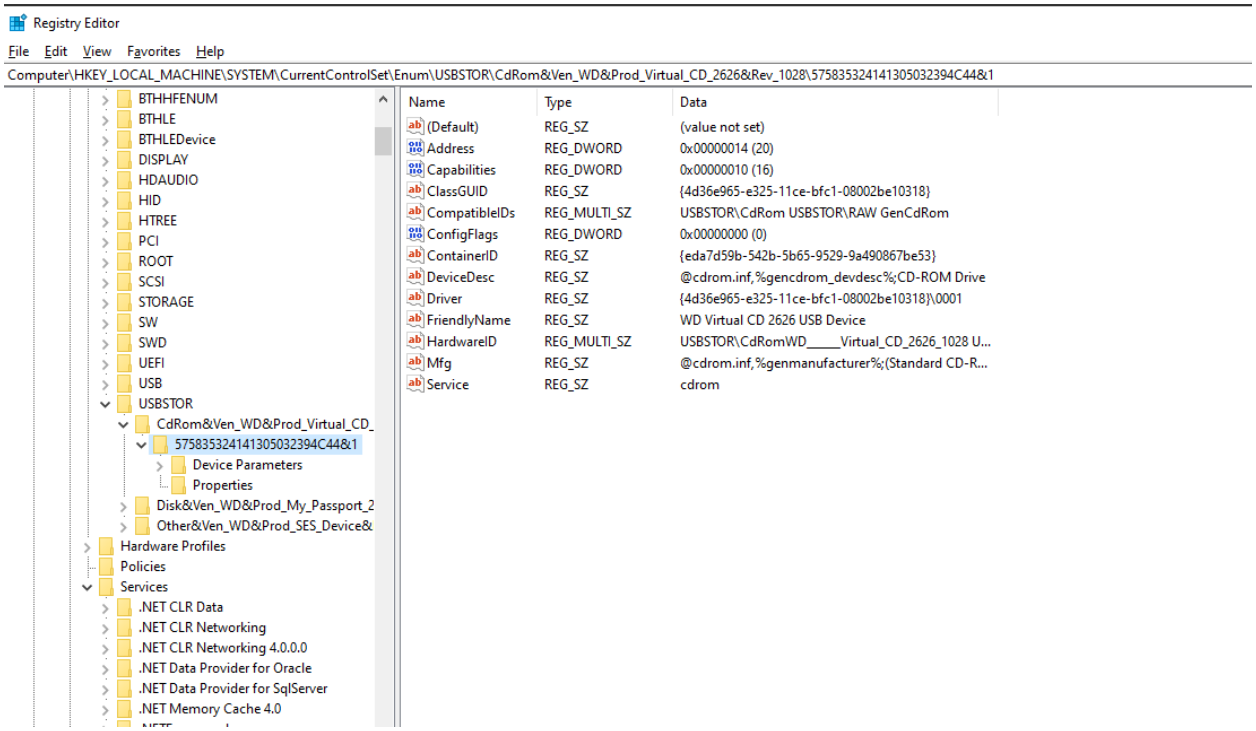


C.

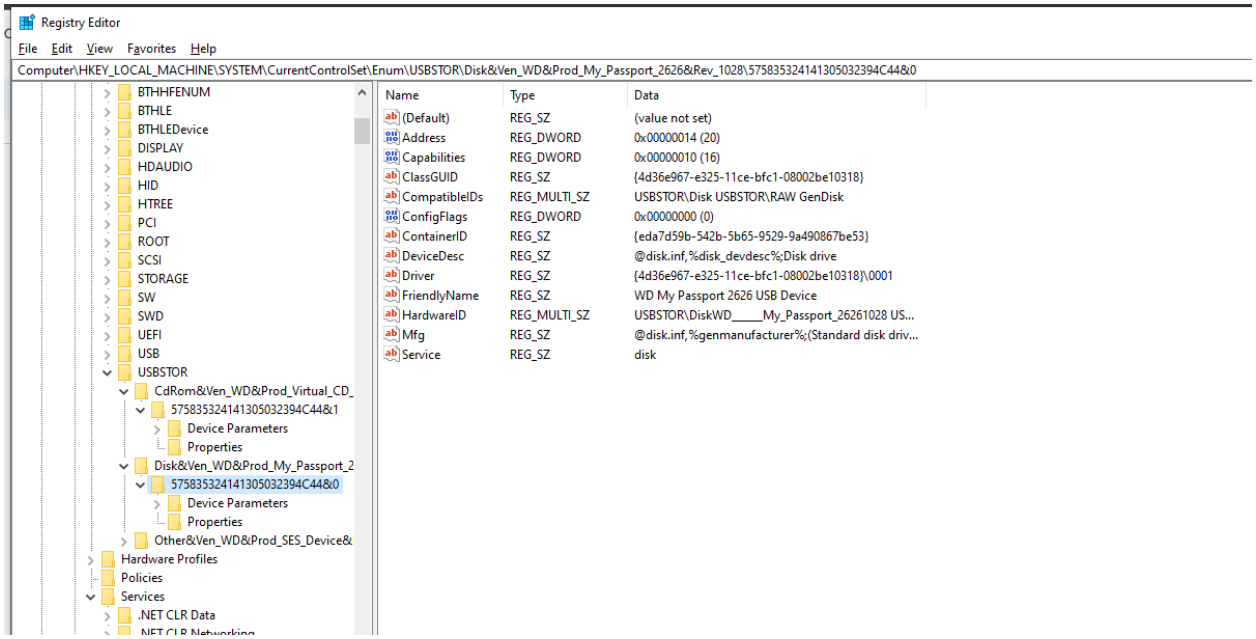
We can trace back and find evidence about the external device that has been connected to the system, if it is not a relative or friendly device, we can have it as the evidence.and we can know the hardware of the device connected.

Step 8 :

A.



B.



This is the harddisk i connected to my laptop, i found it through the name.

C.

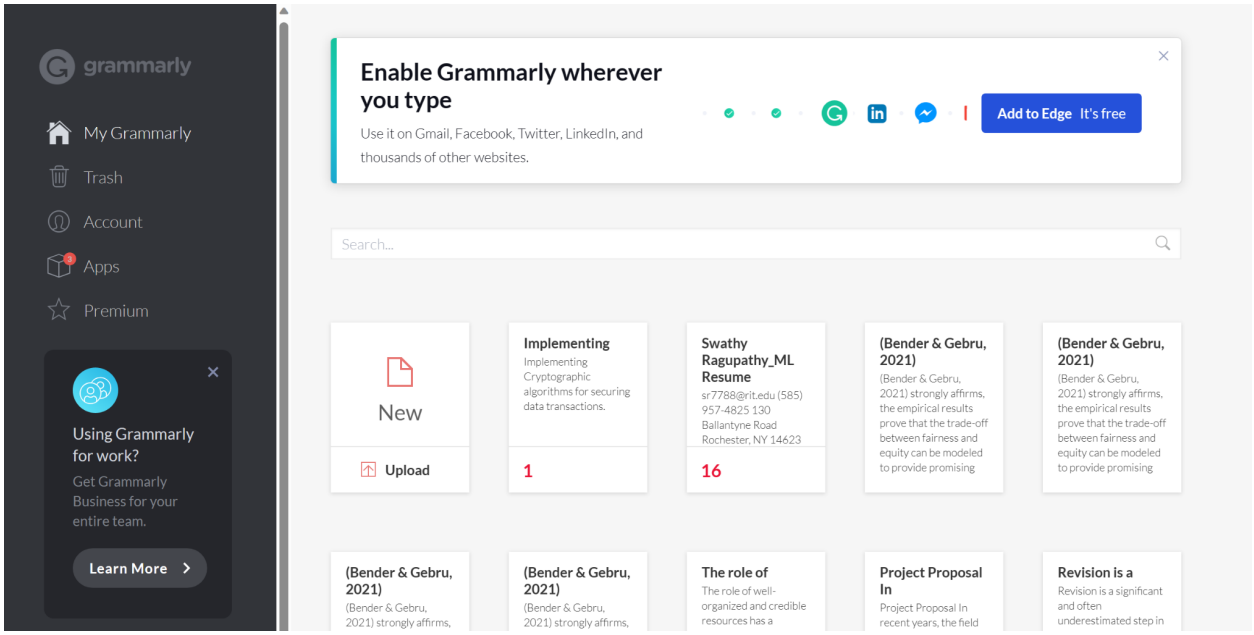
It is very useful for knowing the external bus drivers that been connected, any infected usb devices may be connected to the system.

Exercise 23. 02 :

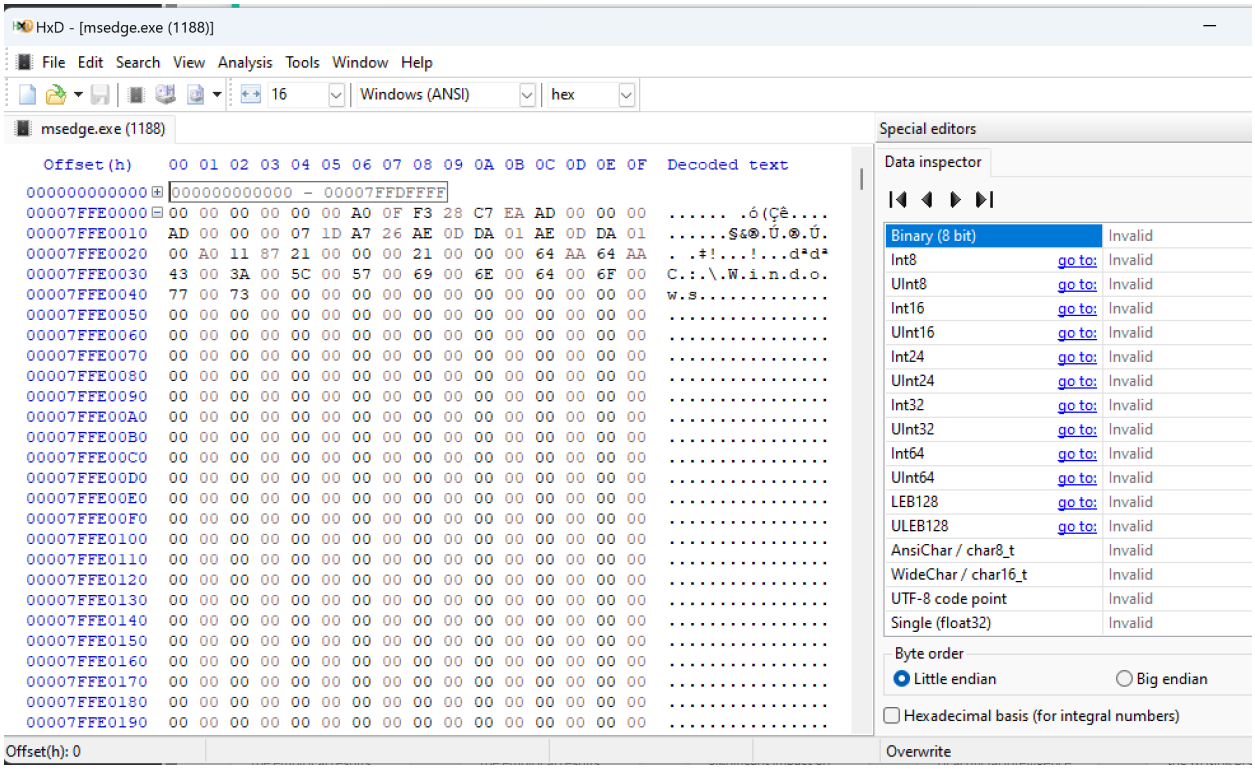
Step 1 :

A.

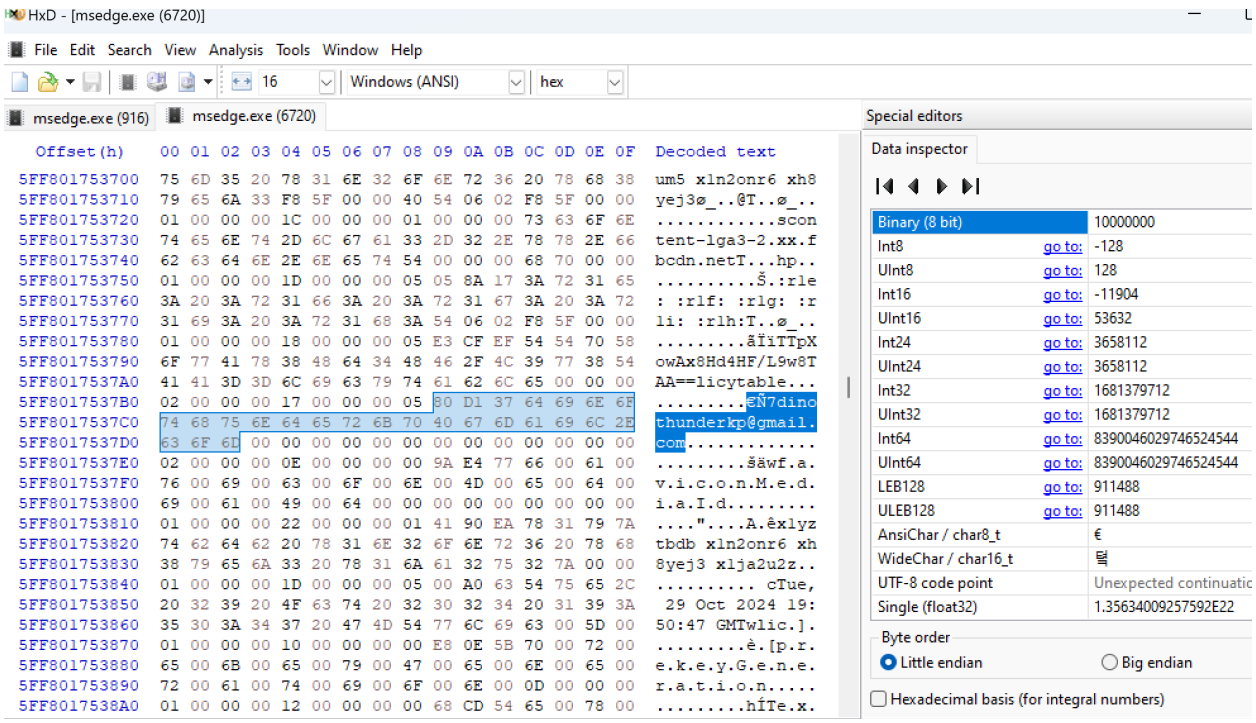
I logged into grammarly



B.

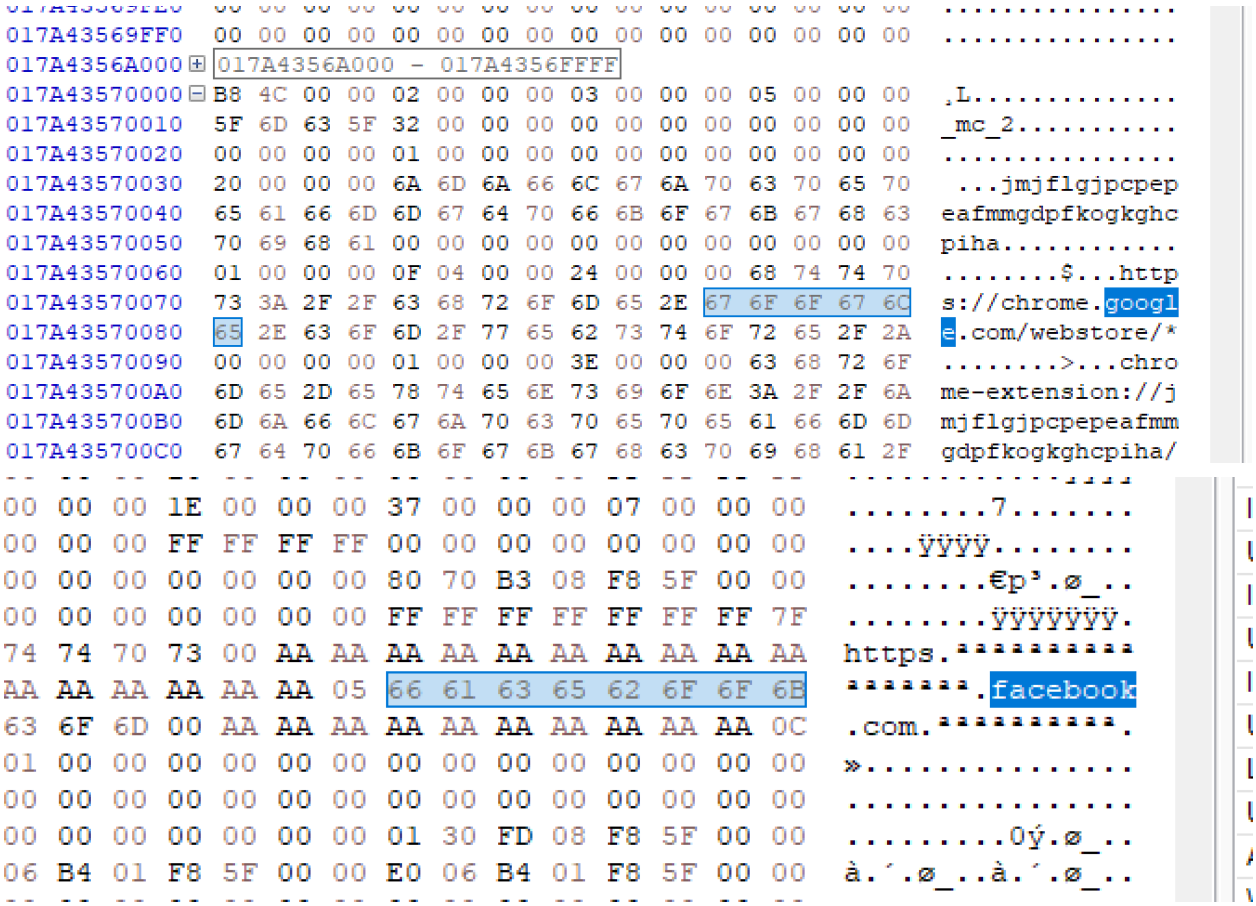


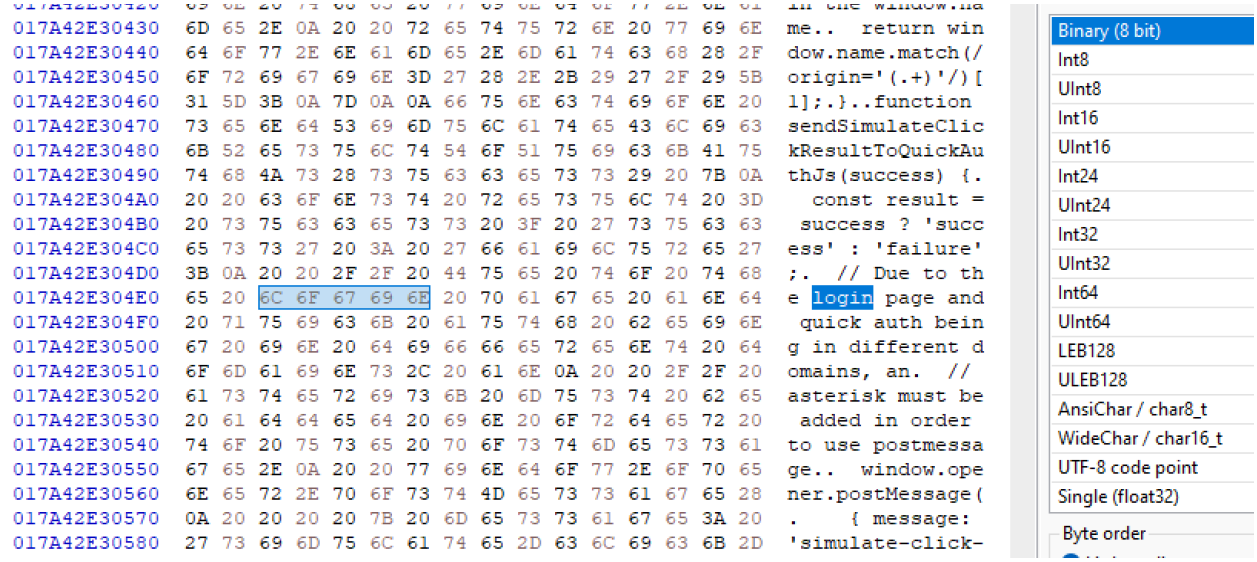
C.



Binary (8 bit)		10000000
Int8	go to:	-128
UInt8	go to:	128
Int16	go to:	-11904
UInt16	go to:	53632
Int24	go to:	3658112
UInt24	go to:	3658112
Int32	go to:	1681379712
UInt32	go to:	1681379712
Int64	go to:	8390046029746524544
UInt64	go to:	8390046029746524544
LEB128	go to:	911488
ULEB128	go to:	911488
AnsiChar / char8_t		€
WideChar / char16_t		덽
UTF-8 code point		Unexpected continuatic
Single (float32)		1.35634009257592E22

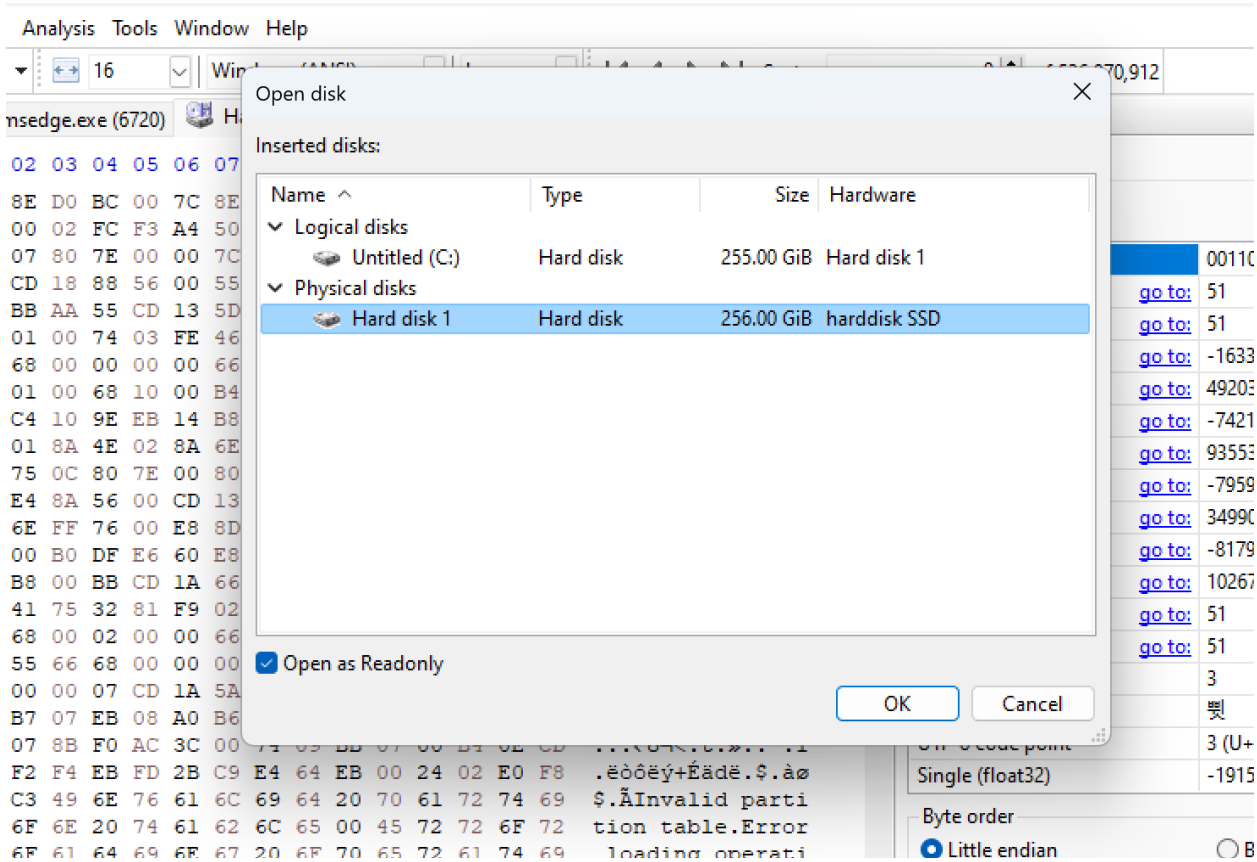
D.



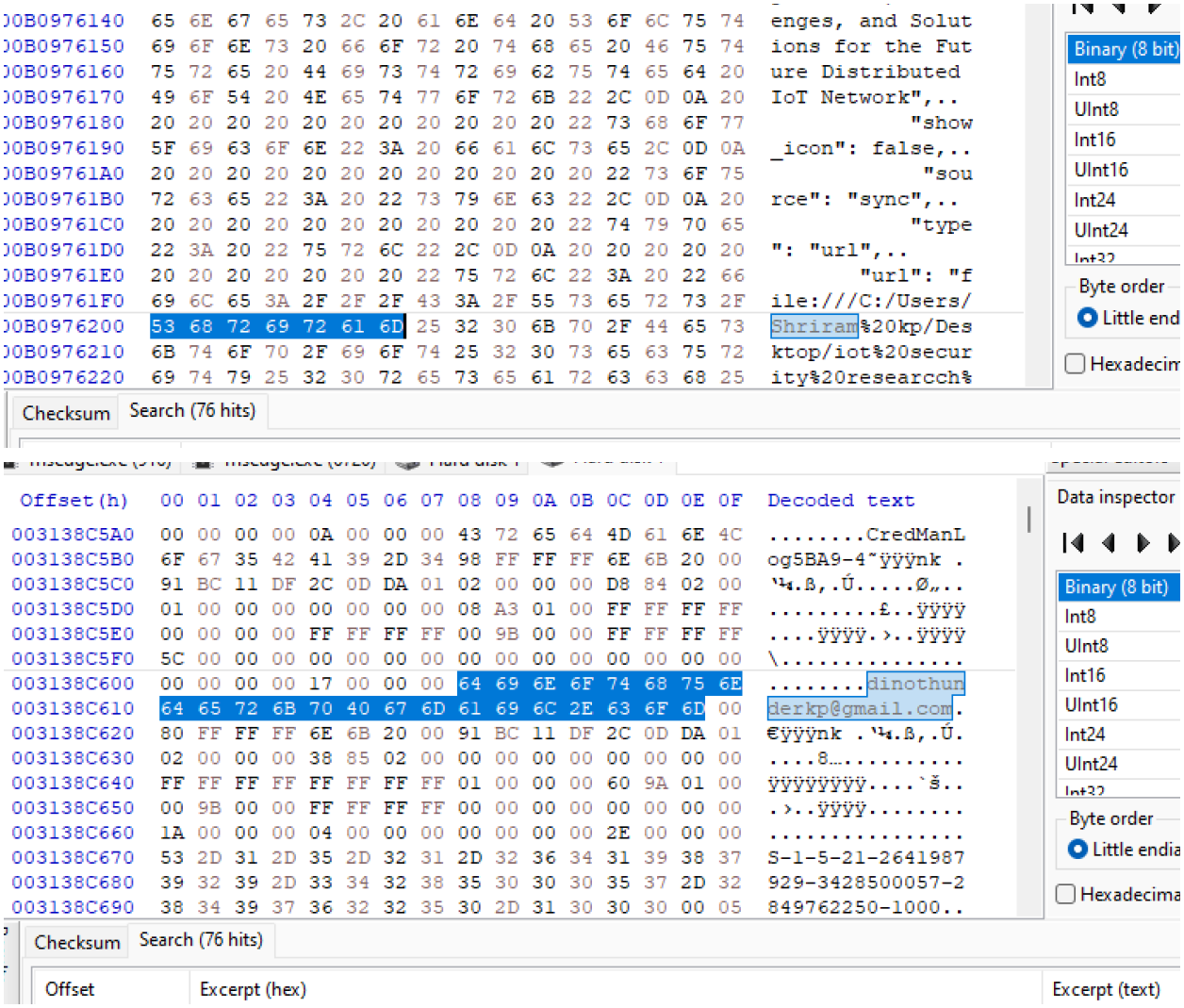

017A42E30430 6D 65 2E 0A 20 20 72 65 74 75 72 6E 20 77 69 6E me.. return win
017A42E30440 64 6F 77 2E 6E 61 6D 65 2E 6D 61 74 63 68 28 2F dow.name.match(/
017A42E30450 6F 72 69 67 69 6E 3D 27 28 2E 2B 29 27 2F 29 5B origin='(.+)'/)[
017A42E30460 31 5D 3B 0A 7D 0A 0A 66 75 6E 63 74 69 6F 6E 20 1];.}..function
017A42E30470 73 65 6E 64 53 69 6D 75 6C 61 74 65 43 6C 69 63 sendSimulateClic
017A42E30480 6B 52 65 73 75 6C 74 54 6F 51 75 69 63 6B 41 75 kResultToQuickAu
017A42E30490 74 68 4A 73 28 73 75 63 63 65 73 73 29 20 7B 0A thJs(success) {.
017A42E304A0 20 20 63 6F 6E 73 74 20 72 65 73 75 6C 74 20 3D const result =
017A42E304B0 20 73 75 63 63 65 73 73 20 3F 20 27 73 75 63 63 success ? 'succ
017A42E304C0 65 73 73 27 20 3A 20 27 66 61 69 6C 75 72 65 27 ess' : 'failure'
017A42E304D0 3B 0A 20 20 2F 2F 20 44 75 65 20 74 6F 20 74 68 ;. // Due to th
017A42E304E0 65 20 6C 6F 67 69 6E 20 70 61 67 65 20 61 6E 64 e login page and
017A42E304F0 20 71 75 69 63 6B 20 61 75 74 68 20 62 65 69 6E quick auth bein
017A42E30500 67 20 69 6E 20 64 69 66 66 65 72 65 6E 74 20 64 g in different d
017A42E30510 6F 6D 61 69 6E 73 2C 20 61 6E 0A 20 20 2F 2F 20 omains, an. //
017A42E30520 61 73 74 65 72 69 73 6B 20 6D 75 73 74 20 62 65 asterisk must be
017A42E30530 20 61 64 64 65 64 20 69 6E 20 6F 72 64 65 72 20 added in order
017A42E30540 74 6F 20 75 73 65 20 70 6F 73 74 6D 65 73 73 61 to use postmessa
017A42E30550 67 65 2E 0A 20 20 77 69 6E 64 6F 77 2E 6F 70 65 ge.. window.ope
017A42E30560 6E 65 72 2E 70 6F 73 74 4D 65 73 73 61 67 65 28 ner.postMessage(
017A42E30570 0A 20 20 20 20 7B 20 6D 65 73 73 61 67 65 3A 20 . { message:
017A42E30580 27 73 69 6D 75 6C 61 74 65 2D 63 6C 69 63 6B 2D 'simulate-click-
Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Int32
UInt32
Int64
UInt64
LEB128
ULEB128
AnsiChar / char8_t
WideChar / char16_t
UTF-8 code point
Single (float32)
Byte order

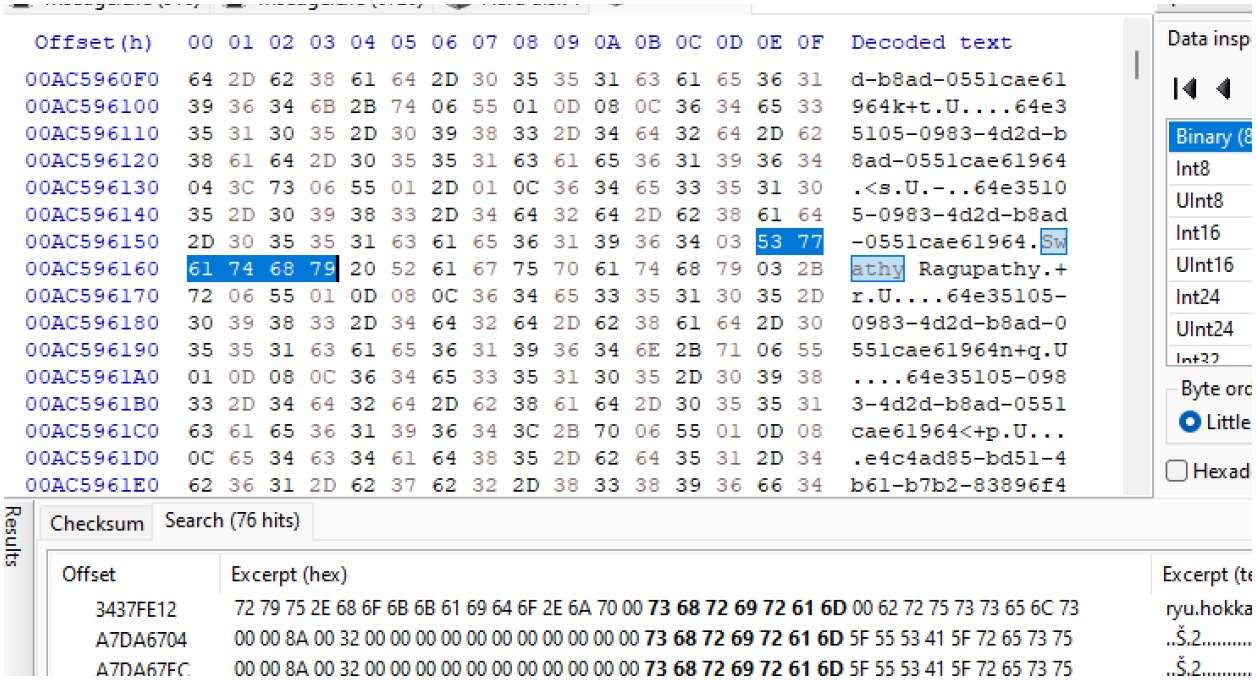
Step 2 :

A.


Analysis Tools Window Help
Open disk
Inserted disks:
Name
Type
Size
Hardware
Logical disks
Untitled (C:) Hard disk 255.00 GiB Hard disk 1
Physical disks
Hard disk 1 Hard disk 256.00 GiB harddisk SSD
Open as Readonly
OK
Cancel
Single (float32)
Byte order
Little endian

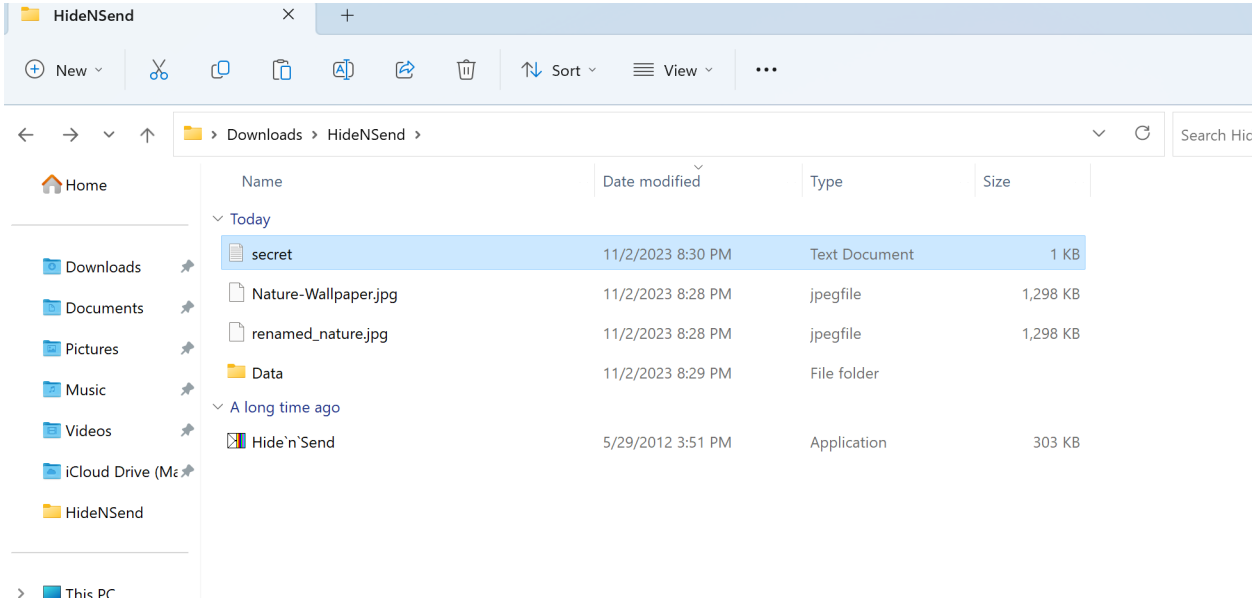
B.


Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Byte order
Little end
Hexadecim
Checksum
Search (76 hits)
Data inspector
Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Byte order
Little endia
Hexadecima
Checksum
Search (76 hits)
Offset
Excerpt (hex)
Excerpt (text)

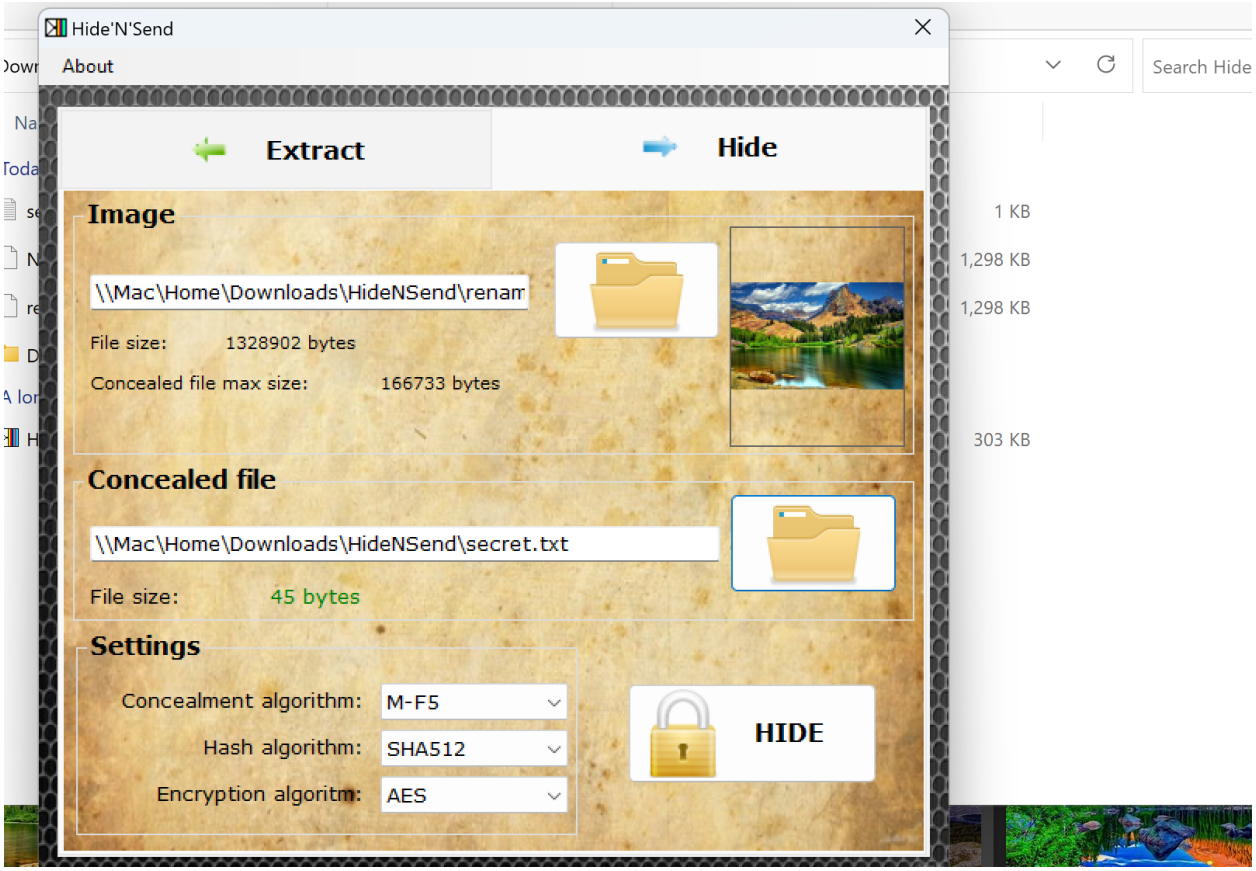


I am amazed that I found so much information on my harddrive which makes me crazy .

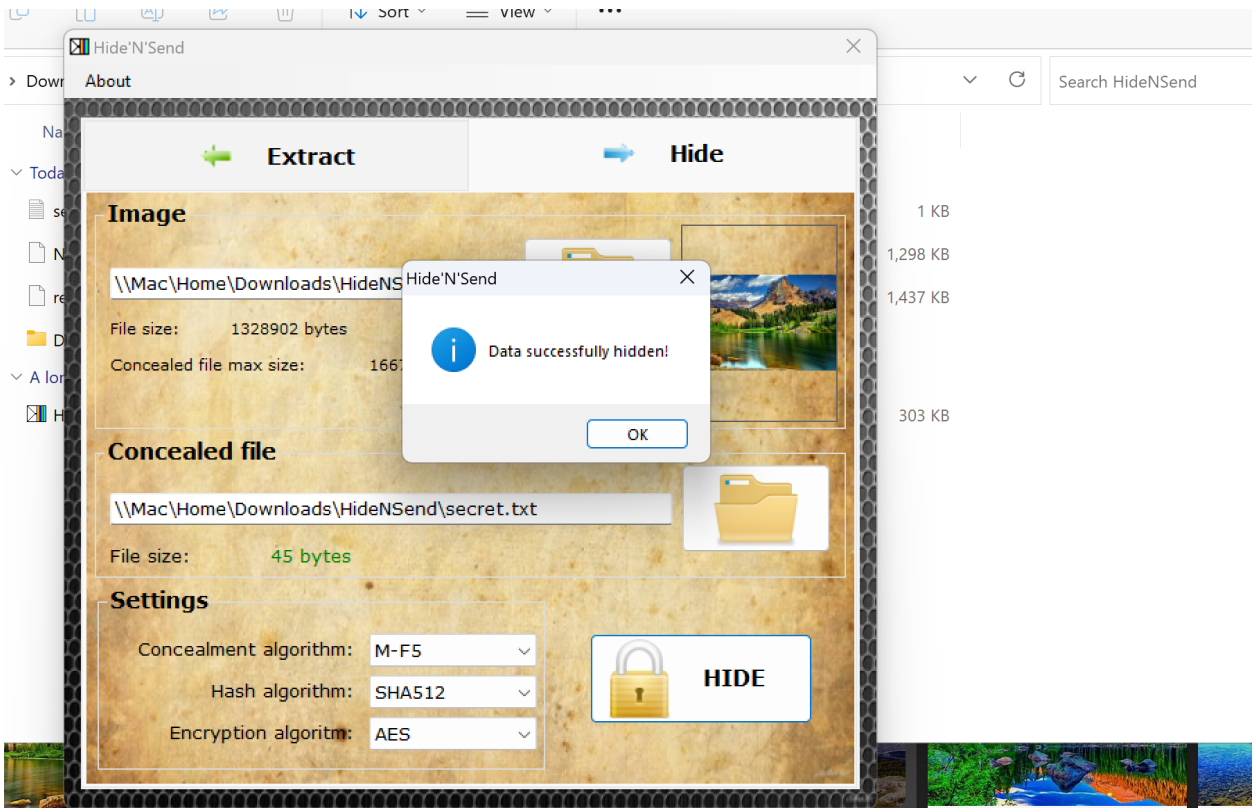
Exercise 23. 03 :
Step 1 :
D.



G.


Hide'N'Send
About
Extract
Hide
Image
\\Mac\Home\Downloads\HideNSend\renam
File size: 1328902 bytes
Concealed file max size: 166733 bytes
Concealed file
\\Mac\Home\Downloads\HideNSend\secret.txt
File size: 45 bytes
Settings
Concealment algorithm: M-F5
Hash algorithm: SHA512
Encryption algoritm: AES
HIDE
Search Hide
1 KB
1,298 KB
1,298 KB
303 KB

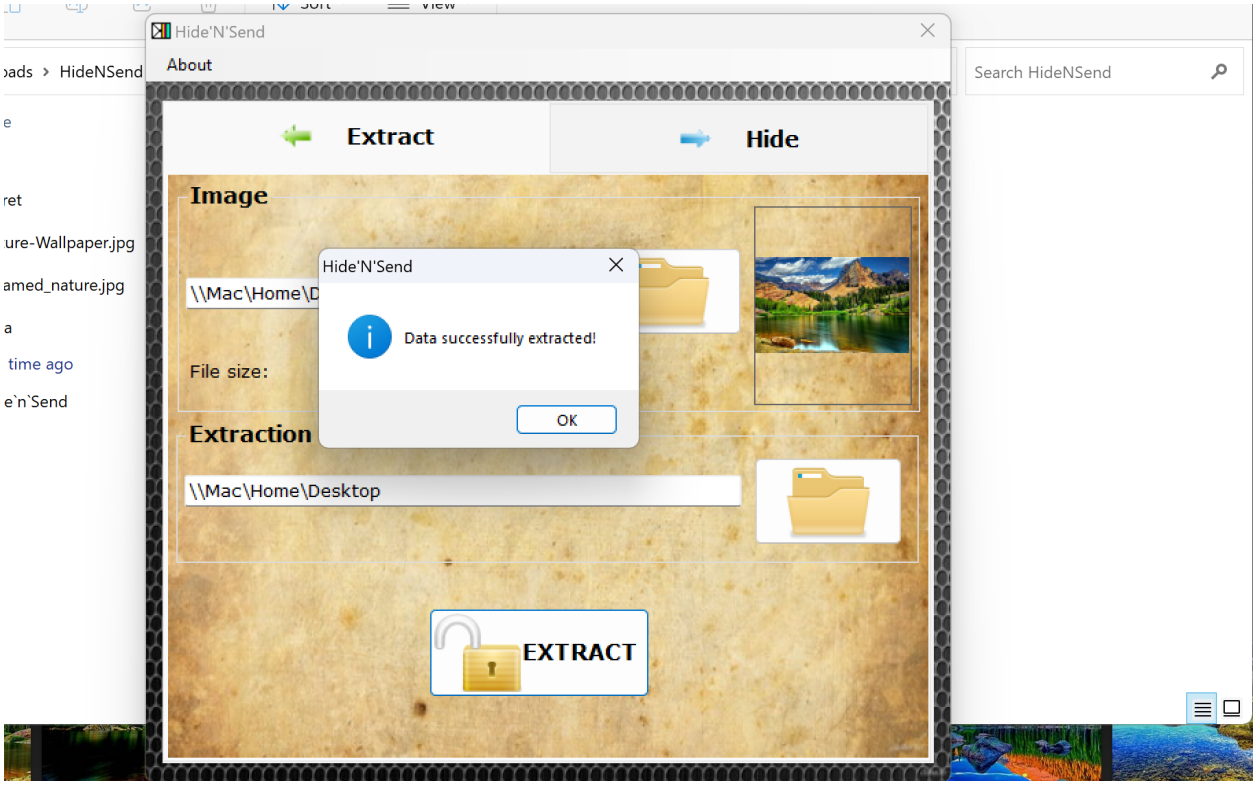
I.



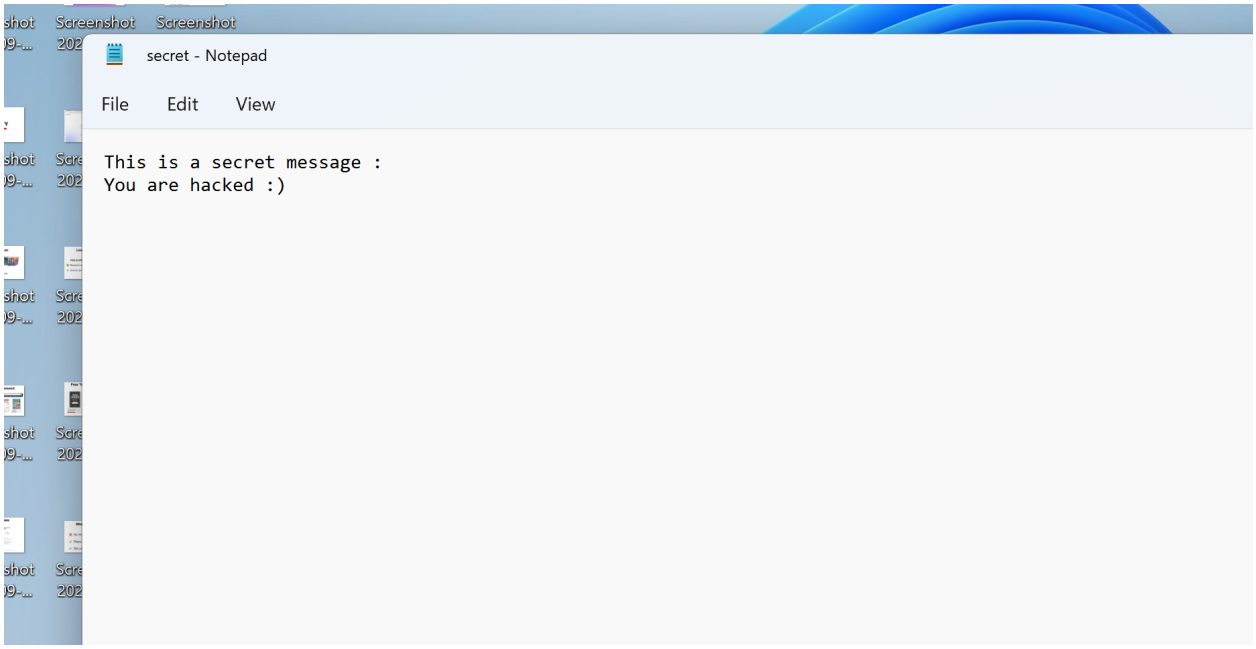
J.

I feel both the images look same, but if i have to see more deep and compare the both, I feel there is a little bit contrast change visible, only if I see side by side. Otherwise I really don't notice anything different at all.

O.



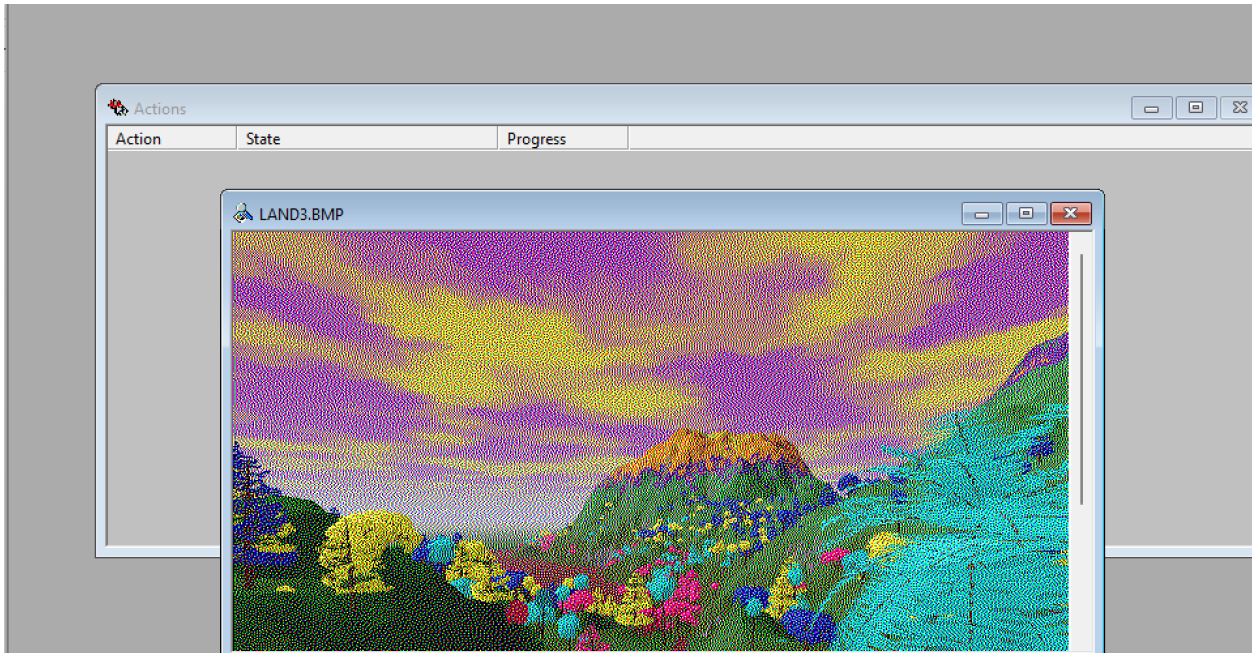
P.



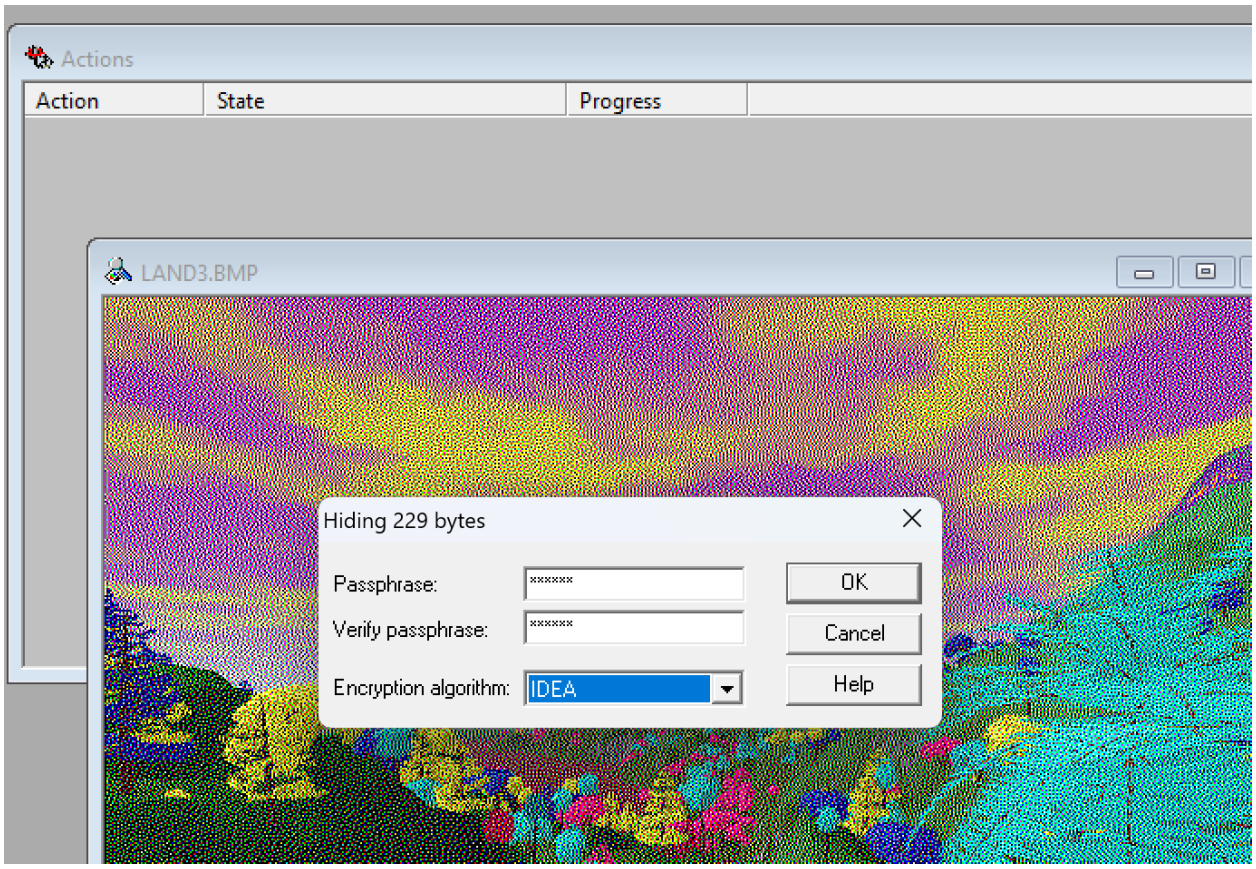
Got the secret back, this is exciting :)

Step 2 :

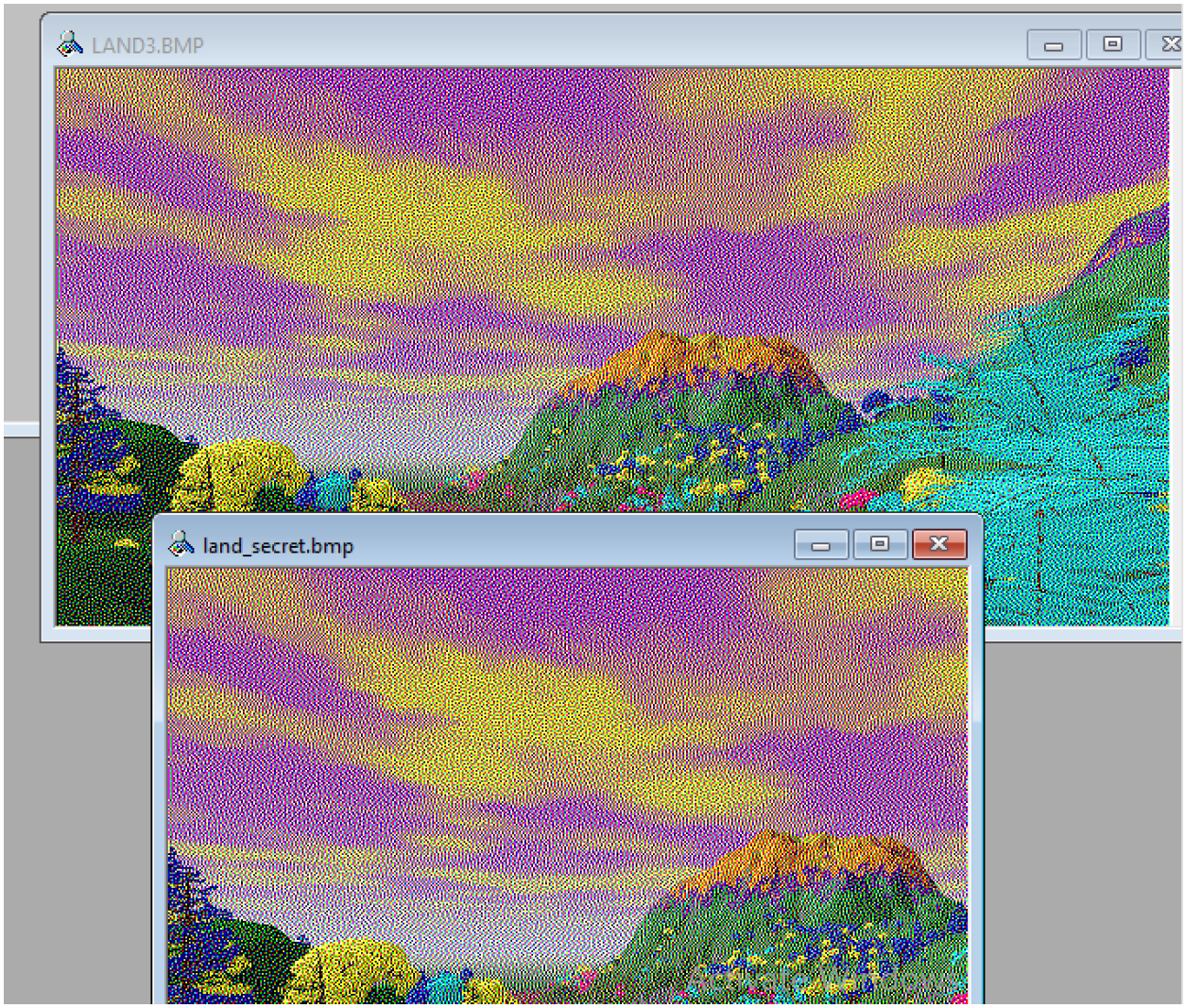
D.


Actions
Action
State
Progress
LAND3.BMP

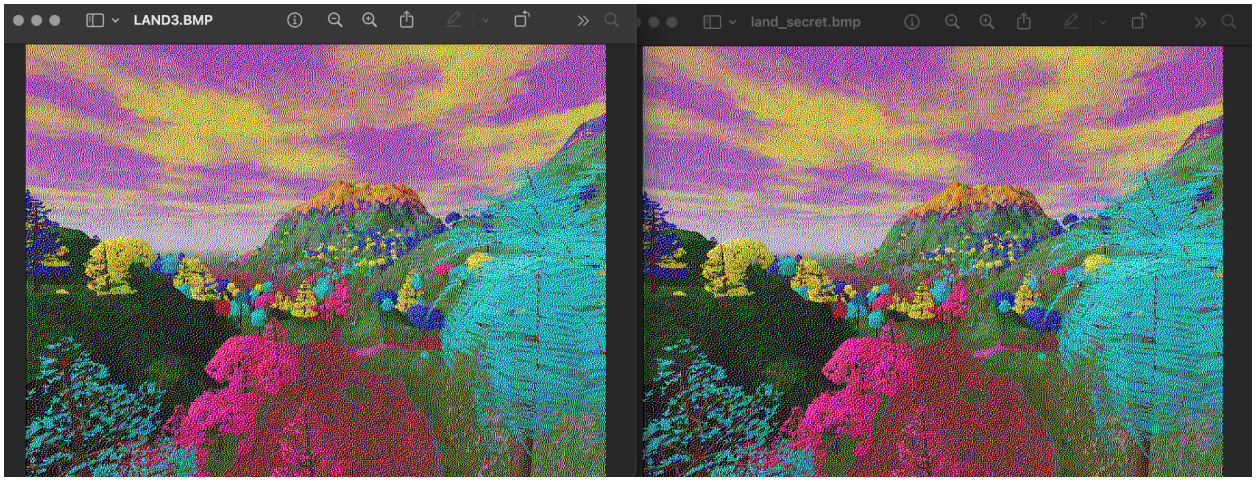
E.


Actions
Action
State
Progress
LAND3.BMP
Hiding 229 bytes
Passphrase:
******
Verify passphrase:
******
Encryption algorithm:
IDEA
OK
Cancel
Help

F.

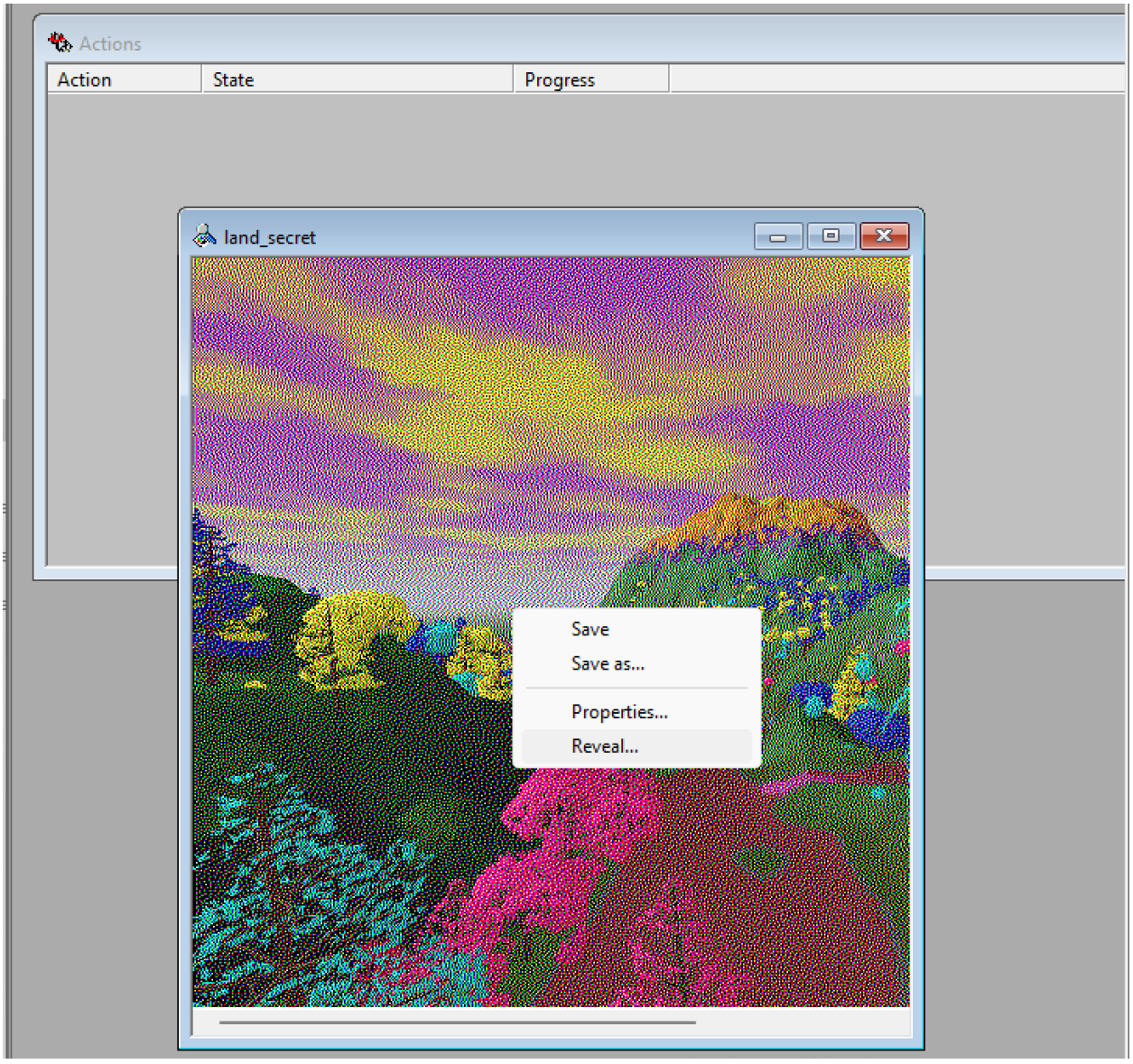


I.

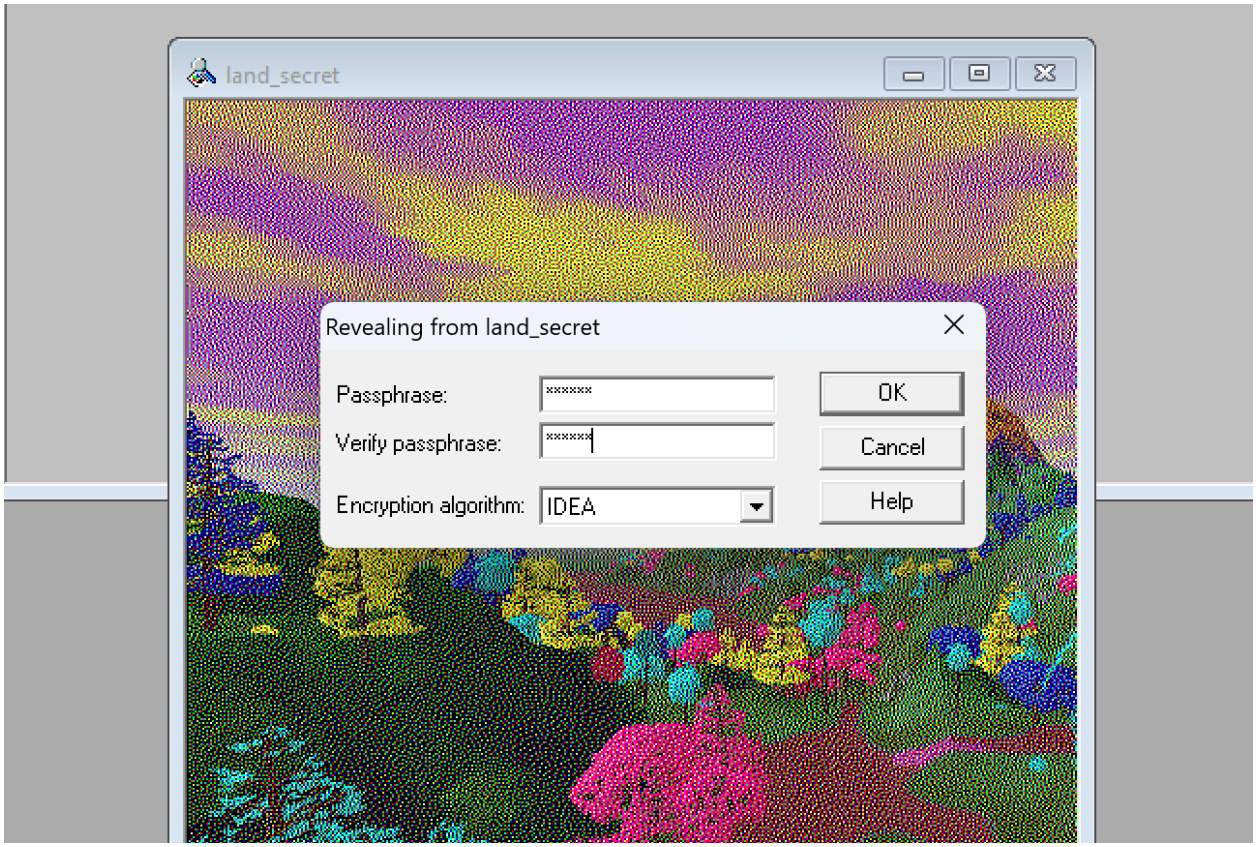


The new image seems to be little bit dull that makes sense because we hide the message by reducing the brightness.
The size of the new image seems to be twice the size of the original image.

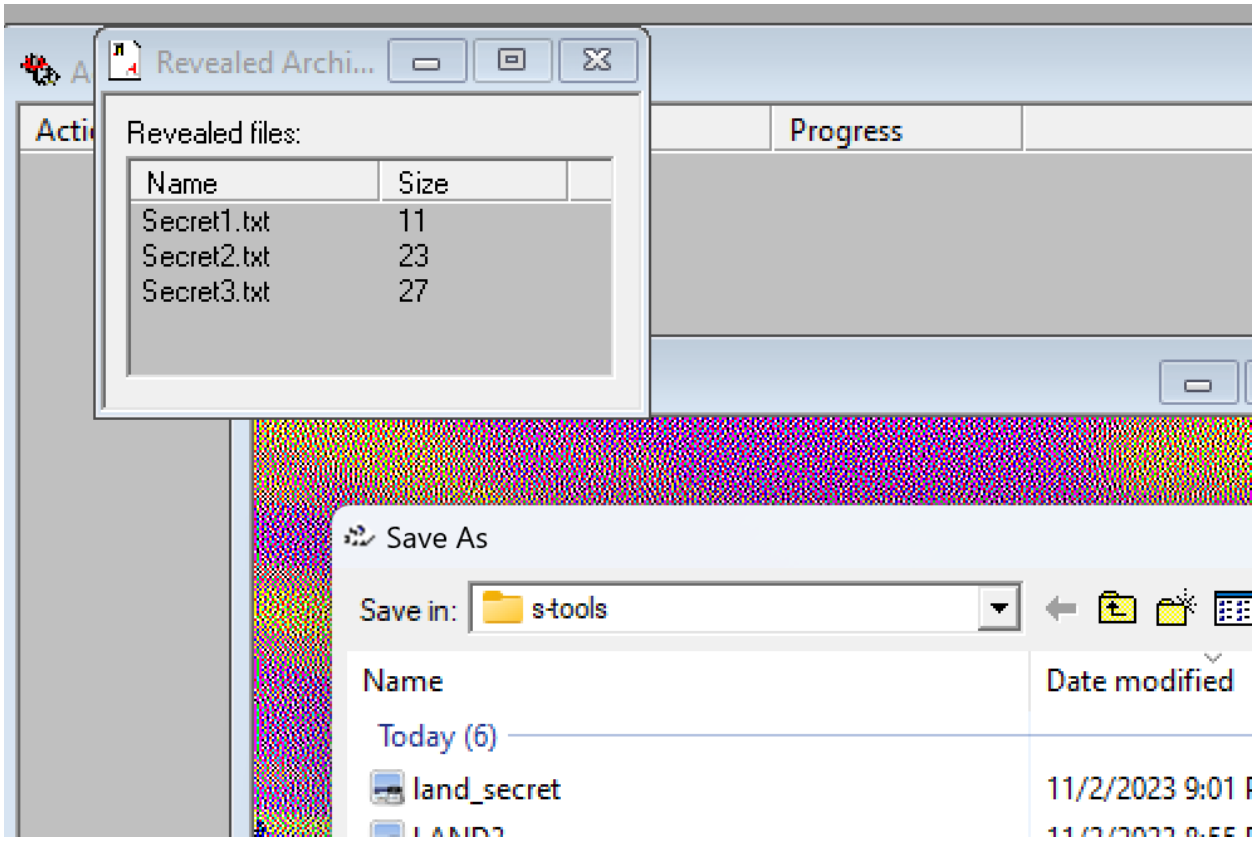
J and K.


Actions
Action
State
Progress
land_secret
Save
Save as...
Properties...
Reveal...

I.

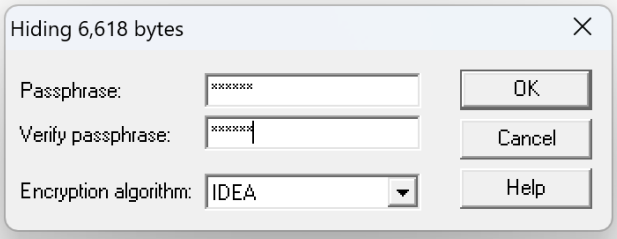

land_secret
Revealing from land_secret
Passphrase:
Verify passphrase:
Encryption algorithm:
IDEA
OK
Cancel
Help

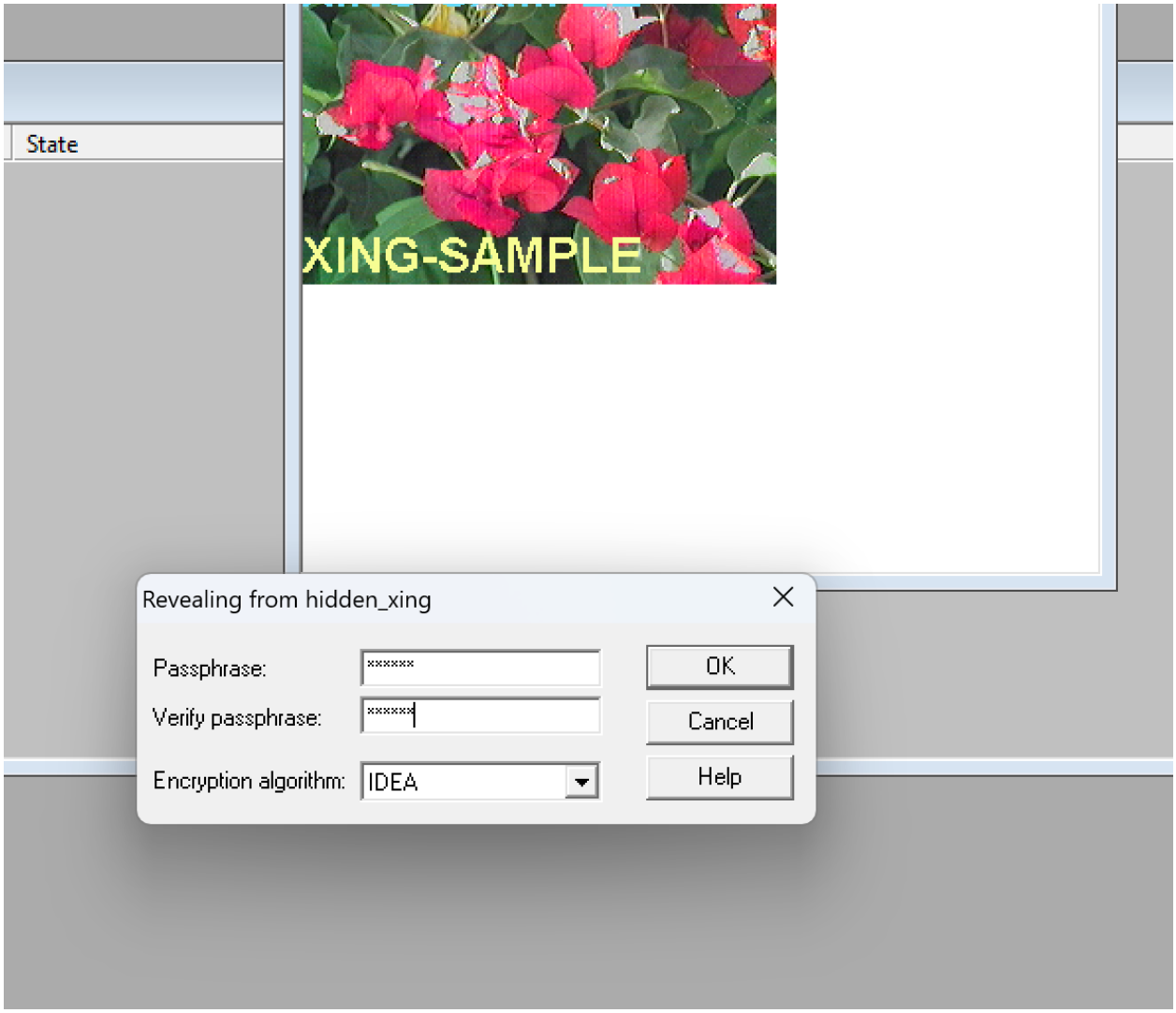
M.

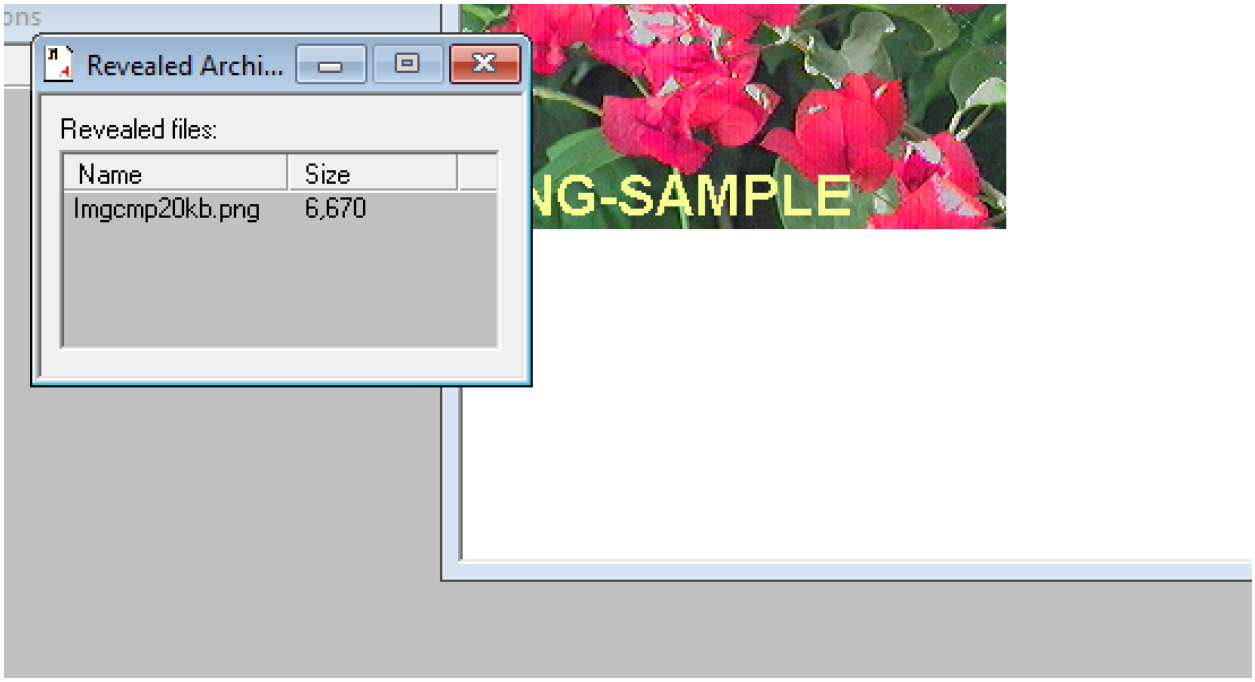

Revealed Archi...
Revealed files:
Name
Size
Secret1.txt
11
Secret2.txt
23
Secret3.txt
27
Progress
Save As
Save in:
s-tools
Name
Date modified
Today (6)
land_secret
11/2/2023 9:01

N.

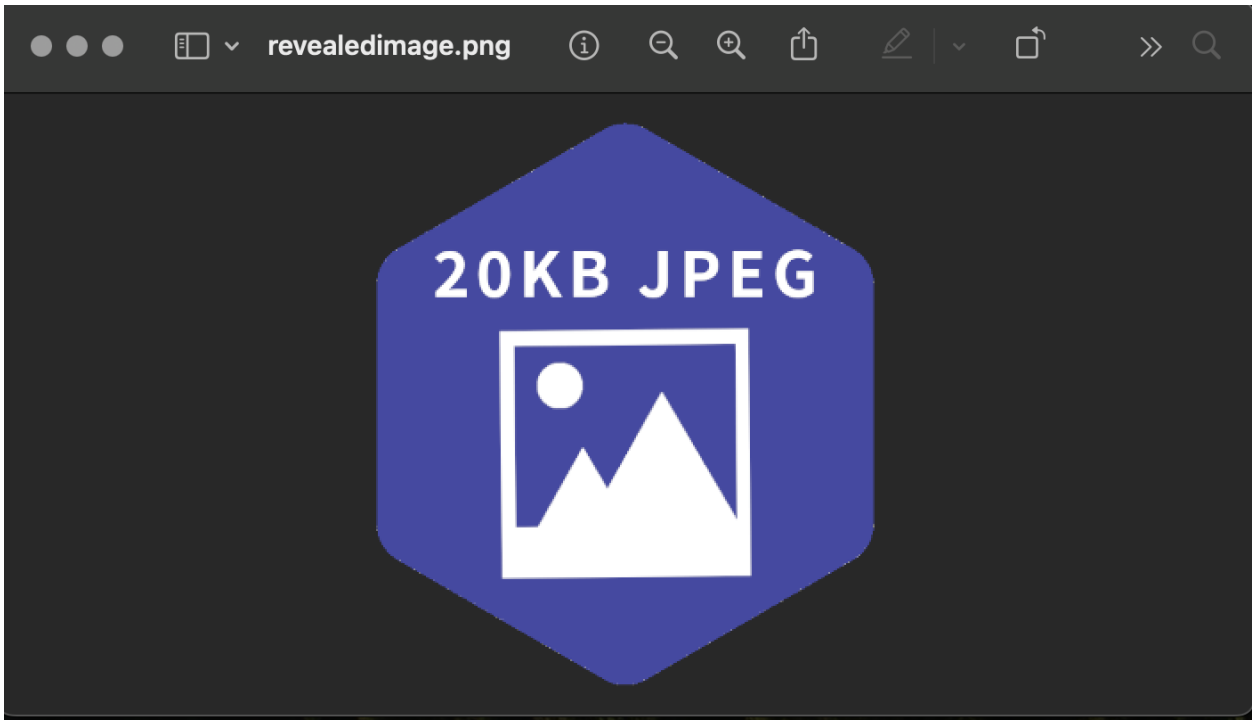

XING-SAMPLE


Hiding 6,618 bytes
Passphrase:
Verify passphrase:
Encryption algorithm:
IDEA
OK
Cancel
Help


State
XING-SAMPLE
Revealing from hidden_xing
Passphrase:
Verify passphrase:
Encryption algorithm:
IDEA
OK
Cancel
Help



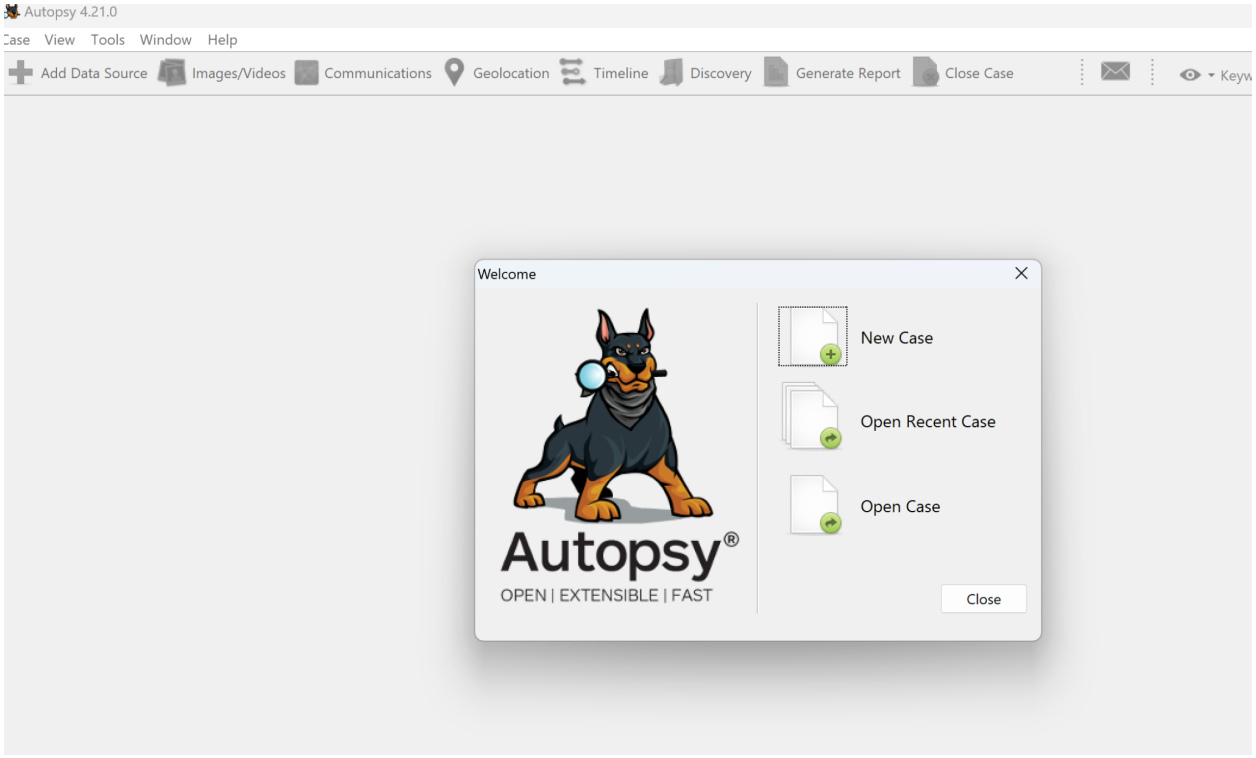
I got the hidden image back.



Exercise 23. 04 :

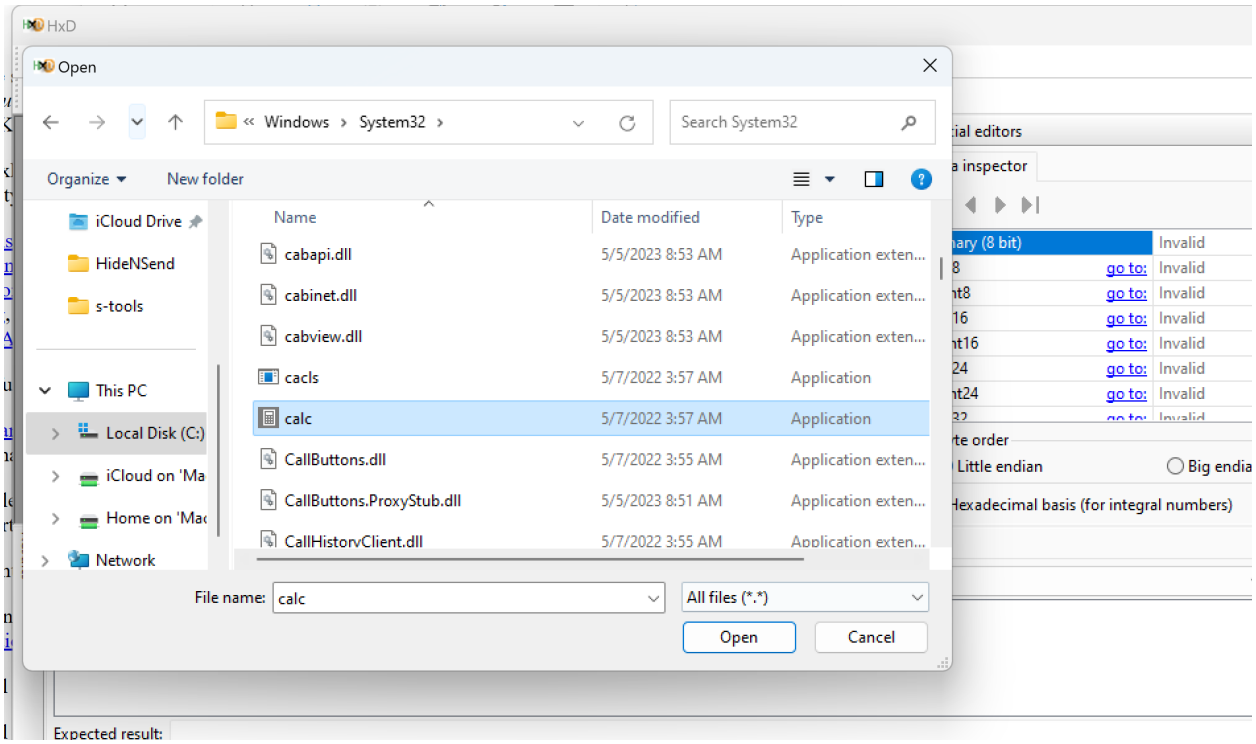
Step 1 :

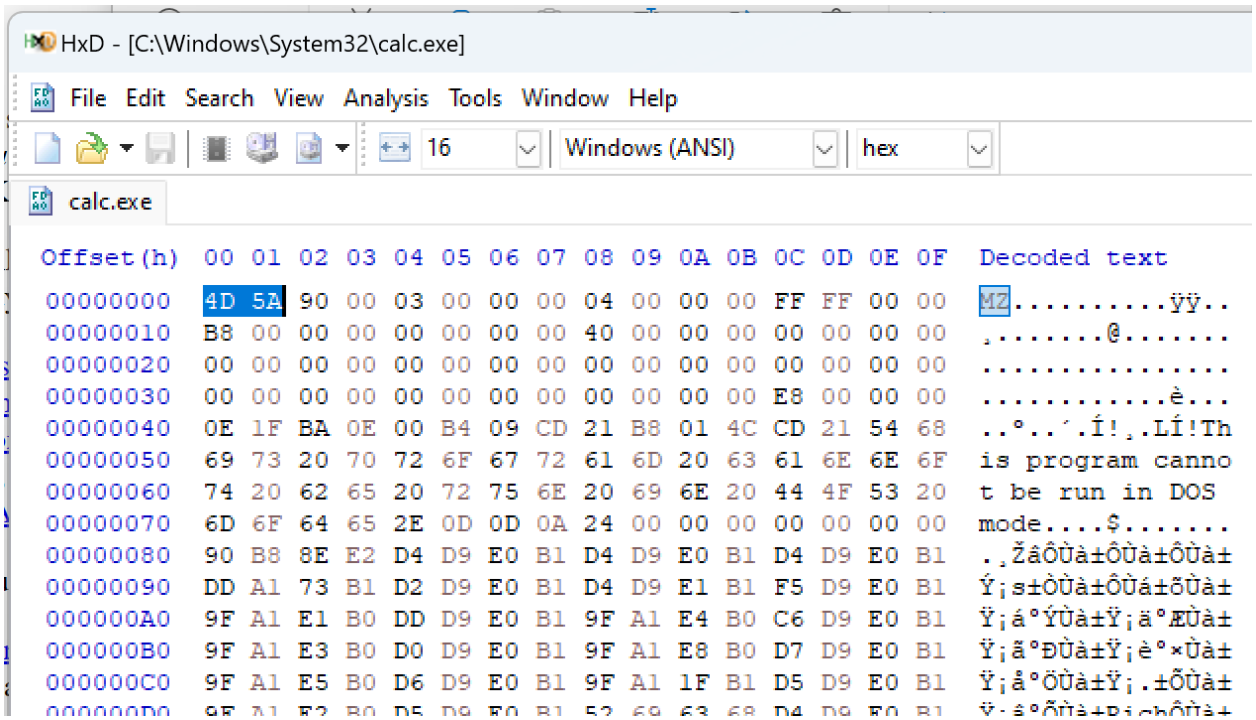
I installed the tool, but I don’t have Flashdrive, all the other images from download used in step 3.



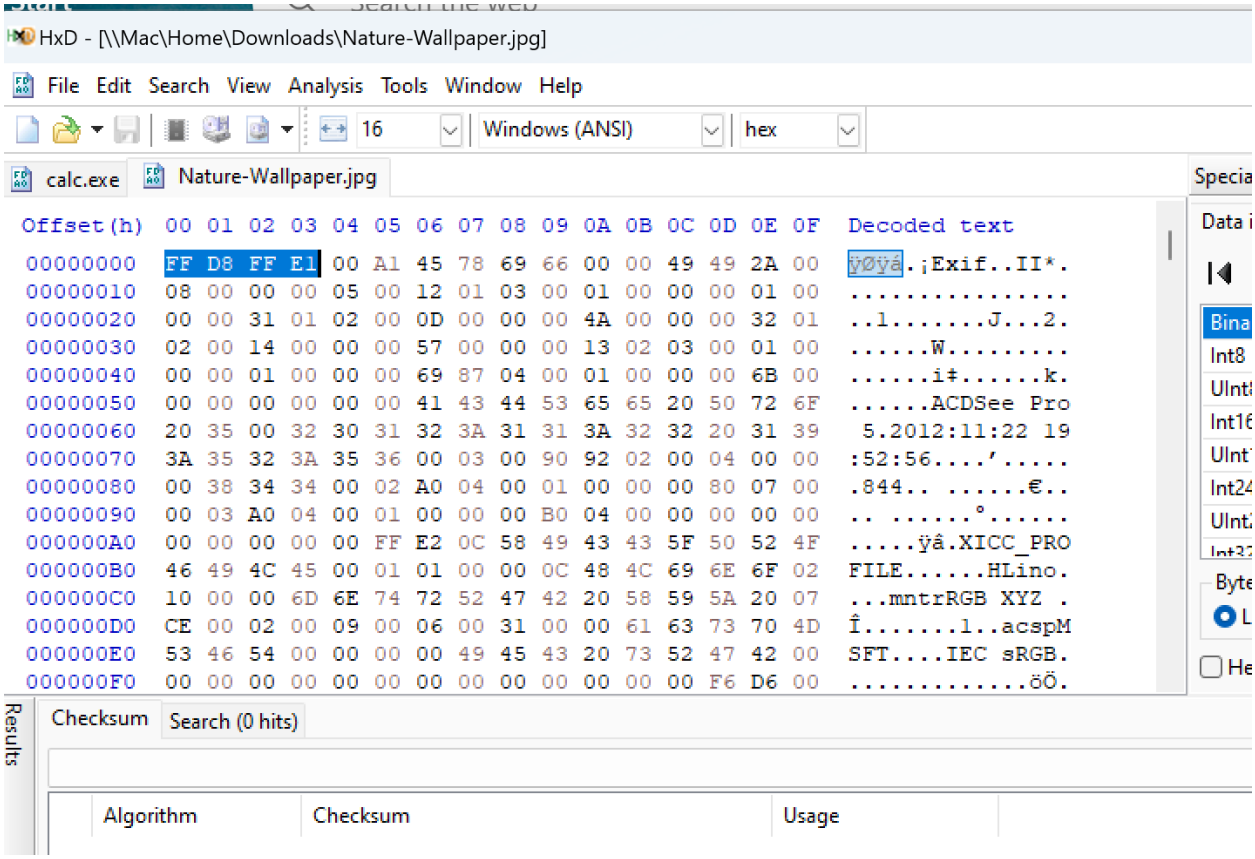
Step 2 :

A.

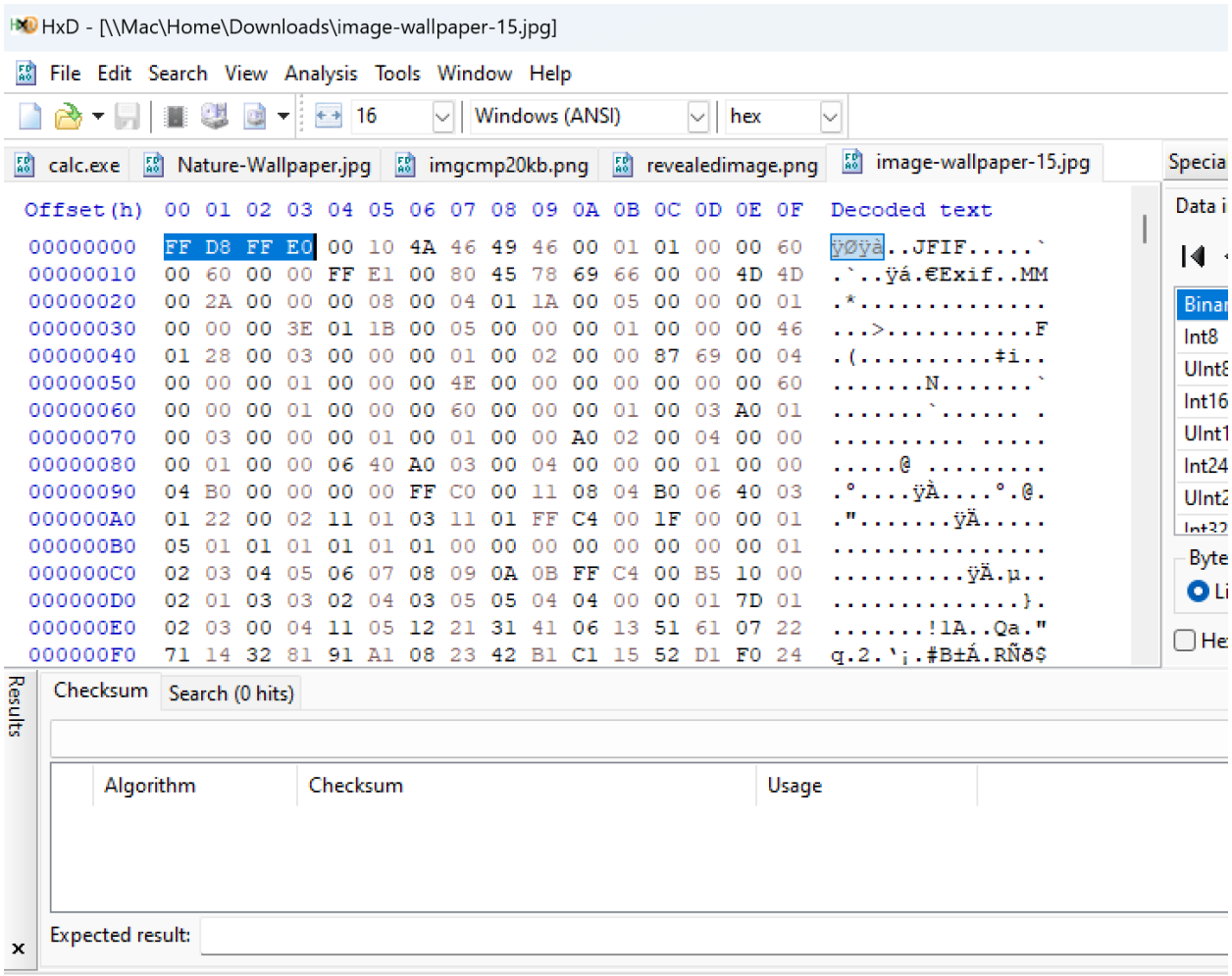

HxD
Open
Windows › System32 ›
Search System32
Organize
New folder
iCloud Drive
HideNSend
s-tools
This PC
Local Disk (C:)
iCloud on 'Ma
Home on 'Mac
Network
Name
Date modified
Type
cabapi.dll 5/5/2023 8:53 AM Application exten...
cabinet.dll 5/5/2023 8:53 AM Application exten...
cabview.dll 5/5/2023 8:53 AM Application exten...
cacls 5/7/2022 3:57 AM Application
calc 5/7/2022 3:57 AM Application
CallButtons.dll 5/7/2022 3:55 AM Application exten...
CallButtons.ProxyStub.dll 5/5/2023 8:51 AM Application exten...
File name: calc
All files (*.*)
Open
Cancel
Little endian
Big endia
Hexadecimal basis (for integral numbers)
Expected result:


HxD - [C:\Windows\System32\calc.exe]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
calc.exe
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ¸.......@.......
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 ....è...
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
00000080 90 B8 8E E2 D4 D9 E0 B1 D4 D9 E0 B1 D4 D9 E0 B1 .¸ŽâÔÙà±ÔÙà±ÔÙà±
00000090 DD A1 73 B1 D2 D9 E0 B1 D4 D9 E1 B1 F5 D9 E0 B1 Ý¡s±ÒÙà±ÔÙá±õÙà±
000000A0 9F A1 E1 B0 DD D9 E0 B1 9F A1 E4 B0 C6 D9 E0 B1 Ÿ¡á°ÝÙà±Ÿ¡ä°ÆÙà±
000000B0 9F A1 E3 B0 D0 D9 E0 B1 9F A1 E8 B0 D7 D9 E0 B1 Ÿ¡ã°ÐÙà±Ÿ¡è°×Ùà±
000000C0 9F A1 E5 B0 D6 D9 E0 B1 9F A1 1F B1 D5 D9 E0 B1 Ÿ¡å°ÖÙà±Ÿ¡.±ÕÙà±

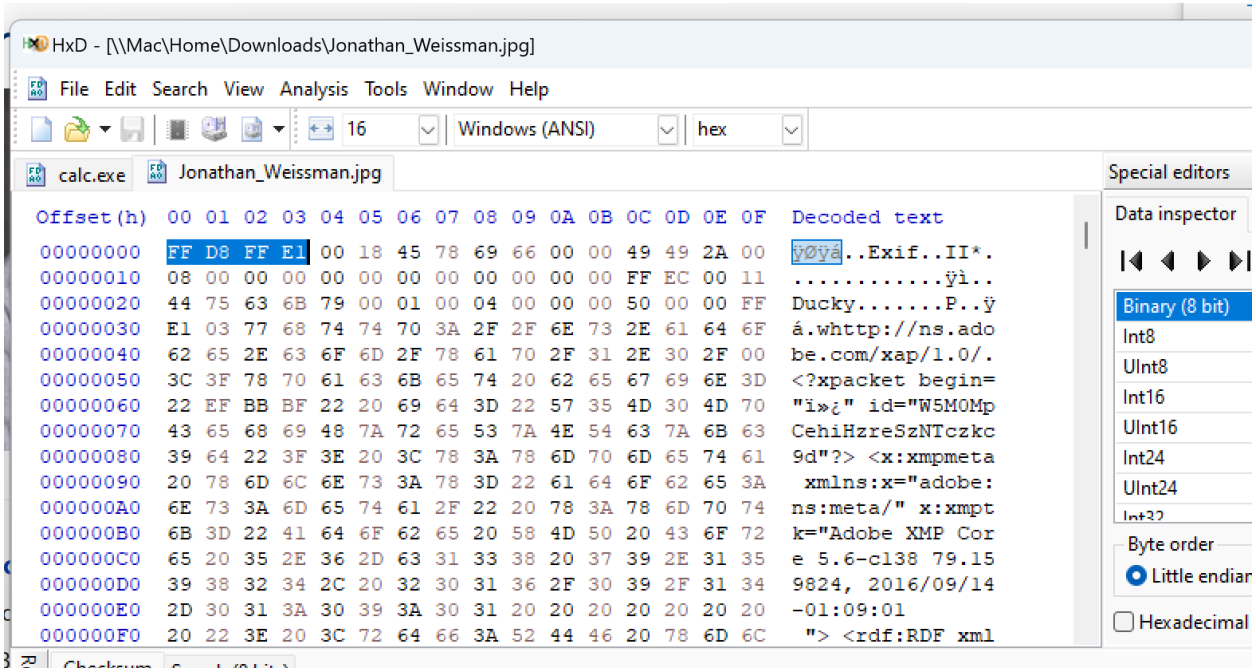
B.

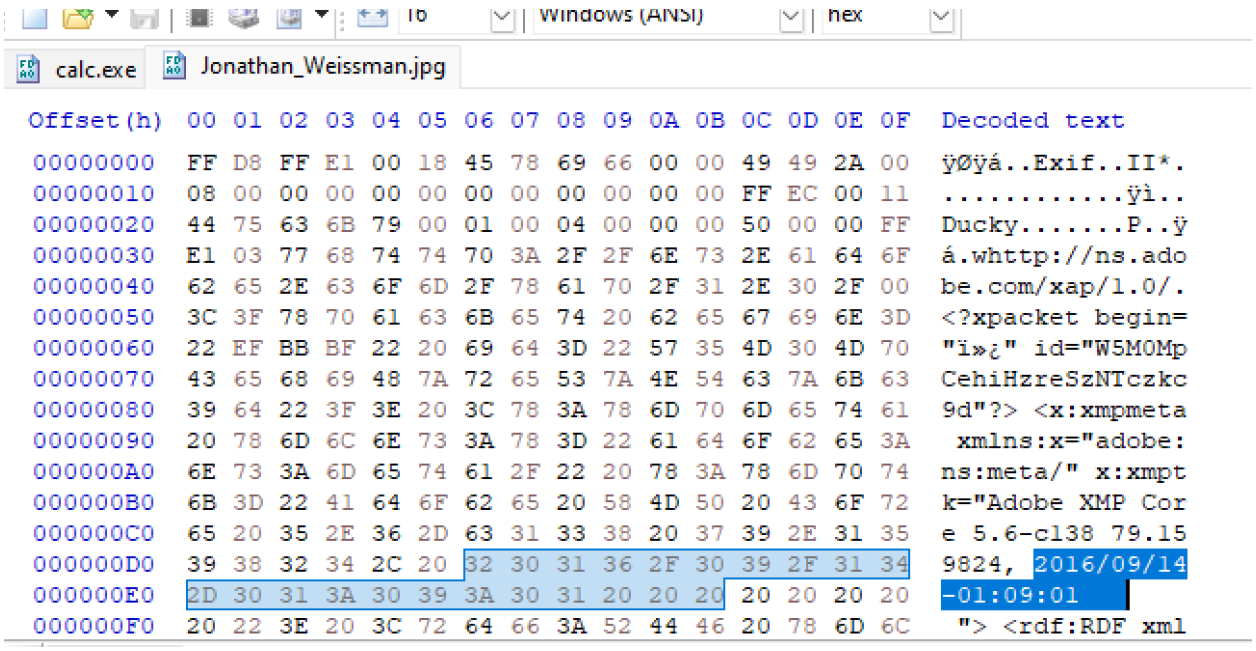


This is the jpeg Image


HxD - [\\Mac\Home\Downloads\image-wallpaper-15.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
calc.exe
Nature-Wallpaper.jpg
imgcmp20kb.png
revealedimage.png
image-wallpaper-15.jpg
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 60 ÿØÿà..JFIF.....`
00000010 00 60 00 00 FF E1 00 80 45 78 69 66 00 00 4D 4D .`..ÿá.€Exif..MM
00000020 00 2A 00 00 00 08 00 04 01 1A 00 05 00 00 00 01 .*..............
00000030 00 00 00 3E 01 1B 00 05 00 00 00 01 00 00 00 46 ...>...........F
00000040 01 28 00 03 00 00 00 01 00 02 00 00 87 69 00 04 .(..........‡i..
00000050 00 00 00 01 00 00 00 4E 00 00 00 00 00 00 00 60 ....N.......`
00000060 00 00 00 01 00 00 00 60 00 00 00 01 00 03 A0 01 ....`...... .
00000070 00 03 00 00 00 01 00 01 00 00 A0 02 00 04 00 00 ....
00000080 00 01 00 00 06 40 A0 03 00 04 00 00 00 01 00 00 .....@ ....
00000090 04 B0 00 00 00 00 FF C0 00 11 08 04 B0 06 40 03 .°....ÿÀ....°.@.
000000A0 01 22 00 02 11 01 03 11 01 FF C4 00 1F 00 00 01 ."........ÿÄ.....
000000B0 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 ....
000000C0 02 03 04 05 06 07 08 09 0A 0B FF C4 00 B5 10 00 ....ÿÄ.µ..
000000D0 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7D 01 ....}.
000000E0 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 ....!1A..Qa."
000000F0 71 14 32 81 91 A1 08 23 42 B1 C1 15 52 D1 F0 24 q.2.'¡.#B±Á.RÑð$
Special
Data i
Binar
Int8
UInt8
Int16
UInt1
Int24
UInt2
Byte
Li
He
Results
Checksum
Search (0 hits)
Algorithm
Checksum
Usage
Expected result:

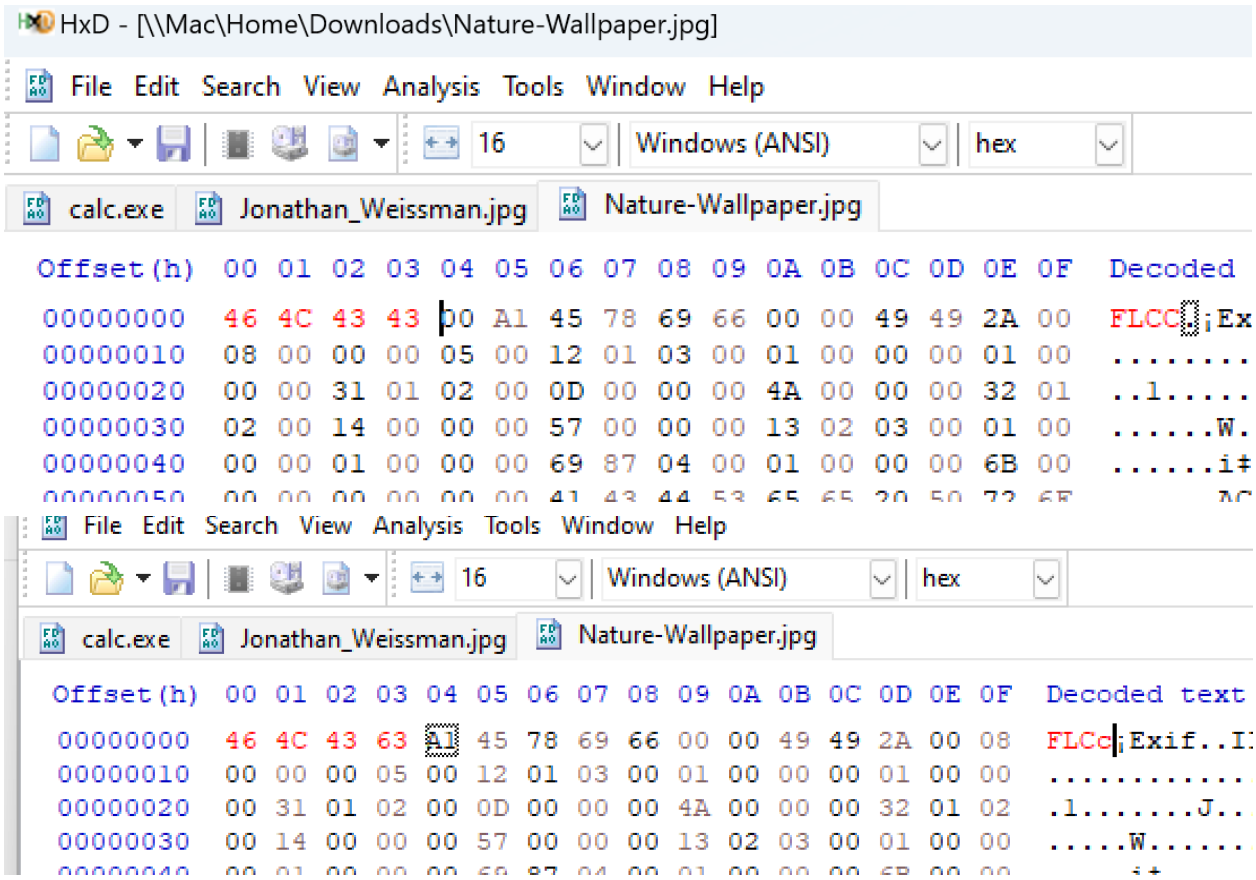
C.


HxD - [\\Mac\Home\Downloads\Jonathan_Weissman.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
calc.exe
Jonathan_Weissman.jpg
Special editors
Data inspector
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 FF D8 FF E1 00 18 45 78 69 66 00 00 49 49 2A 00 ÿØÿá..Exif..II*.
00000010 08 00 00 00 00 00 00 00 00 00 00 00 FF EC 00 11 ....ÿì..
00000020 44 75 63 6B 79 00 01 00 04 00 00 00 50 00 00 FF Ducky.......P..ÿ
00000030 E1 03 77 68 74 74 70 3A 2F 2F 6E 73 2E 61 64 6F á.whttp://ns.ado
00000040 62 65 2E 63 6F 6D 2F 78 61 70 2F 31 2E 30 2F 00 be.com/xap/1.0/.
00000050 3C 3F 78 70 61 63 6B 65 74 20 62 65 67 69 6E 3D <?xpacket begin=
00000060 22 EF BB BF 22 20 69 64 3D 22 57 35 4D 30 4D 70 "i»¿" id="W5M0Mp
00000070 43 65 68 69 48 7A 72 65 53 7A 4E 54 63 7A 6B 63 CehiHzreSzNTczkc
00000080 39 64 22 3F 3E 20 3C 78 3A 78 6D 70 6D 65 74 61 9d"?> <x:xmpmeta
00000090 20 78 6D 6C 6E 73 3A 78 3D 22 61 64 6F 62 65 3A xmlns:x="adobe:
000000A0 6E 73 3A 6D 65 74 61 2F 22 20 78 3A 78 6D 70 74 ns:meta/" x:xmpt
000000B0 6B 3D 22 41 64 6F 62 65 20 58 4D 50 20 43 6F 72 k="Adobe XMP Cor
000000C0 65 20 35 2E 36 2D 63 31 33 38 20 37 39 2E 31 35 e 5.6-c138 79.15
000000D0 39 38 32 34 2C 20 32 30 31 36 2F 30 39 2F 31 34 9824, 2016/09/14
000000E0 2D 30 31 3A 30 39 3A 30 31 20 20 20 20 20 20 20 -01:09:01
000000F0 20 22 3E 20 3C 72 64 66 3A 52 44 46 20 78 6D 6C "> <rdf:RDF xml
Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Byte order
Little endian
Hexadecimal

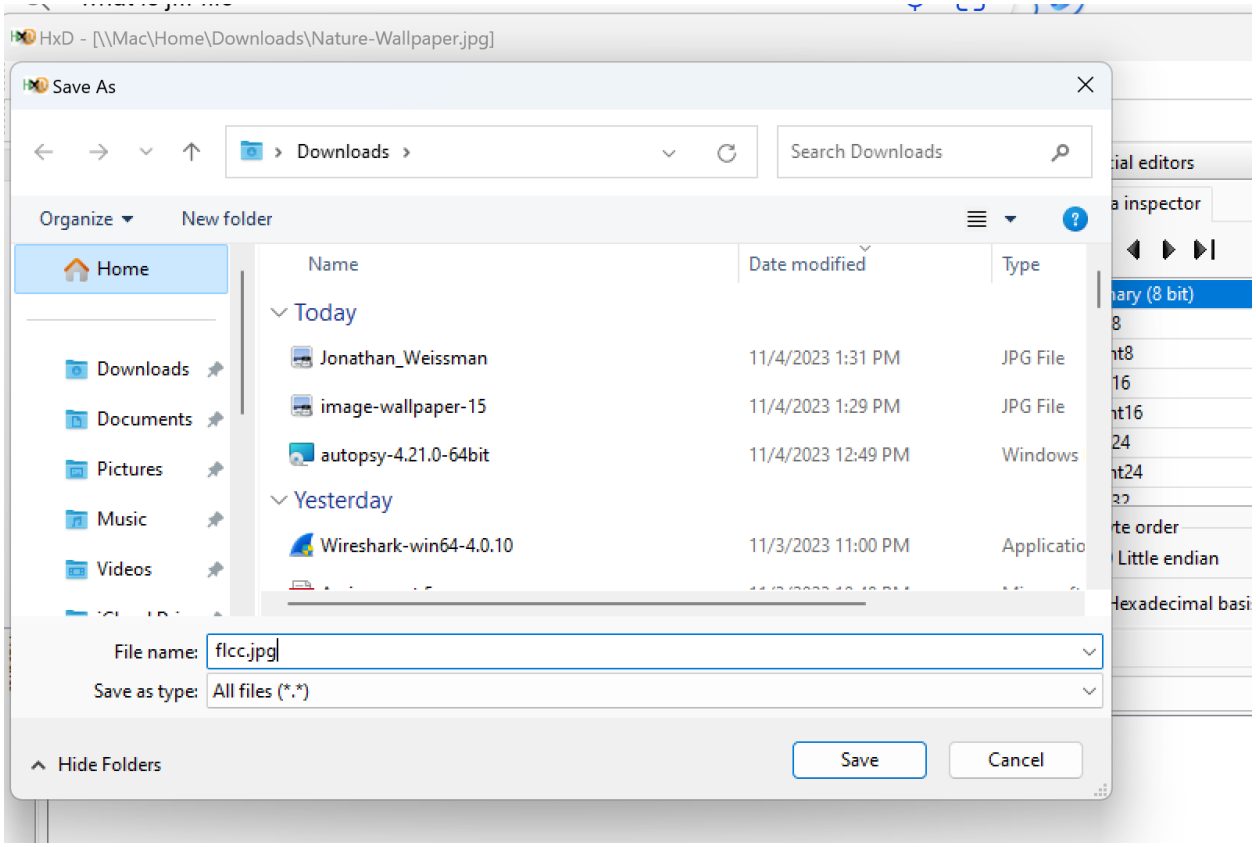


The picture taken on 2016 and sep 14.

D.



E.


HxD - [\\Mac\Home\Downloads\Nature-Wallpaper.jpg]
Save As
Downloads
Search Downloads
Organize
New folder
Home
Downloads
Documents
Pictures
Music
Videos
Name
Date modified
Type
Today
Jonathan_Weissman
11/4/2023 1:31 PM
JPG File
image-wallpaper-15
11/4/2023 1:29 PM
JPG File
autopsy-4.21.0-64bit
11/4/2023 12:49 PM
Windows
Yesterday
Wireshark-win64-4.0.10
11/3/2023 11:00 PM
File name:
flcc.jpg
Save as type:
All files (*.*)
Hide Folders
Save
Cancel
Little endian

F.
This happens because the file is modified and the file got corrupt, as we changed the hex values.

G.
No if you change the signature or hex values, the file get corrupted and it will create a form of suspicion which is not good for him.

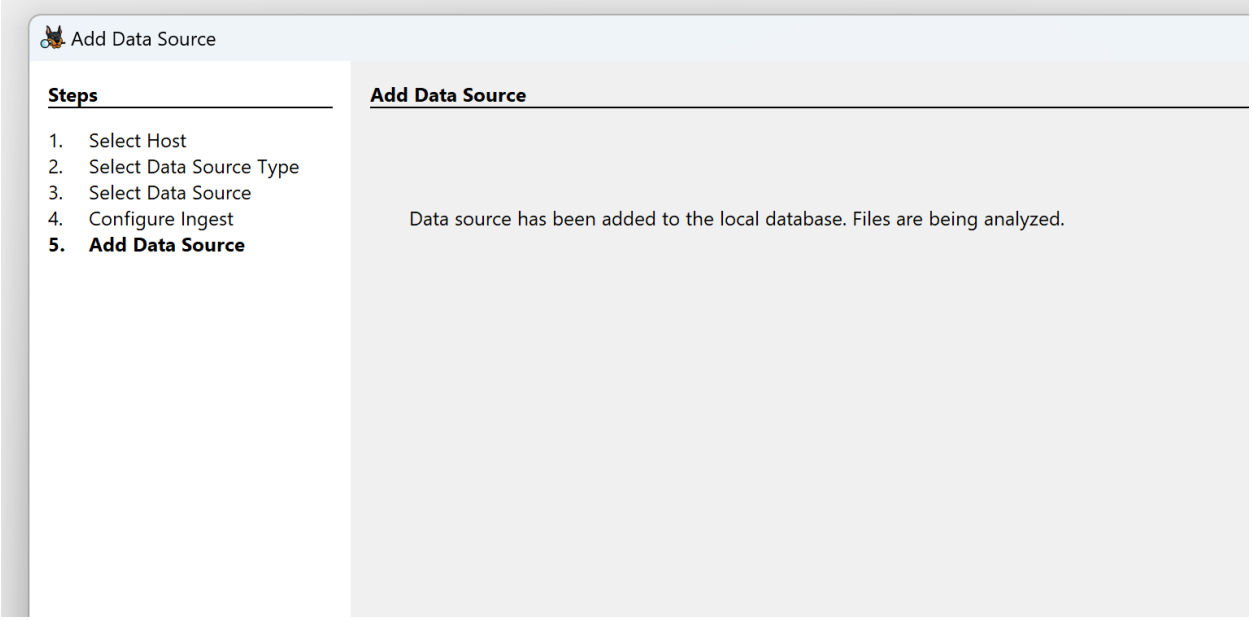
Step 3 :
C.

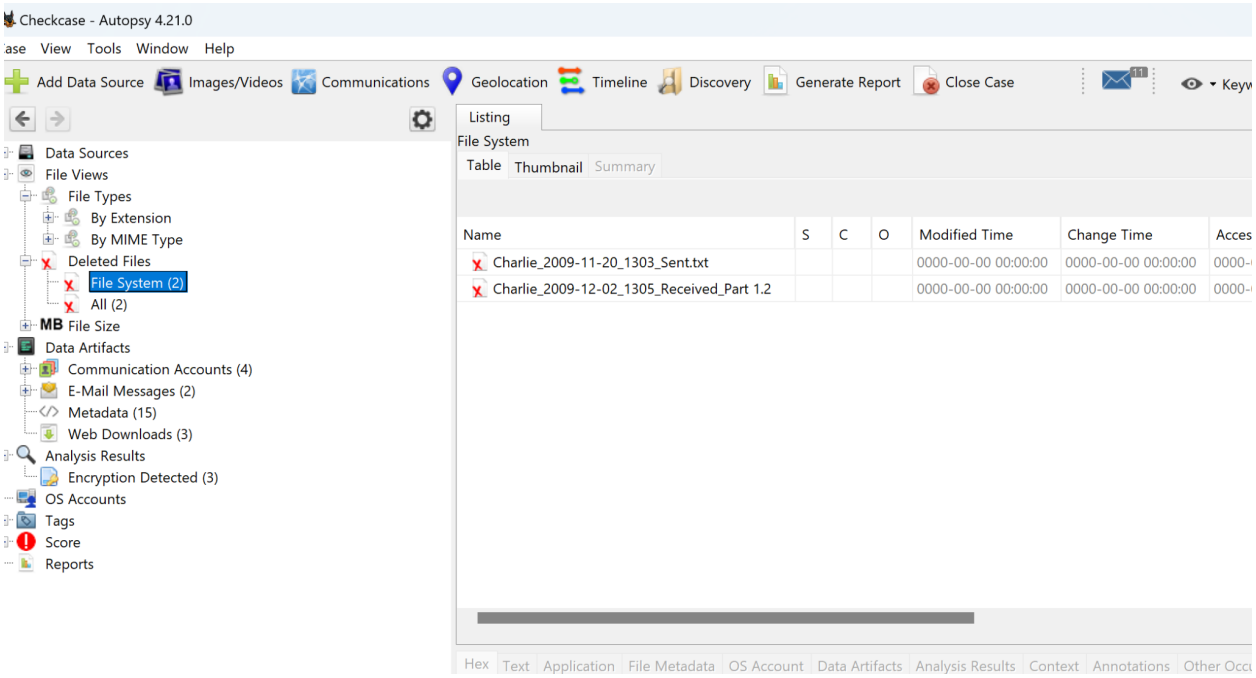
corpora/scenarios/2009-m57-patents/usb/ files:

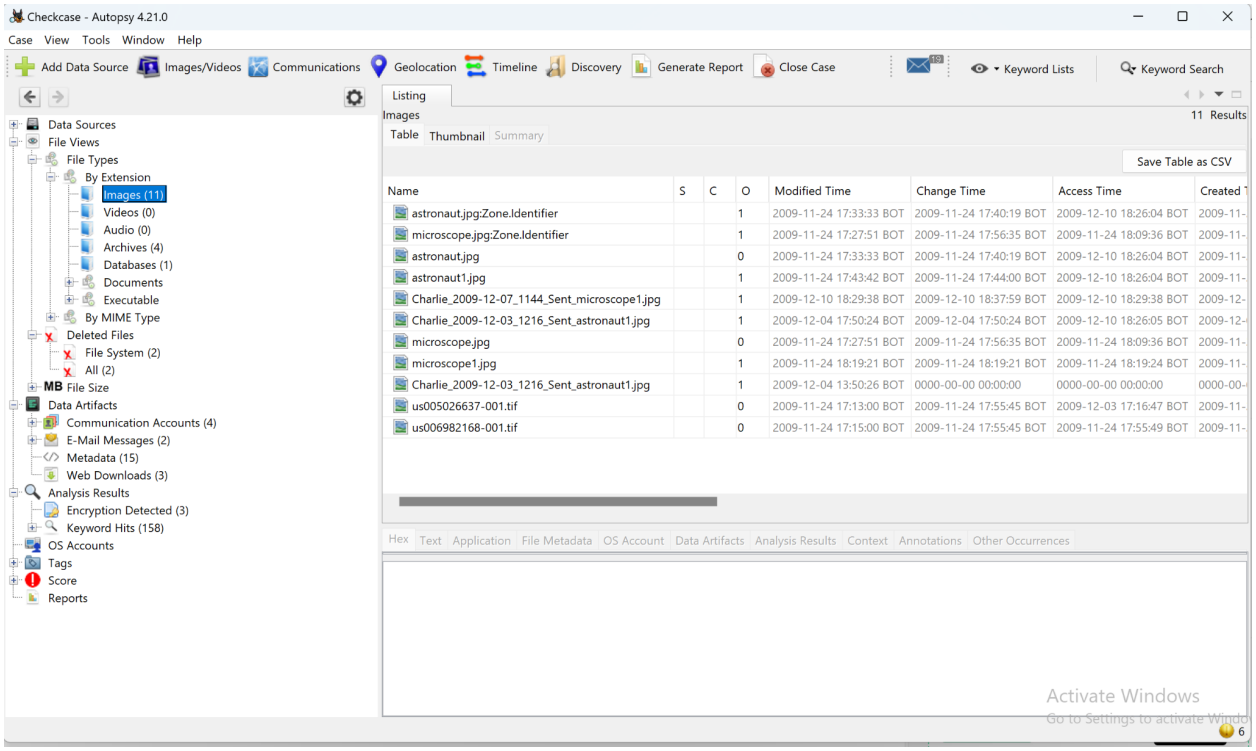
SHOW FILE HASHES

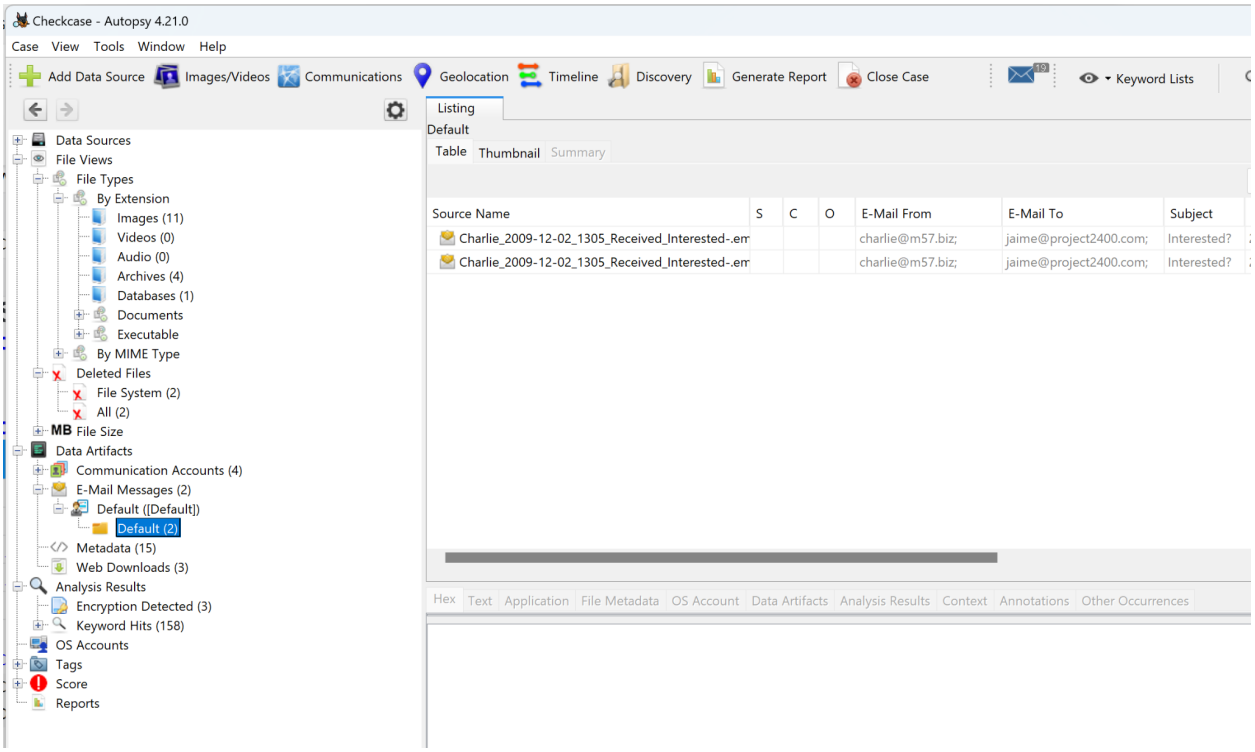
Name	Size	Last Modified
charlie-work-usb-2009-12-11.E01	9,265,553	2020-11-22 09:40:13Z
jo-favorites-usb-2009-12-11.E01	227,073,046	2020-11-22 09:40:15Z
jo-work-usb-2009-12-11.E01	118,233,120	2020-11-22 09:40:39Z
terry-work-usb-2009-12-11.E01	33,499,203	2020-11-22 09:40:41Z

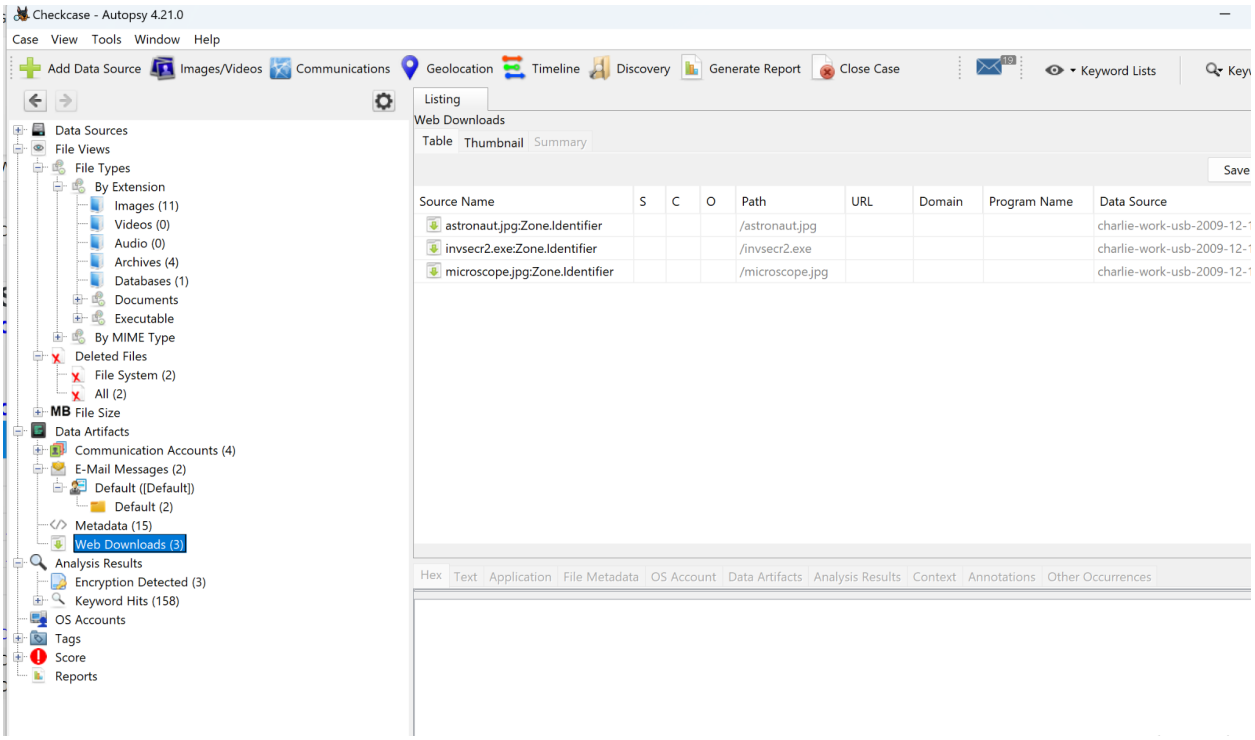
Corpora | Reports | File Dump | About

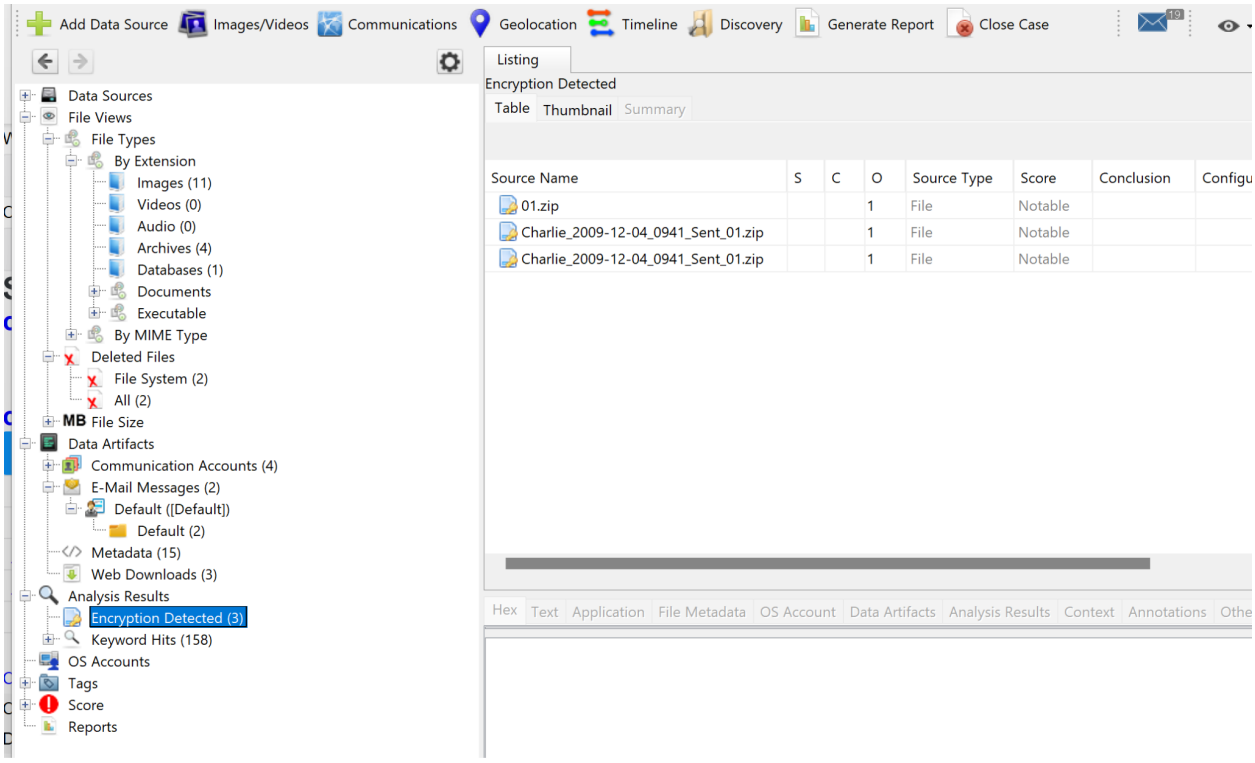



Checkcase - Autopsy 4.21.0
ase View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Data Sources
File Views
File Types
By Extension
By MIME Type
Deleted Files
File System (2)
All (2)
File Size
Data Artifacts
Communication Accounts (4)
E-Mail Messages (2)
Metadata (15)
Web Downloads (3)
Analysis Results
Encryption Detected (3)
OS Accounts
Tags
Score
Reports
Listing
File System
Table
Thumbnail
Summary
Name
S
C
O
Modified Time
Change Time
Charlie_2009-11-20_1303_Sent.txt
Charlie_2009-12-02_1305_Received_Part 1.2
0000-00-00 00:00:00
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations

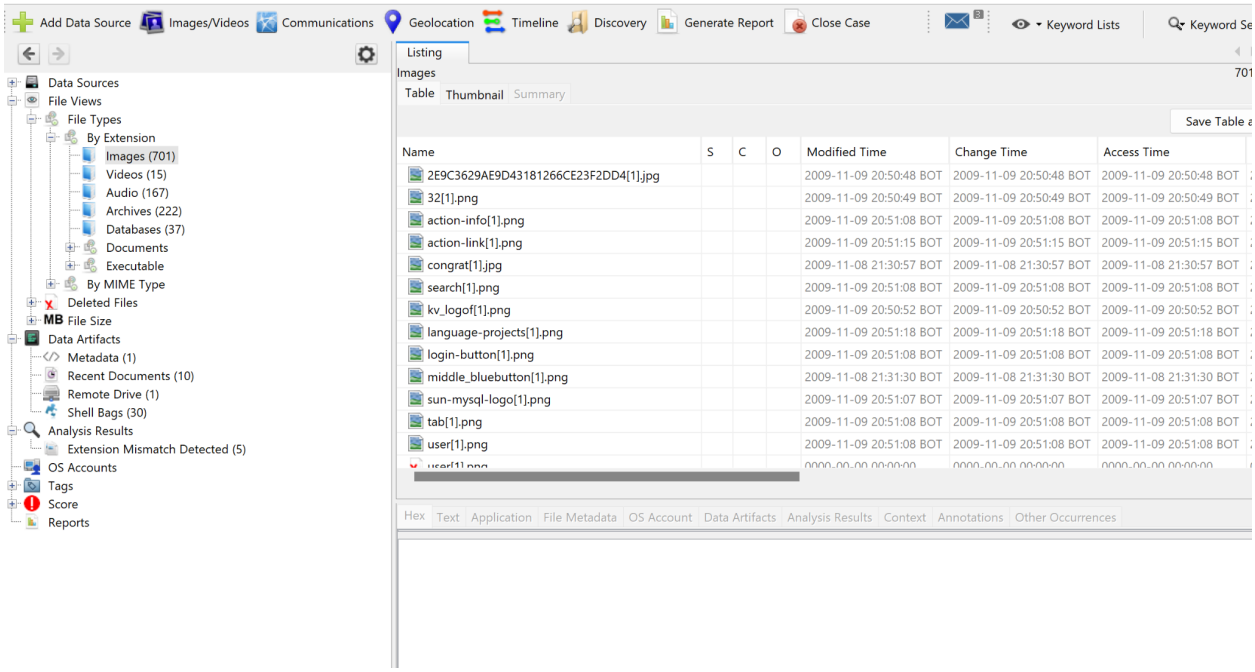

Checkcase - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
By Extension
Images (11)
Videos (0)
Audio (0)
Archives (4)
Databases (1)
Documents
Executable
By MIME Type
Deleted Files
File System (2)
All (2)
File Size
Data Artifacts
Communication Accounts (4)
E-Mail Messages (2)
Metadata (15)
Web Downloads (3)
Analysis Results
Encryption Detected (3)
Keyword Hits (158)
OS Accounts
Tags
Score
Reports
Listing
Images
11 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created
astronaut.jpg:Zone.Identifier
microscope.jpg:Zone.Identifier
astronaut.jpg
astronaut1.jpg
Charlie_2009-12-07_1144_Sent_microscope1.jpg
Charlie_2009-12-03_1216_Sent_astronaut1.jpg
microscope.jpg
microscope1.jpg
Charlie_2009-12-03_1216_Sent_astronaut1.jpg
us005026637-001.tif
us006982168-001.tif
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Activate Windows

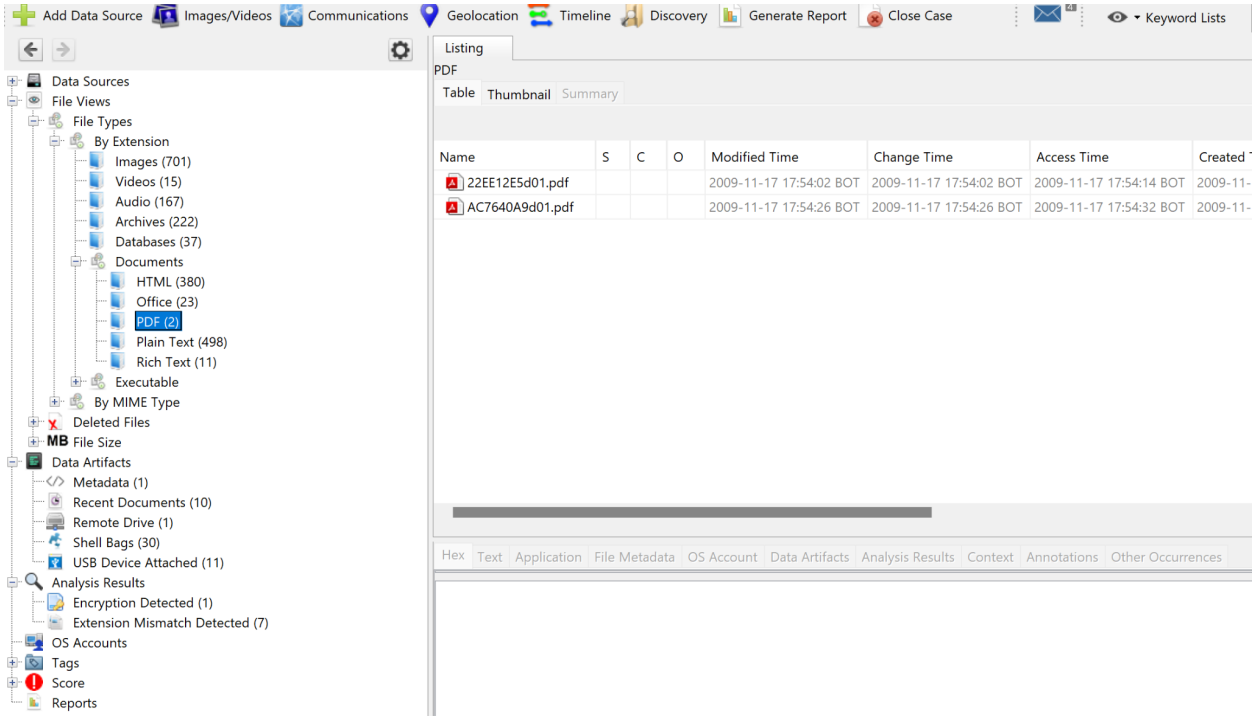

Checkcase - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Listing
Default
Table Thumbnail Summary
Source Name S C O E-Mail From E-Mail To Subject
Charlie_2009-12-02_1305_Received_Interested-.em charlie@m57.biz; jaime@project2400.com; Interested?
Charlie_2009-12-02_1305_Received_Interested-.em charlie@m57.biz; jaime@project2400.com; Interested?
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Data Sources
File Views
File Types
By Extension
Images (11)
Videos (0)
Audio (0)
Archives (4)
Databases (1)
Documents
Executable
By MIME Type
Deleted Files
File System (2)
All (2)
File Size
Data Artifacts
Communication Accounts (4)
E-Mail Messages (2)
Default ([Default])
Default (2)
Metadata (15)
Web Downloads (3)
Analysis Results
Encryption Detected (3)
Keyword Hits (158)
OS Accounts
Tags
Score
Reports


Checkcase - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Listing
Web Downloads
Table Thumbnail Summary
Save
Source Name S C O Path URL Domain Program Name Data Source
astronaut.jpg:Zone.Identifier /astronaut.jpg charlie-work-usb-2009-12-
invsecr2.exe:Zone.Identifier /invsecr2.exe charlie-work-usb-2009-12-
microscope.jpg:Zone.Identifier /microscope.jpg charlie-work-usb-2009-12-
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Data Sources
File Views
File Types
By Extension
Images (11)
Videos (0)
Audio (0)
Archives (4)
Databases (1)
Documents
Executable
By MIME Type
Deleted Files
File System (2)
All (2)
File Size
Data Artifacts
Communication Accounts (4)
E-Mail Messages (2)
Default ([Default])
Default (2)
Metadata (15)
Web Downloads (3)
Analysis Results
Encryption Detected (3)
Keyword Hits (158)
OS Accounts
Tags
Score
Reports


Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Listing
Encryption Detected
Table
Thumbnail
Summary
Source Name
S
C
O
Source Type
Score
Conclusion
01.zip
Charlie_2009-12-04_0941_Sent_01.zip
Charlie_2009-12-04_0941_Sent_01.zip
Data Sources
File Views
File Types
By Extension
Images (11)
Videos (0)
Audio (0)
Archives (4)
Databases (1)
Documents
Executable
By MIME Type
Deleted Files
File System (2)
All (2)
File Size
Data Artifacts
Communication Accounts (4)
E-Mail Messages (2)
Default ([Default])
Default (2)
Metadata (15)
Web Downloads (3)
Analysis Results
Encryption Detected (3)
Keyword Hits (158)
OS Accounts
Tags
Score
Reports

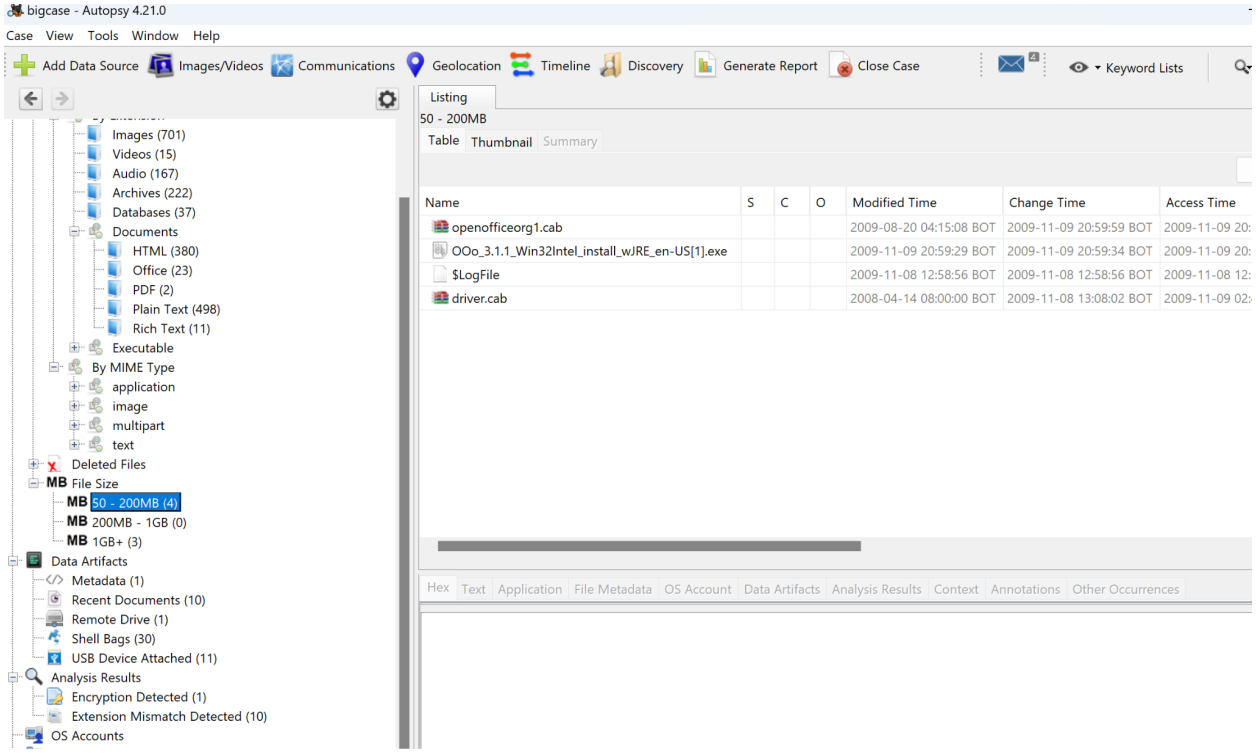
D.


Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Listing
Images
Table
Thumbnail
Summary
Name
S
C
O
Modified Time
Change Time
Access Time
2E9C3629AE9D43181266CE23F2DD4[1].jpg
32[1].png
action-info[1].png
action-link[1].png
congrat[1].jpg
search[1].png
kv_logof[1].png
language-projects[1].png
login-button[1].png
middle_bluebutton[1].png
sun-mysql-logo[1].png
tab[1].png
user[1].png
Data Sources
File Views
File Types
By Extension
Images (701)
Videos (15)
Audio (167)
Archives (222)
Databases (37)
Documents
Executable
By MIME Type
Deleted Files
File Size
Data Artifacts
Metadata (1)
Recent Documents (10)
Remote Drive (1)
Shell Bags (30)
Analysis Results
Extension Mismatch Detected (5)
OS Accounts
Tags
Score
Reports

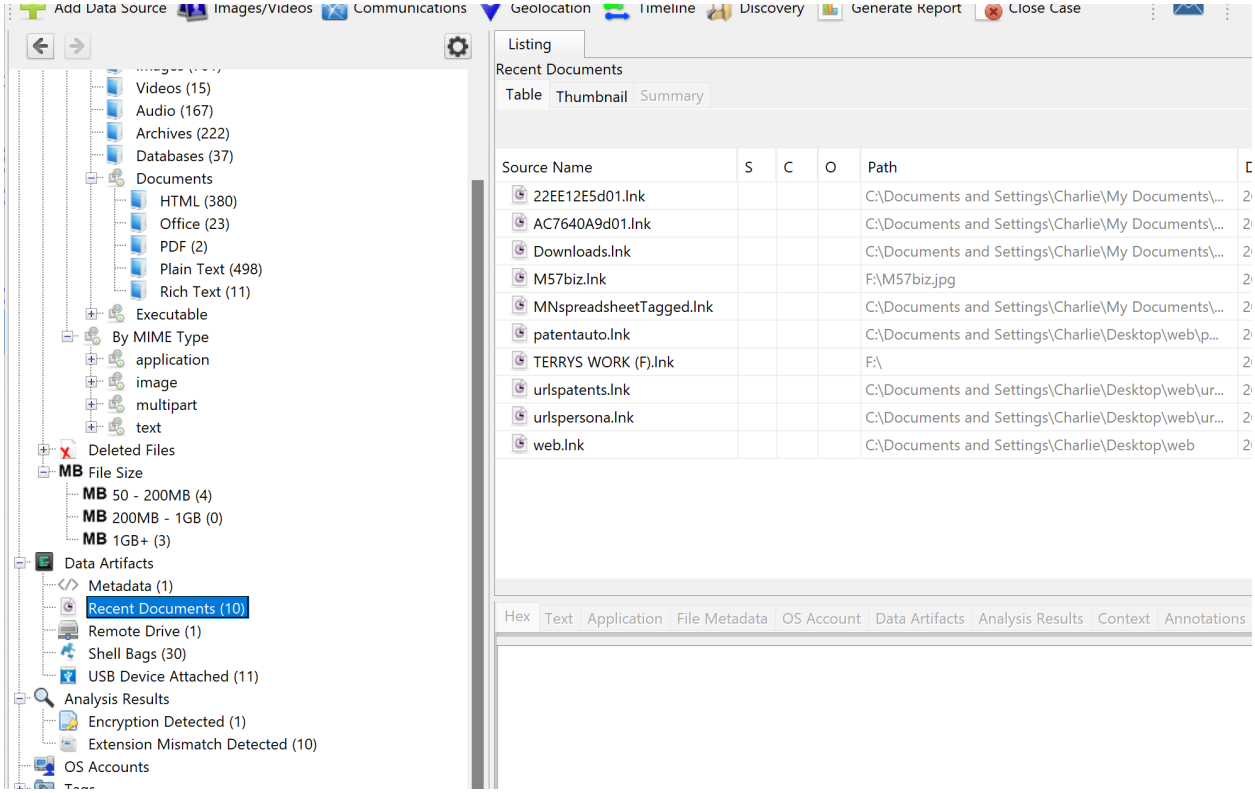


There were two pdf files

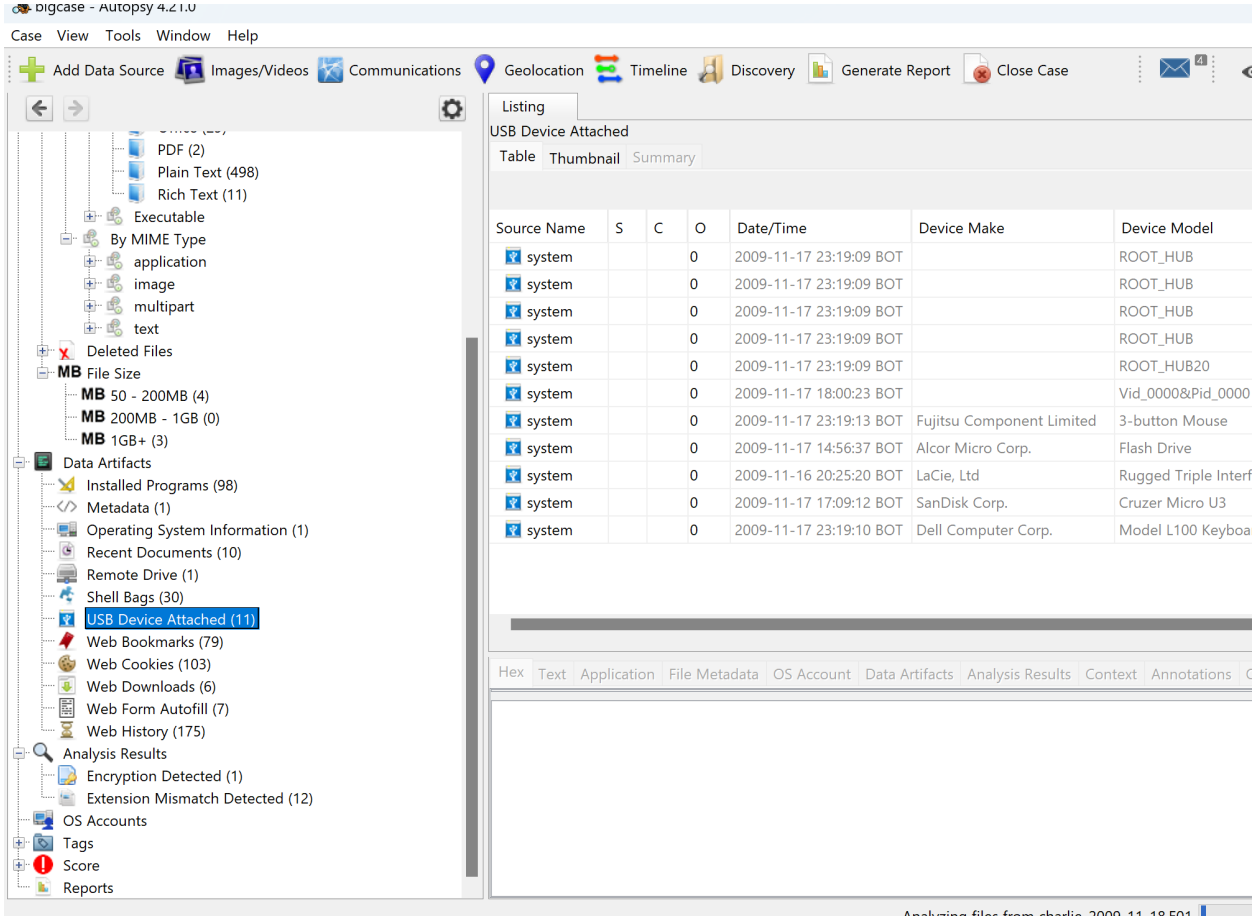
These are the larger files :



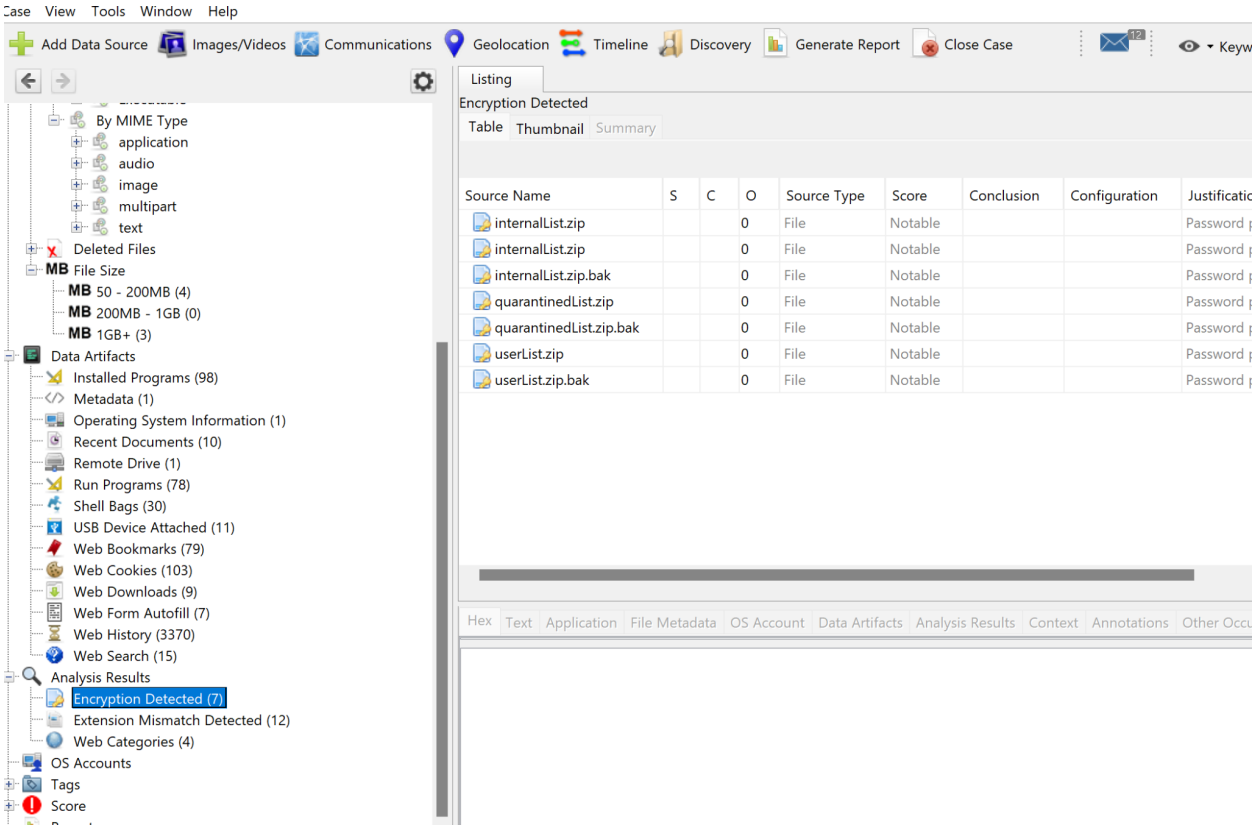
Recently opened documents :



USB Device attached :


bigcase - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
PDF (2)
Plain Text (498)
Rich Text (11)
Executable
By MIME Type
application
image
multipart
text
Deleted Files
File Size
50 - 200MB (4)
200MB - 1GB (0)
1GB+ (3)
Data Artifacts
Installed Programs (98)
Metadata (1)
Operating System Information (1)
Recent Documents (10)
Remote Drive (1)
Shell Bags (30)
USB Device Attached (11)
Web Bookmarks (79)
Web Cookies (103)
Web Downloads (6)
Web Form Autofill (7)
Web History (175)
Analysis Results
Encryption Detected (1)
Extension Mismatch Detected (12)
OS Accounts
Tags
Score
Reports
Listing
USB Device Attached
Table
Thumbnail
Summary
Source Name
S
C
O
Date/Time
Device Make
Device Model
system 0 2009-11-17 23:19:09 BOT ROOT_HUB
system 0 2009-11-17 23:19:09 BOT ROOT_HUB
system 0 2009-11-17 23:19:09 BOT ROOT_HUB
system 0 2009-11-17 23:19:09 BOT ROOT_HUB
system 0 2009-11-17 23:19:09 BOT ROOT_HUB20
system 0 2009-11-17 18:00:23 BOT Vid_0000&Pid_0000
system 0 2009-11-17 23:19:13 BOT Fujitsu Component Limited 3-button Mouse
system 0 2009-11-17 14:56:37 BOT Alcor Micro Corp. Flash Drive
system 0 2009-11-16 20:25:20 BOT LaCie, Ltd Rugged Triple Interf
system 0 2009-11-17 17:09:12 BOT SanDisk Corp. Cruzer Micro U3
system 0 2009-11-17 23:19:10 BOT Dell Computer Corp. Model L100 Keyboa
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations

Encrypted files detected :



E.

Comments and Additional Activities

M57 dotBIZ

Use EnCase to examine the M57 Patents disk images.

- Most of EnCase features can be used on these images.
- They are big enough to be realistic, small enough so that the EnCase functionality will run in 5-30 minutes depending on the image being examined.

Try using FTK or SleuthKit to compare functionality.

Note: Terry's phone is not available in the corpus. However, several files that originated from the phone exist somewhere in the corpus. Can you find them? Are they related to the case?

Documentation on M57 Patent Eavesdropping.

Lab Analysis :
1. In the registry I able to collect the evidence about the USB, recent application, recent files, hardware connected and other important information needed for evidence that happens in windows machine.

2. In the RAM and Harddrive, I can able to see the login details, and all the system information and browser contents, with the data associated with the system is visible.

3. Steganography is performed by modifying the bits in the original image, by modifying the bits in way which is significant and reducing the R, G, B values a little bit, not showing much difference into the image and still performing the steganography, which is so cool in my opinion.

4. Bitstream is the copy of original image and it contains all the contents of the device including files, free space, slack space, metadata etc.
It is very important because :

- It acts as a backup
- It has timestamps for the evidence purposes.
- It acts as a disk image and all the analysis tool like autopsy work on bitstream not on original drives.
- Mainly it captures hidden data, especially deleted files.

Key Term Quiz :
1. Key
2. File slack
3. bitmap
4. Signature