Digital forensics 2013/14
Written exam May 12, 2014

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 75 minutes to take the test.

May your knowledge bring you success!

TASK	POINTS	OUT OF	TASK	POINTS	OUT OF
1			3		
2			4		

IME IN PRIIMEK: ______________________________

ŠTUDENTSKA ŠTEVILKA: ______________________________

DATUM: ______________________________

PODPIS: ______________________________

1. naloga: Basics and digital forensic terminology.

VPRAŠANJA:

1. Based on the rest of the evidence, Peter suspects that Cefizelj has transfered 100 EUR to an account owned by John in exchange for illicit drugs. During the forensic investigation, he has found the following evidence: (i) an entry on the mail server hosting Cefizelj's mailbox showing that Cefizelj received an e-mail with the ID 1JDSV144MNN12N1KK1 from John; (ii) an entry on the mail server hosting John's mailbox showing that John sent an e-mail to Cefizelj with the ID 1JDSV144MNN12N1KK1; (iii) A file on John's computer containing instructions for Cefizelj, saying he should transfer 100 EUR to John for illicit drugs; and (iv) on Cefizelj's computer two blocks which did not belong to any file but contained data showing that Cefizelj had performed a transaction involving 100 EUR (in the first block) and that a transaction to John's accound was performed (in the second block). Peter's report contains all the above mentioned facts and the conclusion based on these facts. Write down the conclusion!

2. Peter has managed to mount the image of a CD on `/mnt/slika` and would like to find all the photos on it. (i) Which sequence of commands should he use to find all the files with the ending `.jpg`?

   Cefizelj is smart and has removed the ending from some of the files. Peter would still like to find all the images, even those not in the *jpeg* format. (ii) How should he find the files?

   HINT: He may (but does not have to) use the file command. The mimetype of JPEG files is `image/jpeg`.

   Among the pictures, Peter has found a picture of Cefizelj standing in front of a house, holding a pitchfork. The pitchfork had been stolen from Lavdon Štimani a year earlier! Peter would like to track Cefizelj down. (iii) How can he do this if the picture was taken with a mobile phone with geolocation turned on. Can he trust the data acquired in this way? (Justify your answer.) (EXTRA) How is the itegrity of EXIF tags in a file *usually* ensured?

3. What is the relation between the scientific truth and legal judgement? Justify your answer.

2. naloga: Computer startup and disk systems.

VPRAŠANJA:

1. Peter Zmeda has received a disk image to investigate. The person in charge of the investigation suspects that the image contains a record of a bank transfer of 1,000,000 EUR from the *National bank of Butale* (*NBB*) to *The First Bank of the Great Isles* (*FBGI*). The investigator does not know the format of the record (jpg, pdf, doc, ods, ...), nor does he know whether it is in a separate file. During the evaluation of the suspect's profile, the investigators found that the record is not encrypted, nor has it been hidden anywhere outside the filesystem. Suggest three places Peter should look for the record and how he should do it.

2. Peter Zmeda has bought a new, larger disk – he has upgraded the computer from 1T to 2T. He installed the disk in the computer which detected it as /dev/sdb. He then (successfully) performed the following command:

   ```
   cat /dev/sda1 > /dev/sdb1 .
   ```

   He then disconnected the computer, removed the old disk and turned the computer back on. But the computer simply would not boot. (i) Why? What should Peter do to make the computer boot from the new disk?

   After getting the system into a state where he could finally log in, Peter was unpleasantly suprised. The command `df` showed that the ammount of space available on the disk had not change – as if he still only had a 1T disk. (ii) How could this happen and how could Peter correct this problem?

   The upgrade took Peter a whole afternoon. Just copying the data took over an hour. (iii) is there any way to perform the copy faster? Take into account that only 20% of the disk was in use.

3. We have a FAT filesystem. (i) How many entries can the FAT contain, (ii) How large can individual files be and (iii) what is the largest disk size that can be used in full?

3. naloga: Networks and forensics

VPRAŠANJA:

1. Cefizelj has decided to attack the website of *NBB* bank which can be accessed using `http`. Not to leave any traces, Cefizelj has decided to change the source address on all outgoing packets to 23.208.163.36. His impersonation attack will not succeed. Why?

2. Peter has gained access to Cefizelj's phone, *Butaphone 3000+* – an Android phone with an i7 processor. Peter knows that Cefizelj has already unlocked – „rooted" the phone. Which tool can Peter use to access the data on the phone?

   Peter has also noticed that Cefizelj has two shortcuts on his home screen, refereing to two different browsers. The first referrs to the built-in web browser while the second points to a browser written by Cefizelj himself, called *IE4Android*. After investigating the files on the phone, it turned out that Cefizelj used a strange, undocumented format to store the browsing history. Peter would only like to find out which websites Cefizelj had visited. (ii) Which tool could he use to inspect the history of the built-in browser (which format is it stored in)? (iii) Which tool can Peter use to try to inspect the history of IE4Android?

3. What does the IMEI number uniquely identify?

4. naloga: Performing a digital investigation.

VPRAŠANJA:

1. During the lectures we mentioned that the digital investigation consists of five steps, two of which are *examinatin* and *analysis*. (i) Where is each of these steps performed? (ii) What is the basic difference in their purpose?

2. General Rupert Gorjača, a fresh resident of Butale, has been accused of having an affair with Klara Buta, the wife of famous Kozmijan Buta. Peter has been assigned the unenviable task of looking for possible evidence which could be used to confirm or deny the affair.

   Because Rupert's computer also contains secret documents, Peter has to be especially careful during the investigation of Rupert's computer. Help him by preparing a plan of the investigation. Form at least three hypotheses and plans to verify them.

3. Which is the highest legal act, that regulates right to privacy in Slovenian legislation?