

JASON RODRIGUEZ

FINAL PROJECT MILESTONE 1

July 22, 2018

EXECUTIVE SUMMARY

In July 2018, student Jason Rodriguez is to conduct computer forensic analysis to examine the file system Harding-3.001. Student Jason Rodriguez objectives for this assignment is to:

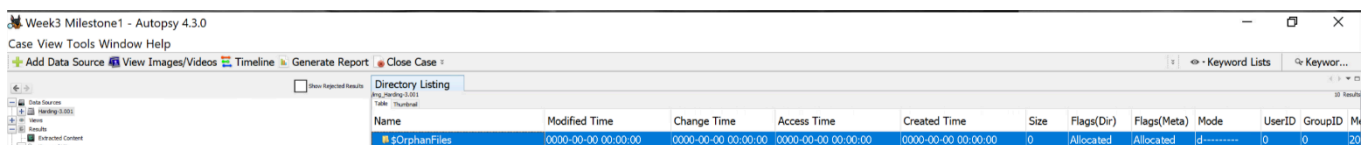
- Using Autopsy as well as FTK Imager to examine the file system image.
- File name, size, and a brief description.
- Investigative relevance or common themes among the files.
- Was the file active or deleted and location of the drive.
- Metadata associated with the file.
- Anything unusual about any files
- Screenshot of each file.
- Applications used to open the file.

Processing Procedures

The analysis was performed utilizing the Forensic Virtual Desktop Infrastructure (VDI)-06 on Windows 10 Enterprise and using Autopsy ver 4.3.0.

Files:

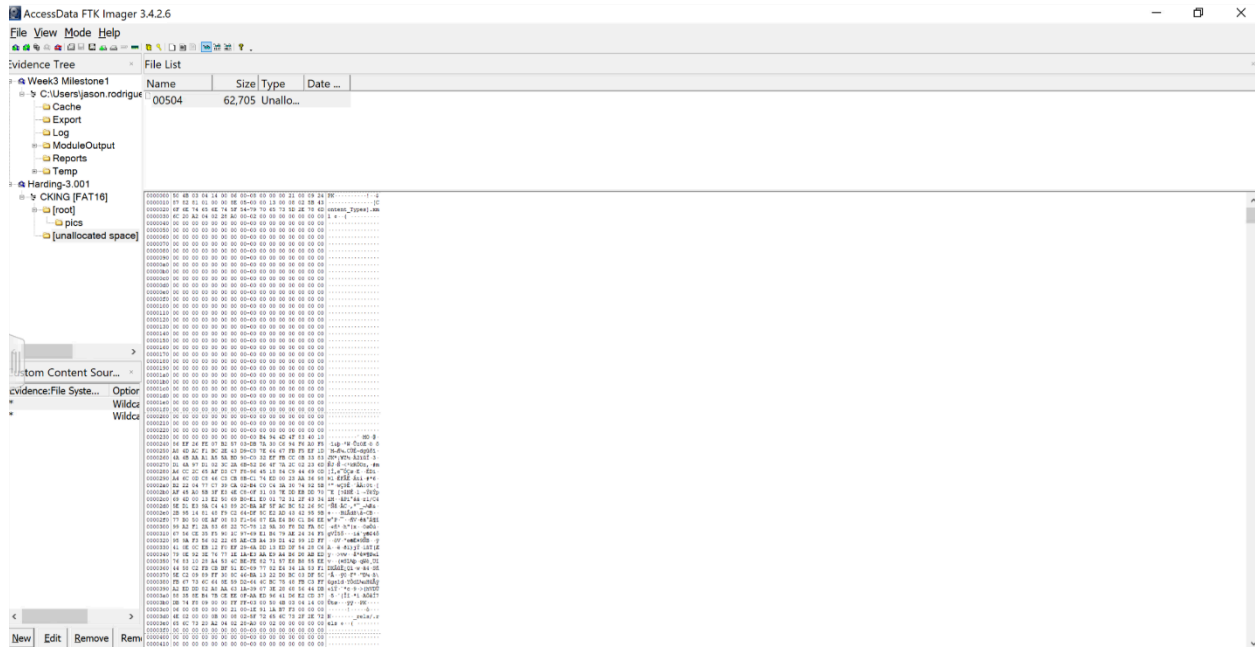
- **\$OrphanFiles**- Are deleted files that still have file metadata in the file system but cannot be accessed from the root directory. The meta address is 2023158.



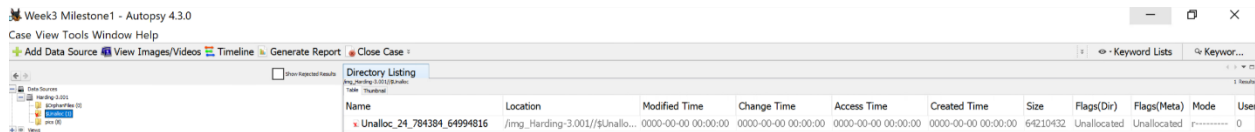
The screenshot shows the Autopsy 4.3.0 interface. The main window displays a 'Directory Listing' for the file system image 'img_harding.3.001'. The listing shows a single entry named '\$OrphanFiles' with various metadata fields.

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID	M...
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	20

- **\$Unalloc-** I was unable to view the content of the folder. The content is an XML. That means is an Extensible Markup Language file. They are plain text files that don't do anything in and of themselves except describe the transportation, structure, and storage of data. Below images are



FTK Imager



Autopsy

- **Pics-** Inside the folder there are three images file types: .png .jpeg and .gif the size of the entire file is 1024bytes. Modified time:2015-03-07 /18:26:20 EST Access time 2015-03-07 /00:00:00 EST Created time 2015-03-07/ 18:27:15 EST.

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID	Meta Addr.
[current folder]	2015-03-07 18:26:20 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	1024	Allocated	Allocated	drwxrwxrwx	0	0	6
[parent folder]	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384	Allocated	Allocated	d-----	0	0	2
7NDhyqf.png	2015-02-25 20:10:26 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	96675	Allocated	Allocated	rwxrwxrwx	0	0	1318
haha.jpg	2015-02-25 20:11:28 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	76915	Allocated	Allocated	rwxrwxrwx	0	0	1319
las-vegas-map-big.gif	2015-02-25 20:12:02 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	312267	Allocated	Allocated	rwxrwxrwx	0	0	1322

- **CKING** (Volume Label Entry)- size is 0, Modified time 2014-09-09/ 09:10:12 EDT\

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID	Me
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	20
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	0
pics	2015-03-07 18:26:20 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	1024	Allocated	Allocated	drwxrwxrwx	0	0	6
CKING (Volume Label Entry)	2014-09-09 09:10:12 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	rw-rw-rw-	0	0	3

- **Links.docx**- Unable to open file, file size is 13318 bytes. Modified time 2015-03-07/ 18:23:00 EST Access Time 2015-03-07/ 00:00:00 EST Created Time 2015-03-07/ 18:27:23 EST.

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID	Me
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	20
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	0
pics	2015-03-07 18:26:20 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	1024	Allocated	Allocated	drwxrwxrwx	0	0	6
CKING (Volume Label Entry)	2014-09-09 09:10:12 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	rw-rw-rw-	0	0	3
links.docx	2015-03-07 18:23:00 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:23 EST	13318	Unallocated	Unallocated	rw-rw-rw-	0	0	8

- **Money.jpg**- File size is 14353 bytes the modified time is 2015-02-28/ 23:38:18 EST Access Time is 2015-03-07/ 00:00:00 EST Created time 2015-03-07/ 18:27:15 EST

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID	Me
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	20
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	0
pics	2015-03-07 18:26:20 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	1024	Allocated	Allocated	drwxrwxrwx	0	0	6
CKING (Volume Label Entry)	2014-09-09 09:10:12 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	rw-rw-rw-	0	0	3
links.docx	2015-03-07 18:23:00 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:23 EST	13318	Unallocated	Unallocated	rw-rw-rw-	0	0	8
money.jpg	2015-02-28 23:38:18 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	14353	Allocated	Allocated	rw-rw-rw-	0	0	4

- **Order.exe**- Size is 9979 bytes. Modified time is 2015-02-23/ 03:13:44 EST. Access Time is 2015-03-07/ 00:00:00

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID	Me
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	20
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	d-----	0	0	0
pics	2015-03-07 18:26:20 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	1024	Allocated	Allocated	drwxrwxrwx	0	0	6
CKING (Volume Label Entry)	2014-09-09 09:10:12 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	rw-rw-rw-	0	0	3
links.docx	2015-03-07 18:23:00 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:23 EST	13318	Unallocated	Unallocated	rw-rw-rw-	0	0	8
money.jpg	2015-02-28 23:38:18 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	14353	Allocated	Allocated	rw-rw-rw-	0	0	4
order.exe	2015-02-23 03:13:44 EST	0000-00-00 00:00:00	2015-03-07 00:00:00 EST	2015-03-07 18:27:15 EST	9979	Allocated	Allocated	rw-rw-rw-	0	0	5
\$FAT1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	126464	Allocated	Allocated	v-----	0	0	20
\$FAT2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	126464	Allocated	Allocated	v-----	0	0	20
\$MBR	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	v-----	0	0	20

Reference:

James, J. I. (2017, January 02). [How to] Beginner Introduction to The Sleuth Kit (command line). Retrieved from <https://dfir.science/2017/01/how-to-beginner-introduction-to-sleuth.html>

TSK Tool Overview. (n.d.). Retrieved from http://wiki.sleuthkit.org/index.php?title=TSK_Tool_Overview