**Chapter 5**

**Chrome Browser Forensics**

**V1**

**A blue outline of a bird with a crown and text

Description automatically generatedSID: 2103022**

**Anglia Ruskin Final Project**

**Table of Contents**

[**Introduction** 2](#_Toc160116814)

[**Objective** 2](#_Toc160116815)

[**1.0** **Chrome History** 3](#_Toc160116816)

[**2.0 Prefetch Files** 7](#_Toc160116817)

[**3.0 Chrome profile picture.** 10](#_Toc160116818)

# **Introduction**

The fifth chapter covers Browser Forensics and Prefetch files which allows an investigator to gather large amount of important information on a suspect’s browsers and application usage. The chapter aims to teach the reader how to firstly view browser history from a different machine, convert prefetch files into a readable format using the command line and view a suspect’s Chrome profile picture.

# **Objective**

* View a suspects Chrome history.
* Convert prefetch files into a ‘csv’ file to see when and how many times a file is ran.
* View suspects Google Chrome profile picture.

1. **Chrome History**

1.Login as Digital-Forensics and use the password **‘password’** to login to the VM.

A login screen with a beach and rocks

Description automatically generated

2. Launch Chrome found on the desktop.

**A logo on a blue background

Description automatically generated**

3. Click the 3 dots in the top right corner then go History>History or press Ctrl+H to go straight to the next page.

**A screenshot of a computer

Description automatically generated**

4. If you have gone straight here you will see the history is empty and no searches have been made on your machine. A screenshot of a computer

Description automatically generated

5. Now close the browser.

A screenshot of a computer

Description automatically generated

6. Open File explorer by searching for it in the search bar or locating it on the taskbar.

A screenshot of a computer menu

Description automatically generated

7. At the top of file explorer click View then tick Hidden items. By default, Windows hides file access from users if they haven’t checked the box. The hidden items will be slightly translucent.

A screenshot of a computer

Description automatically generated

8. On the desktop open the evidence folder, you should now have 2 file exploer windows open. Right click and copy the ‘History’ file.

A screenshot of a computer

Description automatically generated

9. Return to the first file explorer app where you enabled hidden items and locate the Local Disk (C:) from the collum on the left-hand side.

A screenshot of a computer

Description automatically generated

10. Locate the following path **Local Disk (C:) > Users > Digital-Forensics > AppData > Local > Google > Chrome > User Data > Default.**

A screenshot of a computer

Description automatically generated

11. Right click on the blank space on the right-hand side of the files and click paste.

A screenshot of a computer

Description automatically generated

12. A pop-up will appear click ‘Replace the file in the destination’.

A screenshot of a computer

Description automatically generated

13. Repeat steps 2+3 to return to the history tab of Chrome. You should now see the history of the person you are investigating, see anything suspicious?

A screenshot of a computer

Description automatically generated

# **2.0 Prefetch Files**

1. Open Command Prompt by searching for ‘cmd’ in the search bar.

A screenshot of a computer

Description automatically generated

2. Type ‘cd desktop\tools\net6’ to access the tools necessary to convert prefetch files to an excel document.

A screenshot of a computer

Description automatically generated

3. Type ‘PECmd.exe -d "C:\Windows\Prefetch" --csv "C:\users\Digital-Forensics\Desktop\Output"’.



|  |  |
| --- | --- |
| **Line** | **Description** |
| PECmd.exe | Tools used |
| -d | Directory identifier |
| "C:\Windows\Prefetch" | Directory/prefetch location |
| --csv | File type converted to |
| "C:\users\Digital-Forensics\Desktop\Output” | Output folder |

4. Wait until the process is complete, it may take 5 minutes when finished it will look like the figure below.

A computer screen shot of a flag

Description automatically generated

5. Locate and open the folder ‘Output’ on the desktop.

A computer screen shot of a file

Description automatically generated

6. Open the first file in the folder

A screenshot of a computer

Description automatically generated

7. A pop up will appear tick ‘Merge delimiters’ and click ‘OK’.

A screenshot of a computer

Description automatically generated

7. You can now see when each application was opened at what time and how many times. This will reveal if a victim has ‘accidently’ opened a dodgy link or has opened it multiple times at specific times.

A screenshot of a computer

Description automatically generated

# **3.0 Chrome profile picture.**

1. Locate ‘C:\Users\Digital-Forensics\AppData\Local\Google\Chrome\User Data\Default\Google\_Profile’

A screenshot of a computer

Description automatically generated

2. Open the ‘Google\_Profile image’ and click ‘OK’.

A screenshot of a computer

Description automatically generated

3. Below you can see the profile picture of the google account used if it’s a chrome logo they haven’t changed the picture.

A screenshot of a computer

Description automatically generated

4. The chapter is complete, and you can now view a suspect’s history, see their prefetch files to see when an application was opened and view their browser profile picture. You can close all applications and return to the desktop for Chapter 6 or shutdown if you wish to continue later.