

Digitalna forenzika 2021/22

Pisni izpit 13. rožnik 2022

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena. Literatura je v papirni obliki ali na elektronski napravi, ki ni povezana z drugimi napravami.

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. Čas pisanja izpita je 75 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) Ali so digitalni dokazi lahko neposredni (vzpostavijo dejstva) ali so zgolj posredni (namigujejo na dejstva)? Utemeljite odgovor s primerom.
- (a) Lahko so zgolj posredni zaradi prepada med njimi in dogodki, ki jih dokazujejo.
 - (b) Lahko so tudi neposredni, če jih zajame, obdela in predstavi certificiran strokovnjak.
 - (c) Lahko so tudi neposredni, tipično s kombinacijo več posrednih.
 - (d) Lahko so zgolj posredni zaradi kratke zgodovine digitalne forenzike.
- B) (i.) Opišite kaj je to Locardov princip. (ii.) Nekdo je namestil na Petrov računalnik virusni program. Opišite dva primera konkretne udejanitve Locardovega principa.

NAMIG: Bodite zelo konkretni v svojem odgovoru.

- C) Peter Zmeda je dobil nalogo, da pregleda strežnik z operacijskim sistemom *Windows Server 2012*. Da bi pregledal dnevniške zapise (*event log*), je, kot smo to počeli na vajah, poizkusil uporabiti program *GrokEVT* na OS Debian GNU/Linux 10.0. (i.) Zakaj menite, da je imel z uporabo *GrokEVT* težave? (ii.) Kateri program oziroma knjižnico bi pod Linuxom (še?) lahko uporabil za pregledovanje danega strežnika? (iii.) Kateri program bi za pregled dnevniških zapisov uporabili na operacijskem sistemu *Windows Server 2012*?

2. naloga: Diskovna forenzika.

VPRAŠANJA:

- A) Peter Zmeda bi rad sestavil diskovje, na katero bo lahko spravil veliko podatkov. Diskov bo imel precej - vsaj 12. Rad bi, da diskovje preživi odpoved vsaj enega diska. (i.) Katere vrste RAID lahko uporabi? (ii.) Za dve vrsti RAID navedite, koliko odstotkov kapacitete bo izgubil. (iii.) Nekateri sodobni datotečni sistemi omogočajo, da se datotečni sistem razširi na več fizičnih diskov - funkcionalnost RAID je torej vgrajena v datotečni sistem, ni več ločena od njega. Navedite primer takšnega datotečnega sistema.
- B) Peter Zmeda uporablja CHS naslavljanje za trdi disk z naslednjimi parametri: 1024 cilindrov, 256 glav, 63 sektorjev in velikost sektorja 512 bajtov, Izberite za kako velik disk gre in koliko sektorjev ima ter utemeljite svoj odgovor:

	A	B	C
Velikost diska	7,875 GB	15,75 MB	128 MB
Skupno število sektorjev	16 515 072	63	63
	D	E	F
Velikost diska	7,875 GB	15.75 MB	128 MB
Skupno število sektorjev	63	16 515 072	16 515 072

- C) Forenzik Peter Zmeda preiskuje dva diska, od katerih je na enem datotečni sistem NTFS in na drugem `ext3` in na obeh je našel datoteko z identično vsebino. Sedaj bi Peter rad ugotovil, na katerem od diskov je bila datoteka najprej in na katerega je bila nato prekopirana. Datoteka vsebuje navodilo za rop banke in je shranjena kot `odt` dokument. (i.) Opišite tri različne pristope, na podlagih katerih lahko ugotovi, kje je bilo besedilo najprej. Utemeljite svoje odgovore. (ii.) Recimo, da na podlagi vseh treh načinov Peter ugotovi, da je bila datoteka izvirno na NTFS disku. Kako verjetna je ta trditev? Utemeljite odgovor.

3. naloga: Forenzika mobilnih naprav in omrežij.

VPRAŠANJA:

- A) Peter Zmeda si je omislil telefon podjetja *Apple*. Po dobrem tednu uporabe je razbil zaslon. Na srečo je prej na svojem računalniku ustvaril varnostno kopijo podatkov na telefonu. (i.) S katerim programom na *OS Microsoft Windows* izdelamo varnostno kopijo podatkov na *iPhone*? (ii.) Peter je prišel do varnostne kopije, vendar vsebuje čudno poimenovane datoteke. Kako so določena imena teh datotek? (iii.) Peter ne bi rad obnovil celotne vsebine telefona, temveč bi rad na nov telefon prenesel le imenik / kontakte. Ali to sploh lahko stori? Utemeljite odgovor.
- B) Policija je pri preiskavi zločina naletela na celični telefon. Med SMS sporočili na telefonu je našla sporočilo, ki vsebuje navodilo kako storiti zločin. (i.) Policija bi rada preverila, če je telefon osumljenčev. Predlagajte tri različne načine, kako lahko to naredi. (ii.) Ko je le povezala telefon z osumljencem, je ta dejal, da je sporočilo dobil po tem, ko se je zločin že zgodil in da ga je sploh prvič prebral pred nekaj minutami. Ali lahko policija ovrže osumljencevo izjavo? Kako, če da in zakaj ne, če ne.
- C) (i.) Med čem slika ARP (lahko izberete tudi več možnosti) in (ii.) opišite konkreten primer uporabe preslikave v forenzičnem postopku.

- | | |
|----------------------------------|-----------------------------------|
| 1 IP naslovi in MAC naslovi. | 3 Ethernet in ATM MAC naslovi. |
| 2 IP naslovi in številkami vrat. | 4 MAC naslovi in številkami vrat. |

4. naloga: Preiskava.

VPRAŠANJA:

- A) Peter Zmeda je dobil za nalogo, naj pregleda disk računalnika, na katerem je sistem Windows 10. 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:

```
cat slikadiska.raw > /dev/sdb
mount slikadiska.raw /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) Peter Zmeda je šel med zasebne detektive in dela mu ne zmanjka. Zadnji primer zadeva butalsko županjo Špelco, ki je niso videli že cel dan. Zakoni v Butalah so takorekoč enaki kot v Sloveniji in pri odgovoru bodite pozorni na dolžnost oziroma pooblastila. (i.) Kaj lahko po uradni dolžnosti naredi butalski policaj glede Špelce? Utemeljite odgovor. *Zakaj* veljajo takšna pravila? (ii.) Ali lahko Peter naredi kaj drugega? Zakaj da oziroma ne?
- C) Priprava načrta aktivnosti ter pridobitev potrebnih virov ter materialov sodi v kateri korak digitalne preiskave? Utemeljite odgovor.