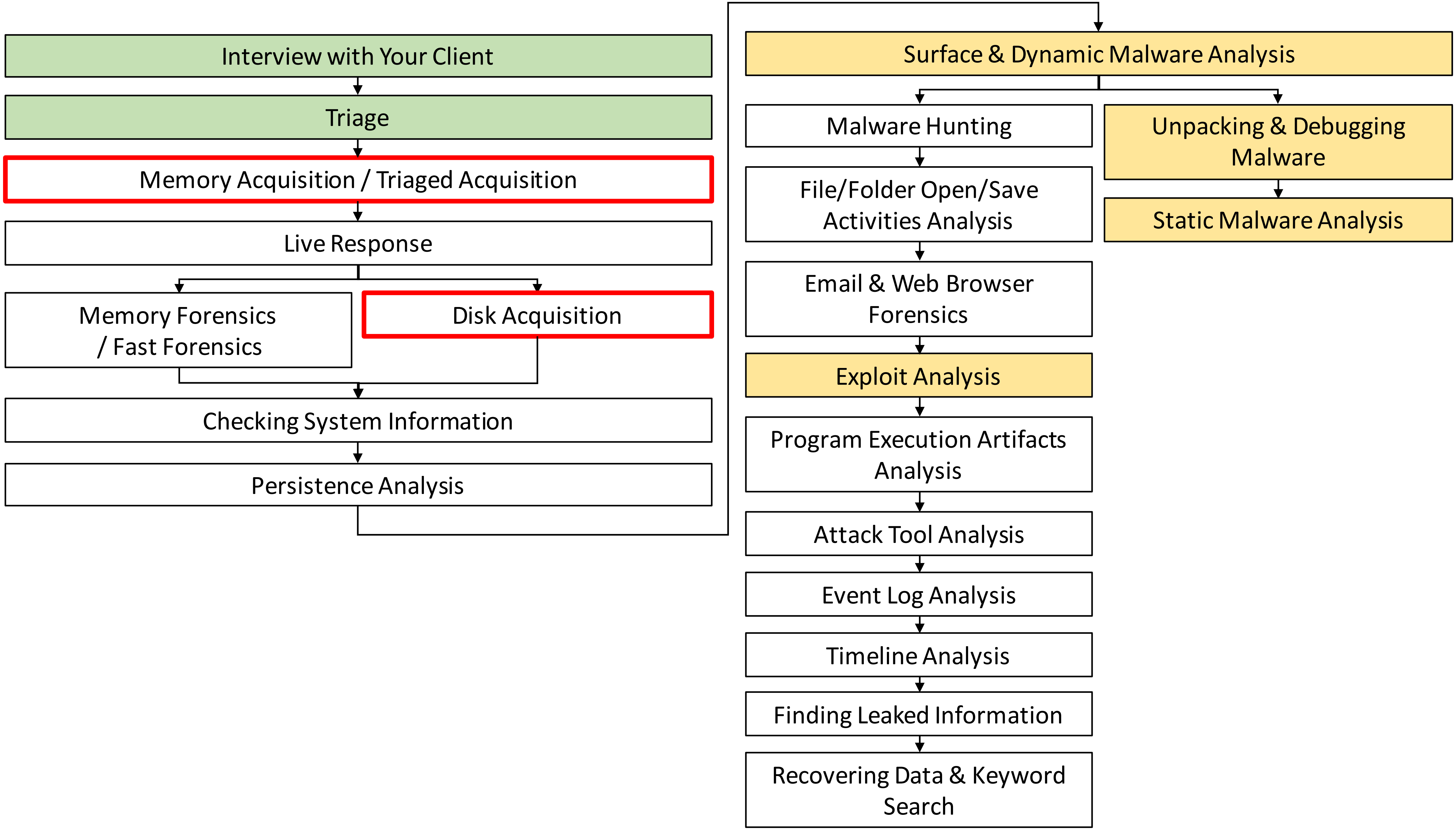
Evidence Preservation (Image Acquisition)



Interview with Your Client

Triage

Memory Acquisition / Triaged Acquisition

Live Response

Memory Forensics / Fast Forensics

Disk Acquisition

Checking System Information

Persistence Analysis

Surface & Dynamic Malware Analysis

Malware Hunting

File/Folder Open/Save Activities Analysis

Email & Web Browser Forensics

Exploit Analysis

Program Execution Artifacts Analysis

Attack Tool Analysis

Event Log Analysis

Timeline Analysis

Finding Leaked Information

Recovering Data & Keyword Search

Unpacking & Debugging Malware

Static Malware Analysis

Evidence Preservation (Image Acquisition)

- Evidence of attack remains on compromised computers just after the incident occurred.
- Various data on the computer are modified and deleted from a moment to a moment.
  - Numerous programs are running on computers, even if the user did not execute them himself/herself.
- We have to acquire the evidences before they are lost.

Evidence Preservation (Image Acquisition) Overview

Data Sources

- Data sources of acquisition are:
  - Computers (servers and clients)
  - Network

- Acquisition should be prioritized based on volatility:
  1. Memory
  2. Disk

Cautions for Acquiring Memory/Disk Images

- When acquiring memory/disk images, **do not**:

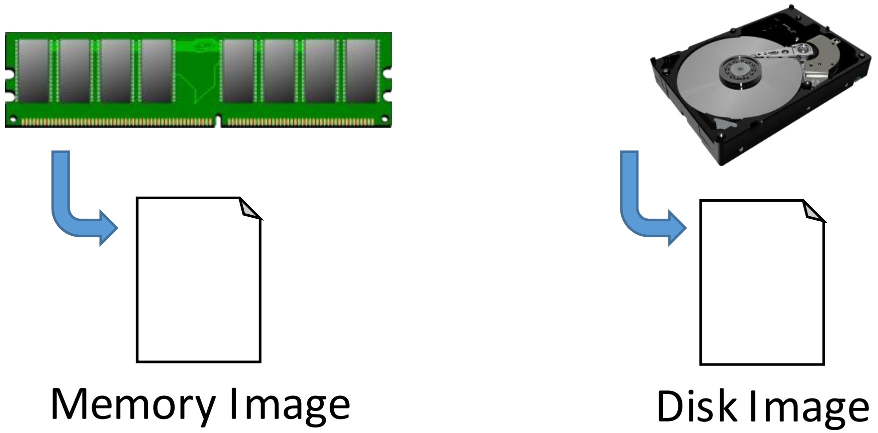
Reboot the computer before the acquisition is done.

Execute any anti-virus scan, as it may modify/delete data/files on memory/disk.

Perform unnecessary operation (such as file creation/deletion).

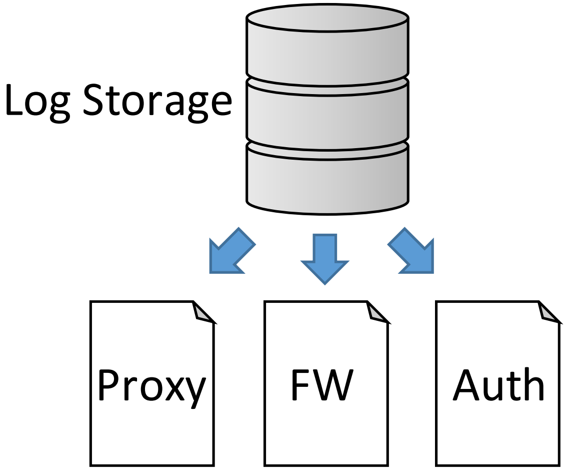
Acquisition from a Computer

- To obtain evidences from a computer, create dump data of a whole memory and disk storage on the victim hosts.
- These tools are called "imaging tools“.
  - Execution of imaging tools require administrator privilege.
  - Dumped data are called "**memory image**" or “**disk image**".



Acquisition from Network Components

- The infected host is on the highest priority for acquiring the evidences.
  - If the evidence on the infected host is lost, it will become difficult to obtain attack details.
- The other network components may also be evidences.
  - Especially the devices that the infected host uses or exists on the route where the infected host accesses the Internet.
    - Logs from firewalls, proxies, etc…
    - Cache data from proxies
- Since these artifacts will be rotated or erased, it is important to acquire the existing contents as soon as possible.



Memory Image Acquisition

Memory Image Acquisition

- Memory images can be acquired by running tools on a running OS.
- Several useful memory imaging tools for Windows includes:
  - WinPmem (Open Source)
  - Comae DumpIt (Commercial)
  - Belkasoft Live RAM Capturer (Free, registration needed)
  - Magnet RAM Capture (Free, registration needed)

Memory Image Formats

- Some frequently used memory image formats:

Format	Extension	Description
RAW	RAW	Copy of the same byte array as the physical memory. The file is not compressed.
Microsoft Crash Dump	DMP	Memory dump created by Windows when application/OS crashes. There are “Small Memory Dump”, “Complete Memory Dump”, and some other dump sizes.
Advanced Forensics Format	AFF*	Open format for storing data. The current version is AFF4, and various tools also support AFF3. It was designed to store disk images, but it also can store memory data. The data can be compressed.

Memory Image Formats and Tools

- Each tools introduced earlier supports some of the formats shown in the previous page.

Format	WinPmem	Comae DumpIt	Belkasoft Live RAM Capture	Magnet RAM Capture
RAW	Y	Y	Y	Y
DMP		Y		
AFF	Y			

  - Comae provides a separate tool for converting between RAW and DMP formats.
- These image formats can convert to each other, although sometimes conversions may fail.
  - Our recommendation is to use DMP.

Memory Imaging Tools and BSOD

- Memory imaging tools sometimes cause bluescreen of death (BSOD).
- Even if the OS stops during the acquisition, retry the procedure after restarting the OS.
  - Many malware has a feature that launches itself during the OS boots up.
    - Therefore, the possibilities of acquiring malware activities remain even after the accidental reboot.

Disk Image Acquisition

Disk Image Acquisition

- Acquisition of disk (HDD/SSD) images may take place on a live system or from an offline system.
- It is recommended to acquire the disk image offline as the disk contents might be changed during the acquisition if it was taken on a running system.
- If the disk is encrypted with tools such as BitLocker or VeraCrypt, it may be necessary to acquire the image on the live system.
  - Many tools cannot decrypt the encrypted disk image.
    - A tool that can decrypt BitLocker: “**libbde**”, https://github.com/libyal/libbde
  - In this case, launch tools from a removal media like USB thumb drive.
    - Do not install tools on a running system as the installation might overwrite disk contents.

Disk Image Formats

- Some frequently used disk image formats:

Format	Extension	Description
RAW	RAW	Copy of the same byte array as the physical disk. The file is not compressed. “dd” in Unix produces this format.
Expert Witness Format	E01	Image format for EnCase, which was formally called Expert Witness, that is frequently used for taking disk images. It can be compressed, and the contents of the image cannot be modified.
Advanced Forensics Format	AFF*	Open format for storing data. The current version is AFF4, and various tools also support AFF3. The data can be compressed.

Disk Image Formats and Tools

- Several useful disk imaging tools for Windows includes:
  - Guymager (Free)
    - Guymarger is included in DEFT (Linux based forensics distribution), BitCurator, and so on. You can boot it from USB thumb drive and launch Guymarger to create a disk image.
  - AccessData FTK Imager Lite (Free, registration needed)
    - The tool is for Windows, and it can be executed from removal drives without installation.
- Both tools support all three formats introduced on the previous page.
  - For, Guymager, since version 0.7.3, AFF support is turned off by default.
  - It is possible to convert a disk image to other formats.

Triaged Acquisition & Fast Forensics

Fast Forensics

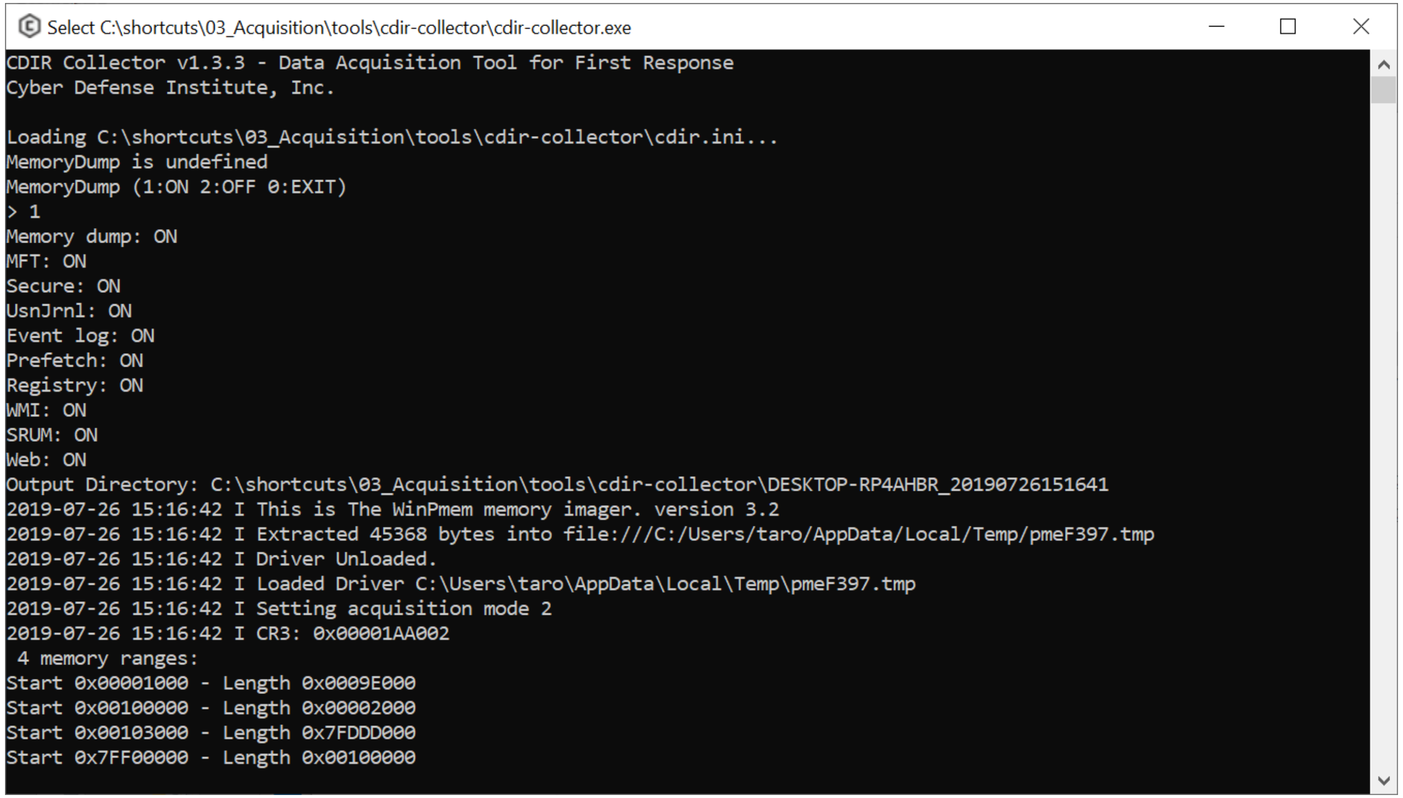
- Nowadays, disks can be several terabytes in size.
    - Makes difficult to take a full copy of a disk.
- Forensics will consume a long time.
- If the deep details of the incident is **not** required, **fast forensics** may be helpful.
    - A possible example of “deep details” is the analysis of malware and its configurations.
    - Fast forensics is to focus on, and illustrate the overview of the incident.
        - It can be finished quickly.

Triaged Acquisition

- **Triaged acquisition** is a method to collect some artifacts for an initial incident response.
  - Some of the examples include: memory images, NTFS metadata, registries, program execution history, logs, and others.
- Triaged acquisition takes longer than just acquiring memory image. However, as the number of artifacts increases, there will be greater chance for faster identification of whether that computer was infected or not.
- Example tools: CDIR Collector, KAPE

Tools for Preserving Evidences (1/2)

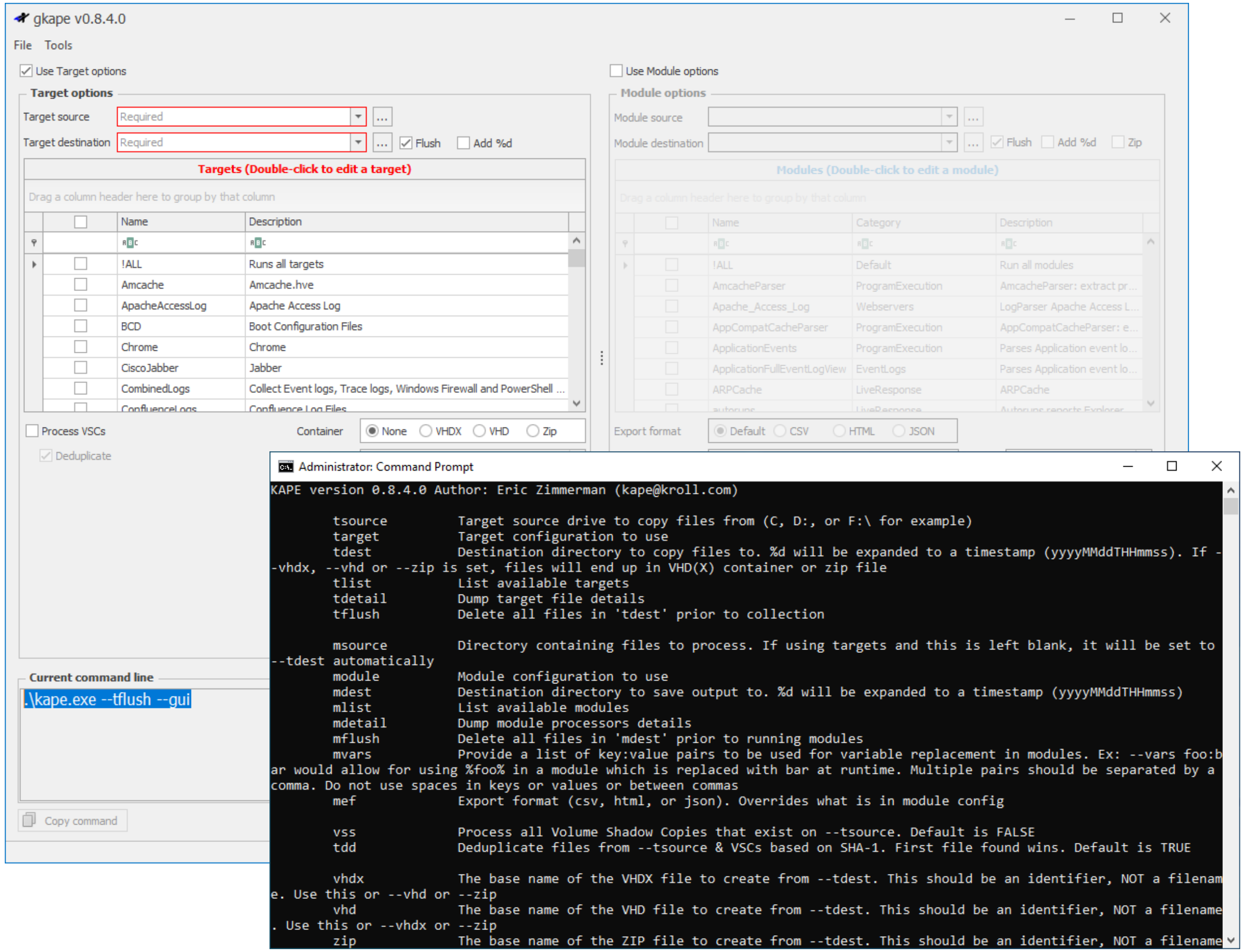
- We will be using “**CDIR Collector**” to preserve evidences.
  - https://github.com/CyberDefenseInstitute/CDIR
- The tool takes memory image and some other artifacts, but it does not take the entire disk image.


Select C:\shortcuts\03_Acquisition\tools\cdir-collector\cdir-collector.exe

```
CDIR Collector v1.3.3 - Data Acquisition Tool for First Response
Cyber Defense Institute, Inc.

Loading C:\shortcuts\03_Acquisition\tools\cdir-collector\cdir.ini...
MemoryDump is undefined
MemoryDump (1:ON 2:OFF 0:EXIT)
> 1
Memory dump: ON
MFT: ON
Secure: ON
UsnJrnl: ON
Event log: ON
Prefetch: ON
Registry: ON
WMI: ON
SRUM: ON
Web: ON
Output Directory: C:\shortcuts\03_Acquisition\tools\cdir-collector\DESKTOP-RP4AHBR_20190726151641
2019-07-26 15:16:42 I This is The WinPmem memory imager. version 3.2
2019-07-26 15:16:42 I Extracted 45368 bytes into file:///C:/Users/taro/AppData/Local/Temp/pmeF397.tmp
2019-07-26 15:16:42 I Driver Unloaded.
2019-07-26 15:16:42 I Loaded Driver C:\Users\taro\AppData\Local\Temp\pmeF397.tmp
2019-07-26 15:16:42 I Setting acquisition mode 2
2019-07-26 15:16:42 I CR3: 0x00001AA002
 4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0x7FDDD000
Start 0x7FF00000 - Length 0x00100000
```

Tools for Preserving Evidences (2/2)

- **KAPE** is another tool for preserving evidences.
  - It is possible to execute it from the Command Prompt, and it contains a GUI wrapper.
    - https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape
    - https://learn.duffandphelps.com/kape
- It supports collection of data related to some applications in addition to the Windows artifacts.
- Its EULA says it is for "internal business use".



Target source: Required

Target destination: Required

	Name	Description
□	!ALL	Runs all targets
□	Amcache	Amcache.hve
□	ApacheAccessLog	Apache Access Log
□	BCD	Boot Configuration Files
□	Chrome	Chrome
□	CiscoJabber	Jabber
□	CombinedLogs	Collect Event logs, Trace logs, Windows Firewall and PowerShell ...
□	ConfluenceLogs	Confluence Log Files

	Name	Category	Description
□	!ALL	Default	Run all modules
□	AmcacheParser	ProgramExecution	AmcacheParser: extract pr...
□	Apache_Access_Log	Webservers	LogParser Apache Access L...
□	AppCompatCacheParser	ProgramExecution	AppCompatCacheParser: e...
□	ApplicationEvents	ProgramExecution	Parses Application event lo...
□	ApplicationFullEventLogView	EventLogs	Parses Application event lo...
□	ARPCache	LiveResponse	ARPCache
□	autoruns	LiveResponse	Autoruns reports Explorer...

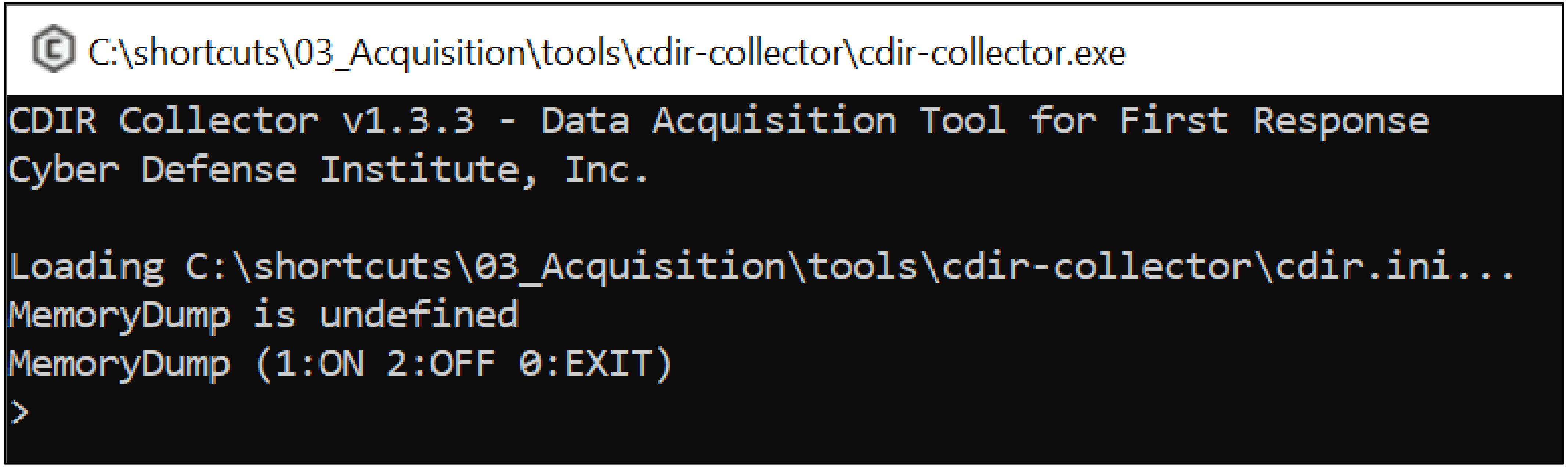
Current command line: .\kape.exe --tflush --gui

```
KAPE version 0.8.4.0 Author: Eric Zimmerman (kape@kroll.com)

        tsource         Target source drive to copy files from (C, D:, or F:\ for example)
        target          Target configuration to use
        tdest           Destination directory to copy files to. %d will be expanded to a timestamp (yyyyMMddTHHmmss). If -
-vhdx, --vhd or --zip is set, files will end up in VHD(X) container or zip file
        tlist           List available targets
        tdetail         Dump target file details
        tflush          Delete all files in 'tdest' prior to collection

        msource         Directory containing files to process. If using targets and this is left blank, it will be set to
--tdest automatically
        module          Module configuration to use
        mdest           Destination directory to save output to. %d will be expanded to a timestamp (yyyyMMddTHHmmss)
        mlist           List available modules
        mdetail         Dump module processors details
        mflush          Delete all files in 'mdest' prior to running modules
        mvars           Provide a list of key:value pairs to be used for variable replacement in modules. Ex: --vars foo:b
ar would allow for using %foo% in a module which is replaced with bar at runtime. Multiple pairs should be separated by a
comma. Do not use spaces in keys or values or between commas
        mef             Export format (csv, html, or json). Overrides what is in module config

        vss             Process all Volume Shadow Copies that exist on --tsource. Default is FALSE
        tdd             Deduplicate files from --tsource & VSCs based on SHA-1. First file found wins. Default is TRUE

        vhdx            The base name of the VHDX file to create from --tdest. This should be an identifier, NOT a filenam
e. Use this or --vhd or --zip
        vhd             The base name of the VHD file to create from --tdest. This should be an identifier, NOT a filename
. Use this or --vhdx or --zip
        zip             The base name of the ZIP file to create from --tdest. This should be an identifier, NOT a filename
```

Acquisition Exercise
- CDIR Collector

Acquisition Exercise - CDIR Collector (1/3)

1. Launch “E:\cdir-collector\cdir-collector.exe".
   Choose "1“ as we need a memory image in an incident investigation.
   WinPmem is used to dump memory by default.

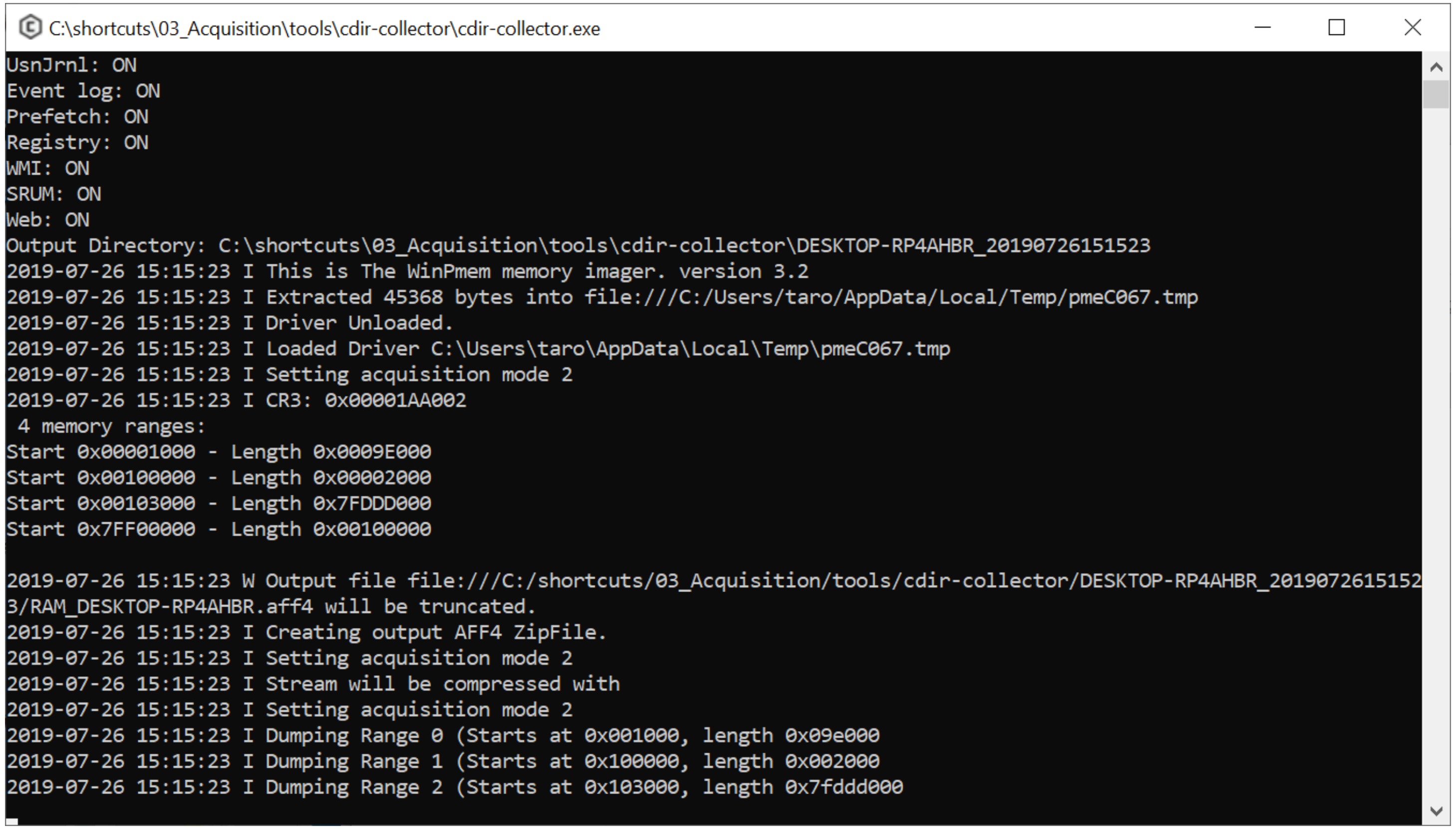


C:\shortcuts\03_Acquisition\tools\cdir-collector\cdir-collector.exe

```
CDIR Collector v1.3.3 - Data Acquisition Tool for First Response
Cyber Defense Institute, Inc.

Loading C:\shortcuts\03_Acquisition\tools\cdir-collector\cdir.ini...
MemoryDump is undefined
MemoryDump (1:ON 2:OFF 0:EXIT)
>
```

Acquisition Exercise - CDIR Collector (2/3)

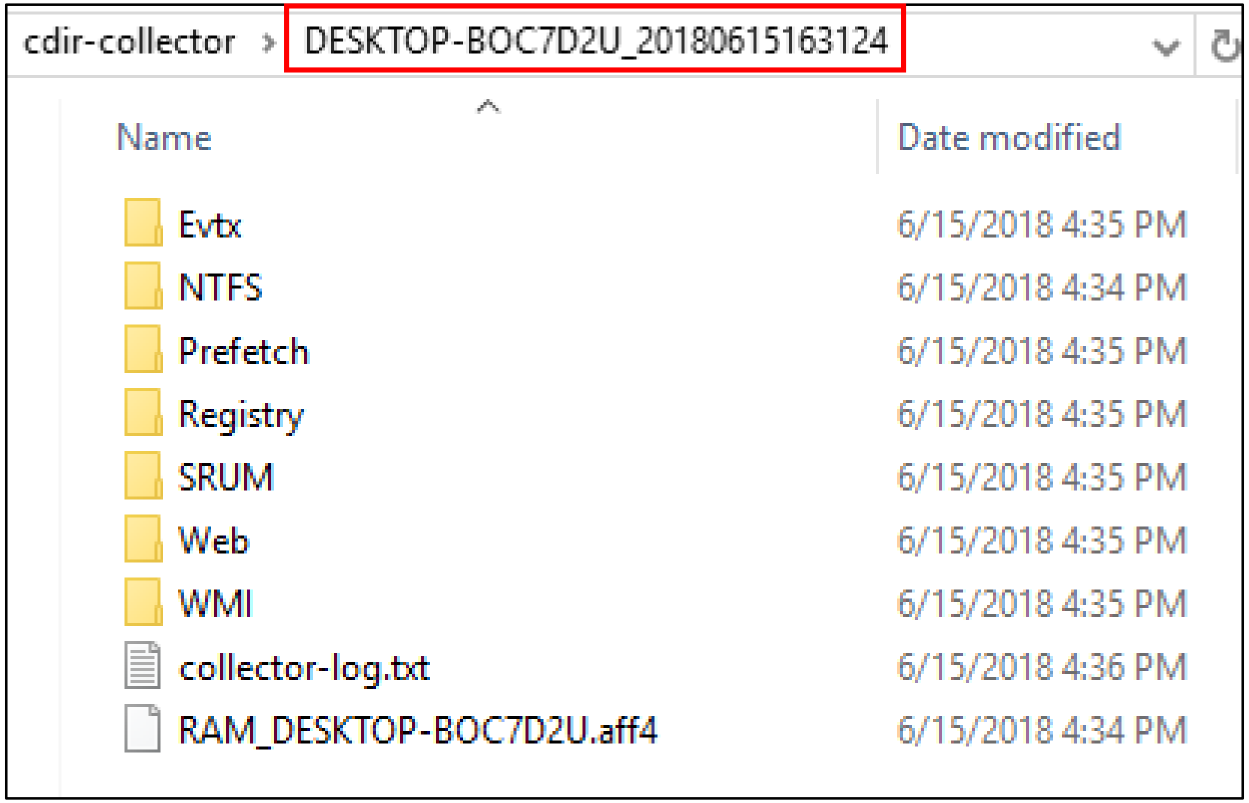
2. The process of collecting artifacts will begin immediately.


C:\shortcuts\03_Acquisition\tools\cdir-collector\cdir-collector.exe

```
UsnJrnl: ON
Event log: ON
Prefetch: ON
Registry: ON
WMI: ON
SRUM: ON
Web: ON
Output Directory: C:\shortcuts\03_Acquisition\tools\cdir-collector\DESKTOP-RP4AHBR_20190726151523
2019-07-26 15:15:23 I This is The WinPmem memory imager. version 3.2
2019-07-26 15:15:23 I Extracted 45368 bytes into file:///C:/Users/taro/AppData/Local/Temp/pmeC067.tmp
2019-07-26 15:15:23 I Driver Unloaded.
2019-07-26 15:15:23 I Loaded Driver C:\Users\taro\AppData\Local\Temp\pmeC067.tmp
2019-07-26 15:15:23 I Setting acquisition mode 2
2019-07-26 15:15:23 I CR3: 0x00001AA002
 4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0x7FDDD000
Start 0x7FF00000 - Length 0x00100000

2019-07-26 15:15:23 W Output file file:///C:/shortcuts/03_Acquisition/tools/cdir-collector/DESKTOP-RP4AHBR_2019072615152
3/RAM_DESKTOP-RP4AHBR.aff4 will be truncated.
2019-07-26 15:15:23 I Creating output AFF4 ZipFile.
2019-07-26 15:15:23 I Setting acquisition mode 2
2019-07-26 15:15:23 I Stream will be compressed with
2019-07-26 15:15:23 I Setting acquisition mode 2
2019-07-26 15:15:23 I Dumping Range 0 (Starts at 0x001000, length 0x09e000
2019-07-26 15:15:23 I Dumping Range 1 (Starts at 0x100000, length 0x002000
2019-07-26 15:15:23 I Dumping Range 2 (Starts at 0x103000, length 0x7fddd000
```

Acquisition Exercise - CDIR Collector (3/3)

3. Collected data is stored in a folder with the computer’s name.

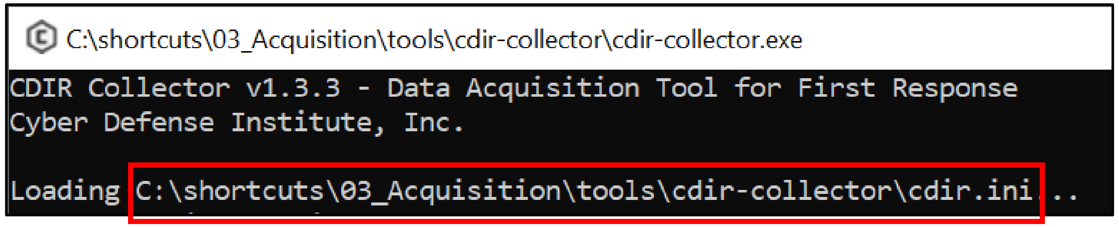


cdir-collector › DESKTOP-BOC7D2U_20180615163124

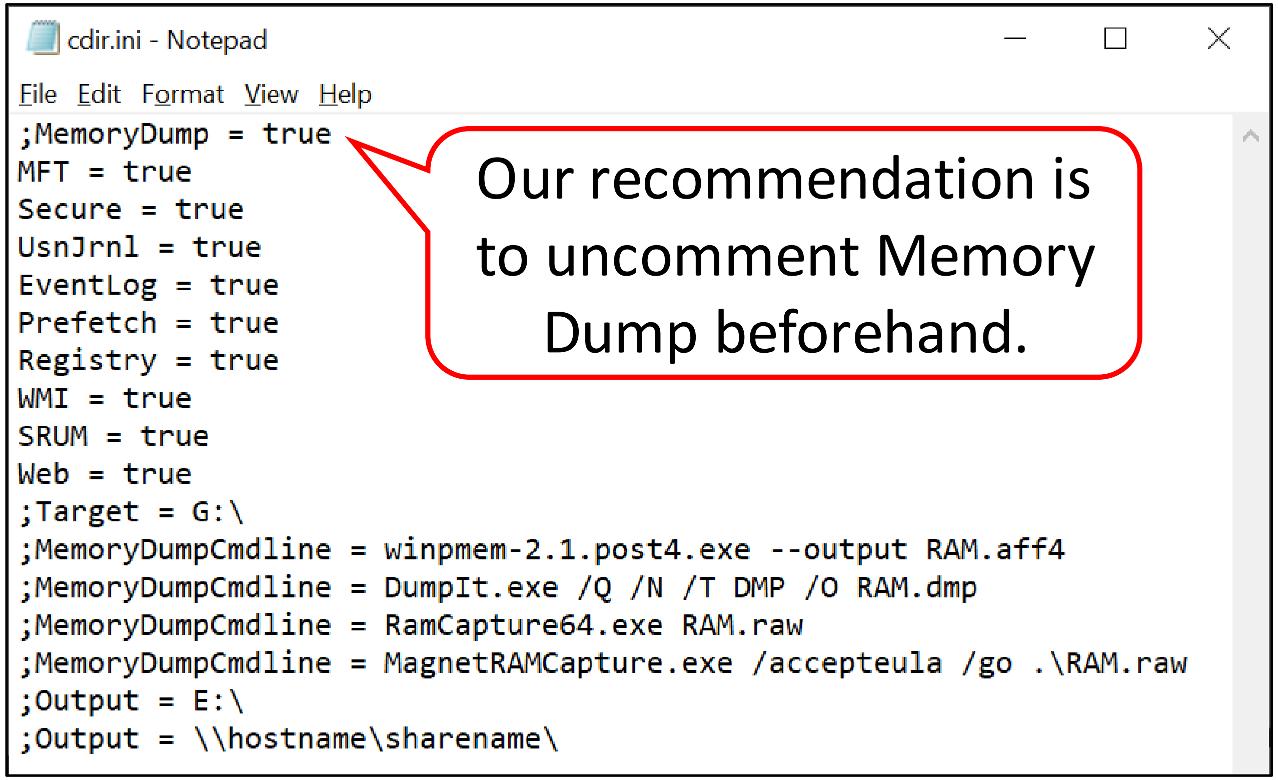
Name	Date modified
Evtx	6/15/2018 4:35 PM
NTFS	6/15/2018 4:34 PM
Prefetch	6/15/2018 4:35 PM
Registry	6/15/2018 4:35 PM
SRUM	6/15/2018 4:35 PM
Web	6/15/2018 4:35 PM
WMI	6/15/2018 4:35 PM
collector-log.txt	6/15/2018 4:36 PM
RAM_DESKTOP-BOC7D2U.aff4	6/15/2018 4:34 PM

Automating CDIR Collector

- By configuring, it is possible to:
  - run it without being asked whether to dump memory or not,
  - specify an alternative memory dump command line, and
  - specify output paths, including a network share.


C:\shortcuts\03_Acquisition\tools\cdir-collector\cdir-collector.exe

```
CDIR Collector v1.3.3 - Data Acquisition Tool for First Response
Cyber Defense Institute, Inc.

Loading C:\shortcuts\03_Acquisition\tools\cdir-collector\cdir.ini...
```



```
;MemoryDump = true
MFT = true
Secure = true
UsnJrnl = true
EventLog = true
Prefetch = true
Registry = true
WMI = true
SRUM = true
Web = true
;Target = G:\
;MemoryDumpCmdline = winpmem-2.1.post4.exe --output RAM.aff4
;MemoryDumpCmdline = DumpIt.exe /Q /N /T DMP /O RAM.dmp
;MemoryDumpCmdline = RamCapture64.exe RAM.raw
;MemoryDumpCmdline = MagnetRAMCapture.exe /accepteula /go .\RAM.raw
;Output = E:\
;Output = \\hostname\sharename\
```

Our recommendation is to uncomment Memory Dump beforehand.

Summary

Summary

- Acquire memory and disk images at the beginning of an incident response.
- It is possible to convert an image file to other formats.
- Acquisition of an encrypted disk must take place on a live system.
- Acquisition priority
    1. Memory
    2. Disk