Digitalna forenzika 2011/12
Pisni izpit 17. kimavec 2012

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.

Želimo vas posebej opozoriti, da večina odgovorov zahteva utemljitev. V utemeljiti morate prepričati ocenjevalca. da v resnici razumete svojo odločitev.

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: _____

1. naloga:

VPRAŠANJA:

1. Tožilec trdi, da je obtoženi zagrešil zločin, ki ga je skrbno načrtoval in načrte vestno shranjeval. Na sodišču odvetnik zaslišuje kriminalista, ki je vodil ogled mesta zločina. Slednji potrdi, da na mestu zločina niso našli nobenega digitalnega dokaza, ki bi podkrepil tožilčevo trditev. Kaj lahko zaključi odvetnik na podlagi tega neobstoja dokaza? Utemeljite odgovor.

2. Kako zagotavljamo avtentičnost dokaza v postopku raziskave? Navedite vsaj tri oblike zagotavljanja.

3. Peter Zmeda je dobil v roke edini disk iz računalnika pokvarjenega zlikovca Cefizlja. Priklopil ga je na računalnik in takoj izdelal sliko, izračunal vsoto md5 slike ter na koncu preveril, da se disk pri zapisu ni pokvaril:

   ```
   peter-01> dd if=/dev/sdb of=tat_racunovodja.img
   peter-02> md5sum tat_racunovodja.img
   484be6f1d548e6999551ab6e050a0405  tat_racunovodja.img
   peter-02> 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:

   ```
   rozi-01> cat tat_racunovodja.img > /dev/sdb
   rozi-02> rm tat_racunovodja.img
   rozi-03> md5sum /dev/sdb1
   7eb49377177c9038a703f382df624d79  /dev/sdb1
   ```

   Ups!! Kje vse je lahko prišlo do napake? Kateri podatki so se najverjetneje izgubili? Jih lahko dobi nazaj?

2. naloga: Peter Zmeda sumi, da je Cefizelj ponovno ušpičil nekaj slabega. Dokazi o tem naj bi se nahajali pri njem doma. Peter sicer gleda takšne in drugačne kriminalke, toda ve, da mora dobiti najprej nalog za preiskavo, če želi do dokazov.

VPRAŠANJA:

1. Kje lahko dobi Peter nalog za preiskavo? Navedite vsaj pet dejstev, ki jih mora Peter napisati na zahtevo za nalog za preiskavo, da ga bo lahko dobil.

2. Peter je ugotovil, da je primer, ki ga preiskuje podoben enemu prejšnjih primerov, ki jih je že nekoč preiskoval. Zato se odloči, da bo nadaljeval preiskavo na enak način. Kako imenujemo takšen način preiskave?

3. Napišite zaporedje ukazov v lupini `bash`, ki:
   (a) ustvari na disku sliko razdelka velikosti 20M;
   (b) v sliki ustvari datotečni sistem FAT;
   (c) premakni se v svojem računalniku v imenik `/mnt`;
   (d) ustvari imenik `/mnt/mojdisk` (ta ukaz naj bo čim krajši);
   (e) priključi prej ustvarjeno sliko na `/mnt/mojdisk`;
   (f) na sliki diska ustvari datoteko `bla.txt`;
   (g) v datoteko shrani domači imenik uporabnika, ki ukaz poganja (seznam datotek iz domačega imenika);

3. naloga: Petra Zmedo so poklicali iz podjetja *Urban in družabniki*. V podjetju sumijo, da nekdo pokradel njihovo intelektualno lastnino – industrijska špijonaža pač. Med preiskavo je Peter ugotovil, da je nekdo na računalnik priključil pomnilniško palčko (ključek) in z njega skopiral program, ki omogoča varno (popolno) brisanje datotek.

VPRAŠANJA:

1. Predložite natančen načrt preiskave, ki naj jo izvede Peter. Pri tem se osredotočite na sam potek raziskave in ne na tehnične podrobnosti ter orodja.

2. Tehnično gledano. Peter je ugotovil, da je na preiskovanem računalniku operacijski sistem Windows z datotečnim sistemom NTFS na disku. Kako lahko na tem sistemu varno (popolno) pobrišemo datoteko?

3. Peter Zmeda res nima sreče. V službi mu dovolijo le uporabo potrjenih orodij. Na žalost med njimi ni orodja `fdisk`. Na srečo ima na voljo šestnajstiški urejevalnik in izpisovalnik (*hex editor* in *hexdump*). Z njim bo pregledal in popravil prvi sektor na disku. Za vas pomembni del sektorja imate v prilogi.

   Peter mora spremeniti tip drugega razdelka iz Linux na NTFS. Katere vrednosti mora zapisati na katera mesta na disku? Izpolnite tabelo v prilogi.

   Koliko razdelkov sploh je na disku?

4. naloga:

VPRAŠANJA:

1. Tri od faz preiskave so: shranjevanje dokaznega gradiva; raziskovanje dokaznega gradiva; in analiza dokaznega gradiva. Opišite omenjene faze, ko imamo opravka z mobilnimi napravami. Pri tem poudarite dejstva v vsaki

od faz, ki so posebna za mobilne naprave in jih ne najdemo pri drugih napravah.

Vprašanje je odprtega tipa in zahteva predvsem razmislek in smiselne odgovore. Zato jih dobro utemeljite.

2. Kaj je osnovni razlog, da se za dostop do SIM kartice ne uporablja preprosto ugibanje PIN kode?

3. Kako s pomočjo šifriranja na ravni bločne naprave ustvarimo skrite nosilce in kaj je namen tega početja?