Digitalna forenzika 2016/17
Pisni izpit 27. rožnik 2018

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.

A) V slovenskem pravnem sistemu imamo v kazenskem postopku sedem korakov. Naštejte jih in napišite vlogo vsakega.

B) Pri rokovanju z digitalnimi dokazi naletimo na več izzivov. Dva sta: (a) ostanki ali rekonstrukcija ni enaka kot celotni podatki (b) podatki niso večni. Za vsakega od izzivov (i) pojasnite, kaj pomeni in navedite primer; (ii) pojasnite, kako ga pri digitalni forenziki poizkusimo premagati.

C) Peter poizkuša ustvariti forenzično kopijo svojega 2. SATA diska. Zaenkrat je pognal spodnji ukaz:

```
dd if=/dev/sda2 of=img.raw bs=4096 count=4096
```

(i) Katero napravo je dejansko skopiral (pojasnite, kaj ta naprava predstavlja)? (ii) Katero ime naprave bi bilo pravilno? (iii) Razen imena naprave, kaj je v ukazu še narobe in kako naj to popravi?

2. naloga: Operacijski sistemi.

VPRAŠANJA:

A) Peter Zmeda poizkuša v svoj stari računalnik brez EFI spraviti nov, velik disk velikosti 6TB. Datotečni sistem in razdelke je ustvaril pri prijatelju, nakar ga je priklopil na svoj računalnik. Preveril je, da disk deluje brez težav ub da lahko pride do podatkov. Ker se boji, da bo stari odpovedal, se je odločil, da bo poskrbel, da se sistem zaganja z novega diska. S starega diska je skopiral GRUB na novega. Po ponovnem zagonu, ki je bil uspešen, se mu je računalnik pritožil, da na disku ni nobenega datotečnega sistema. Peter se je prijel za glavo, saj je takoj razumel, kako ga je polomil. Odpravil je napako in se odločil, da bo GRUB ostal na starem disku.

(i) Kje na disku se običajno nahaja GRUB? (ii) Kaj je Peter po nesreči prepisal? (iii) Kako je lahko obnovil prepisane podatke?

B) Mikrosoftova Okna vsebujejo VSS – *Volume Shadow Copy*. (i) Kaj ta storitev omogoča? (ii) Kako jo lahko uporabimo pri digitalni forenziki?

C) Beleženje je ena od ključnih storitev v sodobnih operacijskih sistemih. Kako je urejeno vključno s tem, kje so podatki shranjeni (i) pod Unix ter GNU/Linux sistemi in (ii) na Mikrosoftovih Oknih?

Peter tudi sumi, da je nekdo vdrl v računalnik njegovega šefa, ki uporablja Mikrosoftova Okna. (iii) Kje naj išče dokaze vdora? Utemeljite odgovor.

3. naloga: Mobilna in omrežna forenzika.

VPRAŠANJA:

A) Peter je dobil v skrb star strežnik, za katerega je doslej skrbel Jože T. V `/home/joze/.bash_history` je Peter našel naslednjo vrstico:

```
telnet localhost splet
```

Ko je ukaz pognal, je dobil naslednji odgovor:

```
peter@slovnica:~/$ telnet localhost splet
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET /
A lepše od tele bilo ni nobene.
Connection closed by foreign host.
```

Katera datoteka na sistemu je bila najverjetneje spremenjena, če vemo, da je Jože T. odličen sistemski administrator ki slučajno obožuje slovenski jezik? Utemeljite odgovor.

B) Peter Zmeda poizkuša analizirati mobilni telefon z OS Android. Rad bi našel zgodovino brskanja in gesla za spletne storitve najbolj razvpitega nepridiprava v Butalah, Cefizlja. (i) Na kateri imenik je običajno priklopljen razdelek, ki vsebuje zgodovino brskanja po spletu? (ii) Ali Peter lahko najde spletna gesla? S kakšno zgoščevalno funkcijo in/ali šifriranjem so zaščitena? (iii) V katerem formatu je spravljena zgodovina brskanja pri Chrome? Napišite vsaj eno orodje, ki bi ga lahko uporabili za dostop do teh podatkov.

C) Oglejmo si pameten in navaden mobilni telefon. (i) Podajte dve hipotezi za digitalno preiskavo, ki bi bili enaki pri obeh tipih naprav. Utemeljite napisano. (ii) Podajte eno hipotezo, ki velja le za pametne telefone, in eno, ki velja le za navadne mobilne telefone. Utemeljite obe.

4. naloga: Vodenje preiskave.

VPRAŠANJA:

A) Butalski policaj je na Cefizljevem domačem računalniku naletel na fotografije pergamenta z receptom butalske soli. Po butalski zakonodaji je posest recepta najstrožje kazniva.

Ker Cefizlja ni nikjer na spregled, je Peter vprašal slavno butalsko bolho Špinco Maroglo, kako bi se tak recept lahko znašel na Cefizljevem računalniku.

Dala mu je tri možnosti:: (i) Cefizelj je recept morda pretihotapil na USB ključku, (ii) morda je sliko ustvaril z mobilnim telefonom, kjer še vedno obstaja kopija, (iii) morda je imel pajdaša, ki je skrivnost pretočil iz Butal s pomočjo Interneta. Kateri od bolhinih predlogov je pravilen, kateri napačen in, kar je najpomembneje, zakaj?

B) Kaj je forenzična preiskava in kaj vključuje? Pri utemeljitvi odgovora podajte primere.

C) Drugi princip navodil ACPI pravi:

> In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions;

in v prevodu:

> V izjemnih primerih, ko preiskovalec smatra, da je potrebno do podatkov dostopati na dokaznem računalniku, mora oseba, ki do podatkov dostopa, biti za to usposobljena ter sposobna pojasniti pomen in posledice svojih dejanj;

Kaj menite o tem principu? Podajte dva primera za in dva primera proti. Utemeljite svoje odgovore.