



Digital Forensics of Lonewolf

Final Report

Shannon Dsouza
11-13-2020

Index

Synthesis	2
Analysis	3
Analysis 1: Analysing documents in the hard disk	3
Analysis 2: Screenshots and downloaded images	4
Analysis 3: User's web history	6
Analysis 4: Attacker's cloud usernames	8

Synthesis

Scope: The analysis of the hard disk of an individual suspected of planning an attack.

Suspicious/Incriminating material identified:

- a) Incriminating documents in the hard disk
- b) Incriminating screenshots and images
- c) The user's web history
- d) Attacker's cloud credentials (which hold the incriminating documents as well)

The evidence extracted from the hard disk is sufficient to find the user as guilty of planning an attack at a library due to his pro-gun sentiments. The list of evidence includes a manifesto the user prepared describing their motivation to carry out the attack as well as detailed plans, thoughts before the attack, and their airline ticket.

The evidence discovered in the hard disk is included in the zip file with this report.

Analysis

Analysis 1: Analysing documents in the hard disk

Incrimination: High

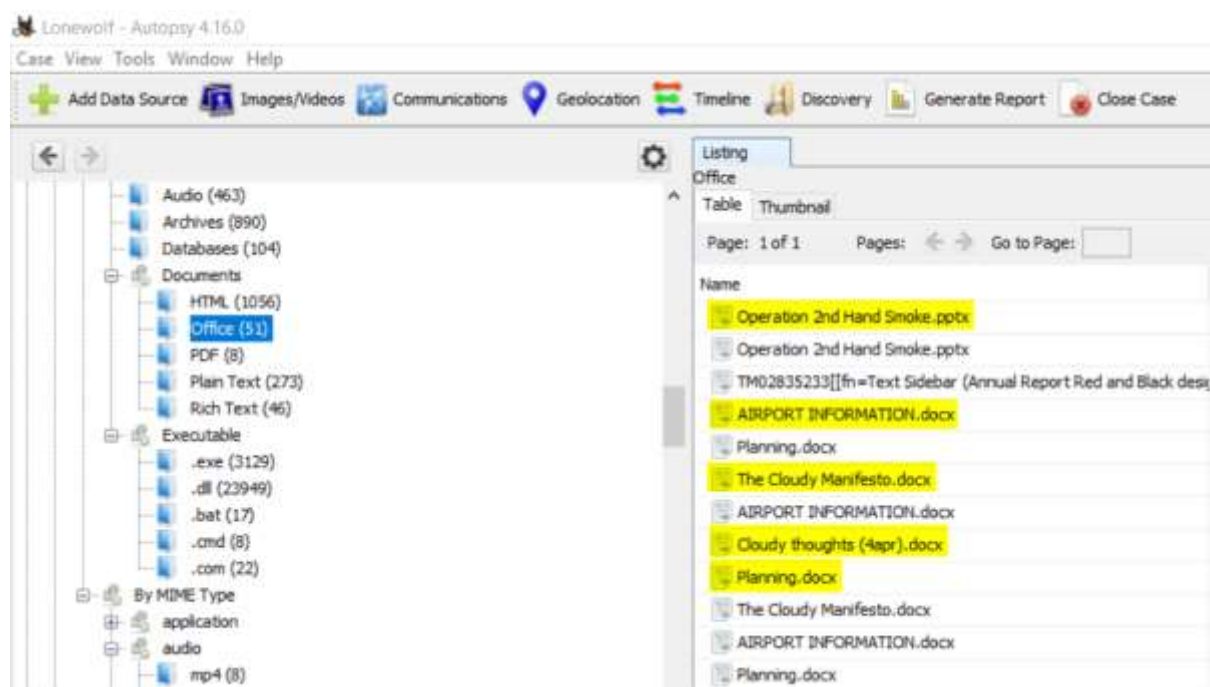
- a) Microsoft Word Documents: Several documents named: Airport Information, Cloudy thoughts, Planning, and The Cloudy Manifesto were retrieved. All had very detailed information about how the attack was to be carried out, the motivation behind the attack as well as personal thoughts of the attacker.
- b) Microsoft PowerPoint Presentation: A presentation titled 'Operation 2nd Hand Smoke' has detailed plans of the attack including the location and time of the attack as well as the possible routes the attacker could take to the event and to the airport after the attack.
- c) PDF Documents: The suspect has downloaded news articles that show an obvious disliking for the 'anti-gun' supporters and their agenda. These documents by themselves are not incriminating.

Description:

The Word documents and the Powerpoint presentation are the most incriminating evidence found in the hard disk. They have detailed plans of how the attack and escape are to be carried out, including pictures of the attack venue, routes to be taken, airline tickets, and hotel reservation in Indonesia. The document containing the thoughts of the attacker also mention someone named Paul who has access to the cloud services on which the attacker backed up his plans.

Identification of these files using Autopsy:

- a) Documents in the hard disk.



The incriminating documents

Analysis 2: Screenshots and downloaded images

Incrimination: Medium

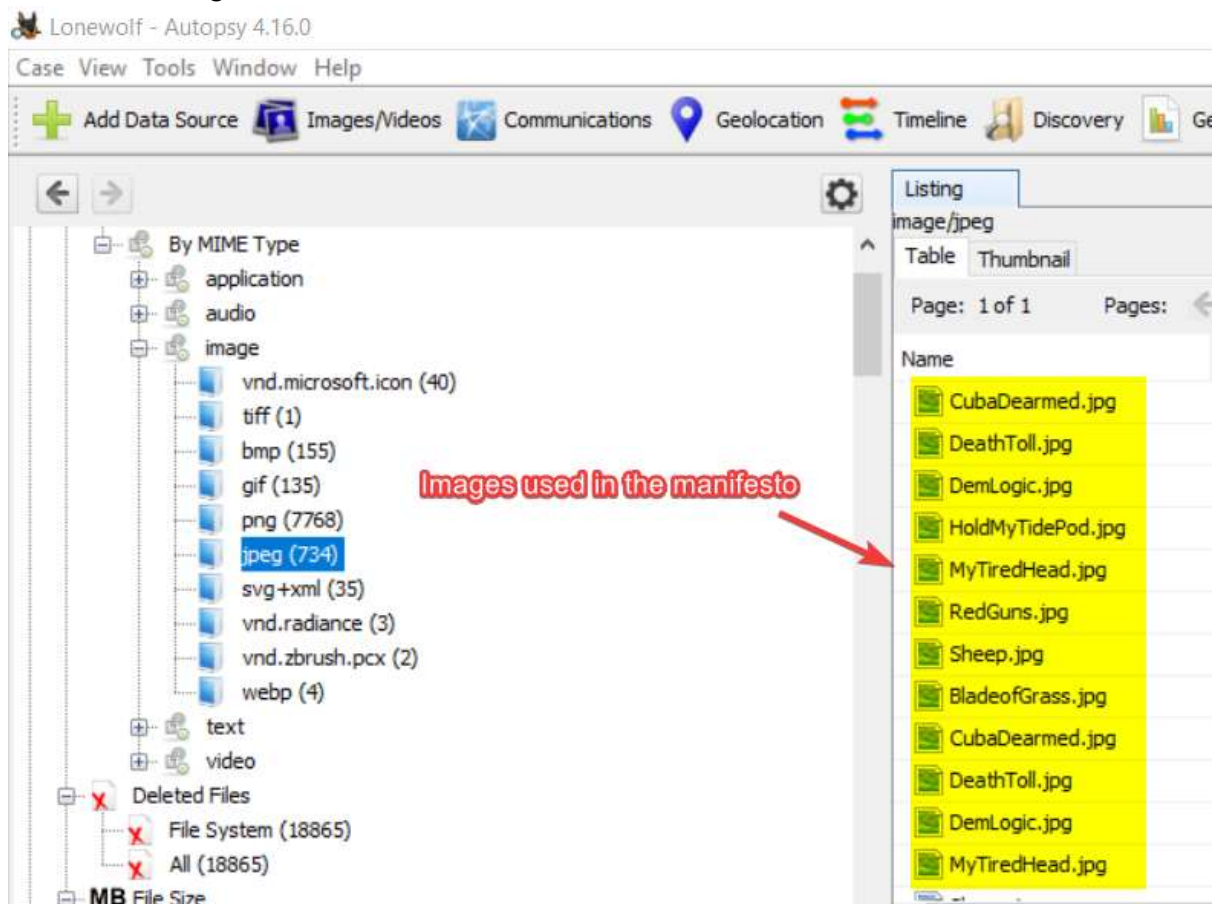
- a) Screenshots: The screenshots taken on the 3rd and 4th of April 2018, are of google maps routes to the venue and the airport, as well as the hotel booking, and airline ticket.
- b) Downloaded images: These are images downloaded for use in the manifesto document, many of these images are memes.

Description:

The screenshots show the routes the attacker plans to take to the target venue, as well as to the airport after the attack, it also includes a google street view image of the venue and an image of the airline ticket.

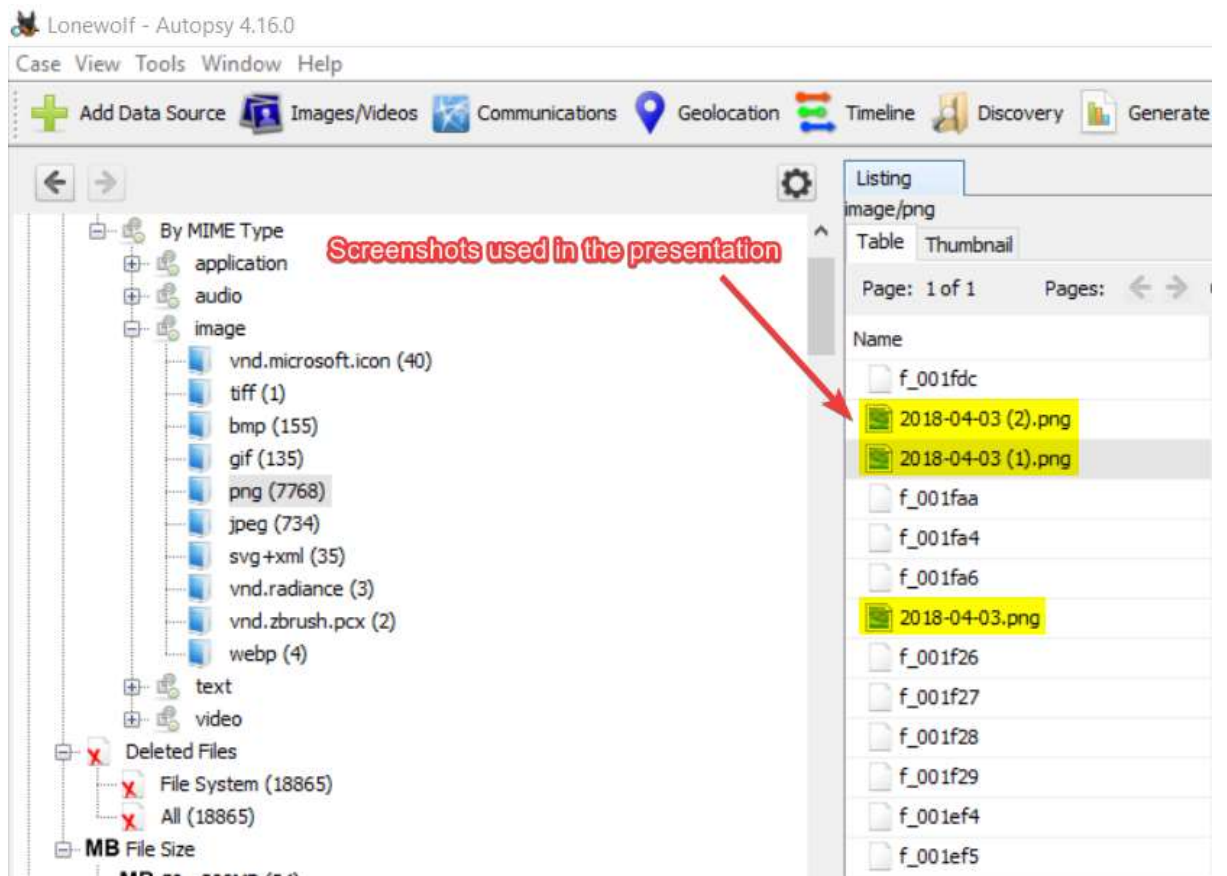
Identification of the images using Autopsy:

- a) Downloaded images.



These images were used in the attacker's manifesto

- b) Screenshots taken by the attacker.



These screenshots were used in the presentation

Analysis 3: User's web history

Incrimination: Medium

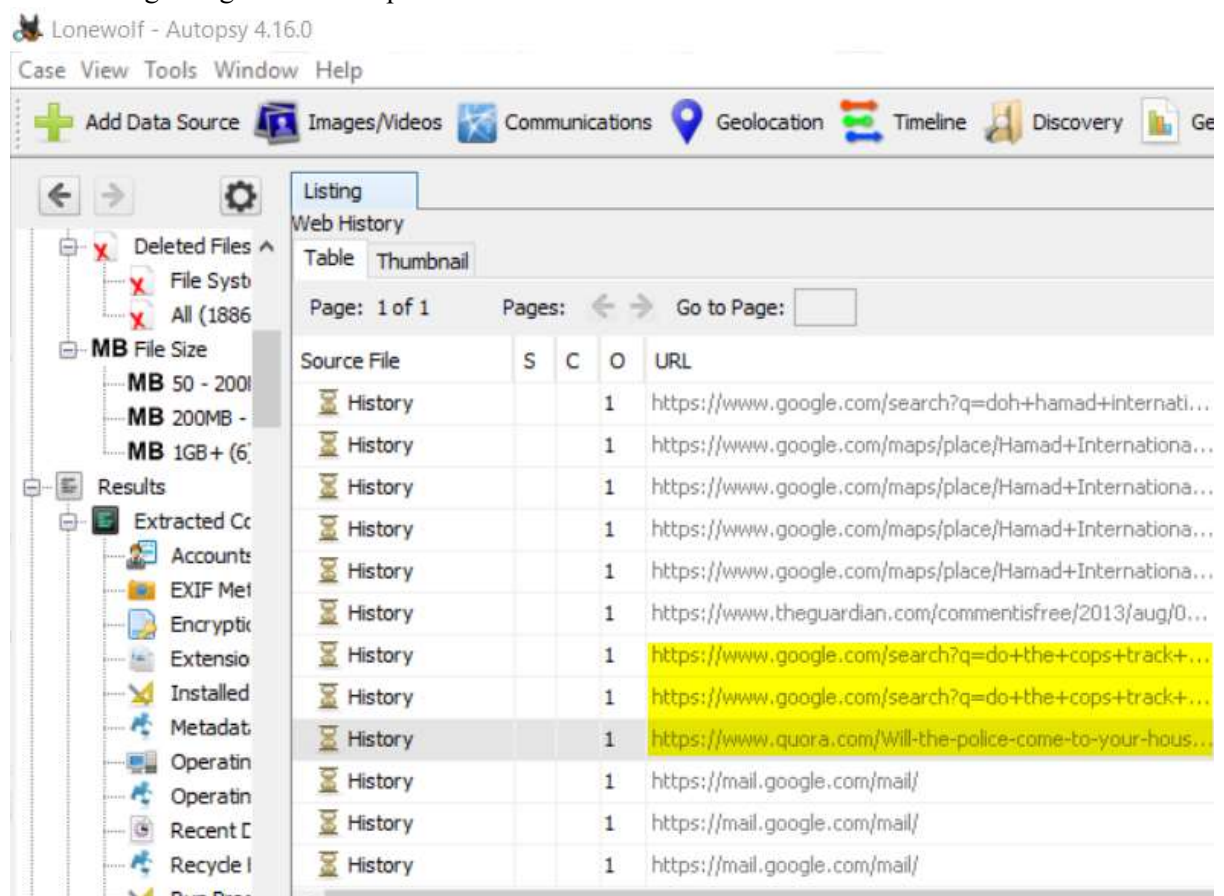
- a) Web History: The attacker's web history reveals several searches linked to the planned attack.

Description:

The attacker's web history reveals several implicating searches and sites such as those of online gun marketplaces and questions such as "how easy is it to buy an illegal gun" and "Will the police come to your house if you search for something illegal online but don't go to any website and exit the tabs quickly".

Identification of the web history using Autopsy:

- a) Searches regarding whether the police track internet searches.



Google searches

b) Visits to weapons purchasing sites.

Lonewolf - Autopsy 4.16.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Ge

Listing

Web History

Table Thumbnail

Page: 1 of 1 Pages: Go to Page:

Source File	S	C	O	URL
History			1	https://www.gunbroker.com/Pistol-Ammunition/search?Key...
History			1	https://www.gunbroker.com/Pistol-Ammunition/search?Key...
History			1	https://www.gunbroker.com/Pistol-Ammunition/search?Key...
History			1	https://www.gunbroker.com/Pistol-Ammunition/search?Key...
History			1	https://www.gunbroker.com/Pistol-Ammunition/search?Key...
History			1	https://www.gunbroker.com/Pistol-Ammunition/search?Key...
History			1	https://www.google.com/search?q=concealable+tactical+...
History			1	https://www.google.com/search?q=concealable+tactical+...
History			1	https://www.google.com/search?rlz=1C1CHBF_enUS790U...
History			1	https://www.cheaperthandirt.com/category/firearms/rifles...
History			1	https://www.gunbroker.com/Pistol-Ammunition/search?Pag...

Visits to gunbroker.com and cheaperthandirt.com

Analysis 4: Attacker's cloud usernames

Incrimination:

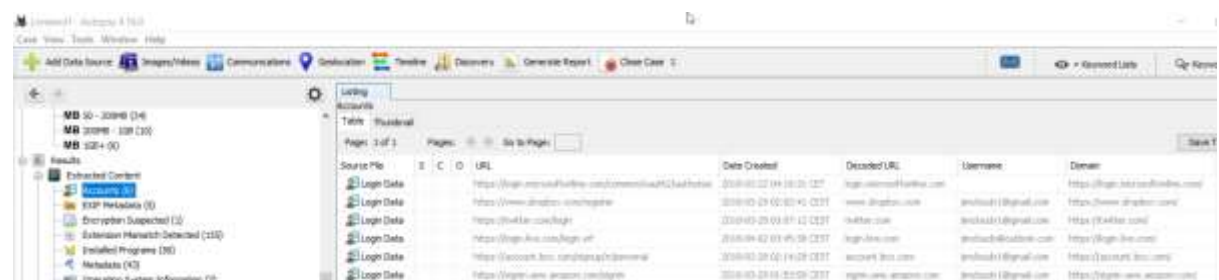
- a) Cloud usernames: The attacker's cloud credentials.

Description:

The attacker's usernames for the cloud services he has subscribed to are present on the hard disk. Accessing those services and finding the copies of the documents uploaded by the attacker will implicate them.

Identification of the cloud credentials using Autopsy:

- a) Attacker's cloud credentials on Autopsy.



The screenshot shows the Autopsy 4.19.0 interface. On the left, a tree view shows the file system structure with 'login_data.txt' selected. The main pane displays a table of extracted login data. The table has columns for Source File, URL, Data Created, Decoded URL, Username, and Domain. There are five rows of data, all from 'login_data.txt'.

Source File	URL	Data Created	Decoded URL	Username	Domain
login_data.txt	https://login.amazonaws.com/console/authenticate	2018-03-22 14:18:31 CEST	login.amazonaws.com	awscloud@bignail.com	https://login.amazonaws.com/
login_data.txt	https://www.dropbox.com/register	2018-03-23 02:52:42 CEST	www.dropbox.com	awscloud@bignail.com	https://www.dropbox.com/
login_data.txt	https://kallax.com/login	2018-03-23 03:51:12 CEST	kallax.com	awscloud@bignail.com	https://kallax.com/
login_data.txt	https://login.live.com/login.asp	2018-03-23 03:56:59 CEST	login.live.com	awscloud@bignail.com	https://login.live.com/
login_data.txt	https://account.live.com/signin?fromnew	2018-03-23 04:14:08 CEST	account.live.com	awscloud@bignail.com	https://account.live.com/
login_data.txt	https://login.live.amazonaws.com/login	2018-03-23 04:22:59 CEST	login.live.amazonaws.com	awscloud@bignail.com	https://login.live.amazonaws.com/

The attacker's cloud credentials