Digital Forensics 2020/21
Written Exam Thrimilce 6th, 2021

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.

No other communication is allowed but chatting over BBB with the instructor. If we suspect cheatting, the exam will be annuled and you will *have to* take an oral exam over the BBB.

You have 75 minutes to take the test.

May your knowledge bring you success!

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

1. task:

QUESTIONS: Basics.

A) Digital evidence can be altered or destroyed either accidentally during collection or maliciously by offenders, without leaving any obvious sign of distortion. Which features of digital evidence mitigate this problem? Choose the right answer and justify it.

   (a) Digital evidence can be duplicated exactly and a copy can be examined as if it were the original.
   (b) When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of.
   (c) With the right tools, it is very easy to determine if digital evidence has been modified or tampered with by comparing it with the original copy.
   (d) Digital evidence is difficult to destroy with simple deletion or formatting and can be recovered.
   (e) All of the listed.

B) Butale police came to Peter Zmeda, who has his own mail server. The police received a report that Peter was sending harassing mail via his server. Peter claims that he has nothing to do with it, but that Cefizelj, a well-known troublemaker who exploited his mail server, is behind it all. (i.) Write down two hypotheses on how to substantiate Peter's claim and how to prove them. (ii.) Let us say that Cefizelj is in fact behind the described case. What role then did Peter's server play in this case: the object, the subject, or the instrument. Justify the answer.

C) Peter Zmeda was given the task of analyzing multiple servers with Arch Linux operating system. First of all, he needs to review system logs. (i.) In which directory are the system logs usually located? (ii.) Peter noticed that some servers were missing the expected log files, as such log files are no longer fashionable. If not syslog, which program takes care of logs on modern systems? How would Peter review logs on a system like this? (iii.) Can the server where rsyslogd takes care of logging send events to the server where syslog-ng takes care of them? What problems can we expect in such a case? Justify the answer.

2. task: File systems.

QUESTIONS:

A) Peter became a real artist. Now he would like to make the first Slovenian film in high definition, where an uncut shot of a suffering mother will last more than for three years. The film will be captured with a camera that will send data over the network directly to a computer with multiple disks. (i.) What technologies can he use if he has several identical disks in his computer, and no single disk will be big enough to fit the entire recording? List at least 4. (ii.) Which of these technologies can he use if the disks are going to be of different sizes? (iii.) If he will back up the film, how can he verify that it is identical to the original?

B) Let's say that we move a file within the same volume in Windows OS. How does this affect the information about file's last access? Justify the answer.

C) The time recorded by individual files represents metadata. Timestamps are found in various places. First, of course, among the metadata stored in the file system, and sometimes the timestamp is also included among the data in the file itself.

This time we are dealing with the file `na-plesu.jpg`, which is stored in the `ext3` file system. The file contains a photo of Luka Kratkohlačnica dancing a Viennese waltz with an unknown girl. Luka claims the picture was taken on Saturday night and proves he has nothing to do with the outrageous theft of salt from the Butale city's warehouses, which also happened on Saturday night around 9pm. Luka also claims that he saved the picture on the computer before a Saturday midnight.

When forensic scientist Bučka reviewed the file metadata, he found that the image file was actually created on Saturday morning at 9am. (i.) Where exactly is the file creation metadata stored? (ii.) Assess how *credible* is the information Bučka found. Justify your assessment. (iii.) Is it then possible that the picture was taken at a Saturday night dance? Write down an appropriate hypothesis to substantiate the possibility and describe how to prove it.

3. task: Mobile and network forensics.

QUESTIONS:

A) Peter Zmeda got a picture showing his chosen one Rosamund kissing an unknown flower. In a fit of jealousy, he uploaded the picture to an online service that told him the painting was created in 1920 in the city of Temir-Han-Shura, the Republic of the League of Nations of the North Caucasus. (i.) On the basis of what data could the service determine the date when the image was taken? Is this information believable? (ii.) What tool could you use to read all this kind of data? (iii.) In addition to the date and location, list at least two other pieces of information that can be found in the image.

B) A smartphone actually consists of two computers. (i.) List the five (types of) data found on the SIM card. (ii.) If we want to check the authenticity of the data, we can find them elsewhere and then compare them. For each of the above five (types of) data, write down at least one more place where you could find it.

C) Peter has been tasked with maintaining an old server which used to be managed by Jože T. In `/home/joze/.bash_history`, Peter found the following line: `telnet localhost splet` When he tried to run the above command, he was surprised to get the following response.

```
peter@slovnica:~/$ telnet localhost splet
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET / Od nekdaj lepe so strani nam slovele a lepše od tele
bilo ni nobene.
Connection closed by foreign host.
```

Which file on the system is most likely to have been changed if we know that Jože T. is an exemplary administrator who just loves the Slovenian language? Justify the answer.

4. task: Investigation.

Questions:

A) Peter Zmeda was given the task of inspecting the disk of a computer running GNU/Linux. On his work computer, the system detected the disk as `/dev/sdb`. He created a directory `search` in which he will analyze the files. To get to really all the files and timestamps, he executed the following sequence of commands:

```
dd if=/dev/sdb of=slikadiska.raw
mount -o ro,nojoliet -t ext4 /dev/sdb1 /mnt
cp -r /mnt/* /home/peter/preiskava
```

For each of the commands, write what he did wrong. You can also list multiple errors.

Hint: The `-r` flag means recursive copying.

B) Evidence analysis is one of the phases of the forensic process. (i.) What phases are ahead of it and what is each of them intended for? (ii.) Why is the analysis so late in the process and not, say, immediately at the crime scene? Justify the answer. (iii.) Normal analysis is performed by forensics on behalf of law enforcement. Can anyone else do it? When does this usually happen in criminal proceedings and why?

C) What is the difference between digital forensic examination and analysis?