# Digitalna forenzika 2013/14
# Pisni izpit 3. kimavec 2014

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. Poleg tega so nekatera vprašanja namenoma postavljeno nedoločeno in zahtevajo postavljanje predpostav za natančen odgovor. Pri slednjem bodi natačni, saj natančnost prinese več točk. Načelni odgovori ne prineso vseh točk.

Čas pisanja izpita je 90 minut.

Veliko uspeha!

| NALOGA | TOČK | OD TOČK | NALOGA | TOČK | OD TOČK |
|---|---|---|---|---|---|
| 1 | | | 3 | | |
| 2 | | | 4 | | |

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

**1. naloga:** V podjetju TamInTu d.o.o. so vdrli v računalniški sistem preko http strežnika. Pri preiskavi strežnika je Peter Zmeda našel med zabeležkami naslednjo vrstico:

```
98.242.111.223 - - [18/Jun/2012:20:44:19 +0200]
  "GET /goods4you HTTP/1.1" 404 207 -" "Mozilla/4.0
  (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

Poleg tega je ugotovil še naslednje:

```
PZ> arp -an
? (192.168.127.1) at 0:13:f7:39:d8:d1 on en0 ifscope [ethernet]
? (192.168.127.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
PZ> nslookup 98.242.111.223
Server:  192.168.127.1
Address:  192.168.127.1#53
Non-authoritative answer:
223.111.242.98.in-addr.arpa
    name = c-98-242-111-223.hsd1.ga.comcast.net.
Authoritative answers can be found from:
111.242.98.in-addr.arpa nameserver = dns105.comcast.net.
111.242.98.in-addr.arpa nameserver = dns102.comcast.net.
111.242.98.in-addr.arpa nameserver = dns103.comcast.net.
111.242.98.in-addr.arpa nameserver = dns101.comcast.net.
111.242.98.in-addr.arpa nameserver = dns104.comcast.net.
```

Na zaslišanju je Peter dejal: „Iz dokaznega gradiva sklepam, da je do spletne strani dostopal zaposleni podjetja `comcast.net`."

VPRAŠANJA:

1. Pojasnite podatke, ki jih je Peter pridobil s pomočjo ukazov (i.) `nslookup` in (ii.) `arp`.

   NAMIG: Ne pričakuje se po eno stran odgovora na ukaz, a le čim bolj temeljiti boste v odgovoru, več točk dobite.

2. Komentirajte Petrovo izjavo na sodišču.

3. Napišite zaporedje ukazov v *bash*, ki bo najprej na zaslon izpisalo

   ```
   Katero je najpogostejše slovensko ime na J?
   ```

   Dvanajst sekund kasneje naj v datoteko `2014.txt` zapiše `Jan` in na zaslon `Janez`.

**2. naloga:** Peter Zmeda sumi, da je Cefizelj ponovno uščipil nekaj slabega. Dokazi o tem naj bi se nahajali pri njem doma. Peter sicer gleda takšne in drugačne kriminalke, toda ve, da mora dobiti najprej nalog za preiskavo, če želi do dokazov.

VPRAŠANJA:

1. (i.) Kdo izdaja nalog za preiskavo? (ii.) Navedite vsaj pet dejstev, ki jih mora Peter napisati na zahtevo za nalog za preiskavo, da ga bo lahko dobil.

2. Peter je ugotovil, da je primer, ki ga preiskuje, podoben enemu prejšnjih primerov, ki jih je že nekoč preiskoval. Zato se odloči, da bo nadaljeval preiskavo na enak način. Kako imenujemo takšen način preiskave?

3. Peter je takoj izdelal kopijo podatkov na disku z ukazom:

   ```
   dd if=/dev/sdb1 of=oslovskaSenca.img bs=512
   ```

   Nato je disk poslal v uničenje, kjer so ga zdrobili na drobne koščke ter pretalili. Za vsak slučaj, da se je znebil potencialnih virusov, je še ponovno namestil sistem na svoj računalnik, pri čemer je nedotaknjeno ohranil sliko diska v datoteki `oslovskaSenca.img`.

   Sedaj mora Peter zajete podatke analizirati.

   (ii) S katerim zaporedjem ukazov lahko ugotovi, kakšne so bile velikosti razdelkov na disku? (ii.) S katerim zaporedjem ukazov lahko dostopa do datotek, zajetih v `oslovskaSenca.img`? (iii.) Na kaj je Peter pri zajemu pozabil? Kako bi zajem izvedli vi? Napišite zaporedje ukazov.

**3. naloga:** Prenosne (mobilne) naprave.

VPRAŠANJA:

1. Kriminalist je na mestu zločina našel nahajal tudi celični telefon. Telefon je še vključen in tehniki so z njega že pobrali prstne odtise. Nato so telefon predali forenziku 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 bistveno različne 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. 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.

**4. naloga:** Na mestu zločina so kriminalisti našli pametni telefon in prenostni računalnik. Sumijo, da sta v lasti velikega razbojnika Cefizlja, ki naj bi zagrešil krajo sence osla iz Višnje gore.

VPRAŠANJA:

1. Omenjali smo pet osnovnih korakov v digitalni preiskavi. (i.) Kateri so ti koraki? (ii.) Opišiti in razložite postopke za vsakega od korakov na primeru pametnega telefona, ki so ga našli na mestu zločina.

2. Eden od korakov digitalne preiskave je raziskava (*examination*). Na primeru zločinskega dejanja pomagajte oblikovati forenziku Petru (i.) hipotezo v povezavi s prenosnim računalnikom in (ii.) način preverjanja le-te. (iii.) V vašem primeru opišite kako izgleda triaža podatkov na prenosnem računalniku.

3. Če nekdo na disku opazi podatke, ki izgledajo naključno, lahko sklepa, da gre za šifrirane podatke in nas poskuša prisiliti, da jih odšifriramo. Da se temu izognemo, lahko uporabimo tehnike za verjetno zanikanje (*plausible deniability*). Ustvarjanje nosilcev za takšne podatke omogoča orodje `Truecrypt`. Razložite princip delovanja teh nosilcev.