Digital Forensics 2016/17
Written Exam, May 8th , 2017

The exam must be taken individually. You may use any literature.

You may be awarded extra points if you answer all questions at least partially. Although individual questions may be more closely related to a single chapter from the lectures, you will often need to use the knowledge from the other chapters as well. Some questions are intentionally vague and require you to make assumptions to give a precise answer. In such cases, be precise in answering the questions and specifying the assumptions. Precise answers will bring more points. You will not get full points for general answers.

You have 60 minutes to take the test.

May your knowledge bring you success!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga:

VPRAŠANJA: Basics. Peter has to examine a disk which was once used by Cefizelj. Because Cefizelj is evil, Peter suspects that he has hidden some data between the first and the second partition. Peter has run a program which has given him the following output:

```
Device       Start        End   Sectors   Size Type
/dev/sdb1     2048    1503231   1501184   733M Microsoft basic
data
/dev/sdb2  1507328    3504127   1996799   974M Linux filesystem
/dev/sdb3  3504128 1000214527 996710400 475.3G Linux filesystem
```

A) (i) Which tool/program can he use to find the beginning and end of each partition? How much space (in bytes) is there between the first and second partition? Explain how you got your result. (iii) How would you store the data between the partitions into a file called vmes.raw? Write down the exact command.

B) Suppose that a digital investigator discovers that their current case is very similar to one of their past cases. This leads them to continue their investigation in the same manner. What do we call such an investigation? Justify your answer.

C) During lectures, we mentioned the *Locard principle*. What is it? Describe three situations where it has come into play and describe how.

2. naloga: File systems

VPRAŠANJA:

A) Peter really likes to film nettles growing by the church. He records their growth throughout the year in high definition, for which he need a lot of disk space - at least 10TiB each year. Unfortunately, the biggest disks Peter can afford to buy are only 1.5TiB in size. Peter would like to have all the video recordings in a single directory on his computer. (i) If Peter is certain that no disk will ever fail, which technology can he use? Name at least two options. How many disks does he need? (ii) If Peter wants to retain his data even if one of his disks fails, how should he assemble them? Draw a sketch of the physical and logical devices involved.

B) Name three locations where Peter Zmeda may look for web-related activities on a Windows OS. For each of these locations, give a trace example and what you could deduce from it.

C) This time, we will look at the `ext3` filesystem. A basic structure for storing metadata regarding a file is called an `inode` – index node, which contains 32-bit references to the disk's contents. (i) What is the maximum size of a partition which we can use `ext3` on with references of this size? Explain your answer. (ii) The index node contains multiple timestamps. Which ones and when (during which operations) are they set/updated? (iii) What is the biggest difference between `ext2` and `ext3` filesystems?

3. naloga: Network forensics and system logs

VPRAŠANJA:

A) Peter Zmeda needs telnet access his device because it can not run an ssh server on it. To achieve at least some level of security, he has made sure that only connections from IP `10.20.30.40` are accepted. Which attack can be used on Peter's device? Explain your answer and describe the attack in as much detail as possible.

HINT: For the description to make sense, you may want to describe the system's topology and note the locations of the device and the attacker.

B) Peter Zmeda has received the follosing message from his server (`bor`) over the `syslog` protocol:

```
<17> 1 2016-10-11T22:14:15.003Z bor pif 2234   Tezave, tezave!
```

Suppose that the message is fully compliant with RFC5424. (i) Is Peter supposed to do something, or can he ignore the message? Explain your answer. (ii) Which service does the program with PID 2234 provide? Explain your answer.

C) People at the company *Butale salt, inc.* realized that someone has stolen the recipe for salt production. They called Peter Zmeda, a computer forensics expert, who has found that someone had broken into Luka Lukež's computer which was inside the company network. (i) Write down three hypotheses how someone could have broken into the computer (ii) For each hypothesis explain how its validity could be tested.

4. naloga: Mobile devices and conducting the investigation process.

VPRAŠANJA:

A) While inspecting a disk, looking for evidence pertaining to a drug-smuggling case, you inadvertantly stumble across some top-secret plans of a military targeting and communications system. What should you do? Justify your answer.

B) A basic difference between a mobile phone and a desktop computer is that the latter is in the same place practically all the time. (i) Describe three methods of figuring out the movement of a mobile phone. (ii) For each method give an estimation of how difficult it is to get the data and the preconditions that must be fulfilled. (iii) Does it make sense to gather the location data using all three methods at the same time? Explain your answer.

C) Peter has been using Firefox as his web browser since time immemorial. While rummaging through his cupboard, he found a disk from 5 years ago which amongst other things contains his old home directory. He would like to check which websites he used to visit while he was using this disk. (i) Where can he find the web history data? (ii) Which format is it stored in? (iii) Which tool can he use to inspect it?