

Case Project 04

**CY5210 Information System Forensics** 

**Instructor: Elton Booker** 

Jonathan Metzger

December 4th, 2022

### **Table of Contents**

TABLE OF CONTENTS	2
EXECUTIVE SUMMARY	3
INTRODUCTION	4
ANALYSIS	5
REGISTRY ANALYSIS	5
USER INFORMATION	6
GROUP INFORMATION	7
SYSTEM INFORMATION	8
USER ACTIVITY	10
USB DEVICE ACTIVITY	11
APPLICATIONS AND MALWARE	12
PREFETCH	13
SHELL ITEMS	14
CONCLUSION	17
APPENDIX	18
APPENDIX I: FORENSIC TOOLS	18
APPENDIX II: REGISTRY PATHS	18
APPENDIX III: ARTIFACTS LIST	19
APPENDIX IV: Prefetch Analysis	20
APPENDIX V: SHELLBAG ANALYSIS	26
APPENDIX VI: LINK ANALYSIS	27
APPENDIX VII: JUMP LIST ANALYSIS	29
APPENDIX VIII: USB Analysis	36
APPENDIX IX: CHAIN OF CUSTODY REPORT	37

#### **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 28<sup>th</sup>, 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.

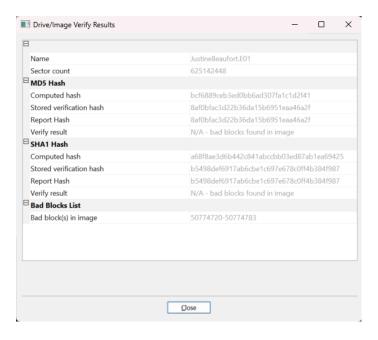


Figure 1 Hash Verification of JustineBeaufort.E01

#### **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 1 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
<b>Build Version</b>	\${CurrentVersion}\CurrentBuild	17134
<b>Current Control Set</b>	\${ControlSet}	001
Computer Name \${ControlSet}\Control\ComputerName\Compute rName		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></reg_binary>	2019-03-27 11:44:54

Table 2 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.



Figure 2 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 3 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	AA01021517035531 0594	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 4 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			Х	Χ
	13:23:03Z				
Mozilla Firefox 66.0.1 (x64 en-US)	2019-03-25	Х	Х	Х	Х
v.66.0.1	13:20:37Z				
Google Chrome v.73.0.3683.86	2019-03-25	X	Х	Х	Х
	13:15:24Z				
<b>Microsoft Office Professional Plus</b>	2019-03-26			Х	Х
2010 v.14.0.6029.1000	15:54:44Z				
DXM_Runtime, MPlayer2	2018-04-12	X	Х	Х	Х
	09:16:26Z				

Table 5 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
CCLEANE R64.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.E XE	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.EX E	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 INSTALLE R.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
MICROSOF T.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
MICROSOF TEDGE.EX E	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
TRUSTEDI NSTALLER .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 6 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\Jus tine B\AppData\Roaming\ Microsoft\Skype	Directory	Skype		2019-03-25 13:11:55
Desktop\C:\\Users\Jus tine B\AppData\Roaming\ Microsoft\Skype\live#3 astevedallas1010	Directory	live#3astevedallas1010	2019-03-25 13:13:25	2019-03-25 13:13:25
Desktop\D:\\GoodOne s	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:\MagnetP rocessCapture- 20190326-140822	Directory	MagnetProcessCapture- 20190326-140822	2019-03-26 18:08:28	2019-03-26 18:08:28

Table 7 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

### 2022\_CaseStudy\_04

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\gr umpy- 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\h qdefault.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\stellaAndS herlock.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.xls x	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_B ro.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 8 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:\GoodOn es\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:\GoodOn es\grumpy- owl_c_2512 435.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.j pg	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\Ju stine B\Download s\stellaAnd Sherlock.jp	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\Ju stine B\Download s\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\Ju stine B\Download s\Whooo_A m_I_Owls_B ro.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\Ju stine B\Download s\Owls and Their Homes.doc x	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_A m_I_Owls_B ro.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 9 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"

<sup>\*</sup>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\Explore	<policies>\RunMRU</policies>	User Command
	r\		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**

- NTFS Files
  - NONAME [NTFS]/[root]/\$MFT
  - NONAME [NTFS]/[root]/\$LogFile
- II. 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
  - o NONAME [NTFS]/[root]/Users/Justine B/NTUSER.DAT
  - NONAME [NTFS]/[root]/Users/Justine
     B/AppData/Local/Microsoft/Windows/UsrClass.dat
- III. Logs
  - NONAME [NTFS]/[root]/Windows/System32/winevt/Logs
- IV. Additional Shellbag Folders
  - NONAME [NTFS]/[root]/Windows/Prefetch
  - NONAME [NTFS]/[root]/Users/Justine
     B/AppData/Roaming/Microsoft/Windows/Recent
- V. 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
- VI. Additional Artifacts
  - NONAME [NTFS]/[root]/\$Recycle.Bin (folder)
  - NONAME [NTFS]/[root]/Windows/INF/setupapi.dev.log

# **APPENDIX IV: Prefetch Analysis**

Executable	Source	Source	Source	Size	Run	Last	First	Volume/
Name	Created	Modified	Accessed		Count	Run	Run	Serial
AM_DELTA	2022-11-30	2019-03-27	2022-11-30	9748	2	2019-03-27	2019-03-25	DCAECB8D
.EXE	01:18:41 2022-11-30	11:50:01 2019-03-27	01:18:52 2022-11-30	62166	5	11:49:51 2019-03-27	16:49:43 2019-03-25	DCAECB8D
APPLICATI ONFRAME	01:18:41	11:46:50	01:18:52	02100	5	11:46:40	13:07:01	DCAECBOD
HOST.EXE	01.10.11	11110.00	01.10.02			11.10.10	10.07.01	
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
ARESREG	2022-11-30	2019-03-25	2022-11-30	50002	1	2019-03-25		DCAECB8D
ULAR246_I NSTALLER .EXE	01:18:41	15:07:52	01:18:52			15:07:42		
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
BACKGRO	2022-11-30	2019-03-27	2022-11-30	95272	18	2019-03-27	2019-03-26	DCAECB8D
UNDTASK HOST.EXE	01:18:41	18:25:03	01:18:52			18:24:53	15:59:13	
BACKGRO UNDTASK HOST.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
CCLEANE R.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
CCLEANE R64.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
CCSETUP5 55.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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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.E XE	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
CHXSMAR TSCREEN. 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

		ı	ı	ı		ı	ı	
CTFMON.E	2022-11-30	2019-03-27	2022-11-30	13460	3	2019-03-27	2019-03-25	DCAECB8D
XE	01:18:41	11:44:40	01:18:53			11:44:40	19:28:19	
DISMHOST	2022-11-30	2019-03-26	2022-11-30	35360	1	2019-03-26		DCAECB8D
.EXE	01:18:41	18:06:00	01:18:53			18:05:50		
DLLHOST.	2022-11-30	2019-03-25	2022-11-30	38168	1	2019-03-25		DCAECB8D
			01:18:53	30100	'	13:10:41		DOALOBOD
EXE	01:18:41	13:10:51						50150505
DLLHOST.	2022-11-30	2019-03-27	2022-11-30	39640	4	2019-03-27	2019-03-25	DCAECB8D
EXE	01:18:41	11:44:28	01:18:53			11:44:17	13:09:12	
DLLHOST.	2022-11-30	2019-03-27	2022-11-30	22462	4	2019-03-27	2019-03-25	DCAECB8D
EXE	01:18:41	11:47:45	01:18:53			11:47:40	16:46:25	
DLLHOST.	2022-11-30	2019-03-27	2022-11-30	28890	9	2019-03-27	2019-03-25	DCAECB8D
EXE	01:18:41	11:42:35	01:18:53	2000		11:42:25	15:54:21	20,120202
DLLHOST.	2022-11-30	2019-03-27	2022-11-30	15074	35	2019-03-27	2019-03-26	DCAECB8D
				15074	აა			DCAECBOD
EXE	01:18:41	11:47:33	01:18:53			11:47:28	15:40:35	
DLLHOST.	2022-11-30	2019-03-27	2022-11-30	26054	1	2019-03-27		DCAECB8D
EXE	01:18:41	12:06:33	01:18:53			12:06:25		
DLLHOST.	2022-11-30	2019-03-27	2022-11-30	22208	5	2019-03-27	2019-03-26	DCAECB8D
EXE	01:18:41	12:05:44	01:18:53			12:05:39	12:36:06	
DLLHOST.	2022-11-30	2019-03-25	2022-11-30	39178	3	2019-03-25	2019-03-25	DCAECB8D
	01:18:41	14:38:08	01:18:53	00170		14:38:02	13:08:59	DOMEODOD
EXE				17004				DOAFODOD
DLLHOST.	2022-11-30	2019-03-27	2022-11-30	17934	8	2019-03-27	2019-03-25	DCAECB8D
EXE	01:18:41	11:44:23	01:18:53			11:44:17	13:09:12	
EASEOFAC	2022-11-30	2019-03-25	2022-11-30	89982	1	2019-03-25		DCAECB8D
CESSDIAL	01:18:41	15:54:55	01:18:53			15:54:51		
OG.EXE								
EXCEL.EX	2022-11-30	2019-03-26	2022-11-30	110856	5	2019-03-26	2019-03-26	FC9BD2D2
E	01:18:41	16:49:40	01:18:53			16:49:34	16:02:02	. 002222
FILECOAU	2022-11-30	2019-03-27	2022-11-30	36878	5	2019-03-27	2019-03-26	DCAECB8D
	01:18:41	12:05:45	01:18:53	30070	3	12:05:39	12:36:07	DOALOBOD
TH.EXE							12.30.07	50450505
FIREFOX	2022-11-30	2019-03-25	2022-11-30	28610	1	2019-03-25		DCAECB8D
INSTALLE	01:18:41	13:19:58	01:18:53			13:19:47		
R.EXE								
FIRSTLOG	2022-11-30	2019-03-25	2022-11-30	51186	1	2019-03-25		DCAECB8D
ONANIM.E	01:18:41	13:06:36	01:18:53			13:06:24		
XE								
GOOGLEU	2022-11-30	2019-03-25	2022-11-30	50348	1	2019-03-25		DCAECB8D
PDATE.EX	01:18:41	13:14:39	01:18:53	30040	'	13:14:29		DOALOBOD
	01.10.41	10.14.09	01.10.55			10.14.25		
E					•			50150505
GOOGLEU	2022-11-30	2019-03-25	2022-11-30	110630	1	2019-03-25		DCAECB8D
PDATE.EX	01:18:41	13:14:48	01:18:53			13:14:38		
E								
GOOGLEU	2022-11-30	2019-03-27	2022-11-30	55044	23	2019-03-27	2019-03-26	DCAECB8D
PDATE.EX	01:18:41	18:20:23	01:18:53			18:20:22	13:19:59	
E								
HITENE.EX	2022-11-30	2019-03-27	2022-11-30	21788	7	2019-03-27	2019-03-27	DCAECB8D
E	01:18:41	18:15:10	01:18:54	200	·	18:15:00	12:15:01	20,120202
INSTUP.EX	2022-11-30	2019-03-25	2022-11-30	196406	7	2019-03-25	2019-03-25	DCAECB8D
				190400	′			DOMECDOD
E	01:18:41	14:38:42	01:18:54	00.170		14:38:31	13:26:36	DOAFODOS
LOGONUI.	2022-11-30	2019-03-27	2022-11-30	83472	2	2019-03-27	2019-03-25	DCAECB8D
EXE	01:18:41	18:47:42	01:18:54			18:47:38	19:28:17	
MAGNETP	2022-11-30	2019-03-26	2022-11-30	82678	1	2019-03-26		74B6B897
ROCESSC	01:18:41	18:08:16	01:18:54			18:08:06		
APTURE.E								
XE								
MICROSOF	2022-11-30	2019-03-27	2022-11-30	275290	13	2019-03-27	2019-03-26	20F3BCE6
T.PHOTOS.	01:18:41	12:06:15	01:18:54	210200		12:06:11	15:42:45	20.0000
	01.10.41	12.00.10	01.10.54			12.00.11	10.72.40	
EXE	0000 11 00	0040 00 07	0000 11 00	100010	40	0040 00 07	0040 00 00	DOAFODOS
MICROSOF	2022-11-30	2019-03-27	2022-11-30	190218	12	2019-03-27	2019-03-26	DCAECB8D
		13:16:38	01:18:54			13:16:28	10:50:53	
TEDGE.EX	01:18:41							
	01:18:41	.00.00						
TEDGE.EX	2022-11-30	2019-03-27	2022-11-30	262002	31	2019-03-27	2019-03-26	DCAECB8D
TEDGE.EX E MICROSOF			2022-11-30 01:18:54	262002	31	2019-03-27 13:16:28	2019-03-26 17:07:53	DCAECB8D
TEDGE.EX E	2022-11-30	2019-03-27		262002	31			DCAECB8D

MICHORSOF   1018-41   1714-19   1018-54   1598-72   6   2019-03-26   1508-020   1508-0									
MOSSYNC   CO22-11-30   2019-03-27   2022-11-30   36478   4   2019-03-27   2019-03-25   DCAEC68D   CO22-11-30   2022-11-30   2022-11-30   2022-11-30   1142/39   CO22-11-30	MICROSOF	2022-11-30	2019-03-26	2022-11-30	158872	6	2019-03-26	2019-03-26	FC9BD2D2
MOBSYING.   2022-11-30   2019-03-27   2022-11-30   2019-03-25   DCAECBBD   1142:39	TPDFREAD	01:18:41	17:14:19	01:18:54			17:14:09	15:32:34	
MOSPINC.   2022-11-30   2019-03-27   2022-11-30   2019-03-26   2022-11-30   2019-03-26   2022-11-30   2019-03-26   2022-11-30   2019-03-26   2022-11-30   2019-03-26   2022-11-30   2019-03-27   2019-									
MCPCOMP   CREE   01:1841   11:42:50   01:18:54   20:00:00   1   20:00:00:00:00:00:00:00:00:00:00:00:00:0		0000 11 00	0010 00 07	0000 11 00	00.470	4	0010 00 07	0010 00 05	DOAFODOD
					36478	4			DCAECR8D
MPCMDRUM   158-4838	EXE	01:18:41	11:42:50	01:18:54			11:42:39	13:08:15	
December   December	MOFCOMP	2022-11-30	2019-03-26	2022-11-30	20206	1	2019-03-26		DCAECB8D
NEXE   11:849   11:8949		01:18:41	15:46:38						
MPCMDRD   11:844					00140	0		2010 02 27	DCAECDOD
Nexe   11:843   11:49:38   11:49:38   11:49:38   11:49:38   11:49:38   11:49:38   11:49:38   11:49:38   11:49:38   11:49:59   11:49:59   11:4					23142	2			DUAEUBOD
N.EKE   0118.41   11.49.33   0118.54   270170   3   2019.03.27   2019-03.25   DARCEBB							11:59:49	11:59:49	
	MPCMDRU	2022-11-30	2019-03-27	2022-11-30	41054	12	2019-03-27	2019-03-25	DCAECB8D
MPSIGSTU   2022-11-30   2019-03-27   2022-11-30   118-95   114-951   149-95   118-	N.EXE	01:18:41	11:49:33	01:18:54			11:49:29	14:39:14	
BEXE         01:18:41         11:49:53         01:18:54         01:36:54         11:49:57         16:49:03         DCAECBBD           MSACCES         2022-11:30         2019-03-27         01:18:54         11:48:57         01:18:54         11:48:50         DCAECBBD           MSACURI         2022-11:30         2019-03-27         2022-11:30         2019-03-27         2022-11:30         2019-03-27         2022-11:30         2019-03-27         2022-11:30         2019-03-27         DCAECBBD           MSCONFIG         2022-11:30         2019-03-27         2022-11:30         2019-03-27         2022-11:30         2019-03-27         2022-11:30         2019-03-27         2022-11:30         2019-03-26         2019-03-26         2019-03-26         2019-03-26         DCAECBBD           MSIBAD.T         2022-11:30         2019-03-26         2022-11:30         45330         1         2019-03-26         DCAECBBD           MSIBAD.T         2022-11:30         2019-03-27         2022-11:30         45330         1         2019-03-27         DCAECBBD           MSIBAD.T         2022-11:30         2019-03-27         2022-11:30         42518         1         2019-03-27         DCAECBBD           MSIBAD.T         2022-11:30         2019-03-27         2022-11:30	MDSIGSTII	2022-11-30	2010-03-27	2022-11-30	270170	3	2010-03-27	2010-03-25	DCAECB8D
MSACCES   2022-11-30   2019-03-27   2019-03-27   0118-54   11.48-57   11.48					270170	0			DOALOBOD
S.EKE   01-18-41   11-88-57   01-18-54   29960   5   2019-03-27   2019-03-25   02AECBBD								10.49.03	
MSACOHIC   2022-11-30   2019-03-27   2022-11-30   2018-03-27   11-48:20   11-48:21   11-48:22   11-48:23   11-48:23   11-48:23   11-48:23   11-48:24   1	MSACCES				63562	1			DCAECB8D
MSCONFIG   01:18:41	S.EXE	01:18:41	11:48:57	01:18:54			11:48:50		
MSCONFIG   01:18:41	MSASCUIL	2022-11-30	2019-03-27	2022-11-30	29960	5	2019-03-27	2019-03-25	DCAECB8D
MSCORSV   Color							11:46:20		
MSCORSY   011841   114738   011854   114878   011854   114728   019-03-27   2019-03-27   2019-03-27   174844   174844   174845   011854   174845   011854   1748444   1748444   1748444   174844   174844   174844   174844   174844   1748444   174844   174					00000	- 1		10.00.20	DCAECDOD
MSCORSY   2022-11-30   2019-03-27   2022-11-30   01:18:54   17:48:45   17:48:44   17:48:45   17:4					28896	I			DOMECRAD
MISSIA14CT   17:48:45							11:47:28		
MISSIA14CT   17:48:45	MSCORSV	2022-11-30	2019-03-27	2022-11-30	41896	2	2019-03-27	2019-03-27	DCAECB8D
MSIB14C.T   2022-11-30   2019-03-26   2022-11-30   1   2019-03-26   DCAECBBD   MP   01:18:41   15:51:18   01:18:54   1   2019-03-26   DCAECBBD   MP   01:18:41   15:55:45   01:18:55   15:55:42   MSMPENG   2022-11-30   2019-03-27   2022-11-30   11:8:55   1   2019-03-27   DCAECBBD   MSMPENG   2022-11-30   2019-03-27   2022-11-30   11:8:55   1   2019-03-27   DCAECBBD   MSMPENG   2022-11-30   2019-03-27   2022-11-30   2019-03-27   2022-11-30   11:49:28   11:49:28   DCAECBBD   MISNOTIF   2022-11-30   2019-03-27   2022-11-30   2019-03-27   2022-11-30   2019-03-27   2022-11-30   2019-03-27   2022-11-30   2019-03-27   2022-11-30   2019-03-27   2019-03-26   2019-03-27   2019-03-26   2019-03-27   2019-03-26   2019-03-26   2019-03-27   2019-03-26   2019-03-27   2019-03-26   2019-03-27   2019-03-26   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27		01:18:41		01:18:54			17:48:44		
MSIGNADLT   15:51:18					45220	-1			DCVECDOD
MSI9AOD.T   2022-11-30					45550	ı			DUALUBOD
MSMPENG   Color									
MSMPENG   2022-11-30   2019-03-27   2022-11-30   01:18:55   11:49:28   DCAECBBD   DCAE	MSI9A0D.T				42518	1			DCAECB8D
MUSNOTIF   2022-11-30	MP	01:18:41	15:55:45	01:18:55			15:55:42		
MUSNOTIF   2022-11-30	MSMPENG	2022-11-30	2019-03-27	2022-11-30	67058	1	2019-03-27		DCAECB8D
MUSNOTIF   2022-11-30					0.000	•			20/120202
CATIONU   CATI					04754				DOAFODOD
MUSNOTIF   2022-11-30					21/54	l			DCAECR8D
MUSNOTIF   2022-11-30   2019-03-27   2022-11-30   219-03-27   2019-03-26   2019-03-27   2019-03-26   2019-03-26   2019-03-27   2019-03-26   2019-0	ICATIONU	01:18:41	11:44:40	01:18:55			11:44:39		
VICON.EXE	X.EXE								
VICON.EXE	MUSNOTIF	2022-11-30	2019-03-27	2022-11-30	22898	17	2019-03-27	2019-03-26	DCAFCB8D
NGEN.EXE   2022-11-30   2019-03-27   2022-11-30   01:18:55   01:18:55   0222-11-30   2019-03-27   0222-11-30   02019-03-27   02019-03-25   02019-03-27   0						• •			20/120202
NGENTAS   2022-11-30   2019-03-27   2022-11-30   64676   2   2019-03-27   2019-03-27   2019-03-27   17:48:44   17:48:45   10:18:41   17:48:47   10:18:41   17:48:47   10:18:45   11:48:47   10:18:41   17:48:47   10:18:55   10:18:55   10:18:39   17:48:46   17:48:46   10:18:41   17:48:47   10:18:55   10:18:55   10:18:41   10:18:55   10:18:55   10:18:55   10:18:55   10:18:41   10:000   10:18:55   10:18:41   10:000   10:18:55   10:18:55   10:18:55   10:18:55   10:18:55   10:18:41   10:000   10:18:55   10:18:41   10:000   10:18:55   10:18:41   10:18:41   10:18:41   10:18:41   10:18:41   10:18:55   10:18:55   10:18:55   10:18:55   10:18:55   10:18:55   10:18:55   10:18:55   10:18:55   10:18:41   10:18:41   10:18:41   10:18:55   10:18					054.40	4			DOAFODOD
NGENTAS   2022-11-30	NGEN.EXE				25140	4			DCAECR8D
N.EXE		01:18:41	17:48:45	01:18:55			17:48:44	17:48:41	
NISSRV.EX   2022-11-30   2019-03-27   2022-11-30   26404   4   2019-03-27   2019-03-25   DCAECBBD	NGENTAS	2022-11-30	2019-03-27	2022-11-30	64676	2	2019-03-27	2019-03-27	DCAECB8D
NISSRV.EX   2022-11-30   2019-03-27   2022-11-30   26404   4   2019-03-27   2019-03-25   DCAECBBD	K.EXE	01:18:41	17:48:47	01:18:55			17:48:39	17:48:46	
Texas   Column   Texas   Texas   Column   Texas   Texas   Column   Texas   Texas   Column   Texas   Texas   Column   Texas   Column   Texas   Texas   Texas   Column   Texas   Texas   Texas   Column   Texas   Texas   Texas   Column   Texas   Texa					26404	1			DCAECB8D
NISSRV.EX   2022-11-30   2019-03-27   11:50:00   01:18:41   11:50:00   01:18:55   12:019-03-27   11:49:50   DCAECB8D					20404				DOALOBOD
E								13.05.17	
NOTIFICAT   2022-11-30   2019-03-27   2022-11-30   01:18:55   2019-03-27   18:25:26   2019-03-27   18:25:26   2019-03-27   18:25:26   2019-03-27   2019-03-26   DCAECB8D   2019-03-27   2019-03-26   10:46:35   2019-03-25   2022-11-30   2019-03-25   2022-11-30   2019-03-25   2022-11-30   2019-03-25   2022-11-30   2019-03-26   2022-11-30   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-27   2019-03-26   2019-03-26   2019-03-26   2019-03-26   2019-03-26   2019-03-26   2019-03-26   2019-03-26   2019-03-26   2019-03-27   2019-03-26   2019-03-26   2019-03-27   2019-03-27   2019-03-26   2019-03-26   2019-03-26   2019-03-27   2019-03-26   201	NISSRV.EX				23330	1			DCAECB8D
ION_HELP   CREXE	E	01:18:41	11:50:00	01:18:55			11:49:50		
ION_HELP   Continue	NOTIFICAT	2022-11-30	2019-03-27	2022-11-30	53544	1	2019-03-27		DCAECB8D
ER.EXE         ONEDRIVE. EXE         2022-11-30 01:18:41         2019-03-27 11:46:35         2019-03-27 11:46:35         2019-03-27 11:46:35         DCAECB8D           OBENET EXE         2022-11-30 01:18:41         2019-03-25 01:18:55         10:1684         1         2019-03-25 10:46:35         DCAECB8D           WORKCON NECTIONF LOW.EXE         01:18:41         16:02:00         01:18:55         118828         4         2019-03-26 2019-03-26 12:41:15         DCAECB8D           OPENWITH LOW.EXE         2022-11-30 01:18:41         17:24:25 01:18:55         118828         4         2019-03-26 20:29-03-26 12:41:15         DCAECB8D           OSE.EXE         2022-11-30 01:18:41         17:24:25 01:18:55         16508         1         2019-03-26 20:29-03-26 12:41:15         A9DEAB73           OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 20:22-11-30 01:18:55         34186 1         2019-03-26 20:22-11-30 13:42:02         A9DEAB73           OSPPSVC. DEVELOR DITER OF THE SET OF TH			18:25:26				18:25:26		
ONEDRIVE. EXE         2022-11-30 01:18:41         2019-03-27 11:46:35         2019-03-27 01:18:55         2019-03-26 11:46:21         DCAECB8D           OOBENET WORKCON NECTIONF LOW.EXE         2022-11-30 01:18:41         2019-03-25 16:02:00         101684         1         2019-03-25 16:01:50         DCAECB8D           OPENWITH .EXE         2022-11-30 01:18:41         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         2019-03-26 15:42:02         DCAECB8D           OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 15:42:02         2019-03-26 15:42:02         A9DEAB73           OSPPSVC. EXE         2022-11-30 01:18:41         2019-03-27 11:49:04         2019-03-27 01:18:55         2022-11-30 01:18:55         2022-11-30 01:18:55         2019-03-27 11:48:53         DCAECB8D           OUTLOOK. EXE         2022-11-30 01:18:41         2019-03-27 11:49:04         2019-03-27 01:18:55         2022-11-30 01:18:55         2022-11-30 01:18:55         2019-03-26 01:18:55         DCAECB8D           PICKERHO ST.EXE         01:18:41         17:14:08         01:18:55         35034         1         2019-03-26 01:18:41         2019-03-26 01:18:15         DCAECB8D           RUNDLL32         2022-11-30 0201-03-27         2022-11-30 01:18:55         35034 01:18:55	_	0	.0.20.20	01110100			.0.20.20		
EXE   01:18:41   11:46:35   01:18:55   11:46:21   10:46:35   DCAECB8D									50450505
OOBENET WORKCON NECTIONF LOW.EXE         2022-11-30 01:18:41         2019-03-25 01:18:55         DCAECB8D           OPENWITH .EXE         2022-11-30 01:18:41         2019-03-26 01:18:55         2022-11-30 01:18:55         118828 01:18:55         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 01:18:55         1 2019-03-26 15:42:02         A9DEAB73           OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 15:42:12         2019-03-26 01:18:55         A9DEAB73           OSPPSVC. EXE         2022-11-30 01:18:41         2019-03-27 01:18:55         2022-11-30 01:18:55         2022-11-30 01:18:55         2022-11-30 01:18:55         2019-03-27 01:18:55         2019-03-27 01:18:55         DCAECB8D           OUTLOOK. EXE         2022-11-30 01:18:41         2019-03-27 18:24:50         2019-03-27 01:18:55         2022-11-30 01:18:55         212270 01:18:55         3 2019-03-27 17:13:59         DCAECB8D           PICKERHO ST.EXE         2022-11-30 01:18:41         2019-03-25 17:13:16         2019-03-26 17:13:16         DCAECB8D           RUNDLL32         2022-11-30 01:18:41         2019-03-27 15:07:59         DCAECB8D           RUNDLL32         2022-11-30 01:18:41         2019-03-27 15:07:59         DCAECB8D					/10/0	3			DCAECB8D
WORKCON NECTIONF LOW.EXE         01:18:41         16:02:00         01:18:55         16:01:50         16:01:50           OPENWITH .EXE         2022-11-30 01:18:41         2019-03-26 17:24:25         2022-11-30 01:18:55         118828 01:18:55         4         2019-03-26 17:24:20         2019-03-26 12:41:15         DCAECB8D APDEAB73           OSE, EXE         2022-11-30 01:18:41         2019-03-26 15:42:02         2019-03-26 01:18:55         1         2019-03-26 15:42:02         APDEAB73           OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 15:42:12         34186         1         2019-03-26 15:42:02         APDEAB73           OSPPSVC. EXE         2022-11-30 01:18:41         2019-03-27 11:49:04         2022-11-30 01:18:55         43762 01:18:55         2         2019-03-27 2019-03-27         DCAECB8D           DUTLOOK. EXE         2022-11-30 01:18:41         2019-03-27 18:25:20         2019-03-27 01:18:55         2022-11-30 01:18:55         2019-03-27 01:18:55         DCAECB8D           PICKERHO ST.EXE         01:18:41 01:18:41         17:14:08 17:14:08         01:18:55 01:18:55         122454 01:18:55         2         2019-03-26 01:18:55         DCAECB8D           RUNDLL32         2022-11-30 01:18:51         2019-03-27 01:18:55         2022-11-30 01:18:55         14834         1         2019-03-27 01:18:09         DCAECB8D     <	EXE	01:18:41	11:46:35	01:18:55			11:46:21	10:46:35	
NECTIONF   LOW.EXE	OOBENET	2022-11-30	2019-03-25	2022-11-30	101684	1	2019-03-25		DCAECB8D
NECTIONF   LOW.EXE	WORKCON	01:18:41	16:02:00	01:18:55			16:01:50		
LOW.EXE         OPENWITH         2022-11-30         2019-03-26         2022-11-30         118828         4         2019-03-26         2019-03-26         DCAECB8D           EXE         01:18:41         17:24:25         01:18:55         18:55         1         2019-03-26         2019-03-26         A9DEAB73           OSE.EXE         2022-11-30         2019-03-26         2022-11-30         16508         1         2019-03-26         A9DEAB73           OSE00000.         2022-11-30         2019-03-26         2022-11-30         34186         1         2019-03-26         A9DEAB73           EXE         01:18:41         15:42:12         01:18:55         43762         2         2019-03-26         DCAECB8D           EXE         01:18:41         11:49:04         01:18:55         2         2019-03-27         2019-03-26         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         2         2019-03-27         2019-03-27         DCAECB8D           PICKERHO         2022-11-30         2019-03-26         2022-11-30         122454         2         2019-03-26         2019-03-26         DCAECB8D           RUNDLL32         2022-11-30         2019-03-25         2022-11-30         35034         1		0	10.02.00	01110100					
OPENWITH .EXE         2022-11-30 01:18:41         2019-03-26 17:24:25         2019-03-26 01:18:55         2019-03-26 01:18:55         2019-03-26 17:24:20         2019-03-26 12:41:15         DCAECB8D           OSE.EXE 01:18:41         2022-11-30 15:42:02         2019-03-26 01:18:55         34186         1 2019-03-26 15:42:02         2019-03-26 15:42:02         A9DEAB73           OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 15:42:12         2019-03-26 01:18:55         A9DEAB73           OSPSVC. EXE         2022-11-30 01:18:41         43762 01:18:55         2 2019-03-27 11:48:53         2019-03-26 15:46:18         DCAECB8D           OUTLOOK. EXE         2022-11-30 01:18:41         212270 18:24:52         3 2019-03-27 18:24:52         2019-03-27 2019-03-27         DCAECB8D           PICKERHO ST.EXE         2022-11-30 01:18:41         2022-11-30 01:18:55         35034 01:18:55         1 2019-03-25 15:07:59         DCAECB8D           RUNDLL32         2022-11-30 01:18:41         2019-03-27 15:08:09         2022-11-30 01:18:55         35034 01:18:55         1 2019-03-27 15:07:59         DCAECB8D           RUNDLL32         2022-11-30 0202-11-30         2019-03-27 2022-11-30         14834         1 2019-03-27         DCAECB8D									
.EXE         01:18:41         17:24:25         01:18:55         17:24:20         12:41:15         A9DEAB73           OSE.EXE         2022-11-30 01:18:41         2019-03-26 15:42:02         1         2019-03-26 15:42:02         A9DEAB73           OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 15:42:12         A9DEAB73         A9DEAB73           OSPPSVC. EXE         2022-11-30 01:18:41         2019-03-26 11:49:04         2019-03-26 01:18:41         DCAECB8D 11:49:04           OUTLOOK. EXE         2022-11-30 01:18:41         2019-03-27 18:24:52         2019-03-27 11:49:04         DCAECB8D 11:49:04           PICKERHO ST.EXE         2022-11-30 01:18:41         2019-03-26 15:08:09         2022-11-30 01:18:55         122454 01:18:55         2         2019-03-26 17:13:59         DCAECB8D 17:13:16           RUNDLL32         2022-11-30 01:18:41         2019-03-25 15:07:59         2022-11-30 01:18:55         35034 01:18:55         1         2019-03-27 15:07:59         DCAECB8D           RUNDLL32         2022-11-30 0202-11-30         2019-03-27 2022-11-30         14834         1         2019-03-27 2019-03-26 2019-									
OSE.EXE         2022-11-30 01:18:41         2019-03-26 15:42:02         A9DEAB73           OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 15:42:02         A9DEAB73           OSPPSVC. EXE         2022-11-30 01:18:41         2019-03-26 15:42:02         A9DEAB73 15:42:02           OSPPSVC. EXE         2022-11-30 01:18:41         2019-03-27 11:48:55         2019-03-26 11:48:53         DCAECB8D 15:46:18           OUTLOOK. EXE         2022-11-30 01:18:41         2019-03-27 18:24:52         2019-03-27 11:49:04         DCAECB8D 11:49:04           PICKERHO ST.EXE         2022-11-30 01:18:41         2019-03-26 17:13:59         2022-11-30 17:13:59         DCAECB8D 17:13:16           RUNDLL32         2022-11-30 01:18:41         2019-03-25 15:08:09         2022-11-30 01:18:55         35034 01:18:55         1         2019-03-25 15:07:59         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D					118828	4			DCAECB8D
O1:18:41         15:42:02         01:18:55         15:42:02         A9DEAB73           OSE00000.         2022-11-30 01:18:41         2019-03-26 15:42:12         A9DEAB73         A9DEAB73           EXE         01:18:41         15:42:12         01:18:55         43762         2         2019-03-27         2019-03-26 11:48:53         DCAECB8D           EXE         01:18:41         11:49:04         01:18:55         212270         3         2019-03-27 11:48:53         2019-03-27 2019-03-27         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         122454         2         2019-03-26 2019-03-26         DCAECB8D           PICKERHO ST.EXE         201:18:41         17:14:08         01:18:55         122454         2         2019-03-26 2019-03-26         DCAECB8D           RUNDLL32         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25 15:07:59         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D	.EXE	01:18:41	17:24:25	01:18:55			17:24:20	12:41:15	
O1:18:41         15:42:02         01:18:55         15:42:02         A9DEAB73           OSE00000.         2022-11-30 01:18:41         2019-03-26 15:42:12         A9DEAB73         A9DEAB73           EXE         01:18:41         15:42:12         01:18:55         43762         2         2019-03-27         2019-03-26 11:48:53         DCAECB8D           EXE         01:18:41         11:49:04         01:18:55         212270         3         2019-03-27 11:48:53         2019-03-27 2019-03-27         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         122454         2         2019-03-26 2019-03-26         DCAECB8D           PICKERHO ST.EXE         201:18:41         17:14:08         01:18:55         122454         2         2019-03-26 2019-03-26         DCAECB8D           RUNDLL32         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25 15:07:59         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D	OSE.EXE	2022-11-30	2019-03-26	2022-11-30	16508	1	2019-03-26		A9DEAB73
OSE00000. EXE         2022-11-30 01:18:41         2019-03-26 15:42:12         A9DEAB73           OSPPSVC. EXE         2022-11-30 01:18:41         34186         1 2019-03-26 15:42:02         A9DEAB73           OSPPSVC. EXE         2022-11-30 01:18:41         2019-03-27 01:18:55         2022-11-30 01:18:55         43762 01:18:55         2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2									
EXE         01:18:41         15:42:12         01:18:55         15:42:02         DCAECB8D           OSPPSVC.         2022-11-30         2019-03-27         2022-11-30         43762         2         2019-03-27         2019-03-26         DCAECB8D           EXE         01:18:41         11:49:04         01:18:55         11:48:53         15:46:18         15:46:18           OUTLOOK.         2022-11-30         2019-03-27         2022-11-30         212270         3         2019-03-27         2019-03-27         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         18:24:52         11:49:04         DCAECB8D           ST.EXE         01:18:41         17:14:08         01:18:55         2         2019-03-26         2019-03-26         DCAECB8D           RUNDLL32         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECBBD	OSEDDOO				3/196	1			ΔΩΠΕΛΕ72
OSPPSVC.         2022-11-30         2019-03-27         2022-11-30         43762         2         2019-03-27         2019-03-26         DCAECB8D           OUTLOOK.         2022-11-30         2019-03-27         2022-11-30         212270         3         2019-03-27         2019-03-27         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         18:24:52         11:49:04         DCAECB8D           PICKERHO         2022-11-30         2019-03-26         2022-11-30         122454         2         2019-03-26         2019-03-26         DCAECB8D           ST.EXE         01:18:41         17:14:08         01:18:55         17:13:59         17:13:16         DCAECB8D           RUNDLL32         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECBBD					J <del>4</del> 100	1			ASPLADIS
EXE         01:18:41         11:49:04         01:18:55         11:48:53         15:46:18           OUTLOOK.         2022-11-30         2019-03-27         2022-11-30         212270         3         2019-03-27         2019-03-27         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         18:24:52         11:49:04         DCAECB8D           PICKERHO ST.EXE         2022-11-30         2019-03-26         2022-11-30         122454         2         2019-03-26         2019-03-26         DCAECB8D           RUNDLL32 I.EXE         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECBBD									
OUTLOOK.         2022-11-30         2019-03-27         2022-11-30         212270         3         2019-03-27         2019-03-27         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         122454         2         2019-03-26         2019-03-26         DCAECB8D           PICKERHO ST.EXE         01:18:41         17:14:08         01:18:55         122454         2         2019-03-26         2019-03-26         DCAECB8D           RUNDLL32 LEXE         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D	OSPPSVC.	2022-11-30	2019-03-27	2022-11-30	43762	2	2019-03-27	2019-03-26	DCAECB8D
OUTLOOK.         2022-11-30         2019-03-27         2022-11-30         212270         3         2019-03-27         2019-03-27         DCAECB8D           EXE         01:18:41         18:25:02         01:18:55         122454         2         2019-03-26         2019-03-26         DCAECB8D           PICKERHO ST.EXE         01:18:41         17:14:08         01:18:55         122454         2         2019-03-26         2019-03-26         DCAECB8D           RUNDLL32 LEXE         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECBBD	EXE	01:18:41	11:49:04	01:18:55			11:48:53	15:46:18	
EXE         01:18:41         18:25:02         01:18:55         18:24:52         11:49:04           PICKERHO ST.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 17:13:16           RUNDLL32 .EXE         2022-11-30 01:18:41         2019-03-25 15:07:59         DCAECB8D 15:07:59           RUNDLL32 2022-11-30         2022-11-30 2019-03-27         2022-11-30 2022-11-30         14834         1         2019-03-27 2019-03-27         DCAECB8D				2022-11-30	212270	3			DCAECB8D
PICKERHO ST.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 17:13:16           RUNDLL32 .EXE         2022-11-30 01:18:41         2019-03-25 15:08:09         2022-11-30 01:18:55         35034 01:18:55         1 2019-03-25 15:07:59         DCAECB8D 15:07:59           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D					2.2270	J			20, (2000)
ST.EXE         01:18:41         17:14:08         01:18:55         17:13:59         17:13:16           RUNDLL32 .EXE         2022-11-30 01:18:41         2019-03-25 15:08:09         2022-11-30 01:18:55         35034 01:18:55         1         2019-03-25 15:07:59         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D					100151	•			DOAFODOS
RUNDLL32         2022-11-30         2019-03-25         2022-11-30         35034         1         2019-03-25         DCAECB8D           .EXE         01:18:41         15:08:09         01:18:55         15:07:59         DCAECB8D           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D					122454	2			DCAECR8D
.EXE         01:18:41         15:08:09         01:18:55         15:07:59           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D	ST.EXE	01:18:41	17:14:08	01:18:55			17:13:59	17:13:16	
.EXE         01:18:41         15:08:09         01:18:55         15:07:59           RUNDLL32         2022-11-30         2019-03-27         2022-11-30         14834         1         2019-03-27         DCAECB8D	RUNDLL32	2022-11-30	2019-03-25	2022-11-30	35034	1	2019-03-25		DCAECB8D
<b>RUNDLL32</b> 2022-11-30 2019-03-27 2022-11-30 14834 1 2019-03-27 DCAECB8D				01:18:55					
					1/192/	1			DCAECDOD
.EAE 01.18:41 17:48:38 01:18:39 17:48:37					14034				DOMEC BOD
	.EXE	01:18:41	17:48:38	01:18:55			17:48:37		

RUNDLL32	2022-11-30	2019-03-27	2022-11-30	12648	1	2019-03-27		DCAECB8D
.EXE	01:18:41	12:11:22	01:18:55			12:11:14		
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	46286	3	2019-03-27	2019-03-27	DCAECB8D
ROKER.EX	01:18:41	11:46:20	01:18:55			11:46:07	11:42:28	
E								
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	72462	37	2019-03-27	2019-03-27	DCAECB8D
ROKER.EX	01:18:41	16:12:31	01:18:55			16:12:21	12:12:49	
E								
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	55960	32	2019-03-27	2019-03-26	DCAECB8D
ROKER.EX	01:18:41	18:47:41	01:18:56	00000	0_	18:47:33	18:25:09	20, (20202
E	01110111	10.17.11	01.10.00			10.17.00	10.20.00	
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	68324	3	2019-03-27	2019-03-26	DCAECB8D
ROKER.EX	01:18:41	11:46:20	01:18:56	00024	3	11:46:05	10:46:12	DOALOBOD
E	01.10.41	11.40.20	01.10.50			11.40.00	10.40.12	
	0000 11 00	0010 00 07	0000 11 00	00000	1.5	0010 00 07	0010 00 00	DCAECDOD
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	39688	15	2019-03-27	2019-03-26	DCAECB8D
ROKER.EX	01:18:41	18:35:17	01:18:56			18:35:07	16:41:19	
E					_			
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	19498	2	2019-03-27	2019-03-26	DCAECB8D
ROKER.EX	01:18:41	11:42:44	01:18:56			11:42:34	10:46:22	
E								
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	31160	2	2019-03-27	2019-03-27	DCAECB8D
ROKER.EX	01:18:41	13:16:38	01:18:56			13:16:28	12:11:52	
E								
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	88412	11	2019-03-27	2019-03-26	DCAECB8D
ROKER.EX	01:18:41	12:11:23	01:18:56			12:11:13	12:56:17	
E		_						
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	44810	4	2019-03-27	2019-03-25	DCAECB8D
ROKER.EX	01:18:41	11:44:27	01:18:56	11010	'	11:44:17	13:09:13	DOMEOBOD
E	01110111		01.10.00				10.00.10	
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	49714	5	2019-03-27	2019-03-25	DCAECB8D
				49714	5			DUAEUDOD
ROKER.EX	01:18:41	11:46:35	01:18:56			11:46:25	13:43:29	
E								
RUNTIMEB	2022-11-30	2019-03-27	2022-11-30	18212	1	2019-03-27		DCAECB8D
ROKER.EX	01:18:41	12:11:50	01:18:56			12:11:40		
E								
SEARCHFI	2022-11-30	2019-03-27	2022-11-30	15384	91	2019-03-27	2019-03-27	DCAECB8D
LTERHOST	01:18:41	18:30:23	01:18:56			18:30:13	16:00:13	
.EXE								
SEARCHIN	2022-11-30	2019-03-27	2022-11-30	68308	6	2019-03-27	2019-03-26	42B2CA5
DEXER.EX	01:18:41	11:46:20	01:18:56			11:46:01	10:45:41	
E								
SEARCHP	2022-11-30	2019-03-27	2022-11-30	17974	81	2019-03-27	2019-03-27	DCAECB8D
ROTOCOL	01:18:41	18:30:23	01:18:56	-	-	18:30:13	16:00:13	
HOST.EXE								
SEARCHP	2022-11-30	2019-03-27	2022-11-30	20204	3	2019-03-27	2019-03-27	DCAECB8D
ROTOCOL	01:18:41	18:25:06	01:18:56			18:24:56	12:02:30	20, (20202
HOST.EXE	0 11 101 11		0.1.10.00			10.2 1.00	12.02.00	
SEARCHUI	2022-11-30	2019-03-27	2022-11-30	324298	4	2019-03-27	2019-03-25	DCAECB8D
.EXE	01:18:41	11:46:20	01:18:56	024230	7	11:46:04	13:06:57	DOALOBOD
SEDSVC.E	2022-11-30	2019-03-27	2022-11-30	55160	4	2019-03-27	2019-03-25	DCAECB8D
XE XE	01:18:41	11:47:54	01:18:56	33100	4	11:47:44	16:48:59	DUALUBOD
				114782	0			DCAECB8D
SETUP-	2022-11-30	2019-03-25	2022-11-30	114/82	2	2019-03-25	2019-03-25	DOMEORAD
STUB.EXE	01:18:41	13:20:01	01:18:56	00400	4	13:19:51	13:19:48	A0DEAD70
SETUP.EX	2022-11-30	2019-03-26	2022-11-30	30402	1	2019-03-26		A9DEAB73
E	01:18:41	15:40:46	01:18:56		-	15:40:36		5015555
SGRMBRO	2022-11-30	2019-03-27	2022-11-30	7380	2	2019-03-27	2019-03-26	DCAECB8D
KER.EXE	01:18:41	11:44:01	01:18:56			11:43:51	10:47:03	
SHELLEXP	2022-11-30	2019-03-27	2022-11-30	159304	3	2019-03-27	2019-03-26	DCAECB8D
ERIENCEH	01:18:41	11:46:20	01:18:56			11:46:02	10:46:11	
OST.EXE								
SHELLEXP	2022-11-30	2019-03-25	2022-11-30	103744	1	2019-03-25		DCAECB8D
ERIENCEH	01:18:41	13:07:07	01:18:57			13:06:56		
OST.EXE								
SIHOST.EX	2022-11-30	2019-03-26	2022-11-30	57124	2	2019-03-26	2019-03-25	DCAECB8D
E	01:18:41	10:45:47	01:18:57	- , <u>-</u> ,	_	10:45:35	14:58:36	
_	3		5					

REEN_EXE	CB8D CB8D CB8D CB8D CB8D CB8D CB8D
SOFTWAR   2022-11-30   2019-03-26   2022-11-30   21928   2   2019-03-26   2019-03-26   DCAE( REPORT   118:41   14:53:15   14:53:15   14:53:05   10:18:41   12:12:14   12:12:14   11:18:57   12:12:04   13:16:44   13:16:44   13:16:44   14:45:05   11:18:57   12:12:04   13:16:44   13:16:44   14:45:05   14:45:05   14:45:09	CB8D CB8D CB8D CB8D CB8D CB8D CB8D
SOFTWAR   2022-11-30	CB8D CB8D CB8D CB8D
ER_TOOL. EXE  SPEECHR 2022-11-30 2019-03-27 2022-11-30 62980 10 2019-03-27 12:12:04 13:16:44  SPLWOW6 2022-11-30 2019-03-26 4.EXE SPLWOW6 4.EXE 01:18:41 11:47:55 01:18:57  SPSVC.E 2022-11-30 2019-03-27 2022-11-30 2019-03-26 EXE 01:18:41 18:25:35 01:18:57 SVCHOST. 2022-11-30 2019-03-27 2022-11-30 2019-03-26 2022-11-30 2019-03-26 EXE 01:18:41 18:47:33 01:18:57 SVCHOST. 2022-11-30 2019-03-27 2022-11-30 2019-03-26 DCAE( 2019-03-27 2019-03-26 DCAE( 2019-0	CB8D CB8D CB8D CB8D
EXE   SPEECHR   2022-11-30   2019-03-27   2022-11-30   62980   10   2019-03-27   2019-03-25   13:16:44   XE   SPLWOW6   2022-11-30   2019-03-26   2022-11-30   47266   2   2019-03-26   16:09:310   2019-03-26   4.EXE   01:18:41   16:49:15   01:18:57   13:16:44   16:49:15   01:18:57   13:16:31   01:18:57   13:16:31   01:18:41   11:47:51   01:18:57   13:16:31   01:18:41   11:46:32   01:18:57   11:46:02   13:08:24   01:18:41   11:46:32   01:18:57   11:46:02   13:08:24   01:18:41   11:46:30   01:18:57   11:46:02   13:08:24   01:18:41   11:46:30   01:18:57   11:46:02   13:08:24   01:18:41   11:46:30   01:18:57   11:46:02   13:08:24   01:18:41   11:46:30   01:18:57   11:46:02   13:08:24   01:18:41   11:46:30   01:18:57   11:46:02   13:08:24   01:18:41   11:46:30   01:18:57   11:46:02   13:08:24   01:18:41   11:46:03   01:18:57   11:46:02   13:08:24   01:18:41   11:46:03   01:18:57   11:46:02   13:08:24   01:18:41   11:46:03   01:18:57   11:46:02   13:08:24   01:18:41   11:46:03   01:18:57   11:46:07   10:46:21   01:46:01   0	CB8D CB8D CB8D CB8D
SPEECHR UNTIME.E U1:18:41   12:12:14   01:18:57   12:12:04   12:	CB8D CB8D CB8D CB8D
UNTIME.E   01:18:41   12:12:14   01:18:57     12:12:04   13:16:44     XE   SPLWOW6   2022-11-30   2019-03-26   2022-11-30   47266   2   2019-03-26   2019-03-26   DCAE( 4.EXE   01:18:41   16:49:15   01:18:57   32430   13   2019-03-27   2019-03-25   DCAE( 4.EXE   01:18:41   11:47:55   01:18:57   11:47:45   14:43:09   STTRAY64.   2022-11-30   2019-03-27   2022-11-30   43668   4   2019-03-27   2019-03-25   DCAE( 4.EXE   01:18:41   11:46:32   01:18:57   11:47:45   14:43:09   SVCHOST.   2022-11-30   2019-03-27   2022-11-30   18764   2   2019-03-27   2019-03-25   DCAE( 4.EXE   01:18:41   11:46:36   01:18:57   11:46:26   11:42:55   DCAE( 4.EXE   01:18:41   11:46:36   01:18:57   11:46:26   11:42:55   DCAE( 4.EXE   01:18:41   11:46:20   01:18:57   11:46:26   11:42:55   DCAE( 4.EXE   01:18:41   11:46:20   01:18:57   11:46:20   01:18:57   DCAE( 4.EXE   01:18:41   11:47:11   01:18:57   DCAE( 4.EXE   01:18:41   11:47:11   01:18:57   DCAE( 4.EXE   01:18:41   11:47:31   01:18:57   DCAE( 4.EXE   01:18:41   11:47:31   01:18:57   DCAE( 4.EXE   01:18:41   11:47:31   01:18:57   DCAE( 4.EXE   01:18:41   11:47:33   01:18:57   DCAE( 4.EXE   01:18:41   11:48:48   01:18:57   DCAE( 4.EXE   01:18:41   11:48	CB8D CB8D CB8D
SPLWOW6 4_EXE         2022-11-30 10:18:41         2019-03-26 16:49:15         2022-11-30 01:18:57         47266         2 2019-03-26 16:49:05         2019-03-26 16:49:05         DCAEC 16:49:05           SPSVC.E XE         2022-11-30 01:18:41         2022-11-30 11:47:55         32430         13 2019-03-27 11:47:45         2019-03-25 11:47:45         DCAEC 14:43:09           STTRAY64.         2022-11-30 01:18:41         2022-11-30 11:46:32         43668 01:18:57         4 2019-03-27 11:46:20         2019-03-25 11:46:20         DCAEC 13:08:24           SVCHOST.         2022-11-30 02:21-11-30         2019-03-27 2022-11-30         2022-11-30 20:21-11-30         2019-03-27 20:22-11-30	CB8D CB8D CB8D
4.EXE         01:18:41         16:49:15         01:18:57         16:49:05         16:03:10           SPPSVC.E         2022-11-30         2019-03-27         2022-11-30         32430         13         2019-03-27         2019-03-25         DCAE(           STTRAY64.         2022-11-30         2019-03-27         2022-11-30         43668         4         2019-03-27         2019-03-25         DCAE(           EXE         01:18:41         11:46:32         01:18:57         18764         2         2019-03-27         2019-03-25         DCAE(           EXE         01:18:41         11:46:32         01:18:57         18764         2         2019-03-27         2019-03-27         DCAE(           EXE         01:18:41         11:46:36         01:18:57         18764         2         2019-03-27         2019-03-27         DCAE(           EXE         01:18:41         11:46:20         01:18:57         11:46:20	CB8D CB8D CB8D
XE         01:18:41         11:47:55         01:18:57         43668         4         2019-03-27         2019-03-27         2022-11-30         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2019-03-27         2022-11-30         2019-03-27         2022-11-30         2019-03-27         2022-11-30         2019-03-27         2022-11-30         2019-03-27         2022-11-30         2019-03-27         2022-11-30         2019-03-27         2022-11-30         2019-03-27         2019-03-27         2022-11-30         2019-03-27         2019-03	CB8D CB8D
STTRAY64.         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         DCAEC DCAEC 13:08:24           SVCHOST.         2022-11-30 01:18:41         2019-03-27 11:46:36         2019-03-27 01:18:57         2019-03-27 11:46:26         DCAEC 11:46:26           SVCHOST.         2022-11-30 01:18:41         2019-03-27 11:46:20         2019-03-27 01:18:57         2019-03-27 11:46:20         2019-03-26 10:46:21         DCAEC 11:46:20           SVCHOST.         2022-11-30 01:18:41         2019-03-27 11:43:06         2022-11-30 01:18:57         22386 11:42:55         4 2019-03-27 11:42:55         2019-03-25 13:04:21         DCAEC 13:04:21           SVCHOST.         2022-11-30 01:18:41         2019-03-27 18:25:35         2022-11-30 01:18:57         2019-03-27 18:25:25         DCAEC 13:04:21           SVCHOST.         2022-11-30 01:18:41         2019-03-27 10:18:57         2022-11-30 10:18:57         10:46:56         DCAEC 16:03:11           SVCHOST.         2022-11-30 01:18:41         2019-03-27 10:46:16         2022-11-30 01:18:57         17726         3 2019-03-27 11:47:20         2019-03-26 2019-03-27         DCAEC 2022-11-30           SVCHOST.         2022-11-30 01:18:41         2019-03-27 11:48:48         2022-11-30 01:18:57         16484 11:49:39         2019-03-27 11:49:39         2019-03-26	CB8D
EXE         01:18:41         11:46:32         01:18:57         11:46:20         13:08:24           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         18764         2         2019-03-27         2019-03-27         DCAE(           EXE         01:18:41         11:46:36         01:18:57         11:46:07         11:42:55           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         25288         3         2019-03-27         2019-03-26         DCAE(           EXE         01:18:41         11:46:20         01:18:57         11:46:07         10:46:21         DCAE(           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         23134         1         2019-03-27         2019-03-27         2022-11-30         23134         1         2019-03-27         DCAE(           EXE         01:18:41         18:25:35         01:18:57         1         2019-03-27         DCAE(         DCAE(           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         18222         1         2019-03-27         2019-03-27         2022-11-30         18:25:25           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         17:26         3 <t< th=""><th>CB8D</th></t<>	CB8D
EXE         01:18:41         11:46:36         01:18:57         11:46:26         11:42:55           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         25288         3         2019-03-27         2019-03-26         DCAE(           EXE         01:18:41         11:46:20         01:18:57         2022-11-30         2019-03-27	
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         25288         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:46:20         01:18:57         22386         4         2019-03-27         2019-03-25         DCAEC           EXE         01:18:41         11:43:06         01:18:57         23134         1         2019-03-27         2019-03-25         DCAEC           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         23134         1         2019-03-27         13:04:21         DCAEC           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         18222         1         2019-03-26         DCAEC           EXE         01:18:41         16:03:21         01:18:57         18222         1         2019-03-26         DCAEC           EXE         01:18:41         11:47:11         01:18:57         42946         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:47:31         01:18:57         3         2019-03-27         2019-03-26         DCAEC           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         17726         3         2019-03	B8D
EXE         01:18:41         11:46:20         01:18:57         11:46:07         10:46:21           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         2019-03-27         2019-03-25         DCAE(           EXE         01:18:41         11:43:06         01:18:57         23134         1         2019-03-27         DCAE(           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         18:25:25         18:25:25         DCAE(           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         18222         1         2019-03-26         DCAE(           EXE         01:18:41         16:03:21         01:18:57         18:25:25         16:03:11         DCAE(           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         42946         3         2019-03-27         2019-03-26         DCAE(           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         17726         3         2019-03-27         2019-03-26         DCAE(           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         16484         2         2019-03-27         2019-03-26         DCAE(           SVCHOST.         2022-11-30         2019-03-27<	
EXE         01:18:41         11:43:06         01:18:57         11:42:55         13:04:21           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         23134         1         2019-03-27         DCAEC           EXE         01:18:41         18:25:35         01:18:57         18:22:25         1         2019-03-26         DCAEC           EXE         01:18:41         16:03:21         01:18:57         16:03:11         2019-03-26         DCAEC           EXE         01:18:41         16:03:21         01:18:57         2022-11-30         10:49:03-27         2019-03-26         DCAEC           EXE         01:18:41         11:47:11         01:18:57         11:47:01         10:46:56         DCAEC           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         17726         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:47:33         01:18:57         16484         2         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:50:09         01:18:57         16484         2         2019-03-27         2019-03-26         DCAEC           SVCHOST.         2022-11-30         2019-03-27	
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         23134         1         2019-03-27         DCAE           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         18222         1         2019-03-26         DCAE           EXE         01:18:41         16:03:21         01:18:57         42946         3         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:47:11         01:18:57         42946         3         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:47:11         01:18:57         17726         3         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:47:33         01:18:57         16484         2         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:47:33         01:18:57         16484         2         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         36958         1         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:48:48         01:18:57         11:48:38         2 <t< th=""><th>B8D</th></t<>	B8D
EXE         01:18:41         18:25:35         01:18:57         18:25:25           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         18222         1         2019-03-26         DCAEC           EXE         01:18:41         16:03:21         01:18:57         42946         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:47:11         01:18:57         17726         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:47:33         01:18:57         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:47:33         01:18:57         16484         2         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:50:09         01:18:57         16484         2         2019-03-27         2019-03-26         DCAEC           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         36958         1         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:48:48         01:18:57         11:48:38         2         2019-03-27         2019-03-26         DCAEC	:B8D
EXE         01:18:41         16:03:21         01:18:57         16:03:11         16:03:11           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         42946         3         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:47:11         01:18:57         17726         3         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:47:33         01:18:57         16484         2         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:50:09         01:18:57         16484         2         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:50:09         01:18:57         36958         1         2019-03-27         2019-03-26         DCAE0           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         36958         1         2019-03-27         2019-03-26         DCAE0           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         51586         2         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:43:43         01:18:57         11:43:31         10:46:28 <th></th>	
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         42946         3         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:47:11         01:18:57         17726         3         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         01:18:57         16484         2         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:50:09         01:18:57         16484         2         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:50:09         01:18:57         36958         1         2019-03-27         10:45:50           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         36958         1         2019-03-27         DCAE           EXE         01:18:41         11:48:48         01:18:57         51586         2         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:49:43         01:18:57         11:43:31         10:46:28         DCAE           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-0	B8D
EXE         01:18:41         11:47:11         01:18:57         11:47:01         10:46:56           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         17726         3         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:47:33         01:18:57         16484         2         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:50:09         01:18:57         36958         1         2019-03-27         10:45:50           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         36958         1         2019-03-27         DCAE0           EXE         01:18:41         11:48:48         01:18:57         51586         2         2019-03-27         2019-03-26         DCAE0           EXE         01:18:41         11:43:43         01:18:57         51586         2         2019-03-27         2019-03-26         DCAE0           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-03-26         DCAE0           EXE         01:18:41         17:08:45         01:18:57         3         2019-03-26         DCAE0           EXE         01:18:41	B8D
EXE         01:18:41         11:47:33         01:18:57         11:47:23         10:46:16           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         16484         2         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:50:09         01:18:57         36958         1         2019-03-27         DCAEC           EXE         01:18:41         11:48:48         01:18:57         11:48:38         DCAEC           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         51586         2         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:43:43         01:18:57         11:43:31         10:46:28           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-03-26         DCAEC           EXE         01:18:41         17:08:45         01:18:57         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         17:08:45         01:18:57         3         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         17:08:45         01:18:57         3         2019-03-27         2019-	
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         16484         2         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:50:09         01:18:57         36958         1         2019-03-27         10:45:50         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         36958         1         2019-03-27         11:48:38         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         51586         2         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:43:43         01:18:57         11:43:31         10:46:28           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-03-26         DCAE           EXE         01:18:41         17:08:45         01:18:57         3         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         15018         3         2019-03-27         2019-03-26         DCAE	B8D
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         36958         1         2019-03-27         DCAE           EXE         01:18:41         11:48:48         01:18:57         11:48:38         1         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         51586         2         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-03-26         DCAE           EXE         01:18:41         17:08:45         01:18:57         15018         3         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         15018         3         2019-03-27         2019-03-26         DCAE	B8D
EXE         01:18:41         11:48:48         01:18:57         11:48:38         11:48:38           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         51586         2         2019-03-27         2019-03-26         DCAEC           EXE         01:18:41         11:43:43         01:18:57         11:43:31         10:46:28           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-03-26         DCAEC           EXE         01:18:41         17:08:45         01:18:57         15018         3         2019-03-27         2019-03-26         DCAEC           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         15018         3         2019-03-27         2019-03-26         DCAEC	
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         51586         2         2019-03-27         2019-03-26         DCAE           EXE         01:18:41         11:43:43         01:18:57         51586         2         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-03-26         DCAE           EXE         01:18:41         17:08:45         01:18:57         15018         3         2019-03-27         2019-03-26         DCAE           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         15018         3         2019-03-27         2019-03-26         DCAE	B8D
SVCHOST.         2022-11-30         2019-03-26         2022-11-30         26268         1         2019-03-26         DCAE           EXE         01:18:41         17:08:45         01:18:57         17:08:34         17:08:34           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         15018         3         2019-03-27         2019-03-26         DCAE	B8D
EXE         01:18:41         17:08:45         01:18:57         17:08:34           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         15018         3         2019-03-27         2019-03-26         DCAE(	,B8D
	,000
	B8D
EXE         01:18:41         11:47:50         01:18:57         11:47:40         10:46:59           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         18340         2         2019-03-27         2019-03-26         DCAE	:B8D
EXE 01:18:41 11:49:00 01:18:57 11:48:50 10:45:50	LOD
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         15410         1         2019-03-27         DCAE           EXE         01:18:41         18:27:55         01:18:57         18:27:45         18:27:45	B8D
EXE         01:18:41         18:27:55         01:18:57         18:27:45           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         41974         2         2019-03-27         2019-03-27         DCAE	B8D
<b>EXE</b> 01:18:41 18:24:52 01:18:57 18:24:41 15:43:23	
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         22560         3         2019-03-27         2019-03-25         DCAE           EXE         01:18:41         11:48:47         01:18:57         11:48:37         16:46:05	B8D
SVCHOST. 2022-11-30 2019-03-26 2022-11-30 24930 1 2019-03-26 DCAE	B8D
EXE 01:18:41 16:01:27 01:18:57 16:01:17	DOD.
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         70918         5         2019-03-27         2019-03-25         DCAE           EXE         01:18:41         11:46:59         01:18:57         11:46:48         13:05:46	'R&D
<b>SVCHOST.</b> 2022-11-30 2019-03-27 2022-11-30 48464 13 2019-03-27 2019-03-26 DCAE	
EXE         01:18:41         12:11:26         01:18:57         12:11:16         11:50:25           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         31820         1         2019-03-27         DCAE	B8D
SVCHOST.         2022-11-30         2019-03-27         2022-11-30         31820         1         2019-03-27         DCAE           EXE         01:18:41         12:12:15         01:18:57         12:12:05         12:12:05	
<b>SVCHOST.</b> 2022-11-30 2019-03-27 2022-11-30 34902 2 2019-03-27 2019-03-26 DCAE	CB8D
EXE         01:18:41         11:47:37         01:18:58         11:47:27         12:40:09           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         22900         2         2019-03-27         2019-03-26         DCAE	CB8D
EXE 01:18:41 11:44:05 01:18:58 22900 2 2019-03-27 2019-03-26 DCAE	CB8D CB8D
SVCHOST. 2022-11-30 2019-03-27 2022-11-30 38516 5 2019-03-27 2019-03-25 DCAE	CB8D
EXE         01:18:41         11:46:56         01:18:58         11:46:45         13:09:01           SVCHOST.         2022-11-30         2019-03-27         2022-11-30         53424         3         2019-03-27         2019-03-25         DCAE0	CB8D CB8D CB8D
EXE 01:18:41 11:47:00 01:18:58 11:46:50 16:46:07	CB8D CB8D CB8D CB8D

CVCUCCT	2022-11-30	2019-03-27	2022-11-30	20226	3	2019-03-27	2019-03-26	DCAECDOD
SVCHOST. EXE	01:18:41	11:47:49	01:18:58	20236	3	11:47:39	10:46:29	DCAECB8D
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	20444	1	2019-03-27	10.40.23	DCAECB8D
EXE	01:18:41	13:45:59	01:18:58	20111	,	13:45:49		BOMEOBOB
SVCHOST.	2022-11-30	2019-03-26	2022-11-30	12012	2	2019-03-26	2019-03-26	DCAECB8D
EXE	01:18:41	17:36:42	01:18:58			17:36:31	15:41:07	
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	21758	2	2019-03-27	2019-03-26	DCAECB8D
EXE	01:18:41	11:44:04	01:18:58			11:43:54	10:47:05	
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	49578	1	2019-03-27		DCAECB8D
EXE	01:18:41	12:12:14	01:18:58	0.101.1	-	12:12:04		DOAFOROD
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.	2022-11-30	2019-03-27	2022-11-30	18612	48	2019-03-27	2019-03-26	DCAECB8D
EXE	01:18:41	11:55:49	01:18:58	.00.2		11:55:39	17:01:52	20/120202
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	42994	2	2019-03-27	2019-03-26	DCAECB8D
EXE	01:18:41	11:48:46	01:18:58			11:48:39	12:36:06	
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	32450	11	2019-03-27	2019-03-26	DCAECB8D
EXE	01:18:41	11:54:46	01:18:58	00.100	4	11:54:36	15:18:39	DOAFOROR
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.	2022-11-30	2019-03-27	2022-11-30	20026	27	2019-03-27	2019-03-26	DCAECB8D
EXE	01:18:41	18:47:43	01:18:58	20020	_,	18:47:33	18:05:33	3020202
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	32442	2	2019-03-27	2019-03-27	DCAECB8D
EXE	01:18:41	12:44:34	01:18:58			12:44:29	12:41:04	
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	71000	4	2019-03-27	2019-03-25	DCAECB8D
EXE	01:18:41	11:47:49	01:18:58	4.4070	4	11:47:39	13:04:49	DOAFORAD
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.	2022-11-30	2019-03-27	2022-11-30	21280	2	2019-03-27	2019-03-27	DCAECB8D
EXE	01:18:41	18:24:59	01:18:58	2.200	_	18:24:49	12:18:07	201120202
SVCHOST.	2022-11-30	2019-03-27	2022-11-30	29120	5	2019-03-27	2019-03-25	42B2CA5
EXE	01:18:41	11:47:52	01:18:58			11:47:42	13:04:52	
	01.10.11	11.77.02	01.10.00			11.77.72	10.01.02	
SYSTEMSE	2022-11-30	2019-03-27	2022-11-30	225044	10	2019-03-27	2019-03-25	DCAECB8D
TTINGS.EX				225044	10			DCAECB8D
TTINGS.EX E	2022-11-30 01:18:41	2019-03-27 12:12:12	2022-11-30 01:18:58			2019-03-27 12:12:02	2019-03-25	
TTINGS.EX E SYSTEMSE	2022-11-30	2019-03-27	2022-11-30	225044 54890	10	2019-03-27	2019-03-25	DCAECB8D
TTINGS.EX E	2022-11-30 01:18:41 2022-11-30	2019-03-27 12:12:12 2019-03-27	2022-11-30 01:18:58 2022-11-30			2019-03-27 12:12:02 2019-03-27	2019-03-25	
TTINGS.EX E SYSTEMSE TTINGSBR	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30			2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27	2019-03-25 13:16:42 2019-03-27	
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588	1 46	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37	2019-03-25 13:16:42	DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR.	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30	54890	1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27	2019-03-25 13:16:42 2019-03-27	DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426	1 46 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40	2019-03-25 13:16:42 2019-03-27 11:50:49	DCAECB8D DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30	54890 68588	1 46	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26	DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426	1 46 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40	2019-03-25 13:16:42 2019-03-27 11:50:49	DCAECB8D DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426 198680	1 46 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35	DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426 198680 18198	1 46 1 11 15	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 13:45:49	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426 198680	1 46 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 13:45:49	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426 198680 18198	1 46 1 11 15	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 13:45:49	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59 2019-03-27 13:49:30	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426 198680 18198	1 46 1 11 15	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 13:45:49 2019-03-27 13:45:49	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426 198680 18198	1 46 1 11 15	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 13:45:49	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL.	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59 2019-03-27 13:45:59	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58	54890 68588 130426 198680 18198	1 46 1 11 15	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 13:45:49 2019-03-27 11:49:20	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:16	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59	54890 68588 130426 198680 18198 53020	1 46 1 1 15 1 1 1 1 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WINSAT.E	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:16 2019-03-26 15:49:15 2019-03-27	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890 68588 130426 198680 18198 53020	1 46 1 11 15 1 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WINSAT.E XE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:16 2019-03-26 15:49:15 2019-03-27 12:11:22	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890  68588  130426  198680  18198  53020  13920  17072  24064	1 46 1 11 15 1 1 1 1 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27 12:11:14	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WINSAT.E XE WINSTORE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:16 2019-03-26 15:49:15 2019-03-27 12:11:22 2019-03-27	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890 68588 130426 198680 18198 53020 13920 17072	1 46 1 1 15 1 1 1 1 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27 12:11:14	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WEVTUTIL. EXE WINSAT.E XE WINSAT.E XE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:16 2019-03-26 15:49:15 2019-03-27 12:11:22 2019-03-27 12:11:47	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890  68588  130426  198680  18198  53020  17072  24064  117166	1 46 1 11 15 1 1 1 1 1 1 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27 12:11:14	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26 12:36:35	DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WINSAT.E XE WINSTORE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:16 2019-03-26 15:49:15 2019-03-27 12:11:22 2019-03-27	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890  68588  130426  198680  18198  53020  13920  17072  24064	1 46 1 11 15 1 1 1 1 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27 12:11:14	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26	DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D  DCAECB8D
SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WINSAT.E XE WINSTORE .APP.EXE WINWORD.	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:16 2019-03-26 15:49:15 2019-03-27 12:11:22 2019-03-27 12:11:47	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890  68588  130426  198680  18198  53020  17072  24064  117166	1 46 1 11 15 1 1 1 1 1 1 1	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27 12:11:14	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26 12:36:35	DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WINSAT.E XE WINSAT.E XE WINSTORE .APP.EXE WINWORD. EXE WMIADAP. EXE	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:15 2019-03-26 15:49:15 2019-03-27 12:11:22 2019-03-27 12:11:22 2019-03-27 12:11:47	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890  68588  130426  198680  18198  53020  17072  24064  117166  201894  16956	1 46 1 11 15 1 1 1 1 5 2	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27 12:11:14 2019-03-27 12:11:37 2019-03-26 16:52:00 2019-03-27 11:49:39	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26 12:36:35	DCAECB8D  DCAECB8D
TTINGS.EX E SYSTEMSE TTINGSBR OKER.EXE TASKHOST W.EXE TASKMGR. EXE TIWORKER .EXE TRUSTEDI NSTALLER .EXE UPDATEPL ATFORM.E XE WEVTUTIL. EXE WINSAT.E XE WINSAT.E XE WINSTORE .APP.EXE WINWORD. EXE WMIADAP.	2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41 2022-11-30 01:18:41	2019-03-27 12:12:12 2019-03-27 18:25:34 2019-03-27 17:48:47 2019-03-27 11:47:50 2019-03-27 13:45:59 2019-03-27 13:45:59 2019-03-27 11:49:30 2019-03-26 15:49:15 2019-03-27 12:11:22 2019-03-27 12:11:47 2019-03-26 16:52:06 2019-03-27	2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:58 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59 2022-11-30 01:18:59	54890 68588 130426 198680 18198 53020 17072 24064 117166 201894	1 46 1 11 15 1 1 1 1 5	2019-03-27 12:12:02 2019-03-27 18:25:24 2019-03-27 17:48:37 2019-03-27 11:47:40 2019-03-27 13:45:49 2019-03-27 11:49:20 2019-03-26 15:49:14 2019-03-26 15:49:14 2019-03-27 12:11:14 2019-03-27 12:11:37 2019-03-26 16:52:00 2019-03-27	2019-03-25 13:16:42 2019-03-27 11:50:49 2019-03-26 12:36:35 2019-03-26 12:36:35	DCAECB8D

WUAUCLT.	2022-11-30	2019-03-27	2022-11-30	130900	12	2019-03-27	2019-03-25	DCAECB8D
EXE	01:18:41	11:49:29	01:18:59			11:49:19	16:48:57	

## **APPENDIX V: Shellbag Analysis**

Absolute	Shell	Value	First	Last
Path	Туре		Interacted	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\Jus tine B	Directory	Justine B		2019-03-25 13:11:37
Desktop\C:\\Users\Jus tine B\AppData	Directory	AppData		2019-03-25 13:11:39
Desktop\C:\\Users\Jus tine B\AppData\Roaming	Directory	Roaming		2019-03-25 13:11:40
Desktop\C:\\Users\Jus tine B\AppData\Roaming\ Microsoft	Directory	Microsoft		2019-03-25 13:11:42
Desktop\C:\\Users\Jus tine B\AppData\Roaming\ Microsoft\New folder	Directory	New folder	2019-03-25 13:11:50	
Desktop\C:\\Users\Jus tine B\AppData\Roaming\ Microsoft\Protect	Directory	Protect	2019-03-25 13:11:54	
Desktop\C:\\Users\Jus tine B\AppData\Roaming\ Microsoft\Skype	Directory	Skype		2019-03-25 13:11:55
Desktop\C:\\Users\Jus tine B\AppData\Roaming\ Microsoft\Skype\live#3 astevedallas1010	Directory	live#3astevedallas1010	2019-03-25 13:13:25	2019-03-25 13:13:25
Desktop\D:\\GoodOne s	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\Ju stine B	Directory	Justine B		2019-03-26 15:32:12
Desktop\My Computer\C:\Users\Ju stine B\Downloads	Directory	Downloads	2019-03-26 15:32:12	2019-03-26 15:32:12
Desktop\My Computer\Desktop\Go odOnes	Directory	GoodOnes	2019-03-26 15:47:01	2019-03-26 15:47:01
Desktop\My Computer\F:\MagnetP rocessCapture- 20190326-140822	Directory	MagnetProcessCapture- 20190326-140822	2019-03-26 18:08:28	2019-03-26 18:08:28

## **APPENDIX VI: Link Analysis**

Local	Source	Source	Source	Target	Target	Target	File	Drive	Volume	Machine
Path	Created	Modified	Accessed	Created	Modified	Accessed	Size	Туре	Serial	ID
C:\Users\Ju stine B\Desktop\ GoodOnes\r esized 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\Ju stine B\Download s\Owls and Their Homes.doc x	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\Ju stine B\Download s\pFRtHLhL 4eOA4de3y oIRiZt1DON VY3milQtn8 qVU0FI.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\Ju stine 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:\d26ac133 21f158c9e5 e2fa459a69 74ba.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\Ju stine B\Documen ts\owlColor s.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\Ju stine B\Desktop\ DWB2x2LVo AAtkWf.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:\owlColor s_backup.xl sx	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\Ju stine B\AppData\ Roaming\Mi	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

crosoft\Sky										
pe C:\Users\Ju stine B\Desktop\ GoodOnes\ 913ada7114 31fb8f3d54c 68c72eb0d9	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
c.jpg F:\nicepic.jp g	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_j53 rBCrjb8J_12 00x900.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\Ju stine B\Pictures\ 52c01a6b56 5fe.image.jp	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\Ju stine B\Desktop\ GoodOnes\ grumpy- owl_c_2512 435.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:\frogmout h.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\Ju stine B\Desktop\ Barn-Owl- Cocked- Head.jpg.69 6x0_q80_cr op-	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	
smart.jpg C:\Users\Ju stine B\Desktop\ GoodOnes\ hqdefault.jp g	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\Ju stine B\Download s\stellaAnd Sherlock.jp	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\Ju stine B\Documen ts\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\Ju stine 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_A m_I_Owls_B ro.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\Ju stine B\Download s\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\Ju stine B\Download s\ARDB_sp ecies_name s_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\Ju stine B\Documen ts\Owl Musings.do cx	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\Ju stine	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	DCAECB8D	desktop- n566fm9

## 2022\_CaseStudy\_04

B\AppData\ Roaming\Mi crosoft								media (Hard drive)		
C:\Users\Ju stine B\Download s\814u1IDE xtLSL1343 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.j pg	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_11 2467978790 101_518773 7_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\Ju stine B\Download s	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\Downlo ads\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)	DCAECB8 D	
C:\Users\ Justine B\Downlo ads\Whoo o_Am_I_O wls_Bro.p df	2019-03- 26 14:49:06	2019-03- 26 15:32:09	2022-11- 30 01:18:16				0	Fixed storage media (Hard drive)	DCAECB8 D	
C:\Users\ Justine B\Downlo ads\814u1 IDExtL_S L1343jp	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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Deskto p\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)	DCAECB8 D	
C:\Users\ Justine B\Deskto p\DWB2x 2LVoAAtk Wf.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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Downlo ads\stella AndSherlo ck.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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Downlo	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	DCAECB8 D	desktop- n566fm9

ads\stella.								(Hard		
jpg								drive)		
C:\Users\ Justine B\Downlo ads\pFRt HLhL4eO A4de3yol RiZt1DON VY3milQt n8qVU0FI. 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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Docum ents\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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Picture s\52c01a6 b565fe.im age.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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Docum ents\Owl Musings.d ocx	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)	DCAECB8 D	desktop- n566fm9
D:\GoodO nes\resize d 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:\owlCol ors_backu p.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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
C:\Users\ Justine B\Docum ents\owlC olors.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)	DCAECB8 D	
F:\Whooo _Am_I_Ow Is_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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
C:\Users\ Justine B\Downlo ads\Owls and Their Homes.do cx	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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Downlo ads\ARDB _species_ names_nu mbers_si mple.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)	DCAECB8 D	desktop- n566fm9
D:\GoodO nes\grum py- owl_c_251 2435.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:\GoodO nes\913ad a711431fb 8f3d54c68 c72eb0d9 c.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:\GoodO nes\hqdef ault.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:\cuteow I.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	Removabl e 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	Removabl e storage media (Floppy, USB)	20F3BCE6	
F:\frogmo uth.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	Removabl e storage media (Floppy, USB)	20F3BCE6	
F:\30588_ 11246797 8790101_5 187737_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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
F:\00y0y_j 53rBCrjb8 J_1200x90 0.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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
F:\814u1I DExtLSL 1343jpg	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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
F:\d26ac1 3321f158c 9e5e2fa45 9a6974ba. 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	Removabl e storage media (Floppy, USB)	20F3BCE6	
F:\owlCol ors_backu p.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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
C:\Users\ Justine B\Docum ents\owlC olors.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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Downlo ads\ARDB _species_ names_nu mbers_si mple.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)	DCAECB8 D	desktop- n566fm9
F:\Whooo _Am_I_Ow ls_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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
C:\Users\ Justine B\Downlo ads\Great	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)	DCAECB8 D	desktop- n566fm9

Horned										
Owl.pdf C:\Users\ Justine B\Downlo	2019-03-	2019-03-	2022-11-	2019-03-	2019-03-	2019-03-		Fixed storage		
ads\Whoo o_Am_I_O wls_Bro.p	25 13:07:03	26 16:09:39	30 01:18:16	26 15:31:37	26 15:31:38	26 15:31:33	3260666	media (Hard drive)	DCAECB8 D	desktop- n566fm9
ui	2019-03- 25 13:07:03	2019-03- 26 16:09:39	2022-11- 30 01:18:16				0	(None)		
C:\Users\ Justine B\Downlo ads\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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Downlo ads\pFRt HLhL4e0 A4de3yol RiZt1DON VY3milQt n8qVU0FI. 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)	DCAECB8 D	desktop- n566fm9
F:\cuteow I.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	Removabl e 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	Removabl e storage media (Floppy, USB)	20F3BCE6	
F:\frogmo uth.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	Removabl e storage media (Floppy, USB)	20F3BCE6	
F:\30588_ 11246797 8790101_5 187737_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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
F:\00y0y_j 53rBCrjb8 J_1200x90 0.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	Removabl e storage media (Floppy, USB)	FC9BD2D 2	
F:\d26ac1 3321f158c 9e5e2fa45 9a6974ba. 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	Removabl e storage media (Floppy, USB)	20F3BCE6	
C:\Users\ Justine B\Docum ents\Owl Musings.d ocx	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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Downlo ads\Owls and Their Homes.do cx	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)	DCAECB8 D	desktop- n566fm9
C:\Users\ Justine B\Downlo ads	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)	DCAECB8 D	desktop- n566fm9

C:\Users\								Fixed		
Justine	2019-03-	2019-03-	2022-11-	2019-03-	2019-03-	2019-03-	4000	storage	DCAECB8	desktop-
B\Deskto	25 13:06:46	27 18:32:16	30 01:18:16	25 13:05:45	27 12:06:06	27 12:06:06	4096	media (Hard	D	n566fm9
р								drive)		
C:\Users\	2019-03-	2019-03-	2022-11-	2019-03-	2019-03-	2019-03-		Fixed storage		
Justine B\Decum	25	27	30	25	26	26	4096	media	DCAECB8 D	desktop- n566fm9
B\Docum ents	13:06:46	18:32:16	01:18:16	13:05:45	17:14:08	17:14:08		(Hard	D	1130011119
								drive) Fixed		
C:\Users\ Justine	2019-03-	2019-03-	2022-11-	2019-03-	2019-03-	2019-03-		storage	DCAECB8	desktop-
B\Picture	25	27 18:32:16	30	25	26 17:13:21	26	4096	media	DOALOBO	n566fm9
s	13:06:46	16.32.10	01:18:16	13:05:45	17.13.21	17:13:21		(Hard drive)		
C:\Users\								Fixed		
Justine B\Deskto	2019-03- 25	2019-03- 27	2022-11- 30	2019-03- 26	2019-03- 26	2019-03- 26	4096	storage media	DCAECB8	desktop-
p\GoodOn	13:06:46	18:32:16	01:18:16	15:46:21	16:51:14	16:51:14	4090	(Hard	D	n566fm9
es								drive)		
C:\Users\	2019-03-	2019-03-	2022-11-	2019-03-	2019-03-	2019-03-		Fixed storage		
Justine	25	27	30	25	25	25	0	media	DCAECB8 D	desktop- n566fm9
B\Videos	13:06:46	18:32:16	01:18:16	13:05:45	13:06:43	13:06:42		(Hard	5	1100011110
								drive) Fixed		
C:\Users\	2019-03-	2019-03-	2022-11-	2019-03-	2019-03-	2019-03-	_	storage	DCAECB8	desktop-
Justine B\Music	25 13:06:46	27 18:32:16	30 01:18:16	25 13:05:45	25 13:06:43	25 13:06:43	0	media (Hard	D	n566fm9
Diffusio	10.00.70	10.02.10	01.10.10	10.00.40	10.00.70	10.00.40		drive)		
5d696d52	2019-03-	2019-03-	2019-03-	17400	4	desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1de238c3	25 13:19:08	27 18:33:50	27 18:33:50	17429	1	n566fm9	1:13:5d	25 13:19:08	27 18:33:50	25 13:15:24
5d696d52	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1de238c3	25 13:19:08	27 18:33:50	27 18:33:50	17429	1	n566fm9	1:13:5d	25 13:19:08	27 18:33:50	25 13:15:24
ENCOCNEO	2019-03-	2019-03-	2019-03-			-11-4	70.560.0	2019-03-	2019-03-	2019-03-
5d696d52 1de238c3	25	27	27	17429	1	desktop- n566fm9	70:5a:b6:9 1:13:5d	25	27	25
	13:19:08 2019-03-	18:33:50 2019-03-	18:33:50 2019-03-					13:19:08 2019-03-	18:33:50 2019-03-	13:15:24 2019-03-
5d696d52 1de238c3	25	27	27	17429	1	desktop- n566fm9	70:5a:b6:9 1:13:5d	25	27	25
14020000	13:19:08 2019-03-	18:33:50 2019-03-	18:33:50 2019-03-			1100011110	1.10.00	13:19:08 2019-03-	18:33:50 2019-03-	13:15:24 2019-03-
5d696d52	25	2019-03-	2019-03-	17429	1	desktop-	70:5a:b6:9	25	2019-03-	25
1de238c3	13:19:08	18:33:50	18:33:50			n566fm9	1:13:5d	13:19:08	18:33:50	13:15:24
5d696d52	2019-03- 25	2019-03- 27	2019-03- 27	17429	1	desktop-	70:5a:b6:9	2019-03- 25	2019-03- 27	2019-03- 25
1de238c3	13:19:08	18:33:50	18:33:50	20		n566fm9	1:13:5d	13:19:08	18:33:50	13:15:24
5d696d52	2019-03-	2019-03-	2019-03-	17400	4	desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1de238c3	25 13:19:08	27 18:33:50	27 18:33:50	17429	1	n566fm9	1:13:5d	25 13:19:08	27 18:33:50	25 13:15:24
5d696d52	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1de238c3	25 13:19:08	27 18:33:50	27 18:33:50	17429	1	n566fm9	1:13:5d	25 13:19:08	27 18:33:50	25 13:15:24
5d696d52	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1de238c3	25 13:10:08	27 18:33:50	27 18:33:50	17429	1	n566fm9	1:13:5d	25 13:19:08	27 18:33:50	25 13:15:24
	13:19:08 2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	13:15:24 2019-03-
5d696d52 1de238c3	25	27	27	17429	1	desktop- n566fm9	70:5a:b6:9 1:13:5d	25	27	25
	13:19:08 2019-03-	18:33:50 2019-03-	18:33:50 2019-03-					13:19:08 2019-03-	18:33:50 2019-03-	13:15:24 2019-03-
5d696d52 1de238c3	25	27	27	17429	1	desktop- n566fm9	70:5a:b6:9 1:13:5d	25	27	25
10023003	13:19:08	18:33:50	18:33:50			1100011113	1.10.00	13:19:08	18:33:50 2019-03-	13:15:24
5d696d52	2019-03- 25	2019-03- 27	2019-03- 27	17429	1	desktop-	70:5a:b6:9	2019-03- 25	2019-03-	2019-03- 25
1de238c3	13:19:08	18:33:50	18:33:50			n566fm9	1:13:5d	13:19:08	18:33:50	13:15:24
5d696d52	2019-03- 25	2019-03- 27	2019-03- 27	17429	1	desktop-	70:5a:b6:9	2019-03- 25	2019-03- 27	2019-03- 25
1de238c3	13:19:08	18:33:50	18:33:50	., , ,		n566fm9	1:13:5d	13:19:08	18:33:50	13:15:24
5d696d52	2019-03-	2019-03-	2019-03-	17/100	4	desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1de238c3	25 13:19:08	27 18:33:50	27 18:33:50	17429	1	n566fm9	1:13:5d	25 13:19:08	27 18:33:50	25 13:15:24
5d696d52	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1de238c3	25 13:19:08	27 18:33:50	27 18:33:50	17429	1	n566fm9	1:13:5d	25 13:19:08	27 18:33:50	25 13:15:24
E4COC-IEO	2019-03-	2019-03-	2019-03-			do-1-t-	70,5-,600	2019-03-	2019-03-	2019-03-
5d696d52 1de238c3	25	27	27	17429	1	desktop- n566fm9	70:5a:b6:9 1:13:5d	25	27	25
1402000	13:19:08	18:33:50	18:33:50					13:19:08	18:33:50	13:15:24

\$\begin{align*} \begin{align*} \be	2019-03-	0010 00
2678tbd   77.20.30   77.34.30	2019-03-	2019-03-
173-190	26	25
Company   Comp	17:34:30	13:20:27
2678fbd   20   20   20   20   20   20   20   2	2019-03-	2019-03-
17:2030	26	25
\$\begin{array}{c c c c c c c c c c c c c c c c c c c	17:34:30	13:20:27
Dec	2019-03-	2019-03-
17:20:30   17:34:30	26	25
68244490   2019-03   201	17:34:30	13:20:27
Control   Cont	2019-03-	2019-03-
2678bbd   17:20:30   17:34:30		
68244490   2019-03   201	26	25
Content   Cont	17:34:30	13:20:27
2c 78thd         2b         2b         1500b         2         n566fm9         1:13:5d         2b         2019-03-26-26         2019-03-26-26-26-26         2019-03-26-26-26-26-26-26-26-26-26-26-26-26-26-	2019-03-	2019-03-
17:20:30   17:34:30   17:34:30   2019-03-26   26   26   26   26   26   26   26	26	25
\$68244490   \$26	17:34:30	13:20:27
2678tbd 17:20:30 17:34:30 10:006 2 n566fm9 1:13:5d 17:20:30 17:20:30 20:19:03-20:19:	2019-03-	2019-03-
6824f4a90 2c78fbd         2019-03- 26	26	25
\$8244490   \$26   \$26   \$26   \$26   \$16006   \$2   \$088tfop   \$70.5a:b6:9   \$26   \$17.20:30   \$2019-03   \$2019	17:34:30	13:20:27
2678thd	2019-03-	2019-03-
17:20:30   2019-03   201	26	25
682414390         26         26         26         26         16006         2         desktop-n566fm9 n566fm9 n5	17:34:30	13:20:27
2c78fbd         26 17:20:30 2019-03- 26 26 26 26 26 27 26 28 26 29 2019-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03-2219-03	2019-03-	2019-03-
17:20:30   17:34:30   17:34:30   17:34:30   17:20:30   17:20:30   17:20:30   17:34:30	26	25
6824f4a90         2019-03- 26	17:34:30	13:20:27
682414a90 2c78/bd         26 26 26 26 26 26 26 26 26 26 26 26 26 2	2019-03-	2019-03-
17:20:30   17:34:30   17:34:30   17:34:30   17:34:30   17:20:30   17:20:30   17:34:30	26	25
6824f4a90 2c78fbd         2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	17:34:30	13:20:27
682414a90 2c78fbd         26 17:20:30         26 17:20:30         26 2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	2019-03-	2019-03-
17:20:30   17:34:30	26	25
6824f4a90 2c78fbd         2019-03- 26 2c8	17:34:30	13:20:27
6824f4a90 2c78fbd         26 17:20:30         26 17:34:30         26 17:34:30         26 17:34:30         26 17:34:30         26 17:20:30         26 17:20:30         26 2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	2019-03-	2019-03-
17:20:30   17:20:30   17:34:30   17:34:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:30:30   17:20:30   17:30:30	26	25
6824f4a90 2c78fbd         2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	17:34:30	13:20:27
6824f4a90 2c78fbd         26 26         26 26 20 15/33/30         17:34:30 17:34:30         16006         2 n566fm9         desktop-n566fm9         70:5a:b6:9 17:20:30         26 17:20:30         26 17:20:30         26 17:20:30         2019-03-2019-03-2019-03-26         26 26 26 26 26         26 26 26 26         26 26 26 26         26 26 26 26         26 26 26 26         26 26 26 26         26 26 26 26         26 26 26 26         2019-03-26 26<	2019-03-	2019-03-
26/3fbd 17:20:30 17:34:30 17:34:30 17:34:30 17:20:30 17:20:30 17:20:30 2019-03- 26 26 26 26 16006 2 desktop- n566fm9 1:13:5d 17:20:30 26 26 26 26 16006 2 desktop- n566fm9 1:13:5d 17:20:30 26 26 26 26 16006 2 desktop- n566fm9 1:13:5d 17:20:30 26 26 26 26 16006 2 desktop- n566fm9 1:13:5d 17:20:30 26 26 26 26 16006 2 desktop- n566fm9 1:13:5d 17:20:30 26 26 26 26 26 26 26 26 26 26 26 26 26		
6824f4a90 2c78fbd         2019-03- 26 26 26 26 26 16006         2 desktop- n566fm9         70:5a:b6:9 1:13:5d         2019-03- 26 26 1:13:5d           6824f4a90 2c78fbd         2019-03- 26 26 26 26 26 26 26 16006         2 desktop- n566fm9         70:5a:b6:9 1:13:5d         2019-03- 26 2019-03- 26 26 26 16006           2c78fbd         2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	26	25
682414a90 2c78fbd         26 17:20:30         26 17:34:30         26 17:34:30         26 17:34:30         26 17:34:30         26 17:20:30         26 17:20:30         26 17:20:30         26 26 26 26 26 26 26 26 26 26 26 26 26 2	17:34:30	13:20:27
2c78fbd         26         26         26         16006         2         n566fm9         1:13:5d         17:20:30         17:20:30         17:20:30         1:13:5d         12:03:30         12:03:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         16006         2         desktop-n566fm9         70:5a:b6:9         2019-03-26         17:20:30         2019-03-26         26         26         26         17:20:30         2019-03-26         26         26         16006         2         desktop-n566fm9         70:5a:b6:9         2019-03-26         26         26         26         17:20:30         2019-03-26         26         26         26         16006         2         desktop-n	2019-03-	2019-03-
17:20:30   17:34:30   17:34:30   17:34:30   2019-03- 20	26	25
6824f4a90 2c78fbd         26 17:20:30 17:34:30 17:34:30         16006         2 desktop-n566fm9         70:5a:b6:9 1:13:5d         26 17:20:30         26 17:20:30         26 26 26 26 26 26 26 26 26 26 26 26 26 2	17:34:30	13:20:27
2c78fbd         17:20:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         17:34:30         16006         2         desktop-n566fm9         70:5a:b6:9 1:13:5d         2019-03-26 17:20:30         2019-03-26 26 26 26 16006         2         desktop-n566fm9         70:5a:b6:9 1:13:5d         2019-03-26 26 17:20:30         26         2	2019-03-	2019-03-
6824f4a90 2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	26	25
2c78fbd   26	17:34:30	13:20:27
2c78fbd         26 17:20:30         26 17:34:30         26 17:34:30         26 26 26 26 26 26 26 26 26 26 26 26 26 2	2019-03-	2019-03-
6824f4a90 2c78fbd         2019-03- 26 26 26 16006         2 desktop- n566fm9         70:5a:b6:9 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 26 26 26 16:00         2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	26	25
682414a90 2c78fbd         26 26 26 26 26 26 26 26 26 26 26 26 26 2	17:34:30	13:20:27
2c78fbd         26 17:20:30         26 17:34:30         26 17:34:30         26 2019-03- 26 26 26 26 26 26 26 26 26 278fbd         26 26 26 26 26 26 26 26 26 26 278fbd         2019-03- 26 26 26 26 26 26 278fbd         2019-03- 26 26 26 26 26 26 26 26 26 26 26 26 26	2019-03-	2019-03-
6824f4a90 2c78fbd         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 17:34:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 16:006         2019-03- 26:006:009         2019-03- 26:009-	26	25
682414a90 2c78fbd         26 17:20:30         26 17:34:30         16006         2 16006         2 1:13:5d         70:5a:b6:9 1:13:5d         26 17:20:30	17:34:30	13:20:27
2c78fbd         26 17:20:30         26 17:34:30         26 17:34:30         26 26 26 26 26 26 26 26 26 26 26 26 26 2	2019-03-	2019-03-
6824f4a90 2c78fbd         2019-03- 26 26 26 26 26 16006         2 desktop- n566fm9         70:5a:b6:9 26 17:20:30         2019-03- 26 26 17:20:30           6824f4a90 2c78fbd         2019-03- 26 26 26 26 26 26 17:20:30         26 26 26 26 26 26 26 26 26 26 26 26 26 2	26	25
682414a90 2c78fbd         26 17:20:30         26 17:34:30         16006         2 desktop-n566fm9         70:5a:b6:9 1:13:5d         26 17:20:30           6824f4a90 2c78fbd         2019-03- 26 26 26 17:20:30         26 26 26 17:34:30         16006         2 desktop-n566fm9         70:5a:b6:9 1:13:5d         2019-03-26 2019-03-26 1:13:5d           6824f4a90 2c78fbd         2019-03- 26 26 26 26 26 16006         2 desktop-n566fm9         70:5a:b6:9 1:13:5d         2019-03-26 1:120:30           9d1f905ce 5044aee         2019-03- 25 26 26 26 26 0         26 26 26 26 0         2019-03-25 25 26 26 26 0         2019-03-25 25 26 26 26 0         2019-03-25 25 26 26 26 0           9d1f905ce 5044aee         2019-03- 25 26 26 26 26 0         26 26 26 0         2019-03-25 25 26 26 26 0         2019-03-25 25 26 26 26 0         2019-03-25 25 26 26 26 0	17:34:30	13:20:27
2c78fbd         26 17:20:30         26 17:34:30         26 17:34:30         26 26 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 26 26 26 26 17:20:30         2019-03- 26 26 26 26 17:20:30         2019-03- 26 26 26 17:20:30         2019-03- 26 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 26 26 17:20:30         2019-03- 25 26 26 26 26 26         2019-03- 25 26 26 26 26 26         2019-03- 25 26 26 26 26         2019-03- 25 26 26 26 26         2019-03- 25 26         2019-03- 25 26         2019-03- 25 26         2019-03- 25 26         2019-03- 25 26         2019-03- 25	2019-03-	2019-03-
17:20:30	26	25
682414a90 2c78fbd         26 17:20:30         26 17:34:30         16006         2 n566fm9         70:5a:b6:9 n566fm9         26 17:20:30         26 17:20:30         26 17:20:30         26 17:20:30         2019-03-26 26 26 26 17:20:30         2019-03-26 26 17:20:30         26 17:20:30         2019-03-26 17:34:30         2019-03-26 17:20:30         2019-03-26 17:20:30         2019-03-25 26 26 26 26 17:15:19         2019-03-25 13:07:14         2019-03-25 2019-03-2019-03-2019-03-25 26 26 26 26         2019-03-25 26 26 26 26         2019-03-25 2019-03-25 26 26 26         2019-03-25 2019-03-25 26 26 26         2019-03-25 26 26 26         2019-03-25 26 26         2019-03-25 2019-03-25 26         2019-03-25 26 </th <th>17:34:30</th> <th>13:20:27</th>	17:34:30	13:20:27
682414a90 2c78fbd         26 17:20:30         26 17:34:30         16006         2 n566fm9         70:5a:b6:9 n566fm9         26 17:20:30         26 17:20:30         26 17:20:30         26 17:20:30         2019-03-26 26 26 26 17:20:30         2019-03-26 26 26 17:20:30         2019-03-26 17:34:30         16006         2 n566fm9         70:5a:b6:9 n566fm9         2019-03-26 17:20:30         2019-03-26 17:20:30         2019-03-26 17:20:30         2019-03-25 13:07:14         2019-03-25 13:07:14         2019-03-25 26 26         2019-03-25 26	2019-03-	2019-03-
17:20:30   17:34:30   17:34:30   17:34:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:20:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:34:30   17:20:30   17:34:30   17:20:30	26	25
6824f4a90 2c78fbd         2019-03- 26 17:20:30         2019-03- 26 17:34:30         2019-03- 26 17:34:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 2019-03- 26 17:20:30         2019-03- 26 17:20:30         2019-03- 2019-03- 2019-03- 2019-03- 2019-03- 2019-03- 25 26 26         2019-03- 2019-03- 2019-03- 2019-03- 2019-03- 25 26         2019-03- 25 26 26         2019-03- 25 26         2019-03- 25 25         2019-03- 25 26         2019-03- 25 25         2019-03- 25 26         2019-03- 25 25         2019-03- 25 26         2019-03- 25 25         2019-03- 25 25         2019-03- 25 25         2019-03- 25 26         2019-03- 25 25         2019-03- 25 26         2019-03- 25 25         2019-03- 25 26         2019-03- 25         2019-03-	17:34:30	13:20:27
682414a90 2c78fbd         26 17:20:30         26 17:34:30         16006         2 n566fm9         70:5a:5b:9 n566fm9         26 17:20:30           9d1f905ce 5044aee         2019-03- 25 13:07:14         2019-03- 2019-03- 2019-03- 2019-03- 25         0 2019-03- 2019-03- 2019-03- 2019-03- 25         26 26 26 26         0 2019-03- 2019-03- 2019-03- 2019-03- 25           9d1f905ce 5044aee         25 26 26 26 26         26 0         0 2019-03- 2019-03- 2019-03- 2019-03- 25         2019-03- 25	2019-03-	2019-03-
2678Tbd         17:20:30         17:34:30         17:34:30         17:20:30           9d1f905ce 5044aee         2019-03- 25         2019-03- 26         0         2019-03- 25         2019-03- 25           9d1f905ce 5044aee         2019-03- 25         2019-03- 26         2019-03- 26         2019-03- 26         2019-03- 25           9d1f905ce 5044aee         25         26         26         0         2019-03- 25         25	26	25
9d1f905ce 5044aee         2019-03- 25         2019-03- 26         2019-03- 26         2019-03- 25         2019-03- 25           9d1f905ce 9d1f905ce 25         2019-03- 26         2019-03- 26         2019-03- 26         2019-03- 26         2019-03- 26         2019-03- 25	17:34:30	13:20:27
9d1f905ce 25 26 26 0 25 13:07:14 17:15:19 17:15:19 2019-03- 2019-03- 25 26 26 0 25 25 26 26 0 25 25	2019-03-	
5044aee     13:07:14     17:15:19     13:07:14       9d1f905ce     2019-03- 25     2019-03- 26     2019-03- 26     2019-03- 25	26	
9d1f905ce 25 26 26 0 2019-03- 50443ce 25 26 26 0	17:15:19	
90119050e 25 26 26 0 25 25 25 26 26 0 25 25 26 26 0 25 25 26 26 0 25 25 26 26 26 26 26 26 26 26 26 26 26 26 26	2019-03-	
	26	
10.07.19 17.10.10 17.10.10	17:15:19	
2019-03- 2019-03- 2019-03- 2019-03-	2019-03-	
	2019-03-	
5044aee 25 26 26 0 25 5044aee 13:07:14 17:15:19 17:15:19 13:07:14	17:15:19	
	2019-03-	
9d1f905ce 2019-03- 2019-03- 2019-03- 2019-03-		
5044299 25 26 26 0	26	
13:07:14 17:15:19 17:15:19 13:07:14	17:15:19	
be71009ff 2019-03- 2019-03- 2019-03- desktop- 70:5a:b6:9 2019-03-	2019-03-	2019-03-
8hh022 27 27 27 25E40 2 n566fm9 1:13:5d 27	27	26
12:02:41   12:02:41	12:02:41	15:54:20

be71009ff	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
	27	27	27	25E40	2			27	27	26
8bb02a2	12:02:41	12:02:41	12:02:41			n566fm9	1:13:5d	12:02:41	12:02:41	15:54:20
	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	2019-03-
be71009ff	27	27	27	25E40	2	desktop-	70:5a:b6:9	27	27	26
8bb02a2	12:02:41	12:02:41	12:02:41	202.0	_	n566fm9	1:13:5d	12:02:41	12:02:41	15:54:20
	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	2019-03-
be71009ff	2019-03-	2019-03-	2019-03-	25E40	2	desktop-	70:5a:b6:9	2019-03-	2019-03-	26
8bb02a2	12:02:41	12:02:41	12:02:41	23040		n566fm9	1:13:5d	12:02:41	12:02:41	15:54:20
be71009ff	2019-03-	2019-03-	2019-03-	05540	_	desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
8bb02a2	27	27	27	25E40	2	n566fm9	1:13:5d	27	27	26
	12:02:41	12:02:41	12:02:41					12:02:41	12:02:41	15:54:20
be71009ff	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
8bb02a2	27	27	27	25E40	2	n566fm9	1:13:5d	27	27	26
ODDOZUZ	12:02:41	12:02:41	12:02:41			1100011110	1.10.00	12:02:41	12:02:41	15:54:20
be71009ff	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
8bb02a2	27	27	27	25E40	2	n566fm9	1:13:5d	27	27	26
ODDUZAZ	12:02:41	12:02:41	12:02:41			1130011113	1.15.50	12:02:41	12:02:41	15:54:20
be71009ff	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
	27	27	27	25E40	2			27	27	26
8bb02a2	12:02:41	12:02:41	12:02:41			n566fm9	1:13:5d	12:02:41	12:02:41	15:54:20
h - 740000	2019-03-	2019-03-	2019-03-			4-411	70.5. 50.0	2019-03-	2019-03-	2019-03-
be71009ff	27	27	27	25E40	2	desktop-	70:5a:b6:9	27	27	26
8bb02a2	12:02:41	12:02:41	12:02:41		_	n566fm9	1:13:5d	12:02:41	12:02:41	15:54:20
	2019-03-	2019-03-	2019-03-				70.5	2019-03-	2019-03-	2019-03-
be71009ff	27	27	27	25E40	2	desktop-	70:5a:b6:9	27	27	26
8bb02a2	12:02:41	12:02:41	12:02:41	20210		n566fm9	1:13:5d	12:02:41	12:02:41	15:54:20
	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	2019-03-
ccc0fa1b9	25	27	27	17A17	3	desktop-	70:5a:b6:9	25	27	25
f86f7b3	13:23:18	12:13:48	12:13:48	177517	U	n566fm9	1:13:5d	13:23:18	12:13:48	13:23:02
	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	10.20.02
ccc0fa1b9	25	2019-03-	2019-03-					25	2019-03-	
f86f7b3	13:23:18	12:13:48	12:13:48					13:23:18	12:13:48	
			2019-03-					2019-03-		2019-03-
ccc0fa1b9	2019-03-	2019-03-		47447	_	desktop-	70:5a:b6:9		2019-03-	
f86f7b3	25	27	27	17A17	3	n566fm9	1:13:5d	25	27	25
	13:23:18	12:13:48	12:13:48					13:23:18	12:13:48	13:23:02
ccc0fa1b9	2019-03-	2019-03-	2019-03-		_	desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
f86f7b3	25	27	27	17A17	3	n566fm9	1:13:5d	25	27	25
	13:23:18	12:13:48	12:13:48				1110100	13:23:18	12:13:48	13:23:02
ccc0fa1b9	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
f86f7b3	25	27	27	17A17	3	n566fm9	1:13:5d	25	27	25
10017.00	13:23:18	12:13:48	12:13:48			1.000		13:23:18	12:13:48	13:23:02
ccc0fa1b9	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
f86f7b3	25	27	27	17A17	3	n566fm9	1:13:5d	25	27	25
1001750	13:23:18	12:13:48	12:13:48			1100011110	1.10.00	13:23:18	12:13:48	13:23:02
ccc0fa1b9	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
f86f7b3	25	27	27	17A17	3	n566fm9	1:13:5d	25	27	25
1001703	13:23:18	12:13:48	12:13:48			1150011113	1.15.50	13:23:18	12:13:48	13:23:02
ccc0fa1b9	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	
f86f7b3	25	27	27					25	27	
1001703	13:23:18	12:13:48	12:13:48					13:23:18	12:13:48	
anaOfa1hO	2019-03-	2019-03-	2019-03-			doolstop	70.5 a.b.c.0	2019-03-	2019-03-	2019-03-
ccc0fa1b9	25	27	27	17A17	3	desktop-	70:5a:b6:9	25	27	25
f86f7b3	13:23:18	12:13:48	12:13:48			n566fm9	1:13:5d	13:23:18	12:13:48	13:23:02
0(-4)-6	2019-03-	2019-03-	2019-03-			ala al III	70.5. 50.0	2019-03-	2019-03-	2019-03-
ccc0fa1b9	25	27	27	17A17	3	desktop-	70:5a:b6:9	25	27	25
f86f7b3	13:23:18	12:13:48	12:13:48			n566fm9	1:13:5d	13:23:18	12:13:48	13:23:02
	2019-03-	2019-03-	2019-03-				705	2019-03-	2019-03-	2019-03-
ccc0fa1b9	25	27	27	17A17	3	desktop-	70:5a:b6:9	25	27	25
f86f7b3	13:23:18	12:13:48	12:13:48			n566fm9	1:13:5d	13:23:18	12:13:48	13:23:02
	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	2019-03-
ccc0fa1b9	25	27	27	17A17	3	desktop-	70:5a:b6:9	25	27	25
f86f7b3	13:23:18	12:13:48	12:13:48	177317	J	n566fm9	1:13:5d	13:23:18	12:13:48	13:23:02
	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	2019-03-
ceb762e6	25	2019-03-	2019-03-	17DA2	5	desktop-	70:5a:b6:9	25	2019-03-	25
1b8637b9	15:29:12	11:47:02	11:47:02	HUMZ	5	n566fm9	1:13:5d	15:29:12	11:47:02	15:16:18
	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	2019-03-
ceb762e6				17040	5	desktop-	70:5a:b6:9			
1b8637b9	25 15:29:12	27	27 11:47:02	17DA2	5	n566fm9	1:13:5d	25 15:29:12	27	25 15:16:18
		11:47:02							11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-	17040	_	desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
	15:29:12	11:47:02	11:47:02				5.00	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
15000155	15:29:12	11:47:02	11:47:02				5.00	15:29:12	11:47:02	15:16:18

## 2022\_CaseStudy\_04

	2019-03-	2019-03-	2019-03-					2019-03-	2019-03-	2019-03-
ceb762e6	25	27	27	17DA2	5	desktop-	70:5a:b6:9	25	27	25
1b8637b9	15:29:12	11:47:02	11:47:02		ŭ	n566fm9	1:13:5d	15:29:12	11:47:02	15:16:18
. =	2019-03-	2019-03-	2019-03-				705 100	2019-03-	2019-03-	2019-03-
ceb762e6	25	27	27	17DA2	5	desktop-	70:5a:b6:9	25	27	25
1b8637b9	15:29:12	11:47:02	11:47:02			n566fm9	1:13:5d	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
1b8637b9	15:29:12	11:47:02	11:47:02			пооопп	1:13:50	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
10003709	15:29:12	11:47:02	11:47:02			Hoodins	1.13.50	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
10003709	15:29:12	11:47:02	11:47:02			1130011119	1.13.50	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
10003703	15:29:12	11:47:02	11:47:02			1100011110	1.10.00	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
10000103	15:29:12	11:47:02	11:47:02			1100011110	1.10.00	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
15000150	15:29:12	11:47:02	11:47:02			1100011110	1.10.00	15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
15000150	15:29:12	11:47:02	11:47:02			1100011110		15:29:12	11:47:02	15:16:18
ceb762e6	2019-03-	2019-03-	2019-03-			desktop-	70:5a:b6:9	2019-03-	2019-03-	2019-03-
1b8637b9	25	27	27	17DA2	5	n566fm9	1:13:5d	25	27	25
.2000.20	15:29:12	11:47:02	11:47:02			1100011110		15:29:12	11:47:02	15:16:18
	SourceCre	SourceMo	SourceAcc	TargetMFT	TargetMFT		MachineM	SourceCre	SourceMo	TargetAcc
Appld	ated	dified	essed	EntryNum	Sequence	MachineID	ACAddres	ated	dified	essed
				ber	Number		S	• •		
	SourceCre	SourceMo	SourceAcc	TargetMFT	TargetMFT	M	MachineM	SourceCre	SourceMo	TargetAcc
Appld	ated	dified	essed	EntryNum	Sequence	MachineID	ACAddres	ated	dified	essed
				ber	Number		S			

# **APPENDIX VIII: USB Analysis**

Serial/UID 🔺	Description	First Connected (UTC)	Last Connected (UTC)	Last Disconnected (UTC)	Volume Name/Label	Drive Letter(s)	VSN	Last User
001D0F0C73C8BA3153110118	Kingston DataTraveler 102 USB Device	3/25/2019 1:12:00 PM	3/25/2019 1:13:40 PM	3/25/2019 1:13:42 PM	F:\		1E2E0C0D	NTUSER
6&2017aed3	General UDisk USB Device	3/26/2019 12:40:21 PM	3/26/2019 12:40:56 PM	3/26/2019 12:40:58 PM	F:\		FC9BD2D2	NTUSER
6&32d15f78	General UDisk USB Device	3/26/2019 3:41:07 PM	3/26/2019 4:49:18 PM	3/26/2019 5:33:41 PM	F:\			NTUSER
b008be2f	GENERIC SD04G				CAMERACARD		20F3BCE6	NTUSER
NA7RL7PR	Seagate BUP Slim Mac SL SCSI Disk Device	3/26/2019 5:36:29 PM	3/26/2019 5:36:29 PM	3/26/2019 6:24:31 PM	Previews			

## **APPENDIX IX: Chain of Custody Report**



### Forensic Lab Northeastern University Chain of Custody Form

Date:	Case	Number (FAC):		Cas	se Type:					
12/04/2022	2022_0	CaseStudy_04		Ille	gal Owl Activity					
Description of Item	Description of Item(s):									
Property Number	Device Type	Make	Model		Serial Number					
2022_CaseStudy_04	Laptop	Windows	10 Pro 17134		DCAECB8D					
Power Cable/Brick	CD/DVD	Case/Peripherals	Dongle	s	Other					
N/A	N/A	N/A	N/A		N/A					
(Ext/Int)ernal Drives (Type)	Make	Model	Size		Serial Number					
External Media "F:"	Kingston	Data Traveler 102 USB Device	8 GB	(	001D0F0C73C8BA3153110118					
External Media "F:"	General UDisk	USB Device	32 GB		6&2017aed3					
External Media "F:"	General UDisk	USB Device	32 GB		6&32d15f78					
CAMERACARD	GENERIC	SD04G	4 GB		b008be2f					
Previews	Seagate	BUP Slim Mac SL SCSI Disk Device	500 GE	3	NA7RL7PR					
	-	n, scratches, blemishes.		itions	s to the hardware collected.					
Obtained from: (owner of item(s), location, phone number)  Digital Evidence Specialist, Jon Metzger – 322 Hayden Hall, 613-373-2200										
Released by: (printed name) Released by: (Signature) Date/Time Released:										
Jon Metzger	8	Von Metzger			03/28/2019 13:44:54 EST					
Released to: (printed	d name)	Released to: (Signature	Date/Time Stored:							
Dir. of Parks and Recreations, Muky Muse 03/28/2019 13:44:54 EST										
Temporary disposition of item (s): (where stored) In an access-restricted, GSA-approved secure container: GSA001 (Asset Tag or Storage Locker number)										