Digital Forensics 2017/18
Written Exam May, 7th, 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) According to Parker, which categories can a computer involved in a crime fall into? List an example for each category.

B) Evidence is central to forensics. A chain of custody is connected to its proper handling. (i) Where does a chain of custody start and where does it end? (ii) Describe an example for each link in che chain of custody. Explain what each of your examples proves. (iii) Why must the chain remain unbroken? Where and how could someone use a missing link in the chain?

C) Peter has received an old disk. Upon being powered on, the disk reported that it has 256 heads. When Peter opened the disk, he only saw one platter and one arm that moves across it. (i) How many read/write heads does the disk actually have? (ii) Why would the disk ”lie”about the actual head count? Explain your answers.

2. naloga: File systems.

VPRAŠANJA:

A) Peter Zmeda is examining a disk which contains an ext2 filesystem. As a good forensic examiner, he has recorded the safety checksum:

```
dd if=/dev/sdb1 | md5sum
```

He then mounted the disk:

```
mount -o ro /dev/sdb1
```

```
dd if=/dev/sdb1 | md5sum
```

The checksums differ! (i) Why? (ii) What does the `-o ro` switch do? (iii) What should he have done in order to not destroy the evidence? Write the sequence of commands.

B) With NTFS, what does the abbreviation VDL stand for? How can VDL be used to hide data?

C) Carving is one way to search for data in other data (e.g. a file). Suppose we have heard that the data we need to carve out is a program in `bash` or an image in the JPG format. (i) Write down the hypothesis you intend to test. (ii) How will you test your hypothesis? Explain your answer.

3. naloga: Mobile, network forensics and system logs.

VPRAŠANJA:

A) Peter has received Cefizelj's computer. He would now like to find out whether Cefizelj has been connecting to the Butale LAN. (i) Can he use tha ARP and routing tables to find out whether Cefizelj's computer has been connected to the network? If yes, how? If not, why not? (ii) Where else could Peter look for data showing whether this computer has ever been present on the network? Answer this as precisely as possible and explain why he should look in each of these particular locations. (iii) Without having access to servers on the network, how could you fool Peter into beleiving that Cefizelj's computer is on the network, even though it's the computer of someone else?

B) Using the `syslog` protocol, we have received a message with `PRI` set to `27`. Is it urgent? Explain your answer.

   NAMIG: Explain how `PRI` is calculated and what 27 means.

C) Peter is unable to get an IP address on one of his computers. The other computers work fine and the problem computer works fine on other networks. Peter suspects that the problem lies with the DHCP server. Which files on the server should he check? Name at least three and explain why.

4. naloga: Conducting an investigation and malware.

VPRAŠANJA:

A) An investigator has found child pornography on a suspect's computer. What may the investigator assume?

   (a) someone has downloaded the pictures off the Internet without authorization
   (b) someone in the suspect's family has downloaded the pictures from the Internet or off a USB stick onto the computer
   (c) someone in the suspect's family has the pictures on their phone
   (d) none of the above

   Explain your answer.

B) Butale also has a policeman. He had long suspected Cefizelj of stealing the Butale salt recipee and conducted an investigation during which he confiscated Cefizelj's laptop. Because he was in a hurry, he put the laptop into a metal suitcase and took it home. In the evening, when everyone was asleep, he took

the disk out of the computer and connected it to his computer. The computer (which runs Ubuntu) detected it as the 2nd SATA disk. The policeman examined the disk and after a while found a picture of a prototype of the first submarine in Butale. After some more searching, he also found plans of the submarine and a list of parts the sub is built from. He immediately calculated the checksum:

```
md5sum /dev/sdb1 > checksum.txt
```

and disconnected the disk which he put on a shelf next to the house entrance so he would not forget it in the morning. In the morning, he picked up the disk and took it to work where he placed it in a well secured safe.

What has the police man done wrong and how should he have performed each step in the investigation?

C) Peter has written the following program:

```
void foo() {
    long int* f;
    f = &f + 1;
    printf("\%lx\n", *f);
}
int main() {
    foo();
}
```

When he compiled and ran the program on his computer (64-bit Ubuntu on an Intel Core2), he got the following output:

```
7ffdf9c32c80
```

(i) What does the value represent? (ii) Why does it change every time the program is run? (iii) Draw a schematic of the memory space of a typical program on GNU/Linux. Mark approximately where the printed out value is. The schematic should include the location of code, data and the stack.