**Text

Description automatically generated**

**Case Project 02**

**CY5210 Information System Forensics**

**Instructor: Elton Booker**

**Jonathan Metzger**

**November 6th, 2022**

# Table of Contents

[Table of Contents 2](#_Toc118647036)

[EXECUTIVE SUMMARY 3](#_Toc118647037)

[INTRODUCTION 4](#_Toc118647038)

[ANALYSIS 6](#_Toc118647039)

[REGISTRY ANALYSIS 6](#_Toc118647040)

[USER INFORMATION 6](#_Toc118647041)

[GROUP INFORMATION 7](#_Toc118647042)

[SYSTEM INFORMATION 8](#_Toc118647043)

[USER ACTIVITY 9](#_Toc118647044)

[USB DEVICE ACTIVITY 10](#_Toc118647045)

[APPLICATIONS AND MALWARE 10](#_Toc118647046)

[PREFETCH 11](#_Toc118647047)

[SHELL ITEMS 11](#_Toc118647048)

[CONCLUSION 14](#_Toc118647049)

[APPENDIX 15](#_Toc118647050)

[APPENDIX I: Forensic Tools 15](#_Toc118647051)

[APPENDIX II: Registry Paths 15](#_Toc118647052)

[APPENDIX III: Artifacts List 16](#_Toc118647053)

[APPENDIX IV: Prefetch Analysis 17](#_Toc118647054)

[APPENDIX V: Shellbag Analysis 24](#_Toc118647055)

[APPENDIX VI: Link Analysis 26](#_Toc118647056)

[APPENDIX VII: Jump List Analysis 26](#_Toc118647057)

[APPENDIX VIII: USB Analysis 28](#_Toc118647058)

[APPENDIX IX: Chain of Custody Report 29](#_Toc118647059)

# EXECUTIVE SUMMARY

In this report, I will include findings that pertain to a recent data exposure of the company Capital Computing. Ethan Thomas was an employee with privileged administrator access to sensitive documents of the company. He reported that his primary windows were running slow and suspected malware on the system. The Cyber Investigations Team inspected the corrupted system and asked the forensics team to perform an analysis of the system for suspicious behavior. The investigation was released to the Directory of Cybersecurity James Smith for a summary of the case report.

Ethan Thomas was reported to Human Resources by multiple employees from his dissatisfaction of the company, and interest of applying to one of the company’s main competitors Next Generation Computing. From the shell items section in the analysis, it was reported that Ethan Thomas connected three USB devices into his system. On one of the devices labeled “IronKey”, included multiple sensitive, proprietary, and intellectual property documents company documents and his resignation letter. There were multiple malware applications found on E. Thomas’s system that can lead to the corruption of the system. From this, it can be shown that Ethan wanted to leave the company and take sensitive information with him. This is a violation of the company’s policy of proprietary data exposure.

E. Thomas then tried covering his tracks by uninstalling the company-controlled cloud service and having the security team wipe his old system. Little did he know that instead of wiping the system, security analyzed the system and found multiple points of malicious activity by the user. This report will conclude with the analysis findings, recommendations, and possible conclusions of the actions of Ethan Thomas.

# INTRODUCTION

The organization Capital Computing which distributes computer related products for corporate, small businesses and educational clients was subject to a potential data exposure. It is suspected that the exposure came from one of their employees Ethan Thomas. He reported that his primary Windows system was running slow and suspected of various adware or malware installed. The system’s anti-virus alerts identified of these possible malware applications installed on the system that can produce harm to the systema and network connected.

The system was analyzed by the Cyber Investigations Team on March 27th, 2018, and a new system was provided to E. Thomas. A remote acquisition of E. Thomas’s old infected system was performed on April 3rd, 2018. After, the Director of Cybersecurity asked for a forensics report of any potential data loss, exposure, or company proprietary data leakage by Ethan Thomas.

Ethan Thomas was reported to Human Resources that he was suspected of drafting his notice and planned to leave the company to work for their competitor Next Generation Computing. He was also known to have privileged access to sensitive information at the company. It is suspected that Ethan Thomas exported sensitive and confidential data from the system using escalated privileges to potentially sell or provide to the competitor organization.

The scope of the investigation includes the infected and any external media that might have been connected. In the below figure is the verification of the system’s hash. The hashes match meaning that the acquisition integrity was maintained. The chain of custody document is provided in APPENDIX IX of this report released at the time of the acquisition of the system. This highlights the connected external media and who managed the systems to be investigated. It will be interesting to see if these dots connect to expose Ethan Thomas as violating the company policy of data loss, exposure, and leakage to the company’s competition.

Graphical user interface, text, application

Description automatically generated

Figure 1 Hash Verification

# ANALYSIS

The analysis will cover Windows Registry, System Information, User activity, USB Device activity, Application and Malware use, Prefetch, Shellbags, Linkfiles, and JumpLists. By the forensics team obtaining this information from the incident response team, we will be able to justify if the user E. Thomas violated company policy.

## REGISTRY ANALYSIS

The Windows Registry identifies current system configurations and settings used during the investigation. They can show the current state of the system and actions performed by all users on the system. The following Hives were analyzed for the analysis using the tool Access Data FTK Imager, which can be found in APPENDIX III:

* **NONAME [NTFS]/[root]/Windows/System32/config/SAM**
* **NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM**
* **NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE**
* **NONAME [NTFS]/[root]/Users/<USER>/NTUSER.DAT**

The SAM Registry Hive focused on profiling users and groups. The SYSTEM Registry Hive identified system information and configuration settings. The SOFTWARE Registry Hive revealed applications downloaded, installed, executed, and uninstalled onto the system. The NTUSER.DAT Registry Hive focused on specific user activity.

## USER INFORMATION

Within the SAM report, the forensic investigator can see user and group information. Users for this system have the Domain UID of **S-1-5-21-82160412-4011698849-1881082856**. With “S” indicating the type is a SID, “1” as the revision level, “5” as the authority value, “21” meaning that it is a domain ID, and 82160412-4011698849-1881082856as the “unique identifier.” Next are each username “RID” of the system specified in the below table. Together make the “Security IDentified” or SID. Using the template:

*“<id\_type>-<revision\_level>-<authority\_value>-<specification\_id>-<unique\_identifier>-<RID>”*

The ethomas SID is **S-1-5-21-82160412-4011698849-1881082856-1001**

The ethan\_local SID is **S-1-5-21-82160412-4011698849-1881082856-1002**

The user information of the system of interest is in the below table with the username, RID, Status with number of logins, last login, group associated with and password information. User accounts ethomas and ethan\_local are a focus of this analysis since that account is given administrative privileges, multiple logins, password reset times of 2018-03-27 00:09:38Z and 2018-03-31 12:53:03Z respectively which are after, password not required and does not expire, and the last login is around the time of the security alert.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Username | RID | Status | Last Login | Password Reset | Group | Password |
| ethomas | 1001 | Enabled, 9 logins | 2018-04-03 16:30:23Z | 2018-03-27 00:09:38Z | Administrators | Not Required/Not Expired |
| ethan\_local | 1002 | Enabled, 10 logins | 2018-04-03 16:14:23Z | 2018-03-31 12:53:03Z | Users, Administrators | Not Required/Not Expired |
| Administrator | 500 | Enabled, 0 logins | Never | Never | Administrators | Not Expire |
| Guest | 501 | Disabled | Never | Never | Guests | Not Required/Not Expired |
| DefaultAccount | 503 | Disabled | Never | Never | System Managed Accounts Group | Not Required/Not Expired |

Table 1 User Information

## GROUP INFORMATION

As shown in the table in the previous section, no user was under the group Remote Desktop Users, so no user was able to ssh into the system. However, the Administrator, ethomas and ethan\_local users are under the privileged group Administrators. Any user in this group can cause potential harm to the system and organization the system is associated with. All but the Administrator account has their password not required and not expired. This can be a vulnerability in the system where privileged accounts can be easily accessed. This analysis states that the ethomas and ethan\_local accounts were not adequately secured and given full privileges. It was also the only account on the system that was enabled with the multiple logins. The last login time of ethomas was at last login time 2018-04-03 16:30:23Z and ethan\_local at 2018-04-03 16:14:23Z which was after the Cyber Investigations Team was notified of the infected system and provided a clean system to E. Thomas on March 27th, 2018, and the same day as the system was analyzed by the forensics team on April 3rd, 2018. This means that the response to this user’s malicious activity was slow and allowed five days of those users to access the system before being scanned.

## SYSTEM INFORMATION

${ControlSet} = HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001

${CurrentVersion} = HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

|  |  |  |
| --- | --- | --- |
| Key | Location | Value |
| Microsoft OS Version | ${CurrentVersion}\ProductName | Windows 10 Pro (10.0.16299.15) |
| Build Version | ${CurrentVersion}\CurrentBuild | 16299 |
| Current Control Set | ${ControlSet} | 001 |
| Computer Name | ${ControlSet}\Control\ComputerName\ComputerName | ETHOMAS\_DESKTOP |
| Time Zone | ${ControlSet}\Control\TimeZoneInformation | Eastern Standard Time |
| OS Install Date | ${CurrentVersion}\InstallDate | 2018-03-26 20:01:29 EST (1522108889) |
| Network Interfaces | ${ControlSet}\Services\NetBT\Parameters\Interfaces\Tcpip\_{49e11da8-a9a9-4046-a9e2-67d832c476b5} | 192.168.171.2 |
| AutoStart Programs | ${CurrentVersion}\Run | LastWrite Time 2018-04-03 13:46:35Z  SlitherIO - "C:\Users\ethan\_local\AppData\Roaming\slitherio\slitherio.exe"  OneDrive - "C:\Users\ethan\_local\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background  CCleaner Monitoring - "C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR |
| Last Shutdown Time | ${ControlSet}\Control\Windows\ShutdownTime | 2018-04-03 00:56:01 EST |

Table 2 System Information

Our goal was to collect the system’s configurations, settings, user data, and activity to scope a full picture of the activity that went on around the time of the alert. The hostname “ETHOMAS\_DESKTOP” was analyzed by the Forensics team to inspect the malicious activity that was reported. On the Windows 10 Pro system, we found that the operating installation time was 2019-01-19 at 03:06:56Z and set in Eastern Standard time. We used Registry Ripper to analyze the hives of SAM, SYSTEM, SOFTWARE, and User (NTUSER.DAT and USRCLASS.DAT). The system’s network configurations are set to IP Address 192.168.171.2. The system’s last shutdown time was five days after the incident was identified which allowed E. Thomas to continue his access while the Cyber Investigations Team was aware of his old infected system.

The three Autostart programs were slitherio.exe, OneDrive and CCleaner. Slitherio seems like the virus that Ethan Thomas reported, and CCleaner was started to clean the computer for better performance. It looks like neither application is a standard Windows software nor should not be installed on a company-controlled system.

## USER ACTIVITY

The forensics team went through the user activity of the user E. Thomas on both of his accounts. They reviewed the user’s Windows Search History, Typed Paths, RecentDocs, Last Executed Commands, and UserAssist findings. These registry locations can be found in APPENDIX II.

* **Windows Search History**

Search list history includes the ccsetup, cc and sensitive. The sensitive search found in the wordwheelquery is concerning since it can contain the Sensitive Potential Client List or other confidential information.

* **Typed Paths**

NTUSER.DAT hive reports no typed paths for either user due to the lack of evidence identified under the registry key.

* **RecentDocs**

There was a lot of recent documents accessed by the ethan\_local and ethomas users. These included Notes, Company Sensitive Document, Intellectual Property Document, Proprietary Corporate Data, Sensitive Potential Client List, Dropbox and IronKey Secure Files (F Drive). This indicates that the users had access to sensitive information and used external media to potentially export these items.

* **LastExecutedCommands**

The list of last executed commands was not populated due to the user not running commands from START -> RUN box. These were instead after launching the “cmd.exe” executable.

* **UserAssist**

A list of the UserAssist executables of interest can be found in the below table. It includes the external media with the name IronKey that was used by E. Thomas, the command line to perform privileged commands, CCSetup for the CCleaner application. It also shows that even though the system reported to have no RDP users, E. Thomas used RemoteDesktop and PuTTY to remote out of the system that forensic investigators can possibly not have oversight of. Lastly the Cat and Dog Screensaver executable is showed in the Downloads directory that can potentially contain malware that the user E. Thomas knowingly or not knowingly installed and corrupted the newly wiped system.

|  |  |
| --- | --- |
| Executables | LastWriteTime |
| C:\Users\ethan\_local\Downloads\Cat\_And\_Dog\_Screensaver.exe (1) | 2018-03-31 16:05:07Z |
| SimonTatham.PuTTY (2) | 2018-03-31 17:14:12Z |
| Microsoft.Windows.RemoteDesktop (2) | 2018-03-31 17:15:54Z |
| E:\ccsetup541pro.exe (1) | 2018-04-03 13:37:01Z |
| {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe (2) | 2018-04-03 13:37:16Z |
| E:\IronKey.exe (2) | 2018-04-03 16:15:09Z |

Table 3 UserAssist

## USB DEVICE ACTIVITY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Name | Serial Number | User Account | First Time | Last Time |
| IronKey Secure Drive USB Device (F:\) | 00787613 | ethomas/ethanlocal | 2018-03-31 14:03:01Z | 2018-04-03 16:17:25Z |
| Kingston DataTraveler G3 USB Device (Personal USB) | 0019E000B499EBB166A2018F | ethomas/ethanlocal | 2018-03-31 15:36:49Z | 2018-04-03 13:49:35Z |
| Kingston DT Rubber 3.0 USB Device (SSD\_FAC) | 0018F30C9FEABD80610D1AAC | ethomas | 2018-04-03 16:20:19Z | 2018-04-03 16:21:12Z |
| WD My Passport 2599 (New Volume) | 575854314541354441545352 | n/a | 2018-04-03 16:22:43Z | 2018-04-03 16:23:33Z |
| PNY USB 3.0 FD | 070877F6181C2830 | n/a | 2018-04-03 16:41:30Z | n/a |

Table 4 USB Device Connected to “ETHOMAS\_DESKTOP”

The forensics team identified five external media devices that were connected to the system. Three of them were under the E. Thomas users with their last time access at the time of the system scan. IronKey Secure Drive has been mentioned multiple times in the analysis section and can contain sensitive and company confidential information that the user exported for their own personal use.

## APPLICATIONS AND MALWARE

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Path | Filename | LastUsed | Download | Installed | Executed | Uninstalled |
| N/A | Microsoft OneDrive v.18.240.1202.0004 | 2018-04-03 00:11:42Z |  |  |  | X |
| C:\Users\ethan\_local\Downloads\ | Cat\_And\_Dog\_Screensaver.exe | 2018-03-31 16:05:07Z | X | X | X |  |
| {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7} | cmd.exe | 2018-04-03 16:56:25 |  |  | X |  |
| C:\Users\ethan\_local\AppData\Roaming\slitherio | slitherio.exe | 2018-04-03 00:58:59 |  | X | X |  |

Table 5 Applications by LastUsed

The applications listed above is also in the Prefetch list. However, this list includes their activity of download, installed, executed, and uninstalled applications. The forensics data shows OneDrive is being uninstalled by the E. Thomas user. This can hide activity that the user can potentially export sensitive data from the system to an external location on the cloud. The Screensaver executable was downloaded, installed, and executed onto the system which can potentially include viruses. The Slitherio executable is a known virus and could have potentially been installed by the E. Thomas users or installed onto the system by a phishing email or malicious application. Finally, the cmd.exe is used over 116 times by the user should be an area of concern since this user has escalated administrator privileges.

## PREFETCH

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Executable Name | Source  Created | Source  Modified | Size | Run  Count | Last  Run | First  Run | Volume  Serial |
| CAT\_AND\_DOG\_SCREENSAVER.EXE | 2018-03-31 16:05:20 | 2018-03-31 16:05:20 | 97026 | 1 | 2018-03-31 16:05:07 |  | 60D53EE6 |
| CCLEANER.EXE | 2018-04-03 14:01:44 | 2018-04-03 14:01:44 | 27064 | 1 | 2018-04-03 14:01:43 |  | 60D53EE6 |
| CMD.EXE | 2018-03-30 15:13:07 | 2018-04-03 16:56:25 | 9576 | 116 | 2018-04-03 16:56:25 | 2018-04-03 16:31:18 | 60D53EE6 |
| DROPBOX.EXE | 2018-03-31 13:09:17 | 2018-04-03 00:59:11 | 171872 | 12 | 2018-04-03 00:59:01 | 2018-03-31 14:44:24 | BAA935F8 |
| IRONKEY.EXE | 2018-03-31 14:03:22 | 2018-04-03 16:15:20 | 61610 | 4 | 2018-04-03 16:15:09 | 2018-03-31 14:03:11 | BAA935F8 |
| ONEDRIVE.EXE | 2018-03-31 14:49:46 | 2018-04-03 00:59:07 | 149932 | 5 | 2018-04-03 00:58:57 | 2018-03-31 14:49:36 | 60D53EE6 |
| PUTTY.EXE | 2018-03-31 16:08:44 | 2018-03-31 17:14:22 | 33362 | 2 | 2018-03-31 17:14:12 | 2018-03-31 16:08:34 | 60D53EE6 |
| SLITHERIO.EXE | 2018-03-31 16:05:12 | 2018-04-03 00:59:03 | 107090 | 3 | 2018-04-03 00:58:59 | 2018-03-31 16:05:09 | 60D53EE6 |

Table 6 Prefix Analysis for "ETHOMAS\_DESKTOP"

The Prefetch data can be found in APPENDIX IV. A snippet of the information gathered by the forensics team with an area of concern can be found in the table above. The cmd.exe was ran 116 times in the period of 25 minutes. That is a lot to run by the user who is suspected of malicious activity by the files he accessed and the user’s plan to work for a competitor company. Included in the prefetch data were several RDP and external media applications. This enabled the user to remote to other systems to potentially secure copy files to other systems, external media, or cloud storages.

## SHELL ITEMS

The below table identifies the areas of interest in the shell bag analysis located in APPENDIX V. The user E. Thomas accesses the System and Security section in control panel. This area is a privileged area and can be used to open firewall protections or permissions for malicious activity. Activity can include allowing the use of cloud-based software like Dropbox or external media. The user also accessed the F drive which can be linked to the IronKey removable media USB. The analysis shows that the user accessed their Documents which can contain sensitive and confidential files to be shared outside of the secured system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AbsolutePath | ShellType | Value | FirstInteracted | LastInteracted |
| Desktop\Control Panel\System and Security | Control Panel Category | System and Security |  | 2018-03-31 12:46:31 |
| Desktop\Control Panel\System and Security\System | GUID: Control panel | System | 2018-03-31 12:46:31 | 2018-03-31 12:46:31 |
| Desktop\E:\ | Users property view: Drive letter | E:\ | 2018-03-31 15:36:58 | 2018-04-03 13:59:22 |
| Desktop\E:\\Documents | Directory | Documents | 2018-03-31 14:43:06 | 2018-03-31 14:43:06 |
| Desktop\F:\ | Users property view: Drive letter | F:\ |  | 2018-04-03 16:43:43 |
| Desktop\My Computer\C:\Users\ethomas | Directory | ethomas | 2018-03-31 14:46:27 | 2018-03-31 14:46:27 |
| Desktop\My Computer\C:\Users\ethomas\Documents | Directory | Documents | 2018-03-31 15:38:00 | 2018-03-31 15:38:00 |
| Desktop\My Computer\Desktop | Root folder: GUID | Desktop | 2018-04-03 00:16:48 | 2018-04-03 00:16:48 |
| Desktop\My Computer\Documents | Root folder: GUID | Documents | 2018-03-31 15:37:41 |  |
| Desktop\My Computer\Downloads | Root folder: GUID | Downloads | 2018-03-31 16:04:50 |  |
| Desktop\My Computer\E: | Drive letter | E: | 2018-04-03 13:36:33 | 2018-04-03 13:36:33 |
| Desktop\Shared Documents Folder (Users Files)\Dropbox | Users Files Folder | Dropbox | 2018-03-31 13:21:49 | 2018-03-31 13:21:49 |

Table 7 Shellbag Items

The below table highlights LNK files of interest. The full list can be found in APPENDIX VI. Of those files, the Intellectual Property Document, Proprietary Corporate Data, Sensitive Potential Client List, Company Sensitive Document are sensitive documents accessed by the E. Thomas users. With the additional access to Dropbox and F drive of the IronKey USB, these documents can be easily exported and shared. The EthanThomas\_Notes can be interesting to investigate since the user can document notes of shared passwords, access steps or anything else that is sensitive towards the organization.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| LocalPath | Src/Dst Created | Src/Dst Modified | Source  Accessed | File  Size | DriveType | VolumeSerial/Label | MachineID |
| C:\Users\ethomas\Dropbox\Intellectual Property Document.docx | 2018-03-31 14:43:38 | 2018-03-31 14:45:17 | 2018-03-31 14:45:17 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents\Proprietary Corporate Data.pptx | 2018-03-31 14:22:00 | 2018-03-31 14:42:39 | 2018-03-31 14:42:39 | 49764 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\Sensitive Potential Client List.xlsx | 2018-03-31 14:22:13 | 2018-03-31 14:22:13 | 2018-03-31 14:22:13 | 9206 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Documents\EthanThomas\_Notes.docx | 2018-03-31 14:44:00 | 2018-03-31 14:45:48 | 2018-03-31 14:45:48 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents\Company Sensitive Document.docx | 2018-03-31 14:21:36 | 2018-03-31 14:45:42 | 2018-03-31 14:45:42 | 9007 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Dropbox | 2018-03-31 14:45:17 | 2018-03-31 14:45:23 | 2018-03-31 14:45:23 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\ | 2018-03-31 14:21:36 | 2018-03-31 14:42:59 | 2018-03-31 14:42:59 | 0 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Downloads | 2018-03-31 14:07:45 | 2018-03-31 14:07:45 | 2018-03-31 14:07:45 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Intellectual Property Document.docx | 2018-03-31 15:38:39 | 2018-03-31 16:04:34 | 2022-11-03 23:08:14 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Sensitive Potential Client List.xlsx | 2018-03-31 15:38:22 | 2018-03-31 15:38:22 | 2018-03-31 15:38:22 | 7412 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\EthanThomas\_Notes.docx | 2018-03-31 15:38:34 | 2018-03-31 16:04:39 | 2018-03-31 16:04:39 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Downloads | 2018-03-31 15:42:45 | 2018-03-31 15:42:45 | 2018-03-31 15:42:45 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |

Table 8 LNK Files

Jump Lists that were collected by the forensics investigation team. Most overlap with the LNK files and can be found in APPENDIX VII. Of those applications or files of interest are shown in the table below. The interesting application “mstsc.exe” relates to Remote Desktop Connections. By running this application on the system can provide access for outside systems to remote in without the need for RDP user created. The remaining files are sensitive documents that were copied over to an internal media.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| LocalPath | Target  Created | Target  Modified | Target  Accessed | File  Size | Drive  Type | VolumeSerial/Label | MachineID |
| C:\Windows\System32\mstsc.exe | 2017-09-29 13:42:03 | 2017-09-29 13:42:03 | 2017-09-29 13:42:03 | 3630080 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| E:\Intellectual Property Document.docx | 2018-03-31 15:39:16 | 2018-03-31 15:39:16 | 2018-03-31 15:39:16 | 9015 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| F:\Company Sensitive Document.docx | 2018-03-30 18:18:45 | 2018-03-30 18:00:42 | 2018-03-31 04:00:00 | 15967 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\Proprietary Corporate Data.pptx | 2018-03-30 18:18:45 | 2018-03-30 18:15:24 | 2018-03-30 04:00:00 | 49764 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\Sensitive Potential Client List.xlsx | 2018-03-30 18:18:45 | 2018-03-30 18:17:48 | 2018-03-30 04:00:00 | 9206 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |

Table 9 Jump Lists

With this analysis, we can prove that the user E. Thomas had privileged access to the system, had access to remote file systems on the system, and exported sensitive documents from the system to external media whether it was a USB or cloud storage.

# CONCLUSION

After observing evidence on the hard drive labeled “ETHOMAS\_DESKTOP” on April 3rd, 2018, the forensics team can conclude that Ethan Thomas intended to leave the company and bring sensitive and proprietary information on his USB external media. It can be connected that E. Thomas downloaded malware to the system after exporting sensitive documents to his personal USB device. The malware set off anti-malware alerts that conducted Thomas to notify security to wipe his system. He thought that by wiping the system, he would be able to cover his tracks. Instead, the forensics team analyzed the system and found evidence of his malicious activities.

The forensics team found applications of interest on the system which includes mstsc.exe, and PuTTY to enable remote desktop connections. They also found that the user tried uninstalling the company’s OneDrive to disable auto syncing his actions. On the external media was found Intellectual Property Document, Company Sensitive Document, Proprietary Corporate Data, Sensitive Potential Client List. By downloading executable CAT\_AND\_DOG\_SCREENSAVER.EXE Thomas was able to install malware onto the system to set off the alert. E. Thomas also used his privileged access to access the System and Security control panel to enable him to export sensitive documents past the companies defenses. The user ran multiple commands on the terminal as an administrator which can cause harm towards the system

It is recommended by the forensics team that this evidence can be used against Ethan Thomas in court that he tried to leave the company and bring sensitive information to one of the competitor organizations. Legal actions should be taken by the organization that owns the sensitive documents against the individual. The organization’s IT department will need to restrict USB access to their system for this does not occur again, even by administrators. They additionally will need to lock down elevated privileges, require administrative rights to download applications not already authorized by the ISSO, and secure these sensitive and confidential documents in a secure location and not on the user's Documents and Desktop directories. Overall, it is a good idea to notify the organization of this breach, to provide reminders on the consequences, and require additional security/human error training. This event may have occurred in a public setting with other employees on the premises. They should be reminded to report any unusual behavior to security.

# APPENDIX

## APPENDIX I: Forensic Tools

|  |  |  |
| --- | --- | --- |
| Tool | Version | Command |
| Access Data Forensic Toolkit (FTK) | v6.4 | GUI |
| Access Data FTK Imager | v3.4.2.6 | GUI |
| Registry Ripper | v3.0 | GUI |
| Autopsy | v4.6.0 | GUI |
| USBDeviceForensics | v1.5.2 | GUI |
| AccessData Registry Viewer | v2.0 | GUI |
| ShellBags Explorer\* | V1.0 | GUI |
| DCode Date | V4.02 | GUI |
| Prefetch\* | v1.5 | PECmd –d “Directory for Prefetch Files” --csv “Directory Output\pf.csv” |
| Link File\* | v1.5 | LECmd –d “Directory for Link Files” --csv “Directory Output\lnk.csv” |
| Jump List\* | v1.5 | JLECmd –d “Directory for Jump Files” --csv “Directory Output\jmp.csv” |
| Shellbags Cmd | v2.0 | SBECmd –d “Directory for ShellBag Items” --csv “Directory Output\sb.csv” |

\*Eric Zimmerman’s Tools (Source: https://ericzimmerman.github.io/#!index.md)

## APPENDIX II: Registry Paths

|  |  |  |  |
| --- | --- | --- | --- |
| Hive | Directory | Name | Description |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Explorer | TypedPaths | Paths Typed by User |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Explorer | WordWheelQuery | Windows Search History |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Explorer | RecentDocs | Recent Documents |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Explorer | UserAssist | User Program execution |
| NTUSER.DAT | \Software\Microsoft\Windows\CurrentVersion\Explorer\ | <Policies>\RunMRU | User Command execution |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion | Run | Applications Ran |
| NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion | RunOnce | Applications Ran Once |
| NTUSER.DAT | Software\Microsoft\Windows\Shell | Bags (Desktop) | ShellBags |
| NTUSER.DAT | Software\Microsoft\Windows\Shell | BagMRU (Desktop) | ShellBags List |
| NTUSER.DAT | System\CurrentControlSet\Services\Tcpip\Parameters | Interfaces | Network Interfaces |
| USRCLASS.DAT | Local Settings\Software\Microsoft\Windows\Shell | Bags (Explorer) | ShellBags |
| USRCLASS.DAT | Local Settings\Software\Microsoft\Windows\Shell | BagMRU (Explorer) | ShellBags List |

## APPENDIX III: Artifacts List

NOTE: <USER> is both ethomas and ethan\_local

1. NTFS Files
   * NONAME [NTFS]/[root]/$MFT
   * NONAME [NTFS]/[root]/$LogFile
2. Registry Hives
   * NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM
   * NONAME [NTFS]/[root]/Windows/System32/config/SECURITY
   * NONAME [NTFS]/[root]/Windows/System32/config/SAM
   * NONAME [NTFS]/[root]/Windows/System32/config/SOFTWARE
   * NONAME [NTFS]/[root]//Users/<USER>/NTUSER.DAT
   * NONAME [NTFS]/[root]//Users/<USER>/AppData/Local/Microsoft/Windows/UsrClass.dat
3. Logs
   * NONAME [NTFS]/[root]/Windows/System32/winevt/Logs
4. Additional Shellbag Folders
   * NONAME [NTFS]/[root]/Windows/Prefetch
   * NONAME [NTFS]/[root]/Users/<USER>/AppData
   * NONAME [NTFS]/[root]/Users/<USER>/AppData/Roaming/Microsoft/Windows/Recent
5. User’s Profile Folders
   * NONAME [NTFS]/[root]/Users/<USER>/Desktop
   * NONAME [NTFS]/[root]/Users/<USER>/Documents
   * NONAME [NTFS]/[root]/Users/<USER>/Downloads
   * NONAME [NTFS]/[root]/Users/<USER>/Dropbox
6. Additional Artifacts
   * NONAME [NTFS]/[root]/$Recycle.Bin (folder)
   * NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log

## APPENDIX IV: Prefetch Analysis

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ExecutableName | SourceCreated | SourceModified | Size | RunCount | LastRun | FirstRun | VolumeSerial |
| 7Z1801-X64.EXE | 2018-03-31 13:22:54 | 2018-03-31 13:22:54 | 70046 | 1 | 2018-03-31 13:22:45 |  | 60D53EE6 |
| ACCESSDATA%20FTK%20IMAGER%203 | 2018-04-03 16:46:17 | 2018-04-03 16:46:17 | 31520 | 1 | 2018-04-03 16:46:07 |  | 60D53EE6 |
| AM\_DELTA\_PATCH\_1.263.1974.0.E | 2018-04-03 16:32:43 | 2018-04-03 16:32:43 | 13212 | 1 | 2018-04-03 16:32:33 |  | 60D53EE6 |
| AM\_DELTA.EXE | 2018-04-01 15:24:03 | 2018-04-01 15:24:03 | 12300 | 1 | 2018-04-01 15:23:53 |  | 60D53EE6 |
| APPLICATIONFRAMEHOST.EXE | 2018-03-30 15:10:09 | 2018-04-03 16:35:36 | 65048 | 8 | 2018-04-03 16:35:26 | 2018-03-30 15:09:59 | 60D53EE6 |
| AUDIODG.EXE | 2018-03-27 00:01:51 | 2018-04-03 16:41:28 | 27130 | 25 | 2018-04-03 16:41:18 | 2018-04-03 00:54:03 | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-03-31 14:52:00 | 2018-03-31 15:10:42 | 40714 | 2 | 2018-03-31 15:10:32 | 2018-03-31 14:51:50 | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-03-31 14:51:58 | 2018-03-31 15:10:42 | 36272 | 2 | 2018-03-31 15:10:32 | 2018-03-31 14:51:48 | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-03-31 18:16:07 | 2018-03-31 18:16:07 | 3034 | 1 | 2018-03-31 18:15:55 |  | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-03-27 00:12:35 | 2018-04-03 13:34:08 | 43044 | 15 | 2018-04-03 13:33:58 | 2018-03-31 19:29:05 | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-01-30 16:22:17 | 2018-04-03 16:32:03 | 46974 | 12 | 2018-04-03 16:31:53 | 2018-04-01 04:40:17 | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-04-03 16:14:29 | 2018-04-03 16:14:29 | 34552 | 1 | 2018-04-03 16:14:19 |  | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-03-30 15:14:58 | 2018-04-03 13:37:32 | 160310 | 22 | 2018-04-03 13:37:17 | 2018-04-01 04:43:40 | 60D53EE6 |
| BACKGROUNDTASKHOST.EXE | 2018-03-27 00:13:08 | 2018-04-03 12:39:42 | 61810 | 7 | 2018-04-03 12:39:42 | 2018-03-27 00:13:06 | 60D53EE6 |
| BACKGROUNDTRANSFERHOST.EXE | 2018-03-27 00:13:23 | 2018-03-31 15:05:12 | 73834 | 3 | 2018-03-31 15:05:09 | 2018-03-27 00:13:13 | 60D53EE6 |
| BCASTDVR.EXE | 2018-03-31 15:06:01 | 2018-04-01 04:43:05 | 54586 | 17 | 2018-04-01 04:42:55 | 2018-03-31 19:30:27 | 60D53EE6 |
| BROWSER\_BROKER.EXE | 2018-03-30 15:10:09 | 2018-04-03 13:37:44 | 36516 | 7 | 2018-04-03 13:37:33 | 2018-03-30 15:09:59 | 60D53EE6 |
| BYTECODEGENERATOR.EXE | 2018-04-03 01:03:32 | 2018-04-03 01:03:32 | 19444 | 1 | 2018-04-03 01:03:31 |  | 60D53EE6 |
| BYTECODEGENERATOR.EXE | 2018-04-03 01:03:34 | 2018-04-03 01:03:34 | 17296 | 1 | 2018-04-03 01:03:34 |  | 60D53EE6 |
| CAT AND DOG.SCR | 2018-03-31 16:06:30 | 2018-04-03 00:10:49 | 76976 | 4 | 2018-04-03 00:10:39 | 2018-03-31 16:06:20 | 60D53EE6 |
| CAT\_AND\_DOG\_SCREENSAVER.EXE | 2018-03-31 16:05:20 | 2018-03-31 16:05:20 | 97026 | 1 | 2018-03-31 16:05:07 |  | 60D53EE6 |
| CCLEANER.EXE | 2018-04-03 14:01:44 | 2018-04-03 14:01:44 | 27064 | 1 | 2018-04-03 14:01:43 |  | 60D53EE6 |
| CCLEANER64.EXE | 2018-04-03 13:37:32 | 2018-04-03 14:01:53 | 84174 | 5 | 2018-04-03 14:01:43 | 2018-04-03 13:37:25 | 60D53EE6 |
| CCUPDATE.EXE | 2018-04-03 13:37:37 | 2018-04-03 13:37:37 | 22678 | 1 | 2018-04-03 13:37:26 |  | 60D53EE6 |
| CHRMSTP.EXE | 2018-04-01 04:17:32 | 2018-04-01 04:17:32 | 26600 | 1 | 2018-04-01 04:17:32 |  | 60D53EE6 |
| CHRMSTP.EXE | 2018-04-01 04:17:32 | 2018-04-01 04:17:32 | 42318 | 1 | 2018-04-01 04:17:32 |  | 60D53EE6 |
| CHROME.EXE | 2018-04-01 04:17:15 | 2018-04-01 04:17:15 | 25606 | 1 | 2018-04-01 04:16:53 |  | 60D53EE6 |
| CHROME.EXE | 2018-01-30 16:23:49 | 2018-04-01 05:24:33 | 45048 | 20 | 2018-04-01 05:24:22 | 2018-03-31 13:02:23 | 60D53EE6 |
| CHROME.EXE | 2018-01-30 16:23:49 | 2018-04-01 05:14:56 | 84932 | 17 | 2018-04-01 05:14:50 | 2018-03-31 12:12:33 | 60D53EE6 |
| CHROME.EXE | 2018-01-30 16:23:49 | 2018-04-01 04:17:15 | 188238 | 4 | 2018-04-01 04:16:52 | 2018-01-30 16:23:41 | 60D53EE6 |
| CHROME.EXE | 2018-04-01 04:46:29 | 2018-04-01 04:53:28 | 48782 | 2 | 2018-04-01 04:53:18 | 2018-04-01 04:46:19 | 60D53EE6 |
| CHROME.EXE | 2018-04-01 04:17:15 | 2018-04-01 04:17:15 | 27002 | 1 | 2018-04-01 04:16:53 |  | 60D53EE6 |
| CHROME.EXE | 2018-04-01 04:17:15 | 2018-04-01 04:17:15 | 43286 | 1 | 2018-04-01 04:16:53 |  | 60D53EE6 |
| CHXSMARTSCREEN.EXE | 2018-03-31 16:05:06 | 2018-04-03 12:40:57 | 118264 | 2 | 2018-04-03 12:40:46 | 2018-03-31 16:04:54 | 60D53EE6 |
| CMD.EXE | 2018-03-30 15:13:07 | 2018-04-03 16:56:25 | 9576 | 116 | 2018-04-03 16:56:25 | 2018-04-03 16:31:18 | 60D53EE6 |
| CMD.EXE | 2018-04-03 00:11:41 | 2018-04-03 00:11:42 | 10078 | 2 | 2018-04-03 00:11:41 | 2018-04-03 00:11:40 | 60D53EE6 |
| COMPATTELRUNNER.EXE | 2018-03-30 15:30:41 | 2018-04-03 00:50:18 | 13728 | 7 | 2018-04-03 00:50:08 | 2018-03-30 15:30:36 | 60D53EE6 |
| CONHOST.EXE | 2018-03-30 15:12:15 | 2018-04-03 16:56:25 | 21646 | 111 | 2018-04-03 16:56:25 | 2018-04-03 16:24:05 | 60D53EE6 |
| CONSENT.EXE | 2018-03-30 15:11:35 | 2018-04-03 16:43:55 | 287240 | 16 | 2018-04-03 16:43:52 | 2018-03-31 13:06:49 | 4EE65D55 |
| CREDENTIALUIBROKER.EXE | 2018-03-31 17:14:58 | 2018-03-31 17:16:27 | 109834 | 2 | 2018-03-31 17:16:17 | 2018-03-31 17:14:48 | 60D53EE6 |
| CSRSS.EXE | 2018-03-27 00:11:12 | 2018-04-03 16:17:52 | 30166 | 7 | 2018-04-03 16:17:42 | 2018-03-27 00:11:01 | 60D53EE6 |
| CTFMON.EXE | 2018-03-30 15:13:34 | 2018-04-03 16:17:40 | 32838 | 10 | 2018-04-03 16:17:40 | 2018-03-31 14:46:48 | 60D53EE6 |
| DEFRAG.EXE | 2018-03-30 15:30:37 | 2018-04-03 01:10:05 | 16604 | 3 | 2018-04-03 01:09:55 | 2018-03-30 15:30:35 | 60D53EE6 |
| DLLHOST.EXE | 2018-04-03 00:45:16 | 2018-04-03 00:45:16 | 21570 | 1 | 2018-04-03 00:45:06 |  | 60D53EE6 |
| DLLHOST.EXE | 2018-03-27 00:13:17 | 2018-04-03 12:39:52 | 47756 | 7 | 2018-04-03 12:39:41 | 2018-03-27 00:13:07 | 60D53EE6 |
| DLLHOST.EXE | 2018-03-27 00:11:17 | 2018-03-31 14:47:54 | 25258 | 2 | 2018-03-31 14:47:49 | 2018-03-27 00:11:12 | 60D53EE6 |
| DLLHOST.EXE | 2018-04-03 14:01:46 | 2018-04-03 14:01:46 | 39032 | 1 | 2018-04-03 14:01:41 |  | BAA935F8 |
| DLLHOST.EXE | 2018-03-27 00:13:13 | 2018-04-03 12:39:47 | 16988 | 11 | 2018-04-03 12:39:41 | 2018-03-31 12:49:33 | 60D53EE6 |
| DLLHOST.EXE | 2018-03-31 15:38:03 | 2018-03-31 15:38:03 | 78032 | 1 | 2018-03-31 15:37:53 |  | 60D53EE6 |
| DLLHOST.EXE | 2018-03-27 00:09:44 | 2018-04-03 16:43:59 | 16960 | 47 | 2018-04-03 16:43:54 | 2018-04-03 01:02:12 | 60D53EE6 |
| DLLHOST.EXE | 2018-03-27 00:02:07 | 2018-04-03 16:47:48 | 27610 | 45 | 2018-04-03 16:47:39 | 2018-04-03 12:29:37 | 60D53EE6 |
| DLLHOST.EXE | 2018-04-03 13:48:18 | 2018-04-03 13:48:18 | 23402 | 1 | 2018-04-03 13:48:13 |  | 60D53EE6 |
| DLLHOST.EXE | 2018-03-31 13:12:04 | 2018-04-03 16:37:45 | 31712 | 10 | 2018-04-03 16:37:35 | 2018-04-03 12:30:04 | 60D53EE6 |
| DLLHOST.EXE | 2018-03-30 15:11:50 | 2018-04-03 16:32:31 | 26184 | 10 | 2018-04-03 16:32:26 | 2018-03-31 12:53:17 | 60D53EE6 |
| DLLHOST.EXE | 2018-03-31 12:53:09 | 2018-03-31 23:52:49 | 38456 | 4 | 2018-03-31 23:52:44 | 2018-03-31 12:53:04 | 60D53EE6 |
| DROPBOX.EXE | 2018-03-31 13:09:17 | 2018-04-03 00:59:11 | 171872 | 12 | 2018-04-03 00:59:01 | 2018-03-31 14:44:24 | BAA935F8 |
| DROPBOXCRASHHANDLER.EXE | 2018-03-31 13:11:00 | 2018-03-31 14:47:36 | 31914 | 2 | 2018-03-31 14:47:35 | 2018-03-31 13:11:00 | 60D53EE6 |
| DROPBOXUPDATE.EXE | 2018-03-31 13:06:53 | 2018-04-03 16:37:42 | 65674 | 44 | 2018-04-03 16:37:35 | 2018-04-03 13:11:19 | 60D53EE6 |
| DROPBOXUPDATE.EXE | 2018-03-31 13:06:38 | 2018-03-31 13:06:38 | 57000 | 1 | 2018-03-31 13:06:29 |  | 60D53EE6 |
| DROPBOXUPDATE.EXE | 2018-03-31 13:06:59 | 2018-03-31 13:07:01 | 97308 | 2 | 2018-03-31 13:06:51 | 2018-03-31 13:06:49 | 60D53EE6 |
| DRVINST.EXE | 2018-03-27 00:01:55 | 2018-04-03 16:41:31 | 57658 | 15 | 2018-04-03 16:41:30 | 2018-03-30 15:12:50 | 60D53EE6 |
| DWM.EXE | 2018-03-27 00:11:12 | 2018-04-03 16:17:53 | 67182 | 7 | 2018-04-03 16:17:42 | 2018-03-27 00:11:01 | 60D53EE6 |
| EXPLORER.EXE | 2018-03-31 13:09:32 | 2018-04-03 00:13:56 | 186378 | 2 | 2018-04-03 00:13:41 | 2018-03-31 13:09:22 | 60D53EE6 |
| FILESYNCCONFIG.EXE | 2018-04-03 00:11:41 | 2018-04-03 00:11:41 | 43924 | 1 | 2018-04-03 00:11:40 |  | 60D53EE6 |
| FINDSTR.EXE | 2018-01-30 16:26:26 | 2018-04-03 16:56:25 | 8612 | 82 | 2018-04-03 16:56:25 | 2018-04-03 01:24:00 | 60D53EE6 |
| FIREFOX INSTALLER.EXE | 2018-01-30 16:26:43 | 2018-01-30 16:26:43 | 29990 | 1 | 2018-01-30 16:26:33 |  | 60D53EE6 |
| FIREFOX.EXE | 2018-01-30 16:27:17 | 2018-04-03 16:41:52 | 148492 | 40 | 2018-04-03 16:41:49 | 2018-04-03 00:45:33 | 60D53EE6 |
| FIRSTLOGONANIM.EXE | 2018-03-27 00:11:13 | 2018-03-27 00:11:13 | 52958 | 1 | 2018-03-27 00:11:01 |  | 60D53EE6 |
| FONTDRVHOST.EXE | 2018-03-27 00:11:12 | 2018-04-03 16:17:53 | 436920 | 7 | 2018-04-03 16:17:42 | 2018-03-27 00:11:01 | 60D53EE6 |
| FSQUIRT.EXE | 2018-03-27 00:12:27 | 2018-03-31 14:48:08 | 40944 | 2 | 2018-03-31 14:48:07 | 2018-03-27 00:12:25 | 60D53EE6 |
| FTK IMAGER.EXE | 2018-04-03 16:44:01 | 2018-04-03 16:45:41 | 19942 | 3 | 2018-04-03 16:45:31 | 2018-04-03 16:43:55 | 4EE65D55 |
| FTK IMAGER.EXE | 2018-04-03 16:47:59 | 2018-04-03 16:47:59 | 108762 | 1 | 2018-04-03 16:47:49 |  | 4EE65D55 |
| GAMEBARPRESENCEWRITER.EXE | 2018-03-31 18:16:28 | 2018-04-01 04:44:14 | 16860 | 5 | 2018-04-01 04:44:03 | 2018-03-31 18:16:16 | 60D53EE6 |
| GAMEPANEL.EXE | 2018-04-01 04:44:49 | 2018-04-01 04:44:56 | 27448 | 1 | 2018-04-01 04:44:39 |  | 60D53EE6 |
| GAMEPANEL.EXE | 2018-03-31 18:16:23 | 2018-04-01 04:44:19 | 67086 | 5 | 2018-04-01 04:44:04 | 2018-03-31 18:16:17 | 60D53EE6 |
| GOOGLEUPDATE.EXE | 2018-01-30 16:22:59 | 2018-01-30 16:22:59 | 126214 | 1 | 2018-01-30 16:22:49 |  | 60D53EE6 |
| GOOGLEUPDATE.EXE | 2018-01-30 16:22:54 | 2018-04-03 16:31:16 | 58752 | 19 | 2018-04-03 16:31:16 | 2018-04-03 00:10:01 | 60D53EE6 |
| GOOGLEUPDATE.EXE | 2018-01-30 16:22:55 | 2018-01-30 16:22:55 | 54528 | 1 | 2018-01-30 16:22:45 |  | 60D53EE6 |
| HELPER.EXE | 2018-03-31 23:52:44 | 2018-03-31 23:52:44 | 36542 | 1 | 2018-03-31 23:52:41 |  | 60D53EE6 |
| HXTSR.EXE | 2018-03-31 16:41:29 | 2018-04-03 16:14:20 | 70292 | 6 | 2018-04-03 16:14:19 | 2018-03-31 16:41:19 | 60D53EE6 |
| ICACLS.EXE | 2018-04-03 00:11:41 | 2018-04-03 00:11:42 | 13076 | 2 | 2018-04-03 00:11:42 | 2018-04-03 00:11:40 | 60D53EE6 |
| IEXPLORE.EXE | 2018-03-31 13:04:04 | 2018-03-31 13:04:12 | 161778 | 2 | 2018-03-31 13:04:02 | 2018-03-31 13:03:54 | 60D53EE6 |
| IEXPLORE.EXE | 2018-03-31 13:04:03 | 2018-03-31 13:04:03 | 92784 | 1 | 2018-03-31 13:03:53 |  | 60D53EE6 |
| IPCONFIG.EXE | 2018-03-31 23:42:30 | 2018-04-03 16:25:15 | 10146 | 8 | 2018-04-03 16:25:08 | 2018-03-31 23:42:26 | 60D53EE6 |
| IRONKEY.EXE | 2018-03-31 14:41:41 | 2018-03-31 14:41:41 | 54718 | 1 | 2018-03-31 14:41:31 |  | BAA935F8 |
| IRONKEY.EXE | 2018-03-31 14:03:22 | 2018-04-03 16:15:20 | 61610 | 4 | 2018-04-03 16:15:09 | 2018-03-31 14:03:11 | BAA935F8 |
| IRONKEY.EXE | 2018-03-31 14:03:12 | 2018-04-03 16:15:09 | 55902 | 4 | 2018-04-03 16:15:09 | 2018-03-31 14:03:11 | BAA935F8 |
| LOCKAPP.EXE | 2018-03-30 15:29:18 | 2018-04-03 01:35:50 | 101274 | 3 | 2018-04-03 01:35:40 | 2018-03-30 15:29:08 | 60D53EE6 |
| LOGONUI.EXE | 2018-03-27 00:11:12 | 2018-04-03 16:17:42 | 132142 | 18 | 2018-04-03 16:17:39 | 2018-04-03 00:12:30 | 60D53EE6 |
| MANAGEMENTAGENTHOST.EXE | 2018-04-03 16:31:27 | 2018-04-03 16:31:27 | 53456 | 1 | 2018-04-03 16:31:17 |  | 60D53EE6 |
| MICROSOFT.PHOTOS.EXE | 2018-03-31 15:37:21 | 2018-04-03 00:58:59 | 221186 | 3 | 2018-04-03 00:58:47 | 2018-03-31 15:37:13 | 60D53EE6 |
| MICROSOFTEDGE.EXE | 2018-04-03 13:37:42 | 2018-04-03 13:37:42 | 140114 | 1 | 2018-04-03 13:37:32 |  | 60D53EE6 |
| MICROSOFTEDGE.EXE | 2018-03-30 15:10:09 | 2018-03-31 16:08:22 | 228222 | 3 | 2018-03-31 16:08:12 | 2018-03-30 15:09:59 | 60D53EE6 |
| MICROSOFTEDGECP.EXE | 2018-03-30 15:10:20 | 2018-03-31 16:08:24 | 200596 | 18 | 2018-03-31 16:08:14 | 2018-03-31 14:48:05 | 60D53EE6 |
| MICROSOFTEDGECP.EXE | 2018-04-03 13:37:46 | 2018-04-03 13:42:35 | 87102 | 6 | 2018-04-03 13:42:24 | 2018-04-03 13:37:36 | 60D53EE6 |
| MMC.EXE | 2018-03-31 12:50:10 | 2018-03-31 12:50:10 | 248104 | 1 | 2018-03-31 12:50:00 |  | 60D53EE6 |
| MMC.EXE | 2018-01-30 16:17:25 | 2018-01-30 16:17:25 | 129324 | 1 | 2018-01-30 16:17:15 |  | 60D53EE6 |
| MOBSYNC.EXE | 2018-03-27 00:12:39 | 2018-04-03 00:59:00 | 36238 | 8 | 2018-04-03 00:58:49 | 2018-03-27 00:12:29 | 60D53EE6 |
| MPAM-9B898230.EXE | 2018-04-01 15:24:45 | 2018-04-01 15:24:45 | 123542 | 1 | 2018-04-01 15:24:35 |  | 60D53EE6 |
| MPAM-C74E2EB3.EXE | 2018-04-03 00:20:36 | 2018-04-03 00:20:36 | 92820 | 1 | 2018-04-03 00:20:24 |  | 60D53EE6 |
| MPCMDRUN.EXE | 2018-03-31 12:57:31 | 2018-04-03 16:39:26 | 38446 | 19 | 2018-04-03 16:39:16 | 2018-04-03 00:19:30 | 60D53EE6 |
| MPCMDRUN.EXE | 2018-03-30 15:14:58 | 2018-03-31 12:22:50 | 33694 | 5 | 2018-03-31 12:22:40 | 2018-03-30 15:14:38 | 60D53EE6 |
| MPSIGSTUB.EXE | 2018-04-03 00:20:47 | 2018-04-03 00:20:47 | 142560 | 1 | 2018-04-03 00:20:44 |  | 60D53EE6 |
| MPSIGSTUB.EXE | 2018-04-01 15:24:38 | 2018-04-01 15:24:38 | 144464 | 1 | 2018-04-01 15:24:37 |  | 60D53EE6 |
| MPSIGSTUB.EXE | 2018-04-01 15:23:54 | 2018-04-03 16:32:34 | 268436 | 2 | 2018-04-03 16:32:33 | 2018-04-01 15:23:53 | 60D53EE6 |
| MRT-KB890830.EXE | 2018-04-03 00:21:33 | 2018-04-03 00:21:33 | 125292 | 1 | 2018-04-03 00:21:31 |  | 60D53EE6 |
| MSASCUIL.EXE | 2018-03-27 00:12:45 | 2018-04-03 16:30:52 | 28942 | 9 | 2018-04-03 16:30:42 | 2018-03-30 15:14:38 | 60D53EE6 |
| MSCORSVW.EXE | 2018-03-31 17:37:18 | 2018-04-03 01:12:53 | 130358 | 14 | 2018-04-03 01:12:53 | 2018-04-03 00:58:24 | 60D53EE6 |
| MSCORSVW.EXE | 2018-03-31 17:37:11 | 2018-04-03 01:12:20 | 88702 | 13 | 2018-04-03 01:12:20 | 2018-03-31 17:37:18 | 60D53EE6 |
| MSI2FF8.TMP | 2018-03-31 14:20:51 | 2018-03-31 14:20:51 | 91094 | 1 | 2018-03-31 14:20:41 |  | BAA935F8 |
| MSIEXEC.EXE | 2018-03-30 15:12:23 | 2018-04-03 16:46:23 | 51514 | 4 | 2018-04-03 16:46:13 | 2018-03-30 15:12:13 | BAA935F8 |
| MSIEXEC.EXE | 2018-03-30 15:11:54 | 2018-04-03 16:46:23 | 102060 | 12 | 2018-04-03 16:46:13 | 2018-03-31 13:06:53 | 60D53EE6 |
| MSINFO32.EXE | 2018-03-27 00:13:21 | 2018-03-27 00:13:21 | 38076 | 2 | 2018-03-27 00:13:11 | 2018-03-27 00:13:11 | 60D53EE6 |
| MSPAINT.EXE | 2018-03-31 15:37:10 | 2018-03-31 15:37:10 | 76642 | 1 | 2018-03-31 15:37:07 |  | 60D53EE6 |
| MSTSC.EXE | 2018-03-31 17:14:52 | 2018-03-31 17:16:04 | 52864 | 2 | 2018-03-31 17:15:54 | 2018-03-31 17:14:42 | 60D53EE6 |
| MUSIC.UI.EXE | 2018-03-31 15:05:13 | 2018-03-31 15:05:13 | 182586 | 1 | 2018-03-31 15:05:08 |  | 60D53EE6 |
| MUSNOTIFICATIONUX.EXE | 2018-04-03 00:54:18 | 2018-04-03 00:54:22 | 60534 | 2 | 2018-04-03 00:54:20 | 2018-04-03 00:54:17 | 60D53EE6 |
| NGEN.EXE | 2018-03-31 17:37:10 | 2018-04-03 01:12:02 | 28084 | 13 | 2018-04-03 01:11:52 | 2018-03-31 17:37:18 | 60D53EE6 |
| NGEN.EXE | 2018-03-31 17:37:10 | 2018-04-03 01:12:06 | 18230 | 13 | 2018-04-03 01:11:57 | 2018-03-31 17:37:19 | 60D53EE6 |
| NGENTASK.EXE | 2018-03-31 17:37:20 | 2018-04-03 01:14:09 | 87616 | 6 | 2018-04-03 01:14:09 | 2018-03-31 17:37:10 | 60D53EE6 |
| NGENTASK.EXE | 2018-03-31 17:37:20 | 2018-04-03 01:14:06 | 88774 | 6 | 2018-04-03 01:14:06 | 2018-03-31 17:37:10 | 60D53EE6 |
| NOTEPAD.EXE | 2018-03-31 16:08:04 | 2018-03-31 16:08:04 | 42820 | 1 | 2018-03-31 16:08:02 |  | 60D53EE6 |
| ONEDRIVE.EXE | 2018-03-31 14:49:46 | 2018-04-03 00:59:07 | 149932 | 5 | 2018-04-03 00:58:57 | 2018-03-31 14:49:36 | 60D53EE6 |
| ONEDRIVE.EXE | 2018-04-03 00:14:22 | 2018-04-03 16:30:57 | 119214 | 2 | 2018-04-03 16:30:47 | 2018-04-03 00:14:12 | 60D53EE6 |
| ONEDRIVESETUP.EXE | 2018-03-31 14:49:47 | 2018-04-03 00:09:56 | 211658 | 4 | 2018-04-03 00:09:53 | 2018-03-31 14:49:46 | 60D53EE6 |
| ONEDRIVESETUP.EXE | 2018-03-27 00:12:37 | 2018-03-31 14:48:31 | 176620 | 4 | 2018-03-31 14:48:21 | 2018-03-27 00:12:36 | 60D53EE6 |
| OOBENETWORKCONNECTIONFLOW.EXE | 2018-03-27 00:07:26 | 2018-03-27 00:07:26 | 172228 | 1 | 2018-03-27 00:07:19 |  | 60D53EE6 |
| OPENWITH.EXE | 2018-03-31 15:37:08 | 2018-03-31 15:37:08 | 110202 | 1 | 2018-03-31 15:37:03 |  | 60D53EE6 |
| PHOTOSCREENSAVER.SCR | 2018-03-31 16:07:34 | 2018-03-31 16:07:34 | 52874 | 1 | 2018-03-31 16:07:31 |  | 60D53EE6 |
| PING.EXE | 2018-04-03 13:37:05 | 2018-04-03 13:37:23 | 12512 | 2 | 2018-04-03 13:37:23 | 2018-04-03 13:37:05 | 60D53EE6 |
| PINGSENDER.EXE | 2018-03-31 15:42:52 | 2018-04-03 16:41:54 | 48048 | 4 | 2018-04-03 16:41:51 | 2018-03-31 15:42:51 | 60D53EE6 |
| POQEXEC.EXE | 2018-04-03 00:54:59 | 2018-04-03 00:54:59 | 42168 | 1 | 2018-04-03 00:54:49 |  | 60D53EE6 |
| PUTTY.EXE | 2018-03-31 16:08:44 | 2018-03-31 17:14:22 | 33362 | 2 | 2018-03-31 17:14:12 | 2018-03-31 16:08:34 | 60D53EE6 |
| QTWEBENGINEPROCESS.EXE | 2018-03-31 13:09:43 | 2018-04-03 16:41:47 | 83268 | 3 | 2018-04-03 16:41:40 | 2018-03-31 13:09:33 | 60D53EE6 |
| REGSVR32.EXE | 2018-03-27 00:01:48 | 2018-03-31 13:08:49 | 29434 | 4 | 2018-03-31 13:08:49 | 2018-03-27 00:01:46 | 60D53EE6 |
| REGSVR32.EXE | 2018-03-27 00:01:51 | 2018-03-31 13:08:49 | 31036 | 6 | 2018-03-31 13:08:49 | 2018-03-27 00:01:48 | 60D53EE6 |
| RUNDLL32.EXE | 2018-03-27 00:01:48 | 2018-04-03 01:03:17 | 24082 | 18 | 2018-04-03 01:03:07 | 2018-03-31 12:49:15 | 60D53EE6 |
| RUNDLL32.EXE | 2018-03-30 15:28:06 | 2018-03-30 15:28:06 | 36130 | 1 | 2018-01-30 16:27:57 |  | 60D53EE6 |
| RUNDLL32.EXE | 2018-04-03 00:50:09 | 2018-04-03 00:50:09 | 16610 | 1 | 2018-04-03 00:50:08 |  | 60D53EE6 |
| RUNDLL32.EXE | 2018-03-31 16:06:20 | 2018-03-31 16:06:20 | 15352 | 1 | 2018-03-31 16:06:08 |  | 60D53EE6 |
| RUNDLL32.EXE | 2018-03-30 15:11:17 | 2018-04-03 12:29:42 | 20068 | 4 | 2018-04-03 12:29:37 | 2018-03-30 15:11:16 | 60D53EE6 |
| RUNDLL32.EXE | 2018-03-31 12:43:42 | 2018-04-03 16:43:42 | 19918 | 6 | 2018-04-03 16:43:41 | 2018-03-31 12:43:42 | 60D53EE6 |
| RUNONCE.EXE | 2018-04-03 00:09:54 | 2018-04-03 16:30:55 | 49190 | 4 | 2018-04-03 16:30:49 | 2018-04-03 00:09:48 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 12:49:25 | 2018-04-03 16:30:41 | 126230 | 6 | 2018-04-03 16:30:31 | 2018-03-31 12:49:15 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-27 00:13:17 | 2018-04-03 12:39:52 | 42022 | 6 | 2018-04-03 12:39:42 | 2018-03-27 00:13:07 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-04-03 13:37:47 | 2018-04-03 13:37:47 | 20706 | 1 | 2018-04-03 13:37:36 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-27 00:11:21 | 2018-04-03 16:30:39 | 56578 | 8 | 2018-04-03 16:30:29 | 2018-03-27 00:11:11 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 15:23:50 | 2018-03-31 15:23:50 | 11266 | 1 | 2018-03-31 15:23:40 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-27 00:01:51 | 2018-04-03 16:47:52 | 111920 | 21 | 2018-04-03 16:47:42 | 2018-04-03 00:22:37 | 4EE65D55 |
| RUNTIMEBROKER.EXE | 2018-03-31 16:41:31 | 2018-04-03 16:30:56 | 33154 | 10 | 2018-04-03 16:30:46 | 2018-04-01 04:40:18 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 15:37:24 | 2018-03-31 15:37:24 | 80092 | 1 | 2018-03-31 15:37:14 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-04-03 00:19:02 | 2018-04-03 00:19:02 | 17938 | 1 | 2018-04-03 00:18:51 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 16:08:23 | 2018-03-31 16:08:23 | 31462 | 1 | 2018-03-31 16:08:13 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 16:08:24 | 2018-03-31 16:08:24 | 20386 | 1 | 2018-03-31 16:08:14 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 23:42:38 | 2018-04-03 01:35:51 | 108012 | 2 | 2018-04-03 01:35:40 | 2018-03-31 23:42:28 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 19:36:32 | 2018-03-31 23:52:41 | 61250 | 2 | 2018-03-31 23:52:31 | 2018-03-31 19:36:17 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-04-03 16:35:36 | 2018-04-03 16:35:36 | 19710 | 1 | 2018-04-03 16:35:26 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-27 00:11:20 | 2018-03-31 14:48:01 | 50000 | 3 | 2018-03-31 14:47:48 | 2018-03-27 00:11:10 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-03-31 16:05:06 | 2018-04-03 12:40:58 | 18342 | 2 | 2018-04-03 12:40:48 | 2018-03-31 16:04:54 | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-04-03 13:37:45 | 2018-04-03 13:37:45 | 31382 | 1 | 2018-04-03 13:37:35 |  | 60D53EE6 |
| RUNTIMEBROKER.EXE | 2018-04-03 00:19:06 | 2018-04-03 00:19:06 | 21790 | 1 | 2018-04-03 00:18:56 |  | 60D53EE6 |
| SCALC.EXE | 2018-03-31 15:38:32 | 2018-03-31 15:38:32 | 10132 | 1 | 2018-03-31 15:38:21 |  | 60D53EE6 |
| SCRNSAVE.SCR | 2018-03-31 16:07:31 | 2018-03-31 16:07:31 | 16814 | 1 | 2018-03-31 16:07:29 |  | 60D53EE6 |
| SDIAGNHOST.EXE | 2018-04-03 00:50:14 | 2018-04-03 00:50:14 | 168934 | 1 | 2018-04-03 00:50:09 |  | 60D53EE6 |
| SEARCHFILTERHOST.EXE | 2018-03-27 00:13:35 | 2018-04-03 16:59:12 | 17528 | 74 | 2018-04-03 16:59:02 | 2018-04-03 13:39:34 | 60D53EE6 |
| SEARCHINDEXER.EXE | 2018-04-03 00:57:54 | 2018-04-03 00:57:54 | 56676 | 1 | 2018-04-03 00:57:44 |  | 60D53EE6 |
| SEARCHPROTOCOLHOST.EXE | 2018-03-27 00:13:35 | 2018-04-03 16:59:12 | 19870 | 65 | 2018-04-03 16:59:02 | 2018-04-03 13:37:25 | 60D53EE6 |
| SEARCHUI.EXE | 2018-03-27 00:14:36 | 2018-04-03 16:30:39 | 327358 | 10 | 2018-04-03 16:30:28 | 2018-03-31 12:49:13 | 60D53EE6 |
| SETTINGSYNCHOST.EXE | 2018-03-27 00:12:34 | 2018-03-31 14:48:16 | 26628 | 2 | 2018-03-31 14:48:06 | 2018-03-27 00:12:24 | 60D53EE6 |
| SETUP-STUB.EXE | 2018-01-30 16:26:43 | 2018-01-30 16:26:45 | 102566 | 2 | 2018-01-30 16:26:35 | 2018-01-30 16:26:33 | 60D53EE6 |
| SETUP64.EXE | 2018-03-30 15:11:36 | 2018-03-30 15:11:36 | 46818 | 1 | 2018-03-30 15:11:35 |  | 60D53EE6 |
| SHELLEXPERIENCEHOST.EXE | 2018-03-31 12:49:23 | 2018-04-03 16:30:39 | 230200 | 9 | 2018-04-03 16:30:28 | 2018-03-31 13:09:25 | 60D53EE6 |
| SIHOST.EXE | 2018-03-27 00:11:13 | 2018-04-03 00:58:48 | 66926 | 6 | 2018-04-03 00:58:38 | 2018-03-27 00:11:01 | 60D53EE6 |
| SIMPRESS.EXE | 2018-03-31 14:22:10 | 2018-03-31 14:42:46 | 10090 | 4 | 2018-03-31 14:42:39 | 2018-03-31 14:22:00 | 60D53EE6 |
| SLITHERIO.EXE | 2018-03-31 16:05:12 | 2018-04-03 00:59:03 | 107090 | 3 | 2018-04-03 00:58:59 | 2018-03-31 16:05:09 | 60D53EE6 |
| SLUI.EXE | 2018-03-27 00:02:06 | 2018-04-03 16:30:39 | 35804 | 41 | 2018-04-03 16:30:28 | 2018-04-03 12:29:45 | 60D53EE6 |
| SMARTSCREEN.EXE | 2018-03-27 00:01:48 | 2018-04-03 16:39:27 | 83040 | 29 | 2018-04-03 16:39:17 | 2018-04-03 00:45:32 | 60D53EE6 |
| SMSS.EXE | 2018-03-27 00:11:01 | 2018-04-03 16:17:42 | 10010 | 7 | 2018-04-03 16:17:42 | 2018-03-27 00:11:01 | 60D53EE6 |
| SOFFICE.BIN | 2018-03-31 14:21:39 | 2018-03-31 23:11:06 | 364312 | 16 | 2018-03-31 23:10:56 | 2018-03-31 14:42:50 | CBB6FC8 |
| SOFFICE.EXE | 2018-03-31 14:21:46 | 2018-03-31 23:11:06 | 15248 | 15 | 2018-03-31 23:10:55 | 2018-03-31 14:42:59 | 60D53EE6 |
| SPEECHRUNTIME.EXE | 2018-03-27 00:02:29 | 2018-04-03 00:54:22 | 77954 | 9 | 2018-04-03 00:54:19 | 2018-03-27 00:05:48 | 60D53EE6 |
| SPPEXTCOMOBJ.EXE | 2018-03-27 00:02:06 | 2018-04-03 16:30:39 | 22324 | 26 | 2018-04-03 16:30:27 | 2018-04-03 00:57:59 | 60D53EE6 |
| SPPSVC.EXE | 2018-03-27 00:13:49 | 2018-04-03 16:31:26 | 45962 | 28 | 2018-04-03 16:31:16 | 2018-04-03 12:29:44 | 60D53EE6 |
| STRITZ.EXE | 2018-03-31 23:52:41 | 2018-03-31 23:52:41 | 338584 | 1 | 2018-03-31 23:52:30 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:31:29 | 2018-04-03 16:31:29 | 20950 | 1 | 2018-04-03 16:31:19 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:44:05 | 2018-04-03 16:44:05 | 60226 | 1 | 2018-04-03 16:43:54 |  | 4EE65D55 |
| SVCHOST.EXE | 2018-04-03 16:30:57 | 2018-04-03 16:30:57 | 30530 | 1 | 2018-04-03 16:30:47 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-03-31 18:16:29 | 2018-04-01 04:43:50 | 18500 | 4 | 2018-04-01 04:43:38 | 2018-03-31 18:16:19 | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:32:39 | 2018-04-03 16:32:39 | 24416 | 1 | 2018-04-03 16:32:28 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-03-27 00:11:16 | 2018-04-03 16:30:51 | 56724 | 19 | 2018-04-03 16:30:40 | 2018-03-30 15:43:04 | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:41:39 | 2018-04-03 16:41:39 | 12240 | 1 | 2018-04-03 16:41:29 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:39:27 | 2018-04-03 16:39:27 | 18496 | 1 | 2018-04-03 16:39:17 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:41:39 | 2018-04-03 16:41:39 | 37500 | 1 | 2018-04-03 16:41:29 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-03-30 15:30:45 | 2018-04-03 01:10:05 | 20140 | 4 | 2018-04-03 01:09:55 | 2018-03-30 15:30:35 | CCD44B81 |
| SVCHOST.EXE | 2018-04-03 16:48:04 | 2018-04-03 16:48:04 | 29328 | 1 | 2018-04-03 16:47:54 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:32:25 | 2018-04-03 16:32:25 | 37632 | 1 | 2018-04-03 16:32:15 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:31:28 | 2018-04-03 16:31:28 | 23112 | 1 | 2018-04-03 16:31:18 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 00:13:56 | 2018-04-03 01:03:16 | 40664 | 2 | 2018-04-03 01:03:06 | 2018-04-03 00:13:41 | 60D53EE6 |
| SVCHOST.EXE | 2018-03-30 15:43:28 | 2018-04-03 14:01:49 | 33944 | 16 | 2018-04-03 14:01:39 | 2018-03-31 23:58:22 | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 00:59:03 | 2018-04-03 16:31:26 | 14974 | 2 | 2018-04-03 16:31:16 | 2018-04-03 00:58:51 | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:41:34 | 2018-04-03 16:41:34 | 19966 | 1 | 2018-04-03 16:41:24 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:39:27 | 2018-04-03 16:39:27 | 43860 | 1 | 2018-04-03 16:39:19 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:32:27 | 2018-04-03 16:45:40 | 21568 | 4 | 2018-04-03 16:45:30 | 2018-04-03 16:32:17 | 60D53EE6 |
| SVCHOST.EXE | 2018-03-31 15:37:18 | 2018-03-31 15:37:18 | 26034 | 1 | 2018-03-31 15:37:08 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 12:32:59 | 2018-04-03 12:32:59 | 38276 | 1 | 2018-04-03 12:32:49 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:44:02 | 2018-04-03 16:44:02 | 17714 | 1 | 2018-04-03 16:43:52 |  | 4EE65D55 |
| SVCHOST.EXE | 2018-03-30 15:13:00 | 2018-04-03 16:31:05 | 22700 | 12 | 2018-04-03 16:30:55 | 2018-03-31 14:38:48 | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:46:24 | 2018-04-03 16:46:24 | 15406 | 1 | 2018-04-03 16:46:14 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-03-30 15:30:46 | 2018-04-03 16:25:19 | 21952 | 16 | 2018-04-03 16:25:09 | 2018-04-01 02:29:19 | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 00:58:37 | 2018-04-03 00:58:37 | 21038 | 1 | 2018-04-03 00:58:27 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:31:27 | 2018-04-03 16:31:27 | 21288 | 1 | 2018-04-03 16:31:17 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-03-30 15:30:46 | 2018-04-03 13:48:23 | 21036 | 8 | 2018-04-03 13:48:13 | 2018-03-30 15:30:36 | 60D53EE6 |
| SVCHOST.EXE | 2018-04-03 16:31:29 | 2018-04-03 16:31:29 | 44920 | 1 | 2018-04-03 16:31:19 |  | 60D53EE6 |
| SVCHOST.EXE | 2018-03-31 14:47:49 | 2018-04-03 00:13:50 | 97500 | 3 | 2018-04-03 00:13:39 | 2018-03-31 14:47:35 | 60D53EE6 |
| SVCHOST.EXE | 2018-03-27 00:02:29 | 2018-04-03 12:33:19 | 50552 | 10 | 2018-04-03 12:33:09 | 2018-03-27 00:09:39 | 60D53EE6 |
| SWRITER.EXE | 2018-03-31 14:21:46 | 2018-03-31 23:11:06 | 11118 | 13 | 2018-03-31 23:10:55 | 2018-03-31 14:45:42 | 60D53EE6 |
| SYSTEMPROPERTIESCOMPUTERNAME. | 2018-03-31 12:44:27 | 2018-03-31 12:44:27 | 42708 | 1 | 2018-03-31 12:44:17 |  | 60D53EE6 |
| SYSTEMSETTINGS.EXE | 2018-03-30 15:16:03 | 2018-04-03 00:54:27 | 229842 | 6 | 2018-04-03 00:54:17 | 2018-03-30 15:15:52 | 60D53EE6 |
| SYSTEMSETTINGSADMINFLOWS.EXE | 2018-03-30 15:16:00 | 2018-03-31 12:53:41 | 99674 | 3 | 2018-03-31 12:53:35 | 2018-03-30 15:16:00 | 60D53EE6 |
| TASKHOSTW.EXE | 2018-03-27 00:05:53 | 2018-04-03 16:45:24 | 69648 | 74 | 2018-04-03 16:45:24 | 2018-04-03 13:44:09 | 60D53EE6 |
| TASKLIST.EXE | 2018-01-30 16:21:25 | 2018-04-03 16:56:25 | 24820 | 83 | 2018-04-03 16:56:25 | 2018-04-03 01:24:00 | 60D53EE6 |
| TIWORKER.EXE | 2018-04-03 00:19:20 | 2018-04-03 16:32:29 | 61488 | 6 | 2018-04-03 16:32:19 | 2018-04-03 00:19:10 | 60D53EE6 |
| TIWORKER.EXE | 2018-03-30 14:07:56 | 2018-04-03 00:12:29 | 819452 | 7 | 2018-04-03 00:12:19 | 2018-03-30 14:07:46 | 60D53EE6 |
| TRUSTEDINSTALLER.EXE | 2018-03-30 14:07:56 | 2018-04-03 16:45:34 | 20056 | 18 | 2018-04-03 16:45:24 | 2018-04-03 00:28:41 | 60D53EE6 |
| UNSECAPP.EXE | 2018-04-03 13:46:46 | 2018-04-03 13:46:46 | 17688 | 1 | 2018-04-03 13:46:36 |  | 60D53EE6 |
| USERINIT.EXE | 2018-04-03 00:13:56 | 2018-04-03 00:13:56 | 13760 | 1 | 2018-04-03 00:13:41 |  | 60D53EE6 |
| VC\_REDIST.X64.EXE | 2018-03-31 14:21:10 | 2018-03-31 14:21:10 | 69348 | 1 | 2018-03-31 14:21:08 |  | 60D53EE6 |
| VCREDIST\_X64.EXE | 2018-03-30 15:11:57 | 2018-03-30 15:11:57 | 61958 | 1 | 2018-03-30 15:11:49 |  | 60D53EE6 |
| VCREDIST\_X86.EXE | 2018-03-30 15:11:46 | 2018-03-30 15:11:46 | 60472 | 1 | 2018-03-30 15:11:36 |  | 60D53EE6 |
| VMTOOLSD.EXE | 2018-03-30 15:13:31 | 2018-04-03 16:30:54 | 229526 | 9 | 2018-04-03 16:30:43 | 2018-03-30 15:13:21 | 60D53EE6 |
| VMWARERESOLUTIONSET.EXE | 2018-04-01 04:48:00 | 2018-04-03 16:15:52 | 32166 | 5 | 2018-04-03 16:15:51 | 2018-04-01 04:47:59 | 60D53EE6 |
| VSSVC.EXE | 2018-03-30 15:30:46 | 2018-04-03 13:48:23 | 23482 | 8 | 2018-04-03 13:48:13 | 2018-03-30 15:30:36 | 60D53EE6 |
| WERFAULT.EXE | 2018-03-31 14:38:49 | 2018-04-03 00:11:20 | 119026 | 3 | 2018-04-03 00:11:10 | 2018-03-31 14:38:48 | BAA935F8 |
| WERFAULT.EXE | 2018-04-03 00:18:42 | 2018-04-03 00:18:52 | 31764 | 2 | 2018-04-03 00:18:42 | 2018-04-03 00:18:42 | 60D53EE6 |
| WERMGR.EXE | 2018-04-03 00:19:52 | 2018-04-03 01:05:49 | 25108 | 2 | 2018-04-03 01:05:48 | 2018-04-03 00:19:46 | 60D53EE6 |
| WHOAMI.EXE | 2018-04-03 13:37:18 | 2018-04-03 13:37:18 | 15160 | 1 | 2018-04-03 13:37:18 |  | 60D53EE6 |
| WINDOWS-KB890830-X64-V5.58.EX | 2018-04-03 00:21:15 | 2018-04-03 00:21:15 | 8130 | 1 | 2018-04-03 00:21:10 |  | 60D53EE6 |
| WINLOGON.EXE | 2018-03-27 00:11:12 | 2018-04-03 16:17:52 | 33798 | 7 | 2018-04-03 16:17:42 | 2018-03-27 00:11:01 | 60D53EE6 |
| WINSAT.EXE | 2018-04-03 01:14:20 | 2018-04-03 01:14:20 | 39676 | 1 | 2018-04-03 01:14:10 |  | 60D53EE6 |
| WINSTORE.APP.EXE | 2018-04-03 16:35:36 | 2018-04-03 16:35:36 | 124894 | 1 | 2018-04-03 16:35:26 |  | 60D53EE6 |
| WMIADAP.EXE | 2018-03-27 00:03:53 | 2018-04-03 16:33:09 | 20628 | 15 | 2018-04-03 16:33:09 | 2018-04-01 15:14:55 | 60D53EE6 |
| WMIAPSRV.EXE | 2018-04-03 00:22:37 | 2018-04-03 16:33:46 | 21750 | 7 | 2018-04-03 16:33:36 | 2018-04-03 00:22:26 | 60D53EE6 |
| WMIPRVSE.EXE | 2018-03-27 00:09:56 | 2018-04-03 16:26:23 | 50656 | 20 | 2018-04-03 16:26:13 | 2018-04-01 15:13:46 | 60D53EE6 |
| WMIPRVSE.EXE | 2018-03-31 13:09:35 | 2018-04-03 16:31:06 | 24584 | 5 | 2018-04-03 16:30:55 | 2018-03-31 13:09:25 | 60D53EE6 |
| WUAUCLT.EXE | 2018-04-01 15:24:02 | 2018-04-03 16:32:43 | 103366 | 6 | 2018-04-03 16:32:33 | 2018-04-01 15:23:52 | 60D53EE6 |
| WUDFHOST.EXE | 2018-03-31 14:03:15 | 2018-04-03 16:41:35 | 27256 | 11 | 2018-04-03 16:41:25 |  | 60D53EE6 |
| WWAHOST.EXE | 2018-03-27 00:01:48 | 2018-03-31 12:51:42 | 258802 | 2 | 2018-03-31 12:51:32 | 2018-03-27 00:01:37 | 60D53EE6 |

## APPENDIX V: Shellbag Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AbsolutePath | ShellType | Value | FirstInteracted | LastInteracted |
| Desktop\Control Panel | Root folder: GUID | Control Panel |  |  |
| Desktop\Control Panel\System and Security | Control Panel Category | System and Security |  | 2018-03-31 12:46:31 |
| Desktop\Control Panel\System and Security\System | GUID: Control panel | System | 2018-03-31 12:46:31 | 2018-03-31 12:46:31 |
| Desktop\E:\ | Users property view: Drive letter | E:\ |  |  |
| Desktop\E:\ | Users property view: Drive letter | E:\ | 2018-03-31 15:36:58 | 2018-04-03 13:59:22 |
| Desktop\E:\\Documents | Directory | Documents | 2018-03-31 14:43:06 | 2018-03-31 14:43:06 |
| Desktop\F:\ | Users property view: Drive letter | F:\ |  | 2018-04-03 16:43:43 |
| Desktop\F:\\Forensic Software | Directory | Forensic Software |  | 2018-04-03 16:43:41 |
| Desktop\F:\\Forensic Software\FTK Imager | Directory | FTK Imager |  | 2018-04-03 16:43:42 |
| Desktop\F:\\Forensic Software\FTK Imager\FTK Imager | Directory | FTK Imager | 2018-04-03 16:43:43 | 2018-04-03 16:43:43 |
| Desktop\Home Folder | Root folder: GUID | Home Folder | 2018-03-31 12:43:42 |  |
| Desktop\Home Folder | Root folder: GUID | Home Folder | 2018-03-31 15:36:58 |  |
| Desktop\My Computer | Root folder: GUID | My Computer |  |  |
| Desktop\My Computer | Root folder: GUID | My Computer |  |  |
| Desktop\My Computer\C: | Drive letter | C: |  |  |
| Desktop\My Computer\C: | Drive letter | C: |  |  |
| Desktop\My Computer\C:\Users | Directory | Users |  | 2018-03-31 14:46:26 |
| Desktop\My Computer\C:\Users | Directory | Users |  | 2018-03-31 15:37:50 |
| Desktop\My Computer\C:\Users\ethomas | Directory | ethomas | 2018-03-31 14:46:27 | 2018-03-31 14:46:27 |
| Desktop\My Computer\C:\Users\ethomas | Directory | ethomas |  | 2018-03-31 15:37:51 |
| Desktop\My Computer\C:\Users\ethomas\Documents | Directory | Documents | 2018-03-31 15:38:00 | 2018-03-31 15:38:00 |
| Desktop\My Computer\Desktop | Root folder: GUID | Desktop | 2018-04-03 00:16:48 | 2018-04-03 00:16:48 |
| Desktop\My Computer\Desktop | Root folder: GUID | Desktop | 2018-03-31 15:54:12 |  |
| Desktop\My Computer\Documents | Root folder: GUID | Documents | 2018-03-31 13:06:23 |  |
| Desktop\My Computer\Documents | Root folder: GUID | Documents | 2018-03-31 15:37:41 |  |
| Desktop\My Computer\Downloads | Root folder: GUID | Downloads | 2018-03-31 12:43:42 |  |
| Desktop\My Computer\Downloads | Root folder: GUID | Downloads | 2018-03-31 16:04:50 |  |
| Desktop\My Computer\E: | Drive letter | E: | 2018-04-03 13:36:33 | 2018-04-03 13:36:33 |
| Desktop\Search Folder | Users property view | Search Folder | 2018-04-03 00:15:17 |  |
| Desktop\Search Folder | Users property view | Search Folder | 2018-04-03 00:15:21 |  |
| Desktop\Search Folder | Users property view | Search Folder | 2018-04-03 00:16:53 |  |
| Desktop\Search Folder | Users property view | Search Folder | 2018-04-03 00:16:54 |  |
| Desktop\Search Folder | Users property view | Search Folder | 2018-04-03 00:10:04 |  |
| Desktop\Shared Documents Folder (Users Files) | Root folder: GUID | Shared Documents Folder (Users Files) |  |  |
| Desktop\Shared Documents Folder (Users Files)\Dropbox | Users Files Folder | Dropbox | 2018-03-31 13:21:49 | 2018-03-31 13:21:49 |

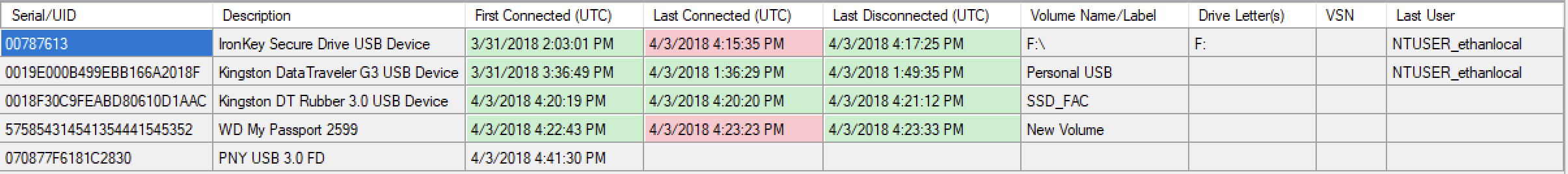
## APPENDIX VI: Link Analysis

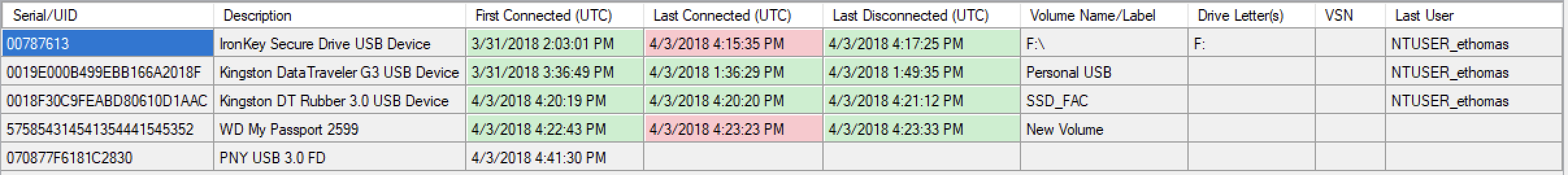
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| LocalPath | Src/Dst Created | Src/Dst Modified | Source  Accessed | File  Size | DriveType | VolumeSerial/Label | MachineID |
| C:\Users\ethomas\Dropbox\Intellectual Property Document.docx | 2018-03-31 14:43:38 | 2018-03-31 14:45:17 | 2018-03-31 14:45:17 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents\Proprietary Corporate Data.pptx | 2018-03-31 14:22:00 | 2018-03-31 14:42:39 | 2018-03-31 14:42:39 | 49764 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\9781111310646\_PPT\_ch07.pptx | 2018-03-31 14:41:52 | 2018-03-31 14:41:52 | 2018-03-31 14:41:52 | 493205 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\SFIR Lab Lesson 5.pptx | 2018-03-31 14:42:01 | 2018-03-31 14:42:01 | 2018-03-31 14:42:01 | 2193088 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\Sensitive Potential Client List.xlsx | 2018-03-31 14:22:13 | 2018-03-31 14:22:13 | 2018-03-31 14:22:13 | 9206 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Documents\EthanThomas\_Notes.docx | 2018-03-31 14:44:00 | 2018-03-31 14:45:48 | 2018-03-31 14:45:48 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents\Company Sensitive Document.docx | 2018-03-31 14:21:36 | 2018-03-31 14:45:42 | 2018-03-31 14:45:42 | 9007 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Dropbox | 2018-03-31 14:45:17 | 2018-03-31 14:45:23 | 2018-03-31 14:45:23 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\ | 2018-03-31 14:21:36 | 2018-03-31 14:42:59 | 2018-03-31 14:42:59 | 0 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Downloads | 2018-03-31 14:07:45 | 2018-03-31 14:07:45 | 2018-03-31 14:07:45 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| E:\Adorable Cats.jpg | 2018-03-31 15:37:03 | 2018-03-31 15:37:03 | 2018-03-31 15:37:03 | 14901 | Removable storage media (Floppy, USB) | 7295345F/Personal USB | ethomas\_desktop |
| C:\Users\ethan\_local\Desktop\Ethan Thomas Resignation Letter.docx | 2018-03-31 15:54:33 | 2018-03-31 23:10:56 | 2022-11-03 23:08:14 | 4620 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Intellectual Property Document.docx | 2018-03-31 15:38:39 | 2018-03-31 16:04:34 | 2022-11-03 23:08:14 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Sensitive Potential Client List.xlsx | 2018-03-31 15:38:22 | 2018-03-31 15:38:22 | 2018-03-31 15:38:22 | 7412 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\EthanThomas\_Notes.docx | 2018-03-31 15:38:34 | 2018-03-31 16:04:39 | 2018-03-31 16:04:39 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| E:\Cat in cute pose.jpg | 2018-03-31 15:37:14 | 2018-03-31 15:37:14 | 2018-03-31 15:37:14 | 25880 | Removable storage media (Floppy, USB) | 7295345F/Personal USB | ethomas\_desktop |
| E:\ | 2018-03-31 15:37:03 | 2018-03-31 15:39:16 | 2018-03-31 15:39:16 | 8192 | Removable storage media (Floppy, USB) | 7295345F/Personal USB | ethomas\_desktop |
| E:\Cat with Tongue Out.jpg | 2018-03-31 15:37:21 | 2018-03-31 15:37:21 | 2018-03-31 15:37:21 | 5919 | Removable storage media (Floppy, USB) | 7295345F/Personal USB | ethomas\_desktop |
| C:\Users\ethan\_local\Downloads | 2018-03-31 15:42:45 | 2018-03-31 15:42:45 | 2018-03-31 15:42:45 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |

## APPENDIX VII: Jump List Analysis

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| LocalPath | Target  Created | Target  Modified | Target  Accessed | File  Size | Drive  Type | VolumeSerial/Label | MachineID |
| F:\Sensitive Potential Client List.xlsx | 2018-03-30 18:18:45 | 2018-03-31 14:22:40 | 2018-03-31 04:00:00 | 7412 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Documents\EthanThomas\_Notes.docx | 2018-03-31 14:43:58 | 2018-03-31 14:44:00 | 2018-03-31 14:44:00 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents\Company Sensitive Document.docx | 2018-03-31 14:42:31 | 2018-03-30 18:00:42 | 2018-03-31 14:42:31 | 15967 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Dropbox\EthanThomas\_Notes.docx | 2018-03-31 14:45:12 | 2018-03-31 14:44:00 | 2018-03-31 14:45:12 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Dropbox\Intellectual Property Document.docx | 2018-03-31 14:45:12 | 2018-03-30 18:01:50 | 2018-03-31 14:45:12 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents\Intellectual Property Document.docx | 2018-03-31 14:42:31 | 2018-03-30 18:01:50 | 2018-03-31 14:42:31 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\Company Sensitive Document.docx | 2018-03-30 18:18:45 | 2018-03-30 18:00:42 | 2018-03-31 04:00:00 | 15967 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Documents\Proprietary Corporate Data.pptx | 2018-03-31 14:42:31 | 2018-03-30 18:15:24 | 2018-03-31 14:42:31 | 49764 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\SFIR Lab Lesson 5.pptx | 2018-03-31 14:40:26 | 2017-09-04 20:31:52 | 2018-03-31 04:00:00 | 2193088 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\9781111310646\_PPT\_ch07.pptx | 2018-03-31 14:41:00 | 2013-08-15 13:46:04 | 2018-03-31 04:00:00 | 493205 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\Proprietary Corporate Data.pptx | 2018-03-30 18:18:45 | 2018-03-30 18:15:24 | 2018-03-31 04:00:00 | 49764 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Dropbox | 2018-03-31 13:21:49 | 2018-03-31 14:45:54 | 2018-03-31 14:45:54 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents | 2018-03-27 00:09:38 | 2018-03-31 14:45:51 | 2018-03-31 14:45:51 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Downloads | 2018-03-27 00:09:38 | 2018-03-31 14:07:45 | 2018-03-31 14:07:45 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Desktop | 2018-03-27 00:09:38 | 2018-03-27 00:11:05 | 2018-03-27 00:11:05 | 0 | Fixed storage media (Hard drive) | 60D53EE6 | desktop-impb9r9 |
| C:\Users\ethomas\Videos | 2018-03-27 00:09:38 | 2018-03-27 00:11:05 | 2018-03-27 00:11:04 | 0 | Fixed storage media (Hard drive) | 60D53EE6 | desktop-impb9r9 |
| C:\Users\ethomas\Music | 2018-03-27 00:09:38 | 2018-03-27 00:11:05 | 2018-03-27 00:11:05 | 0 | Fixed storage media (Hard drive) | 60D53EE6 | desktop-impb9r9 |
| C:\Users\ethomas\Pictures | 2018-03-27 00:09:38 | 2018-03-27 00:11:05 | 2018-03-27 00:11:05 | 0 | Fixed storage media (Hard drive) | 60D53EE6 | desktop-impb9r9 |
| C:\Users\ethomas\Documents\EthanThomas\_Notes.docx | 2018-03-31 14:43:58 | 2018-03-31 14:44:00 | 2018-03-31 14:44:00 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Dropbox\Company Sensitive Document.docx | 2018-03-31 14:42:31 | 2018-03-31 14:43:21 | 2018-03-31 14:42:31 | 9007 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Dropbox\EthanThomas\_Notes.docx | 2018-03-31 14:45:12 | 2018-03-31 14:44:00 | 2018-03-31 14:45:12 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents\Intellectual Property Document.docx | 2018-03-31 14:42:31 | 2018-03-30 18:01:50 | 2018-03-31 14:42:31 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\Company Sensitive Document.docx | 2018-03-30 18:18:45 | 2018-03-30 18:00:42 | 2018-03-31 04:00:00 | 15967 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| C:\Users\ethomas\Documents\Proprietary Corporate Data.pptx | 2018-03-31 14:42:31 | 2018-03-30 18:15:24 | 2018-03-31 14:42:31 | 49764 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| F:\SFIR Lab Lesson 5.pptx | 2018-03-31 14:40:26 | 2017-09-04 20:31:52 | 2018-03-31 04:00:00 | 2193088 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\9781111310646\_PPT\_ch07.pptx | 2018-03-31 14:41:00 | 2013-08-15 13:46:04 | 2018-03-31 04:00:00 | 493205 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\Sensitive Potential Client List.xlsx | 2018-03-30 18:18:45 | 2018-03-30 18:17:48 | 2018-03-30 04:00:00 | 9206 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| F:\Proprietary Corporate Data.pptx | 2018-03-30 18:18:45 | 2018-03-30 18:15:24 | 2018-03-30 04:00:00 | 49764 | Removable storage media (Floppy, USB) | 0CBB6FC8/IronKey USB |  |
| E:\Cat with Tongue Out.jpg | 2018-03-30 19:18:13 | 2018-03-30 19:18:13 | 2018-03-30 19:18:13 | 5919 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| E:\Cat in cute pose.jpg | 2018-03-30 19:17:31 | 2018-03-30 19:17:31 | 2018-03-30 19:17:31 | 25880 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| E:\Adorable Cats.jpg | 2018-03-30 19:17:09 | 2018-03-30 19:17:09 | 2018-03-30 19:17:09 | 14901 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Sensitive Potential Client List.xlsx | 2018-03-31 15:38:15 | 2018-03-31 14:22:40 | 2018-03-31 15:38:15 | 7412 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
|  |  |  |  | 0 | (None) |  |  |
| C:\Windows\System32\mstsc.exe | 2017-09-29 13:42:03 | 2017-09-29 13:42:03 | 2017-09-29 13:42:03 | 3630080 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Desktop\Ethan Thomas Resignation Letter.docx | 2018-03-31 15:54:33 | 2018-03-31 15:54:33 | 2018-03-31 15:54:33 | 4619 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\EthanThomas\_Notes.docx | 2018-03-31 15:38:15 | 2018-03-31 14:44:00 | 2018-03-31 15:38:15 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Intellectual Property Document.docx | 2018-03-31 15:38:15 | 2018-03-30 18:01:50 | 2018-03-31 15:38:15 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| E:\Intellectual Property Document.docx | 2018-03-31 15:39:16 | 2018-03-31 15:39:16 | 2018-03-31 15:39:16 | 9015 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| C:\Users\ethan\_local\Desktop | 2018-03-31 14:47:33 | 2018-03-31 23:11:20 | 2018-03-31 23:11:20 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents | 2018-03-31 14:47:33 | 2018-03-31 16:04:42 | 2018-03-31 16:04:42 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Downloads | 2018-03-31 14:47:33 | 2018-03-31 15:42:45 | 2018-03-31 15:42:45 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethomas\Documents | 2018-03-27 00:09:38 | 2018-03-31 14:45:54 | 2018-03-31 14:45:54 | 4096 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Videos | 2018-03-31 14:47:33 | 2018-03-31 14:47:39 | 2018-03-31 14:47:39 | 0 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Music | 2018-03-31 14:47:33 | 2018-03-31 14:47:39 | 2018-03-31 14:47:39 | 0 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Pictures | 2018-03-31 14:47:33 | 2018-03-31 14:47:39 | 2018-03-31 14:47:39 | 0 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| E:\Adorable Cats.jpg | 2018-03-30 19:17:09 | 2018-03-30 19:17:09 | 2018-03-30 19:17:09 | 14901 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| C:\Users\ethan\_local\Desktop\Ethan Thomas Resignation Letter.docx | 2018-03-31 15:54:33 | 2018-03-31 15:54:44 | 2018-03-31 15:54:33 | 4620 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\EthanThomas\_Notes.docx | 2018-03-31 15:38:15 | 2018-03-31 14:44:00 | 2018-03-31 15:38:15 | 9015 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Intellectual Property Document.docx | 2018-03-31 15:38:15 | 2018-03-30 18:01:50 | 2018-03-31 15:38:15 | 16063 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| E:\Intellectual Property Document.docx | 2018-03-31 15:39:16 | 2018-03-31 15:39:16 | 2018-03-31 15:39:16 | 9015 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| C:\Users\ethan\_local\Documents\Sensitive Potential Client List.xlsx | 2018-03-31 15:38:15 | 2018-03-31 14:22:40 | 2018-03-31 15:38:15 | 7412 | Fixed storage media (Hard drive) | 60D53EE6 | ethomas\_desktop |
| E:\Cat with Tongue Out.jpg | 2018-03-30 19:18:13 | 2018-03-30 19:18:13 | 2018-03-30 19:18:13 | 5919 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| E:\Cat in cute pose.jpg | 2018-03-30 19:17:31 | 2018-03-30 19:17:31 | 2018-03-30 19:17:31 | 25880 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |
| E:\Adorable Cats.jpg | 2018-03-30 19:17:09 | 2018-03-30 19:17:09 | 2018-03-30 19:17:09 | 14901 | Removable storage media (Floppy, USB) | 7295345F/ Personal USB | ethomas\_desktop |

## APPENDIX VIII: USB Analysis





## APPENDIX IX: Chain of Custody Report

