

Digitalna forenzika 2020/21

Pisni izpit 6. veliki traven 2021

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 postavljena nedoločeno in zahtevajo postavljanje predpostavk za natančen odgovor. Pri slednjem bodite natančni, saj natančnost prinese več točk. Načelni odgovori ne prinesejo vseh točk.

Edina dovoljena komunikacija je z uporabo pogovora (*chat*) s profesorjem preko BBB. Če bomo posumili, da ste prepisovali, boste *moral*i opravljati ustni izpit preko BBB.

Čas pisanja izpita je 75 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

1. naloga:

VPRAŠANJA: Osnove.

- A) Digitalni dokazi se lahko med zbiranjem slučajno spremenijo ali odstranijo ali pa za to poskrbijo storilci, ne da bi pri tem prišlo do očitnih znakov spremembe. Katere značilnosti digitalnih dokazov blažijo to težavo? Izberite pravi odgovor in ga utemeljite.
- (a) Digitalne dokaze je mogoče natančno podvojiti in kopijo je mogoče pregledati, kot da je original.
 - (b) Ko zločinci poskušajo uničiti digitalne dokaze, lahko kopije in z njimi povezani ostanki ostanejo na mestih, za katero niso vedeli da obstajajo.
 - (c) S pravimi orodji je zelo enostavno ugotoviti, ali je bil digitalni dokaz spremenjen ali prirejen, če ga primerjamo z izvirno kopijo.
 - (d) Digitalne dokaze je težko uničiti s preprostim brisanjem ali formatiranjem in jih je mogoče obnoviti.
 - (e) Vse od naštetega.
- B) Butalska policija je prišla k Petru Zmedi, ki ima svoj poštni strežnik. Policija je namreč prejela prijavo, da naj bi Peter preko svojega strežnika pošiljal nadlegovalno pošto. Peter zatrjuje, da nima nič pri tem, ampak da je za vsem skupaj znani nebodigatreba Cefizelj, ki da je izrabil njegov poštni strežnik. (i.) Zapišite dve hipotezi, kako bi podkrepili Petrovo trditev in kako bi ju dokazali. (ii.) Recimo, da je v resnici za opisanim primerom Cefizelj. Kakšno vlogo je potem v tem primeru imel Petrov strežnik: predmeta, osebka ali orodja. Utemeljite odgovor.
- C) Peter Zmeda je dobil nalogo, naj pregleda več strežnikov z operacijskim sistemom Arch Linux. Predvsem mora pregledati systemske dnevnike (*system logs*). (i.) V katerem imeniku se systemski dnevniki običajno nahajajo? (ii.) Peter je opazil, da na nekaterih strežnikih manjkajo pričakovane datoteke z dnevniki, saj baje takšno shranjevanje beležnic ni več moderno. Če ne syslog, kateri program skrbi za dnevnike na sodobnih sistemih? Kako bi na takšnem sistemu Peter pregledal dnevnike? (iii.) Ali lahko strežnik, kjer za beleženje skrbi rsyslogd, pošilja dogodke na strežnik, kjer zanje skrbi syslog-ng? Kakšne težave lahko v takšnem primeru pričakujemo? Odgovor utemeljite.

2. naloga: Datotečni sistemi.

VPRAŠANJA:

- A) Peter je postal pravi umetnik. Sedaj bi rad posnel prvi slovenski film v visoki ločljivosti, kjer bo en kader trpeče matere brez reza trajal več kot tri leta. Film bo zajemal s kamero, ki bo podatke po mreži pošiljala naravnost na računalnik, na katerem bo imel več diskov.
- (i.) Katere tehnologije lahko uporabi, če bo imel v računalniku več enakih diskov, pri čemer noben posamezni disk ne bo dovolj velik, da bi nanj spravil celoten posnetek? Naštete vsaj 4. (ii.) Katere od teh tehnologij lahko uporabi, če bodo diski različnih velikosti? (iii.) Če bo izdelal varnostno kopijo filma, kako lahko preveri, da je enaka originalu?
- B) Recimo, da v OS Windows premaknemo datoteko v okviru istega zvezka (*volume*). Kaj se zgodi s podatkom o zadnjem dostopu do datoteke? Utemeljite odgovor.
- C) Čas, ki se beleži s posameznimi datotekami, predstavlja metapodatek. Časovne značke najdemo na različnih mestih. Najprej seveda med metapodatki shranjenimi v datotečnem sistemu, včasih pa je časovna značka vključena tudi med podatki v sami datoteki.

Tokrat imamo opravka z datoteko `na-plesu.jpg`, ki je shranjena v `ext3` datotečnem sistemu. V datoteki je fotografija Luka Kratkohlačnice, kako z neznanim dekletom plešeta dunajski valček. Luka trdi, da je bila slika posneta v soboto zvečer in da dokazuje, da nima nič z nezaslišano krajo soli iz mestnih butalskih skladišč, ki se je prav tako zgodila v soboto zvečer okoli 9h. Luka tudi trdi, da je sliko shranil na računalnik že v soboto pred polnočjo.

Ko je forenzik Bučka pregledal datotečne metapodatke, je ugotovil, da je bila datoteka s sliko v resnici ustvarjena v soboto zjutraj ob 9h. (i.) Kje natančno je shranjen metapodatek o ustvarjanju datoteke? (ii.) Ocenite, kako *verodostojen* je podatek, ki ga je Bučka našel. Utemeljite svojo oceno. (iii.) Je potem možno, da je bila slika posneta na sobotnem večernem plesu? Zapišite ustrezno hipotezo, ki bo utemeljila to možnost ter opišite, kako bi jo dokazali.

3. naloga: Forenzika mobilnih naprav in omrežij.

VPRAŠANJA:

- A) Peter Zmeda je dobil sliko, ki prikazuje njegovo izbranko Rozamundo, kako poljublja neznano rožo. V navalu ljubosumja je sliko naložil na spletno storitev, ki mu je povedala, da je bila slika ustvarjena leta 1920 v mestu Temir-Han-Šura, Republika zveze narodov severnega Kavkaza. (i.) Na osnovi katerih podatkov bi lahko storitev določila datum izdelave slike? Je tem podatkom mogoče verjeti? (ii.) Katero orodje bi lahko uporabili za branje vseh tovrstnih

podatkov? (iii.) Poleg datuma in lokacije naštejte še vsaj dva podatka, ki ju lahko dobite v sliki.

- B) Pametni telefon se dejansko sestoji iz dveh računalnikov. (i.) Naštejte pet (vrst) podatkov, ki jih najdemo na SIM kartici. (ii.) Če želimo preveriti verodostojnost podatkov, jih lahko poiščemo še kje drugje ter jih nato primerjamo. Za vsakega od zgornjih petih (vrst) podatkov zapišite vsaj še eno mesto, kje bi ga lahko našli.
- C) Peter je dobil v upravljanje star strežnik, za katerega je prej skrbel Jože T. V `/home/joze/.bash_history` je naletel na vrstico: `telnet localhost sple` Ko je dani ukaz za šalo pognal, je presenečen dobil odgovor.

```
peter@slovnica:~/$ telnet localhost sple
Trying ::1...
Connected to localhost.
Escape character is '^]'.
GET / Od nekdanj lepe so strani nam slovele 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. zgleden administrator, ki samo ljubi slovenski jezik? Utemeljite odgovor.

4. naloga: Preiskava.

VPRAŠANJA:

- A) Peter Zmeda je dobil za nalogo, naj pregleda disk računalnika, na katerem je sistem GNU/Linux. Na svojem delovnem računalniku je sistem disk zaznal kot `/dev/sdb`. Ustvaril je imenik `preiskava`, v katerem bo pregledoval datoteke. Da bi prišel do res vseh datotek in časovnih značk, je izvedel naslednje zaporedje ukazov:

```
dd if=/dev/sdb of=slikadiska.raw
mount -o ro,nojoliet -t ext4 /dev/sdb1 /mnt
cp -r /mnt/* /home/peter/preiskava
```

Za vsakega od ukazov napišite, kaj je storil narobe. Lahko naštejete tudi več napak.

NAMIG: Zastavica `-r` pomeni rekurzivno kopiranje.

- B) Analiza dokaznega gradiva je ena od faz forenzičnega procesa. (i.) Katere faze so pred njo in čemu je vsaka od njih namenjena? (ii.) Zakaj je analiza tako pozno v procesu in ne, recimo, takoj na mestu zločina? Utemeljite odgovor. (iii.) Običajno analizo izvedejo forenziki po nalogu organov pregona. Jo lahko izvede še kdo drug? Kdaj v kazenskem postopku se to običajno zgodi in zakaj?
- C) Kakšna je razlika med digitalno forenzično preiskavo in analizo?