Document Metadata

Assignment Part 3
Report

48436
Digital Forensics

Table Of Contents

1 Introduction

Digital Forensics is an important extension of forensic science. Regular forensics is, by definition, a discipline used to discover facts about what happened during a crime. It can be broken into many specialisations such as Pathology, Toxicology, Psychiatry, and more relevantly, Digital. Digital Forensics offers a way to discover information during a crime scene through recovery and investigation of digital based data found on devices such as Hard Drives, USB Drives, Mobile Phones, Smart Watches, and many, many more.

The investigation process itself may branch off into many different methods, however, this project will focus on Metadata investigation. Metadata itself is more of an umbrella term, with its simplest definition being "data about data". Structural and Descriptive metadata refer to information about the containers of data and the intellectual content of data respectively. Collectively, metadata can include authors, creation/modification date, file sizes, paths, and even the type of camera used on image files. Most computer files will have some sort of metadata, and gathering information through metadata is possibly one of the easiest ways to acquire initial bits of evidence.

Many metadata analysis/modification programs exist. Naming a few important ones include: OSForensics, HxD Hex Editor, and even the file command in Linux. A trivial use of metadata is evidence obfuscation. For example, a suspect may corrupt a file by changing its extension type in the file header using a Hex Editor such as HxD. By inspecting this file we could determine a mismatch between the extension in the file name and the "Magic Signature". Forensics experts can then revert the hex changes and make the file accessible, possibly uncovering some evidence. Malware is often masked as a different file type, inspecting its magic signature can help easily identify any possible malware. The list for the use of metadata goes on, and it is an extremely useful way of uncovering evidence or information.

This report will explore what metadata actually is, how it's used, how it can be extracted and how malware can be embedded into files. This report will contain an interview conducted with a Cybersecurity professional, addressing many questions in the digital forensics, and metadata fields. We will also explore sound business practices for securing metadata. Finally our reflections and conclusion will end the report.

Note this introduction was adapted from our earlier Mid-Project Review Submission

2 Metadata

2.1 Introduction to Metadata

To understand the significance of metadata in Digital Forensics, we have to dive into its definition. Metadata isn't specific to the digital field, in fact, the concept of metadata has been used prior to the invention of any computer. The Great Library of Alexandria attached tags containing the title, author, and subject to the end of scrolls[4]. These tags helped save time when searching for specific scrolls, as they eliminated the need to unroll the scrolls when searching for specific titles or authors[4]. This was in 280 BC, long before the invention of the first computer, and although the term *metadata* did not exist back then, it is clear that the concept of metadata predates any computer. The term *metadata* is defined as:

> "Data that provides information about other data"[5].

There are many different types/categories of digital metadata. Three important categories to digital forensics are Structural, Descriptive, and Administrative Metadata:

> **Structural Metadata:** Describes the layout/assembly of a data container. An example would be page numbers, which must be arranged in increasing order to form a cohesive chapter/book[6,7]
>
> **Descriptive Metadata:** Identifies specific characteristics of an asset. This can include the title, author, city, and more[6,7]
>
> **Administrative Metadata:** Describes the origin and use case of an asset. This can include the owner of the asset, date of creation, and data type[6,7]

Most file types on a computer system will have some associated metadata. When this metadata is applied in a digital forensics context it can yield massive amounts of information to digital forensics specialists on the files which are being investigated. This metadata is generated both by the operating system and also by the applications these files are created in, dynamically allowing for real-time and accurate information on the files. This includes Office documents, PDF's, and images. See below for examples of metadata for each of the three file types containing metadata, and the explanation on them:

All example images below are using an online metadata extraction tool, will be included in references

Office Document metadata:

File Name	Week 10 Law Report.docx
File Size	25 KiB
File Type	DOCX
File Type Extension	docx
Mime Type	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version	20
Zip Bit Flag	0x0006
Zip Compression	Deflated
Zip Modify Date	1980:01:01 00:00:00
Zip Crc	0x5e47dfd1
Zip Compressed Size	399
Zip Uncompressed Size	1962
Zip File Name	[Content_Types].xml
Creator	Graham Lee
Last Modified By	Xu Wang
Revision Number	24
Last Printed	2020:09:12 07:19:00Z
Create Date	2019:08:20 07:17:00Z
Modify Date	2021:10:01 09:37:00Z
Template	Normal.dotm
Total Edit Time	3 minutes
Pages	2
Words	268
Characters	1531
Application	Microsoft Office Word
Doc Security	None
Lines	12
Paragraphs	3
Scale Crop	No

Figure 1: Office document metadata

Image metadata:

File Name	IMAG1672a.jpg
File Size	520 KiB
File Type	JPEG
File Type Extension	jpg
Mime Type	image/jpeg
Jfif Version	1.01
Resolution Unit	inches
X Resolution	72
Y Resolution	72
Exif Byte Order	Big-endian (Motorola, MM)
Make	HTC
Model	HTC Sensation Z710a
Y Cb Cr Positioning	Centered
Iso	75
Exif Version	220
Date Time Original	2013:01:06 08:44:57
Create Date	2013:01:06 08:44:57
Components Configuration	Y, Cb, Cr, -
Focal Length	4.3 mm
Sub Sec Time Original	0
Sub Sec Time Digitized	0
Flashpix Version	100
Color Space	sRGB
Exif Image Width	3264
Exif Image Height	2448
Interop Version	100
Gps Latitude Ref	South
Gps Longitude Ref	East
Gps Altitude Ref	Above Sea Level
Gps Time Stamp	21:44:52
Gps Date Stamp	2013:01:05
Padding	(Binary data 2060 bytes)
About	uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Image Width	1632
Image Height	1224
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
Image Size	1632x1224
Megapixels	2
Sub Sec Create Date	2013:01:06 08:44:57.00
Sub Sec Date Time Original	2013:01:06 08:44:57.00
Gps Altitude	0 m Above Sea Level
Gps Date Time	2013:01:05 21:44:52Z
Gps Latitude	33 deg 49' 37.86" S
Gps Longitude	151 deg 15' 7.42" E
Focal Length35Efl	4.3 mm
Gps Position	33 deg 49' 37.86" S, 151 deg 15' 7.42" E

Figure 2: JPEG Metadata

PDF metadata:

File Name	Sample.pdf
File Size	327 KiB
File Type	PDF
File Type Extension	pdf
Mime Type	application/pdf
Pdf Version	1.5
Linearized	No
Page Count	1
Language	en-AU
Tagged Pdf	Yes
Title	Forensic Sample
Author	G G Lee
Subject	Forensics

KEYWORDS

0	Forensics
1	Metadata

Creator	Microsoft® Word 2010
Create Date	2013:09:29 16:36:31+10:00
Modify Date	2013:09:29 16:36:31+10:00
Producer	Microsoft® Word 2010
Category	application
Raw Header	25 50 44 46 2D 31 2E 35 0D 0A 25 B5 B5 B5 B5 0D 0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20 32 20 30 20 52 2F 4C 61 6E 67 28 65 6E 2D 41 55 29 20 2F 53 74 72 75 63 74 54 72 65 65 52 6F 6F 74 20 31 39 20 30 20 52 2F 4D 61 72 6B 49 6E 66 6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 3E 3E 3E 3E 0D 0A 65 6E 64 6F 62 6A 0D 0A 32 20 30

Title	Forensic Sample
Subject	Forensics
Keywords	Forensics, Metadata
Author	G G Lee
Creator	Microsoft® Word 2010
Producer	Microsoft® Word 2010
Creationdate	Sun Sep 29 08:36:31 2013 CEST
Moddate	Sun Sep 29 08:36:31 2013 CEST
Tagged	yes
Userproperties	no
Suspects	no
Form	none
Javascript	no
Pages	1
Encrypted	no
Page Size	595.32 x 841.92 pts (A4)
Page Rot	0
File Size	334930 bytes
Optimized	no
Pdf Version	1.5

Figure 3A: PDF metadata

PDF FONTS

Name	ABCDEE+Calibri
Type	TrueType
Encoding	WinAnsi
Embedded	1
Subset	1
Object Id	5
Name	ABCDEE+Calibri,Bold
Type	TrueType
Encoding	WinAnsi
Embedded	1
Subset	1
Object Id	9
Name	ABCDEE+Cambria,Bold
Type	TrueType
Encoding	WinAnsi
Embedded	1
Subset	1
Object Id	11
Name	ABCDEE+Algerian
Type	TrueType
Encoding	WinAnsi
Embedded	1
Subset	1
Object Id	13

PDF IMAGES

Page Number	1
Image Number	0
Type	image
Width	281
Height	316
Color Space	RGB
Color Components	3
Bits Per Component	8
Encoding	jpeg
Interpolation	1
Object Id	17
X-Ppi	150
Y-Ppi	150
Size	26.1K
Compression Ratio	10%

Figure 3B: PDF Metadata

On inspection of the metadata presented in figures *1*, *2*, and *3*, we can see the similarities and differences. File names, file types, creation/modification dates, and file sizes are common throughout all of the samples. Author metadata would obviously be associated with text based documents such as PDF files or word documents. These are all examples of metadata attached to digital files, some might not be significant to digital forensics whilst some may boost an investigation dramatically.

Forensics experts can extrapolate a lot of information using metadata, and when it comes to images, the amount of information stored as metadata is quite scary. As seen in *Figure 2*, there are fields for GPS metadata. Digital cameras store GPS metadata due to the *Exchangeable Image File Format (EXIF)* standard. *EXIF* is used to store extra details about captured images such as the focal length, aperture, shutter speed and the aforementioned GPS data[9]. The main reason for this extra information is to help photographers save time and store extra details about their images which they may later use in editing software or for whatever other purpose they may have[9]. *EXIF* data is extremely easy to strip off captured images, however, most people don't know of its existence and leave it as part of the metadata. In 2016, two Harvard university students were able to pin-point the exact location of 229 drug/weapon dealers using images uploaded on the dark web[10]. They extracted the metadata data associated with said images, and realised that the *EXIF* data was not removed. The students were able to identify the GPS coordinates of these images, leading to the locations of these drug dealers. Another common use case would be kidnappings. Abductors often send images of the victim to family or friends for use as ransom, these images could contain *EXIF* data storing the exact GPS location of the kidnapper. These are just a few examples of how GPS metadata can be used, there are many different cases and investigations using all kinds of metadata.

We have mostly looked at the metadata aspect of files so far, however, the purpose of this report is to examine regular files that can be of forensic use, and metadata alone is just the tip of the spectrum. Regular files can act as a payload for malware through embedding attacks. One such file capable of this is the PDF file format, which is more than just a way to display text on a screen. It is designed to allow interaction with any type of document layout through the use of JavaScript[11]. This will be explored and even demonstrated further in the report. For now a brief explanation of embedded attacks will be given by understanding the PDF file structure.

PDF documents are split based on objects. Now these objects can serve many different purposes, such as defining the tree structure of the document, providing metadata, version and pretty much anything which is stored within the document[13]. Whenever an interactive element within a PDF is created, multiple objects will be added to the file structure of that particular document. There will be a *Dictionary* object, as well as a *Stream* object added to the structure[13]. A *Dictionary* gives the ability for a particular *stream* object to use another object, or even *Dictionary[12,13].* Here is where things get interesting, a *Dictionary* object can feed *JavaScript* libraries into a specified *Stream* object[12,13]. This is where *embedding attacks* can occur. JavaScript is an embedded language within the PDF file format, meaning that the full extent of the JavaScript library is available to be called upon in PDF documents. Whilst this can provide a lot of interactivity to a PDF, it can also open up doors to malicious attacks. An in depth example of this will be demonstrated further along in the report, however a general example would be the use of the embedded file feature in PDF documents to attach a malicious program, and then using the embedded JavaScript to automatically execute this program upon opening the PDF[11]. PDF documents can be extremely dangerous, as they can essentially run any executable without the user knowing. This can lead to credential theft, ransom attacks, deletion of essential files in an investigation, the possibilities are pretty much endless. Examples and demonstrations of the use of metadata, as well as embedded scripts will be provided in the upcoming sections.

2.2 Demonstrations and explanations of tools/scripts used in metadata extraction

2.2.3 Extracting PDF metadata using AutoMetadata

AutoMetadata is software that allows users to view and edit metadata of PDF documents. This is able to view multiple PDF documents at a time and allows for a GUI interface to inspect the metadata of each PDF file.

Loading Files and Folders

To load the files you can use the menu option provided as "Select Files". To load various PDF's, first, ensure they are all in a folder then select the menu option of "Load Folders". The PDF file upload will look something like this.

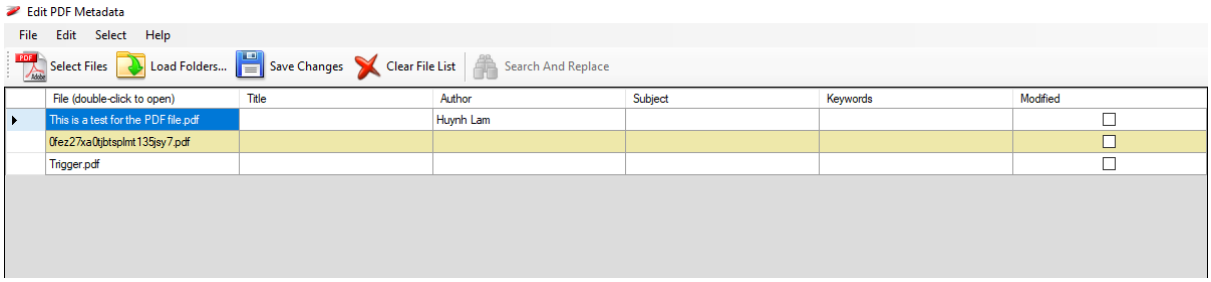

Figure 16: AutoMetadata File Upload

Metadata

Once the PDF files have loaded into the application a simple click on a certain file will display metadata information on the right-hand side of the page. This will contain a list of Access Permissions, Document Statistics, File Details, Metadata, PDF details, and Viewer Preferences.

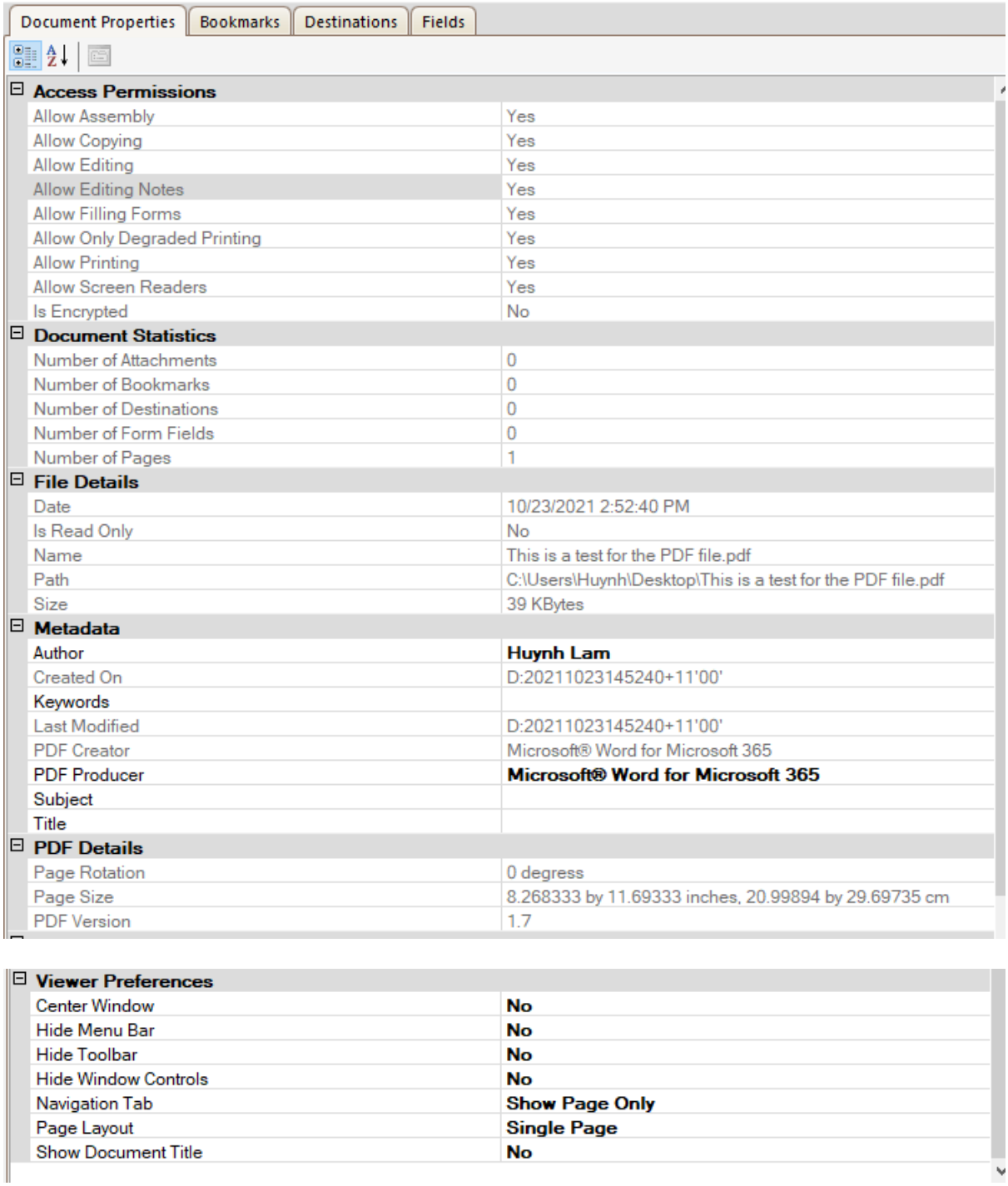

Figure 17: Document Properties Screenshot

Here is the view of the 2nd PDF document for comparison:

- There is a notable difference in the metadata and file details

Access Permissions	
Allow Assembly	Yes
Allow Copying	Yes
Allow Editing	Yes
Allow Editing Notes	Yes
Allow Filling Forms	Yes
Allow Only Degraded Printing	Yes
Allow Printing	Yes
Allow Screen Readers	Yes
Is Encrypted	No
Document Statistics	
Number of Attachments	0
Number of Bookmarks	1
Number of Destinations	0
Number of Form Fields	0
Number of Pages	1
File Details	
Date	10/23/2021 3:09:00 PM
Is Read Only	No
Name	0fez27xa0tjbtsplmt135jsy7.pdf
Path	C:\Users\Huynh\Desktop\0fez27xa0tjbtsplmt135jsy7.pdf
Size	5 KBytes
Metadata	
Author	
Created On	D:20150722163851+02'00'
Keywords	
Last Modified	D:20150722164131+02'00'
PDF Creator	Acrobat Pro 15.8.20082
PDF Producer	**Acrobat Pro 15.8.20082**
Subject	
Title	
PDF Details	
Page Rotation	0 degress
Page Size	8.5 by 11 inches, 21.5873 by 27.93651 cm
PDF Version	1.6
Viewer Preferences	
Center Window	**No**
Hide Menu Bar	**No**
Hide Toolbar	**No**

Figure 18: 2nd Document Properties

This software has 3 different tabs next to the Document Properties tab which are Bookmarks, Destination, and fields. If there is any data in those tabs they can be viewed and the Bookmarks tab can be exported into a XML file.

2.3 Demonstrations and explanations of malware embedded in documents

2.3.1 Malware Embedded in Microsoft Office Documents (DDE Exploit)

DDE is Microsoft's Dynamic Data Exchange which is a protocol that allows the transportation of data between MS office applications. Attackers have been able to exploit code execution occurring when a user opens a Microsoft application. The attack is quite similar to malware executed with macros, but as macros can be detected quite easily through antivirus software. This method was produced due to the fact they can go undetected.

Let's start by injecting some code into our Excel sheet through the use of formulas. In any of the insert this payload:

- =cmd|'/c calc.exe'!A1

The payload is using Excel to open the command prompt on the user's PC and execute the command afterwards. In our payloads case it will be opening up the calculator application.

Now we will explore what it will look like on the user's end. When the user is sent this type of document and opening it will prompt a dialogue by the Microsoft application.

The payload will only work with one condition and this condition is for the user to accept the dialogue that is popped up by the Microsoft application.

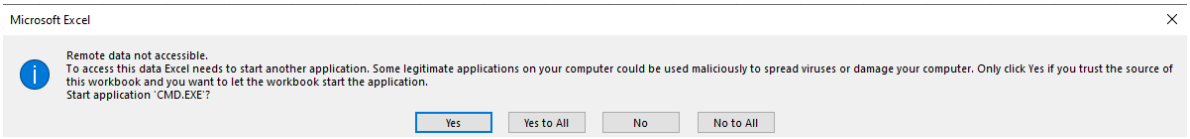

Figure 35: Microsoft Prompt

After the user has accepted this prompt the code will now execute and bring up the calculator application.

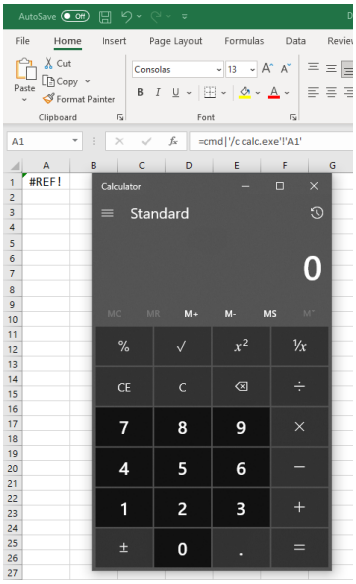

Figure 36: Calculator Opened

We can append our payload to use command prompt to ping google.com
Our new code:

- =cmd|'/c ping google.com -t '!A1

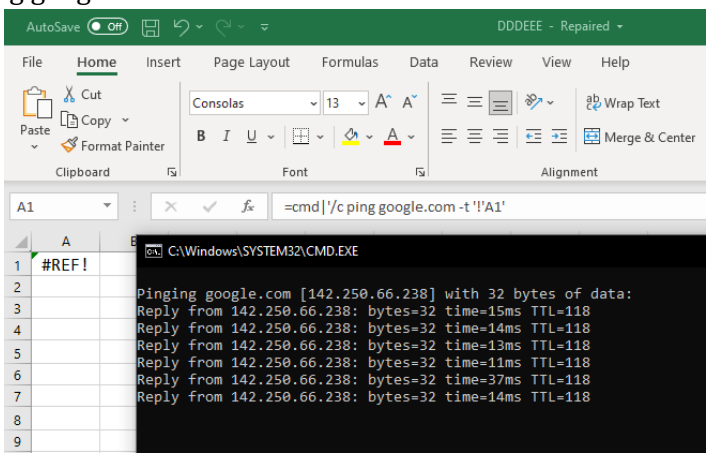

Figure 37: Ping in Command Prompt

This tool relies heavily on the user accepting the warning prompt which can prove quite hard to pull off this attack on a user. The type of attack can also enable privilege escalation as gaining user shells is possible.

Taking a closer look at the warning prompt there is no way to get rid of it and the last line “Start Application ‘CMD.EXE’?” already puts an alert on the user to know that something suspicious is going on. There is a method to alter this message into a less disbelieving message.
The command:

- =MSEXCEL|'\..\..\..\Windows\System32\cmd.exe /c calc.exe'!''

This new payload will alter our message and try to trick the user that Microsoft Excel needs permission to run this excel workbook

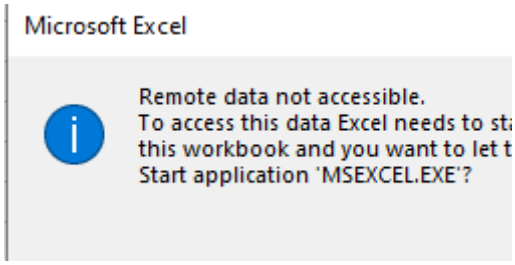

Figure 38: Edited Microsoft Prompt

This type of malware can also be embedded into Word, Outlook and Calendar invites. As useful as it looks to attackers being able to trick users in different ways hoping that one method is able to catch their victims. This is quite an old attack now and there have been improvements to antivirus software where it is impossible for this technique to go undetected. Microsoft has also implemented their own safety measures making the fresh installation of Microsoft applications automatically turn off the DDE as a service.

2.4 Business practices for securing document metadata

The technology advances in the modern world have allowed businesses to take the benefits from these technology products to rapidly transform the way there business processes. As a consequence to increased transformation of technological capabilities by businesses there is also increasing pressure to better address some of the challenges that come with technology. Specifically in this report we will recommend some practices that will need to be implemented to secure metadata.

One of the main business practices for securing metadata information would be to wipe as much of the metadata information that may be contained within files, this way no one can try to analyse the files contained. There are many ways this can be done but one of the most effective is using tools like Metadata Assistant from Payne Group. Metadata Assistant works like an integration tool when needing to transfer files and works to alert/remove the users metadata that may be contained in files before they are processed. This effectively only sends the file with no metadata.

Though the drawback is that oftentimes tools like these do cost businesses time to integrate into their environments and also are a significant cost burden to their budgets. Businesses can work to create guidelines that users will need to adhere to, when using files that may be interacted with, specifically stating what will need to be done with the files. Such guidelines can contain links to the official Microsoft documentation with removing metadata as per [25], which shows users how to remove metadata and can be a basic process which safeguards some of the metadata for smaller organisations that cannot afford to use tools or do not have a technology team capable of integrating into their business environment.

Another business practice for organisations which use some level of device management services on their technology, is using scripting tools which will work to automatically go through all files and remove metadata. This can be done at many organisations with this capability and is a basic command line process to wipe the metadata with a tool like exiftool to overwrite the metadata. This process can be seen from the following medium article as per [26], where it was done in a smaller use case, though this can be used as a script that can be deployed business wide. Running this script on a cron schedule which can be determined by the business (i.e once an hour) will ensure that all users metadata from files will be removed.

As such metadata contains varying pieces of information, in some instances this information can be used with malicious intentions and leak information to external parties. Thus safeguarding metadata is an important step towards creating a secure work environment. The above practices mention state some basic processes which can be implemented to business to help safeguard some of their business approaches to make them more secure against the imminent threat of metadata being leaked to external parties.

3 Interview

About Mitchell Tuck:
Digital forensics graduate program at Deloitte, BScIT with a cyber major. Sub majored in digital forensics subjects. Currently studying at UNSW ADFA Canberra for his Masters.

Down below we have transcribed some of the talking points we had in the interview with Mitchell.

1) **What motivated you to work in the digital forensics field?**
    a) Cyber peaked Mitchells interest, and saw the large impact of cybersecurity, the effects go well passed, and understanding the consequences of attacks. Cyber plays a massive role in protecting people. Doing that is preventing bad actors (helping people out).

2) **What is your favorite part of being a digital forensics professional?**
    a) Loves the challenge and the hunt. Achieving the end goal. For legal proceedings, companies, intelligence agencies. Finding the information, being able to prove who has done something.

3) **Name an experience that you will never forget thanks to digital forensics ?**
    a) Can't name an experience due to NDA. Though has had personal experience with websites injecting malicious code, and with his skills was able to report it to the website administration team to notify them.

4) **Could you name one time where you have been challenged working in the digital forensics field (specifically with an investigation)**
    a) non disclosure agreement

5) **What process do you follow as a digital forensics professional and would you recommend that process to new students within digital forensics?**
    a) The Field is broad; Identification (knowing plan), Collection (you get one shot, need to make sure you do it correctly), ANalyse, Document, present, preserve (Import stage, ie if process with memory (mem capture, vol memory ftkimager) is favorite tool. As needed for further stages or if other DES need it). Master Copy vs Working Copy → Grab hashes! (of captures) shows proof.
    b) Think acquisition, how will we approach it ? What process are required ?
    c) Will the investigation need other types of data, what network (corporate or individual)

6) **What is the importance of metadata in forensics?**
    a) Metadata is data that describes other data; not visible to general users; similar to fingerprints, adds unique identifiers/characteristics to a file/document; author, last modified date, creation date, deletion date; builds a temporal analysis for the specific file;

b) Can help rebuild the investigation and scenarios; Something removed from a workplace document, metadata can provide a look into the modification history and give insight into investigation; image metadata can be especially useful (gps location, date taken, camera type, sensor pattern); compare camera fingerprint data to other known fingerprints (triangulate location, identify suspects); adds an extra layer of information which is crucial to an investigation

7) **What are the different types of metadata**
    a) Structural Metadata, Descriptive Metadata, Administrative Metadata.
    b) Mostly beneficial for presentations; Not as useful in this midst of an investigation

8) **We are researching the topic of metadata as a professional, what tools do you use to analyse documents metadata ? (What metadata)**
    a) Image data first (FTKImager, Cellebrite), exiftool, fotoforensics, Python scripting (used to carry out specific tasks using different libraries, simple, quick, and powerful), specialty tools)

9) **What would you recommend as sound business practice to secure document Metadata?**
    a) Be cautious as to who you are sending documents to; strip metadata if sent to external recipients
    b) Word has different methods to secure document which can be used in the software
    c) PDF's have electronic signing features
    d) Adobe protect; Adobe security policies

5 Conclusion

Metadata is a very important aspect of Digital Forensics. This report has explored how most computer files contain some sort of metadata. We have demonstrated ways of extracting such metadata using Python scripts, Command-line tools, and even GUI based tools. We concluded that different file types can carry different metadata which can be more or less useful to an investigation, a great example of this is EXIF data in images. GPS coordinates are stored in EXIF data, this information can sometimes conclude or boost an investigation. Information is priceless, and it is scary to think that most files which we sometimes even upload, may have some sort of information stored about us which we may not even know about.

Our report explored ways malware can be embedded in PDFs and even Word document. We explored how both of these file formats can be exploited. PDFs can handle embedded JavaScript and files, which we exploited in our demonstrations. While Word documents can be exploited by injecting code using other word documents such as Excel, which we also explored.

On top of demonstrating how to extract metadata and how to inject malware into a system by using regular looking files we also provided a literature review on malware. This literature review was succinct, but had the sole purpose of providing enough information for this report. We leveraged our interview with a Cybersecurity professional to incorporate even more information into our report. Using what we learned we even provided suggestions into sound business for securing metadata, such as by using encryption.

Finally, we provided our reflections, methodologies, and issues we encountered during our project work. All-in-all, this report has been an extremely interesting learning tool and helped every group member elevate their knowledge on digital forensics and metadata.

7 References (APA 7TH)

[1] Kogalovsky, M. (2013). Metadata in computer systems. *Programming And Computer Software*, *39*(4), 182-193. https://doi.org/10.1134/s0361768813040038

[2] Document Metadata. (n.d.). Retrieved October 16, 2021, from https://www.sciencedirect.com/topics/computer-science/document-metadata

[3] CSDL: IEEE Computer Society. (n.d.). Retrieved October 16, 2021, from https://www.computer.org/csdl/proceedings-article/eisic/2015/8657a182/12OmNBrV1PH

[4] Foote, K. (2021). *A Brief History of Metadata - DATAVERSITY*. DATAVERSITY. Retrieved 7 October 2021, from https://www.dataversity.net/a-brief-history-of-metadata/.

[5] Merriam-Webster. (n.d.). Metadata. In *Merriam-Webster.com dictionary*. Retrieved October 17, 2021, from https://www.merriam-webster.com/dictionary/metadata

[6] Kranz, G. (2021). *What is metadata and how does it work?*. WhatIs.com. Retrieved 8 October 2021, from https://whatis.techtarget.com/definition/metadata.

[7] *Types of Metadata (Plus Examples & Uses for Each) - MerlinOne*. MerlinOne. (2021). Retrieved 7 October 2021, from https://merlinone.com/types-of-metadata/.

[8] Daniel, L., & Daniel, L. (2011). Digital forensics for legal professionals : Understanding digital evidence from the warrant to the courtroom. ProQuest Ebook Central http://ebookcentral.proquest.com Created from uts on 2021-10-18 04:01:53.

[9] Mansurov, N. (2021). *What is EXIF Data and How You Can Remove it From Your Photos*. Photography Life. Retrieved 7 October 2021, from https://photographylife.com/what-is-exif-data#what-is-exif-data.

[10] Pauli, D. (2016). *Dark web drug sellers shutter location-tracking EXIF data from photos*. Theregister.com. Retrieved 4 October 2021, from https://www.theregister.com/2016/09/19/dark_web_drug_sellers_shutter_locationtracking_exif_data_from_photos/.

[11] Tindall, L. (2018). *PDF Embedding Attacks | Nora Codes*. Nora.codes. Retrieved 8 October 2021, from https://nora.codes/post/pdf-embedding-attacks/.

[12] Stokes, P. (2019). *Malicious PDFs | Revealing the Techniques Behind the Attacks*. SentinelOne. Retrieved 6 October 2021, from https://www.sentinelone.com/blog/malicious-pdfs-revealing-techniques-behind-attacks/.

[13] Lukan, D. (2020). *PDF file format: Basic structure [updated 2020] - Infosec Resources*. Infosec Resources. Retrieved 7 October 2021, from https://resources.infosecinstitute.com/topic/pdf-file-format-basic-structure/.

[14] Evermap. (2021). *Free Software For Exploring and Editing Metadata in PDF files*. Retrieved 15 October 2021, from https://www.evermap.com/autometadata.asp

[15] Swati Khandelwal. (2017). *MS Office Built-in Feature Allows Malware Execution Without Macros Enabled*. The Hacker News. Retrieved 16 October 2021, from https://thehackernews.com/2017/10/ms-office-dde-malware.html

[16] HOID. (2017). *Exploit DDE in Microsoft Office & Defend Against DDE-Based Attacks*. Wonder How To. Retrieved 16 October 2021, from https://null-byte.wonderhowto.com/how-to/exploit-dde-microsoft-office-defend-against-dde-based-attacks-0180706/

[17] Administrator. (2018). *Microsoft Office – DDE Attacks*. Penetration Testing Lab. Retrieved 17 October 2021, from https://pentestlab.blog/2018/01/16/microsoft-office-dde-attacks/

[18] Ameer Pornillos. (2017) *MS WORD BUILT-IN FEATURE (DDE): MALWARE EXECUTION AND ATTACKS DEMO*. Ethical Hackers Club. Retrieved 18 October 2021, from https://ethicalhackers.club/ms-word-built-feature-dde-malware-execution-attacks-demo/

[19] *Online exif data viewer*. Online exif data viewer. Retrieved 7 October 2021, from https://www.metadata2go.com/.

[20] Asim Code. (2021). *Exifread to get the EXIF data from an image in Python* [Video]. Retrieved 13 October 2021, from https://www.youtube.com/watch?v=FvFUBr10b9k.

[21] *ExifRead*. PyPI. Retrieved 13 October 2021, from https://pypi.org/project/ExifRead/.

[22] *PyPDF2*. PyPI. Retrieved 9 October 2021, from https://pypi.org/project/PyPDF2/.

[23] Whitington, J. (n.d.). PDF Explained. Retrieved October 19, 2021, from https://www.oreilly.com/library/view/pdf-explained/9781449321581/ch04.html

[24] BigHand. (n.d.). PayneGroup, Inc. - Metadata, Metadata Removal. Retrieved October 20,

2021, from https://new.thepaynegroup.com/metadata-assistant

[25] Microsoft. (n.d.). Retrieved October 22, 2021, from https://support.microsoft.com/en-gb/topic/remove-hidden-data-and-personal-information-by-inspecting-documents-presentations-or-workbooks-356b7b5d-77af-44fe-a07f-9aa4d085966f?ui=en-us&rs=en-gb&ad=gb

[26] Riot, B. (2021, June 20). Remove EXIF & Metadata From Your Files Automatically. Retrieved October 22, 2021, from https://medium.com/swlh/remove-exif-metadata-from-your-files-automatically-21bb82618fc3, Github Script Included:https://github.com/BiasedRiot/Glana