Digital Forensics 2022/23
Written Exam Ærralitha 2nd, 2023

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 90 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.*
TASK:

1. Assign to each of the functions *SHA-256*, *MD5*, *SHA-1*, *Parity*, and *CRC* one of the properties below that best describes the function in relation to providing data integrity in forensic investigation. Justify your choice.

1. Safe and in use for a long time.
2. Not safe but is still used
3. Recently broken but still used.
4. Safe.
5. Broken and should never be used.
6. Not useful.
7. Uporabna za odpravljanje naključnih napak.

2. In the Butale court, Cefizlj has a bad time, because the prosecutor Luka Kratkohlačnica presented a picture from which it is clear that he was in fact the one stealing salt from the people of Butale. Cefizl's defense attorney disputed the authenticity of the evidence. (i.) What is meant by authenticity of evidence? How does the prosecution prove the authenticity of the evidence? (ii.) Write down three significantly different hypotheses that the material presented is not authentic and describe the procedures for proving the hypotheses.

3. Peter Zmeda likes Windows very much. Unfortunately, his predecessor preferred to use FreeBSD and set up the entire information system on the basis of this OS. Peter now has a server *syslog* that is well secured and powerful enough, only Windows computer data does not arrive to it. (i.) Do the log entries under Windows contain all the data needed to create *syslog* entries? If not, which one are missing? If so, what will the map be like? (ii.) What tool do we usually use to view log records under Windows? (iii.) Peter visited FRI years ago and has learned that he can review log entries using the *grokevt*. Does this also apply to Windows 10 and later? If yes, what OS files will you need and why? If not, which tool can he use?

Task 2. *File systems.*
TASK:

1. Peter Zmeda was given a disk on the table and asked by the prosecutor's office whether it contained a file named `butalska-sol.txt`. (i.) Write down five significantly different places where the file can be located in its entirety. (ii.) Write down three other fundamentally different ways in which the contents of a file could be hidden (possibly in separate parts) in other files.

2. Write down an example of a concrete boot sequence and comment it. What exactly is a boot sequence?

1. A sequence (stored in MBR) of devices, where computer looks for a bootable operating system.
2. A sequence of programs that are executed when a computer is turned on.
3. Hard drive initialization order when a computer is turned on.
4. A sequence (stored in CMOS chip) of devices, where computer looks for a bootable operating system.

3. Peter Zmeda got a computer for review, on which the administrator used the ZFS file system. When he opened the computer opened, it contained two 2TB and 3TB hard disks and two SSD 512GB disks. (i.) What is the minimum number of file systems on these disks? What is the maximum number? Please justify the answer. (ii.) At least one file system is located on multiple disks at the same time. Peter has heard that in this case we use *mdadm* tools or tools to work with *LVM*. Depending on the size of the disks and the file system, which tool will he most likely use? Why? (iii.) Specify at least one advantage of *ZFS* over *ext4* and one advantage of *ext4* over *ZFS*.

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

1. Viruses can spread in different ways. Which of the ones below is not possible and why not?

1. Computer network.
2. USB stick.
3. Main memory (RAM).
4. A text we received in postscript format.

2. Cefizelj claims that he was in Tepanje at the time of the salt theft and, according to the video conference application, with which he participated in the consultation. To confirm his claim, he attached a statement from the participants that he had indeed participated in the consultation and a printout from the `www.iplocation.net` service, which confirmed that his computer with the IP address `7.7.7.7` is really in Tepanje. (i.) From the point of view of network forensics, write down two hypotheses how it would be possible for the IP address of his computer to be visible in Tepanje, but he would be in Butale at the same time. (ii.) Explain how you would test the hypothesis.

3. Peter Zmeda is convinced his phone was stolen. Luckily, before losing his phone, he put his SIM card out. In the park, where he often sits, he found one of same phones on the bench. (i.) He put his SIM card in the phone, opened the phone app, and immediately saw all his 20 contacts. Is the phone his? Justify the answer. (ii.) Before the loss he had Facebook opened on his phone, but the phone was locked. Could anyone hack his Facebook account? If not, why not? If yes, how (describe the procedure)? (iii.) He heard that the data on the phone was stored in the SQLite database. He looked at all the icons on all the screens, but he couldn't find an app with that name. Where is this database supposed to be on the phone?

Task 4. *Investigation.*
TASK:

1. From definitions below choose the best description of a term an attack vector, and write down a concrete example of the attack vector and how does it work.

1. A model or activity that obfuscates the real attack.
2. Detailed description of an exploitable vulnerability in the system.
3. An action plan with priorities, what will an attacker do, which vulnerabilities will the attack first and what are they hoping to achieve.
4. The means by which an attacker gains access to infrastructure.
5. A vector in threat versus risk chart.

2. At the same time, criminal proceedings fulfill the conflicting functions of the *law-enforcement* and *safeguards*. (i.) Why and how are the two functions contradictory? (ii.) With which instrument the process operators, when a opposition it the proceedings occurs, enable the law-enforcement function to carry out its activities? (iii.) We know the different models of criminal proceedings, and two of them are *accusatorial* and *inquisitorial*. What is the difference? (iv.) How does the role of digital forensics differ in each of the models? Justify the answer.

3. Peter Zmeda got a server with an SSD hard drive for review. He created a disk image:

```
1 cat /dev/sdb > preiskanidisk.raw
2 sha512sum /dev/sdb
3 sha512sum preiskanidisk.raw
```

(i.) A friend told him that he should use the *dd* command, which is specifically used to copy disks, not *cat*. Is his friend right? Justify the answer. (ii.) The check sums are the same. Peter is convinced he did everything right. Is that true? Justify the answer. (iii.) Peter would like to mount and inspect the file systems on the disk. Specify the commands to do so.
