Digitalna forenzika
(2023/24)
Pisni izpit 11. rožnika 2024

Izpit pišete posamič. Dovoljena je literatura v papirni obliki ali na računalniku, ki ni povezan v omrežje. Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti dodatne točke. Čeprav so posamezna vprašanja lahko bolj vezana na določeno poglavje predavanj, je za reševanje potrebno uporabiti znanje še iz drugih poglavij. Poleg tega nekatera vprašanja zahtevajo postavljanje predpostavk za natančen odgovor. Pri slednjem bodite 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: _____

Naloga 1. *Osnove.*
VPRAŠANJA:

1. V katero od štirih kategorij (po Parker-ju) spada računalnik, ki so ga uporabili za ponarejanje dokumentov in nato uničili? Utemeljite odgovor in ga ilustrirajte s primerom.

(a) Je subjekt, objekt in orodje (instrument) zločina.
(b) Je objekt in orodje (instrument) zločina.
(c) Je subjekt in orodje (instrument) zločina.
(d) Je objekt in subjekt zločina.

2. Peter Zmeda je dobil od nadrejenega v roke sliko sistemskega diska računalnika, na katerem je domovalo več uporabnikov. Policija sumi, da je eden od uporabnikov zbiral otroško pornografijo in pri tem uporabljal brskalnik. (i) Napišite hipotezo kje iskati datoteke s sledmi in zakaj? Celovitejši odgovori bodo bolje ocenjeni. (ii) Na predavanjih smo spoznali, da imajo dokazi skupne lastnosti in posebne lastnosti. Opredelite obe vrsti lastnosti v primeru iz točke (i). Podajte še konkretne primere.

3. Peter bi rad pregledal dogodke in register na računalniku z *Microsoft Windows 8* in več uporabniki. Ne bi rad prenašal in shranjeval vseh datotek, temveč le potrebne. (i) Kje vse se nahaja register (*registry*)? Kje se nahajajo dnevniki (*event logs*)? (ii) Katera orodja lahko uporabi za pregled teh podatkov? (iii) Peter je slišal, da so pri *Windows* opisi dogodkov shranjeni v .DLL datotekah programov, ki dogodke ustvarjajo. Katere od teh datotek bo dejansko potreboval? Lahko opišete tudi, kako bo prišel do seznama.

Naloga 2. *Datotečni sistemi.*
VPRAŠANJA:

1. Osrednja struktura za rokovanje z datotekami v operacijskem sistemu UNIX je `inode`. (i) Katere metapodatke hrani `inode`, oziroma kaj sporočajo ti metapodatki? (ii) Cefizelj je vdrl v Petrov računalnik in posebej sta ga zanimali besedili izpita s predroka in s prvega roka pri predmetu *Digitalna forenzika*. Res je našel imenik `PI` in v njem obe besedili:

```
[peter PI]> ls -lai
total 352
115817034 drwxr-xr-x  4 peter  .
 23110634 drwxr-xr-x  8 peter  ..
115817723 -rw-r--r--@ 2 peter  2324DF-PI00.pdf
115817723 -rw-r--r--@ 2 peter  2324DF-PI01.pdf
[peter PI]>
[peter@Peter-Macbook PI01]>
```

Kaj lahko sklepamo na podlagi izpisa o obeh besedilih in zakaj?

2. Kje se običajno nahaja tabela razdelkov GPT? Zakaj prav tam in zakaj na ostalih mestih ne?

(a) Na začetku diska.
(b) Za MBR in na koncu diska.
(c) Na začetku in na koncu diska.
(d) Na koncu diska.
(e) V MBR.

3. Peter je dobil v pregled 8 10TB diskov. Na vseh diskih naj bi bil en sam datotečni sistem. (i) Razen z uporabo RAID, kako bi še lahko nanje spravili en sam datotečni sistem? (ii) Če je na njih RAID5, kakšna je maksimalna kapaciteta datotečnega sistema? Kaj pa, če je RAID10? (iii) Ali je na diskih uporabljen GPT, MBR ali nič od naštetega? Utemeljite odgovor.

Naloga 3. *Forenzika mobilnih naprav in omrežij.*
VPRAŠANJA:

1. Z dražjim pametnim telefonom z običajnimi nastavitvami naredimo fotografijo sredi mesta. Iz vsebine fotografije ni moč razbrati lokacije fotografiranja. Lahko to naredimo (zlahka) kako drugače? Za vsako od možnosti utemeljite zakaj ne, oziroma, če da, kako in zakaj da.

1. Ne.
2. Da, z iskanjem prič.
3. Da, s pomočjo operaterja.
4. Da, tak telefon ima GPS, ki trenutno lokacijo zapiše v datoteko fotografije.

2. Računalniška komunikacija je modularizirana tako, da je razdeljena na plasti (ISO/OSI: povezavna - 2, mrežna - 3, prenosna - 4, ... plast). Ena ključnih zahtev komunikacije je varovanje prenesenih podatkov - lahko zakrivanje (šifriranje) ali celovitost (integriteta) - ali oboje. (i) Zakaj je pomembno vprašanje pri forenzični preiskavi, ali komunikacija zagotavljala celovitost prenosa podatkov? (ii) Recimo, da pri načrtovanju komunikacije zagotovimo zaščito podatkov na plasti p. Kaj to pomeni kar zadeva varovanja podatkov na višjih plasteh? Pri odgovoru upoštevajte različne vrednosti p in kaj to pomeni glede možnega napada na komunikacijo.

3. Peter Zmeda preiskuje podatke z mobilnega telefona. Gre za telefon *Android*, Peter pa je dobil sliko celotnega razdelka, priklopljenega na `/data`. (i) Katerih podatkov s tem ni dobil? (ii) Kako bi lahko prišel do seznama kontaktov? (iii) Kako bi mu pri pregledu fotografij pomagalo orodje SQLITE3? Odgovor utemeljite.

Naloga 4. *Preiskava.*
VPRAŠANJA:

1. Katere od naštetih faz ne sodijo v (pod)fazni model? Čemu so namenjene faze, ki sodijo v (pod)fazni model in zakaj preostale ne sodijo?

(a) Rekonstrukcija mesta zločina.
(b) Vse sodijo.
(c) Analiza gradiva.
(d) Priprava.

2. Eno od temeljnih načel kazenskega postopka je načelo *oficialnosti* - da mora državni tožilec po uradni dolžnosti preganjati kazniva dejanja. (i) Zakaj menite se je znašlo načelo med temeljnimi načeli? Kaj bi pomenilo, če bi ne bilo v naboru temeljnih načel? (ii) Butalski policaj je našel Cefizljevo skrivališče, v katerem sumi, da Cefizelj skriva nakradeno sol. Da bi lahko preiskal skrivališče, ve, da mora dobiti ustrezni nalog. Glede na to, da mora državni tožilec po uradni dolžnosti kazniva dejanja, meni, da je tudi prava oseba, ki bo izdala potrebni nalog. Utemeljite zakaj je Petrov razmislek pravilen, oziroma, če ni, zakaj je razmislek napačen. Najbolje s primerom.

3. Peter Zmeda je v pregled dobil strežnik z dvema trdima diskoma. Oba diska je priklopil na svoj računalnik, na katerem uporablja Ubuntu 22.04 Desktop. Ustvaril je kopiji diskov:

```
dd if=/dev/sdc of=prvidisk.raw
sha512sum /dev/sdc
cat /dev/sdd > drugidisk.raw
sha512sum /dev/sdd
sha512sum prvidisk.raw
sha512sum drugidisk.raw
```

Vsakič je dobil drugačno varnostno vsoto. Potem je poizkusil z ukazoma:

```
mount -o ro prvidisk.raw /mnt
mount -o ro drugidisk.raw /mnt
```

Računalnik mu je javil, da v sliki ni znanega datotečnega sistema. (i) Zakaj bi lahko dobil različne varnostne vsote? (ii) Je bil njegov postopek pravilen? Če da, zakaj? Če ne, katere podatke je izgubil? (iii) Kako lahko preveri, kateri razdelki so (bili) na diskih, ne da bi dostopal do samih diskov?