

Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : Malware and Forensics

Lab : 10

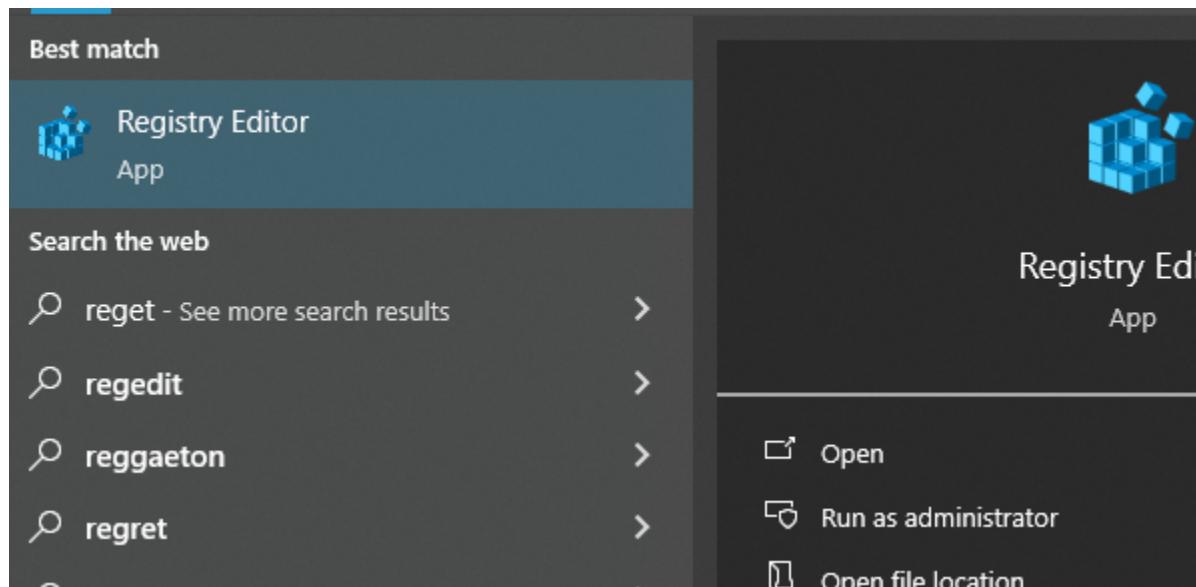
Chapter : 23 (Digital Forensics)

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
ab (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.

File Edit View Favorites Help

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

	Name	Type	Data
FirewallSync	ab (Default)	REG_SZ	(value not set)
NewNetworks	Category	REG_DWORD	0x00000000 (0)
Nla	DateCreated	REG_BINARY	e7 07 01 00 05 00 06 00 0b 00 06 00 f0 00 2c 01
Permissions	DateLastConnec...	REG_BINARY	e7 07 01 00 05 00 06 00 0b 00 06 00 f0 00 2e 01
Policies	ab Description	REG_SZ	SRIHER CAMPUS WIFI 1
Profiles	Managed	REG_DWORD	0x00000000 (0)
{1A697866-3C35-461C-A248-71}	NameType	REG_DWORD	0x00000047 (71)
{214A5BBC-67F4-47C4-8824-81}	ab ProfileName	REG_SZ	SRIHER CAMPUS WIFI 1
{23055E6A-8D65-4C6E-8335-05}			
{2C139C79-11F9-4220-9D37-8E}			
{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-C			
{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-4			
{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			

C.

The screenshot shows the DCode v5.5 application interface. On the left, a tree view displays registry keys under 'crosFotoWindows NT\CurrentVersion\NetworkList\Profiles'. The 'Oswald Family' key is selected. The main pane shows a table of registry values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	e7070a00000008001000330009000003
DateLastConnec...	REG_BINARY	e7070a0001001e001600270011004e03
Description	REG_SZ	Oswald Family
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD	0x00000047 (71)
ProfileName	REG_SZ	Oswald Family

Below the table is a timestamp conversion tool. It shows several timestamp entries:

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

The 'Value Input' section contains a hex value 'e7070a00000008001000330009000003' in 'Hexadecimal (Little-Endian)' format, with a 'Decode' button. The 'Time Zone' section shows '(UTC-05:00) Eastern Time (US & Canada)' with 'No Adjustment' and 'Select' buttons. The 'Date Output' section shows a pattern 'yyyy'-MM'-dd HH':mm':ss',ffffffff K' and a sample value '2023-10-30 23:37:28.7450415 -04:00' with a 'Default' button.

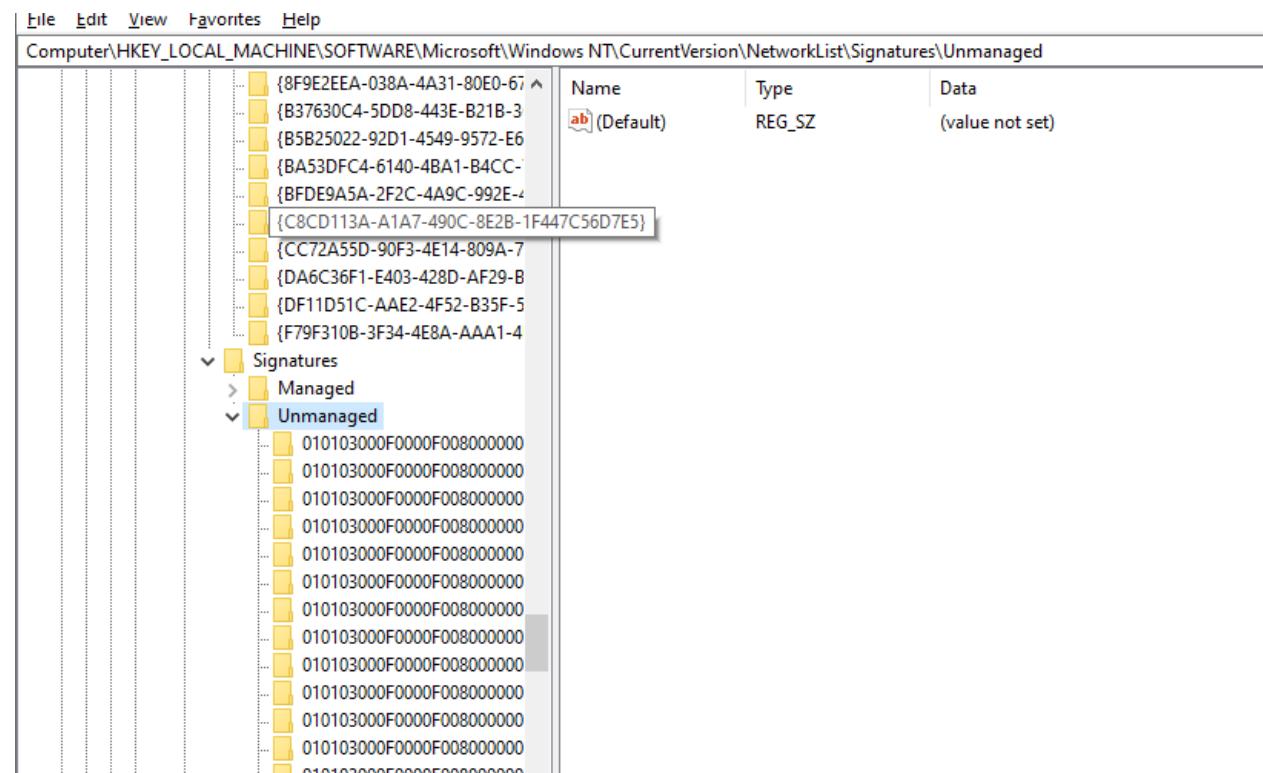
This screenshot is identical to the one above, showing the same registry key structure, table of values, and timestamp conversion interface in the DCode v5.5 application.

D.

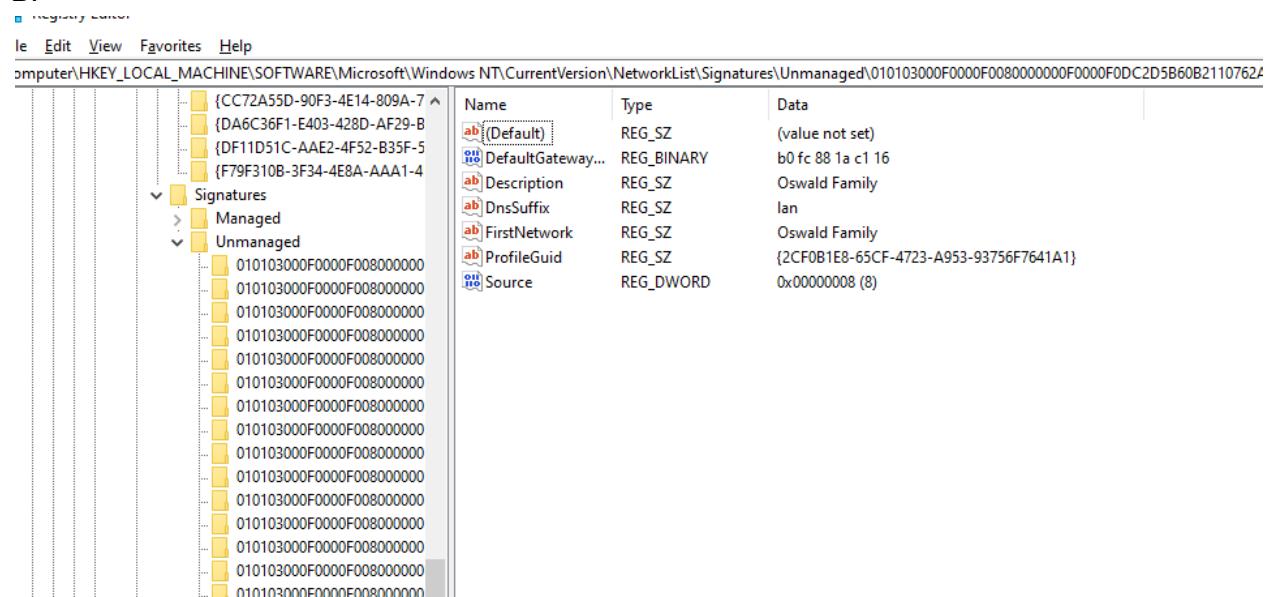
These wifi connections and information like last connected are very useful to understand about and store evidence on particular ssid, if we come to find it has any issues or caused any incident, it will be great practice for collecting evidence and reverse engineering the problem.

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.

File	Edit	View	Favorites	Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{a20b06cb-7177-4ad4-8b5b-748546a81f06}				

Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForce...	REG_DWORD	0x00000000 (0)
DhcpDefaultGat...	REG_MULTI_SZ	192.168.1.1
DhcpDomain	REG_SZ	lan
DhcpGatewayH...	REG_BINARY	c0 a8 01 01 06 00 00 b0 fc 88 1a c1 16
DhcpGatewayH...	REG_DWORD	0x00000001 (1)
DhcpInterfaceO...	REG_BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2c 49...
DhcpIPAddress	REG_SZ	192.168.1.35
DhcpNameServer	REG_SZ	192.168.1.1
DhcpNetworkInt	REG_SZ	F4377716C646026416D696C697
DhcpServer	REG_SZ	192.168.1.1
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMas...	REG_MULTI_SZ	255.255.255.0
Domain	REG_SZ	
EnableDHCP	REG_DWORD	0x00000001 (1)
IsServerNapAware	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x0000a8c0 (43200)
LeaseObtainedTi...	REG_DWORD	0x654068d5 (1698719957)
LeaseTerminates...	REG_DWORD	0x65411195 (1698763157)
NameServer	REG_SZ	
T1	REG_DWORD	0x6540bd35 (1698741557)
T2	REG_DWORD	0x6540fc7d (1698757757)

B.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DefaultGateway	REG_MULTI_SZ	
DefaultGateway...	REG_MULTI_SZ	
DhcpConnForce...	REG_DWORD	0x00000000 (0)
DhcpDefaultGat...	REG_MULTI_SZ	172.17.0.1
DhcpGatewayH...	REG_BINARY	ac 11 00 01 06 00 00 00 00 10 f3 80 5f dc
DhcpGatewayH...	REG_DWORD	0x00000001 (1)
DhcpInterfaceO...	REG_BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00 bb 5f...
DhcpIPAddress	REG_SZ	0.0.0.0
DhcpNameServer	REG_SZ	8.8.8.4.2.2.2
DhcpServer	REG_SZ	172.17.0.1
DhcpSubnetMask	REG_SZ	255.0.0.0
DhcpSubnetMas...	REG_MULTI_SZ	255.255.224.0
Domain	REG_SZ	
EnableDHCP	REG_DWORD	0x00000001 (1)
IPAddress	REG_MULTI_SZ	
IsServerNapAware	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x00005460 (21600)
LeaseObtainedTi...	REG_DWORD	0x63a2b8eb (1671608555)
LeaseTerminates...	REG_DWORD	0x63a30d4b (1671630155)
NameServer	REG_SZ	
RegisterAdapter...	REG_DWORD	0x00000000 (0)
RegistrationEna...	REG_DWORD	0x00000001 (1)
SubnetMask	REG_MULTI_SZ	
T1	REG_DWORD	0x63a2e31b (1671619355)
T2	REG_DWORD	0x63a302bf (1671627455)

C.

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

Step 4 :

A.

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 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 6e 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 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.

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 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 6e 00 63 00 68 00 61 00 69 00...
12	REG_BINARY	
13	REG_BINARY	
14	REG_BINARY	
15	REG_BINARY	
16	REG_BINARY	
17	REG_BINARY	
18	REG_BINARY	
19	REG_BINARY	
2	REG_BINARY	
3	REG_BINARY	
4	REG_BINARY	
5	REG_BINARY	
6	REG_BINARY	
7	REG_BINARY	
8	REG_BINARY	
9	REG_BINARY	
MRUListEx	REG_BINARY	

Value name:

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	S	.
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	7
00000050	65	70	6F	72	74	5F	49	4E	e	p	o	r	T
00000058	44	35	30	30	2F	6C	6F	6R	T	s	a	T	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'.ffffffff K

Sample: 2023-11-01 21:41:55.6089924 -04:00

Default

www.digital-detective.net

C.

DISCARDED

Name	Type	Data
MRUListEx		

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																

X

OK Cancel

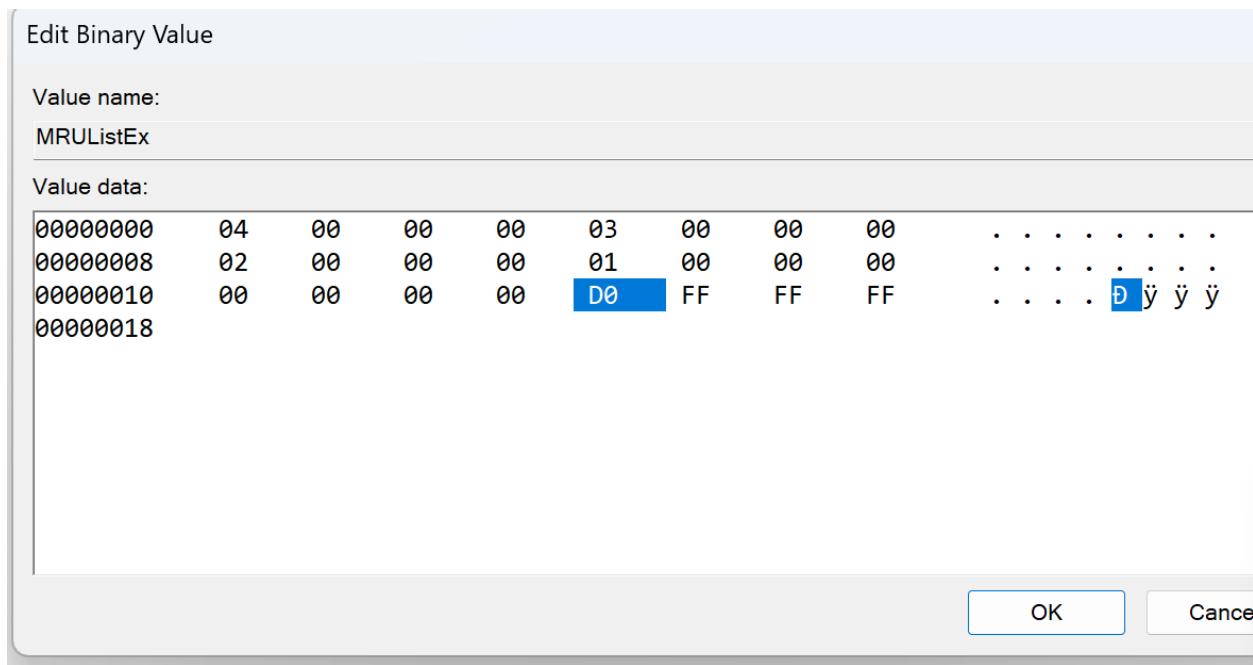
TabletMod

Taskband

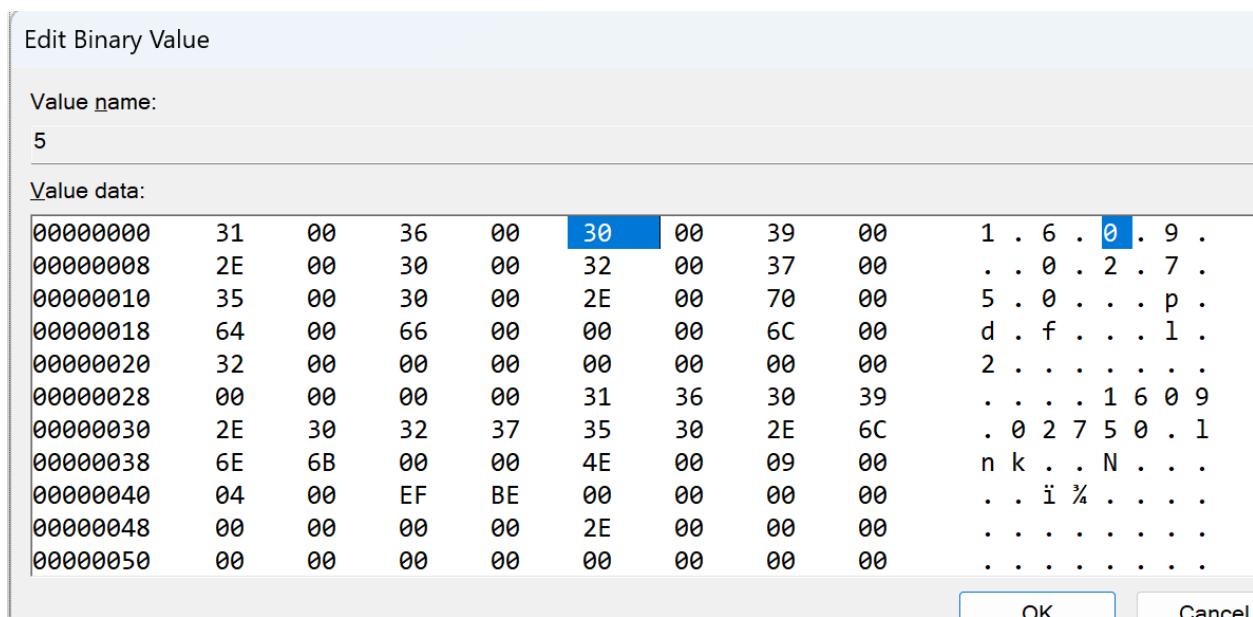
UI Client

D.

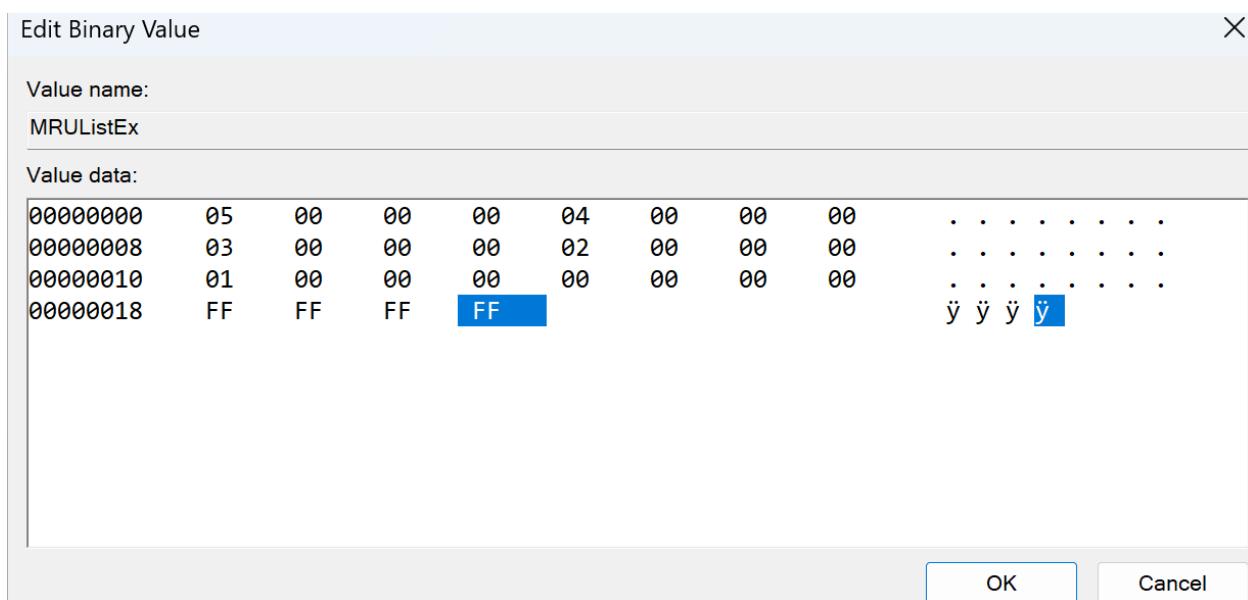
Recent file i worked on



E.



FF is 30 :

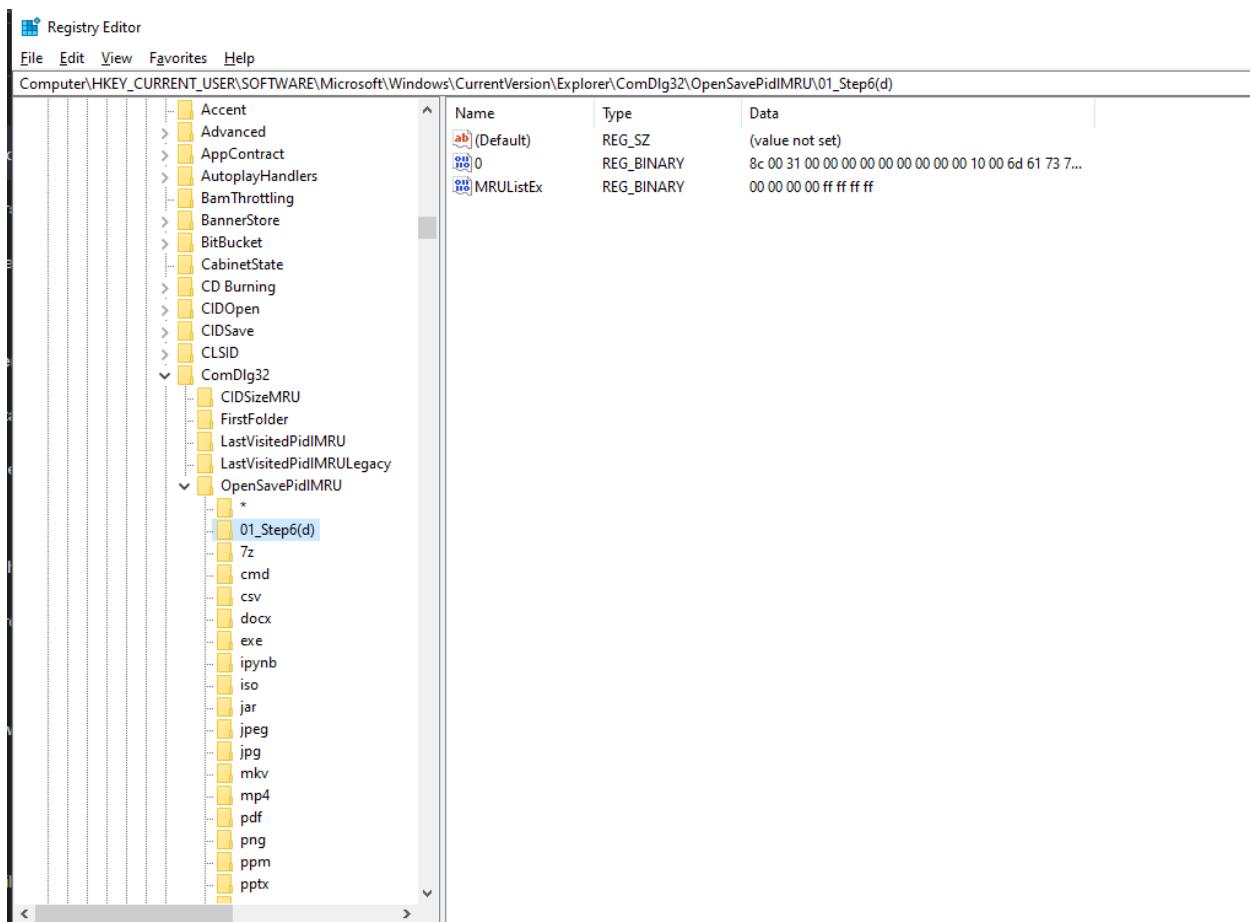


F.

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.



B.

Accent

Name	Type	Data
MRUListEx	REG_BINARY	e0 4f d0 20 ea 3a 69 10 a2 d8 C
01_Step6(d)	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
7z	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
cmd	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
csv	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
docx	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
exe	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
ipynb	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
iso	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
jar	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C

Accent

Name	Type	Data
5	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
01_Step6(d)	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
7z	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
cmd	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C
csv	REG_BINARY	14 00 1f 50 e0 4f d0 20 ea 3a 69 10 a2 d8 C

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.

Registry Editor			
File	Edit	View	Favorites Help
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidIMRU			
Name	Type	Data	
(Default)	REG_SZ	(value not set)	
0	REG_BINARY	6e 00 6f 00 74 00 65 00 70 00 61 00 64 00 2e 00 65 00...	
1	REG_BINARY	6d 00 73 00 65 00 64 00 67 00 65 00 2e 00 65 00 78 0...	
10	REG_BINARY	7b 00 43 00 35 00 41 00 41 00 44 00 45 00 32 00 36 0...	
11	REG_BINARY	7b 00 35 00 36 00 37 00 45 00 45 00 33 00 38 00 43 0...	
12	REG_BINARY	73 00 74 00 61 00 74 00 73 00 2e 00 65 00 78 00 65 0...	
13	REG_BINARY	62 00 72 00 61 00 76 00 65 00 2e 00 65 00 78 00 65 0...	
14	REG_BINARY	7b 00 30 00 34 00 38 00 42 00 41 00 44 00 33 00 35 0...	
15	REG_BINARY	76 00 6d 00 70 00 6c 00 61 00 79 00 65 00 72 00 2e 0...	
16	REG_BINARY	65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 0...	
17	REG_BINARY	56 00 69 00 72 00 74 00 75 00 61 00 6c 00 42 00 6f 00...	
18	REG_BINARY	76 00 6d 00 77 00 61 00 72 00 65 00 2e 00 65 00 78 0...	
2	REG_BINARY	50 00 69 00 63 00 6b 00 65 00 72 00 48 00 6f 00 73 0...	
3	REG_BINARY	54 00 65 00 6c 00 65 00 67 00 72 00 61 00 6d 00 2e 0...	
4	REG_BINARY	7b 00 34 00 38 00 30 00 41 00 38 00 37 00 32 00 41 0...	
5	REG_BINARY	6d 00 73 00 70 00 61 00 69 00 6e 00 74 00 2e 00 65 0...	
6	REG_BINARY	56 00 69 00 72 00 74 00 75 00 61 00 6c 00 42 00 6f 00...	
7	REG_BINARY	63 00 68 00 72 00 6f 00 6d 00 65 00 2e 00 65 00 78 0...	
8	REG_BINARY	43 00 6f 00 64 00 65 00 2e 00 65 00 78 00 65 00 00 00...	
9	REG_BINARY	65 00 63 00 6c 00 69 00 70 00 73 00 65 00 2e 00 65 00...	
MRUListEx	REG_BINARY	07 00 00 00 03 00 00 05 00 00 05 00 00 12 00 00 00 0d 0...	

B.

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\explorer\ComDlg32\LastVisitedFileList

Accent

Value name: MRUListEx

Value data:

00000000	07	00	00	00	03	00	00	00	set)
00000008	05	00	00	00	12	00	00	00	74 00 65 00 70 00 61 00 64 0C
00000010	0D	00	00	00	0F	00	00	00	0 65 00 64 00 67 00 65 00 2e 0
00000018	06	00	00	00	11	00	00	00	0 35 00 41 00 41 00 44 00 45 0
00000020	00	00	00	00	10	00	00	00	0 36 00 37 00 45 00 45 00 33 0
00000028	0E	00	00	00	04	00	00	00	0 61 00 74 00 73 00 2e 00 65 0
00000030	02	00	00	00	0A	00	00	00	0 61 00 76 00 65 00 2e 00 65 0
00000038	0C	00	00	00	0B	00	00	00	0 34 00 38 00 42 00 41 00 44 0
00000040	09	00	00	00	08	00	00	00	0 70 00 6c 00 61 00 79 00 65 0
00000048	01	00	00	00	FF	FF	FF	FF y y y y	0 70 00 6c 00 6f 00 72 00 65 0C
00000050										0 70 00 6c 00 6f 00 72 00 61 0

OK Cancel

01_Step6(d) 7z cmd csv docx

Accent

Value name: 3

Value data:

00000000	54	00	65	00	6C	00	65	00	T . e . l . e .	set)
00000008	67	00	72	00	61	00	6D	00	g . r . a . m .	74 00 65 00 70 C
00000010	2E	00	65	00	78	00	65	00	. . e . x . e .	0 65 00 64 00 67
00000018	00	00	14	00	1F	50	E0	4F P à O	0 35 00 41 00 41
00000020	D0	20	EA	3A	69	10	A2	D8	Ø ê : i . ¢ Ø	0 36 00 37 00 45
00000028	08	00	2B	30	30	9D	14	00	. . + 0 0 . . .	0 61 00 74 00 73 I
00000030	2E	80	D4	3A	AD	24	69	A5	. . Ø : - \$ i ¥	0 61 00 76 00 65 I
00000038	30	45	98	E1	AB	02	F9	41	Ø E . á « . ù A	0 34 00 38 00 42
00000040	7A	A8	00	00					z . . .	0 70 00 6c 00 6f 0

OK Cancel

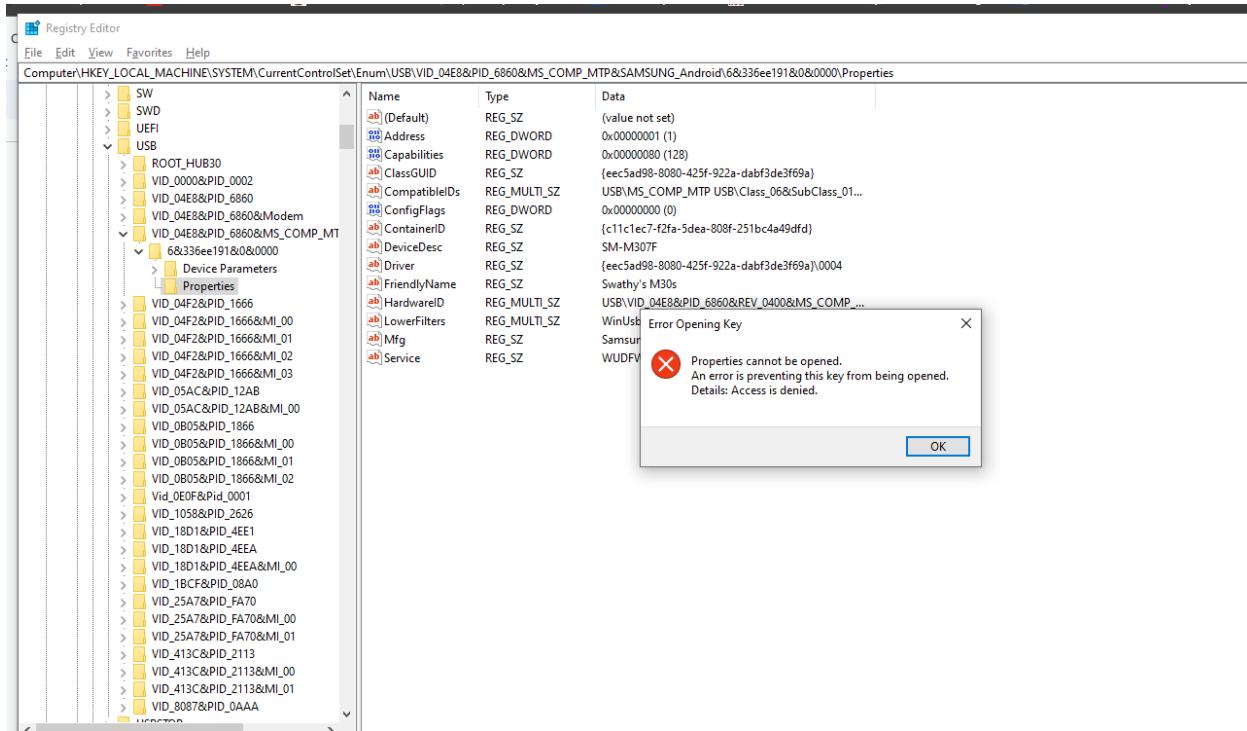
01_Step6(d) 7z cmd csv docx

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.

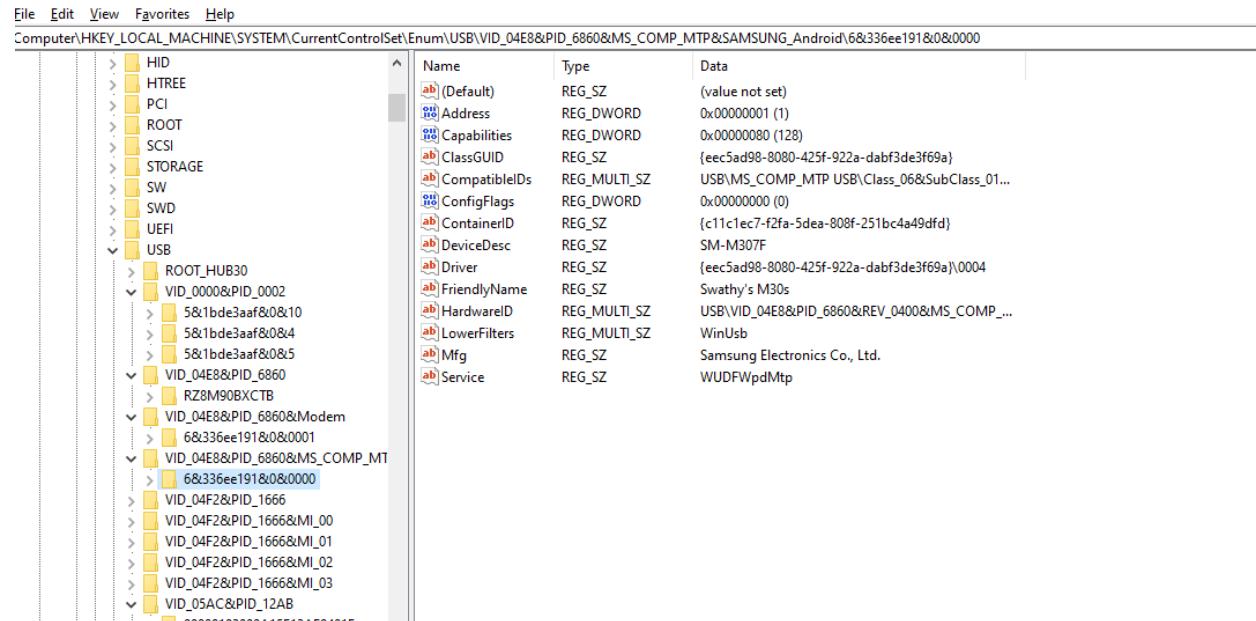
Step 7 :

A.



B.

This device is plugged into my system

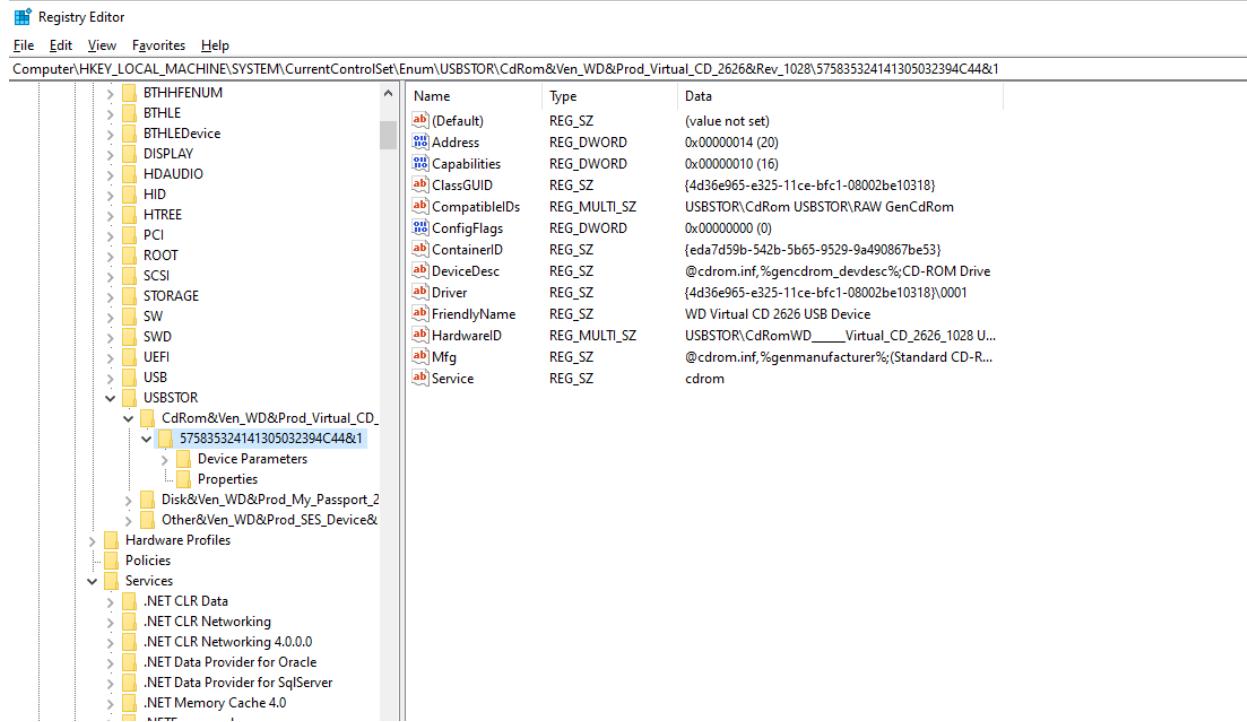


C.

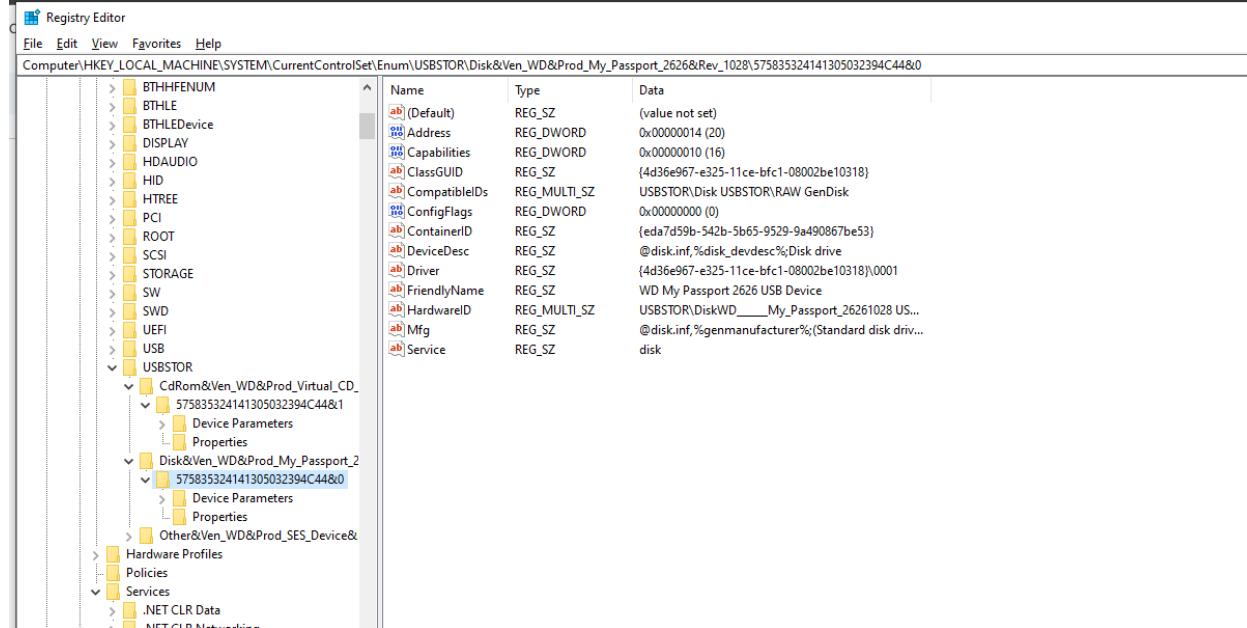
We can trace back and find evidence about the external device that has been connected to the system, if it is not a relative or friendly device, we can have it as the evidence and we can know the hardware of the device connected.

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

The screenshot shows the Grammarly website interface. On the left, there's a sidebar with links for 'My Grammarly', 'Trash', 'Account', 'Apps', and 'Premium'. A modal window titled 'Using Grammarly for work?' is open, encouraging users to get Grammarly Business for their entire team. The main area displays a search bar and a grid of search results. One result is highlighted in red: 'Implementing Cryptographic algorithms for securing data transactions.' by Swathy Ragupathy_ML Resume. Other results include 'Project Proposal In' and 'Revision is a'.

B.

The screenshot shows the HxD hex editor with the file 'msedge.exe (1188)' loaded. The main pane displays memory dump data with columns for 'Offset(h)', 'Decoded text', and 'Hex'. The 'Decoded text' column shows various characters and symbols. The right side of the interface includes 'Special editors' and 'Data inspector' panes, which are mostly empty or show invalid data for most formats. At the bottom, there are options for 'Byte order' (set to Little endian) and 'Overwrite'.

C.

HxD - [msedge.exe (6720)]

File Edit Search View Analysis Tools Window Help

16 Windows (ANSI) hex

msedge.exe (916) msedge.exe (6720)

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
5FF801753700	75 6D 35 20 78 31 6E 32 6F 6E 72 36 20 78 68 38	um5 xln2onr6 xh8
5FF801753710	79 65 6A 33 F8 5F 00 00 40 54 06 02 F8 5F 00 00	ye3ø_@T..ø_..
5FF801753720	01 00 00 00 1C 00 00 00 01 00 00 00 73 63 6F 6Escon
5FF801753730	74 65 6E 74 2D 6C 67 61 33 2D 32 2E 78 78 2E 66	tent-lga3-2.xx.f
5FF801753740	62 63 64 6E 2E 6E 65 74 54 00 00 68 70 00 00	bcdn.netT..hp..
5FF801753750	01 00 00 00 1D 00 00 00 05 05 8A 17 3A 72 31 65Š..:rl
5FF801753760	3A 20 3A 72 31 66 3A 20 3A 72 31 67 3A 20 3A 72	: :rlf: :rlg: :r
5FF801753770	31 69 3A 20 3A 72 31 68 3A 54 06 02 F8 5F 00 00	li: :rlh:T..ø_..
5FF801753780	01 00 00 00 18 00 00 00 05 E3 CF EF 54 54 70 58äiTTpX
5FF801753790	6F 77 41 78 38 48 64 34 48 46 2F 4C 39 77 38 54	owAx8Hd4HF/L9w8T
5FF8017537A0	41 41 3D 3D 6C 69 63 79 74 61 62 6C 65 00 00	AA==licytable..
5FF8017537B0	02 00 00 00 17 00 00 00 05 80 D1 37 64 69 6E 6FEN7dino
5FF8017537C0	74 68 75 6E 64 65 72 6B 70 40 67 6D 61 69 6C 2E	thunderkp@gmail.
5FF8017537D0	63 6F 61 00 00 00 00 00 00 00 00 00 00 00 00 00	com.....
5FF8017537E0	02 00 00 00 0E 00 00 00 00 9A E4 77 66 00 61 00šawf.a.
5FF8017537F0	76 00 69 00 63 00 6F 00 6E 00 4D 00 65 00 64 00	v.i.c.o.n.M.e.d.
5FF801753800	69 00 61 00 49 00 64 00 00 00 00 00 00 00 00 00	i.a.I.d.....
5FF801753810	01 00 00 00 22 00 00 00 01 41 90 EA 78 31 79 7A"-A.éxyz
5FF801753820	74 62 64 62 20 78 31 6E 32 6F 6E 72 36 20 78 68	tbdb xln2onr6 xh
5FF801753830	38 79 65 6A 33 20 78 31 6A 61 32 75 32 7A 00 00	8yej3 xlja2au2z..
5FF801753840	01 00 00 00 1D 00 00 00 05 00 A0 63 54 75 65 2CcTue,
5FF801753850	20 32 39 20 4F 63 74 20 32 30 32 34 20 31 39 3A	29 Oct 2024 19:
5FF801753860	35 30 3A 34 37 20 47 4D 54 77 6C 69 63 00 5D 00	50:47 GMTwlic.]
5FF801753870	01 00 00 00 10 00 00 00 00 E8 0E 5B 70 00 72 00è.[p.r.
5FF801753880	65 00 6B 00 65 00 79 00 47 00 65 00 6E 00 65 00	e.k.e.y.G.e.n.e.
5FF801753890	72 00 61 00 74 00 69 00 6F 00 6E 00 0D 00 00 00	r.a.t.i.o.n....
5FF8017538A0	01 00 00 00 12 00 00 00 00 68 CD 54 65 00 78 00hiTe.x.

Special editors

Data inspector

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 𩶫

UTF-8 code point Unexpected continuatio

Single (float32) 1.35634009257592E22

Byte order

Little endian Big endian

Hexadecimal basis (for integral numbers)

D.

017A43569FF0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
017A4356A000	017A4356A000 - 017A4356FFFF	
017A43570000	B8 4C 00 00 02 00 00 00 03 00 00 00 05 00 00 00	,L.....
017A43570010	5F 6D 63 5F 32 00 00 00 00 00 00 00 00 00 00 00	_mc_2.....
017A43570020	00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00
017A43570030	20 00 00 00 6A 6D 6A 66 6C 67 6A 70 63 70 65 70	...jmjf1lgjpcpep
017A43570040	65 61 66 6D 6D 67 64 70 66 6B 6F 67 6B 67 68 63	eafmmgdpfkogkghc
017A43570050	70 69 68 61 00 00 00 00 00 00 00 00 00 00 00 00	piha.....
017A43570060	01 00 00 00 0F 04 00 00 24 00 00 00 68 74 74 70\$.http
017A43570070	73 3A 2F 2F 63 68 72 6F 6D 65 2E 67 6F 6F 67 6C	s://chrome.googl
017A43570080	65 2E 63 6F 6D 2F 77 65 62 73 74 6F 72 65 2F 2A	e.com/webstore/*
017A43570090	00 00 00 00 01 00 00 00 03 E0 00 00 00 63 68 72 6F>...chro
017A435700A0	6D 65 2D 65 78 74 65 6E 73 69 6F 6E 3A 2F 2F 6A	me-extension://j
017A435700B0	6D 6A 66 6C 67 6A 70 63 70 65 70 65 61 66 6D 6D	mjf1lgjpcpepeafmm
017A435700C0	67 64 70 66 6B 6F 67 6B 67 68 63 70 69 68 61 2F	gdpfkogkghcpiha/
00 00 00 1E 00 00 00 37 00 00 00 07 00 00 007.....	
00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00ÿÿÿ.....	
00 00 00 00 00 00 00 80 70 B3 08 F8 5F 00 00€p..ø_..	
00 00 00 00 00 00 00 FF FF FF FF FF FF FF 7Fÿÿÿÿÿÿ.	
74 74 70 73 00 AA	https.....	
AA AA AA AA AA AA 05 66 61 63 65 62 6F 6F 6B	*****.facebook	
63 6F 6D 00 AA 0C	.com.*****.	
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>.....	
00 00 00 00 00 00 00 01 30 FD 08 F8 5F 00 000ý.ø_..	
06 B4 01 F8 5F 00 00 E0 06 B4 01 F8 5F 00 00	à..ø_..à..ø_..	

```

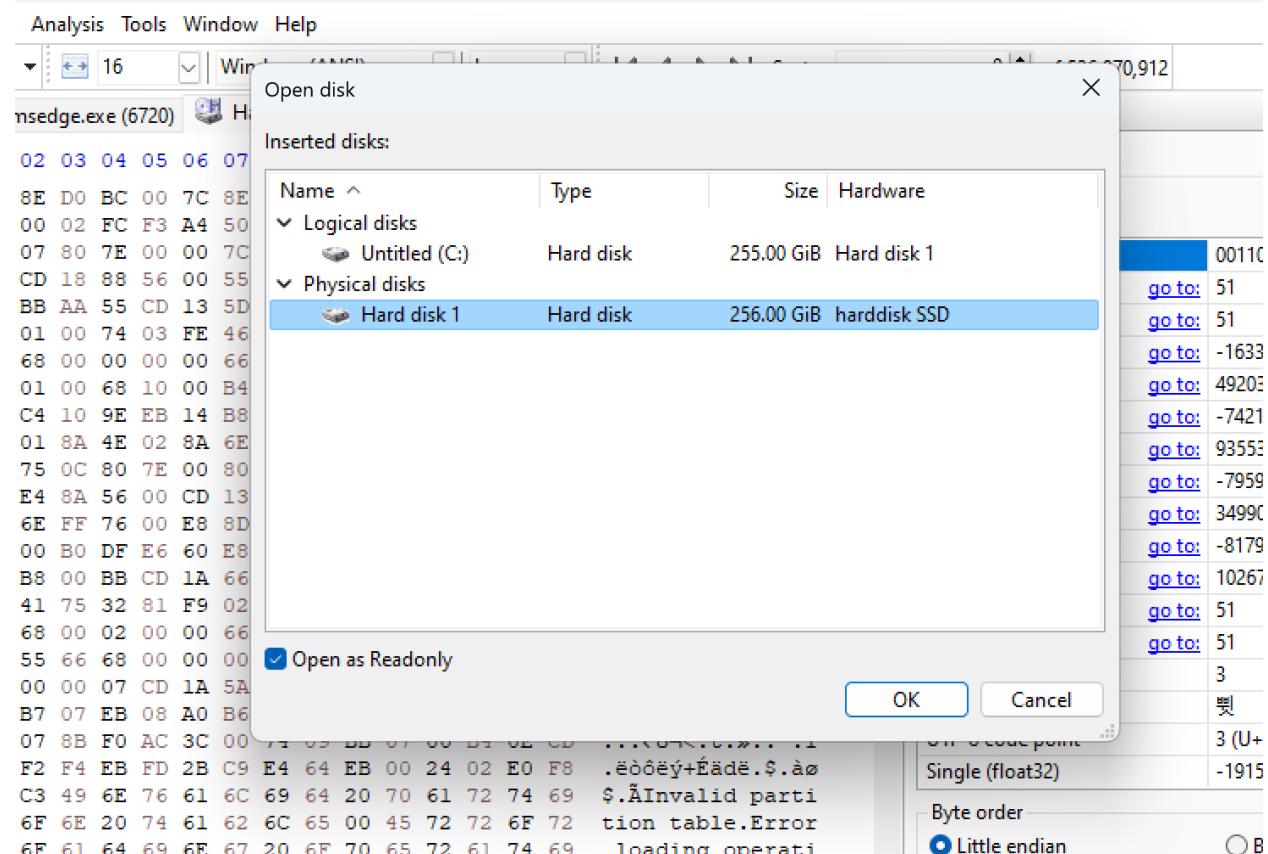
017A42E30430 6D 65 2E 0A 20 20 72 65 74 75 72 6E 20 77 69 6E me.. return win
017A42E30440 64 6F 77 2E 6E 61 6D 65 2E 6D 61 74 63 68 28 2F dow.name.match(/ 
017A42E30450 6F 72 69 67 69 6E 3D 27 28 2E 2B 29 27 2F 29 5B origin='(.+)/)[ 
017A42E30460 31 5D 3B 0A 7D 0A 0A 66 75 6E 63 74 69 6F 6E 20 1]...}.function 
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 70 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 postmessag 
017A42E30550 67 65 2E 0A 20 20 77 69 6E 64 6F 77 2E 6F 70 65 e.. 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.



B.

00B0976140	65 6E 67 65 73 2C 20 61 6E 64 20 53 6F 6C 75 74	enges, and Solut
00B0976150	69 6F 6E 73 20 66 6F 72 20 74 68 65 20 46 75 74	ions for the Fut
00B0976160	75 72 65 20 44 69 73 74 72 69 62 75 74 65 64 20	ure Distributed
00B0976170	49 6F 54 20 4E 65 74 77 6F 72 6B 22 2C 0D 0A 20	IoT Network",..
00B0976180	20 20 20 20 20 20 20 20 20 20 20 22 73 68 6F 77	"show
00B0976190	5F 69 63 6F 6E 22 3A 20 66 61 6C 73 65 2C 0D 0A	_icon": false,..
00B09761A0	20 20 20 20 20 20 20 20 20 20 20 20 22 73 6F 75	"sou
00B09761B0	72 63 65 22 3A 20 22 73 79 6E 63 22 2C 0D 0A 20	rce": "sync",..
00B09761C0	20 20 20 20 20 20 20 20 20 20 20 22 74 79 70 65	"type
00B09761D0	22 3A 20 22 75 72 6C 22 2C 0D 0A 20 20 20 20 20	
00B09761E0	20 20 20 20 20 20 22 75 72 6C 22 3A 20 22 66	"url": "f
00B09761F0	69 6C 65 3A 2F 2F 43 3A 2F 55 73 65 72 73 2F	ile:///C:/Users/
00B0976200	53 68 72 69 72 61 6D 25 32 30 6B 70 2F 44 65 73	Shriram%20kp/Des
00B0976210	6B 74 6F 70 2F 69 6F 74 25 32 30 73 65 63 75 72	ktop/iot%20secur
00B0976220	69 74 79 25 32 30 72 65 73 65 61 72 63 63 68 25	ity%20researcch%

Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Int32
Byte order
 Little end
 Hexadecimal

Checksum Search (76 hits)

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
003138C5A0	00 00 00 00 0A 00 00 00 43 72 65 64 4D 61 6E 4CCredManL
003138C5B0	6F 67 35 42 41 39 2D 34 98 FF FF FF 6E 6B 20 00	og5BA9-4~ÿÿÿnk .
003138C5C0	91 BC 11 DF 2C 0D DA 01 02 00 00 00 D8 84 02 00	ÿ4.B,.Ú.....Ø...
003138C5D0	01 00 00 00 00 00 00 00 08 A3 01 00 FF FF FF FF£..ÿÿÿ
003138C5E0	00 00 00 00 FF FF FF FF 00 9B 00 00 FF FF FF FF	...ÿÿÿ>..ÿÿÿ
003138C5F0	5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	\.....
003138C600	00 00 00 00 17 00 00 00 64 69 6E 6F 74 68 75 6Edinothun
003138C610	64 65 72 6B 70 40 67 6D 61 69 6C 2E 63 6F 6D 00	derkp@gmail.com.
003138C620	80 FF FF FF 6E 6B 20 00 91 BC 11 DF 2C 0D DA 01	€ÿÿÿnk .ÿ4.B,.Ú.
003138C630	02 00 00 00 38 85 02 00 00 00 00 00 00 00 00 008.....
003138C640	FF FF FF FF FF FF 01 00 00 00 60 9A 01 00	ÿÿÿÿÿÿÿ.....š..
003138C650	00 9B 00 00 FF FF FF 00 00 00 00 00 00 00 00 00 00	>..ÿÿÿ.....
003138C660	1A 00 00 00 04 00 00 00 00 00 00 00 2E 00 00 00
003138C670	53 2D 31 2D 35 2D 32 31 2D 32 36 34 31 39 38 37	S-1-5-21-2641987
003138C680	39 32 39 2D 33 34 32 38 35 30 30 30 35 37 2D 32	929-3428500057-2
003138C690	38 34 39 37 36 32 32 35 30 2D 31 30 30 30 00 05	849762250-1000..

Data inspector

Binary (8 bit)
Int8
UInt8
Int16
UInt16
Int24
UInt24
Int32
Byte order
 Little end
 Hexadecimal

Checksum Search (76 hits)

Offset Excerpt (hex) Excerpt (text)

The screenshot shows the OllyDbg debugger interface. The assembly dump window displays memory starting at address 00AC5960F0. The search results window shows three hits for the hex pattern 73 68 72 69 72 61 6D.

Offset (h)	Decoded text
00AC5960F0	d-b8ad-0551cae61
00AC596100	964k+t.U....64e3
00AC596110	5105-0983-4d2d-b
00AC596120	8ad-0551cae61964
00AC596130	.<s.U...64e3510
00AC596140	5-0983-4d2d-b8ad
00AC596150	-0551cae61964.5w
00AC596160	Ragupathy.+
00AC596170	r.U....64e35105-
00AC596180	0983-4d2d-b8ad-0
00AC596190	551cae61964n+q.U
00AC5961A064e35105-098
00AC5961B0	3-4d2d-b8ad-0551
00AC5961C0	cae61964<+p.U...
00AC5961D0	.e4c4ad85-bd51-4
00AC5961E0	b61-b7b2-83896f4

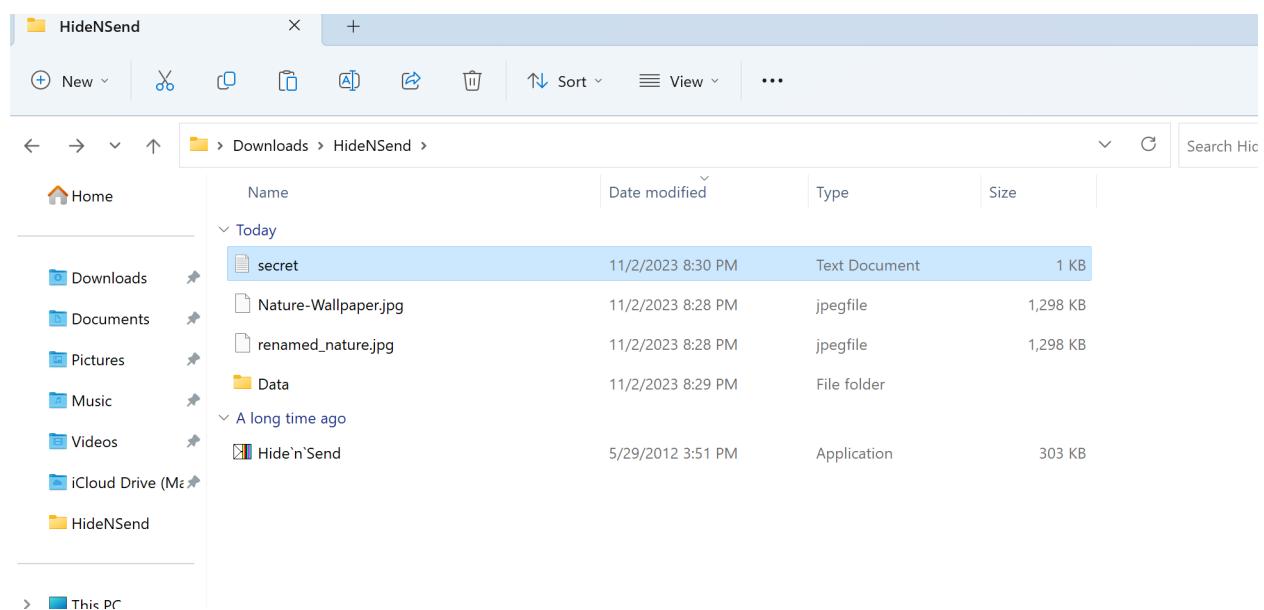
Results	Checksum	Search (76 hits)	
	Offset	Excerpt (hex)	Excerpt (text)
	3437FE12	72 79 75 2E 68 6F 6B 6B 61 69 64 6F 2E 6A 70 00 73 68 72 69 72 61 6D 00 62 72 75 73 73 65 6C 73	ryu.hokka
	A7DA6704	00 00 8A 00 32 00 00 00 00 00 00 00 00 00 00 00 73 68 72 69 72 61 6D 5F 55 53 41 5F 72 65 73 75	..\$2.....
	A7DA67FC	00 00 8A 00 32 00 00 00 00 00 00 00 00 00 00 00 73 68 72 69 72 61 6D 5F 55 53 41 5F 72 65 73 75	..\$2.....

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

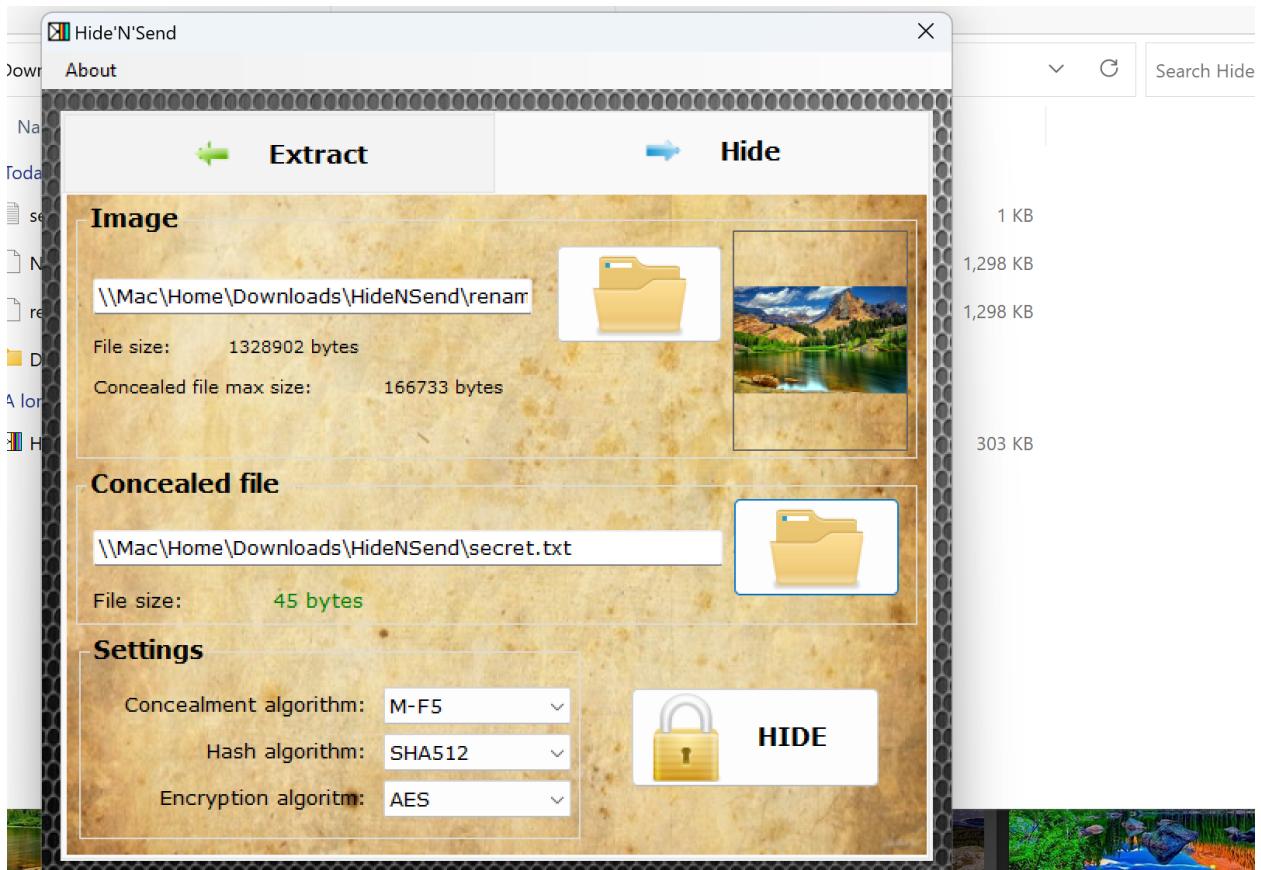
Exercise 23. 03 :

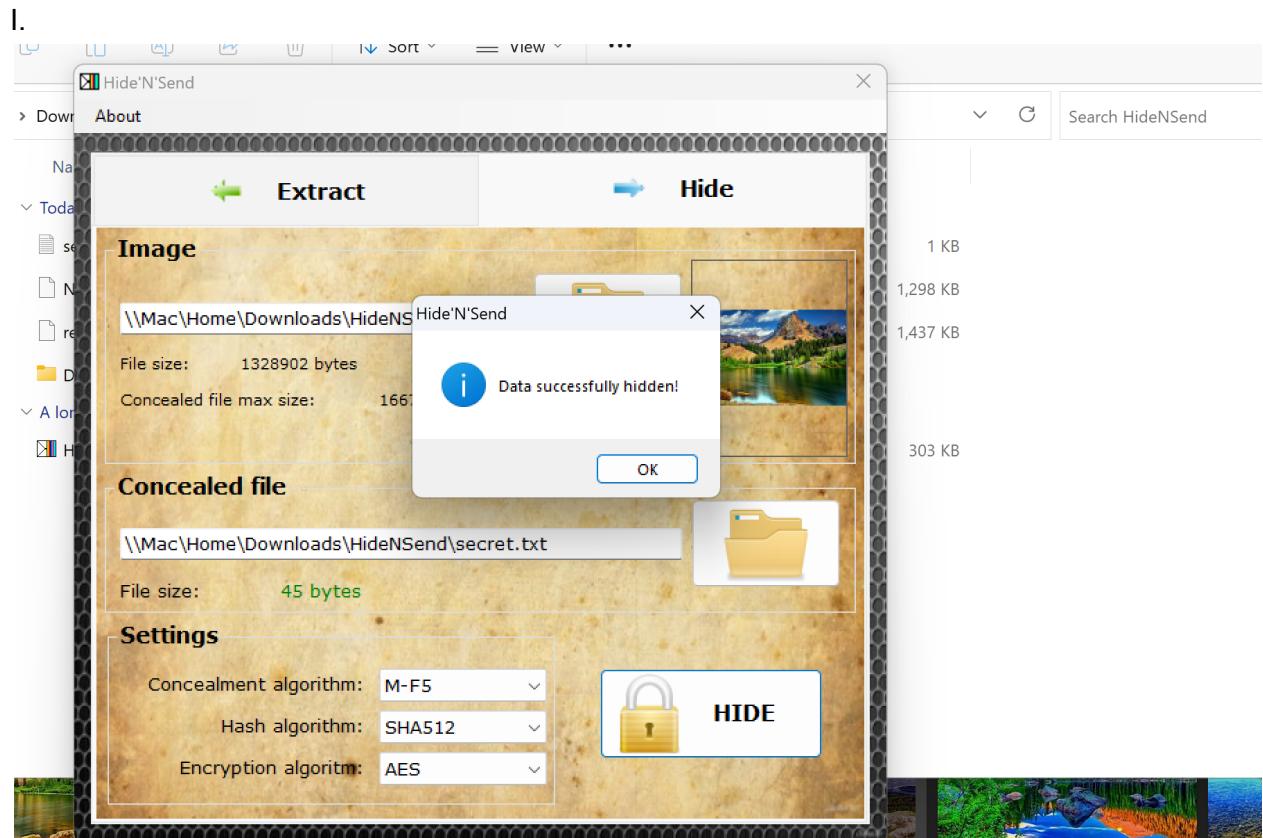
Step 1 :

D.



G.

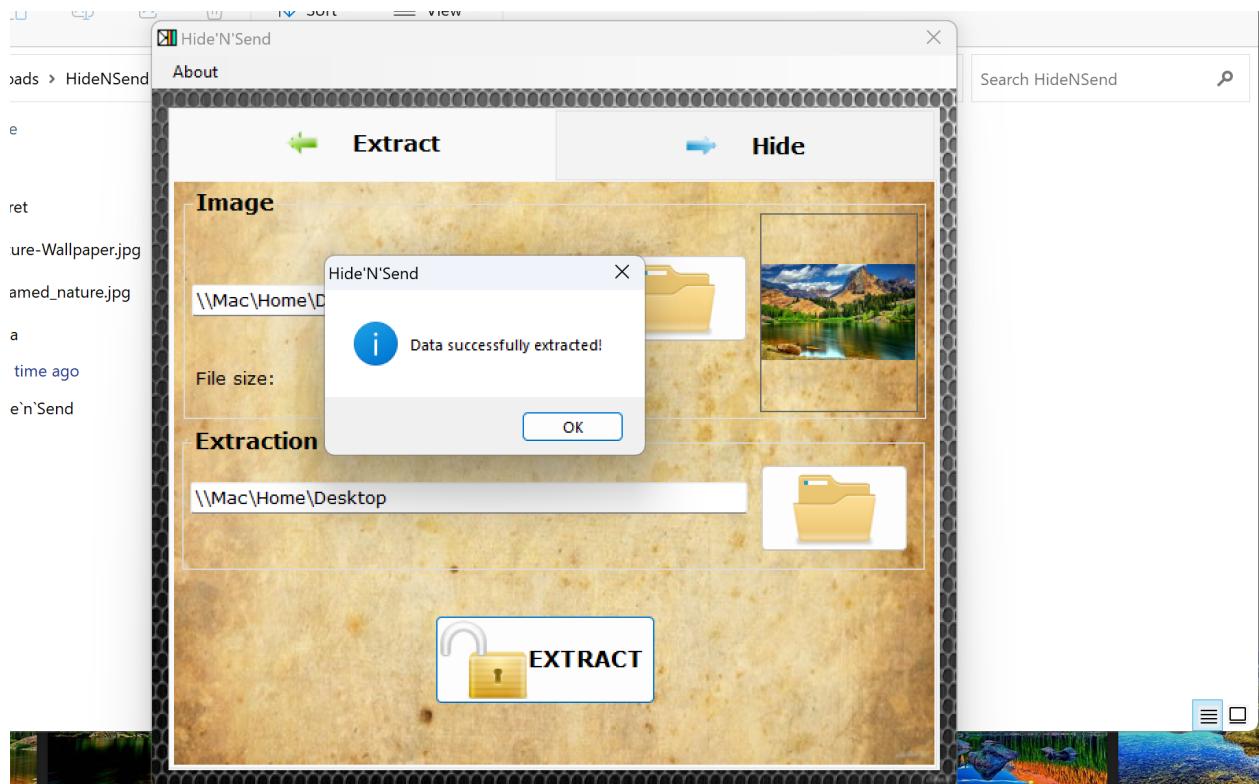




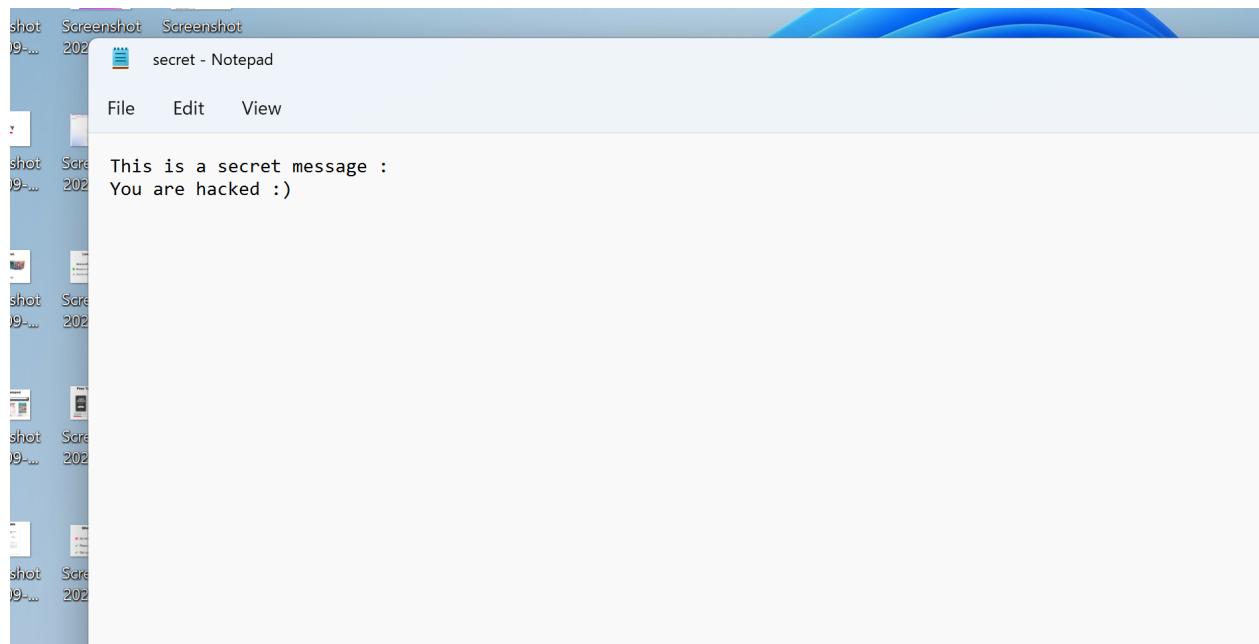
J.

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.



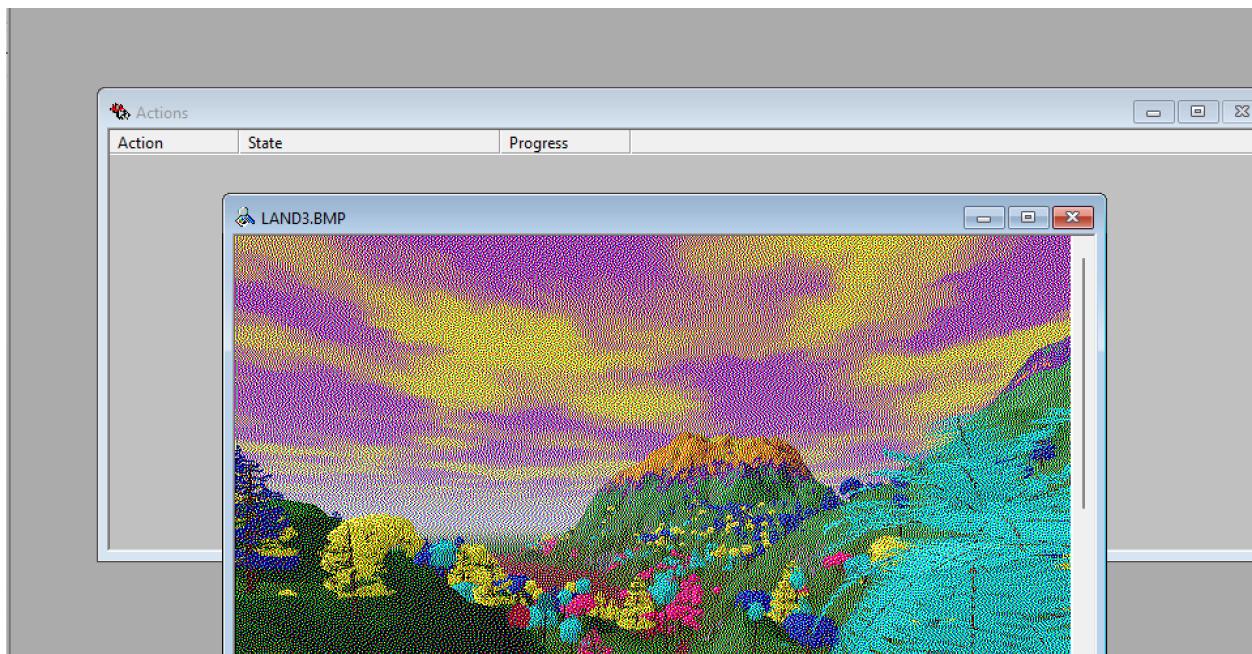
P.



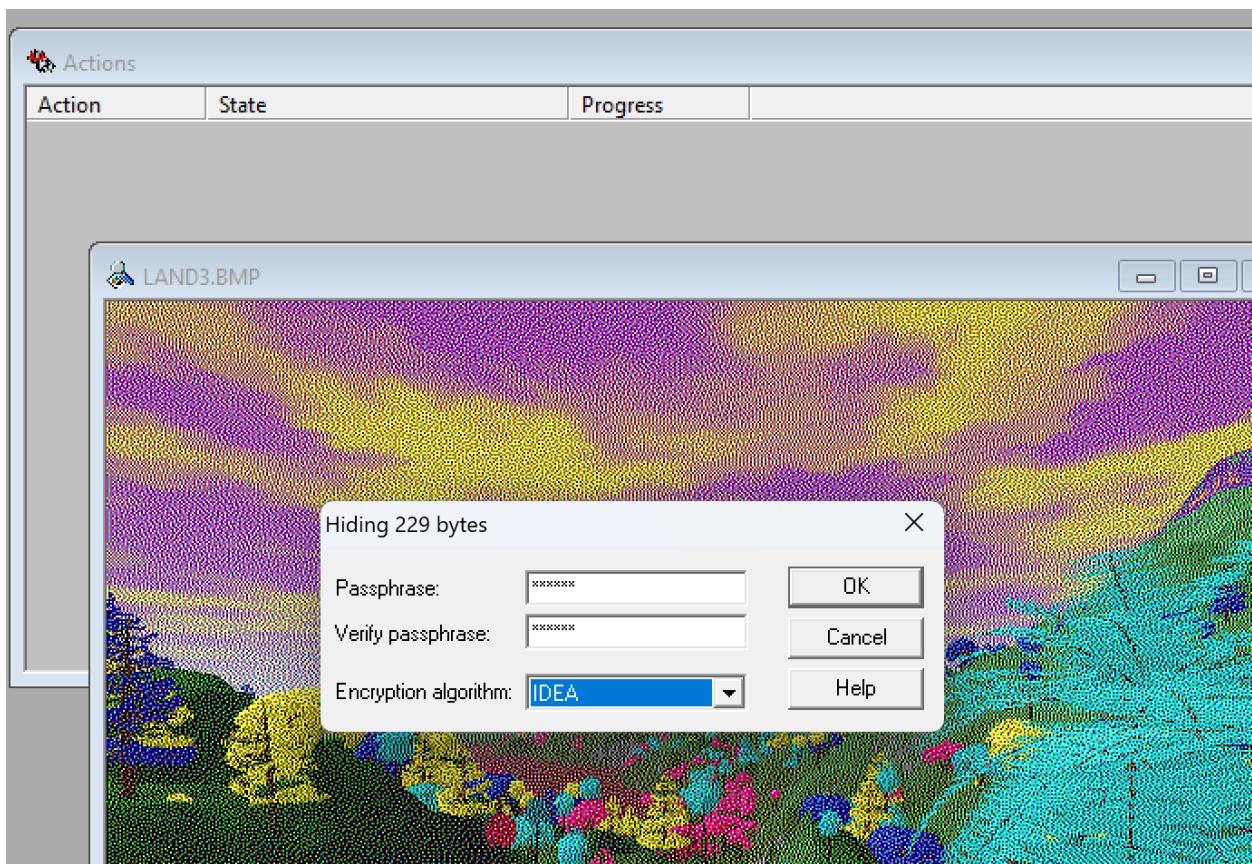
Got the secret back, this is exciting :)

Step 2 :

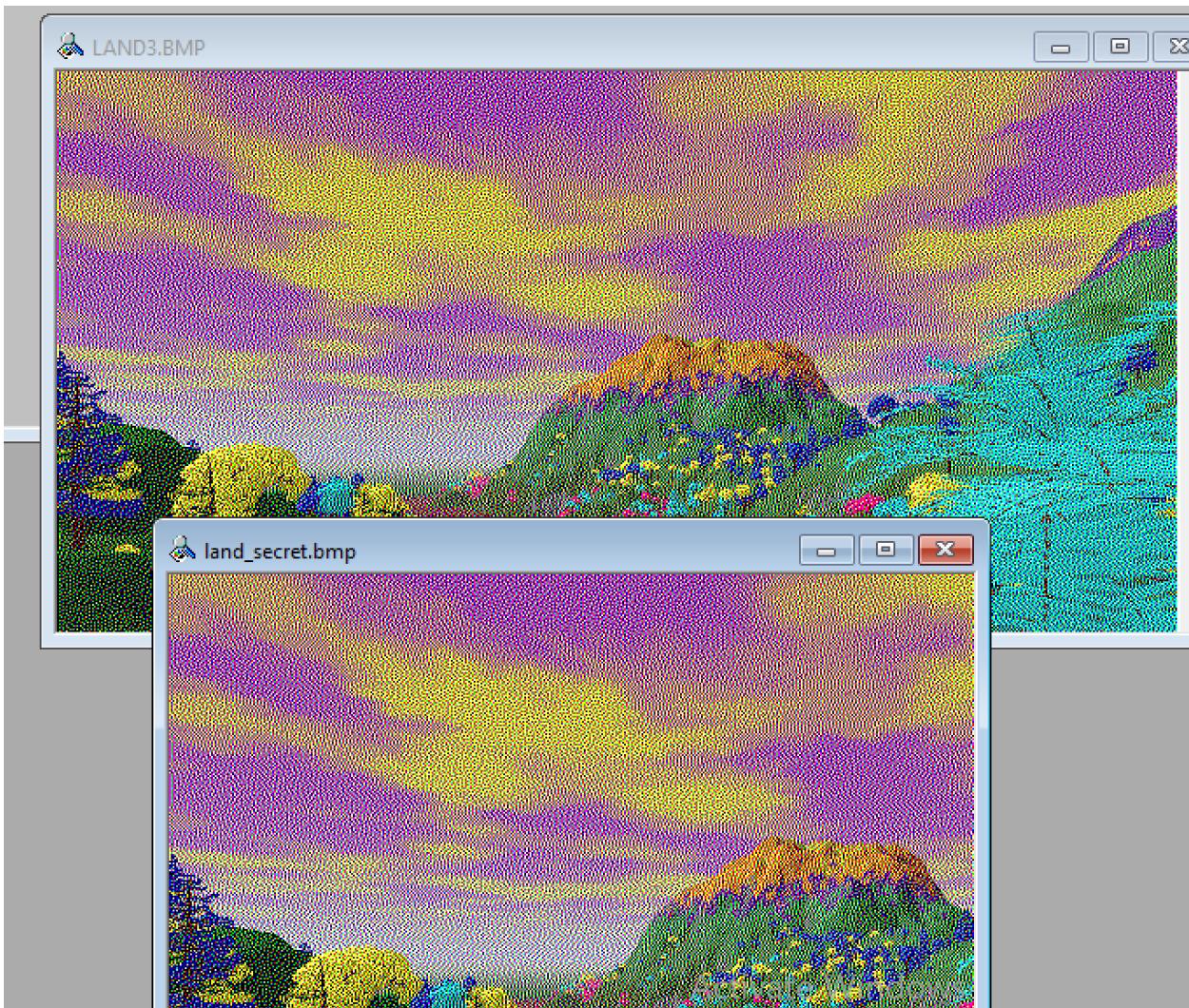
D.



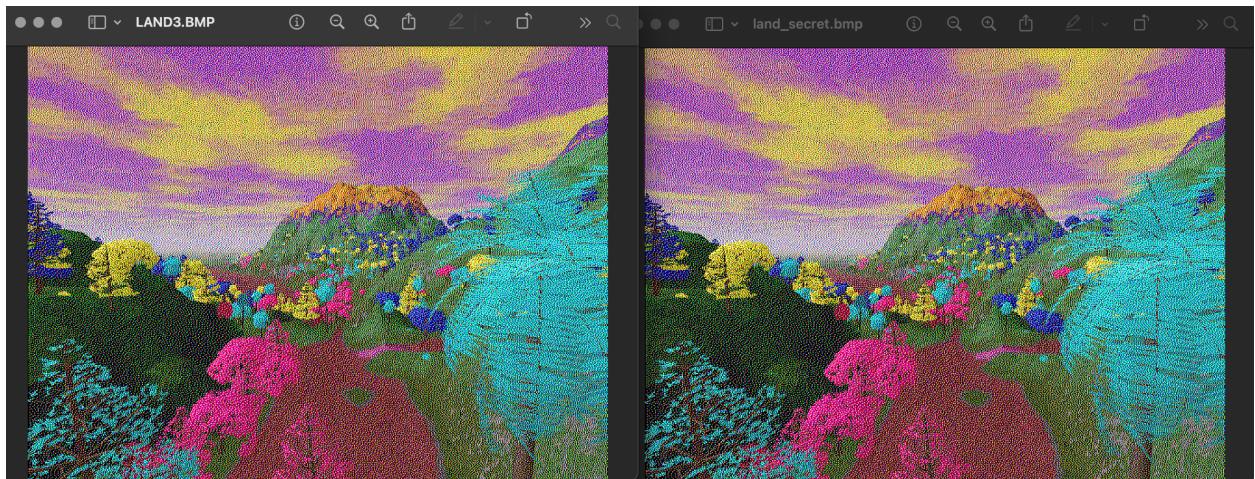
E.



F.



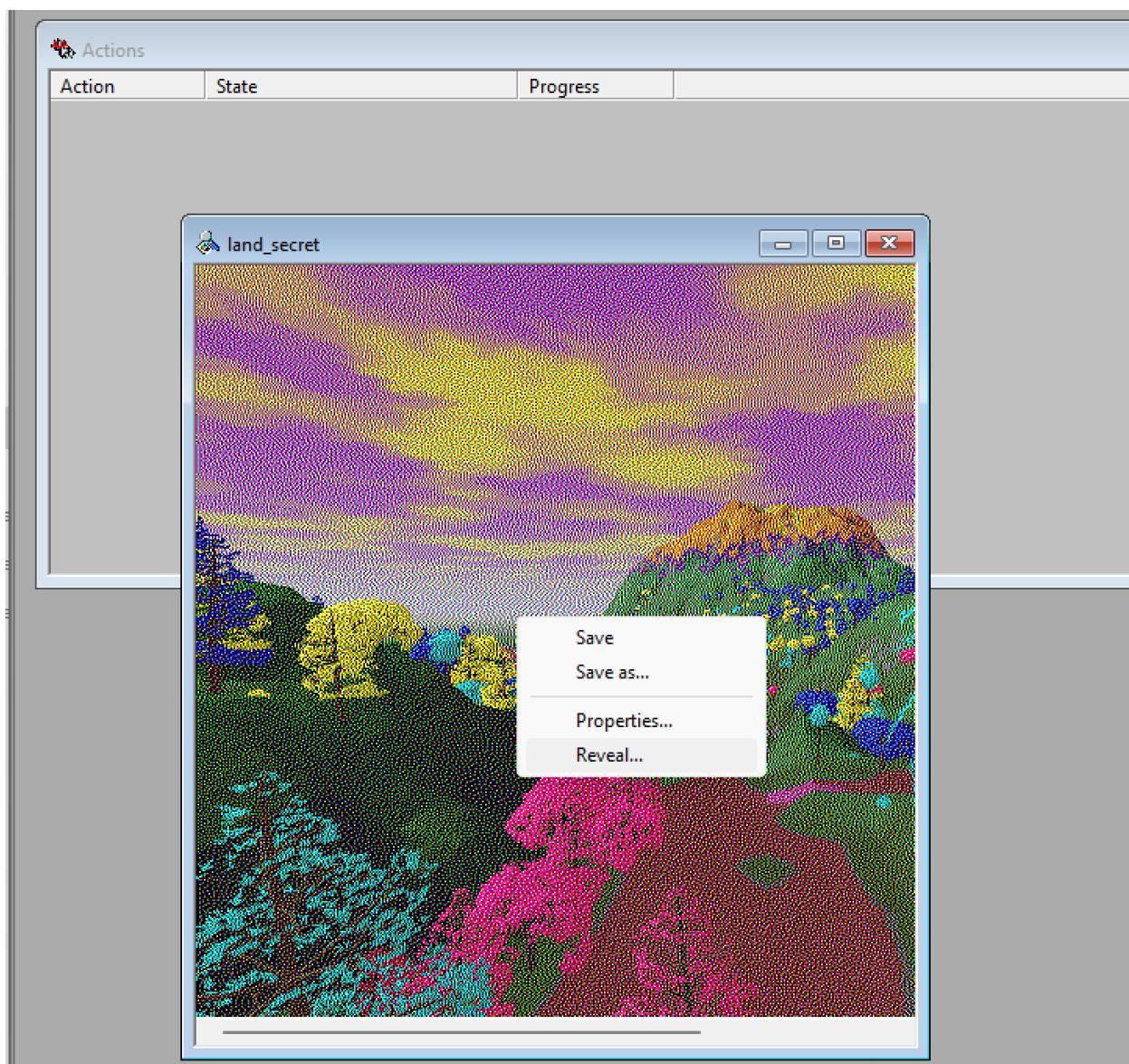
I.



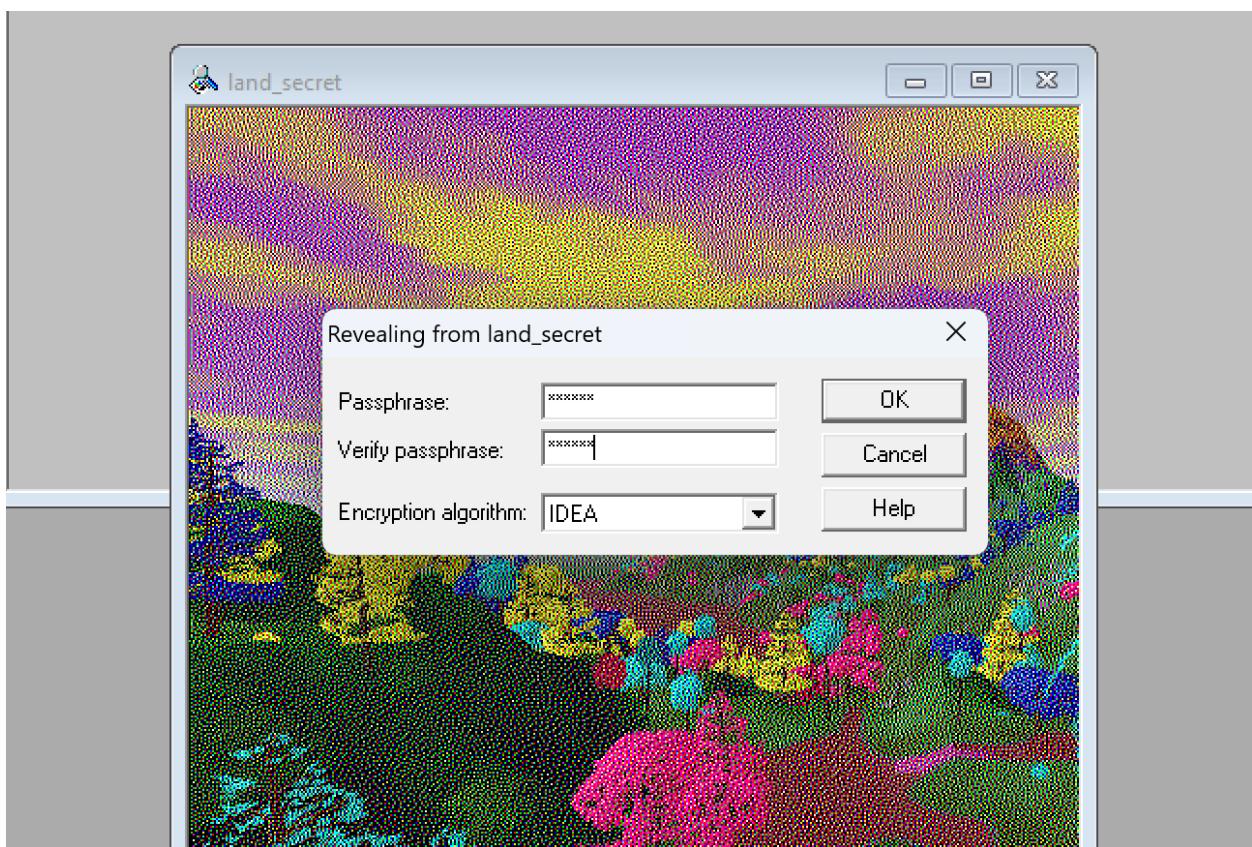
The new image seems to be little bit dull that makes sense because we hide the message by reducing the brightness.

The size of the new image seems to be twice the size of the original image.

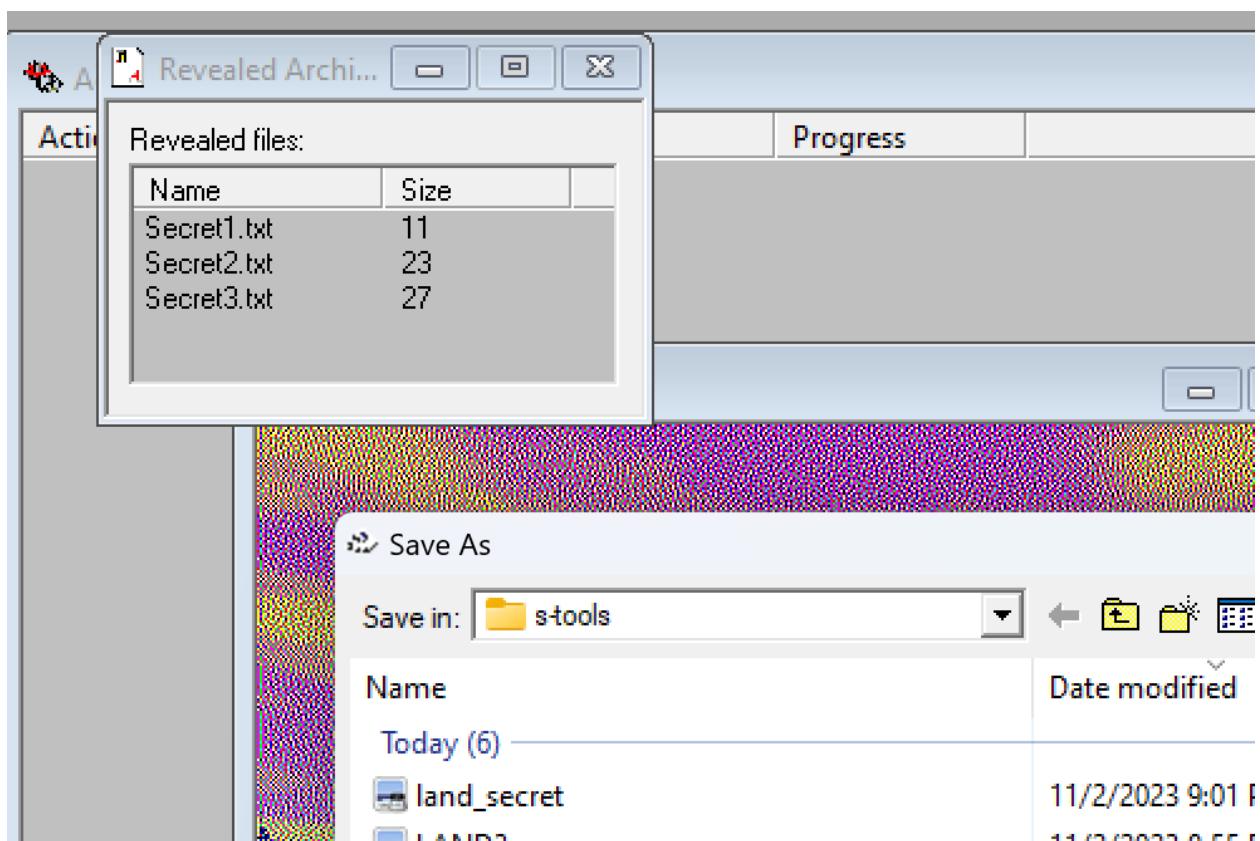
J and K.



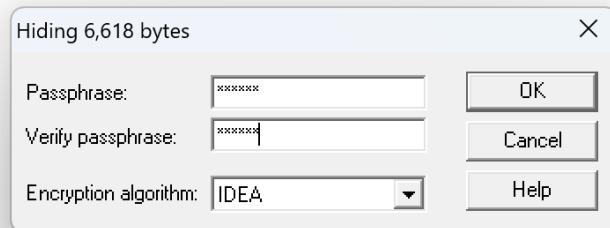
I.

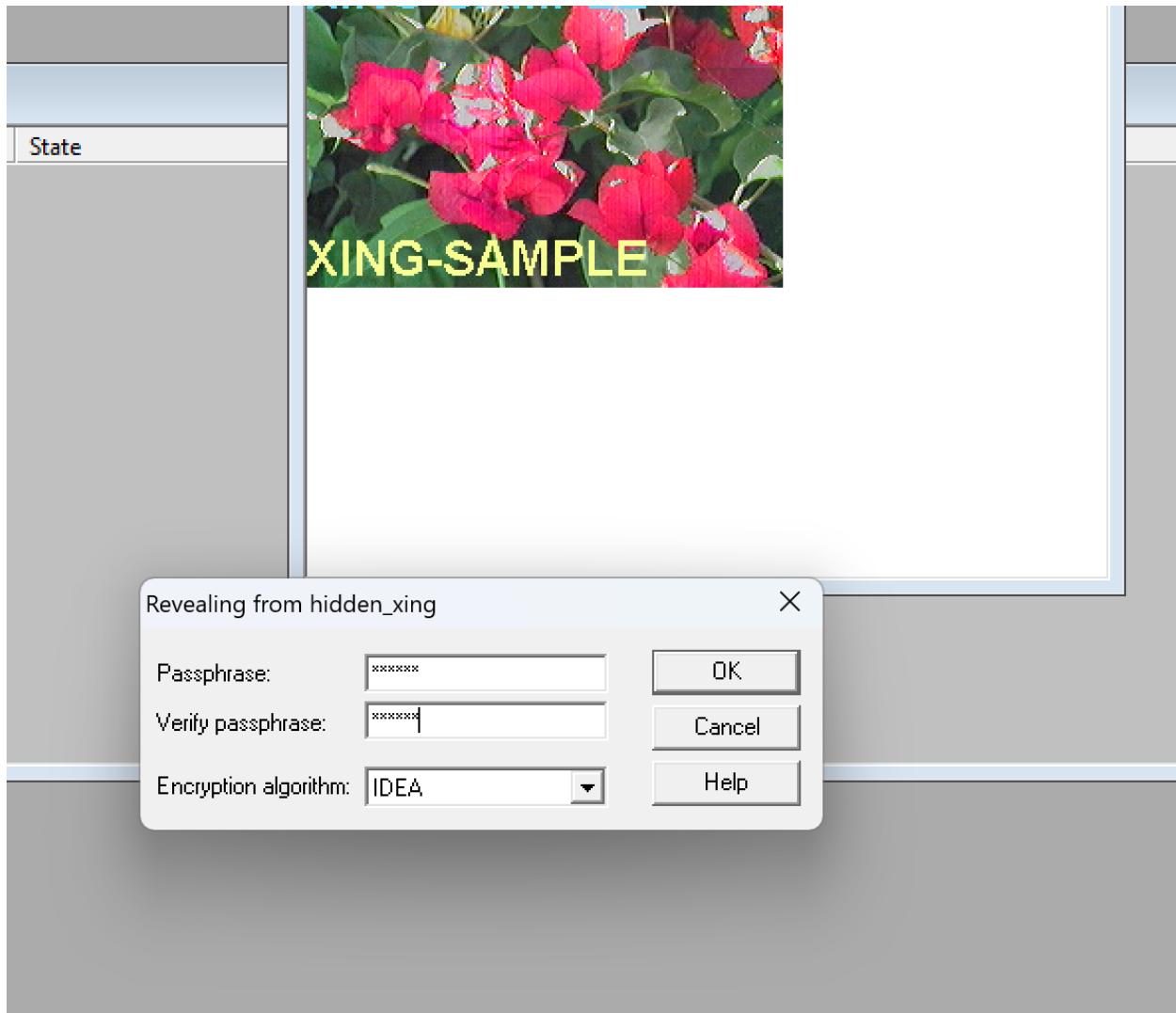


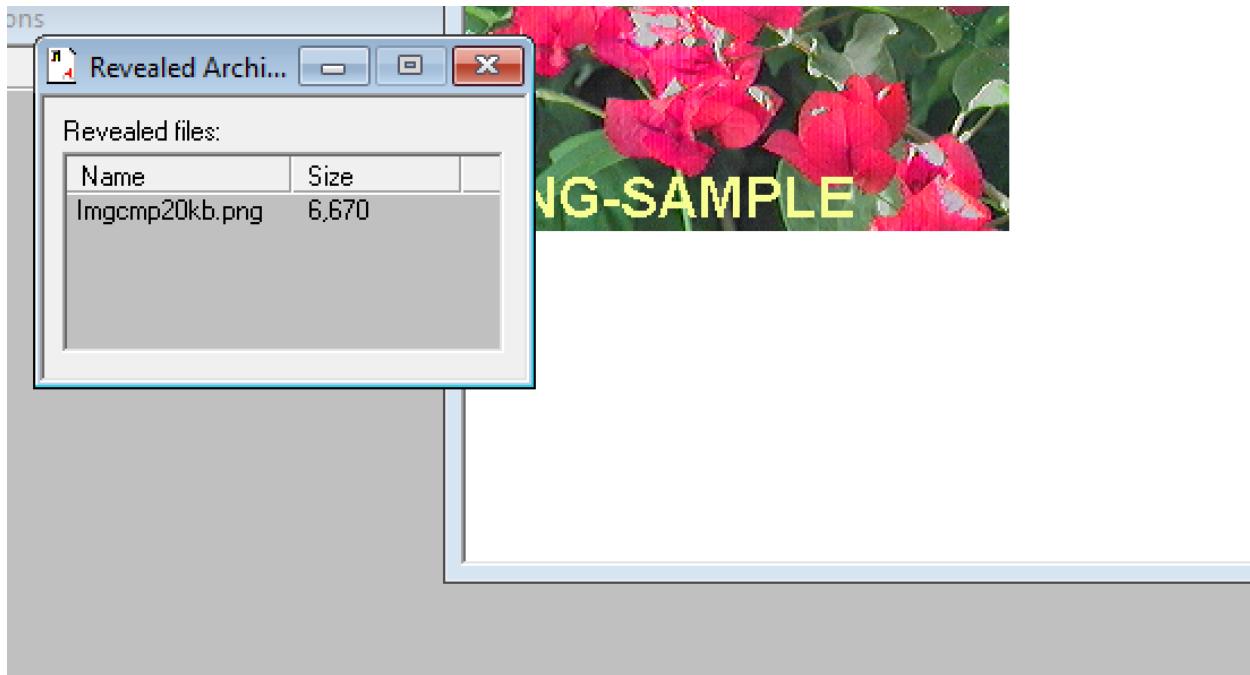
M.



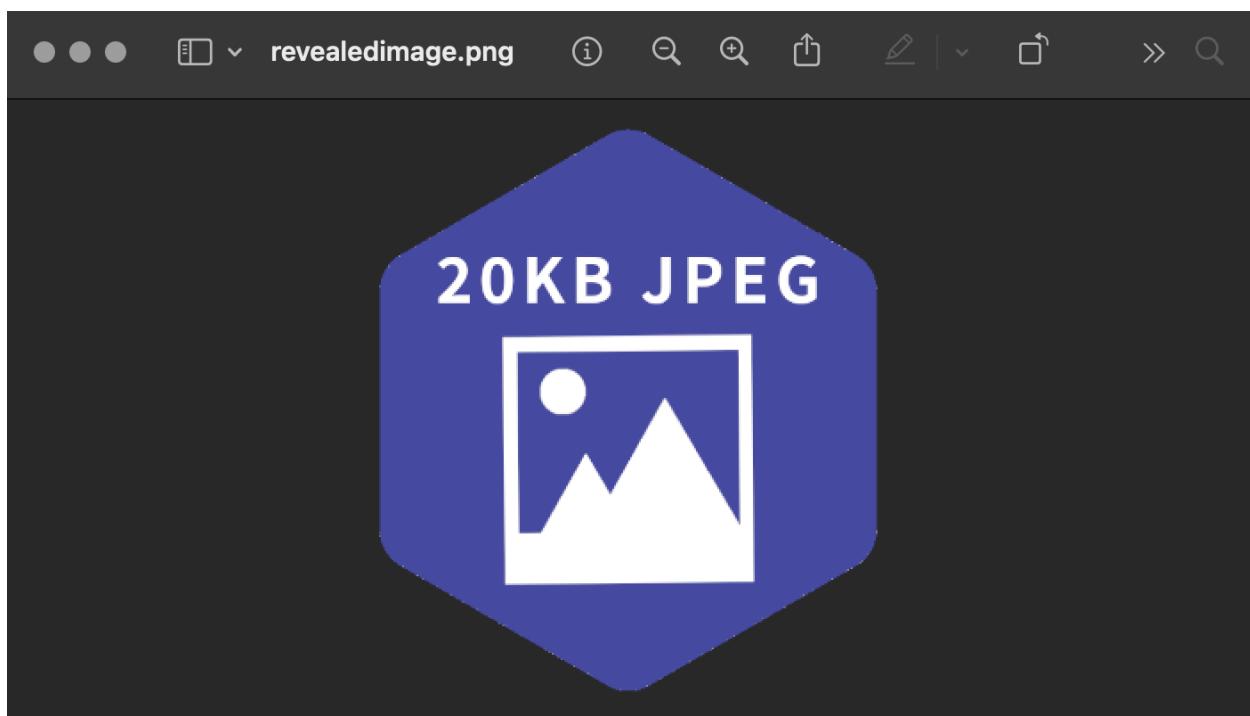
N.







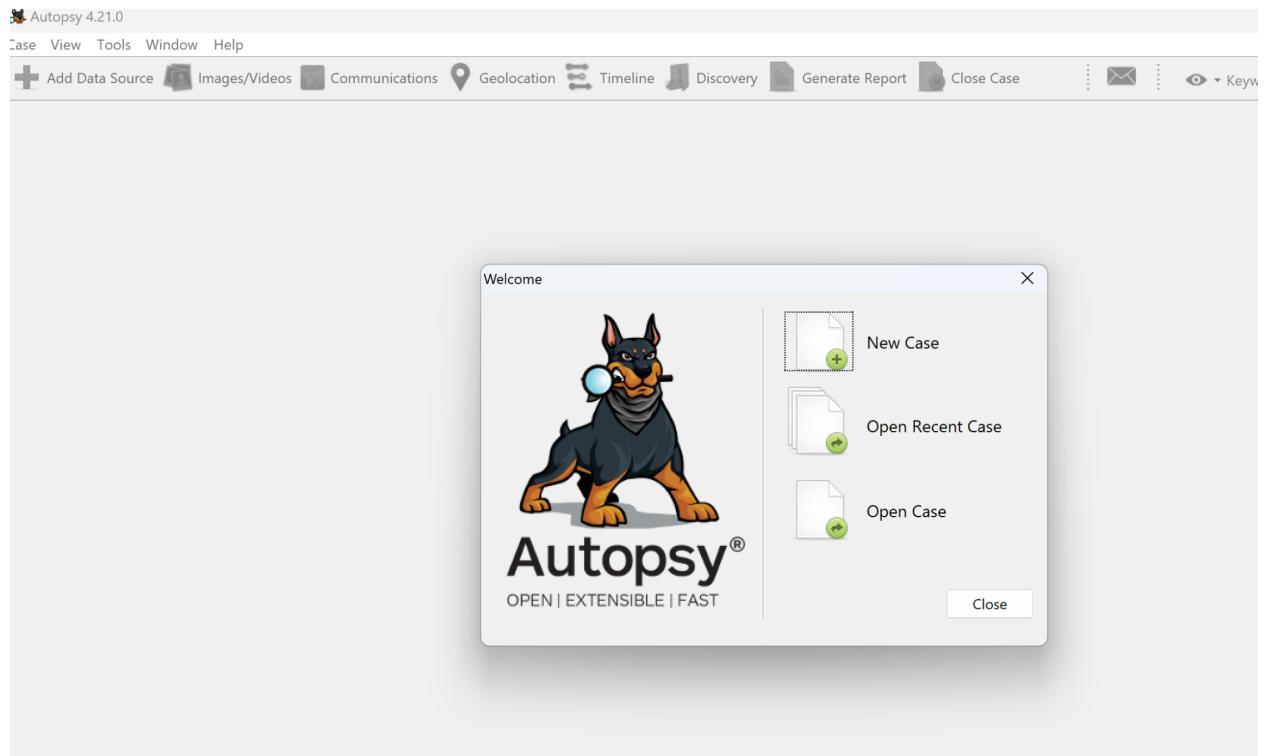
I got the hidden image back.



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

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...
- CallHistoryClient.dll 5/7/2022 3:55 AM Application exten...

File name: calc All files (*.*) Open Cancel

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.....YY...
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 00è....
00000040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..°...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;si±ÔÙà±ÔÙá±ôÙà±
000000A0	9F A1 E1 B0 DD D9 E0 B1 9F A1 E4 B0 C6 D9 E0 B1	Ý;á°ÝÙà±Ý;ä°ÆÙà±
000000B0	9F A1 E3 B0 D0 D9 E0 B1 9F A1 E8 B0 D7 D9 E0 B1	Ý;ä°ÐÙà±Ý;è°×Ùà±
000000C0	9F A1 E5 B0 D6 D9 E0 B1 9F A1 1F B1 D5 D9 E0 B1	Ý;å°ÖÙà±Ý;.±ÖÙà±
000000D0	0F A1 F2 B0 D5 D9 E0 B1 F2 E9 E8 D4 D9 E0 B1	Ý;ç°ØÙà±D;çØÙà±

B.

HxD - [\\Mac\\Home\\Downloads\\Nature-Wallpaper.jpg]

File Edit Search View Analysis Tools Window Help

calc.exe Nature-Wallpaper.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 E1 00 A1 45 78 69 66 00 00 49 49 2A 00	ÿþÿ. ;Exif..II*
00000010	08 00 00 00 05 00 12 01 03 00 01 00 00 00 01 00
00000020	00 00 31 01 02 00 0D 00 00 00 4A 00 00 00 32 01	.1.....J...2.
00000030	02 00 14 00 00 00 57 00 00 00 13 02 03 00 01 00W.....
00000040	00 00 01 00 00 00 69 87 04 00 01 00 00 00 6B 00i#.....k.
00000050	00 00 00 00 00 00 41 43 44 53 65 65 20 50 72 6FACDSee Pro
00000060	20 35 00 32 30 31 32 3A 31 31 3A 32 32 20 31 39	5.2012:11:22 19
00000070	3A 35 32 3A 35 36 00 03 00 90 92 02 00 04 00 00	:52:56.....'
00000080	00 38 34 34 00 02 A0 04 00 01 00 00 00 80 07 00	.844...€...
00000090	00 03 A0 04 00 01 00 00 00 B0 04 00 00 00 00 00°.....
000000A0	00 00 00 00 00 FF E2 0C 58 49 43 43 5F 50 52 4Fÿâ.XICC_PRO
000000B0	46 49 4C 45 00 01 01 00 00 0C 48 4C 69 6E 6F 02	FILE.....HLino.
000000C0	10 00 00 6D 6E 74 72 52 47 42 20 58 59 5A 20 07	...mntrRGB XYZ .
000000D0	CE 00 02 00 09 00 06 00 31 00 00 61 63 73 70 4D	í.....l..acspM
000000E0	53 46 54 00 00 00 00 49 45 43 20 73 52 47 42 00	SFT.....IEC sRGB.
000000F0	00 00 00 00 00 00 00 00 00 00 00 00 F6 D6 00öö.

Results Checksum Search (0 hits)

Algorithm	Checksum	Usage
-----------	----------	-------

This is the jpeg Image

HxD - [\\Mac\\Home\\Downloads\\image-wallpaper-15.jpg]

File Edit Search View Analysis Tools Window Help

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	ÿþÿ...JFIF.....
00000010	00 60 00 00 FF E1 00 80 45 78 69 66 00 00 4D 4D	.ÿ...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 4E 00 00 00 00 00 00 00 60N.....
00000060	00 00 00 01 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	."......ÿÀ.....
000000B0	05 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 00ÿÀ.u..
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.'j..#B±Á.RÑø\$

Results Checksum Search (0 hits)

Algorithm	Checksum	Usage

x Expected result: _____

C.

HxD - [\\Mac\\Home\\Downloads\\Jonathan_Weissman.jpg]

File Edit Search View Analysis Tools Window Help

calc.exe Jonathan_Weissman.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 E1	ÿþÿ...Exif..II*.
00000010	00 00 00 00 00 00 00 00 00 00 00 00 FF EC 00 11ÿi..
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»ç" 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-cl38 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	-01:09:01
000000F0	20 22 3E 20 3C 72 64 66 3A 52 44 46 20 78 6D 6C	

calc.exe Jonathan_Weissman.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 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 11ÿì..
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»í" 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	

The picture taken on 2016 and sep 14.

D.

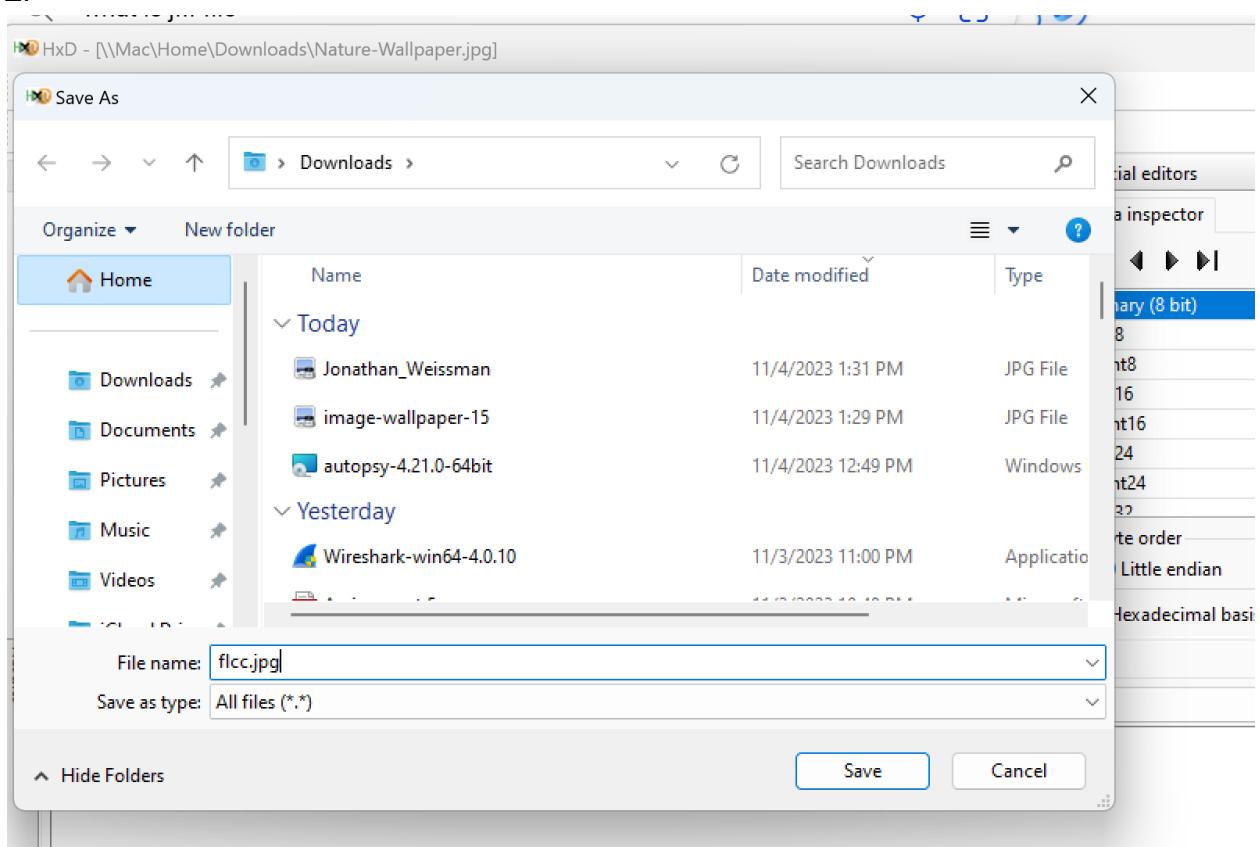
HxD - [\\Mac\\Home\\Downloads\\Nature-Wallpaper.jpg]

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded
00000000	46 4C 43 43 43 43 43 43 43 43 43 43 43 43 43 43	FLCCÿìExif..I*
00000010	08 00 00 00 05 00 12 01 03 00 01 00 00 00 01 00
00000020	00 00 31 01 02 00 0D 00 00 00 4A 00 00 00 32 01	.1.....
00000030	02 00 14 00 00 00 00 57 00 00 00 13 02 03 00 01 00W.
00000040	00 00 01 00 00 00 69 87 04 00 01 00 00 00 6B 00i#
00000050	00 00 00 00 00 00 41 43 44 53 65 65 20 50 72 6Fñr
00000060	00 01 00 00 00 49 87 04 00 01 00 00 00 5B 00 00	++

calc.exe Jonathan_Weissman.jpg Nature-Wallpaper.jpg

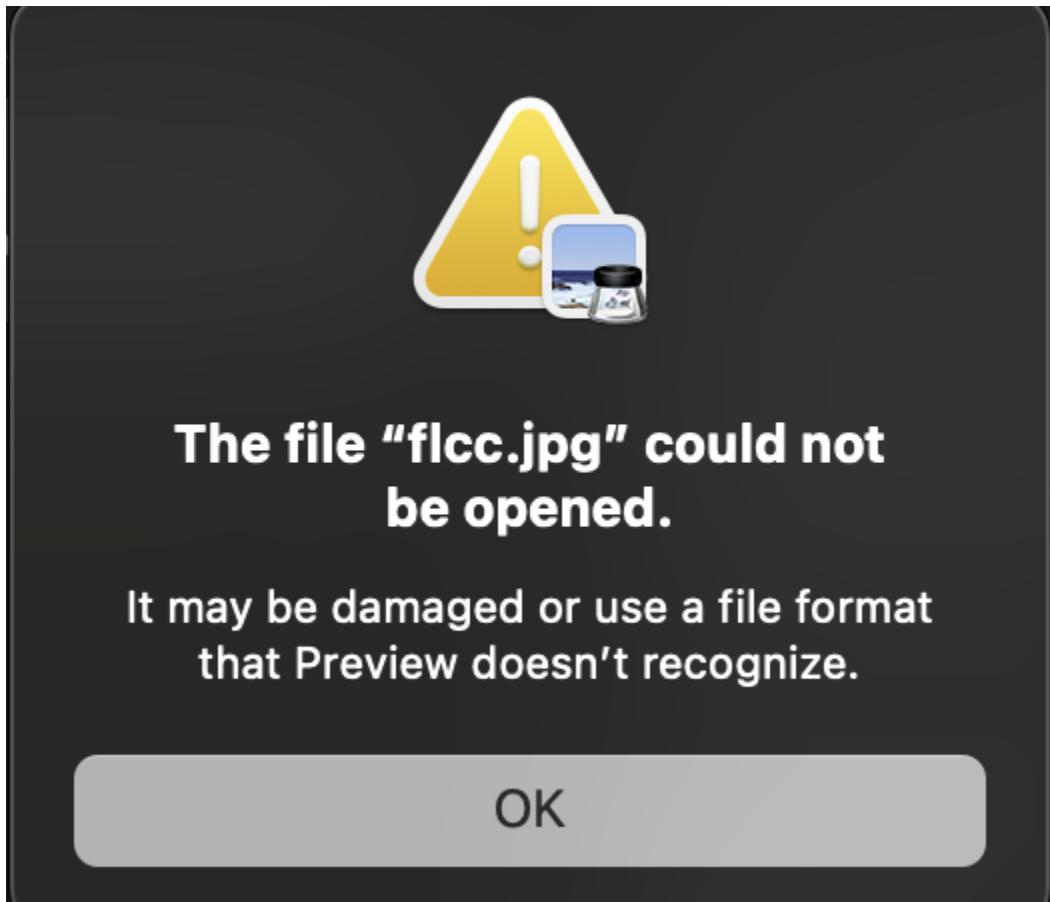
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	46 4C 43 63 A1 45 78 69 66 00 00 49 49 2A 00 08	FLCcÿìExif..I*
00000010	00 00 00 05 00 12 01 03 00 01 00 00 00 01 00 00
00000020	00 31 01 02 00 0D 00 00 00 4A 00 00 00 32 01 02	.1.....J..
00000030	00 14 00 00 00 57 00 00 00 13 02 03 00 01 00 00W.....
00000040	00 01 00 00 00 49 87 04 00 01 00 00 00 5B 00 00	++

E.



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](#)

Copyright © 2009-2022 Simson Garfinkel

The screenshot shows a user interface for adding a data source. On the left, a sidebar titled "Steps" lists five numbered steps: 1. Select Host, 2. Select Data Source Type, 3. Select Data Source, 4. Configure Ingest, and 5. **Add Data Source**. Step 5 is bolded. To the right, a main panel is titled "Add Data Source". It contains a message: "Data source has been added to the local database. Files are being analyzed." There is also a small icon of a cat at the top left of the main panel.

Checkcase - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

11 Keyword Lists

Listing File System

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access
Charlie_2009-11-20_1303_Sent.txt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Charlie_2009-12-02_1305_Received_Part 1.2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Checkcase - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

11 Keyword Lists

Listing Images

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created
astronaut.jpg:Zone.Identifier	1			2009-11-24 17:33:33 BOT	2009-11-24 17:40:19 BOT	2009-12-10 18:26:04 BOT	2009-11-24 18:09:36 BOT
microscope.jpg:Zone.Identifier	1			2009-11-24 17:27:51 BOT	2009-11-24 17:56:35 BOT	2009-12-10 18:26:04 BOT	2009-11-24 18:09:36 BOT
astronaut.jpg	0			2009-11-24 17:33:33 BOT	2009-11-24 17:40:19 BOT	2009-12-10 18:26:04 BOT	2009-11-24 18:09:36 BOT
astronaut1.jpg	1			2009-11-24 17:43:42 BOT	2009-11-24 17:44:00 BOT	2009-12-10 18:26:04 BOT	2009-11-24 18:09:36 BOT
Charlie_2009-12-07_1144_Sent_microscope1.jpg	1			2009-12-10 18:29:38 BOT	2009-12-10 18:37:59 BOT	2009-12-10 18:29:38 BOT	2009-12-10 18:29:38 BOT
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	1			2009-12-04 17:50:24 BOT	2009-12-04 17:50:24 BOT	2009-12-10 18:26:05 BOT	2009-12-10 18:26:05 BOT
microscope.jpg	0			2009-11-24 17:27:51 BOT	2009-11-24 17:56:35 BOT	2009-11-24 18:09:36 BOT	2009-11-24 18:09:36 BOT
microscope1.jpg	1			2009-11-24 18:19:21 BOT	2009-11-24 18:19:21 BOT	2009-11-24 18:19:24 BOT	2009-11-24 18:19:24 BOT
Charlie_2009-12-03_1216_Sent_astronaut1.jpg	1			2009-12-04 13:50:26 BOT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
us005026637-001.tif	0			2009-11-24 17:13:00 BOT	2009-11-24 17:55:45 BOT	2009-12-03 17:16:47 BOT	2009-11-24 17:55:45 BOT
us006982168-001.tif	0			2009-11-24 17:15:00 BOT	2009-11-24 17:55:45 BOT	2009-11-24 17:55:49 BOT	2009-11-24 17:55:49 BOT

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Activate Windows
Go to Settings to activate Windows

6

Checkcase - Autopsy 4.21.0

Case View Tools Window Help

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.eml				charlie@m57.biz;	jaime@project2400.com;	Interested?
Charlie_2009-12-02_1305_Received_Interested.eml				charlie@m57.biz;	jaime@project2400.com;	Interested?

File Views

- 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)
- MB 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

Geolocation Timeline Discovery Generate Report Close Case Keyword Lists

Listing

Web Downloads

Table Thumbnail Summary

Source Name	S	C	O	Path	URL	Domain	Program Name	Data Source
astronaut.jpg:Zone.Identifier				/astronaut.jpg				charlie-work-usb-2009-12-1
invsecr2.exe:Zone.Identifier				/invsecr2.exe				charlie-work-usb-2009-12-1
microscope.jpg:Zone.Identifier				/microscope.jpg				charlie-work-usb-2009-12-1

File Views

- 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)
- MB 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.

The screenshot shows a digital forensic analysis interface. On the left, a sidebar navigation pane includes options like 'Add Data Source', 'Images/Videos', 'Communications', 'Geolocation', 'Timeline', 'Discovery', 'Generate Report', 'Close Case', and various search and reporting tools. The main area displays a table titled 'Listing' under the heading 'Encryption Detected'. The table has columns for 'Source Name', 'S', 'C', 'O', 'Source Type', 'Score', 'Conclusion', and 'Config'. Three entries are listed:

Source Name	S	C	O	Source Type	Score	Conclusion	Config
01.zip				File	Notable		
Charlie_2009-12-04_0941_Sent_01.zip				File	Notable		
Charlie_2009-12-04_0941_Sent_01.zip				File	Notable		

Below the table are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other'. The sidebar also lists 'Data Sources', 'File Views', 'File Types' (with sub-options like 'By Extension' and 'By MIME Type'), 'Deleted Files', 'MB File Size', 'Data Artifacts' (including 'Communication Accounts', 'E-Mail Messages', 'Metadata', 'Web Downloads'), 'Analysis Results' (specifically 'Encryption Detected' which is selected), 'Keyword Hits', 'OS Accounts', 'Tags', 'Score', and 'Reports'.

D.

This screenshot shows the same digital forensic interface as above, but the 'Analysis Results' section is now expanded to show 'Extension Mismatch Detected (5)'. The main listing table is titled 'Images' and contains the following data:

Name	S	C	O	Modified Time	Change Time	Access Time
2E9C3629AE9D43181266CE23F2DD4[1].jpg				2009-11-09 20:50:48 BOT	2009-11-09 20:50:48 BOT	2009-11-09 20:50:48 BOT
32[1].png				2009-11-09 20:50:49 BOT	2009-11-09 20:50:49 BOT	2009-11-09 20:50:49 BOT
action-info[1].png				2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT
action-link[1].png				2009-11-09 20:51:15 BOT	2009-11-09 20:51:15 BOT	2009-11-09 20:51:15 BOT
congrat[1].jpg				2009-11-08 21:30:57 BOT	2009-11-08 21:30:57 BOT	2009-11-08 21:30:57 BOT
search[1].png				2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT
kv.logof[1].png				2009-11-09 20:50:52 BOT	2009-11-09 20:50:52 BOT	2009-11-09 20:50:52 BOT
language-projects[1].png				2009-11-09 20:51:18 BOT	2009-11-09 20:51:18 BOT	2009-11-09 20:51:18 BOT
login-button[1].png				2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT
middle_bluebutton[1].png				2009-11-08 21:31:30 BOT	2009-11-08 21:31:30 BOT	2009-11-08 21:31:30 BOT
sun-mysql-logo[1].png				2009-11-09 20:51:07 BOT	2009-11-09 20:51:07 BOT	2009-11-09 20:51:07 BOT
tab[1].png				2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT
user[1].png				2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT	2009-11-09 20:51:08 BOT
user11.png				nnnn.nnn.nnn.nnnnnnnn	nnnn.nnn.nnn.nnnnnnnn	nnnn.nnn.nnn.nnnnnnnn

Below the table are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The sidebar remains the same as in the first screenshot.

File Types

- Images (701)
- Videos (15)
- Audio (167)
- Archives (222)
- Databases (37)
- Documents
 - HTML (380)
 - Office (23)
 - PDF (2)**
 - Plain Text (498)
 - Rich Text (11)
- Executable
- By MIME Type
- Deleted Files
- MB File Size**
- Data Artifacts
 - Metadata (1)
 - Recent Documents (10)
 - Remote Drive (1)
 - Shell Bags (30)
 - USB Device Attached (11)**
- Analysis Results
 - Encryption Detected (1)
 - Extension Mismatch Detected (7)
- OS Accounts
- Tags
- Score
- Reports

Name	S	C	O	Modified Time	Change Time	Access Time	Created
22EE12E5d01.pdf				2009-11-17 17:54:02 BOT	2009-11-17 17:54:02 BOT	2009-11-17 17:54:14 BOT	2009-11-17 17:54:14 BOT
AC7640A9d01.pdf				2009-11-17 17:54:26 BOT	2009-11-17 17:54:26 BOT	2009-11-17 17:54:32 BOT	2009-11-17 17:54:32 BOT

There were two pdf files

These are the larger files :

MB 50 - 200MB (4)

Name	S	C	O	Modified Time	Change Time	Access Time
openofficeorg1.cab				2009-08-20 04:15:08 BOT	2009-11-09 20:59:59 BOT	2009-11-09 20:59:59 BOT
OOo_3.1.1_Win32Intel_install_wJRE_en-US[1].exe				2009-11-09 20:59:29 BOT	2009-11-09 20:59:34 BOT	2009-11-09 20:59:34 BOT
\$LogFile				2009-11-08 12:58:56 BOT	2009-11-08 12:58:56 BOT	2009-11-08 12:58:56 BOT
driver.cab				2008-04-14 08:00:00 BOT	2009-11-08 13:08:02 BOT	2009-11-09 02:00:00 BOT

Recently opened documents :

The screenshot shows a digital forensic analysis interface. On the left is a navigation tree with the following structure:

- ... (1)
- Videos (15)
- Audio (167)
- Archives (222)
- Databases (37)
 - Documents
 - HTML (380)
 - Office (23)
 - PDF (2)
 - Plain Text (498)
 - Rich Text (11)
 - Executable
 - By MIME Type
 - application
 - image
 - multipart
 - text
- Deleted Files
- MB File Size
 - MB 50 - 200MB (4)
 - MB 200MB - 1GB (0)
 - MB 1GB+ (3)
- Data Artifacts
 - Metadata (1)
 - Recent Documents (10) Recent Documents (10)
 - Remote Drive (1)
 - Shell Bags (30)
 - USB Device Attached (11)
- Analysis Results
 - Encryption Detected (1)
 - Extension Mismatch Detected (10)
- OS Accounts

USB Device attached :

digicase - Autopsy 4.2.1.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

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
system		0	2009-11-17 14:56:37 BOT	Alcor Micro Corp.
system		0	2009-11-16 20:25:20 BOT	LaCie, Ltd
system		0	2009-11-17 17:09:12 BOT	SanDisk Corp.
system		0	2009-11-17 23:19:10 BOT	Dell Computer Corp.
system		0	2009-11-17 23:19:10 BOT	Model L100 Keyboa

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations C

Analyzing files from Charlie 2009-11-19 19:01

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Case View Tools Window Help

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

Encrypted files detected :

The screenshot shows the EnCase software interface. The left pane displays a tree view of file types and categories. The right pane shows a table titled "Encryption Detected" with the following data:

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification
internalList.zip		0		File	Notable			Password ↗
internalList.zip		0		File	Notable			Password ↗
internalList.zip.bak		0		File	Notable			Password ↗
quarantinedList.zip		0		File	Notable			Password ↗
quarantinedList.zip.bak		0		File	Notable			Password ↗
userList.zip		0		File	Notable			Password ↗
userList.zip.bak		0		File	Notable			Password ↗

E.

Comments and Additional Activities



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