Incident Response – Data Acquisition Guidelines for Investigation Purposes[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 CERT-EU team.

2 Introduction

IT security incidents sometimes are of such nature that the organisation 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.

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 an end-user workstation is impacted (e.g., a desktop or a laptop). It does not try to describe other specific cases of (e.g., different type of servers, smart phones, and others devices).

4 Context

4.1 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.

4.2 Types of Data

There are several types of data that an investigation could require. These 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.).

[1] NIST (SP 800-86) on "Integrating Forensic Techniques into Incident Response" provides more detailed technical background.

4.3 Handling

To avoid damage and loss of potentially crucial data, manipulation of the system should be done according to the following four general principles[2]:

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 those 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.

5 Documentation

5.1 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:

- **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.

5.2 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.

5.3 Impacted machines

- Fully identify the machines involved in the incident (manufacturer, serial number, user(s), location, etc.).
- Keep the machine in original state **AND** acquire the volatile and non-volatile data on the machine.

[2] Good Practice Guide for Computer-Based Electronic Evidence, v4.0, Association of Chief Police Officers (APCQ), UK.

6 IT Interventions

6.1 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.

6.2 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 on-site a forensic copy of the encrypted hard drives/containers before removing the plug. 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.
- 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 machine - see section 7.1 below for an example procedure.
- Pull the plug on the machine (and remove battery in case of a laptop).
- Perform the disk image acquisition according to the procedure described in section 7.2 below.

7 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.

7.1 Memory Acquisition

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 (http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7) stored on the same USB stick.
- The machine needs to be running and accessible (i.e., no locked screen, etc.).

Procedure:

- The application needs to be run with administrator privileges.
- 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 (Y) that you want to proceed. The memory image will be stored directly on the USB stick.
- When the operation finishes, you may safely remove the USB and cleanly shutdown the computer.

7.2 Disk Acquisition (in the absence of a write blocker)

Pre-requisites:

- CD or USB with CAINE (Computer Aided Investigative Environment) Linux distribution (http://www.caine-live.net).
- 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 shut down. Pull the plug 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 in read-write mode:
    - Choose **MENU -> Forensic Tools -> Safe Mount**
    - Find your external drive on the drop-down list (Use button: **Device Information**), (e.g. **/dev/sdc1**) Make sure that **Make Writable** option is selected and click **OK**.
    - Click **Mount**.
- 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 recommended split size of **2047 MiB**)
    - 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.
    - 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.

7.3 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. The following write blockers are available at CERT-EU:*
>
> - *Tableau T3u for SATA hard-disks;*
> - *Tableau T5 for IDE hard-disks;*

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 Blocke**r 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 **ONE** of the **USB 2.0**, **FireWire 800**, or **FireWire 400** connectors (only USB connectors are supported on Linux)
- 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 (not Lite!) tool and the user guide here: http://accessdata.com/support/product-downloads. The procedure to use with* ***Guymager*** *has been explained above – this procedure explains the use of* ***FTK Imager****.*

Procedure (FTK Imager):

- Run **FTK Imager** on the **Forensic PC**
- (Optional) Add the **Subject Drive** to the Evidence Tree:
  - **Menu File → 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 **Menu File → 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:

- unselect "Verify images after they are created" if the disk is very large as this is time consuming;
- 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.