# Digitalna forenzika 2012/13
# Pisni izpit 26. rožnik 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:**

VPRAŠANJA:

1. Klasičen primer Locardovage principa predstavljajo prstni odtisi storilca na mestu zločina. Opredelite digitalni primer in utemeljite odgovor.

   NAMIG: Prstni oddtisi natančno določajo storilca.

2. Petru je prijatelj prinesel disk, ki naj bi nekoč pripadal Mojci. Mojca je Petru všeč in Peter bi rad preveril, ali imata kake skupne iterese. Mojca običajno dela z Google Chrome ali Internet Explorerjem 8.

   V katerem formatu je shranjena zgodovina brskalnikov, ki ju uporablja Mojca? Ali je mogoče, da je prijatelj v zgodovino podtaknil svoje strani, če vemo, da prijatelj računalnika ni zaganjal s tega diska? Če je to mogoče, kako bi prijatelj sploh lahko dodal vnose v zgodovino?

3. V katero od štirih kategorij (po Parker-ju) spada računalnik, na katerega je bila naložena programska oprema, ki lastniku otežuje delo, hkrati pa izvaja napade na druge računalnike? Odgovor utemeljite.

**2. naloga:** Peter je tokrat v novem poslu – razvija in tiska fotografije. Prva investicija je nakup novega diska, na katerega bo spravljal slike. Po prvi oceni bo na leto imel opravka s približno milijon slikami – ne sprašujte kako je prišel do te številke. Še predno je prišel novi disk v hišo, se je Peter seznanil s programom za formatiranje diska `newfs` in ena od stvari, ki jo program želi izvedeti od Petra je, koliko inode vozlišč naj naredi. Peter želi uporabiti datotečni sistem `ufs`.

Čez tri leta je Peter kupil nov disk, ki je bil osem krat večji. Slišal je, da mora poskrbeti za podatke na starem disku, predno ga zavrže. Zato je ponovno sformatiral disk s programom `newfs`.

VPRAŠANJA:

1. (i) Predlagajte kako velik disk naj kupi Peter? Utemeljite odgovor. (ii) Predlagajte Petru število inode vozlišč. Utemeljite odgovor. (iii) Prepričajte Petra, da je ravnanje s starim diskom v redu ali ne ter utemeljite svoj odgovor.

2. Na disku lahko šifriramo podatke na dva načina. Katera sta ta dva načina in zapišite vsaj po dva primera programja za vsakega od njih.

   Eden od načinov šifriranja je posebej primeren za tvorjenje skritih nosilcev: (i) kateri, (ii) kako to naredimo in (iii) zakaj bi to želeli narediti?

3. Katero vrsto šifriranja uporablja PGP za epošto?

**3. naloga:** Omrežja in forenzika.

VPRAŠANJA:

1. Ena od občutljivih komponent stikal in usmerjevlanikov je tabela MAC naslovov – *Content addressable memory (CAM) table*. (i.) Kaj točno je shranjenega v tej tabeli (MAC naslovi ne bo dovolj)? (ii.) Kako bi lahko napadalec napadel tabelo in dosegel nedovoljen dostop? (iii.) Kakšno sled bi forenzik iskal po izvedenem napadu?

2. Prvega aprila 2013 je Peter Zmeda dobil elektronsko pošto s sporočilom:

   > Pozdravljeni,
   > Zaradi spora pri predmetu Podatkovne Baze 2 (63713), z nosilcem predmeta, viš. pred. dr. Janez Novak, je ob vložitvi pritožbe s stani nosilca predmeta bil izdan sklep, da se zglasite na zagovor pred disciplinsko komisijo, ki bo potekal v predavalnici 9, Tržaška cesta 25, 1000 Ljubljana, v četrtek 11.04.2013 ob 17 uri. Na zagovoru bo obravnavana vaša morebitna izključitev zaradi neprimernega vedenja ter kršenja več členov pravilnika, ki bodo izpostavljeni na obravnavi.
   > S spoštovanjem,
   > prof. dr. Nadja Kosmatin

   Ker je bil pa le tak dan, se je Peter odločil pogledati celotno sporočila:

```
Delivered-To: peter.zmeda@gmail.com
Received: by 10.76.10.73 with SMTP id g9csp95881oab;
  Mon, 1 Apr 2013 08:27:26 -0700 (PDT)
X-Received: by 10.14.219.7 with SMTP
  id l7mr38929832eep.12.1364830045836;
  Mon, 01 Apr 2013 08:27:25 -0700 (PDT)
Return-Path: <www-data@sv3.mankuc.com>
Received: from sv3.mankuc.com (89-212-19-39.static.t-2.net.
   [89.212.19.39])
  by mx.google.com with ESMTP
  id i43si20233149eem.154.2013.04.01.08.27.25;
  Mon, 01 Apr 2013 08:27:25 -0700 (PDT)
Received-SPF: neutral (google.com: 89.212.19.39
  is neither permitted nor denied by best guess
  record for domain of www-data@sv3.mankuc.com)
  client-ip=89.212.19.39;
Authentication-Results: mx.google.com;
  spf=neutral (google.com: 89.212.19.39 is neither
  permitted nor denied by best guess record for
```

```
  domain of www-data@sv3.mankuc.com)
  smtp.mail=www-data@sv3.mankuc.com
Received: by sv3.mankuc.com (Postfix, from userid 33)
  id BB4B31705; Mon,  1 Apr 2013 17:25:27 +0200 (CEST)
To: Sandi Mikus <peter.zmeda@gmail.com>
Subject: Vabilo na zagovor
From:Nadja Kosmatin <nkosmatin@uni-lj.si>
X-Mailer: uni-lj
Message-Id: <20130401152527.BB4B31705@sv3.mankuc.com>
Date: Mon,  1 Apr 2013 17:25:27 +0200 (CEST)

Pozdravljeni,
...
```

Vemo, da je fakulteta priključena na omrežje ARNES. Katerim podatkom v celotenm sporočilu lahko Peter zaupa? Utemeljite odgovor.

NAMIG: Preveri iz katerega omrežja je prišlo sporočilo.

3. Katera (ena ali več) omrežna plast izvaja detekcijo napak? Utemeljite odgovor.

**4. naloga:**

VPRAŠANJA:

1. Varovanje zasebnosti je eno temeljnih načel človeške družbe. V sodobnem, digitalnem svetu postaja zasebnost po eni strani še pomembnejša in po drugi težko določljiva. Tako se je razvil koncept „upravičenega pričakovanja zasebnosti“. Opišite ta koncept in podajte dva primera njegove uporabe.

2. Eden od seminarjev se je ukvarjal s steganografijo in sicer tako, da skrivamo poljubne podatke v zvočne datoteke. Predlagajte kakšen izvirnejši način, kot je metoda zamenjave najmanj pomembnih bitov. Pri razvoju lahko sodelujete s strokovnjakom za analizo zvočnih signalov.

   NAMIG: Skriti podatki morajo izgledati kot del zvočnih podatkov, hkrati pa ne smejo vplivati na posnetek.

3. Ali drži, da morajo biti digitalni preiskovalci pozorni zgolj na digitalne sledi? Utemeljite odgovor.