universidade
de aveiro

Computer Systems Forensic Analysis
AFSC

Documentation and Reporting

Artur Varanda

School Year 2021-2022

All computer and digital media examinations are different

- consider all circumstances as you proceed
- some recommendations may not apply to every situations
- examiners may need to adjust to unusual or unexpected conditions in the field take into account that computers and other electronic devices are borderless
  - ✓ multiple jurisdictions and agencies may be involved

About these guidelines
They just outline general principles; examiners may need to adjust to unusual or unexpected conditions

Electronic devices

In the context of these guidelines "Electronic devices" are all computer system components and other electronic devices, including digital and electronic media.

Physical examination

All electronic devices should be:

- examined physically
  - ✓ include a physical description and detailed notation of any irregularities, peculiarities, identifying markings, and numberings
- catalogued with photos and all details that allow its unique identification
- listed in a inventory
  - ✓ apply the tag system as mentioned in previous classes

When examining a computer:

- clock and time zone:
  - ✓ the system date and time should be collected, preferably from the BIOS
  - ✓ date and time should be compared to a reliable known time source and any differences noted
  - ✓ in the triage phase read the OS configured time zone. By default:
    - Windows OS configures the BIOS' clock to local time
    - Linux and Mac OS configure the BIOS' clock to UTC
- if the BIOS is accessible then
  - ✓ take note of the drives parameters and boot order
  - ✓ if present, take note also of system serial numbers, component serial numbers, hardware component hashes, *etc*

BIOS Access – Warning

Before trying to access the BIOS, first unplug all storage media (SSD, HDD, memory cards, *etc*) from the computer.

Media examination

Examination of media should be conducted in a forensic environment

- one which is completely under the control of the examiner
- no actions are taken without the examiner permit them to happen
- when the examiner permits or causes an action, he must be able to predict with reasonable certainty the outcome of the action
- use a forensically sound operating system
- physical write-blocking devices are mandatory in OS that are not forensically sound
- avoid conducting an examination on the original evidence media, always use forensic copies

Digital evidence is said to be **forensically sound** if it was collected, analyzed, handled and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so.

Examples of things to write in the report

- number and type of partitions or volumes (in SSD, HDD, or other large writable media)
- number of sessions in optical discs
- file system type
- installed operating systems
- in some cases, *e. g.* illegal content, pedophile images, *etc*, include folder structure, filenames, date/time stamps, logical file sizes, hash values (MD5 and SHA256)
- files created by the OS including, but not limited to
  - ✓ boot files, registry files, swap files, temporary files, cache files, history files and log files
- list of installed applications
- user created files should be examined using native applications, file viewers or hex viewers
  - ✓ this includes text documents, spreadsheets, databases, financial data, electronic mail, digital photographs, sound, other multimedia files, etc

Examples of things to write in the report

(continuation)

- report unused and unallocated space on each volume
  - ✓ search for previously deleted data, deleted folders
  - ✓ slack space data and data placed there by the user with the intent to hide it
  - ✓ deleted filenames of apparent evidentiary value
- report any irregularities or peculiarities in the system area of the volume (*i. e.* FAT, MFT, *etc*)
- report any hidden areas of the media, such as HPA
- report any recovered data and the process used
- forensic tools used
  - ✓ name and version of the tool
  - ✓ reference any validation test performed by examiner, the examiner's agency, or other reputable organization

Windows OS

Users directory

Windows XP

`C:\Documents and Settings`

Windows 7 and newer versions

`C:\Users`

Inside users directory (some of these names may be translated accordingly to the configured local)

`Desktop`

`AppData` or `Application Data` `Contacts`, `Favorites`, `Downloads`

`Documents`, `Pictures`, `Music`, `Videos`, `Virtual Machines`, *etc*

Recycle Bin

From Windows Vista to newer versions: `C:\$Recycle.Bin`

- it's a special directory, hidden and protected by SO
- stores files before their complete deletion
- has one subdir for each user with his SID *e. g.*

  `S-1-5-21-743533327-1274932866-229777416-1000`

  ✓ in Windows always begin with `S-1-5-21`
  ✓ `S` = SID, `1` = version, `5` = Identifier authority
  ✓ `21-743533327-1274932866-229777416` = domain identifier
  ✓ `1000` = user account relative identifier (RID),
  ✓ RID can be paired with user account name in the systems' registry
    - `HKLM\SAM\Domains\Account\Users` – not accessible through the normal Registry view on a live system
  ✓ Administrator account RID is `500` by default
  ✓ missing RID in the registry means the account was deleted

AppData directory

`AppData` replaces `Application Data` from Windows XP

- stores data from applications, because they don't have security permissions to write data to the User's primary directories
- There are 3 sub-directories: `Local`, `LocalLow` and `Roaming`

`AppData\Local`

- stores user specific application data, *e. g.* temporary files and cache files
  - ✓ Internet Explorer: `C:\Users\<User>\AppData\Local\Microsoft\Windows`
  - ✓ Firefox: `C:\Users\<User>\AppData\Local\Mozilla\Firefox`
  - ✓ Windows 8 and 10
    - `C:\Users\<User>\AppData\Local\Packages`

AppData directory

`AppData\LocalLow`

- similar to the `Local` folder
- only to write low integrity data, *e. g.* Internet Explorer add-ons

`AppData\Roaming`

- specific data which are computer independent
- should roam with the user's profile
  - ✓ data stored in this directory should be accessible when the user logs into another computer from the same network
- there maybe subfolders related to a variety of installed application

The Windows Registry is a central hierarchical database used to store information necessary to configure the system for one or more users, applications and hardware devices.

Windows Registry can be an excellent source of potential evidence

- there are two distinct types of registries
  - ✓ 95 / 98 / 98SE / ME
  - ✓ NT / 2000 / XP / VISTA / WINDOWS 7 / WINDOWS 8 / WINDOWS 10

Windows Registry – Physical layout

95 / 98 / 98SE / ME

- <windir>/SYSTEM.DAT
- <windir>/USER.DAT
- <profiles>/<username>/USER.DAT – Zero or more User files

NT / 2000 / XP / VISTA / WINDOWS 7 / WINDOWS 8 / WINDOWS 10

- <windir>/system32/config/SYSTEM
- <windir>/system32/config/SOFTWARE
- <windir>/system32/config/SECURITY
- <windir>/system32/config/SAM
- <windir>/system32/config/systemprofile/NTUSER.DAT
- <profiles>/<username>/NTUSER.DAT – One or more User files
- <profiles>/<username>/<local appdata>/Microsoft/Windows/UsrClass.DAT – User's Class File

The Registry contains 3 major categories:

- User Specific Information
  - ✓ *e. g.* Desktop Preferences, Typed URLs, Messenger Contacts, Most Recently Used (MRU) Lists and Passwords
- System Specific Information
  - ✓ *e. g.* Network Settings, Time Zone Information, Registered Owner details, Last Shutdown Date/Time and Hardware information
- Application Specific Information
  - ✓ *e. g.* File Associations, Application Registration Information, *etc*

There are typically 5 root level keys in a Windows registry

- `HKEY LOCAL MACHINE (HKLM)` – is by far the most significant key in the registry
  - ✓ has subkeys named Software, System, Security, Sam and Hardware
  - ✓ stored in separate files: `SOFTWARE`, `SYSTEM`, `SECURITY`, `SAM`
- `HKEY USERS` – stored in one `NTUSER.DAT` file per user
- `HKEY CLASSES ROOT` – can be ignored, it is merely an alias for `HKLM/Software/Classes`
- `HKEY CURRENT USER` – is an alias for `HKEY USERS` for the user currently logged on
- `HKEY CURRENT CONFIG` – is an alias to the current hardware profile stored at

  `HKLM/System/CurrentControlSet/Hardware Profiles/Current`

Tools to analyze the Windows Registry

regedit %windir%\regedit.exe

- ✓ included in all Windows installations
- ✓ hides some registry entries

Registry Browser https://lockandcode.com/software/registry_browser

- ✓ nice GUI, shows registry with similar structure as `regedit`
- ✓ shows all registry entries
- ✓ has a "device manager" like view
- ✓ has a nice report tool

Registry Report https://www.gaijin.at/en/files?dir=old-software

- ✓ easy to use GUI, but requires some knowledge about the registry structure
- ✓ produces detailed reports

Reg Ripper https://github.com/kireyn/RegRipper2.8

- ✓ powerful command line tool, very good to automate tasks
- ✓ requires good knowledge about the registry structure

Forensic Report

Report Structure

The forensic report should contain:

- Preamble – pages with roman numeration
  - ✓ Declaration of honor – sometimes it's a separate document
  - ✓ List of acronyms in alphabetical order
  - ✓ List of contents
- Body – start the Arabic numeration of the pages
  - ✓ Introduction
  - ✓ Several analysis chapters, usually one per device
  - ✓ Conclusions
- Epilogue
  - ✓ Bibliography – not always required
  - ✓ Appendixes – not always required
  - ✓ Glossary – recommended

Declaration of honor

- usually it's a separated document
- but can be included in the report

Example

I, (expert full name), holder of the identity card number XXXXXXXX, valid until 20XX-XX-XX, with professional domicile at the University of Aveiro, located at Campos Universitário de Santiago, Gloria, 3810 - 193 Aveiro, declare on a commitment to honor the veracity of the information provided in this report, of which this declaration is a part.

Introduction

- what are you looking for and why
- list of the devices being analyzed and their IDs
- explain the structure of the report

Example

The authors of this report were appointed computer experts in the NUIPC XXXXXXXX process under the protocol between the Aveiro University and the Office of Cybercrime of the Generals' Attorney Office. In this context, XX devices of the defendant (full name) were delivered for analysis. The devices are described in Table X with their assigned identification code (ID). [...]
In this case, the following diligences were requested:

- bla, bla, . . .

Analysis

- one chapter per analysis, *e. g.* for each device, or DNS analysis, *etc*
- for each chapter:
  - ✓ detail the device characteristics and ID
  - ✓ the procedures you made on that device, *e. g.* forensic copy, run anti-virus, *etc*
  - ✓ explain clearly what you found
  - ✓ anti-virus results
  - ✓ . . .

Conclusions

- reconstruct the events based on the evidences found
  - ✓ and include a reference to the chapter and section in the report where you detailed how you found the evidence
- report all the found evidences, either incriminating or exculpatory
- always use clear text and avoid complex technical terms when possible, if needed reference to a glossary explaining the technical terms

Example

Under the NUIPC XXXXXX process, a total of XX devices of the defendant (full name) were submitted for analysis. In YY devices, no relevant information was found for the process (list the IDs).

Only ZZ devices contain relevant information (list the IDs). In this report it was possible to establish the following:

- bla, bla, . . .

Bibliography

- citations help to increase the credibility of the report and the expert
- cite reference books in the field, or other medium with high reputation in the filed being analysed, *e. g.* RFC
- there are many bibliography styles, *e. g.* APA, Chicago, IEEE, Harvard, . . .
  - ✓ choose one and be consistent through the report
  - ✓ use tools to help format the references, *e. g.* JabRef, Mendeley, MS Word Reference tool

Example

1 Y. Rekhter et al. Address Allocation for Private Internets. RFC 1918 (Best Current Practice). RFC. Updated by RFC 6761. Fremont, CA, USA: RFC Editor, fev. de 1996. doi: 10.17487/RFC1918. url: https://www.rfc-editor.org/rfc/rfc1918.txt.

2 J. Postel. Simple Mail Transfer Protocol. RFC 821 (Internet Standard). RFC. Obsoleted by RFC 2821. Fremont, CA, USA: RFC Editor, ago. de 1982. doi:10.17487/RFC0821. url: https://www.rfc-editor.org/rfc/rfc821.txt.

Appendices

The Appendices section should be used to include information that helps to demonstrate, or complements, the expert conclusions.

- include documents **relevant** to the case being analysed:
  - ✓ reports generated by used tools
  - ✓ technical specifications from hardware vendors
  - ✓ reports, or parts of a report, produced by someone else
  - ✓ . . .

Glossary

- explain technical terms in lay language
- this section is important for the non technical staff that must read the report

Example

Phishing – Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

QUESTIONS?