FORENSIC ANALYSIS REPORT

Case: HAY 2016 05 11 14

Client: FinanceCorp

Client Contact: Jane Smith , 713-265-1524, JSmith@fc.com

Client Case: Anna Johnson

**Assignment**

HAYSTACKID was engaged to forensically analyze the forensic image of a computer and cell phone used by Anna Johnson while employed by FinanceCorp. The forensic images were supplied by FinanceCorp. Forensic analysis should cover Ms. Johnson’s activities for the last 60 days of her employment. Ms. Johnson’s last day at FinanceCorp was reported to be June 10, 2016. The specified date range for all searches and reports will be between April 10, 2016 and June 10, 2016, inclusive.

**Tools Used During Examination**

1. EnCase Forensic, 64 bit, Version 7.12.01.
2. Internet Evidence Finder, Version 6.8

**Objects of Examination**

1. Forensic image of a FinanceCorp Mac laptop computer reported to have been assigned to Anna Johnson.
2. Anna Johnson’s Outlook email messages from .OST file.

**Appendices**

1. Appendix A. About the Examiner

**Exhibits**

1. Exhibit 1. Excel Spreadsheet “USB Devices of Interest”.
2. Exhibit 2. Excel Spreadsheet “Shellbags Report”.
3. Exhibit 3. Excel Spreadsheet “Link files 06/06/2016”.
4. Exhibit 4. Excel Spreadsheet “Recently Accessed Documents”.
5. Exhibit 5. Zip Folder “Emails of Interest”.
6. Exhibit 6. Excel Spreadsheet “Recycle Bin Report”.
7. Exhibit 7. Excel Spreadsheet “Recent Files”

**User Accounts**

Besides the default administrative accounts, there were four user accounts observed within the Users directory.

|  |  |  |  |
| --- | --- | --- | --- |
| User Account | SID# | Activity Start Date | Activity End Date |
| johnson | 320750 | 12/12/2014 |  |
| smith | 278591 | 09/15/2015 | 09/17/2015 |
| sk | 307691 | 09/15/2015 | 05/13/2016 |
| lcranston | 29951 |  |  |

The creation date of the ajohnson user account folder is listed as 12/12/2014. The last folder access activity for the ajohnson user account was listed as 06/21/2016. This activity was most likely caused by an automated operating system function such as a disk defragmentation of virus scan. The last document access activity observed on the ajohnson user account was listed as 06/13/2016 system activity for the for folders for the ajohnson user account is listed as 06/21/2016.

**Software Installations**

Registry records show that an executable file was last written on 05/23/2016. The executable was msoxmled.exe. Msoxmled.exe is a file developed by Microsoft and is associated with MSDN disc 2029 for the Windows operating system. Its process is known as XML editor and the application using this process is Microsoft office info path. It appears that this executable program was updated and is part of the Microsoft Office 12 software package.

**Email Addresses**

Custodian used the following email addresses:

1. johnson@fc.com
2. anna.johnson@rocketmail.com

**External Devices**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Make** | **Model** | **Mapped Drive Letter** | **S/N** | **First Plug-In (UTC -5:00)** | **Last Plug-In (UTC -5:00)** | **User Account** |
| Emtec | 2.0 USB Device |  | 9000643604276A45 | 6/6/2016 5:12:25 PM | 6/6/2016 5:12:25 PM | ajohnson |
| Emtec | 2.0 USB Device | “D” | 9000643604276A45 | 06/08/2016 01:04:04 PM | 6/8/2016 1:05:03 PM | ajohnson |
| Emtec | 2.0 USB Device |  | 9000643604276A45 |  | 06/10/2016 09:01:52 AM | ajohnson |
| Kingston | DT 101 G2 |  | 0013729940C4EBA145160224 | 12/16/2014 05:14:05PM | 12/16/2014 05:21:03PM | ajohnson |
| Kingston | DT 101 G2 |  | 0013729940C4EBA145160224 |  | 06/06/2016 09:03:14 AM | ajohnson |
| Kingston | DT 101 G2 |  | 0013729940C4EBA145160224 |  | 6/10/2016 9:01:52 AM |  |
| Toshiba | USB 3.0 |  | 20160212000813F | 06/13/2016 11:29:06AM | 06/13/2016 11:29:06AM | Not Listed |

From artifacts parsed from the registry, backup registry, and link files it appears as though there were 3 occasions of interest where USB external drives were connected to the ajohnson user account. The connections occurred on June 6th, June 8th, and June 10th, 2016.

The Emtec USB 2.0 device, serial number 9000643604276A45, was connected June 6, 2016 at 5:12pm, June 8, 2016 at 1:05pm, and June 10, 9:01am. This USB device was mapped as drive letter “D” when it was connected to the computer on June 8, 2016 at 1:05pm.

The Kingston USB device, serial number 0013729940C4EBA145160224, was connected June 6, 2016 at 9:03am, and June 10, 2016 at 9:01am. This USB device did not have a mapped drive letter parsed out of the registry files.

The Toshiba USB device, serial number 20160212000813F, was connected on June 13, 2016 at 11:29am. This USB device did not have a mapped drive letter parsed out of the registry files. It should be noted that the “Employee Info – Copy” and the “Sales Meeting – Copy” desktop folders, on ajohnson’s user account, were created on June 13, 2016 at 11:32am. (*Exhibit 1*)

**Shellbag Analysis**

Shellbag is a Windows registry key that stores the user’s preferences for how a file or folder opens on the user’s desktop. The Shellbag registry key is only created for folders that have been opened and closed in Windows Explorer by the user. In other words, the Shellbag registry key for a given folder indicates that the user’s account opened/viewed that folder.

In the examination of the artifact viewed in the Shellbag registry key it was observed that a “D” drive was connected to the Johnson computer on three specific dates, June 6th, June 8th, and June 13th, 2016

The table below shows the “D” drive connection and the folders visited on the dated mentioned above. (*Exhibit 2*)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Path** | **Last Explored Date/Time - (UTC-5:00)** | **File System Last Modified Date/Time - (UTC-5:00)** | **File System Last Accessed Date/Time - (UTC-5:00)** | **File System Created Date/Time - (UTC-5:00)** |
| D:\FCU\ |  | 06/06/2016 08:59:24 AM | 06/06/2016 12:00:00 AM | 06/06/2016 05:44:24 PM |
| D:\BDD Signed Agreements\ |  | 06/06/2016 05:52:10 PM | 06/06/2016 12:00:00 AM | 06/06/2016 05:52:10 PM |
| D:\Customer Emails\ |  | 06/06/2016 06:00:00 PM | 06/06/2016 12:00:00 AM | 06/06/2016 06:00:00 PM |
| D:\Customer Conversations\ |  | 06/06/2016 06:00:00 PM | 06/06/2016 12:00:00 AM | 06/06/2016 06:00:00 PM |
| D:\Customer Conversations\JOSS\ | 06/06/2016 06:17:49 PM | 06/06/2016 06:17:48 PM | 06/06/2016 12:00:00 AM | 06/06/2016 06:17:48 PM |
| D:\Important Web Pages\ |  | 06/06/2016 06:47:00 PM | 06/06/2016 12:00:00 AM | 06/06/2016 06:47:00 PM |
| D:\PICS\ |  | 06/08/2016 01:04:32 PM | 06/08/2016 12:00:00 AM | 06/08/2016 01:04:32 PM |
| D:\New folder\ |  | 06/13/2016 11:29:56 AM | 06/13/2016 11:29:56 AM | 06/13/2016 11:29:56 AM |
| D:\Anna\ | 06/13/2016 11:29:57 AM | 06/13/2016 11:29:56 AM | 06/13/2016 11:29:56 AM | 06/13/2016 11:29:56 AM |
| D:\Anna\Employment\ |  | 06/13/2016 11:30:04 AM | 06/13/2016 11:30:04 AM | 06/13/2016 11:30:04 AM |
| D:\Anna\Johnson, Anna\ |  | 06/13/2016 11:30:40 AM | 06/13/2016 11:30:40 AM | 06/13/2016 11:30:40 AM |
| D:\Anna\Employee Info - Copy\ |  | 06/13/2016 11:32:36 AM | 06/13/2016 11:32:36 AM | 06/13/2016 11:32:34 AM |
| D:\Anna\Sales Meetings - Copy\ |  | 06/13/2016 11:32:36 AM | 06/13/2016 11:32:36 AM | 06/13/2016 11:32:36 AM |
| D:\Anna\FCU\ | 06/13/2016 11:35:54 AM | 06/13/2016 11:33:38 AM | 06/13/2016 11:33:38 AM | 06/13/2016 11:32:36 AM |

It should be noted that the two folders highlighted above appear to be copies of files that already existed on the ajohnson’s user account desktop.

The “Sales Meetings” file on the desktop shows a creation date of 06/22/2015 and currently has a logical file size of 4,096 bites. According to the Shellbag analysis, the “Sales Meetings – Copy” was created on the “D” drive on 06/13/2016 at 11:32:13am EDT and had a logical file size of 4,096 bites.

The “Employee Info” file on the desktop shows a creation date of 12/12/2014 and currently has a logical file size of 12,288 bites. According to the Shellbag analysis the “Employee Info - Copy” was created on the “D” drive, on 06/13/2016 at 11:32:14am and had a logical file size of 8,192 bites. These two files were then deleted from the ajohnson desktop and placed in the Recycle bin on June 13, 2016 at 11:36am.

Although the Toshiba thumb drive was never mapped with the “D” drive letter, the Shellbag analysis shows that activity on 06/13/2016 started at 11:29:56am which is 50 seconds after the Registry show the Toshiba thumb drive being connected to the ajohnson computer.

**Transfer to External Devices**

**Activity on June 6, 2016**

The external USB device with serial number 0013729940C4EBA145160224 was connected to the computer at 9:03am. Through analysis of the registry files it was identified as a Kingston brand external USB device. It is unknown what files may have been copied to or from this device but the link file analysis shows that the following files were accessed by the ajohnson account user between 9:04 and 9:07am. (*Exhibit 3*)

1. C:\Users\johnson\Desktop\Employment\CART
2. C:\Users\johnson\Desktop\Employment\CART\Monthly Finance Report
3. C:\Users\johnson\Desktop\Employment\Invoices
4. C:\Users\johnson\Desktop\Employment\Monthly Revenue Breakdown
5. C:\Users\johnson\Desktop\Employment\Personal\2014 CONTRACTS AND AGREEMENTS.pdf
6. C:\Users\johnson\Desktop\Employment\Personal
7. C:\Users\johnson\Desktop\Employment\Personal\2014\_Employment\_Services\_Account\_Manager\_Plan.pdf

The thumb drive with serial number 9000643604276A45 was connected to the computer at 5:12pm. Through link file analysis this thumb drive was identified as am Emtec brand external USB device. From the Shellbag and Recent folder reports it appears that certain files were accessed on a thumb drive between 5:44 and 6:47pm. Although the Shellbag analysis does not identify the individual device that was accessed, I believe the device may have been the Emtec external USB device. In order to determine if the Emtec drive was the device accessed between 5:44 and 6:47pm, I would need to examine the Emtec drive. The files accessed on this thumb drive include the following: (*Exhibit 4*)

1. D:\FCU\
2. D:\Customer Emails\
3. D:\Customer Conversations\
4. D:\Customer Conversations\MOSS\
5. D:\Important Web Pages\
6. EMTEC (D)

**Activity on June 8, 2016**

The thumb drive with serial number 9000643604276A45 was connected to the computer at 1:04pm. Through link file analysis this thumb drive was identified as am Emtec brand external USB device. The registry shows that this drive was mapped as drive letter “D”. From the shellbag report listed above it appears that a file was accessed on a thumb drive at 1:04pm. The file accessed on the thumb drive was as follows:

1. D:\PICS\

**Activity on June 10, 2016**

The thumb drive with serial number 9000643604276A45 was connected to the computer at 9:01am. Through link file analysis this thumb drive was identified as am Emtec brand external USB device. It is unknown if any files were copied to or from this thumb drive. There are no link file artifacts for that date and time.

**Activity on June 13, 2016**

The thumb drive with serial number 20160212000813F was connected to the computer at 11:29am. Through analysis of the registry files the device was identified as a Toshiba brand external USB device. From the Shellbag and Recent folder reports it appears that certain files were accessed on the external USB device between 11:29 and 11:33am. Although the Shellbag analysis does not identify the individual device that was accessed, I believe the device may have been the Toshiba external USB device. In order to determine if the Toshiba drive was the device accessed between 11:29 and 11:33am, I would need to examine the Toshiba drive. The files accessed on this thumb drive include the following:

1. D:\New folder\
2. D:\Anna\
3. D:\Anna\Employment\
4. D:\Anna\Johnson, Anna\
5. D:\Anna\Employee Info - Copy\
6. D:\Anna\Sales Meetings - Copy\
7. D:\Anna\FCU\

**Emails**

There were two email repositories that were examined. One repository was located on the computer in the form of an OST files. The second repository was supplied by FinanceCorp’s forensic lab personnel and was reported to be the .PST file from the network Exchange server.

The specified date range filter was applied to the email repositories. Once the date range was applied, two email files of interest were observed.

The emails of interest were located in the following path:

johnson@fc.com - Default Outlook Profile.ost\Root folder\Root - Mailbox\Sync Issues\Local Failures\Customer emails A-N

johnson@fc.com - Default Outlook Profile.ost\Root folder\Root - Mailbox\Sync Issues\Local Failures\Customer emails A-D

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject Line** | **From** | **Recipient** | **Date & Time Sent** |
| Customer emails A-N | Not Listed – Signature block belongs to Anna Johnson | anna.johnson@rocketmail.com | 06/06/2016 10:57:33am |
| Customer emails A-D | Not Listed – Signature block belongs to Anna Johnson | anna.johnson@rocketmail.com | 06/06/2016 11:40:00am |

The first email was attempted on June 6, 2016 at 10:57:33. From the signature block of the email it appears as though the email was sent from the Anna Johnson, FinanceCorp email account johnson@fc.com. The email’s intended recipient was listed as anna.johnson@rocketmail.com.

The email had a subject line of “Customer emails A-N”.

Within the email were 72 attached email messages (.msg) along with 19 office documents or PDF files.

All these email messages and documents appear to be FinanceCorp Customer related items.

The second email message was attempted on June 6, 2016 at 11:40:00 and had a subject line of “Customer emails A-D”.

Within the email were 81 attached email messages (.msg) along with 19 office documents or PDF files.

All these email messages and documents appear to be FinanceCorp Customer related items.

Each of the email files were over 30MB in size. Most email services only allow email messages to be between 5-10 MB in size.

Since both email messages exceeded the 5-10MB size limitations, the email messages failed delivery to the rocketmail.com account. This is why both email messages were found in the “Local Failures” folder of the ajohnson .OST file. (*Exhibit 5*)

**Deleted Documents**

Upon examination of the Recycle Bin belonging to the ajohnson user account, SID# 320750, it was observed that 64 documents had been placed into the Recycle Bin for deletion. These documents were all placed in the recycle bin on June 13, 2016 at 11:36am. It appears that 2 of the 64 items were folders on the ajohnson user account desktop. These folders were named “Employee Info – Copy” and “Sales Meetings – Copy”. The remaining 62 items were documents or sub-folders within the two main folders. This would indicate that both folders deleted and sent from the user’s desktop to the recycle bin at the same time (June 13, 2016 at 11:36am). (*Exhibit 6*)

**Recently Accessed Documents**

There were 140 files that were listed in the recent folder of the ajohnson user account. The report shows the “D” volume as Emtec and three files that were accessed on the “D” drive volume. A file listing of the recently accessed documents was created for later review *(Exhibit 7)*.

**File Listings**

Excel Spreadsheets were created for Exhibits 1-4 and 6-7. Exhibit 5 is a zip folder that contains the contents of the failed email messages and the attachments.

Respectfully Submitted,

David Knutson, EnCE

Forensic Examiner

HAYSTACKID

Direct: 312.845.1000 x 4221

Cell: 815.530.6108

Email: [dknutson@haystackid.com](mailto:dknutson@haystackid.com)

[www.haystackid.com](http://www.haystackid.com)

**Appendix A.**

**About the Examiner**

David Knutson is Computer Forensic Examiner with HAYSTACKID.

David Knutson specializes in computer forensics, conducting analysis of legal evidence found in computers, digital storage media and on the Internet.

David Knutson holds the following professional certifications:

EnCE, EnCase Certified Examiner, by Guidance Software;

NET+, by CompTIA

Michigan Licensed Private Detective #3701-2006.