Digitalna forenzika 2013/14
Pisni izpit 1. mali srpan 2014

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 90 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: Here is a short excerpt from the documentation:

> INT 10h / AH = 0Eh - teletype output.
> Input:
> AL = character to write.
> BL = (graphics modes only) foreground color number
> Comment:
> This functions displays a character on the screen, advancing the cursor and scrolling the screen as necessary. the printing is always done to current active page.

1. Write a program in 80286 assembler which would, if it were located in the MBR, write out `NONA` to the screen. You can use the piece of code below as inspiration. You can assume that the graphic adapter is in text mode.

```
error:
        popw    %si
2:
        lodsb
        movb    $0x0e, %ah
        movb    (BIOS_page), %bh
        movb    $0x07, %bl
        int     $0x10           /* May destroy %bp */
        cmpb    $10, %al        /* Newline? */
        jne     2b
```

2. Whenever an evil doer uses a computer for their evil deeds, that can help you with the investigation. List three *fundamentally different* examples of how the use of a computer by an evil doer can help you with the investigation. Describe a realistic scenario for each example.

3. An eager young attorney wants to confirm an assumption in a case. He asks the digital investigator to steer the investigation in a certain direction. Is this allowed? Explain your answer.

2. naloga: Disk systems.

Vprašanja:

1. A peculiarity of the New Technology File System (NTFS) is that there is a difference between the *file size* and an *end of file*. (i.) What is the difference between the two (show an example)? (ii.) Why did the designer implement both concepts (describe a use case)? (iii.) How/why should a forensic investigator pay attention to both concepts?

2. Peter Zmeda wrote his first benign virus that would be hidden somewhere on a disk. His idea is to hide it in a file `virus` in a directory `imenik`, which is *read only*. List two reasons why this is a bad way to hide a virus.

3. Peter Zmeda received the only disk from the computer of a famous felon, Cefizelj. He attached it to a computer and immediately created a disk image, calcualted the md5 sum and checked that the data had not been corrupted:

   ```
   peter-01> dd if=/dev/sdb of=tat_racunovodja.img
   peter-02> md5sum tat_racunovodja.img
   484be6f1d548e6999551ab6e050a0405  tat_racunovodja.img
   peter-02> md5sum /dev/sdb
   484be6f1d548e6999551ab6e050a0405  /dev/sdb
   ```

   He sent the image and md5 sum to Rozamunda Žingelj from the analytics department. She created a virtual machine with an attached virtual disk of the same size as the original. She transfered the received data to the disk:

   ```
   rozi-01> cat tat_racunovodja.img > /dev/sdb
   rozi-02> rm tat_racunovodja.img
   rozi-03> md5sum /dev/sdb1
   7eb49377177c9038a703f382df624d79  /dev/sdb1
   ```

   Whoops! (i.) Where could the error have occured? (ii.) Which data is most likely to have been lost? (iii.) Can she get the data back?

3. naloga: Mobilne naprave.

VPRAŠANJA:

1. We learned about the IMSI. (i.) What is it? (ii.) Suppose that we created a tool which could track and log IMSIs in each cell. Would this be completely legitimate and legal? Explain your answer.

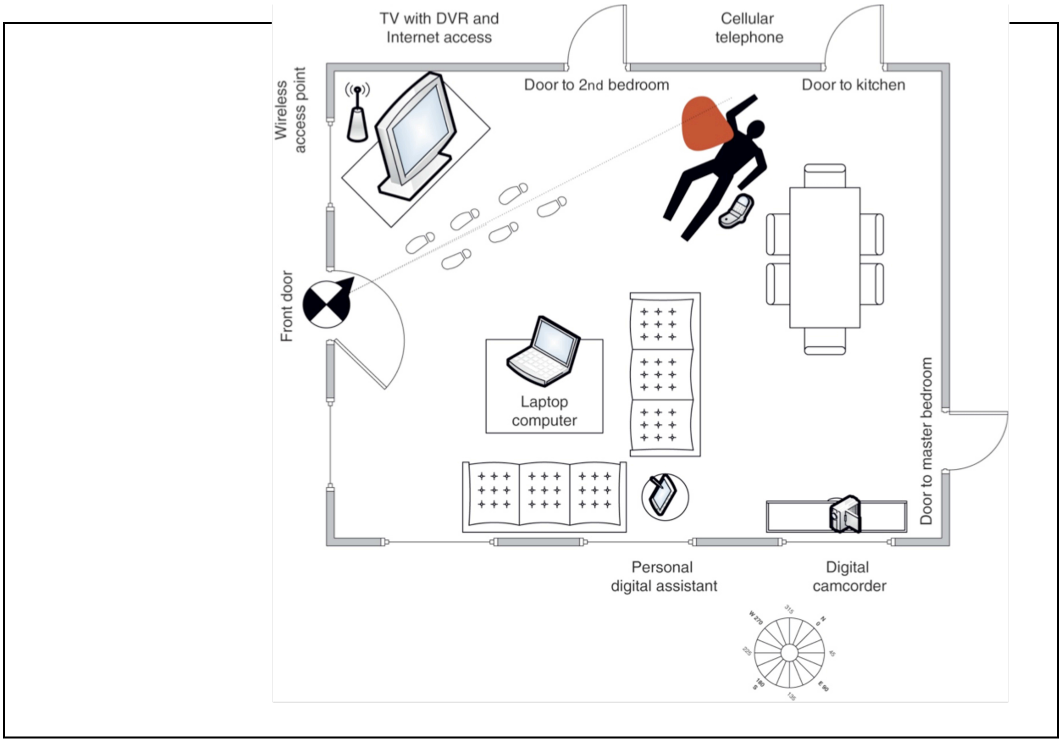
2. During the investigation of a mobile device the information can be found also elsewhere. List three additional sources and explain your answers.

3. On a crime scene Peter Zmeda found a phone Nokia N900. To access the personal contact data of its owner he copied all the user data from the phone, and moved into the directory where the contacts are kept:

   ```
   peter/najdena-nokia/user/.osso-abook/db> ls
   addressbook.db    index_first_last.db   index_last_first.db
   log.0000000001    fre1.changes.db       index_full_name.db
   index_nick.db     running_id.db         index_email.db
   index_im_jabber.db  index_phone.db      tp-cache
   ```

Which format do you think the data is in? How would he access it? Write the actual command sequence he would use. You do not have to use the exact same commands we used in class (but you may).

4. naloga: The investigator Peter Zmeda arrives at the crime scene depicted by sl. 1, We have seen this crime scene at the lectures.



Slika 1: Mesto zločina.

VPRAŠANJA:

1. Peter found images with child pornography on a laptop on sl. 1 (i.) Write down three hypotheses how the images got onto the computer; (ii.) justify your hypotheses; and (iii.) describe how would you check them.

2. Devices which trust other devices based on the IP alone are succeptible to an attack. Which attack is it? Explain your answer.

3. Peter Zmeda suspects that someone is snooping around his computer. To avoid public disgrace, he decided to remove everything that people could use to ridicule him from his browser's history. Most of all, he would like to remove all the URLS containing words `MLP`, `pony` or `donald`, but keep all the others. What is the easiest way to do that? You do not have to write the exact commands. Peter uses Firefox to browse the web.