Digital forensic 2015/16
Written Exam, May 3rd , 2016

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.

1. According to the literature, what is the most common mistake made when processing evidence that leads to inadmissibility? Explain your answer.

2. We mentioned that a computer can have four roles in a criminal act. (i) list at least two of these roles. (ii) Give an example for each listed role (iii) Come up with a hypothesis how the crime might have hapended and how you could test it for each listed role.

3. Peter Zmeda received an USB flash drive for analysis. He plugged it into his computer, mounted it and found only an ISO9660 filesystem. Only after mounting it, he remembered that he was supposed to have created a disk image first and only analyzed that.

   Has he changed any data on the disk? Explain your answer. If he wanted to create the disk image, and then mount it, which commands could he have used? List the exact commands. Assume that the system detected the flash drive as `/dev/sdc`.

2. naloga: Disk systems. Peter Zmeda has found the following file on a floppy disk:

```
   Name    .Ext    ID     Size    Date      Time    Cluster  76  ARSHDV
 _REENF˜1   DOC   Erased  19968  5-08-03  2:34 pm    275         A-----
```

VPRAŠANJA:

1. How many clusters did the file occupy? Explain your answer.

2. Peter would like to save what is left of the file into a file on his disk. Peter is using Linux as his operating system and is using the ext3 filesystem which is set up so that it uses a journal. (i) How many inodes will he use? Explain your answer. (ii) Write and explain what sort of entries are stored in the journal? When describing a transaction, list which blocks are stored when.

3. This time Peter Zmeda has bought two 3TB disks. He would like to store at least 5TB of data on them. At least 500GB of data is so important that he really does not want to lose it - especially if one of the disks fails.

   (i) List at least two technologies he can use.

   (ii) For one technology, explain how he should configure partitions, file systems, e.t.c. so that his requirements are met.

3. naloga: Mobile forensics, network forensics and system logs. Yesterday, Cefizelj managed to connect to a wireless network using his computer. Because Peter is investigating a crime where the IP of the perpetrator is known, he has to find out which IP Cefizelj's computer was using. He can check the following places: (i) the log on the router; (ii) the DHCP lease table; (ii) the output of `ifconfig` on Cefizelj's computer; (iv) the `syslog` on Cefizelj's computer.

VPRAŠANJA:

1. Which of the listed places are probably not worth checking? Explain your answer.

2. For two of the places which make sense (i) write a hypothesis regarding *where* and *how* you could look for data regarding the IP address and (ii) why you think your hypothesis makes sense (why useful data could be there).

3. Cefizelj has also somehow managed to get to Peter Zmeda's computer. Peter was running Microsoft Windows XP. Cefizelj has managed to boot the system off a USB drive and would like to steal Peter's passwords. (i) Which directories should he copy? (ii) Which file? (iii) Can he easily read the passwords from the file?

   The directory containing passwords also contains most of the registry. (iv) Which part of the registry is not in this directory? (v) Where might the rest of the registry be located?

4. naloga:

VPRAŠANJA: Conducting the investigation and digital image forensics

1. One of the steps taken in a forensic investigation is securing the scene of the crime. (i) what is it's purpose? Which steps come before it?

   NAMIG: „*To secure the scene of the crime*“ is not a valid answer. Explain what securing the crime scene is.

   In Butale there has been a heinous crime. Evildoers have stolen the famous salt-making recipe from a Butalian server. The server was installed in a well guarded room and the only access to the server was over a computer network. Even then, the server was behind a firewall. Peter suspects that some residents of Tepanje did it, but he does not know how they might have stolen the recipe. (ii) Describe how Peter can secure the crime scene to keep as much evidence intact as possible. Explain your answer.

   NAMIG: The more detailed your answer, the more points you will get.

2. Our friend Peter Zmeda has come upon a picture during his investigation. The picture contains a suspect committing a crime. The picture is in JPEG format and if we are to believe the metadata, was created using a mobile phone. Which of the following properties of the picture can you use to determine whether the contents of the picture were modified: (i) EXIF tags; (ii) geometric distortion; (iii) DCT coefficients; (iv) indicators of double compression; (v) face recognition techniques; (vi) chromatic abberation; (vii) average image lighting; (viii) linearity of the image sensor response? Explain your answer.

3. Peter Zmeda is an artist who creates low resolution images (*pixel art*) in his free time. He posts them on a web portal in both BMP and PNG formats. Lately, he has been getting commercials on the portal which clearly show that the advertisers know that Peter lives in Butale.

   (i) How do you think the advertisers know where Peter is? Explain your answer. (ii) What can he do with the pictures to make the advertiser's jobs harder?