Czech Cybercrime Centre of Excellence
for training, research and education

Digital Evidence, E-mails & Cloud

2nd LIVE-FOR Workshop
Masaryk University Brno

13 – SEP – 2018

Marian Svetlik
svetlik@gmail.com

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Outline

- Basic properties of the digital evidence
- E-mail trustworthiness
- Cloud specifics

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Basic properties of the Digital Evidence

- Definition
- Originality
- Fragility
- Integrity
- Latency
- Lifetime

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Digital Evidence - Definition

- Digital evidence is the physical representation of immaterial information in the form of recording that information in digital form.
- Digital evidence (information stored/tranfered in digital form) does not depend on the recording/transfering medium.

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Properties

- Immateriality of the digital evidence vs. materiality of the data storage
- Time traceability
- Information value
- Storage and quality of archive records
- Big data
- High data density
- Dynamics of the development of ICT technologies
- Speed of ICT operations
- Complexity of the digital environment
- Big geographical scope
- Data protection and encryption
- Potential automation of identification/analysis
- Undefined identity identification
- Reconstruction of digital traces
- Distrust of the probative value of digital evidence

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Originality

- Original digital evidence is evidence, which is going to be seized
- Copy is seized digital evidence
- Forensic copy has the same evidence value as the original digital evidence
- In investigation and forensic examination we work with copies of the original digital evidence
- Physical and Logical forensic copy

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Fragility

- Original digital evidence IS FRAGILE!
- Forensic copy of digital evidence IS NOT FRAGILE!
- Live Forensic (Wiretapping):
  - Volatile Memory (RAM) & Data Flow (network data in a flow) IS FRAGILE
  - Forensic copy of such data IS NOT FRAGILE

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Integrity

- All the life-time of digital evidence (from seizing up to presenting at the court) the integrity must be protected & ensured.
- HASH or Digital Signature (with time-stamp) or similar

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Latency

- Digital Evidence is invisible
  - You need to find & transform digital data to the perceptible form & to interpret digital information in context of ICT operation

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Lifetime

- Long-term lifetime
  - Archiving
- Short-term lifetime
  - You can delete about ½ million of files in one scond

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Break/Questions

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

e-mail

- SMTP (Simple + Mail + Transfer + Protocol)
  - Full text format without any security measures
    - Do not believe e-mails without additional verification tests
    - Printed e-mail (even with header) is not a valid evidence (except the print is made by verified expert using certified method/process)

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

SMPT

- MAIL FROM <text>
- RCPT TO <text>
- DATA <text> (whatever you want to send in text form, even the mail header content)

- Protocol Extensions
  - SPF (Sender Policy Framework)
    - sender server verification
  - DKIM (Domain Key Identified Mail)
    - mail content digital signature
  - ARC (Authenticated Received Chain)
    - chain of resender servers verification

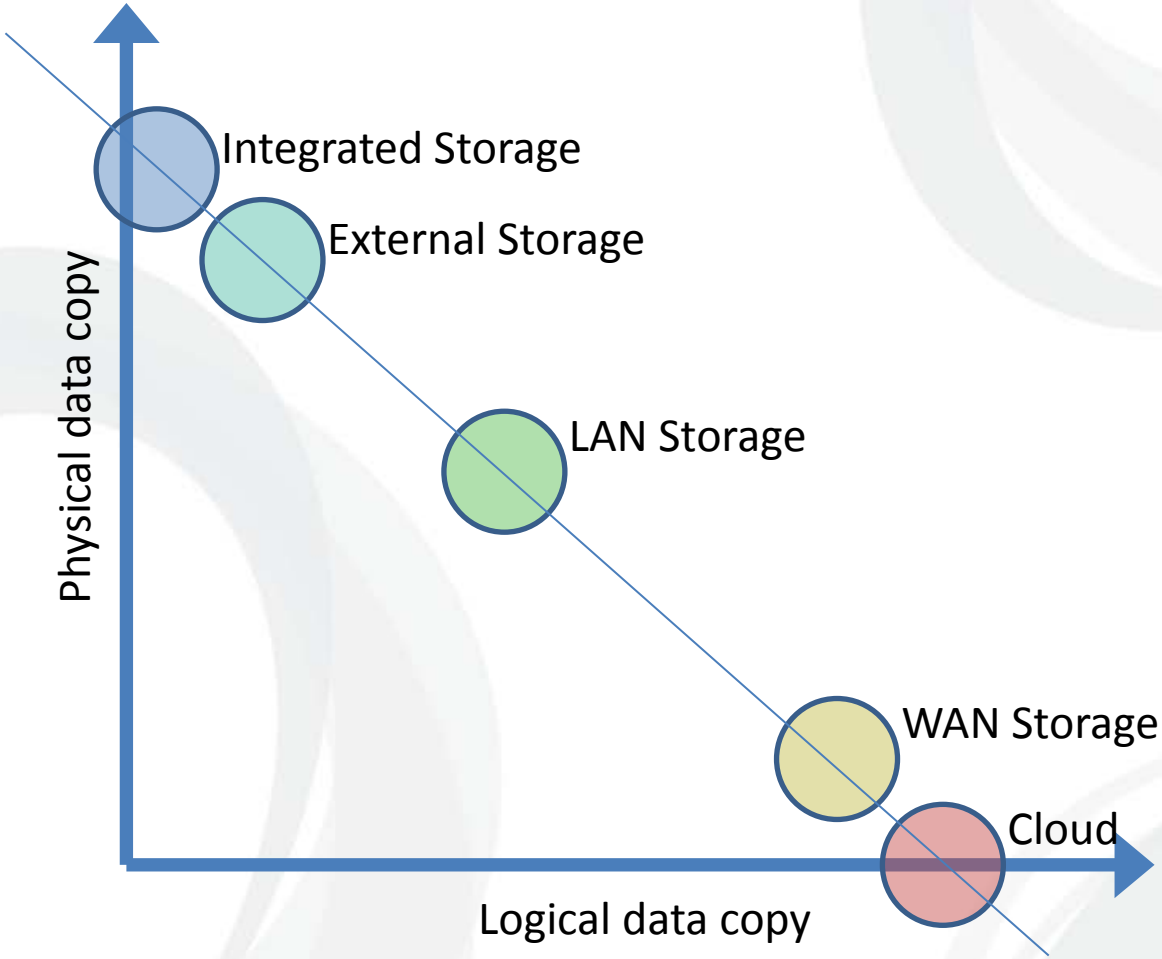
With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Cloud

- Storage
  - Integrated storage
  - External storage
  - LAN (Local Area Network) storage
  - WAN (Wide Area Network) Storage
  - Cloud

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Cloud Seizure



With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs

Questions

With the financial support from the Prevention of and Fight against Crime Programme of the European Union European Commission - Directorate-General Home Affairs