Digital Forensics 2022/23
Written Exam Thrimilce 4th, 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.*
QUESTIONS:

1. When evaluating the credibility of digital evidence, the investigator is interested in whether the computer on which the evidence was created was operating normally and one of the following options. Which and why the others the answers are not correct?

1. Is there any suspicion that someone may have tampered with the evidence?
2. Whether the evidence was properly secured during transit?
3. Are the media on which the evidence was stored compatible with forensic equipment?
4. Whether the analysis of the material was done as requested by the prosecutor?

2. One of the basic conditions for the admissibility of evidentiary material is that it does not lead to unnecessary conclusions. (i.) Describe an example of such material and justify how it misleads. (ii.) What are the remaining four conditions of material admissibility?

3. Peter Zmeda follows the latest trends, so he will use *systemd-journald* to log events on his system. He heard that the journal entries are now somewhere in the directory */var/log/journal*. There he found a bunch of files with the extension *.journal*. He intends to review them with *less*. (i) Will it be successful? If so, how could I find occurrences of the word ”trend”within the file? If not, why? (ii) Peter would still like to continue using *syslog-ng* for data collection. Can he use both *systemd-journald* and *syslog-ng* on the same machine? (iii) How does the *syslog* protocol described in RFC5424 ensure that events are not lost?

Task 2. *File systems.*
QUESTIONS:

1. During the house search of the Butale notorious Cefizel, the police seized quite a few data drives, that were formatted differently. The SSD was formatted as NTFS, the USB stick as FAT and the hard drive as ext-3. A file with a picture of Šprinca Maroglja was found on all three drives. Now they are wondering which of the three versions is the original and which are copies. (i.) State your hypothesis about this and describe the procedure for testing whether your hypothesis is correct. (ii.) Metadata will play a key role. Which data appear on each file system and how are they related to the metadata on the other file systems?

2. MS Windows includes VSS - *Volume Shadow Copy*. What service does it enable and how?

1. Making backup copies of NTFS file systems.
2. Making backup copies of individual files.
3. Making backup copies of disk partitions.
4. Hiding passwords (shadow).

3. Peter Zmeda received the disks of two computers for inspection. The first was in the workstation where Cefizelj worked. He learned from his colleagues that Cefizelj used the NFS file system for his home directory. The second was on a computer that supposedly ran the company's file server. (i) How (with which commands) could Peter get the files that Cefizelj was saving from the workstation disk? (ii) How would you find out what file system they were using on the server? (iii) How (with which commands) could Peter check whether Cefizelj really used NFS, or maybe his colleagues were wrong?

Task 3. *Mobile and network forenzics.*

QUESTIONS:

1. With which command do we find out which domain is bound to IP 212.235.188.20 and what do the other three commands tell us?

1. `whois 212.235.188.20`
2. `dig -t ptr 20.188.235.212.in-addr.arpa`
3. `ip domain get 212.235.188.20`
4. `dig -t ptr 212.235.188.20.in-addr.arpa`

2. The `sockstat` tool with `-l` switch returns all sockets that the client can connect to. Peter checked the command on the Butale server and got the following response used in the rest of the task.

```
@butale:> sockstat -l
bind named 904 514 udp4  192.168.126.1:53      *:*
bind named 904 515 udp4  192.168.125.1:53      *:*
```

(i.) What is the id of the process that is waiting on the client and why? (ii.) Is the response a combination of responses from two machines or is it possible that it is coming from one machine? Justify your answer? (iii.) What do the first two columns of the response contain?

3. Peter Zmeda investigates data from a mobile phone. He got an error while reviewing the file `contacts2.db` (copied from the phone) using `sqlitebrowser`. (i) With which command / how could he find out if it is really a `sqlite` file? (ii) Peter suspects something is wrong with the permissions. He checked that he has the permission to read the file. What other permissions does he need to use the `sqlite3` tool to inspect the file? (iii) Peter had heard that Android phones are ordinary computers running Linux. He was supposed to get all the data from the phone for review, but he couldn't find the home directory of its user anywhere. Where is user data usually stored on Android phones? How are they organized by directories?

Task 4. *Investigation.*

QUESTIONS:

1. The preparation of the activity plan and the acquisition of the necessary resources and materials belong to which step of the digital investigation? Describe a concrete example of preparation and acquisition.

1 Investigation and analysis.
2 Preservation.
3 Survey/identification.
4 Preparation.

2. One of the fundamental concepts is the Concept of (reasonable) expectation of privacy. Luka Kratkohlačnica has his email inbox at ButaleOL. (i.) How does the described concept concern Jurež Pismouk, who is the system administrator of the mail server at ButaleOL? Justify your answer. (ii.) Peter Zmeda was granted a court order to inspect the mail received by Gregor Copataka, who also has his mailbox at ButaleOL. How does the above concept relates to Peter? The answer is multifaceted, and please justify it.

3. Peter Zmeda received a server with two hard drives for review. He connected both disks to his computer running Ubuntu 20.04 Desktop. He created copies of disks:

```
dd if=/dev/sdc1 of=prvidisk.raw
sha512sum /dev/sdc
cat /dev/sdd1 > drugidisk.raw
sha512sum /dev/sdd
sha512sum prvidisk.raw
sha512sum drugidisk.raw
```

He got a different checksum each time and consequently tried commands:

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

The computer did not report errors. (i) Why did he get different checksums? (ii) Was his procedure correct? If so, why? If not, which data did he loose? (iii) Under `/mnt` he got only the content of the second disk. Did he manage to mount the first disk at all? What happened to the content of the first disc?