Digital Forensics 2018/19
Written Exam Ærraliða, 13th, 2019

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.

A) In the suspect's apartment we found a running but locked computer. We believe the disk is encrypted. How could we proceed? Explain your answer.

B) In order for evidence to be admissible in court, it needs to meet five basic criteria. (i.) Which are they? For each criterium, explain why the evidence should meet it. (ii.) For three criteria, give an example of when evidence does not meet it.

C) Peter Zmeda suspects that someone has slipped a virus into his *initial ram disk*, `initrd`. (i.) Can this be done? If yes, how? If not, why not? (ii.) Peter would like to get rid of the initrd. Is this even possible? If yes, how? If not, why not?

2. naloga: File systems.

VPRAŠANJA:

A) Peter Zmeda received a disk containing an XFS filesystem to analyze. In order to preserve all data, he mounted it as read-only (`-o ro`). He then copied all the files. (i.) Which data has he destroyed? (ii.) Which data has he missed? (iii.) How shoud he really have inspected the disk? Write the sequence of commands and explain each command.

B) How many entries does a FAT table have? Explain your answer.

C) Journals appeared as a part of filesystem in order to solve multiple problems. (i.) Describe at least one problem they solve and how. (ii.) In the journal of the `ext` filesystem, there are 4 types of blocks. Which ones? (iii.) Two of the four block types never appear in a single transaction. Which ones and why? (iv.) Draw a schematic of a partition and mark where the journal(s) is(are).

3. naloga: Mobile, network forensics and system logs.

VPRAŠANJA:

A) Peter has received a computer running Windows XP to investigate. He would only like to know who and how many times has logged in on the computer. He has a tool which accepts the path to the filesystem and outputs a list of all logins. Unfortunately, he can not afford to copy the whole disk because it is 4TiB in size and almost full while Peter has only 500GiB to spare. Which files does he actually have to copy? Explain your answer.

B) The most defining characteristic of mobile devices is that they are mobile. (i.) Describe three ways Peter Zmeda might find out where a suspect's mobile device is located. (ii.) For each, describe where Peter can find information regarding the device's location. (iii.) Peter suspects that Luka Kratkohlačnica has been speaking to the horrible bandit Cefizelj over a mobile phone. List 5 hypotheses regarding where and how Peter may check whether this is true. The hypotheses must, ofcourse, be reasonable.

   NAMIG: You will have to be inventive answering this question.

C) To what kind of attack are the devices that trust other network devices only on the basis of their IP address suspectible? Explain your answer, preferably by explaining how such an attack is performed.

4. naloga: Conducting an investigation and malware.

VPRAŠANJA:

A) Peter Zmeda has received a computer containing two hard disks to investigate. The root directory or drive `C:` is visible on his Linux workstation as /dev/md0. He has created a copy of the root directory without first mounting the disk. He then performed his investigation on the copy.

   At court, they accused him of destroying some data. Has he really? If yes, how? What should he have done to avoid the destruction? If not, what should he do to prove that he has not?

B) Which of the listed principles is *not* a basic principle that digital investigators at the scene of a crime should adhere to? Explain your answer.

   a.) first find the suspect so that they are not able to destroy any evidence;
   b.) never change the data on the device which is under investigation;
   c.) always maintain a journal containing all activities at the scene of a crime;
   d.) all of the above.

C) There are multiple models for conducting an investigation. (i.) If we look at the models in general, we get five basic steps. Which ones? (ii.) Think of a crime and describe it. Then, for each of the five steps, describe an action performed during this step while investigating the crime you have come up with.