Digitalna forenzika 2014/15
Pisni izpit 5. veliki traven 2015

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 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: Osnove.

1. Eden od temeljnih principov, na katerem je zasnovana sodobna forenzika je Lockardov princip. (i) Kaj točno pravi? (ii) Zgodil se je zločin izsiljevanja po e-pošti. Opišite primer principa na tem zločinu in utemeljite opis glede na svojo definicijo iz prvega dela vprašanja.

2. Peter je dobil v pregled štiri diske, vsakega velikosti 1TB iz nekega strežnika. Takoj jih je priklopil na svoj računalnik in naredil kopije podatkov:

   ```
   for i in abcde; do dd if=/dev/sd$i of=slika-$i.raw; done
   ```

   Nato je izvedel nekaj ukazov in ugotovil, da je bil na diskih nameščen Linux in da se je v enem od imenikov skrivala ogromna datoteka velikosti 1,5TB. Ugotovil je tudi, da bi vse podake lahko zagotovo še vedno dobil, če bi kateri koli disk manjkal. Možno bi bilo celo, da bi prišel do vseh podatkov, če bi manjkala dva diska. (i) Kako menite, da so bili organizirani podatki na diskih? Predlagajte vsaj dve možnosti. Katere konkretne ukaze bi uporabili, da bi prišli do podatkov na diskih? (ii) Izkazalo se je, da je Peter naredil napako, saj so bili podatki na diskih, ko jih je prejel, drugačni kot takrat, ko je naredil sliko. Kako je to mogoče, če ni nikdar pognal ukaza mount? Predlagajte vsaj dva razloga in kako bi se lahko napaki izognil.

3. Kakšna je razlika med posestjo vojaškega računalniškega sistema za nadzor gibanja podmornic in posestjo programske opreme za vdore v sisteme? Utemeljite odgovor.

2. naloga: Diskovni sistemi.

VPRAŠANJA:

1. Pri Cefizlju so forenziki na disku odkrili skrito particijo, ki je vsebovala v Butalah prepovedane slike orehovih dreves. Cefizelj trdi, da nima nič s temi slikami in da je nedolžen. (i) Na kakšni osnovi lahko Cefizelj zastavi svojo obrambo o nedolžnosti? (ii) Kakšno dokazno gradivo bi lahko naredilo njegovo trditev verodostojnejšo? Utemeljite svoj odgovor.

2. Tokrat mora Peter Zmeda pregledati disk iz računalnika znanega zlikovca Cefizlja. Naredil je sliko diska:

   ```
   dd if=/dev/sdb of=slika.zip
   ```

   Zajeto sliko si želi podrobneje ogledati in je poskusil z naslednjim nizom ukazov:

```
unzip slika.zip
mkdir mnt
mount -o loop slika.raw mnt .
```

Ups, ukaz unzip ni deloval. (i) Zakaj? (ii) In zakaj ni deloval ukaz mount? (iii) Kako naj pogleda vsebino slike diska? Napišite konkretne ukaze, ki bi jih za to uporabil, po možnosti z vsemi potrebnimi argumenti.

3. Katera je posebna lastnost na UNIX operacijskih sistemih, ki je ne srečamo na običajnih Windows/DOS sistemih ter je ključna pri forenzični preiskavi, saj zagotavlja nespremenljivost podatkov na diskovni enoti? Utemeljite odgovor.

3. naloga: Mobilne naprave in omrežna forenzika.

VPRAŠANJA:

1. Kriminalisti so pri Cefizlju našli telefon, s katerega naj bi se prijavljal v e-banko BB (*Banka Butale*) in pridno praznil račun Lavdona Štimanega. Nalogo preiskave primera so dali Petru. (i) Pripravite načrt preiskave in (ii) pripravite tri primerne hipoteze, ki naj jih Peter preveri v svoji preiskavi primera. (iii) Kako naj preveri predlagane hipoteze? Utemeljite svoj odgovor.

   NAMIG: Pozor, vprašanje govori o preiskavi primera in ne preiskavi naprave.

2. Peter ima občutek, da ga zasledujejo. Vsakič, ko naredi nov selfie in ga objavi na Facebooku, dobi na poštni naslov reklamo, naj obišče neko trgovino v svoji neposredni bližini. Včasih se mu takšna situacija zgodi tudi, ko se naprimer fotografira v kopalnici, kjer iz ozadja na sliki ni mogoče razbrati, kje se Peter nahaja. (i) Kako lahko Facebook ugotovi, kje je Peter naredil selfie? (ii) Ali obstaja kak način, da bi se Peter sledenju izognil? (iii) Kako lahko Peter svoje zasledovalce zmede, da bodo mislili, da se nahaja drugje, kot je v resnici (napišite zaporedje ukazov oz. opišite postopek)?

   NAMIG: Če boste dovolj temeljito odgovorili na vprašanje (i), bosta preostali precej preprosti.

3. Sistemski inženir Peter Zmeda je dobil pošto svojega nadrejenega, da ga odpušča iz službe. Pošta se je pričela z naslednjo glavo:

```
From francek.sef@gov.butale  Mon Jan 20 15:50:49 2014
X-Original-To: francek.sef@localhost
Received: from francek.estoritve.gov.butale (localhost [127.0.0.1])
```

```
        by posta.gov.butale (Postfix) with ESMTP id A2B584AC47
        for <fsef@localhost>; Mon, 20 Jan 2014 15:50:49 +0100
(CET)
MIME-Version: 1.0
From: "Franček Sef" <Francek.Sef@gov.butale>
To: "Peter Zmeda" <Peter.Zmeda@gov.butale>
CC: Špela Copatko" <Kadrovska@gov.butale>
Subject: Delovno razmerje
Date: Mon, 20 Jan 2014 15:56:10 +0100
Message-ID: <4C9375CBA7CA62439F16162CCB9D0F1901FFFEB9@GOV-BUTALE>
Content-Type: text/html; charset="iso-8859-2"
Content-Transfer-Encoding: quoted-printable
X-Keywords: NonJunk
```

Peter sumi, da gre za prevaro. Kje naj prične z iskanjem dokaza? Utemeljite odgovor.

4. naloga: Izvajanje preiskave.

VPRAŠANJA:

1. Na predavanjih smo predstavili več procesnih modelov digitalne preiskave. Recimo, da se morate odločiti za enega med njimi, po katerem boste vodili digitalne preiskave v vaši enoti. Odločite se za enega in utemeljite zakaj ste izbrali le-tega ter ne preostalih.

   NAMIG: Dejansko morate primerjati model, ki ste ga izbrali, s preostalimi in pokazati, zakaj menite, da je vaša izbira primernejša. Seveda, tukaj nikakor ni samo ena izbira pravilna, ampak je pomembna utemeljitev.

2. Peter Zmeda je nadvse ljubosumen človek. Rad bi preveril, kaj si njegovo dekle Roberta dopisuje prek e-pošte. Preko omrežja se je prijavil na njen računalnik. Ve, da je Roberta prijavljena na svojo spletno pošto v brskalniku Firefox. Sedaj bi rad dostopal do njene pošte. (i) Katere podatke mora prenesti z njenega računalnika, da bo lahko prevzel njeno sejo? (ii) Peter svoje nečedno delo opravlja v lupini na računalniku svojega dekleta prek programa ssh. Kako bi Roberta lahko ugotovila, kaj je Peter počel? (iii) Roberta si je na spletu ogledovala tudi postavne mladce. S katerim orodjem oz. orodji in na kakšen način bi Peter lahko prišel do njihovih slik?

3. Kot forenzik med preiskavo diska, v kateri iščete dokaze v zvezi s tihotapljenjem drog, naletite na strogo zaupne načrte vojaškega sistema za komunikacijo in določanje ciljev. Kaj morate storiti? Utemeljite odgovor.