CT106-3-1-IFT

INTRODUCTION TO FORENSIC TOOLS AND TECHNIQUES

Table of Contents

Figures

Introduction

Rodger Lewis is CEO at Kericu Company. The Department of justice indicated lewis for altering quarterly statements to boost his company's earnings. Our team ceased his devices, a laptop, and a USB at the crime scene. The forensic investigation team performed all the necessary procedures at the evidence collection time, created a digital clone of his devices, and attached a hash value with files to maintain the integrity. Vice president, Mr. Aiden Paluchi, gave one file and an email to help through the case.
Digital forensic officer Mr. Devdat Kumar will analyze the digital evidence to conclude whether Rodger Lewis is guilty.

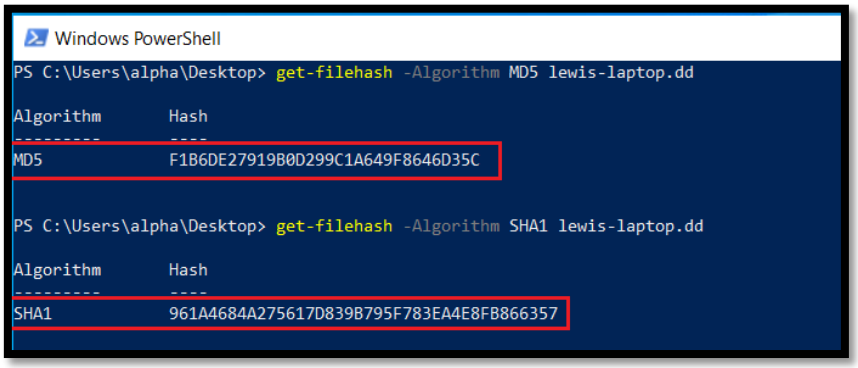


Figure 1 [Windows power shell]

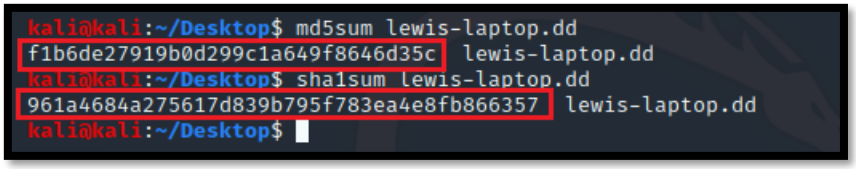


Figure 2 [Linux command terminal]

Before starting any investigation, hash value SHA1 and MD5 of the evidence file was checked using two methods: Windows Power Shell(Figure 1), and Linux terminal(Figure 2), and It was compared with recorded hash values at the time of evidence gathering to ensure the integrity of the process, that no data was altered.

Figure 3 [Evidence and Evidence-copy]

A copy of the evidence (Figure 3) was created, that copy of evidence was examined instead of the original file, to make sure that the original file does not get tampered or corrupted.

Tools:

Figure 4 [Autopsy tool]

Evidence was examined with a forensic tool: Autopsy (Figure 4); it allows multi-user access that users can collaborate on one large case, text can be extracted, and the index searched modules can retrieve files; also, Geolocation and camera information can be extracted, and File Type Sorting can be done too. Tag files with arbitrary tag names are also available, such as 'bookmark' or 'suspicious,' and add comments. There is many more function available in Autopsy tools such as Unicode Strings Extraction, File Type Detection, Android Support, Timeline Analysis, web Artefacts, LNK File Analysis, Email Analysis, Registry Analysis, Robust File System Analysis, Hash Set Filtering, Media Playback, and Thumbnail viewer.

There are other Autopsy alternative tools, such as Encase, FTK, and X ways. However, the Autopsy tool is used preferred at most because of its verity of functionality and easy graphical user interface, but again it still depends on the case type; For example, to find how malware infected a machine, Autopsy is used; To process evidence for fraud cases, Encase is preferred; X-Ways is used to do complex filtering and fast extraction of some evidence. FTK Imager is also a fast and reliable tool.

Laptop analysis

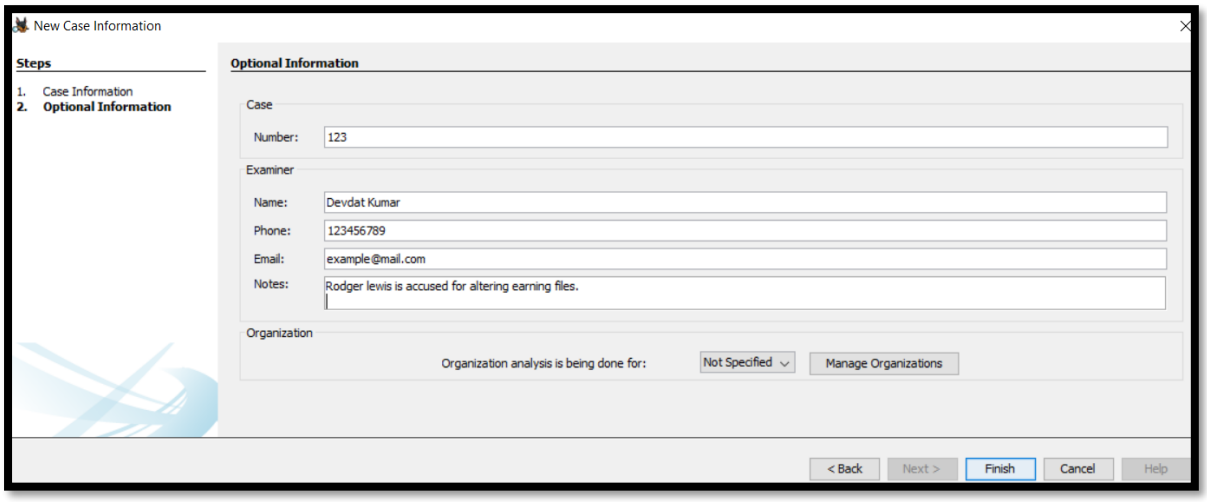


Figure 5 [Case details]

The case (Figure: 5) was named as 'Rodger Lewis Kericu,' case number 123, and examined by digital investigation officer Mr. Devdat Kumar.

Operating System User Account — 8 Results

Table | Thumbnail — Save Table as CSV

Source File	S	C	O	Username	User ID	Path	Data Source	Date Created
software				systemprofile	S-1-5-18	%systemroot%\system32\config\systemprofile	lewis-laptop.dd	
software				LocalService	S-1-5-19	%SystemDrive%\Documents and Settings\LocalService	lewis-laptop.dd	
software				NetworkService	S-1-5-20	%SystemDrive%\Documents and Settings\NetworkService	lewis-laptop.dd	
software				rlewis	S-1-5-21-796845957-73586283-682003330-1003	%SystemDrive%\Documents and Settings\rlewis	lewis-laptop.dd	2004-09-21 22:27:0
SAM				Guest	S-1-5-21-796845957-73586283-682003330-501		lewis-laptop.dd	2004-09-21 04:28:5
SAM				Administrator	S-1-5-21-796845957-73586283-682003330-500		lewis-laptop.dd	2004-09-21 04:28:5
SAM				SUPPORT_388945a0	S-1-5-21-796845957-73586283-682003330-1002		lewis-laptop.dd	2004-09-21 21:56:5
SAM				HelpAssistant	S-1-5-21-796845957-73586283-682003330-1000		lewis-laptop.dd	2004-09-21 21:54:1

Figure 6 [Operating system users]

Operating System User Account list (Figure: 2) was checked to make sure how many people were using the device; there were a couple of users. Most of them were used for internal processes, but Lewis was using the device under the name of user "rlewis." Even if the device user name was under lewis' name, but right now, it cannot be concluded that Lewis was using the device, anyone could have used his device at his non-presence near the device; also, there was no password set up on his operating system user access too.

/img_lewis-laptop.dd/vol_vol2/System Volume Information — 4 Results

Table | Thumbnail — Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
tracking.log			1	2004-09-21 22:28:08 SGT	2004-09-21 22:28:08 SGT	2004-09-23 21:47:07 SGT	2004-09-21 22:05:15 SGT	20480
_restore{457AB8A7-201F-48F3-B434-6DD1792D0D4C}				2004-09-22 22:35:02 SGT	2004-09-22 22:35:02 SGT	2004-09-23 21:44:23 SGT	2004-09-21 22:05:16 SGT	56
[parent folder]				2004-09-23 03:38:10 SGT	2004-09-23 21:44:32 SGT	2004-09-23 21:44:23 SGT	2004-09-21 04:24:48 SGT	56
[current folder]				2004-09-21 22:05:16 SGT	2004-09-21 22:05:16 SGT	2004-09-23 21:44:23 SGT	2004-09-21 22:05:15 SGT	440

Figure 7 [tracking log file]

The Distributed Link Tracking Client service observer's activity on NTFS volumes and saves maintenance information in a file called **tracking.log**, *which is located at the base of each volume in a hidden folder called System Volume Information. (* wondering_chs*)*

The Tracking.log file can be used to analyze the logs of alteration of data in data storage.

/img_lewis-laptop.dd/vol_vol2/RECYCLER/S-1-5-21-796845957-73586283-682003330-1003 — 5 Results

Table | Thumbnail — Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2004-09-23 03:38:12 SGT	2004-09-23 03:38:12 SGT	2004-09-23 22:09:03 SGT	2004-09-23 03:38:10 SGT	344	Allocated	Allocated	unknown
[parent folder]				2004-09-23 03:38:10 SGT	2004-09-23 03:38:10 SGT	2004-09-23 03:38:10 SGT	2004-09-23 03:38:10 SGT	320	Allocated	Allocated	unknown
Dc1.xls			1	2004-09-23 03:31:12 SGT	2004-09-23 03:38:12 SGT	2004-09-23 03:38:12 SGT	2004-09-23 03:31:03 SGT	30208	Allocated	Allocated	unknown
desktop.ini			1	2004-09-23 03:38:10 SGT	2004-09-23 03:38:10 SGT	2004-09-23 03:38:10 SGT	2004-09-23 03:38:10 SGT	65	Allocated	Allocated	unknown
INFO2			1	2004-09-23 11:33:05 SGT	2004-09-23 11:33:05 SGT	2004-09-23 11:33:05 SGT	2004-09-23 03:38:10 SGT	820	Allocated	Allocated	unknown

Figure 8 [Dc1.xls and INFO2]

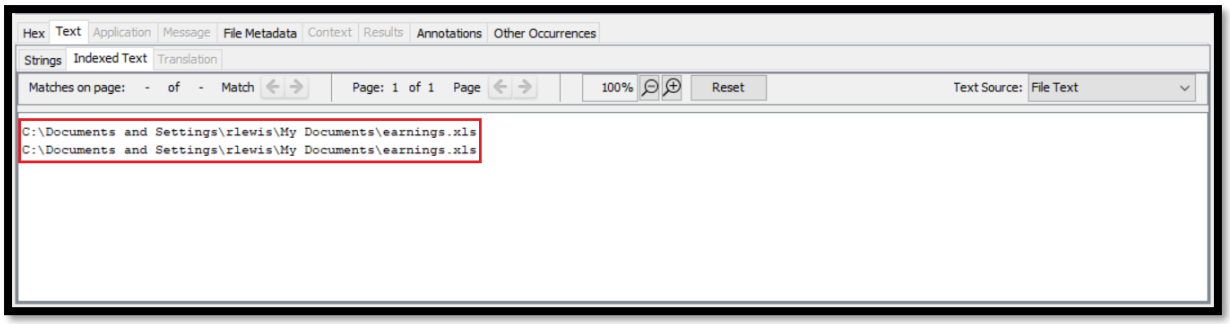


Figure 9 [INFO2 result]

Deleted files (Figure: 8) were searched in the recycler, in case if Lewis deleted any data or files; Lewis two files, the 'Dc1.xls' file, which has data about the company's earnings, and the 'earning.xls' file, which was not available in the recycler, lewis deleted this file using a particular method; but INFO2 (Figure: 9) contained the name and path of 'earnings.xls' file. The path found in INFO2 (Figure: 2) for the deleted file was followed to retrieve the file from the actual path location.

INFO file is located inside the Recycler folder, and it contains a file or folder's complete path and name. (Raymond)

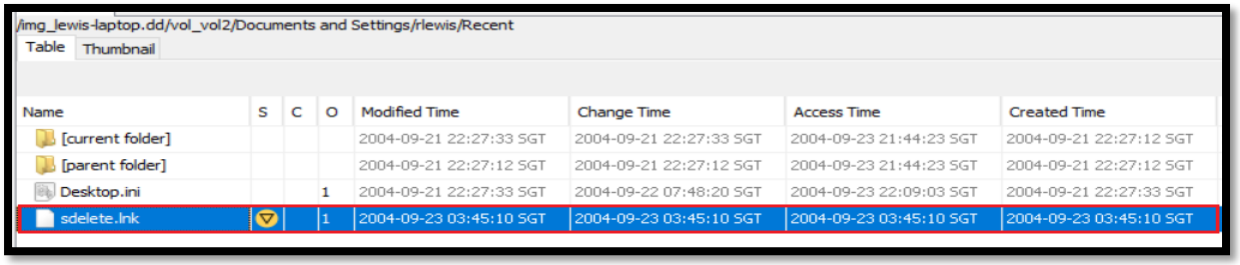
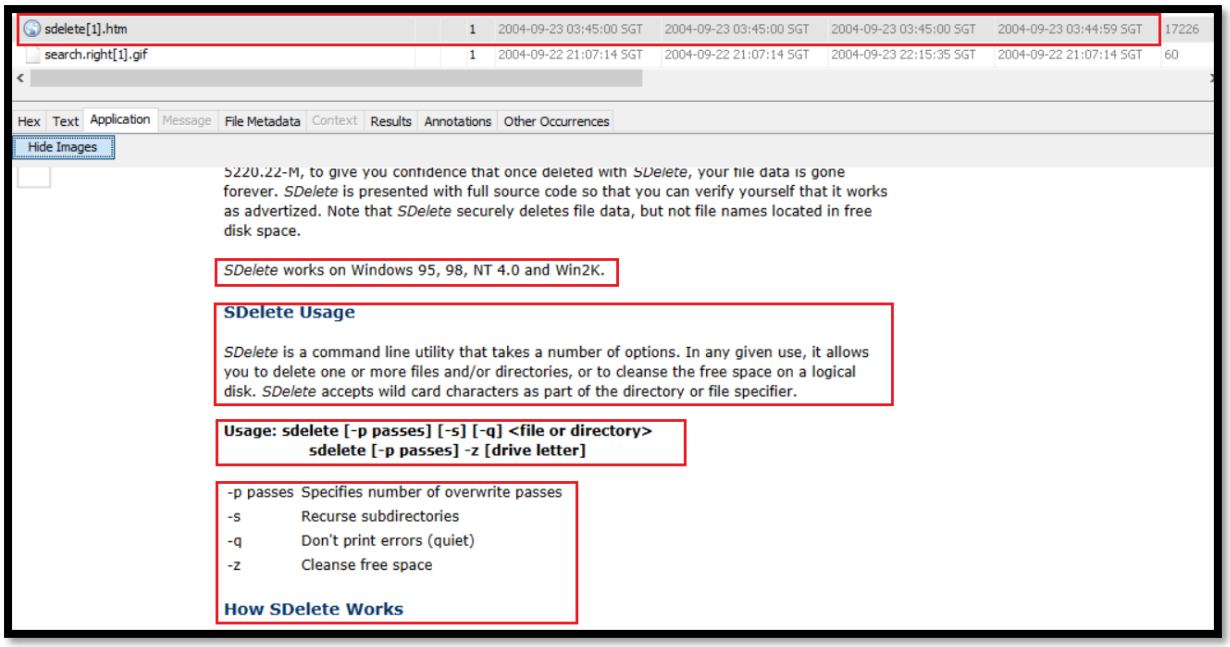


Figure 10 [sdelete.ink]

Figure 11 [sdelete description]

Following the path for earnings.xls, it seems that Lewis deleted the file earnings.xls using the 'sdelete' command (Figure: 10). Sdelete is a command-line utility that uses a command to delete data permanently by overwriting data over it, and data is not retrievable, since lewis used the sdelete command utility to delete 'earnings.xls' file, that why the file cannot be retrieved from his device.

A file named: sdelete.htm (Figure: 12) was found in cookies about 'sdelete' that Lewis searched about 'sdelete' to check how to use the sdelete command-line utility. There is also a time and date that when he searched for this over the internet. Fortunately, there was an image available that shows how graphically the webpage looks.



sdelete[1].htm	1	2004-09-23 03:45:00 SGT	2004-09-23 03:45:00 SGT	2004-09-23 03:45:00 SGT	2004-09-23 03:44:59 SGT	17226
search.right[1].gif	1	2004-09-22 21:07:14 SGT	2004-09-22 21:07:14 SGT	2004-09-23 22:15:35 SGT	2004-09-22 21:07:14 SGT	60

Hex | Text | Application | Message | File Metadata | Context | Results | Annotations | Other Occurrences

Hide Images

5220.22-M, to give you confidence that once deleted with *SDelete*, your file data is gone forever. *SDelete* is presented with full source code so that you can verify yourself that it works as advertized. Note that *SDelete* securely deletes file data, but not file names located in free disk space.

SDelete works on Windows 95, 98, NT 4.0 and Win2K.

SDelete Usage

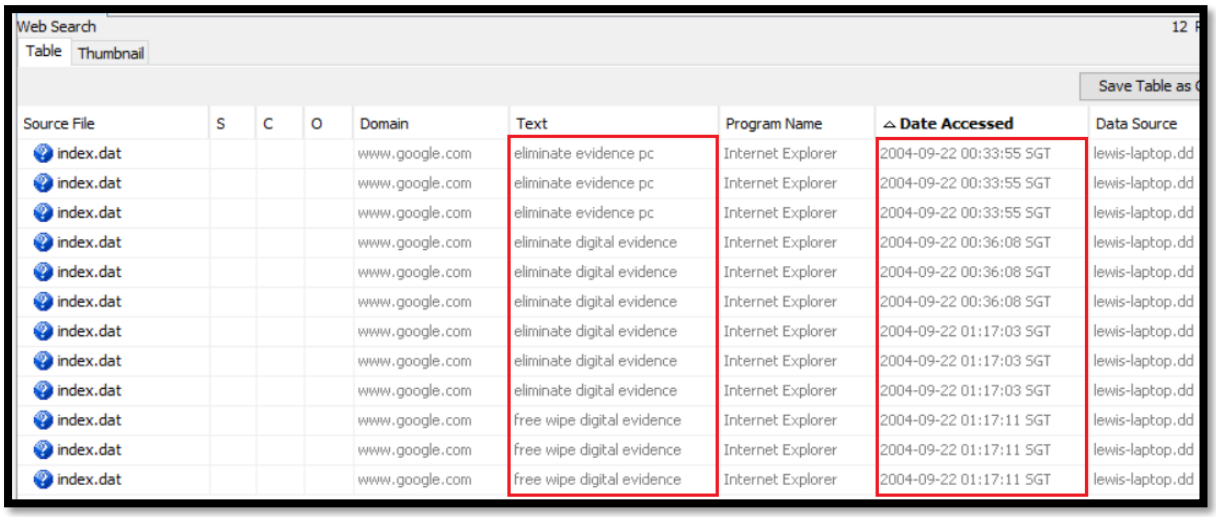
SDelete is a command line utility that takes a number of options. In any given use, it allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk. *SDelete* accepts wild card characters as part of the directory or file specifier.

Usage: sdelete [-p passes] [-s] [-q] <file or directory>
sdelete [-p passes] -z [drive letter]

-p passes	Specifies number of overwrite passes
-s	Recurse subdirectories
-q	Don't print errors (quiet)
-z	Cleanse free space

How SDelete Works

Figure 12 [sdelete search image]

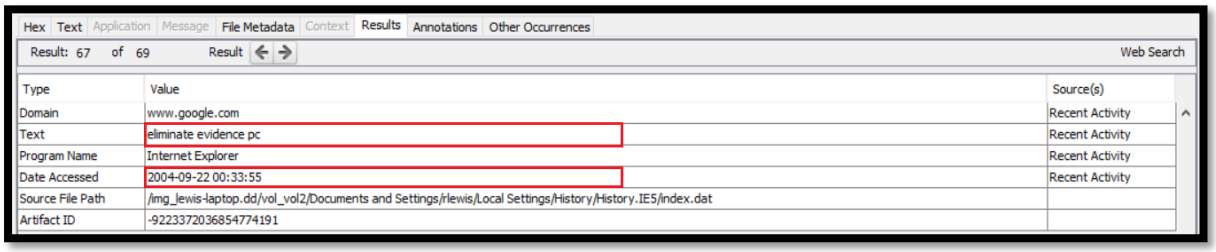


Web Search — Table | Thumbnail — 12

Save Table as

Source File	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
index.dat				www.google.com	eliminate evidence pc	Internet Explorer	2004-09-22 00:33:55 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate evidence pc	Internet Explorer	2004-09-22 00:33:55 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate evidence pc	Internet Explorer	2004-09-22 00:33:55 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate digital evidence	Internet Explorer	2004-09-22 00:36:08 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate digital evidence	Internet Explorer	2004-09-22 00:36:08 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate digital evidence	Internet Explorer	2004-09-22 00:36:08 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate digital evidence	Internet Explorer	2004-09-22 01:17:03 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate digital evidence	Internet Explorer	2004-09-22 01:17:03 SGT	lewis-laptop.dd
index.dat				www.google.com	eliminate digital evidence	Internet Explorer	2004-09-22 01:17:03 SGT	lewis-laptop.dd
index.dat				www.google.com	free wipe digital evidence	Internet Explorer	2004-09-22 01:17:11 SGT	lewis-laptop.dd
index.dat				www.google.com	free wipe digital evidence	Internet Explorer	2004-09-22 01:17:11 SGT	lewis-laptop.dd
index.dat				www.google.com	free wipe digital evidence	Internet Explorer	2004-09-22 01:17:11 SGT	lewis-laptop.dd

Figure 13 [web search]



Hex | Text | Application | Message | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 67 of 69 — Result — Web Search

Type	Value	Source(s)
Domain	www.google.com	Recent Activity
Text	eliminate evidence pc	Recent Activity
Program Name	Internet Explorer	Recent Activity
Date Accessed	2004-09-22 00:33:55	Recent Activity
Source File Path	/img_lewis-laptop.dd/vol_vol2/Documents and Settings/rlewis/Local Settings/History/History.IE5/index.dat	
Artifact ID	-9223372036854774191	

Figure 14 [web search result]

Lewis searched (Figure: 13) for three different keywords multiple times over the domain: www.google.com, on date and time: 2004-09-22 00:33:55 SGT to 01:17:11 SGT, the time trial of the search was followed to find more evidence.

Web History 1558 Re

Table | Thumbnail

Save Table as CS

Source File	...	...	...	URL	Date Accessed	Referrer URL	Program Name	Domain	Username
index.dat			1	http://www.google.com/search?hl=en&ie=UTF-8&q=eliminat...	2004-09-22 00:33:55 SGT		Internet Explorer	www.google.com	rlewis
index.dat			1	http://www.google.com/search?hl=en&ie=UTF-8&q=eliminat...	2004-09-22 00:33:55 SGT		Internet Explorer	www.google.com	rlewis
index.dat			1	http://www.google.com/search?hl=en&ie=UTF-8&q=eliminat...	2004-09-22 00:33:55 SGT		Internet Explorer	www.google.com	
index.dat			1	http://www.evidence-eliminator.com/product.d2w	2004-09-22 00:33:59 SGT		Internet Explorer	www.evidence-eliminator.com	rlewis

Figure 15 [Web history]

Hex | Text | Application | Message | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 31 of 69 Result Web History

Type	Value	Source(s)
URL	http://www.evidence-eliminator.com/product.d2w	Recent Activity
Date Accessed	2004-09-22 00:33:59	Recent Activity
Referrer URL		Recent Activity
Program Name	Internet Explorer	Recent Activity
Domain	www.evidence-eliminator.com	Recent Activity
Username	rlewis	Recent Activity
Source File Path	/img_lewis-laptop.dd/vol_vol2/Documents and Settings/rlewis/Local Settings/History/History.IE5/index.dat	
Artifact ID	-9223372036854775714	

Figure 16 [web search result]

Hex | Text | Application | Message | File Metadata | Context | Results | Annotations | Other Occurrences

Hide Images

Go to Google Home

Web Images Groups News Froogle more »

eliminate evidence pc Search Advanced Search Preferences

Web Results 1 - 10 of about 403,000 for eliminate evidence pc. (0.56 seconds)

Evidence Eliminator - What evidence is on your hard drive?
... If you do not use Evidence Eliminator™ your PC is "a ticking Time Bomb waiting to go off!" Only with Evidence Eliminator™ can you get the protection you ...
www.evidence-eliminator.com/product.d2w - 35k - Cached - Similar pages

Response to Andy@Evidence-Eliminator.com
... my reply, with his message fully quoted: Date: Sat, 02 Feb 2002 08:04:56 -0800 To: "Andy [EE]" <andy@evidence-eliminator.com> From: pchelp <pchelp@pc-help.org ...
www.pc-help.org/opinion/eeemail.htm - 11k - Sep 19, 2004 - Cached - Similar pages

UK Evidence Eliminator - What evidence is on your hard drive?
... Professionally Clean your PC with Evidence Eliminator Software. ... If you use just one program on your PC - make it Evidence Eliminator™ before it's too late! ...
www.evidence-eliminate.co.uk/ - 40k - Cached - Similar pages

Sponsored Links

Evidence Eliminator 6.0
Highly advanced latest version of Evidence Eliminator security. Aff
Evidence-Eliminator.on-sale-now.com

Clear your History 100%
Erase Windows & Internet tracks. New software. Seen on CNN. $22.95!
www.Evidence-Blaster.com

Eliminate hidden PC files
Hard drive cleaning software. Remove incriminating evidence!

Figure 17 [Web search image]

Following the same time trail from the web search (Figure: 14), evidence was searched in the web search history (Figure: 15) at the similar time, as per web history (Figure: 15), lewis searched for few queries to eliminate the evidence earnings.xls; According to web history, it seems lewis visited one other domain, in cookies, a graphical image (Figure: 17) was found in web history, after the search, lewis clicked on the first link (Figure: 16); But the question remains that is it Lewis who is doing all this or someone else who is using this device.

Lewis' emails (Figure: 18) were checked to analyze his conversation to ensure whether lewis is the suspect or not.

3ed36eda-0ccc-11d9-9039-000a9566a9fe@kericu.com

Table | Thumbnail

Source File	S	C	O	Keyword	Keyword Regular Expression
search[1]-slack				3ed36eda-0ccc-11d9-9039-000a9566a9fe@kericu.com	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...
Unalloc_20055_679424_1050238464				3ed36eda-0ccc-11d9-9039-000a9566a9fe@kericu.com	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...
Unalloc_20055_1651871232_3684777472				3ed36eda-0ccc-11d9-9039-000a9566a9fe@kericu.com	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...
Sent Items.dbx			1	3ed36eda-0ccc-11d9-9039-000a9566a9fe@kericu.com	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...
Kericu - Inbox.dbx			1	3ed36eda-0ccc-11d9-9039-000a9566a9fe@kericu.com	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...
4325819222_0[1].jpg-slack				3ed36eda-0ccc-11d9-9039-000a9566a9fe@kericu.com	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([...

Figure 18 [Email source files]

```
Date:       Wed, 22 Sep 2004 18:14:24 -0700 (PDT)
From:       "James Bolton" <jbolton_recruiter@yahoo.com>  Add to Address Book
Subject:    Interview Date
To:         rlewis_kericu@yahoo.com

Rodger,

Our company was very impressed with your resume.  Please send some
dates next week when we could sit down for an interview.  If you have any
questions, please give me a call.
```

Figure 19 [Interview email]

```
[wbk21.tmp, Rodger,<BR>
<BR>
We will be discussing the discrepancies reported in this earnings <BR>
spreadsheet originally submitted last year.  Please be at the meeting <BR>
and come prepared.<BR>
<BR>
<P><HR></P><BR>
<BR>
<BR>
On Sep 22, 2004, at 3:20 PM, Rodger Lewis wrote:<BR>
<BR>
&gt; Joe,<BR>
&gt;<BR>
&gt; I will be unable to make the meeting due to a family event.<BR>
&gt;<BR>
&gt; Please send along any notes you may have from the meeting.<BR>
&gt;<BR>
&gt;<BR>
&gt; ----- Original Message -----<BR>
&gt; From: &quot;Joe Harvey&quot; &lt;jharvey@kericu.com&gt;<BR>
&gt; To: &lt;rlewis@kericu.com&gt;<BR>
&gt; Sent: Wednesday, September 22, 2004 3:18 PM<BR>
&gt; Subject: All Company Meeting<BR>
&gt;<BR>
&gt;<BR>
&gt;&gt; Rodger:<BR>
&gt;&gt;<BR>
&gt;&gt; Just a reminder that our all company meeting will be in Smith Park,<BR>
&gt;&gt; Noon, on Friday.<BR>
&gt;&gt;<BR>
```

Figure 20 [Lewis chat over Email]

```
All Company MeetingD
<AA9F4DFA-0CCD-11D9-9039-000A9566A9FE@kericu.com>Re: All Company Meeting
<3ED36EDA-0CCC-11D9-9039-000A9566A9FE@kericu.com> <001501c4a0d9$3775c930$670
Joe Harveyjharvey@kericu.com
Rodger Lewisrlewis@kericu.comKericu00000002
.  Please be at the meeting
and come prepared.
--Apple-Mail-4--537455129
Content-Transfer-Encoding: base64
Content-Type: application/octet-stream;
          x-unix-mode=0755;
          name="earnings.xls"
Content-Disposition: attachment;
          filename=earnings.xls
```

Figure 21 [earning.xls file Email]

As per this email source files (Figure: 18), lewis was using two emails 'rlewis_kericu@yahoo.com' (Figure: 19) and 'rlewis@kericu.com (Figure: 20).' The time he deleted the file using sdelete command, and the time he searched for evidence eliminator method just sometime before that lewis was talking to Mr. Harvey over one his emails about the All company meeting, "replied: he cannot join the meeting due to family event and ask for notes of the meeting (Figure: 20)," and he received earning.xls (Figure: 21) at that time, he edited that file and deleted it after some time. The time when he replied to Mr. Harvey is almost the same as when he deleted the file, which proves Lewis was the only one who was using his device. Figure: 19 to figure: 21 shows the of what conversation Lewis and Harvey had over their emails.

USB Analysis

Data Sources — 1 Results

Table | Thumbnail — Save Table as CSV

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
lewis-usb.dd	Image	32768000	512	Asia/Singapore	37f1570b-2dc0-4ab3-982f-0c6e536c765a

Figure 22 [Data source]

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
earnings2.xls			3	2003-07-04 12:53:50 SGT	0000-00-00 00:00:00	2003-07-08 00:00:00 SGT	2003-07-08 12:56:34 SGT	35840
earnings-original.xls			3	2003-07-04 12:54:44 SGT	0000-00-00 00:00:00	2003-07-08 00:00:00 SGT	2003-07-08 12:56:34 SGT	35840
Kericu Mission Statement.doc			3	2003-07-04 12:52:08 SGT	0000-00-00 00:00:00	2003-07-08 00:00:00 SGT	2003-07-08 12:56:34 SGT	19456

Figure 23 [files in USB]

Three files (Figure: 23) were found in the USB (Figure: 22) found at Lewis' home; this USB belongs to Lewis because its device ID was found on this laptop too that it was connected to Lewis' laptop. One of the file (Figure: 24) contains information about the mission statement of company Kericu, but the other two files are also about the earnings of the company, one of the file Earning-orignal.xls (Figure: 26), is the same as file Dc1.xls (Figure: 25) found in his laptop containing data about actual and real earnings for the company, another file: earning2.xls (Figure: 27) has altered data by Lewis.

Kericu's Mission Statement:

"To provide for our clients a unique brand of software products coupled with top of the line consulting services to meet their shipping needs."

Kericu's Background:

Kericu is a company founded in 1984 that provides specialized, world-wide overnight shipping. Kericu uses a web portal to ship and track the packages as they are processed. Kericu is a publicly traded company with a bright future. Kericu competes well with the larger shipping companies because of its dedication to client satisfaction.

Figure 24 [Kericu company's vision]

KERICU

Kericu, Inc. Company Earnings, Q2 2003

Expenses	Apr-03	May-03	Jun-03	**Totals**
Sales	$523,532.05	$623,592.03	$521,343.15	$1,668,467.23
Development	$1,235,662.32	$1,482,342.10	$1,831,235.52	$4,549,239.94
HR	$135,234.00	$200,145.23	$152,628.23	$488,007.46
Legal	$523,923.93	$812,351.13	$312,235.19	$1,648,510.25
IT	$2,512,519.84	$2,193,218.18	$1,912,345.73	$6,618,083.75
Security	$102,482.15	$139,258.92	$129,415.93	$371,157.00
Document Destruction	$15,232.93	$10,342.28	$97,123.72	$122,698.93
Admin	$151,910.01	$159,123.91	$130,158.83	$441,192.75
Total	**$5,200,497.23**	**$5,620,373.78**	**$5,086,486.30**	**$15,907,357.31**

Income	Apr-03	May-03	Jun-03	**Totals**
Products	$7,151,801.00	$9,125,152.75	$8,145,198.51	$24,422,152.26
Consulting	$253,925.93	$315,323.93	$293,815.93	$863,065.79
Legal Settlements	$0.00	$0.00	$1,250,000.00	$1,250,000.00
Total	**$7,405,726.93**	**$9,440,476.68**	**$9,689,014.44**	**$26,535,218.05**
Net Earnings	$2,205,229.70	$3,820,102.90	$4,602,528.14	$10,627,860.74

Figure 25 [DC1.xls]

Kericu, Inc. Company Earnings, Q2 2003

Expenses	Apr-03	May-03	Jun-03	**Totals**
Sales	$523,532.05	$623,592.03	$521,343.15	$1,668,467.23
Development	$1,235,662.32	$1,482,342.10	$1,831,235.52	$4,549,239.94
HR	$135,234.00	$200,145.23	$152,628.23	$488,007.46
Legal	$523,923.93	$812,351.13	$312,235.19	$1,648,510.25
IT	$2,512,519.84	$2,193,218.18	$1,912,345.73	$6,618,083.75
Security	$102,482.15	$139,258.92	$129,415.93	$371,157.00
Document Destruction	$15,232.93	$10,342.28	$97,123.72	$122,698.93
Admin	$151,910.01	$159,123.91	$130,158.83	$441,192.75
Total	**$5,200,497.23**	**$5,620,373.78**	**$5,086,486.30**	**$15,907,357.31**

Income	Apr-03	May-03	Jun-03	**Totals**
Products	$7,151,801.00	$9,125,152.75	$8,145,198.51	$24,422,152.26
Consulting	$253,925.93	$315,323.93	$293,815.93	$863,065.79
Legal Settlements	$0.00	$0.00	$1,250,000.00	$1,250,000.00
Total	**$7,405,726.93**	**$9,440,476.68**	**$9,689,014.44**	**$26,535,218.05**
Net Earnings	$2,205,229.70	$3,820,102.90	$4,602,528.14	$10,627,860.74

Figure 26 [Earning-orignal.xls]

Kericu, Inc. Company Earnings, Q2 2003

Expenses	Mar-99	Apr-99	May-99	**Totals**
Sales	$523,532.05	$623,592.03	$521,343.15	$1,668,467.23
Development	$1,235,662.32	$1,482,342.10	$1,831,235.52	$4,549,239.94
HR	$135,234.00	$200,145.23	$152,628.23	$488,007.46
Legal	$523,923.93	$812,351.13	$312,235.19	$1,648,510.25
IT	$2,512,519.84	$2,193,218.18	$1,912,345.73	$6,618,083.75
Security	$102,482.15	$139,258.92	$129,415.93	$371,157.00
Document Destruction	$0.00	$0.00	$0.00	$0.00
Admin	$151,910.01	$159,123.91	$130,158.83	$441,192.75
Total	**$5,185,264.30**	**$5,610,031.50**	**$4,989,362.58**	**$15,784,658.38**

Income	Mar-99	Apr-99	May-99	**Totals**
Products	$9,151,801.00	$10,125,152.75	$12,145,198.51	$31,422,152.26
Consulting	$253,925.93	$315,323.93	$293,815.93	$863,065.79
Legal Settlements	$0.00	$0.00	$1,500,000.00	$1,500,000.00
Total	**$9,405,726.93**	**$10,440,476.68**	**$13,939,014.44**	**$33,785,218.05**
Net Earnings	$4,220,462.63	$4,830,445.18	$8,949,651.86	$18,000,559.67

Figure 27 [Earning2.xls]

Case Analysis

Lewis is found guilty according to the data retrieved from laptop and USB. In quarterly statements Lewis changed the dates for all the months for both income and expense, also decreased the expenses [from $15,907,357.31 to $15,784,658.38} and increased the income {from 26,535,218.05 to 33,785,218.15} to boost company's earnings. He made a massive blunder in earnings and expanses of about approximately $7.3 million {$7,372,698.93} in the net earnings {from $18,000,559.67 to $10,627860.74}.

References

Social.technet.microsoft.com. 2020. *Tracking.Log Mystery*. [online] Available at: <https://social.technet.microsoft.com/Forums/windows/en-US/f09051b2-f5f3-4a19-b620-d2f71b5f0833/trackinglog-mystery> [Accessed 5 September 2020].

Raymond.CC Blog. 2020. *What Is INFO2 File Hidden In Recycled Or Recycler Folder? • Raymond.CC*. [online] Available at: <https://www.raymond.cc/blog/what-is-info2-file-hidden-in-recycled-or-recycler-folder/> [Accessed 5 September 2020].

Chan, K., 2020. *Encase Vs Autopsy Vs Xways*. [online] Securityisfun.net. Available at: <http://www.securityisfun.net/2014/02/encase-vs-autopsy-vs-xways.html> [Accessed 5 September 2020].

Latest Hacking News. 2020. *Autopsy - A Digital Forensic Tool - Latest Hacking News*. [online] Available at: <https://latesthackingnews.com/2017/01/02/autopsy-digital-forensic-tool/> [Accessed 5 September 2020].

Unodc.org. 2020. *Cybercrime Module 6 Key Issues: Handling Of Digital Evidence*. [online] Available at: <https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html> [Accessed 5 September 2020].