



University
of Victoria

ECE 570 - Digital Forensics Methodologies PROJECT PART 2

Data Exfiltration

**Somayeh Roshandel V00942553
Behnaz Saropourian V00857804**

July 2020



Table content

1. Check the validity of the forensic image.....	4
2. Indicate Explain the specific files that contain such data and explain the importance of the different pieces of information for the investigation.....	7
3. what processes were taken by the suspect to mask them from others	39
4.Investigate and discuss whether or not the email evidence	49
5. Discuss and justify whether or not the overall evidence is enough to conclude data theft by the suspect.	55



Abstract

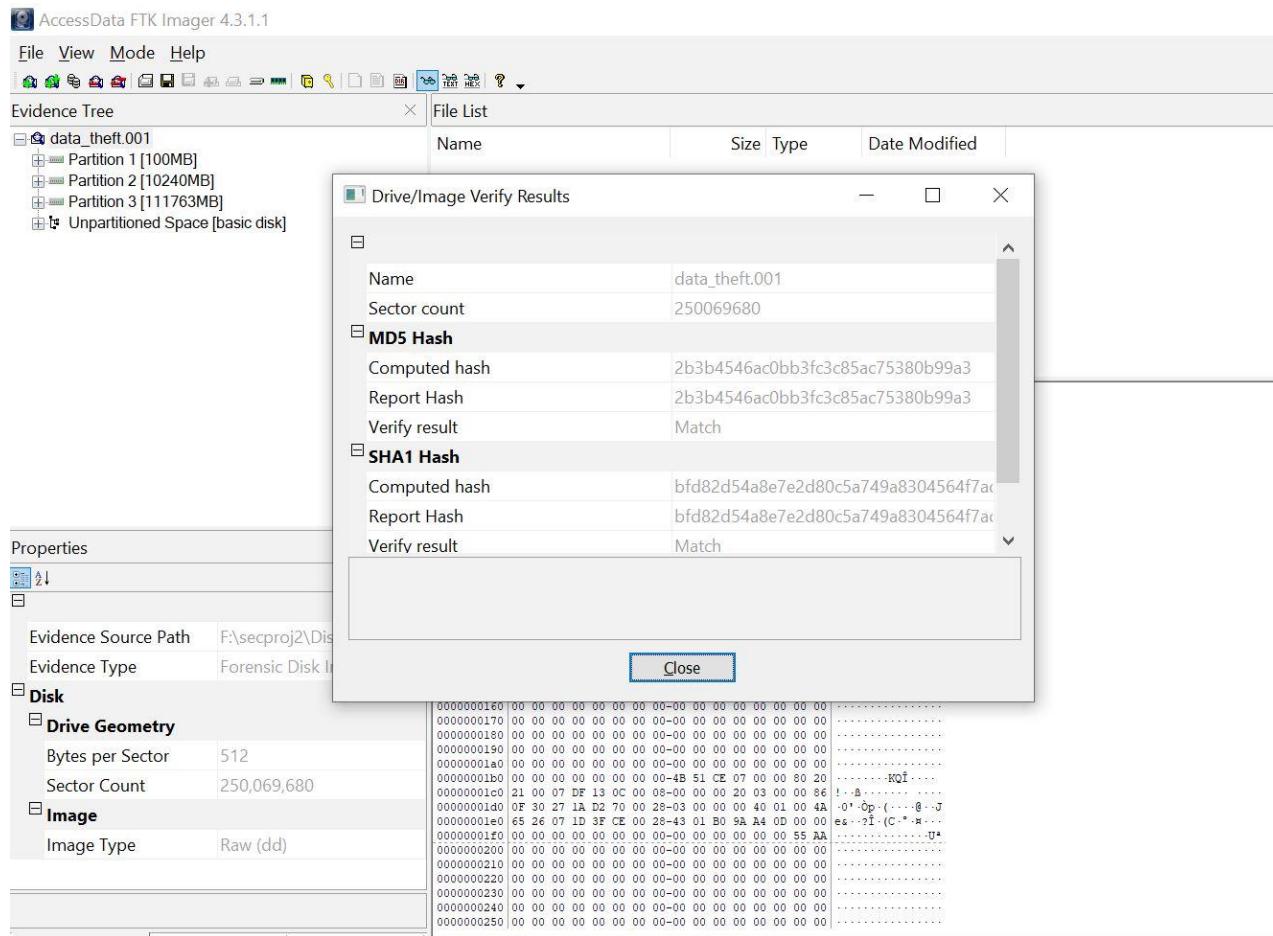
The purpose of this report is to provide evidence based on information gathered about Mr JLewis secretary of Dr Eli Drucker who is suspected for sharing some files which assume related to Freescale semiconductor Inc.'s important project, Mobile Extreme Convergence(MXC), with their competitor Cybernetics 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.



- 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:



Drive/Image Verify Results	
Name	data_theft.001
Sector count	250069680
MD5 Hash	
Computed hash	2b3b4546ac0bb3fc3c85ac75380b99a3
Report Hash	2b3b4546ac0bb3fc3c85ac75380b99a3
Verify result	Match
SHA1 Hash	
Computed hash	b7d82d54a8e7e2d80c5a749a8304564f7a...
Report Hash	b7d82d54a8e7e2d80c5a749a8304564f7a...
Verify result	Match

MD5 generated by Autopsy that run on Kali LInux is :





Kali-Linux-2020.2a-vbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Add a new image to an Autopsy Case - Mozilla Firefox [Disk - File Manager]

03:05 AM

Add a new image to an Autopsy Case - Mozilla Firefox

localhost:9999/autopsy?mod=0&view=15&img_path=%2Fmedia%2Fsf_ECE570-2020-project2-Disk%2FD

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Calculating MD5 (this could take a while)
Current MD5: 2B3B4546AC0BB3FC3C85AC75380B99A3
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Disk image (type dos) added with ID vol1
Volume image (2048 to 206847 - ntfs - C:) added with ID vol2
Volume image (206848 to 21178367 - ntfs - D:) added with ID vol3
Volume image (21178368 to 250069679 - ntfs - E:) added with ID vol4

OK ADD IMAGE

FILE SYSTEM IMAGES

data_theft.001 2B3B4546AC0BB3FC3C85AC75380B99A3

VALIDATE CLOSE REFRESH HELP

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



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 emails. 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.



Listing Keyword search 5 - LOCK X Keyword search 6 - 19/12/2017 X Keyword search 10 - MXCWP X 8 Results

Keyword search

Table Thumbnail Save Table as CSV

Name	Keyword Preview	Location	Modified Time
Sent-1	requested files:1. <MXCWP< Design2. <MXCWP< Mobile Ap... /img_data_theft.001/vol_vo...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:23:34 PST
Drafts-1	files: 1. <MXCWP< Design 2. <MXCWP< Mobile App ... /img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:18:05 PST
E-Mail Messages Artifact	<p>1. <MXCWP< Design </p> <p>2. <MXCWP< Mobile App ... /img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:18:05 PST
INBOX	requested files:1. <MXCWP< Design2. <MXCWP< Mobile Ap... /img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:23:46 PST
global-messages-db.sqlite	requested files:1. <MXCWP< Design2. <MXCWP< Mobile Ap... /img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:24:08 PST
E-Mail Messages Artifact	requested files:1. <MXCWP< Design2. <MXCWP< Mobile Ap... /img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:23:34 PST
E-Mail Messages Artifact	requested files:1. <MXCWP< Design2. <MXCWP< Mobile Ap... /img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:23:34 PST
Deleted	requested files:1. <MXCWP< Design2. <MXCWP< Mobile Ap... /img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 14:24:00 PST

< >

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: 1 of 4 Match ← → Page: 1 of 1 Page ← → 100% ⚡ Reset Text Source: Search Results

1. **MXCWP** Design

2. **MXCWP** Mobile App Source code

3. Board meeting minutes

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

And also,

Keyword search 28 Results

Name	Keyword Preview	Location	Modified Time
rtmpal.dll	Timeout waiting for objects! «Stuff» was leaked!done. No ...	/img_data_theft.001/vol_vo4/Program Files/Windows Apps...	2017-03-18 1...
rtmpltfm.dll	Timeout waiting for objects! «Stuff» was leaked!Awaiting all	/img_data_theft.001/vol_vo4/Program Files/Windows Apps...	2017-03-18 1...
global-messages-db.sqlite	brainstorm more. Good «stuff»! About the project: <jekyll	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 1...
E-Mail Messages Artifact	brainstorm more. Good «stuff»!Message ID : Not available	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 1...
bulletin_board.html	onclick="setup(testItems)">Add «Stuff»</button> Others... /img_data_theft.001/vol_vo4/Program Files/Windows Apps...		2017-12-19 1...
Deleted	Hello, Some great «stuff» this time around; device	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roami...	2017-12-21 1...
calStorageUpgrade.jsm	try { * // Do «stuff» here * setDbV	/img_data_theft.001/vol_vo4/Program Files (x86)/Mozilla ...	2017-11-21 1...

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: 1 of 1 Match Page: 1 of 1 Page 100% Text Source: Search Results

```
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
```

This email was sent on December 21 and deleted.

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

E-Mail Messages Artifact : Hello, Some great «stuf... /img_data_theft... 2017-12-21 14:23:34 PST 2017-12-21 14:23:34 PST 2017-12-21 14:12:11 PST 2017-12-21 14:12:11 PST 37976

INBOX brainstrom more. Good ... /img_data_theft... 2017-12-21 14:23:46 PST 2017-12-21 14:23:46 PST 2017-12-19 15:44:54 PST 2017-12-19 15:44:54 PST 4889316

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: 1 of 1 Match Page: 1 of 1 Page 100% Text Source: Search Results

```
E-Mail From : jl Lewis4000@outlook.com;
E-Mail To : jdeer@cybernetics.com;
Subject : Hello again!
Date Received : 2017-12-21 14:18:18 PST
Date Sent : 2017-12-21 14:18:18 PST
Message (Plaintext) : Hello,

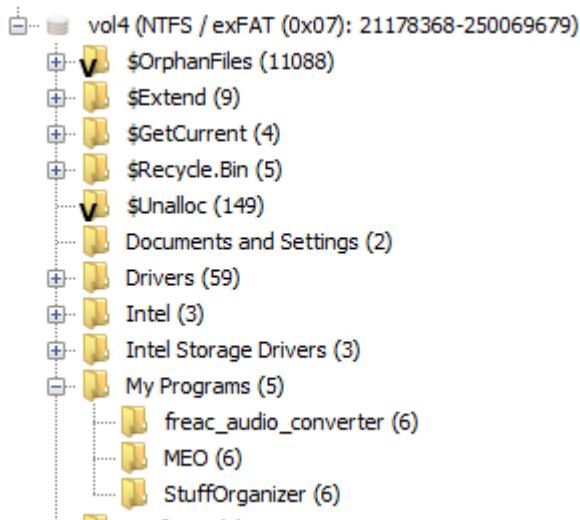
Some great stuff this time around; device contains all 3 requested files:
1. MXCWP Design
2. MXCWP Mobile App Source code
3. Board meeting minutes

Please send payments in bitcoins through same channel.
```

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 17:57:52 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.



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 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 LICENSE.txt Physical size and size of file are different.



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 .





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	LICENSE.txt	34	Regular File	12/14/2017
File Class	Regular File	LICENSE.txt.FileSlack	3	File Slack	
File Size	234,722	setup_stuff_organizer.exe	4,545	Regular File	12/14/2017
Physical Size	237,568	stuff_organizer.exe	230	Regular File	12/19/2017
Start Cluster	16,611,977	stuff_organizer.exe.FileSlack	3	File Slack	
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	393b0	F4	67	D3 C0 D2 E9 FF B6-18 E8 C1 30 AC EF A2 54
Hidden	False	393c0	A7	2B	3D 73 D7 6F A0 F6-8D 20 AD E9 1E DA 86 14
System	False	393d0	E3	77	7E 26 2D D3 C0 01-DC 7E FB 8F E9 78 24 EB
Read only	False	393e0	6C	9E	98 E6 EF 72 A2 7E-B6 2C 3B F6 7C 71 0F 3C
Archive	True	393f0	29	E7	40 A1 0E 23 CE 46-BF 63 2A 39 70 AB 09 9B
		39400	8A	94	D0 B5 33 C2 82 DD-1F CC AB 7F 33 99 65 71
		39410	03	E7	9D 1A D3 70 50 BD-AD F9 47 C1 5A 08 F2 AA
		39420	CD	48	83 87 08 72 BD E6-CE 83 AE FC BB 55 C3 1E
		39430	94	A6	7F 63 C8 4F 46 55-BD BE 5C 9B 00 82 44 14
		39440	32	F7	C7 D9 4E 0F AC A3-03 C1 0A B6 03 AB A9 AF
		39450	EE	C5	3B 90 DF 75 A4 04-20 1C 88 9A A0 73 65 DC
		39460	D5	71	C2 16 17 76 BF FE-A7 7B BE E5 39 F7 BD 4A
		39470	01	04	06 00 01 09 C3 50-94 00 07 0B 01 00 02 24
		39480	06	F1	07 01 0A 53 07 1E-8B 93 0C EF 9F 8E 18 21
		39490	21	01	0C 00 0C C3 43-94 C3 33 94 00 08 0A 01
		394a0	48	46	ED 69 00 00 05 01-19 03 00 00 00 11 19 00
		394b0	63	00	6F 00 00 6F 00 6B 00-69 00 6E 00 67 00 2E 00
		394c0	64	00	6F 00 63 00 00 00 19 02 00 00 14 0A 01 00

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



Name	stuff_organizer.exe.FileSlack	LICENSE.txt	34	Regular File	12/14/2017 5:41:11 PM
File Class	File Slack	LICENSE.txt.FileSlack	3	File Slack	
File Size	2,846	setup_stuff_organizer.exe	4,545	Regular File	12/14/2017 5:35:11 PM
Physical Size	2,846	stuff_organizer.exe	230	Regular File	12/19/2017 2:14:54 AM

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	7z ⁴	-	-	-	-	0!P					
00010	00	00	00	00	72	00	00	00-00	00	00	00	BA	66	56	C1	-	r	-	-	-	fVA					
00020	92	D4	86	C5	E5	D5	8A	8B-06	0C	96	04	6E	A4	A8	E2	-	Ö	Å	Ä	Ö	n	ä				
00030	5F	AF	6C	7C	2F	F2	07	B6-46	8A	83	3C	9D	73	1E	C2	-	l	/	ö	TF	<	s	Å			
00040	7A	85	E8	0B	2E	C9	D4	4F-7D	39	1C	2F	99	26	FC	BA	z	·	è	·	É	Ö	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		
<u>Extension</u>	<u>Signature</u>	<u>Description</u>
 7Z	<u>37 7A BC AF 27 1C</u>	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.

File List

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	
393b0 F4 67 D3 C0 D2 E9 FF B6-18 E8 C1 30 AC EF A2 54	0gÓÀÓéý¶·éÁ0-i«T		
393c0 A7 2B 3D 73 D7 6F A0 F6-8D 20 AD E9 1E DA 86 14	¶+=sxo ö. -é.Ú..		
393d0 E3 77 7E 26 2D D3 C0 01-DC 7E FB 8F E9 78 24 EB	åw~ç-ÓÀ.Ü~û.éx\$ë		
393e0 6C 9E 98 E6 EF 72 A2 7E-B6 2C 3B F6 7C 71 0F 3C	l..-æirc~¶,;ö q.<		
393f0 29 E7 40 A1 0E 23 CE 46-BF 63 2A 39 70 AB 09 9B)ç@i #íFçç*9pk..		
39400 8A 94 D0 B5 33 C2 82 DD-1F CC AB 7F 33 99 65 71	.-Ðu3À.Ý.í«-3.eq		
39410 03 F7 9D 1A D3 70 50 BD-AD F9 47 C1 5A 08 F2 AA	.+..ÓpP¾-ùGÀZ.ö²		
39420 CD 48 83 87 08 72 BD E6-CE 83 AE FC BB 55 C3 1E	ÍH...-r¾æÍ.Øù»UÀ.		
39430 94 A6 7F 63 C8 4F 46 55-BD BE 5C 9B 00 82 44 14	. -cÈOFU¾\...D-		
39440 32 F7 C7 D9 4E 0F AC A3-03 C1 0A B6 03 AB A9 AF	2-ÇÙN.-£.À.¶.«@-		
39450 EE C5 3B 90 DF 75 A4 04-20 1C 88 9A A0 73 65 DC	iÀ;.ßuà.... seÙ		
39460 D5 71 C2 16 17 76 BF FE-A7 7B BE E5 39 F7 BD 4A	ÖqÀ..vçþS{¾ä9÷¾J		
39470 01 04 06 00 01 09 C3 50-94 00 07 0B 01 00 02 24ÅP.....\$		
39480 06 F1 07 01 0A 53 07 1E-8B 93 0C EF 9F 8A 18 21	.ñ...S....i...!		
39490 21 01 0C 01 00 0C C3 43-94 C3 33 94 00 08 0A 01	!.....ÀC.À3.....		
394a0 48 46 ED 69 00 00 05 01-19 03 00 00 00 11 19 00	HFIi.....		
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.....		
394d0 02 A4 91 9A 6E 78 D3 01-15 06 01 00 20 00 00 00	.ñ..-nxO.....		
394e0 00 00	..		

Cursor pos = 0; clus = 16611977; log sec = 132895816; phy sec = 154074184

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.

Select a volume to analyze or add a new image file.

CASE GALLERY		HOST GALLERY		HOST MANAGER	
mount	name			fs type	
<input checked="" type="radio"/> disk	data_theft.001-disk			raw	details
<input type="radio"/> C:/	data_theft.001-2048-206847			ntfs	details
<input type="radio"/> D:/	data_theft.001-206848-21178367			ntfs	details
<input type="radio"/> E:/	data_theft.001-21178368-250069679			ntfs	details

[ANALYZE](#) [ADD IMAGE FILE](#) [CLOSE HOST](#)
[HELP](#)

[FILE ACTIVITY TIME LINES](#) [IMAGE INTEGRITY](#) [HASH DATABASES](#)
[VIEW NOTES](#) [EVENT SEQUENCER](#)

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

LICENSE.txt	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
setup_stuff_organizer.exe	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: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)	4653702	0	0	222357-128-1
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](#)

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

[REPORT](#) [NEXT](#) [PREVIOUS](#) [VIEW CONTENTS](#) [EXPORT CONTENTS](#) [ADD NOTE](#)

File Type: 7-zip archive data, version 0.4

MD5 of content: 949feba9609eb0a5580ae0f02942966d6 -

SHA-1 of content: bf1e7ca36693e5c2cf730d99edef636f1f05bf2 -

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)

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





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 seem correct and it does not open password of cooking.doc

Hex details show as a following image:

d / d	<u>..</u>	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	<u>..</u>	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	<u>LICENSE.txt</u>	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	<u>setup_stuff_organizer.exe</u>	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	<u>setup_stuff_organizer.exe:Zone.Identifier</u>	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	<u>stuff_organizer.exe</u>	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

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

ASCII details show as a following image:

d / d	.L	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	.L	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

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

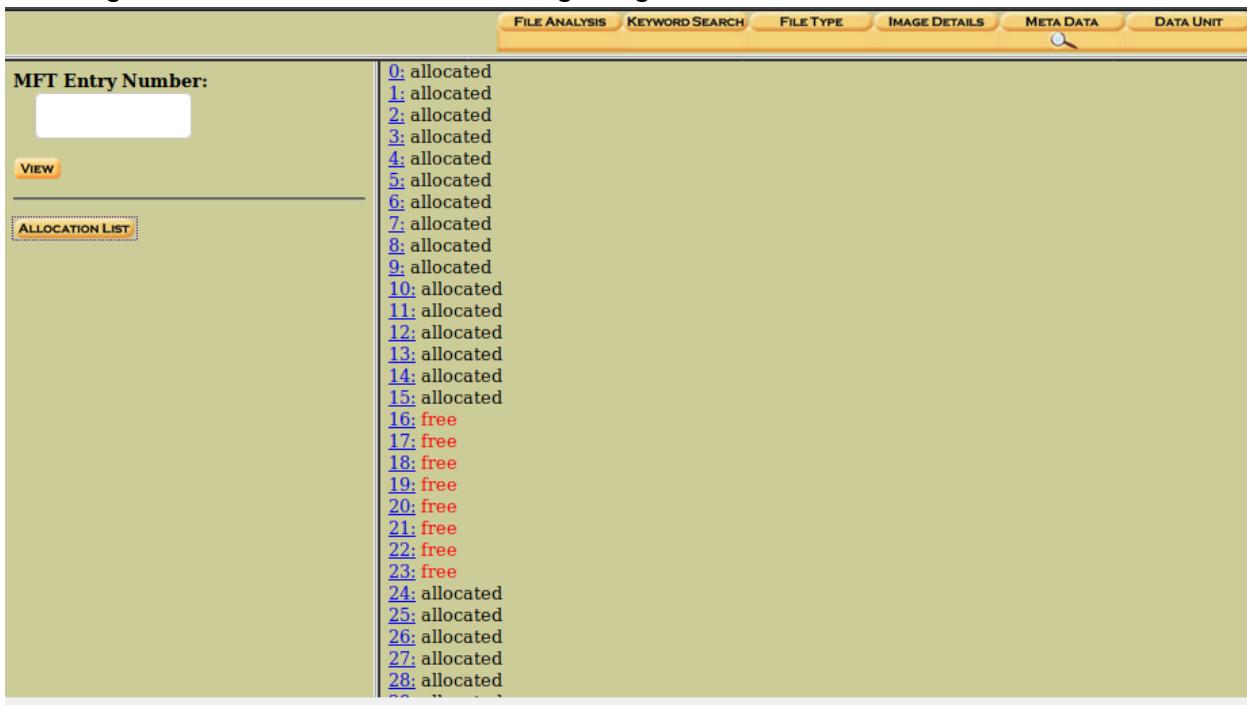


ASCII s code shows that Autopsy has recognised this file as Zip Archive. And will be opened with 7zip.

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

7z00*060000P0000000fV0000000000n000001|/000F00<0s0z00.000}90/0000000000|`0000000:00b00Jd0q0200g0005v0-Jm00{F000
030ck200eH90wV0bb0y00300000Wn|qyi00000p0z0qtk00[g000090VB0C,p00U09

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

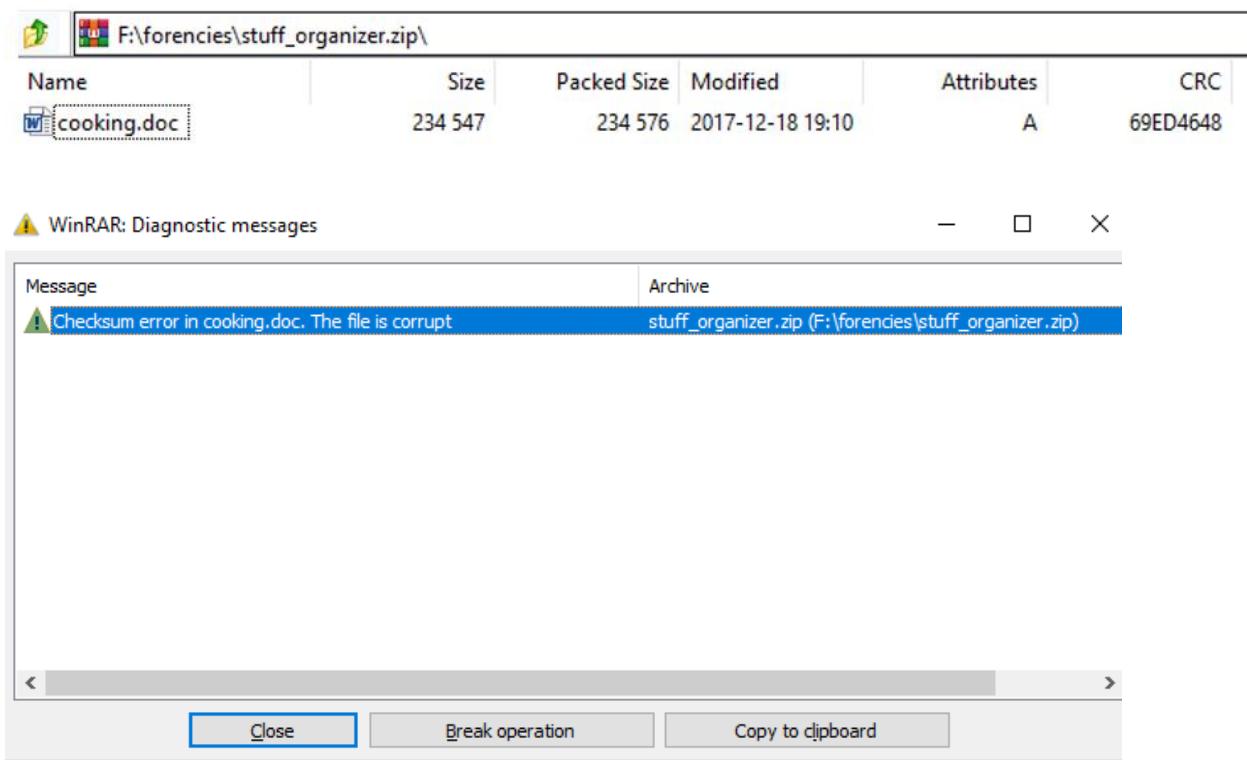


MFT Entry Number:	Allocation Status
	VIEW
	ALLOCATION LIST
0	allocated
1	allocated
2	allocated
3	allocated
4	allocated
5	allocated
6	allocated
7	allocated
8	allocated
9	allocated
10	allocated
11	allocated
12	allocated
13	allocated
14	allocated
15	allocated
16	free
17	free
18	free
19	free
20	free
21	free
22	free
23	free
24	allocated
25	allocated
26	allocated
27	allocated
28	allocated

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**.

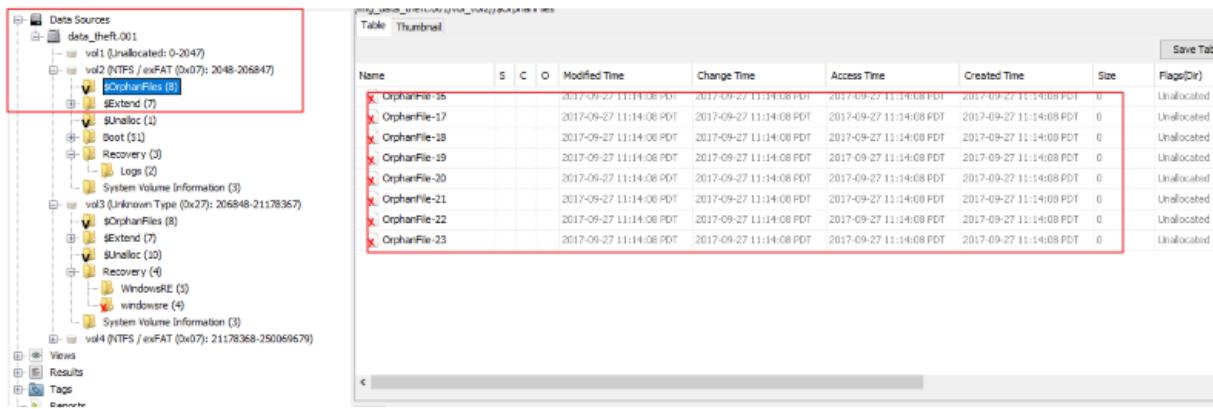
MFT Entry Number: <div style="border: 1px solid #ccc; padding: 2px; width: fit-content;">16</div> VIEW <hr/> ALLOCATION LIST	Pointed to by file: File name not found for inode File Type (Recovered): empty MD5 of recovered content: d41d8cd98f00b204e9800998ecf8427e - SHA-1 of recovered content: da39a3ee5e6b4b0d3255bfef95601890afdb0709 - Details: MFT Entry Header Values: Entry: 16 Sequence: 16 \$LogFile Sequence Number: 0 Not Allocated File Links: 0 \$STANDARD_INFORMATION Attribute Values: Flags: Hidden, System Owner ID: 0 Security ID: 0 () Created: 2017-09-27 14:14:08.000000000 (EDT) File Modified: 2017-09-27 14:14:08.000000000 (EDT) MFT Modified: 2017-09-27 14:14:08.000000000 (EDT) Accessed: 2017-09-27 14:14:08.000000000 (EDT) Attributes: \$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
---	---



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.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag(Dir)
OrphanFile-16				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-17				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-18				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-19				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-20				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-21				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-22				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-23				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated

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.

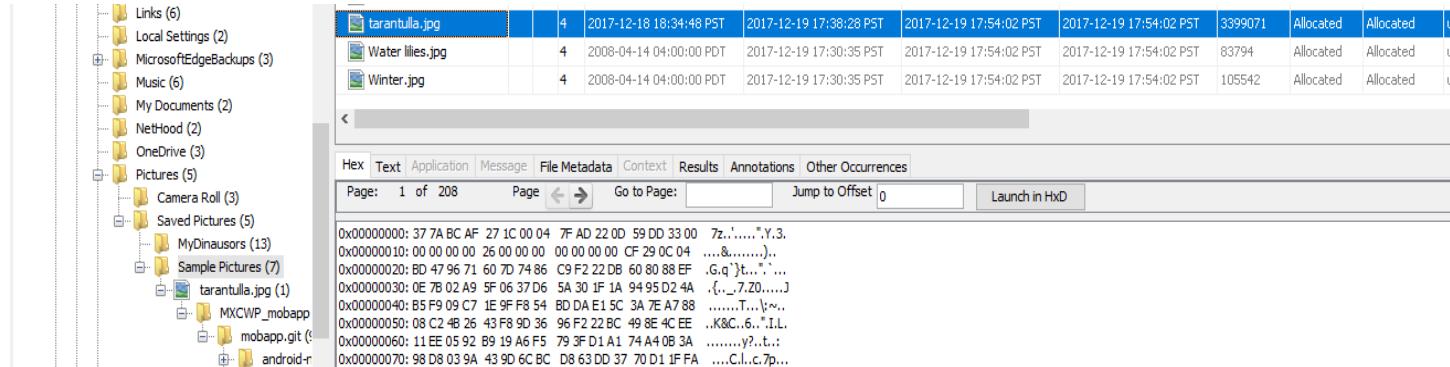
So, analysis of Lewis Disk Image gives information that some part of this file was damaged. The date of deleting this file illustrates that this file was not open on December 21 on target machine.

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.



Name	Size	Modified Time	Access Time	Created Time	Flags
tarantula.jpg	4	2017-12-18 18:34:48 PST	2017-12-19 17:38:26 PST	2017-12-19 17:54:02 PST	Allocated
Water lilies.jpg	4	2008-04-14 04:00:00 PDT	2017-12-19 17:30:35 PST	2017-12-19 17:54:02 PST	Allocated
Winter.jpg	4	2008-04-14 04:00:00 PDT	2017-12-19 17:30:35 PST	2017-12-19 17:54:02 PST	Allocated

```

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences
Page: 1 of 208 Page Go to Page: Jump to Offset 0 Launch in HxD

0x00000000: 37 7A BC AF 27 1C 00 04 7F AD 22 0D 59 DD 33 00 7z.'....."Y.3.
0x00000010: 00 00 00 00 26 00 00 00 00 00 00 CF 29 0C 04 .....&.....).
0x00000020: BD 47 96 71 60 7D 74 86 C9 F2 22 DB 60 80 88 EF .G.q"}t.,'...
0x00000030: 0E 7B 02 A9 5F 06 37 D6 5A 30 1F 1A 94 95 D2 4A .{,_-7.Z0....J
0x00000040: B5 F9 09 C7 1E 9F F8 54 BD DA E1 5C 3A 7E A7 8A .....T...{\~.
0x00000050: 08 C2 4B 26 43 F8 9D 36 96 F2 22 BC 49 8E 4C EE .K&C.6..".L.
0x00000060: 11EE 05 92 B9 19 A6 F5 79 3F D1 A1 74 A4 08 3A .....y?..t.:
0x00000070: 98 D8 03 9A 43 9D 6C BC D8 63 DD 37 70 D1 1F FA ....C.l.c.7...

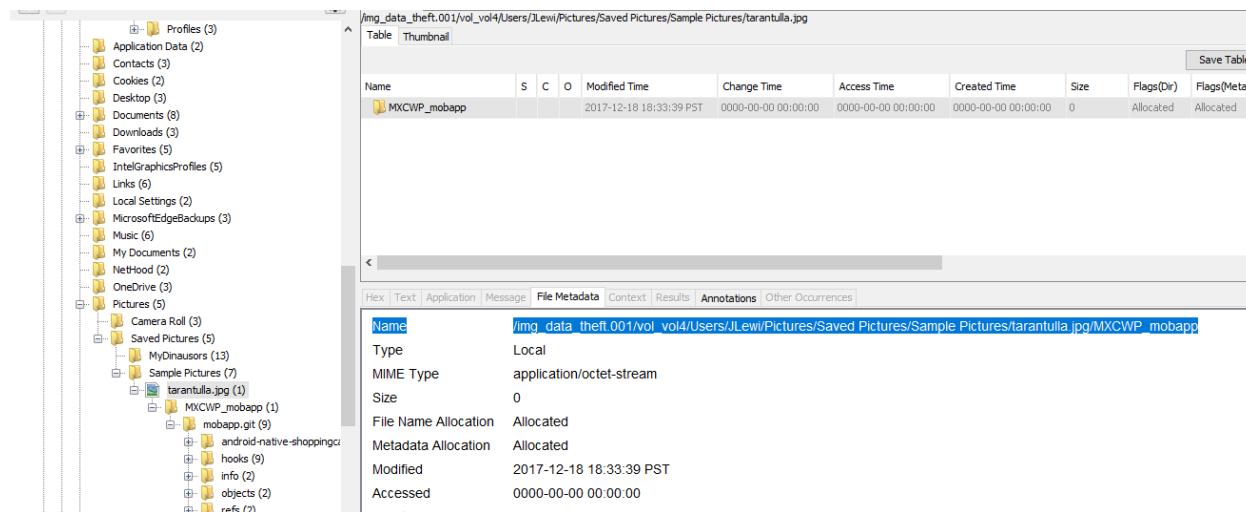
```

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.

1 Results Found For 377ABCAF271C		
Extension	Signature	Description
 7Z	37 7A BC AF 27 1C	7-Zip compressed file
	ASCII	Size: 6 Bytes
	7z•	Offset: 0 Bytes

Evidence illustrates that double click on it shows MXCWP FOLDER.



Name	Type	MIME Type	Size	File Name Allocation	Metadata Allocation	Modified	Accessed
/img_data_theft.001/vol_vo4/Users/JLewi/Pictures/Saved Pictures/tarantula.jpg	Local	application/octet-stream	0	Allocated	Allocated	2017-12-18 18:33:39 PST	0000-00-00 00:00:00



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.

/img_data_theft.001/vol_vol4/Users/JLewis/Pictures/Saved Pictures/Sample Pictures/tarantulla.jpg/MXCWP_mobapp/mobapp.git 9 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
android-native-shoppingcart-master				2017-12-18 18:34:01 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
branches				2017-12-15 23:48:02 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
config				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
description				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
HEAD				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
hooks				2017-12-18 18:34:03 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
info				2017-12-18 18:34:03 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
objects				2017-12-18 18:34:03 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot
refs				2017-12-18 18:34:03 PST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allot

Save Table as CSV

Pictures (5)

- Camera Roll (3)
- Saved Pictures (5)
 - MyDinosaurs (13)
 - Sample Pictures (7)
 - tarantulla.jpg (1)
 - MXCWP_mobapp (1)
 - mobapp.git (9)
 - android-native-shoppingcart-master (5)
 - hooks (9)
 - info (2)
 - objects (2)
 - refs (2)

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.



 meofree.exe			2017-12-18 19:28
 meofreesetup.exe			2017-11-11 13:13
 meofreesetup.exe:Zone.Identifier			2017-11-11 13:13
 README.txt			2017-12-14 09:47

< []

Hex Text Application Message File Metadata Context Results Annotations

0° C C 22% ⌂ + Reset



Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Page: 1 of 198 Page ← → Go to Page: Jump to Offset 0

```
0x00000000: 42 4D 76 70 31 00 00 00 00 00 36 00 00 00 28 00 BMvp1.....6...(.  
0x00000010: 00 00 B0 04 00 00 84 03 00 00 01 00 18 00 00 00 .....  
0x00000020: 00 00 40 70 31 00 00 00 00 00 00 00 00 00 00 ..@p1.....  
0x00000030: 00 00 00 00 00 00 8B 9C A9 8B 9E AB 82 9A A6 7F .....  
0x00000040: 99 A7 85 9F AF 83 9D AD 7C 96 A7 7C 96 A7 90 AA .....|....
```

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





Listing Keyword search 1 - codes

/mg_data_theft.001/vol.vol4/My Programs/MEO

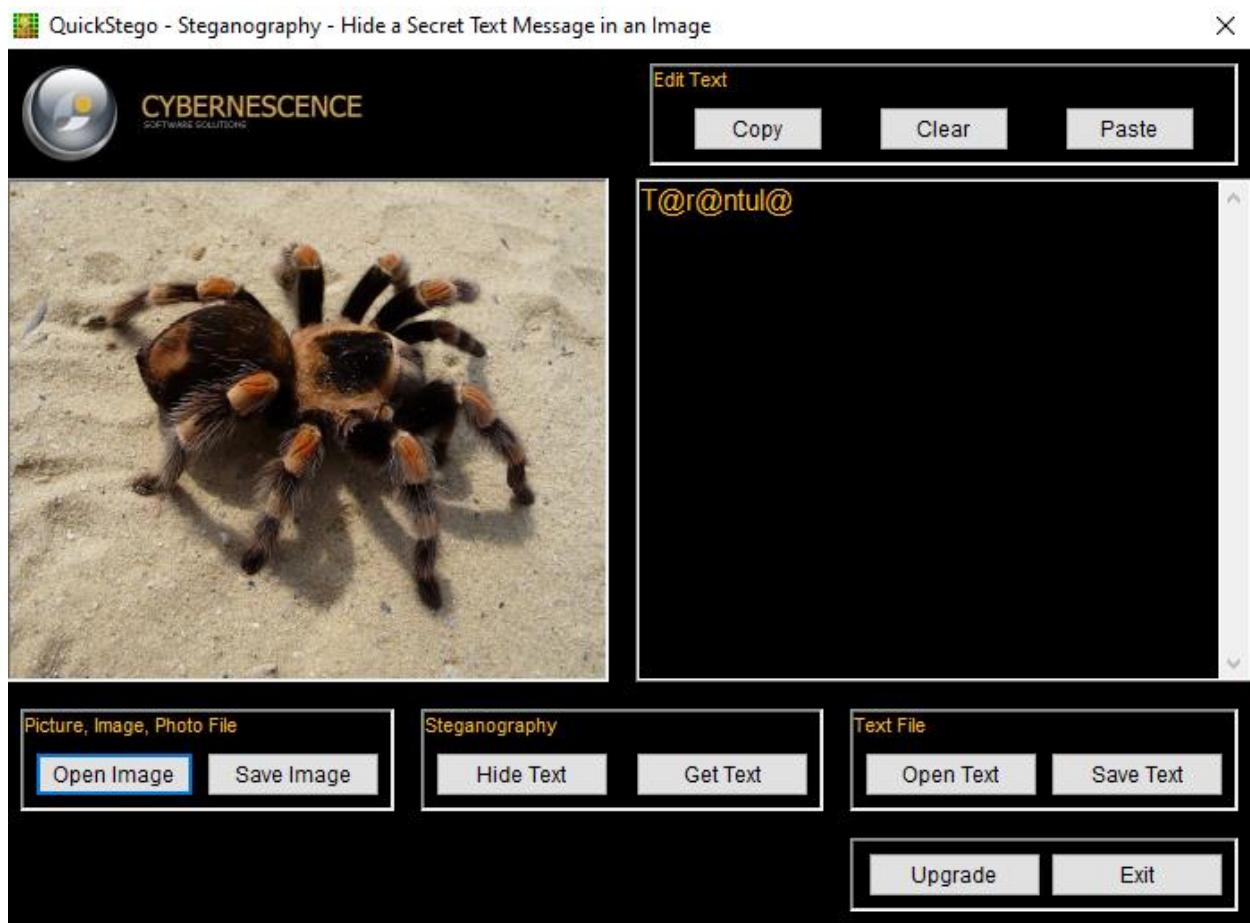
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:51 PST	2017-12-19 17:57:51 PST	488
[parent folder]				2017-12-19 17:57:52 PST	2017-12-19 17:57:53 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:51 PST	56
mefree.exe				2017-12-18 19:28:08 PST	2017-12-18 19:35:13 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST	3240054
mefreesetup.exe				2017-11-11 13:13:39 PST	2017-12-18 19:33:31 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST	448232
mefreesetup.exe\Zone.Identifier				2017-11-11 13:13:39 PST	2017-12-18 19:33:31 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST	26
README.txt				2017-12-14 09:47:49 PST	2017-12-18 19:33:31 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST	5871

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

0° C | 22% | Reset

Tags M

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.



Listing Keyword search 1 - codes X

/img_data_theft.001/vol_voi4/Users/JLewi/Music

Table Thumbnail

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2017-12-19 17:53:07 PST	2017-12-19 17:53:07 PST	2017-12-19 17:53:07 PST	2017-12-19 13:47:25 PST	56
[parent folder]				2017-12-19 15:31:10 PST	2017-12-19 15:31:10 PST	2017-12-19 15:31:10 PST	2017-12-19 15:18:06 PST	176
Beethoven's Symphony No. 9 (Scherzo).wma	4			2008-04-14 04:00:00 PDT	2017-12-19 15:30:50 PST	2017-12-19 17:52:55 PST	2017-12-15 10:43:48 PST	613638
desktop.ini	4			2017-12-19 15:30:50 PST	2017-12-19 15:30:50 PST	2017-12-19 13:49:52 PST	2017-12-19 13:49:52 PST	504
Mozart'sSymphony_no_187.wma	4			2017-12-18 20:01:15 PST	2017-12-19 17:23:29 PST	2017-12-19 17:52:55 PST	2017-12-18 20:01:15 PST	24252
New Stories (Highway Blues).wma	4			2008-04-14 04:00:00 PDT	2017-12-19 15:30:48 PST	2017-12-19 17:53:07 PST	2017-12-19 17:53:07 PST	760748

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: - of - Match Page: 1 of 1 Page 100% Reset Text Source: File Text

Board Meeting Minutes (Confidential)
Freescale Semiconductor, Inc.
(Board Meeting Minutes: November 18, 2017)

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:

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.

2 PST	2017-12-19 13:49:52 PST	504	Allocated	Allocated	unknown	..._06e8f7e6ddd6...	text/x-ini	ini
5 PST	2017-12-18 20:01:15 PST	24252	Allocated	Allocated	unknown	...3b1d1ff436e0...	application/vnd.openxmlformats-officedocument.wordprocessingml.doc...	wma
7 PST	2017-12-19 17:53:07 PST	760748	Allocated	Allocated	unknown	..._74369361fdb0...	audio/x-ms-wma	wma

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: - of - Match Page: 1 of 1 Page 100% Reset Text Source: File Text

Board Meeting Minutes (Confidential)
Freescale Semiconductor, Inc.
(Board Meeting Minutes: November 18, 2017)

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:

50 4B 03 04 14 00 06 00

DOCX, PPTX, XLSX

PK.....

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.



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.



- *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.

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:



Default 110 Results

Table Thumbnail

[Save Table as CSV](#)

Source 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;	amaderiras2000@hotmail.com;	Re: Weekly Environemetal Activity Report	2017-12-21 14:12:08 PST	Nc
Sent-1				jlewis4000@outlook.com;	amaderiras2000@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;	amaderiras2000@hotmail.com;	Re: Nutcracker Market Invitation	2017-12-21 14:19:50 PST	Nc
Sent-1				jlewis4000@outlook.com;	amaderiras2000@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

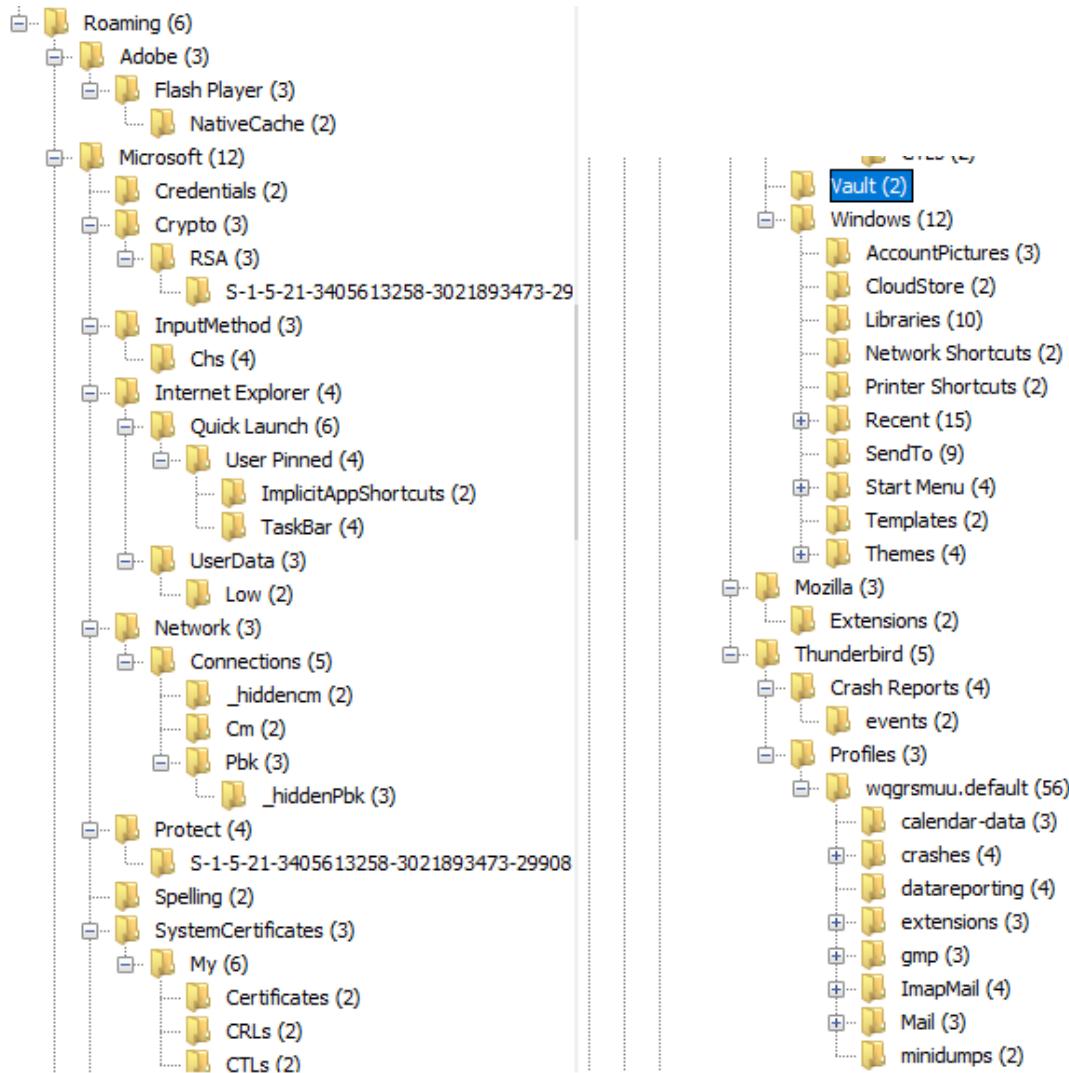
He mentioned that he sends payments in bitcoins. Looking for collecting evidence and information leads to finding some files that prove bitcoins account, bitcoins wallet.

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.





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.

Keyword search 8 Results

Table Thumbnail [Save Table as CSV](#)

Name	Key...	Location	Modified Time
blocklist-addons.json	14:35...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roaming/Thunderbird/Pro...	2017-12-19 15:
xlsrvintl.dll	Befor...	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/SharedLimitedTime/...	2017-03-18 19:
C972AC86BA22ADBFC038B134C02101C894D0078A	9T14:...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Local/Thunderbird/Profiles...	2017-12-19 15:
MSOINTL.DLL	XML.....	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/SharedLimitedTime/...	2017-03-18 19:
xlsrvintl.dll	Befor...	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/SharedLimitedTime/...	2017-03-18 19:
appsglobals.txt	57-A3...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Local/Packages/Microsoft....	2017-03-29 01:
kinto.sqlite	9T14:...	/img_data_theft.001/vol_vo4/Users/JLewi/AppData/Roaming/Thunderbird/Pro...	2017-12-19 15:
en-US.dic	bitchin...	/img_data_theft.001/vol_vo4/Program Files (x86)/Mozilla Thunderbird/dictiona...	2017-11-21 19:

< >

[Hex](#) [Text](#) [Application](#) [Message](#) [File Metadata](#) [Context](#) [Results](#) [Annotations](#) [Other Occurrences](#)

[Strings](#) [Indexed Text](#) [Translation](#)

Matches on page: 1 of 2 Match Page: 4 of 12 Page [←](#) [→](#) 100% [🔍](#) [➕](#) [Reset](#) Text Source: [Search](#)

```
{6D809377-6AF0-444B-8957-A3773F02200E}\Bitcoin\bitcoin-qt.exe 10918
C:\MAMP\MAMP.exe 10919
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA0E}\TypingMaster10\tmaster.exe 10919
SiliconBendersLLC.Sketchable_r2kxzpx527qgj!App 10922
AcerControlCenter.ToastProperty 10922
wind..tion_c3bce3770c238a49_0e5786c29a718416 10925
```

Bitcoin-qt.exe file information

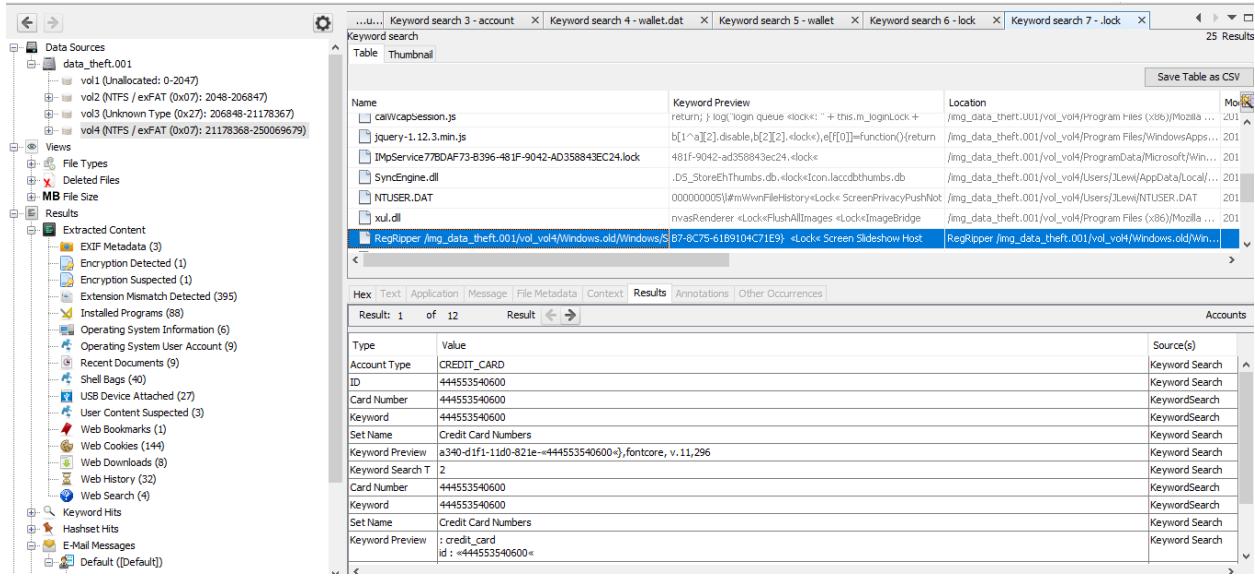
The process known as Bitcoin Core (GUI node for Bitcoin) or Bitcoin Gold (GUI node for Bitcoin) belongs to software Bitcoin Core or Bitcoin Gold by Bitcoin.

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



Type	Value	Source(s)
Account Type	CREDIT_CARD	Keyword Search
ID	444553540600	Keyword Search
Card Number	444553540600	KeywordSearch
Keyword	444553540600	KeywordSearch
Set Name	Credit Card Numbers	Keyword Search
Keyword Preview	a340-d1f1-11d0-821e-444553540600>,fontcore, v.11,296	Keyword Search
Keyword Search T	2	Keyword Search
Card Number	444553540600	KeywordsSearch
Keyword	444553540600	KeywordsSearch
Set Name	Credit Card Numbers	Keyword Search
Keyword Preview	: credit_card id : <444553540600<	Keyword Search

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.

new case - Autopsy 4.15.0 Case View Tools Window Help

Add Data Source Communications Geolocation Timeline File Discovery Generate Report Close Case Keyword Lists Keyword Search

...PG Keyword search 9 - MPG Keyword search 10 - MXCWP design Keyword search 12 - payment Keyword search 13 - payment Keyword search 15 - bc1* 124 Results Save Table as CSV

Keyword search Table Thumbnail

Name	Keyword Preview	Location
bcmhvsvr.dll	etattr-cerisetattr=<pgw/cappayment> gateway capability	/img_data_theft.001/vol_vo4/Drivers/Network_Driver_71TSD_WN32_7.3t
bcmhvsvr64.dll	uestauauthorized<paymentrequired>forbiddennotfound	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/Shared/limited1
vhstNew.Store.dll	etattr-cerisetattr=<pgw/cappayment> gateway capability	/img_data_theft.001/vol_vo4/Drivers/Network_Driver_71TSD_WN32_7.3t
Command_Configure.msi	uestaunauthorized<paymentrequired>forbiddennotfound	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/Shared/limited1
LICENSE.txt	ceiving your timely <payment> of any fees or roya	/img_data_theft.001/vol_vo4/Drivers/Systems-Management_Application_
Microsoft.Wallet.dll	nder which you make <payment> to the third party	/img_data_theft.001/vol_vo4/Programs/StuffOrganizer/LICENSE.txt
MozartSSymphony_no_187.wma	mpany receives more <payments> on time, after bri	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/Shared/united1
IntelWebAPIUpdaterActiveX.dll	psetattr-tokentype<payment> gateway capability	/img_data_theft.001/vol_vo4/Drivers/Chipset_Application_PRRRC_WN_9.
BingLocalSearchService.dll	reviewcountreview<paymentaccepted>servesusinameni	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/Shared/united1
RegRipper /mg_data_theft.001/vol_vo4/Windows/System32/config/SOFT	8b87-dfb08f54c12) <paymentmediatorserviceuseragent<	RegRipper /mg_data_theft.001/vol_vo4/Windows/System32/config/SOFT
Microsoft.People.Relevance.dll	equestunauthorized<paymentrequired>forbiddennotfound	/img_data_theft.001/vol_vo4/Program Files/WindowsApps/Shared/united1
checkout_payment_method_bg.png	<checkout_payment>method_bg.png<	/img_data_theft.001/vol_vo4/Users/Jewl/Pictures/Saved Pictures/Sample

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences Result: 1 of 5 Result Keyword Hits

Type Value Source(s)

Keyword payment Keyword Search

Keyword Regular Express payment Keyword Search

Keyword Preview <bc52-bb45fb59a0b8> <paymentmediatorservicewallet> Keyword Search

(d1e460dc-a564-4b Keyword Search

Keyword Search Type 1 Keyword Search

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.

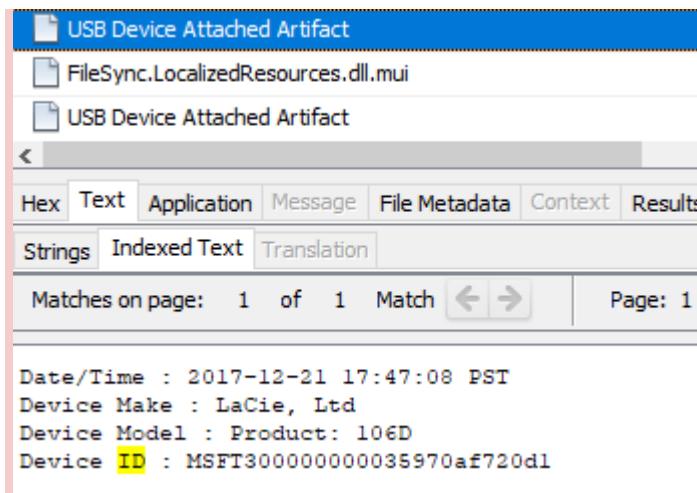
Windows (118) Windows.old (10)

Views File Types Deleted Files MB File Size Results Extracted Content EXIF Metadata (3) Encryption Detected (1) Encryption Suspected (1) Extension Mismatch Detected (395) Installed Programs (88) Operating System Information (6) Operating System User Account (9) Recent Documents (9) Shell Bags (40) USB Device Attached (27) User Content Suspected (3) Web Bookmarks (1) Web Cookies (144) Web Downloads (8) Web History (32) Web Search (4) Keyword Hits Hashset Hits E-Mail Messages Default (Default) Default (110) Interesting Items Accounts Email

USB Device Attached Table Thumbnail 27 Results Save Table as CSV

Source File	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM	▼	5	2017-12-19 15:20:03 PST		ROOT_HUB20	48377f931380	data_theft.001	
SYSTEM	▼	5	2017-12-19 15:20:03 PST		ROOT_HUB20	48f1465280	data_theft.001	
SYSTEM	▼	5	2017-12-19 15:20:04 PST		ROOT_HUB30	481e2c18c58080	data_theft.001	
SYSTEM	▼	5	2017-12-21 17:47:29 PST	LaCie, Ltd	Product: 106D	MSFT300000000035970af720d1	data_theft.001	
SYSTEM	▼	5	2017-12-21 17:47:29 PST	LaCie, Ltd	Product: 106D	MSFT30000000003597a9912087	data_theft.001	
SYSTEM	▼	5	2017-12-21 14:10:36 PST	Lexar Media, Inc.	Product: A81D	AACQMFFN6W/BFESG	data_theft.001	
SYSTEM	▼	5	2017-12-19 15:20:05 PST	Microdia	Product: 643F	681260f0e48085	data_theft.001	
SYSTEM	▼	5	2017-12-19 15:20:05 PST	Microdia	Product: 643F	788fb9168080000	data_theft.001	
SYSTEM	▼	5	2017-12-19 15:20:05 PST	Intel Corp.	Integrated Rate Matching Hub	582270d3f8a80&1	data_theft.001	
SYSTEM	▼	5	2017-12-19 15:20:04 PST	Intel Corp.	Integrated Rate Matching Hub	5857d852f6061	data_theft.001	
SYSTEM	▼	5	2017-12-19 13:41:23 PST	ROOT_HUB20	48377f931380	data_theft.001		
SYSTEM	▼	5	2017-12-19 13:41:23 PST	ROOT_HUB30	48f1465280	data_theft.001		
SYSTEM	▼	5	2017-12-19 13:41:23 PST	Primax Electronics, Ltd	HP Optical Mouse	58259a0eba80&1	data_theft.001	
SYSTEM	▼	5	2017-09-28 08:58:26 PDT	Primax Electronics, Ltd	HP Optical Mouse	58259a0eba80&2	data_theft.001	
SYSTEM	▼	5	2017-09-28 08:58:29 PDT	Primax Electronics, Ltd	HP Optical Mouse	6824fce818083	data_theft.001	
SYSTEM	▼	5	2017-09-28 08:58:32 PDT	Primax Electronics, Ltd	HP Optical Mouse	681260f0e48085	data_theft.001	
SYSTEM	▼	5	2017-12-19 13:41:24 PST	Microdia	Product: 643F	788fb9168080000	data_theft.001	
SYSTEM	▼	5	2017-12-19 13:41:25 PST	Microdia	Product: 643F	48377f931380	data_theft.001	
SYSTEM	▼	5	2017-12-19 13:41:24 PST	Intel Corp.	Integrated Rate Matching Hub	582270d3f8a80&1	data_theft.001	
SYSTEM	▼	5	2017-12-19 13:41:24 PST	Intel Corp.	Integrated Rate Matching Hub	5857d852f6061	data_theft.001	
SYSTEM	▼	5	2017-12-19 13:41:23 PST	ROOT_HUB20	48377f931380	data_theft.001		

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

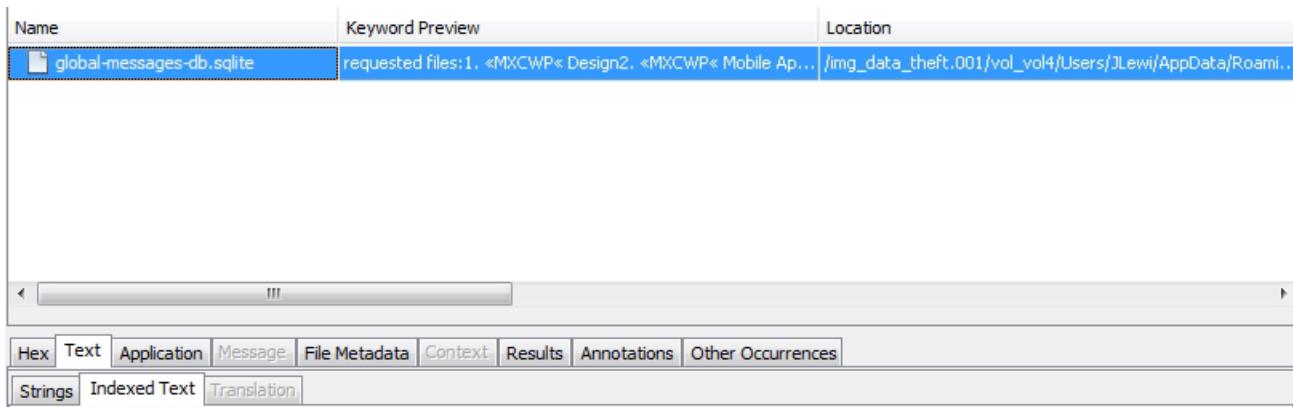


The screenshot shows a forensic analysis interface with a blue header bar. The main window displays a file tree with two entries: 'FileSync.LocalizedResources.dll.mui' and 'USB Device Attached Artifact'. Below the tree, there are tabs for Hex, Text, Application, Message, File Metadata, Context, Results, Strings, Indexed Text, and Translation. The 'Strings' tab is selected. A search bar indicates 'Matches on page: 1 of 1 Match' and 'Page: 1'. The results pane contains the following text:

```
Date/Time : 2017-12-21 17:47:08 PST
Device Make : LaCie, Ltd
Device Model : Product: 106D
Device ID : MSFT300000000035970af720d1
```

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.



The screenshot shows a forensic analysis interface with a table view. The columns are 'Name', 'Keyword Preview', and 'Location'. One row is visible, showing 'global-messages-db.sqlite' in the Name column, 'requested files:1. <MXCWP< Design2. <MXCWP< Mobile Ap...' in the Keyword Preview column, and '/img_data_theft.001/vol_vol4/Users/JLewi/AppData/Roam...' in the Location column. Below the table, there are tabs for Hex, Text, Application, Message, File Metadata, Context, Results, Annotations, Other Occurrences, Strings, Indexed Text, and Translation. The 'Text' tab is selected.



theft di - Autopsy 4.15.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline File Discovery Keyword Lists Keyword Search

Keyword search 2 - stuff Keyword search 3 - MXCWP Keyword search 4 - MXCWP Keyword search 5 - design Keyword search 5 - design

1 Results

Data Sources

data_theft.001

- vol1 (Unallocated: 0-2047)
- vol2 (NTFS / exFAT (0x07): 20
- vol3 (Unknown Type (0x27): 2
 - \$OrphanFiles (8)
 - \$Extend (7)
 - \$Unalloc (10)
 - Recovery (4)
 - System Volume Information
- vol4 (NTFS / exFAT (0x07): 21
 - \$OrphanFiles (11088)
 - \$Extend (9)
 - \$GetCurrent (4)
 - \$Recycle.Bin (5)
 - \$Unalloc (149)
 - Documents and Settings (2)
 - Drivers (59)
 - Intel (3)
 - Intel Storage Drivers (3)
 - My Programs (5)
 - PerfLogs (0)
 - PerfLogs (3)

Table Thumbnail

Name Keyword Preview Location

global-messages-db.sqlite requested file:1, <MXCWP> Design2, <MXCWP> Mobile Ap... /img_data_theft.001/vol_vo4/Users/jlewi/AppData/Roam...

Save Table as CSV

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: 1 of 6 Match Page: 26 of 27 Page 100% 9:03 PM Reset Text Source: Se

1. MXCWP Design

2. MXCWP Mobile App Source code

3. Board meeting minutes

Please send payments in bitcoins through same channel.

Thank you.

JL Hello again! John Lewis <jlewis4000@outlook.com> jdeer@cybernetics.com

134 Hello,

9:03 PM 7/11/2020

theft di - Autopsy 4.15.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline File Discovery Keyword Lists Keyword Search

Keyword search 2 - stuff Keyword search 3 - MXCWP Keyword search 4 - MXCWP Keyword search 5 - design Keyword search 5 - design

12 Results

Data Sources

data_theft.001

- vol1 (Unallocated: 0-2047)
- vol2 (NTFS / exFAT (0x07): 20
- vol3 (Unknown Type (0x27): 206848-21178367)
 - \$OrphanFiles (8)
 - \$Extend (7)
 - \$Unalloc (10)
 - Recovery (4)
 - System Volume Information
- vol4 (NTFS / exFAT (0x07): 21
 - \$OrphanFiles (11088)
 - \$Extend (9)
 - \$GetCurrent (4)
 - \$Recycle.Bin (5)
 - \$Unalloc (149)
 - Documents and Settings (2)
 - Drivers (59)
 - Intel (3)
 - Intel Storage Drivers (3)
 - My Programs (5)
 - PerfLogs (0)
 - PerfLogs (3)

Table Thumbnail

Name Keyword Preview Location

Country Meeting Minutes - July.pdf Manager to consider a re-design of the Country Bowler /img_data_theft.001/vol_vo4/Users...

Save Table as CSV

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: 1 of 1 Match Page: 1 of 1 Page 100% 9:02 PM Reset Text Source: Se

Action: The CEO with the Competitions Manager to consider a re-design of the Country Bowler of the Year (men), with the inclusion of state events in the point's allocation.

9.2 Delegates meeting at Country Week
It was agreed that a meeting would be called of delegates (ladies) at the Metropolitan vs Country match and gauge its popularity at that time. NOTED.

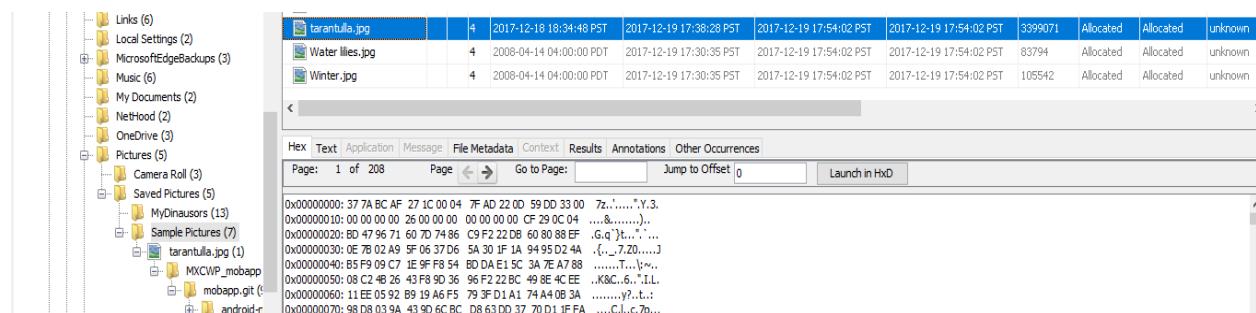
9.3 BWA strategic plan
The CEO explained the process for the formulation of the next BWA strategic plan which will

9:02 PM 7/11/2020

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 compressed 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:



Screenshot of a file search interface showing a list of files in a folder. The files listed are:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D)	File
[current folder]				2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	96	Allocated	All
[parent folder]				2017-12-19 17:54:06 PST	2017-12-19 17:54:06 PST	2017-12-19 17:54:06 PST	2017-12-19 17:54:06 PST	56	Allocated	All
Blue Hills.jpg	2			2009-04-14 04:00:00 PDT	2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	28921	Allocated	All
Sunset.jpg	2			2009-04-14 04:00:00 PDT	2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	71102	Allocated	All
tarantula.jpg	2			2017-12-10 18:34:46 PST	2017-12-19 17:00:20 PST	2017-12-19 17:04:02 PST	2017-12-19 17:04:02 PST	1299071	Allocated	All
Waterfall.jpg	2			2009-04-14 04:00:00 PDT	2017-12-18 17:00:36 PST	2017-12-18 17:04:02 PST	2017-12-18 17:04:02 PST	93264	Allocated	All
Winter.jpg	2			2009-04-14 04:00:00 PDT	2017-12-19 17:30:35 PST	2017-12-19 17:54:02 PST	2017-12-19 17:54:02 PST	105942	Allocated	All

Hex	Text	Application	Message	File Metadata	Context	Results	Annotations	Other Occurrences
Page: 1 of 208	Page	← →	Go to Page:			Jump to Offset	0	
0x00000000: 37 7A BC AF 27 1C 00 04 7F AD 22 0D 59 DD 33 00	7z.'....".Y.3.							
0x00000010: 00 00 00 00 26 00 00 00 00 00 00 00 CF 29 0C 04&.....).							
0x00000020: BD 47 96 71 60 7D 74 86 C9 F2 22 DB 60 80 88 EF	.G.q')t...: ...							
0x00000030: 0E 7B 02 A9 5F 06 37 D6 5A 30 1F 1A 94 95 D2 4A	.{.._.7.20....J							
0x00000040: B5 F9 09 C7 1E 9F F8 54 BD DA E1 5C 3A 7E A7 88T...\\~..							
0x00000050: 08 C2 4B 26 43 F8 9D 36 96 F2 22 BC 49 8E 4C EE	.K&C..6."I.L.							
0x00000060: 11 EE 05 92 B9 19 A6 F5 79 3FD1 A1 74 A4 0B 3Ay?..t.:.							
0x00000070: 98 D8 03 9A 43 9D 6C BC D8 63 DD 37 70 D1 1F FAC.I..c.7p..							
0x00000080: B5 1B A6 06 D7 9F 45 82 FE E5 73 FC 0F 4D 64 31E..s..Md1							

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



	meofree.exe			2017-12-18 19:28
	meofreesetup.exe			2017-11-11 13:13
	meofreesetup.exe:Zone.Identifier			2017-11-11 13:13
	README.txt			2017-12-14 09:47

< [Navigation Buttons]

Hex Text Application Message File Metadata Context Results Annotation

0° C C 22% ⌂ ⌂ ⌂ Reset



Documents and Settings (2)

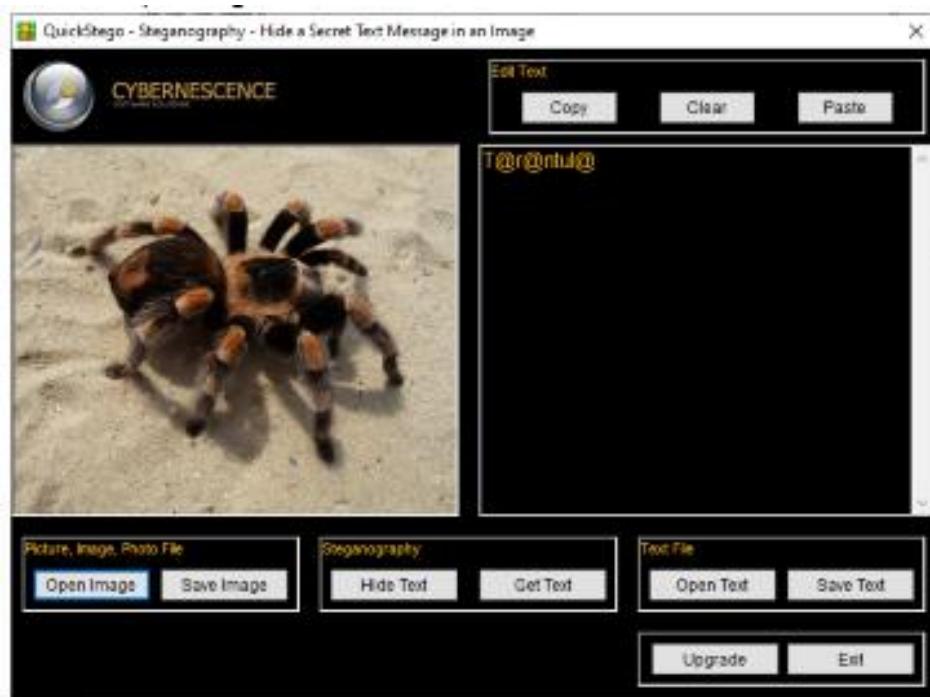
- Drivers (59)
- Intel (3)
- Intel Storage Drivers (3)
- My Programs (5)
 - freac_audio_converter
 - MEO (6)**
 - StuffOrganizer (6)
- PerfLogs (0)
- PerfLogs (3)
- Program Files (0)
- Program Files (25)
- Program Files (x86) (0)
- Program Files (x86) (17)
- ProgramData (0)
- ProgramData (14)
- Recovery (2)
- System Volume Information
- Users (0)

	[current folder]			2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST	2017-12-19 17:57:52 PST	2017-12-19
	[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
	meofree.exe			2017-12-18 19:20:00 PST	2017-12-18 19:35:13 PST	2017-12-19 17:57:52 PST	2017-12-19
	meofreesetup.exe:Zone.Identifier			2017-11-11 13:13:39 PST	2017-12-18 19:33:31 PST	2017-12-19 17:57:52 PST	2017-12-18
	README.txt			2017-12-14 09:47:49 PST	2017-12-18 19:33:31 PST	2017-12-19 17:57:52 PST	2017-12-11

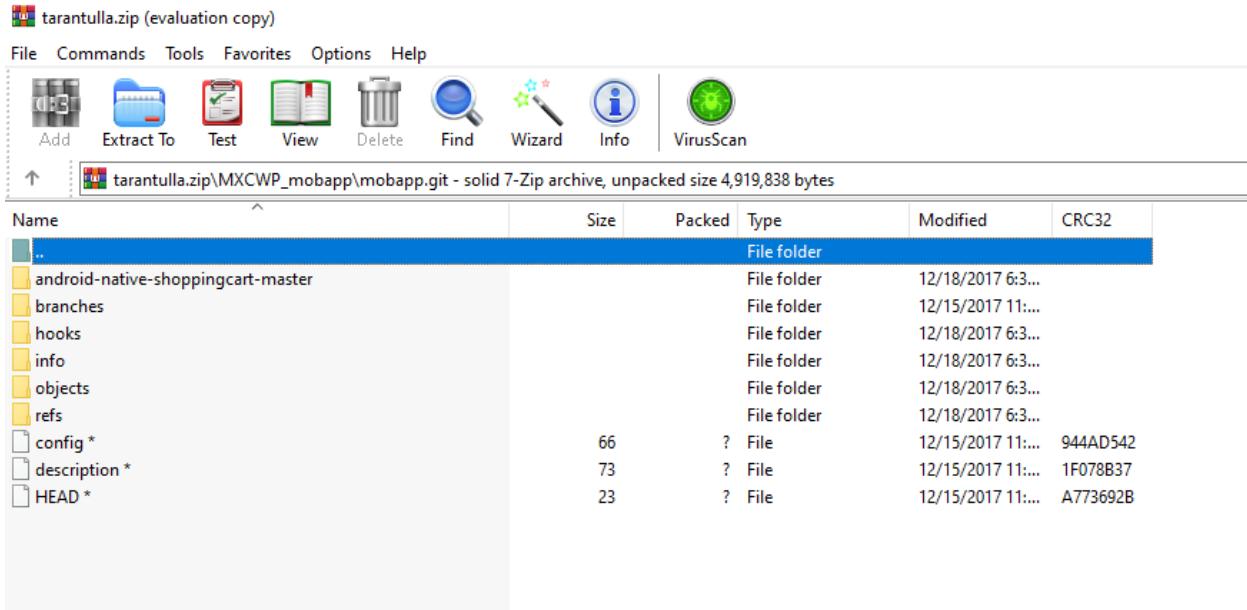
Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Page: 1 of 198 Page Go to Page: Jump to Offset: 0 Launch in HxD

```
0x00000000: 42 4D 7C 70 31 00 00 00 00 00 36 00 00 00 28 00 BMvpt.....6...,
0x00000010: 00 00 80 04 00 00 84 03 00 00 01 00 18 00 00 00 .....,
0x00000020: 00 00 40 70 31 00 00 00 00 00 00 00 00 00 00 00 ..@p1.....,
0x00000030: 00 00 00 00 00 00 88 9C A9 B8 9E AB 82 9A A6 7F .....,
0x00000040: 99 A7 85 9F AF B3 9D AD 7C 96 A7 7C 96 A7 90 AA .....|,
0x00000050: BA 93 B4 C3 8E B3 C1 83 A5 B2 85 9C AB 8D A0 AF .....|,
0x00000060: 89 A0 AF 7C 99 A7 75 97 A4 71 90 9F 66 84 95 69 ...].u.,q,f,.
0x00000070: 85 96 7A 9d A5 84 9D AD 8C 4A B0 98 B1 BB 88 A2 .....
```



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

Listing Keyword search 5 - LOCK X Keyword search 6 - 19/12/2017 X Keyword search 7 - (\?)[a-zA-Z0-9... X

/Img_data_thef001/vol_v04/Users/JLewi/Music 6 Results

Thumbnail

Name S C O Modified Time Change Time Access Time Created Time

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2017-12-19 17:53:07 PST	2017-12-19 17:53:07 PST	2017-12-19 17:53:07 PST	2017-12-19 13:47:25 PST
[parent folder]				2017-12-19 15:31:10 PST	2017-12-19 15:31:10 PST	2017-12-19 15:18:06 PST	2017-12-19 15:18:06 PST
Beethoven's Symphony No. 9 (Scherzo).wma	2			2008-04-14 04:00:00 PDT	2017-12-15 10:43:48 PST	2017-12-19 17:52:55 PST	2017-12-15 10:43:48 PST
desktop.ini	2			2017-12-19 15:30:50 PST	2017-12-19 15:30:50 PST	2017-12-19 13:49:52 PST	2017-12-19 13:49:52 PST
Mozart's Symphony_no_187.wma	2			2017-12-18 20:01:15 PST	2017-12-19 17:23:29 PST	2017-12-19 17:52:55 PST	2017-12-18 20:01:15 PST
New Stories (Highway Blues).wma	2			2008-04-14 04:00:00 PDT	2017-12-15 10:43:48 PST	2017-12-19 17:53:07 PST	2017-12-19 17:53:07 PST

Save Table as CSV

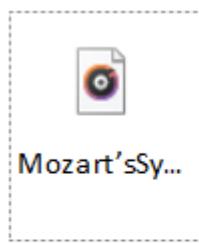
Hex Text Application Message File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Matches on page: - of - Match Page: 1 of 1 Page 100% Reset Text Source: File Text

Board Meeting Minutes (Confidential)
Freescale Semiconductor, Inc.
(Board Meeting Minutes: November 16, 2017)

Board Members:



Board
Meeting...



File List		Size	Type	Date Modified
	\$I30	4	NTFS Index All...	12/20/2017 1:53:07 AM
	Beethoven's Symphony No. 9 (Scherzo)....	600	Regular File	4/14/2008 11:00:00 AM
	Beethoven's Symphony No. 9 (Scherzo)....	1	File Slack	
	desktop.ini	1	Regular File	12/19/2017 11:30:50 PM
	Mozart's Symphony_no_187.wma	24	Regular File	12/19/2017 4:01:15 AM
	New Stories (Highway Blues).wma	743	Regular File	4/14/2008 11:00:00 AM
	New Stories (Highway Blues).wma.FileSla...	2	File Slack	

0000	50 4B 03 04 14 00 06 00-08 00 00 00 21 00 67 73	PK.....!-gs
0010	28 2F 97 01 00 00 28 09-00 00 13 00 08 02 5B 43	(/(.....[C
0020	6F 6E 74 65 6E 74 5F 54-79 70 65 73 5D 2E 78 6D	ontent_Types].xm
0030	6C 20 A2 04 02 28 A0 00-02 00 00 00 00 00 00 00 00	l e-(.....
0040	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0050	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0060	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0070	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0080	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0090	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
00b0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
00c0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
00d0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
00e0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
00f0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0100	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0110	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0120	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
0130	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00

Cursor pos = 0; clus = 4613848; log sec = 36910784; phy sec = 58089152

50 4B 03 04 14 00 06 00
DOCX, PPTX, XLSX

PK.....

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.



- 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

00000	37 7A BC AF 27 1C 00 04-97 AD 30 A6 50 94 03 00	7z!-----0!P---
00010	00 00 00 00 72 00 00 00-00 00 00 BA 66 56 C1r-----rVA
00020	92 D4 86 C5 E5 D5 8A 8B-06 0C 96 04 6E A4 A8 E2	·Ô·Å·Ö-----n·H·â
00030	5F AF 6C 7C 2F F2 07 B6-46 8A 83 3C 9D 73 1E C2	_1!/_ô·¶F·..<·s·Å
00040	7A 85 E8 0B 2E C9 D4 4F-7D 39 1C 2F 99 26 FC BA	z·è..ÉÔO}9·/-·çü°

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
ZZ	37 7A BC AF 27 1C ASCII 7z*	7-Zip compressed file Size: 6 Bytes Offset: 0 Bytes



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	Name	LICENSE.txt	34	Regular File	12/14/2017 5
File Class	Regular File		LICENSE.bbt.FileSlack	3	File Slack	
File Size	234,722		setup_stuff_organizer.exe	4,545	Regular File	12/14/2017 5
Physical Size	237,568		stuff_organizer.exe	230	Regular File	12/19/2017 2
Start Cluster	16,611,977		stuff_organizer.exe.FileSlack	3	File Slack	
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					

```

393b0 F4 67 D3 C0 D2 E9 FF B6-18 E8 C1 30 AC EF A2 54 0g0M0eyq-BÄ0-i=T
393c0 A7 2B 3D 73 D7 6F A0 F6-8D 20 AD E9 1E DA 86 14 $=m=0. .-6.Ü..
393d0 E3 77 TE 26 2D D3 C0 01-DC TE FB 8F E9 78 24 EB ßm=s-DÄ-U-d-exSe
393e0 6C 9E 96 EF 72 A2 7E-B6 2C 3B F6 7C 71 0F 3C l.-mirs-;.olq-<
393f0 29 E7 40 A1 0E 23 CE 46-BF 63 2A 39 70 AB 09 9B )g8i #Ific+9pw...
39400 8A 94 DD B5 33 C2 82 DD-1F CC AB 7F 33 99 65 71 -Bp3A Y i< 3-eq
39410 03 E7 9D 1A D3 70 50 BD-AD F9 47 C1 5A 00 F2 AA --OpP=+dGzZ-*
39420 CD 48 83 87 08 72 BD E6-CE B3 AE FC BB 55 C3 1E 1B ..rmei .dwUH.
39430 94 A6 7F 63 C8 4F 46 55-BD BE 5C 9B 00 82 44 14 ! cFORUM\... D
39440 32 E7 C7 D9 4E 0F A3-03 C1 0A BA 03 AB A9 A7 2-QUN-E-A-i-w-
39450 EE C5 3B 99 DF 75 A4 04-20 1C 88 9A A0 73 65 DC iA; But- ... seU
39460 D5 71 C2 16 17 76 BF FE-A7 7B BE E5 39 F7 BD 4A 0gA- vbps|419+hJ
39470 01 04 06 00 01 09 C3 50-94 00 07 0B 01 00 02 24 .....AP.....
39480 06 F1 07 01 0A 53 07 1E-EB 93 OC EF 9Y CA 18 21 -S...-S...-i...!
39490 21 01 0C 01 00 OC C3 43-94 C3 33 94 00 08 0A 01 !...AcAs....
394a0 48 46 ED 69 00 00 05 01-19 03 00 00 00 11 19 00 HFii.....
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 OA 01 00 d-o-c.....

```

File Explorer View

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
OrphanFile-16				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-17				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-18				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-19				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-20				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-21				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-22				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated
OrphanFile-23				2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	2017-09-27 11:14:08 PDT	0	Unallocated



University
of Victoria

⚠ WinRAR: Diagnostic messages

Message	Archive
⚠ Checksum error in cooking.doc. The file is corrupt	stuff_organizer.zip (F:\forencies\stuff_organizer.zip)

< >

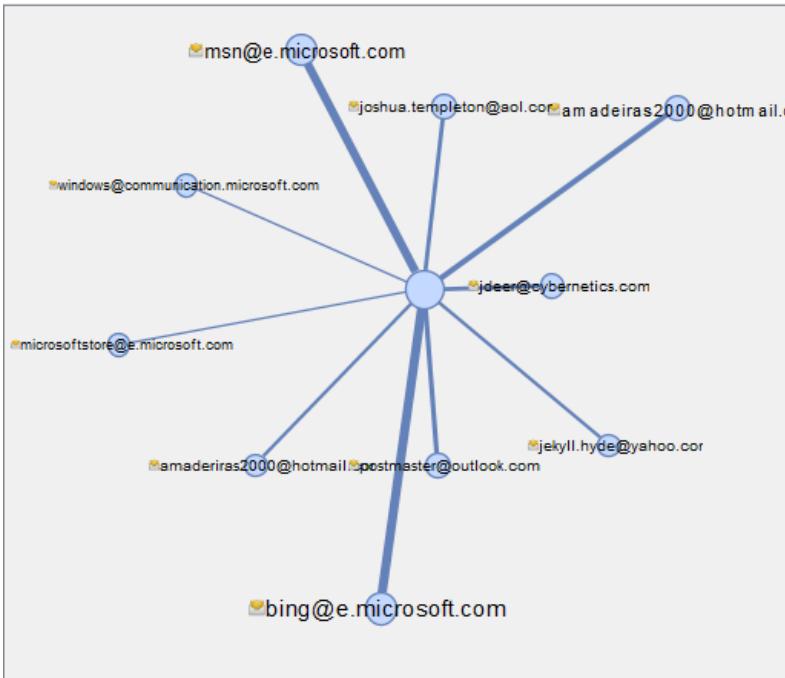
[Close](#) [Break operation](#) [Copy to clipboard](#)



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.





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



Communications Visualization - Editor

Communications Visualization X

Browse **Visualize**

Filters Apply Refresh

Account Types:

- Device
- Email

Uncheck All Check All

Devices:

- data_theft.001

Uncheck All Check All

Date Range (America/Los_Angeles):

Start: November 14, 2016

Account	Device	Type	Items
jlewis4000@outlook.com	data_theft.001	Email	82
bing@e.microsoft.com	data_theft.001	Email	36
msn@e.microsoft.com	data_theft.001	Email	26
amadeiras2000@hotmail.com	data_theft.001	Email	6
postmaster@outlook.com	data_theft.001	Email	4
jdeer@cybernetics.com	data_theft.001	Email	3
joshua.templeton@aol.com	data_theft.001	Email	3
jekyll.hyde@yahoo.com	data_theft.001	Email	2
amaderiras2000@hotmail.com	data_theft.001	Email	2
windows@communication.microsoft.com	data_theft.001	Email	1
microsoftstore@e.microsoft.com	data_theft.001	Email	1

Showing Messages for Thread: Hello again! Threads

From: jlewis4000@outlook.com; 2017-12-21 14:18:18 PST
To: jdeer@cybernetics.com;
CC:
Subject: Hello again!

Headers Text HTML RTF Attachments (0)

Original Text

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

The IP address that email sent to Jdeer is :

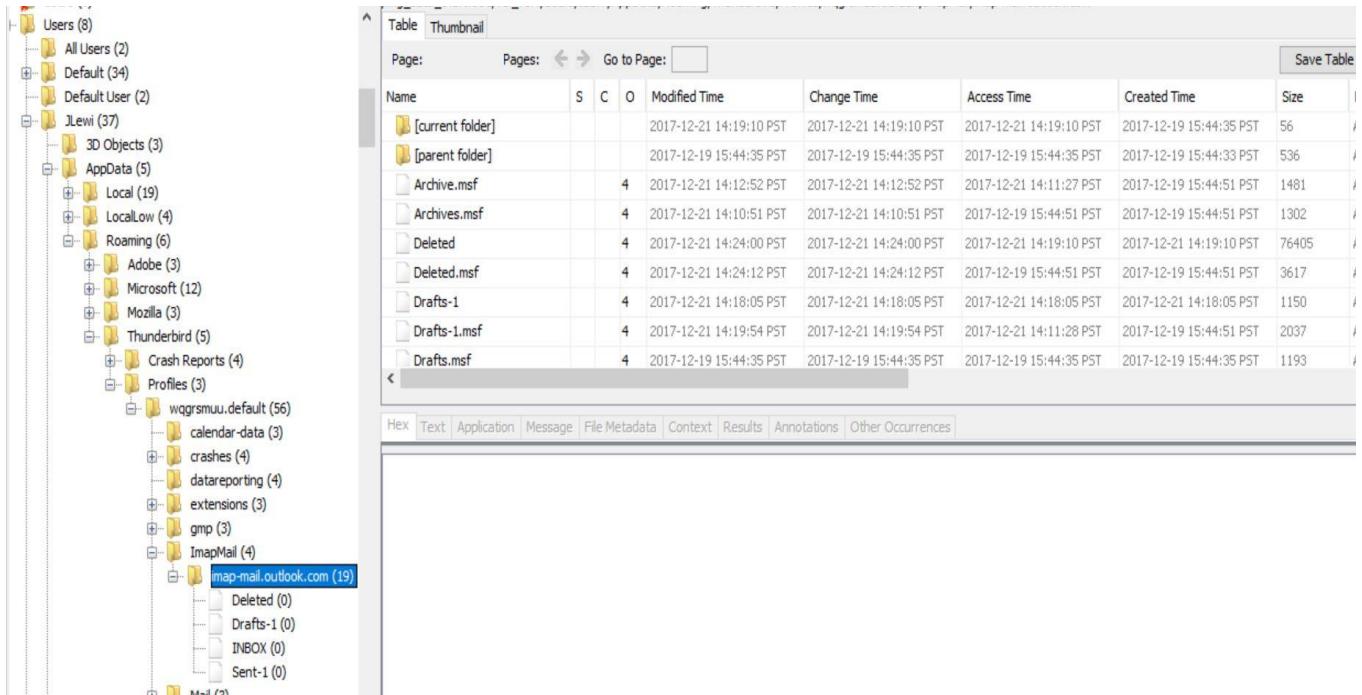
Source File	S	C	O	Keyword	Keyword Preview	Access Time	Change Time
Sent-1				10.172.26.29	d79:1132:87e4:def7] <>10.172.26.29<> by cy4pr16mb1749.na	2017-12-21 14:12:11 PST	2017-12-21 14:23:34 PST

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.



The screenshot displays a digital forensic analysis interface. On the left, a tree view of the file system shows the following structure under 'Users (8)':

- All Users (2)
- Default (34)
- Default User (2)
- JLewi (37)
 - 3D Objects (3)
 - AppData (5)
 - Local (19)
 - LocalLow (4)
 - Roaming (6)
 - Adobe (3)
 - Microsoft (12)
 - Mozilla (3)
 - Thunderbird (5)
 - Crash Reports (4)
 - Profiles (3)
 - wwgrsmuu.default (56)
 - calendar-data (3)
 - crashes (4)
 - datareporting (4)
 - extensions (3)
 - gmp (3)
 - ImapMail (4)
 - imap-mail.outlook.com (19)
 - Deleted (0)
 - Drafts-1 (0)
 - INBOX (0)
 - Sent-1 (0)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2017-12-21 14:19:10 PST	2017-12-21 14:19:10 PST	2017-12-21 14:19:10 PST	2017-12-19 15:44:35 PST	56
[parent folder]				2017-12-19 15:44:35 PST	2017-12-19 15:44:35 PST	2017-12-19 15:44:35 PST	2017-12-19 15:44:33 PST	536
Archive.msf	4			2017-12-21 14:12:52 PST	2017-12-21 14:12:52 PST	2017-12-21 14:11:27 PST	2017-12-19 15:44:51 PST	1481
Archives.msf	4			2017-12-21 14:10:51 PST	2017-12-21 14:10:51 PST	2017-12-19 15:44:51 PST	2017-12-19 15:44:51 PST	1302
Deleted	4			2017-12-21 14:24:00 PST	2017-12-21 14:24:00 PST	2017-12-21 14:19:10 PST	2017-12-21 14:19:10 PST	76405
Deleted.msf	4			2017-12-21 14:24:12 PST	2017-12-21 14:24:12 PST	2017-12-19 15:44:51 PST	2017-12-19 15:44:51 PST	3617
Drafts-1	4			2017-12-21 14:18:05 PST	2017-12-21 14:18:05 PST	2017-12-21 14:18:05 PST	2017-12-21 14:18:05 PST	1150
Drafts-1.msf	4			2017-12-21 14:19:54 PST	2017-12-21 14:19:54 PST	2017-12-21 14:11:28 PST	2017-12-19 15:44:51 PST	2037
Drafts.msf	4			2017-12-19 15:44:35 PST	2017-12-19 15:44:35 PST	2017-12-19 15:44:35 PST	2017-12-19 15:44:35 PST	1193

Hex Text Application Message File Metadata Context Results Annotations Other Occurrences





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-5e6fb6809d6@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.



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 secretary 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.

