University of Victoria

University of Victoria

ECE 570 - Digital Forensics Methodologies
PROJECT PART 2

Data Exfiltration

Somayeh Roshandel V00942553
Behnaz Saropourian V00857804

July 2020

University of Victoria

Table content

University of Victoria

Abstract

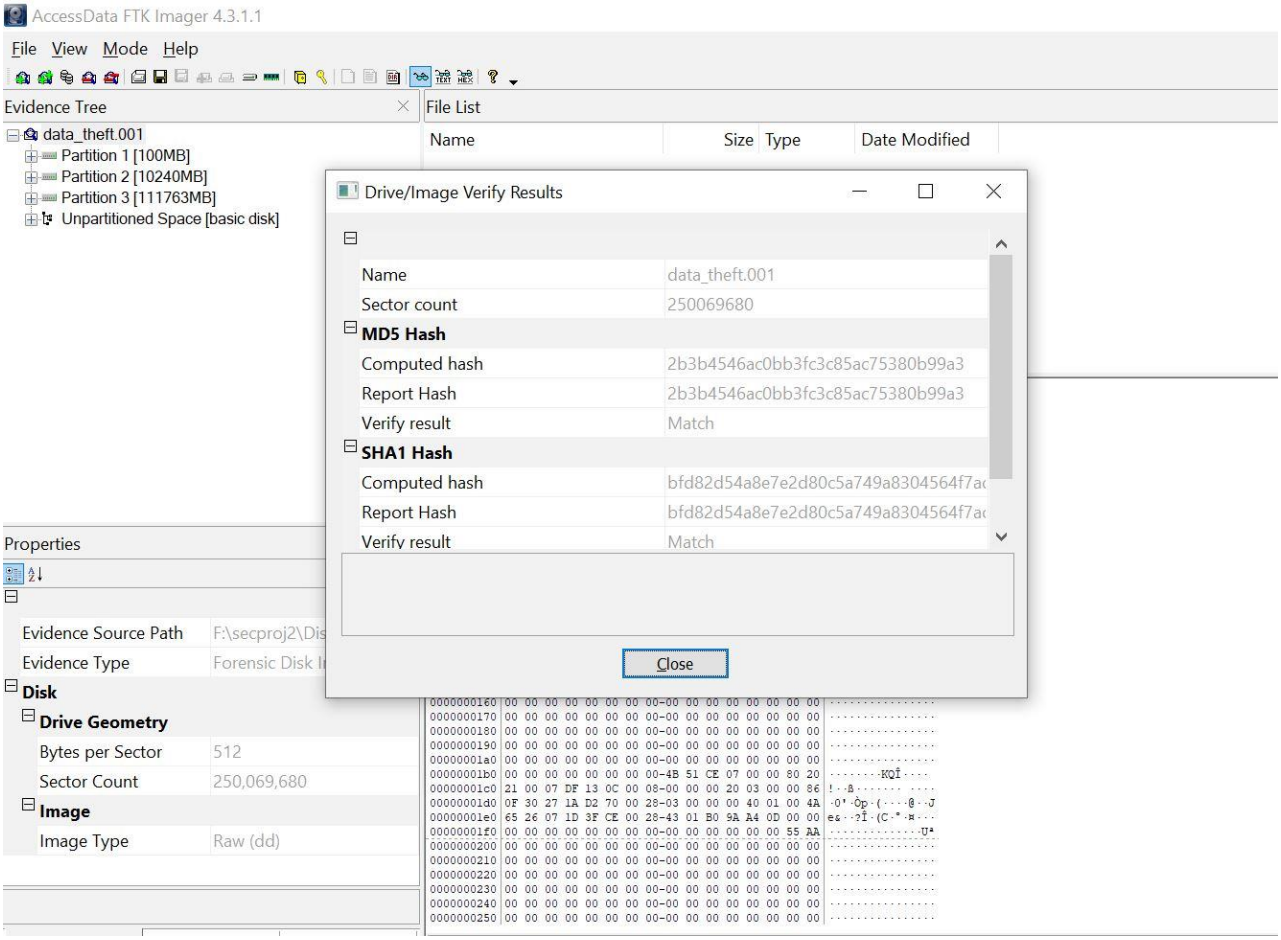
The purpose of this report is to provide evidence based on information gathered about Mr JLewis secretory of Dr Eli Drucker who is suspected for sharing some files which assume related to Freescale semiconductor Inc.'s important project, Mobile Extreme Convergence(MXC), with their competitor Cybernetics based on random email checking which has been done and shows he sent an email to Cybernetics and also he brought his personal laptop against company policy to work,video record shows that he transferred some files from his company computer to his USB. Image of his laptop provided.we have started our investigation to authenticate the evidence by calculating the hash value of the evidence gathered and that on the original data and make sure they are identical. and then for investigation on this case we use forensics tools such as Autopsy on widows and also kali linux version and FTKimager to analysis, reading deleted data, searching hidden data and breaking passcodes to gain our access to suspected files and checking files and directories for a specific possible key values. Beside that we use stragraphy tool, Quickstego to find hidden text on suspected image or text documents.

University of Victoria

1. Check the validity of the forensic image using the supplied hashes.

For verifying integrity of forensic digital image to validate it is an exact copy of the original image we use both autopsy and FTK imager to create a hash of the file as following figures. By looking at MD5 hash and SHA1 hash created by these two forensics tools and compare it with computed hashes provided as .txt file, its validity is confirmed.

MD5 hash created from FTK imager:



MD5 generated by Autopsy that run on Kali LInux is :

University of Victoria

Original data_theft001 MD5 hash:

```
 Cylinders: 15,566
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 250,069,680
[Physical Drive Information]
 Drive Model: SAMSUNG MZ7TD128HAFV-000L1
 Drive Serial Number: S14TNSAD642078
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 122104 MB
 Sector count:    250069680
[Computed Hashes]
 MD5 checksum:    2b3b4546ac0bb3fc3c85ac75380b99a3
 SHA1 checksum:   bfd82d54a8e7e2d80c5a749a8304564f7ad4fc6f
```

University of Victoria

2. What crucial data are available on the seized device? Indicate the specific files that contain such data and explain the importance of the different pieces of information for the investigation. All relevant information must be identified. Explain what processes did you (the investigator) used to successfully examine the image and uncover the evidence, by highlighting explicitly the logical process or thought that led to the discovery of the relevant information.

At very first point as first digital evidence we check his communication websites, his messages and his emials. We found he has some suspicious emails that Mr Jlewis sent an email to jdeer from cybernetics,one of the competitor company. This email contains some information about exchange document and money which those documents are related to one of the company's revolutionary product architecture. So now we have a hint about period of time that we can consider more. Dec2017
(more information about emails provided in Question4)

Hello,

Some great stuff this time around; device contains all 3 requested files:

1. MXCWP Design

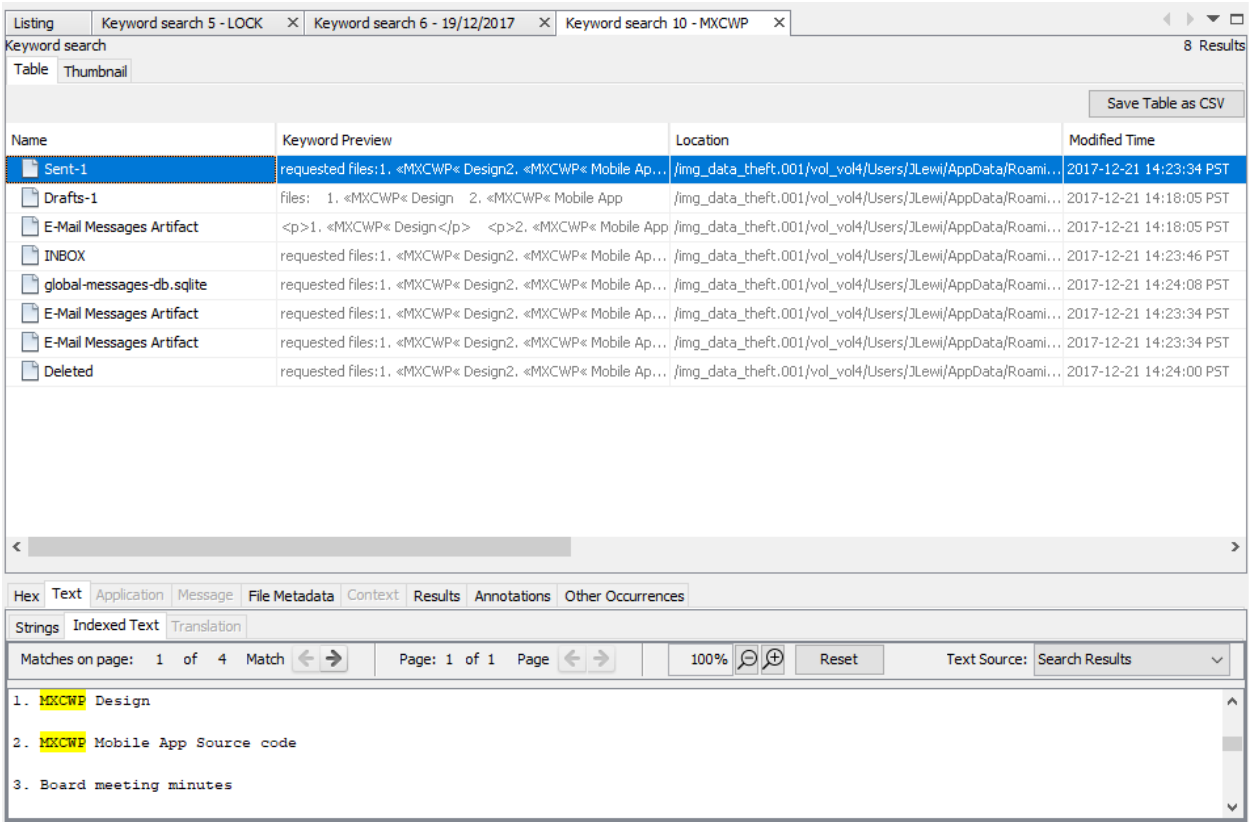
2. MXCWP Mobile App Source code

3. Board meeting minutes

Please send payments in bitcoins through same channel.

Thank you.

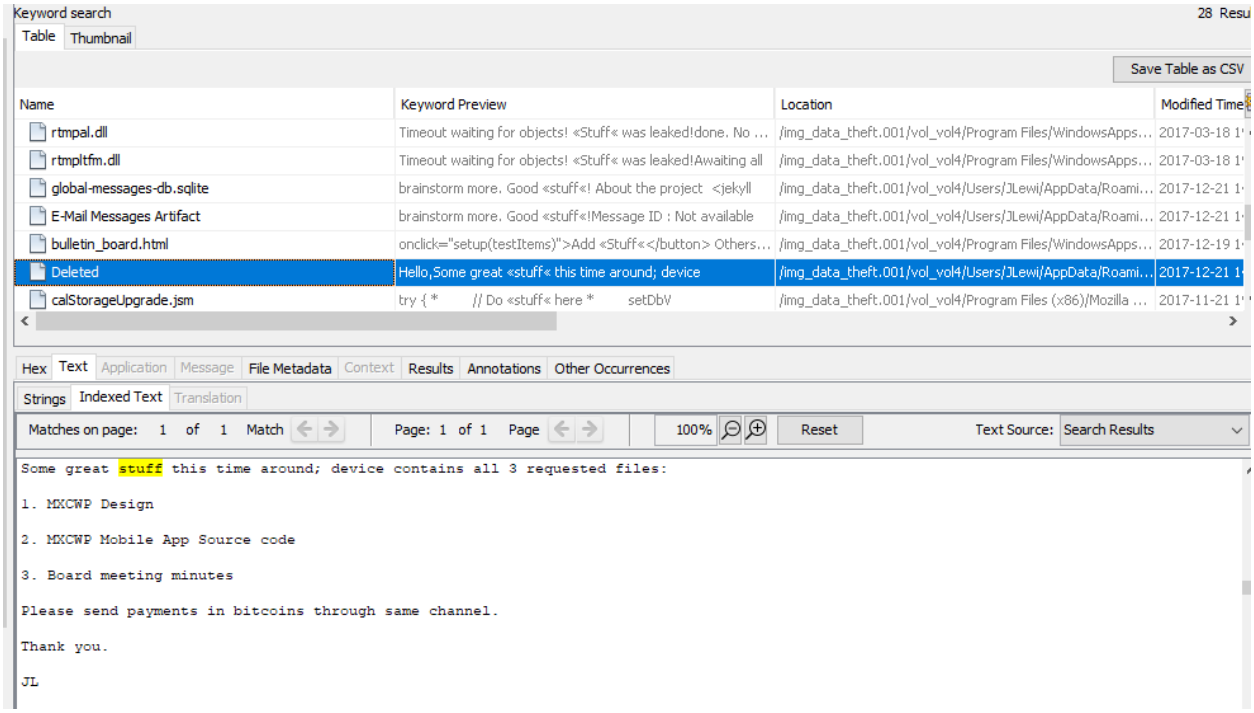
According to the email mentioned on the project that was sent on December 20.
We understand that around those days, we found essential evidence. Mr. Lewis communicated with cybernetics company members in December 2017.
First we search for MXCWP keywords based on project description.
Some Emails found that contain information mentioned on three emails. These are the first clues in anticipation of possible lawsuit, the company decided to collect and analyze evidence supporting their case.



First we found the above pictures that showed some emails that were sent or remained on the mailbox and never sent.

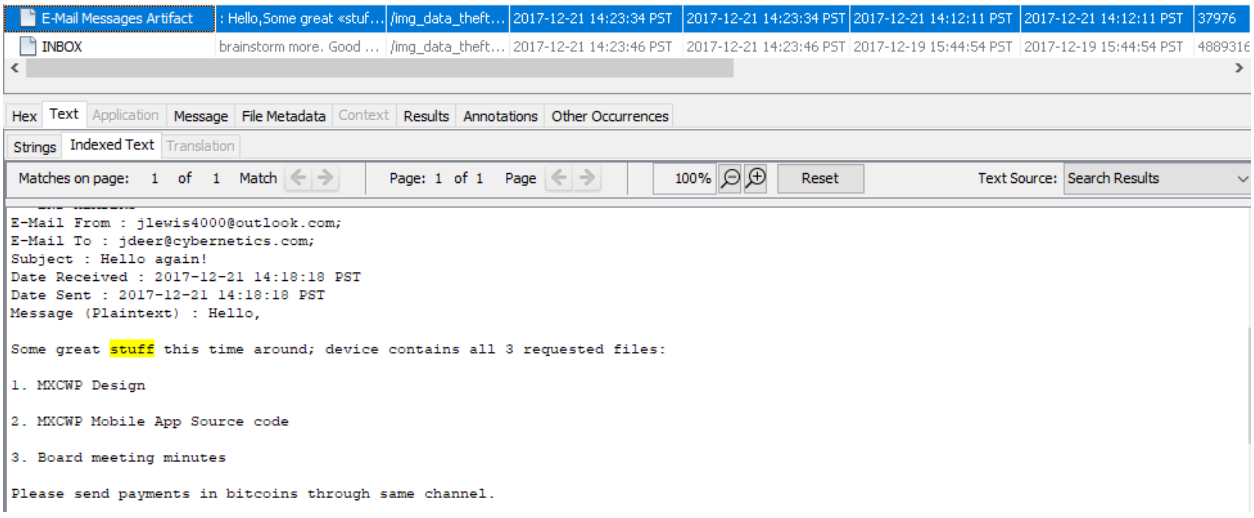
University of Victoria

And also,



This email was sent on December 21 and deleted.

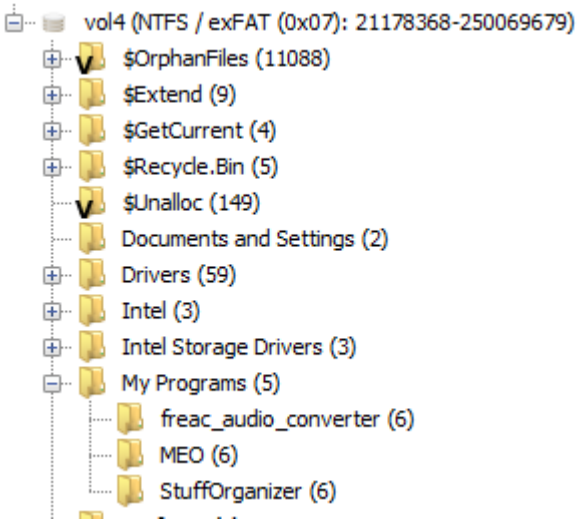
And also, Here on 21 December again this email sent to Jdeer from JLewis



According to those three emails reported, John Lewis mentioned three files will be sent to Jdeer. By collecting this information in the next step we tried to figure out whether or not he has these files in his personal laptops.

According to our investigation in the hard drive of Mr. Lewis and based on collecting and analyzing evidence supporting his case. We guess that the file located on My programs of volume 4 of Hard drive may be the **MXCWP Design data.**

The following image represents that this folder contains three folders that all of them are executable files. But after deep investigation of those evidence we found that the stuff-organizer folder contains another file format.



In Autopsy, stuff-organizer folder contains four files.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2017-12-19 17:57:53 PST	2017-12-19 17:57:53 PST	2017-12-19 17:57:53 PST	2017-12-19 17:57:52 PST
[parent folder]				2017-12-19 17:57:52 PST	2017-12-19 17:57:53 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:51 PST
LICENSE.txt				2017-12-14 09:41:11 PST	2017-12-18 18:18:34 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST
setup_stuff_organizer.exe				2017-12-14 09:35:11 PST	2017-12-18 18:19:50 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST
setup_stuff_organizer.exe:Zone.Identifier				2017-12-14 09:35:11 PST	2017-12-18 18:19:50 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST
stuff_organizer.exe				2017-12-18 18:14:54 PST	2017-12-18 18:18:59 PST	2017-12-19 17:57:53 PST	2017-12-19 17:57:53 PST

In FTKImager we found other information for this folder.

University of Victoria

Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	12/20/2017 1:57:53 AM
LICENSE.txt	34	Regular File	12/14/2017 5:41:11 PM
LICENSE.txt.FileSlack	3	File Slack	
setup_stuff_organizer.exe	4,545	Regular File	12/14/2017 5:35:11 PM
stuff_organizer.exe	230	Regular File	12/19/2017 2:14:54 AM
stuff_organizer.exe.FileSlack	3	File Slack	

If you pay attention to the time of access and modification of stuff-organizer.exe in both Autopsy and FTKImager, it will recognize these files accessed after working hours.

According to FTKImager information. We found both licenses. txt and stuff_organizer.exe have two .FileSlack files. These are good evidence for finding more information. In fact, SlackFiles represent some information that is separated from the original file. We can recover the password of this file based on SlackFile. Unfortunately, we cannot access SlackFiles in Autopsy. Encase Forensics is the best option in that case. But the information of SlackFiles cannot open in the stuff_organizer.zip.
The procedure of finding password based on SlackFiles is described as a follows:

First of all when we focus on extra information about file size and physical size we found weird information in FTKImager.

Evidence indicate that LICENCE.txt Physical size and size of file are different.

University of Victoria

Name	LICENSE.txt
File Class	Regular File
File Size	34,652
Physical Size	36,864
Start Cluster	19,264,266
Date Accessed	12/20/2017 1:57:52 AM
Date Created	12/20/2017 1:57:52 AM
Date Modified	12/14/2017 5:41:11 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	175,292,496
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	222,339 (227675136)
Date Changed (MFT)	12/19/2017 2:18:34 AM
Resident	False
Offline	False
Sparse	False

We can see that 36,864 as a Physical Size mines 34,652 as a File Size equal to 2,212.

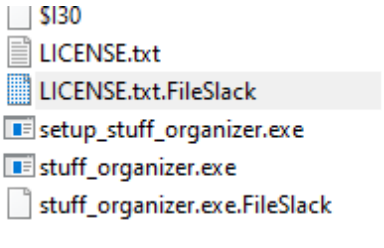
36,864-34,652= 2,212

Pay attention this file **start Cluster is 19,264,266** .

Here the **.FileSlack** of LICENCE.txt.FileSlack information is here.
THe FileSlack size is 2,212 .

University of Victoria

Name	LICENSE.txt.FileSlack
File Class	File Slack
File Size	2,212
Physical Size	2,212



For the another file stuff-organizer.exe
We can see that the 237,568 as a Physical Size mines 234,722 as a File Size equal to 2,846.
237,568 - 234,722 = 2,846
Pay attention this file start Cluster is 16,611,977 .

Name	stuff_organizer.exe
File Class	Regular File
File Size	234,722
Physical Size	237,568
Start Cluster	16,611,977
Date Accessed	12/20/2017 1:57:53 AM
Date Created	12/20/2017 1:57:53 AM
Date Modified	12/19/2017 2:14:54 AM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	154,074,184
DOS Attributes	
8.3 Short Filename	STUFF_~1.EXE
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	222,358 (227694592)
Date Changed (MFT)	12/19/2017 2:18:59 AM
Resident	False
Offline	False

LICENSE.txt	34	Regular File	12/14/2017 5
LICENSE.txt.FileSlack	3	File Slack	
setup_stuff_organizer.exe	4,545	Regular File	12/14/2017 5
stuff_organizer.exe	230	Regular File	12/19/2017 2
stuff_organizer.exe.FileSlack	3	File Slack	

```
393b0 F4 67 D3 C0 D2 E9 FF B6-18 E8 C1 30 AC EF A2 54 ôgÓÀÒéÿ¶·èÁ0¬ï¢T
393c0 A7 2B 3D 73 D7 6F A0 F6-8D 20 AD E9 1E DA 86 14 §+=s×o ö· -é·Ú··
393d0 E3 77 7E 26 2D D3 C0 01-DC 7E FB 8F E9 78 24 EB ãw~&-ÓÀ·Ü~û·éx$ë
393e0 6C 9E 98 E6 EF 72 A2 7E-B6 2C 3B F6 7C 71 0F 3C l··æïr¢~¶,;ö|q·<
393f0 29 E7 40 A1 0E 23 CE 46-BF 63 2A 39 70 AB 09 9B )ç@¡·#ÎF¿c*9p«··
39400 8A 94 D0 B5 33 C2 82 DD-1F CC AB 7F 33 99 65 71 ··Ðµ3Â·Ý·Ì«·3·eq
39410 03 F7 9D 1A D3 70 50 BD-AD F9 47 C1 5A 08 F2 AA ·÷··ÓpP½-ùGÁZ·ò²
39420 CD 48 83 87 08 72 BD E6-CE 83 AE FC BB 55 C3 1E ÍH···r½æÎ·®ü»UÃ·
39430 94 A6 7F 63 C8 4F 46 55-BD BE 5C 9B 00 82 44 14 ·¦·cÈOFU½¾\···D·
39440 32 F7 C7 D9 4E 0F AC A3-03 C1 0A B6 03 AB A9 AF 2÷ÇÙN·¬£·Á·¶·«©¯
39450 EE C5 3B 90 DF 75 A4 04-20 1C 88 9A A0 73 65 DC îÅ;·ßu¤·· ···seÜ
39460 D5 71 C2 16 17 76 BF FE-A7 7B BE E5 39 F7 BD 4A Õq Â···v¿þ§{¾å9÷½J
39470 01 04 06 00 01 09 C3 50-94 00 07 0B 01 00 02 24 ·····ÃP·····$
39480 06 F1 07 01 0A 53 07 1E-8B 93 0C EF 9F 8A 18 21 ·ñ···S····ï···!
39490 21 01 0C 01 00 0C C3 43-94 C3 33 94 00 08 0A 01 !·····ÃC·Ã3·····
394a0 48 46 ED 69 00 00 05 01-19 03 00 00 00 11 19 00 HFíi············
394b0 63 00 6F 00 6F 00 6B 00-69 00 6E 00 67 00 2E 00 c·o·o·k·i·n·g·.·
394c0 64 00 6F 00 63 00 00 00-19 02 00 00 14 0A 01 00 d·o·c···········
```

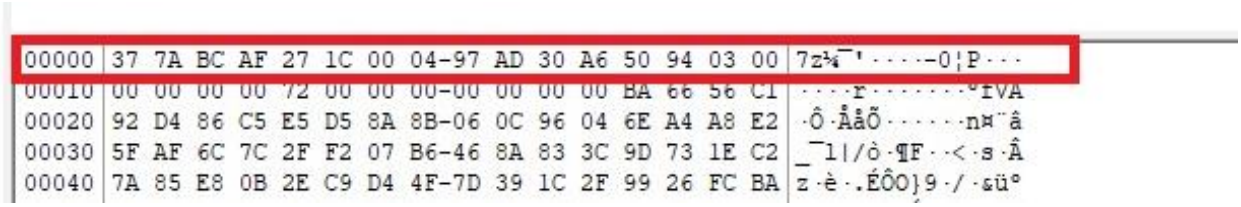
And also the .FileSlack information of stuff_organizer.exe.FileSlack is here
The fileSlack size is 2,846 .

University of Victoria

Name	stuff_organizer.exe.FileSlack
File Class	File Slack
File Size	2,846
Physical Size	2,846

LICENSE.txt	34	Regular File	12/14/2017 5:41:11 PM
LICENSE.txt.FileSlack	3	File Slack	
setup_stuff_organizer.exe	4,545	Regular File	12/14/2017 5:35:11 PM
stuff_organizer.exe	230	Regular File	12/19/2017 2:14:54 AM
stuff_organizer.exe.FileSlack	3	File Slack	

As we explained, stuff-organizer.exe is a zip file.
Some evidence prove this information:
1- Hex information of this file contains that this file is zip file



00000	37 7A BC AF 27 1C 00 04-97 AD 30 A6 50 94 03 00	7z¼¯'·····-0¦P···
00010	00 00 00 00 72 00 00 00-00 00 00 00 BA 66 56 C1	····r·······ºfVÁ
00020	92 D4 86 C5 E5 D5 8A 8B-06 0C 96 04 6E A4 A8 E2	·Ô·ÅåÕ·····n¤¨â
00030	5F AF 6C 7C 2F F2 07 B6-46 8A 83 3C 9D 73 1E C2	_¯l|/ò·¶F··<·s·Â
00040	7A 85 E8 0B 2E C9 D4 4F-7D 39 1C 2F 99 26 FC BA	z·è·.ÉÔO}9·/·&ü°

At first line, numbers 37 7A BC AF is Hex signature of 7 zip compressed files.
Note: we check this signature in https://www.filesignatures.net/

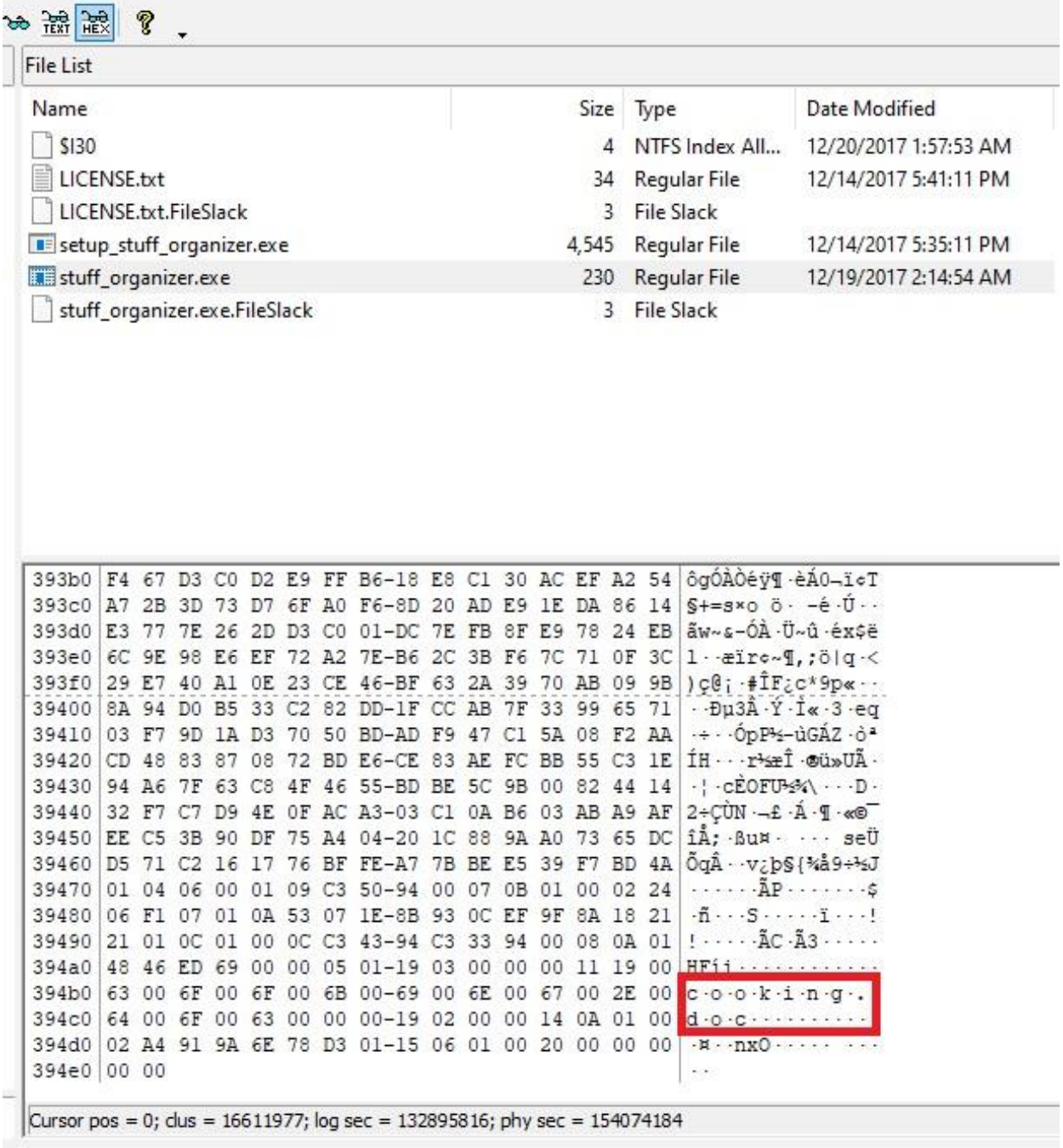
1 Results Found For 377ABCAF271C

Extension	Signature	Description
7Z	37 7A BC AF 27 1C	7-Zip compressed file
	ASCII 7z'•	Sizet: 6 Bytes Offset: 0 Bytes

When we extract this file on Autopsy and save on the hard drive we change the file format from .exe to .zip

So, when this file opened . This file contained one word file.
And also NOTE:> Here at the end of HEX File of stuff-organizer.exe in FTKImager mentioned that this file contains file that name is cooking.doc
Each file in Hex separated to 512 bytes data.

University of Victoria

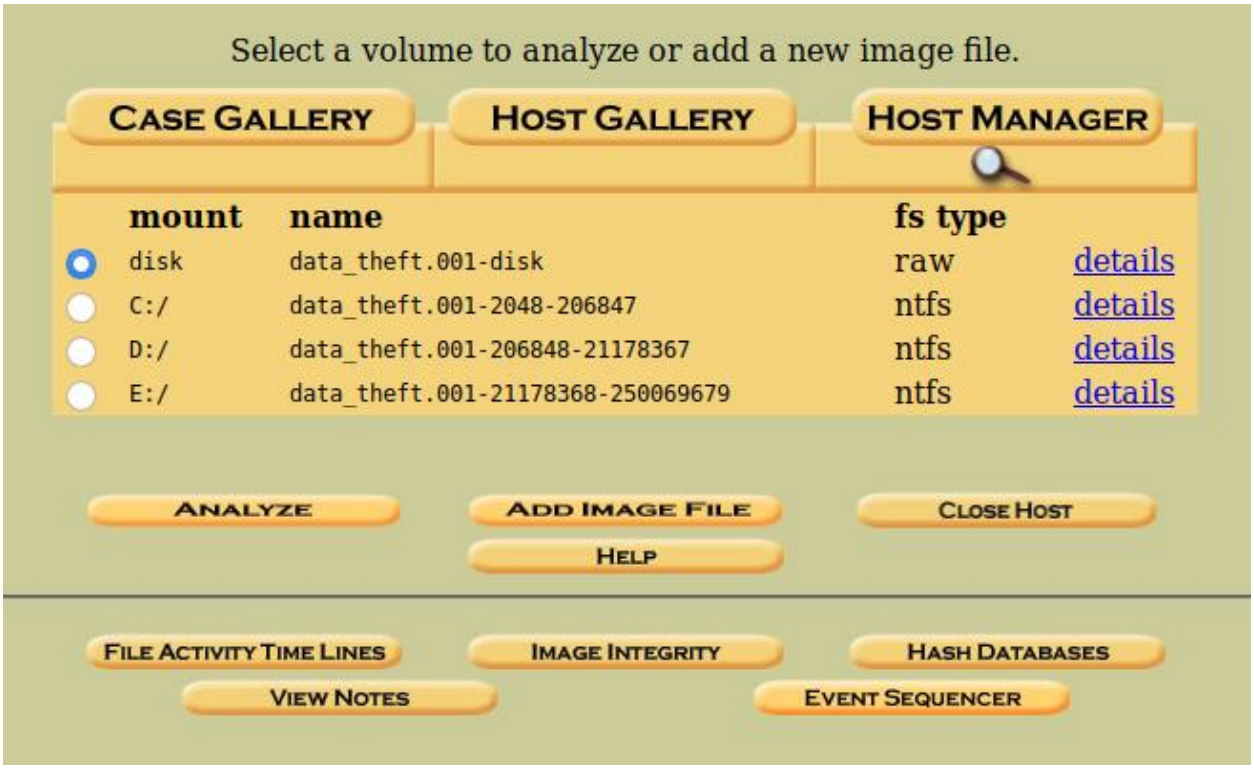


University of Victoria

F:\forencies\stuff_organizer.zip\

Name	Size	Packed Size	Modified	Attributes	CRC
cooking.doc	234 547	234 576	2017-12-18 19:10	A	69ED4648

3- we have file size, physical size and cluster size based on FTKImager report.
So, we use Autopsy in Kali Linux to recover the password of this file.



We have 4 partitions and select E as a fourth partition. Because our file is located in volum4.

In Autopsy go to E:/My programs/Stuff-Otrganizer

University of Victoria

./	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:52 (EST)	56	0	0	222327-144-6
LICENSE.txt	2017-12-14 12:41:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:18:34 (EST)	2017-12-19 20:57:52 (EST)	34652	0	0	222339-128-1
setup_stuff_organizer.exe	2017-12-14 12:35:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:19:50 (EST)	2017-12-19 20:57:52 (EST)	4653702	0	0	222357-128-1
setup_stuff_organizer.exe:Zone.Identifier	2017-12-14 12:35:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:19:50 (EST)	2017-12-19 20:57:52 (EST)	26	0	0	222357-128-4
stuff_organizer.exe	2017-12-18 21:14:54 (EST)	2017-12-19 20:57:53 (EST)	2017-12-18 21:18:59 (EST)	2017-12-19 20:57:53 (EST)	234722	0	0	222358-128-1

MFT Entry Number: 222358-128-1

VIEW

ALLOCATION LIST

PREVIOUS NEXT

REPORT VIEW CONTENTS EXPORT CONTENTS ADD NOTE

Pointed to by file:
E:/My Programs/StuffOrganizer/stuff_organizer.exe

File Type:
7-zip archive data, version 0.4

MD5 of content:
949feba9609eb0a580ae0f02942966d6 -

SHA-1 of content:
bf1e7ca36693e5c2cfe730d99edaf636f1f05bf2 -

Details:

MFT Entry Header Values:
Entry: 222358 Sequence: 3
$LogFile Sequence Number: 912613878
Allocated File
Links: 2

MFT Entry Number: 222358-128-1

VIEW

ALLOCATION LIST

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 3822 (S-1-5-21-3405613258-3021893473-2990877082-1003)
Last User Journal Update Sequence Number: 268475408
Created: 2017-12-19 20:57:53.012304500 (EST)
File Modified: 2017-12-18 21:14:54.220800200 (EST)
MFT Modified: 2017-12-18 21:18:59.271800200 (EST)
Accessed: 2017-12-19 20:57:53.012304500 (EST)

$FILE_NAME Attribute Values:
Flags: Archive
Name: STUFF_~1.EXE
Parent MFT Entry: 222327 Sequence: 6
Allocated Size: 237568 Actual Size: 0
Created: 2017-12-19 20:57:53.012304500 (EST)
File Modified: 2017-12-19 20:57:53.012304500 (EST)
MFT Modified: 2017-12-19 20:57:53.012304500 (EST)
Accessed: 2017-12-19 20:57:53.012304500 (EST)

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

MFT Entry Number: 222358-128-1

VIEW

ALLOCATION LIST

$FILE_NAME Attribute Values:
Flags: Archive
Name: stuff_organizer.exe
Parent MFT Entry: 222327 Sequence: 6
Allocated Size: 237568 Actual Size: 0
Created: 2017-12-19 20:57:53.012304500 (EST)
File Modified: 2017-12-19 20:57:53.012304500 (EST)
MFT Modified: 2017-12-19 20:57:53.012304500 (EST)
Accessed: 2017-12-19 20:57:53.012304500 (EST)

Attributes:
$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
$FILE_NAME (48-3) Name: N/A Resident size: 90
$FILE_NAME (48-2) Name: N/A Resident size: 104
$DATA (128-1) Name: N/A Non-Resident size: 234722 init_size: 234722
16611977 16611978 16611979 16611980 16611981 16611982 16611983 16611984
16611985 16611986 16611987 16611988 16611989 16611990 16611991 16611992
16611993 16611994 16611995 16611996 16611997 16611998 16611999 16612000
16612001 16612002 16612003 16612004 16612005 16612006 16612007 16612008
16612009 16612010 16612011 16612012 16612013 16612014 16612015 16612016
16612017 16612018 16612019 16612020 16612021 16612022 16612023 16612024
16612025 16612026 16612027 16612028 16612029 16612030 16612031 16612032
16612033 16612034

University of Victoria

Based on data that investigated from FTKImager
Put cluster name 16611977 and the number of clusters 1.
The first link in the image above. But the information in Hex and ASCCII does not seems correct and it does not open password of cooking.doc
Hex details show as a following image:

d / d	../	2017-12-19 20:57:52 (EST)	2017-12-19 20:57:52 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:51 (EST)	56	0	0	1383-144-6
d / d	./	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:52 (EST)	56	0	0	222327-144-6
r / r	LICENSE.txt	2017-12-14 12:41:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:18:34 (EST)	2017-12-19 20:57:52 (EST)	34652	0	0	222339-128-1
r / r	setup_stuff_organizer.exe	2017-12-14 12:35:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:19:50 (EST)	2017-12-19 20:57:52 (EST)	4653702	0	0	222357-128-1
r / r	setup_stuff_organizer.exe:Zone.Identifier	2017-12-14 12:35:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:19:50 (EST)	2017-12-19 20:57:52 (EST)	26	0	0	222357-128-4
r / r	stuff_organizer.exe	2017-12-18 21:14:54 (EST)	2017-12-19 20:57:53 (EST)	2017-12-18 21:18:59 (EST)	2017-12-19 20:57:53 (EST)	234722	0	0	222358-128-1

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: 7-zip archive data, version 0.4

```
Hex Contents Of File: E:/My Programs/StuffOrganizer/stuff_organizer.exe

00000000:  377A BCAF 271C 0004 97AD 30A6 5094 0300    7z..'.....0.P...
00000010:  0000 0000 7200 0000 0000 0000 BA66 56C1    ....r........fV.
00000020:  92D4 86C5 E5D5 8A8B 060C 9604 6EA4 A8E2    ............n...
00000030:  5FAF 6C7C 2FF2 07B6 468A 833C 9D73 1EC2    _.l|/...F..<.s..
00000040:  7A85 E80B 2EC9 D44F 7D39 1C2F 9926 FCBA    z.......O}9./.&..
00000050:  9593 FD9D 6FE9 7C60 DA14 111D AD0B 3ABD    ....o.|`......:.
00000060:  8B62 CF1E DF4A 64F0 718F 32FB C367 06A6    .b...Jd.q.2..g..
00000070:  C924 761D 2DDA B56D 90E9 9A7B 4684 BD30    .$v.-..m...{F..0
00000080:  0AB7 6902 8263 6B32 90C5 6548 3990 7756    ..i..ck2..eH9.wV
00000090:  D662 62EB 9079 F617 9B33 D112 877F 1980    .bb..y...3......
000000A0:  576E 7C71 7969 19E4 80C8 15EE D770 107A    Wn|qyi.......p.z
```

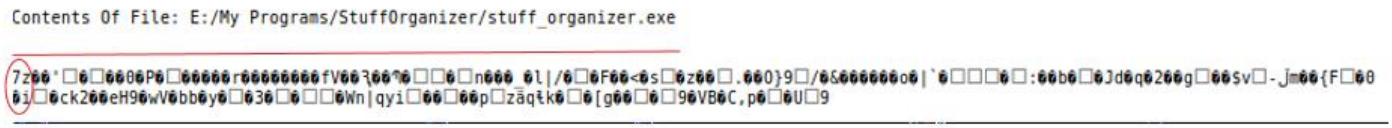
ASCII details show as a following image:

d / d	../	2017-12-19 20:57:52 (EST)	2017-12-19 20:57:52 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:51 (EST)	56	0	0	1383-144-6
d / d	./	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:53 (EST)	2017-12-19 20:57:52 (EST)	56	0	0	222327-144-6
r / r	LICENSE.txt	2017-12-14 12:41:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:18:34 (EST)	2017-12-19 20:57:52 (EST)	34652	0	0	222339-128-1
r / r	setup_stuff_organizer.exe	2017-12-14 12:35:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:19:50 (EST)	2017-12-19 20:57:52 (EST)	4653702	0	0	222357-128-1
r / r	setup_stuff_organizer.exe:Zone.Identifier	2017-12-14 12:35:11 (EST)	2017-12-19 20:57:52 (EST)	2017-12-18 21:19:50 (EST)	2017-12-19 20:57:52 (EST)	26	0	0	222357-128-4
r / r	stuff_organizer.exe	2017-12-18 21:14:54 (EST)	2017-12-19 20:57:53 (EST)	2017-12-18 21:18:59 (EST)	2017-12-19 20:57:53 (EST)	234722	0	0	222358-128-1

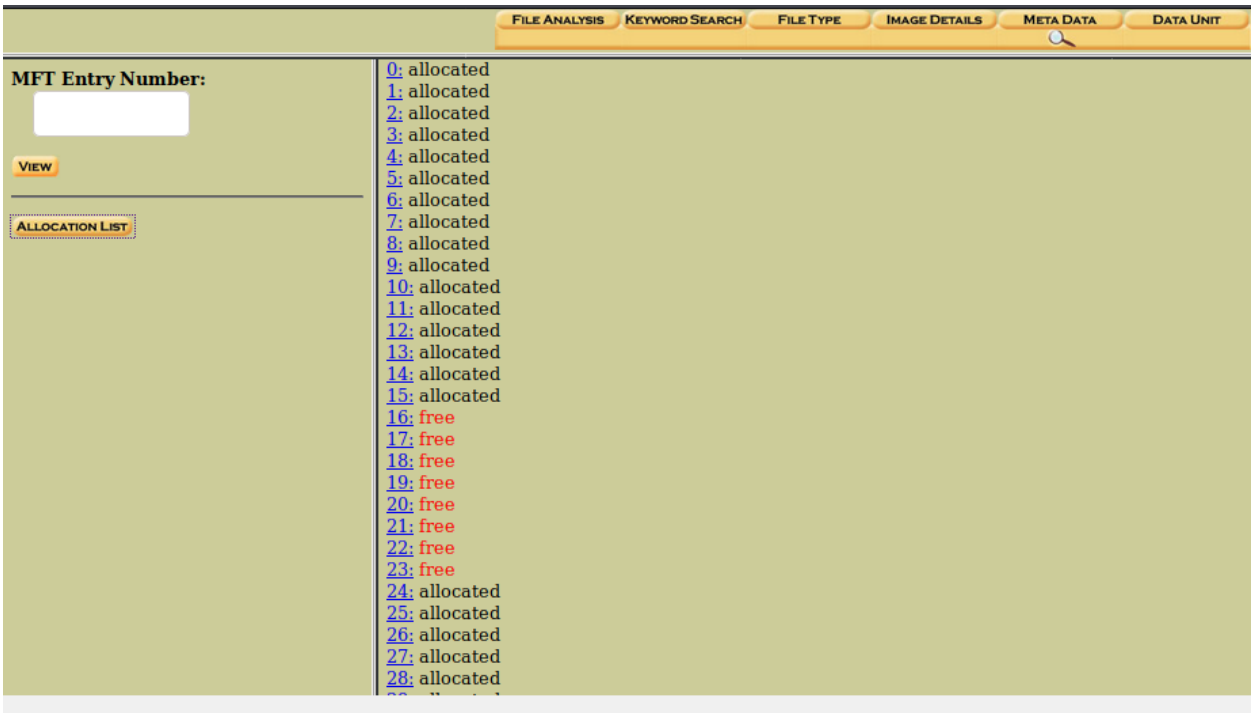
ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: 7-zip archive data, version 0.4

```
Contents Of File: E:/My Programs/StuffOrganizer/stuff_organizer.exe
```

ASCII s code shows that Autopsy has recognised this file as Zip Archive. And will be opened with 7zip.



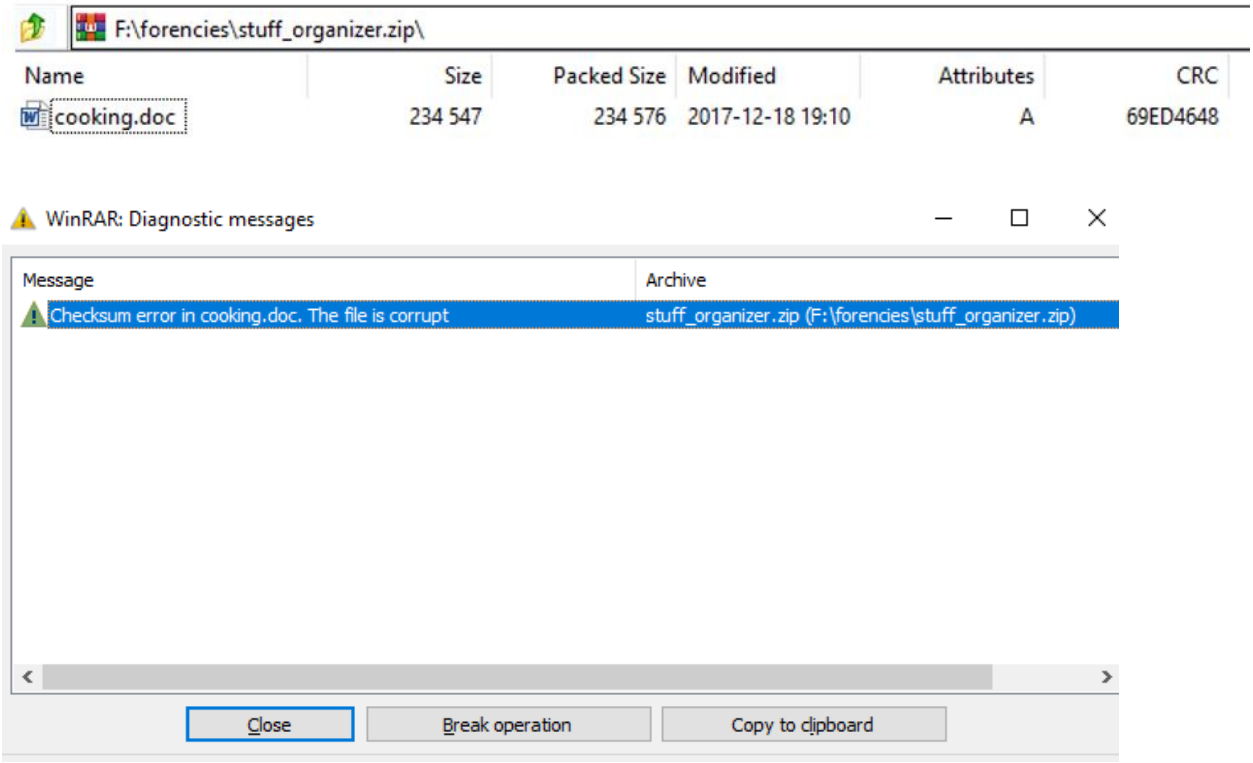
In Meta Data part, some information related to allocation parts of the Disk in particular stuff-organizer.exe shown as a following image:



Here surprisingly from sector 16 to sector 23 are unallocated. Or Free.

```
15: allocated
16: free
17: free
18: free
19: free
20: free
21: free
22: free
23: free
24: allocated
```

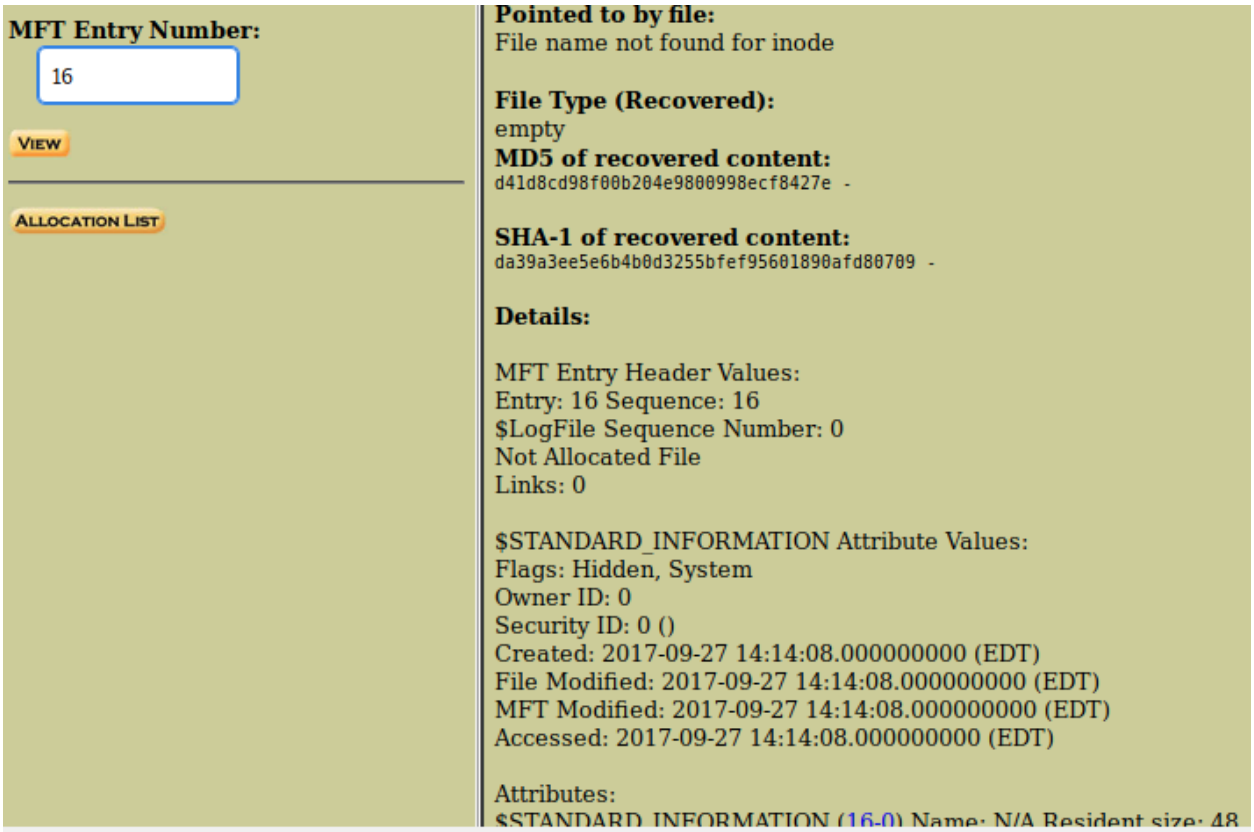
Not only tested passwords for this file is not successful but also error related that The file is corrupt shown as a following image:



Corrupt files can result from a variety of issues including bad drive sectors, malware, an incomplete download or transfer such as during a drop in your connection, or any

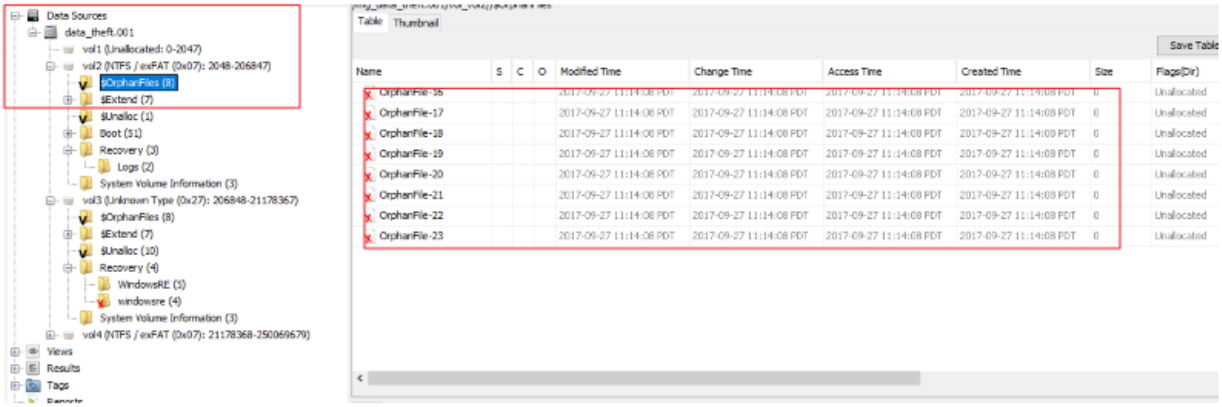
other sudden interruption like a power failure or an improper shut down while working with the **ZIP file.**
This file was found in two locations of Image Forensics Disk.
Stuff-organizer located in two locations in Image Disk. All two locations are corrupted. It may be when moving from one drive to another drive file is damaged.
We guess that this file contains MXCWP Design information. This file is compressed by 7zip.

Investigation deeply on Forensics Image of Mr. Lewis laptop shows those 8 MFT that are free or unallocated in stuff_organizer.exe in Autopsy report. Some images regarding this claim are shown as follows: .
In Kali Autopsy:
MFT number 16, the first line that is free. The details show that Created, Modified, MFT Modified, and Accessed file was returned to **September 29, 2017.**



All sectors of this file (stuff-organizer.exe) especially unallocated part (16-23) represent Created, Modified, MFT Modified, and Accessed file was returned to September 29, 2017.

So, it definitely proves that the theft did not fetch this file.
Moreover, in Windows Autopsy search those files deleted from vol 2 of Disk image on 2017-09-27. Suppose to those evidence, never and ever this file is fetched with theft.

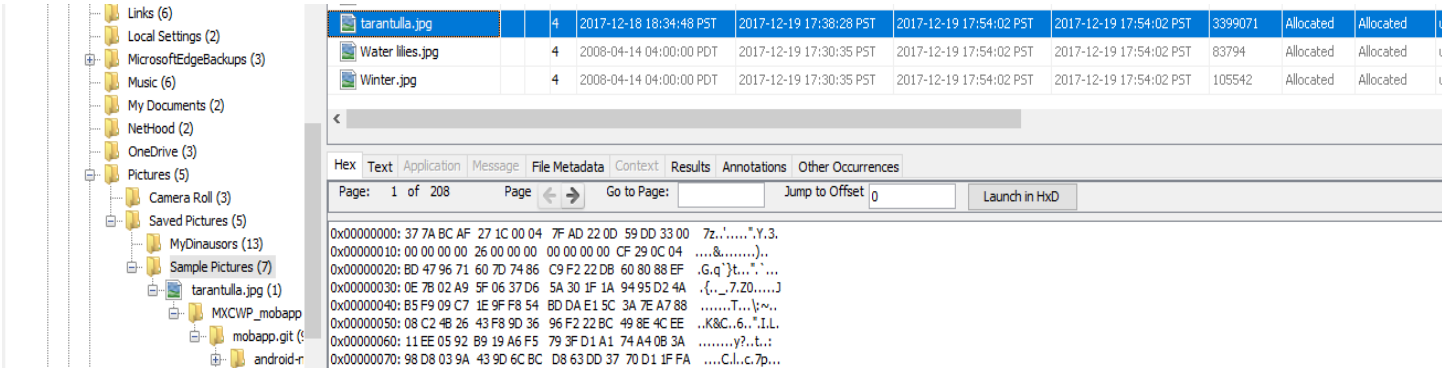


On a computer's hard drive, an **orphan file** is a support file (such as a DLL file) that no longer serves a purpose because the "parent" application it is associated with has been **moved or uninstalled**. **Orphan files can be deleted manually if the user is confident that the file is not being used by any other application.**
So, analysis of Lewis Disk Image gives information that some part of this file was damaged. The date of deleting this file illustrates that this file was not open on December 21 on target machine.

The second specific content that is recognized based on Email is **MXCWP Mobile App Source Code**.

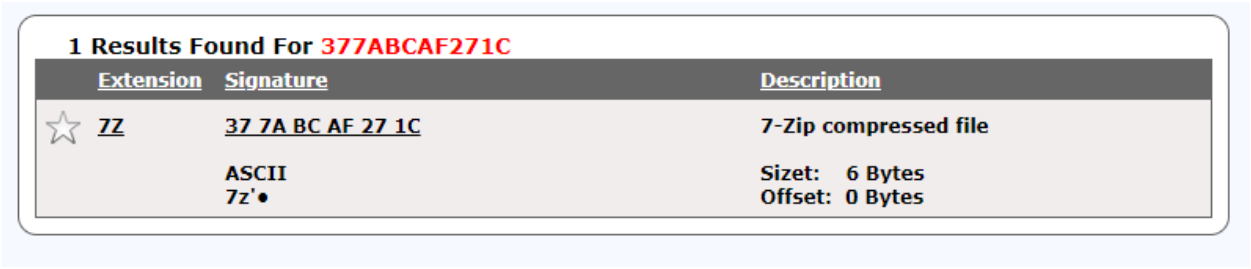
According to our investigation on Disk. Based on time and keyword We found a malicious file which was listed with other photos with extension .jpg.

When we select tarantula.jpg and check Hex value on that file we found that Hex value in started with 37 7A BC AF which shows it must have extension zip instead of jpg.

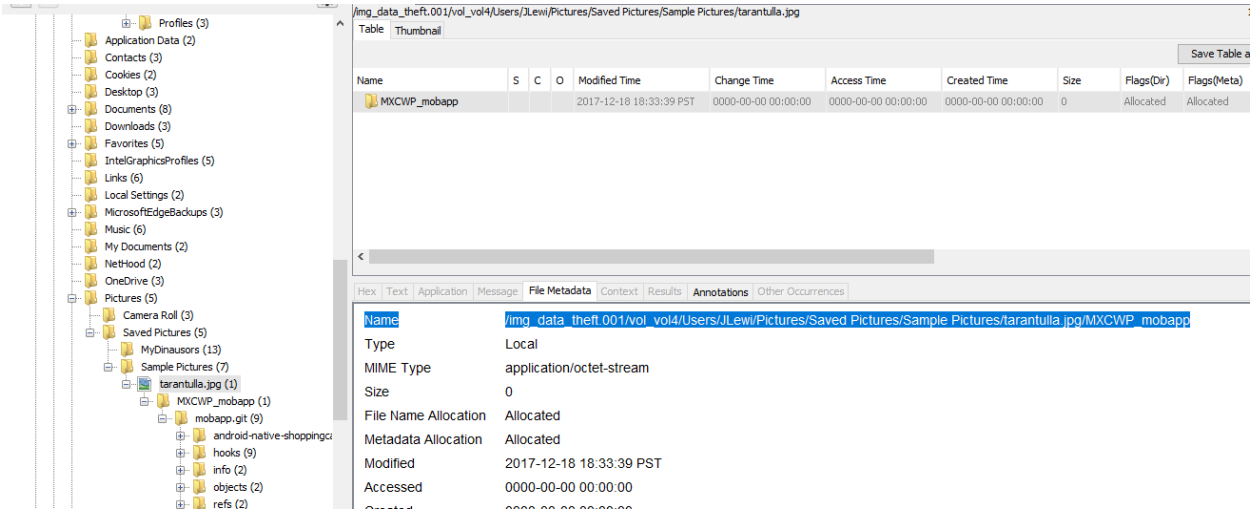


With click on tarantula.jpg illustrates No pictures preview.

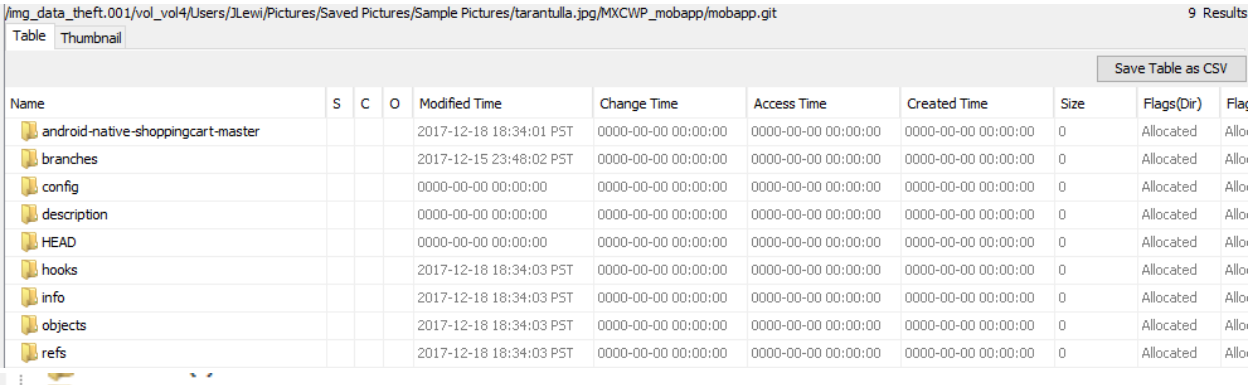
Then, check the Hex details of this picture. Analyzing information on the Hex part represents that this file is a zip file. 7z shows that the file is a compressed format. It will open with 7zip.

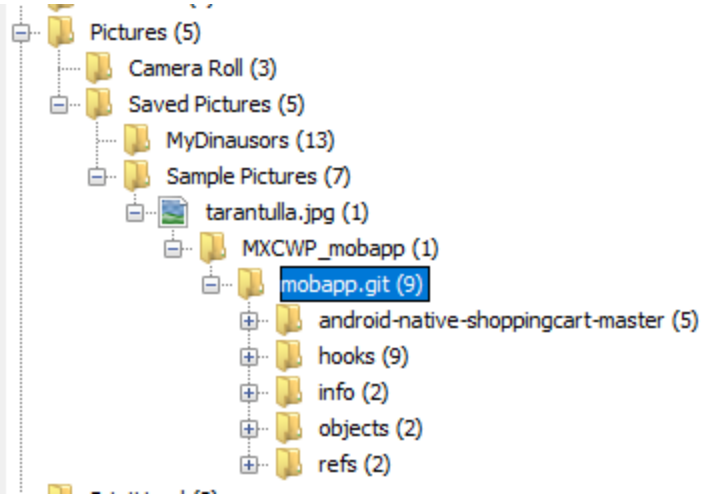


Evidence illustrates that double click on it shows MXCWP FOLDER.



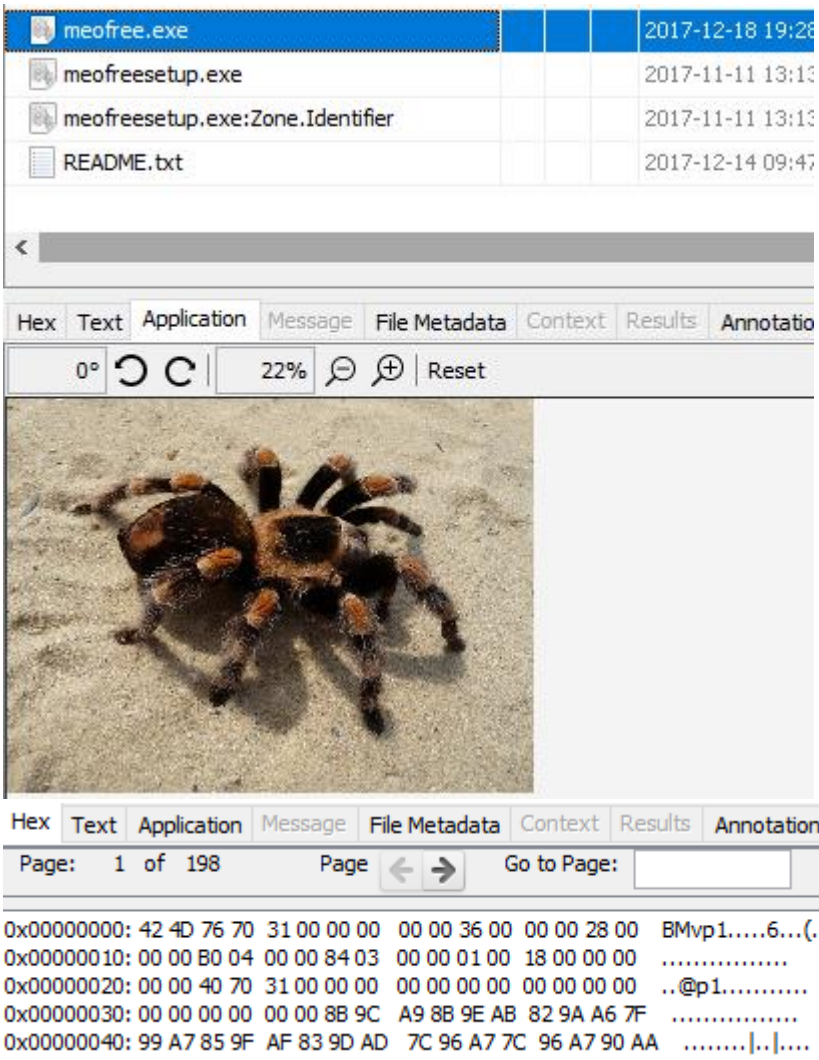
And also,
This file was modified on December 18. And it seems that Mr. Lewis deleted it.
Data and information about MXCWP can fetch by theft. But some of the data is lost.



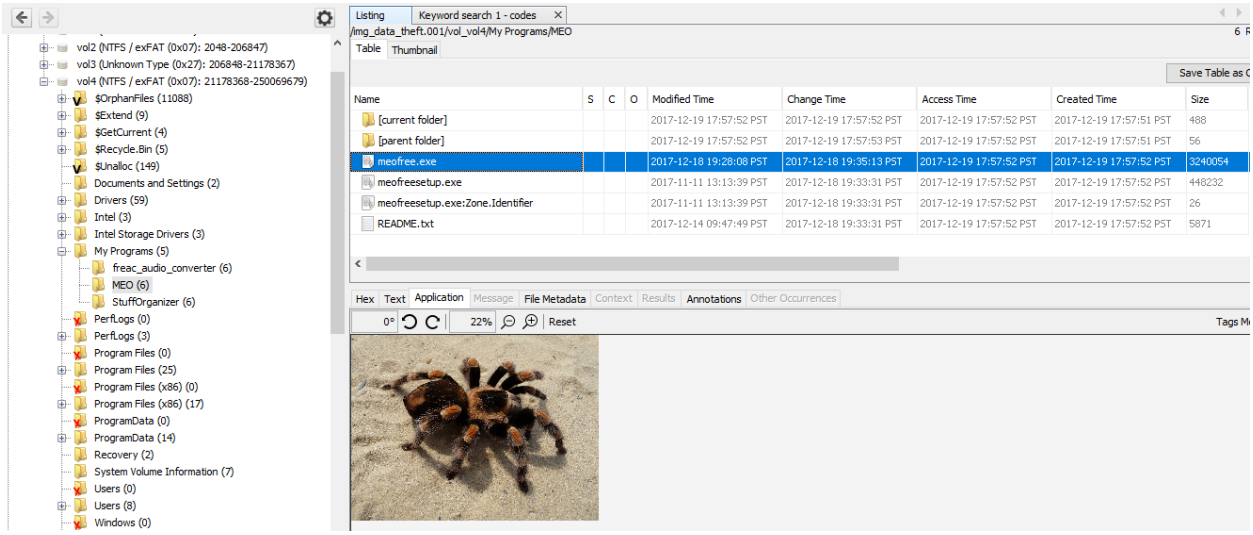


But this file is password protected and we need to find the password of this file.
In My programs under folder MEO we found a suspected file, moefreesetup.exe with extension .exe but doing more search on hex value to represent this file is not an execution file. It is a jpg file. changing extension file to jpg and use steganography tool, quick stego, to see whether or not there is hidden text.

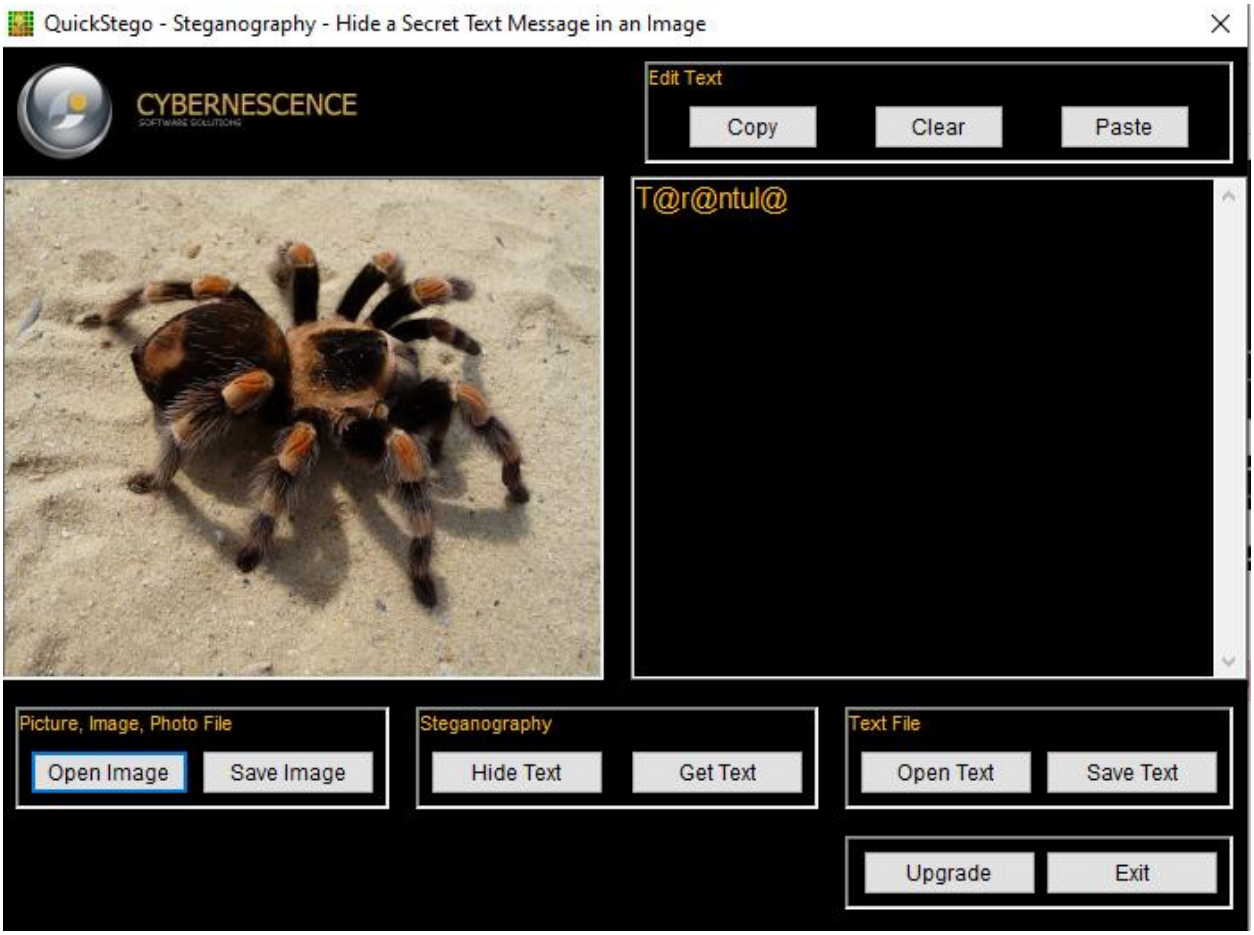
University of Victoria



Hex and description BMp prove that this file is picture not an executable file.



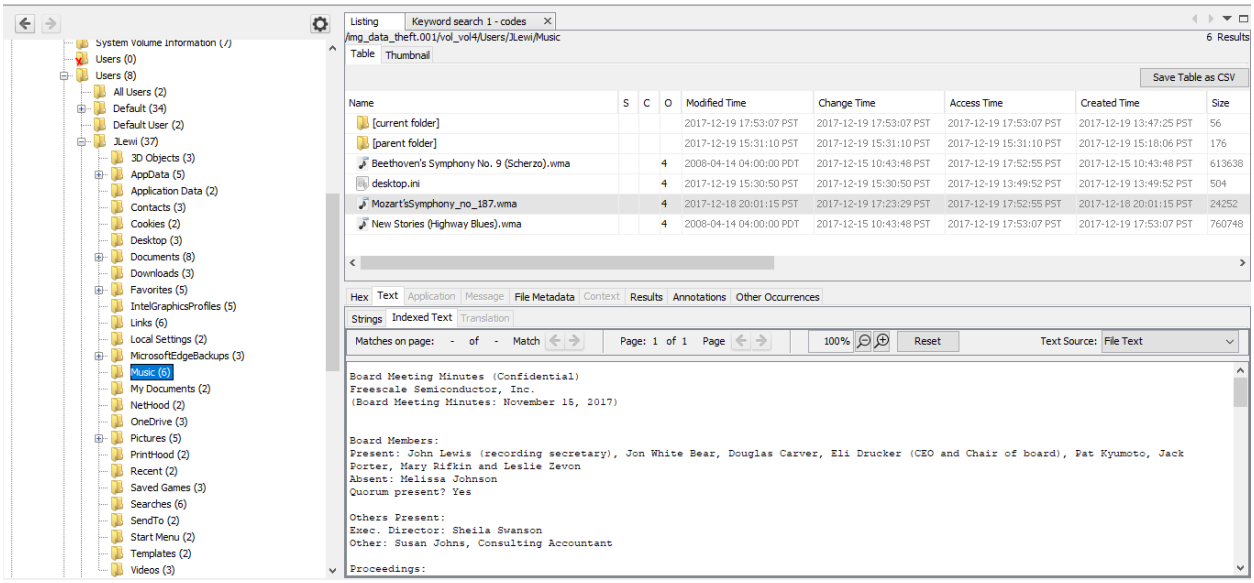
This image has encrypted and hidden passwords, **T@r@ntul@**. We tried this password to open the previous suspected folder, tarantula.zip and it was its passcode.



This is password of Tarantula.zip

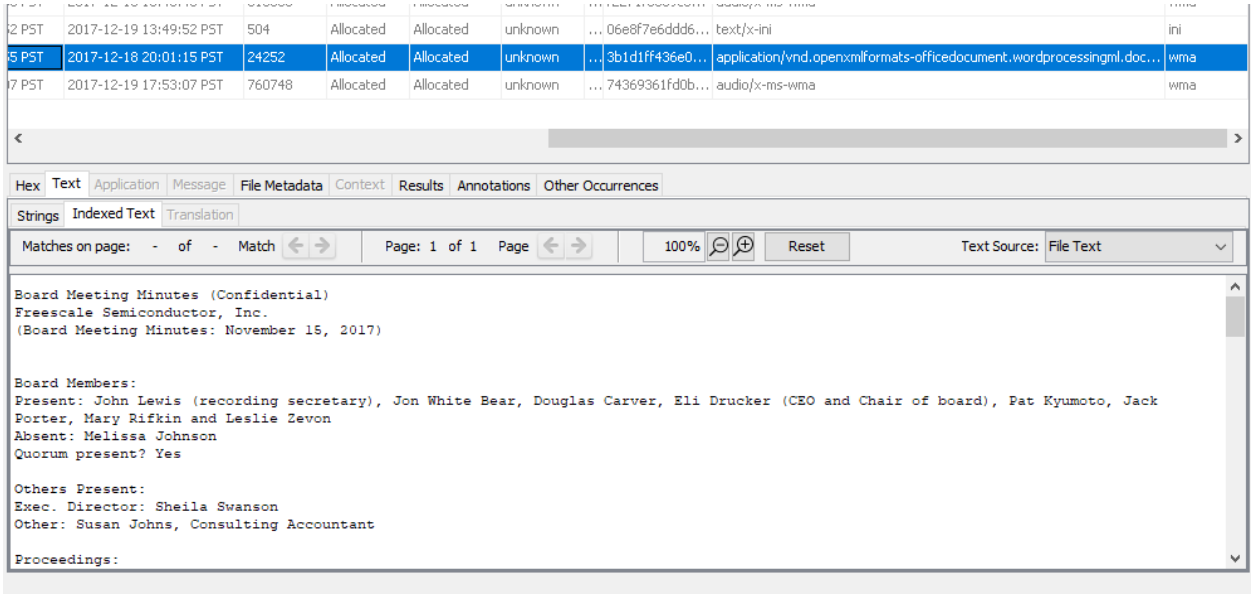
Third part of data that was transferred between Mr, Lewis and one employee from Cybernetics.

Surprisingly, Mr. Lewis hides the “Board Meeting Minutes” word file in the music folder in his user information. He changed the format name from.doc to .wma.



clicking on this file represents that it is the text message instead of the music track.

And also, checked the MIME Type of the file is prove that this word file is not music file.



50 4B 03 04 14 00 06 00		PK.....
	DOCX, PPTX, XLSX	Microsoft Office Open XML Format (OOXML) Document **NOTE:** There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively.

Here is a copy of this file that is in a word format.

University of Victoria

Board Members:
Present: John Lewis (recording secretary), Jon White Bear, Douglas Carver, Eli Drucker (CEO and Chair of board), Pat Kyumoto, Jack Porter, Mary Rifkin and Leslie Zevon
Absent: Melissa Johnson
Quorum present? Yes

Others Present:
Exec. Director: Sheila Swanson
Other: Susan Johns, Consulting Accountant

Proceedings:
· *Meeting called to order* at 7:00 p.m. by Chair, Eli Drucker
· (Last month's) meeting minutes were amended and approved

· *Chief Executive's Report:*
- Summarizes great progress achieved by the R&D department in developing the new algorithms and architecture for the Mobile Extreme Convergence platform. The performances achieved exceed by far existing benchmark and will position the company as the undisputed leader of the market segment.

- Raises concerns that Cybernetics Inc., the closest competitor of Freescale Semiconductor, might try to steal the intellectual property (IP) related to the Mobile Extreme Convergence platform.

- Recommends, to mitigate the threat of IP theft that the core designs and formulas be kept tightly as trade secrets, and only generic description of the system be filed as patent.

- Staff member, Jackson Browne, and Swanson attended the National Practitioner's Network meeting in Atlanta last month and gave a brief extemporaneous presentation. Both are invited back next year to give a longer presentation about our company. After brief discussion, Board congratulated Swanson and asked her to pass on their congratulations to Browne as well.

- Drucker asserts that our company must ensure its name is associated with whatever materials are distributed at that practitioner's meeting next year. The company should generate revenues where possible from the materials, too.

- Swanson mentioned that staff member, Sheila Anderson's husband is ill and in the hospital. MOTION to send a gift to Anderson's husband, expressing the organization's sympathy and support; seconded and passed.

CONFIDENTIAL

University of Victoria

· *Finance report* provided by Chair, Eli Drucker:
- Drucker explained that consultant, Susan Johns, reviewed the organization's bookkeeping procedures and found them to be satisfactory, in preparation for the upcoming yearly financial audit. Funds recommends that our company ensure the auditor provides a management letter along with the audit financial report.
- Drucker reviewed highlights, trends and issues from the balance sheet, income statement and cash flow statement. Issues include that high accounts receivables require Finance department attention to policies and procedures to ensure our company receives more payments on time. After brief discussion of the issues and suggestions about how to ensure receiving payments on time, MOTION to accept financial statements; seconded and passed.

· Business *Development report* provided by VP Business Development, Douglas Carver:
- Carver reminded the Board of the scheduled retreat coming up in three months, and provided a drafted retreat schedule for board review. MOTION to accept the retreat agenda; seconded and passed.
- Carver presented members with a draft of the reworded By-laws paragraph that would allow members to conduct actions over electronic mail. Carver suggested review and a resolution to change the By-laws accordingly. Kyumoto suggested that Swanson first seek legal counsel to verify if the proposed change is consistent with state statute. Swanson agreed to accept this action and notify members of the outcome in the next Board meeting.

· *Other business:*
- Porter noted that he was working with staff member, Jacob Smith, to help develop an information management systems plan, and that two weeks ago he (Porter) had mailed members three resumes from consultants to help with the plan. In the mailing, Porter asked members for their opinions to help select a consultant. Porter asked members for their opinions. The majority of members agreed on Lease-or-Buy Consultants. MOTION to use Lease-or-Buy Consultants; seconded and passed.
- Swanson announced that she had recently hired a new secretary, Karla Writewell.

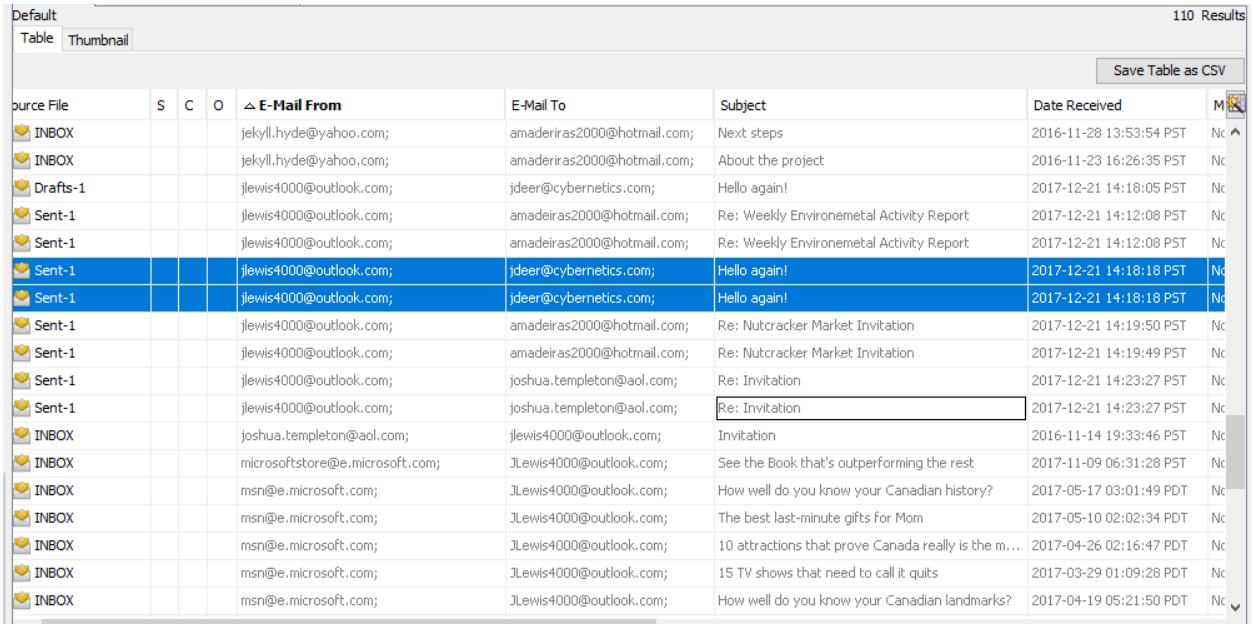
· *Assessment of the Meeting:*
- Kyumoto noted that the past three meetings have run over the intended two-hour time slot by half an hour. He asked members to be more mindful and focused during discussions, and suggested that the Business Development takes an action to identify solutions to this issue. Chair, Carver, agreed.

· Meeting adjourned at 9:30 p.m.
· Minutes submitted by Secretary, John Lewis.

CONFIDENTIAL

Based on the date we found on email and also the date when he planned to fetch information to theft, his personal laptop against company policy at work we tried to check all created,changed and modified files and directories, as follows:

University of Victoria



Default 110 Results

Table | Thumbnail

Save Table as CSV

ource File	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	M
INBOX				jekyll.hyde@yahoo.com;	amaderiras2000@hotmail.com;	Next steps	2016-11-28 13:53:54 PST	Nc
INBOX				jekyll.hyde@yahoo.com;	amaderiras2000@hotmail.com;	About the project	2016-11-23 16:26:35 PST	Nc
Drafts-1				jlewis4000@outlook.com;	jdeer@cybernetics.com;	Hello again!	2017-12-21 14:18:05 PST	Nc
Sent-1				jlewis4000@outlook.com;	amadeiras2000@hotmail.com;	Re: Weekly Environemetal Activity Report	2017-12-21 14:12:08 PST	Nc
Sent-1				jlewis4000@outlook.com;	amadeiras2000@hotmail.com;	Re: Weekly Environemetal Activity Report	2017-12-21 14:12:08 PST	Nc
Sent-1				jlewis4000@outlook.com;	jdeer@cybernetics.com;	Hello again!	2017-12-21 14:18:18 PST	Nc
Sent-1				jlewis4000@outlook.com;	jdeer@cybernetics.com;	Hello again!	2017-12-21 14:18:18 PST	Nc
Sent-1				jlewis4000@outlook.com;	amadeiras2000@hotmail.com;	Re: Nutcracker Market Invitation	2017-12-21 14:19:50 PST	Nc
Sent-1				jlewis4000@outlook.com;	amadeiras2000@hotmail.com;	Re: Nutcracker Market Invitation	2017-12-21 14:19:49 PST	Nc
Sent-1				jlewis4000@outlook.com;	joshua.templeton@aol.com;	Re: Invitation	2017-12-21 14:23:27 PST	Nc
Sent-1				jlewis4000@outlook.com;	joshua.templeton@aol.com;	Re: Invitation	2017-12-21 14:23:27 PST	Nc
INBOX				joshua.templeton@aol.com;	jlewis4000@outlook.com;	Invitation	2016-11-14 19:33:46 PST	Nc
INBOX				microsoftstore@e.microsoft.com;	JLewis4000@outlook.com;	See the Book that's outperforming the rest	2017-11-09 06:31:28 PST	Nc
INBOX				msn@e.microsoft.com;	JLewis4000@outlook.com;	How well do you know your Canadian history?	2017-05-17 03:01:49 PDT	Nc
INBOX				msn@e.microsoft.com;	JLewis4000@outlook.com;	The best last-minute gifts for Mom	2017-05-10 02:02:34 PDT	Nc
INBOX				msn@e.microsoft.com;	JLewis4000@outlook.com;	10 attractions that prove Canada really is the m...	2017-04-26 02:16:47 PDT	Nc
INBOX				msn@e.microsoft.com;	JLewis4000@outlook.com;	15 TV shows that need to call it quits	2017-03-29 01:09:28 PDT	Nc
INBOX				msn@e.microsoft.com;	JLewis4000@outlook.com;	How well do you know your Canadian landmarks?	2017-04-19 05:21:50 PDT	Nc

Email sent to jdeer from jlewis on December 21.

Some evidence prove that Mr. Lewis suspicious are listed here:

1- Bitcoins

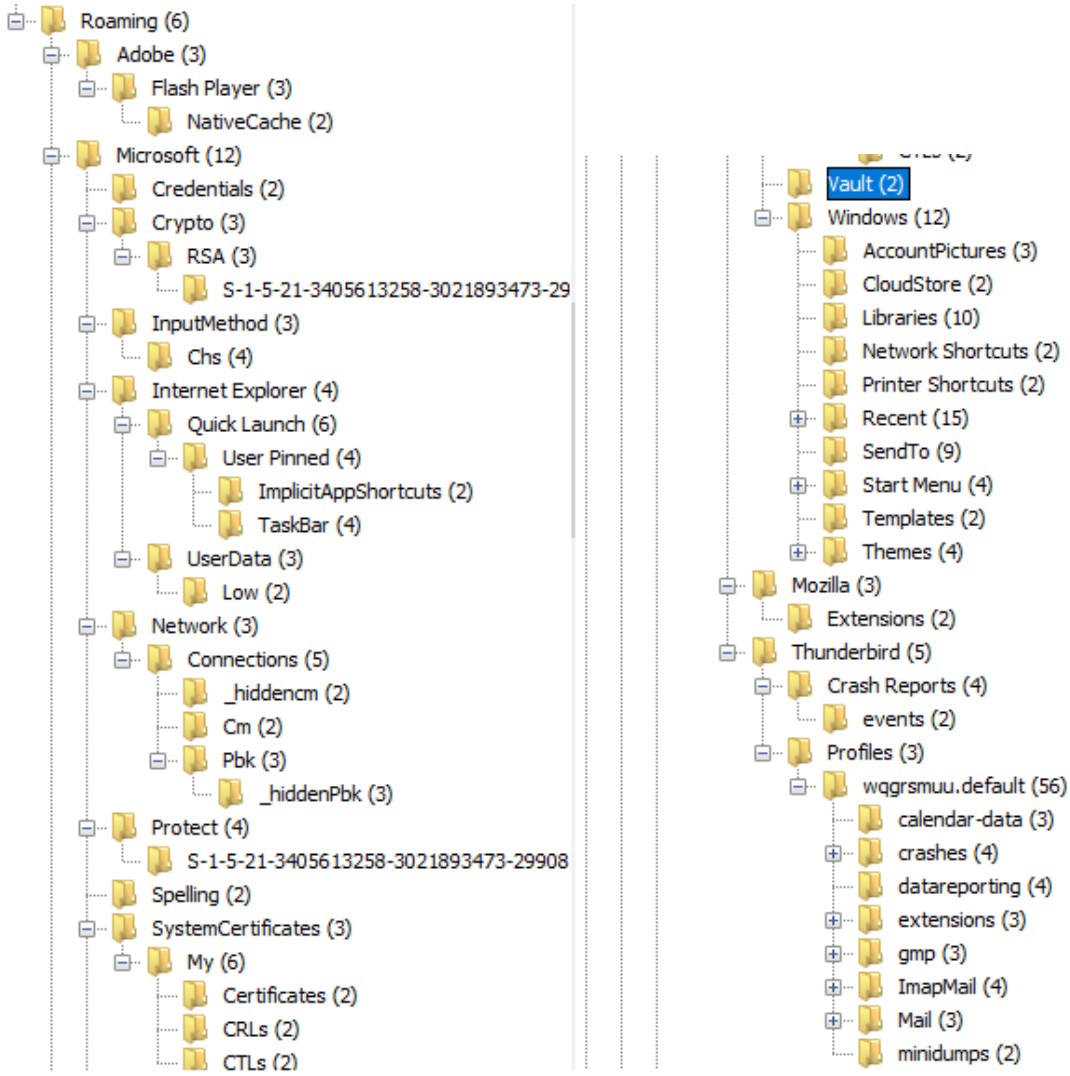
He mentioned that he sends payments in bitcoins. Looking for collecting evidence and information leads to finding some files that prove bitcoins account, bitcoins wallet.

In win 7 or later, These are files and folders in Appdata/roaming
This is the folder that has bitcoin information on it.

In win XP this file is located in documents/application data/
But here folder is empty, in both Autopsy and FTKImager
Folder empty means that he deleted all files related to bitcoin information.

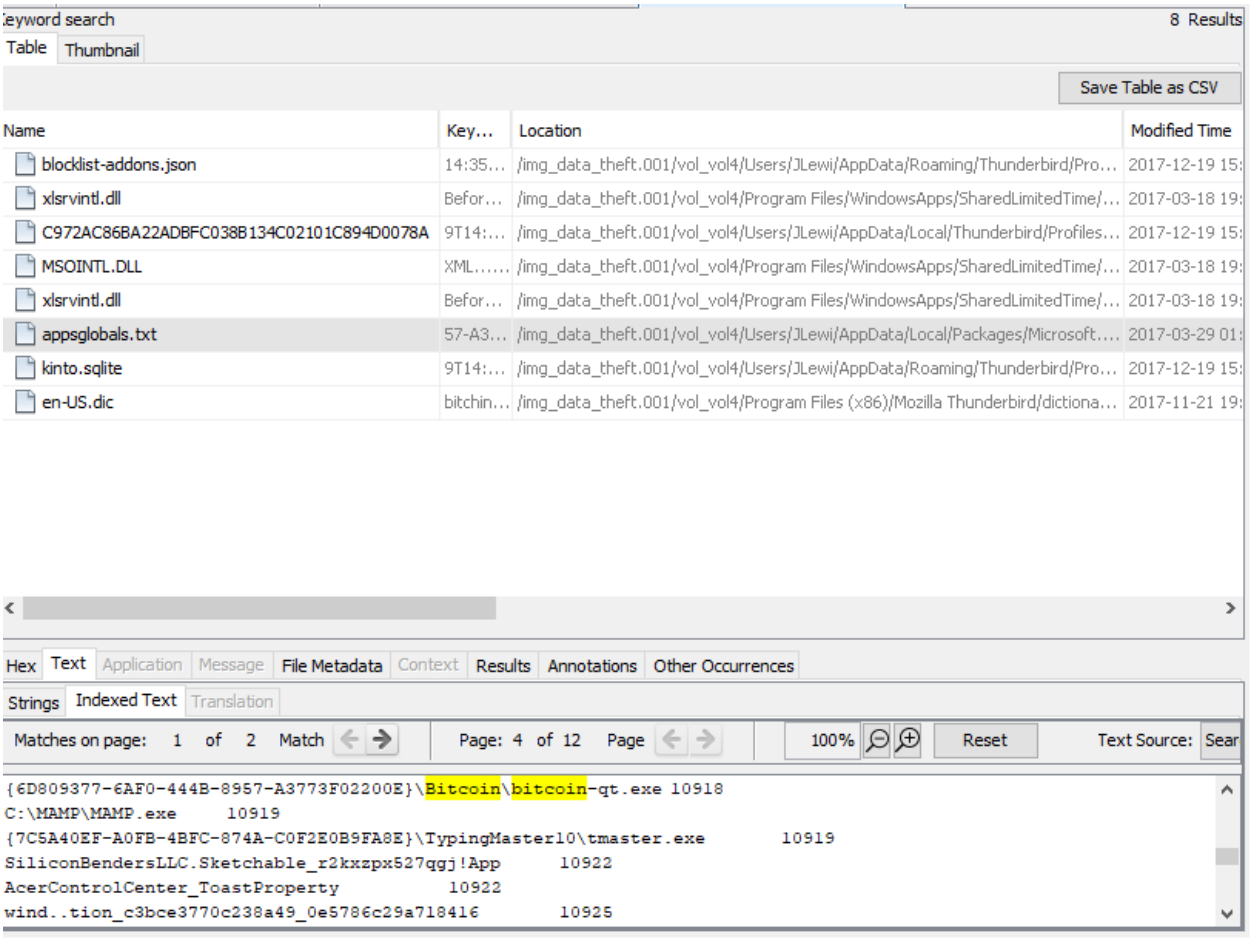
Bitcoin.Qt is shown the bitcoin
"AppData" and "Application data" are hidden by default.

University of Victoria



These are logs and files that were installed on this computer that suppose to support this idea, bitcoins account, which is used as a payment method.

University of Victoria



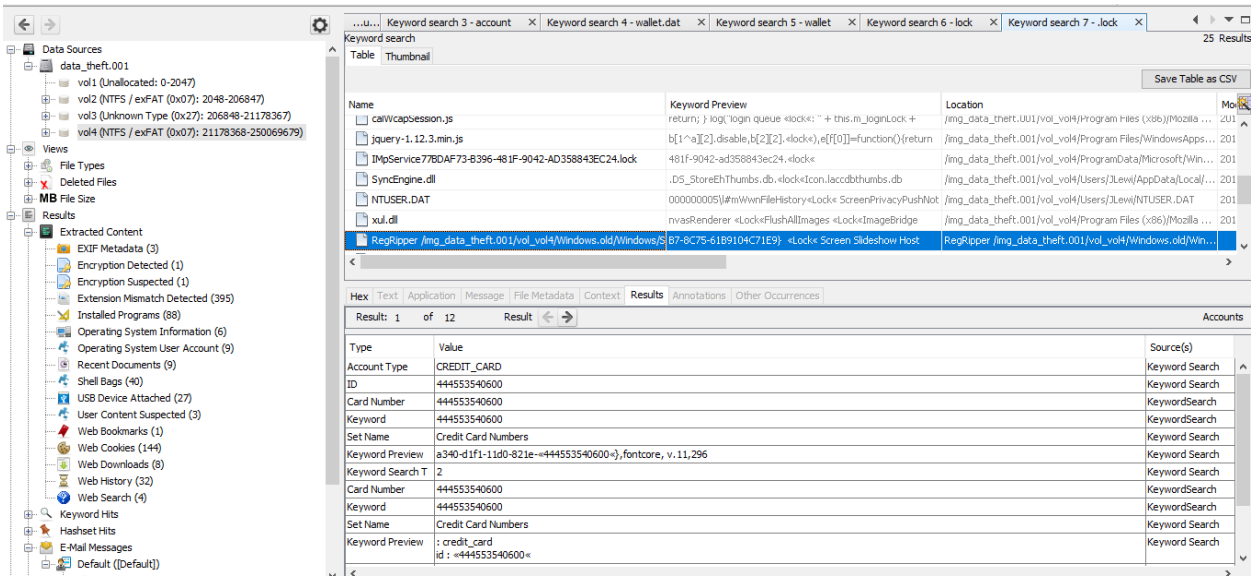
Bitcoin-qt.exe file information

The process known as Bitcoin Core (GUI node for Bitcoin) or Bitcoin Gold (GUI node for Bitcoin) belongs to software Bitcoin Core or Bitcoin Gold by Bitcoin.

Description: Bitcoin-qt.exe is not essential for the Windows OS and causes relatively few problems. Bitcoin-qt.exe is located in a subfolder of "C:\Program Files"—common is *C:\Program Files\Bitcoin*\. The file size on Windows 10/8/7/XP is 13,179,660 bytes.

The file is not a Windows core file. The application uses ports to connect to or from a LAN or the Internet. Bitcoin-qt.exe is able to connect to the Internet, record keyboard and mouse inputs and monitor applications. Therefore the technical security rating is *24% dangerous*, however you should also read the user reviews.

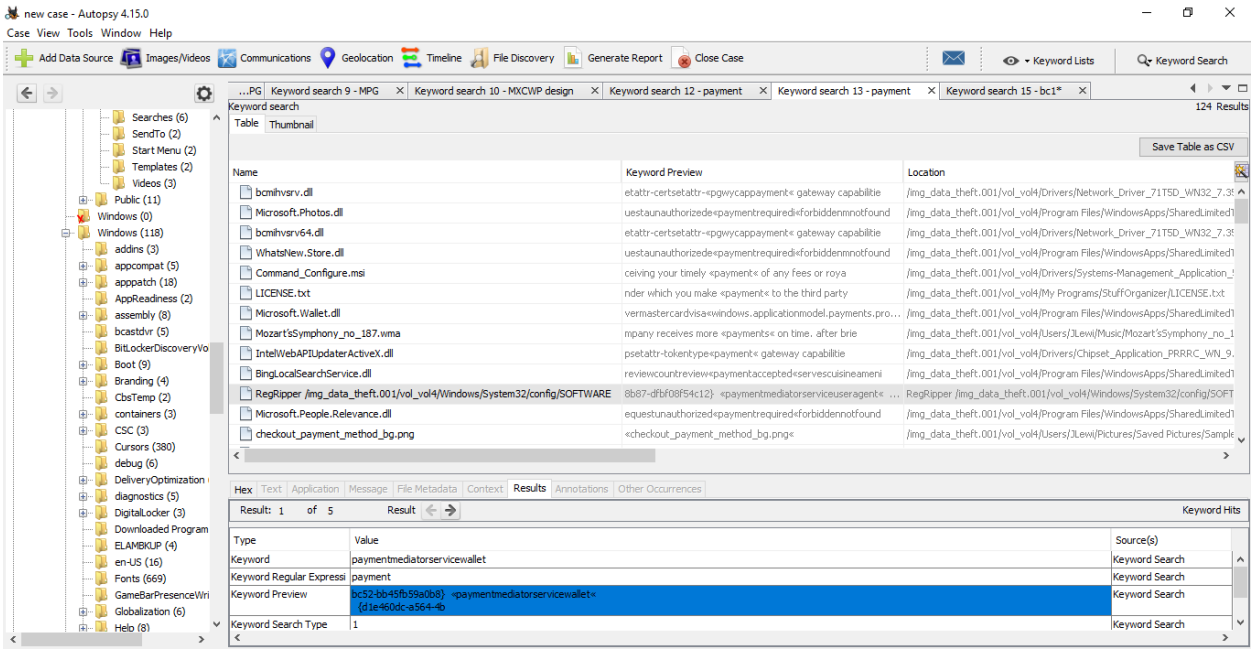
One file that is important in bitcoins is .lock



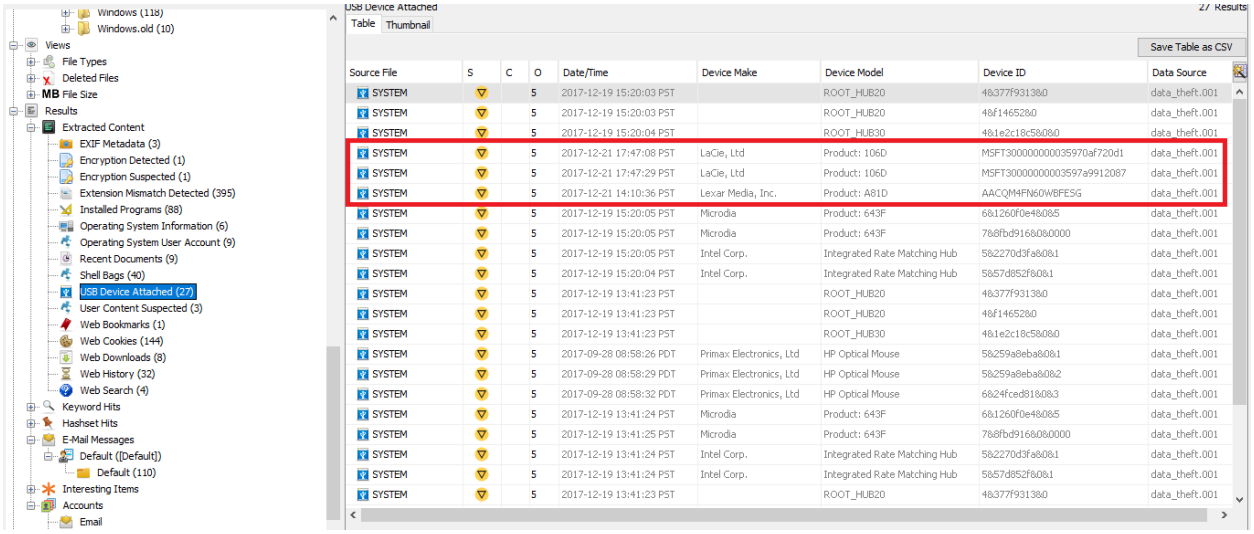
Lock file and credit card number all together represent bitcoins and blockchains data in Disk. It shows that Jlewis use bitcoins as a payment method for his illegal work.

And also here is a piece of information about payment information.

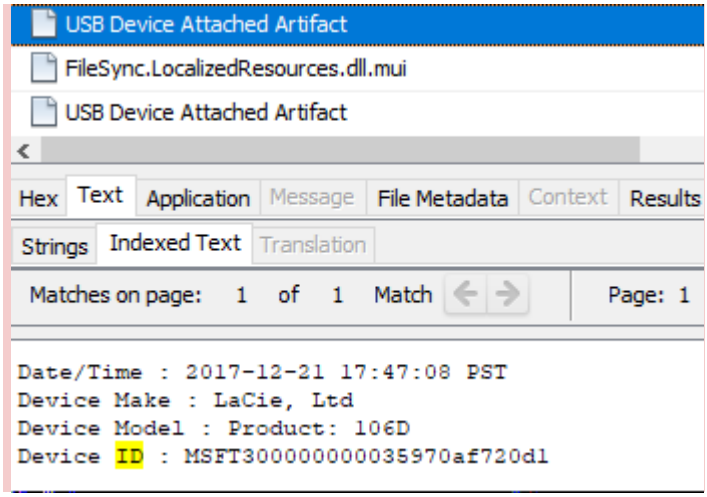
University of Victoria



2- investigation of USB logs file illustrates the information about which device connected to the computer. It seems that on December 19 three hardware devices connected to the disk. But on Dec 21 two new devices connected to the computer and transferred data through a system.

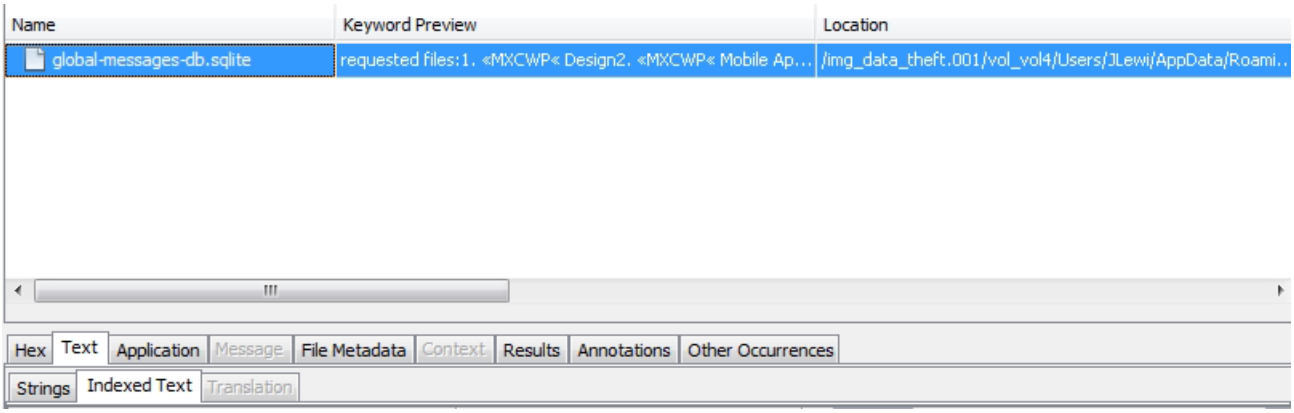


One of the Device ID, Model and make it shown as a following image: .

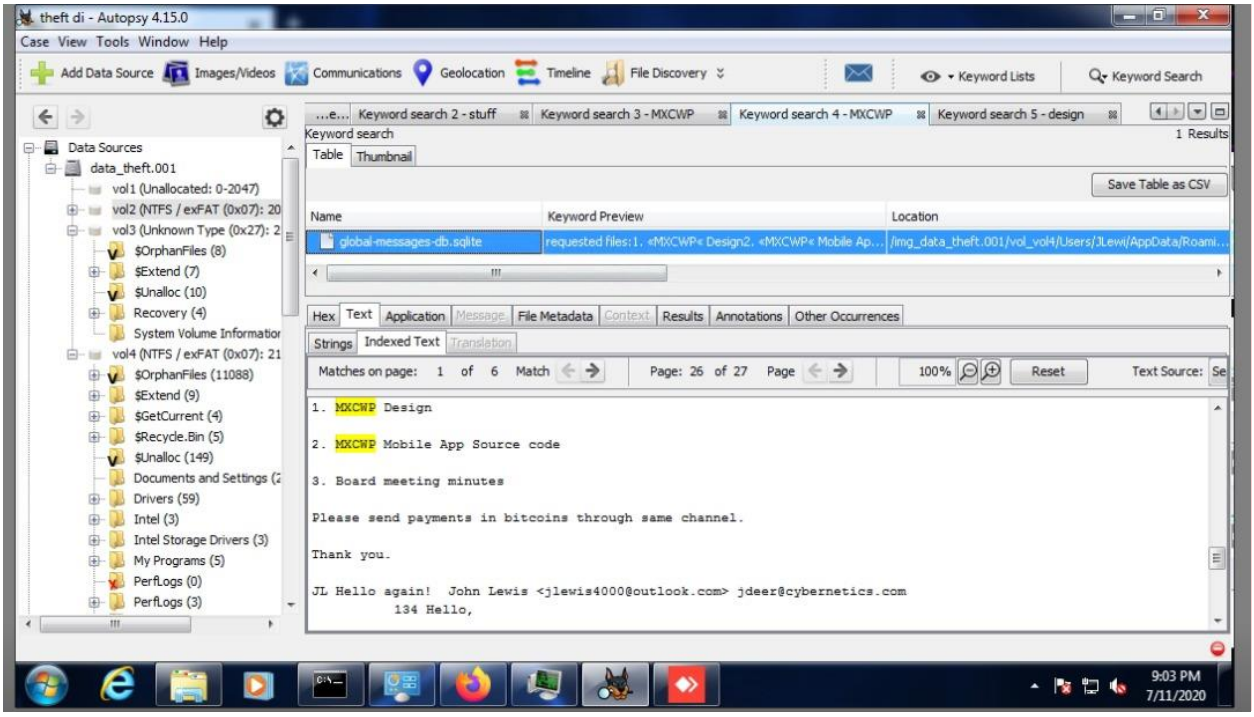


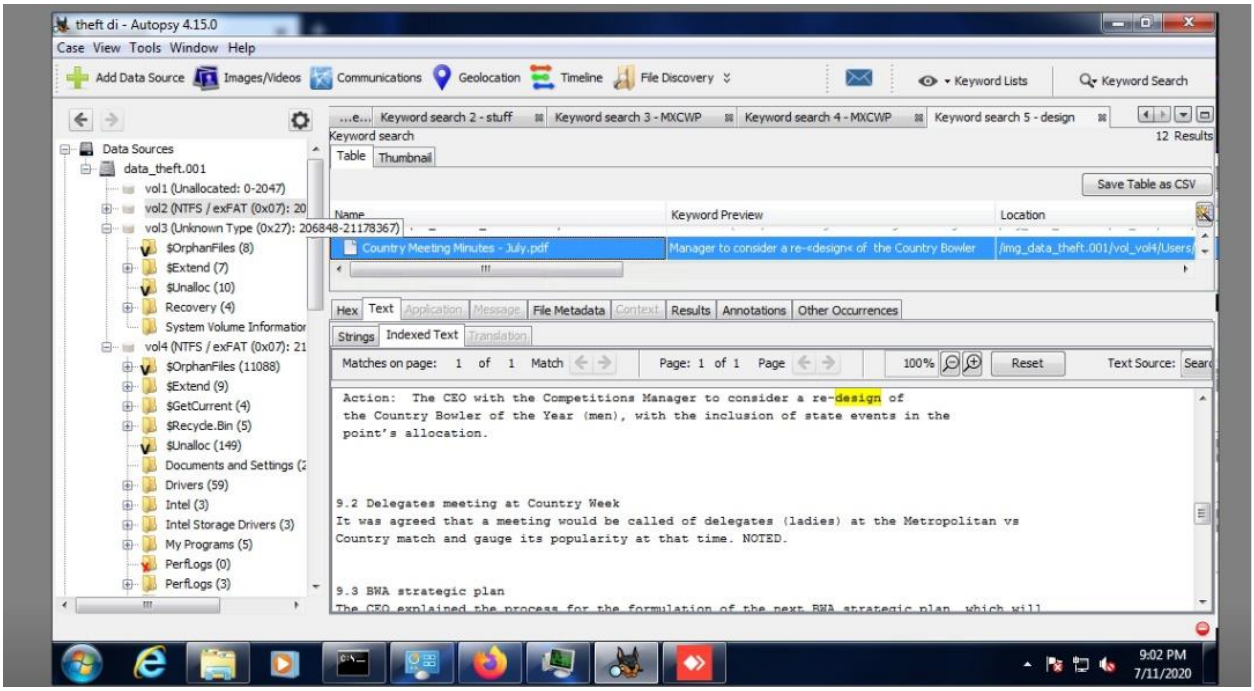
At the end, checking and analyzing information of Forensics Disk illustrates that JLweis had some activity out of working hours related to work.All screen shots of Question 2 prove this claim.

At the end, one Emails represents some clues about design. It is not related to MXCWP Design exactly. But one thing is weird that all emails send under the first email of this question. The first email mentioned three important information. This file investigates in all there allocated volume of Disk Image.



University of Victoria

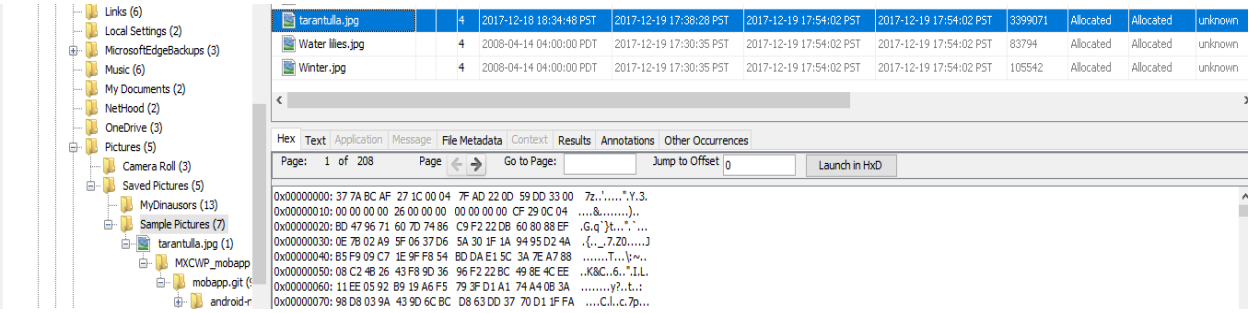




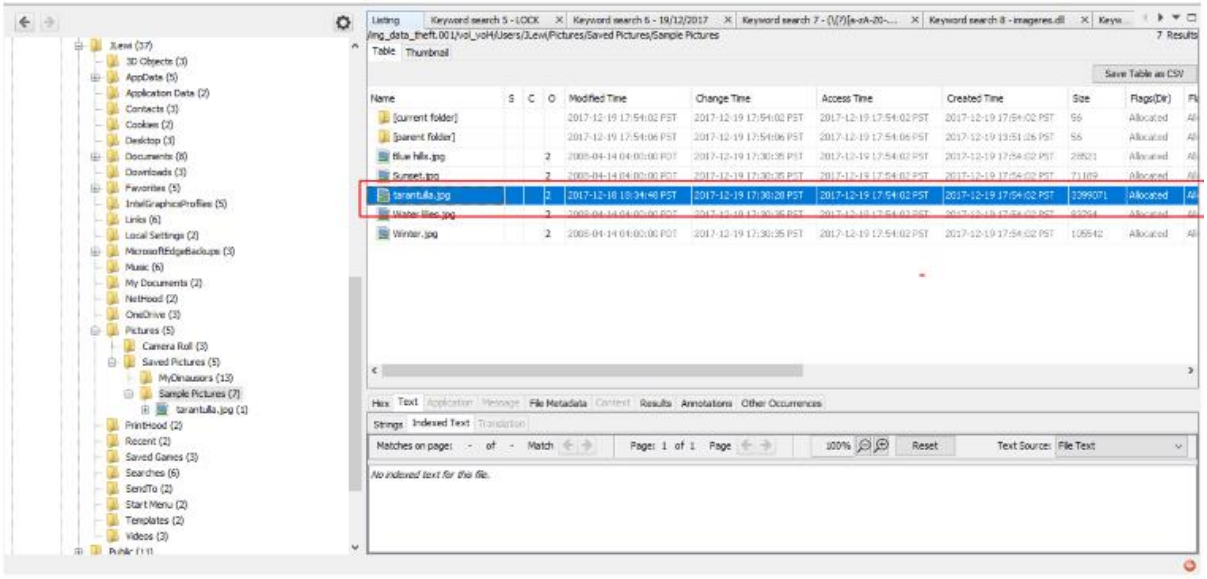
3. For each file, what processes were taken by the suspect to mask them from others? All masking processes used for relevant information must be identified, even redundant ones.

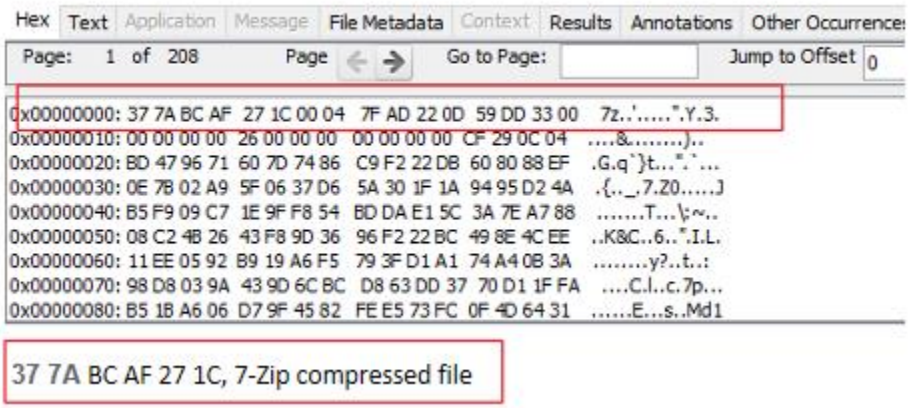
- For hiding the file MXCWP mobile-apps files,
    1. first of all Mr. JLewis compresed all of these files in the folder MXCWP
    2. This folder has been encrypted by using an encryption program which he installed on his laptop.
    3. put this encrypted file inside another folder, tarantula, and instead of using extension .7z as it is a zip file he hide this file by changing its extension to the jpg.
    4. Since this folder is some kind of document which is usually categorized under a document folder, he concealed this folder under his picture folder, and saved it with his other pictures with extension jpg.
    5. Then he tried to hide the passcode for this file instead of putting it in plaintext, he used steganography tools to hide the passcode inside the pictures.
    6. Extension of this image has been changed from bmp to exe
    7. we use quickstego to find the hidden text
    8. it looks after transferring the file he deleted this folder.

This procedure explain in a following image:



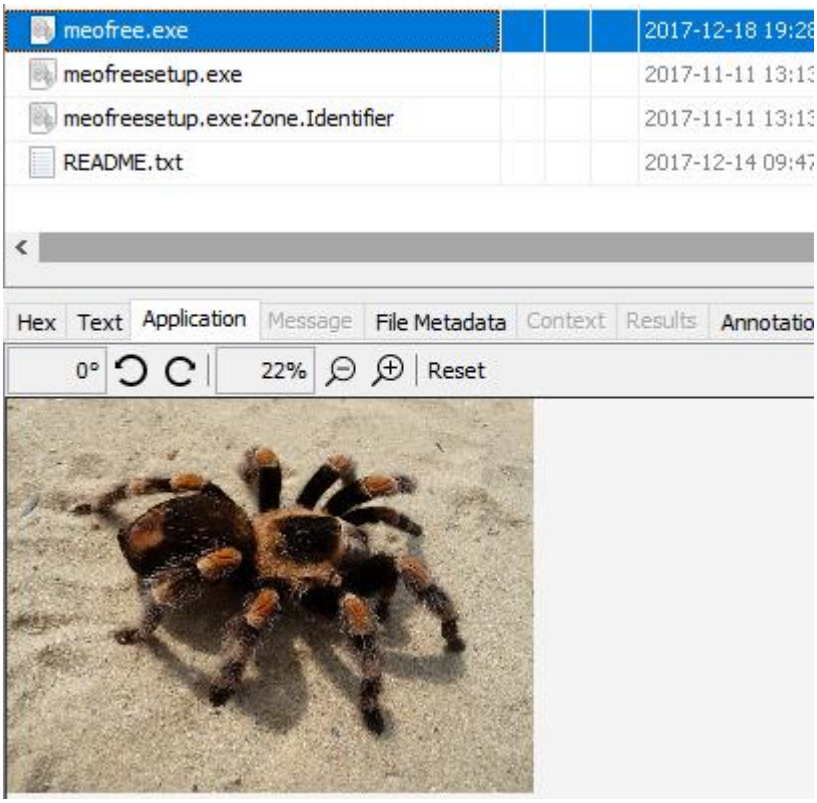
University of Victoria

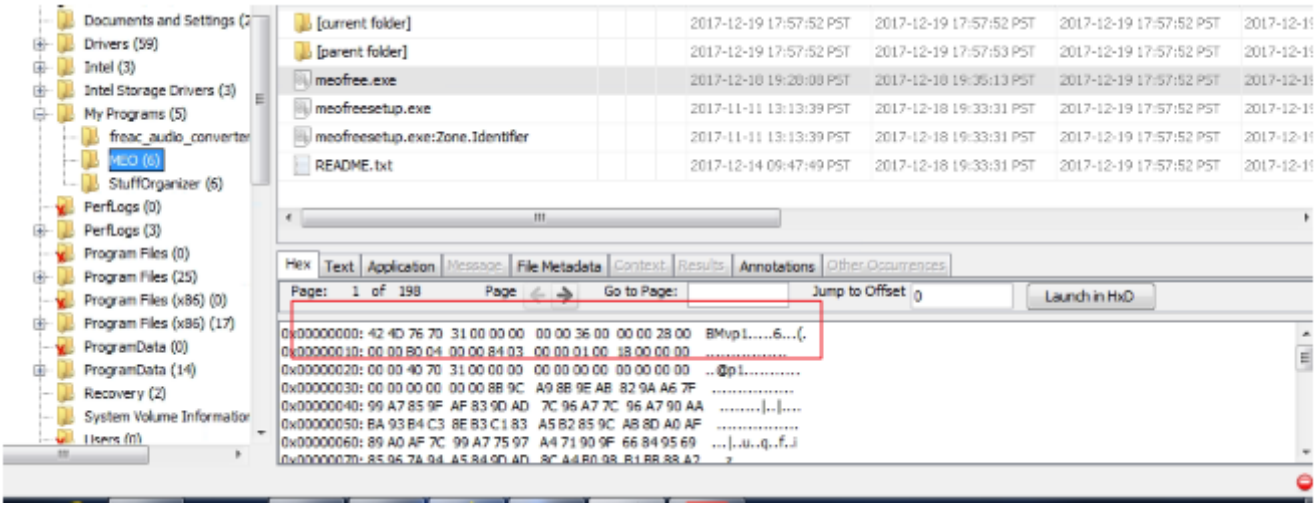


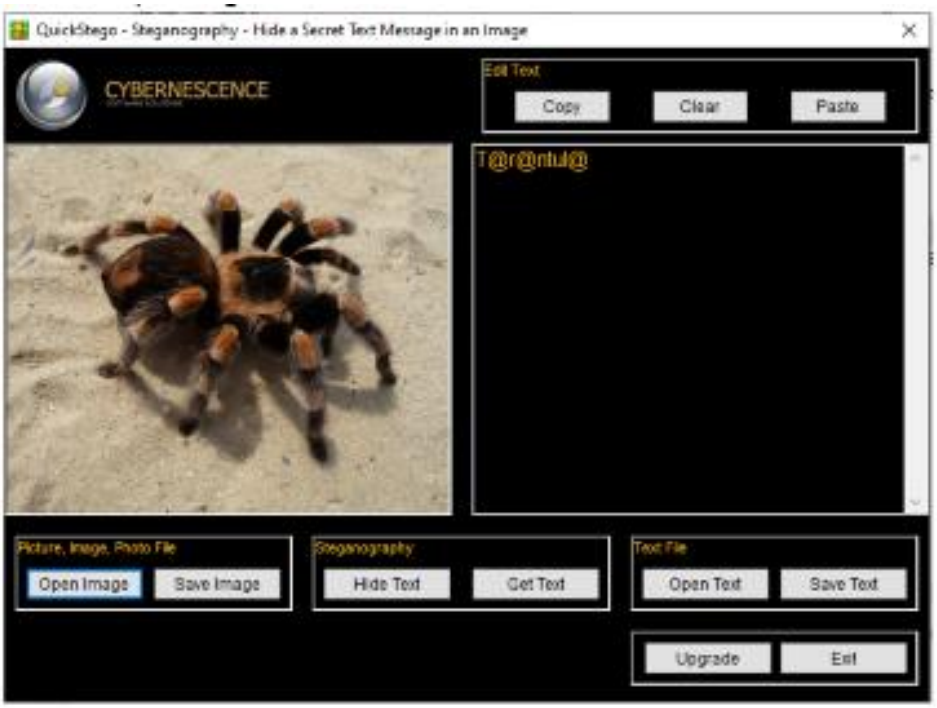


37 7A BC AF 27 1C, 7-Zip compressed file

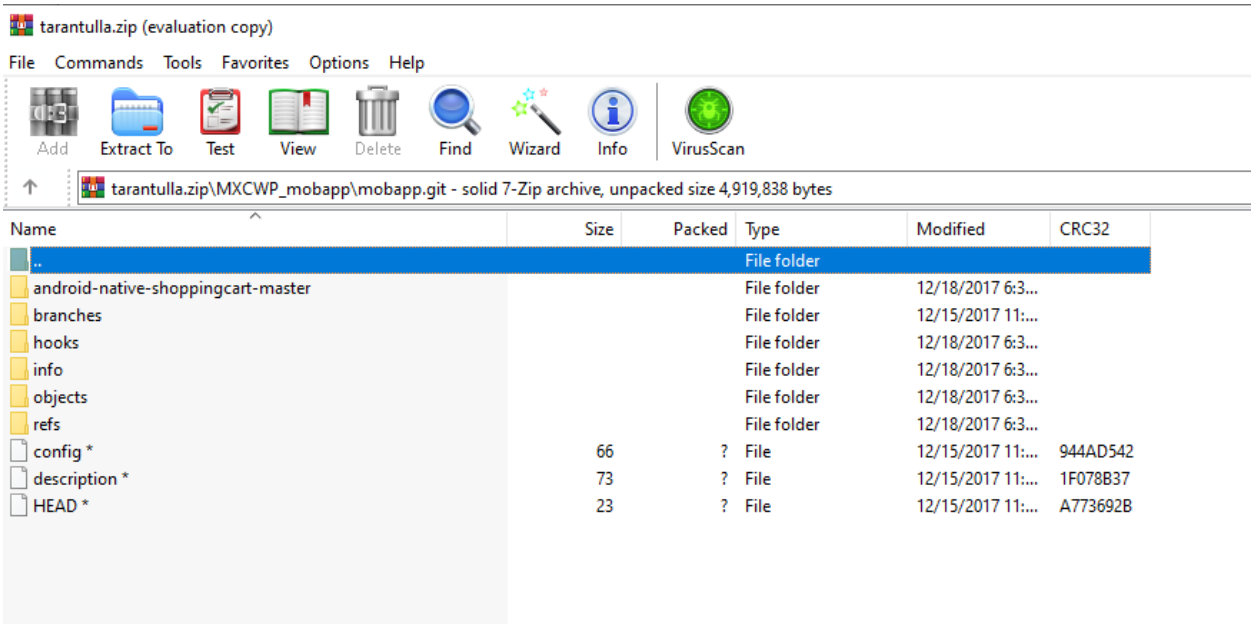
University of Victoria





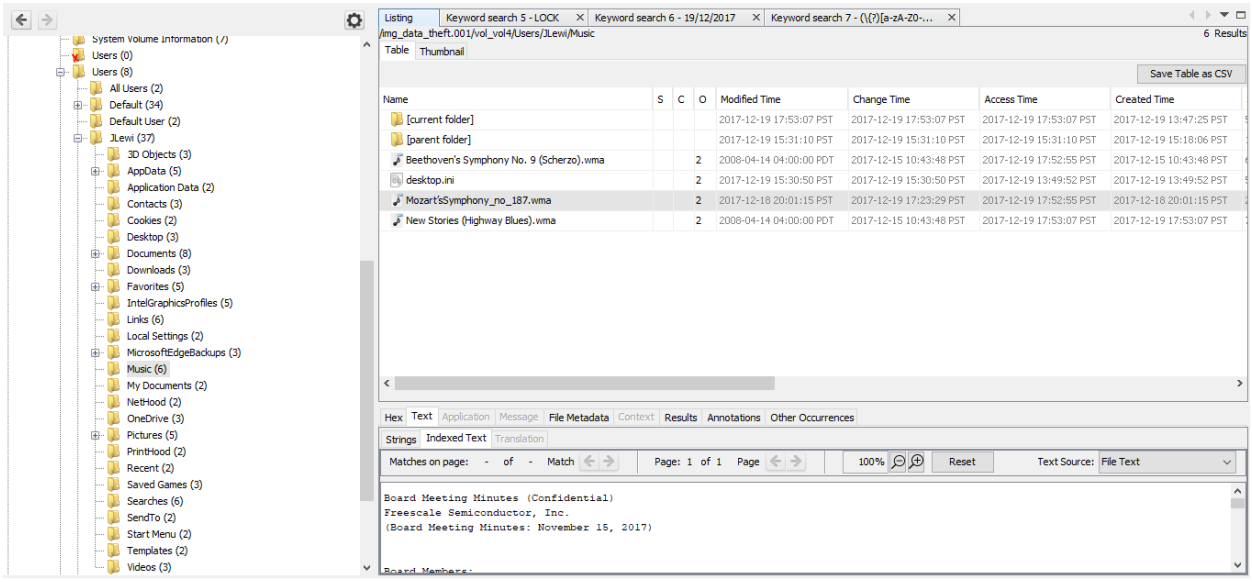


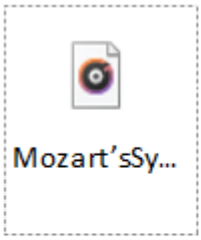
Then zip folder is open



- For boarding meeting minutes which was a word file.
    1. He changed the name of the file to Mozart'sSymp_no_187.
    2. he changed the extension from docx to wma which helps to looks like a music file
    3. Concealed this file between his other music files under music folder

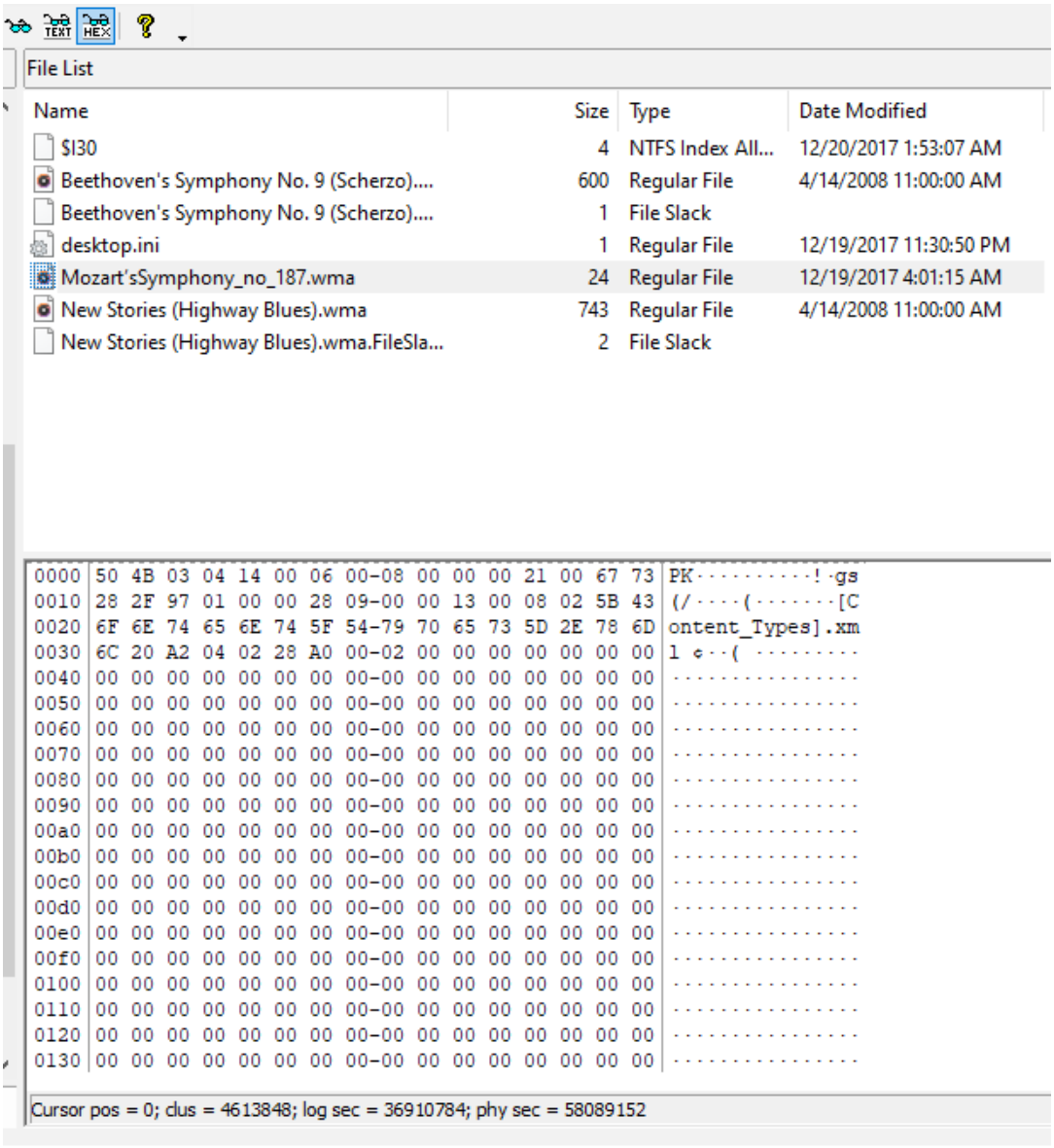
University of Victoria





Board Meeting...

University of Victoria



`50 4B 03 04 14 00 06 00` `PK.....`

DOCX, PPTX, XLSX Microsoft Office Open XML Format (OOXML) Document

NOTE: There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively.

University of Victoria

- For MXCWP design,

1. The file of cooking have been encrypted by using an encryption program which was installed in his laptop.

2. encrypted file compressed in the folder stuff_organizer by 7zip compress file.

3. Extension of this compressed file changed from .7z to exe

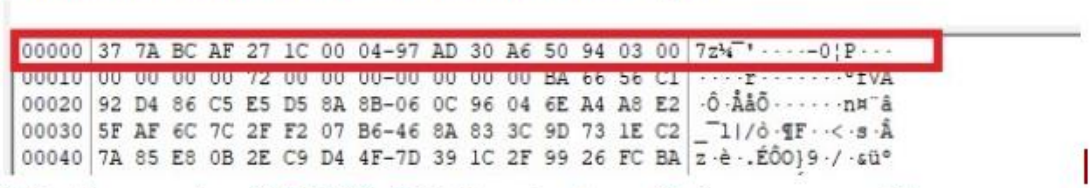
4.concealed this folder with extension .exe inside the my program folder between his other exe files

5.we assume to hide the passcode for this file instead of put it in plaintext, he hide it between slack of files.

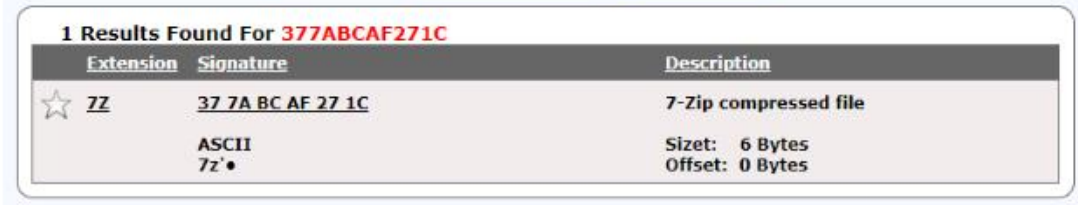
6.some part the file has been deleted and sit in orphan folder on Vol2

7.file is corrupted.

As we explained, stuff-organizer.exe is a zip file.
Some evidence prove this information:
1- Hex information of this file contains that this file is zip file



At first line, numbers 37 7A BC AF is Hex signature of 7 zip compressed files.
Note: we check this signature in https://www.filesignatures.net/



University of Victoria

For the another file stuff-organizer.exe

We can see that the 237,568 as a Physical Size mines 234,722 as a File Size equal to 2,846.

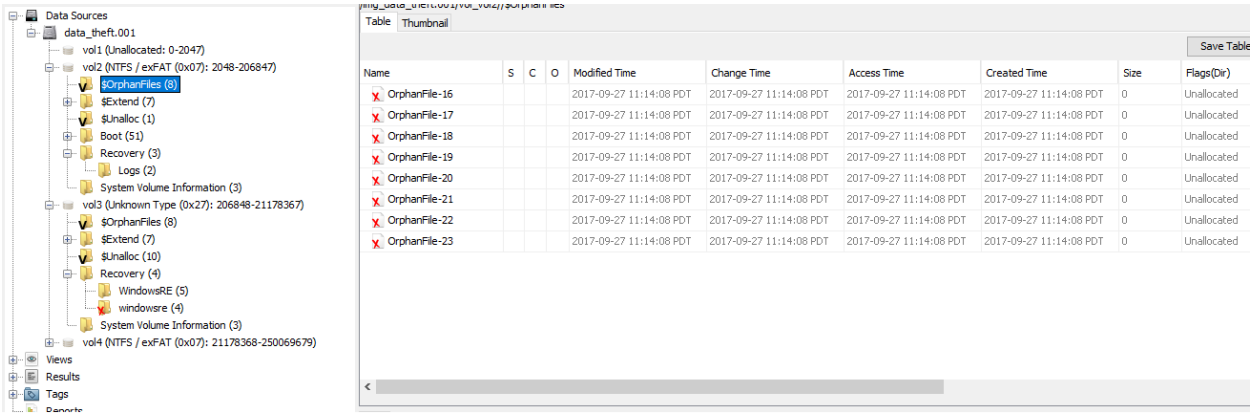
237,568 - 234,722 = 2,846

Pay attention this file start Cluster is 16,611,977 .

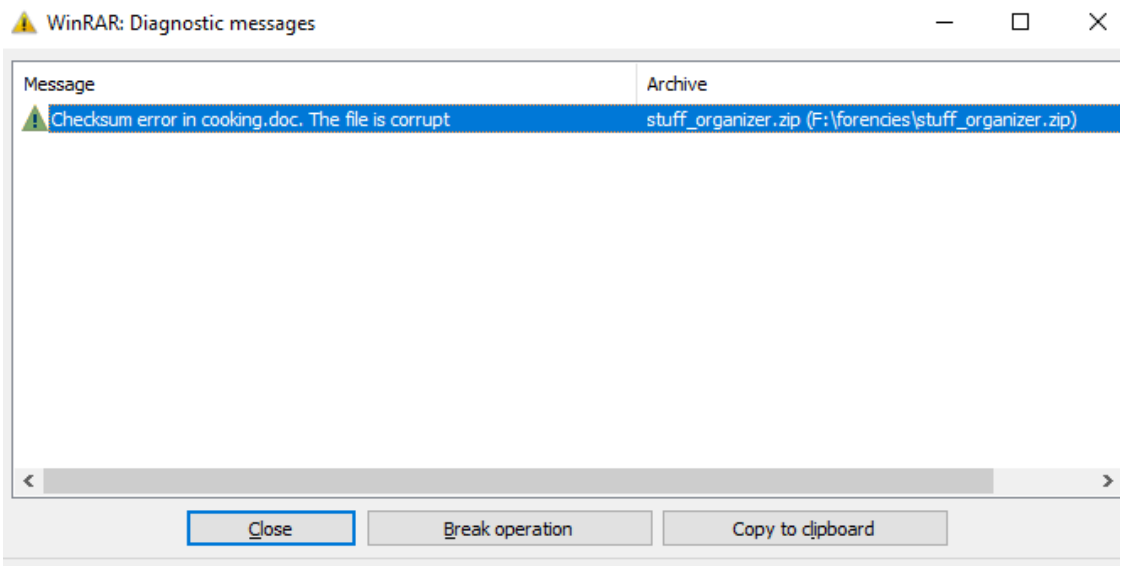
Name	stuff_organizer.exe
File Class	Regular File
File Size	234,722
Physical Size	237,568
Start Cluster	16,611,977
Date Accessed	12/20/2017 1:57:53 AM
Date Created	12/20/2017 1:57:53 AM
Date Modified	12/19/2017 2:14:54 AM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	154,074,184
DOS Attributes	
8.3 Short Filename	STUFF_~1.EXE
Hidden	False
System	False
Read only	False
Archive	True
NTFS Information	
MFT Record Number	222,358 (227694592)
Date Changed (MFT)	12/19/2017 2:18:59 AM
Resident	False
Offline	False

LICENSE.txt	34	Regular File	12/14/2017 5
LICENSE.txt.FileSlack	3	File Slack	
setup_stuff_organizer.exe	4,545	Regular File	12/14/2017 5
stuff_organizer.exe	230	Regular File	12/19/2017 2
stuff_organizer.exe.FileSlack	3	File Slack	

```
393b0  F4 67 D3 C0 D2 E9 FF B6-18 E8 C1 30 AC EF A2 54  ôgÓÀÒéÿ¶·èÁ0¬ï¢T
393c0  A7 2B 3D 73 D7 6F A0 F6-8D 20 AD E9 1E DA 86 14  §+=s×o ö· é·Ú··
393d0  E3 77 7E 26 2D D3 C0 01-DC 7E FB 8F E9 78 24 EB  ãw~&-ÓÀ·Ü~û·éx$ë
393e0  6C 9E 98 E6 EF 72 A2 7E-B6 2C 3B F6 7C 71 0F 3C  l··æïr¢~¶,;ö|q·<
393f0  29 E7 40 A1 0E 23 CE 46-BF 63 2A 39 70 AB 09 9B  )ç@¡·#ÎF¿c*9p«··
39400  8A 94 D0 B5 33 C2 82 DD-1F CC AB 7F 33 99 65 71  ··Ðµ3Â·Ý·Ì«·3·eq
39410  03 F7 9D 1A D3 70 50 BD-AD F9 47 C1 5A 08 F2 AA  ·÷··ÓpP½ùGÁZ·ò*
39420  CD 48 83 87 08 72 BD E6-CE 83 AE FC BB 55 C3 1E  ÍH···r½æÎ·®ü»UÃ·
39430  94 A6 7F 63 C8 4F 46 55-BD BE 5C 9B 00 82 44 14  ··¦·cÈOFU½¾\···D·
39440  32 F7 C7 D9 4E 0F AC A3-03 C1 0A B6 03 AB A9 AF  2÷ÇÙN·¬£·Á·¶·«©¯
39450  EE C5 3B 90 DF 75 A4 04-20 1C 88 9A A0 73 65 DC  îÅ;·ßu¤· ···· seÜ
39460  D5 71 C2 16 17 76 BF FE-A7 7B BE E5 39 F7 BD 4A  Õq Â···v¿þ§{¾å9÷½J
39470  01 04 06 00 01 09 C3 50-94 00 07 0B 01 00 02 24  ·····ÃP·····ç
39480  06 F1 07 01 0A 53 07 1E-8B 93 0C EF 9F 8A 18 21  ·ñ···S·····ï···!
39490  21 01 0C 01 00 0C C3 43-94 C3 33 94 00 08 0A 01  !·····ÃC·Ã3·····
394a0  48 46 ED 69 00 00 05 01-19 03 00 00 00 11 19 00  HFíi·····
394b0  63 00 6F 00 6F 00 6B 00-69 00 6E 00 67 00 2E 00  c·o·o·k·i·n·g·.·
394c0  64 00 6F 00 63 00 00 00-19 02 00 00 14 0A 01 00  d·o·c·····
```



University of Victoria

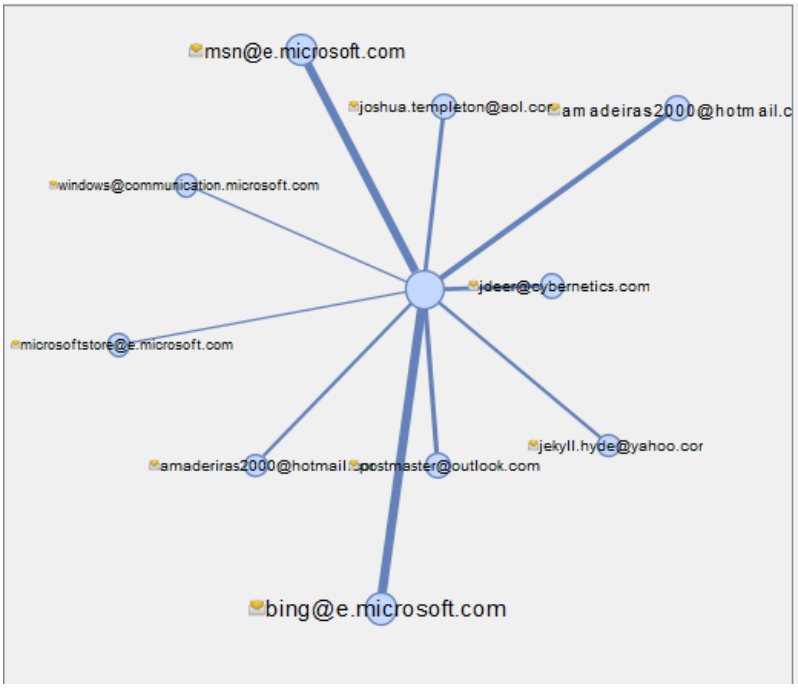


University of Victoria

4.Investigate and discuss whether or not the email evidence helps in making the case against the suspect. All sources of relevant email evidence must be considered.

Since emails, text and instant messages are some kind of information which are possible to gather from the suspected device and use it effectively as evidence.

The evidence of email gathered on Autopsy Jlewis sent 82 emails. As follow:



by reviewing user Jlewis' s email folder we found communication between Jlewis and jdeer from cybernetics Inc. one of the competitors of Freescale semiconductor which he sent it from his outlook on Dec 21,2017 at 14:18:05. As following figure.

University of Victoria

jdeer@cybernetics.com

This account was referenced by a device in the case.

Communications

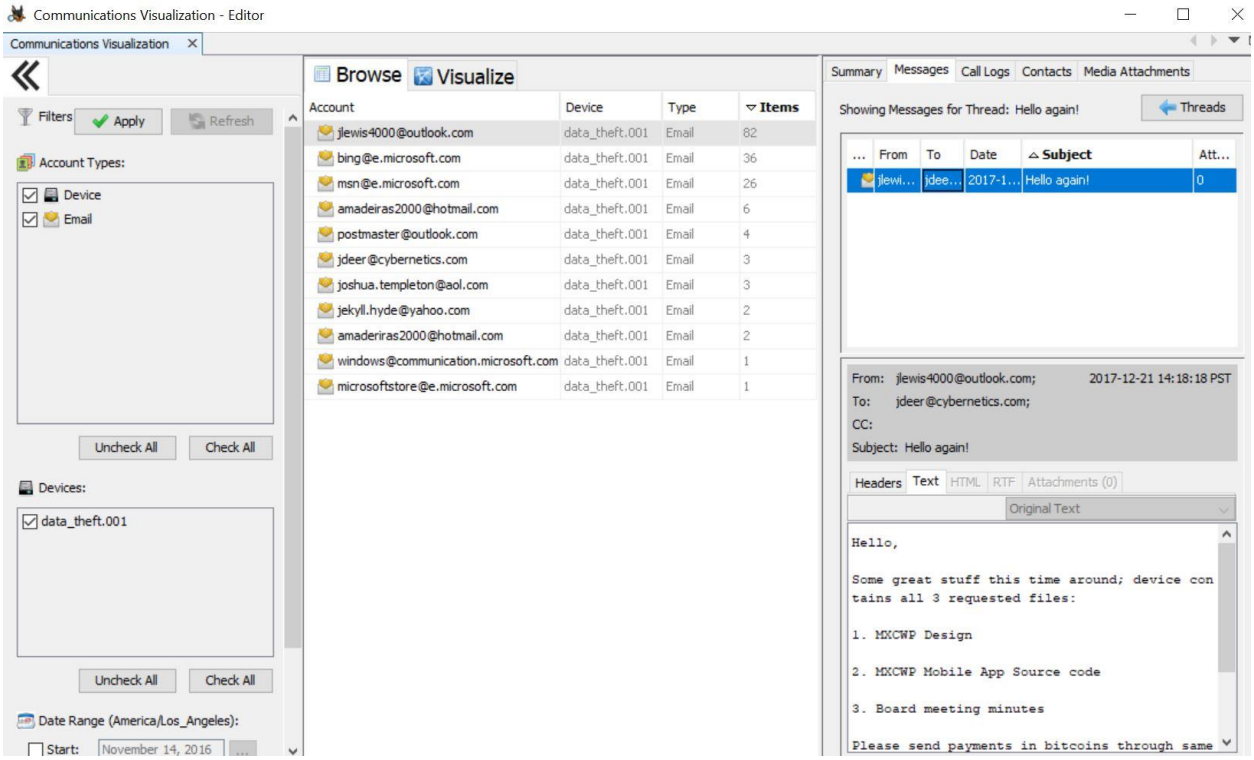
Messages:	3
Call Logs:	0
Media Attachments:	0
Total Attachments:	0

Account Contacts

Book Entries:	0
Communication References:	0

Type	From	To	Date	Subject	Attac...
E-Mail	jlewis4000@outlook.com	jdeer@cybernetics.com	2017-12-21 14:18:...	Hello a...	0
E-Mail	jlewis4000@outlook.com	jdeer@cybernetics.com	2017-12-21 14:18:...	Hello a...	0
E-Mail	jlewis4000@outlook.com	jdeer@cybernetics.com	2017-12-21 14:18:...	Hello a...	0

University of Victoria



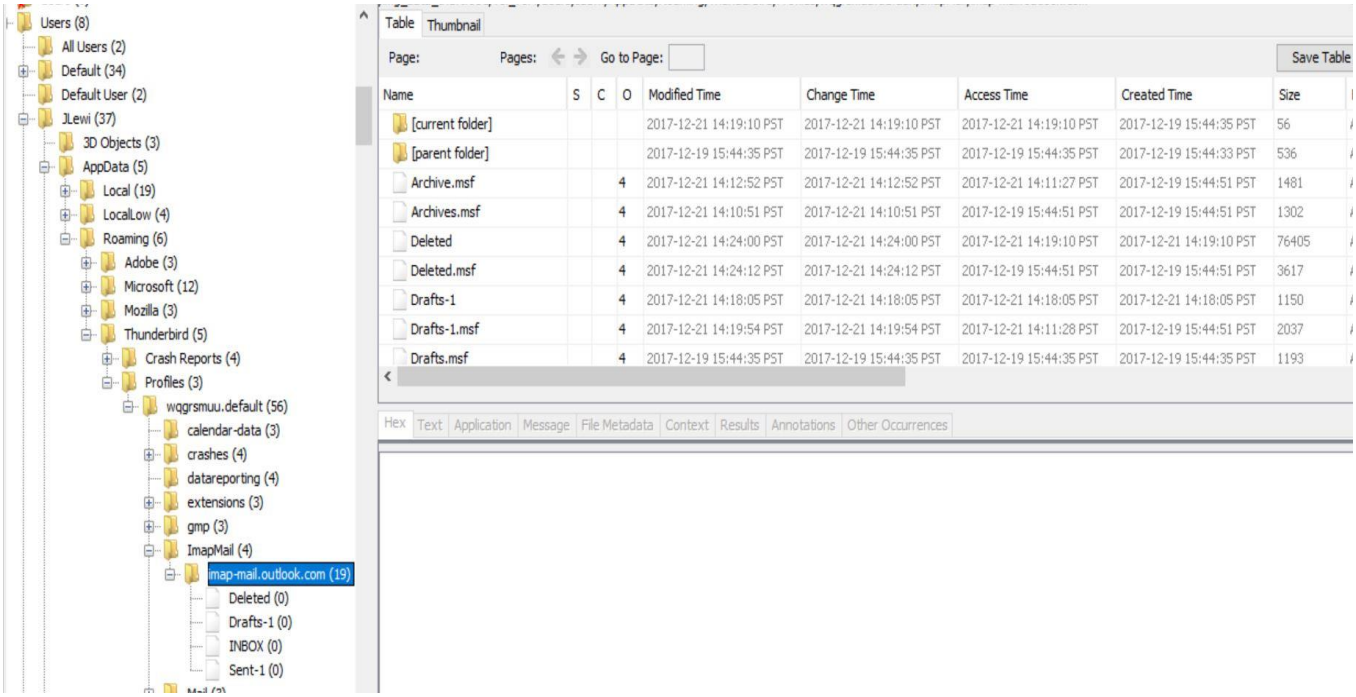
The IP address that email sent to Jdeer is :

Source File	S	C	O	Keyword	Keyword Preview	Access Time	Change Time
Sent-1				10.172.26.29	d79:1132:87e4:def7] «10.172.26.29» by cy4pr16mb1749.na	2017-12-21 14:12:11 PST	2017-12-21 14:23:34 PST

So, 10.172.26.29 is the IP address that is used by the company. So, J Lewis sent this email from a computer which connects to the internet on his company.

Also by searching from a deleted folder under ImapMail, there was an email which shows Mr JLewis sent an email on Dec 21 To Deer who is from cybernetics Inc. one of the competitors of Freescale semiconductor.As there was a mistake on the email address, Mr Jlewis received an failed delivery message from the server which also contained the original sent email on Dec 21,2017 at 14:19:10. And this failed delivery message modified, deleted, same day at 14:24:00. He mentioned in the body of email about three documents related to one of the important company's projects such as

MXC design, MXCWP mobile app source code and board meeting minutes and method of payment. It can be suspected for stealing information and this email is one good item to do more investigation to see the possibility of existence of those secret company's files in his laptop and possibility of any suspicious money transfer in his account.



University of Victoria

```
Final-Recipient: rfc822;jdeer@cybernetics.com
Action: failed
Status: 5.1.1
Diagnostic-Code: smtp;550 5.1.1 <jdeer@cybernetics.com>: Recipient address rejected: User unknown
Remote-MTA: dns;mail.cybernetics.com
X-Display-Name: jdeer@cybernetics.com
```

Hello,

Some great stuff this time around; device contains all 3 requested files:

1. MXCWP Design

2. MXCWP Mobile App Source code

3. Board meeting minutes

Please send payments in bitcoins through same channel.

Thank you.

JL

mail.cybernetics.com rejected your message to the following email addresses:

jdeer@cybernetics.com (jdeer@cybernetics.com)

The address you sent your message to wasn't found at the destination domain. It might be misspelled or it might not exist. Try to fix the problem by doing one or more of the following:

Send the message again, but before you do, delete and retype the address. If your email program automatically suggests an address to use, don't select it.

Clear the recipient AutoComplete cache in your email program by following the steps in this article: Status code 5.1.1. Then resend the message, but before you do, be sure to delete and retype the address.

Contact the recipient by some other means (by phone, for example) to confirm you're using the right address. Ask them if they've set up an email forwarding rule that could be forwarding your message to an incorrect address.

Also the following email did not exist in the digital image, looks it was deleted .But it was the primary email which gave us a hint for collecting and analyzing evidence supporting this case.It encouraged me to look for evidence that Mr.Lewis sold information of his company to another one. How? How does he earn money? What data did he give them without permission?

-------- Sent Message --------
To: jdeer@cybernetics.com
From: John Lewis <jlewis@freescale.com>
Subject: Hey!
Message-ID: <f9065505-bbc5-d8b3-478a-5e6bfb6809d6@freescale.com>
Date: Wed, 20 Dec 2017 14:51:34 -0800
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101
 Thunderbird/52.5.0
MIME-Version: 1.0
Content-Type: multipart/alternative;
 boundary="------------2CB0785977D5F282F06ACAA3"
Content-Language: en-US

This is a multi-part message in MIME format.
--------------2CB0785977D5F282F06ACAA3
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit

Good Afternoon,

Some great development in the last period. Please visit our common
friend for more. I'll leave the laptop with him; please return it to the
same location after fetching the data. More details on specific content
to come later in a separate email. Content and pass codes can be
recovered using the usual procedure. Stay tuned!

Thank you,

JL

So in this case email evidence gives us more keyword and clue at the first point But we need more supporting documents, real evidence, to be covered against lawsuits. As provided in the previous question.

University of Victoria

5. Discuss and justify whether or not the overall evidence is enough to conclude data theft by the suspect.

According to all evidence gather during the investigation , it's possible to say and conclude company faced the data theft by secretory of CEO , Mr Lewis..So in identification phase all preliminary information like bringing laptop at work against company's policy and transfer data form his workstation to his USB are obtained and make it suspicious to be cybercrime case but is not enough To confirm that any theft by itself happened. But after starting digging more and complete investigation on the files and folders and his communication via email between him and jdeer from competitor company , Cybernetics which mentioned exchanging company's new product files exactly with the name MXCWP with some kind of money bitcoin . Give us hints that it's more likely Freescale Inc faced data theft on their confidential documents. Just considering email gives probable results of theft but its not enough for conclusion to be defendable on lawsuit. By having these idea we tried to figure out whether or not he has those file anywhere in his laptop so at the next step by analysing, checking his data and directories, deleted files and searching specific related case sensitive words, , finally searching shows that he has those confidential proprietary files in his laptop and shows that he intently compressed, encrypted and concealed , renaming and changing file format and extensions and mislocation by hiding them between his other unrelated files and using passcodes which encrypted by steganography tools to be hidden inside photo.

All of this evidence concluded that Mr Lewis abused his position in the company and committed fraud on confidential documents.