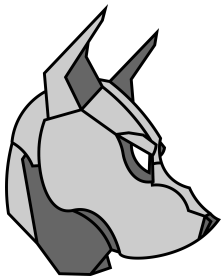
Cyber Defense Organization



P2P Illegal Download Investigation Lab - Collin Clark

Case Background

In this case, we are investigating a possible data leakage with regards to a uTorrent client found disseminating proprietary files over the internet. The company in question is called Beat Step, a company that produces sound effects for popular tv shows and movies. Two files were found to be distributed over the internet, one was copyrighted the other was intended to be kept confidential. Beat Step has hired you to find out who stole the files and how they stole the files in question. The title of the case indicates that this case is associated with a P2P transfer however, we must not assume that it started off this way. We have to assume the investigator did not know the suspect uses P2P to transfer data when starting the investigation. The investigator needs to find these details.

P2P Details

P2P is a type of Peer-to-Peer communication protocol.

P2P is used primarily for the distribution of digital media files.

In a peer-to-peer network, each computer acts as both a server and a client—supplying and receiving files—with bandwidth and processing distributed among all members of the network.

Pertinent Details

The following information regarding the case has been given:

- Information regarding files:
    - The file '*Contraband.mp3*' has a binary signature and is a copyrighted file. This file was planned to be included in the upcoming movie 'Fate With Money'.
    - The file '*Sample-1.mp3*' does not have a binary signature and is not a copyrighted file. However, the file was planned to be presented in a meeting. They want to know if the file was leaked by an employee
    - The MD5 and SHA1 hash of the .mp3 files were provided.
- Possible Suspects:
    - Kamryn Allen
    - Willis Gibbs
- Evidence:
    - Kamryn Alle's Personal Computer

Case Goals

- Prove or disprove that Kamryn downloaded the .mp3 files.
- If copyrighted material is found, prove or disprove that it originated from the company.
- Determine how Kamryn acquired the copyrighted material if any are found.
- Look for any instances where Kamryn downloaded/shared the file(s) with someone else.

- Determine if there are other suspects that may have the file.

Environment Setup

What I am Utilizing

For my personal environment, I utilized VirtualBox to run a Kali Linux Virtual Machine.

You can download VirtualBox here.

There are countless ways to virtualize Kali Linux, some options are VMWare or WSL.

Installation of Kali Linux

You can get ready to import OVA files for Kali Linux here.

An OVA is a preconfigured virtual machine that is very easy to install. If you need to control aspects of the installation such as disk space, it is recommended that you perform a regular install using an ISO file. This will grant you more control over several aspects of the installation process.

Other Options

ParrotOS - https://parrotsec.org/download/
Fedora Security - https://labs.fedoraproject.org/security/download/index.html
Backbox Linux - https://www.backbox.org/download/

Retrieving Case Materials

Case materials are hosted on dropbox.

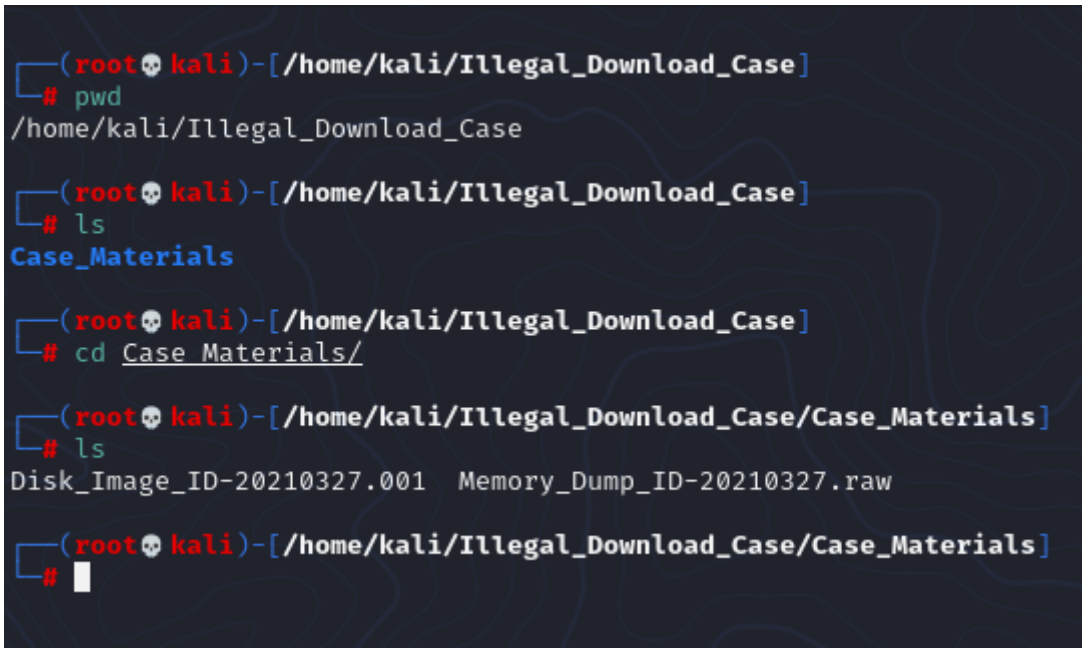
I successfully downloaded the case materials using *wget*.

I downloaded the disk image and the raw memory dump.

Disk Image - https://www.dropbox.com/s/1fop1ooadb2yshu/Disk_Image_ID-20210327.001

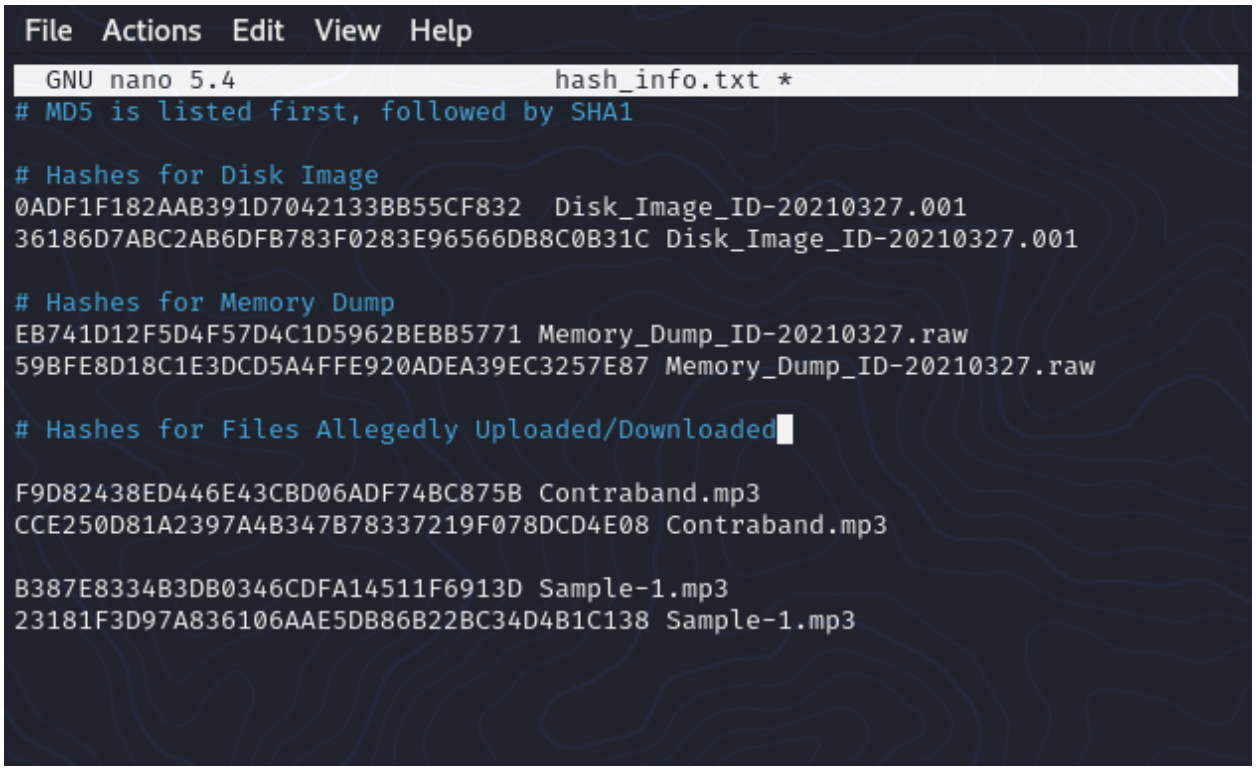
Memory Dump -
https://www.dropbox.com/s/0rxqi65v62njd6v/Memory_Dump_ID-20210327.raw

In the screenshot below, you can see the materials downloaded in a separate working directory made specifically for this case.



Recording Hash Information

Recording hashes of evidence are crucial, as it will help us later identify evidence files. This also ensures the forensic integrity of our examination can be verified.



Tools

- AnalyzeMFT
- Exiftool
- Git
- Hashdeep
- Liblnk-utils
- Mutt
- Python 2 & 3
- Regripper
- Sleuthkit
- SQLite3
- Torrent File Editor
- USN Journal Parser
- UN Record Carver
- Volatility
- Wine

Install Script

These labs and learning materials put together by Frank Xu of the University of Baltimore are quite comprehensive. Instead of manually installing each and every package, there is a script that has been created with every tool needed for the labs that are also maintained and updated as materials are added.

The script is here:

https://github.com/frankwxu/digital-forensics-lab/blob/main/P2P_Leakage/Scripts/p2p_lab_tool_install.bash

Alternatively, the option exists to install each necessary package separately if you so desire.

Forensic Examination

Verifying Integrity of Disk Image MD5 Hash

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case]
└─# md5deep Case_Materials/Disk_Image_ID-20210327.001 -bewM Case_Materials/hash_info.txt
md5deep: Case_Materials/hash_info.txt: No hash found in line 1
md5deep: Case_Materials/hash_info.txt: No hash found in line 2
md5deep: Case_Materials/hash_info.txt: No hash found in line 3
md5deep: Case_Materials/hash_info.txt: No hash found in line 5
md5deep: Case_Materials/hash_info.txt: No hash found in line 6
md5deep: Case_Materials/hash_info.txt: No hash found in line 7
md5deep: Case_Materials/hash_info.txt: No hash found in line 9
md5deep: Case_Materials/hash_info.txt: No hash found in line 10
md5deep: Case_Materials/hash_info.txt: No hash found in line 11
md5deep: Case_Materials/hash_info.txt: No hash found in line 12
md5deep: Case_Materials/hash_info.txt: No hash found in line 14
md5deep: Case_Materials/hash_info.txt: No hash found in line 15
md5deep: Case_Materials/hash_info.txt: No hash found in line 17
0adf1f182aab391d7042133bb55cf832  Disk_Image_ID-20210327.001 matched Disk_Image_ID-20210327.001
```

Verifying Integrity of Disk Image SHA1 Hash

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case]
└─# sha1deep Case_Materials/Disk_Image_ID-20210327.001 -bewM Case_Materials/hash_info.txt
sha1deep: Case_Materials/hash_info.txt: No hash found in line 1
sha1deep: Case_Materials/hash_info.txt: No hash found in line 2
sha1deep: Case_Materials/hash_info.txt: No hash found in line 3
sha1deep: Case_Materials/hash_info.txt: No hash found in line 4
sha1deep: Case_Materials/hash_info.txt: No hash found in line 6
sha1deep: Case_Materials/hash_info.txt: No hash found in line 7
sha1deep: Case_Materials/hash_info.txt: No hash found in line 8
sha1deep: Case_Materials/hash_info.txt: No hash found in line 10
sha1deep: Case_Materials/hash_info.txt: No hash found in line 11
sha1deep: Case_Materials/hash_info.txt: No hash found in line 12
sha1deep: Case_Materials/hash_info.txt: No hash found in line 13
sha1deep: Case_Materials/hash_info.txt: No hash found in line 15
sha1deep: Case_Materials/hash_info.txt: No hash found in line 16
36186d7abc2ab6dfb783f0283e96566db8c0b31c  Disk_Image_ID-20210327.001 matched Disk_Image_ID-20210327.001
```

Verification

The output from the commands returned that they matched; therefore, the disk image is validated as being the correct one provided for this lab.

Alternatives to MD5/SHA1Deep

There are other alternatives to md5deep and sha1deep however, md5deep and sha1 deep are the easiest methods. There are options that require more steps as well as far more complex commands. There are also GUI-based programs that will perform similar operations, most notably *GTKHash.*

Operating System Identification

Using fdisk to See Partition Table

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Case_Materials]
└─# fdisk -l Disk Image ID-20210327.001
Disk Disk_Image_ID-20210327.001: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x8afa8be3

Device                          Boot    Start      End  Sectors  Size Id Type
Disk_Image_ID-20210327.001p1 *          2048   104447   102400   50M  7 HPFS/NT
Disk_Image_ID-20210327.001p2          104448 61890501 61786054 29.5G  7 HPFS/NT
Disk_Image_ID-20210327.001p3        61890560 62910463  1019904  498M 27 Hidden
```

Using *fdisk*, we can see the information regarding the disk image's partitions. Here we can see that the disklabel type is dos.

Using fsstat to Get Partition Information

Partition 1

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Case_Materials]
└─# fsstat -o 2048 Disk Image ID-20210327.001
FILE SYSTEM INFORMATION
--------------------------------------------

File System Type: NTFS
Volume Serial Number: 18EC42BBEC4292C4
OEM Name: NTFS
Volume Name: System Reserved
Version: Windows XP
```

Partition 2

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Case_Materials]
└─# fsstat -o 104448 Disk Image ID-20210327.001
FILE SYSTEM INFORMATION
--------------------------------------------

File System Type: NTFS
Volume Serial Number: E8DE4350DE4315EA
OEM Name: NTFS
Version: Windows XP
```

Partition 3

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Case_Materials]
└─# fsstat -o 61890560 Disk Image ID-20210327.001
FILE SYSTEM INFORMATION
--------------------------------------------

File System Type: NTFS
Volume Serial Number: 9E46F86046F83A9B
OEM Name: NTFS
Version: Windows XP
```

Summary of the Information Found Using fdisk and fsstat

Partition Table			**MS-DOS**				
Partition	**Flag**	**Start**	**End**	**Sectors**	**Size**	**File System**	**Serial #**
1st System Reserved	Boot	2048	104447	102400	50 MB	NTFS	18EC42BBEC4292C4
2nd Partition	-	104448	61890501	61786054	29.5 GB	NTFS	E8DE4350DE4315EA
3rd Partition	-	61890560	62910463	1019904	498 MB	NTFS/ Hidden NTFS	9E46F86046F83A9B

Explanation of Partitions

Partition 1

This is the boot partition/system reserved partition. This partition contains operating system files that are needed to boot.

Partition 2

This partition holds the user files. This is what is viewable to the user and is where most user-accessible items are stored.

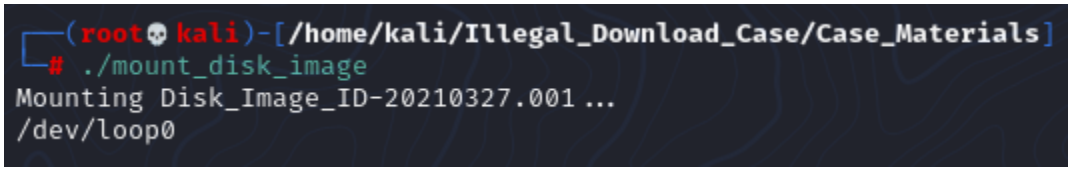
Partition 3

This partition is a recovery partition, which is utilized to factory reset in the event that something goes wrong.

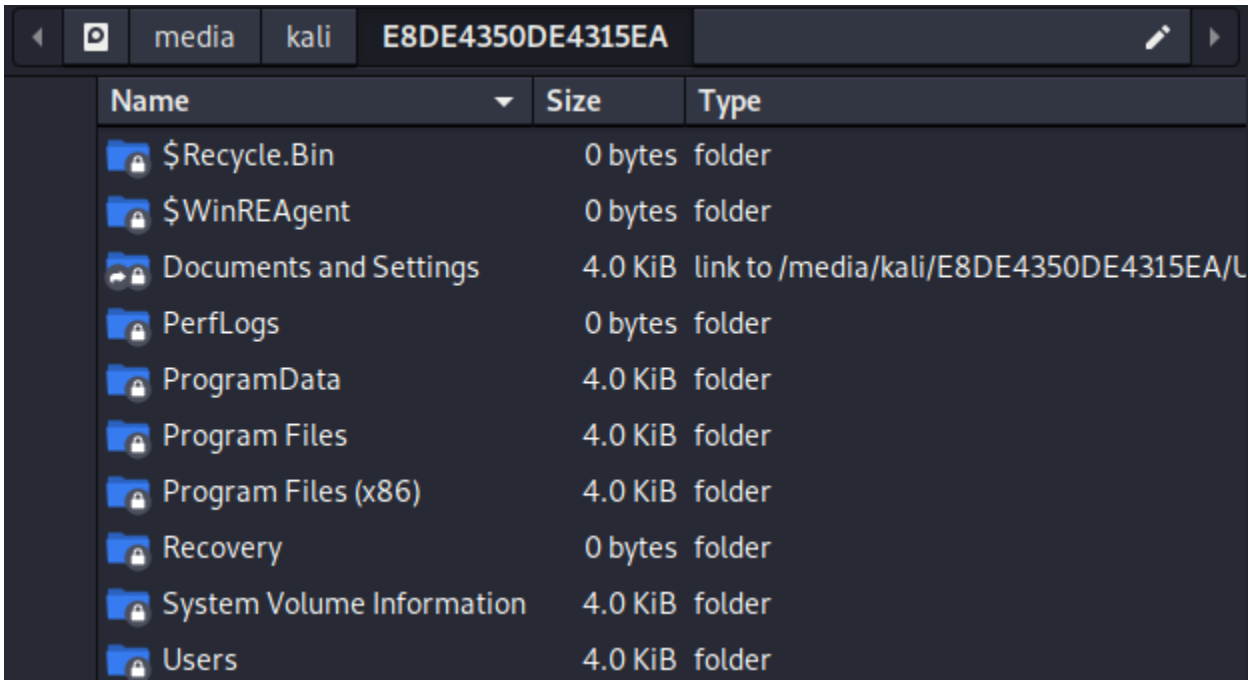
Mounting Disk Image

Using a Script to Mount the Disk Image

Running the Script to Mount the Disk Image



Disk Image Mounted



Creation of Folder for Exports

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case]
└─# mkdir Exports && mkdir Exports/Registry_files
```

Copying Registry Files to Export Folder

```
┌──(root💀kali)-[/media/…/E8DE4350DE4315EA/Windows/System32/config]
└─# cp -v /media/kali/E8DE4350DE4315EA/Windows/System32/config/SAM /home/kali/Illegal_Download_Case/Exports/Registry_files
'/media/kali/E8DE4350DE4315EA/Windows/System32/config/SAM' → '/home/kali/Illegal_Download_Case/Exports/Registry_files/SAM'

┌──(root💀kali)-[/media/…/E8DE4350DE4315EA/Windows/System32/config]
└─# cp -v /media/kali/E8DE4350DE4315EA/Windows/System32/config/SECURITY /home/kali/Illegal_Download_Case/Exports/Registry_files
'/media/kali/E8DE4350DE4315EA/Windows/System32/config/SECURITY' → '/home/kali/Illegal_Download_Case/Exports/Registry_files/SECURITY'

┌──(root💀kali)-[/media/…/E8DE4350DE4315EA/Windows/System32/config]
└─# cp -v /media/kali/E8DE4350DE4315EA/Windows/System32/config/SOFTWARE /home/kali/Illegal_Download_Case/Exports/Registry_files
'/media/kali/E8DE4350DE4315EA/Windows/System32/config/SOFTWARE' → '/home/kali/Illegal_Download_Case/Exports/Registry_files/SOFTWARE'

┌──(root💀kali)-[/media/…/E8DE4350DE4315EA/Windows/System32/config]
└─# cp -v /media/kali/E8DE4350DE4315EA/Windows/System32/config/SYSTEM /home/kali/Illegal_Download_Case/Exports/Registry_files
'/media/kali/E8DE4350DE4315EA/Windows/System32/config/SYSTEM' → '/home/kali/Illegal_Download_Case/Exports/Registry_files/SYSTEM'

┌──(root💀kali)-[/media/…/E8DE4350DE4315EA/Windows/System32/config]
└─# cp -v /media/kali/E8DE4350DE4315EA/Users/Kamryn/NTUSER.DAT /home/kali/Illegal_Download_Case/Exports/Registry_files
'/media/kali/E8DE4350DE4315EA/Users/Kamryn/NTUSER.DAT' → '/home/kali/Illegal_Download_Case/Exports/Registry_files/NTUSER.DAT'
```

Regripper

Using Regripper to Get System Time

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Exports/Registry_files]
└─# rip.pl -r SYSTEM -p timezone
Launching timezone v.20200518
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2021-03-21 20:03:44Z
  DaylightName    → @tzres.dll,-211
  StandardName    → @tzres.dll,-212
  Bias            → 480 (8 hours)
  ActiveTimeBias  → 420 (7 hours)
  TimeZoneKeyName→ Pacific Standard Time
```

Reading System Time Information

Pacific Standard Time (PST) is 8 hours behind UTC and 1 hour behind Pacific Daylight Time (PDT).

On Regripper's output where it says 'Bias' and 'ActiveTimeBias':

Bias -> 480 minutes (8 hours) from UTC time (no Daylight Savings = Pacific Standard Time)

ActiveTimeBias -> 420 minutes (7 hours) from UTC Time (Daylight Savings = Pacific Daylight Time)

This timezone is used in the western United States. This disk image was acquired from a computer in Maryland. Therefore, this system's timezone was not changed to the right setting by the suspect.

Since it was Daylight Savings Time when this image was acquired, we must assume that timestamps from the system could be in PDT.

Using Regripper to Get Windows Version

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Exports/Registry_files]
└─# rip.pl -r SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName              Windows 10 Home
ReleaseID                2009
BuildLab                 19041.vb_release.191206-1406
BuildLabEx               19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID     Core
RegisteredOrganization
RegisteredOwner          Kamryn
InstallDate              2021-03-10 00:04:29Z
InstallTime              2021-03-10 00:04:29Z
```

Using Regripper to See Computer Name

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Exports/Registry_files]
└─# rip.pl -r SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = DESKTOP-E4SUNT2
TCP/IP Hostname = DESKTOP-E4SUNT2
```

Using Regripper to View User Accounts

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Exports/Registry_files]
└─# rip.pl -r SAM -p samparse | grep -E 'Username|Created|Date' --color=none
Launching samparse v.20200825
Username        : Administrator [500]
Account Created : 2021-03-10 03:04:01Z
Last Login Date : 2020-09-27 14:54:30Z
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Username        : Guest [501]
Account Created : 2021-03-10 03:04:01Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Username        : DefaultAccount [503]
Account Created : 2021-03-10 03:04:01Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Username        : WDAGUtilityAccount [504]
Account Created : 2021-03-10 03:04:01Z
Last Login Date : Never
Pwd Reset Date  : 2020-09-27 14:50:45Z
Pwd Fail Date   : Never
Username        : Kamryn [1002]
Account Created : 2021-03-10 00:13:56Z
Last Login Date : 2021-03-21 20:04:35Z
Pwd Reset Date  : 2021-03-10 00:13:56Z
Pwd Fail Date   : 2021-03-10 00:21:18Z
```

User Account Information

User Account	Kamryn
User Account Creation Date	03/10/2021 00:13:56
Last Login Date	03/10/2021 20:04:35
Operating System	Windows 10 Home
OS Build	19041
System Name	DESKTOP-E4SUNT2
Owner	Kamryn
System Timezone	PST
System Install Date & Time	03/10/2021 00:04:29

Regripper to see Most Recently Logged on User

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Exports/Registry_files]
└─# rip.pl -r SOFTWARE -p lastloggedon
Launching lastloggedon v.20200517
lastloggedon v.20200517
(Software) Gets LastLoggedOn* values from LogonUI key

LastLoggedOn
Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastWrite: 2021-03-21 20:04:35Z

LastLoggedOnUser    = .\Kamryn
LastLoggedOnSAMUser = .\Kamryn
LastLoggedOnUserSID = S-1-5-21-1987397543-1106735666-2059573275-1002
```

As we can see `Kamryn` is the last user to logon on 03/21/2021 at 20:04:35Z

Finding When the Computer was Last Shutdown

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Exports/Registry_files]
└─# rip.pl -r SYSTEM -p shutdown
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2021-03-10 00:49:11Z
ShutdownTime  : 2021-03-10 00:49:11Z
```

As we can see, the last shutdown was 3/10/2021 04:49:11
This could mean that the person who had control of the system did not shut down for some time. This indicates that the system could have been in ‘sleep’ mode or ‘hibernation’

Utilizing Regripper to Find Recently Opened Files

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Exports/Registry_files]
└─# rip.pl -r NTUSER.DAT -p recentdocs                                    127 ✕
Launching recentdocs v.20200427
recentdocs v.20200427
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2021-03-27 14:25:45Z
  20 = Torrent-Sources
  19 = Contraband.mp3
  15 = Captures
  18 = ID-20210327.raw
  13 = Torrents
  17 = Contraband.mp3.torrent
  16 = ms-gamingoverlay:///
  0 = kglcheck/
  14 = ID-20210321.raw
  12 = Sample-1.mp3.torrent
  4 = Reference
  8 = List-2.txt
  7 = List-1.txt
  11 = Downloads
  10 = Sample-1.mp3
  9 = List-3.txt
  6 = This PC
  5 = Documents
  3 = Pictures
  2 = wallpaperflare.com_wallpaper.jpg
  1 = The Internet
```

Notable Files

As we can see in the screenshot above, there are some files that may be of interest to us. Most notably the following files:

- Torrent-Sources
- Contraband.mp3
- Torrents
- Contraband.mp3.torrent
- Sample-1.mp3.torrent
- Sample-1.mp3
- List-1.txt
- List-2.txt
- List-3.txt

Using *fls* to Generate a Directory Listing

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case]
└─# fls -o 104448 Case_Materials/Disk_Image_ID-20210327.001 -r -l -p -z UTC >> Reference_Files/file_directory_original.csv
```

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case]
└─# exa -l Reference_Files
.rw-r--r--  70M root 14 Nov 23:26 file_directory_original.csv
```

Using *grep* to Find Torrent Related Files and Files of Interest

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Reference_Files]
└─# grep -F '.exe' file_directory_original.csv | grep -i 'torrent' | cut -f 1,2,4,5
r/r 205974-128-3:       Users/Kamryn/AppData/Roaming/uTorrent/helper/helper.exe 2021-03-27 14:02:54 (UTC)       2021-03-21 20:40:17
 (UTC)
r/r 205783-128-4:       Users/Kamryn/AppData/Roaming/uTorrent/updates/3.5.5_45852/utorrentie.exe        2021-03-27 14:02:53 (UTC) 2
021-03-21 20:39:53 (UTC)
r/r 158784-128-1:       Users/Kamryn/AppData/Roaming/uTorrent/updates/3.5.5_45852.exe   2021-03-21 16:59:06 (UTC)       2021-03-21
20:39:08 (UTC)
r/r 205967-128-4:       Users/Kamryn/AppData/Roaming/uTorrent/updates/3.5.5_45966.exe   2021-03-21 20:40:19 (UTC)       2021-03-21
20:40:17 (UTC)
r/r 205772-128-3:       Users/Kamryn/AppData/Roaming/uTorrent/uTorrent.exe      2021-03-27 14:04:01 (UTC)       2021-03-21 20:39:08
 (UTC)
r/r 97182-128-4:        Users/Kamryn/Desktop/uTorrent.exe       2021-03-27 14:04:10 (UTC)       2021-03-21 20:37:28 (UTC)
r/r 97182-128-7:        Users/Kamryn/Desktop/uTorrent.exe:SmartScreen   2021-03-27 14:04:10 (UTC)       2021-03-21 20:37:28 (UTC)
```

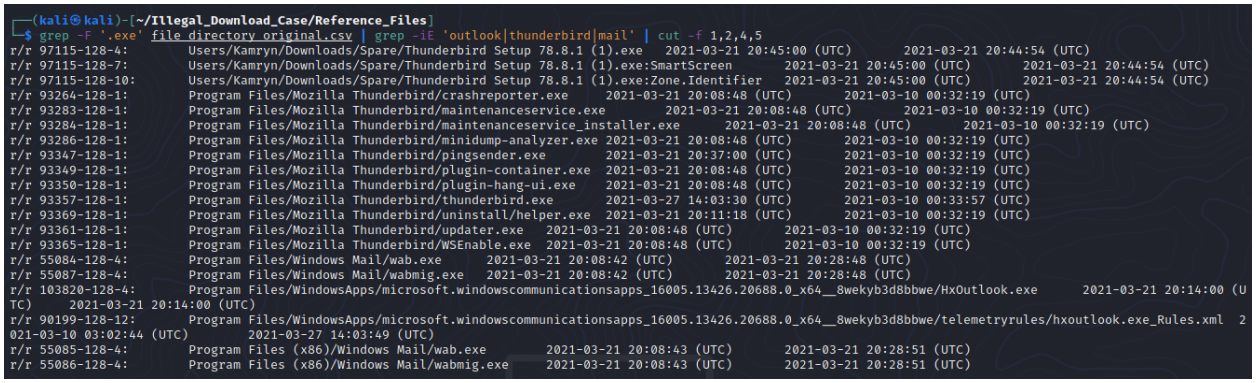
```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Reference_Files]
└─# grep -F '.mp3' file_directory_original.csv | grep -F 'torrent' | cut -f 1,2,4,5
r/r 79927-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent    2021-03-27 14:10:14 (UTC)       2021-03-27
14:10:14 (UTC)
r/r 79927-128-5:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent:Zone.Identifier    2021-03-27 14:10:14 (UTC) 2
021-03-27 14:10:14 (UTC)
r/r 206281-128-1:       Users/Kamryn/AppData/Roaming/uTorrent/Sample-1.mp3.torrent      2021-03-21 20:42:39 (UTC)       2021-03-21
20:42:39 (UTC)
r/r 55634-128-4:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent  2021-03-27 14:10:00 (UTC)       2021-03-27 14:10:11
 (UTC)
r/r 55634-128-5:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent:Zone.Identifier  2021-03-27 14:10:00 (UTC)       202
1-03-27 14:10:11 (UTC)
r/r 206280-128-4:       Users/Kamryn/Downloads/Torrents/Sample-1.mp3.torrent    2021-03-21 20:42:39 (UTC)       2021-03-21 20:52:23
 (UTC)

┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Reference_Files]
└─#
```

```
┌──(root💀kali)-[/home/kali/Illegal_Download_Case/Reference_Files]
└─# grep -F '.mp3' file_directory_original.csv | grep -iE 'contraband|sample-' | cut -f 1,2,4,5
r/r 54027-128-4:        Users/Kamryn/AppData/Roaming/Microsoft/Windows/Recent/Contraband.mp3.lnk        2021-03-27 14:10:00 (UTC) 2
021-03-27 14:10:00 (UTC)
r/r 206278-128-4:       Users/Kamryn/AppData/Roaming/Microsoft/Windows/Recent/Sample-1.mp3.lnk  2021-03-21 20:52:23 (UTC)       202
1-03-21 20:52:23 (UTC)
r/r 79927-128-4:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent    2021-03-27 14:10:14 (UTC)       2021-03-27
14:10:14 (UTC)
r/r 79927-128-5:        Users/Kamryn/AppData/Roaming/uTorrent/Contraband.mp3.torrent:Zone.Identifier    2021-03-27 14:10:14 (UTC) 2
021-03-27 14:10:14 (UTC)
r/r 206281-128-1:       Users/Kamryn/AppData/Roaming/uTorrent/Sample-1.mp3.torrent      2021-03-21 20:42:39 (UTC)       2021-03-21
20:42:39 (UTC)
r/r 79968-128-1:        Users/Kamryn/Documents/Reference/Work/Contraband.mp3    2021-03-27 14:16:12 (UTC)       2021-03-27 14:16:51
 (UTC)
r/r 80800-128-1:        Users/Kamryn/Documents/Reference/Work/Sample-1.mp3       2021-03-27 14:16:12 (UTC)       2021-03-27 14:16:51
 (UTC)
r/r 80800-128-3:        Users/Kamryn/Documents/Reference/Work/Sample-1.mp3:Zone.Identifier       2021-03-27 14:16:12 (UTC)       202
1-03-27 14:16:51 (UTC)
r/r 205963-128-5:       Users/Kamryn/Downloads/Sample-1.mp3     2021-03-27 14:16:11 (UTC)       2021-03-21 20:40:54 (UTC)
r/r 205963-128-7:       Users/Kamryn/Downloads/Sample-1.mp3:Zone.Identifier      2021-03-27 14:16:11 (UTC)       2021-03-21 20:40:54
 (UTC)
r/r 52901-128-4:        Users/Kamryn/Downloads/Torrent-Sources/Contraband.mp3    2021-03-27 14:25:43 (UTC)       2021-03-27 14:25:44
 (UTC)
r/r 207115-128-1:       Users/Kamryn/Downloads/Torrent-Sources/Sample-1.mp3      2021-03-27 14:25:41 (UTC)       2021-03-21 20:40:54
 (UTC)
r/r 207115-128-3:       Users/Kamryn/Downloads/Torrent-Sources/Sample-1.mp3:Zone.Identifier      2021-03-27 14:25:41 (UTC)       202
1-03-21 20:40:54 (UTC)
r/r 55634-128-4:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent  2021-03-27 14:10:00 (UTC)       2021-03-27 14:10:11
 (UTC)
r/r 55634-128-5:        Users/Kamryn/Downloads/Torrents/Contraband.mp3.torrent:Zone.Identifier  2021-03-27 14:10:00 (UTC)       202
1-03-27 14:10:11 (UTC)
r/r 206280-128-4:       Users/Kamryn/Downloads/Torrents/Sample-1.mp3.torrent    2021-03-21 20:42:39 (UTC)       2021-03-21 20:52:23
 (UTC)
```

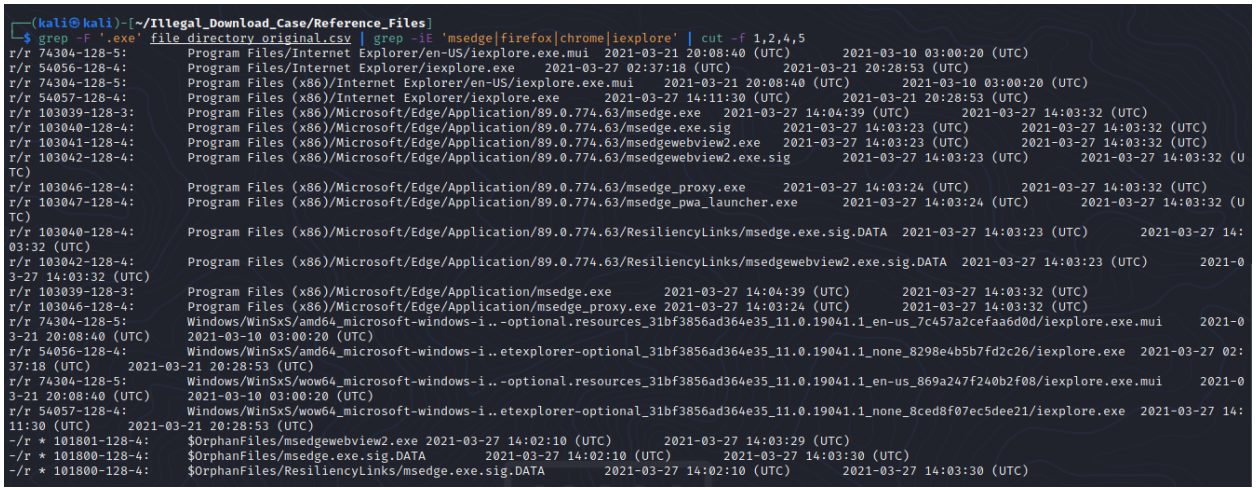
Searching for Lists

```
┌──(kali㉿kali)-[~/Illegal_Download_Case/Reference_Files]
└─$ grep -F '.txt' file_directory_original.csv | grep -F 'List-' | cut -f 1,2,4,5
r/r 215259-128-1:       Users/Kamryn/Documents/Reference/List-1.txt     2021-03-21 20:41:24 (UTC)       2021-03-21 20:25:46 (UTC)
r/r 217188-128-3:       Users/Kamryn/Documents/Reference/List-2.txt     2021-03-21 20:41:44 (UTC)       2021-03-21 20:26:16 (UTC)
r/r 218931-128-3:       Users/Kamryn/Documents/Reference/List-3.txt     2021-03-21 20:26:43 (UTC)       2021-03-21 20:26:42 (UTC)
```

Searching for Email Client



Searching for Web Browsers



Summary Thus Far

Utilizing Regripper *recentdocs* plugin, we were able to find files the user recently accessed. We found a torrent application, torrent files, mp3 files with similar names to the torrent files, an email client, and web browsers. With this information, we also have timestamps to help us narrow down the timeline of our investigation. Kamryn has '*Contraband.mp3.torrent*' and '*Contraband.mp3*'. '*Contraband.mp3*' could have been downloaded from the torrent file, or Kamryn already had it and then proceeded to create a torrent file out of it. The same applies for both '*Sample-1.mp3.torrent*' and '*Sample-1.mp3*'. When we acquire more information, we will be able to determine how Kamryn acquired these files. For now, we know that Kamryn is in possession of the files the company is looking for and could possibly be responsible for torrenting them.

Files of Interest Thus Far

- utorrentie.exe (uTorrent setup executable)
- uTorrent.exe (uTorrent executable)

- Contraband.mp3.torrent
- Contraband.mp3 and its link file
- Sample-1.mp3.torrent
- Sample-1.mp3 and its link file
- List-(1,2,3).txt
- Mozilla Thunderbird
- Microsoft Edge
- Internet Explorer