Digitalna forenzika 2018/19
Pisni izpit 13. rožnik 2019

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) Pri hišni preiskavi smo našli prižgan, a zaklenjen računalnik. Predpostavljamo tudi, da je disk zašifriran. Kako lahko postopamo? Utemeljite odgovor.

B) Za to, da je dokazno gradivo sprejemljivo na sodišču, mora zadoščati petim osnovnim pravilom. (i.) Katera so ta? Utemeljite za vsako od pravil, zakaj mu mora dokazno gradivo zadoščati. (ii.) Za tri pravila navedite primer, ko gradivo ne zadošča glede na to pravilo.

C) Peter Zmeda sumi, da mu je nekdo vrinil virus v zagonski ram-disk (*initial ram disk*, `initrd`). (i.) Je to sploh mogoče storiti? Če ne, zakaj? Če da, kako? (ii.) Peter bi se rad znebil initrd-ja. Je to sploh mogoče? Če ne, zakaj? Če da, kako?

2. naloga: Datotečni sistemi.

VPRAŠANJA:

A) Peter Zmeda je dobil v preiskavo disk z datotečnim sistemom XFS. Da ne bi uničil podatkov, ga je priklopil samo za branje (`-o ro`). Nato je skopiral vse datoteke. (i.) Katere podatke je uničil? (ii.) Na katere podatke je pozabil? (iii.) Kako bi moral disk v resnici pregledati? Zapišite zaporedje ukazov in vsakega utemeljite.

B) Čemu je enako število možnih vnosov tabele FAT? Utemeljite odgovor.

C) Dnevniški zapisi so se pojavili kot del datotečnega sistema iz več razlogov. (i.) Opišite vsaj eno težavo, ki jo dnevniški zapisi odpravljajo na sistemu. Kako? (ii.) Pri dnevniških zapisih `ext` datotečnega sistema obstajajo 4 vrste blokov. Katere? (iii.) Dva od štirih blokov nikoli ne nastopita hkrati v isti transakciji. Katera in zakaj? (iv.) Skicirajte particijo in označite, kje se v njej nahajajo dnevniški zapisi.

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

VPRAŠANJA:

A) Peter je v pregled dobil računalnik z OS Windows XP. Zanima ga samo, kdo in kolikokrat se je prijavljal na računalnik. Ima orodje, ki sprejme pot do datotečnega sistema in izpiše vse prijave. Na žalost si ne more privoščiti, da bi skopiral celoten disk, saj je le-ta velik 4T in skoraj povsem zaseden, Peter pa ima le približno 500G prostora. Katere datoteke mora dejansko skopirati? Odgovor utemeljite.

B) Najznačilnejša lastnost mobilih naprav je, da so mobilne. (i.) Opišite tri načine, kako lahko Peter Zmeda ugotovi, kje se nahaja mobilna naprava osumljenca. (ii.) Za vsakega od načinov opišite, kje naj Peter išče podatke o nahajanju naprave. (iii.) Peter sumi, da se je Luka Kratkohlačnica po mobilnem telefonu pogovarjal s strašnim razbojnikom Cefizljem. Zapišite pet hipotez, kje in kako lahko Peter preveri, če je to res. Seveda, hipoteze morajo biti smiselne.

NAMIG: Pri tem odgovoru je potrebno nekaj domiselnosti.

C) Kateremu napadu so podvržene naprave, ki zaupajo ostalim napravam zgolj na podlagi njihovega IP naslova? Utemeljite odgovor, še najbolje tako, da opišete, kako se takšen izvede.

4. naloga: Izvajanje preiskave.

VPRAŠANJA:

A) Peter Zmeda je v preiskavo dobil računalnik z dvema diskoma. Korenski imenik oziroma `C:` je na njegovi delovni postaji, na kateri poganja Linux, dostopen kot `/dev/md0`. Naredil je kopijo korenskega imenika, ne da bi datotečni sistem prej priklopil. Nato je preiskavo izvajal na tej kopiji.

Na sodišču so ga obtožili, da je uničil dokaze. Jih je res? Če da, kako? Kaj bi moral storiti, da jih ne bi? Če ne, kaj je moral storiti, da lahko dokaže, da jih ni?

B) Kateri od naštetih principov *ni* osnovni princip, katerega se morajo držati digitalni preiskovalci na mestu zločina? Utemeljite odgovor.

a.) najprej poiščemo osumljence, da ne pokvarijo dokazov;
b.) podatkov na preiskovani napravi ne spreminjamo;
c.) voditi moramo zapis o vseh dejavnostih na mestu zločina;
d.) vse našteto.

C) Obstaja več načinov oziroma modelov vodenja preiskave. (i.) Če modele posplošimo dobimo pet osnovnih korakov. Katerih? (ii.) Zamislite si neko kaznivo dejanje in ga opišite. Nato za vsakega od petih korakov zapišite tipično opravilo, ki se izvaja v njem, pri obravnavi zamišljenega kaznivega dejanja.