Lab / CTF Preparation

In order to follow along or use the tools that we have used during this presentation, you can follow this guide.

We won't tell you what kind of a machine you need to run the applications, so please ensure that you have enough specs needed.

▪ MUS2019 DFIR CTF

The Magnet User Summit 2019 DFIR CTF Challenge was released to the public. This CTF was created by David Cowen, Matthew Seyer and Jessica Hyde. We'll use this evidence and questions to demonstrate the fundamentals of digital forensics.

In order to play along you will need to download the artefacts - https://drive.google.com/drive/u/0/folders/1E0lELj9NouMwSMGZCI7lXWRqYE2uQCpW

▪ Exterro FTK Imager

Download Link: https://go.exterro.com/l/43312/2022-01-21/f6h1s3

- NOTE: You will need to fill out the form in order to download the software.

FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence. FTK Imager 4.7 now supports the AFF4 format and also supports execution on a portable drive; copy the installation directory to a portable drive, e.g., C:\Program Files\AccessData\FTK Imager.

Create forensic images of local hard drives, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media.

Preview the contents of forensic images stored on the local machine or on a network drive.

Create hashes of files to check the integrity of the data by using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).

▪ Autopsy

Download and install Autopsy. For the demo we will need to user TWO versions of Autopsy as there is a known bug in version 4.19.3 when importing an E01 image file.

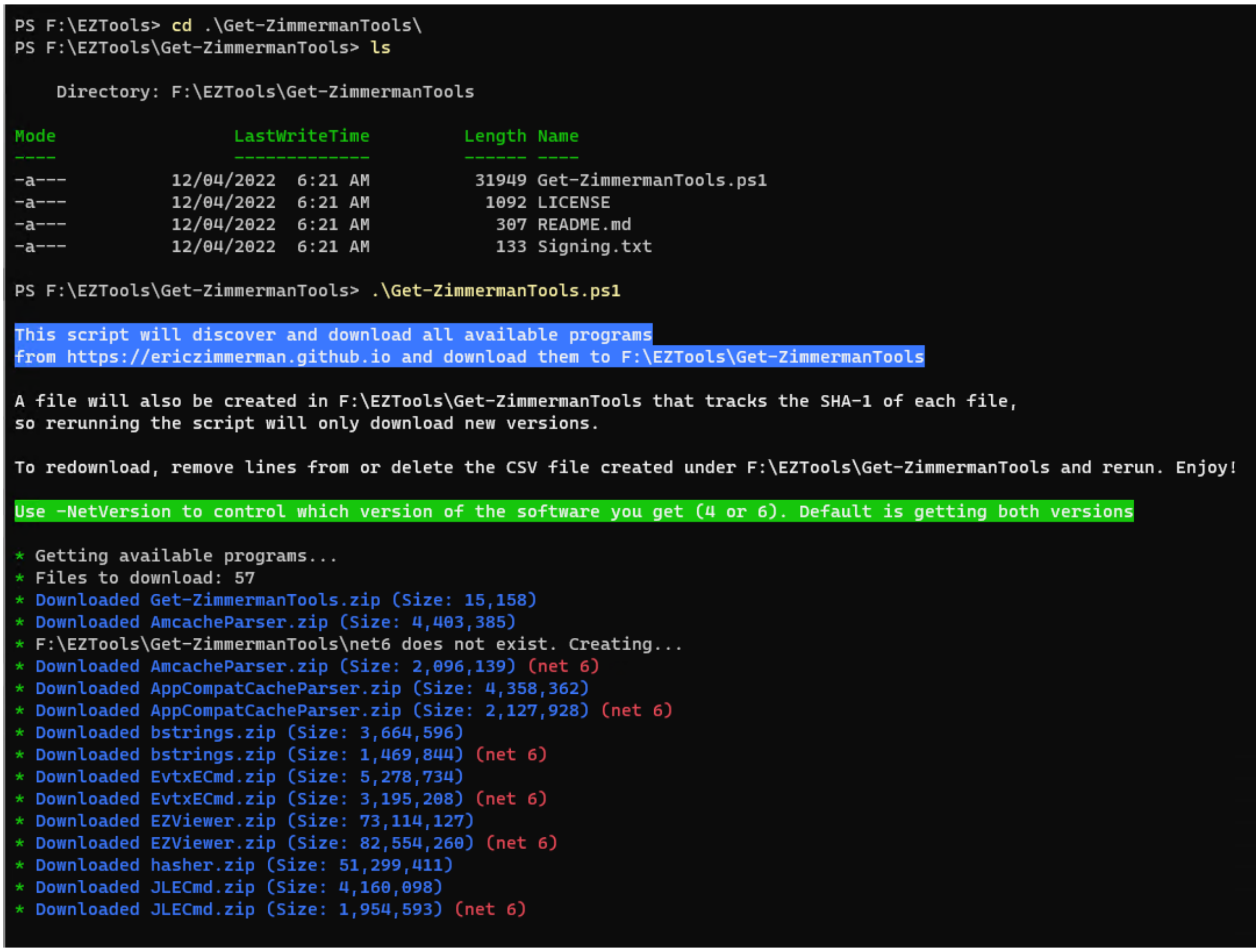
1. Autopsy 4.19.3 – https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.19.3/autopsy-4.19.3-64bit.msi
2. Autopsy 4.19.0 - https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.19.0/autopsy-4.19.0-64bit.msi

You can install both versions of Autopsy side-by-side.

▪ EZTools

Eric Zimmerman provides a PowerShell script to download and catalogue the versions of the tools on your system. Use this script to install and update the EZTools.

```
Git clone https://github.com/EricZimmerman/Get-ZimmermanTools
cd .\Get-ZimmermanTools\
.\Get-ZimmermanTools.ps1
```



```
PS F:\EZTools> cd .\Get-ZimmermanTools\
PS F:\EZTools\Get-ZimmermanTools> ls

    Directory: F:\EZTools\Get-ZimmermanTools

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a---          12/04/2022   6:21 AM          31949 Get-ZimmermanTools.ps1
-a---          12/04/2022   6:21 AM           1092 LICENSE
-a---          12/04/2022   6:21 AM            307 README.md
-a---          12/04/2022   6:21 AM            133 Signing.txt

PS F:\EZTools\Get-ZimmermanTools> .\Get-ZimmermanTools.ps1

This script will discover and download all available programs
from https://ericzimmerman.github.io and download them to F:\EZTools\Get-ZimmermanTools

A file will also be created in F:\EZTools\Get-ZimmermanTools that tracks the SHA-1 of each file,
so rerunning the script will only download new versions.

To redownload, remove lines from or delete the CSV file created under F:\EZTools\Get-ZimmermanTools and rerun. Enjoy!

Use -NetVersion to control which version of the software you get (4 or 6). Default is getting both versions

* Getting available programs...
* Files to download: 57
* Downloaded Get-ZimmermanTools.zip (Size: 15,158)
* Downloaded AmcacheParser.zip (Size: 4,403,385)
* F:\EZTools\Get-ZimmermanTools\net6 does not exist. Creating...
* Downloaded AmcacheParser.zip (Size: 2,096,139) (net 6)
* Downloaded AppCompatCacheParser.zip (Size: 4,358,362)
* Downloaded AppCompatCacheParser.zip (Size: 2,127,928) (net 6)
* Downloaded bstrings.zip (Size: 3,664,596)
* Downloaded bstrings.zip (Size: 1,469,844) (net 6)
* Downloaded EvtxECmd.zip (Size: 5,278,734)
* Downloaded EvtxECmd.zip (Size: 3,195,208) (net 6)
* Downloaded EZViewer.zip (Size: 73,114,127)
* Downloaded EZViewer.zip (Size: 82,554,260) (net 6)
* Downloaded hasher.zip (Size: 51,299,411)
* Downloaded JLECmd.zip (Size: 4,160,098)
* Downloaded JLECmd.zip (Size: 1,954,593) (net 6)
```

Figure 1: Installing EZTools

▪ Cado Host & Cado Live

Cado Host collects forensic artefacts from Windows/Linux/OSX systems (MFT, Logs, etc.) and uploads them directly to cloud storage (AWS/Azure/Google Cloud). Cado Host supports uploading to Amazon AWS, Microsoft Azure and Google Cloud Storage. It also supports storing captured files locally.

Cado Live allows you to build a bootable USB disk to grab a forensic copy of a machine and write that evidence to cloud storage for processing.

Note: we wont use these tools on the day, but they are part of our toolkit and we will walk through setting up a USB drive with Cado Live.