

Digital Forensics

Federico Conti - 4991779

2024/25

Contents

OWL Trafficking Investigation	3
Timeline Spreadsheet	3
Report	3
January 27	3
January 28	3
January 31	4
February 1	4
February 2	4
Key Evidence	4

OWL Trafficking Investigation

Timeline Spreadsheet

A detailed timeline has been compiled in the following spreadsheet:

- <https://docs.google.com/spreadsheets>

The timeline includes:

- MFT (for relevant files)
- System Registry
- User Registry
- LNK files
- Jumplists
- Analysis of USB devices
- Prefetch
- Google Chrome

Report

Observation Period: January 27 – February 2, 2017

Primary User: Sarah M (alias “Sarah McAvoy”; SID 1001)

Computer: DESKTOP-KLOQJ0V – Windows 10 Pro v1607, installed January 27, 2017

Others Device: SanDisk Cruzer Glide USB Device (VID_0781 & PID_5575)

Time Zone: Eastern Standard Time (UTC-5)

January 27

Sarah M created her account at 12:33 AM and immediately installed Chrome, using it to download images and documents related to owls, including:

- **Luna Owl.jpg**
- **Great Horned Owl Info.pdf**

She performed suspicious searches on Craigslist using the query “**huntington for sale ‘owls’**”, suggesting an intention to purchase an owl illegally.

In the afternoon, she continued targeted searches on owl care and captivity:

- “**what do owls eat**”
- “**how to care for an owl**”
- “**where to keep a snowy owl**”

Later, she opened an email titled “**Owls for Sale**” and downloaded various attachments received via email, including images of owls (Great Horned, Snowy, and Pygmy). She viewed these images using Paint and Microsoft Photos, indicating a growing interest in selecting a specific owl.

She moved these images to a desktop folder named pet, potentially preparing for purchase or identification of specimens.

January 28

Sarah further explored information about owls through searches on YouTube and commercial platforms like Tumblr and Etsy, possibly to acquire materials or accessories related to owl care.

January 31

The planning became concrete:

- She created a specific folder named **“New Pet Care”** to store detailed files on emergency care and domestic raising of owls, including:
 - **Owl_Emergency_Care.pdf** (This guide addresses what to do if someone finds a lost or injured owl chick)
 - **Owl_Keeping.pdf** (This document emphasizes why keeping an owl is not recommended and encourages potential owners to “tick every box” before proceeding)
 - **Snowy_Owl.pdf** (This document is a comprehensive profile of the Snowy Owl)
 - **Sightings2005.xls** (A detailed table of owl observations made at various locations)

In the evening, she downloaded additional materials, such as a bibliographic document on the Snowy Owl and a photo named **Next pet.jpg**.

February 1

She received a highly significant SMS message from the number +13045184333:

“Sarah, the delivery is today 7 tonight the confirmation will come later through pidgin.”

Clearly, this indicates a planned purchase of an owl, confirmed later through encrypted communication or chat on Pidgin.

Sarah downloaded and installed the instant messaging software **Pidgin**, attempting to configure it for private communication using Facebook XMPP, confirming the intent to hide traces of the conversations.

February 2

Sarah connected a SanDisk USB device, on which she saved important files:

- **My New Pet.jpg**
- **Snowy Owl Care.pdf**
- **Snowy_Owl.pdf**

She repeatedly opened these files, confirming the actual receipt and possession of the material.

The SanDisk USB device was then permanently disconnected at 10:38 PM.

Key Evidence

1. SMS message explicitly confirming delivery via Pidgin.
2. Suspicious searches (Craigslist, Etsy).
3. Specific documents for owl care, downloaded and repeatedly opened.
4. Use of USB devices for the secure transfer of compromising files.

These elements allow us to reasonably assert that Sarah M is involved in the illegal trafficking of owls, with clear evidence of planning, communication, and acquisition of material.