# Forensics Toolkit

## FTK Imager

## Review:

Windows software platform that performs a variety of imaging tasks including acquiring the running memory of the system. Using this tool, it’s possible to navigate through the full file structure of the machine with ease and can even search for different file names or types. This tool is a great way to dive deep into the suspect computer and file system.

## Notes:

Use Instructions:

* Once downloaded, install the executable in the Tools partition of the USB drive. Open the FTK Image folder and run the executable as administrator.
* Click on File and then on Capture Memory.
* Destination File: Browse to the Evidence partition of the USB drive attached to the system and provide a name for the capture file.
* Check Include Pagefile
* Click on Capture Memory

## Download:

* <https://accessdata.com/product-download/ftk-imager-version-3.4.3>

## Windows PMEM

## Review:

This tool can be used to gain access to physical memory on a device. This tool can be used to acquire physical memory without installing anything on the machine being analyzed. The output can be sent to a netcat listener, so it doesn’t have to write the output to memory. The use instructions below highlights that functionality.

## Notes:

Use Instructions:

* Uses the output file format of AFF4 (Advanced Forensic Framework 4).
* To acquire physical memory:
  + Open Windows Command Prompt as an administrator
  + Type D:\winpmem-2.1.exe -h (help menu)
  + To configure Winpmem to acquire the memory of system:
    - D:\winpmem-2.1.exe –format raw -o e:\Laptop1
* This tool can be deployed on remote systems through native applications such as Remote Desktop or PsExec. Once installed on the remote system, the output can be piped to another system using netcat.
  + Command:
    - C:/winpmem-2.1.exe - | nc 192.168.0.56 4455

## Download:

* <http://releases.rekall-forensic.com>
* Available for Linux, macOS, and Windows systems.

## F-Response:

## Review:

Software platform that allows incident response analysts to perform remote acquisition of evidence over a network. This doesn’t require direct access through SSH or RDS to the remote system.

## Notes:

Use Instructions:

* Install F-Response Enterprise
* Navigate to the menu Scan and click Custom Scan.
* Enter suspect system’s IP address.
* Click OK.

(Textbook Page 178)

## Download:

* <https://www.f-response.com/buyfresponse/software>

## Snort

## Review:

Snort has a lot of different tools that can be used, such as: a sniffer mode, packet logger mode, or a network intrusion detection system mode. These tools can be very useful during a forensic investigation. As part of our analysis, Snort was useful in comparing network captures against preconfigured snort rules to see if there are any signs of a viruses. The use instructions are for that scenario. Other instructions can be found here: <https://www.snort.org/documents#OfficialDocumentation>

## Notes:

Use Instructions for Windows (From Class Instruction):

* Step 1.
  + Download WinPcap installer: http://www.winpcap.org
* Step 2.
  + Install WinPcap
* Step 3.
  + Download the Snort installer.exe: http://www.snort.org
* Step 4.
  + Install Snort
* Step 5.
  + Register an account with Snort
* Step 6.
  + Download the Snort rules that match your version (e.g., snortrules-snapshot-xxxxx.tar.gz).
* Step 7.
  + Decompress the Snort rules (see 7-zip)
* Step 8.
  + Move the rules and preproc\_rules folders into your Snort installation folder.
* Step 9.
  + Open the config file: c:\Snort\etc\snort.conf and make the following changes:
    - 
* Step 10.
  + In the rules folder create a white\_list.rules file and a black\_list.rules file. They can both be empty.
* Step 11.
  + Run Snort
    - snort -r <pcap file> -c <config file>
      * \*this may not run on pcap-ng files
* Step 12.
  + See alerts
    - Check the Snort/log file for alert.ids

## Download:

* <https://www.snort.org>

## Volatility

## Review:

Volatility is a great tool to acquire artifacts from volatile memory. This can provide some critical information into the run-time state of the machine. This tool can be used to look into network connections, malware signatures using Yara, extracting Windows event logs, and more.

## Notes:

Use Instructions:

* Download Volatility
  + sudo apt-get install volatility
* Navigate to directory where Volatility.exe is located
* Using suspect memory, find out what profile to use for memory using the following command:
  + volatility-2.6.standalone.exe imageinfo -f memdump3.raw
* With the profile identified from the previous command, run all subsequent commands using that profile
* Run desired commands:
  + volatility-2.6.standalone.exe –profile=Win7SP0x86 pslist -f memdump3.raw
* To find out other commands:
  + volatility-2.6.standalone.exe -h

## Download:

* Using apt-get install volatility
* Online at <https://www.volatilityfoundation.org/26>

## Wireshark

## Review:

Wireshark is a great tool to analyze network traffic. There are options for live network traffic analysis, or you can import and open a previously captured network capture. Wireshark allows you to filter based on IP address, protocol, and many other packet level options. You can view the content of the packets and this can provide insight into what’s going on with the connection and if there is anything malicious going on.

## Notes:

Use Instructions:

* Download and install Wireshark (<https://www.wireshark.org/#download>)
* From Wireshark, select interface to start collecting packets from
* Packet capture begins
* Filter packets accordingly
* Other Option:
  + Import pcap file
  + Filter packets accordingly

\*Wireshark allows live packet capture or importing of pcap files for analysis

## Download:

* <https://www.wireshark.org/#download>

## Windows Event Viewer

## Review:

Windows Event Viewer is great for troubleshooting and can provide lots of information such as system messages, errors, warnings, security issues, etc. These logs can be obtained from a host using tools such as Volatility and then can be important and analyzed and used to gain insight into the timeline of events in a forensic investigation.

## Notes:

Use Instructions:

* Launch Windows Event Viewer app – Event Viewer Desktop App
* By default, local machine’s event logs are displayed
* Click on a certain Windows Log (Application, Security, System, Setup, etc.)
* Events are displayed on center pane

\*By default, local events are displayed, but you can import other machine’s event logs for analysis

## Download:

* Preinstalled on Windows machines

## WinPrefetchView

## Review:

Anytime an application is started on a Windows machine, a Prefetch file is created by the Windows operating system that contains the files associated with the application. This can provide insight into the associated files with an application and can be very useful in a forensic analysis.

WinPrefetchView is a tool that allows you to view the prefetch files associated with your machine. This allows you to select an application and in the lower pane the list of associated files are displayed, as well as their location.

## Notes:

Use Instructions:

* Download WinPrefetchView.exe (32 or 64-bit) from <https://www.nirsoft.net/utils/win_prefetch_view.html>
* Run WinPrefetchView.exe and open the application
* By default, if running on Windows machine, the prefetch files from local machine are displayed
  + If other prefetch files need to be analyzed, import the necessary DLL files for analysis.
* Click on an application in the top pane and view associated files in the bottom pane.

## Download:

* <https://www.nirsoft.net/utils/win_prefetch_view.html>

## Netcat

## Review:

In a forensic investigation or acquisition netcat is a great tool to acquire host-based evidence over the network. A listener can be setup on the investigators machine and then evidence can be sent over the network to the investigators machine. There are lots of other functions that netcat can perform such as DNS functions, port-scanning, and a tunneling mode.

## Notes:

Use Instructions:

* Download and install netcat (preinstalled on some Linux distros)
  + apt-get install netcat
* For help and for netcat functionality instructions run:
  + nc -h
* To configure a listener and push output to a file:
  + nc -v -l -p 2222 | output.txt
* To send from other host to listener run:
  + some command | nc forensic\_station\_ip 2222

## Download:

* sudo apt-get install netcat
* brew install netcat