Digital Forensics 2017/18
Written Exam June, 12th , 2018

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.

You have 60 minutes to take the test.

May your knowledge bring you success!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga:

VPRAŠANJA: Basics.

A) In Slovenian justice system there are seven steps in criminal proceedings. List them and describe the role of each of them.

B) There are several challenges in handling digital evidence and two of them are: (a) remains or reconstruction is not the same as the whole material; and (b) data is not eternal. For each of the challenges (i) explain what it is including an example of it; and (ii) eaxplain how does a digital forensics tries to overcome it.

C) Peter is trying to create a forensic copy of his 2nd SATA disk. He has tried running the following command:

```
dd if=/dev/sda2 of=img.raw bs=4096 count=4096
```

(i) Which device did he actually copy (explain what it represents)? (ii) What should the device name actually be? (iii) Apart from the device name, what else did he get wrong and how should he correct the mistake?

2. naloga: Operating systems.

VPRAŠANJA:

A) Peter Zmeda is trying to add a new, 6TB disk to his computer which does not support EFI. He used his friend's computer to create a single huge partition and file system on the disk. Now, he has attached the disk to his computer. He has checked that the disk works without problems and that he can access the data on it. Since he is afraid the old disk might fail soon, he has decided to make the system boot from the new disk. He has copied GRUB from the old disk to the new one. After running the reboot command, the system has booted into GRUB and is complaining that it can not load the configuration file or Linux. Peter knows how to fix the problem but would like to hear your opinion.

(i) Where on the disk is GRUB usually located? (ii) What has Peter accidentaly overwritten? (iii) How can Peter to recover the overwritten data?

B) Microsoft Windows contains a service called *Volume Shadow Copy*. (i) What does it do? (ii) How this service can be used in digital forensics?

C) Logging is one of the key services in modern operating systems. How is it organized including where do the data reside (i) in Unix/Linux operating systems and (ii) in Microsoft Windows operating system.

Further, Peter is suspecting that sombody broke into his boss' computer running Microsoft Windows. (iii) Where should he look for traces of a break in? Justify your answer.

3. naloga: Mobile and network forensics.

VPRAŠANJA:

A) 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 /
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 Slovene language? Justify your answer.

B) Peter Zmeda is analyzing an Android mobile phone, trying to find the mobile browsing history and online passwords of Butale's most notorious criminal, Cefizelj. (i) On which path is usually mounted the partition containing the browsing history? (ii) Is it possible for Peter to find the online passwords? How are they hashed and/or encrypted? (iii) Which format is the Chrome browsing history stored in? Name at least one tool you could use to access it.

C) Let us consider a smart phone and regular cellular phone. (i) Give two hypotheses for digital investigation about the analysis of a device that would be the same considering either of devices. Justify your answer. (ii) Give also one hypothesis that is valid only for smart phones and not for the regular phones. Justify your answer.

4. naloga: Conducting an investigation.

VPRAŠANJA:

A) The policeman found pictures of a parchment containing the recipee for Butalian salt on Cefizelj's home computer. According to the law in Butale, possesion of the recipe is highly illegal.

   Because Cefizelj can not be found anywhere, Peter asked the fameous Butale flea Špinca Marogla, how the recipee might have ended up on Cefizelj's computer. The flea suggested three possibilities: (i) Cefizelj might have smuggled the recipee on a USB stick, (ii) he might have taken the picture on a mobile phone where a copy still remains, (iii) he might have an accomplice who has exfiltrated the secret out of Butale using the Internet. Which of the flea's suggestions are correct, which are not and (most importantly) why?

B) What is forensic examination and what does it include? Give the example to justify your answer.

C) The second principle of ACPO Guide says:

   > In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions;

   Discuss this principle. Give two examples against it and one in support of it. Justify your answers.