Digitalna forenzika 2012/13
Pisni izpit 27. 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 75 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. V kriminalistični preiskavi smo spoznali pojem *dokazne verige*. i.) Kaj je to dokazna veriga; opišite pojem in njen pomen v procesu kriminalistične preiskave. ii.) Kdaj pravimo, da se je dokazna veriga pretrgala? iii.) Recimo, da je pretrgana dokazna veriga pri fizičnih in pri digitalnih dokazih. Katero pretrganje menite je bolj usodno in kdaj – utemeljite odgovor.

2. Na računalniku hranite pomembne podatke na šifrirani particiji (nosilcu), sistemski nosilec (kjer je naložen OS) pa ni skrit niti šifriran. Po potrebi pripnete (`mount`) šifrirani nosilec v datotečni sistem in delate s podatki na njem (urejate word dokumente, pregledujete fotografije, ...). Naštejte tri primere, ki so bistveno med seboj različni, kako lahko pri tem scenariju podatki „odtečejo“ na nešfiriran sistemski nosilec.

3. Ali so digitalni dokazi lahko neposredni (vzpostavijo dejstva) ali so zgolj posredni (namigujejo na dejstva)? Utemeljite odgovor.

2. naloga: Zagon računalnika.

VPRAŠANJA:

1. Peter ne zaupa računalnikom v kiber-kavarni KK, kjer redno dostopa do svojih spletnih storitev. Zato si je pripravil pomnilniško palčko, s katere naloži svoj operacijski sistem. Z drugimi besedami, ko pride v KK, ponovno zažene računalnik in naloži operacijski sistem neposredno s palčke. Žal je zadnjič pozabil palčko na mizi, medtem ko je šel na stranišče. Ko se je vrnil nazaj ni več vedel, ali ni morda Cefizelj naložil na palčko kaj takšnega, da bi mu škodoval. i.) Opišite scenarij, kako bi lahko Cefizelj pridobil s popravljanjem podatkov na palčki Petrova gesla za dostop do spletnih storitev. ii.) Kako naj se Peter zavaruje v bodoče, če bi ponovno pozabil palčko na mizi.

   NAMIG: Večino točk boste dobili s preprostim odgovorom, če pa boste upoštevali še zaščito zaščite palčke – dobite vse točke.

2. Napišite *čim krajši* program v 80286 zbirniku, ki bi, če bi se nahajal v MBR, na zaslon izpisal besedo `MAMA`. 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
```

In temle koščkom 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.

3. Kaj je to zagonsko zaporedje (*boot sequence*)?

3. naloga: Omrežja in forenzika.

VPRAŠANJA:

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

2. Peter Zmeda je na ulici našel SD kartico z nekaj slikami. Ko jo je prinesel domov, je z ukazom exiv2 pregledal podatke o eni od njih:

```
peter@racunalnik:SDKARTICA$ exiv2 photo.JPG
File name       : photo.JPG
File size       : 2742987 Bytes
MIME type       : image/jpeg
Camera make     : Apple
Camera model    : iPhone 4S
Image timestamp : 2013:05:03 11:50:38
Exposure time   : 1/120 s
Aperture        : F2.4
```

```
Exposure bias   :
Focal length    : 4.3 mm (35 mm equivalent: 35.0 mm)
Subject distance:
ISO speed       : 80
Macro mode      :
Image quality   :
Exif Resolution : 3264 x 2448
Thumbnail       : image/jpeg, 11584 Bytes
Copyright       :
```

Peter bi kartico zelo rad vrnil lastniku. Ali je z zgornjim ukazom res izpisal vse metapodatke, ki bi se lahko nahajali na kartici? Če ne, kako bi prišel do ostalih? Naštejte še vsaj pet različnih metapodatkov, ki se lahko skrivajo v .jpg datoteki.

3. Ali lahko uporabimo forenzična orodja, ki niso specializirana za mobilne naprave, za pregled datotek na mobilnih napravah? Utemeljite odgovor.

4. naloga:

VPRAŠANJA:

1. Med drugim smo srečali tudi predkazenski postopek. i.) Kdo ga izvaja in kakšen je njegov namen? ii.) Ena od dejavnosti predkazenskega predkazenskega postopka je zbiranje dokazov. Ali lahko le-tega policija izvaja na osumljenčevem domu? Utemeljite odgovor.

2. Peter Zmeda se je med poletjem na počitnice spravil na bližnji vzhod. Ko je stopil nekaj korakov iz hotela, ga je razgled na izsušeno pokrajino povsem prevzel. Ko pa je naredil nekaj fotografij, se je iz peska izmotala postava do zob oboroženega vojaka v kamuflaži. Vojak je zahteval, da Peter takoj izbriše vse podatke. Ko se je Peter obotavljal, mu je vojak iz rok iztrgal fotoaparat, se sprehodil po menuju in na koncu izbral možnost FORMAT CARD.

   Po prihodu domov se je Peter takoj lotil obnavljanja podatkov na kartici. Z Interneta je potegnil nekaj zastonjskih programov in jih uporabil na kartici. Noben od programov mu ni našel ničesar, eden od njih pa mu je podatke delno „popravil“ – neuspešno je obnovil datotečni sistem tako, da so postala vidna imena datotek.

   i.) Kaj je Peter storil narobe? Kako bi moral postopati pri obnavljanju podatkov?

Po neuspešnem iskanju slik je Peter odnesel kartico prijatelju, ki se ukvarja z digitalno forenziko. Le-ta mu je uspel obnoviti prvih 32kb vsake datoteke. Originali so bili seveda večji – Peter ima fotoaparat z več kot 16MP senzorjem nastavljen tako, da mu dela JPEG in RAW (TIFF) slike. ii.) Naštejte vsaj dva načina, kako bi Peter iz obnovljenih podatkov lahko izvedel, kaj je bilo na kateri sliki? Utemeljite odgovora. iii.) Katere podatke bi še lahko našel na začetku datoteke? Naštejte vsaj tri.

3. Kaj je (eden ali več) glavni namen preiskave elektronske naprave (po ZKP)?