

# Northeastern University

College of Computer and Information Science

**Case Project**

**CY5210 Information System Forensics**

**Instructor: Elton Booker**

**Samyukta Kurikala**

## EXECUTIVE SUMMARY

An investigation was initiated into a suspected policy violation involving illegal digital content associated with owl-related material. The incident was flagged through internal monitoring systems that identified irregular user activity. In accordance with forensic practices, the suspect's device, DESKTOP-N566FM9, was seized and forensically imaged for analysis. The chain of custody was maintained, and hash verification was performed to confirm image integrity.

Partition analysis revealed three partitions on the drive, one of which was hidden and not accessible through normal system use. The hidden partition was mounted and analyzed, revealing owl-related content consistent with the case criteria. A detailed registry and file artifact analysis was conducted, focusing on core system hives, user-specific registry hives, USB activity, and application usage. Tools including FTK Imager, Registry Ripper, Arsenal Image Mounter, and Eric Zimmerman's suite were used throughout the examination.

The user account "Justine B" was identified as the primary system user. Evidence shows that owl-related files were accessed, saved, and organized across various storage locations, including USB devices. Prefetch and Jump List artifacts confirmed frequent execution of applications such as Chrome, Microsoft Photos, and CCleaner, suggesting both interaction with and possible concealment of illegal files. Shellbags and USB analysis further confirmed that external storage devices were used to access and potentially transfer owl-themed content.

Based on the findings, it is evident that there was intentional engagement with illegal material. The evidence supports deliberate access, storage, and potential duplication of contraband content. The report recommends further questioning of the user, full forensic examination of USB devices, and a review of communications and cloud storage accounts. Depending on the organization's policy and legal stance, the case may warrant disciplinary action, legal escalation, or further internal review.

## INTRODUCTION

On March 28, 2019, the digital forensics team was notified of a suspected policy violation involving the possession of illegal digital content. The alert was triggered by internal monitoring, which flagged irregular user activity, and the presence of content related to “owls”, classified as illegal under the parameters of this case and thus considered digital evidence.

The system under investigation, identified as DESKTOP-N566FM9 and assigned to the suspect, was forensically acquired following standard chain of custody procedures. All investigative actions were conducted under proper authority and academic guidance.

A forensic image of the system’s primary hard drive was created using FTK Imager v4.7.1, with hash verification confirming the integrity of the acquisition (see Figure 1).

Partition analysis of the image revealed three volumes, including one hidden partition not accessible under normal user operations. This volume was mounted using Arsenal Image Mounter and examined separately. Its contents were relevant to the case, indicating an attempt to conceal data from standard system access.

Subsequent analysis focused on key system and user artifacts, including registry hives (SAM, SYSTEM, SOFTWARE, NTUSER.DAT, and USRCLASS.DAT), USB device logs, prefetch files, Jump Lists, LNK files, and Shellbags. The findings of this analysis are detailed in the sections that follow.

```
Bytes per Sector: 512
Sector Count: 625,142,448
[Physical Drive Information]
Drive Model: Voyager S3 SCSI Disk Device
Drive Serial Number: 210987654321
Drive Interface Type: SCSI
Removable drive: False
Source data size: 305245 MB
Sector count: 625142448
[Computed Hashes]
MD5 checksum: 8af0bfac3d22b36da15b6951eaa46a2f
SHA1 checksum: b5498def6917ab6cbe1c697e678c0ff4b384f987

Image Information:
Acquisition started: Thu Mar 28 12:07:20 2019
Acquisition finished: Thu Mar 28 13:44:54 2019
Segment list:
D:\Testing\JustineBeaufort\JustineBeaufort.E01
D:\Testing\JustineBeaufort\JustineBeaufort.E02
D:\Testing\JustineBeaufort\JustineBeaufort.E03
D:\Testing\JustineBeaufort\JustineBeaufort.E04
D:\Testing\JustineBeaufort\JustineBeaufort.E05
D:\Testing\JustineBeaufort\JustineBeaufort.E06
D:\Testing\JustineBeaufort\JustineBeaufort.E07

Image Verification Results:
Verification started: Thu Mar 28 13:44:54 2019
Verification finished: Thu Mar 28 14:17:40 2019
MD5 checksum: 8af0bfac3d22b36da15b6951eaa46a2f : verified
SHA1 checksum: b5498def6917ab6cbe1c697e678c0ff4b384f987 : verified
```

Figure 1 : Hash verification

The hash verification of the acquired image was successful, ensuring the integrity of the forensic image.

## ANALYSIS

I focused my analysis on the key registry hives (SAM, SECURITY, SOFTWARE, SYSTEM) and user hives (NTUSER.DAT and USERCLASS.DAT). These hives played a critical role in identifying user-specific activities, system configurations and security settings that provided insight into unauthorized or malicious activities.

During my analysis, I identified USB devices that were plugged into the system. A detailed examination of the devices determined a potential involvement in the incident.

Further, an application analysis was carried out using artifacts like Prefetch files, LNK files, Jump Lists and Shellbags. These were essential in identifying recently executed applications and potentially malicious programs running on the system.

The subsections below explain the findings in detail, providing a comprehensive view of the analysis process and the obtained evidence.

### REGISTRY ANALYSIS

The Windows registry for DESKTOP-N566FM9 was analyzed for specific system configurations and settings, user specific settings, and user activity using Windows Registry Ripper v2.8. The SAM, SYSTEM, SOFTWARE and user hives (NTUSER.DAT and USERCLASS.DAT) were reviewed for relevant information pertinent to this investigation. The Windows registry identifies current system configuration and settings that may be useful to show the current state of the system and the actions performed by all users on a system.

### USER/GROUP INFORMATION

- **Users:**

**Table 1 – Users in DESKTOP-N566FM9**

Username	SID	Last Login
Administrator	S-1-5-21-2457848455-339827241-3711018272-500	Never
Guest	S-1-5-21-2457848455-339827241-3711018272-501	Never
DefaultAccount	S-1-5-21-2457848455-339827241-3711018272-503	Never
WDAGUtilityAccount	S-1-5-21-2457848455-339827241-3711018272-504	Never
Justine B	S-1-5-21-2457848455-339827241-3711018272-1001	2019-03-27 11:46:06Z

- **Groups:**

- **Administrators**

- S-1-5-21-2457848455-339827241-3711018272-1001 – Justine B

- S-1-5-21-2457848455-339827241-3711018272-500 – Administrator

Justine B has logged into the system 9 times.

Password Policies:

- > Password does not expire
- > Password not required
- > Normal user account

- The Administrator group has 2 users Administrator and Justine B
- There do not seem to be any other groups of interest.
- No user is given access to login remotely.

## SYSTEM INFORMATION

- **Microsoft OS Version:** Windows 10 Pro
- **Build Version:** 17134.rs4\_release.180410-1804
- **Current Control Set:** ControlSet001
- **OS Install Date:** 2019-03-25 15:53:27Z
- **Computer Name:** DESKTOP-N566FM9
- **Time Zone:** US Eastern Standard Time
- **Network Interfaces with Last Connection Time:** ATT-WIFI-3YLA; 2019-03-27 07:45:41
- **Autostart Programs:** SecurityHealth, SysTrayApp, ares, Chromium
- **Last Shutdown Time:** 2019-03-27 11:44:54Z

## USER ACTIVITY

- **Windows Search History** Justine B does not seem to have any windows search history according to the lack of evidence identified under the registry key according to the lack of evidence identified under the registry key  
NTUSER.DAT \Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery.
- **Typed Paths:** url1 - http://go.microsoft.com/fwlink/p/?LinkId=255141, cmd
- **RecentDocs:** There are 33 recent docs opened by the user and will be listed in a separate section.
- **Last Executed Commands:** This may not be populated if commands were not run from the START  
-> RUN box as Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU has no values.

## RECENT DOCS

9 = Downloads	12 = Whooo_Am_I_Owls_Bro.pdf
8 = 814u1IDExtL_SL1343_.jpg	20 = Owls and Their Homes.docx
32 = Barn-Owl-Cocked-Head.jpg.696x0_q80_crop-smart.jpg	19 = ARDB_species_names_numbers_simple.xlsx
31 = DWB2x2LVoAAtkWf.jpg large.jpg	18 = grumpy-owl_c_2512435.jpg
30 = stellaAndSherlock.jpg	17 = 913ada711431fb8f3d54c68c72eb0d9c.jpg
29 = stella.jpg	16 = hqdefault.jpg

28 = pFRtHLhL4eOA4de3yoIRiZt1DONVY3miQtn8qVU0FI.gif	4 = CAMERACARD (F:)
27 = owls.pdf	3 = cuteowl.jpg
26 = Pictures	7 = frogmouth.jpg
25 = 52c01a6b565fe.image.jpg	6 = nicepic.jpg
24 = Owl Musings.docx	11 = 30588_112467978790101_5187737_n.jpg
15 = GoodOnes	10 = 00y0y_j53rBCrjb8J_1200x900.jpg
23 = resized owl moon.jpg	13 = Great Horned Owl.pdf
14 = USB Drive (F:)	5 = d26ac13321f158c9e5e2fa459a6974ba.jpg
22 = owlColors_backup.xlsx	2 = Microsoft
21 = owlColors.xlsx	1 = Skype
0 = The Internet	

## USB DEVICE ANALYSIS

**Table 2 – USB Devices Connected to DESKTOP-N566FM9**

Device Name	Serial Number	User Account	First Time	Last Time
General UDisk USB Device	6&2017aed3&0&_	Justine B	3/26/2019 8:40:21 AM	3/26/2019 8:40:58 AM
General UDisk USB Device	6&32d15f78&0&_	Justine B	3/26/2019 11:41:07 AM	3/26/2019 1:33:41 PM
Kingston DataTraveler 102 USB Device	001D0F0C73C8BA3153110118	Justine B	3/25/2019 9:12:00 AM	3/25/2019 9:13:42 AM
Seagate BUP Slime Mac SL SCSI Disk Device	NA7RL7PR	Justine B	3/26/2019 1:36:29 PM	3/26/2019 2:24:31 PM
GENERIC SD04G	6&25d662b7&0&b008be2f	Justine B	-	-

The USB device was analyzed using USB Detective v1.3.6. The SYSTEM, SOFTWARE, NTUSER.DAT and setupapi.log files were given to the tool for analysis. FTK Imager v4.7.1 was used to extract these files from the image.

5 devices have been identified out of which 2 seem to be relevant to the case.

## APPLICATION ANALYSIS

An application analysis was conducted to identify the frequently used applications. The prefetch files were exported using FTK Imager. I used PECmd.exe v1.5.1 for prefetch analysis. Out of all the applications. The table below shows the applications of interest.

## PREFETCH ANALYSIS

**Table 3 – Prefetch Analysis for DESKTOP-N566FM9**

Application Name	Times Ran	First Time	Last Time
CCLEANER64.EXE	9	3/25/2019 13:23	3/27/2019 12:13
CHROME.EXE	137	3/25/2019 13:15	3/27/2019 18:29
MICROSOFT.PHOTOS.EXE	13	3/26/2019 15:42	3/27/2019 12:06
ONEDRIVE.EXE	3	3/26/2019 10:46	3/27/2019 11:46

These applications appear to be of particular interest based on their execution patterns. The presence of CCleaner suggests a possible attempt to remove traces of activity or conceal evidence. Chrome was executed frequently, indicating it may have been the primary method used to download or access owl-related images, warranting a deeper browser history and cache analysis. Additionally, Microsoft Photos and OneDrive were actively used and should be examined further, as they may contain or synchronize image files relevant to the case, including those depicting prohibited owl content.

## SHELL ITEM ANALYSIS

Shell item analysis was done using SBECmd. I analyzed Shellbags, Jump Lists and LNK Files. Shellbags provide evidence of accessed or deleted directories, even if the files themselves no longer exist. Jumplists identify frequently used programs and LNK files contain metadata about files and applications that were opened.

**Table 5 – Shellbag Analysis for DESKTOP-N566FM9**

Filename	Location	User Account	Created Time	Modified Time
GoodOnes	Desktop\My Computer\Desktop\GoodOnes	Justine B	3/26/2019 15:46	3/26/2019 15:46
Downloads	Desktop\My Computer\Downloads	Justine B	3/25/2019 13:05	3/26/2019 15:32
MagnetProcessCapture-20190326-140822	Desktop\My Computer\F:\MagnetProcessCapture-20190326-140822	Justine B	3/26/2019 15:46	3/26/2019 15:46
Protect	Desktop\C:\Users\Justine B\AppData\Roaming\Microsoft\Protect	Justine B	3/25/2019 13:06	3/25/2019 13:06

Shellbag artifacts revealed user interaction with various directories, including local, system, and external USB paths. Notably, the directory GoodOnes and other owl-related folders were identified, suggesting that the suspect curated and possibly organized owl-themed images and documents. The presence of paths leading to removable media—such as F:\MagnetProcessCapture-20190326-140822—supports the use of external devices for storing or accessing contraband content. These artifacts provide strong

evidence of historical folder access, even in cases where the directories or their contents may have been deleted.

**Table - 6 – Jump List Analysis for DESKTOP-N566FM9**

SourceCreated	SourceModified	AppId	M RU	Hostname	Path
3/26/2019 14:49	3/26/2019 15:32	5d696d521de238c3	0		C:\Users\Justine B\Downloads\Great Horned Owl.pdf
3/26/2019 14:49	3/26/2019 15:32	5d696d521de238c3	1		C:\Users\Justine B\Downloads\Whooo_Am_I_Owls_Bro.pdf
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	0	desktop-n566fm9	C:\Users\Justine B\Downloads\814u1IDExtL_SL1343_.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	1		C:\Users\Justine B\Desktop\Barn-Owl-Cocked-Head.jpg.696x0_q80_crop-smart.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	2	desktop-n566fm9	C:\Users\Justine B\Desktop\DWB2x2LVoAAtkWf.jpg large.jpg

A Jump list analysis was done using JLECmd. Jump List artifacts confirmed that the user repeatedly accessed owl-related files across multiple directories and storage volumes, including system folders and removable USB drives. Documents such as Whooo\_Am\_I\_Owls\_Bro.pdf, Great Horned Owl.pdf, and numerous owl-related images were opened frequently. The consistency of access timestamps and their presence across both local and external drives indicate deliberate interaction with the content. These findings reinforce the user's intent and awareness, as well as the possibility of file duplication or transfer between storage locations. The table is continued in the appendix below.

LNK file analysis was conducted using LECmd to identify evidence of recently accessed files and applications. However, no significant or owl-related content was recovered from the LNK artifacts. The recovered shortcuts pointed primarily to standard system files and commonly used applications, with no links to files of evidentiary interest. As such, LNK analysis did not contribute materially to the findings in this case.

#### ACTIVITY TIMELINE

- 2019-03-25 09:12 AM – Kingston USB device inserted.
- 2019-03-25 13:07 PM – Owl-related files appear in Downloads, Pictures, and Documents folders.
- 2019-03-25 13:23 PM – CCleaner64.exe executed; indicates potential data cleaning attempt.
- 2019-03-26 08:40 AM – General USB UDisk connected; used again later that day.
- 2019-03-26 14:08 PM – MagnetProcessCapture identified on external drive.



- 2019-03-26 15:32 PM – Multiple owl-related documents accessed (Whoooo\_Am\_I\_Owls\_Bro.pdf, Great Horned Owl.pdf).
- 2019-03-26 16:03 PM – Owl Musings.docx opened; confirms interest in owl-related materials.
- 2019-03-26 16:49 PM – Multiple owl-related Excel files opened from external media.
- 2019-03-27 18:32 PM – Last access timestamps for several owl-related images and documents.

## USER ACTIVITY

The user account **Justine B** appears to be the primary user on the system. Analysis of recent files, Jump Lists, LNK files, and Shellbags all link her to the viewing, saving, and organizing of owl-related media. Notably:

- Files such as Whoooo\_Am\_I\_Owls\_Bro.pdf, Great Horned Owl.pdf, and Owl Musings.docx were opened multiple times and across different storage volumes.
- Multiple owl-related images were saved with consistent naming and categorized in folders such as GoodOnes, suggesting deliberate collection and curation.
- Shellbags indicate the existence of organized folders for this material, including removable drives.
- Jump List artifacts confirm frequent access to owl-related documents from different directories (Downloads, Desktop, USB).

This behavior suggests intentional engagement with content that the case scenario deems illegal.

## CONCLUSION

### Findings:

1. The suspect system contained and repeatedly accessed owl-related media, meeting the case's definition of illegal content.
2. The user Justine B is tied directly to these files through Jump Lists, Shellbags, LNKs, and registry evidence.
3. USB analysis revealed external devices were used, potentially for storage or transfer of illegal content.
4. The presence of CCleaner suggests an effort to remove traces or hide activity.
5. A MagnetProcessCapture folder on a USB device implies monitoring or collection tools were used, potentially to further gather data.

### Recommendations:

1. Further questioning of Justine B regarding the sources and intent behind these files.

2. Forensic analysis of the external USB drives for additional owl-related material or deleted data.
3. Investigation of communications (email, chat apps) to check for sharing or acquisition of prohibited content.
4. Consider legal escalation based on established possession and repeated access to illegal content.
5. Recommend administrative action or training depending on organizational policy, especially if this is an insider threat or policy violation in a professional context.

## TOOLS

- Access Data FTK Imager v4.7.1
- Arsenal Image Mounter v3.4.141
- Registry Ripper v3.0
- Access Data Registry Viewer v2.0.0
- Autopsy v4.6.0
- Eric Zimmerman's tools and version numbers
  - LECmd v1.5.1
  - JLECmd v1.5.1
  - SBECmd v2.1.0
  - PECmd v1.5.1
- USB Detective v1.3.6

## APPENDIX

**Table - 6 – Jump List Analysis for DESKTOP-N566FM9**

SourceCr eated	SourceMo dified	AppId	M RU	Hostn ame	Path
3/26/2019 14:49	3/26/2019 15:32	5d696d521de238c3	0		C:\Users\Justine B\Downloads\Great Horned Owl.pdf
3/26/2019 14:49	3/26/2019 15:32	5d696d521de238c3	1		C:\Users\Justine B\Downloads\Whooo_Am_I_Owls_Bro.pdf
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	0	deskt op- n566f m9	C:\Users\Justine B\Downloads\814u1IDExtL_SL1343_.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	1		C:\Users\Justine B\Desktop\Barn-Owl-Cocked-Head.jpg.696x0_q80_crop-smart.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	2	deskt op- n566f m9	C:\Users\Justine B\Desktop\DWB2x2LVoAAtkWf.jpg large.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	3	deskt op- n566f m9	C:\Users\Justine B\Downloads\stellaAndSherlock.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	4	deskt op- n566f m9	C:\Users\Justine B\Downloads\stella.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	5	deskt op- n566f m9	C:\Users\Justine B\Downloads\pFRtHLhL4eOA4de3yolRiZt1DONVY3milQtn8qVU0FI.gif
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	6	deskt op- n566f m9	C:\Users\Justine B\Documents\owls.pdf
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	7	deskt op- n566f m9	C:\Users\Justine B\Pictures\52c01a6b565fe.image.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	8		C:\Users\Justine B\Documents\Owl Musings.docx
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	9	deskt op- n566f m9	D:\GoodOnes\resized owl moon.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	10		F:\owlColors_backup.xlsx

3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	11		C:\Users\Justine B\Documents\owlColors.xlsx
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	12		F:\Whooo_Am_I_Owls_Bro.pdf
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	13	deskt op- n566f m9	C:\Users\Justine B\Downloads\Owls and Their Homes.docx
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	14	deskt op- n566f m9	C:\Users\Justine B\Downloads\ARDB_species_names_numbers_simple.xlsx
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	15	deskt op- n566f m9	D:\GoodOnes\grumpy-owl_c_2512435.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	16	deskt op- n566f m9	D:\GoodOnes\913ada711431fb8f3d54c68c72eb0d9c.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	17	deskt op- n566f m9	D:\GoodOnes\hqdefault.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	18		F:\cuteowl.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	19		F:\nicepic.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	20		F:\frogmouth.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	21	deskt op- n566f m9	F:\30588_112467978790101_5187737_n.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	22	deskt op- n566f m9	F:\00y0y_j53rBCrjb8J_1200x900.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	23		F:\Great Horned Owl.pdf
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	24		F:\814u1IDExtL_SL1343_.jpg
3/25/2019 13:07	3/27/2019 18:32	5f7b5f1e01b83767	25		F:\d26ac13321f158c9e5e2fa459a6974ba.jpg
3/26/2019 16:02	3/26/2019 16:49	9839aec31243a928	0		F:\owlColors_backup.xlsx
3/26/2019 16:02	3/26/2019 16:49	9839aec31243a928	1	deskt op-	C:\Users\Justine B\Documents\owlColors.xlsx

				n566f m9	
3/26/2019 16:02	3/26/2019 16:49	9839aec31243a928	2	deskt op- n566f m9	C:\Users\Justine B\Downloads\ARDB_species_names_numbers_simple.xlsx
3/25/2019 13:07	3/26/2019 16:09	9d1f905ce5044aee	0		F:\Whooo_Am_I_Owls_Bro.pdf
3/25/2019 13:07	3/26/2019 16:09	9d1f905ce5044aee	1		F:\Great Horned Owl.pdf
3/25/2019 13:07	3/26/2019 16:09	9d1f905ce5044aee	2	deskt op- n566f m9	C:\Users\Justine B\Downloads\Great Horned Owl.pdf
3/25/2019 13:07	3/26/2019 16:09	9d1f905ce5044aee	3	deskt op- n566f m9	C:\Users\Justine B\Downloads\Whooo_Am_I_Owls_Bro.pdf
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	0	deskt op- n566f m9	C:\Users\Justine B\Downloads\stella.jpg
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	1	deskt op- n566f m9	C:\Users\Justine B\Downloads\pFRtHLhL4eOA4de3yoiRiZt1DONVY3milQtn8qVU0FI.gif
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	2		F:\cuteowl.jpg
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	3		F:\nicepic.jpg
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	4		F:\frogmouth.jpg
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	5		F:\30588_112467978790101_5187737_n.jpg
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	6		F:\00y0y_j53rBCrjb8J_1200x900.jpg
3/26/2019 12:41	3/26/2019 17:24	a52b0784bd667468	7		F:\d26ac13321f158c9e5e2fa459a6974ba.jpg
3/26/2019 16:03	3/26/2019 16:51	a7bd71699cd38d1c	0	deskt op- n566f m9	C:\Users\Justine B\Documents\Owl Musings.docx
3/26/2019 16:03	3/26/2019 16:51	a7bd71699cd38d1c	1	deskt op- n566f m9	C:\Users\Justine B\Downloads\Owls and Their Homes.docx