TecbizFrisman
DISCOVER. DETECT. DETER.

Computer Forensic Report

Case No: 2010888

22 September 2010

This report contains 9 pages

Table of Contents

1 Purpose and Organization of this Report

1.1 This computer forensic report states the key observations, analysis and opinions from the work performed by Tecbiz Frisman Pte Ltd (Tecbiz Frisman) in reviewing the forensic image of the hard disk drive of the exhibit 2010888-E01 belonging to ABC Company Pte Ltd (ABC Company). Tecbiz Frisman has issued the Exhibit Management and Image Acquisition Report for this exhibit dated 5 August 2010.

1.2 Observations and discovery are made on data on the forensic image of the hard disk drive 2010888-E01HD1. Our observations, analysis and opinions are organized into different sections and sub-titles for ease of reading.

1.3 Section 2 contains the executive summary on our opinions from the forensic review. The subsequent sections describe the observations and analysis of relevant data discovered during the review.

1.4 The sub-titles in the sections are:

1.4.1 Observation: describes the data noted during the reviews; and

1.4.2 Analysis and Opinion: describes our analysis and opinions on a specific set of data.

1.5 Appendices referred to in this report are enclosed at the last section of this report.

2 Executive Summary

2.1 We were instructed that the exhibit 2010888-E01 was the desktop computer used by Ray Lin (Ray) when he was an employee of ABC Company until his resignation on 27 May 2010. The hard disk drive with exhibit reference number 2010888-E01HD1, which was attached to exhibit 2010888-E01 was imaged by Tecbiz Frisman.

2.2 We were instructed that user id 'rlin' is assigned and used by Ray during his course of employment.

2.3 We are instructed to examine 2010888-E01HD1 to determine the following:

2.3.1 To establish if Ray copied out files containing ABC Company's proprietary and confidential information without ABC Company's consent from December 2009 to prior to his resignation.

2.4 Based on the data reviewed and analyzed on exhibit 2010888-E01HD1, which is outlined in Section 3, it is highly probable the user 'rlin' has copied many files into external storage media.

2.5 We were instructed that the files with serial number 1, 4 and 32 in Appendix C of this report are proprietary and confidential information of ABC Company. We were instructed that if these files have been copied out, it has been done without the consent of ABC Company.

2.6 In summary, it is highly probable that user 'rlin' has copied many files into at least 6 external storage media devices from December 2009 onwards prior to his resignation; and at least three (3) of the files in the external storage media devices contain proprietary and confidential information of ABC Company.

3 Forensic Examinations on External Storage Devices

Observation 1

3.1 We have analyzed the data in the Personal Storage Table (.PST) files of the exhibit 2010888-E01.

3.2 We noted there is an email correspondence with subject title "答复_ card" dated 19 December 2009 8:50 AM in the PST file in Ray's user account located at C:\Documents and Settings\rlin\Local Settings\Application Data\Microsoft\Outlook\archive.pst. The contents are in Chinese and the contents of the email appears to be of Ray airing his grievances to one Candy Lee. A copy of the email is enclosed in Appendix A.

Observation 2

3.3 To obtain the list and usage of external storage devices attached to the exhibit 2010888-E01 that can be associated to user 'rlin', we have analyzed the data in the following registry hives:

3.3.1 The mounted devices registry keys ControlSet001\Enum\USBStor in the Windows system registry file at C:\WINDOWS\system32\config\system of exhibit 2010888-E01; and

3.3.2 The registry hives $$$PROTO.HIV\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 in the Windows user registry file associated with the user 'rlin' located at C:\Documents and Settings\rlin\NTUSER.DAT.

3.4 The list of external storage devices attached to exhibit 2010888-E01 that can be associated to the user 'rlin' is enclosed in Appendix B.

Analysis & Opinion 1

3.5 It is highly probable that there are at least 27 external storage devices that have been attached to the desktop computer by the user 'rlin' between the period 31 October 2008 and 26 May 2010.

3.6 It is probable to conclude that user ‘rlin’ has connected these external storage devices to copy/move or to access files.

Observation 3

3.7 We have analyzed the data of links files residing on exhibit 2010888-E01HD1 that show accesses to files and folders residing in external storage devices attached to the desktop computer.

3.8 There are many links showing accesses to files\folders on external storage devices attached to the desktop computer. Some of these files have names that resemble work related documents. The list of link files that were last written from December 2009 onwards and refers to actual files residing on G:\ drive of external storage media is enclosed in Appendix C.

3.9 These link files reside in the directory belonging to user ‘rlin’. Data in the link files indicate that there are six unique external storage media devices assigned with the drive letter G:\ attached to the desktop computer since December 2009 onwards by user ‘rlin’.

Analysis & Opinion 2

3.10 Based on Observations 1, 2 and 3 it is highly probable that user ‘rlin’ has copied many files into at least 6 external storage media devices from December 2009 to prior to his resignation; and at least 3 of the files in the external storage media devices contains proprietary and confidential information of ABC Company.

Appendix A: Copy of email correspondence with subject “答复: card”

From: Lee, Candy [Candy.Lee@abccompany.com]

Date: 18 December 2009 8:50 AM

To: Ray, Lin<Ray.Lin@abccompany.com>;

Subject: 答复: card

兄弟，别多说了，不容易。。。我明白。放松点

Regards,

Candy Lee

发件人: Ray, Lin
发送时间: 2009 年 12 月 17 日 22:10
收件人: Lee, Candy
主题: 答复: card

Candy,

... Contents of email showing Ray airing grievances to Candy Lee

Regards,

Ray

Appendix B: List of External Storage Devices attached to Exhibit 2010888-E01

No.	Vendor	Product	Serial No	First Time Connected (USBStor)	Last Time Connected (MountPoints2)
1	Ven_USB_2.0	Prod_Flash_Disk	1818590112591700	31 Oct 2008 4:27:50 PM	31 Oct 2008 4:28:01 PM
2	Ven_CBM	Prod_Flash_Disk	2714490022B5F000	03 Dec 2008 4:01:25 PM	03 Dec 2008 4:01:35 PM
3	Ven_USB_2.0	Prod_Flash_Disk	32084579354	29 Dec 2008 11:45:07 AM	29 Dec 2008 11:45:16 AM
4	Ven_CBM	Prod_USB2.0	232147007F3BC703	07 Jan 2009 9:15:43 AM	07 Jan 2009 9:15:49 AM
5	Ven_USB_2.0	Prod_Flash_Disk	31243881712	05 Mar 2009 2:45:47 PM	05 Mar 2009 2:45:54 PM
20	Ven_CBM	Prod_USB2.0	231726004F13E501	25 Nov 2009 2:22:19 PM	25 Nov 2009 2:22:26 PM
21	Ven_CBM	Prod_Flash_Disk	2713170082338B07	25 Nov 2009 3:15:58 PM	25 Nov 2009 3:16:04 PM
22	Ven_CBM	Prod_USB2.0	23222300277E6901	25 Nov 2009 2:04:59 PM	25 Nov 2009 4:19:53 PM
23	Ven_CBM	Prod_USB2.0	2315360078130300	15 Mar 2010 1:42:48 PM	15 Mar 2010 1:42:54 PM
24	Ven_	Prod_	3fbf5000-7351-0801-3575-680126162100	18 Mar 2010 12:19:54 AM	18 Mar 2010 12:20:01 AM
25	Ven_Kingston	Prod_DataTraveler_2.0	899801162008011514252D03	13 Apr 2010 5:40:06 PM	13 Apr 2010 5:40:14 PM
26	Ven_USB_Mass	Prod_Storage_Device	812320090519	17 May 2010 4:08:59 PM	20 May 2010 5:18:31 PM
27	Ven_CBM	Prod_USB2.0	231510006014AE00	26 May 2010 9:24:43 AM	26 May 2010 9:24:50 AM

This is just a sample. The table has been intentionally shortened.

TecbizFrisman
DISCOVER. DETECT. DETER.

Appendix C: List of link files referring to actual files residing on G:\ with Link File Last Written Date on or after Dec 2009

S/N	Link File Path	Link File Created	Link File Last Written	G:\ Drive Volume Serial	G:\ Drive Volume Label	Target File\Folder in G:\ Drive	Target File Logical Size in Bytes	Target File Created	Target File Last Written
1	C\Documents and Settings\rlin\Application Data\Microsoft\Office\Recent\技术会议纪要-200904.LNK	13 Apr 2010 5:42:59 PM	13 Apr 2010 5:42:59 PM	34 33 32 31	KINGSTON	G:\ABC Company\技术会议纪要-200904	0	14 Dec 2009 12:35:31 PM	14 Dec 2009 12:35:32 PM
2	C\Documents and Settings\rlin\Recent\Comments on previous experienc v1.lnk	13 Apr 2010 5:42:58 PM	13 Apr 2010 5:43:10 PM	34 33 32 31	KINGSTON	G:\ABC Company\技术会议纪要-200904\Comments on previous experienc v1.doc	29696	14 Dec 2009 12:35:31 PM	19 Aug 2009 8:06:52 AM
4	C\Documents and Settings\rlin\Recent\Technical Specification.lnk	13 Apr 2010 5:44:12 PM	13 Apr 2010 5:44:23 PM	34 33 32 31	KINGSTON	G:\Technical Specification.doc	4131840	20 Dec 2009 10:18:37 PM	21 Dec 2009 12:50:20 AM
5	C\Documents and Settings\rlin\Recent\Offer Let[1]...lnk	12 May 2010 10:52:16 AM	12 May 2010 10:52:16 AM	B0 82 E7 2B	G	G:\Offer Let[1]...pdf	77185	10 May 2010 8:10:45 PM	10 May 2010 8:10:52 PM
10	C\Documents and Settings\rlin\Recent\Tool - H.S1.A3A.N1-cs.lnk	15 May 2010 11:02:20 PM	15 May 2010 11:02:23 PM	DC F9 24 0B	lwg	G:\New Folder\培训\KAM1-Tools-cs\Tool - H.S1.A3A.N1-cs.ppt	212480	12 May 2010 8:56:49 PM	17 Mar 2009 10:03:02 AM
11	C\Documents and Settings\rlin\Application Data\Microsoft\Office\Recent\KAM1-Tools-cs.LNK	01 Jan 2010 12:24:09 AM	15 May 2010 11:02:35 PM	DC F9 24 0B	lwg	G:\New Folder\培训\KAM1-Tools-cs	0	12 May 2010 8:56:49 PM	12 May 2010 8:56:50 PM
12	C\Documents and Settings\rlin\Recent\KAM1-Tools-cs.lnk	15 May 2010 11:02:04 PM	15 May 2010 11:02:43 PM	DC F9 24 0B	lwg	G:\New Folder\培训\KAM1-Tools-cs	0	12 May 2010 8:56:49 PM	12 May 2010 8:56:50 PM
13	C\Documents and Settings\rlin\Recent\Tool - T.S1.A1B.N2-cs (Excel Worksheet).lnk	15 May 2010 11:02:33 PM	15 May 2010 11:02:43 PM	DC F9 24 0B	lwg	G:\New Folder\培训\KAM1-Tools-cs\Tool - T.S1.A1B.N2-cs (Excel Worksheet).xls	17920	12 May 2010 8:56:49 PM	17 May 2007 5:21:52 PM
32	C\Documents and Settings\rlin\Recent\报价单-ABC 销售公司.lnk	26 May 2010 9:24:55 AM	26 May 2010 9:24:55 AM	FA EF 29 C1	G	G:\报价单-ABC 销售公司.pdf	135143	26 May 2010 9:23:48 AM	26 May 2010 9:23:36 AM

This is just a sample. The table has been intentionally shortened.