UVF Digital Forensics Toolkit

Introduction

This document is for use by UVF personnel. It documents the approved resources for use in forensic analysis and provides the basic functionality of each. The document is divided into two sections, hardware and software. All hardware resources should be maintained together in one location, providing for an easy mobility to any location. Software listed includes its source of origin to allow new personnel to obtain the needed tools.

Hardware

These items should be taken to every site requiring retrieval of data to facilitate access, documentation, and retrieval of suspect items/data.

- Digital forensics Standard Operating Procedure form
- Chain of custody forms
- Screwdrivers – both Phillips-head and flathead of varying sizes/lengths
- Jump drive containing pre-installed software tools
- Static-proof bags for transporting drives, etc.
- Write blocker (Digital Intelligence - UltraBlock)
- Network cables
- Power cables
- Monitor
- VGA/DVI/HDMI/Diplay Port adapters
- Flashlight
- Wiped hard drives
- Camera
- Pens/Sharpie

Software

While some of this software is valuable in the capture and imaging of suspect devices and drives, others are only useful in lab analysis. Please see the next section for descriptions of each.

- Autopsy
- FTK
- FTK Imager
- Nmap
- OSXPMem
- Snort
- Suricata
- Wireshark
- Volatility

Software

Autopsy

Name: Autopsy
Type: Disk analysis
Developer: Basis Technology
Source: https://www.autopsy.com/
License: Free/Open-source
License Notes: None
Description: Reads disk images, detects partitions, and allows the analyst to view/extract files from the image.
Pros: Has a dedicated way to view deleted files. Filters allow specific file type to be viewed. Detects temporary files.
Cons: With large disk images, the internals of the program get slow, especially while it is indexing files.
Usage: Select the image to begin analysis. Autopsy will then show the partitions and files in a folder structure. By clicking on a folder, the UI will diplay other files and folders available within, allowing the tree structure to be viewed as much as desired. Various filters can be used to search for specific file types. Previews of files are available in the viewer. Files can be exported to the local OS for further review as needed. The display will also show the file name and *real* type, as a file may have been re/mis-named with a different extension.

FTK

Name: FTK
Type: Disk analysis
Developer: AccessData
Source: https://accessdata.com/products-services/forensic-toolkit-ftk
License: Paid
License Notes: Requires dongle for activation and use
Description: Reads disk images, detects partitions, and allows the analyst to view/extract files from the image.
Pros: Tabs across the top of the work area filter files by type. Numerous hashes given. Bookmarking allows for easy access to files and reports.
Cons: Expensive license. Does not detect temporary files.
Usage: Select the image to begin analysis. FTK will then show the partitions and files in a folder structure. By clicking on a folder, the UI will diplay other files and folders available within, allowing the tree structure to be viewed as much as desired. Tabs across the top can be used to search for

specific file types. Previews of files are available in the viewer. Files can be exported to the local OS for further review as needed. The display will also show the file name and *real* type, as a file may have been re/mis-named with a different extension.

FTK Imager

Name: FTK Imager
Type: Drive copying/replication
Developer: AccessData
Source: https://accessdata.com/product-download/ftk-imager-version-4-2-0
License: Free
License Notes: None
Description: Allows file copy or bit-by-bit replication of a drive.
Pros: Free. Simple to use.
Cons: On-screen documentation is lacking. Windows only. Does not guarantee that data is not written to the drive being replicated.
Usage: Connect the drive in question to the computer through a write blocker. Make sure that an empty drive is also connected, as this will be the destination for the source drive. Select “Create a Disk Image” from the “File” menu. With “Physical Drive” as the source type, choose the drive to image from the source selection drop-down. Now, click the “Add...” button to add the destination drive. If the “Verify images after they are created” is checked then hashes will automatically be generated and displayed by the tool. Select “E01” as the image type. Info can be added about the device if desired, but the image destination and filename must be added. Click “Start” and wait for hours while the imaging occurs!

Nmap

Name: Nmap
Type: Network scanner
Developer: Insecure.Com LLC
Source: https://nmap.org/
License: Free
License Notes: None
Description: Tool used to scan networks for open ports, the IP address of visible systems, etc.
Pros: Free, simple to use.
Cons: Known by intrusion detection systems as a tool often used by malicious actors, running scans may trigger rules that cut off your access.
Usage: Once installed, run from the command line. To scan a block, (let’s take the local block, for example,) type `nmap 192.168.0.0/24` to get a list of devices and ports that are accessible.

OSXPMem

Name: OSXPMem
Type: Memory capture
Developer: Volatile Systems/Google Inc
Source: http://www.rekall-forensic.com/
License: Free/Modifiable
License Notes: None
Description: Allows the capture and analysis of memory (RAM) from target system.
Pros: Free. Lots of options.
Cons: Getting old; the last release (at the time of this writing) was two years ago.
Usage: Install it on a jump drive. Once it is loaded into the target machine, run `kextload ./osxpmem.app/MacPmem.kext/` With the file loaded, execute `./osxpmem.app/osxpmem --format fat32 -o {drive}/pmem.dump`; be sure to replace {drive} with the letter of the external hard drive. Once the capture has finished, eject the drive.

Snort

Name: Snort
Type: Network intrusion detection
Developer: Cisco
Source: https://www.snort.org/
License: Free
License Notes: None
Description: Analyzes network traffic and applies rules to see if the traffic should be flagged.
Pros: Free, lots of rules available.
Cons: Will not catch everything. False positives are also possible.
Usage: Snort can either run on current traffic or on pre-captured data. For our analysis we use packet captures given to us for analysis. Given a file named "captures.pcap", and a Snort configuration called, "snortPcap.conf", in the terminal execute `snort –c snortPcap.conf –r captures.pcap` to run the captures through Snort. Any alerts will be displayed to the terminal.

Suricata

Name: Suricata
Type: Network intrusion detection/signature matching
Developer: Open Information Security Foundation
Source: https://suricata-ids.org/
License: Free/open-source

License Notes: None

Description: Analyzes network traffic and applies rules to see if the traffic should be flagged.

Pros: Open source, extensible enough to be used for pattern-matching within text files as well.

Cons: The eye on the logo makes the animal look like he’s coming for you.

Usage: Create a file, add Suricata rules to it (view the documentation), and save it. Then, add the ruleset to /etc/suricata/suricata.yaml (on Linux). To scan the desired file, run `sudo suricata -c /etc/suricata/suricata.yaml -r path/to/file` and view the results in `/var/log/suricata/fast.log.`

Wireshark

Name: Wireshark

Type: Network traffic analysis

Developer: Wireshark Foundation

Source: https://www.wireshark.org/

License: Free

License Notes: None

Description: Used to view network traffic, including source and destination IP addresses/sites, allows for export of transferred files, and has filtering capabilities.

Pros: Widely used in industry, lots of documentation available, lots of abilities in the tool.

Cons: Volume of information can be overwhelming without proper filtering.

Usage: Load the capture file. To quickly see what files were received over the internet, go to the menu and choose `File → Export Objects → HTTP`. Each item can also be saved to the host OS, allowing further analysis with VirusTotal and other methods. Filters can be used to search for specific items, such as `ip.addr==x`, where “x” is the IP address to search for. See the documentation for a list of filters that can be applied to the data set.

Volatility

Name: Volatility

Type: Memory analysis

Developer: Volatility Foundation

Source: https://www.volatilityfoundation.org/

License: Free/open-source

License Notes: None

Description: Allows review of in-memory actions, including running processes, startup scripts, network traffic, and so forth. Initially assesses OS type to suggest a memory profile.

Pros: Free, provides numerous ways to review a memory dump.

Cons: Command line only. Makes review more difficult with larger outputs.

Usage: The OS must first be ascertained from the dump. Run `volatility -f {file} imageinfo` to see the possible profiles that should be used. We will assume that our target memory file is named “lab.vmem”, and that the profile is “WinXPSP2x86”. To verify that the profile is correct, run `volatility -f lab.vmem --profile=WinXPSP2x86 kdbgscan`; if the tool returns a number of real processes and modules being loaded, then there was success with the profile. To see running processes, use `volatility -f lab.vmem --profile=WinXPSP2x86 psscan`. The full process tree can be seen with `volatility -f lab.vmem --profile=WinXPSP2x86 pstree`. For network connections, use `volatility -f lab.vmem --profile=WinXPSP2x86 connscan`, and for open socket connections use `volatility -f lab.vmem --profile=WinXPSP2x86 sockscan`. To dump the memory of a process, execute `volatility -f lab.vmem --profile=WinXPSP2x86 procdump -p {pid} --dump-dir {directory to save file to}`.