Digital Forensics 2019/20
Written Exam Thrimilce 5th, 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.

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. naloga:

QUESTIONS: Basics.

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

B) In digital forensics, we say that a device or data can have the role of an object, a subject or an instrument. (i.) For each role describe two specific examples. (ii.) For each of the six examples, describe how would you secure the digital evidence. (iii.) What do we want to achieve by securing the digital evidence? Justify the answer.

C) Peter Zmeda was tasked with inspecting multiple servers with operating system Windows Server 2012. He should focus on examining system logs. (i.) In which directory are system logs usually located? (ii.) Peter has heard about the `grokevt` program. Will it be useful? If so, for what? If not, why not?

2. naloga: File systems.

QUESTIONS:

A) Peter runs two operating systems on his computer – Linux and Microsoft Windows. Since he does not trust the hardware, he will install two disks, so that if one fails, the data does not disappear. (i.) Which technology should he use for this purpose? If there are multiple levels in it, which one exactly? (ii.) How can he setup the system, that he can access the data from both operating systems? (iii.) If the access to Windows data is not important to him, which alternative technology can he use?

B) For the disk we have we use CHS addressing with the following parameters:

- Cylinders: 1024,
- Heads: 256,
- Sectors: 63, and
- Sector size: 512B

(i.) How many sectors are on a disk? (ii.) How big is the disk in bytes? Show the calculation in both cases.

C) When formatting a new disk for the file system `ext2`, the operating system asked us how many *inode*-s do we want to create. (i.) What exactly is determined by the number of *inode*-s? (ii.) Do we also have any similar restriction when formatting a disk for the NTFS file system? Justify your answer. (iii.) Suppose we have a disk from the question B. How many *inode*-s would you create on it? Justify your answer.

HINT: For a more specific answer, you will probably think about what you plan to use the disk for.

3. naloga: Mobile and network forensics.

QUESTIONS:

A) A stream flows from Tepanje to Butale, but it is called a river. This river was smeared with oil on a beautiful day. There are photos of the oil stain on the stream created with a modern mobile phone. The people of Butale claim that the photos were taken in Butale exactly on a day after the canola oil was made in Tepanje. (i.) Where can we find the timestamps in the pictures? (ii.) How is determined the recorded time? (iii.) What is the name of the standard for storing such metadata?

B) When investigating a crime, one of the key factors is communication between individuals. If, for example, we suspect that person A is involved in a crime and there is evidence that there was a possibility of communication between persons A and B, then B should also be examined. (i.) Which principle dictates that the examination should be performed? Justify your answer. (ii.) Write down three technically significantly different ways of examining possibility of communication between mobile units. For each of them write down how would you check it.

   HINT: This answer requires some ingenuity.

C) What VPN enables to the attacker? Justify your answer.

   - Launching their attack from their computer with a forged IP address to hide their true IP address and geographic location.
   - Launching their attack from their computer with a forged MAC address to hide their true MAC address and geographic location.
   - Launching their attack from a compromised computer from a distant location to hide their MAC address and geographic location.
   - Launching their attack from a compromised computer from a distant location to hide their IP address and geographic location.

4. naloga: Investigation.

QUESTIONS:

A) Peter Zmeda was commissioned to inspect the disk of a computer running the NTFS file system. On his work computer, the system detected the disk as `/dev/sdb`. He created a directory `investigation` in which he will examine the files. To get to all the files and timestamps from the disk, he ran the following sequence of commands:

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

For each of the commands describe what he did wrong. You can also list several errors.

HINT: The `-r` flag means recursive copy.

B) In the latest case, where police investigated drug smuggling, the head of the investigation suspected that the seized disk also contains a list of drug traffickers. Peter Zmeda was assigned to search for documents on disk. (i.) Help Peter and make five substantially different hypotheses as to where to search for the list. (ii.) For each hypothesis, propose a procedure for its testing. Justify each your procedure proposal. (iii.) Let us assume that Peter did not find anything. What should his report to the investigator contain? Justify the answer.

C) While inspecting a disk, looking for evidence pertaining to a drug-smuggling case, Peter inadvertently stumble across some top-secret plans of a military targeting and communications system. What should he do? Justify why the answers that were not selected, are wrong.

- Investigate the files since the evidence will be of great use to the court.
- Nothing, since the files found are none of your concern.
- Report his find and wait for a court order for further investigation.
- Delete all the files because he is breaking the law simply by possessing the top-secret plans.