Arcane Guide Document

Contents

Introduction

Arcane provides the following functions:

1. Display Files
2. Keyword Search
3. Export File
4. Process and Display Web History
5. Scan for Virus

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.

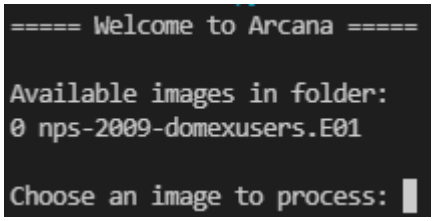
The one with the full system, distributed as an encrypted disk image, is used.

Download URL:

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

Image Data Preprocessing

Upon executing the application, the following is shown.

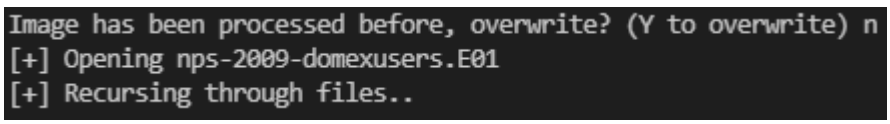


The application checks for available images of the E01 type in the folder and displays them all, if any. The user will then be prompt to select the disk image to use for the analysis.

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.



After the preprocessing is done, the function menu for the application will then be available.

```
===== Arcane Functions =====
1. Display Files
2. Keyword Search
3. Export File
4. Process and display Web History
5. Scan for Virus
6. Exit

Choose an option:
```

Selecting the Exit option, 6, will end the application.

```
Choose an option: 6
Exiting the program..
```

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  \
0      PARTITION 2      $AttrDef      NaN      FILE  2008-10-20 14:26:07
1      PARTITION 2       $Bitmap      NaN      FILE  2008-10-20 14:26:07
2      PARTITION 2         $Boot      NaN      FILE  2008-10-20 14:26:07
3      PARTITION 2       $Extend      NaN       DIR  2008-10-20 14:26:07
4      PARTITION 2      $LogFile      NaN      FILE  2008-10-20 14:26:07
...            ...           ...      ...       ...                  ...
37468  PARTITION 2  explorer.scf      scf      FILE  2004-08-04 12:00:00
37469  PARTITION 2           mui      NaN       DIR  2008-10-20 14:26:16
37470  PARTITION 2  muisetup.exe      exe      FILE  2004-08-04 12:00:00
37471  PARTITION 2    regopt.log      log      FILE  2008-10-20 14:30:46
37472  PARTITION 2  twunk_32.exe      exe      FILE  2004-08-04 12:00:00
```

	Modify Date	Change Date	Size	\
0	2008-10-20 14:26:07	2008-10-20 14:26:07	2560	
1	2008-10-20 14:26:07	2008-10-20 14:26:07	1310304	
2	2008-10-20 14:26:07	2008-10-20 14:26:07	8192	
3	2008-10-20 14:26:07	2008-10-20 14:26:07	344	
4	2008-10-20 14:26:07	2008-10-20 14:26:07	67108864	
...	...	...	...	
37468	2008-10-20 14:31:08	2004-08-04 12:00:00	80	
37469	2008-10-21 00:52:48	2008-10-21 00:52:48	160	
37470	2008-10-21 00:52:48	2008-04-14 00:12:29	90624	
37471	2008-10-20 14:31:08	2008-10-20 14:30:50	1052	
37472	2008-10-20 14:31:10	2004-08-04 12:00:00	25600	

	File Path	\
0	/$AttrDef	
1	/$Bitmap	
2	/$Boot	
3	/$Extend	
4	/$LogFile	
...	...	
37468	/WINDOWS/explorer.scf	
37469	/WINDOWS/mui	
37470	/WINDOWS/mui/muisetup.exe	
37471	/WINDOWS/regopt.log	
37472	/WINDOWS/twunk_32.exe	

	SHA256 Hash
0	d7de5b1b2f79f45f235ceb1adbc46908ed64eae174eb90...
1	a77d28805ee0cda71d57a7d4f3640add95faaa697cc7f6...
2	b61bc96521689c7ebde9012fce6de688dab582c61c17c6...
3	f8e93d5ae6496fa5c1a849f2f1eb649c7dca41402617bf...
4	edae303de891399a608b38155d9d75b865fccc5932ff0c...
...	...
37468	2b2f21d2cda3f368df17a4bebda157f2d69bc5cf6058b8...
37469	099fa94fec5d8381ce6b1da34a385bcc9b884a0eb5e2f4...
37470	d8ea15b0970dccadc6ddc46652a1516aa95bb00d90e7b6...
37471	675c9b3e14d9acb734db5d25df561b08062b30f2f5fb25...
37472	5bc5845586e11b41457dd0fa02e4d347c6bdc11325e60d...

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  \
62    PARTITION 2           Google Chrome.lnk      lnk      FILE
150   PARTITION 2           Google Chrome.lnk      lnk      FILE
1401  PARTITION 2               Google Chrome      NaN       DIR
1402  PARTITION 2           Google Chrome.lnk      lnk      FILE
1403  PARTITION 2  Uninstall Google Chrome.lnk      lnk      FILE

             Create Date          Modify Date          Change Date  Size  \
62    2008-10-21 04:16:23  2008-10-21 04:16:23  2008-10-21 04:16:23  2322
150   2008-10-21 04:16:23  2008-10-21 04:16:23  2008-10-21 04:16:23  2304
1401  2008-10-21 04:15:34  2008-10-21 04:15:35  2008-10-21 04:15:35   528
1402  2008-10-21 04:15:34  2008-10-21 04:15:34  2008-10-21 04:15:34  2316
1403  2008-10-21 04:15:35  2008-10-21 04:15:35  2008-10-21 04:15:35  2574
```

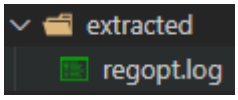
```
                                                File Path  \
62    /Documents and Settings/Administrator/Applicat...
150   /Documents and Settings/Administrator/Desktop/...
1401  /Documents and Settings/Administrator/Start Me...
1402  /Documents and Settings/Administrator/Start Me...
1403  /Documents and Settings/Administrator/Start Me...

                                              SHA256 Hash
62    d056bbd30f707752bb48cfdb9751d8ff8c2cdaf5ed93cb...
150   06206215621fadacb2eb4c6ac460a0e125501ef07c28ed...
1401  08d7e4a144253e29404e0c3d2a8b9637d507551afd3d4c...
1402  d8d7b1cae21c312f4cddaf07aa515128c0a363b026128b...
1403  6dafdd9f228da9b20b4a741337064ead90dc6eae830348...
```

Export File

The application allows for exports 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 filePath: /WINDOWS/regopt.log
[+] File ./extracted/regopt.log Extracted Successfully.
```



Process and Display Web History

For analysing Web History from the disk image. The history logfiles 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  \
0                              http://picasa.google.com/
1    http://www.microsoft.com/genuine/downloads/non...
2    http://sourceforge.net/project/downloading.php...
3    http://downloads.sourceforge.net/pidgin/pidgin...
4    http://www.update.microsoft.com/windowsupdate/...
..                                                 ...
132  http://co101w.col101.mail.live.com/mail/EditMe...
133  http://co101w.col101.mail.live.com/mail/SendMe...
134  http://view.atdmt.com/iview/msnnkhac001300x250...
135  http://this.content.served.by.adshuffle.com/p/...
136  http://ad.doubleclick.net/adi/N5304.advertisin...
```

```
                                  Title  Browser
0    Picasa 3: Free download from Google   Chrome
1              Genuine Microsoft Software   Chrome
2       SourceForge.net: Downloading ...   Chrome
3                                   NaN   Chrome
4                Microsoft Windows Update   Chrome
..                                    ...      ...
132                 Windows Live Hotmail  Firefox
133                SendMessageLight.aspx  Firefox
134                                 NaN  Firefox
135                                 NaN  Firefox
136          Click here to find out more!  Firefox
```

Scan for Virus

The virus scan component of this application allows for full or selective scans. The Virus Total API is used whereby the 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
```

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 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
```

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

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

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

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
```

The back option just sends the user back to the main menu.