Digitalna forenzika 2011/12
Pisni izpit 11. veliki traven 2012

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		

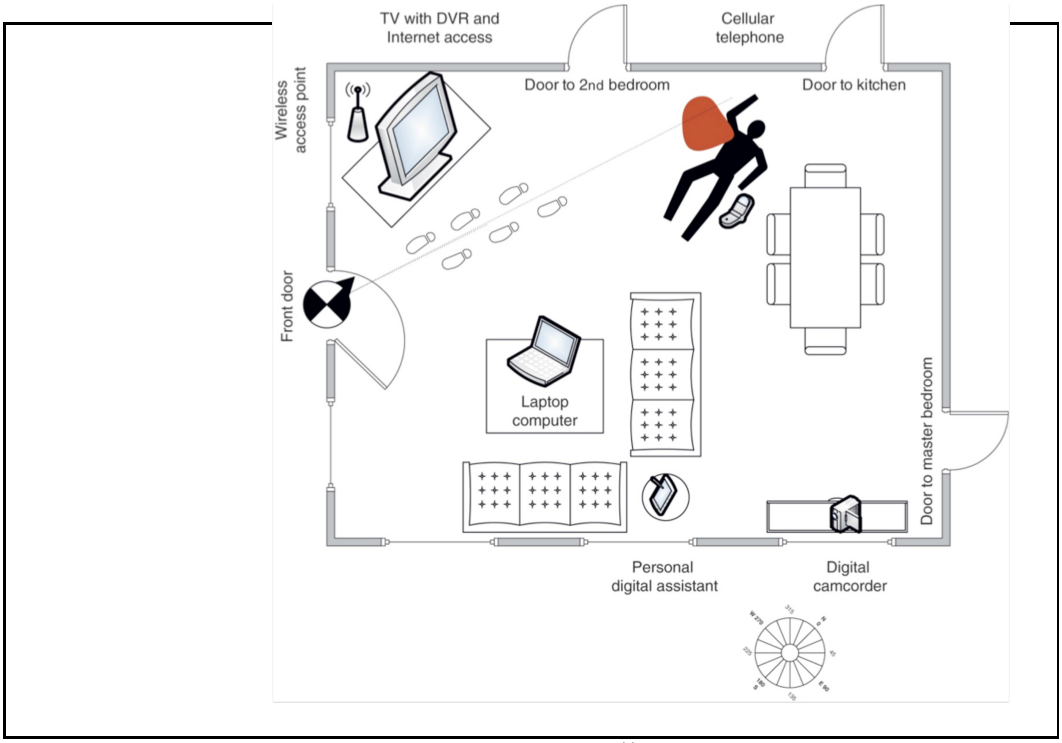
IME IN PRIIMEK: _____

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. Prva faza digitalne preiskave je priprava načrta raziskave mesta zločina. Pripravite čim podrobnejši načrt raziskave mesta zločina, kjer boste navedli kaj boste naredili v kakšenm vrstnem redu s katero napravo.

   NAMIG: Za to vprašanje naj ne bi porabili več kot 10 minut in napisali več kot eno stran in pol.

2. Za preiskavo diska je Peter razvil novo orodje `pzFTK`. Kako naj preveri pravilnost delovanja svojega orodja? Utemeljite svoj odgovor.

3. Napiši zaporedje ukazov v bash, ki bo datoteko bla.txt spravilo vse vnose v sistemski beležnici (*log*), ki vsebujejo besedo „`disk`“.

2. naloga: Delo z diskom.

VPRAŠANJA:

1. V podjetju Petra Zmede kupujejo nove računalnike in stare bodo podarili bližnji šoli. Petra, ki skrbi za varnost v podjetju, so vprašali, če morajo narediti kaj posebnega, predno oddajo stare računalnike. Podajte čim natančneje, kako naj Peter odgovori. Vključno z morebitno uporabo kakšnih orodij ter kako naj se le-ta uporabijo.

2. Dober mesec po namestitvi računalnikov je prišel k Petru direktor podjetja. Namreč vsi ostali so dobili namizne računalnike, le zanj so kupili prenosnik. Direktor je slišal, da je dobro, če ima podatke na svojem disku zakriptirane in je še slišal, da obstaja v ta namen orodje TRUECRYPT. Predlagal je Petru, da bi mu namestil omenjeno orodje na prenosnik ter za kriptiranje uporabil ali algoritem podoben MP3 ali ROT13. Ločeno komentirajte (utemeljite upravičensot in smiselnost): (i) direktorjevega predloga o kriptiranju diska; in (ii) direktorjeva predloga postopkov za kriptiranje.

3. Peter Zmeda je naredil manjšo napako. Pognal je namreč naslednji ukaz:

   ```
   dd if=/dev/zero of=/dev/sda size=460 count=1
   ```

   S tem je zbrisal svojo primarno particijo. Ve, da je imel na particiji Linux. Ker gre za moderen disk, si predstavlja, da ima disk 1023 cilindrov, 255 glav in 63 sektorjev / cilinder. Popravite particijsko tabelo!

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. Nato so telefon predali Petru Zmedi v nadaljnjo obdelavo. Ravno v trenutku, ko Peter dobi telefon, pride na telefon SMS sporočilo. Kaj vse naj Peter naredi, da bo čim bolje zavaroval dokaze?

   NAMIG: Navedite vsaj tri ukrepe in jih utemeljite.

2. Pri forenzični obdelavi prenosnih naprav je možno podatke iskati ne samo na napravi. Navedite vsaj še tri vire podatkov in utemeljite svoje odgovore.

3. Peter Zmeda je v roke dobil prenosni računalnik osumljenca Cefizlja iz Butal. Peter naj bi disk pregledal. Iz njega je izvlekel disk in ga priklopil na svojo delovno postajo. Pri tem vprašanju zapišite konkretne ukaze, ki naj jih Peter uporabi z znanimi orodji, ki ste jih uporabili na vajah.

(i) Kako naj naredi sliko diska? Recimo, da strojni opremi povsem zaupa in bo za istovetnost diska poskrbel nekoč kasneje.

(ii) Potem, ko je naredil sliko diska, so njegovi nadrejeni računalnik vrnili lastniku. Peter je pozabil, kakšni razdelki so bili na disku. Kako lahko spet pride do tega podatka?

(iii) Izkazalo se je, je bil na disku le en razdelek, formatiran z datotečnim sistemom NTFS. S katerim zaporedjem ukazov bi lahko prišel do seznama datotek v njegovem korenskem imeniku? Recimo, da je imel Miran na svojem računalniku datoteko `C:\SKRITO\MOJAOVCKA.JPG`. Kako bi si jo Peter skopiral v svoj domači imenik?

4. naloga:

VPRAŠANJA:

1. Na predavanjih smo srečali Locardovo načelo izmenjave. (i) O čem govori to načelo? (ii) Opišite ga na pirmeru mesta zločina s slike sl. 1.

2. Recimo, da je preiskovalec Peter našel na prenosniku na sl. 1 slike z otroško pornografijo. Kaj lahko predpostavi o tem, kako so prišle na ta prenosnik? Utemeljite svoj odgovor.

3. Tokrat ne bomo preiskovalci, ampak bomo skrivali podatke in sicer v zvočno datoteko. Za zapis zvoka lahko izbiramo med zapisoma MP3 in FLAC (*Free Lossless Audio Codec*). Za oba zapisa imamo na voljo tako podprogram (orodje) za kodiranje (stiskanje), kot za dekodiranje (razširjanje). Za katerega se naj odločimo? Utemeljite odgovor.

   NAMIG: Orodij za stiskanje in razširjanje ne moremo spreminjati.