

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
- Computer 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

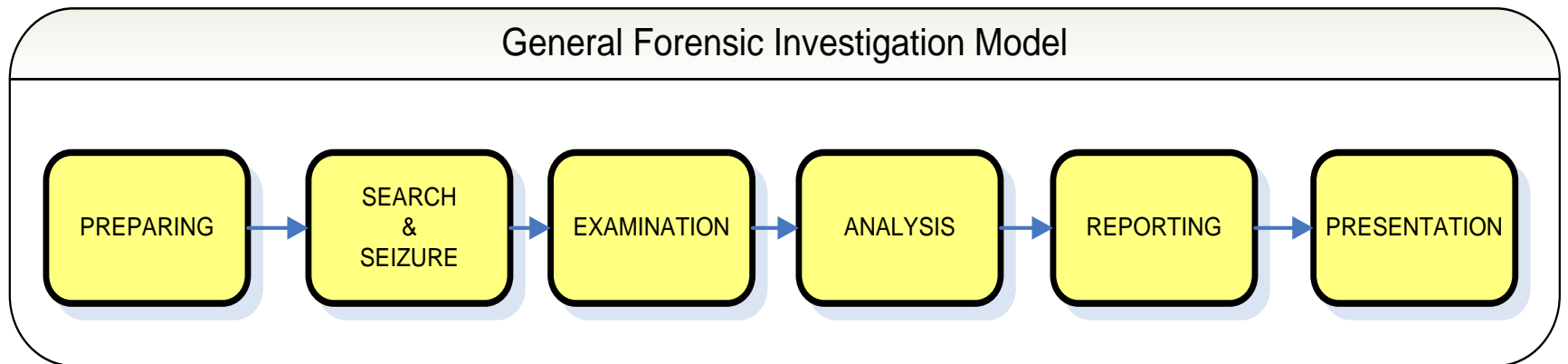
Recap

- 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









Today outline

Process of the Digital Forensic Examination

Digital Forensic Examination Model

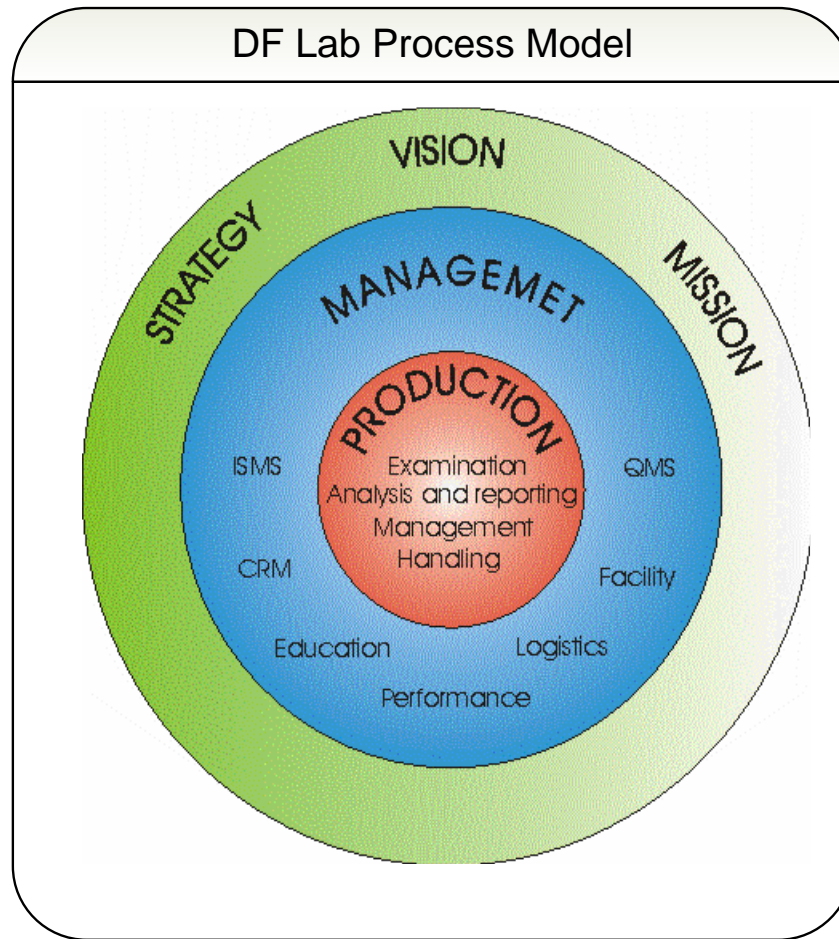


Models

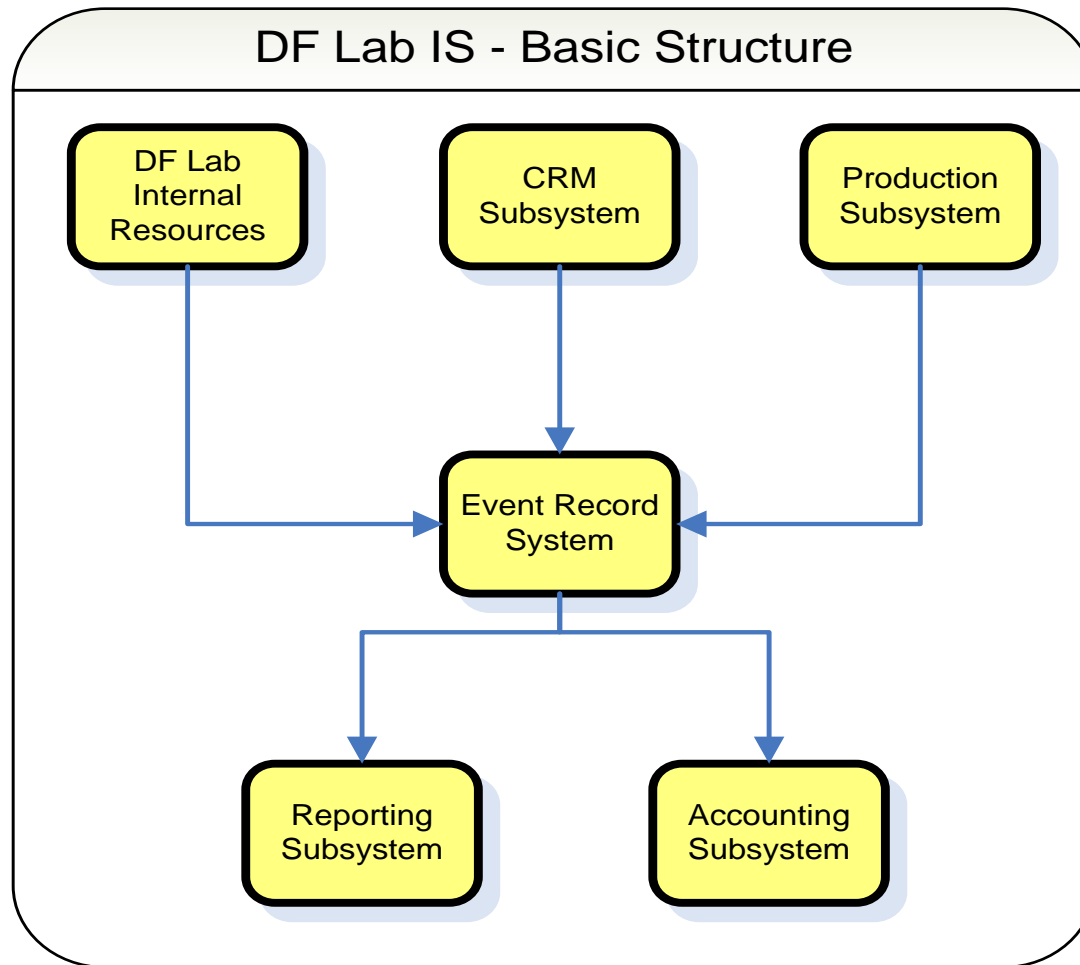
- The Abstract Digital Forensic Model (Reith, et al., 2002)
- The Integrated Digital Investigative Process (Carrier & Spafford, 2003) [1] 
- An Extended Model of Cybercrime Investigations (Ciardhuain, 2004)
- The Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004)[2] 
- The Digital Crime Scene Analysis Model (Rogers, 2004)
- A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe & Clark, 2004)
- Framework for a Digital Investigation (Kohn, et al., 2006)[3] 
- The Four Step Forensic Process (Kent, et al., 2006)
- FORZA - Digital forensics investigation framework (leong, 2006)[4] 
- Process Flows for Cyber Forensics Training and Operations (Venter, 2006)
- The Common Process Model (Freiling & Schwittay, (2007) [5] 
- The Two-Dimensional Evidence Reliability Amplification Process Model (Khatir, et al., 2008)[6] 
- The Digital Forensic Investigations Framework (Selamat, et al., 2008)
- The Systematic Digital Forensic Investigation Model (SRDFIM) (Agarwal, et al., 2011)[7] 
- The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice (Adams, 2012) [8] 

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

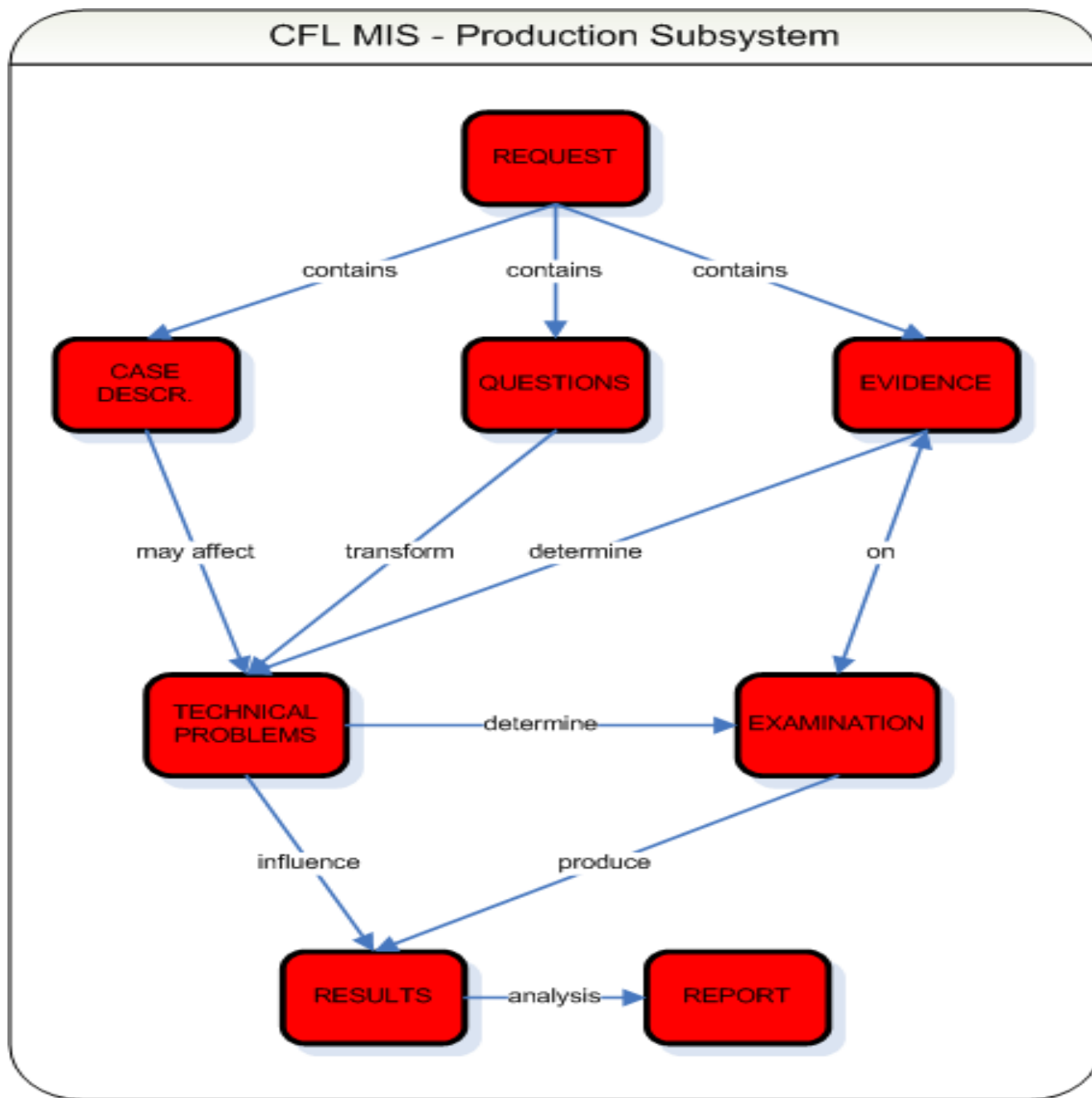
DF Lab Process Model

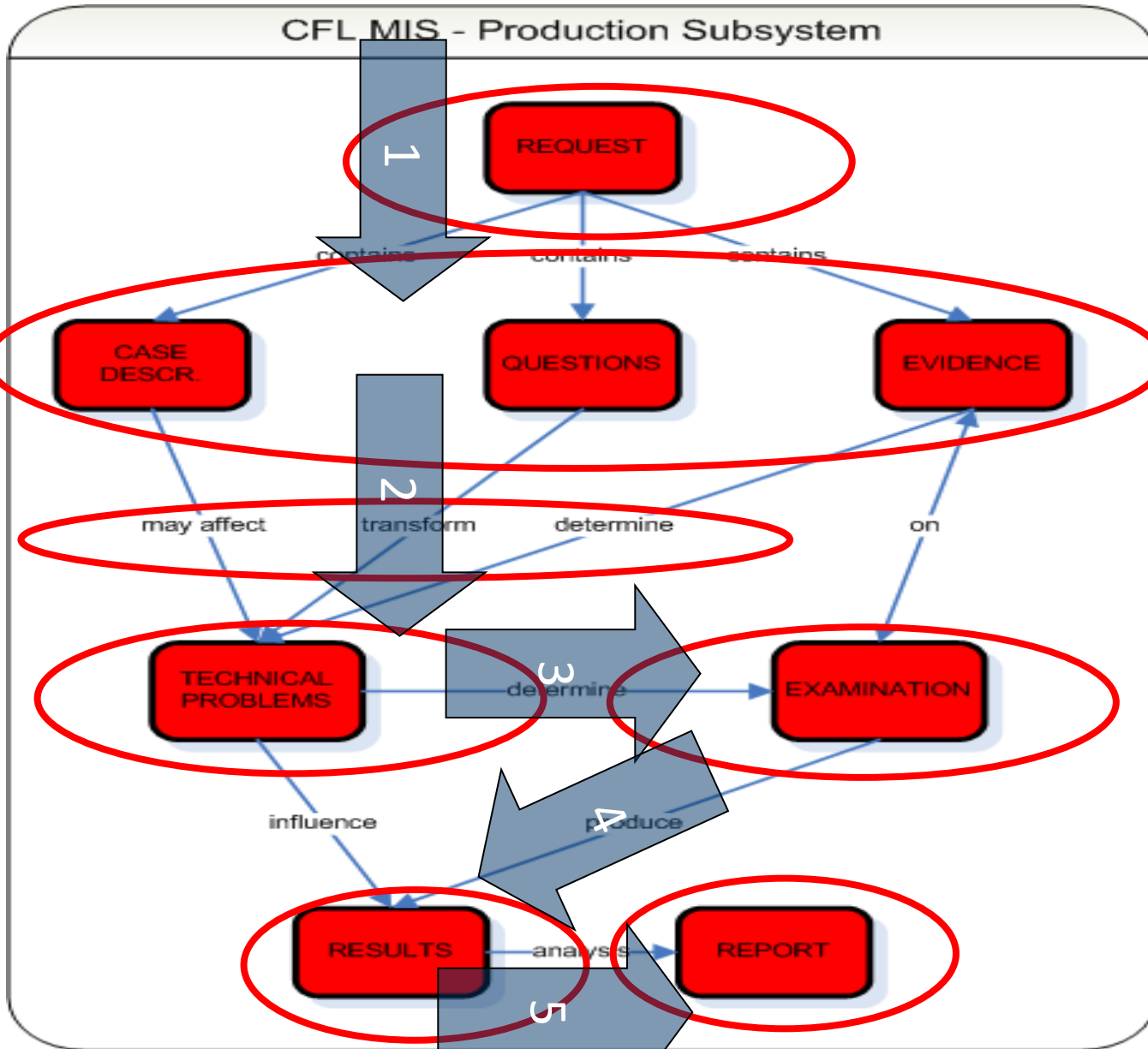


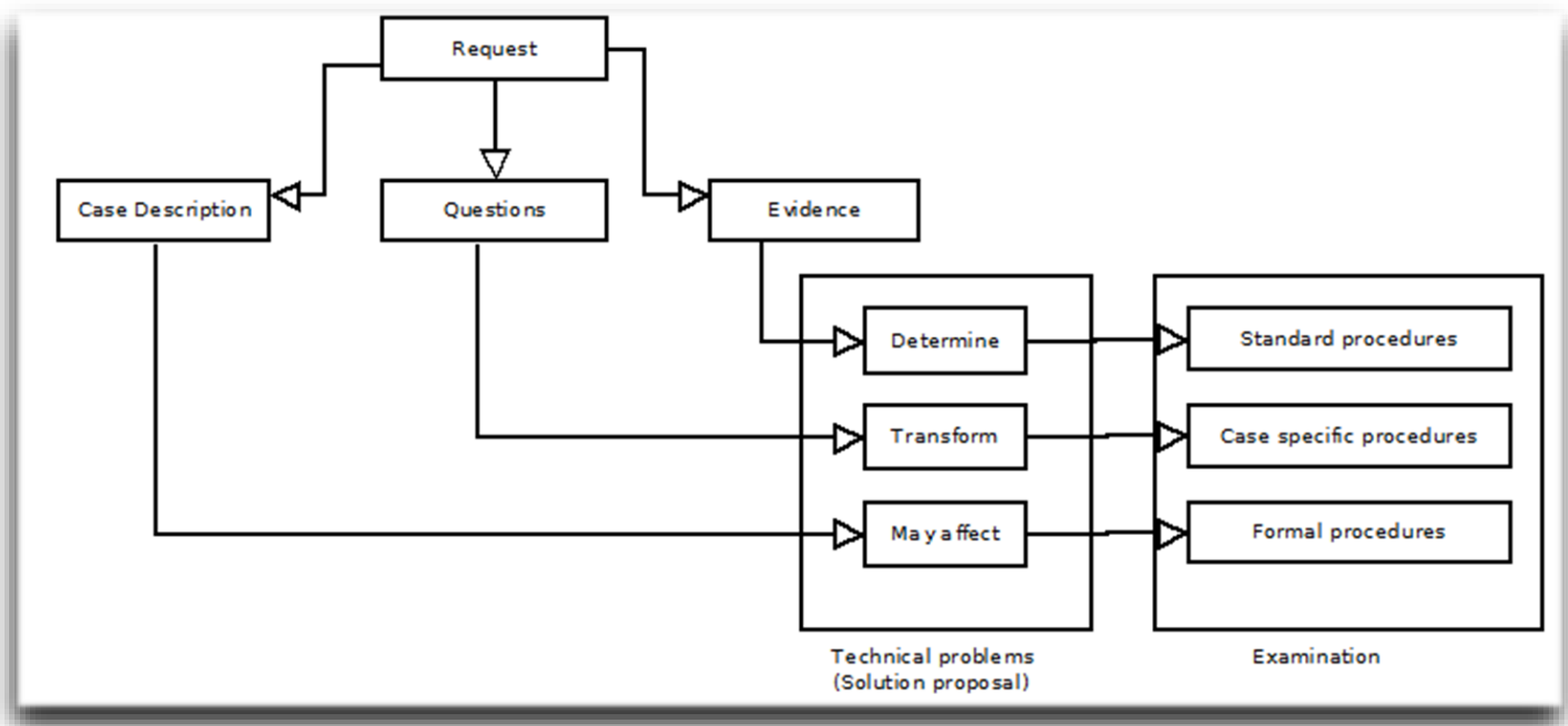
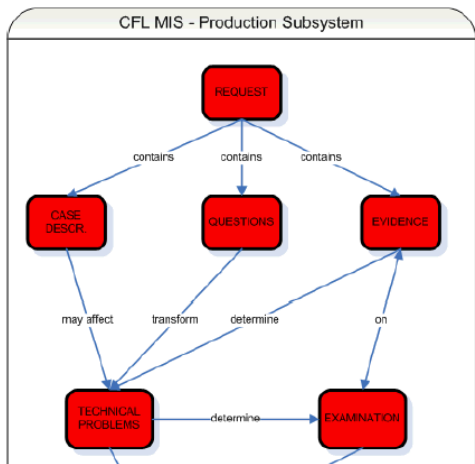
DF Lab Process Model



CFL MIS - Production Subsystem





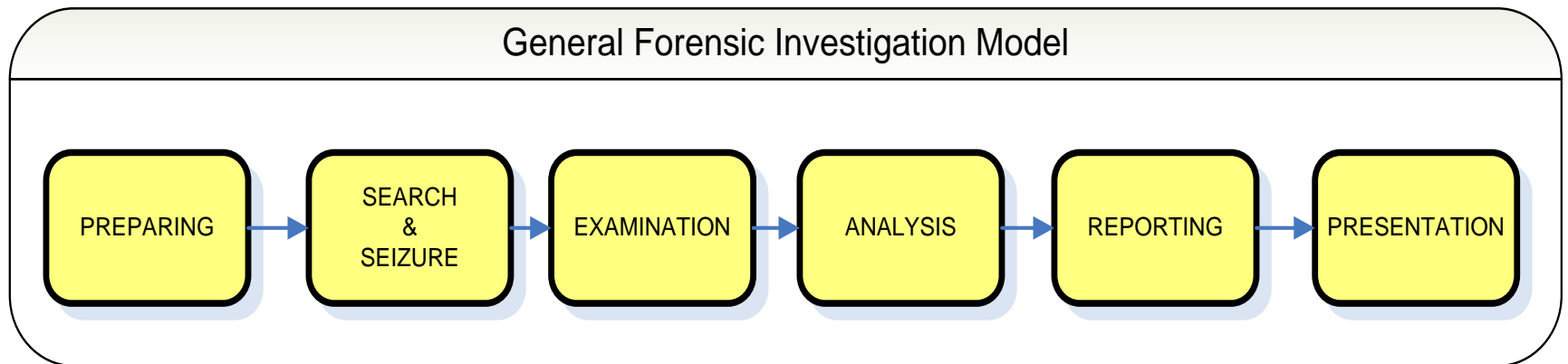


- **Description of the case**
 - describes the reason / purpose of the inquiry request
- **Questions**
 - Specific problem specification
- **Traces / samples**
 - They determine standard procedures

The specificity of forensic work can therefore be described by the definition:
Knowledge of input objects (footprints / samples) and activities that need to be done in a way appropriate to the purpose of the task in order to solve the given problem

6 step of digital forensic exam

- DF Laboratory view



9 steps of digital forencic exam

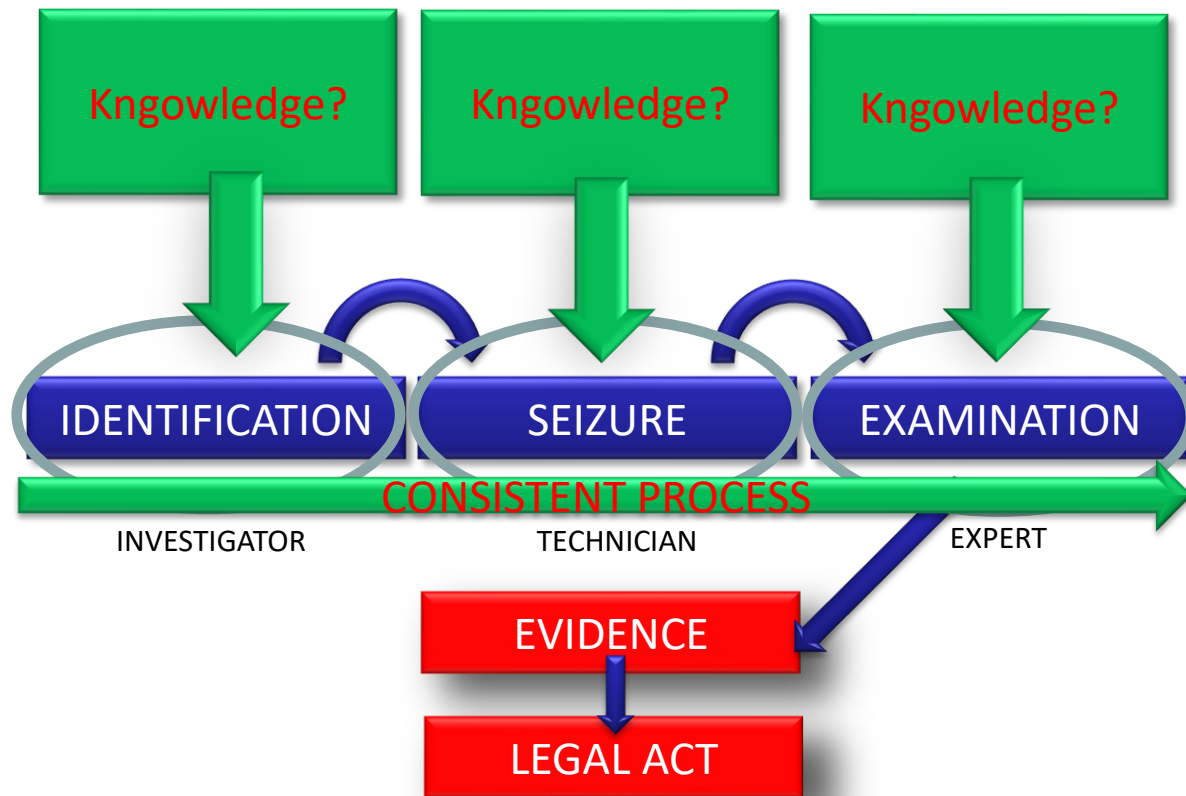
- Preparation
- Identification
- Collection / seizing
- Integrity
- Examination
- Analysis
- Reporting
- Presentation
- Archiving / deleting / returning

Preparation

- Assumptions
 - Organizational (efficiency and work organization)
 - Technical (tools, devices, HW and SW, venue ...)
 - Qualifying (relevant expertise and experience)
 - Material (few cases vs too many cases)

Identification

At the crime scene...



Identification

The nature of the case is crucial

The essential role of the investigator

It should always be the responsibility of the investigator to consult possible traces / information in ICT with expert.

Information is crucial to the investigation, and at present digital means are one of the essential sources of information for investigating virtually any crime.

Diversity of information character

“Documents” are only a fraction of the information that can help in the investigation (see “Fatal error”, DFJ 2/2005, p. 20)

The result of the identification assessment is a strategy of seizing digital information

Collection/Seizing

- The seizing strategy determines:
 - Individual seizure activities
 - Selection of appropriate methods and procedures
 - Qualification of a technician who realize data seizing
 - Used technical and logistic means
- **... everything so that the data can be examined effectively**

Integrity

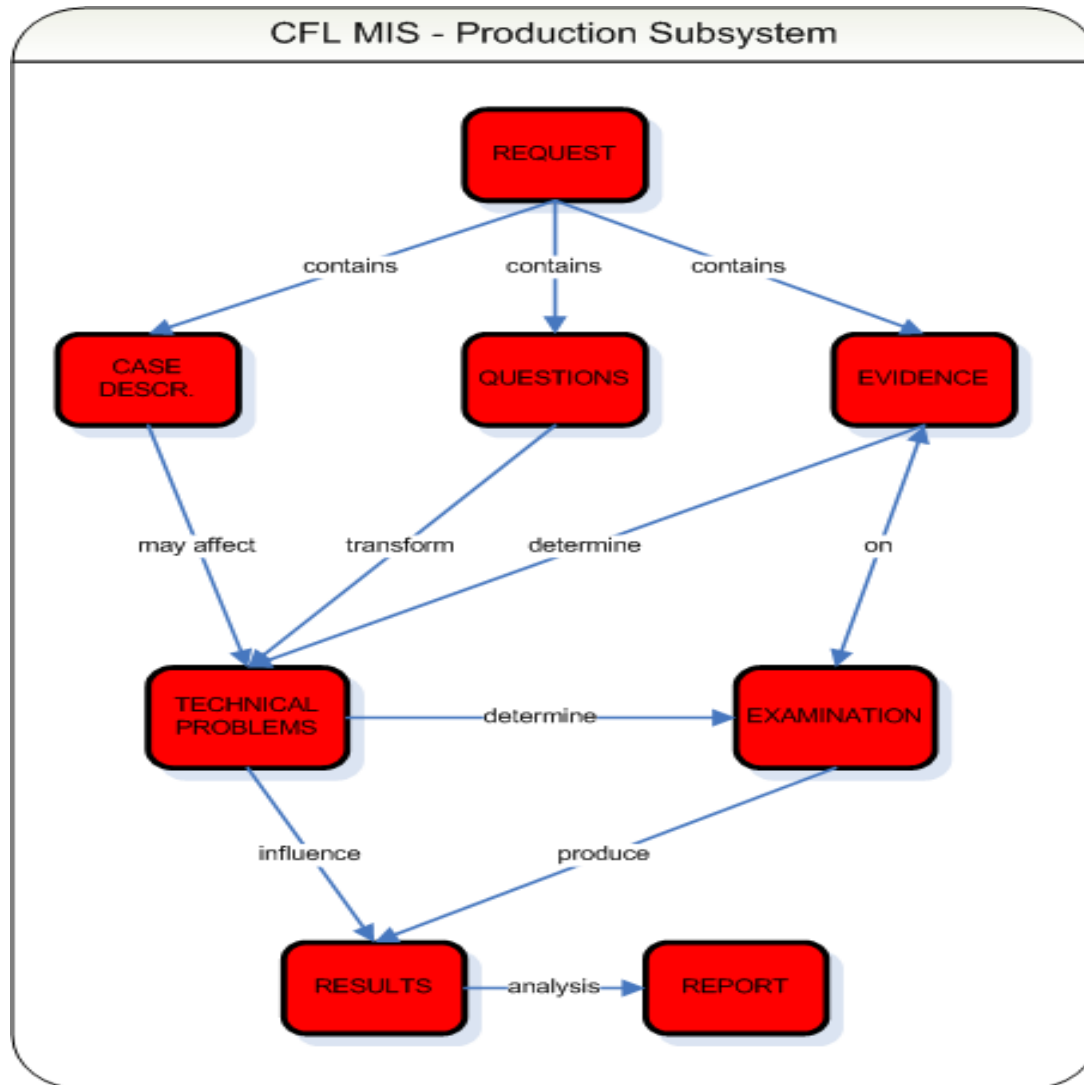
- Integrity of data traces
- Integrity of physical traces
 - Computer seizing procedure

Examination

- Unidentified and subsequently not seized traces cannot be examined
- Poorly seized traces can give poor, misleading or even false results
- Bad traces (both in terms of complexity and quality) multiply the difficulty of examination

(Digital Forensic Triage processes)

Analysis



Reporting

Presentation

Archiving / Deleting / Returning

DFMS

