Digital Forensics

Marian Svetlik
svetlik@df-pro.cz
svetlik@fi.muni.cz
www.digital-forensic.pro

Digital Forensics Course Concept

Marian Svetlik

- Expert Witness in Digital Forensics
- Information Security Expert
- Vice-president a CEO of The Academy of Forensic Sciences
- Digital Forensic Review - Journal Editor
- ISMS Lector at University of Economics Prague
- Comuter Crime Lector at University of Finance and Administration Prague
- Cybercrime Lector at CEVRO Institute
- Digital Forensic Special Expert C4e at MUNI
- Programme Committee member of the DFRWS EU
- IDFA Management Board Member

Course Content

- DF definition, relation to the cybersecurity and to the cybercrime
- Digital Traces & Digital Evidence, properties, documentation
- Sources, Handling, Gathering and Protection
- DF Examination Principles
- DF Lab creation and management, Assessment, Certification, Accreditation
- DF in Law, Electronic Evidence

Recap

- Digital Trace
  - Immaterial
  - Latent
  - Coded
- Digital Trace
  - Seizable
  - Understandable
  - Relevant
- Locard's Principle in Digital World
- Digital Traces and their properties

Today outline

- Typical sources of the digital traces
- Digital evidence gathering, handling and protection

Typical Sources of the Digital Traces

Starting with Theory:

- Digital information is the record of (immaterial) information in digital form **on a material medium that is capable of carrying or transmitting such kind of record**.

Where they are?

- Integrated
  - Permanent (static)
  - Volatile (dynamic)
- External/Removable
- Remote
  - Local network storage (file server, NAS)
  - Cloud storage
- Data lines (dynamic)
  - Electric current/wires, light, el-mag filed, ….

1st Break

- Is there some difference between:
  - Local network storage
  - and Cloud?

Integrated static

- HDD

Integrated static

- SSD

Integrated static

- SSD

Integrated static

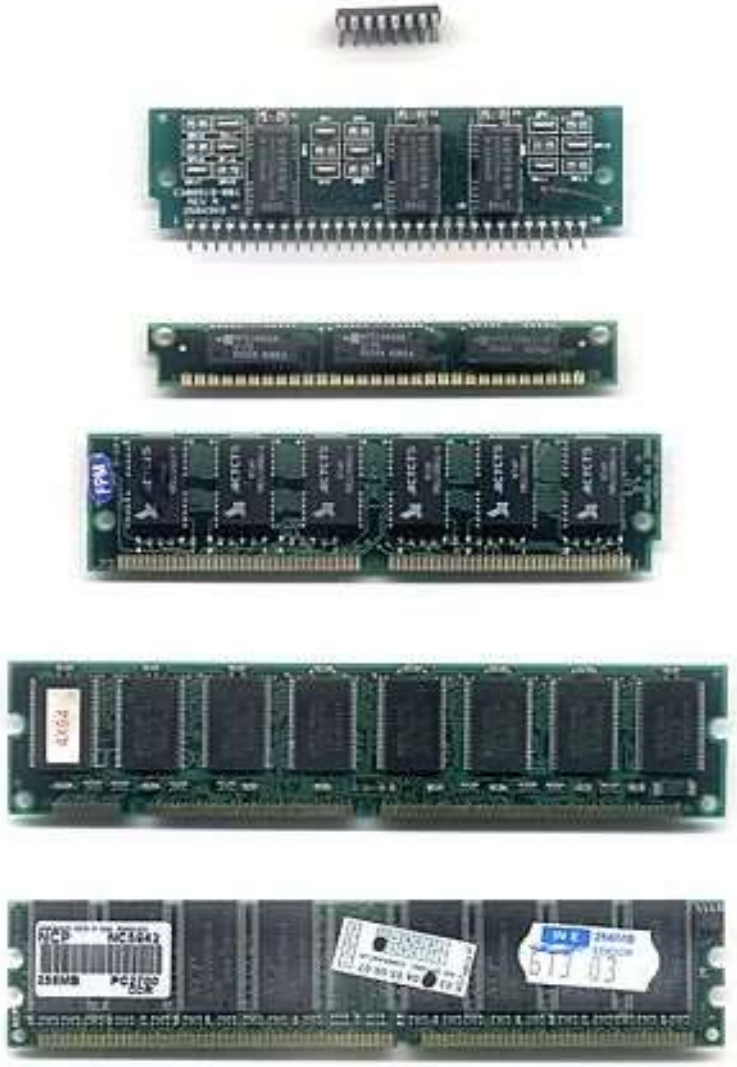
- SSD

Integrated Volatile

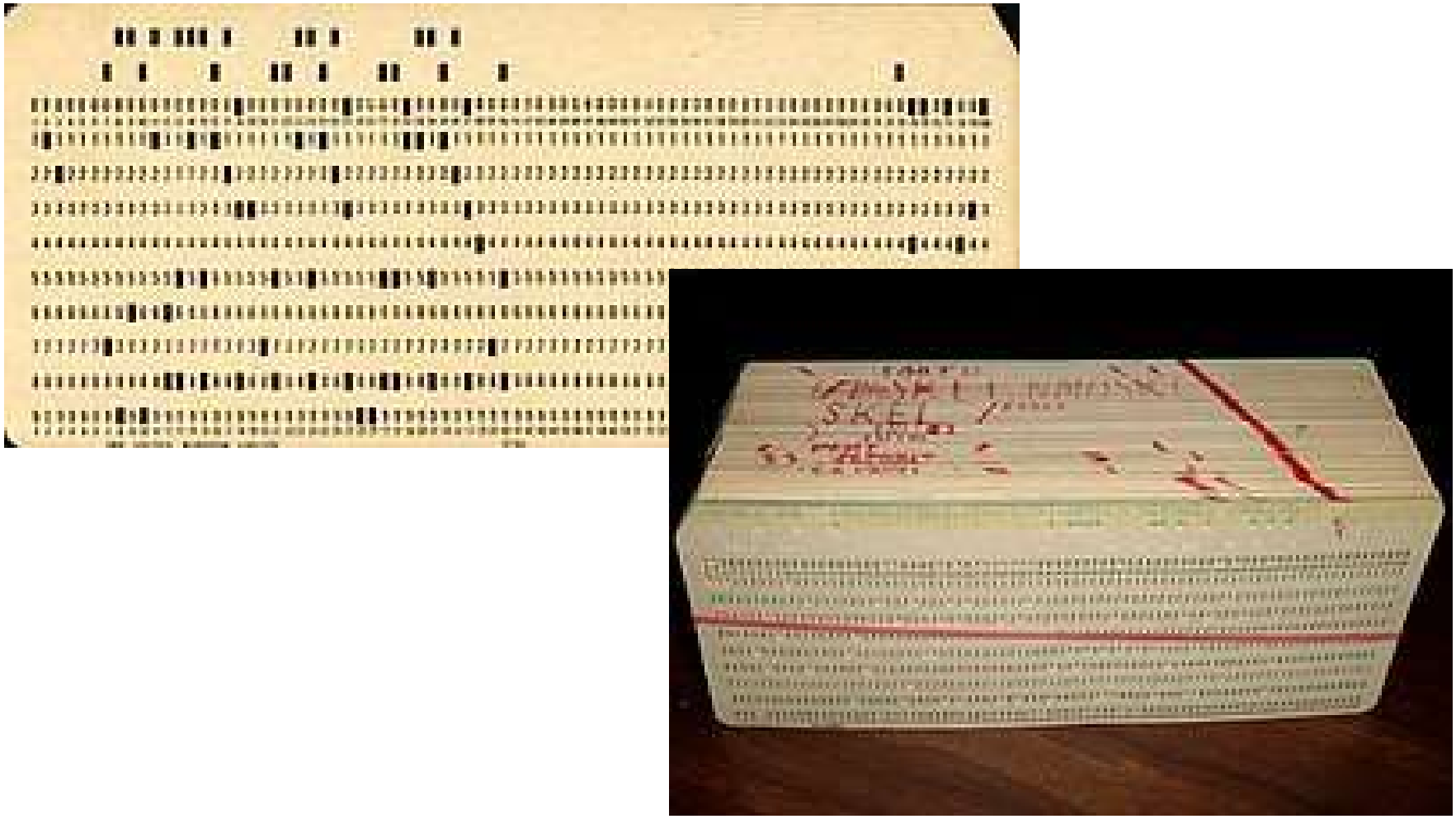
- RAM (Random Access Memory)
  - SRAM (static)
  - DRAM (dynamic)

Integrated Volatile

- RAM



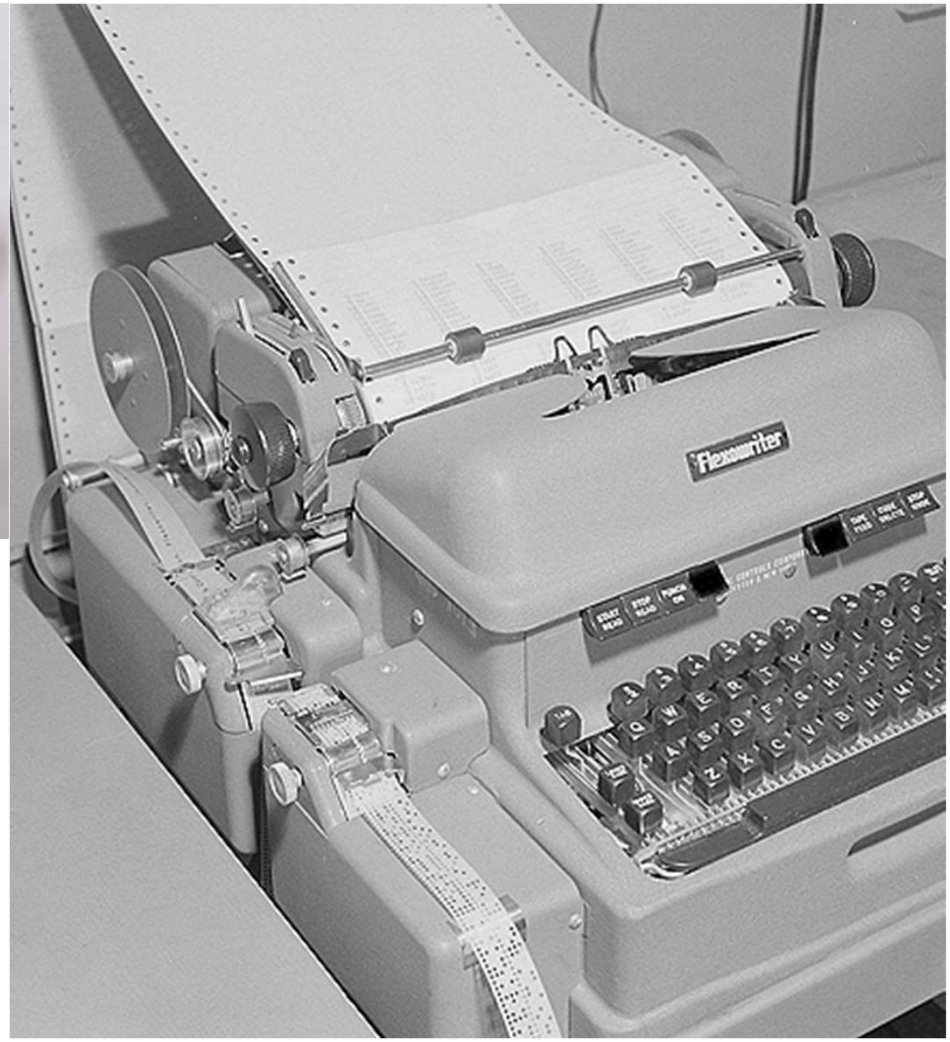
External/Removable



https://en.wikipedia.org/wiki/Punched_card

External/Removable

https://en.wikipedia.org/wiki/Punched_tape

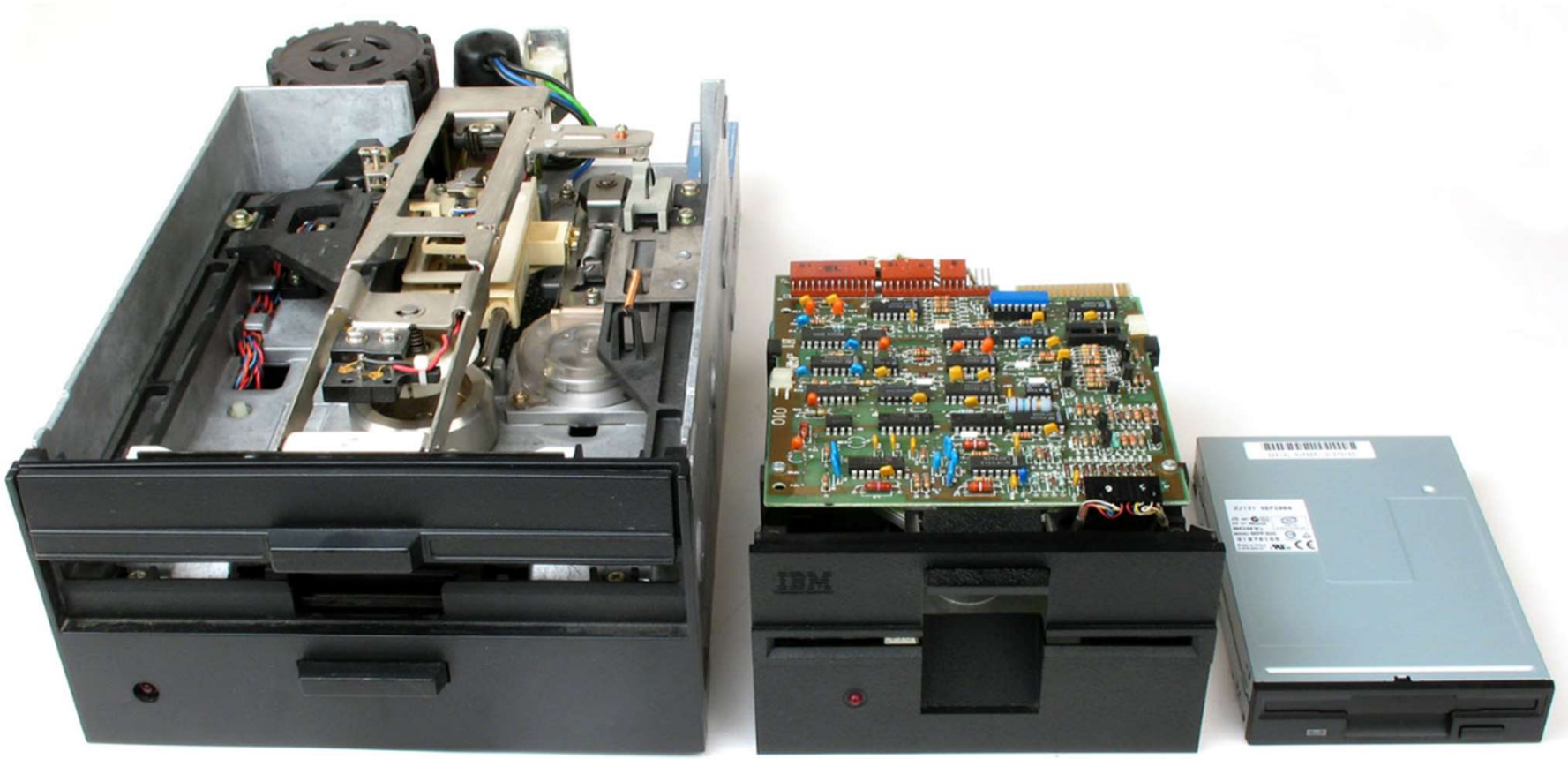


https://encyclopedia2.thefreedictionary.com/paper+tape

External/Removable

https://en.wikipedia.org/wiki/Magnetic_tape

External/Removable



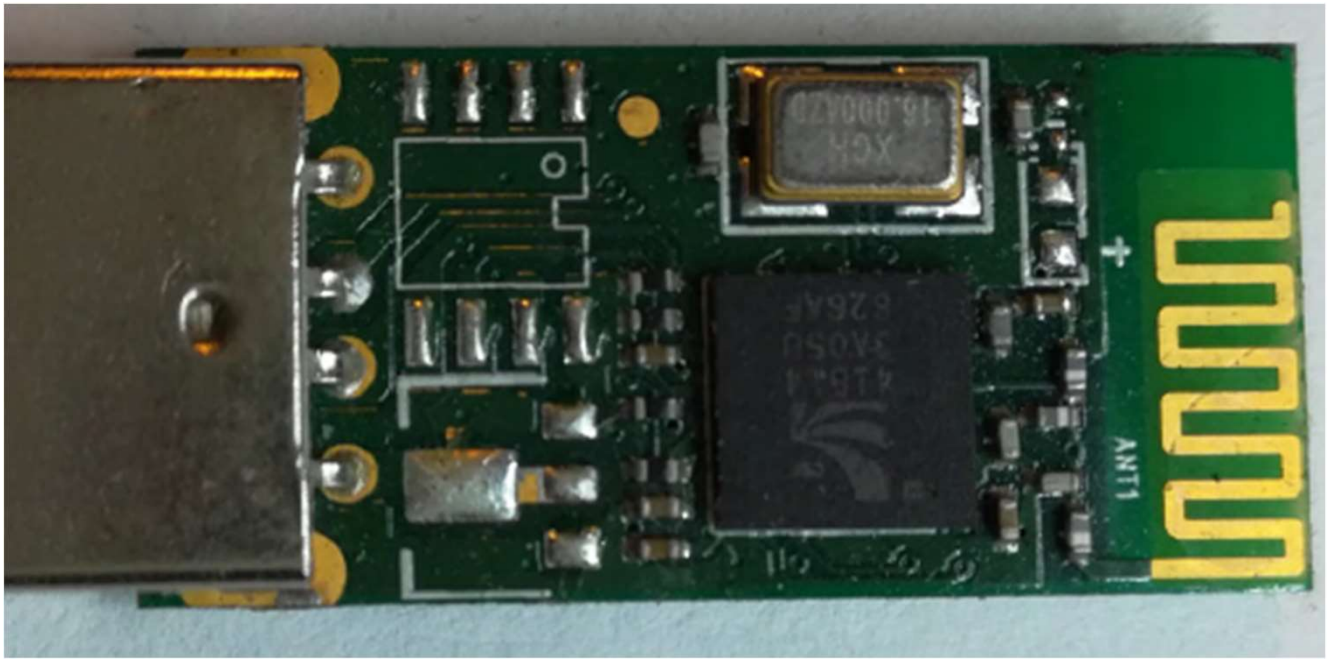
External/Removable

External/Removable

External/Removable

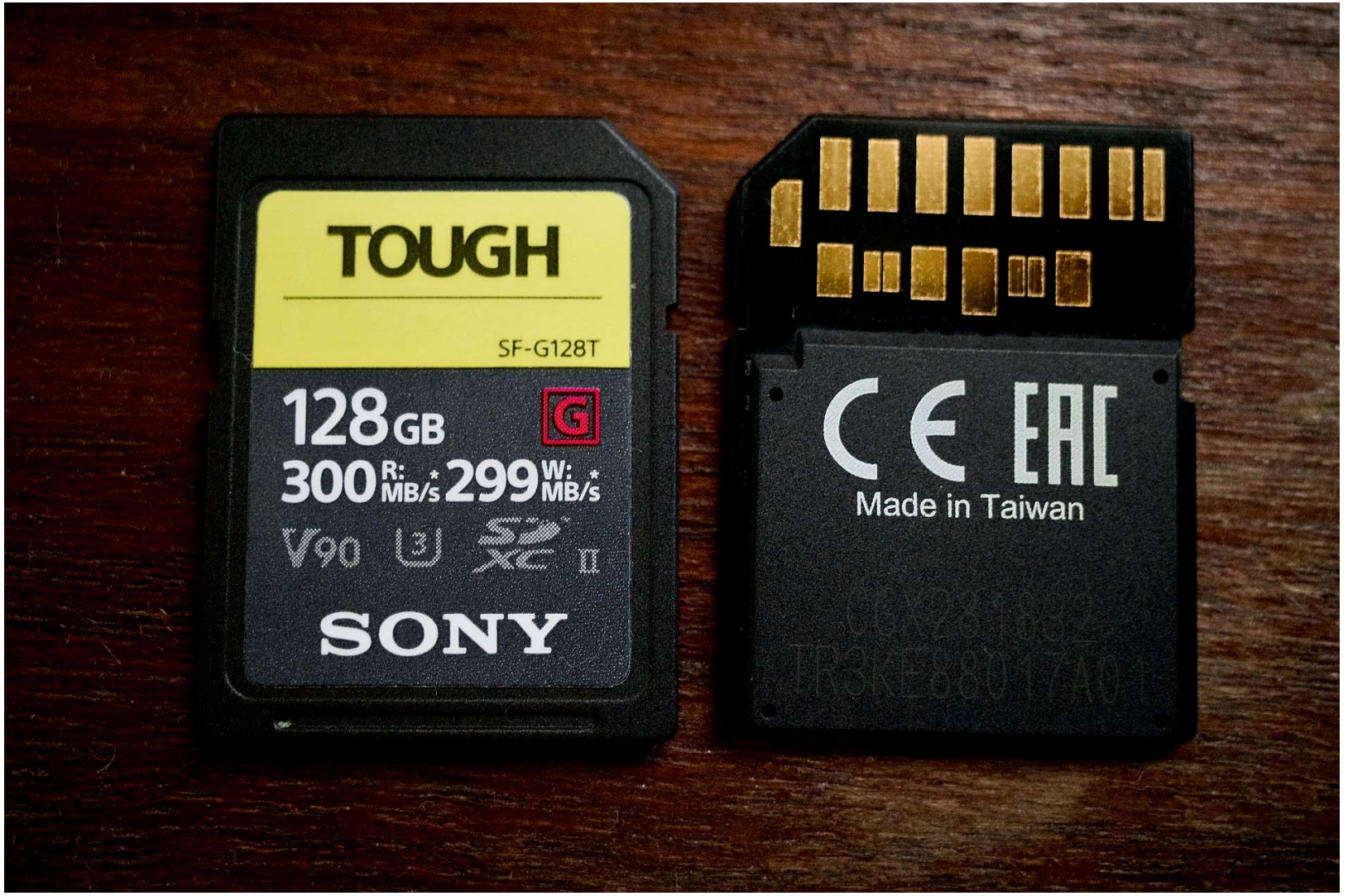
External/Removable

External/Removable



External/Removable

External/Removable



External/Removable

… and others

Remote

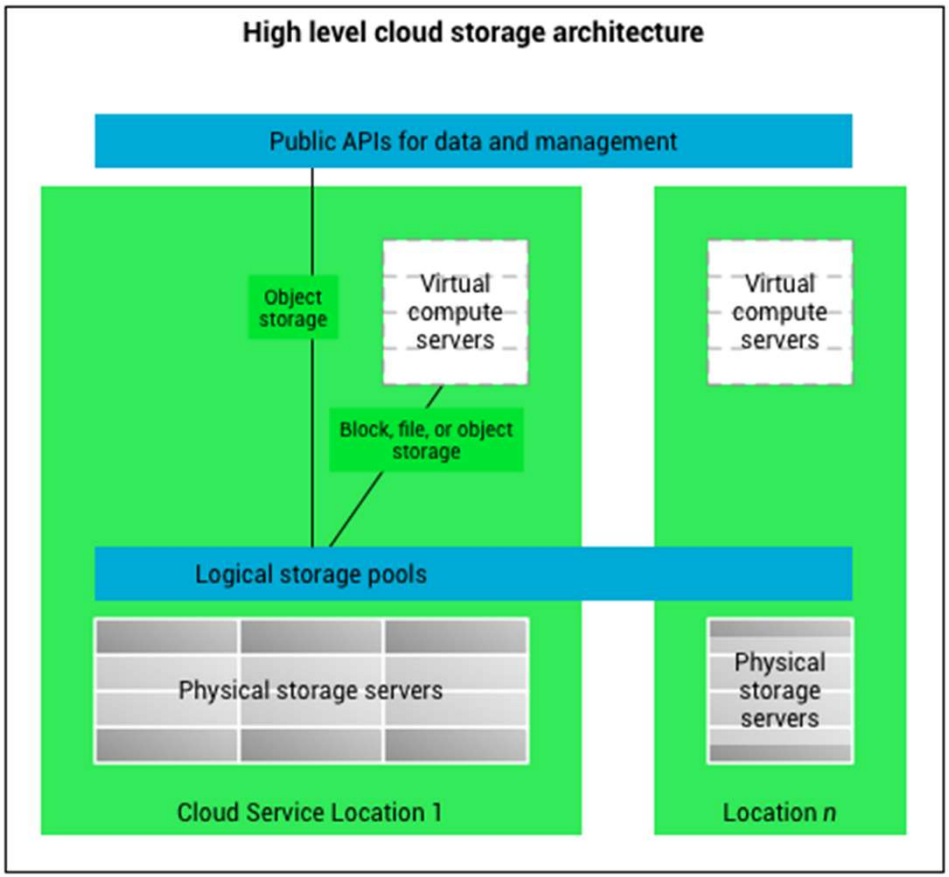
- File Srver

Remote

- NAS (Network Attached Storage)

Remote

- Cloud



Network Lines

How to deal with digital evidence

- Gathering/Seizing
- Manipulate
- Protection
- Documentation of all activities

Gathering/Seizing Digital Evidence

The goal is to seize as much as possible of all accessable digital data.

Why?

Where they are? (recap)

- Integrated
  - Permanent (static)
  - Volatile (dynamic)
- External/Removable
- Remote
  - Local network storage (file server, NAS)
  - Cloud storage
- Data lines (dynamic)
  - Electric current/wires, light, el-mag filed, ….

Seizing order

1. Network flow
2. Volatile memory
3. Cloud storage
4. NAS
5. Integrated permanent
6. Removable

Why such order?

The degree of control over the data

- Network flow – just at the moment of flow
- Volatile memory (RAM) – up till power is on
- Cloud storage – risk of the remote tampering
- NAS – similar as cloud
- Internal disks – quite often at crime place
- Removable media – could be seized as media and gather a data later

Bit copy vs. Logical copy

- Bit copy (forensic image)
- Logical copy (forensic file copy)

What are Cons and Pros of both versions?

Limits

- Legal limits (vary based on jurisdiction)
- Size of the data
- Technical limits
- Time limits

Integrity

- Once you have a control over the seized data, integrity is one of the core conditions to take a care

- Checksums
  - MD5 (!)
  - SHA1 (!)
  - SHA256

Spec forensic SW

- Imaging SW
  - Reliability (crash could lead to error in data)
  - Error handling (what in case of reading error?)
  - Hashing (reliable integrity)
  - Maximum compatibility (various sources & formats)
  - Speed (multithread processes)

Handling & Securing

- 2 copies as minimum on different HW
  - 1st copy compressed & archived
  - 2nd copy as working
- Read-only access (?)
- Encryption(?)
- Blockchain(?)

Practice

- How to protect electronic attachement to the forensic report?