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

1st break

- Digital Forensic
- Digital Forensics

Science & Practice

Přemysl Janíček, Jiří Marek a kol., Expertní inženýrství v systémovém pojetí, Grada 2013, ISBN 978-80-247-8196-9

*„**Attribute A0** - definition of entity of interest. When one talks about something, one should know what. Otherwise, they are gibberish. This is true in everyday life and at professional conferences. It should be no different in written private, professional or scientific texts and of course in publications. Thus, in all these cases, what is the subject of our interest in "expression", regardless of its form, must be defined in terms of content, logic and linguistics. In many cases, this is not the case, so we read the book and only think what the author is imagining under the entity he writes about.*

***Attribute A1** - conceptual purity requirement. Conceptual purity means the correct definition of terms in terms of meaning and content. It is a prerequisite for rational and correct communication between people. An individual who does not have clear terms in terms of meaning has no inhibition to create any sentence, even completely meaningless. Compliance with conceptual purity is not a vocabulary, it is a communication duty. Each of us should have a clear structure of terms, both in everyday life and in our profession. The expression of pure content should be one of the cultural characteristics of everyone.*

The following principle also relates to conceptual purity: if a publication, an article or just a paper deals with a particular entity that may not be known to everyone, it is always necessary to define that entity at the beginning.

***Attribute A2** - correct problem definition and formulation. Whatever one does, one must always be clear about what it is and what it wants to achieve. Usually one solves a certain problem situation*

(This is a situation that requires subjective or objective reasons to change). First, it needs to make a comprehensive analysis of this situation, clarify what is essential in it, and then formulate the problem. However, they must all be preceded by a proper definition of the concept of 'problem'.“

Science & Practice

Přemysl Janíček, Jiří Marek a kol., Expertní inženýrství v systémovém pojetí, Grada 2013, ISBN 978-80-247-8196-9

„System approach and system thinking have two spheres. The first is philosophical-theoretical, the second is application, and there should be two-way interactions between the two in this sense: the application sphere needs a theoretical elaboration of problem situations and proposals of methods for their solution. The philosophical-theoretical sphere should take from the application sphere incentives for its theoretical work.“

Forensic Science & Practice

- ISO 17025, chapter 5.4.

> When the customer does not specify the method to be used, the laboratory shall select appropriate methods that have been published either in international, regional or national standards, or by reputable technical organizations, or in relevant scientific texts or journals, or as specified by the manufacturer of the equipment. Laboratory-developed methods or methods adopted by the laboratory may also be used if they are appropriate for the intended use and if they are validated. The customer shall be informed as to the method chosen. The laboratory shall confirm that it can properly operate standard methods before introducing the tests or calibrations. If the standard method changes, the confirmation shall be repeated.

Forensic Science

Wikipedia (https://en.wikipedia.org/wiki/Forensic_science):

Forensic science, also known as **criminalistics**, is the application of science to criminal and civil laws, mainly - on the criminal side - during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure.

Criminalistics & Forensic Science

(from CS and EN Wikipedia):

- (CS) **Criminalistics** explains the rules of origin, collection and use of the traces and the court evidence. In the Czech concept, it is based primarily on criminal law and develops methods, procedures, means and operations for the successful detection, investigation and prevention of crime.
- (EN) **Forensic science** is the application of science to criminal and civil laws, mainly during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure.

Criminalistics & Forensic Science

- (prof. Musil:)“**Criminalistics** is an independent discipline serving to protect citizens and the state from crime by clarifying origin, collection and use of traces and other criminally relevant information, and by developing methods, procedures, means and operations in accordance with the Criminal Code and Criminal Procedure Code for the successful detection, investigation and prevention of crime. ”
- (Svetlik:) „**Forensic science** manage and influence the scientific activities related to the discovery, seizing and follow-up examination of traces scientifically, professionally, methodically and practically, search for new forms of traces, to determine their recoverability, processability, meaningful value, to find suitable, effective and feasible procedures for their securing and consequently to scientifically justifiable procedures for their examination, either by their own development or by adopting and adapting existing procedures, and provide credibility and reliability of such methods.“

2nd break

- Criminalistics
- Forensic Science

Forensic Sciences

Forensic sciences are sciences focused on cognition and analysis of traces (or more generally subjects of examination - expert problems) and ***the actual use of the results of such examinations in cases of legal acts (decision-making and other needs of state bodies or legal acts of other subjects) is not the problem of forensic sciences****.*

Digital Forensics

DFRWS [https://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf, p. 16] in 2001:

"The use of scientifically derived and proven methods towards preservation, validation, identification, analysis, interpretation, documentation, and presentation of digital records 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. "

Digital Forensic Science

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

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

Independency

Svetlik (https://msvetlik.wordpress.com/2012/06/04/kde-stoji-soudni-znalci-ii/):

“The only goal of the expert work and its only mission is to document the truth. We do not decide how the true is used, exploited or abused this truth. We do not want to have anything to do with it, we should not have anything to do with it. Our position should be totally independent. Regardless of whom we find the truth for, and for what and in what way the truth we find is used or misused. Strict independence. ”

Professionalism

Act on Experts (Section 4 (1) (e) and (f)) [Act No. 36/1967 Coll.]:

"…has the necessary knowledge and experience in the field in which he is to act as an expert, he has received special training for an expert activity, in the case such training is introduced, has such personal qualities that give the presumption that the expert activity can be properly performed "

Repeatability

- For repeatability is necessary detailed planning and documentation of all work with the traces, the same starting conditions, elimination of external influences and, if possible, permanent preservation of the examined traces.
- Digital traces can fulfill all abovementioned conditions

3rd Break

permanent preservation of the digital traces

Reviewability

- For the review it is necessary to ensure identical starting conditions, i.e. identical digital traces.
- If we are faced with the task of reviewing the original expert examination, we must realize that the same input information and traces must be available to carry out this task as the original expert examination.
- If the scope and quality of the input information and tracks changed from the original investigation, especially if the original tracks were not available in their entirety or if the track range was additionally extended, it would no longer be a review but an entirely new examination.

4th Break

Repeatability & Reviewability

Integrity

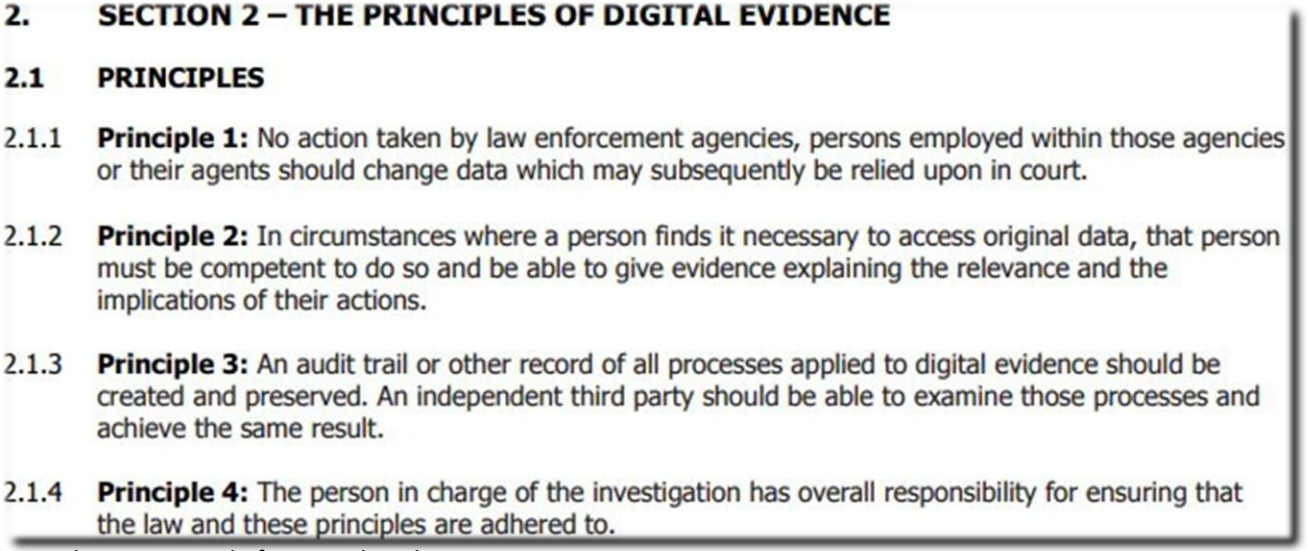
- The original and copies of digital data have identical predicative ability.
- Ensuring the integrity of digital tracks is a diverse set of procedures and measures designed to perform all activities and operations in a way that does not change data.
- The calculation of the checksum itself does not in any way ensure that there is no change in the data and the checksum serves only to verify whether the changes have occurred.

5th Break

Original & Copy of the Digital Trace

Legality

- Legality of the digital traces
- Legality of methods used in examination process



2. SECTION 2 – THE PRINCIPLES OF DIGITAL EVIDENCE

2.1 PRINCIPLES

2.1.1 **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

2.1.2 **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

2.1.3 **Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

2.1.4 **Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

ACPO Good Practice Guide for Digital Evidence, Version 5
http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Documentation

- Independency
- Professionalism
- Repeatability
- Reviewability
- Integrity
- Legality

All abovementioned properties have to be precisely documented.

6th Break

(general) expert report & forensic expert report