Digitalna forenzika
(2022/23)
Pisni izpit 4. velikega travna 2023

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 90 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. Ko ocenjuje verodostojnost digitalnih dokazov, preiskovalca zanima, ali je računalnik, na katerem so bili ustvarjeni dokazi, deloval normalno in še ena od spodnjih možnosti. Katera in zakaj ostali odgovori niso pravilni?

1. Ali obstaja sum, da je nekdo lahko dokaze pokvaril.
2. Ali so bili dokazi pravilno zaščiteni med prenosom.
3. Ali so mediji, na katerih so bili dokazi, kompatibilni z opremo forenzikov.
4. Ali je bila analiza gradiva narejena kot je zahteval tožilec.

2. Eden od osnovnih pogojev sprejemljivosti dokaznega gradiva je, da brez potrebe ne napeljuje na zaključke. (i.) Opišite primer takšnega gradiva in utemeljite kako napeljuje. (ii.) Kateri so preostali štirje pogoji sprejemljivosti gradiva?

3. Peter Zmeda sledi najnovejšim trendom, zato bo za zapisovanje dogodkov na svojem sistemu uporabil *systemd-journald*. Slišal je, da so dnevniški zapisi sedaj nekje imeniku */var/log/journal*. Tam je našel kup datotek s končnico *.journal*. Namerava jih pregledati s programom *less*. (i) Bo uspešen? Če da, kako bi lahko našel pojavitve besede "*trend*" znotraj datoteke? Če ne, zakaj? (ii) Peter bi rad vseeno še naprej uporabljal *syslog-ng* za zbiranje podatkov. Ali lahko uporablja obenem *systemd-journald* in *syslog-ng* na istem računalniku? (iii) Kako je pri protokolu *syslog*, opisanem v RFC5424, poskrbljeno, da se dogodki ne izgubijo?

Naloga 2. *Datotečni sistemi.*
VPRAŠANJA:

1. Pri hišni preiskavi butalskega nepridiprava Cefizlja je policija zasegla kar nekaj podatkovnih nosilcev, ki pa so bili različno formatirani. SSD je bil formatiran kot NTFS, USB ključek kot FAT in trdi disk kot ext-3. Na vseh treh nosilcih so našli datoteko s sliko Šprince Maroglje. Sedaj se sprašujejo, katera od treh različic je original in kateri sta kopiji. (i.) Postavite svojo hipotezo o tem in opišite postopek, kako bi preverili, ali je vaša hipoteza pravilna. (ii.) Ključno vlogo bodo odigrali metapodatki. Kateri vse podatki nastopajo na posameznem datotečnem sistemu in v kakšni povezavi so z metapodatki na preostalih datotečnih sistemih?

2. Mikrosoftova Okna vsebujejo VSS - *Volume Shadow Copy*. Kaj ta storitev omogoča in kako?

1. Izdelavo varnostnih kopij NTFS datotečnih sistemov.
2. Izdelavo varnostnih kopij posamezne datoteke.
3. Izdelavo varnostnih kopij razdelkov na disku.
4. Skrivanje gesel (shadow).

3. Peter Zmeda je v pregled dobil diske dveh računalnikov. Prvi je bil v delovni postaji, na kateri je delal Cefizelj. Od njegovih sodelavcev je izvedel, da je Cefizelj za svoj domači imenik uporabljal datotečni sistem NFS. Drugi je bil v računalniku, na katerem je baje deloval datotečni strežnik podjetja. (i) Kako (s katerimi ukazi) bi Peter lahko z diska delovne postaje dobil datoteke, ki jih je Cefizelj shranjeval? (ii) Kako bi ugotovil, kateri datotečni sistem so uporabljali na strežniku? (iii) Kako (s katerimi ukazi) bi Peter lahko preveril, ali je Cefizelj res uporabljal NFS, ali pa so se morda sodelavci motili?

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

1. S katerim ukazom ugotovimo, katera domena je vezana na IP 212.235.188.20 in kaj nam povedo preostali trije ukazi?

1. `whois 212.235.188.20`
2. `dig -t ptr 20.188.235.212.in-addr.arpa`
3. `ip domain get 212.235.188.20`
4. `dig -t ptr 212.235.188.20.in-addr.arpa`

2. Orodje `sockstat` pri uporabi stikala `-l` vrne vse vtičnike, na katere se lahko priključi odjemalec. Peter je ukaz preveril na butalskem strežniku in dobil naslednji odgovor, ki ga upoštevajte nalogi.

```
@butale:> sockstat -l
bind named 904 514 udp4  192.168.126.1:53      *:*
bind named 904 515 udp4  192.168.125.1:53      *:*
```

(i.) Kakšen je id procesa, ki čaka na odjemalca in zakaj? (ii.) Ali je izpis kombinacija odgovorov z dveh strojev ali je možno, da prihaja z enega stroja? Utemeljite odgovor. (iii.) Kaj vsebujeta prva stolpca izpisa?

3. Peter Zmeda preiskuje podatke z mobilnega telefona. `sqlitebrowser` mu pri pregledu datoteke `contacts2.db`, ki jo je skopiral s telefona, javlja napako. (i) S katerim ukazom / kako bi lahko ugotovil, ali gre res za datoteko `sqlite`? (ii) Peter sumi, da je nekaj narobe s pravicami. Preveril je, da ima datoteko pravico brati. Kakšne pravice še potrebuje, če želi z orodjem `sqlite3` pregledati datoteko? (iii) Peter je slišal, da so Android telefoni navadni računalniki, na katerih teče Linux. V pregled naj bi dobil vse podatke s telefona, a nikjer ni našel domačega imenika njegovega uporabnika. Kje so običajno shranjeni podatki uporabnika na Androidnih telefonih? Kako so urejeni po imenikih?

Naloga 4. *Preiskava.*
VPRAŠANJA:

1. Priprava načrta aktivnosti ter pridobitev potrebnih virov ter materialov sodi v kateri korak digitalne preiskave? Opišite konkreten primer priprave in pridobitve.

1 Raziskava in analiza.
2 Ohranjanje.
3 Pregledovanje/identifikacija.
4 Priprava.

2. Eden temeljnih konceptov je Koncept (razumnega) pričakovanja zasebnosti. Luka Kratkohlačnica ima svoj e-poštni nabiralnik pri ButaleOL. (i.) Kako zadeva opisani koncept zadeva Jureža Pismouka, ki je sistemski administrator poštnega strežnika na ButaleOL? Utemeljite odgovor. (ii.) Peter Zmeda je dobil sodni nalog, da lahko pregleda pošto, ki jo je prejel Gregor Copataka, ki ima svoj poštni nabiralnik prav tako pri ButaleOL. Kako Petra zadeva zgornji koncept? Odgovor je večplasten in ga tudi utemeljite.

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/sdc1 of=prvidisk.raw
sha512sum /dev/sdc
cat /dev/sdd1 > 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 pri tem ni javil nobene napake. (i) Zakaj je dobil različne varnostne vsote? (ii) Je bil njegov postopek pravilen? Če da, zakaj? Če ne, katere podatke je izgubil? (iii) Pod `/mnt` je dobil samo vsebino drugega diska. Je prvega sploh uspel priklopiti? Kaj se je zgodilo z vsebino prvega diska?