

# USB Device Analysis

- **Identify connected USB Devices**
- **USB Device information**
  - Vendor
  - Model
  - Firmware Revision
  - Physical Serial Number
  - First usage
  - Last usage
  - Volume name
  - Volume Serial Number
- **Source of information**
  - Registry
    - SYSTEM, SOFTWARE, NTUSER.DAT
  - Shell Items

# USB – Vendor ID – Product ID - Physical S/N

**SYSTEM\Current Control Set\ENUM\USB**

The screenshot displays the Windows Registry Editor. The left pane shows the tree structure with the path **SYSTEM\Current Control Set\ENUM\USB\VID\_0781&PID\_5575\20051739911AEFC1DE29** selected. The right pane shows the values for this key:

Value Name	Value Type	Data
DeviceDesc	RegSz	@usbstor.inf,%genericbulkonly.devicedesc%;USB Mass Storage Device
LocationInformation	RegSz	Port_#0005.Hub_#0001
Capabilities	RegDword	148
ContainerID	RegSz	{29fdf3c1-8caf-5136-bf90-2118ad324356}
HardwareID	RegMultiSz	USB\VID_0781&PID_5575&REV_0127 USB\VID_0781&PID_5575
CompatibleIDs	RegMultiSz	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
ClassGUID	RegSz	{36fc9e60-c465-11cf-8056-444553540000}
<b>Service</b>	RegSz	<b>USBSTOR</b>
Driver	RegSz	{36fc9e60-c465-11cf-8056-444553540000}\0003
Mfg	RegSz	@usbstor.inf,%generic.mfg%;Compatible USB storage device
ConfigFlags	RegDword	0

# USB – Vendor ID – Product ID - Physical S/N

**www.devicehunt.com**

DEVICE  
H U N T

[Login](#) [Register](#)

[About](#) [Why](#) [PCI Vendors](#) [USB Vendors](#) [Forum](#) [Donate](#) [Contact](#)

Type  
USB

Vendor ID  
0781

Device ID  
5575

Q

Device Details


Cruzer Glide

Type	Information
ID	5575

Vendor Details

SanDisk Corp.

Type	Information
ID	0781



Download gratuito

all downloads [Apri >](#)

# USB – Vendor – Product – Physical S/N – Friendly Name

**SYSTEM\Current Control Set\ENUM\USBSTOR**

Registry Editor window showing the path **SYSTEM\Current Control Set\ENUM\USBSTOR**. The left pane displays the tree structure, and the right pane displays the values for the selected key.

**Key name:** **20051739911AEFC1DE29&0**

Value Name	Value Type	Data
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	RegDword	16
ContainerID	RegSz	{29fdf3c1-8caf-5136-bf90-2118ad324356}
HardwareID	RegMultiSz	USBSTOR\DiskSanDisk_Cruzer_Glide____1.27 USBSTOR\DiskSanDisk_Cruzer_Glide____ USBSTOR\...
CompatibleIDs	RegMultiSz	USBSTOR\Disk USBSTOR\RAW GenDisk
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}
Service	RegSz	disk
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
Mfg	RegSz	@disk.inf,%genmanufacturer%:(Standard disk drives)
<b>FriendlyName</b>	RegSz	<b>SanDisk Cruzer Glide USB Device</b>
ConfigFlags	RegDword	0

# USB – Installation date / First connection

SYSTEM\Current Control Set\ENUM\USBSTOR\<device>\<S/N>\  
Properties\{83da6326-97a6-4088-9453-a1923f573b29}\00000064

The screenshot shows the Windows Registry Editor with the following structure:

- Registry hives (5)
- Available bookmarks (112/0)
- Enter text to search... Find
- Key name
- USBSTOR
  - Disk&Ven\_General&Prod\_USB\_Flash\_Disk&Rev\_1100
  - Disk&Ven\_SanDisk&Prod\_Cruzer\_Glide&Rev\_1.27
  - 20051739911AEEC1DE29&0
    - Device Parameters
    - Properties
      - {3464f7a4-2444-40b1-980a-e0903cb6d912}
      - {540b947e-8b40-45bc-a8a2-6a0b894cbda2}
      - {80497100-8c73-48b9-aad9-ce387e19c56e}
      - {83da6326-97a6-4088-9453-a1923f573b29}**
        - 0003
        - 000A
        - 0064**
        - 0065
        - 0066
        - 0067
      - {a8b865dd-2e3d-4094-ad97-e593a70c75d6}

The right pane shows the 'Values' list with the following data:

Value Name	Value Type	Data
(default)	RegFileTime	2017-02-02 21:53:08

# USB – Last connection

**SYSTEM\Current Control Set\ENUM\USBSTOR\<device>\<S/N>\  
Properties\{83da6326-97a6-4088-9453-a1923f573b29}\00000066**

The screenshot shows the Windows Registry Editor. The left pane displays the tree structure under 'USBSTOR'. The right pane shows the 'Values' list. A red box highlights the '(default)' value in the 'Values' list.

Value Name	Value Type	Data
(default)	RegFileTime	2017-02-02 22:38:09

# USB – Last removal

**SYSTEM\Current Control Set\ENUM\USBSTOR\<device>\<S/N>\  
Properties\{83da6326-97a6-4088-9453-a1923f573b29}\00000067**

The screenshot shows the Windows Registry Editor. The left pane displays the tree structure of the registry. The path **SYSTEM\Current Control Set\ENUM\USBSTOR\<device>\<S/N>\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\00000067** is highlighted with a red box. The right pane shows the 'Values' tab for the selected key. It contains a table with the following data:

Value Name	Value Type	Data
(default)	RegFileTime	2017-02-02 22:38:47

# USB – Volume Serial Number

SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name

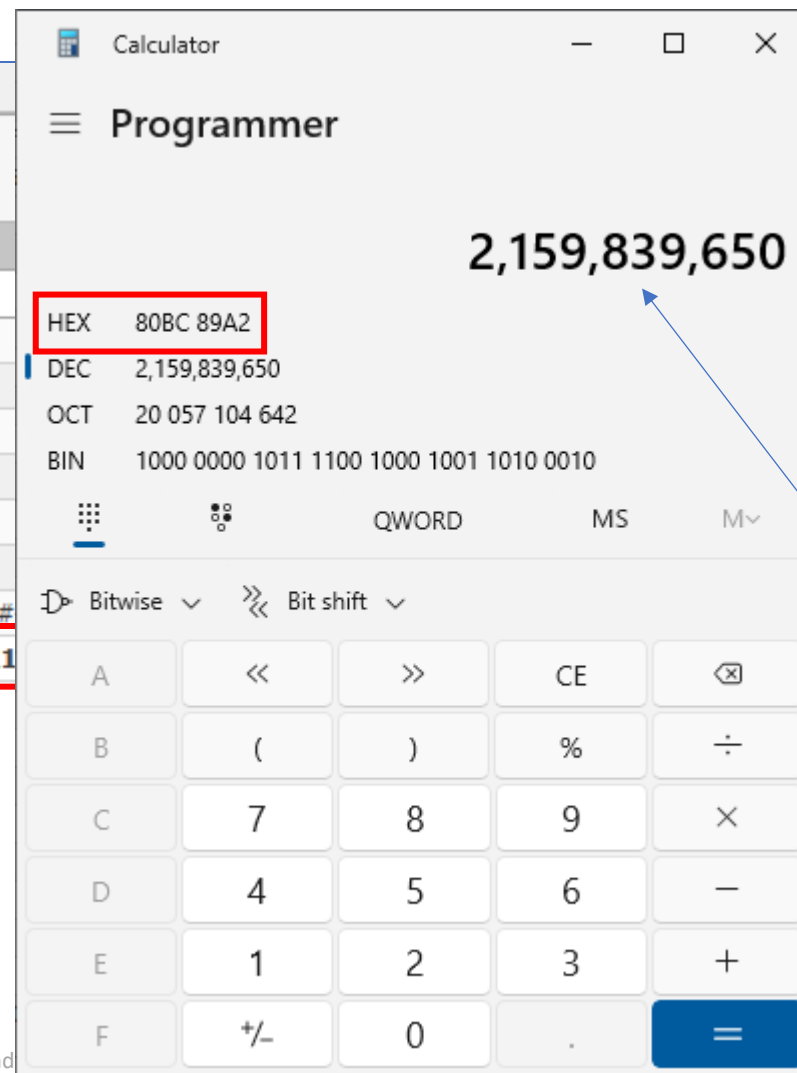
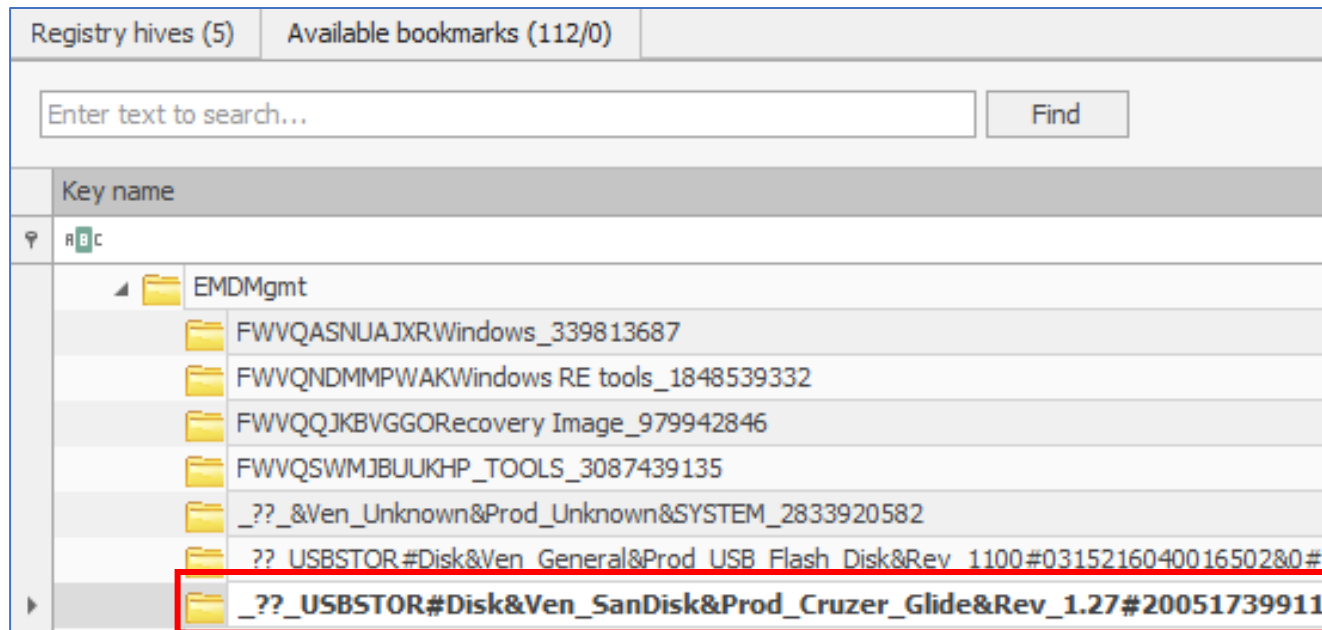
▼ EMDMgmt

- FWVQASNUAJXRWindows\_339813687
- FWVQNDMPWAKWindows RE tools\_1848539332
- FWVQQJKBVGGORecovery Image\_979942846
- FWVQSWMJBUUKHP\_TOOLS\_3087439135
- \_??\_&Ven\_Unknown&Prod\_Unknown&SYSTEM\_2833920582
- ?? USBSTOR#Disk&Ven\_General&Prod\_USB\_Flash\_Disk&Rev\_1100#0315216040016502&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}PALADIN EDG 369500500
- ??\_USBSTOR#Disk&Ven\_SanDisk&Prod\_Cruzer\_Glide&Rev\_1.27#20051739911AEEC1DE29&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\_2159839650**



# USB – Volume Serial Number

SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt



# USB – Volume Serial Number

SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt

Registry hives (5) Available bookmarks (112/0)

Enter text to search... Find

Key name

EMDMgmt

FWVQASNUAJXRWindows\_339813687

FWVQNDMMPWAKWindows RE tools\_1848539332

FWVQQJKBVGGORecovery Image\_979942846

FWVQSWMJBUEKHP\_TOOLS\_3087439135

??\_&Ven\_Unknown&Prod\_Unknown&SYSTEM\_2833920582

??\_USBSTOR#Disk&Ven\_General&Prod\_USB Flash Disk&Rev\_1100#0315216040016502&0#

**??\_USBSTOR#Disk&Ven\_SanDisk&Prod\_Cruzer\_Glide&Rev\_1.27#20051739911**

F:\My New Pet.jpg	80BC89A2
F:\Snowy Owl Care.pdf	80BC89A2
F:\Snowy_Owl.pdf	80BC89A2

Calculator

Programmer

2,159,839,650

HEX 80BC 89A2

DEC 2,159,839,650

OCT 20 057 104 642

BIN 1000 0000 1011 1100 1000 1001 1010 0010

QWORD MS Mv

Bitwise Bit shift

A << >> CE <X>

B ( ) % ÷

C 7 8 9 ×

D 4 5 6 −

E 1 2 3 +

F +/- 0 . =

# Exercise 9

Identify all the information about connected USB Devices

- Vendor
- Model
- Firmware Revision
- Physical Serial Number
- First usage
- Last usage
- Volume name
- Volume Serial Number

# Prefetch

- Windows XP/Vista/7/8/10 feature
- Used to increase system performances by preloading libraries/code
- Stored in .pf files in **C:\Windows\Prefetch**
- One file per executable
- **Vista/7 → 128 file max**
- **8/10 → 1024 file max**
- It contains **last time run (Vista/7)** and **last 8 times run (8/10)**

The screenshot displays the Windows Prefetch directory structure and a specific file's properties. The 'Evidence Tree' on the left shows the hierarchy of system folders, with 'Prefetch' highlighted. The 'File List' on the right shows a list of prefetch files, with 'CMD.EXE-0BD30981.pf' selected and highlighted in red. The 'Properties' window at the bottom shows the details for this file, with the 'Date Accessed', 'Date Created', and 'Date Modified' fields highlighted in red.

**Evidence Tree**

- Media
- mib.bin
- Microsoft.NET
- Migration
- MiracastView
- ModemLogs
- notepad.exe
- OCR
- Offline Web Pages
- Panther
- Performance
- PLA
- PolicyDefinitions
- Prefetch
- PrintDialog
- Professional.xml
- Provisioning
- regedit.exe
- Registration
- RemotePackages
- rescache
- Resources
- SchCache
- schemas
- security
- ServiceProfiles
- servicing
- Setup

**File List**

Name	Size	Type	Date Modified
ASPNETCA.EXE-571146CF.pf	6	Regular File	27/01/2017 02:43:29
ASPNETCA.EXE-575DB5AB.pf	6	Regular File	27/01/2017 02:43:27
ASPNET_REGIIS.EXE-8545410E.pf	8	Regular File	27/01/2017 02:43:33
ASPNET_REGIIS.EXE-E7D16D20.pf	8	Regular File	27/01/2017 02:43:34
AUDIODG.EXE-AB22E9A6.pf	6	Regular File	01/02/2017 17:31:21
BACKGROUNDTASKHOST.EXE-45FE2909.pf	30	Regular File	02/02/2017 22:49:09
BACKGROUNDTASKHOST.EXE-897AD46E.pf	9	Regular File	31/01/2017 19:14:12
BACKGROUNDTASKHOST.EXE-BE112A50.pf	12	Regular File	02/02/2017 22:48:53
BROWSER_BROKER.EXE-EEC8D935.pf	8	Regular File	02/02/2017 22:39:18
BYTECODEGENERATOR.EXE-62D6B3D7.pf	5	Regular File	27/01/2017 17:35:17
BYTECODEGENERATOR.EXE-FB938A53.pf	4	Regular File	27/01/2017 17:35:20
CHRMSTP.EXE-B1C7BB6B.pf	9	Regular File	27/01/2017 16:54:51
CHRMSTP.EXE-B1C7BB72.pf	5	Regular File	27/01/2017 16:54:51
CHROME.EXE-5349D2D7.pf	29	Regular File	02/02/2017 21:57:10
CHROME.EXE-5349D2D8.pf	10	Regular File	02/02/2017 22:49:15
CHROME.EXE-5349D2D9.pf	16	Regular File	02/02/2017 21:57:10
CHROME.EXE-5349D2DA.pf	12	Regular File	01/02/2017 17:05:23
CHROME.EXE-5349D2DD.pf	9	Regular File	02/02/2017 21:57:20
CHROME.EXE-5349D2DE.pf	7	Regular File	02/02/2017 21:57:20
CHROME.EXE-5349D2DF.pf	26	Regular File	02/02/2017 21:57:56
CHROME.EXE-5349D2DF.pf		\$130 INDX Entry	
CLIPUP.EXE-1C5C7B66.pf	8	Regular File	27/01/2017 16:54:45
CMD.EXE-0BD30981.pf	3	Regular File	02/02/2017 21:24:15
CMD.EXE-0D0290C3.pf	3	Regular File	02/02/2017 22:23:37
COMPATTELRUNNER.EXE-B7A68ECC.pf	24	Regular File	01/02/2017 17:00:47
CONHOST.EXE-0C6456FB.pf	6	Regular File	06/02/2017 19:25:52
CONHOST.EXE-0C6456FB.pf.FileSlack	8	File Slack	

**Properties**

Name	CMD.EXE-0BD30981.pf
File Class	Regular File
File Size	2,547
Physical Size	4,096
Start Cluster	13,715,795
Date Accessed	30/01/2017 22:34:50
Date Created	30/01/2017 22:34:50
Date Modified	02/02/2017 21:24:15
Encrypted	False

**Hex Dump**

Offset	Hex	ASCII
000	4D 41 4D 04 3A 20 00 00-84 97 96 AA A9 98 9B 99	MAM : . . . . .
010	B9 98 AA A0 09 A7 9A AA-A9 98 9B B0 A9 97 80 09	1 . . . . . \$ . . . . .
020	98 87 98 99 A8 88 BB AB-89 77 8A 09 98 97 88 B9	. . . . . >>> . . . . .
030	A8 87 99 A9 A9 97 B9 BB-99 97 A9 0B 99 98 9A BA	. . . . . @ . . . . .
040	98 A8 BB 0A A9 97 99 B0-99 A7 BB 0B B0 A8 00 BB	. . . . . @ . . . . . \$ . . . . .
050	9A 07 0B B0 BA B7 BB A0-09 A7 0A BB 09 97 0A A0	. . . . . . . . . . \$ . . . . .
060	09 98 0B B0 09 98 0B 09-B9 98 00 0B 08 98 0B 90	. . . . . . . . . . . . . . .
070	B8 87 BB BB 09 A8 00 B0-06 98 06 B0 08 98 00 B0	. . . . . . . . . . . . . . .
080	B9 A7 AB 00 B9 98 9A 80-0B 00 00 00 00 00 00	. . . . . \$ << . . . . .
090	00 00 00 00 00 00 00 B0-77 00 0B 00 00 00 00 0B	. . . . . . . . . . . W . . . . .

# Parsing Prefetch

- **PECmd** by Eric Zimmerman

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\ForensicTools\ZimmermanTools\net6>pecmd
Description:
  PECmd version 1.5.0.0

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/PECmd

  Examples: PECmd.exe -f "C:\Temp\CALC.EXE-3FBF7FD.pf"
            PECmd.exe -f "C:\Temp\CALC.EXE-3FBF7FD.pf" --json "D:\jsonOutput" --jsonpretty
            PECmd.exe -d "C:\Temp" -k "system32, fonts"
            PECmd.exe -d "C:\Temp" --csv "c:\temp" --csvf foo.csv --json c:\temp\json
            PECmd.exe -d "C:\Windows\Prefetch"

            Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:
  PECmd [options]

Options:
  -f <f>          File to process. Either this or -d is required
  -d <d>          Directory to recursively process. Either this or -f is required
  -k <k>          Comma separated list of keywords to highlight in output. By default, 'temp' and 'tmp' are highlighted. Any
                  additional keywords will be added to these
  -o <o>          When specified, save prefetch file bytes to the given path. Useful to look at decompressed Win10 files
  -q             Do not dump full details about each file processed. Speeds up processing when using --json or --csv [default:
                  False]
  --json <json>  Directory to save JSON formatted results to. Be sure to include the full path in double quotes
  --jsonf <jsonf> File name to save JSON formatted results to. When present, overrides default name
  --csv <csv>    Directory to save CSV formatted results to. Be sure to include the full path in double quotes
  --csvf <csvf>  File name to save CSV formatted results to. When present, overrides default name
  --html <html>  Directory to save xhtml formatted results to. Be sure to include the full path in double quotes
  --dt <dt>     The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for options [default:
                  yyyy-MM-dd HH:mm:ss]
  --mp          When true, display higher precision for timestamps [default: False]
  --vss         Process all Volume Shadow Copies that exist on drive specified by -f or -d [default: False]
  --dedupe      Deduplicate -f or -d & VSCs based on SHA-1. First file found wins [default: False]
  --debug       Show debug information during processing [default: False]
  --trace       Show trace information during processing [default: False]
```



# Parsing a single PF file

- **PEcmd.exe -f "filename.pf"**

```
C:\Windows\System32\cmd.exe
C:\ForensicTools\ZimmermanTools\net6>pecmd -f e:\Windows\Prefetch\MICROSOFT.PHOTOS.EXE-CD521852.pf
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f e:\Windows\Prefetch\MICROSOFT.PHOTOS.EXE-CD521852.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing e:\Windows\Prefetch\MICROSOFT.PHOTOS.EXE-CD521852.pf

Created on: 2017-01-27 17:23:12
Modified on: 2017-01-27 17:23:36
Last accessed on: 2024-04-07 10:08:09

Executable name: MICROSOFT.PHOTOS.EXE
Hash: CD521852
File size (bytes): 155,634
Version: Windows 10 or Windows 11

Run count: 4
Last run: 2017-01-27 17:23:32
Other run times: 2017-01-27 17:23:28, 2017-01-27 17:23:25, 2017-01-27 17:23:02

Volume information:
#0: Name: \VOLUME{01d2783140af8e9f-14412537} Serial: 14412537 Created: 2017-01-27 00:06:48 Directories: 39 File references: 171
```

# Parsing a single PF file

- PEcmd.exe -f "filename.pf"

```
C:\Windows\System32\cmd.exe
10: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\WINSPOOL.DRV
11: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\VERSION.DLL
12: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\WINDOWS.APPLICATIONMODEL.LOCKSCREEN.DLL
13: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\WINCORLIB.DLL
14: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\EFSWRT.DLL
15: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\MPR.DLL
16: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\TZRES.DLL
17: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\EN-US\TZRES.DLL.MUI
18: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\EN-US\WINDOWS.STORAGE.DLL.MUI
19: \VOLUME{01d2783140af8e9f-14412537}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\CVERSIONS.2.DB
20: \VOLUME{01d2783140af8e9f-14412537}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.VER0X0000000000000001.DB
21: \VOLUME{01d2783140af8e9f-14412537}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.VER0X0000000000000001.DB
22: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\EN-US\WINDOWS.UI.XAML.DLL.MUI
23: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\TWINAPI.DLL
24: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SERVICEPROFILES\LOCALSERVICE\APPDATA\LOCAL\FONTCACHE\~FONTCACHE-SYSTEM.DAT
25: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SERVICEPROFILES\LOCALSERVICE\APPDATA\LOCAL\FONTCACHE\~FONTCACHE-FONTFACE.DAT
26: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SERVICEPROFILES\LOCALSERVICE\APPDATA\LOCAL\FONTCACHE\~FONTCACHE-S-1-5-21-929903582-3707417421-3176878646-1002.DAT
27: \VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.511.8780.0_X64__8WEKYB3D8BBWE\APPCS\ASSETS\PHOTOMDL2.1.61.TTF
28: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\FONTS\SEGOEUI.TTF
29: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\FONTS\SEGMDL2.TTF
30: \VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\DESKTOP\PETS\SNOWY OWL.JPG
31: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\PHOTOMETADATAHANDLER.DLL
32: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\EN-US\KERNELBASE.DLL.MUI
33: \VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\DESKTOP\PETS\PYGMY OWL.JPG
34: \VOLUME{01d2783140af8e9f-14412537}\$MFT
35: \VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\LOGONCLI.DLL
36: \VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\DESKTOP\PETS\GREAT HORNED OWL.JPG
```



# Parsing a folder

- **PEcmd.exe -d <PATH-TO-FOLDER> --csv <PATH-TO-OUTPUT> -q**

```
C:\Windows\System32\cmd.exe
C:\ForensicTools\ZimmermanTools\net6>pecmd -d e:\Windows\Prefetch\ --csv D:\UNIGE\EXTRACTED\ -q
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -d e:\Windows\Prefetch\ --csv D:\UNIGE\EXTRACTED\ -q

Warning: Administrator privileges not found!

Keywords: temp, tmp

Looking for prefetch files in e:\Windows\Prefetch\

Found 225 Prefetch files

----- Processed e:\Windows\Prefetch\56.0.2924.87_56.0.2924.76_CHR-D7B50B6D.pf in 0.00552420 seconds -----
----- Processed e:\Windows\Prefetch\ACCELEROMETERST.EXE-41616180.pf in 0.00021120 seconds -----
----- Processed e:\Windows\Prefetch\AM_DELTA.EXE-78CA83B0.pf in 0.00024460 seconds -----
----- Processed e:\Windows\Prefetch\AM_DELTA_PATCH_1.235.1383.0.E-789A3F12.pf in 0.00011460 seconds -----
----- Processed e:\Windows\Prefetch\AM_DELTA_PATCH_1.235.1750.0.E-CF523DC0.pf in 0.00013780 seconds -----
----- Processed e:\Windows\Prefetch\APPCMD.EXE-047C9281.pf in 0.00017480 seconds -----
----- Processed e:\Windows\Prefetch\APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf in 0.00032730 seconds -----
----- Processed e:\Windows\Prefetch\ASPNETCA.EXE-571146CF.pf in 0.00018710 seconds -----
----- Processed e:\Windows\Prefetch\ASPNETCA.EXE-575DB5A8.pf in 0.00019220 seconds -----
----- Processed e:\Windows\Prefetch\ASPNET_REGIIS.EXE-8545410E.pf in 0.00023090 seconds -----
----- Processed e:\Windows\Prefetch\ASPNET_REGIIS.EXE-E7D16D20.pf in 0.00022700 seconds -----
----- Processed e:\Windows\Prefetch\AUDIODG.EXE-AB22E9A6.pf in 0.00016980 seconds -----
----- Processed e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-45FE2909.pf in 0.00096500 seconds -----
----- Processed e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-897AD46E.pf in 0.00027940 seconds -----
----- Processed e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-BE112A50.pf in 0.00040290 seconds -----
----- Processed e:\Windows\Prefetch\BROWSER_BROKER.EXE-EEC8D935.pf in 0.00025970 seconds -----
----- Processed e:\Windows\Prefetch\BYTECODEGENERATOR.EXE-62D6B3D7.pf in 0.00021040 seconds -----
----- Processed e:\Windows\Prefetch\BYTECODEGENERATOR.EXE-FB938A53.pf in 0.00022130 seconds -----
----- Processed e:\Windows\Prefetch\CHRMSTP.EXE-B1C7BB6B.pf in 0.00032160 seconds -----
----- Processed e:\Windows\Prefetch\CHRMSTP.EXE-B1C7BB72.pf in 0.00019250 seconds -----
----- Processed e:\Windows\Prefetch\CHROME.EXE-5349D2D7.pf in 0.00065770 seconds -----
----- Processed e:\Windows\Prefetch\CHROME.EXE-5349D2D8.pf in 0.00029600 seconds -----
----- Processed e:\Windows\Prefetch\CHROME.EXE-5349D2D9.pf in 0.00039610 seconds -----
----- Processed e:\Windows\Prefetch\CHROME.EXE-5349D2DA.pf in 0.00031200 seconds -----
----- Processed e:\Windows\Prefetch\CHROME.EXE-5349D2DD.pf in 0.00023530 seconds -----
----- Processed e:\Windows\Prefetch\CHROME.EXE-5349D2DE.pf in 0.00019020 seconds -----
----- Processed e:\Windows\Prefetch\CHROME.EXE-5349D2DF.pf in 0.00056090 seconds -----
----- Processed e:\Windows\Prefetch\CLIPUP.EXE-4C5C7B66.pf in 0.00022140 seconds -----
----- Processed e:\Windows\Prefetch\CMD.EXE-0BD30981.pf in 0.00010130 seconds -----
----- Processed e:\Windows\Prefetch\CMD.EXE-6D6290C5.pf in 0.00011150 seconds -----
----- Processed e:\Windows\Prefetch\COMPATTELRUNNER.EXE-B7A68ECC.pf in 0.00257130 seconds -----
Error opening e:\Windows\Prefetch\CONHOST.EXE-0C6456FB.pf. Message: Invalid signature! Should be 'SCCA'
System.Exception: Invalid signature! Should be 'SCCA'
```



# Parsing a folder

Extracted\_Files > prefetch

Name	Date modified	Type	Size
20200423075719_PECmd_Output_for_D_UNIGE_2020_Extracted_Files_prefetch	23/04/2020 09:57	File folder	
20200423075719_PECmd_Output.csv	23/04/2020 09:57	Microsoft Excel C...	1.088 KB
20200423075719_PECmd_Output_Timeline.csv	23/04/2020 09:57	Microsoft Excel C...	8 KB

L...	Tag	Note	Source Filename	Volume1Ser...	Source Created	Source Modified	Executable Name	Run Count	Hash	Size	Version	Last Run
1			e:\Windows\Prefetch\56.0.2924.87_56.0.2924.76_C...		2017-02-02 21:25:54	2017-02-02 21:25:54	56.0.2924.87_56.0.2924.76_CHR	1	D7B50B6D	36808	Windows ...	2017-02-02 21:25:44
2			e:\Windows\Prefetch\ACCELEROMETERST.EXE-4161618...		2017-01-30 18:46:42	2017-02-02 21:24:51	ACCELEROMETERST.EXE	5	41616180	29360	Windows ...	2017-02-02 21:24:40
3			e:\Windows\Prefetch\AM_DELTA.EXE-78CA83B0.pf		2017-01-30 18:47:35	2017-02-02 21:26:44	AM_DELTA.EXE	3	78CA83B0	45236	Windows ...	2017-02-02 21:26:33
4			e:\Windows\Prefetch\AM_DELTA_PATCH_1.235.1383.0...		2017-01-27 17:13:25	2017-01-27 17:13:25	AM_DELTA_PATCH_1.235.1383.0.E	1	789A3F12	14882	Windows ...	2017-01-27 17:13:15
5			e:\Windows\Prefetch\AM_DELTA_PATCH_1.235.1750.0...		2017-02-01 16:59:03	2017-02-01 16:59:03	AM_DELTA_PATCH_1.235.1750.0.E	1	CF523DC0	15770	Windows ...	2017-02-01 16:58:53
6			e:\Windows\Prefetch\APPCMD.EXE-047C9281.pf		2017-01-27 02:43:22	2017-01-27 02:43:23	APPCMD.EXE	5	47C9281	25282	Windows ...	2017-01-27 02:43:23
7			e:\Windows\Prefetch\APPLICATIONFRAMEHOST.EXE-8C...		2017-01-27 17:22:31	2017-02-02 22:00:50	APPLICATIONFRAMEHOST.EXE	7	8CE9A1EE	50612	Windows ...	2017-02-02 22:00:40
8			e:\Windows\Prefetch\ASPNETCA.EXE-571146CF.pf		2017-01-27 02:43:29	2017-01-27 02:43:29	ASPNETCA.EXE	1	571146CF	24844	Windows ...	2017-01-27 02:43:28
9			e:\Windows\Prefetch\ASPNETCA.EXE-575DB5AB.pf		2017-01-27 02:43:27	2017-01-27 02:43:27	ASPNETCA.EXE	1	575DB5AB	25602	Windows ...	2017-01-27 02:43:26
10			e:\Windows\Prefetch\ASPNET_REGIIS.EXE-8545410E...		2017-01-27 02:43:33	2017-01-27 02:43:33	ASPNET_REGIIS.EXE	1	8545410E	34884	Windows ...	2017-01-27 02:43:32
11			e:\Windows\Prefetch\ASPNET_REGIIS.EXE-E7D16D20...		2017-01-27 02:43:34	2017-01-27 02:43:34	ASPNET_REGIIS.EXE	1	E7D16D20	34848	Windows ...	2017-01-27 02:43:33
12			e:\Windows\Prefetch\AUDIODG.EXE-AB22E9A6.pf		2017-01-27 16:57:20	2017-02-01 17:31:21	AUDIODG.EXE	6	AB22E9A6	22530	Windows ...	2017-02-01 17:31:11
13			e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-45FE...		2017-01-27 17:17:04	2017-02-02 22:49:09	BACKGROUNDTASKHOST.EXE	13	45FE2909	132288	Windows ...	2017-02-02 22:48:59
14			e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-897A...		2017-01-30 19:20:40	2017-01-31 19:14:12	BACKGROUNDTASKHOST.EXE	3	897AD46E	36294	Windows ...	2017-01-31 19:14:12
15			e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-BE11...		2017-01-27 17:22:19	2017-02-02 22:48:53	BACKGROUNDTASKHOST.EXE	6	BE112A50	48004	Windows ...	2017-02-02 22:48:53
16			e:\Windows\Prefetch\BROWSER_BROKER.EXE-EEC8D935...		2017-01-27 17:22:27	2017-02-02 22:39:18	BROWSER_BROKER.EXE	6	EEC8D935	32396	Windows ...	2017-02-02 22:39:08
17			e:\Windows\Prefetch\BYTECODEGENERATOR.EXE-62D6B...		2017-01-27 17:12:36	2017-01-27 17:35:17	BYTECODEGENERATOR.EXE	10	62D6B3D7	16526	Windows ...	2017-01-27 17:35:16
18			e:\Windows\Prefetch\BYTECODEGENERATOR.EXE-FB938...		2017-01-27 17:13:30	2017-01-27 17:35:20	BYTECODEGENERATOR.EXE	3	FB938A53	14236	Windows ...	2017-01-27 17:35:19
19			e:\Windows\Prefetch\CHRMSTP.EXE-B1C7BB6B.pf		2017-01-27 16:54:51	2017-01-27 16:54:51	CHRMSTP.EXE	1	B1C7BB6B	42686	Windows ...	2017-01-27 16:54:50
20			e:\Windows\Prefetch\CHRMSTP.EXE-B1C7BB72.pf		2017-01-27 16:54:51	2017-01-27 16:54:51	CHRMSTP.EXE	1	B1C7BB72	22610	Windows ...	2017-01-27 16:54:50
21			e:\Windows\Prefetch\CHROME.EXE-5349D2D7.pf		2017-01-27 16:57:59	2017-02-02 21:57:10	CHROME.EXE	13	5349D2D7	138304	Windows ...	2017-02-02 21:57:10
22			e:\Windows\Prefetch\CHROME.EXE-5349D2D8.pf		2017-01-27 16:58:06	2017-02-02 22:49:15	CHROME.EXE	62	5349D2D8	43132	Windows ...	2017-02-02 22:49:15
23			e:\Windows\Prefetch\CHROME.EXE-5349D2D9.pf		2017-01-27 16:58:05	2017-02-02 21:57:10	CHROME.EXE	14	5349D2D9	61966	Windows ...	2017-02-02 21:57:10
24			e:\Windows\Prefetch\CHROME.EXE-5349D2DA.pf		2017-01-27 17:01:43	2017-02-01 17:05:23	CHROME.EXE	10	5349D2DA	53532	Windows ...	2017-02-01 17:05:13
25			e:\Windows\Prefetch\CHROME.EXE-5349D2DD.pf		2017-01-27 16:58:04	2017-02-02 21:57:20	CHROME.EXE	16	5349D2DD	34832	Windows ...	2017-02-02 21:57:10
26			e:\Windows\Prefetch\CHROME.EXE-5349D2DE.pf		2017-01-27 16:58:03	2017-02-02 21:57:20	CHROME.EXE	16	5349D2DE	27458	Windows ...	2017-02-02 21:57:10
27			e:\Windows\Prefetch\CHROME.EXE-5349D2DF.pf		2017-01-27 16:58:43	2017-02-02 21:57:56	CHROME.EXE	24	5349D2DF	108842	Windows ...	2017-02-02 21:57:56
28			e:\Windows\Prefetch\CLIPUP.EXE-4C5C7B66.pf		2017-01-27 02:47:59	2017-01-27 16:54:45	CLIPUP.EXE	5	4C5C7B66	31608	Windows ...	2017-01-27 16:54:44
29			e:\Windows\Prefetch\CMD.EXE-0BD30981.pf		2017-01-30 22:34:50	2017-02-02 21:24:15	CMD.EXE	7	BD30981	8250	Windows ...	2017-02-02 21:24:15
30			e:\Windows\Prefetch\CMD.EXE-6D6290C5.pf		2017-02-02 22:25:27	2017-02-02 22:25:37	CMD.EXE	6	6D6290C5	12480	Windows ...	2017-02-02 22:25:37
31			e:\Windows\Prefetch\COMPATTELRunner.EXE-B7A68EC...		2017-01-27 02:48:31	2017-02-01 17:00:47	COMPATTELRunner.EXE	7	B7A68ECC	153870	Windows ...	2017-02-01 17:00:46
32			e:\Windows\Prefetch\CONSENT.EXE-40419367.pf		2017-01-27 16:54:36	2017-02-02 21:24:15	CONSENT.EXE	4	40419367	35262	Windows ...	2017-02-02 21:24:15
33			e:\Windows\Prefetch\CREDENTIALUIBROKER.EXE-8CED...		2017-01-30 22:40:07	2017-01-30 22:40:07	CREDENTIALUIBROKER.EXE	1	8CEDA3EB	104982	Windows ...	2017-01-30 22:40:04

# Parsing a folder

Extracted\_Files > prefetch

Name	Date modified	Type	Size
20200423075719_PECmd_Output_for_D_UNIGE_2020_Extracted_Files_prefetch	23/04/2020 09:57	File folder	
20200423075719_PECmd_Output.csv	23/04/2020 09:57	Microsoft Excel C...	1.088 KB
20200423075719_PECmd_Output_Timeline.csv	23/04/2020 09:57	Microsoft Excel C...	8 KB

L...	Tag	Note	Source Filename	Volume1Ser...	Source Created	Source Modified	Executable Name	Run Count	Hash	Size	Version	Last Run
1			e:\Windows\Prefetch\56.0.2924.87_56.0.2924.76_C...		2017-02-02 21:25:54	2017-02-02 21:25:54	56.0.2924.87_56.0.2924.76_CHR	1	D7B50B6D	36808	Windows ...	2017-02-02 21:25:44
2			e:\Windows\Prefetch\ACCELEROMETERST.EXE-4161618...		2017-01-30 18:46:42	2017-02-02 21:24:51	ACCELEROMETERST.EXE	5	41616180	29360	Windows ...	2017-02-02 21:24:40
3			e:\Windows\Prefetch\AM_DELTA.EXE-78CA83B0.pf		2017-01-30 18:47:35	2017-02-02 21:26:44	AM_DELTA.EXE	3	78CA83B0	45236	Windows ...	2017-02-02 21:26:33
4			e:\Windows\Prefetch\AM_DELTA_PATCH_1.235.1383.0...		2017-01-27 17:13:25	2017-01-27 17:13:25	AM_DELTA_PATCH_1.235.1383.0.E	1	789A3F12	14882	Windows ...	2017-01-27 17:13:15
5			e:\Windows\Prefetch\AM_DELTA_PATCH_1.235.1750.0...		2017-02-01 16:59:03	2017-02-01 16:59:03	AM_DELTA_PATCH_1.235.1750.0.E	1	CF523DC0	15770	Windows ...	2017-02-01 16:58:53
6			e:\Windows\Prefetch\APPCMD.EXE-047C9281.pf		2017-01-27 02:43:22	2017-01-27 02:43:23	APPCMD.EXE	5	47C9281	25282	Windows ...	2017-01-27 02:43:23
7			e:\Windows\Prefetch\APPLICATIONFRAMEHOST.EXE-8C...		2017-01-27 17:22:31	2017-02-02 22:00:50	APPLICATIONFRAMEHOST.EXE	7	8CE9A1EE	50612	Windows ...	2017-02-02 22:00:40
8			e:\Windows\Prefetch\ASPNETCA.EXE-571146CF.pf		2017-01-27 02:43:29	2017-01-27 02:43:29	ASPNETCA.EXE	1	571146CF	24844	Windows ...	2017-01-27 02:43:28
9			e:\Windows\Prefetch\ASPNETCA.EXE-575DB5AB.pf		2017-01-27 02:43:27	2017-01-27 02:43:27	ASPNETCA.EXE	1	575DB5AB	25602	Windows ...	2017-01-27 02:43:26
10			e:\Windows\Prefetch\ASPNET_REGIIS.EXE-8545410E...		2017-01-27 02:43:33	2017-01-27 02:43:33	ASPNET_REGIIS.EXE	1	8545410E	34884	Windows ...	2017-01-27 02:43:32
11			e:\Windows\Prefetch\ASPNET_REGIIS.EXE-E7D16D20...		2017-01-27 02:43:34	2017-01-27 02:43:34	ASPNET_REGIIS.EXE	1	E7D16D20	34848	Windows ...	2017-01-27 02:43:33
12			e:\Windows\Prefetch\AUDIODG.EXE-AB22E9A6.pf		2017-01-27 16:57:20	2017-02-01 17:31:21	AUDIODG.EXE	6	AB22E9A6	22530	Windows ...	2017-02-01 17:31:11
13			e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-45FE...		2017-01-27 17:17:04	2017-02-02 22:49:09	BACKGROUNDTASKHOST.EXE	13	45FE2909	132288	Windows ...	2017-02-02 22:48:59
14			e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-897A...		2017-01-30 19:20:40	2017-01-31 19:14:12	BACKGROUNDTASKHOST.EXE	3	897AD46E	36294	Windows ...	2017-01-31 19:14:12
15			e:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-BE11...		2017-01-27 17:22:19	2017-02-02 22:48:53	BACKGROUNDTASKHOST.EXE	6	BE112A50	48004	Windows ...	2017-02-02 22:48:53
16			e:\Windows\Prefetch\BROWSER_BROKER.EXE-EEC8D935...		2017-01-27 17:22:27	2017-02-02 22:39:18	BROWSER_BROKER.EXE	6	EEC8D935	32396	Windows ...	2017-02-02 22:39:08
17			e:\Windows\Prefetch\BYTECODEGENERATOR.EXE-62D6B...		2017-01-27 17:12:36	2017-01-27 17:35:17	BYTECODEGENERATOR.EXE	10	62D6B3D7	16526	Windows ...	2017-01-27 17:35:16
18			e:\Windows\Prefetch\BYTECODEGENERATOR.EXE-FB938...		2017-01-27 17:13:30	2017-01-27 17:35:20	BYTECODEGENERATOR.EXE	3	FB938A53	14236	Windows ...	2017-01-27 17:35:19
19			e:\Windows\Prefetch\CHRMSTP.EXE-B1C7BB6B.pf		2017-01-27 16:54:51	2017-01-27 16:54:51	CHRMSTP.EXE	1	B1C7BB6B	42686	Windows ...	2017-01-27 16:54:50
20			e:\Windows\Prefetch\CHRMSTP.EXE-B1C7BB72.pf		2017-01-27 16:54:51	2017-01-27 16:54:51	CHRMSTP.EXE	1	B1C7BB72	22610	Windows ...	2017-01-27 16:54:50
21			e:\Windows\Prefetch\CHROME.EXE-5349D2D7.pf		2017-01-27 16:57:59	2017-02-02 21:57:10	CHROME.EXE	13	5349D2D7	138304	Windows ...	2017-02-02 21:57:10
22			e:\Windows\Prefetch\CHROME.EXE-5349D2D8.pf		2017-01-27 16:58:06	2017-02-02 22:49:15	CHROME.EXE	62	5349D2D8	43132	Windows ...	2017-02-02 22:49:15
23			e:\Windows\Prefetch\CHROME.EXE-5349D2D9.pf		2017-01-27 16:58:05	2017-02-02 21:57:10	CHROME.EXE	14	5349D2D9	61966	Windows ...	2017-02-02 21:57:10
24			e:\Windows\Prefetch\CHROME.EXE-5349D2DA.pf		2017-01-27 17:01:43	2017-02-01 17:05:23	CHROME.EXE	10	5349D2DA	53532	Windows ...	2017-02-01 17:05:13
25			e:\Windows\Prefetch\CHROME.EXE-5349D2DD.pf		2017-01-27 16:58:04	2017-02-02 21:57:20	CHROME.EXE	16	5349D2DD	34832	Windows ...	2017-02-02 21:57:10
26			e:\Windows\Prefetch\CHROME.EXE-5349D2DE.pf		2017-01-27 16:58:03	2017-02-02 21:57:20	CHROME.EXE	16	5349D2DE	27458	Windows ...	2017-02-02 21:57:10
27			e:\Windows\Prefetch\CHROME.EXE-5349D2DF.pf		2017-01-27 16:58:43	2017-02-02 21:57:56	CHROME.EXE	24	5349D2DF	108842	Windows ...	2017-02-02 21:57:56
28			e:\Windows\Prefetch\CLIPUP.EXE-4C5C7B66.pf		2017-01-27 02:47:59	2017-01-27 16:54:45	CLIPUP.EXE	5	4C5C7B66	31608	Windows ...	2017-01-27 16:54:44
29			e:\Windows\Prefetch\CMD.EXE-0BD30981.pf		2017-01-30 22:34:50	2017-02-02 21:24:15	CMD.EXE	7	BD30981	8250	Windows ...	2017-02-02 21:24:15
30			e:\Windows\Prefetch\CMD.EXE-6D6290C5.pf		2017-02-02 22:25:27	2017-02-02 22:25:37	CMD.EXE	6	6D6290C5	12480	Windows ...	2017-02-02 22:25:37
31			e:\Windows\Prefetch\COMPATTELRunner.EXE-B7A68EC...		2017-01-27 02:48:31	2017-02-01 17:00:47	COMPATTELRunner.EXE	7	B7A68ECC	153870	Windows ...	2017-02-01 17:00:46
32			e:\Windows\Prefetch\CONSENT.EXE-40419367.pf		2017-01-27 16:54:36	2017-02-02 21:24:15	CONSENT.EXE	4	40419367	35262	Windows ...	2017-02-02 21:24:15
33			e:\Windows\Prefetch\CREDENTIALUIBROKER.EXE-8CED...		2017-01-30 22:40:07	2017-01-30 22:40:07	CREDENTIALUIBROKER.EXE	1	8CEDA3EB	104982	Windows ...	2017-01-30 22:40:04

# Parsing a folder

Extracted\_Files > prefetch

Name	Date modified	Type	Size
20200423075719_PECmd_Output_for_D_UNIGE_2020_Extracted_Files_prefetch	23/04/2020 09:57	File folder	
20200423075719_PECmd_Output.csv	23/04/2020 09:57	Microsoft Excel C...	1.088 KB
20200423075719_PECmd_Output_Timeline.csv	23/04/2020 09:57	Microsoft Excel C...	8 KB



Line	Tag	Run Time	Executable Name
379		2017-02-02 22:00:41	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
528		2017-02-02 22:01:10	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\RUNDLL32.EXE
700		2017-02-02 22:05:12	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SVCHOST.EXE
737		2017-02-02 22:05:21	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\IMMERSIVECONTROL PANEL\SYSTEMSETTINGS.EXE
810		2017-02-02 22:05:22	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\WIFITASK.EXE
378		2017-02-02 22:05:31	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
655		2017-02-02 22:07:18	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SVCHOST.EXE
81		2017-02-02 22:07:25	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
566		2017-02-02 22:11:28	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SEARCHFILTERHOST.EXE
578		2017-02-02 22:11:28	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SEARCHPROTOCOLHOST.EXE
678		2017-02-02 22:12:11	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SVCHOST.EXE
80		2017-02-02 22:23:43	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
565		2017-02-02 22:25:03	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SEARCHFILTERHOST.EXE
577		2017-02-02 22:25:03	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SEARCHPROTOCOLHOST.EXE
624		2017-02-02 22:25:10	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\SMARTSCREEN.EXE
869		2017-02-02 22:25:11	YAHOO-MESSENGER-0.8.288-WIN32
790		2017-02-02 22:25:12	\VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\APPDATA\LOCAL\SQUIRRELTEMP\UPDATE.EXE
862		2017-02-02 22:25:20	\VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\APPDATA\LOCAL\YAHOOMESSENGER\APP-0.8.288\YAHOO MESSENGER.EXE
518		2017-02-02 22:25:23	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSDOW64\REG.EXE
789		2017-02-02 22:25:23	\VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\APPDATA\LOCAL\YAHOOMESSENGER\UPDATE.EXE
868		2017-02-02 22:25:23	\VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\APPDATA\LOCAL\YAHOOMESSENGER\APP-0.8.288\YAHOO MESSENGER.EXE
198		2017-02-02 22:25:25	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSTEM32\DLLHOST.EXE
861		2017-02-02 22:25:25	\VOLUME{01d2783140af8e9f-14412537}\USERS\SARAH M\APPDATA\LOCAL\YAHOOMESSENGER\APP-0.8.288\YAHOO MESSENGER.EXE
838		2017-02-02 22:25:26	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSDOW64\WBEM\WMIC.EXE
140		2017-02-02 22:25:27	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSDOW64\CMD.EXE
141		2017-02-02 22:25:27	\VOLUME{01d2783140af8e9f-14412537}\WINDOWS\SYSDOW64\CMD.EXE

# Exercise 10

1. When was **Google Chrome** executed for the **last time**?
2. When was **Microsoft Photos** executed for the **last time**?
3. When was **Skype** executed for the **last time**?



# Exercise 10.1

Line	Tag	Run Time	Executable Name
=	<input type="checkbox"/>	=	chrome
125	<input type="checkbox"/>	2017-01-31 19:15:53	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
113	<input type="checkbox"/>	2017-02-01 16:57:11	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
88	<input type="checkbox"/>	2017-02-01 16:57:12	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
105	<input type="checkbox"/>	2017-02-01 16:57:12	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
124	<input type="checkbox"/>	2017-02-01 16:57:58	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
123	<input type="checkbox"/>	2017-02-01 17:00:03	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
122	<input type="checkbox"/>	2017-02-01 17:03:13	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
94	<input type="checkbox"/>	2017-02-01 17:05:13	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
112	<input type="checkbox"/>	2017-02-01 19:09:34	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
87	<input type="checkbox"/>	2017-02-01 19:09:35	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
104	<input type="checkbox"/>	2017-02-01 19:09:35	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
84	<input type="checkbox"/>	2017-02-01 19:09:36	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
85	<input type="checkbox"/>	2017-02-01 19:09:36	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
121	<input type="checkbox"/>	2017-02-01 19:10:21	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
590	<input type="checkbox"/>	2017-02-02 21:25:44	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\56.0.2924.76\INSTALLER\SETUP.EXE
591	<input type="checkbox"/>	2017-02-02 21:25:44	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\56.0.2924.76\INSTALLER\SETUP.EXE
71	<input type="checkbox"/>	2017-02-02 21:28:24	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
103	<input type="checkbox"/>	2017-02-02 21:28:25	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
111	<input type="checkbox"/>	2017-02-02 21:28:25	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
83	<input type="checkbox"/>	2017-02-02 21:28:26	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
120	<input type="checkbox"/>	2017-02-02 21:29:11	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
119	<input type="checkbox"/>	2017-02-02 21:35:08	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
70	<input type="checkbox"/>	2017-02-02 21:57:10	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
82	<input type="checkbox"/>	2017-02-02 21:57:10	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
86	<input type="checkbox"/>	2017-02-02 21:57:10	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
102	<input type="checkbox"/>	2017-02-02 21:57:10	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
110	<input type="checkbox"/>	2017-02-02 21:57:10	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
118	<input type="checkbox"/>	2017-02-02 21:57:56	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
81	<input type="checkbox"/>	2017-02-02 22:07:25	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
80	<input type="checkbox"/>	2017-02-02 22:23:43	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
79	<input type="checkbox"/>	2017-02-02 22:42:30	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
78	<input type="checkbox"/>	2017-02-02 22:49:15	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE

# Exercise 10.2

Line	Tag	Run Time	Executable Name
=	<input type="checkbox"/>	=	photos
389	<input type="checkbox"/>	2017-01-27 17:23:02	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.511.8780.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
388	<input type="checkbox"/>	2017-01-27 17:23:25	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.511.8780.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
387	<input type="checkbox"/>	2017-01-27 17:23:28	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.511.8780.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
386	<input type="checkbox"/>	2017-01-27 17:23:32	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.511.8780.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
385	<input type="checkbox"/>	2017-01-27 17:30:54	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
384	<input type="checkbox"/>	2017-01-28 22:09:25	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
383	<input type="checkbox"/>	2017-01-30 22:56:34	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
382	<input type="checkbox"/>	2017-01-31 19:36:24	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
381	<input type="checkbox"/>	2017-01-31 19:36:44	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
380	<input type="checkbox"/>	2017-02-01 17:31:09	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
379	<input type="checkbox"/>	2017-02-02 22:00:41	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE
378	<input type="checkbox"/>	2017-02-02 22:05:31	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.WINDOWS.PHOTOS_16.1118.10000.0_X64__8WEKYB3D8BBWE\MICROSOFT.PHOTOS.EXE

# Exercise 10.3

Line	Tag	Run Time	Executable Name
=	<input type="checkbox"/>	=	skype
612	<input type="checkbox"/>	2017-01-30 18:47:50	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\PHONE\SKYPE.EXE
792	<input type="checkbox"/>	2017-01-30 18:48:07	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\UPDATER\UPDATER.EXE
620	<input type="checkbox"/>	2017-01-30 18:51:25	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
611	<input type="checkbox"/>	2017-01-30 18:51:31	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\PHONE\SKYPE.EXE
619	<input type="checkbox"/>	2017-01-30 18:52:09	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
618	<input type="checkbox"/>	2017-01-30 18:52:51	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
610	<input type="checkbox"/>	2017-01-30 19:20:39	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\PHONE\SKYPE.EXE
617	<input type="checkbox"/>	2017-01-30 19:20:41	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
609	<input type="checkbox"/>	2017-01-31 18:59:38	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\PHONE\SKYPE.EXE
616	<input type="checkbox"/>	2017-01-31 18:59:51	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
791	<input type="checkbox"/>	2017-01-31 18:59:52	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\UPDATER\UPDATER.EXE
615	<input type="checkbox"/>	2017-01-31 19:01:05	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
608	<input type="checkbox"/>	2017-01-31 19:01:08	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\PHONE\SKYPE.EXE
614	<input type="checkbox"/>	2017-01-31 19:01:09	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
613	<input type="checkbox"/>	2017-01-31 19:01:14	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\BROWSER\SKYPEBROWSERHOST.EXE
607	<input type="checkbox"/>	2017-01-31 19:26:31	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\PHONE\SKYPE.EXE
606	<input type="checkbox"/>	2017-01-31 20:01:41	\VOLUME{01d2783140af8e9f-14412537}\PROGRAM FILES (X86)\SKYPE\PHONE\SKYPE.EXE

# Internet Browsers

- More than one browser can be installed on a system
- Most commonly used browsers are:
  - **Google Chrome**
  - **Microsoft Edge**
  - **Mozilla Firefox**
- We can recover:
  - **History**
  - **Cache**
  - **Cookies**
  - **Filled forms**
  - **And more...**



# Google Chrome

- User data stored in

**C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default**

- Data stored in **SQLite databases**

- Most relevant

- **History**
- **Cookies**
- **Last Session**
- **Last Tabs**
- **Login Data**

**Evidence Tree**

- Sarah M
  - AppData
    - Local
      - ActiveSync
      - Application Data
      - Comms
      - Conexant
      - ConnectedDevicesPlatform
      - DigitalPersona
      - Google
        - Chrome
          - User Data
            - CertificateTransparency
            - Crashpad
            - Default
              - Cache
              - data\_reduction\_proxy\_leveldb
              - databases
              - Extension Rules
              - Extension State
              - Extensions
              - File System
              - GPUCache
              - IndexedDB
              - JumpListIcons
              - JumpListIconsOld
              - Local Extension Settings
              - Local Storage

**File List**

Name	Size	Type	Date Modified
Cache	1	Directory	02/02/2017 22:53:15
databases	1	Directory	27/01/2017 00:55:19
data_reduction_proxy_leveldb	1	Directory	02/02/2017 21:57:10
Extension Rules	1	Directory	27/01/2017 00:56:22
Extension State	1	Directory	02/02/2017 21:57:12
Extensions	1	Directory	27/01/2017 00:56:44
File System	1	Directory	28/01/2017 21:54:33
GPUCache	1	Directory	27/01/2017 00:55:11
IndexedDB	1	Directory	02/02/2017 21:28:28
JumpListIcons	1	Directory	02/02/2017 22:53:05
JumpListIconsOld	1	Directory	02/02/2017 22:48:17
Local Extension Settings	1	Directory	27/01/2017 00:55:28
Local Storage	1	Directory	02/02/2017 22:53:17
Media Cache	1	Directory	02/02/2017 22:50:02
Pepper Data	1	Directory	27/01/2017 01:13:25
Platform Notifications	1	Directory	27/01/2017 17:14:15
Service Worker	1	Directory	27/01/2017 00:55:26
Session Storage	1	Directory	02/02/2017 22:53:16
Sync Extension Settings	1	Directory	27/01/2017 00:55:35
Web Applications	1	Directory	27/01/2017 00:55:22
120	16	NTFS Index All	02/02/2017 22:53:16
Cookies	768	Regular File	02/02/2017 22:53:16
Cookies-journal	0	Regular File	02/02/2017 22:53:16
Cookies.FileSlack	16	File Slack	
Current Session	150	Regular File	02/02/2017 22:53:16
Current Tabs	155	Regular File	02/02/2017 22:53:16
DownloadMetadata	5	Regular File	02/02/2017 22:25:10
Favicons	352	Regular File	02/02/2017 22:52:48
Favicons-journal	0	Regular File	02/02/2017 22:52:48
Favicons.FileSlack	16	File Slack	
Google Profile.ico	173	Regular File	27/01/2017 00:55:06
History	384	Regular File	02/02/2017 22:53:16
History Provider Cache	227	Regular File	02/02/2017 22:53:16
History-journal	0	Regular File	02/02/2017 22:53:16
History.FileSlack	12	File Slack	
Last Session	1,075	Regular File	02/02/2017 21:57:08
Last Tabs	76	Regular File	02/02/2017 21:57:08
Login Data	18	Regular File	02/02/2017 22:50:04
Login Data-journal	0	Regular File	02/02/2017 22:50:04
Network Action Predictor	72	Regular File	02/02/2017 22:49:18
Network Action Predictor-journal	0	Regular File	02/02/2017 22:49:18
Network Persistent State	1	Regular File	02/02/2017 22:24:11
Origin Bound Certs	20	Regular File	01/02/2017 17:06:45
Origin Bound Certs-journal	0	Regular File	01/02/2017 17:06:45
Preferences	149	Regular File	02/02/2017 22:53:16

**Properties**

Name	Default
File Class	Directory
File Size	432
Physical Size	432
Date Accessed	02/02/2017 22:53:16
Date Created	27/01/2017 00:55:05
Date Modified	02/02/2017 22:53:16
Encrypted	False
Compressed	False
Actual File	True
Alternate Data Stream Count	1
<b>DOS Attributes</b>	
Hidden	False
System	False
Read only	False
Archive	False

# Parsing Google Chrome

- **Hindsight** by Ryan Benson  
(<https://github.com/obsidianforensics/hindsight>)

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

D:\UNIGE\TOOLS>hindsight.exe -i "E:\Users\Sarah M\AppData\Local\Google\Chrome\User Data\Default" -o "D:\UNIGE\EXTRACTED"

#####

             _   _       _   _       _   _ 
            | | | |     | | | |     | | | |
            |_|_|_|_    |_|_|_|_    |_|_|_|_
           / \ / \ / \ / \ / \ / \ / \ / \
          /___/___/___/___/___/___/___/___
         by @_RyanBenson      |_/ v2023.03

#####

Start time: 2024-04-07 12:29:05.483
Input directory: E:\Users\Sarah M\AppData\Local\Google\Chrome\User Data\Default
Output name: D:\UNIGE\EXTRACTED.xlsx

Processing:

Profile: E:\Users\Sarah M\AppData\Local\Google\Chrome\User Data\Default
Detected Chrome version: [ 54-58 ]
URL records: [ 793 ]
Download records: [ 34 ]
Cache records: [ 8237 ]
GPU Cache records: [ 54 ]
Media Cache records: [ 57 ]
Cookie records: [ 1795 ]
Autofill records: [ 13 ]
Local Storage records: [ 247 ]
Session Storage records: [ 212 ]
Extensions: [ 10 ]
```

# Parsing Google Chrome

	A	B	C	D	E	F
1	Hindsight Internet History Forensics (v2023.03)					
2	Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path	Interpretation
7	url	2017-01-27 00:55:15.267	http://tools.google.com/chrome/intl/en/welcome.html	Getting Started		
8	url	2017-01-27 00:55:15.267	https://www.google.com/intl/en/chrome/browser/welcome.html	Getting Started		
24	site setting (hsts)	2017-01-27 00:55:20.399	ssl.google-analytics.com	HSTS observed	26YaoM4gVrY0ie3hywpFBUJh47nllvTljf0QEZuoLCM=: {'dynamic_spki_hashes_expiry': 0.0, 'expiry': 1496364920.399954, 'mode': 'force-https', 'pkp_include_subdom	
66	url	2017-01-27 00:56:32.273	http://www.youtube.com/	YouTube		
67	url	2017-01-27 00:56:32.273	https://www.youtube.com/	YouTube		
76	url	2017-01-27 00:56:34.110	https://www.youtube.com/	YouTube		
27	url	2017-01-27 00:56:52.542	https://www.youtube.com/	YouTube		
28	url	2017-01-27 00:56:52.544	https://www.youtube.com/results?search_query=game+theory+harry+potter	game theory harry potter - YouTube		search_query: game theory harry potter [Query String Parser]
42	url	2017-01-27 00:56:56.959	https://www.youtube.com/results?search_query=game+theory+harry+potter	game theory harry potter - YouTube		search_query: game theory harry potter [Query String Parser]
43	url	2017-01-27 00:56:56.963	https://www.youtube.com/watch?v=mbC-sDMHypU	Film Theory: Harry Potter, MORE VOLDEMORT than Voldemort! - YouTube		v: mbC-sDMHypU [Query String Parser]
72	url	2017-01-27 00:59:36.219	https://www.google.com/search?q=pottermore&rlz=1C1CHBD_enUS729US729	pottermore - Google Search		Searched for "pottermore" [ Using chrome ]
77	url	2017-01-27 00:59:39.852	https://www.pottermore.com/	Pottermore - The digital heart of the Wizarding World		
113	url	2017-01-27 00:59:54.799	https://www.google.com/	Google		
117	url	2017-01-27 01:02:03.713	https://www.pottermore.com/cursed-child	Harry Potter and the Cursed Child - Pottermore		
131	url	2017-01-27 01:02:15.454	https://www.pottermore.com/news	News - Pottermore		
133	url	2017-01-27 01:02:21.449	https://my.pottermore.com/account/confirm-age	Join - Pottermore		
146	url	2017-01-27 01:02:29.611	https://my.pottermore.com/account/confirm-age	Join - Pottermore		
148	url	2017-01-27 01:02:56.615	https://www.google.com/	Google		
149	url	2017-01-27 01:03:01.911	https://my.pottermore.com/account/confirm-age	Join - Pottermore		
150	url	2017-01-27 01:03:20.355	https://my.pottermore.com/account/join/verify	Join - Pottermore		
151	autofill	2017-01-27 01:04:17.000		name Sarah McAvoy		
152	autofill	2017-01-27 01:04:17.000		email McAvoyS87@gmail.com		
153	url	2017-01-27 01:04:18.064	https://my.pottermore.com/account/join	Join - Pottermore		
154	url	2017-01-27 01:04:28.241	https://www.pottermore.com/	Pottermore - The digital heart of the Wizarding World		
155	url	2017-01-27 01:05:00.337	https://www.google.com/#q=brightness+setting	brightness setting - Google Search		Searched for "brightness setting"
159	url	2017-01-27 01:05:03.752	http://www.howtogeek.com/241771/how-to-adjust-your-pcs-screen-brightness-manually-and-automatically	How to Adjust Your PC's Screen Brightness, Manually and Automatically		
157	url	2017-01-27 01:05:33.381	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1CHBD_enUS729US729	Google		sourceid: chrome-instant   rlz: 1C1CHBD_enUS729US729   ion: 1   es
158	url	2017-01-27 01:05:34.904	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1CHBD_enUS729US729	Google		Searched for "owls" [ Using chrome-instant ]
162	url	2017-01-27 01:05:37.396	https://www.google.com/imgres?imgurl=https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/Athene_noctua_(cropped).jpg	Google Image Result for https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/Athene_noctua_(cropped).jpg		imgurl: https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/Athene_noctua_(cropped).jpg
168	download	2017-01-27 01:05:43.967	https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/Athene_noctua_(cropped).jpg	Complete - 100% [12121/121 C:\Users\Sarah M\Downloads\Luna Owl.jpg		
170	url	2017-01-27 01:06:30.515	https://www.pottermore.com/explore-the-story	Explore the story - Pottermore		
175	url	2017-01-27 01:06:44.548	https://www.pottermore.com/writing-by-jk-rowling	Writing by J.K. Rowling - Pottermore		
176	url	2017-01-27 01:06:57.204	https://www.pottermore.com/collection/jk-rowling-how-the-wizarding-world-works	How the wizarding world works - Pottermore		
180	url	2017-01-27 01:07:18.651	https://my.pottermore.com/shop/cart?return_to=%3Futm_source%3DPottermore			return_to: ?utm_source=CartIcon&utm_medium=Pottermore&utm_campaign=
181	url	2017-01-27 01:07:18.651	https://usd.shop.pottermore.com/?utm_source=CartIcon&utm_medium=Pottermore			utm_source: CartIcon   utm_medium: Pottermore   utm_campaign: S
195	url	2017-01-27 01:07:27.370	https://usd.shop.pottermore.com/products/harry_potter_the_complete_collection	Harry Potter: The Complete Collection - Pottermore Shop		

# Exercise 11

1. Which **Gmail email address** was **accessed by the Sarah M user**?
2. Which **Facebook account** was **accessed by the Sarah M user**?
3. Which **files** were **downloaded**?

# Exercise 11.1 / 11.2

Hindsight Internet History Forensics (v2023.03)				
Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path
url	2017-01-27 17:07:25.416	https://mail.google.com/mail/?pli=1	Gmail	
url	2017-01-27 17:07:25.416	https://mail.google.com/mail/	Gmail	
url	2017-01-27 17:07:27.195	https://mail.google.com/mail/#inbox	Inbox (1) - mcavoys87@gmail.com - Gmail	
url	2017-01-27 17:07:50.993	https://mail.google.com/mail/#inbox/159d73b41b53f2e8	Confirm your Twitter account, Sarah McAvoy - mcavoys87@gmail.com - Gmail	
url	2017-01-27 17:08:11.276	https://mail.google.com/mail/#inbox	Inbox (1) - mcavoys87@gmail.com - Gmail	
url	2017-01-27 17:08:12.501	https://mail.google.com/mail/#inbox/159d0e02b296fde4	Sarah, get more out of your new Android device - mcavoys87@gmail.com - Gmail	
url	2017-01-27 17:08:14.645	https://mail.google.com/mail/#inbox	Inbox (1) - mcavoys87@gmail.com - Gmail	

Hindsight Internet History Forensics (v2023.03)				
Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path
url	2017-01-27 17:29:19.594	https://www.facebook.com/	(1) Facebook	
url	2017-01-27 17:29:25.297	https://www.facebook.com/sarah.mcavoy.9638	Sarah Mcavoy	
url	2017-01-27 17:29:25.426	https://www.facebook.com/sarah.mcavoy.9638	Sarah Mcavoy	
url	2017-01-27 17:29:30.146	https://www.facebook.com/sarah.mcavoy.9638	Sarah Mcavoy	
url	2017-01-27 17:42:54.117	https://www.facebook.com/sarah.mcavoy.9638#	(2) Sarah Mcavoy	
url	2017-01-27 17:42:54.634	https://www.facebook.com/sarah.mcavoy.9638#	(2) Sarah Mcavoy	
url	2017-01-27 17:42:55.892	https://www.facebook.com/sarah.mcavoy.9638#	(2) Sarah Mcavoy	
url	2017-01-27 17:42:56.829	https://www.facebook.com/sarah.mcavoy.9638#	(2) Sarah Mcavoy	



# Exercise 11.3

Hindsight Internet History Forensics (v2023.03)					
Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path	
download	2017-01-27 01:05:43.967	https://upload.wikimedia.org/wikipedia/commons/thumb/3/39/At	Complete - 100% [12121/121	C:\Users\Sarah M\Downloads\Luna Owl.jpg	
download	2017-01-27 01:16:17.426	http://www.ncwildlife.org/Portals/0/Learning/documents/Profiles/	Complete - 100% [355574/35	C:\Users\Sarah M\Downloads\Great Horned Owl Info.pdf	
download	2017-01-27 01:47:51.888	https://get.skype.com/go/gets skype-windows	Complete - 100% [43918808/	C:\Users\Sarah M\Downloads\SkypeSetupFull.exe	
download	2017-01-27 01:47:51.888	https://get.skype.com/go/gets skype	Complete - 100% [43918808/	C:\Users\Sarah M\Downloads\SkypeSetupFull.exe	
download	2017-01-27 01:47:51.888	https://download.skype.com/f0ea4d7f41d9561cc0d5b27925a74910/p	Complete - 100% [43918808/	C:\Users\Sarah M\Downloads\SkypeSetupFull.exe	
download	2017-01-27 17:19:12.131	https://mail.google.com/mail/?ui=2&ik=411bfb1f1f&view=att&th=15	Complete - 100% [64476/644	C:\Users\Sarah M\Downloads\Great Horned Owl.jpg	
download	2017-01-27 17:19:12.131	https://mail-attachment.googleusercontent.com/attachment/?ui=2&	Complete - 100% [64476/644	C:\Users\Sarah M\Downloads\Great Horned Owl.jpg	
download	2017-01-27 17:19:14.359	https://mail.google.com/mail/?ui=2&ik=411bfb1f1f&view=att&th=15	Complete - 100% [94519/945	C:\Users\Sarah M\Downloads\Pygmy Owl.jpg	
download	2017-01-27 17:19:14.359	https://mail-attachment.googleusercontent.com/attachment/?ui=2&	Complete - 100% [94519/945	C:\Users\Sarah M\Downloads\Pygmy Owl.jpg	
download	2017-01-27 17:19:16.139	https://mail.google.com/mail/?ui=2&ik=411bfb1f1f&view=att&th=15	Complete - 100% [5948982/5	C:\Users\Sarah M\Downloads\Snowy Owl.jpg	
download	2017-01-27 17:19:16.139	https://mail-attachment.googleusercontent.com/attachment/?ui=2&	Complete - 100% [5948982/5	C:\Users\Sarah M\Downloads\Snowy Owl.jpg	
download	2017-01-27 17:33:16.765	https://mail.google.com/mail/?ui=2&ik=411bfb1f1f&view=att&th=15	Complete - 100% [10051/100	C:\Users\Sarah M\Downloads\Snowy Owl 2.jpg	
download	2017-01-27 17:33:16.765	https://mail-attachment.googleusercontent.com/attachment/?ui=2&	Complete - 100% [10051/100	C:\Users\Sarah M\Downloads\Snowy Owl 2.jpg	
download	2017-01-27 17:33:18.234	https://mail.google.com/mail/?ui=2&ik=411bfb1f1f&view=att&th=15	Complete - 100% [74943/749	C:\Users\Sarah M\Downloads\Snowy Owl 3.jpg	
download	2017-01-27 17:33:18.234	https://mail-attachment.googleusercontent.com/attachment/?ui=2&	Complete - 100% [74943/749	C:\Users\Sarah M\Downloads\Snowy Owl 3.jpg	
download	2017-01-27 17:33:19.630	https://mail.google.com/mail/?ui=2&ik=411bfb1f1f&view=att&th=15	Complete - 100% [3496271/3	C:\Users\Sarah M\Downloads\Snowy Owl 4.jpg	
download	2017-01-27 17:33:19.630	https://mail-attachment.googleusercontent.com/attachment/?ui=2&	Complete - 100% [3496271/3	C:\Users\Sarah M\Downloads\Snowy Owl 4.jpg	
download	2017-01-28 22:34:20.181	https://s-media-cache-ak0.pinimg.com/236x/69/d4/55/69d4553fcd5	Complete - 100% [18285/182	C:\Users\Sarah M\Downloads\Cool picture of a tiger maybe wallhanging.jpg	
download	2017-01-28 22:36:33.987	data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAQABAAD/2wCEA/	Complete - 100% [9707/9707	C:\Users\Sarah M\Downloads\Background.jpg	
download	2017-01-31 19:08:56.141	http://www.owlpages.com/download/Owl_Emergency_Care.pdf	Complete - 100% [142534/14	C:\Users\Sarah M\Downloads\Owl_Emergency_Care.pdf	
download	2017-01-31 19:09:08.662	http://www.owlpages.com/download/Owl_Keeping.pdf	Complete - 100% [218461/21	C:\Users\Sarah M\Downloads\Owl_Keeping.pdf	
download	2017-01-31 19:12:14.687	http://dnr2.maryland.gov/wildlife/Documents/Snowy_Owl.pdf	Complete - 100% [593265/59	C:\Users\Sarah M\Desktop\Snowy_Owl.pdf	
download	2017-01-31 19:12:43.719	http://www.globalowlproject.com/snowy-owl/Bibliography%20-%20	Complete - 100% [396800/39	C:\Users\Sarah M\Downloads\Bibliography - Snowy Owl 14 April 2014 - GLOW posting.xls	
download	2017-01-31 19:14:57.544	http://dnr2.maryland.gov/wildlife/Documents/Snowy_Owl.pdf	Complete - 100% [593265/59	C:\Users\Sarah M\Desktop\Snowy_Owl.pdf	
download	2017-01-31 19:21:13.808	http://www.fosc.org/Sightings2005.xls	Complete - 100% [112128/11	C:\Users\Sarah M\Downloads\Sightings2005.xls	
download	2017-01-31 19:22:01.756	http://www.fosc.org/Sightings2005.xls	Complete - 100% [112128/11	C:\Users\Sarah M\Downloads\Sightings2005 (1).xls	
download	2017-01-31 19:26:59.107	http://www.nwf.org/~media/Content/Animals/Reptiles%20and%20	Complete - 100% [44730/447	C:\Users\Sarah M\Desktop\Next pet.jpg	
download	2017-02-01 16:59:24.573	https://downloads.sourceforge.net/project/pidgin/Pidgin/2.11.0/pi	Complete - 100% [9256224/9	C:\Users\Sarah M\Downloads\pidgin-2.11.0.exe	
download	2017-02-01 16:59:24.573	https://superb-sea2.dl.sourceforge.net/project/pidgin/Pidgin/2.11.0	Complete - 100% [9256224/9	C:\Users\Sarah M\Downloads\pidgin-2.11.0.exe	
download	2017-02-01 17:05:32.243	https://downloads.sourceforge.net/project/pidgin/Pidgin/2.11.0/pi	Complete - 100% [9256224/9	C:\Users\Sarah M\Downloads\pidgin-2.11.0 (1).exe	
download	2017-02-01 17:05:32.243	https://superb-sea2.dl.sourceforge.net/project/pidgin/Pidgin/2.11.0	Complete - 100% [9256224/9	C:\Users\Sarah M\Downloads\pidgin-2.11.0 (1).exe	
download	2017-02-02 22:25:03.628	https://s.yimg.com/jd/desktop/0.8.288/yahoo-messenger-0.8.288-w	Complete - 100% [46966800/	C:\Users\Sarah M\Downloads\yahoo-messenger-0.8.288-win32.exe	
download	2017-02-02 22:51:41.348	https://www.flickr.com/photos/142118881@N02/28036340661/in/ph	Complete - 100% [49/49]	C:\Users\Sarah M\Desktop\WOLF Awsome.html	
download	2017-02-02 22:52:25.487	https://www.flickr.com/photos/95843423@N03/9851468684/in/ph	Complete - 100% [49/49]	C:\Users\Sarah M\Desktop\what is this.html	

# Exercise 11.4

Hindsight Internet History Forensics (v2023.03)					
Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path	Interpretation
url	2017-01-27 00:59:36.219	https://www.google.com/search?q=pottermore&rlz=1C1CHBD_enUS	pottermore - Google Search		Searched for "pottermore" [ Using chrome ]
url	2017-01-27 01:05:00.337	https://www.google.com/#q=brightness+setting	brightness setting - Google Search		Searched for "brightness setting"
url	2017-01-27 01:05:34.904	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "owls" [ Using chrome-instant ]
url	2017-01-27 01:08:19.811	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "sirius the dog star" [ Using chrome-instant ]
url	2017-01-27 01:08:24.800	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	sirius the dog - Google Search		Searched for "sirius the dog" [ Using chrome-instant ]
url	2017-01-27 01:08:28.545	https://www.google.com/search?q=sirius+the+dog&rlz=1C1CHBD_er	sirius the dog - Google Search		Searched for "sirius the dog" [ Browser screen 1536x759]
url	2017-01-27 01:08:42.423	https://www.google.com/search?q=sirius+the+dog&rlz=1C1CHBD_er	harry pottersirius the dog - Google Search		Searched for "harry pottersirius the dog" [ Browser screen 1536x759]
url	2017-01-27 01:08:48.518	https://www.google.com/search?q=sirius+the+dog&rlz=1C1CHBD_er	harry potter sirius the dog - Google Search		Searched for "harry potter sirius the dog" [ Browser screen 1536x759]
url	2017-01-27 01:08:50.700	https://www.google.com/search?q=sirius+the+dog&rlz=1C1CHBD_er			Searched for "harry potter sirius the dog" [ Browser screen 1536x759]
url	2017-01-27 01:11:03.738	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "www.instagram" [ Using chrome-instant ]
url	2017-01-27 01:11:31.793	https://www.google.com/#q=instagram	Google		Searched for "instagram"
url	2017-01-27 01:11:39.601	https://www.google.com/#q=instagram	Google		Searched for "instagram"
url	2017-01-27 01:13:06.314	https://www.google.com/#q=can+you+buy+owl+eggs	can you buy owl eggs - Google Search		Searched for "can you buy owl eggs"
url	2017-01-27 01:13:13.123	https://www.google.com/#q=can+you+buy+snow+owl+eggs	can you buy snow owl eggs - Google Search		Searched for "can you buy snow owl eggs"
url	2017-01-27 01:13:16.826	https://www.google.com/#q=can+you+buy+snowy+owl+eggs	Google		Searched for "can you buy snowy owl eggs"
url	2017-01-27 01:13:28.850	https://www.google.com/#q=can+you+buy+snowy+owl+eggs	Google		Searched for "can you buy snowy owl eggs"
url	2017-01-27 01:13:44.929	https://www.google.com/#q=can+you+buy+snowy+owl+eggs	Google		Searched for "can you buy snowy owl eggs"
url	2017-01-27 01:14:56.175	https://www.google.com/#q=can+you+buy+snowy+owl+eggs	Google		Searched for "can you buy snowy owl eggs"
url	2017-01-27 01:15:10.815	https://www.google.com/#q=owl+wingspans+in+america	owl wingspans in america - Google Search		Searched for "owl wingspans in america"
url	2017-01-27 01:16:06.986	https://www.google.com/#q=owl+wingspans+in+america+pdf	owl wingspans in america pdf - Google Search		Searched for "owl wingspans in america pdf"
url	2017-01-27 01:42:19.077	https://www.google.com/#q=craigslist			Searched for "craigslist"
url	2017-01-27 01:43:15.605	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "are owls endangered" [ Using chrome-instant ]
url	2017-01-27 01:44:08.314	https://www.google.com/#q=endangered+owls	endangered owls - Google Search		Searched for "endangered owls"
url	2017-01-27 01:44:31.865	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "monkeys" [ Using chrome-instant ]
url	2017-01-27 01:44:43.767	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	can you buy monkeys - Google Search		Searched for "can you buy monkeys" [ Using chrome-instant ]
url	2017-01-27 01:47:43.411	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "skype download" [ Using chrome-instant ]
url	2017-01-27 16:59:39.179	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	birdtrader - Google Search		Searched for "pigmy owl" [ Using chrome-instant ]
url	2017-01-27 16:59:59.008	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	birdtrader.com - Google Search		Searched for "birdtrader.com" [ Using chrome-instant ]
url	2017-01-27 17:00:54.538	https://www.google.com/search?q=what+do+owls+eat&rlz=1C1CHB	what do owls eat - Google Search		Searched for "what do owls eat" [ Typed "what do owls " before click
url	2017-01-27 17:02:06.437	https://www.google.com/search?q=where+to+keep+a+snowy+owl&where	where to keep a snowy owl - Google Search		Searched for "where to keep a snowy owl" [ Using chrome ]
url	2017-01-27 17:02:18.186	https://www.google.com/search?q=where+to+keep+a+snowy+owl&where	where to keep a snowy owl - Google Search		Searched for "where to keep a snowy owl" [ Using chrome ]
url	2017-01-27 17:02:28.235	https://www.google.com/search?q=where+to+keep+a+snowy+owl&where	where to keep a snowy owl - Google Search		Searched for "where to keep a snowy owl" [ Using chrome ]
url	2017-01-27 17:02:41.970	https://www.google.com/search?q=where+to+keep+a+snowy+owl&where	where to keep a snowy owl - Google Search		Searched for "where to keep a snowy owl" [ Using chrome ]
url	2017-01-27 17:03:50.315	https://www.google.com/search?q=where+to+keep+a+snowy+owl&where	where to keep a snowy owl - Google Search		Searched for "where to keep a snowy owl" [ Using chrome ]
url	2017-01-27 17:03:57.167	https://www.google.com/search?q=where+to+keep+a+snowy+owl&where	where to keep a snowy owl - Google Search		Searched for "how much does a snowy owl cost" [ Typed "where to k
url	2017-01-27 17:04:08.630	https://www.google.com/search?q=where+to+keep+a+snowy+owl&where	where to keep a snowy owl - Google Search		Searched for "how much does a snowy owl cost" [ Typed "where to k



# Exercise 11.4

Hindsight Internet History Forensics (v2023.03)					
Type	Timestamp (UTC)	URL	Title / Name / Status	Data / Value / Path	Interpretation
url	2017-01-27 17:04:12.329	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how much does a snowy owl cost" [ Typed "where to k
url	2017-01-27 17:04:23.325	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	how to care for a owl - Google Search		Searched for "purchase a snowy owl in the united states" [ Typed "wl
url	2017-01-27 17:04:37.620	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	how to care for a owl - Google Search		Searched for "purchase a snowy owl in the united states" [ Typed "wl
url	2017-01-27 17:04:52.529	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	how to care for a owl - Google Search		Searched for "purchase a snowy owl in the united states" [ Typed "wl
url	2017-01-27 17:05:33.404	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how to care for a owl" [ Typed "where to keep a snowy
url	2017-01-27 17:05:42.518	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how to care for a owl" [ Typed "where to keep a snowy
url	2017-01-27 17:05:57.984	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how to care for a owl" [ Typed "where to keep a snowy
url	2017-01-27 17:05:58.226	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	how to care for a owl - Google Search		Searched for "purchase a snowy owl in the united states" [ Typed "wl
url	2017-01-27 17:06:00.610	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how to care for a owl" [ Typed "where to keep a snowy
url	2017-01-27 17:06:02.764	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how to care for a owl" [ Typed "where to keep a snowy
url	2017-01-27 17:06:13.924	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how to care for a owl" [ Typed "where to keep a snowy
url	2017-01-27 17:06:32.276	https://www.google.com/search?q=where+to+keep+a+snowy+owl&	where to keep a snowy owl - Google Search		Searched for "how to care for a owl" [ Typed "where to keep a snowy
url	2017-01-27 17:29:54.659	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	Google		Searched for "harry potter.com" [ Using chrome-instant ]
url	2017-01-27 17:30:01.846	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	Google		Searched for "harry potter.com" [ Using chrome-instant ]
url	2017-01-27 17:30:06.823	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "amazon" [ Using chrome-instant ]
url	2017-01-27 17:31:03.290	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	birdtrader.com - Google Search		Searched for "birdtrader.com" [ Using chrome-instant ]
url	2017-01-28 21:51:01.471	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	Google		Searched for "harry potter screenplay" [ Using chrome-instant ]
url	2017-01-28 21:53:16.469	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	Google		Searched for "harry potter screenplay" [ Using chrome-instant ]
url	2017-01-28 22:15:45.713	https://www.google.com/#q=falcons	falcons - Google Search		Searched for "falcons"
url	2017-01-28 22:15:52.953	https://www.google.com/#q=falcons+birds	Google		Searched for "falcons birds"
url	2017-01-28 22:17:22.293	https://www.google.com/#q=falcons+birds	Google		Searched for "falcons birds"
url	2017-01-28 22:17:37.641	https://www.google.com/#q=where+can+I+learn+falconry	Google		Searched for "where can I learn falconry"
url	2017-01-28 22:17:49.574	https://www.google.com/#q=where+can+I+learn+falconry	Google		Searched for "where can I learn falconry"
url	2017-01-28 22:18:02.708	https://www.google.com/#q=where+can+I+learn+falconry	Google		Searched for "where can I learn falconry"
url	2017-01-28 22:26:13.468	https://www.google.com/#q=gmail	gmail - Google Search		Searched for "gmail"
url	2017-01-28 22:32:25.230	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1			Searched for "mystical bengal tiges" [ Using chrome-instant ]
url	2017-01-28 22:32:29.937	https://www.google.com/search?rlz=1C1CHBD_enUS729US729&espn	mystical bengal tigers - Google Search		Searched for "mystical bengal tigers" [ Browser screen 1536x720]
url	2017-01-28 22:32:42.667	https://www.google.com/search?q=mystical+bengal+tigers&rlz=1C1	mystical bengal tigers - Google Search		Searched for "mystical bengal tigers" [ Browser screen 1536x720]
url	2017-01-28 22:33:59.199	https://www.google.com/search?q=mystical+bengal+tigers&rlz=1C1			Searched for "mystical bengal tigers" [ Browser screen 1536x720]
url	2017-01-28 22:35:53.666	https://www.google.com/#q=athena+with+an+owl+artistic	athena with an owl artistic - Google Search		Searched for "athena with an owl artistic"
url	2017-01-28 22:35:59.552	https://www.google.com/search?q=athena+with+an+owl+artistic&b	athena with an owl artistic - Google Search		Searched for "athena with an owl artistic" [ Browser screen 1536x710]
url	2017-01-28 22:36:28.538	https://www.google.com/search?q=athena+with+an+owl+artistic&b			Searched for "athena with an owl artistic" [ Browser screen 1536x710]
url	2017-01-28 22:37:56.595	https://www.google.com/search?q=athena+with+an+owl+artistic&b	athena with an owl artistic - Google Search		Searched for "athena with an owl artistic" [ Browser screen 1536x710]
url	2017-01-28 22:38:13.733	https://www.google.com/search?q=athena+with+an+owl+artistic&b	Physics notes - Google Search		Searched for "Physics notes" [ Browser screen 1536x710]
url	2017-01-28 22:39:39.861	https://www.google.com/#q=etsy	etsy - Google Search		Searched for "etsy"
url	2017-01-28 22:42:00.830	https://www.google.com/#q=clavin+and+hobbes	clavin and hobbes - Google Search		Searched for "clavin and hobbes"



# Exercise 11.4

Hindsight Internet History Forensics (v2023.03)				
Type	Timestamp (UTC)	URL	Title / Name / Status	Interpretation
url	2017-01-28 22:38:13.733	https://www.google.com/search?q=athena+with+an+owl+artistic&b	Physics notes - Google Search	Searched for "Physics notes" [ Browser screen 1536x710]
url	2017-01-28 22:39:39.861	https://www.google.com/#q=etsy	etsy - Google Search	Searched for "etsy"
url	2017-01-28 22:42:00.830	https://www.google.com/#q=clavin+and+hobbes	clavin and hobbes - Google Search	Searched for "clavin and hobbes"
url	2017-01-28 22:42:03.873	https://www.google.com/#q=calvin+and+hobbes	calvin and hobbes - Google Search	Searched for "calvin and hobbes"
url	2017-01-30 19:22:12.062	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1		Searched for "Logan movie" [ Using chrome-instant ]
url	2017-01-30 19:24:15.299	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1		Searched for "Logan trailer" [ Using chrome-instant ]
url	2017-01-31 19:08:39.712	https://www.google.com/#q=how+to+care+for+an+owl+pdg	Google	Searched for "how to care for an owl pdg"
url	2017-01-31 19:09:01.391	https://www.google.com/#q=how+to+care+for+an+owl+pdg	Google	Searched for "how to care for an owl pdg"
url	2017-01-31 19:12:04.819	https://www.google.com/#q=snowy+owl+care+pdf	Google	Searched for "snowy owl care pdf"
url	2017-01-31 19:12:23.350	https://www.google.com/#q=snowy+owl+care+pdf	Google	Searched for "snowy owl care pdf"
url	2017-01-31 19:12:39.280	https://www.google.com/#q=snowy+owl+wingspan+xls	Google	Searched for "snowy owl wingspan xls"
url	2017-01-31 19:14:27.788	https://www.google.com/#q=snowy+owl+wingspan+xls	Google	Searched for "snowy owl wingspan xls"
url	2017-01-31 19:20:57.753	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1		Searched for "Owl wingspans" [ Using chrome-instant ]
url	2017-01-31 19:21:04.468	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	Owl wingspans xls - Google Search	Searched for "Owl wingspans xls" [ Using chrome-instant ]
url	2017-01-31 19:25:43.288	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	snowy owl wingspans - Google Search	Searched for "snowy owl wingspans" [ Using chrome-instant ]
url	2017-01-31 19:26:20.768	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1		Searched for "sea turtles" [ Using chrome-instant ]
url	2017-01-31 19:53:32.712	https://www.google.com/#q=trippy+owl+pictures	trippy owl pictures - Google Search	Searched for "trippy owl pictures"
url	2017-01-31 19:55:20.555	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi	trippy owl pictures - Google Search	Searched for "trippy owl pictures" [ Browser screen 1536x710]
url	2017-01-31 19:55:24.375	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi		Searched for "trippy owl pictures" [ Browser screen 1536x710]
url	2017-01-31 19:56:35.509	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi	Skyrim meme poster - Google Search	Searched for "Skyrim meme poster" [ Browser screen 1536x710]
url	2017-01-31 19:56:40.318	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi		Searched for "Skyrim meme poster" [ Browser screen 1536x710]
url	2017-01-31 19:56:59.427	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi		Searched for "Skyrim meme poster" [ Browser screen 1536x710]
url	2017-01-31 19:57:06.247	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi		Searched for "Skyrim meme poster" [ Browser screen 1536x710]
url	2017-01-31 19:57:15.485	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi		Searched for "Skyrim meme poster" [ Browser screen 1536x710]
url	2017-01-31 19:57:26.083	https://www.google.com/search?q=trippy+owl+pictures&biw=1536&bi		Searched for "Skyrim meme poster" [ Browser screen 1536x710]
url	2017-02-01 16:58:47.121	https://www.google.com/#q=pidgin	pidgin - Google Search	Searched for "pidgin"
url	2017-02-01 17:06:34.295	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1		Searched for "how to use pidgin im" [ Using chrome-instant ]
url	2017-02-01 17:21:30.961	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	Google	Searched for "how to get facebook xmpp" [ Using chrome-instant ]
url	2017-02-01 17:21:58.710	https://www.google.com/webhp?sourceid=chrome-instant&rlz=1C1	Google	Searched for "how to get facebook xmpp" [ Using chrome-instant ]
url	2017-02-01 17:22:38.784	https://www.google.com/#q=google+talk	Google	Searched for "google talk"
url	2017-02-01 17:23:28.895	https://www.google.com/#q=google+talk	Google	Searched for "google talk"
url	2017-02-02 21:29:26.960	https://www.google.com/#q=gmail	gmail - Google Search	Searched for "gmail"
url	2017-02-02 22:07:40.976	https://www.google.com/#q=gmail	gmail - Google Search	Searched for "gmail"
url	2017-02-02 22:24:05.762	https://www.google.com/#q=yahoo+messenger		Searched for "yahoo messenger"