Digitalna forenzika 2011/12
Pisni izpit 18. rožnik 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: Pri preiskavi računalnika je Peter Zmeda našel med zabeležkami naslednjo vrstico:

```
98.242.111.223 - - [18/Jun/2012:20:44:19 +0200]
  "GET /goods4you HTTP/1.1" 404 207 -" "Mozilla/4.0
  (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

Poleg tega je ugotovil še naslednje:

```
PZ> nslookup 98.242.111.223
Server:  192.168.127.1
Address:  192.168.127.1#53
Non-authoritative answer:
223.111.242.98.in-addr.arpa name = c-98-242-111-223.hsd1.ga.comcast.net.
Authoritative answers can be found from:
in-addr.arpa nameserver = c.in-addr-servers.arpa.
in-addr.arpa nameserver = d.in-addr-servers.arpa.
in-addr.arpa nameserver = b.in-addr-servers.arpa.
in-addr.arpa nameserver = a.in-addr-servers.arpa.
in-addr.arpa nameserver = f.in-addr-servers.arpa.
in-addr.arpa nameserver = e.in-addr-servers.arpa.
a.in-addr-servers.arpa has AAAA address 2001:500:13::73
c.in-addr-servers.arpa has AAAA address 2001:43f8:110::10
d.in-addr-servers.arpa has AAAA address 2001:13c7:7010::53
```

Na zaslišanju je Peter dejal: „Iz dokaznega gradiva sklepam, da je nekdo dostopal do spletne strani iz podjetja `comcast.net`.“

VPRAŠANJA:

1. Opišite vse podatke v vrstici iz zabeležk.
2. Pojasnite podatke, ki jih je Peter pridobil s pomočjo ukaza `nslookup`.

   NAMIG: Pri obeh vprašanjih se ne pričakuje po eno stran odgovora, a le čim bolj temeljiti boste v odgovoru, več točk dobite.
3. Komentirajte Petrovo izjavo na sodišču.
4. Napišite zaporedje ukazov v *bash*, ki bo najprej na zaslon izpisalo

   ```
   Katero je najpogostejše slovensko ime na J?
   ```

   Pet sekund kasneje naj v datoteko `ime.txt` zapiše `Janez` in na zaslon `Jan`.

2. naloga: Delo z diskom.

VPRAŠANJA:

1. Poseben del diska predstavlja razdelilna tabela (*partition table*). Kje se nahaja ter katere podatke vsebuje?

   NAMIG: Morda si pomagate s samo obliko tabele.

2. Med predavanji smo srečali različne oblike kriptiranja podatkov na disku. Poznamo dve ravni. Kateri? Za vsako raven naštejte po tri orodja, ki omogočajo kriptiranje.

3. Peter Zmeda je naredil svoj prvi virusni program. Za sedaj je povsem neškodljiv, le želi ga narediti tako, da se bo skril nekam na disk. Žal je njegova ideja precej slaba, saj se je virus skril v datoteko `virus` v imenik `imenik` in to tako, da je dovoljeno zgolj branje imenika (*read only*). Zakaj je ta način skrivanja slab? Napišite vsaj *dva* razloga.

4. Predlagajte Petru, kako naj se virus *bolje* in *bolj uporabno* skrije.

3. naloga: Peter Zmeda pride na mesto zločina in tam najde: računalnik, tiskalnik, povezovalne kable, kabel do telefonske vtičnice ter na polici nad računalnikom knjige, priročnike ter tiskalniške izpise.

VPRAŠANJA:

1. Kaj je vaš prvi korak pri obravnavi mesta zločina? Ali bi zasegli računalnik? In če da, bi zasegli tudi tiskalnik? Kaj pa lahko poveste o povezavah (komunikaciji) med elektronskimi elementi na mestu zločina?

   Utemeljite vsak odgovor v parih vrsticah.

2. Komentirajte trditev: „Vsak celični telefon (mobitel) ‚govori' vsaj protokol IEEE 802.15."

3. Stikalo (*switch*) je element, ki deluje na drugi plasti. Zakaj pravimo, da deluje na drugi plasti?

4. Peter je ugotovil, da ima disk v računalniku nekaj slabih sektorjev. Podatki na disku so seveda nadvse pomembni. Peter ve, da je datotečni sistem na disku ohranjen v celoti, manjkajo le nekateri bloki z vsebino datotek.

   Peter bi rad skopiral vse datoteke na nov disk, formatiran z drugačnim, boljšim in novejšim datotečnim sistemom.

   Kako naj to stori? Napišite zaporedje ukazov.

NAMIG: V pomoč izsek iz `man dd`:

```
DD(1)                                          User Commands
NAME  dd - convert and copy a file
SYNOPSIS
       dd [OPERAND]...
       dd OPTION
DESCRIPTION
Copy a file, converting and formatting according to the operands.
  bs=BYTES   read and write up to BYTES bytes at a time
  cbs=BYTES  convert BYTES bytes at a time
  conv=CONVS convert the file as per the comma separated symbol
list
  count=BLOCKS copy only BLOCKS input blocks
  ibs=BYTES   read up to BYTES bytes at a time (default: 512)
  if=FILE     read from FILE instead of stdin
  iflag=FLAGS read as per the comma separated symbol list
  obs=BYTES   write BYTES bytes at a time (default: 512)
  of=FILE     write to FILE instead of stdout
  oflag=FLAGS write as per the comma separated symbol list
....
Each CONV symbol may be:
  ascii  from EBCDIC to ASCII
  ebcdic from ASCII to EBCDIC
  ibm    from ASCII to alternate EBCDIC
  block  pad newline-terminated records with spaces to cbs-size
  unblock
         replace trailing spaces in cbs-size records with newline
  lcase  change upper case to lower case
  ucase  change lower case to upper case
  swab   swap every pair of input bytes
  sync   pad every input block with NULs to ibs-size; when used
with
         block or unblock, pad with  spaces  rather  than NULs
  excl   fail if the output file already exists
  nocreat
         do not create the output file
  notrunc
         do not truncate the output file
  noerror
         continue after read errors
  fdatasync
         physically write output file data before finishing
  fsync  likewise, but also write metadata
```

4. naloga:

VPRAŠANJA:

1. Razložite frazo: „Neobstoj dokaza ni dokaz o neobstoju.“ Podajte primer, kjer omenjena fraza pride do izraza.

2. Kot primer procesnega modela preiskave smo srečali *fizični model*. Zakaj se imenuje fizični model in naštejte vseh pet njegovih faz. Za tri faze podajte cilje digitalne preiskave.

3. Na mestu zločina smo našli prižgan računalnik, na katerega je bil preko kabla priključen celični telefon. Naštejte in utemeljite vsaj tri dejanja, ki jih moramo izvesti, da zavarujemo mesta zločina.

4. Tokrat je naša prenosna naprava celovit računalnik vključno z diskom. 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 delovanja.

```
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
```

Pomagate si lahko še z naslednjim koščkom zagotovo veljavne dokumentacije:

```
INT 10h / AH = 0Eh -- teletype output.
input:
AL = character to write.
BL = (graphics modes only) foreground color number
description:
  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.
```