Digitalna forenzika 2014/15
Pisni izpit 18. rožnik 2015

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 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. Pri klasifikaciji možnih vlog računalnika pri zločinu smo govorili o zločinih, kjer je računalnik: (i.) predmet (objekt) zločina; (ii.) dejavnik (subjekt) zločina; (iii.) orodje pri zločinu; in (iv.) uporabljen v zločinu zaradi svojih lastnosti (*symbol*). Za vsako od vlog napišite primer zločina in utemeljite svojo izbiro vloge računalnika.

2. Cefizelj je zelo previden mož in zato zasleduje Petra in še druge ljudi, ki bi lahko bile njegove morebitne žrtve. O žrtvah dela zaznamke v obliki navadnega teksta v nezasedeni prostor na koncih datotek (*file slack*). Za vsako žrtev Cefizelj na svoje skrito mesto zapiše takole vrstico:

   ```
   Danes je <IME ŽRTVE> na koordinatah <KOORDINATE>
   ob <ČAS>.
   ```

   Naprimer:

   ```
   Danes je Peter Zmeda na koordinatah
   46.149205,14.992997 ob 2014-06-11T13:02:50+0200.
   ```

   Kako bi Peter lahko našel vse tovrstne vnose? Sliko razdelka s Cefizljevim datotečnim sistemom ima v datoteki `cefizelj.raw`. Napišite konkreten ukaz ali zaporedje ukazov.

3. Kaj je eden najbolj zahtevnih vidikov Interneta v sodnem procesu? Utemeljite odgovor.

2. naloga: Peter Zmeda je dobil v preiskavo Cefizljev računalnik. V njem je našel dva diska velikosti po 1TB. Ob pogovoru s Cefizljem je izvedel, da ima Cefizelj na diskih spravljeno datoteko z načrti prve butalske podmornice in da ta datoteka zaseda vsaj 1.5TB.

VPRAŠANJA:

1. Tokrat Cefizelj ne laže. (i.) Kako bi Cefizelj lahko v enem kosu shranil tako veliko datoteko? Naštejte vsaj 4 načine / tehnologije.

2. Peter je za potrebe preizkave prepričal svoje nadrejene, da so mu omogočili nakup diska s kapaciteto 3TB. (i.) Kako naj na novem disku ustvari razdelke, da bo imel na njem sistem, s katerim bo lahko pregledal Cefizljeve diske? (ii.) Kam na novem disku bo shranil zagonski nalagalnik (bootloader)?

3. V datotečnem sistemu NTFS imamo o dolžini (velikosti) datoteke tri podatke. Kateri so ti podatki in opišite, kaj točno pomenijo.

3. naloga: Mobilne naprave in omrežna forenzika.

VPRAŠANJA:

1. V podjetju VseImamo, kjer je Peter sistemski inženir, je prišlo do vdora v strežniški sistem. Peter sumi, da je prišlo do DNS zastrupljanja (*DNS poisoning*). (i.) Kako deluje DNS zastrupljanje? (ii.) Kako lahko Peter ugotovi, če je res prišlo do tega napada? (iii.) Kako se lahko Peter v bodoče zavaruje pred tem napadom?

2. Peter Zmeda se je odločil, da bo postal pravi heker. Kot prvi korak se je odločil, da v zbirniku (*assembler*) napiše program, ki bo zagnal nek drug program. Ker ima v svojem računalniku procesor AMD Opteron FX-8150, na njem pa poganja jedro Linux 3.10-2-amd64, je program napisal za to arhitekturo. Program izgleda takole:

```
        .globl  main
main:
        mov     $0, %rsi
        mov     $0x3b, %rax
        mov     $0, %rdx
        mov     $.SH, %rdi
        movb    $0x3b, %al
        syscall
.SH:    .string "/usr/local/bin/mojprogram"
```

   (i.) Kaj bi Peter moral storiti, da bi program lahko poganjal tudi na najnovejših procesorjih podjetja Intel? (ii.) Kako bi izgledal del programa v C ali katerem koli drugem prevedenem jeziku, s katerim bi Peter storil isto? (iii.) Ali lahko s strojnim ukazom `syscall` Peter dostopa do podatkov na disku? Če da, kako? (iv.) S katerim strojnim ukazom se sistemski klici izvajajo pod Linuxom na arhitekturi i386?

   NAMIG: Ne pričakuje se, da boste na pamet poznali vloge registrov v Linux amd64 ABI ali syscall tabelo - odgovora na podvprašanji (i.) in (iii.) naj bosta splošna in naj ne bosta daljša od 4 stavkov vsak.

3. Od naslednjih nevarnosti izberite tisto, ki se vam zdi največja pri forenzični analizi mobilnih naprav: (i.) povezane v omrežje omogočajo oddaljeni dostop; (ii.) samo omrežni operaterji so tisti, ki lahko nudijo nekatere podatke, ki jih nato primerjamo s podatki z mobilne naprave; (iii.) povezovalna omrežja so tista, ki lahko vsebujejo potrebne/uporabne podatke; (iv.)

samo omrežni operaterji so tisti, ki lahko nudijo dodatne zgodovinske podatke. Utemeljite svoj odgovor.

4. naloga: Izvajanje preiskave.

VPRAŠANJA:

1. V preiskavi sta ločena postopka zbiranja in pregledovanja dokaznega gradiva ter analiza dokaznega gradiva. Zakaj, menite, je potrebno oba postopka (koraka) ločiti?

   NAMIG: Premislite, kaj bi bilo, če bi bila združena in v povezavi s postopkom nato pred sodiščem, kjer nastopata dve stranki.

2. Peter Zmeda je dobil v roke sliko starega IDE diska. Prvi sektor tega diska si lahko ogledate v prilogi. (i.) Koliko razdelkov je na disku? (ii.) Kakšna je velikost vsakega razdelka v byte-ih? (iii.) Kateri operacijski sistem se je zaganjal s tega diska? Vse odgovore utemelji!

3. SIM kartica omogoča komunikacijo celičnega (mobilnega) telefona preko GMS omrežja. (i.) Iz česa sestoji kartica (npr. pomnilnik, ...). (ii.) Opišite, kaj se zgodi, ko vključite svoj celični telefon? Pri tem upoštevajte, da imate sestavne dele: SIM kartica, telefon, omrežje in kako poteka komunikacija med njimi (kaj kdo komu pošlje).