Digitalna forenzika 2012/13
Pisni izpit 26. mali traven 2013

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke.

Čeprav so posamezna vprašanja morda malce bolj vezana na določeno poglavje predavanj, je za reševanje vprašanja pogosto potrebno uporabiti znanje še iz drugih poglavij.

Čas pisanja izpita je 60 minut.

Veliko uspeha!

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

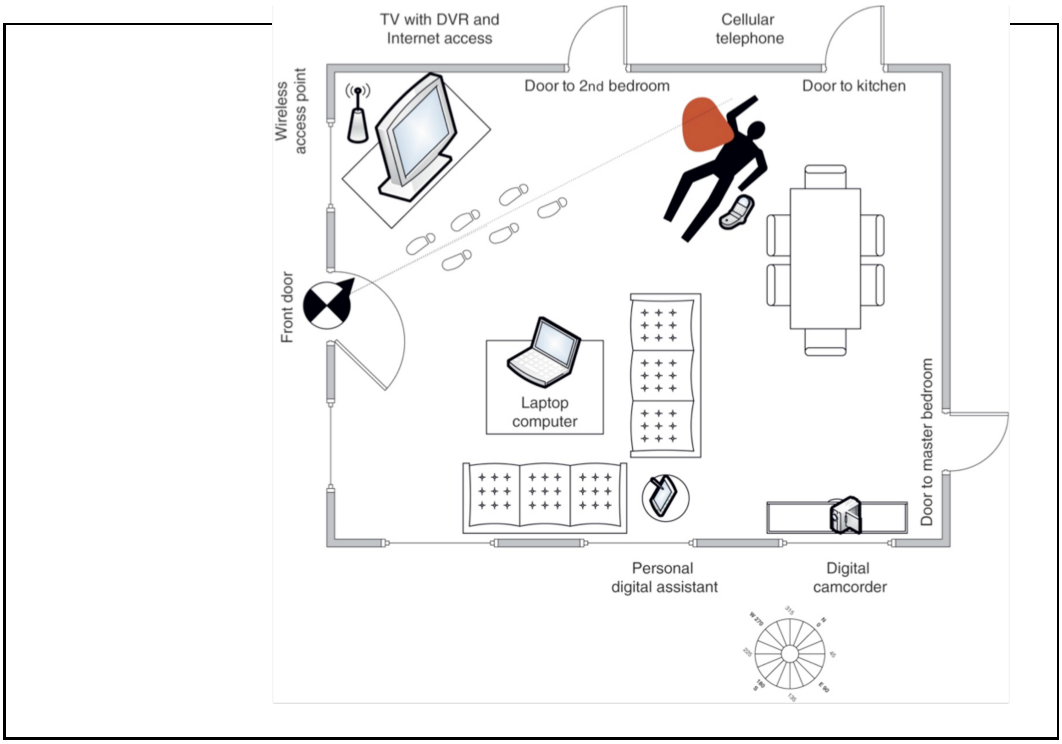
IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Peter Zmeda pride na mestom zločina na sl. 1, ki smo ga že srečali na



Slika 1: Mesto zločina.

predavanjih.

VPRAŠANJA:

1. Poleg računalnika, ki je na mizi, je še kar nekaj elektronskih enot na mestu zločina. Izberite tri izmed njih in za vsako izbrano napravo napišite vsaj tri mesta, kje bi iskali na njej podatke in kakšni so ti podatki.

   NAMIG: Za to vprašanje naj ne bi porabili več kot 10 minut in napisali več kot eno stran in pol. Pri tem *mislite širše*.

2. Peter Zmeda je dobil po pošti ISO datoteko, ki naj bi vsebovala sliko zgoščenke, katero so kriminalisti tudi našli na mestu zločina. Na njej naj bi bila med drugim gesla uporabnikov na nekem računalniku, na katerem tečejo Okna (Windows). Človek, ki je zgoščenko ustvaril, je nanjo skopiral celoten imenik, v katerem je datoteka z gesli. (i) Opišite postopek, kako naj pride do podatkov v ISO datoteki? (ii) Katere zanimive podatke (poleg gesel) lahko Peter še najde na sliki zgoščenke?

3. Ali niza bitov `0101 1111` in `1111 0101` na dveh različnih računalnikih lahko pomenita isto vrednost v dvojiškem komplementu? Utemeljite odgovor.

2. naloga: Delo z diskom.

VPRAŠANJA:

1. Omenjali smo pojma notranja in zunanja fragmentacija. Opišite oba pojma in razložite, pri katerih od datotečnih sistemov *ufs*, *ext3*, *fat* in *ntfs* nastopata in kje.

2. Peter je disk iz računalnika priklopil na svoj računalnik, ki mu ga je zaznal kot 2. disk na 1. SATA kanalu. Da bi si olajšal delo in ker se ni nikdar naučil, kako delati s slikami celotnih diskov, je najprej pognal ukaz:

   ```
   cat /dev/sdb1 > ~/racunovodja.img
   ```

   Nato se je zamislil in pognal še:

   ```
   dd if=/dev/sdb of=racunovodja.raw count=4096
   ```

   ter disk odklopil in ga predal policistom. Sedaj bi rad dokončal svoje delo. Pomagajte mu!

   i Kako naj ugotovi, kakšen je bil tip razdelka `/dev/sdb1`? Lahko to sploh stori?
   ii Katere podatke je Peter morda pozabil zajeti?
   iii Ali se lahko zanese, da so zajeti podatki dovolj?
   iv Disk bi rad pregledal neodvisni izvedenec. Peter mu je po pošti poslal `racunovodja.raw`. Kaj bi moral izvedenec storiti, da bi lahko prebral podatke na disku? Če je mogoče, napišite zaporedje ukazov.

3. Kakšen je pomen postopka *SHA-1* v digitlni forenziki? Kje naj bi se ga uporabilo pri prejšnjem vprašanju? Utemeljite odgovor.

3. naloga: Prenosne (mobilne) naprave.

VPRAŠANJA:

1. Kot vidimo na sliki sl. 1 se je na mestu zločina nahajal tudi celični telefon. Telefon je še vključen in tehniki so z njega že pobrali prstne odtise. Mladi forenzik, ki malce preveč gleda televizijo, je pričel pritiskati po telefonu, da bi videl, kdo je bil zadnji klican z njega. Našel je neko številko, ki jo tudi pokliče. (i) To, da je pričel tipkati po telefonu, je sicer napaka, vendar bi v določenem primeru le lahko tipkal. Kdaj? Utemeljite odgovor. (ii) Opišite ter utemeljite vsaj še dve napaki, ki jih je pri tem naredil.

   NAMIG: Uporabite ACPO.

2. Mobilne naprave so običajno najbolj trdovratne pri zajemu podatkov. Opišite tri tehnično različne načine zajema podatkov iz mobilne napreve in utemeljite, kdaj bi kakšneg od njih uporabili.

3. Iz česa se „podatkovno“ sestoji SIM kartica? Opišite vsaj tri podatke, ki jih najdemo na telefonu, in njihov pomen.

4. naloga:

VPRAŠANJA:

1. Kateri so osnovni koraki v digitalni preiskavi? Naštejte jih in jih opišite na pirmeru mesta zločina s slike sl. 1.

2. Cefizelj je ponovno v težavah. Točno do opoldne 29. marca bi moral oddati na davčno upravo v Butalah prijavo dohodnine. Trdi, da je to naredil, le davčna uprava se ne strinja s tem, saj so oni prejeli prijavo nekaj minut po poldnevu. Po drugi strani Cefizelj trdi, da jo je oddal pravočasno glede na uro na njegovem računalniku. Peter Zmeda je naredil digitalno forenzično preiskavo in našel naslednji zapis o poslani pošti:

```
Return-Path: <cefizelj@butale.si>
Received: from mail.butale.si (mail.butale.si [1.2.3.4])
    (using TLSv1 with cipher AES128-SHA (128/128 bits))
    (No client certificate requested)
    by svarun.du-butale.org (Postfix) with ESMTPS id
    DDD8B4AC64;
    Fri, 29 Mar 2013 12:03:32 +0100 (CET)
Received: from NT.butale.local ([fe80::63d6:d793:9d8:e512])
    by NT.butale.local ([fe80::63d6:d793:9d8:e512%11]) with
    mapi; Fri, 29 Mar 2013 12:03:36 +0100
From: Cefizelj <cefizelj@butale.si>
To: "prijava@du-butale.org" <prijava@du-butale.org>
Date: Fri, 29 Mar 2013 12:03:36 +0100
Subject: =?utf-8?B?b3ByYXZpxI1pbG8g?=
Message-ID: <D32FBF3752A0E36F083C1C8939A5@NT.butale.local>
```

   Recimo, da zaupamo, da je zapis avtentičen. Ali menite, da je morda Cefizelj tokrat le nedolžen in je oddal prijavo pravočasno? Utemeljite odgovor.

3. Kateremu napadu so podvržene naprave, ki zaupajo ostalim napravam zgolj na podlagi njihovega IP naslova? Utemeljite odgovor.