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 1

- Digital Forensic vs. Digital Forensics
- Digital Forensic Science Definition
  - **Digital Forensic Science** is an exact forensic science that examines the processes and patterns of the origin, existence and extinction of digital information and interprets this knowledge to explain the processes associated with it for the purposes of forensic examination.
- Digital Forensic Analysis Definition
  - **Digital Forensic Analysis** is the process of applying scientifically justified and proven methods to examine digital traces for decision-making by government agencies (e.g. police investigators, prosecutors and judges but other state bodies too) and other legal entities (e.g. organizations and private persons) for purposes of legal acts.
- Digital Forensic Analysis Basic Properties
  - Independency, Professionalism, Repeatability, Reviewability, Integrity, Legality, Documentation
- Expert vs. Forensic Expert

Recap 2

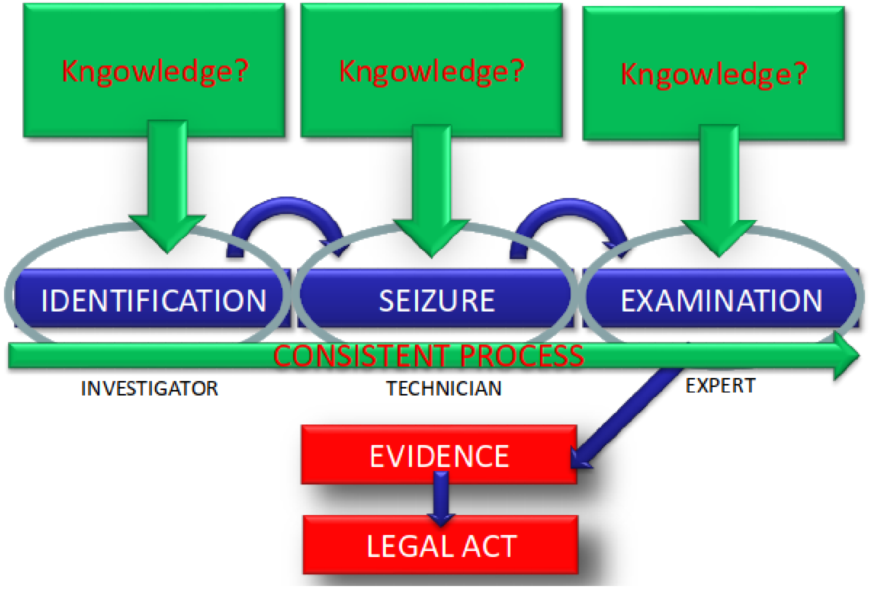
- Digital Trace
    - Immaterial, Latent, Coded,
- Digital Trace
    - Seizable, Understandable, Relevant
- Locard ’s Principle in Digital World
- Digital Traces and their properties
    - Material substance of digital trace, Latency, Time identification, Information value, Lifetime, Quality of Archives, Big volumes of data, Big density of information, Dynamics of development of ICT, Speed, Complexity, Territorial dimension, Data protection, Automatisation, Hiding of identity, Restoration of data, Low confidence in digital evidence weight, …

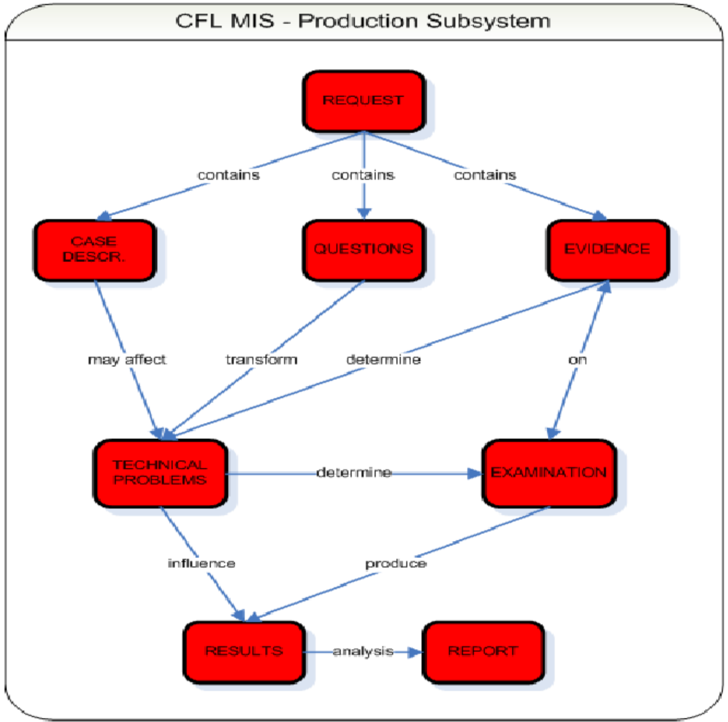
Recap 3

- Where the digital traces are?
  - Integrated (Permanent (static) and 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 (based on level of control over the seized data)
- Bit Copy vs Logical Copy
- General rules for handling

Recap 4

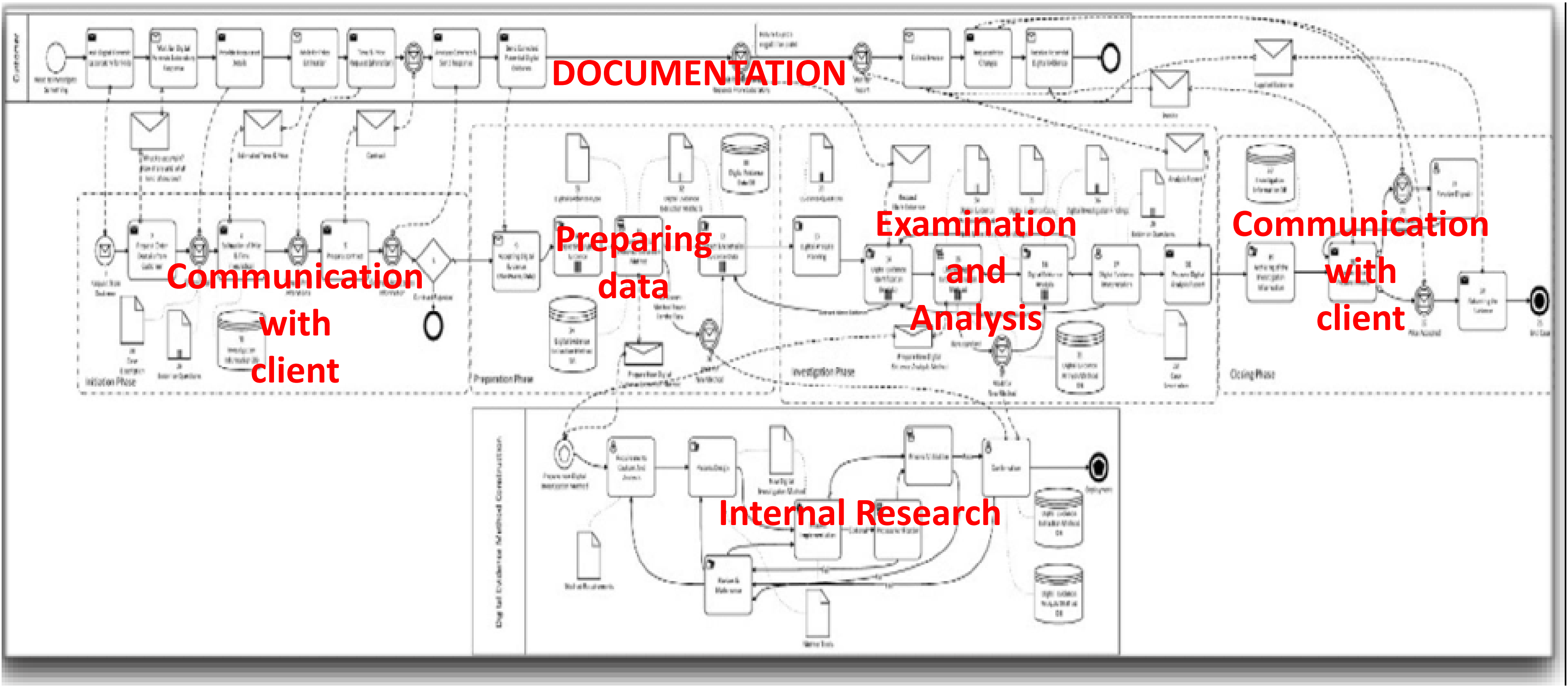
- Digital Forensics Examination Models
  - Preparation ; Identification ; Collection/seizing ; Integrity ; Examination ; Analysis ; Reporting ; Presentation ; Archiving/deleting/returning





Recap 5

- Digital Forensics Lab Buliding



Recap 6

- Elecrtonic evicence and the Law
  - Informal Cooperation
  - MLA
  - Interpol
  - Europol
  - Budapest Cybercrime Convention
  - European Investigation Order

Seminar 1

- **FTK Imager**
  - **Making copy of digital evidence based on digital forensic best practices**
    - Find and install this tool on their computers
    - become familiar with the features and capabilities of this tool
    - practice to make a forensic copy of USB Flash-drive and get to know the results of copying
    - become familiar with other tool options, in particular viewing the contents of a copy
- **The result**
  - the ability to make a forensically correct copy of data storage data and to perform elementary evaluation of the content of such a copy of data.

Seminar 2

- **Autopsy**
  - install Autopsy and become acquainted individually with the functions and capabilities with the aim to find in the seized data information which is part of the assignment of the seminar paper
- **The result**
  - the ability to make a forensically correct copy of data storage data and perform basic analytical work on forensically seized digital data according to the assignment.

Seminar 3

- Digital forensic report
  - Basic structure
  - Best practices
    - Precise documentation
      - Photo, Video, Paper, Notices, Temp and Working Data, …
    - Correct Data Acquisition
    - Examination Plan
    - Exam Results
    - Exam Analysis
    - Results and Anwers Formulation
- Autopsy Tips and Tricks