Theory and Basics of DF

1. Name of the subject:

"Theory and Basics of DF"

2. Objective of the course:

To explain to students the essence of forensic examination, that is, what is specific about forensic work, what distinguishes it from other forms of examination. The general nature of forensic work can be inferred from the source [1]. The specific basics of DF must be derived based on the theory of digital trace, which will be submitted and explained within the subject. The theory of the digital trace, as given in this subject, is newly conceived and has not yet been published anywhere in the world aboutthe form (according to the available information).

3. Exit from the subject

Students will be able to correctly understand the place, role, purpose, and ways of using DF in practice (see "Outline of the subject"). They will be able to evaluate whether of analyses are appropriate and effective in a given situation, they will be able to evaluate in a framework whether DF analysis can be carried out internally or with the help of an external expert, and they will be able to evaluate whether the implemented DF analysis meets the elementary requirements that are placed on such analysis.

4. Outline of the subject

The course is built for one semester - a total of 6-7 basic lecture circuits:

(a) ***The basics, place and role of DF***, forensic science vs. the performance of forensic examination, forensic examination as a special group of activities and their purpose in society. DF in Cybersecurity (e.g. according to ISO/IEC 27000 series) and DF in Cybercrime Investigation.
(b) ***Digital trace as*** a basic subject of research in DF. Definition of digital trace, properties, basic principles of working with digital traces. Documentation of digital traces.
(c) Types of ***digital traces***, ways of obtaining/securing them. Principles of digital trace manipulation, protection, security, and durability. Typical digital trace sources, basic physical principles of digital data recording and typical recording media.
(d) ***DF expert examination process***. Procedures, principles, methods, process models. Principles of structure, form and content of forensic report (expert opinion).
(e) ***Work in DF laboratory***. Construction, organization, laboratory management. Quality management of work in DF lab. Certification andproof of competencies, regulatory.
(f) ***Laws and other regulatory*** for the performance of expert work, the situation in the Czech Republic, Europe, and the world. Rules of international cooperation in the field of DF. The term "Electronic Evidence". How the performance of forensic examination is regulated. Status of experts

in relation to the LEA.
g) ***Development of digital forensic*** science - perspectives and current challenges, "classic" and new areas of DF, current and potentially future needs of exploration in new areas of digital technology use.

In the frameworkand practical exercises, the aim is to develop a simple forensic report, on which students will practice the methodology, structure, and procedures of working with digital traces. To do this, it is necessary to manage at the basic level of data acquisition and work with forensic analytical SW (naturally only at the elementary level) so that they are able to properly process simple assignments and write an expert report formally correctly. As a result, it is not so much about the correctness of the analysis, but about the methodologically and formally correct procedure for processing report.
3 practical exercises are foreseen:
(a) practicing the procedure for correct data acquisition and documentation
b) practicing the procedure of working with forensic analytical SOFTWARE
c) procedures for the preparation of a forensic report

5. Scope of the subject

The scope of the course is divided between lectures, exercises and a separate task.
Lecture range: 2 hours per week (4 hours once every 14 days)
Exercise range: 3 times during the exercise semester each 2 hours

Lectures are therefore in a more-or-less standard range of teaching. Exercises are less demanding for practical work,therefore only 3x2 hours per semester are assumed.

In addition, the practical part of the homework is assigned to students, which is precisely the processing of a simple expert report, where their task in practice is to apply theoretical and methodological data of work with digital traces and to test compliance with the formal requirements for the processing of the report so that it can be accepted by the courts as evidence. Practical exercises, albeit to a minimum extent, are being prepared to assist students in solving a home assignment.

6. Professional qualifications

A prerequisite for completing the course are good basics of ICT (I would like to say that it is not only the user level, it is necessary to know the technical basics), in particular:
- knowledge of the principles of the work of conventional operating systems,
- basic knowledge of the principles of file systems work
- basics of network communication and internet

7. Continuity with other objects

In relation to DF issues, this is a basic "signboard" subject. Rather, all other subjects in the DF field should be based on the knowledge of this subject.

8. Technical (and other) requirements

Requirements for lectures:
- data projector,
- whiteboard
- Internet connection for lecturers and students,
- students will use their own NB (min. average performance parameters, OS WIN or LINUX), tablet potentially sufficient to solve ad-hoc requirements at lectures (online search for required information from open sources)
- SW - opensource only according to the speaker's requirements

Requirements for exercises minimum:
- own NB students of min. average performance, OS WIN/LINUX, word processor, PDF printer, basic SW for photo processing, ev. spreadsheet
- opensource/free data acquisition tools and basic digital forensics and analysis for WIN/LINUX OS (e.g. FTKImager, Autopsy)
- camera of its own, mobile phone camera is sufficient

9. Other/other requirements:
First exercise after the third lecture - see above 4.c)

10.Rated
Written exam 40%
Seminar work (test forensic expert report) 30%
Work/participation in exercises 30%

[1] - Přemysl Janíček , Jiří Marek and kol ., Expert Engineering in System Concept , Grada 2013, ISBN 978 80 247 8196 9