CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

CERT-EU Security Whitepaper 2012-004

Data Acquisition Guidelines for Investigation Purposes

Ciprian BOLDEA, Dimitrios ANTONIOU
ver. **1.6**
July 19, 2019

TLP: WHITE

Contents

1 Introduction

1.1 Target Audience

This document is aimed at **general IT staff** that may be in the position of being required to take action in response to an IT security incident, and who does not have specific training in the area of computer forensics. **This document only provides high-level guidelines. It does not supersede any specific applicable policies or procedures, which should be followed if they exist.**

Furthermore, this document does not describe the only possible way of performing data acquisition. Different approaches are possible and may be valid. This document should rather be seen as a best practice guideline in case of the absence of more specific local policies and procedures related to this topic.

In case of doubts or any additional questions about this document, do not hesitate to seek further advice and assistance from your respective authorities or the CERT-EU team.

1.2 Foreward

IT security incidents sometimes are of such nature that the organization affected by the incident wants to pursue prosecution. However, often the facts are not necessarily immediately communicated to the police for a variety of reasons, including the fact that their scope and nature is not clear from the beginning. For prosecution to be successful, the chain of custody needs to be preserved in a legally accepted manner, which requires the evidence to be preserved immediately after the detection of the incident.

It should be noted that communication to law enforcement authorities must be made as soon as possible after discovery of the facts, given the volatility of traces and actions that could be taken (Internet identification, etc.). The decision to contact law enforcement authorities lies solely with the organization that is impacted by the incident. CERT-EU may assist, but it will never contact the law enforcement on behalf of the organization.

1.3 Purpose

The purpose of these guidelines is to help IT services to preserve evidence in an IT security incident in such a way that the investigation by IT security experts or law enforcement authorities can be carried out in an optimal manner. This procedure described herein focuses primarily on a case when either an end-user workstation (e.g., a desktop or a laptop) or a mobile device is impacted.

2 Context

2.1 Authority

Before any data acquisition may be done, it must be clearly established who has the authority to perform it. The persons performing the data acquisition must be clearly identified and have the rights (given the situation and based on local policies and procedures) to acquire the data. This right should be clearly documented as part of the procedure.

2.2 Types of Data

There are several types of data that an investigation could require. The data can be of volatile or non-volatile nature:

- **Volatile data** – data that may disappear when the system is switched off, i.e., the data in memory (processes, network connections, etc.), or data that may be deleted for one reason or another (rotated log files, etc.).
- **Non-volatile data** — data on hard disks and other media as well as data on other systems for which there is a risk of alteration through improper handling (logs, etc.).

2.3 Handling

To avoid damage and loss of potentially crucial data, manipulation of the system should be done according to the following four general principles:

1. No action taken should change data held on a computer or storage media that may subsequently be relied upon in court.
2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine these processes and achieve the same result.
4. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

As a rule of thumb, and specifically for cases where prosecution in court is being considered, the original evidence has to be seized as a copy or it will not generally be accepted as valid forensic evidence in court. This applies mainly to computers, peripherals, cabling, and storage devices that must be seized, inventoried and packed following sound a forensic methodology to preserve the chain of custody.

3 Documentation

3.1 Intervention Report

Logbook of actions - document all actions in chronological order. Take photos of the front and back of the client machines and any other relevant detail such as cable connections, environment, etc.

Describe all the actions, and in particular document the following details:

- **Why** - incident that has triggered the alert and caused the forensic intervention (Description, Indicators, Metadata, etc.).
- **When** - timing of forensic intervention and of every single action.
- **Who** – persons performing the actions, e.g., certified Investigator, etc.
- **What** - actions taken on every machine (clearly identified), which could alter their state (insertion of an USB key, interaction with the keyboard, etc.)
- **Where** - location in the infrastructure of the systems involved, physical location, etc.

- **How** - method (tools, etc.) used, data retention.

Any problems encountered and the solutions applied must also be documented in detail. It must be possible to be able to explain the origin of all logs, equipment, etc.

3.2 Network Topology

- Obtain the network diagram at the time of the forensic intervention, if applicable.
- Identify the systems involved in the incident (e.g., firewalls, proxy, IDS, Active Directory, LDAP, etc.) and describe the links between these systems.
- Identify all the sources of logs, the formats of the logs used.

3.3 Impacted Machines

- Fully identify the machines involved in the incident (manufacturer, serial number, user(s), location, etc.).
- Identify the each system's owner and provide a description of the application's or device's purpose.
- Keep the machine in original state **AND** acquire the volatile and non-volatile data on the machine.

4 IT Interventions

4.1 Network Equipment

The following data should be obtained:

- Logs of all intermediate systems involved (e.g., network switches, firewalls, proxy, IDS, Active Directory, LDAP, etc.) for a time window surrounding the incident (if possible, keep all earlier logs as well). Do not filter logs, and if possible keep them in the original format.
- If possible, try to obtain a packet capture of the packets sent/received from the impacted machine before it is unplugged from the network.

4.2 Impacted Machine(s)

If the machine is up and running, the first thing to verify is whether there is a destructive program running on the machine such as disk wiping utilities. Should this be the case, the power plug should be removed as soon as possible to limit the amount of data lost due to the destructive program. For laptops, not only the power plug has to be removed but also the battery.

If encryption is used or suspected to be used, request the relevant service for support and:

- Ensure the machine is running and accessible. If the machine is not running, then it must be seized and NOT powered on. Then try to obtain the decryption password from the appropriate services (e.g., IT helpdesk) or by interviewing the victim or suspect. In any case, never try to boot the machine but take a forensic copy of the hard drive itself and mount it in a dedicated forensic workstation for analysis. If the machine is running, consider taking a live forensic copy of the encrypted hard drives/containers before shutting

the machine down. The exact procedure for this case is more complex and depends on the actual situation, and as such it is outside the scope of this document.

- If an encrypted image is acquired, ensure the password is included in the documentation of the case, so that it may be used to decrypt the disk image later.

If there is no encryption:

- If the machine is running, perform the memory image acquisition - see section Memory Acquisition for an example procedure.
- Shut down the device gracefully.
- Perform the disk image acquisition according to the procedure described in section Disk Acquisition.

5 Tools to Perform Data Acquisition

This section presents an example of tools and procedures that can be used for the acquisition of volatile and non-volatile data. Other tools exist, which could also be used, also other procedures may be valid. The ones presented here are open source, free, and relatively easy to use for acquisition of memory and disk images of an average Windows workstation (**with no encryption/disk passwords used**). In absence of any other guidance or procedures, these should be used to preserve the evidence. The procedures work with both 32 and 64 bit versions of Windows.

5.1 Memory Acquisition

Memory acquisition can be accomplished with one of the three tools presented below. The first two are command line tools, and the last is a GUI application. Regardless of the acquiring method used, it is important to do memory acquisition **BEFORE** any other actions such as:

1. Restarting the machine,
2. Stopping processes
3. Running AV
4. Patching Systems / Fixing Bugs
5. Pull the plug
6. System backup
7. Moving / copying malware
8. Uploading malware to Virus Total etc,

in order to capture important volatile data that might be lost otherwise. Dumping Memory to a local hard drive is also not recommended, otherwise data may be overwritten and lost.

5.1.1 Memory Acquisition with `winpmem` (the recommended method)

Pre-requisites:

- USB stick with enough free space to hold the raw memory image, and a filesystem allowing storing large (i.e., over 2GB) files. NTFS filesystem is recommended for Windows workstations.
- Tool: `winpmem` (`winpmem_3.1.rc3.exe`[1] as of time of this writing) from Rekall-forensic /

[1] https://github.com/Velocidex/c-aff4/releases/download/3.1.rc1/winpmem_3.1.rc3.exe

Volatile Systems stored on the same USB stick.
- The machine needs to be running and accessible (i.e., no locked screen, etc.).
- Administrator credentials (the application needs to be run with administrator privileges).

Procedure:

- Insert the USB stick into the computer that you want to image.
- Start a command prompt as administrator (example for Windows 7): Click *Start*, click *All Programs*, and then click *Accessories*. Right-click *Command prompt*, and then click *Run as administrator*. If the *User Account Control* dialog box appears, confirm that the action it displays is what you want, and then click *Continue*.
- Execute: `F:\>winpmem_3.1.rc3.exe --output <output_file>`, where the `<output_file>` is the chosen name of the image file.
- When the operation finishes, safely remove the USB and cleanly shutdown the computer.

5.1.2 Memory Acquisition with `dumpit.exe`

Pre-requisites:

- USB stick with enough free space to hold the raw memory image, and a filesystem allowing storing large (i.e., over 2GB) files. NTFS filesystem is recommended for Windows workstations.
- Tool: `dumpit.exe` from MoonSols[2] stored on the same USB stick.
- The machine needs to be running and accessible (i.e., no locked screen, etc.).
- Administrator credentials (the application needs to be run with administrator privileges)
- DumpIt may create corrupt memory dumps on more recent Windows 10 computers.

Procedure:

- Insert USB stick into the computer that you want to image.
- Right-click on the `dumpit.exe` application and choose to *Run as administrator*.
- Confirm that you want to proceed. The memory image will be stored directly on the USB stick.
- When the operation finishes, safely remove the USB and cleanly shutdown the computer.

5.1.3 Memory Acquisition with FTK Imager

Pre-requisites:

- USB stick with enough free space to hold the raw memory image and a filesystem allowing storing large (i.e., over 2GB) files are required. NTFS filesystem is recommended for Windows workstations.
- Tool: FTK Imager from AccessData (the version used as an example in this paper is 4.2.0[3]) stored on the same USB stick:
  1. On a machine other than the system to be imaged, install FTK Imager.
  2. Insert the flash drive.
  3. Copy the entire FTK Imager installation folder (typically `C:\Program Files\AccessData\FTK Imager` or `C:\Program Files (x86)\AccessData\FTK Imager`) to your flash drive.
- The machine needs to be running and accessible (i.e., no locked screen, etc.).
- Administrator credentials (the application needs to be run with administrator privileges)

[2] http://qpdownload.com/dumpit/
[3] https://accessdata.com/product-download/ftk-imager-version-4.2.0

Procedure:

- Insert USB stick into the computer that you want to image.
- Right-click on the `FTK Image.exe` and choose to *Run as administrator*. Provide administrator credentials.
- In the *File* menu chose *Capture Memory*.

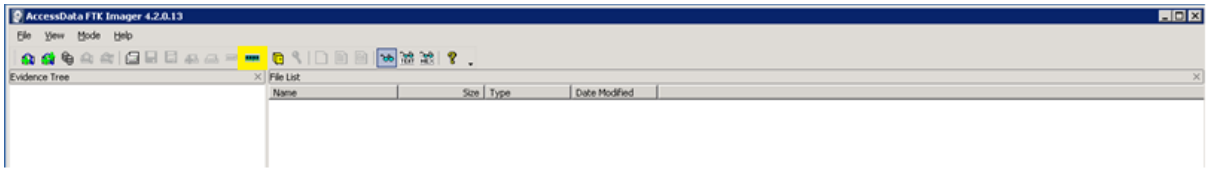

Figure 1: Capture Memory

- Select destination.
- Tick *Include page file* and *Create AD1 file* (if page files and custom content images are needed).

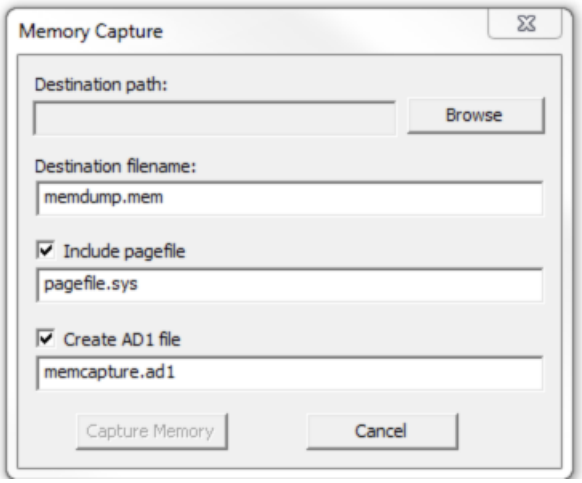

Figure 2: Select destination and files

- When the operation finishes, safely remove the USB and cleanly shutdown the computer.

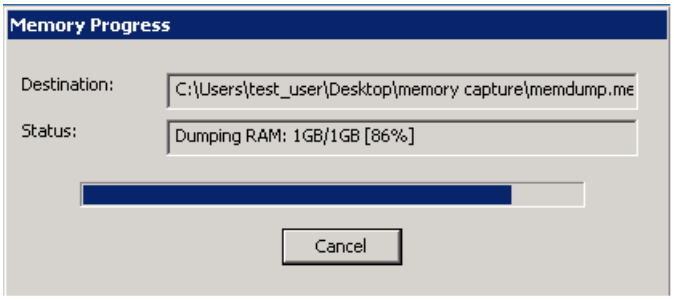

Figure 3: Memory Acquisition Progress

5.2 Disk Acquisition

5.2.1 Disk Acquisition with a Write-Blocker

NOTE: *If you plan to use the acquired data for persecution purposes with law enforcement, the use of a hardware write-blocker is recommended to ensure the integrity and authenticity of the data. Check your local law enforcement requirements for more details and make sure that the used hardware write-blocker is supported and/or certified for such purpose. CERT-EU uses Tableau writeblockers.*

Pre-requisites:

- Write-blocker and cables.
- The hard disk to acquire (removed from the original machine), we will refer to it as *Subject Drive*.
- A dedicated PC, we will refer to it as *Forensic PC*.
- A data acquisition software, e.g. Guymager (Linux) or FTK Imager (Windows).

Installation of the write-blocker:

- *Subject Drive* configuration: before attaching a subject drive to the write-blocker, the drive must be configured as a *Single Master Device* (not slave or cable select).
- Connecting the write-blocker:
- SATA/IDE Drive Interface:
- Confirm the write-blocker power switch is in the OFF position.
- Connect write-blocker to the SATA/IDE *Subject Drive* (both data and power cables).
- *Forensic PC* interface:
- Confirm *Forensic PC* is powered off.
- Connect *Forensic PC* to the write-blocker using USB.
- Power-on the write-blocker and then power-on the *Forensic PC*.
- Prior to disconnecting the write-blocker, shut down the *Forensic PC*.

NOTE: *For a Forensic PC you can use CAINE as explained above, or you can use any other Linux distribution that supports GUYMAGER (e.g., Ubuntu). However, if the Forensic PC is Windows based, we suggest using FTK Imager from Access Data. You can download the FTK Imager tool and the user guide*[4]*. The procedure to use with Guymager has been explained above – this procedure explains the use of FTK Imager. FTK Imager version 4.2.0 was used as an example below.*

Procedure (FTK Imager):

- Run FTK Imager on the *Forensic PC*.
- (Optional) Add the *Subject Drive* to the *Evidence Tree*:
- *File Menu -> Add Evidence Item -> Physical Drive*.
- Select the *Subject Drive* from the drop-down.
- Acquire the data from the *Subject Drive*:
- Select the *Subject Drive* from the *Evidence Tree*.
- In *File Menu -> Create Disk Image*.
- In *Select Source* window -> *Physical Drive*.
- In *Select Drive* window -> select the *Subject Drive*.
- In *Create Image* window -> click on *Add*. You may want to also:
- unselect *Verify images after they are created* if the disk is very large as this is time consuming;

[4] https://support.accessdata.com/hc/en-us/articles/204275735-FTK-Imager-version-3-3-0-User-Guide

- select *Precalculate Progress Statistics*.
- In *Select Image Type -> E01* (Expert Witness Format, which is recommended).
- Fill-in the *Evidence Item Information* as required by your local policy and procedure.
- In *Select Image Destination*:
- Choose an *Image Destination Folder* and *Image Filename*.
- Recommendation for *Image Fragment Size (MB)* is 2047 MB
- Click *Start*
- Once finished, you will then see the *Image Verify Results*. You can also access an *Image Summary* report.

5.2.2 Disk Acquisition without a Write-Blocker

Pre-requisites:

- CD or USB with CAINE (Computer Aided Investigative Environment) Linux distribution[5]. Caine 10.0 was used at the time of writing this document.
- External hard drive with enough free space to hold the raw image of the hard drive to be acquired.
- Access to the machine under investigation.

Procedure:

- Make sure the computer that is to be investigated is properly shut down. Pull the plug only if necessary.
- Connect the external hard drive to the computer.
- Insert CAINE CD, start the computer and ensure that it boots from the CD (some configuration changes in BIOS may be necessary). If necessary, it is also possible to use Live CAINE USB.
- CAINE does not mount any hard drives to prevent unwanted changes on them. Hence, when CAINE has started, mount the external hard drive – the destination for the acquired image, in read-write mode. Use *mounter* - this is a GUI mounting tool that sits in the system tray.

Instructions for mounter usage:

- Left-click the disk icon to mount a device.
- Right-click the disk icon to change the system mounting policy.
- Middle-click will close the mounter application. Prelaunch from the menu.

The mounted devices will not be affected by mount policy changes. Only subsequent mounting operations will be affected.

- Use GUYMAGER to create the image of the disk:
  - Choose *MENU -> Forensic Tools -> Guymager*
  - From the list of devices in the main window choose the one that is to be acquired – e.g. `sda`. Select it for acquiring by right clicking on it and choosing *Acquire image*.
  - Choose the file format (recommended: *Expert Witness Format*, leave the split size of 2047)
  - Optionally fill-in additional notes (case, evidence, examiner, description, etc.)
  - Choose the destination of the image by choosing *Image directory* and *Image filename*.
  - Click *OK* to start the acquisition.

[5] http://www.caine-live.net

- Once finished (it may take several hours), shutdown the computer (*MENU -> Shut Down -> Shutdown*) and remove the CD.
- Disconnect the external hard drive when the computer has shut down.

5.3 VMWare Virtual Machine Acquisition

In case of a VMWare virtual machine, the memory and disk dumps can both be acquired without any service outage on the machine using the following techniques:

- The memory dump can be acquired directly as a file. Please perform a live snapshot (with memory) of the guest machine: the memory file to retrieve from the datastore is the one with a `.vmsn` extension.
- The disk dump can been acquired from a VMWare clone of the machine; the disk is the file with the `-flat.vmdk` suffix.

6 Guide to Mobile Devices Forensic Examination

In the case of detection or suspicion of malicious behavior in mobile devices, in order to perform the examination of the device, it has to be first acquired. Because of the huge diversity in smartphone and tablet hardware and software, collecting evidence from mobile devices poses special challenges and requires special tools. Therefore, the best option for mobile devices is to send the device to CERT-EU or to share a backup of the device.

NOTE: *In both cases, the constituent should perform some necessary steps before sending or backing up the device. Mobile devices are by design intended to communicate via cellular phone networks, and to other networks via Bluetooth, infrared and wireless (WiFi) network capabilities. For this reason, isolation of the device is essential to take place as soon as possible. Isolation of the phone prevents overwriting data to the phone through incoming communications or accidental actions of the examiner as well as the potential destruction of data through remote access or remote wiping.*

The isolation can be performed by simply switching the device off or using *Airplane Mode* function. However, the following should be taken into consideration:

- *Airplane Mode* is are not available in all devices. Also, this function may not prevent some GPS services.
- Switching a device off can cause security functions to be implemented and RAM may be cleared.

In addition, all backups should take place on a PC and not locally on the device (e.g, on an SD card). Backing up on an SD card belonging to the mobile device poses the risk of overwriting valuable data.

6.1 Sending the Mobile Device to CERT-EU

When transporting the mobile device to CERT-EU, it is important to consider the environment it is contained in. The following issues address recommendations for the transportation of mobile devices:

- Magnetic field can cause data to be wiped; ensure the device does not come into contact with any possible magnetic fields.

- Avoid storing evidence in plastic bags; static electricity may cause issues and condensation may affect the device.
- Generally handle with care when transporting in order to avoid any damage.

NOTE: *The constituent should share with CERT-EU any security passcodes used on the device or passwords used for backups. Without such information, the examination will be limited to specific data. Specifically, usually physical acquisitions (or even logical acquisitions in case of Apple devices) are not available without the device's passcode. You should also make sure to send along with the device the corresponding connection cables and charger.*

6.2 Providing Backup of the Mobile Device to CERT-EU

6.2.1 Android Device

6.2.1.1 Manual Extraction Using ADB

ADB – or Android Debug Bridge – is a command-line utility included with Google's Android SDK. ADB can control your Android device over USB from a computer, copy files back and forth, install and uninstall apps, run shell commands, and more. Please follow the instructions available online[6] in order to setup the Android SDK, enable *USB Debugging* on your phone, and finally enabling ADB backup of your phone.

The `adb pull` command can be used to pull single files or entire directories directly from the device on to the forensic examiner's computer. For this method, *USB Debugging* should be enabled on the device.

Device with non-root access can be acquired using logical acquisition techniques. The following steps enumerates the procedure to acquire a non-rooted device:

- Run `cmd.exe` on Windows or terminal window on a Linux/macOS machine.
- Discovering the device via ADB: `adb devices`
- Executing ADB backup : `adb backup -all -f back.ab`
- Unlock device and confirm the *Full Desktop* backup by entering a secure password.

6.2.1.2 Backup Samsung Devices (Android 4.4 or Higher)

Also in this case, the aim is to back up data to computer. Prior to the back-up, *Smart Switch PC Version* app has to be downloaded[7].

1. On the computer download Smart Switch PC version[8].
2. On the computer, launch Smart Switch.
3. Connect your device to the computer using the device's USB cable.
4. On the computer, follow the on-screen instructions to back up data from the device. Then, disconnect your device from the computer.

6.2.1.3 Backup Samsung Devices Using Kies 2.6

1. Connect your device to your computer.
2. Open Kies and click the *Backup/Restore* tab.
3. If necessary, click *Data backup*.

[6] https://developer.android.com/studio/command-line/adb.html
[7] http://www.samsung.com/hk_en/support/skp/faq/1058404
[8] https://www.samsung.com/smartswitch

4. Mark the checkbox next to the content you want to back up. You can select all content by marking the checkbox next to Select all items. Click *Backup*.
5. Click *Complete* when the backup is finished.
6. You can have Kies automatically back up your device every time it's connected by clicking the checkbox next to *Automatically backup when USB connection is established*.

6.2.2 iPhone, iPad, or iPod Touch

Again, we are interested only in backups performed towards a computer not the iCloud. Therefore, backup with iTunes [9] is described[10]:

1. Open iTunes and connect your device to your computer.
2. If a message asks for your device passcode or to *Trust This Computer*, follow the onscreen steps.
3. Select your iPhone, iPad, or iPod when it appears in iTunes.
4. If you want to save *Health and Activity* data from your iOS device or Apple Watch, you need to encrypt your backup: select the box called *Encrypt [device] backup* and create a password. If you don't need to save your *Health and Activity* data, you can make a backup that isn't encrypted. Just click *Back Up Now*. Write down your password and store it somewhere safe, because there's no way to recover your iTunes backups without this password.
5. When the process ends, you can see if the backup finished successfully on the *Summary* screen in iTunes. Just look under *Latest Backup* to find the date and time.

7 Image Integrity

Device acquisition depends on the investigator to thoroughly maintain integrity of the image. Image integrity can be maintained using hashing methods. Image hashing depends on the algorithm investigator defines to check data for integrity. The hashing algorithms such as MD5, SHA1 , SHA256 are utilized to create a unique hash value . The hash value can be re validated at any point of the investigation to denote that the image data stays intact. The procedure of how to verify the MD5 Hash Value of an Image using FTK Imager may be found here: [11]

[9] https://www.apple.com/lae/itunes/download/
[10] https://support.apple.com/en-in/HT203977
[11] https://support.accessdata.com/hc/en-us/articles/203921395-How-to-Verify-the-MD5-Hash-Value-of-an-Image