COMP6845: Digital Forensics

Extended Research Project Report

Extended Attributes & Alternate Data Streams

OCTOBER 2018

Prepared by:

Sarah Agbulos z5059829
Maxwell Lambert z3463892
Kaylen Payer z5076219

Overview

Aims & Objectives

To develop a deeper understanding on the topic of Alternate Data Streams (ADS) and Extended Attributes in the context of Digital Forensics, and subsequently develop a tool to assist in the extraction, analysis and investigation of this metadata.

The tools developed throughout the duration of the research project had the following objectives:

1. Reconstruct an alternate, time-lined download history from an image or drive out of ADS metadata on NTFS, EXT and/or HFSPlus file systems without modifying the drive or files
2. Interpret and extract meaningful data from known extended attributes and alternate data streams found while creating the alternate time-lined download history
3. Output results in a portable format which can be used in subsequent digital forensic tools for further analysis
4. Auto-generate a PDF summary report of the present alternate data streams/extended attributes and their associated metadata, in a human-readable format

xattr-reporter

Description

This tool produces a time-lined report of the extended attributes and their associated metadata found in macOS and Linux systems, within a given directory.

Usage

```
usage: xattr-reporter.py [-h] [-r] [-o OUTPUT] [-a] path

positional arguments:
  path                  path to directory to be scanned for extended
                        attributes

optional arguments:
  -h, --help            show this help message and exit
  -r, --recursive       recursively scan for extended attributes
  -o OUTPUT, --output OUTPUT
                        name of file to output to
  -a, --ascending       sort by time ascending (default is descending)
```

The default behaviour non-recursively scans the directory for any extended attributes and their values, sorts by most recent (descending) create time and outputs the results in a valid JSON format.

Requirements

The current requirements for xattr-reporter include the following libraries and their dependencies:

- Python 2.7
- xattr 0.9.6
- pathlib 1.0.1
- Markdown 3.0.1
- pdfkit 0.6.1

- wkhtmltopdf 0.2
- hexdump 3.3

All of the above requirements can be installed using the command

```
pip install -r requirements.txt
```

ads-reporter

Description

This tool produces a time-lined report of the alternate data streams and their associated metadata found in Windows systems, within a given directory.

Usage

```
.\ads-reporter.ps1 <path>
```

The default behaviour non-recursively scans the directory for any alternate data streams and their values, sorts by most recent (descending) create time and outputs the results in a valid JSON format.

Requirements

This tool requires Powershell to be installed on the Windows system.

Findings

macOS Extended Attributes

Below is an outline of extended attributes typically found on macOS, particularly High Sierra and Mojave. This is not an exhaustive list and only represents those extended attributes that were created by Apple and are frequently found within the file system. It is worth bearing in mind that any user is also able to create their own extended attributes to attach to files. Naturally, these have not been included in our research.

com.apple.quarantine

All files which have been downloaded from the internet, either via web browser or mail client, feature this extended attribute. The contents of this attribute (the gatekeeper score in particular) are used to determine if the file needs its signature checked before use by applications.

```
[gatekeeper score];[clock time];[downloaded from];[UUID]
```

com.apple.FinderInfo

Used to store some minimal Finder information in binary format. This attribute allows backwards compatibility with pre macOS Mavericks HFS+ metadata. A typical use involves certain bits set within the attribute represent the current tags/label colour finder. It may also contain old file formats if the file type was changed.

com.apple.ResourceFork

The resource fork of a file. Often used to store information such as preview or thumbnail images, dialogue definitions or text collections. This attribute is also proxy for legacy HFS+ metadata.

com.apple.lastuseddate#PS

Simply the last time a file was accessed in binary data (non-human readable) format.

com.apple.diskimages.fsck

This attribute records binary data information about the most recent file system consistency check fsck of the disk image file it is associated with. This check occurs during an attempt to mount the image.

com.apple.diskimages.recentcksum

This attribute is tied to disk image files that have been successfully mounted and contains a record the most recent checksum verification using hdiutil.

```
i:[integer] on [Event UUID] @ [system time] - CRC32: $[checksum]
```

com.apple.metadata:kMDItemWhereFroms

Contains information regarding the origin URL of the downloaded file. This data appears in the 'Get Info' Finder dialogue box. The URL is stored in a binary property list (bplist).

In the case of an email attachment, the bplist contains details of the original email. including the subject line of the email, the contact name and email address from which it was sent as well as a hash of the message.

com.apple.metadata:_kMDItemUserTags

Similar to com.apple.FinderInfo but solely for finder tag information, particularly for macOS post-Mavericks. It does, however store this in a binary property list (bplist) and can represent multiple tag colours in the order they were added.

com.apple.metadata:kMDLabel_

Contains a string of characters written when the OS discovers a checksum verification failed.

com.apple.metadata:_kTimeMachine[Newest|Oldest]Snapshot

Contains the timestamp for the newest or oldest time machine backup of the given folder.

com.apple.metadata:kMDItemDownloadedDate

Timestamp of when the file was downloaded.

com.apple.metadata:kMDItemIsScreenCapture:
Flag designating whether the file is a screenshot.

com.apple.metadata:kMDItemScreenCaptureGlobalRect:
Contains values designating the positioning of the screenshot, as well as its dimensions. These are half of the screenshots pixel width and height.

com.apple.metadata:kMDItemScreenCaptureType:
Designates whether the screenshot is a manual selection, full screen or a specific window.

Linux Extended Attributes

Below is an outline of extended attributes discovered during further research on extended attributes on Linux systems, however is not an exhaustive list. These are typically found through within the 'user' namespace.

It is also useful to note that any user is also able to create their own extended attributes to attach to files. As these are user-defined, they have not been included in the research of standard Linux extended attributes.

user.mime_type
Explicitly sets the mime type of the file.

user.charset
The character encoding of a file.

user.creator
Which application created the file.

user.xdg.comment
User defined comment. Often visible by file managers.

user.xdg.origin.url
The URL from which the file was downloaded.

user.xdg.referrer.url
The URL from which the file was referred from.

user.xdg.origin.email.subject
The subject line of an email from which the file attachment was downloaded.

user.xdg.origin.email.from
The sender address of the email form which the file attachment was downloaded.

user.xdg.origin.email.message-id
The message ID of the email from which the file attachment was downloaded.

user.xdg.language
The content-language http header is written to this attribute when a file is downloaded.

user.xdg.publisher:
Name of the application which created the file.

Windows Alternate Data Streams

Below is an outline of the alternate data streams which are automatically created and form part of NTFS file systems. This list omits data streams which are user created.

Zone.Identifier
Created when a file contains a text stream holding an integer value representing where the file came from:

- 0 - Local Computer
- 1 - Local Intranet Zone
- 2 - Trusted Sites Zone
- 3 - Internet Zone
- 4 - Restricted Sites Zone

SummaryInformation & DocumentSummaryInformation

Created by the operating system if a user edits the summary information for a file.

Encryptable

A stream attached to the thumbs.db image cache which typically is empty

Favicon

Attached to favourite links stored by web browsers which hold the link icon

Taskicon_%d

Referenced by Internet Explorer DLLs

OECustomProperty

Stores custom properties created by MS Outlook Express and Windows Mail

{4c8cc155-6c1e-11d1-8e41-00c04fb9386d}

Document Properties Stream Name created if editing the properties of a file inside a folder

AFP_AfpInfo and AFP_Resource

Macintosh streams

Discussion

Upon comparing the use of extended attributes and alternate data across file systems, it becomes clear that the volume and detail of metadata is varied between OS file systems.

macOS

The Apple File System (APFS) on macOS High Sierra and Mojave makes significant use of extended attributes. Almost all of those macOS attributes listed in the previous section were found on the macOS Mojave system upon which we conducted our research.

From a forensics perspective, some of the most noteworthy attributes discovered on our test system by the xattr-reporter.py script include:

Downloaded email attachments

The extended attributes show the date of download and the application used to download the file (the in-built mail app). In addition, it detail the display name and email address of the email's 'sender'. Furthermore, the 'Subject' of the email is also stored.

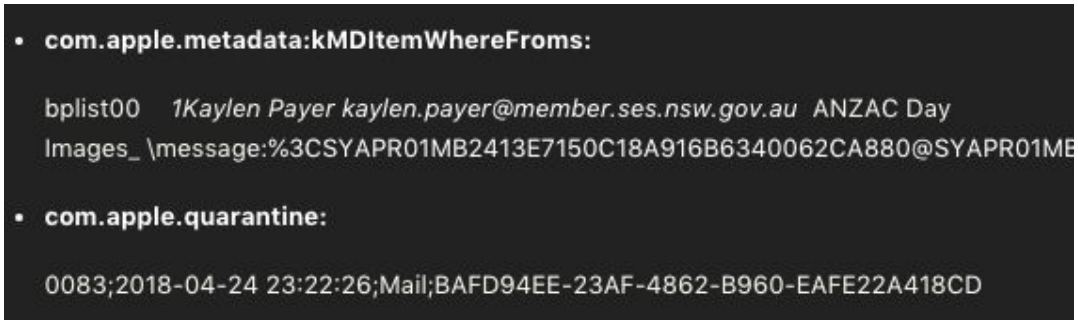

Fig. 1

Screenshot image files

The extended attribute records the application used to take the screenshot, as well as the type of screenshot - in this case a 'selection' of the screen, rather than full screen or window specific was used to capture the image.

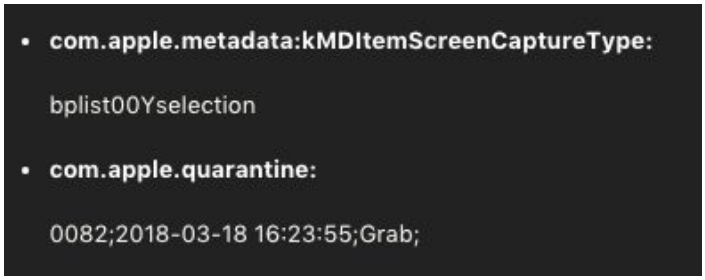

Fig. 2

Disk image files

The existence and contents of the diskimages.fsck extended attribute implies that an attempt was made to mount the image, as the file system performs fsck check at this time.
Similarly, the checksum calculated by hdiutil is stored in diskimages.recentcksum. This implies the image was successfully mounted, and this checksum can be used to verify the image.

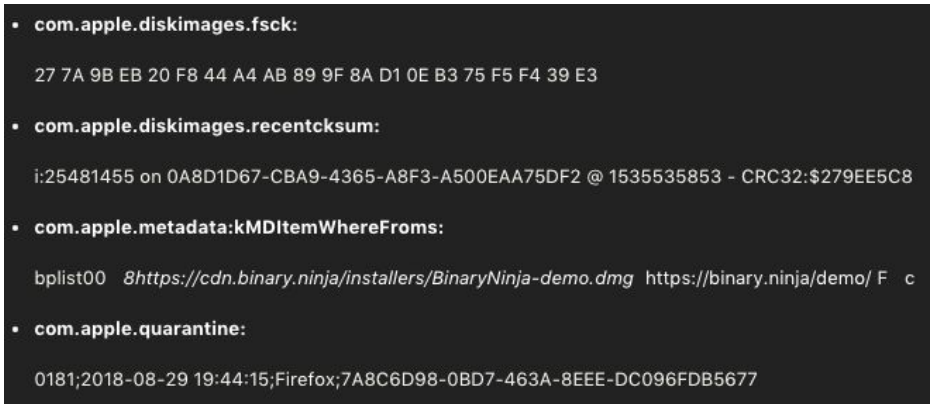

Fig. 3

Overall, macOS stores a significant amount of file metadata that is used to display further information about files to the user, to track the precise origin and type of the file, as well as to perform security checks.

Linux

Comparing these results to our tests on our Ubuntu 18.04.1 test machine highlights the large volume of metadata that macOS stores in file extended attributes. Examining a typical downloaded file on the Ubuntu machine, simply displays the origin and referrer URLs:

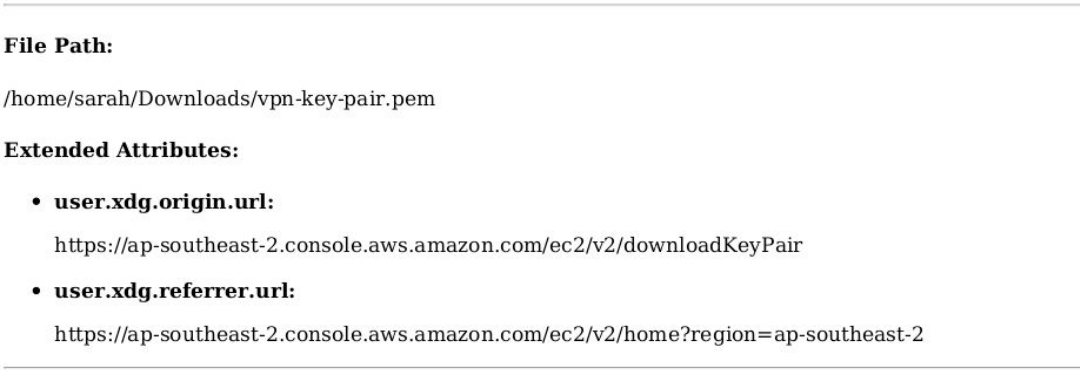

Fig. 4

Whilst they cannot be directly compared in a fair manner, given the use of different mail applications, it is worth noting that the in-built mail application, Thunderbird produces no extended attributes at all for a downloaded email, nor for a downloaded email attachment.

File Path:

/home/sarah/Downloads/We've processed your refund!.eml

Extended Attributes:

File Path:

/home/sarah/Downloads/26GT6JT379FZ8M.pdf

Extended Attributes:

Fig. 5

Linux systems store similar metadata in extended attributes, however the volume and detail of information, as well as the frequency of occurrence, is far less by comparison. Metadata such as file types, their origin and descriptions are stored, with minimal forensics information compared to macOS.

Windows

Perhaps the most conservative in its use of alternate data streams to store file metadata is NTFS. The NTFS Windows 10 file system used during testing the ads-reporter tool appears to store considerably less metadata again, in volume, frequency and detail. Similarly to Linux systems, the most commonly seen alternate data streams are the origin and referrer URLs.

In addition, ZoneTransfer value identified downloaded from the internet, rather than the local computer or an intranet . This is far broader than the fine grain detail stored in macOS attributes.

```
Path:  Microsoft.PowerShell.Core\FileSystem::D:\Downloads\r-lambert-resume.docx:Zone.Identifier
Creation Date:  4/06/2018 3:29:56 AM
PSChildName:  r-lambert-resume.docx:Zone.Identifier
Parent Path:  Microsoft.PowerShell.Core\FileSystem::D:\Downloads
Filename:  D:\Downloads\r-lambert-resume.docx
Length:  248
Content:
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://l.messenger.com/
HostUrl=https://cdn.fbsbx.com/v/t59.2708-21/33651813_10215611513136278_9020599389495754752_n.docx/r-lambert-resume.docx?_nc_cat=0&oh
```

Fig. 6

Conclusion

Extended attributes and alternate data streams are used by different operating systems to varying degrees. macOS heavily utilises extended attributes to store file metadata while Windows and Linux systems generally have less information stored in the extended attributes and alternate data streams of files.

Some of the metadata stored within the alternate data streams and extended attributes of downloaded files have potential to be interesting information for digital forensic investigations, particularly those from macOS systems which tend to store more details, while others reveal information which can also be found using other forensic methods.

Appendix

References

- https://eclecticlight.co/2017/08/14/show-me-your-metadata-extended-attributes-in-macos-sierra/
- https://eclecticlight.co/2018/02/08/xattr-com-apple-diskimages-recentcksum-disk-image-checksum/
- https://eclecticlight.co/2018/02/08/xattr-com-apple-diskimages-fsck-record-of-disk-image-integrity-check/
- https://eclecticlight.co/2017/12/21/xattr-com-apple-metadatakmditemwherefroms-origin-of-downloaded-file/
- http://rixstep.com/2/20180729,00.shtml
- http://krypted.com/tag/com-apple-finderinfo/
- https://arstechnica.com/gadgets/2013/10/os-x-10-9/9/
- https://www.pressreader.com/australia/mac-life/20180529/283034055211985
- https://blog.padil.la/2016/06/30/using-file-attributes-to-fill-volumes-and-bypass-os-x-server-limits/
- https://www.freedesktop.org/wiki/CommonExtendedAttributes/
- https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
- http://www.rootkitanalytics.com/userland/Exploring-Alternate-Data-Streams.php