Digitalna forenzika 2012/13
Pisni izpit 11. rožnik 2013

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.

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: Najširša definicija digitalne forenzike pravi, da zadeva (digitalni) računanalanik v takšni ali drugačni obliki. Po Parkerju lahko računalnik nastopa v štirih različnih vlogah in ena od teh je kot orodje za pripravo in/ali izvedbo zločina.

VPRAŠANJA:

1. Katere so ostale tri vloge ter pri vsaki na kratko opišite primer nastopanja.
2. Opišite primer zločina, kjer računalnik (recimo brskalnik) nastopa kot orodje za pripravo in/ali izvedbo zločina ter kako bi forenzično zbrali podatke za preiskavo v vašem primeru.
3. Peter Zmeda je na, mestu zločina našel telefon – Nokia N900. Rad bi prišel do vseh kontaktov, ki jih je imel lastnik na njem. Uspešno si je skopiral domači imenik uporabnika in se premaknil v imenik, kjer so shranjeni kontakti:

   ```
   peter/najdena-nokia/user/.osso-abook/db> ls
   addressbook.db   index_first_last.db  index_last_first.db
   log.0000000001   fre1.changes.db     index_full_name.db
   index_nick.db     running_id.db       index_email.db
   index_im_jabber.db  index_phone.db    tp-cache
   ```

   V kakšnem formatu, menite, so shranjeni podatki? Kako bi lahko do njih prišli? Napišite zaporedje ukazov. Ni nujno, da uporabite ravno ukaze, ki smo jih uporabili na vajah (lahko pa jih).
4. Kdo lahko izvaja digitalno forenzično preiskavo?

2. naloga:

VPRAŠANJA:

1. Posebna značilnost datotečnega sistema NTFS je, da pri datoteki obstajata pojem velikosti datoteke in pojem konca datoteke. (i.) V čem se razlikujeta (opišite primer)? (ii.) Zakaj je načrtovalec predvidel oba pojma (opišite primer uporabe)? (iii.) Kako mora biti forenzik pozoren na obstoj obeh pojmov?
2. Peter Zmeda je dobil v roke edini disk iz računalnika pokvarjenega zlikovca. Priklopil ga je na računalnik in takoj izdelal sliko:

   ```
   > dd if=/dev/sdb of=tat-racunovodja.img
   ```

   Nato je izračunal vsoto md5 slike:

```
> md5sum tat-racunovodja.img
484be6f1d548e6999551ab6e050a0405  tat-racunovodja.img
```

Preveril je, da se disk pri zapisu ni pokvaril:

```
> md5sum /dev/sdb
484be6f1d548e6999551ab6e050a0405  /dev/sdb
```

Sliko in vsoto md5 je nato poslal Rozamundi Žingelj v analitičnem oddelku. Rozamunda je ustvarila virtualni stroj z dodanim diskom iste velikosti, kot je bil originalni. Nanj je posnela podatke, ki jih je dobila od Petra:

```
> cat tat-racunovodja.img > /dev/sdb
> rm tat-racunovodja.img
> md5sum /dev/sdb1
7eb49377177c9038a703f382df624d79  /dev/sdb1
```

(i.) Kje vse je lahko prišlo do napake? (ii.) Kateri podatki so se najverjetneje izgubili? Jih lahko dobi nazaj?

3. Je kopija trdega diska, ki smo jo pridobili tako, da smo skopirali vse datoteke vseh datotečnih sistemov, ustrezna kot digitalni dokaz? Utemeljite odgovor.

3. naloga: Omrežja in forenzika.

VPRAŠANJA:

1. Ena od občutljivih komponent stikal in usmerjevlanikov je tabela MAC naslovov – *Content addressable memory (CAM) table*. (i.) Kaj točno je shranjenega v tej tabeli (MAC naslovi ne bo dovolj)? (ii.) Kako bi lahko napadalec napadel tabelo in dosegel nedovoljen dostop? (iii.) Kakšno sled bi forenzik iskal po izvedenem napadu?

2. Peter Zmeda sumi, da mu nekdo brska po računalniku. Da se ne bi osramotil, se je odločil, da iz zgodovine svojega brskalnika pobriše vse, kar bi ga lahko osramotilo. Predvsem bi rad izbrisal vse strani, ki v URL vsebujejo besede `MLP`, `pony` ali `donald`, ostale pa bi obdržal.

   Kako naj to najlaže stori? Ni potrebno, da napišete konkretne ukaze. Peter za brskanje po spletu uporablja FireFox.

3. Med čem slika ARP?

4. naloga:

VPRAŠANJA:

1. Kdo so udeleženci kazenskega postopka in opišite vlogo vsakega od njih? Forenzik lahko nastopa kot kdo v kazenskem postopku?

   Ena od nalog kazenskega postopka je tudi zaščita zasebnosti posameznika. Opišite vsaj dva primera zaščite zasebnosti.

   NAMIG: Na predavanjih smo našteli sedem udeležencev.

2. Peter Zmeda se je odločil, da napiše svoj prvi virus. Virus naj bi se zagnal iz MBR.

   (i.) Kakšna je največja dolžina virusa, ki si jo Peter lahko privošči? Utemeljite odgovor. Upoštevajte, da je virus lahko razbit na več delov.

   (ii.) Peter se je odločil, da svoj virus stestira. Pognal je naslednji ukaz:

   ```
   > dd if=virus.mbr of=/dev/sdb
   ```

   Velikost `virus.mbr` pri tem je bila 300B. Je s tem ukazom izgubil kake podatke?

   (iii.) Virus je zloben in vedno pobriše CHS zapis začetka 2. razdelka. Napišite ukaz, ki naredi varnostno kopijo podatkov, ki jih virus uniči ter ukaz, ki dane podatke spet zapiše na disk. Za vse točke naj vaš ukaz shrani manj kot 310B podatkov.

3. Na kaj morajo biti preiskovalci pozorni pri pregledu SSD diskov? Naštejte vsaj tri elemente in pri vsakem dodajte razlago, čemu morajo biti pozorni.