

METADATA IN DIGITAL FORENSICS

by Bert Moss

In this article I will write about what is Metadata, some metadata analysis / extraction tools and the various techniques used in extracting and analyzing metadata mainly from a Digital Forensics point of view.

> s you may already know, data is usually described as a collection of facts, such as values or measurements. It can be numbers, words, measurements, observations or just descriptions of things. Data is presented in:

- Qualitative data Contains descriptive information about something
- Quantitative data Contains numerical information (numbers)
- Discrete data Can only take certain value
- Continuous data Can take any value within a range

ABOUT METADATA

Simply put, metadata can be described as data about data. This descriptive information can be about a particular data set, object, or resource, including its format, when and by whom it was collected. Metadata can describe either physical or electronic resources. Note: The process collecting metadata is also creating metadata traces.

The essential "concept" of metadata has always existed since the collection of information or data began. An example of this concept can be found in a public library system, where information in library card catalogs serves as a collection management and resource discovery tool which can then be indexed. This is a good example of metadata indexing.

Metadata helps to support the data that you produced; this is essential for retrieving information at a later time about a particular file or document. To the average computer user, data is generated every day.

A simple file, word document or spreadsheet file will contain metadata. In more advanced scenarios, data managers who are usually more technically inclined or computer specialists will manually create metadata.

At Scientific or Data Research Warehouses where cataloging is of great significance, specialized software will be used that usually will allow a user to manually create and update metadata. In this scenario, it is not uncommon where the data producer and metadata producer are two separate different individuals or entities. However, in this environment they (Data producer and Metadata producer) must work hand in hand having good communication between them to ensure that the data and the metadata are in tandem.

WORKING WITH METADATA (CREATION)

Creating metadata requires an understanding of both the data you are trying to describe and the metadata standard or scheme itself (for more information about the different meta-



data standards, visit *http://en.wikipedia.org/wiki/ Metadata_standards*). This is important because you will need to decide how you will encode the information. Usually, a single disk file is created for each metadata record where one disk file describes one data set. You can then use a tool for instance, (USGS Online Metadata Editor – online freeware) to enter information into this disk file so that the metadata will conform to the appropriate standard.

METADATA IN FORENSICS

METADATA ANALYSIS / EXTRACTION TECHNIQUES

In Digital Forensics, the recovered data needs to be properly documented. As previously mentioned earlier in the article, the data that is analyzed contains information about "Metadata".

The Digital Forensics industry standards require certified computer examiners or forensics experts to follow certain protocols during their investigations. The main objective of a properly conducted investigation or analysis of a computer or digital media by a professional examiner is to locate possible evidence by means of seizure, search, and retrieval, while maintaining "data integrity" of the original or suspect media. This evidence must be able be upheld in a Court of Law.

A good practice would be to perform a hash of the 'suspect media' prior to beginning any investigation. A forensically clean copy (sanitized copy) of the suspect media should be made bit for bit. This is known as the "Evidence media".

Once the investigation is completed, another hash is then performed against the evidence media to ensure an exact match with the suspect media still exists.

Hashing is the process of getting a validated exclusive fixed string of data that defines the originality of a digital property. A hash is achieved when a collection of information that you may want to pre-



Figure 1. *Metadata of a simple word document file (titled document 15)*

serve is run through a hash function. This process is what we term hashing and the resulting hash is exclusive to the original content and can therefore be used as a fingerprint of that data. Since a hash creates its own exclusive fingerprint or exclusive data signature, it can be used to determine whether a set of data was modified.

The evidence's metadata is extremely crucial as it presents evidence as to;

- · when the data in question was created,
- last accessed or;
- modified or;
- deleted and;
- by whom and ;
- · what time each action was performed.

Data can come in many forms such as, database files, document files, spreadsheet files, picture or media files, email and chat files, as well as temporary internet files (from browsers).

The commercial and free forensic tools listed later in this article, are just a few of the tools that most digital forensic professionals like myself use to carry out metadata analysis during their investigations.

Recommended tools for metadata analysis in Windows based environments are FTK, Paraben and Metadata Assistant, with MacQuisition being preferred for MAC OSX based environments. These tools are mostly automated, and do a terrific job of producing precise metadata extraction results when examining the evidence's media.

You will be able to view, document and create reports for the metadata of the data set investigated. The metadata information can work hand in hand with the hashing results during an investigation. For instance, if the hashing results do not match a particular file, folder or media after the investigations, then the metadata results can be used to determine which possible files included in the investigations or analysis were modified.

METADATA OF A SIMPLE WORD DOCUMENT FILE (TITLED DOCUMENT 15)

The above picture shows a Figure 1 of a simple word document (titled DOCument 15). Here, you

Worl Metadata Tuces			
Built in document properties (Clear All)	~	Default:	Clean
Document Statistics (Reset E dr Time only) Custom document properties (Delete All)		High	Cancel
Last 10 authors (Replace with astensks) Template (Convert to Normal)		Medium	ALLA
✓ Routing stp (Removes entries) ✓ Versions (Delete)	1	Low	Heb
✓ Track Changes (Acces) All) ✓ Fast Saves (Turn off)		Çica Al	@ 2003. Payne Consulting Group. In
2 Hidden text (Delete All except single hidden paragraph marks) 2 Comments (Delete Al) 4 Graphics (Convert to picture) 9 Handride (Delete All		Save Current	Version 1.61.0161
Document Variables (VBA) (Delete All)	*	Get Sayed	Website
Select/UnSelect Metadata types to check			

Figure 2. MetaData Assistant (Payne Consulting Group) – Metadata Options Snapshot



can see information about the word document such as who created the document, the creation date, last saved date and the date the document was last modified. It is this information that is contained in the generated forensic reports.

		1001100		TIEN HEX
		~	Nore	
E [* Dati (NTFS) (noot) (unaloc (orphan	laled space]]		TEMP TEST TEST TEST_JISFA TOMTOM	1.1
operties		×		
1 2↓			5 \$AttrDef	
Date Accessed	19/04/2007 7.21.58	-	SACOURT. HIESIACK	_
Date Created	19/04/2007 7.21.58	- 11	1 \$Bitman	4
Date Modified	19/04/2007 7.21.58		sBoot	0
Encrypted	False		\$130	
Compressed	False		sLogFile	65
Actual File	True		5MFT	88
Alternate Data Strea	am Cr 1		SMFTMirr \$	
DOS Attributes				
Hidden	True			
System	True		1	
Read only	False			
Archive	False			
NTFS Informati	on			
MET Record Numb	ner 8/819264d)			
Record date	19/04/2007 7.21.58			
Resident	True			
Offline	False			
Sparse	False			

Figure 3. FTK Imager (AccessData) – Metadata Snapshot

BrCase Law Enforcement									
His Life Key Tank Hitty									
and a constant of the sector o									
Caus	C Table Diegort Gabler Streeve Qos Cove								
Dinne States Dinennis 4. Seachrite 418		1		same	Last	File Created	Last	Bity Modified	和武
E Hone Al-File Extents 🔒 Remasors ()Refere 1		18	3	OPRIMITYS EVE-36996 TOP of	01/08/08 09: 99-1844	01/08/05 19:29: 1844	01/08/08 09:59 1844	01/08/08 09:59: 38AM	1
+ trees +		30	Э	DEFRALE/E/27/F131E.pf	01/08/08 39:58:1744	01/08/08 09:59:17494	01/08/08 09:99:17494	00/08/08 09:59:17AM	pf.
B-OC Dik Inste		21	3	Lavation	01,08,08 09-99-0784	01/05/05 09: 59-0784	01/08/08 09:59-0744	\$1,08,08 09-59-274M	
-OCO Extend		22	3	VMANARESERVICE EVE-20496453.uf	11/02/07 12:02:4384	11020712-02-4584	11/02/07 11:02-4144	10/02/07 10/02:4584	#
B-Cr. Convents and Settings		27	3	RADICEDE-2019707-07	110007 1102 3744	11/02/07 11:00:21AM	11/02/07 11:02:3748	11/02/07 11:02 3744	#
a CL C Program Page		24	3	WANNELSER EVE-FT28E4gt	01/08/08 10:08:05444	10/02/07 12:00-14404	01/08/08 10:08:0544	01/08/08 10:08:054M	
a contract further that are information		25	b	WANNETRAY ENE ODDFATHE of	01/08/08 12:08:05AH	11/02/07 12:00-1344	01/08/08 10:08:0544	01/06/08 10:08:0544	#
8-(C) WEDOWS		3	0	WWWARSERVICE EVE-300054-64-pf	11/09/09 12:39:1894	11/00/07 11:00:10AM	11/09/09 02:39:1899	11/09/09 02:29:3899	2
-CCTED addin		27	0	STIP DE MEMALI	11/02/07 10:58 2044	11/02/07 12:58:20444	11020710-58-2044	11/02/07 10:58:20AM	#
-CCCC AMPROT		3	2	RUNCHLILENE-SHRENKS of	11/02/07 12:53:2844	11/02/07 10:53-25AM	11/02/07 10:53-2544	11/02/07 10:53:2844	#
-ocia carla		28	0	2018179.8XE-25011314.pf	110007 10.510144	11/02/07 10:51:0544	11/02/07 10:51:0144	10/02/07 10:510 544	#
-Crimecten Ward		m	b	R.MOLITER-2008903.df	11/02/07 12:49-4044	11/02/07 10:49-40494	1002/07 10:49:4044	1002/07 10:49:4044	of.
#000 csc		11	0	SISDOMIR ENE-SUBRICINAN	11/02/07 10:50-3544	11/02/07 10-49-40491	11/02/07 10:50-35AM	11/02/07 10:50:35AM	#
-OCIC Carmen	a	1	5	Distances in the owner of the	CONTRACTOR OF ADDRESS	CONTRACT OF ALL PROPERTY.	LUMPER OF STREET	TAXABLE IN ALCOHOM	-



	Value
name:	statement.pdf
node type	file
generated by	local
\$17E	681131
attributes	Contraction of the second s
* local	
accessed	2013-07-17 18:31:03
changed	2012-12-18 22:05:36
gid	1000 - 0x3e8
inode	456 - 0x1c8
modified.	2012-04-09 15:33:59
orignal path	/media/OS/Downloads/Software/statement.pdf
uid	1000 - 0x3e8
= type	
magic	PDF document, version 1.6
magic mime	application/pdf, charset=binary

Figure 5. SANS Investigative Forensics – Metadata Snapshot

File: vide	o.lst'						
Size: 4	Block	s: 1	IO Blo	k 102	4 regul	ar fil	e
Device 70	01/1792d	Inod	e: 1959	12 1	inks 1		
Access: (0	544/-rw-r-	-r) Uid:	(0/	root)	Gid (0/	root)
Access: 20	10-05-12	11:56:32	000000	0000 +0	0200		



The subsequent snapshots below are metadata information from a few commercial and free Forensic applications (Figure 2).

The metadata options, provides a list of criteria that can be used to produce the resultant metadata (Figure 3 and Figure 4).

FORENSICS METADATA ANALYSIS / EXTRACTION TOOLS (COMMERCIAL)

- FTK v5.0 (Forensic Toolkit) by AccessData (Windows Based Platform)
- Encase Forensic v7.0 by Guidance Software (Windows Based Platform)
- Metadata Assistant v4.0 by Payne Group (Windows Based Platform)
- Helix v3.0 by e-Fense Carpe Datum (Windows/MAC OSX/ Linux Based Platforms)
- Paraben P2 Commander 2.0 by Paraben Corporation (Windows Based Platform)
- BlackLight 2013 R1.1 by BlackBag Technologies (Windows/MAC OSX/IOS Based Platforms)
- MacQuisition 2013 R1.1 by BlackBag Technologies (MAC OSX Based Platforms)

FORENSICS METADATA ANALYSIS / EXTRACTION TOOLS (FREE)

SANS Investigative Forensics Toolkit v2.1 – SFT (UBUNTU Platform) (Figure 5).

CAINE v3.0 – (Linux Platform) (Figure 6).

NOTE

Keep in mind, the tools listed above both commercial and free, have far greater features than just the analysis / extraction of metadata.

ABOUT THE AUTHOR

Bert Moss is the president of Integrated Systems Explorers (Bahamas) (aka. ISEBahamas) and a partner in Tri-Technology Ltd (Bahamas) both located in Nassau, The Bahamas. As an IT professional, he has over 24 years experience in the field of Information Technology and 5 years experience as a Computer Forensic Examiner. Email: isebahamas@coralwave.com

