SEMINAR 2

Cílem cvičení je seznámit se s principy práce nástrojů pro forenzní analýzu digitálních dat.

Jako příklad bude použit nástroj Autopsy (opensource).

Úkolem studentů je:
- najít a instalovat tento nástroj na jejich počítače
- seznámit se individuálně s funkcemi a možnostmi tohoto nástroje
- pořídit pomocí nástroje FTK Imager forenzní kopii předem připraveného USB Flash-disku, který bude sloužit jako příklad pro forenzní analýzu pomocí nástroje Autopsy
- seznámit se s možnostmi nástroje Autopsy s cílem nalézt v datech zájmové informace, které jsou součástí zadání seminární práce (viz zadání seminární práce).

Výsledkem cvičení je schopnost studentů pořídit forenzně správným způsobem kopii dat datového úložiště a provádět základní analytické práce nad forenzně zajištěnými digitálními daty dle zadání.

The aim of the exercise is to become familiar with the principles of digital forensic analysis tools.

Autopsy (opensource) will be used as an example.

Students' tasks are:
- Find and install this tool on their computers
- become acquainted individually with the functions and capabilities of this tool
- use FTK Imager to make a forensic copy of a pre-made USB Flash Drive, which will serve as an example for forensic analysis using Autopsy
- to get acquainted with the possibilities of the Autopsy tool with the aim to find in the seized data information which is part of the assignment of the seminar paper (see assignment of the seminar paper).

The result of the exercise is the ability of students to make a forensically correct copy of data storage data and perform basic analytical work on forensically seized digital data according to the assignment.