Cyber Defense Organization

Fall 2020 - Digital Forensics + CTF Walkthrough

Attendance

https://forms.gle/hrQfSqmqHPMkAD2S7

Word of the week: CyberChef

What is digital forensics??

Digital forensics is the modern day version of forensic science and deals with the recovery and investigation of material found in digital devices.

My favorite way to explain it to friends and family:

“You know forensics in science with, like, fingerprints?”

“Yea, but it’s like fingerprints on a computer”

How is forensics used?

- Generally speaking, used for investigations
- Public sector: used by police to investigate crimes (murderer left note on pc, meth drug dealer googled “How to make meth” 42 times in the month of february, etc)
- Private sector: used by businesses to investigate incidents (employee went from company A to company B, company A said employee stole information and brought it to company B)

How do they investigate these?

-Through the use of artifacts (any objects that contain data or evidence of something that occurred. Such as logs, registry and hives to name a few)

Autopsy

Autopsy is generally self explanatory although it is extremely powerful. Use these steps as a guideline in your investigation:

Make a new case, title it, etc

Load in the image file

Go through the image's files, there are files you'll want to extract. You can do so by selecting it, right clicking, and extracting. Then you can analyze that file with other tools.

Autopsy is also able to give you plenty of "summary information" on the image

Some locations you should know:

C:\Windows\System32\config

Volume\$MFT

Volume\$Boot

Registry Hives

“ A *hive* is a logical group of keys, subkeys, and values in the registry that has a set of supporting files loaded into memory when the operating system is started or a user logs in.”

These are the artifacts mentioned earlier that investigators use. So far in my career in forensics, registry hives have been the most important aspect. There is more information there than you could imagine.

https://www.dfir.training/ultimate-registry-forensics-cheat-sheet

….ultimate cheat sheet...every location of every artifact you might need.

There are 6 registry hives that reside in the registry of a Windows system

HKLM - Abbreviated from the registry key name HKEY_LOCAL_MACHINE. HKLM stores settings that are general to all users on the computer. On my XP system, HKLM contains five subkeys, HARDWARE, SAM, SECURITY, SOFTWARE and SYSTEM.

This is the registry hive we will be concerning ourselves with today.

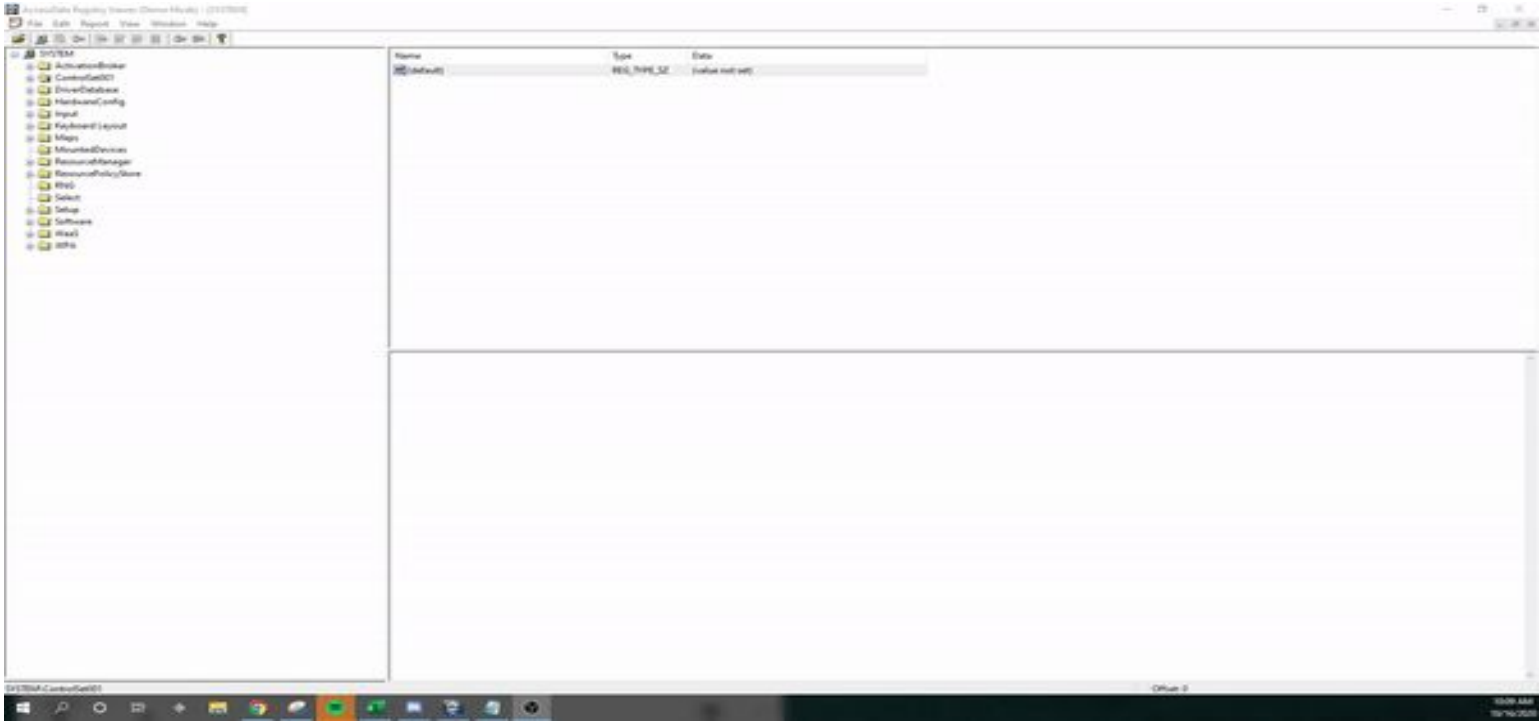
These are located in C:\Windows\system32\config

Registry Keys

Here is a gif of the SYSTEM registry file loaded into registry viewer.

There is tons of useful information an investigator would find here.

Such as time zone information



Important Files - $MFT

There are several very important files within NTFS systems. The most important one would be $MFT.

This is the keeps track of all files on the volume, their logical location in folders, their physical location on the hard, and metadata about the files, including:

- Created Date, Entry Modified Date, Accessed Date and Last Written Date, in the Standard Information Attribute.
- The Physical and Logical Size of the file
- Permissions (security access) for the file

This one single file has information about every single file on the system. That can really be important in an investigation especially when files have been deleted.

Important Files - Prefetch

Prefetch is a folder located at C:\Windows\Prefetch and within it are cache files (.pf) of files on your system.

Prefetch files are great artifacts for forensic investigators trying to analyze applications that have been run on a system. Windows creates a prefetch file when an application is run from a particular location for the very first time. This is used to help speed up the loading of applications. For investigators, these files contain some valuable data on a user's application history on a computer.

The most prominent piece of information prefetch can give you is program execution.

How do we Analyze These Important Files?

How do we Analyze These Important Files?

For real though, that man was Eric Zimmerman, a regular old dude that has contributed a lot to the forensic community. He released zimmerman tools, a group of free, open source tools used to analyze files like the ones we spoke about.

Forensic tools

Name	Version	Purpose
AmcacheParser	1.4.0.0	Amcache.hve parser with lots of extra features. Handles locked files
AppCompatCacheParser	1.4.4.0	AppCompatCache aka ShimCache parser. Handles locked files
bstrings	1.5.1.0	Find them strings yo. Built in regex patterns. Handles locked files
EZViewer	1.0.0.0	Standalone, zero dependency viewer for .doc, .docx, .xls, .xlsx, .txt, .log, .rtf, .otd, .htm, .html, .mht, .csv, and .pdf. Any non-supported files are shown in a hex editor (with data interpreter!)
Evtx Explorer/EvtxECmd	0.6.0.2	Event log (evtx) parser with standardized CSV, XML, and json output! Custom maps, locked file support, and more!
Hasher	1.9.3.0	Hash all the things
JLECmd	1.4.0.0	Jump List parser
JumpList Explorer	1.4.0.0	GUI based Jump List viewer
LECmd	1.4.0.0	Parse lnk files
MFTECmd	0.5.0.0	$MFT, $Boot, $J, $SDS, and $LogFile (coming soon) parser. Handles locked files
MFTExplorer	0.5.1.0	Graphical $MFT viewer
PECmd	1.4.0.0	Prefetch parser
RBCmd	0.5.0.0	Recycle Bin artifact (INFO2/$I) parser
RecentFileCacheParser	1.0.0.0	RecentFileCache parser
Registry Explorer/RECmd	1.5.2.0	Registry viewer with searching, multi-hive support, plugins, and more. Handles locked files
SDB Explorer	1.0.0.0	Shim database GUI
ShellBags Explorer	1.4.0.0	GUI for browsing shellbags data. Handles locked files
SQLECmd	0.5.0.0	Find and process SQLite files according to your needs with maps!
Timeline Explorer	1.1.2.0	View CSV and Excel files, filter, group, sort, etc. with ease
VSCMount	1.0.0.0	Mount all VSCs on a drive letter to a given mount point
WxTCmd	0.5.0.0	Windows 10 Timeline database parser

Your(I guess my) hands on assignment

You (I) will receive a virtual machine file. This virtual machine is a standard Windows 10 machine but includes the following items for your use:

- Autopsy
- All Zimmerman Tools
- Registry Viewer
- An evidence file

You (I) will get 8 questions and this will be a small Capture the Flag. Use what you've learned so far + google to find the answers

Everything you need to practice

Autopsy - https://www.autopsy.com/download/

Zimmerman - https://ericzimmerman.github.io/#!index.md

Registry viewer - https://accessdata.com/product-download/registry-viewer-2-0-0

Image File - https://tinyurl.com/yym243ua

Coming up next week!

Tuesday: Blue Team Practice @ 7pm

Wednesday: Security + @ 5pm

Thursday: Red Team Practice @ 7:30pm

Friday: Forensics something @ 3:30pm

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!