Digital Forensics 2019/20
Written Exam Ærraliða, 19th, 2020

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!

TASK	POINTS	MAX. POINTS	TASK	MAX. POINTS	POINTS
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga:

QUESTIONS: Basics.

A) According to Parker, in which categories can fall computer involved in a crime? List an example for each category.

B) Evidence is central to forensics. A chain of custody is connected to its proper handling. (i) Where does a chain of custody start and where does it end? (ii) Describe an example for each link in che chain of custody. Explain what each of your examples proves. (iii) Why must the chain remain unbroken? Where and how could someone abuse a missing link in the chain?

C) Peter has received an old disk. Upon being powered on, the disk reported that it has 256 heads. When Peter opened the disk, he only saw one platter and one arm that moves across it. (i) How many read/write heads does the disk actually have? (ii) Why would the disk "lie" about the actual head count? Explain your answers.

2. naloga: File systems.

QUESTIONS:

A) One (`sda`) of the two Peter's disks (`sda` and `sdb`) broke down. The disks were successfully configured as a classic RAID 1 mirrored disk pair. In a panic, he tried to plug in the disk and copy the data, but he failed. As `root` he ran:

```
mkdir /rescue; mount /dev/sdb /rescue
```

(i) Can he still rescue the data at all? (ii) In general, describe the procedure how would he can do this. (iii) Draw a sketch of how the data on the disk `sdb` can be organized (partitions, file systems, etc.).

B) File metadata also contains various time data. (i) Write down what time data is present in both `ufs` and NTFS file systems. (ii) For each of the listed data, write down what they record and (iii) its format.

C) (i) Where is the GPT partition table (*GUID partition table*) usually located? (ii) What if it is located in several places, where is it then? (iii) Why would you want to have it in multiple places?

3. naloga: Network forensics and system logs.

QUESTIONS:

A) The Butale salt incident is complicating. Criminal investigators checked the records on Luka Kratkohlačnica's home computer and then also the records in the router. The final estimate was that almost 95% of the IP traffic from Luka's computer was to the address `abc.butale.si`. Based on this, the prosecutor decided to charge Luka with the theft of the receipt. Luke's advocate, of course, claims that Luke is innocent. (i) Give at least two possible reasons why Luka would legitimately communicate with the address so often. (ii) Justify your answers.

B) We'd like to find out what address Peter's computer had when he accessed the Internet yesterday. Where it is it *not worth* to look at?

   - in the log on the router;
   - printout of the `ifconfig` command;
   - in `syslog` on Peter's computer; or
   - to the address assignment table of the DHCP server.

   Justify your answer.

   HINT: Justification should include the reason why to look or not to look at a given place.

C) Peter Zmeda received a message from his server (`bor`) over the `syslog` protocol:

```
<63> 1 2016-10-11T22:14:15.003Z bor pif 2234  How come I didn't
see that?
```

   Let's say the message is fully compliant with RFC 5424. (i) Does Peter have to do something, or can he ignore the message? Justify your answer. (ii) Which functionality on the system is taken care of by the program with PID 2234? Justify the answer.

4. naloga: Mobile and network forensics.

QUESTIONS:

A) A cell phone was also located at the crime scene. The phone is still on and the technicians have already taken fingerprints from it. The phone was then handed over to Peter Zmeda for further processing. Just as Peter gets the

phone, an SMS message arrives on the phone. What should Peter do to secure the evidence as good as he can?

HINT: List at least three measures and justify them.

B) In the forensic processing of portable devices, it is also possible to search for data not only on the device. List at least three other data sources and justify your answers.

C) Peter Zmeda got his hands on the laptop of the suspect Cefizelj from Butale. Peter is supposed to inspect the disk. He pulled a disk out of the laptop and plugged it into his workstation. At this question, write down the specific commands that Peter should use with the familiar tools you used on the laboratory exercises.

   (i) How should he make a disk image? Let's say he completely trusts the hardware and will take care of the integrity of the disk sometime later.

   (ii) After he took an image of the disk, his superiors returned the computer to his owner. Peter forgot what partitions were on the disk. How can he obtain this information again?

   (iii) It turns out there was only one partition on the disk, formatted with the NTFS file system. What sequence of commands could he use to get a list of files in its root directory? Let's say Miran had the following file on his computer `C:\HIDDEN\MYSHEEPE.JPG`. How would Peter copy it to his home directory?