Digital Forensics 2023/2
Written Exam Ærra Līþa 11th, 2024

The exam must be taken individually. Literature in a paper form or on disconnected computer. If you successfully solve all tasks at least partially, you might get extra points. Although individual questions may be more tied to a specific topic, it is necessary to use knowledge from other topics. Some questions require assumptions for an accurate answer. Be precise with them because accuracy earns more points. Principle answers do not bring all the points.

The time for writing the exam is 60 minutes.

May your knowledge bring you success!

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

NAME AND SURNAME: _____

STUDENT ID: _____

DATE: _____

SIGNATURE: _____

Task 1. *Basics.*
QUESTIONS:

1. To which of the four categories (according to Parker) does a computer, which was used to forge documents and then destroyed, belong? Justify your answer and illustrate it with an example.

(a) It is the subject, the object and the tool (instrument) of a crime.
(b) It is the object and the tool (instrument) of a crime.
(c) It is the subject and the tool (instrument) of a crime.
(d) It is the object and the subject of a crime.

2. Peter Zmeda received from his superior an image of the computer's system disk, which was home to several users. The police suspect that one of the users was collecting child pornography using a browser. (i) Write a hypothesis where to look for trace files and why? More complete answers will be graded better. (ii) In the lectures, we learned that proofs have common properties and special properties. Define the two types of properties in the example from point (i). Alos give concrete examples.

3. Peter would like to review the events and registry on a computer with *Microsoft Windows 8* and multiple users. He would not like to download and save all the files, but only the necessary ones. (i) Where is the registry located? Where are the event logs located? (iii) Peter heard that on *Windows* the event descriptions are stored in the .DLL files of the programs that generate the events. Which of these files will he actually need? You can also describe how it will arrive at the list.

Task 2. *File systems.*
QUESTIONS:

1. The central structure for handling files in the UNIX operating system is the `inode`. (i) What metadata does the `inode` store, or what does this metadata tell us? (ii) Cefizelj hacked into Peter's computer and was particularly interested in the texts of the exam from the previous term and from the first term in the subject *Digital Forensics*. He indeed found the directory `PI` and in it both texts:

```
[peter PI]> ls -lai
total 352
115817034 drwxr-xr-x  4 peter  .
 23110634 drwxr-xr-x  8 peter  ..
115817723 -rw-r--r--@ 2 peter  2324DF-PI00.pdf
115817723 -rw-r--r--@ 2 peter  2324DF-PI01.pdf
[peter PI]>
[peter@Peter-Macbook PI01]>
```

Based on the printout, what can we conclude about the two texts and why?

2. Where is the GPT partition table usually located? Why right there and why not in other places?

(a) At the beginning of the disk.
(b) After MBR and at the end of the disk.
(c) At the beginning and end of the disk.
(d) At the end of the disk.
(e) In MBR.

3. Peter received 8 10TB drives for review. There should be a single file system on all disks. (i) Other than using RAID, how else could you get a single filesystem on them? (ii) If they are in a RAID5 pool, what is the maximum capacity of the file system? What if they are in a RAID10 pool? Are the drives using GPT, MBR, or none of the above? Justify your answer.

Task 3. *Mobile and network forenzics.*
QUESTIONS:

1. Using a high-end smartphone with typical settings, we take a photo in the middle of the city. We cannot tell the location of the photo by looking at it. Is there another (easy) way to find the location? Can we do this (easily) in any other way? For each option, justify why not, or, if yes, how and why yes.

1. No.
2. Yes, by looking for witnesses.
3. Yes, with the help of the network operator.
4. Yes, such a phone has a GPS that stores the current location in a photo file.

2. Computer communication is modularized so that it is divided into layers (ISO/OSI: link - 2, network - 3, transport - 4, ... layer). One of the key requirements of communication is the protection of transmitted data - it can be obfuscation (encryption) or integrity (integrity) - or both. (i) Why is whether the communication ensured the integrity of the data transfer an important question in a forensic investigation? (ii) Suppose we provide data protection at layer p in the communication design. What does this mean in terms of data protection at higher layers? When answering consider the different valueS of p and what this means in terms of a possible attack on the communication.

3. Peter Zmeda investigates data from a mobile phone. It's an *Android* phone, and Peter got an image of the entire partition attached to `/data`. (i) What information did he not get from this? (ii) How could I get the contact list? (iii) How would the SQLITE3 tool help him to examine the photographs? Justify your answer.

Task 4. *Investigation.*
QUESTIONS:

1. Which of the listed phases do not belong to the (sub)phase model? What are the phases that belong to the (sub)phase model intended for and why do the rest not?

(a) Reconstruction.
(b) All.
(c) Material analysis.
(d) Preparation.

2. One of the basic principles of the criminal procedure is the principle of *official prosecution* - which states that the state prosecutor must prosecute criminal acts according to their official duty. (i) Why do you think the principle found itself among the fundamental principles? What would it mean if it wasn't in the core set of principles? (ii) The Butala policeman found Cefizlj's hiding place, in which he suspects that Cefizlj is hiding stolen salt. In order to search the hideout, he knows he needs to get the proper warrant. Given that the state prosecutor has to prosecute crimes according to the principle of *official prosecution*, he believes that he is also the right person to issue the necessary warrant. Justify why Peter's reasoning is correct, or, if not, why the reasoning is wrong. Best with an example.

3. Each time he got a different hash value. Then he tried the following commands:

```
1 mount -o ro prvidisk.raw /mnt
2 mount -o ro drugidisk.raw /mnt
```

The computer told him that there was no known file system in the image. (i) Why might he get different hash values? (ii) Was his procedure correct? If so, why? If not, what data did he lose? (iii) How can he check which partitions are (were) on the disks without accessing the disks themselves?