Digitalna forenzika 2016/17
Pisni izpit 8. veliki traven 2017

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) Peter Zmeda pregleduje disk, na katerem je datotečni sistem ext3. Kot priden forenzik je najprej izračunal varnostno vsoto:

```
dd if=/dev/sdb1 | md5sum
```

Nato je disk priklopil:

```
mount -o ro /dev/sdb1

dd if=/dev/sdb1 | md5sum
```

Varnostni vsoti sta različni! (i) Zakaj? (ii) Kaj pomeni stikalo `-o ro`? (iii) Kaj bi moral storiti, da bi disk pregledal, ne da ga pokvari? Napišite zaporedje ukazov.

B) Kaj pri datotečnem sistemu NTFS pomeni angleška kratica VDL? Kako lahko z uporabo VDL skrivamo podatke?

C) Izrezovanje (*carving*) je eden od postopkov iskanja podatkov v drugih podatkih (npr. datoteki). Recimo, da smo slišali, da so podatki, ki jih moramo izrezati, program napisan v lupini `bash` ali slika v formatu jpg. (i) Zapišite hipotezo, ki jo boste preverjali. (ii) Kako boste hipotezo preverili? Utemeljite svoj odgovor.

3. naloga: Forenzika mobilnih naprav, omrežij ter sistemske zabeležke.

VPRAŠANJA:

A) Peter je v roke dobil Cefizljev računalnik. Sedaj bi rad ugotovil, ali se je Cefizelj priklapljal na butalsko lokalno mrežo. (i) Ali lahko iz usmerjevalne in ARP tabele na računalniku ugotovi, če je bil računalnik na butalski mreži? Če da, kako? Če ne, zakaj ne? (ii) Kje bi Peter še lahko iskal podatek o tem, ali je bil ta računalnik prisoten na omrežju? Bodite čim natančnejši v odgovoru in utemljite, zakaj tam. (iii) Kako bi brez dostopa do strežnikov pretentali Petra, da bi mislil, da je bil Cefizeljev računalnik na omrežju, čeprav je v resnici šlo za računalnik nekoga drugega.

B) Po protokolu `syslog` smo dobili sporočilo s `PRI 27`. Ali je nujno? Utemeljite odgovor.

   NAMIG: Pojasnite, kako se `PRI` izračuna in kaj vrednost 27 pomeni.

C) Petru na enem od računalnikov ne deluje mreža – računalnik ne dobi IP naslova. Ostali računalniki delujejo normalno, problematični računalnik pa na drugih mrežah deluje normalno. Peter sumi, da je problem v strežniku DHCP. Katere datoteke na strežniku naj pregleda? Naštejte vsaj tri in zakaj.

4. naloga: Izvajanje preiskave in zlonamerno programje.

VPRAŠANJA:

A) Preiskovalec je našel na osumljevčenem domačem računalniku slike z otroško pornografijo. Kaj lahko predpostavlja?

   (a) nekdo je iz interneta uspel neavtorizirano naložiti slike na računalnik;
   (b) od domačih je z USB palčke ali s spleta naložil slike na računalnik;
   (c) nekdo od domačih ima slike na svojem telefonu in jih je zložil na računalnik;
   (d) nič od naštetega

   Utemeljite odgovor.

B) V Butalah imajo tudi policaja. Že dolgo je sumil Cefizlja kraje recepta butalske soli. Tako se je odločil narediti pri njem preiskavo in je v preiskavi zasegel Cefizljev prenosni računalnik. Ker se mu je zelo mudilo, ga je spravil v kovinski kovček in odnesel domov. Zvečer, ko so vsi spali, je iz računalnika vzel disk in ga priklopil na svoj računalnik, na katerem poganja Ubuntu, ki ga je prepoznal kot 2. SATA disk. Disk je pregledal in našel sliko prototipa prve butalske podmornice. Po krajšem iskanju je našel še načrte podmornice ter seznam delov, iz katerih je sestavljena. Takoj je z ukazom

```
md5sum /dev/sdb1 > checksum.txt
```

izračunal varnostno vsoto, disk odklopil in postavil na polico v predsobi, da ga ne bi zjutraj pozabil. Zjutraj je disk pobral in odnesel v službo, kjer ga je spravil v varen sef.

Kaj vse je policaj storil narobe in kako bi preiskavo izpeljal pravilno?

C) Peter je napisal naslednji program:

```
void foo() {
    long int* f;
    f = &f + 1;
    printf("\%lx\n", *f);
}
int main() {
    foo();
}
```

Ko ga je prevedel na svojem računalniku (64-bitni Ubuntu na Intel Core2) in pognal, je dobil izpis:

```
7ffdf9c32c80
```

(i) Kaj izpisana vrednost predstavlja? (ii) Zakaj se vrednost ob vsakem zagonu spremeni? (iii) Narišite shemo naslovnega procesa tipičnega programa in označite, kje je izpisana vrednost. Shema naj vključuje, kje približno je program, kje podatki in kje sklad.