Digitalna forenzika 2021/22
Pisni izpit 29. rožnik 2022

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena. Literatura je v papirni obliki ali na elektronski napravi, ki ni povezana z drugimi napravami.

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 bodite natačni, saj natančnost prinese več točk. Načelni odgovori ne prineso vseh točk. Čas pisanja izpita je 75 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) Klasičen primer Locardovage principa predstavljajo prstni odtisi storilca na mestu zločina. Opredelite digitalni primer in utemeljite odgovor.

NAMIG: Prstni oddtisi natančno določajo storilca.

B) Petru je prijatelj prinesel disk, ki naj bi nekoč pripadal Mojci. Mojca je Petru všeč in Peter bi rad preveril, ali imata kake skupne iterese. Mojca običajno dela z Google Chrome ali Internet Explorerjem 8.

V katerem formatu je shranjena zgodovina brskalnikov, ki ju uporablja Mojca? Ali je mogoče, da je prijatelj v zgodovino podtaknil svoje strani, če vemo, da prijatelj računalnika ni zaganjal s tega diska? Če je to mogoče, kako bi prijatelj sploh lahko dodal vnose v zgodovino?

C) V katero od štirih kategorij (po Parker-ju) spada računalnik, na katerega je bila naložena programska oprema, ki lastniku otežuje delo, hkrati pa izvaja napade na druge računalnike? Odgovor utemeljite.

2. naloga: Diskovna forenzika.

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 in omrežij.

VPRAŠANJA:

A) Iz Tepanj v Butale teče potok, pa mu pravijo, da je reka. Ta reka je bila lepega dne zamazana z oljem. Obstajajo fotografije oljnega madeža na potoku, ustvarjene s sodobnim mobilnim telefonom. Butalci trdijo, da so bile fotografije ustvarjene v Butalah ravno dan po tem, ko so v Tepanjah iz repice olje delali. (i.) Kje vse bi lahko našli časovne značke v slikah? (ii.) Kako se določa čas, ki je v njih zapisan? (iii.) Kako se imenuje standard za zapis tovrstnih metapodatkov?

B) Pri preiskavi kaznivega dejanja, je eden ključnih dejavnikov komunikacija med posamezniki. Če, recimo, sumimo, da je oseba A vpletena v kaznivo dejanje in obstaja dokaz, da je obstajala možnost komunikacije z osebo B, potem velja pregledati tudi osebo B. (i.) Zaradi katerega principa velja opraviti pregled. Utemeljite odgovor. (ii.) Zapišite tri tehnično bistveno različne načine preverjanja možne komunikacije med mobilnimi enotami. Za vsakega zapišite, kako bi ga preverili.

   NAMIG: Pri tem odgovoru je potrebno nekaj domiselnosti.

C) Kaj omogoča napadalcu VPN? Utemeljite odgovor.

   - Izvajanje napada preko njihovega računalnika s ponarejenim IP naslovom z namenom skrivanja njihovega pravega IP naslova in geografske lokacije.
   - Izvajanje napada preko njihovega računalnika s ponarejenim MAC naslovom z namenom skrivanja njihovega pravega MAC naslova in geografske lokacije.
   - Izvajanje napada preko kompromitiranega računalnika iz oddaljene lokacije z namenom skrivanja njihovega MAC naslova in geografske lokacije.
   - Izvajanje napada preko kompromitiranega računalnika iz oddaljene lokacije z namenom skrivanja njihovega IP naslova in geografske lokacije.

4. naloga: Izvajanje preiskave in digitalna forenzika na slikah.

VPRAŠANJA:

1. Eden od korakov forenzične preiskave je zavarovanje mesta zločina. (i) Kateri po vrsti je in kaj je njegova naloga?

   NAMIG: „*Zavarovanje mesta zločina,*“ seveda ni pričakovan odgovor. Napišite, kaj to pomeni.

V Butalah je prišlo do hudega zločina. Nepridipravi so z butalskega strežnika ukradli slavni recept za proizvodnjo soli. Strežnik je bil nameščen v zelo dobro zavarovanem prostru in do njega je bil možen dostop samo preko računalniškega omrežja. Pa še tukaj je bil strežnik za požarno pregrado. Peter sumi na Tepanjce, a ne ve, kako bi lahko ukradli recept. (ii) Opišite, kako naj Peter zavaruje mesto zločina, da bo ohranil čim več dokaznega gradiva. Utemeljite svoj odgovor.

NAMIG: Natančnejši kot bo vaš odgovor, več točk boste dobili.

2. Naš prijatelj Peter Zmeda je med preiskavo prišel do slike, da kateri je osumljenec med tem, ko izvaja kaznivo dejanje. Slika je v formatu JPEG in je bila, če verjamemo metapodatkom, ustvarjena z mobilnim telefonom. Katere od naslednjih lastnosti slike lahko uporabite, da preverite, ali je bila vsebina slike predelana: (i) značke EXIF; (ii) geometrijsko popačenje; (iii) DCT koeficienti; (iv) indikatorji dvojne kompresije; (v) tehnike razpoznavanja obraza; (vi) kromatična aberacija; (vii) povprečna osvetlitev slike; (viii) linearnost odziva slikovnega senzorja? Utemeljite odgovor.

3. Peter Zmeda je umetnik, ki se v prostem času ukvarja z risanjem slik v nizki ločljivosti (*pixel art*). Objavlja jih na spletnem portalu v formatih BMP in PNG. Zadnje čase na portalu dobiva reklame, iz katerih je očitno, da oglaševalci vedo, da Peter živi v Butalah. (i) Kako, menite, da oglaševalci uganejo, kje se Peter nahaja? Utemeljite odgovor. (ii) Kaj lahko stori s slikami, da bo oglaševalcem otežil delo?