SINGAPORE INSTITUTE OF TECHNOLOGY

Information and Communications Technology AY2021/2022

ICT 2202 Digital Forensics Assignment 1

Arcana User Manual

Team Spectre	
Name	**Student ID**
Muhamad Afiq Busari	**2000476**
Jeremy Jevon Chow Zi You	**2001558**
Tse Kin Ping, Matthew	**2001568**
Lee Zhi Yang Aloysius	**2001348**

Contents

Installation

```
git clone https://github.com/afiqbusari7/Arcana
cd Arcana
pip install -r requirements.txt
```

Required Libraries

- libewf-python
- lxml
- pandas
- pytsk3
- python-evtx
- requests
- tabulate
- validators
- virustotal-python

Application Setup

- Disk Image

For this application, we will be using the following test disk image.

nps-2009-domexusers — This is a disk image of a Windows XP SP3 system that has two users, domexuser1 and domexuser2, who communicate with a third user (domexuser3) via IM and email.

The one with the full system, distributed as an encrypted disk image, is used.

Download URL: https://digitalcorpora.s3.amazonaws.com/corpora/drives/nps-2009-domexusers/nps-2009-domexusers.E01

- Virus Total API Key

To make use of the VirusTotal API, you will need to first sign up an account on VirusTotal with the following link: https://www.virustotal.com/gui/join-us

You will then need to copy the API key found in the VirusTotal account user menu.

The user will then need to paste the API key into the following string found in virusTotalAPI.py

Arcana Functions
1. Raw Image
2. File
3. URL
4. Analyse Logs (LIVE)

Raw Image Functions
1. Display Files
2. Keyword Search
3. Select File to Extract from Image
4. Process and Display Web History
5. Scan for Virus

Virus Scan Functions
1. Full Scan (All Files and URLs)
2. Scan Files by Keyword
3. Scan URLs by Keyword

When the application prompts the user for input, the user can use the following commands:

Commands	Description
break	To return to the previous menu
exit	To stop the application

1. Raw Image

On launch, the application will display the Arcana main menu.

Disk Image Data Pre-processing

The application checks for available images of the E01 type in the folder and displays them all, if any. The user will then be prompted to select the disk image to use for the analysis.

Upon selecting the disk image to use, the image volume is then loaded.

The application will also check if the disk image has been processed before. If so, there will be an option to overwrite the existing processed file.

The disk image is crawled recursively, with all files timestamped and hashed.

```
Image has been processed before, overwrite? (Y to overwrite) n
[+] Opening nps-2009-domexusers.E01
[+] Recursing through files..
```

After processing the disk image and producing the CSV output files, the Raw Image Function menu will be shown. The programme prompts the user for an input.

```
===== Raw Image Functions =====
1. Display Files
2. Keyword Search
3. Select File to Extract from Image
4. Process and Display Web History
5. Scan for Virus
6. Back
7. Exit

Choose an option:
```

1.1. Display Files

The display files option shows file data for all the files in the disk image. The following attributes are displayed:

- Partition
- File
- File Ext
- File Type
- Create Date
- Modify Date
- Change Date
- Size
- File Path
- SHA256 Hash

```
Choose an option: 1
      Partition                      File File Ext File Type    Create Date         Modify Date         Change Date        Size
0  PARTITION 2                    $AttrDef    NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07     2560
1  PARTITION 2                    $Bitmap     NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07  1310304
2  PARTITION 2                      $Boot     NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07     8192
3  PARTITION 2                    $Extend     NaN      DIR   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07      344
4  PARTITION 2                    $LogFile    NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07 67108864
5  PARTITION 2                       $MFT     NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07 37765120
6  PARTITION 2                    $MFTMirr    NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07     4096
7  PARTITION 2                    $Secure     NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07        0
8  PARTITION 2                    $UpCase     NaN     FILE   2008-10-20 14:26:07 2008-10-20 14:26:07 2008-10-20 14:26:07   131072
9  PARTITION 2                    boot.ini    ini     FILE   2008-10-20 14:29:40 2008-10-20 21:38:02 2008-10-20 21:33:39      211
10 PARTITION 2       Documents and Settings  NaN      DIR   2008-10-20 14:30:07 2008-10-21 19:29:51 2008-10-21 19:29:51       56

     Size                          File Path                        SHA256 Hash
     2560                          /$AttrDef   d7de5b1b2f79f45f235ceb1adbc46908ed64eae174eb90...
  1310304                          /$Bitmap   a77d28805ee0cda71d57a7d4f3640add95faaa697cc7f6...
     8192                            /$Boot   b61bc96521689c7ebde9012fce6de688dab582c61c17c6...
      344                          /$Extend   f8e93d5ae6496fa5c1a849f2f1eb649c7dca41402617bf...
 67108864                         /$LogFile   edae303de891399a608b38155d9d75b865fccc5932ff0c...
 37765120                            /$MFT    c280709fc3275decb8e5b82f241e0eb51821dec9c7d470...
     4096                         /$MFTMirr   ce490525f60cf2960165f78afd569552c847ee247bce2f...
        0                          /$Secure   e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b93...
   131072                          /$UpCase   19442bdd7623101de9e217a943b103283406ff96d332f6...
      211                          /boot.ini   69c6eaa43ec6b89a61e0c6294be8ea88447efa011b3d26...
       56               /Documents and Settings  d77ccbb210a64e41eb67d47c8d7b074968f4255fbe4a54...
```

1.2. Keyword Search

The application includes keyword search functionality whereby the file names within the processed document can be searched and all results displayed.

```
Choose an option: 2
Enter search: Google Chrome
Searching for Google Chrome..
      Partition                      File File Ext File Type    Create Date         Modify Date         Change Date
62   PARTITION 2          Google Chrome.lnk    lnk     FILE   2008-10-21 04:16:23 2008-10-21 04:16:23 2008-10-21 04:16:23
150  PARTITION 2          Google Chrome.lnk    lnk     FILE   2008-10-21 04:16:23 2008-10-21 04:16:23 2008-10-21 04:16:23
1401 PARTITION 2            Google Chrome      NaN      DIR   2008-10-21 04:15:34 2008-10-21 04:15:35 2008-10-21 04:15:35
1402 PARTITION 2          Google Chrome.lnk    lnk     FILE   2008-10-21 04:15:34 2008-10-21 04:15:34 2008-10-21 04:15:34
1403 PARTITION 2 Uninstall Google Chrome.lnk   lnk     FILE   2008-10-21 04:15:35 2008-10-21 04:15:35 2008-10-21 04:15:35

Size                          File Path                        SHA256 Hash
2322  /Documents and Settings/Administrator/Applicat...  d056bbd30f707752bb48cfdb9751d8ff8c2cdaf5ed93cb...
2304  /Documents and Settings/Administrator/Desktop/...  06206215621fadacb2eb4c6ac460a0e125501ef07c28ed...
 528  /Documents and Settings/Administrator/Start Me...  08d7e4a144253e29404e0c3d2a8b9637d507551afd3d4c...
2316  /Documents and Settings/Administrator/Start Me...  d8d7b1cae21c312f4cddaf07aa515128c0a363b026128b...
2574  /Documents and Settings/Administrator/Start Me...  6dafdd9f228da9b20b4a741337064ead90dc6eae830348...
```
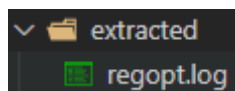
1.3. Select File to Extract from Image

The application allows for the export of files from the disk image. The file is identified using its file path and then copied to an extracted folder for future use.

```
Choose an option: 3
Enter object file path: /Windows/regopt.log
[+] File ./extracted/regopt.log Extracted Successfully.
```

```
∨ 📁 extracted
      📗 regopt.log
```

1.4. Process and Display Web History

For analysing Web History from the disk image. The history log files from both the Chrome and Firefox browsers are located using regex and then parsed and saved in a browser folder.

```
Choose an option: 4
[+] File ./browser/History Extracted Successfully.
[+] File ./browser/places.sqlite Extracted Successfully.
```

The data is then concatenated with an additional variable name to denote which browser is used for each URL.

```
                                           URL                                Title  Browser
0                     http://picasa.google.com/        Picasa 3: Free download from Google  Chrome
1    http://www.microsoft.com/genuine/downloads/non...           Genuine Microsoft Software  Chrome
2    http://sourceforge.net/project/downloading.php...        SourceForge.net: Downloading ...  Chrome
3    http://downloads.sourceforge.net/pidgin/pidgin...                                 NaN  Chrome
4    http://www.update.microsoft.com/windowsupdate/...              Microsoft Windows Update  Chrome
5    http://www.mozilla.com/products/download.html?...                                 NaN  Chrome
6       http://descubre-latino.aol.com/aim/version_68     AIM Version 6.8 - Descubre AOL Latino  Chrome
7             http://windowsupdate.microsoft.com/                                 NaN  Chrome
8    http://update.microsoft.com/microsoftupdate/v6...  http://go.microsoft.com/fwlink/?LinkId=40747  Chrome
9           http://www.pidgin.im/download/windows        Windows | Download | Pidgin  Chrome
10   http://www.update.microsoft.com/microsoftupdat...                      Microsoft Update  Chrome
```

1.5. Scan for Virus

The virus scan component of this application allows for full or selective scans. The Virus Total API is used whereby a valid API_KEY is required.

Full scans process both files and URLs while selective scan performs the scan using a search string for the files or URLs.

```
Choose an option: 5

===== Virus Scan (VirusTotal) =====
1. Full Scan (All files and URLs)
2. Scan Files by Keyword
3. Scan URLs by Keyword
4. Back
5. Exit
```

1.5.1 Full Scan (All files and URLs)

A full scan processed both files and URLs. However, how this application this scan is limited to a single scan due to API limitation on a public API_KEY.

The file hashes or URLs are passed through the API and the results are processed to determine whether any of the various sources deem it to be malicious. Just a single malicious verdict will result in an overall malicious verdict.

```
Choose an option: 1
Scanning Files..
Scanning Websites..
Files:
   Index  File Path Verdict
0      0 /$AttrDef    Safe
URLs:
   Index                       URL Verdict
0      0 http://picasa.google.com/    Safe
```

1.5.2 Scan Files by Keyword

Scan files by Keyword allow the user to enter a search keyword, which will be used to find matching files and then process them through the Virus Total API.

```
Choose an option: 2
Please enter the file path, or part thereof: Attr
Scanning Files (Attr):
Scanning Files..


Files:
   Index  File Path Verdict
0       0  /$AttrDef    Safe
```

1.5.3 Scan URLs by Keyword

Likewise, Scan URLs by Keyword allows the user to enter a search keyword to find matching URLs in the web history and process them through the Virus Total API.

```
Choose an option: 3
Please enter the URL, or path thereof: http://picasa.google.com/
Scanning Websites (http://picasa.google.com/):
Scanning Websites..


URLs:
   Index                        URL Verdict
0       0  http://picasa.google.com/    Safe
```

2. File

This function performs a VirusTotal scan on a file in the user's local directory to check for malware.

```
Choose an option: 1

Input directory of file you would like to scan: C:\Users\jerem\Desktop\Document.docx
| File                            | Verdict   |
|---------------------------------+-----------|
| C:\Users\jerem\Desktop\Document.docx | Safe      |
```

3. URL

This function performs a VirusTotal scan on any website URL entered by the user.

```
Choose an option: 1

Input URL you would like to scan eg. https://www.facebook.com: https://www.facebook.com
| URL                       | Verdict   |
|---------------------------+-----------|
| https://www.facebook.com | Safe      |
```

4. Analyse Logs (LIVE)

This function allows the user to analyse logs in their local directory to identify any suspicious events that have transpired based on the event IDs that were predefined.

The user will first be prompted to enter the directory which contains the logs file or enter "1" for the default path.

```
Choose an option: 4
Please enter the path to the directory containing the logs (e.g. C:\Windows\System32\winevt\Logs) or enter "1" to use default path: 1
Scanning for log files...
1:  Application.evtx
2:  Cisco AnyConnect Secure Mobility Client.evtx
3:  Dell.evtx
4:  HardwareEvents.evtx
5:  IntelAudioServiceLog.evtx
6:  Internet Explorer.evtx
7:  Key Management Service.evtx
8:  Microsoft-Client-Licensing-Platform%4Admin.evtx
9:  Microsoft-Windows-AAD%4Operational.evtx
10: Microsoft-Windows-AllJoyn%4Operational.evtx
```

```
190:    System.evtx
191:    Windows Azure.evtx
192:    Windows PowerShell.evtx
193:    *ALL LOGS
194:    **Automated Scan for suspicious events
Enter numerical value of your choice of log file scan: 192
Event ID: 600   Log File Name: Windows PowerShell.evtx
Event ID: 400   Log File Name: Windows PowerShell.evtx
Event ID: 403   Log File Name: Windows PowerShell.evtx
```