

Digital Forensics

Advancing Solutions for
Indonesia's Escalating
Cybercrime

Table of Contents

01

Statistics

Cyber attack statistics

02

Digital Forensic

What is Digital Forensic

03

Importance

Why Digital Forensic is Important

04

Incorporating

How to incorporate Digital Forensic into Infosec





Ewaldo Simon

Digital Forensic in Directorate General of Taxes of Indonesia

DFIR Enthusiast


contact me aldo@aldosimon.com

...



DISCLAIMER

opinions are **my own** and not the
views of **my** employer



cyber attack statistics



Attacks

98.243.896 attacks
throughout 2019
from 647.303
unique IPs

...



Malware

22.750 malware
attack from 705
unique malware

...



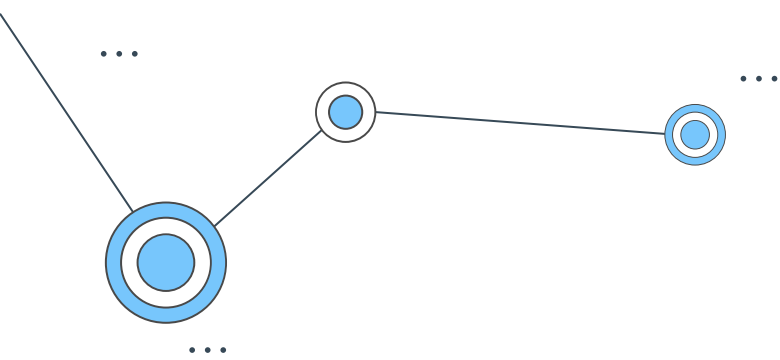
Damage

USD 3.2 billion in
monetary damage

...

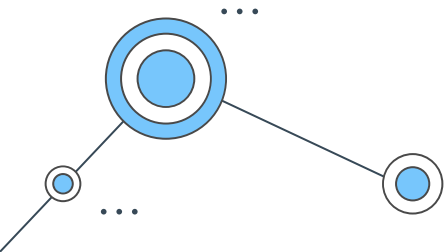
Digital Forensic



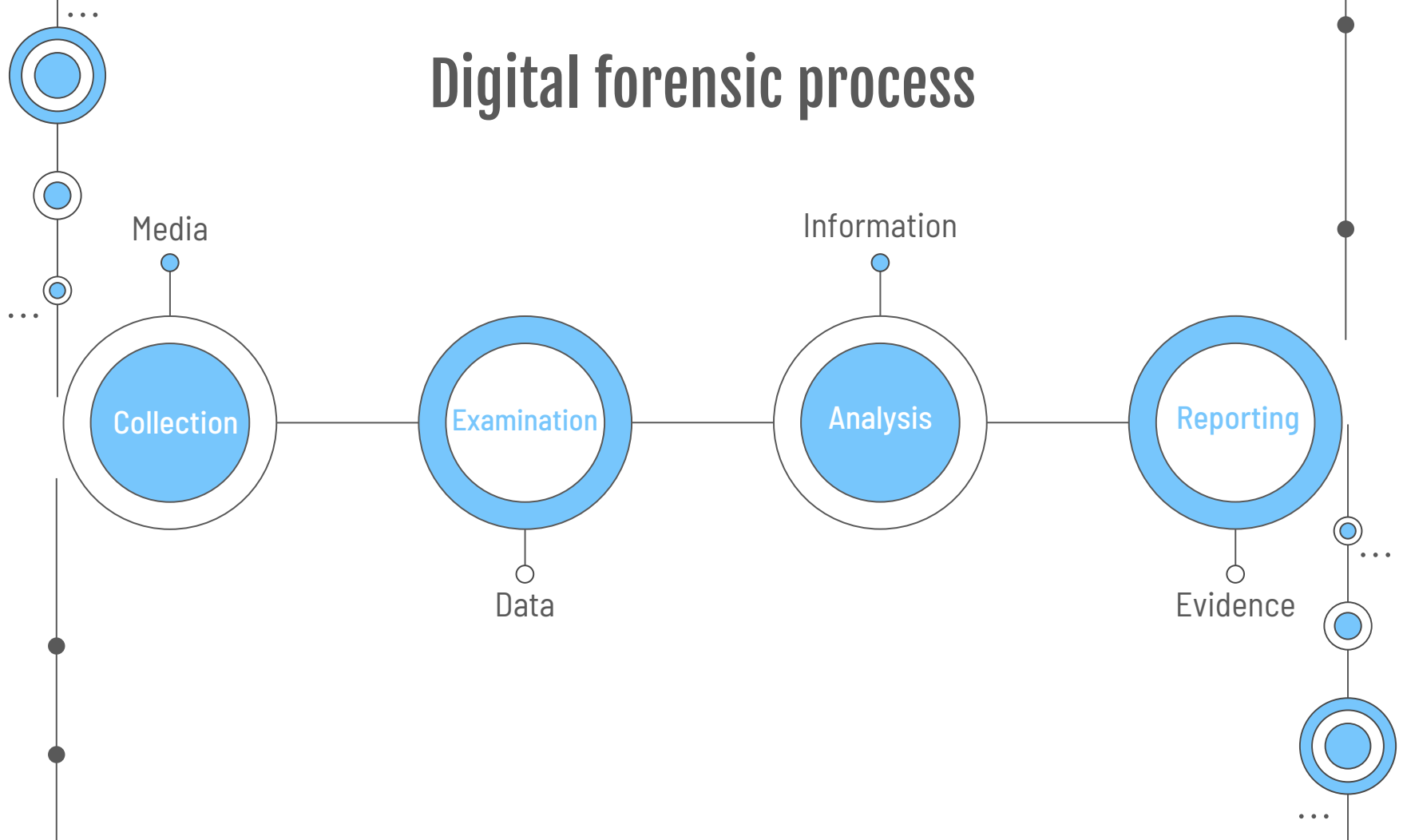


The use of **scientifically** derived and proven methods toward the **preservation, collection, validation, identification, analysis, interpretation, documentation** and **presentation** of digital evidence derived from digital sources for the **purpose** of facilitating or furthering the **reconstruction of events** found to be criminal, or helping to **anticipate** unauthorized actions shown to be disruptive to planned operations.

—Brian Carrier



Digital forensic process





Importance



01

Evidence handling

forensic is about
handling evidence

02

Data Recovery

digital forensic tools
deals with data
recovery all the time

03

Analysis

digital forensic (esp.
e-discovery) deals
with huge data to
extract information

04

Due Dilligence

often used as a mean to
do due dilligence or are
required by laws

Digital Forensic

reactive

digital forensic as a tool
used after an incident
happen

proactive

digital forensic as a tool
used before an incident
happen



Be Ready!

Digital Forensic Readiness: The art of
maximizing the environment's **ability** to
collect **credible evidence**.

why DFR matter

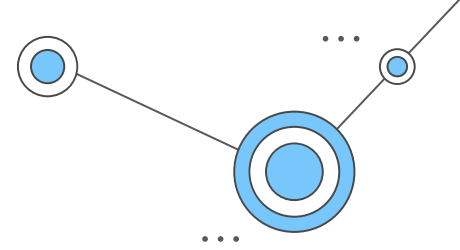
...
**better
investigation**
ensure credible
evidence

...
**lower cost
& time**
lower downtime
and eventually
cost

...
security posture
implementation
will improve
posture



Implementing digital forensic readiness

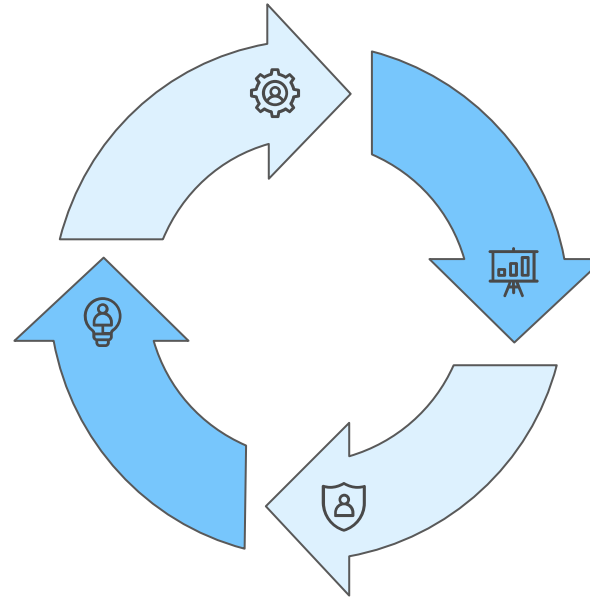


needs

understanding
required evidence

im(prove)plement

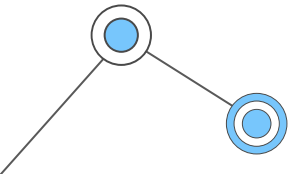
overlap with IS,
changes, etc.



current
understanding
currently available
"evidence"

policies

develop policy to cover
gap



Credits

- Endicott-Popovsky (2006)
- Grobler-Louwrence (2007)
- IBM report: cost of data breach (2020)
- Carrier-Spafford (2003)
- Honeynet-ID 2020 report (2020)
- NIST SP 800-86: incorporating digital forensic to incident response
- Art, Fonts from slidego

Thanks!

Do you have any questions?

aldo@aldosimon.com
aldosimon.com

CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#) and illustrations by [Stories](#)

