Digitalna forenzika 2013/14
Pisni izpit 12. mali traven 2014

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 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: Osnove in jezik digitalne forenzike.

VPRAŠANJA:

1. Na podlagi preostalega dokaznega gradiva Peter sumi, da je Cefizelj Johnu nakazal 100 EUR za prepovedana mamila. Pri forenzični preiskavi je našel naslednje dokaze: (i) na poštnem strežnku s Cefizljevim nabiralnikom zapis, da je Cefizelj prejel e-pošto z ID-jem 1JDSV144MNN12N1KK1 od Johna; (ii) na poštnem strežnku s Johnovim nabiralnikom zapis, da je John poslal pošto Cefizlju z ID-jem 1JDSV144MNN12N1KK1; (iii) na Johnovem računalniku datoteko, v kateri piše, da naj Cefizelj nakaže Johnu 100 EUR za prepovedana mamila; in (iv) na disku Cefizljevega računalnika dva bloka, ki nista bila del nobene datoteke, ampak sta samo vsebovala podatek, da je Cefizelj izvedel transakcijo za 100 EUR (prvi blok) in da je bila izvedena transkacija na Johnov račun (drugi blok). Petrovo poročilo vsebuje vsa zgoraj zapisana dejstva ter zaključek, ki ga je pripravil na podlagi najdenih dejstev. Zapišite ta zaključek!

2. Peter je uspel priklopiti sliko zgoščenke priklopiti na `/mnt/slika` in bi rad na njej našel vse fotografije. (i) Katero zaporedje ukazov naj uporabi, da bo našel vse datoteke s končnico `.jpg`?

   Cefizelj je pameten in je nekaterim datotekam odstranil končnico. Peter bi še vedno rad našel vse slike, tokrat celo tiste, ki niso v formatu *jpeg*. (ii) Kako naj poišče datoteke?

   NAMIG: Pri tem si lahko (ni pa nujno) pomaga z ukazom `file`. *Mimetype* JPEG datotek je `image/jpeg`.

   Med slikami je Peter našel tudi sliko Cefizlja, ko stoji pred neko hišo z vilami v rokah. Vilami, ki so jih bili Lavdonu Štimanemu ukradli pred letom! Peter bi rad Cefizlja izsledil. (iii) Kako lahko to stori, če je bila slika narejena z mobilnim telefonom z vklopljeno geolokacijo, in ali lahko tako dobljenim koordinatam zaupa? (Odgovor utemeljite.) (DODATNO) Na kakšen način je *običajno* poskrbljeno za integriteto podatkov v EXIF značkah datoteke?

3. Kakšno je razmerje med znanstveno resnico in pravno presojo? Utemeljite svoj odgovor.

2. naloga: Zagon računalnika in diskovni sistemi.

VPRAŠANJA:

1. Peter Zmeda je dobil v preiskavo sliko diska. Vodja preiskave sumi, da je nekje na disku shranjen zapis bančnega nakazila, s katerim je Cefizelj nakazal 1.000.000 EUR iz *Nacionalne banke Butal* (*NBB*) na *Prvo banko Velikega otočja* (*PBVO*). Preiskovalec ne ve v kakšni obliki je zapis (jpg, pdf, doc, ods, ...) niti ali je v samostojni datoteki. Pri oceni profila storilca pa so ugotovili, da dokument ni kriptiran niti ni skrit kjerkoli izven datotečnega sistema. Predlagajte Petru tri možna mesta, kjer naj išče dokument in kako.

2. Peter Zmeda si je kupil nov, večji disk – računalnik je nadgradil z 1T na 2T disk. Novi disk je vgradil v računalnik, ki ga je zaznal kot /dev/sdb. Nato je izvedel naslednji ukaz:

   ```
   cat /dev/sda1 > /dev/sdb1 .
   ```

   Nato je računalnik izklopil, odstranil stari disk in računalnik ponovno vklopil. Toda glej ga zlomka, računalnik se preprosto ni hotel zagnati. (i) Zakaj? Kaj bi moral Peter storiti, da bi se računalnik uspešno zagnal z novega diska?

   Ko je Peter sistem spravil v stanje, da se je končno lahko prijavil, je bil neprijetno presenečen. Ukaz `df` mu je namreč pokazal, da se količina prostega prostora na disku ni spremenila – kot bi imel še vedno le 1T disk. (ii) Zakaj je do tega prišlo in kako bi Peter ta problem odpravil?

   Ves postopek nadgradnje je Petru vzel celo popoldne. Že samo kopiranje je trajalo debelo uro. (iii) Ali obstaja kak način, da bi Peter kopiranje izvedel hitreje? Upoštevajte, da je bilo na disku zasedenih le 20% prostora.

3. Imamo datotečni sistem FAT. (i) Koliko vnosov ima tabela FAT, (ii) Kako velike so lahko posamezne datoteke in (iii) kako velik je lahko disk, da ga v celoti še lahko izkoristimo?

3. naloga: Omrežja in forenzika.

VPRAŠANJA:

1. Cefizelj se je odločil napasti spletni portal banke *NBB*, do katerega se dostopa z uporabo protokola `http`. Vendar Cefizelj pri tem noče puščati nobenih sledi ter se je odločil, da bo v vseh odhodnih paketih spremenil izvorni naslov na naslov 23.208.163.36. Napad s pretvarjanjem mu ne bo uspel. Zakaj?

2. Peter je dobil v roke Cefizljev telefon *Butaphone 3000+* – Android telefon z i7 procesorjem. Peter ve, da je Cefizelj telefon že „odklenil“ – Američani bi rekli, da je bil telefon *rooted*. (i) Katero orodje lahko Peter uporabi za dostop do podatkov na telefonu?

   Peter je tudi opazil, da ima Cefizelj na domačem zaslonu bližnjici do kar dveh brskalnikov. Prvi je vgrajen, drugega pa je Cefizelj napisal sam in se imenuje *IE4Android*. Ob pregledu datotek na telefonu se je izkazalo, da je Cefizelj za shranjevanje zgodovine uporabil datoteke v čudnem, nedokumentiranem formatu. Peter bi rad samo izvedel, katere spletne strežnike je Cefizelj obiskoval. (ii) S katerim orodjem lahko pregleda zgodovino vgrajenega brskalnika (v kakšnem formatu je shranjena)? (iii) S katerim orodjem oz. orodji lahko Peter poizkusi pregledati zgodovino IE4Android?

3. Kaj enolično identificira IMEI številka?

4. naloga: Izvajanje digitalne preiskave.

VPRAŠANJA:

1. Na predavanjih smo dejali, da digitalna preiskava sestoji iz petih korakov, od katerih sta dva *pregled* in *raziskava*. (i) Kje se izvaja vsak od njiju in (ii) v čem je osnovna razlika med njunima namenoma?

2. General Rupert Gorjača, sveže priseljen v Butale, je obtožen, da si je privoščil razmerje s Klaro Buta, ženo znanega Kozmijana Bute. Peter je dobil nezavidljivo nalogo, da poišče morebitne dokaze, ki bi lahko potrdili ali ovrgli obstoj razmerja.

   Ker ima Rupert na svojem računalniku tudi zaupne dokumente, mora biti Peter še posebej pazljiv pri pregledovanju diska Rupertovega računalnika. Pomagajte mu tako, da zanj pripravite načrt preiskave in pri tem oblikujte vsaj tri hipoteze ter načrt za njihovo preverjanje.

3. Kateri je najvišji pravni akt, ki ureja pravico do zasebnosti po slovenski zakonodaji?