Digitalna forenzika 2013/14
Pisni izpit 1. mali srpan 2014

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 predpostav za natančen odgovor. Pri slednjem bodi 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: _____

1. naloga:

VPRAŠANJA: Imamo tale košček zagotovo veljavne dokumentacije:

> INT 10h / AH = 0Eh - teletype output.
> INPUT:
> AL = character to write.
> BL = (graphics modes only) foreground color number
> COMMENT:
> This functions displays a character on the screen, advancing the cursor and scrolling the screen as necessary. the printing is always done to current active page.

1. Napišite program v 80286 zbirniku, ki bi, če bi se nahajal v MBR, na zaslon izpisal besedo `NONA`. Pri tem si lahko pomagate s spodnjim odlomkom kode. Lahko privzamete, da je grafični vmesnik v tekstovnem načinu.

```
error:
        popw    %si
2:
        lodsb
        movb    $0x0e, %ah
        movb    (BIOS_page), %bh
        movb    $0x07, %bl
        int     $0x10           /* May destroy %bp */
        cmpb    $10, %al        /* Newline? */
        jne     2b
```

2. 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.

3. 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.

2. naloga: Diskovni sistemi.

VPRAŠANJA:

1. Posebnost datotečnega sistema NTFS je, da pri datoteki obstajata pojma *velikost datoteke* in *konec 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 napisal svoj prvi neškodljiv virusni program, za katerega želi, da se skrije nekam na disk. Zamislil si je, da se bo virus skril v datoteko `virus` v imenik `imenik`, ki se ga lahko zgolj bere (*read only*). Napišite vsaj *dva* razloga zakaj je to slab način skrivanja.

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

3. naloga: Mobilne naprave.

VPRAŠANJA:

1. Na predavanjih smo spoznali IMSI. (i.) Kaj je to? (ii.) Recimo, da bi naredili orodje, ki bi bilo sposobno slediti in beležiti IMSI v vsaki celici. Bi bilo to povsem legitimno in legalno? Utemeljite odgovor.

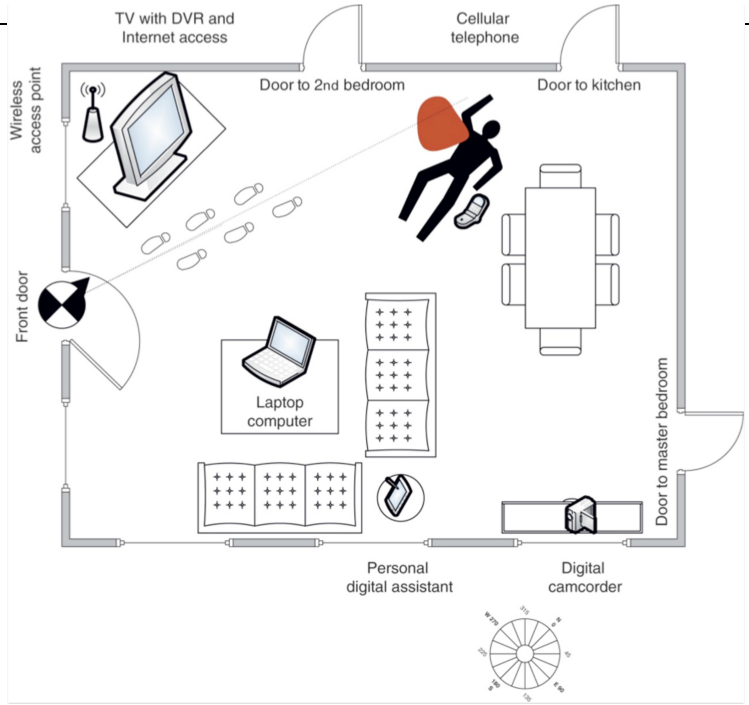
2. Pri preiskavi prenosnih naprav je možno podatke iskati ne samo na prenosni napravi. Navedite vsaj še tri vire podatkov in utemeljite svoje odgovore.

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 s shranjenimi 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
   ```

(i.) V kakšnem formatu, menite, so shranjeni podatki? (ii.) Kako bi lahko do njih prišli? (iii.) Napišite zaporedje ukazov. Ni nujno, da uporabite ravno ukaze, ki smo jih uporabili na vajah (lahko pa jih).

4. naloga: Peter Zmeda pride na mesto zločina na sl. 1, ki smo ga že srečali na



Slika 1: Mesto zločina.

predavanjih.

VPRAŠANJA:

1. Preiskovalec Peter je našel na prenosniku na sl. 1 slike z otroško pornografijo. (i.) Zapišite tri hipoteze, kako so prišle na prenosnik, (ii.) utemeljite hipoteze ter (iii.) zapišite, kako bi jih preverili.

2. Kateremu napadu so podvržene naprave, ki zaupajo ostalim napravam zgolj na podlagi njihovega IP naslova? Utemeljite odgovor.

3. 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.