Digitalna forenzika 2011/12
Pisni izpit 5. mali srpan 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. Kadar zlikovci uporabljajo računalnik pri svojem zlodelu, nam lahko to tudi pomaga pri preiskavi. Naštejte tri *bistveno različne* primere ter za vsakega od njih zapišite realističen scenarij ter obrazložite kako nam raba računalnika s strani zlikovca pomaga v preiskavi.

2. Na sodišču nadobudni mlajši odvetnik želi potrditi neko predpostavko v procesu in zato naroči digitalnemu preiskovalcu, da usmeri raziskavo v določeno smer. Je to dovoljeno? Utemeljite odgovor.

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 *hex editor* in *hexdump*. Z njima bo pregledal in popravil prvi sektor na disku. V pomoč so vam podatki na dodatnem listu.

   Peter mora spremeniti tip prvega razdelka iz *NTFS* na *Linux Swap*. Poleg tega razdelek ne sme več imeti nastavljene zastavice za zagon (*bootable flag*). Katere vrednosti mora zapisati na katera mesta na disku?

   Koliko razdelkov sploh je na disku?

   Disk je velik skoraj 100M (98703360 bajtov). Koliko prostora je „prostega“ pred prvim sektorjem prve particije? Koliko za zadnjim sektorjem zadnje particije?

2. naloga: Peter Zmeda je dobil računalniški disk, na katerem so morda podatki pomembni za preiskavo. Kriminalisti sumijo, da je Cefizelj na disk skril podatke o kraji oslove sence v Butalah in to v pisni dokument, ki ga je natisnil, poskeniral in shranil nekam na disk.

VPRAŠANJA:

1. Zapišite vsaj pet hipoteze, kje se lahko nahaja dokument s podatki, utemeljite svoje hipoteze ter čim podrobneje opišite kje ter kako jih boste preverili. Na disku je *ext2* datotečni sistem.

2. Peter je takoj izdelal kopijo podatkov na disku z ukazom:

   ```
   dd if=/dev/sdb1 of=oslovskaSenca.img bs=512
   ```

   Nato je disk poslal v uničenje, kjer so ga zdrobili na drobne koščke ter pretalili. Za vsak slučaj, da se je znebil potencialnih virusov, je še ponovno

namestil sistem na svoj računalnik, pri čemer je nedotaknjeno ohranil sliko diska v datoteki `oslovskaSenca.img`.

Sedaj mora Peter zajete podatke analizirati.

(i) S katerim zaporedjem ukazov lahko ugotovi, kakšne so bile velikosti razdelkov na disku? (ii) S katerim zaporedjem ukazov lahko dostopa do datotek, zajetih v `oslovaSenca.img`? (iii) Na kaj je Peter pri zajemu pozabil? Kako bi zajem izvedli vi? Napišite zaporedje ukazov.

3. Peter Zmeda je postavil poštni strežnik in se je odločil, da bo shranjeval pošto na `maildir` in ne na `mbox` način. Kje se nahaja odhajajoča pošta?

3. naloga: Peter Zmeda je od kriminalistov dobil naslednji kos zapisov o Cefizljevem zločinskem skrivanju podatkov o kraji oslovske sence. Tokrat kriminalisti sumijo, da je Cefizelj pred svojo zlikovsko dejavnostjo pridobil podatke o vremenski napovedi v Butalah. Kriminalisti so Petru dostavili sedaj še zapise o celotni omrežni aktivnosti Cefizljevega računalnika `oslovskaSenca.traffic` – pomeni celoten promet. Seveda, datoteko `oslovskaSenca.img` s kopijo diska ima Peter še od prej.

VPRAŠANJA:

1. Zapišite vsaj pet hipoteze, kje se lahko nahajajo podatki o pridobivanju vremenskih podatkov, utemeljite svoje hipoteze ter čim podrobneje opišite kje ter kako jih boste preverili.

2. Pri preiskavi mobilnih naprav na forenzika preži vrsta morebitnih nevarnosti. Ali je dejstvo, da omrežni operaterji lahku nudijo dodatne zgodovinske podatke o dejavnosti naprave takšna nevarnost? Kaj pa povezanost mobilne naprave v omrežje in omogočenost oddaljenega dostopa? Utemeljite svoja odgovora.

3. Napišite zaporedje ukazov v *bash*, ki na konec datoteke `bla.txt` doda vsebino okoljske spremenljivke `HOME`, nato pa vzporedno ustvari dve datoteki, poimenovani `2kilo.bin` in `3kilo.txt`. Velikost `2kilo.bin` naj bo 2048 bajtov, velikost `3kilo.txt` pa 3072 bajtov.

4. naloga:

VPRAŠANJA:

1. Pridobivanje podatkov z mesta zločina je zapleten postopek. Recimo, da ste kriminalist in bi želeli dobiti vse dokaze, katere boste dostavili Petru (dokazi iz prejšnjih dveh vprašanj). Natančno opišite postopek kje in kako boste pridobili disk ter kje in kako boste pridobili podatke o omrežnem prometu. Bodite pozorni, da morate podatke tehnološko in legalno pravilno zajeti ter tudi verodostojno shraniti.

2. Kriminalist Peter se pripravlja na izpraševanje prič. Tako se je odločil, da bo med izpraševanjem od priče zahteval najprej priznanje krivde. Poleg tega bo zahteval tudi ključ za dostop do podatkov na kriptiranem disku. Ocenite njegov namen ter utemeljite odgovor.

3. Če nekdo na disku opazi podatke, ki izgledajo naključno, lahko sklepa, da gre za šifrirane podatke in nas poskuša prisiliti, da jih odšifriramo. Da se temu izognemo, lahko uporabimo tehnike za verjetno zanikanje (*plausible deniability*). Ustvarjanje nosilcev za takšne podatke omogoča orodje `Truecrypt`. Razložite princip delovanja teh nosilcev.