Digitalna forenzika 2015/16
Pisni izpit 3. veliki traven 2016

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. Poleg tega so nekatera vprašanja namenoma postavljeno nedoločeno in zahtevajo postavljanje predpostavk za natančen odgovor. Pri slednjem bodi natačni, saj natančnost prinese več točk. Načelni odgovori ne prineso vseh točk.

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:

VPRAŠANJA: Osnove.

1. Katero napako učbenik navaja kot najbolj pogosto napako, ki se dela pri zajemu dokazov in nato prepreči uporabo dokaza na sodišču. Opišite jo in utemeljite zakaj gre za napako.

2. Omenjali smo, da računalnik lahko nastopa v štirih vlogah v kazenskem dejanju. (i) Zapišite vsaj dve od štirih vlog. (ii) Za vsako od zapisanih vlog opišite po en konkreten primer. (iii) Za vsakega od primerov zapišite hipotezo, kako je prišlo do kazenskega dejanja ter kako bi to hipotezo preverili.

3. Peter Zmeda je v obdelavo dobil ključek USB. Vtaknil ga je v računalnik, ga priklopil (mount) in ugotovil, da je na njem (samo) datotečni sistem ISO9660. Šele potem se je spomnil, da bi moral namesto z diskom delati s sliko diska.

   Ali je s priklopom spremenil podatke na ključku? Utemeljite odgovor. Če bi hotel narediti sliko ključka in jo priklopiti, katere ukaze bi lahko uporabil? Napišite točno zaporedje ukazov. Privzemite, da je sistem ključek zaznal kot `/dev/sdc`.

2. naloga: Diskovni sistemi. Peter Zmeda je našel naslednjo zbrisano datoteko na disketi:

```
  Name    .Ext    ID     Size    Date     Time    Cluster  76  ARSHDV
_REENF~1  DOC   Erased  19968  5-08-03  2:34 pm    275        A-----
```

VPRAŠANJA:

1. Koliko gruč (*cluster*) je zasedala omenjena datoteka? Utemeljite odgovor.

2. Peter bi rad shranil kar je ostalo od zbrisane datoteke v eno datoteko na svoj disk. Peter poganja Linux operacijski sistem in ima ext3 datotečni sistem, ki je nastavljen tako, da vodi celovit dnevniški zapis (*journal*). (i) Koliko `inode` vozlišč bo uporabil? Utemeljite odgovor. (ii) Zapišite in utemeljite kakšni zapisi vse se shranijo v dnevniku? Pri opisu transakcije navedite, kateri bloki se kdaj shranijo.

3. Tokrat je Peter Zmeda je kupil dva diska po 3TB. Nanju bi rad spravil vsaj 5TB podatkov. Vsaj 500GB podatkov ima takšnih, da jih nikakor ne bi rad izgubil - še posebej, če odpove eden od diskov. (i) Predlagajte vsaj dve

tehnologiji, ki ju lahko uporabi. (ii) Za eno od njiju natančno opišite, kako naj na diskih ustvari razdelke, datotečne sisteme, ... – da bo zadoščeno njegovim zahtevam.

3. naloga: Mobilne naprave in omrežna forenzika ter sistemske zabeležke. Cefizelj se je včeraj s svojim računalnikom priključil na brezžično omrežje. Ker Peter raziskuje zločin, pri katerem je poznan IP naslov storilca, mora ugotoviti, kateri IP naslov je uporabljal Cefizljev računalnik. Na razpolago ima naslednja možna mesta, kjer lahko išče IP naslov: (i) dnevnik na usmerjevalniku; (ii) tabela dodeljenih naslovov strežnika DHCP; (ii) izpis ukaza `ifconfig` na Cefizljevem računalniku; in (iv) `syslog` na Cefizljevem računalniku.

VPRAŠANJA:

1. Za katero od mest pregled verjetno ni smiselen? Utemeljite odgovor.

2. Za dve od smiselnih mest (i) zapišite hipotezo *kje* in *kako* bi iskali podatke o IP naslovu ter (ii) zakaj menite, da je vaša hipoteza smiselna – zakaj je smiselno tam iskati podatke.

3. Poleg tega se je Cefizelj nekako prikradel do računalnika Petra Zmede, na katerem je imel Peter nameščen operacijski sistem Microsoft Windows XP. Cefizelj je uspel zagnati sistem z USB prenosnega diska in želi Petru ukrasti gesla. (i) Kateri imenik si mora prekopirati? (ii) Katero datoteko? (iii) Ali lahko gesla preprosto prebere iz datoteke?

   V imeniku z gesli je tudi večina registra. (iv) Katerega dela registra ni v tem imeniku? (v) Kje se preostali del registra lahko nahaja?

4. naloga: Izvajanje preiskave in digitalna forenzika na slikah.

VPRAŠANJA:

1. Eden od korakov forenzične preiskave je zavarovanje mesta zločina. (i) Kateri po vrsti je in kaj je njegova naloga?

   NAMIG: „*Zavarovanje mesta zločina,*“ seveda ni pričakovan odgovor. Napišite, kaj to pomeni.

   V Butalah je prišlo do hudega zločina. Nepridipravi so z butalskega strežnika ukradli slavni recept za proizvodnjo soli. Strežnik je bil nameščen v zelo dobro zavarovanem prostru in do njega je bil možen dostop samo preko računalniškega omrežja. Pa še tukaj je bil strežnik za požarno pregrado. Peter sumi na Tepanjce, a ne ve, kako bi lahko ukradli recept. (ii) Opišite,

kako naj Peter zavaruje mesto zločina, da bo ohranil čim več dokaznega gradiva. Utemeljite svoj odgovor.

NAMIG: Natančnejši kot bo vaš odgovor, več točk boste dobili.

2. Naš prijatelj Peter Zmeda je med preiskavo prišel do slike, da kateri je osumljenec med tem, ko izvaja kaznivo dejanje. Slika je v formatu JPEG in je bila, če verjamemo metapodatkom, ustvarjena z mobilnim telefonom. Katere od naslednjih lastnosti slike lahko uporabite, da preverite, ali je bila vsebina slike predelana: (i) značke EXIF; (ii) geometrijsko popačenje; (iii) DCT koeficienti; (iv) indikatorji dvojne kompresije; (v) tehnike razpoznavanja obraza; (vi) kromatična aberacija; (vii) povprečna osvetlitev slike; (viii) linearnost odziva slikovnega senzorja? Utemeljite odgovor.

3. Peter Zmeda je umetnik, ki se v prostem času ukvarja z risanjem slik v nizki ločljivosti (*pixel art*). Objavlja jih na spletnem portalu v formatih BMP in PNG. Zadnje čase na portalu dobiva reklame, iz katerih je očitno, da oglaševalci vedo, da Peter živi v Butalah. (i) Kako, menite, da oglaševalci uganejo, kje se Peter nahaja? Utemeljite odgovor. (ii) Kaj lahko stori s slikami, da bo oglaševalcem otežil delo?