PENANGANAN INSIDEN SIBER (AKUISISI BUKTI DIGITAL)

Direktorat Operasi Keamanan Siber
Jakarta, 31 Mei 2022

Bintang Wahyudono, S.Tr.Kom.
Analis Tata Kelola Keamanan Siber
Direktorat Operasi Keamanan Siber
Deputi II

Lingkungan Palamanis, Cirimekar, Cibinong
+6285817509659
bintang.wahyudono@bssn.go.id
https://www.linkedin.com/in/bintang-wahyudono-6aa88a20b

Review

Metode Digital Forensic

NIJ (National Institure of Justice)

- **Identification,** mencari (identifikasi) bukti digital mana saja yang dapat digunakan untuk mengungkap suatu incident atau aktivitas yang terkait dengan suatu kasus. Di dalamnya terdapat proses seperti pelabelan dan pencatatan barang bukti.
- **Collection,** mengumpulkan barang bukti untuk mendukung penyelidikan. Umumnya dilakukan akuisisi barang bukti dengan cara ***Imaging*** (melakukan copy terhadap sumber data secara presisi 1 banding 1 atau bit by bit copy) terhadap source yang akan dianalisis
- **Examination,** tahap pemeriksaan data yang telah dikumpulkan secara forensik baik secara otomatis atau manual

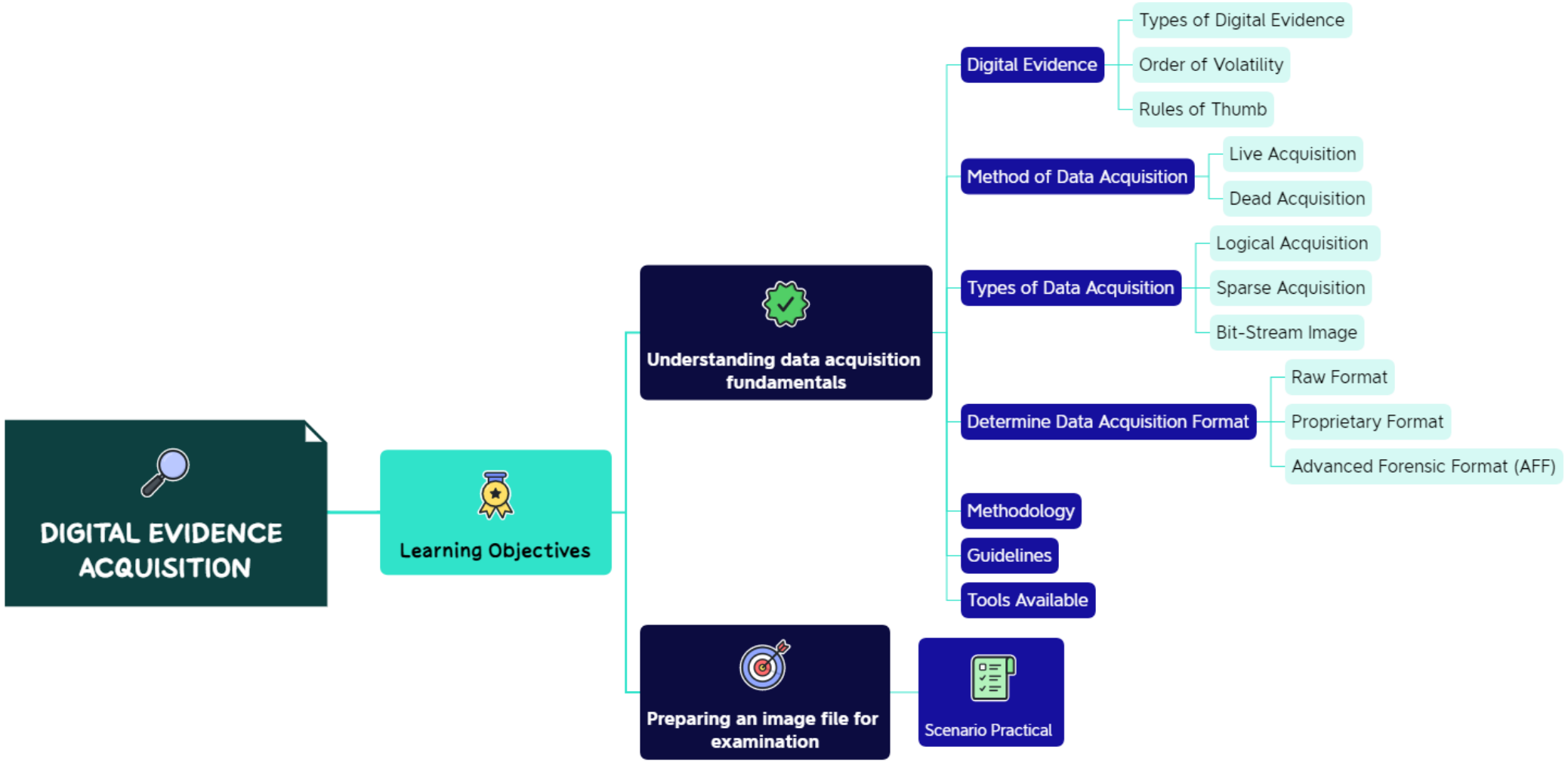
Review

Metode Digital Forensic (2/2)

NIJ (National Institure of Justice)

- **Analysis,** tahap utama dimana setiap image yang telah didapat dianalisis untuk mencari bukti atau artifak-artifak tertentu yang berkaitan dengan kasus, untuk menjawab 5W+1H
- **Reporting,** dilakukan pelaporan hasil analisis mulai dari metode yang dilakukan, perilaku apa yang diberikan kepada barang bukti, alat (tools) apa yang digunakan, dan juga temuan-temuan terkait dengan kasus. Dalam pelaporan juga diberikan kesimpulan dari analisis yang dilakukan.

Study Map


DIGITAL EVIDENCE ACQUISITION
Learning Objectives
Understanding data acquisition fundamentals
Digital Evidence
Types of Digital Evidence
Order of Volatility
Rules of Thumb
Method of Data Acquisition
Live Acquisition
Dead Acquisition
Types of Data Acquisition
Logical Acquisition
Sparse Acquisition
Bit-Stream Image
Determine Data Acquisition Format
Raw Format
Proprietary Format
Advanced Forensic Format (AFF)
Methodology
Guidelines
Tools Available
Preparing an image file for examination
Scenario Practical

Digital Evidence

A digital evidence can be defined as any information which has probative value that is stored or transmitted in digital form.

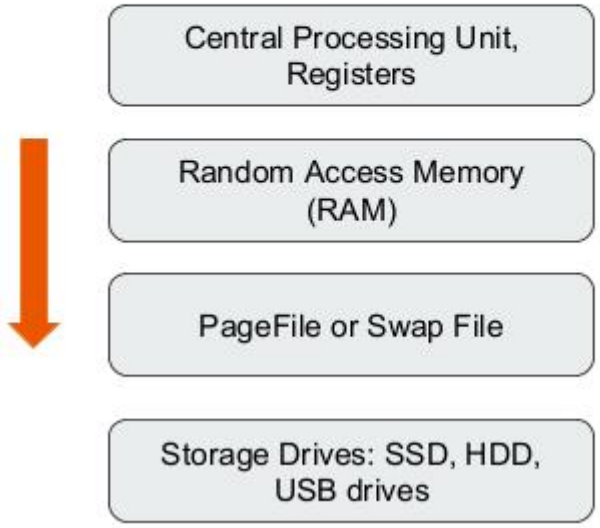
Volatile	Non Volatile
Volatile Data is not permanent. It is lost when power is removed from the memory.	Non-volatile data is any data that can be retrieved even after the computer loses power or is turned off.
RAM, cache, DLLs	Hard drive, USB thumb drives, CDs and DVDs

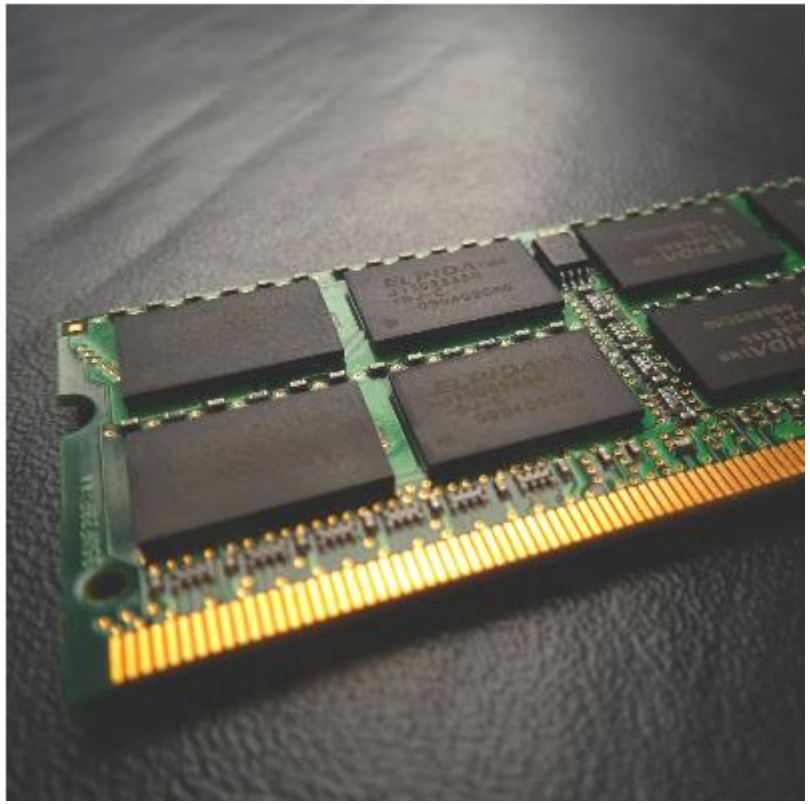
Source:

- Hard Drive
- Network
- Memory
- Cloud
- External hard drive
- etc

Order of Volatility

According to the RFC 3227, below is an example of the order of volatility for a typical system:





Rules of Thumb for Data Acquisition

- Acquire the evidence without altering or damaging the original

- Establish and demonstrate that the examined evidence is the same as that which was originally obtained

- Analyze the evidence in an accountable and repeatable fashion

Rules of Thumb for Data Acquisition

A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody.

Method of Data Acquisition

Live Acquisition

- Live data acquisition involves collecting volatile data from a live system. Volatile information assists in determining the logical timeline of the security incident, and the possible users responsible
- Live acquisition can then be followed by static/dead acquisition, where an investigator shuts down the suspect machine, removes the hard disk and then acquires its forensic image

Dead Acquisition

- Dead acquisition is defined as the acquisition of data from a suspect machine that is powered off
- Dead acquisition usually involves acquiring data from storage devices such hard drives, DVD-ROMs, USB drives, flash cards, and smart phones
- Examples of static data: emails, word documents, web activity, spreadsheets, slack space, unallocated drive space, and various deleted files

Types of Data Acquisition

a. Logical Acquisition

- Acquiring bit-by-bit copy of a large disk requires more time. In a situation with time constraints and when the investigator is aware of what files need to be acquired, logical acquisition is an ideal method.
- Logical acquisition allows an investigator to capture only selected files or files types of interest to the case.

b. Sparse acquisition

Similar to logical acquisition, which in addition collects fragments of unallocated data, allowing investigators to acquire deleted files. Use this method when inspection of the entire drive is not required.

c. Bit-Stream Image

- Bit-stream imaging creates a bit-by-bit copy of a suspect drive, which is a cloned copy of the entire drive including all its sectors and clusters.
- This image contains not just a copy of all the files and folders, but also the ambient data, which allows forensic investigators to retrieve deleted files or folders.

Determine Data Acquisition Format

Data in forensic acquisition tool is stored as an image file.

Format	Advantages	Disadvantages
Raw	• Fast data transfers • Ignores minor data read errors on source drive • Most computer forensics tools can read raw format	• Requires as much storage as original disk or data • Tools might not collect marginal (bad) sectors
Proprietary (Most forensics tools have their own formats)	• Features offered • Image files can include metadata	• Inability to share an image between different tools • File size limitation for each segmented volume • Consumes more time for evidence search than raw format
Advanced Forensic Format (Developed by Simson L. Garfinkel (2006) as an open-source acquisition format)	• No size limitation for disk-to-image files • Simple design and customizable • Compatible in multiple computing environments	

Methodology

1. Determining the data acquisition method
2. Determining the data acquisition tool
3. Sanitizing the target media
4. Acquiring volatile data

Methodology (cont)

5. Enabling write protection on the evidence media
6. Acquiring non-volatile data
7. Planning for contingency
8. Validating data acquisition

Guidelines for Proper Collection of Digital Evidence

- Photograph the system and general scene
- Determine whether the system is powered up
- Acquire the running memory
- Acquire registry and log files
- Unplug the power from the back of the system
- Photograph the back or bottom of the system to capture the model and serial numbers
- Remove the cover to system and photograph the HDD to capture the model and serial number
- Remove the HDD from the system and place it into an anti-static bag
- Secure the drive in sealable envelope or box
- Document all actions

Forensic – Related Tools

Awesome DFIR - Digital Forensics & Incident Response / DFIR Tooling

DFIR Tooling

Name	Site	Tags	Pricing	Description
AccessData FTK Imager	accessdata.com	disk image creation, live memory acquisition	Free	Forensics tool whose main purpose is to preview recoverable data from a disk of any kind. FTK Imager can also acquire live memory and paging file on 32bit and 64bit systems.
AChoir	github.com	artifact collection, windows, acquisition	Free	Framework/scripting tool to standardize and simplify the process of scripting live acquisition utilities for Windows.
AMAaaS	amaaas.com	sandbox, apk analysis, android, saas	Free	Android Malware Analysis as a Service, executed in a native Android environment.
anlyz.io	sandbox.anlyz.io	file analysis, url analysis, saas	Free	Malware sandbox to analyze file and url with a main dashboard and search features!
Any Run	any.run	sandbox, saas	Free, Commercial	Malware hunting with live access to the heart of an incident Watch the epidemic as if it was on your computer, but in a more convenient and secure way, with a variety of monitoring features.
AppCompatProcessor	github.com	log, parsing, osx, linux	Free, Beta	AppCompatProcessor has been designed to extract additional value from enterprise-wide AppCompat / AmCache data beyond the classic stacking and grepping techniques.
Appliance for Digital Investigation and Analysis (ADIA)	forensics.cert.org	linux distribution, all-in-one, forensics	Free	VMware-based appliance used for digital investigation and acquisition and is built entirely from public domain software. Among the tools contained in ADIA are Autopsy, the Sleuth Kit, the Digital Forensics Framework, log2timeline, Xplico, and Wireshark. Most of the system maintenance uses Webmin. It is designed for small-to-medium sized digital investigations and acquisitions. The appliance runs under Linux, Windows, and Mac OS. Both i386 (32-bit) and x86_64 (64-bit) versions are available.
APTSimulator	github.com	adversary emulation	Free	APT Simulator is a Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised. In contrast to other adversary simulation tools, APT Simulator is deisgned to make the application as simple as possible. You don't need to run a web server, database or any agents on set of virtual machines. Just download the prepared archive, extract and run the contained Batch file as Administrator. Running APT Simulator takes less than a minute of your time.
artifactcollector	github.com	artifact collection	Free	The artifactcollector project provides a software that collects forensic artifacts on systems. These artifacts can be used in forensic investigations to understand attacker behavior on compromised computers.
Atomic Red Team	github.com	adversary emulation	Free	Atomic Red Team allows every security team to test their controls by executing simple "atomic tests" that exercise the same techniques used by adversaries (all mapped to Mitre's ATT&CK).

https://awesomedfir.com/dfir-tooling

Practice Time

“(Ingatlah) Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”

MAYJEN TNI DR. ROEBIONO KERTOPATI
(1914 - 1984)
BAPAK PERSANDIAN REPUBLIK INDONESIA