Università di Genova | DIBRIS DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

Report - Windows Forensics

Digital Forensics Course - University of Genova - a.a 2023/24

Author:
Cattaneo Kevin - S4944382

Index

Introduction

The timeline that has been produced tracks events from the image HD1.E01 of a Windows 10 Host, NTFS File System, with machine name DESKTOP-KLOQJ0V.
Some parts of the timeline of the browser history **have been voluntarily removed** when duplicated or when information does not follow and is not useful to the case scenario of illegal trading of owls. I accurately choose small portions where the chain of the events does not break in meaning.
Note that in the timeline I have highlighted in yellow the proofs of Owl / bird interest and trading.
In this report the dates are written as dd/mm/yyyy, in the timeline as yyyy/mm/dd.
[Note added after the mobile lesson]
Please notice also that I have also introduced a few referments about Mobile Forensics, highlighted in blue. Some information in this report has been integrated with Mobile Forensics, where accurately reported on the title.

Day 1 - 26/01/2017 (late evening)

On this day the machine has been initialized, by connecting to MU WiFi Network and by creating the account for Sarah McAvoy (Admin).

Day 2 - 27/01/2017

On this day Sarah M account was created and Sarah McAvoy account password changed. Sarah M is the main and most frequent user of the machine, so will be referred to as "the user" in the following. The user installs Google Chrome Browser from Microsoft Edge and then surfs the internet watching some Youtube videos about Harry Potter. The user is interested and register into a Harry Potter fan page. Then downloads an image of Luna Owl. After that the user downloads and deletes the picture Pygmy Owl and then downloads another image of an owl: Great Horned Owl; also the user removes the PDF file called Great Horned Owl Info. Then spends the time by surfing the internet again regarding Harry Potter stuff, until coming into a theater page to buy tickets for a Harry Potter show. Then log in into Twitter (X) and Instagram. After this the user browses Amazon, searching Christmas decorations and after that searches on Google a way to buy owl eggs. The user continues to search for owl eggs in different sites and then watch a couple of videos; after some time continues the searching for owl eggs and get to know some more information about owls.
Then the user goes to an online video games website but after a couple of minutes surfs to the Skype homepage and downloads the Skype executable.
After that the user logs out and for the last time the user Sarah McAvoy connects into the personal account. Here there is the first connection to MU_GUEST Network which follows a Windows Update completion.

Presumably the user Sarah M logs in again, and after about an hour a Skype Update starts. In the afternoon Microsoft Paint and Photos are executed to open some previously downloaded pictures. After five minutes the user starts again the search for birds and in particular snowy owls together with some information about how and where to keep an owl.
After ten minutes the user logs into the email account, confirms the Twitter (X) account confirmation email and starts to write an email.
Then the user logs into Facebook (Meta) and searches the profiles of Monica Neff and Isaiah Dashner. Then the user opens an email titled “Owls for sale” and here downloads an image of Snowy Owl and creates a folder “pets”. Then she deletes two pictures of owls. Then the user executes Microsoft Paint to view a picture of an owl and then executes the Edge Browser to search for a red ribbon. Then again opens Microsoft Paint to view several pictures of owls and some more images of Snowy Owls are downloaded.
After a couple of minutes the user searches for groceries on the Amazon site and then views the owned profile of Facebook: sarah.mcavoy.
After ten minutes the system boots without a proper shutdown and Skype updates start.

Day 3 - 28/01/2017

At 9 PM the system is connected for the first time to the McDonalds Free WiFi Network and the user restarts the searches about owls and some ebooks. Then the user watches some videos on Youtube about Harry Potter and Hunger Games and then searches how to learn falconry. After that the user registers in Tumblr and then logs into Yahoo. Then watch some videos, search for Game Theory and review some emails. Then the user alternates some surfing on Facebook (Meta), Tumblr and Pinterest. Then searches for a photo of “Athena with an owl” that saves as Background picture. After that the user surfs into the Etsy website.

Day 4 - 30/01/2017

The user started Google Chrome and searched for Game Theory videos. After an hour the user starts Skype that updates itself and starts a chat with Matt Haze about feelings about the Rings movie. After some minutes the user opens some owl images with both Edge and Chrome browsers. Then explore the emails and execute Microsoft Photos. About an hour later Skype updates itself.

Day 5 - 31/01/2017

The user starts Chrome and Skype. Then opens some saved pictures of owls and searches online how to care for owls. Then some of those images are moved, deleted and copied. Then with the browser the user opens several images. After a couple of minutes a new USB

device (SanDisk) is connected and probably a PDF file about owls (Snowy_Owl.pdf) is copied into it. Also the user deletes a PDF file called Snowy Owl, which contains information about this particular species of owls.
After that the user searches again for owl care and downloads a series of titles (Sightings2005.xls) that are copied in the Document folder. Then the user starts some new searches about owl care, opens some images with Microsoft Photos. After that the user downloads and deletes a picture of a turtle, then goes into a BirdTrading website.
Then the user starts Skype and a new chat with Matt Haze about the Resident Evil movie appointment for Friday at 7.

Day 6 - 01/02/2017 (+ Mobile Forensics)

The user received an SMS message about a delivery confirmation that would have continued through the Pidgin application.
The user starts Google Chrome and searches for and downloads the Pidgin application. Then watch some videos about Game Theory. Then surfs into Facebook.

Day 7 - 02/02/2017

The user logs in for the last time, executes Pidgin, opens Google Chrome and watches some videos about Game Theory. Here verifies the last connection to MU WiFi Network. Then the user connects the same SanDisk USB device as before and presumably a new image of owl is copied into it. Then another email is composed. And continues to alternate watching videos to reading emails. Then the user searches and downloads the Yahoo Messenger application. Then opens several images, also from the USB device, with the browsers. Then the user surfs into Facebook (Meta) and then logs into Tumblr.
After a couple of minutes the user also goes into the Flickr website and searches some pictures of different owls and “awesome animals”.
Some drivers for the USB device finish installing.

Day 8 - 03/02/2017 (Mobile Forensics)

On this day some web searches about “birds”, “owl” and “snowy owl” have been made on Google Chrome application on the mobile device.

Day 9 - 06/02/2017

A general USB device (VSN: 16062154) is connected to the computer and installed. The device contains a Paladin Live Linux distribution.

Day 10 - 07/02/2017

The general USB device (VSN: 16062154) is connected for the last time to the computer. The system boots without a regular shutdown, Skype starts and updates itself and some drivers for the USB finish the installation.

Interpretation

The following paragraph will represent a personal interpretation of the facts, about what happened and the cause of actions.

Sarah M (McAvoy) is a person that studies physics and is interested in Harry Potter, also views some theories behind the plot. She also saw Hunger Games, a film whose symbol is a Phoenix. From those films maybe Sarah took the will to adopt an Owl, just like Harry Potter. She does a lot of research about how to care for owls and some ways to buy them. Also searches a lot of images about owls in several sites (Tumblr, Pinterest, Flickr etc.). The alternation of emails may represent some buying order that has taken in action (probably from BirdTrades website) and some confirmations of delivering; a different interpretation could be someone that instructs this person on how to get the Owl without getting to know the public.

Some confirmation about the delivery we have through the view of the SMS Message.

After this presumably trading this person continues her life, going to the theater with her friends that Friday.

In the last two days (6-7) I think a third authorized actor (e.g. Police) accessed the computer to retrieve a complete copy of the disk via Paladin Live Linux distribution, started by an external USB device.