**Text

Description automatically generated**

Case Project 04

CY5210 Information System Forensics

Instructor: Elton Booker

Jonathan Metzger

December 4th, 2022

# Table of Contents

[Table of Contents 2](#_Toc120960897)

[EXECUTIVE SUMMARY 3](#_Toc120960898)

[INTRODUCTION 4](#_Toc120960899)

[ANALYSIS 5](#_Toc120960900)

[REGISTRY ANALYSIS 5](#_Toc120960901)

[USER INFORMATION 6](#_Toc120960902)

[GROUP INFORMATION 7](#_Toc120960903)

[SYSTEM INFORMATION 8](#_Toc120960904)

[USER ACTIVITY 10](#_Toc120960905)

[USB DEVICE ACTIVITY 11](#_Toc120960906)

[APPLICATIONS AND MALWARE 12](#_Toc120960907)

[PREFETCH 13](#_Toc120960908)

[SHELL ITEMS 14](#_Toc120960909)

[CONCLUSION 17](#_Toc120960910)

[APPENDIX 18](#_Toc120960911)

[APPENDIX I: Forensic Tools 18](#_Toc120960912)

[APPENDIX II: Registry Paths 18](#_Toc120960913)

[APPENDIX III: Artifacts List 19](#_Toc120960914)

[APPENDIX IV: Prefetch Analysis 20](#_Toc120960915)

[APPENDIX V: Shellbag Analysis 26](#_Toc120960916)

[APPENDIX VI: Link Analysis 27](#_Toc120960917)

[APPENDIX VII: Jump List Analysis 29](#_Toc120960918)

[APPENDIX VIII: USB Analysis 36](#_Toc120960919)

[APPENDIX IX: Chain of Custody Report 37](#_Toc120960920)

# EXECUTIVE SUMMARY

Justine Beaufort has been known to do things that are considered illegal on her private Windows system. One of which is researching a rare owl named Stella and its counterpart Sherlock. Under a recent law passed by the United States Government, any person with evidence of owl research can be subjected to up to ten years in prison.

FBI received insider information on J. Beaufort’s activities and reported to forensics with an issued warrant to investigate the Windows system for any activity on this rare owl. With the permission to investigate the system of interest, investigators found five external media that contained illegal documents, spreadsheets, and photographs of owls. This case study is documented on Justine’s activity and the evidence of her crime on researching owls.

# INTRODUCTION

On March 28th, 2019, the Director of Parks and Recreation Mickey Mouse has received intel from the FBI of possible criminal activity. This criminal activity relates to the recent law passed by the United States that prohibited research of owls specifically the types of rare breeds. M. Mouse has notified his forensic investigators to confiscate Justine Beaufort’s Windows system with motive of owl research, specifically for the rare owl named Stella and her counterpart Sherlock. Investigators have the authority to search her system and any external media connected to it.

What was collected for this investigation by the forensics team is collected in the chain of custody document found in APPENDIX IX of this document the system that was analyzed, any relevant external media, and who worked on the case study report. Below is the hash verification of the image obtained by police of Justine’s laptop, which was believed to hold evidence of her incrimination. Any tools or paths used for the analysis portion of the case study can be found in APPENDIX I and APPENDIX II.

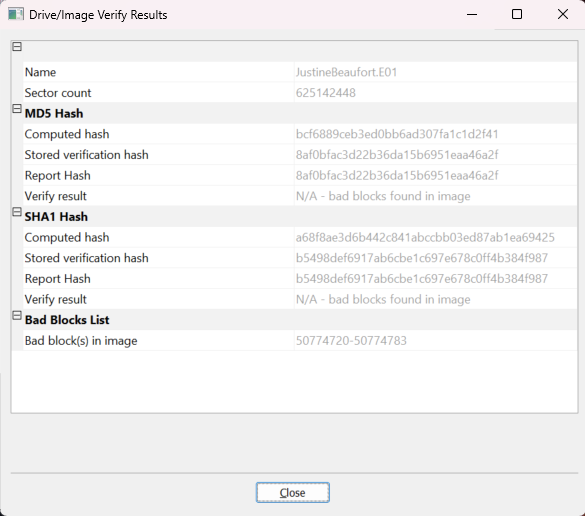


Figure Hash Verification of JustineBeaufort.E01

# 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 piece together Justine B’s intensions to research on Owls which is an illegal activity.

## 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/Justine B/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, forensic investigator can see user and group information. Users for this system have the Domain UID of **S-1-5-21-2457848455-339827241-3711018272**. 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 2457848455-339827241-3711018272 as 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>-<rev\_level>-<auth\_value>-<spec\_id>-<unique\_identifier>-<RID>”**

**The Justine B SID is S-1-5-21-2457848455-339827241-3711018272-1001**

The user information of the system of interest is in the below table with the username, RID, Status with the number of logins, last login, group associated with, and password information. User account Justine B is the focus of this analysis since it was used on the system of interest with 9 logins up until the time of acquisition. Justine B had administrator access to the system and could have done a better job covering the tracks of her illegal activity. She attempted to use her admin privileges to remove applications from the system but was later found in the forensic investigations. The latest password reset on 2019-03-25 correlated to right before the system was presented to investigators.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Username | RID | Status | Last Login | Password Reset | Group | Password |
| Justine B | 1001 | Enabled, 9 logins | 2019-03-27 11:46:06Z | 2019-03-25 13:05:44Z | Administrators | Not Required/Not Expired |
| Administrator | 500 | Disabled | 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 User Information

## GROUP INFORMATION

As shown in the table in the previous section, no user was under the group Remote Desktop Users, so that no user could SSH into the system. However, the Administrator, Justine B, is under the privileged group of Administrators. Any user in this group can cause potential harm to the system and the organization the system is associated with. The Justine B user account was the only one enabled on the system, which shows that J. Beaufort executed actions on the system. Beaufort did activities on the system with the RID 1001. That information can be important when tracking her efforts on the system and how her actions can prove that she searched images of owls which is illegal activity.

## SYSTEM INFORMATION

**KEY**

${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 |
| Build Version | ${CurrentVersion}\CurrentBuild | 17134 |
| Current Control Set | ${ControlSet} | 001 |
| Computer Name | ${ControlSet}\Control\ComputerName\ComputerName | DESKTOP-NS66FM9 |
| Time Zone | ${ControlSet}\Control\TimeZoneInformation | US Eastern Standard Time |
| OS Install Date | ${CurrentVersion}\InstallDate | 2019-03-25 10:53:27Z |
| Network Interfaces | ${ControlSet}/… | 192.168.1.48 |
| AutoStart Programs | ${CurrentVersion}\Run | LastWrite Time 2019-03-27 11:49:49Z  SecurityHealth - %ProgramFiles%\Windows Defender\MSASCuiL.exe  SysTrayApp - C:\Program Files\IDT\WDM\sttray64.exe |
| Last Shutdown Time | ${ControlSet}\Control\Windows\ShutdownTime  $ ./convert\_binary\_time.py <REG\_BINARY> | 2019-03-27 11:44:54 |

Table System Information

Our goal was to collect the system’s configurations, settings, user data, and activity by scoping a complete picture of the action that went on around the time of the alert. The hostname “DESKTOP-NS66FM9” 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 2019-03-25 at 10:53:27 and set in US Eastern Standard time. This proved that the new system was used right before her malicious activity. 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 192.168.1.48. The system’s last shutdown time was the day before the system acquisition. This made it easier for investigators to access the Justine B user account and retrieve any impersonating evidence.

There were two Autostart actions on the system. The Windows Defender application seemed to be protecting J. Beaufort from any viruses that was present during her Owl searches. The system information is critical for investigators to provide more information on when she looked up owl images and correlate to what was on the system. Below is one of the photos on the system that investigators found that is proof of Justine’s illegal search activity of a photograph of Stella and Sherlock at a county fair.

**A picture containing person, outdoor

Description automatically generated**

Figure Owls Stella and Sherlock at the County fair

## USER ACTIVITY

The forensics team went through the user activity of J. Beaufort on her account on the system. 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**

There was no search history performed on the system. However, the application CCLeaner was found on the Windows system with the attempt to remove any malicious activity performed by J. Beaufort.

* **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 were many documents found in RecentDocs that relate to owls. Some include “Owls and Their Homes.docx”, “Owls.pdf” and “Stella.jpg”. These documents are discussed later in the analysis.

* **LastExecutedCommands**

The only relevant command for this case on 2019-03-25 at 15:125:17Z when the user opened Internet Explorer to use. This can be traced to other documents and downloads that proposes that the user downloaded Owl images from the internet.

* **UserAssist**

A list of the UserAssist executables of interest can be found in the below table. They relate to activity related to the scope of the investigation and can be found throughout the analysis. They involve internet browsers, Microsoft office applications and media players that can be used for illegal owl activity.

|  |  |
| --- | --- |
| Executables | LastWriteTime |
| CCleaner v.5.55 | 2019-03-25 13:23:03Z |
| Mozilla Firefox 66.0.1 (x64 en-US) v.66.0.1 | 2019-03-25 13:20:37Z |
| Google Chrome v.73.0.3683.86 | 2019-03-25 13:15:24Z |
| Microsoft Office Professional Plus 2010 v.14.0.6029.1000 | 2019-03-26 15:54:44Z |
| DXM\_Runtime, MPlayer2 | 2018-04-12 09:16:26Z |

Table UserAssist

## USB DEVICE ACTIVITY

The forensics team identified an external media device that was connected to the system. It was used when the new system was installed which shows that data was copied from the media to the system. From the evidence collected, there were various documents that showed documents and pictures related to Owls. The table below shows the external media, serial number, account used on the system, and first and last time the external media was used. It can be concluded that Justine copied owl related items to and from the external media onto the system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Name | Serial Number | User Account | First Time | Last Time |
| Kingston Data Traveler 102 USB Device | AA010215170355310594 | Justine B. | 2019-03-25 13:12:00Z | 2019-03-25 13:13:42Z |
| General Udisk USB Device | 6&2017aed3 | Justine B. | 2019-03-26 12:40:21Z | 2019-03-26 12:40:58Z |
| General Udisk USB Device | 6&32d15f78 | Justine B. | 2019-03-26 15:41:07Z | 2019-03-26 17:33:41Z |
| GENERIC SD04G | b008be2f | Justine B. |  |  |
| Seagate BUP Slim Mac SL SCSI Disk Device | NA7RL7PR | Justine B. | 2019-03-26 17:36:29Z | 2019-03-26 18:24:31Z |

Table USB Device Connected to “DESKTOP-NS66FM9”

## APPLICATIONS AND MALWARE

Below shows the applications and potential malware that was on the system. These applications relate to the investigation since they are internet browsers, media viewers and Microsoft Office applications. These can be traced to user activity that involves owls and were attempted by the user to be uninstalled to cover their tracks. CCleaner was also found on the system which would be evidence that the user tried to remove their activity history. From the investigation, it can be said that the user J. Beaufort download web browsers to perform internet search on owls, and then removed from the system.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Executables | LastUsed | Downloaded | Installed | Executed | Uninstalled |
| CCleaner v.5.55 | 2019-03-25 13:23:03Z |  |  | X | X |
| Mozilla Firefox 66.0.1 (x64 en-US) v.66.0.1 | 2019-03-25 13:20:37Z | X | X | X | X |
| Google Chrome v.73.0.3683.86 | 2019-03-25 13:15:24Z | X | X | X | X |
| Microsoft Office Professional Plus 2010 v.14.0.6029.1000 | 2019-03-26 15:54:44Z |  |  | X | X |
| DXM\_Runtime, MPlayer2 | 2018-04-12 09:16:26Z | X | X | X | X |

Table Applications by LastUsed

## PREFETCH

The list below is the prefetch applications related to the investigation. They include web applications like Chrome, Firefox, and Edge. As well as cloud applications like OneDrive, email applications like outlook, spreadsheet Excel and Microsoft Photos to observe Owl photos. The full list of Prefetch applications can be found in APPENDIX IV. The usage of these applications by the Justine user can be connected to the items shown later in the analysis.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Executable  Name | Source  Created | Source  Modified | Source  Accessed | Size | Run  Count | Last  Run | First  Run | Volume/  Serial |
| CCLEANER64.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:13:57 | 2022-11-30 01:18:52 | 176090 | 9 | 2019-03-27 12:13:47 | 2019-03-25 13:23:17 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:54 | 2022-11-30 01:18:52 | 51252 | 17 | 2019-03-27 11:46:44 | 2019-03-25 15:29:55 | DCAECB8D |
| CONHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 17:48:47 | 2022-11-30 01:18:53 | 20914 | 39 | 2019-03-27 17:48:40 | 2019-03-26 18:05:35 | DCAECB8D |
| CONSENT.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:28 | 2022-11-30 01:18:53 | 188586 | 12 | 2019-03-27 11:47:27 | 2019-03-25 13:22:42 | 74B6B897 |
| EXCEL.EXE | 2022-11-30 01:18:41 | 2019-03-26 16:49:40 | 2022-11-30 01:18:53 | 110856 | 5 | 2019-03-26 16:49:34 | 2019-03-26 16:02:02 | FC9BD2D2 |
| FIREFOX INSTALLER.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:19:58 | 2022-11-30 01:18:53 | 28610 | 1 | 2019-03-25 13:19:47 |  | DCAECB8D |
| MICROSOFT.PHOTOS.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:06:15 | 2022-11-30 01:18:54 | 275290 | 13 | 2019-03-27 12:06:11 | 2019-03-26 15:42:45 | 20F3BCE6 |
| MICROSOFTEDGE.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:16:38 | 2022-11-30 01:18:54 | 190218 | 12 | 2019-03-27 13:16:28 | 2019-03-26 10:50:53 | DCAECB8D |
| ONEDRIVE.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:35 | 2022-11-30 01:18:55 | 71070 | 3 | 2019-03-27 11:46:21 | 2019-03-26 10:46:35 | DCAECB8D |
| OUTLOOK.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:02 | 2022-11-30 01:18:55 | 212270 | 3 | 2019-03-27 18:24:52 | 2019-03-27 11:49:04 | DCAECB8D |
| TRUSTEDINSTALLER.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:45:59 | 2022-11-30 01:18:58 | 18198 | 15 | 2019-03-27 13:45:49 | 2019-03-26 12:36:35 | DCAECB8D |

Table Prefetch Analysis

## SHELL ITEMS

The below table identifies the areas of interest in the shell bag analysis located in APPENDIX V. These items are relevant to the case since it shows the user activity between external media and the system. It shows that on the F and D drives, external media contained the directory “Good Ones” which are items related to Owls. It is interesting to also see the users interaction with Skype, which is a sharing application, and MagnetProcessCapture which captures screenshots of the computer actions. That can be used to document Skype messages or any internet searches on the system.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Absolute  Path | Shell  Type | Value | First  Interacted | Last  Interacted |
| Desktop\F:\ | Users property view: Drive letter | F:\ | 2019-03-25 13:12:08 |  |
| Desktop\Shared Documents Folder (Users Files) | Root folder: GUID | Shared Documents Folder (Users Files) | 2019-03-26 14:53:23 |  |
| Desktop\GoodOnes | Directory | GoodOnes | 2019-03-26 16:01:40 |  |
| Desktop\C:\\Users\Justine B\AppData\Roaming\Microsoft\Skype | Directory | Skype |  | 2019-03-25 13:11:55 |
| Desktop\C:\\Users\Justine B\AppData\Roaming\Microsoft\Skype\live#3astevedallas1010 | Directory | live#3astevedallas1010 | 2019-03-25 13:13:25 | 2019-03-25 13:13:25 |
| Desktop\D:\\GoodOnes | Directory | GoodOnes | 2019-03-27 11:44:12 | 2019-03-27 11:44:12 |
| Desktop\My Computer\Downloads | Root folder: GUID | Downloads | 2019-03-26 14:48:50 | 2019-03-27 18:32:06 |
| Desktop\My Computer\Documents | Root folder: GUID | Documents | 2019-03-26 16:48:04 |  |
| Desktop\My Computer\Pictures | Root folder: GUID | Pictures | 2019-03-26 17:13:17 |  |
| Desktop\My Computer\F:\MagnetProcessCapture-20190326-140822 | Directory | MagnetProcessCapture-20190326-140822 | 2019-03-26 18:08:28 | 2019-03-26 18:08:28 |

Table Shellbag Items

Below are the Link files relevant to the case. The full list can be found in APPENDIX VI. These go a step further into the Shellbags identified previously with pictures, documents and spreadsheets that relate to Owl activity. This connects any documents that are in the scope of this investigation on the C drive local system and F drive which contained multiple external media connected to the system at various times of use.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Local  Path | Source  Created | Source  Modified | Source  Accessed | Target  Created | Target  Modified | Target  Accessed | File  Size | Drive  Type | Volume  Serial | Machine  ID |
| C:\Users\Justine B\Desktop\GoodOnes\grumpy-owl\_c\_2512435.jpg | 2019-03-26 15:47:32 | 2019-03-26 15:47:32 | 2019-03-26 15:47:32 | 2019-03-26 15:47:31 | 2019-03-26 15:47:32 | 2019-03-26 15:47:29 | 54324 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Desktop\GoodOnes\hqdefault.jpg | 2019-03-26 15:47:03 | 2019-03-26 15:47:03 | 2019-03-26 15:47:03 | 2019-03-26 15:47:02 | 2019-03-26 15:46:57 | 2019-03-26 15:46:56 | 40209 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Documents\Owl Musings.docx | 2019-03-26 16:51:52 | 2019-03-26 16:53:13 | 2019-03-26 16:53:13 | 2019-03-26 16:51:52 | 2019-03-26 16:51:53 | 2019-03-26 16:51:52 | 20931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\Owls and Their Homes.docx | 2019-03-26 16:03:02 | 2019-03-26 16:03:02 | 2019-03-26 16:03:02 | 2019-03-26 15:49:45 | 2019-03-26 15:49:49 | 2019-03-26 15:49:45 | 5529698 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\stella.jpg | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 45931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\stellaAndSherlock.jpg | 2019-03-26 17:24:49 | 2019-03-26 17:26:23 | 2019-03-26 17:26:23 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 255490 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\cuteowl.jpg | 2019-03-26 12:41:15 | 2019-03-26 15:43:20 | 2019-03-26 15:43:20 | 2019-02-20 18:41:45 | 2019-02-19 18:21:14 | 2019-02-20 04:00:00 | 7827 | Removable storage media (Floppy, USB) | 20F3BCE6 | USB 1 |
| F:\nicepic.jpg | 2019-03-26 12:41:37 | 2019-03-26 15:43:11 | 2019-03-26 15:43:11 | 2019-02-20 18:41:45 | 2019-02-19 18:19:58 | 2019-03-26 04:00:00 | 11320 | Removable storage media (Floppy, USB) | 20F3BCE6 | USB 1 |
| F:\Great Horned Owl.pdf | 2019-03-26 15:32:09 | 2019-03-26 15:42:32 | 2019-03-26 15:42:32 | 2019-03-26 15:32:09 | 2019-03-26 15:32:10 | 2019-03-26 04:00:00 | 1048178 | Removable storage media (Floppy, USB) | FC9BD2D2 | USB 2 |
| F:\owlColors\_backup.xlsx | 2019-03-26 16:49:36 | 2019-03-26 16:49:36 | 2019-03-26 16:49:36 | 2019-03-26 16:49:23 | 2019-03-26 16:48:16 | 2019-03-26 04:00:00 | 9073 | Removable storage media (Floppy, USB) | FC9BD2D2 | USB 2 |
| F:\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-26 15:31:37 | 2019-03-26 16:09:39 | 2019-03-26 16:09:39 | 2019-03-26 15:31:37 | 2019-03-26 15:31:40 | 2019-03-26 04:00:00 | 3260666 | Removable storage media (Floppy, USB) | FC9BD2D2 | USB 2 |

Table LNK Files

The table below covers the JumpList files that relate to the case study. A lot of the information overlaps with the LNK files but focuses more on what was found within the Justine B user directories. The entire Jump Lists can be found in APPENDIX VII. It can be shown that there were four different volume serials being used for owl activity. One was the system being analyzed, the other three were external media that was plugged into the system.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Local  Path | Source  Created | Source  Modified | Source  Accessed | Target  Created | Target  Modified | Target  Accessed | File  Size | Drive  Type | Volume  Serial | Machine  ID |
| D:\GoodOnes\resized owl moon.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 16:51:14 | 2019-03-26 16:51:15 | 2019-03-27 11:44:11 | 7154 | Fixed storage media (Hard drive) | 042B2CA5 | desktop-n566fm9 |
| D:\GoodOnes\grumpy-owl\_c\_2512435.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:47:31 | 2019-03-26 15:47:32 | 2019-03-27 11:44:11 | 54324 | Fixed storage media (Hard drive) | 042B2CA5 | desktop-n566fm9 |
| F:\cuteowl.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 18:21:14 | 2019-02-20 04:00:00 | 7827 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| C:\Users\Justine B\Downloads\stellaAndSherlock.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 255490 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\Great Horned Owl.pdf | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 | 2019-03-26 15:32:09 | 2019-03-26 15:32:09 | 2019-03-26 15:32:02 | 1048178 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 | 2019-03-26 15:31:37 | 2019-03-26 15:31:38 | 2019-03-26 15:31:33 | 3260666 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\Owls and Their Homes.docx | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:49:45 | 2019-03-26 15:49:49 | 2019-03-26 15:49:45 | 5529698 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\Great Horned Owl.pdf | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:32:09 | 2019-03-26 15:32:10 | 2019-03-26 04:00:00 | 1048178 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 | 2019-03-26 15:31:37 | 2019-03-26 15:31:40 | 2019-03-26 04:00:00 | 3260666 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |

Table Jump Lists

Throughout this analysis, the system showed the time of use by Justine Beaufort. The analysis showed applications used and which documents were collected by the internet that is illegal. This showed that external media was connected to the system to extract owl information to be used elsewhere. Finally, the user tried to erase her activity by uninstalling applications and removing files of illegal content.

# CONCLUSION

To conclude, evidence provided to investigators in JustineBeaufort.E01 proved that Justine Beaufort is guilty of researching owls specifically the rare breed by the named of Stella and Sherlock. Insiders reported on her strange behavior and obsession of owls which sparked interest in the FBI investigation. There is enough evidence in this analysis to prove that Justine downloaded web browsers, searched owls, downloaded illegal documents to her multiple external media, and attempted to uninstall applications used on the system.

Recommendations include to charge Justine Beaufort with her intentional use of owl internet searches which is illegal in the United States. To prevent this incident from happening again, there should be an internet tag of keywords related to “owls”. However, this is an invasion of privacy by the fourth amendment, but law officials need to balance the idea of privacy with safety. It will be a tough task to handle but at the end of the day, we need to protect the mice in the world from any owl predators that can be lurking for a meal.

# 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

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/Justine B/NTUSER.DAT
   * NONAME [NTFS]/[root]/Users/Justine B/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/Justine B/AppData/Roaming/Microsoft/Windows/Recent
5. User’s Profile Folders
   * NONAME [NTFS]/[root]/Users/Justine B/Desktop
   * NONAME [NTFS]/[root]/Users/Justine B/Documents
   * NONAME [NTFS]/[root]/Users/Justine B/Downloads
6. Additional Artifacts
   * NONAME [NTFS]/[root]/$Recycle.Bin (folder)
   * NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log

## APPENDIX IV: Prefetch Analysis

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Executable  Name | Source  Created | Source  Modified | Source  Accessed | Size | Run  Count | Last  Run | First  Run | Volume/  Serial |
| AM\_DELTA.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:50:01 | 2022-11-30 01:18:52 | 9748 | 2 | 2019-03-27 11:49:51 | 2019-03-25 16:49:43 | DCAECB8D |
| APPLICATIONFRAMEHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:50 | 2022-11-30 01:18:52 | 62166 | 5 | 2019-03-27 11:46:40 | 2019-03-25 13:07:01 | DCAECB8D |
| ARES.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:44 | 2022-11-30 01:18:52 | 101170 | 6 | 2019-03-27 11:46:32 | 2019-03-25 15:07:57 | DCAECB8D |
| ARESREGULAR246\_INSTALLER.EXE | 2022-11-30 01:18:41 | 2019-03-25 15:07:52 | 2022-11-30 01:18:52 | 50002 | 1 | 2019-03-25 15:07:42 |  | DCAECB8D |
| AUDIODG.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:30:07 | 2022-11-30 01:18:52 | 33166 | 22 | 2019-03-27 18:29:57 | 2019-03-26 16:56:26 | DCAECB8D |
| BACKGROUNDTASKHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:03 | 2022-11-30 01:18:52 | 95272 | 18 | 2019-03-27 18:24:53 | 2019-03-26 15:59:13 | DCAECB8D |
| BACKGROUNDTASKHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:18 | 2022-11-30 01:18:52 | 64646 | 4 | 2019-03-27 11:44:16 | 2019-03-25 13:09:12 | DCAECB8D |
| BROWSER\_BROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:16:38 | 2022-11-30 01:18:52 | 24602 | 2 | 2019-03-27 13:16:28 | 2019-03-27 12:11:52 | DCAECB8D |
| CCLEANER.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:13:47 | 2022-11-30 01:18:52 | 28530 | 1 | 2019-03-27 12:13:46 |  | DCAECB8D |
| CCLEANER64.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:13:57 | 2022-11-30 01:18:52 | 176090 | 9 | 2019-03-27 12:13:47 | 2019-03-25 13:23:17 | DCAECB8D |
| CCSETUP555.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:22:47 | 2022-11-30 01:18:52 | 77158 | 1 | 2019-03-25 13:22:44 |  | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:48 | 2022-11-30 01:18:52 | 78088 | 6 | 2019-03-27 11:46:34 | 2019-03-25 15:29:07 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:54 | 2022-11-30 01:18:52 | 51252 | 17 | 2019-03-27 11:46:44 | 2019-03-25 15:29:55 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:53 | 2022-11-30 01:18:52 | 34286 | 3 | 2019-03-27 11:46:43 | 2019-03-26 10:46:45 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:43:14 | 2022-11-30 01:18:52 | 54536 | 2 | 2019-03-27 11:43:03 | 2019-03-26 10:46:40 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:49 | 2022-11-30 01:18:52 | 28060 | 6 | 2019-03-27 11:46:39 | 2019-03-25 15:29:07 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:24:44 | 2022-11-30 01:18:52 | 202454 | 5 | 2019-03-27 18:24:42 | 2019-03-25 13:16:37 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:24:45 | 2022-11-30 01:18:53 | 42544 | 38 | 2019-03-27 18:24:42 | 2019-03-26 16:55:07 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:37 | 2022-11-30 01:18:53 | 71886 | 12 | 2019-03-27 18:25:26 | 2019-03-25 15:06:45 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:31:38 | 2022-11-30 01:18:53 | 34060 | 1 | 2019-03-26 15:31:27 |  | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:25:23 | 2022-11-30 01:18:53 | 34698 | 1 | 2019-03-26 15:25:13 |  | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:36 | 2022-11-30 01:18:53 | 34294 | 8 | 2019-03-27 18:25:26 | 2019-03-25 13:15:27 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:36 | 2022-11-30 01:18:53 | 29148 | 9 | 2019-03-27 18:25:26 | 2019-03-25 13:16:37 | DCAECB8D |
| CHROME.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:30:07 | 2022-11-30 01:18:53 | 86832 | 29 | 2019-03-27 18:29:56 | 2019-03-26 15:18:38 | DCAECB8D |
| CHXSMARTSCREEN.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:22:42 | 2022-11-30 01:18:53 | 110832 | 2 | 2019-03-25 13:22:39 | 2019-03-25 13:19:41 | DCAECB8D |
| CONHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 17:48:47 | 2022-11-30 01:18:53 | 20914 | 39 | 2019-03-27 17:48:40 | 2019-03-26 18:05:35 | DCAECB8D |
| CONSENT.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:28 | 2022-11-30 01:18:53 | 188586 | 12 | 2019-03-27 11:47:27 | 2019-03-25 13:22:42 | 74B6B897 |
| CTFMON.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:40 | 2022-11-30 01:18:53 | 13460 | 3 | 2019-03-27 11:44:40 | 2019-03-25 19:28:19 | DCAECB8D |
| DISMHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 18:06:00 | 2022-11-30 01:18:53 | 35360 | 1 | 2019-03-26 18:05:50 |  | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:10:51 | 2022-11-30 01:18:53 | 38168 | 1 | 2019-03-25 13:10:41 |  | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:28 | 2022-11-30 01:18:53 | 39640 | 4 | 2019-03-27 11:44:17 | 2019-03-25 13:09:12 | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:45 | 2022-11-30 01:18:53 | 22462 | 4 | 2019-03-27 11:47:40 | 2019-03-25 16:46:25 | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:42:35 | 2022-11-30 01:18:53 | 28890 | 9 | 2019-03-27 11:42:25 | 2019-03-25 15:54:21 | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:33 | 2022-11-30 01:18:53 | 15074 | 35 | 2019-03-27 11:47:28 | 2019-03-26 15:40:35 | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:06:33 | 2022-11-30 01:18:53 | 26054 | 1 | 2019-03-27 12:06:25 |  | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:05:44 | 2022-11-30 01:18:53 | 22208 | 5 | 2019-03-27 12:05:39 | 2019-03-26 12:36:06 | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-25 14:38:08 | 2022-11-30 01:18:53 | 39178 | 3 | 2019-03-25 14:38:02 | 2019-03-25 13:08:59 | DCAECB8D |
| DLLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:23 | 2022-11-30 01:18:53 | 17934 | 8 | 2019-03-27 11:44:17 | 2019-03-25 13:09:12 | DCAECB8D |
| EASEOFACCESSDIALOG.EXE | 2022-11-30 01:18:41 | 2019-03-25 15:54:55 | 2022-11-30 01:18:53 | 89982 | 1 | 2019-03-25 15:54:51 |  | DCAECB8D |
| EXCEL.EXE | 2022-11-30 01:18:41 | 2019-03-26 16:49:40 | 2022-11-30 01:18:53 | 110856 | 5 | 2019-03-26 16:49:34 | 2019-03-26 16:02:02 | FC9BD2D2 |
| FILECOAUTH.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:05:45 | 2022-11-30 01:18:53 | 36878 | 5 | 2019-03-27 12:05:39 | 2019-03-26 12:36:07 | DCAECB8D |
| FIREFOX INSTALLER.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:19:58 | 2022-11-30 01:18:53 | 28610 | 1 | 2019-03-25 13:19:47 |  | DCAECB8D |
| FIRSTLOGONANIM.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:06:36 | 2022-11-30 01:18:53 | 51186 | 1 | 2019-03-25 13:06:24 |  | DCAECB8D |
| GOOGLEUPDATE.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:14:39 | 2022-11-30 01:18:53 | 50348 | 1 | 2019-03-25 13:14:29 |  | DCAECB8D |
| GOOGLEUPDATE.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:14:48 | 2022-11-30 01:18:53 | 110630 | 1 | 2019-03-25 13:14:38 |  | DCAECB8D |
| GOOGLEUPDATE.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:20:23 | 2022-11-30 01:18:53 | 55044 | 23 | 2019-03-27 18:20:22 | 2019-03-26 13:19:59 | DCAECB8D |
| HITENE.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:15:10 | 2022-11-30 01:18:54 | 21788 | 7 | 2019-03-27 18:15:00 | 2019-03-27 12:15:01 | DCAECB8D |
| INSTUP.EXE | 2022-11-30 01:18:41 | 2019-03-25 14:38:42 | 2022-11-30 01:18:54 | 196406 | 7 | 2019-03-25 14:38:31 | 2019-03-25 13:26:36 | DCAECB8D |
| LOGONUI.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:47:42 | 2022-11-30 01:18:54 | 83472 | 2 | 2019-03-27 18:47:38 | 2019-03-25 19:28:17 | DCAECB8D |
| MAGNETPROCESSCAPTURE.EXE | 2022-11-30 01:18:41 | 2019-03-26 18:08:16 | 2022-11-30 01:18:54 | 82678 | 1 | 2019-03-26 18:08:06 |  | 74B6B897 |
| MICROSOFT.PHOTOS.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:06:15 | 2022-11-30 01:18:54 | 275290 | 13 | 2019-03-27 12:06:11 | 2019-03-26 15:42:45 | 20F3BCE6 |
| MICROSOFTEDGE.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:16:38 | 2022-11-30 01:18:54 | 190218 | 12 | 2019-03-27 13:16:28 | 2019-03-26 10:50:53 | DCAECB8D |
| MICROSOFTEDGECP.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:16:38 | 2022-11-30 01:18:54 | 262002 | 31 | 2019-03-27 13:16:28 | 2019-03-26 17:07:53 | DCAECB8D |
| MICROSOFTPDFREADER.EXE | 2022-11-30 01:18:41 | 2019-03-26 17:14:19 | 2022-11-30 01:18:54 | 158872 | 6 | 2019-03-26 17:14:09 | 2019-03-26 15:32:34 | FC9BD2D2 |
| MOBSYNC.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:42:50 | 2022-11-30 01:18:54 | 36478 | 4 | 2019-03-27 11:42:39 | 2019-03-25 13:08:15 | DCAECB8D |
| MOFCOMP.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:46:38 | 2022-11-30 01:18:54 | 20206 | 1 | 2019-03-26 15:46:35 |  | DCAECB8D |
| MPCMDRUN.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:59:49 | 2022-11-30 01:18:54 | 23142 | 2 | 2019-03-27 11:59:49 | 2019-03-27 11:59:49 | DCAECB8D |
| MPCMDRUN.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:33 | 2022-11-30 01:18:54 | 41054 | 12 | 2019-03-27 11:49:29 | 2019-03-25 14:39:14 | DCAECB8D |
| MPSIGSTUB.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:53 | 2022-11-30 01:18:54 | 270170 | 3 | 2019-03-27 11:49:51 | 2019-03-25 16:49:03 | DCAECB8D |
| MSACCESS.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:48:57 | 2022-11-30 01:18:54 | 63562 | 1 | 2019-03-27 11:48:50 |  | DCAECB8D |
| MSASCUIL.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:32 | 2022-11-30 01:18:54 | 29960 | 5 | 2019-03-27 11:46:20 | 2019-03-25 13:08:23 | DCAECB8D |
| MSCONFIG.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:38 | 2022-11-30 01:18:54 | 28896 | 1 | 2019-03-27 11:47:28 |  | DCAECB8D |
| MSCORSVW.EXE | 2022-11-30 01:18:41 | 2019-03-27 17:48:45 | 2022-11-30 01:18:54 | 41896 | 2 | 2019-03-27 17:48:44 | 2019-03-27 17:48:44 | DCAECB8D |
| MSI814C.TMP | 2022-11-30 01:18:41 | 2019-03-26 15:51:18 | 2022-11-30 01:18:54 | 45330 | 1 | 2019-03-26 15:51:13 |  | DCAECB8D |
| MSI9A0D.TMP | 2022-11-30 01:18:41 | 2019-03-26 15:55:45 | 2022-11-30 01:18:55 | 42518 | 1 | 2019-03-26 15:55:42 |  | DCAECB8D |
| MSMPENG.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:29 | 2022-11-30 01:18:55 | 67058 | 1 | 2019-03-27 11:49:28 |  | DCAECB8D |
| MUSNOTIFICATIONUX.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:40 | 2022-11-30 01:18:55 | 21754 | 1 | 2019-03-27 11:44:39 |  | DCAECB8D |
| MUSNOTIFYICON.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:11:15 | 2022-11-30 01:18:55 | 22898 | 17 | 2019-03-27 12:11:14 | 2019-03-26 10:49:16 | DCAECB8D |
| NGEN.EXE | 2022-11-30 01:18:41 | 2019-03-27 17:48:45 | 2022-11-30 01:18:55 | 25140 | 4 | 2019-03-27 17:48:44 | 2019-03-27 17:48:41 | DCAECB8D |
| NGENTASK.EXE | 2022-11-30 01:18:41 | 2019-03-27 17:48:47 | 2022-11-30 01:18:55 | 64676 | 2 | 2019-03-27 17:48:39 | 2019-03-27 17:48:46 | DCAECB8D |
| NISSRV.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:27 | 2022-11-30 01:18:55 | 26404 | 4 | 2019-03-27 11:49:26 | 2019-03-25 13:05:17 | DCAECB8D |
| NISSRV.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:50:00 | 2022-11-30 01:18:55 | 23330 | 1 | 2019-03-27 11:49:50 |  | DCAECB8D |
| NOTIFICATION\_HELPER.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:26 | 2022-11-30 01:18:55 | 53544 | 1 | 2019-03-27 18:25:26 |  | DCAECB8D |
| ONEDRIVE.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:35 | 2022-11-30 01:18:55 | 71070 | 3 | 2019-03-27 11:46:21 | 2019-03-26 10:46:35 | DCAECB8D |
| OOBENETWORKCONNECTIONFLOW.EXE | 2022-11-30 01:18:41 | 2019-03-25 16:02:00 | 2022-11-30 01:18:55 | 101684 | 1 | 2019-03-25 16:01:50 |  | DCAECB8D |
| OPENWITH.EXE | 2022-11-30 01:18:41 | 2019-03-26 17:24:25 | 2022-11-30 01:18:55 | 118828 | 4 | 2019-03-26 17:24:20 | 2019-03-26 12:41:15 | DCAECB8D |
| OSE.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:42:02 | 2022-11-30 01:18:55 | 16508 | 1 | 2019-03-26 15:42:02 |  | A9DEAB73 |
| OSE00000.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:42:12 | 2022-11-30 01:18:55 | 34186 | 1 | 2019-03-26 15:42:02 |  | A9DEAB73 |
| OSPPSVC.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:04 | 2022-11-30 01:18:55 | 43762 | 2 | 2019-03-27 11:48:53 | 2019-03-26 15:46:18 | DCAECB8D |
| OUTLOOK.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:02 | 2022-11-30 01:18:55 | 212270 | 3 | 2019-03-27 18:24:52 | 2019-03-27 11:49:04 | DCAECB8D |
| PICKERHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 17:14:08 | 2022-11-30 01:18:55 | 122454 | 2 | 2019-03-26 17:13:59 | 2019-03-26 17:13:16 | DCAECB8D |
| RUNDLL32.EXE | 2022-11-30 01:18:41 | 2019-03-25 15:08:09 | 2022-11-30 01:18:55 | 35034 | 1 | 2019-03-25 15:07:59 |  | DCAECB8D |
| RUNDLL32.EXE | 2022-11-30 01:18:41 | 2019-03-27 17:48:38 | 2022-11-30 01:18:55 | 14834 | 1 | 2019-03-27 17:48:37 |  | DCAECB8D |
| RUNDLL32.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:11:22 | 2022-11-30 01:18:55 | 12648 | 1 | 2019-03-27 12:11:14 |  | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:20 | 2022-11-30 01:18:55 | 46286 | 3 | 2019-03-27 11:46:07 | 2019-03-27 11:42:28 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 16:12:31 | 2022-11-30 01:18:55 | 72462 | 37 | 2019-03-27 16:12:21 | 2019-03-27 12:12:49 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:47:41 | 2022-11-30 01:18:56 | 55960 | 32 | 2019-03-27 18:47:33 | 2019-03-26 18:25:09 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:20 | 2022-11-30 01:18:56 | 68324 | 3 | 2019-03-27 11:46:05 | 2019-03-26 10:46:12 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:35:17 | 2022-11-30 01:18:56 | 39688 | 15 | 2019-03-27 18:35:07 | 2019-03-26 16:41:19 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:42:44 | 2022-11-30 01:18:56 | 19498 | 2 | 2019-03-27 11:42:34 | 2019-03-26 10:46:22 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:16:38 | 2022-11-30 01:18:56 | 31160 | 2 | 2019-03-27 13:16:28 | 2019-03-27 12:11:52 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:11:23 | 2022-11-30 01:18:56 | 88412 | 11 | 2019-03-27 12:11:13 | 2019-03-26 12:56:17 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:27 | 2022-11-30 01:18:56 | 44810 | 4 | 2019-03-27 11:44:17 | 2019-03-25 13:09:13 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:35 | 2022-11-30 01:18:56 | 49714 | 5 | 2019-03-27 11:46:25 | 2019-03-25 13:43:29 | DCAECB8D |
| RUNTIMEBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:11:50 | 2022-11-30 01:18:56 | 18212 | 1 | 2019-03-27 12:11:40 |  | DCAECB8D |
| SEARCHFILTERHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:30:23 | 2022-11-30 01:18:56 | 15384 | 91 | 2019-03-27 18:30:13 | 2019-03-27 16:00:13 | DCAECB8D |
| SEARCHINDEXER.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:20 | 2022-11-30 01:18:56 | 68308 | 6 | 2019-03-27 11:46:01 | 2019-03-26 10:45:41 | 42B2CA5 |
| SEARCHPROTOCOLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:30:23 | 2022-11-30 01:18:56 | 17974 | 81 | 2019-03-27 18:30:13 | 2019-03-27 16:00:13 | DCAECB8D |
| SEARCHPROTOCOLHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:06 | 2022-11-30 01:18:56 | 20204 | 3 | 2019-03-27 18:24:56 | 2019-03-27 12:02:30 | DCAECB8D |
| SEARCHUI.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:20 | 2022-11-30 01:18:56 | 324298 | 4 | 2019-03-27 11:46:04 | 2019-03-25 13:06:57 | DCAECB8D |
| SEDSVC.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:54 | 2022-11-30 01:18:56 | 55160 | 4 | 2019-03-27 11:47:44 | 2019-03-25 16:48:59 | DCAECB8D |
| SETUP-STUB.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:20:01 | 2022-11-30 01:18:56 | 114782 | 2 | 2019-03-25 13:19:51 | 2019-03-25 13:19:48 | DCAECB8D |
| SETUP.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:40:46 | 2022-11-30 01:18:56 | 30402 | 1 | 2019-03-26 15:40:36 |  | A9DEAB73 |
| SGRMBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:01 | 2022-11-30 01:18:56 | 7380 | 2 | 2019-03-27 11:43:51 | 2019-03-26 10:47:03 | DCAECB8D |
| SHELLEXPERIENCEHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:20 | 2022-11-30 01:18:56 | 159304 | 3 | 2019-03-27 11:46:02 | 2019-03-26 10:46:11 | DCAECB8D |
| SHELLEXPERIENCEHOST.EXE | 2022-11-30 01:18:41 | 2019-03-25 13:07:07 | 2022-11-30 01:18:57 | 103744 | 1 | 2019-03-25 13:06:56 |  | DCAECB8D |
| SIHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 10:45:47 | 2022-11-30 01:18:57 | 57124 | 2 | 2019-03-26 10:45:35 | 2019-03-25 14:58:36 | DCAECB8D |
| SMARTSCREEN.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:24:51 | 2022-11-30 01:18:57 | 52588 | 22 | 2019-03-27 18:24:41 | 2019-03-26 17:07:05 | DCAECB8D |
| SMSS.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:47:38 | 2022-11-30 01:18:57 | 7510 | 1 | 2019-03-27 18:47:38 |  | DCAECB8D |
| SOFTWARE\_REPORTER\_TOOL.EXE | 2022-11-30 01:18:41 | 2019-03-26 14:53:15 | 2022-11-30 01:18:57 | 21928 | 2 | 2019-03-26 14:53:05 | 2019-03-26 14:53:05 | DCAECB8D |
| SPEECHRUNTIME.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:12:14 | 2022-11-30 01:18:57 | 62980 | 10 | 2019-03-27 12:12:04 | 2019-03-25 13:16:44 | DCAECB8D |
| SPLWOW64.EXE | 2022-11-30 01:18:41 | 2019-03-26 16:49:15 | 2022-11-30 01:18:57 | 47266 | 2 | 2019-03-26 16:49:05 | 2019-03-26 16:03:10 | DCAECB8D |
| SPPSVC.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:55 | 2022-11-30 01:18:57 | 32430 | 13 | 2019-03-27 11:47:45 | 2019-03-25 14:43:09 | DCAECB8D |
| STTRAY64.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:32 | 2022-11-30 01:18:57 | 43668 | 4 | 2019-03-27 11:46:20 | 2019-03-25 13:08:24 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:36 | 2022-11-30 01:18:57 | 18764 | 2 | 2019-03-27 11:46:26 | 2019-03-27 11:42:55 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:20 | 2022-11-30 01:18:57 | 25288 | 3 | 2019-03-27 11:46:07 | 2019-03-26 10:46:21 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:43:06 | 2022-11-30 01:18:57 | 22386 | 4 | 2019-03-27 11:42:55 | 2019-03-25 13:04:21 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:35 | 2022-11-30 01:18:57 | 23134 | 1 | 2019-03-27 18:25:25 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 16:03:21 | 2022-11-30 01:18:57 | 18222 | 1 | 2019-03-26 16:03:11 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:11 | 2022-11-30 01:18:57 | 42946 | 3 | 2019-03-27 11:47:01 | 2019-03-26 10:46:56 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:33 | 2022-11-30 01:18:57 | 17726 | 3 | 2019-03-27 11:47:23 | 2019-03-26 10:46:16 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:50:09 | 2022-11-30 01:18:57 | 16484 | 2 | 2019-03-27 11:49:59 | 2019-03-26 10:45:50 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:48:48 | 2022-11-30 01:18:57 | 36958 | 1 | 2019-03-27 11:48:38 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:43:43 | 2022-11-30 01:18:57 | 51586 | 2 | 2019-03-27 11:43:31 | 2019-03-26 10:46:28 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 17:08:45 | 2022-11-30 01:18:57 | 26268 | 1 | 2019-03-26 17:08:34 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:50 | 2022-11-30 01:18:57 | 15018 | 3 | 2019-03-27 11:47:40 | 2019-03-26 10:46:59 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:00 | 2022-11-30 01:18:57 | 18340 | 2 | 2019-03-27 11:48:50 | 2019-03-26 10:45:50 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:27:55 | 2022-11-30 01:18:57 | 15410 | 1 | 2019-03-27 18:27:45 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:24:52 | 2022-11-30 01:18:57 | 41974 | 2 | 2019-03-27 18:24:41 | 2019-03-27 15:43:23 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:48:47 | 2022-11-30 01:18:57 | 22560 | 3 | 2019-03-27 11:48:37 | 2019-03-25 16:46:05 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 16:01:27 | 2022-11-30 01:18:57 | 24930 | 1 | 2019-03-26 16:01:17 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:59 | 2022-11-30 01:18:57 | 70918 | 5 | 2019-03-27 11:46:48 | 2019-03-25 13:05:46 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:11:26 | 2022-11-30 01:18:57 | 48464 | 13 | 2019-03-27 12:11:16 | 2019-03-26 11:50:25 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:12:15 | 2022-11-30 01:18:57 | 31820 | 1 | 2019-03-27 12:12:05 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:37 | 2022-11-30 01:18:58 | 34902 | 2 | 2019-03-27 11:47:27 | 2019-03-26 12:40:09 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:05 | 2022-11-30 01:18:58 | 22900 | 2 | 2019-03-27 11:43:55 | 2019-03-26 10:47:05 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:46:56 | 2022-11-30 01:18:58 | 38516 | 5 | 2019-03-27 11:46:45 | 2019-03-25 13:09:01 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:00 | 2022-11-30 01:18:58 | 53424 | 3 | 2019-03-27 11:46:50 | 2019-03-25 16:46:07 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:49 | 2022-11-30 01:18:58 | 20236 | 3 | 2019-03-27 11:47:39 | 2019-03-26 10:46:29 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:45:59 | 2022-11-30 01:18:58 | 20444 | 1 | 2019-03-27 13:45:49 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 17:36:42 | 2022-11-30 01:18:58 | 12012 | 2 | 2019-03-26 17:36:31 | 2019-03-26 15:41:07 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:44:04 | 2022-11-30 01:18:58 | 21758 | 2 | 2019-03-27 11:43:54 | 2019-03-26 10:47:05 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:12:14 | 2022-11-30 01:18:58 | 49578 | 1 | 2019-03-27 12:12:04 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 18:05:45 | 2022-11-30 01:18:58 | 24314 | 1 | 2019-03-26 18:05:35 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:55:49 | 2022-11-30 01:18:58 | 18612 | 48 | 2019-03-27 11:55:39 | 2019-03-26 17:01:52 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:48:46 | 2022-11-30 01:18:58 | 42994 | 2 | 2019-03-27 11:48:39 | 2019-03-26 12:36:06 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:54:46 | 2022-11-30 01:18:58 | 32450 | 11 | 2019-03-27 11:54:36 | 2019-03-26 15:18:39 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 18:05:43 | 2022-11-30 01:18:58 | 20482 | 1 | 2019-03-26 18:05:33 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:47:43 | 2022-11-30 01:18:58 | 20026 | 27 | 2019-03-27 18:47:33 | 2019-03-26 18:05:33 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:44:34 | 2022-11-30 01:18:58 | 32442 | 2 | 2019-03-27 12:44:29 | 2019-03-27 12:41:04 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:49 | 2022-11-30 01:18:58 | 71000 | 4 | 2019-03-27 11:47:39 | 2019-03-25 13:04:49 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-26 17:21:11 | 2022-11-30 01:18:58 | 14872 | 1 | 2019-03-26 17:21:01 |  | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:24:59 | 2022-11-30 01:18:58 | 21280 | 2 | 2019-03-27 18:24:49 | 2019-03-27 12:18:07 | DCAECB8D |
| SVCHOST.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:52 | 2022-11-30 01:18:58 | 29120 | 5 | 2019-03-27 11:47:42 | 2019-03-25 13:04:52 | 42B2CA5 |
| SYSTEMSETTINGS.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:12:12 | 2022-11-30 01:18:58 | 225044 | 10 | 2019-03-27 12:12:02 | 2019-03-25 13:16:42 | DCAECB8D |
| SYSTEMSETTINGSBROKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:25:34 | 2022-11-30 01:18:58 | 54890 | 1 | 2019-03-27 18:25:24 |  | DCAECB8D |
| TASKHOSTW.EXE | 2022-11-30 01:18:41 | 2019-03-27 17:48:47 | 2022-11-30 01:18:58 | 68588 | 46 | 2019-03-27 17:48:37 | 2019-03-27 11:50:49 | DCAECB8D |
| TASKMGR.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:47:50 | 2022-11-30 01:18:58 | 130426 | 1 | 2019-03-27 11:47:40 |  | DCAECB8D |
| TIWORKER.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:45:59 | 2022-11-30 01:18:58 | 198680 | 11 | 2019-03-27 13:45:49 | 2019-03-26 12:36:35 | DCAECB8D |
| TRUSTEDINSTALLER.EXE | 2022-11-30 01:18:41 | 2019-03-27 13:45:59 | 2022-11-30 01:18:58 | 18198 | 15 | 2019-03-27 13:45:49 | 2019-03-26 12:36:35 | DCAECB8D |
| UPDATEPLATFORM.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:30 | 2022-11-30 01:18:58 | 53020 | 1 | 2019-03-27 11:49:20 |  | DCAECB8D |
| WEVTUTIL.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:49:16 | 2022-11-30 01:18:59 | 13920 | 1 | 2019-03-26 15:49:14 |  | DCAECB8D |
| WEVTUTIL.EXE | 2022-11-30 01:18:41 | 2019-03-26 15:49:15 | 2022-11-30 01:18:59 | 17072 | 1 | 2019-03-26 15:49:14 |  | DCAECB8D |
| WINSAT.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:11:22 | 2022-11-30 01:18:59 | 24064 | 1 | 2019-03-27 12:11:14 |  | DCAECB8D |
| WINSTORE.APP.EXE | 2022-11-30 01:18:41 | 2019-03-27 12:11:47 | 2022-11-30 01:18:59 | 117166 | 1 | 2019-03-27 12:11:37 |  | DCAECB8D |
| WINWORD.EXE | 2022-11-30 01:18:41 | 2019-03-26 16:52:06 | 2022-11-30 01:18:59 | 201894 | 5 | 2019-03-26 16:52:00 | 2019-03-26 16:01:09 | DCAECB8D |
| WMIADAP.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:49 | 2022-11-30 01:18:59 | 16956 | 2 | 2019-03-27 11:49:39 | 2019-03-26 10:48:27 | DCAECB8D |
| WMIPRVSE.EXE | 2022-11-30 01:18:41 | 2019-03-27 18:03:07 | 2022-11-30 01:18:59 | 27310 | 52 | 2019-03-27 18:02:57 | 2019-03-27 13:14:21 | DCAECB8D |
| WUAUCLT.EXE | 2022-11-30 01:18:41 | 2019-03-27 11:49:29 | 2022-11-30 01:18:59 | 130900 | 12 | 2019-03-27 11:49:19 | 2019-03-25 16:48:57 | DCAECB8D |

## APPENDIX V: Shellbag Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Absolute  Path | Shell  Type | Value | First  Interacted | Last  Interacted |
| Desktop\Home Folder | Root folder: GUID | Home Folder | 2019-03-25 13:10:06 |  |
| Desktop\C:\ | Users property view: Drive letter | C:\ |  |  |
| Desktop\D:\ | Users property view: Drive letter | D:\ |  |  |
| Desktop\F:\ | Users property view: Drive letter | F:\ | 2019-03-25 13:12:08 |  |
| Desktop\My Computer | Root folder: GUID | My Computer |  | 2019-03-27 12:06:02 |
| Desktop\Shared Documents Folder (Users Files) | Root folder: GUID | Shared Documents Folder (Users Files) | 2019-03-26 14:53:23 |  |
| Desktop\GoodOnes | Directory | GoodOnes | 2019-03-26 16:01:40 |  |
| Desktop\C:\\Users | Directory | Users |  | 2019-03-25 13:11:35 |
| Desktop\C:\\Users\Justine B | Directory | Justine B |  | 2019-03-25 13:11:37 |
| Desktop\C:\\Users\Justine B\AppData | Directory | AppData |  | 2019-03-25 13:11:39 |
| Desktop\C:\\Users\Justine B\AppData\Roaming | Directory | Roaming |  | 2019-03-25 13:11:40 |
| Desktop\C:\\Users\Justine B\AppData\Roaming\Microsoft | Directory | Microsoft |  | 2019-03-25 13:11:42 |
| Desktop\C:\\Users\Justine B\AppData\Roaming\Microsoft\New folder | Directory | New folder | 2019-03-25 13:11:50 |  |
| Desktop\C:\\Users\Justine B\AppData\Roaming\Microsoft\Protect | Directory | Protect | 2019-03-25 13:11:54 |  |
| Desktop\C:\\Users\Justine B\AppData\Roaming\Microsoft\Skype | Directory | Skype |  | 2019-03-25 13:11:55 |
| Desktop\C:\\Users\Justine B\AppData\Roaming\Microsoft\Skype\live#3astevedallas1010 | Directory | live#3astevedallas1010 | 2019-03-25 13:13:25 | 2019-03-25 13:13:25 |
| Desktop\D:\\GoodOnes | Directory | GoodOnes | 2019-03-27 11:44:12 | 2019-03-27 11:44:12 |
| Desktop\My Computer\Downloads | Root folder: GUID | Downloads | 2019-03-26 14:48:50 | 2019-03-27 18:32:06 |
| Desktop\My Computer\C: | Drive letter | C: |  |  |
| Desktop\My Computer\Desktop | Root folder: GUID | Desktop |  |  |
| Desktop\My Computer\Documents | Root folder: GUID | Documents | 2019-03-26 16:48:04 |  |
| Desktop\My Computer\Pictures | Root folder: GUID | Pictures | 2019-03-26 17:13:17 |  |
| Desktop\My Computer\F: | Drive letter | F: |  |  |
| Desktop\My Computer\C:\Users | Directory | Users |  | 2019-03-26 15:32:12 |
| Desktop\My Computer\C:\Users\Justine B | Directory | Justine B |  | 2019-03-26 15:32:12 |
| Desktop\My Computer\C:\Users\Justine B\Downloads | Directory | Downloads | 2019-03-26 15:32:12 | 2019-03-26 15:32:12 |
| Desktop\My Computer\Desktop\GoodOnes | Directory | GoodOnes | 2019-03-26 15:47:01 | 2019-03-26 15:47:01 |
| Desktop\My Computer\F:\MagnetProcessCapture-20190326-140822 | Directory | MagnetProcessCapture-20190326-140822 | 2019-03-26 18:08:28 | 2019-03-26 18:08:28 |

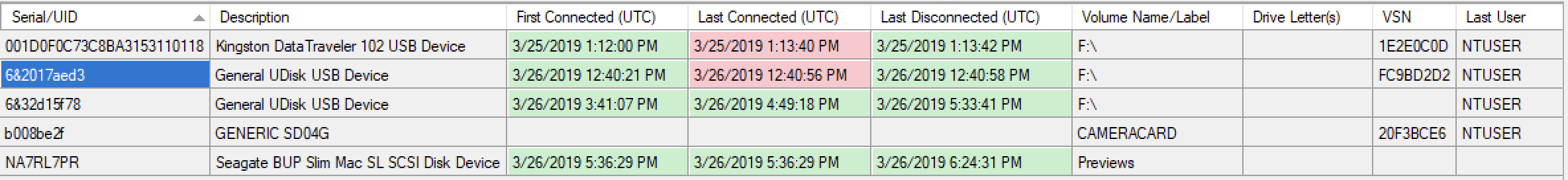
## APPENDIX VI: Link Analysis

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Local  Path | Source  Created | Source  Modified | Source  Accessed | Target  Created | Target  Modified | Target  Accessed | File  Size | Drive  Type | Volume  Serial | Machine  ID |
| C:\Users\Justine B\Desktop\GoodOnes\resized owl moon.jpg | 2019-03-26 16:51:14 | 2019-03-26 16:51:15 | 2022-11-30 01:06:52 |  |  |  | 0 | Fixed storage media (Hard drive) | DCAECB8D |  |
| C:\Users\Justine B\Downloads\Owls and Their Homes.docx | 2019-03-26 16:03:02 | 2019-03-26 16:03:02 | 2019-03-26 16:03:02 | 2019-03-26 15:49:45 | 2019-03-26 15:49:49 | 2019-03-26 15:49:45 | 5529698 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\pFRtHLhL4eOA4de3yoIRiZt1DONVY3miIQtn8qVU0FI.gif | 2019-03-26 17:19:17 | 2019-03-26 17:19:17 | 2019-03-26 17:19:17 | 2019-03-26 17:19:17 | 2019-03-26 17:19:17 | 2019-03-26 17:19:17 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\Great Horned Owl.pdf | 2019-03-26 15:32:09 | 2019-03-26 15:42:32 | 2019-03-26 15:42:32 | 2019-03-26 15:32:09 | 2019-03-26 15:32:10 | 2019-03-26 04:00:00 | 1048178 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Desktop\GoodOnes | 2019-03-26 15:46:26 | 2019-03-26 16:51:15 | 2019-03-26 16:51:15 | 2019-03-26 15:46:21 | 2019-03-26 16:51:14 | 2019-03-26 16:51:14 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\d26ac13321f158c9e5e2fa459a6974ba.jpg | 2019-03-26 12:41:31 | 2019-03-26 12:41:31 | 2019-03-26 12:41:31 | 2019-02-20 18:41:45 | 2019-02-19 18:27:18 | 2019-02-20 04:00:00 | 35920 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| C:\Users\Justine B\Documents\owlColors.xlsx | 2019-03-26 16:48:15 | 2019-03-26 16:48:15 | 2019-03-26 16:48:15 |  |  |  | 0 | Fixed storage media (Hard drive) | DCAECB8D |  |
| C:\Users\Justine B\Desktop\DWB2x2LVoAAtkWf.jpg large.jpg | 2019-03-26 17:31:05 | 2019-03-26 17:31:05 | 2019-03-26 17:31:05 | 2019-03-26 17:31:05 | 2019-03-26 17:31:05 | 2019-03-26 17:31:05 | 452851 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\owlColors\_backup.xlsx | 2019-03-26 16:49:36 | 2019-03-26 16:49:36 | 2019-03-26 16:49:36 | 2019-03-26 16:49:23 | 2019-03-26 16:48:16 | 2019-03-26 04:00:00 | 9073 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\AppData\Roaming\Microsoft\Skype | 2019-03-25 13:11:54 | 2019-03-25 13:11:54 | 2019-03-25 13:11:54 | 2019-03-25 13:11:50 | 2019-03-25 13:11:50 | 2019-03-25 13:11:50 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Desktop\GoodOnes\913ada711431fb8f3d54c68c72eb0d9c.jpg | 2019-03-26 15:47:12 | 2019-03-26 15:47:12 | 2019-03-26 15:47:12 | 2019-03-26 15:47:12 | 2019-03-26 15:47:12 | 2019-03-26 15:47:10 | 41500 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\nicepic.jpg | 2019-03-26 12:41:37 | 2019-03-26 15:43:11 | 2019-03-26 15:43:11 | 2019-02-20 18:41:45 | 2019-02-19 18:19:58 | 2019-03-26 04:00:00 | 11320 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\00y0y\_j53rBCrjb8J\_1200x900.jpg | 2019-03-26 14:50:24 | 2019-03-26 15:42:42 | 2019-03-26 15:42:42 | 2019-03-26 14:50:24 | 2019-03-26 14:50:26 | 2019-03-26 04:00:00 | 28989 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Pictures\52c01a6b565fe.image.jpg | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Desktop\GoodOnes\grumpy-owl\_c\_2512435.jpg | 2019-03-26 15:47:32 | 2019-03-26 15:47:32 | 2019-03-26 15:47:32 | 2019-03-26 15:47:31 | 2019-03-26 15:47:32 | 2019-03-26 15:47:29 | 54324 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\frogmouth.jpg | 2019-03-26 12:41:43 | 2019-03-26 15:43:16 | 2019-03-26 15:43:16 | 2019-02-20 18:41:45 | 2019-02-19 15:30:26 | 2019-03-26 04:00:00 | 8632 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| C:\Users\Justine B\Desktop\Barn-Owl-Cocked-Head.jpg.696x0\_q80\_crop-smart.jpg | 2019-03-27 12:06:06 | 2019-03-27 12:06:06 | 2019-03-27 12:06:06 |  |  |  | 0 | Fixed storage media (Hard drive) | DCAECB8D |  |
| C:\Users\Justine B\Desktop\GoodOnes\hqdefault.jpg | 2019-03-26 15:47:03 | 2019-03-26 15:47:03 | 2019-03-26 15:47:03 | 2019-03-26 15:47:02 | 2019-03-26 15:46:57 | 2019-03-26 15:46:56 | 40209 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\stellaAndSherlock.jpg | 2019-03-26 17:24:49 | 2019-03-26 17:26:23 | 2019-03-26 17:26:23 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 255490 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Documents\owls.pdf | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Pictures | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 2019-03-25 13:05:45 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-26 15:31:37 | 2019-03-26 16:09:39 | 2019-03-26 16:09:39 | 2019-03-26 15:31:37 | 2019-03-26 15:31:40 | 2019-03-26 04:00:00 | 3260666 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Downloads\stella.jpg | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 45931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\ARDB\_species\_names\_numbers\_simple.xlsx | 2019-03-26 16:02:04 | 2019-03-26 16:02:04 | 2019-03-26 16:02:04 | 2019-03-26 15:49:04 | 2019-03-26 15:49:06 | 2019-03-26 15:49:04 | 21499 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Documents\Owl Musings.docx | 2019-03-26 16:51:52 | 2019-03-26 16:53:13 | 2019-03-26 16:53:13 | 2019-03-26 16:51:52 | 2019-03-26 16:51:53 | 2019-03-26 16:51:52 | 20931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\AppData\Roaming\Microsoft | 2019-03-25 13:11:54 | 2019-03-25 13:11:54 | 2019-03-25 13:11:54 | 2019-03-25 13:05:45 | 2019-03-25 13:11:54 | 2019-03-25 13:11:54 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\814u1lDExtL.\_SL1343\_.jpg | 2019-03-26 14:49:06 | 2019-03-27 18:32:16 | 2019-03-27 18:32:16 | 2019-03-26 15:45:00 | 2019-03-26 14:49:08 | 2019-03-26 15:45:00 | 220536 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\cuteowl.jpg | 2019-03-26 12:41:15 | 2019-03-26 15:43:20 | 2019-03-26 15:43:20 | 2019-02-20 18:41:45 | 2019-02-19 18:21:14 | 2019-02-20 04:00:00 | 7827 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\30588\_112467978790101\_5187737\_n.jpg | 2019-03-26 14:54:31 | 2019-03-26 15:42:46 | 2019-03-26 15:42:46 | 2019-03-26 14:54:30 | 2019-03-26 14:54:32 | 2019-03-26 04:00:00 | 17585 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Downloads | 2019-03-26 14:49:07 | 2019-03-27 18:32:16 | 2019-03-27 18:32:16 | 2019-03-25 13:05:45 | 2019-03-27 12:06:06 | 2019-03-27 12:06:06 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |

## APPENDIX VII: Jump List Analysis

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Local  Path | Source  Created | Source  Modified | Source  Accessed | Target  Created | Target  Modified | Target  Accessed | File  Size | Drive  Type | Volume  Serial | Machine  ID |
| C:\Users\Justine B\Downloads\Great Horned Owl.pdf | 2019-03-26 14:49:06 | 2019-03-26 15:32:09 | 2022-11-30 01:18:16 |  |  |  | 0 | Fixed storage media (Hard drive) | DCAECB8D |  |
| C:\Users\Justine B\Downloads\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-26 14:49:06 | 2019-03-26 15:32:09 | 2022-11-30 01:18:16 |  |  |  | 0 | Fixed storage media (Hard drive) | DCAECB8D |  |
| C:\Users\Justine B\Downloads\814u1lDExtL.\_SL1343\_.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:45:00 | 2019-03-26 14:49:08 | 2019-03-26 15:45:00 | 220536 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Desktop\Barn-Owl-Cocked-Head.jpg.696x0\_q80\_crop-smart.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 |  |  |  | 0 | Fixed storage media (Hard drive) | DCAECB8D |  |
| C:\Users\Justine B\Desktop\DWB2x2LVoAAtkWf.jpg large.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 17:31:05 | 2019-03-26 17:31:05 | 2019-03-26 17:31:05 | 452851 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\stellaAndSherlock.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 2019-03-26 17:24:49 | 255490 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\stella.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 45931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\pFRtHLhL4eOA4de3yoIRiZt1DONVY3miIQtn8qVU0FI.gif | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 17:19:17 | 2019-03-26 17:19:17 | 2019-03-26 17:19:17 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Documents\owls.pdf | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Pictures\52c01a6b565fe.image.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Documents\Owl Musings.docx | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 16:51:52 | 2019-03-26 16:51:53 | 2019-03-26 16:51:52 | 20931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| D:\GoodOnes\resized owl moon.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 16:51:14 | 2019-03-26 16:51:15 | 2019-03-27 11:44:11 | 7154 | Fixed storage media (Hard drive) | 042B2CA5 | desktop-n566fm9 |
| F:\owlColors\_backup.xlsx | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 16:49:23 | 2019-03-26 16:48:16 | 2019-03-26 04:00:00 | 9073 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Documents\owlColors.xlsx | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 |  |  |  | 0 | Fixed storage media (Hard drive) | DCAECB8D |  |
| F:\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:31:37 | 2019-03-26 15:31:40 | 2019-03-26 04:00:00 | 3260666 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Downloads\Owls and Their Homes.docx | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:49:45 | 2019-03-26 15:49:49 | 2019-03-26 15:49:45 | 5529698 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\ARDB\_species\_names\_numbers\_simple.xlsx | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:49:04 | 2019-03-26 15:49:06 | 2019-03-26 15:49:04 | 21499 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| D:\GoodOnes\grumpy-owl\_c\_2512435.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:47:31 | 2019-03-26 15:47:32 | 2019-03-27 11:44:11 | 54324 | Fixed storage media (Hard drive) | 042B2CA5 | desktop-n566fm9 |
| D:\GoodOnes\913ada711431fb8f3d54c68c72eb0d9c.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:47:12 | 2019-03-26 15:47:12 | 2019-03-27 11:44:11 | 41500 | Fixed storage media (Hard drive) | 042B2CA5 | desktop-n566fm9 |
| D:\GoodOnes\hqdefault.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:47:02 | 2019-03-26 15:47:03 | 2019-03-27 11:44:11 | 40209 | Fixed storage media (Hard drive) | 042B2CA5 | desktop-n566fm9 |
| F:\cuteowl.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 18:21:14 | 2019-02-20 04:00:00 | 7827 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\nicepic.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 18:19:58 | 2019-03-26 04:00:00 | 11320 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\frogmouth.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 15:30:26 | 2019-03-26 04:00:00 | 8632 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\30588\_112467978790101\_5187737\_n.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 14:54:30 | 2019-03-26 14:54:32 | 2019-03-26 04:00:00 | 17585 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\00y0y\_j53rBCrjb8J\_1200x900.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 14:50:24 | 2019-03-26 14:50:26 | 2019-03-26 04:00:00 | 28989 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\Great Horned Owl.pdf | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:32:09 | 2019-03-26 15:32:10 | 2019-03-26 04:00:00 | 1048178 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\814u1lDExtL.\_SL1343\_.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 14:49:06 | 2019-03-26 14:49:08 | 2019-03-26 04:00:00 | 220536 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\d26ac13321f158c9e5e2fa459a6974ba.jpg | 2019-03-25 13:07:15 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 18:27:18 | 2019-02-20 04:00:00 | 35920 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\owlColors\_backup.xlsx | 2019-03-26 16:02:04 | 2019-03-26 16:49:36 | 2022-11-30 01:18:16 | 2019-03-26 16:49:23 | 2019-03-26 16:48:16 | 2019-03-26 04:00:00 | 9073 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Documents\owlColors.xlsx | 2019-03-26 16:02:04 | 2019-03-26 16:49:36 | 2022-11-30 01:18:16 | 2019-03-26 16:48:14 | 2019-03-26 16:48:15 | 2019-03-26 16:48:15 | 9073 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\ARDB\_species\_names\_numbers\_simple.xlsx | 2019-03-26 16:02:04 | 2019-03-26 16:49:36 | 2022-11-30 01:18:16 | 2019-03-26 15:49:04 | 2019-03-26 15:49:06 | 2019-03-26 15:49:04 | 21499 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 | 2019-03-26 15:31:37 | 2019-03-26 15:31:40 | 2019-03-26 04:00:00 | 3260666 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\Great Horned Owl.pdf | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 | 2019-03-26 15:32:09 | 2019-03-26 15:32:10 | 2019-03-26 04:00:00 | 1048178 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| C:\Users\Justine B\Downloads\Great Horned Owl.pdf | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 | 2019-03-26 15:32:09 | 2019-03-26 15:32:09 | 2019-03-26 15:32:02 | 1048178 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\Whooo\_Am\_I\_Owls\_Bro.pdf | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 | 2019-03-26 15:31:37 | 2019-03-26 15:31:38 | 2019-03-26 15:31:33 | 3260666 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
|  | 2019-03-25 13:07:03 | 2019-03-26 16:09:39 | 2022-11-30 01:18:16 |  |  |  | 0 | (None) |  |  |
| C:\Users\Justine B\Downloads\stella.jpg | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 2019-03-26 17:24:13 | 45931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\pFRtHLhL4eOA4de3yoIRiZt1DONVY3miIQtn8qVU0FI.gif | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-03-26 17:19:17 | 2019-03-26 17:19:18 | 2019-03-26 17:19:13 | 264855 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| F:\cuteowl.jpg | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 18:21:14 | 2019-02-20 04:00:00 | 7827 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\nicepic.jpg | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 18:19:58 | 2019-03-26 04:00:00 | 11320 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\frogmouth.jpg | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 15:30:26 | 2019-03-26 04:00:00 | 8632 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| F:\30588\_112467978790101\_5187737\_n.jpg | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-03-26 14:54:30 | 2019-03-26 14:54:32 | 2019-03-26 04:00:00 | 17585 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\00y0y\_j53rBCrjb8J\_1200x900.jpg | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-03-26 14:50:24 | 2019-03-26 14:50:26 | 2019-03-26 04:00:00 | 28989 | Removable storage media (Floppy, USB) | FC9BD2D2 |  |
| F:\d26ac13321f158c9e5e2fa459a6974ba.jpg | 2019-03-26 12:41:15 | 2019-03-26 17:24:25 | 2022-11-30 01:18:16 | 2019-02-20 18:41:45 | 2019-02-19 18:27:18 | 2019-02-20 04:00:00 | 35920 | Removable storage media (Floppy, USB) | 20F3BCE6 |  |
| C:\Users\Justine B\Documents\Owl Musings.docx | 2019-03-26 16:03:02 | 2019-03-26 16:51:53 | 2022-11-30 01:18:16 | 2019-03-26 16:51:52 | 2019-03-26 16:51:53 | 2019-03-26 16:51:52 | 20931 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads\Owls and Their Homes.docx | 2019-03-26 16:03:02 | 2019-03-26 16:51:53 | 2022-11-30 01:18:16 | 2019-03-26 15:49:45 | 2019-03-26 15:49:49 | 2019-03-26 15:49:45 | 5529698 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Downloads | 2019-03-25 13:06:46 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-25 13:05:45 | 2019-03-27 12:06:06 | 2019-03-27 12:06:06 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Desktop | 2019-03-25 13:06:46 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-25 13:05:45 | 2019-03-27 12:06:06 | 2019-03-27 12:06:06 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Documents | 2019-03-25 13:06:46 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-25 13:05:45 | 2019-03-26 17:14:08 | 2019-03-26 17:14:08 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Pictures | 2019-03-25 13:06:46 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-25 13:05:45 | 2019-03-26 17:13:21 | 2019-03-26 17:13:21 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Desktop\GoodOnes | 2019-03-25 13:06:46 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-26 15:46:21 | 2019-03-26 16:51:14 | 2019-03-26 16:51:14 | 4096 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Videos | 2019-03-25 13:06:46 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-25 13:05:45 | 2019-03-25 13:06:43 | 2019-03-25 13:06:42 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| C:\Users\Justine B\Music | 2019-03-25 13:06:46 | 2019-03-27 18:32:16 | 2022-11-30 01:18:16 | 2019-03-25 13:05:45 | 2019-03-25 13:06:43 | 2019-03-25 13:06:43 | 0 | Fixed storage media (Hard drive) | DCAECB8D | desktop-n566fm9 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 5d696d521de238c3 | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-27 18:33:50 | 17429 | 1 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:19:08 | 2019-03-27 18:33:50 | 2019-03-25 13:15:24 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 6824f4a902c78fbd | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-26 17:34:30 | 16006 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-26 17:20:30 | 2019-03-26 17:34:30 | 2019-03-25 13:20:27 |
| 9d1f905ce5044aee | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 | 2019-03-26 17:15:19 | 0 |  |  |  | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 |  |
| 9d1f905ce5044aee | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 | 2019-03-26 17:15:19 | 0 |  |  |  | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 |  |
| 9d1f905ce5044aee | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 | 2019-03-26 17:15:19 | 0 |  |  |  | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 |  |
| 9d1f905ce5044aee | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 | 2019-03-26 17:15:19 | 0 |  |  |  | 2019-03-25 13:07:14 | 2019-03-26 17:15:19 |  |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| be71009ff8bb02a2 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 25E40 | 2 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-27 12:02:41 | 2019-03-27 12:02:41 | 2019-03-26 15:54:20 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 |  |  |  |  | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 |  |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 |  |  |  |  | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 |  |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ccc0fa1b9f86f7b3 | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-27 12:13:48 | 17A17 | 3 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 13:23:18 | 2019-03-27 12:13:48 | 2019-03-25 13:23:02 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| ceb762e61b8637b9 | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-27 11:47:02 | 17DA2 | 5 | desktop-n566fm9 | 70:5a:b6:91:13:5d | 2019-03-25 15:29:12 | 2019-03-27 11:47:02 | 2019-03-25 15:16:18 |
| AppId | SourceCreated | SourceModified | SourceAccessed | TargetMFTEntryNumber | TargetMFTSequenceNumber | MachineID | MachineMACAddress | SourceCreated | SourceModified | TargetAccessed |
| AppId | SourceCreated | SourceModified | SourceAccessed | TargetMFTEntryNumber | TargetMFTSequenceNumber | MachineID | MachineMACAddress | SourceCreated | SourceModified | TargetAccessed |

## APPENDIX VIII: USB Analysis



## APPENDIX IX: Chain of Custody Report

