Digitalna forenzika 2019/20
Pisni izpit 19. rožnik 2020

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.

A) V katere kategorije lahko po Parkerju spada računalnik, vpleten v zločinu? Podajte primer za vsako od njih.

B) Dokazno gradivo je osrednji element v forenziki in za dokaz o pravilnem rokovanjum z njim uporabljamo pojem dokazne verige. (i) Kje se dokazna veriga prične in kje konča? (ii) Zapišite primer vsebine posameznega člene dokazne verige in razložite, kaj dokazuje vaš primer. (iii) Zakaj mora biti dokazna veriga nepretrgana? Kje in kako bi lahko kdo izkoristil pretrganost verige?

C) Peter je v roke dobil star disk. Ob priklopu je disk javil, da ima 256 glav. Ko ga je odprl, je videl le eno ploščo in ročico, ki se ob njej premika. (i) Koliko bralno/pisalnih glav dejansko ima njegov disk? (ii) Zakaj bi disk lagal glede števila glav? Odgovora utemeljite.

2. naloga: Datotečni sistemi.

VPRAŠANJA:

A) Petru se je pokvaril eden (`sda`) od dveh diskov (`sda` in `sdb`), ki ju je imel uspešno povezana v RAID 1. V navalu panike je poizkusil priklopiti disk in z njega pobrati podatke, a mu ni uspelo. Kot `root` je pognal:

```
mkdir /resitev; mount /dev/sdb /resitev
```

(i) Ali do podatkov sploh še lahko pride? (ii) V splošnem opišite postopek, kako bi to storil. (iii) Narišite skico, kako so lahko organizirani podatki na disku `sdb` (razdelki, datotečni sistemi in podobno).

B) Meta podatki o datotekah vsebujejo tudi različne časovne podatke. (i) Zapišite, kateri časovni podatki so prisotni tako v `ufs` kot pri NTFS datotečnem sistemu. (ii) Za vsakega od naštetih podatkov zapišite kaj beleži in (iii) format zapisa.

C) (i) Kje se običajno nahaja tabela razdelkov GPT (*GUID partition table*)? (ii) Kaj pa, če se nahaja na več mestih, kje je še tedaj? (iii) Zakaj bi jo želeli imeti na več mestih?

3. naloga: Omrežna forenzika ter sistemske zabeležke.

VPRAŠANJA:

A) Stvar z butalsko soljo se zapleta. Kriminalisti so na domačem računalniku Luke Kratkohlačnice pregledali zapise in potem še zapise v usmerjevalniku. Končna ocena je bila, da je skoraj 95% IP prometa z Lukinega računalnika bilo do naslova `abc.butale.si`. Na podlagi tega se je tožilec odločil, da bo Luko obtožil kraje recepta. Lukin zagovornik seveda trdi, da je Luka nedolžen. (i) Navedite vsaj dva možna razloga, zakaj je lahko Luka legitimno tako pogosto komuniciral z omenjenim naslovom. (ii) Utemeljite odgovora.

B) Radi bi ugotovili, na katerem naslovu je bil Petrov računalnik, ko je včeraj dostopal do Interneta. Kam se nam *ne izplača* pogledati?

   - v dnevnik na usmerjevalniku;
   - izpis ukaza `ifconfig`;
   - `syslog` na Petrovem računalniku; ali
   - v tabelo dodeljenih naslovov strežnika DHCP.

   Utemeljite odgovor.

   NAMIG: Utemeljitev naj vključuje razlog, zakaj bi tja pogledal ali ne.

C) Peter Zmeda je od svojega strežnika (`bor`) po `syslog` protokolu dobil sporočilo:

```
<63> 1 2016-10-11T22:14:15.003Z bor pif 2234  Kako tega nisem
videl?
```

   Recimo, da je sporočilo povsem v skladu z RFC 5424. (i) Ali mora Peter kaj storiti, ali lahko sporočilo zanemari? Utemeljite odgovor. (ii) Za katero funkcionalnost na sistemu skrbi program s PID 2234? Utemeljite odgovor.

4. naloga: Prenosne (mobilne) naprave.

VPRAŠANJA:

1. Na mestu zločina se je nahajal tudi celični telefon. Telefon je še vključen in tehniki so z njega že pobrali prstne odtise. Nato so telefon predali Petru Zmedi v nadaljnjo obdelavo. Ravno v trenutku, ko Peter dobi telefon, pride na telefon SMS sporočilo. Kaj vse naj Peter naredi, da bo čim bolje zavaroval dokaze?

   NAMIG: Navedite vsaj tri ukrepe in jih utemeljite.

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

3. Peter Zmeda je v roke dobil prenosni računalnik osumljenca Cefizlja iz Butal. Peter naj bi disk pregledal. Iz računalnika je izvlekel disk in ga priklopil na svojo delovno postajo. Pri tem vprašanju zapišite konkretne ukaze, ki naj jih Peter uporabi z znanimi orodji, ki ste jih uporabili na vajah.

   (i) Kako naj naredi sliko diska? Recimo, da strojni opremi povsem zaupa in bo za istovetnost diska poskrbel nekoč kasneje.

   (ii) Potem, ko je naredil sliko diska, so njegovi nadrejeni računalnik vrnili lastniku. Peter je pozabil, kakšni razdelki so bili na disku. Kako lahko spet pride do tega podatka?

   (iii) Izkazalo se je, je bil na disku le en razdelek, formatiran z datotečnim sistemom NTFS. S katerim zaporedjem ukazov bi lahko prišel do seznama datotek v njegovem korenskem imeniku? Recimo, da je imel Miran na svojem računalniku datoteko `C:\SKRITO\MOJAOVCKA.JPG`. Kako bi si jo Peter skopiral v svoj domači imenik?