Digitalna forenzika 2016/17
Pisni izpit 8. veliki traven 2017

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 predpostavk 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. Peter je v pregled dobil disk, ki ga je uporabljal Cefizelj. Ker je Cefizelj zloben, Peter sumi, da je skril nekaj podatkov med 1. in 2. razdelek. Pognal je nek program, ki mu je izpisal:

```
Device       Start         End   Sectors   Size Type
/dev/sdb1     2048     1503231   1501184   733M Microsoft basic
data
/dev/sdb2  1507328     3504127   1996799   974M Linux filesystem
/dev/sdb3  3504128  1000214527 996710400 475.3G Linux filesystem
```

A) (i) S katerim orodjem bi lahko ugotovili, kje se začne in kje konča vsak razdelek? (ii) Koliko prostora (v byte-ih) je med 1. in 2. razdelkom? Napišite postopek, kako ste prišli do rezultata. (iii) Kako bi v datoteko vmes.raw spravil podatke, ki so med razdelkoma? Napišite ukaz.

B) Recimo, da digitalni preiskovalec ugotovi, da je primer, ki ga preiskuje podoben enemu prejšnjih primerov, ki jih je preiskoval. Zato se odloči, da bo nadaljeval preiskavo na enak način. Kako imenujemo takšen način? Utemeljite odgovor.

C) Na predavanjih smo omenjali *Locardov princip*. Kaj je to? Navedite tri situacije, kjer nastopi in opišite kako je nastopil.

2. naloga: Datotečni sistemi.

VPRAŠANJA:

A) Peter nadvse rad snema, kako rastejo koprive ob cerkvi. Snema jih v visoki ločljivosti skozi celo leto, za kar potrebuje precej prostora – na leto vsaj 10TiB. Na žalost so največji diski, ki si jih Peter lahko privošči, veliki le 1,5TiB. Peter hoče imeti na računalniku vse posnetke v enem samem imeniku. (i) Če je Peter prepričan, da noben disk ne bo nikdar odpovedal, katero tehnologijo lahko uporabi? Naštejte vsaj dve možnosti. Napišite, koliko diskov potrebuje. (ii) Če Peter želi, da bi podatki ostali nedotaknjeni, čeprav mu eden od diskov odpove – kako naj jih poveže? Narišite skico s fizičnimi in navideznimi bločnimi napravami.

B) Naštejte vsaj tri mesta, kjer naj Peter Zmeda pri forenzični obdelavi Windows OS išče sledi o delu na spletu. Za vsako od mest podajte primer sledi in kaj bi lahko na podlagi le-te sklepali.

C) Tokrat bomo pogledali datotečni sistem `ext3`. Osnovna struktura za shranjevanje metapodatkov o eni datoteki je `inode` – indeksno vozlišče, ki vsebuje 32-bitne reference na vsebino diska. (i) Na kako veliko particijo še lahko namestimo datotečni sistem `ext3` s tako velikimi referencami? Utemeljite odgovor. (ii) Indeksno vozlišče vsebuje več različnih časovnih zabeležk. Katere in ob katerih operacijah se nastavijo/spremenijo? (iii) Kaj je največja razlika med datotečnima sistemoma `ext2` in `ext3`?

3. naloga: Omrežna forenzika ter sistemske zabeležke.

VPRAŠANJA:

A) Peter Zmeda nujno potrebuje na svoji napravi dostop preko storitve telnet, saj nima ssh strežnika. Da bi dosegel vsaj določeno mero varnosti, je dodal zaščito, da se na napravo lahko priključi samo odjemalec z IP naslovom `10.20.30.40`. Kateremu napadu je podvržena Petrova naprava? Utemeljite odgovor in čim podrobneje opišite možni napad.

   NAMIG: Da bo opis smiselen, je smotrno opisati topologijo sistema in v njem označiti, kje se nahaja naprava in kje napadalec.

B) Peter Zmeda je od svojega strežnika (`bor`) po `syslog` protokolu dobil sporočilo:

```
<17> 1 2016-10-11T22:14:15.003Z bor pif 2234   Tezave, tezave!
```

   Recimo, da je sporočilo povsem v skladu z RFC 5424. (i) Ali mora Peter kaj storiti, ali lahko sporočilo zanemari? Utemeljite odgovor. (ii) Za katero funkcionalnost na sistemu skrbi program s PID 2234? Utemeljite odgovor.

C) V podjetju *Butalska Sol, d.o.o.* so ugotovili, da jim je nekdo ukradel recept za proizvodnjo soli. Poklicali so digitalnega forenzika Petra Zmedo, ki je ugotovil, da je nekdo vdrl v računalnik Luke Lukeža, ki je bil v notranjem omrežju. (i) Zapišite tri hipoteze, kako so vdrli v računalnik in (ii) za vsako hipotezo opišite oziroma utemeljite, kako bi preverili njeno resničnost.

4. naloga: Mobilne naprave in izvajanje preiskave.

VPRAŠANJA:

A) 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.

B) Osnovna razlika med mobilnim telefonom in navadnim računalnikom je v tem, da je slednji več ali manj neprestano na istem mestu. (i) Opišite tri načine, kako lahko ugotovimo, kje se je gibal mobilni telefon. (ii) Za vsakega od načinov ocenite kako zapleteno je priti do podatkov in kaj vse moramo pri tem izpolniti. (iii) Ali je smiselno pridobiti vse troje podatke? Utemeljite odgovor.

C) Peter že od nekdaj rad uporablja brskalnik Firefox. Nekje v omari je našel disk iz pred 5 let, na katerem je tudi njegov stari domači imenik. Rad bi ugotovil, katere strani je obiskoval, ko je ta disk uporabljal. (i) Kje lahko najde podatke o zgodovini obiskanih strani? (ii) V kakšni obliki je shranjen seznam obiskanih strani? (iii) Katero orodje lahko uporabi, da ga pregleda?