Digitalna forenzika 2015/16
Pisni izpit 30. rožnik 2016

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: Osnove. Peter je napisal naslednji program, sestavljen iz dveh datotek, `main.c`:

```
#include<stdio.h>
#include "N.h"
void f() {
    int i;
    char **r;
    r=(char**)(((char*)&r) + N); /* r kaže na naslov r+N */
    for (i = 0; i < X; i++) { /* zapiši X kazalcev */
        *r += M;
        r += 1;
    }
}
int main() {
    int x = 99;
    f();
    printf("%d%% ljudi se strinja, da je bedak, kdor pravi:\n", x);
    printf("Peter, ti si car\n");
}
```

in `N.h`:

```
#define N 1
#define X 2
#define M 20
```

VPRAŠANJA:

1. Ker mu program ni všeč, bi ga rad popravil tako, da ne bi več izpisoval prve vrstice. Na žalost lahko popravlja le datoteko `N.h`. (i.) Kakšni sta najmanjša in največja smiselna vrednost za `N` in `X`? Odgovor utemeljite. (ii.) Kako bi določili konstanto `M` (ki je, mimogrede, za amd64 pravilna)?

2. Ali se lahko na sodišču kot dokaz uporabi podatke z računalnika, do katerega so imele dostop neznane osebe? Utemeljite odgovor.

3. Vsaka datoteka, ki je shranjena na računalniku, sestoji iz dveh delov podatkov. (i.) Katerih? (ii.) Pri pridobivanju datoteke z izrezovanjem ene vrste podatkov običajno ne moremo dobiti. Katerih in zakaj? Odgovor utemeljite.

2. naloga: Diskovni sistemi.

VPRAŠANJA:

1. Naštejte (i.) štiri mesta na datotečnem sistemu NTFS, kjer lahko skrijemo podatke in (ii.) za vsakega od njih opišite, kje se nahaja ter (iii.) ocenite koliko podatkov lahko skrijemo v posamezno mesto. (iv.) Med štirimi mesti se odločite za eno, ki ga je najtežje, po vašem mnenju, odkriti in utemeljite odgovor.

2. Pod OS Windows lahko disk razdelimo na več različnih načinov. Naštejte tri med njimi in jih opišite.

3. Peter Zmeda je slišal, da so manjši diski precej hitrejši od velikih. Zato si je kupil osem 500GiB diskov. Postavil jih je tako, da lahko na njih ustvari 4TiB datotečni sistem. Obenem bo njegov sistem diskov obdržal shranjene podatke tudi, če mu odpove kateri koli posamičen disk. (i.) Predlagajte vsaj tri načine, kako je lahko diske povezal. (ii.) Ali je lahko na diskih uporabil MBR?

3. naloga: Mobilne naprave in omrežna forenzika. Našega prijatelja Petra Zmedo so poklicali z Butalske Policije, da jim priskoči na pomoč. Na mestu zločina se je pojavil nek mobilni telefon. Ko je Peter butalskega policaja vprašal, za kakšen telefon gre, mu je le-ta znal samo razložiti, da gre za nek očitno cenen telefon, saj je na njem slika na pol pojedenega jabolka.

VPRAŠANJA:

1. Napišite hipotezo, ki bo vsebovala vsaj tri mesta, kjer naj Peter zajame podatke v zvezi z zločinom in utemeljite svoj odgovor.

2. Ni pa to prvič, da ima naš prijatelj Peter Zmeda opravka z mobilnimi napravami. Ondan je dobil za nalogo, da forenzično pregleda neznano mobilno napravo. Toda, ker je njegov predpostavljeni precej na kratko s proračunom, ima na voljo samo orodja namenjena forenzični analizi diskovnih sistemov. Mu bodo ta orodja kaj pomagala? Utemeljite odgovor.

3. Na vajah smo si ogledali podatke z vsaj dveh različnih telefonov. Z enega od njiju so bili pridobljeni z uporabo programa adb. (i.) Kaj pomeni kratica ADB? (ii.) Opišite, kako bi z uporabo tega programa prišli do seznama kontaktov na telefonu.

   NAMIG: Ni potrebno, da navedete točne poti do vseh datotek, je pa pomembno, kako točno bi do datotek prišli in kako bi iz njih na računalniku izluščili zanimive podatke.

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

VPRAŠANJA:

1. Pri forenzični obdelavi in obravnavi moramo spoštovati vrsto zakonskih omejitev. Ena je *pričakovana zasebnost*. (i.) Kaj to je, (ii.) opišite primer v forenzični preiskavi, ko le-ta nastopi in primer, ko ne nastopi ter (iii.) utemeljite svoja primera.

2. V okviru preiskave je butalski policaj zajel sliko Cefizlja, kako nalaga tajne butalske načrte o gojenju soli v svojo torbo. Slika je v formatu JPEG in je bila, če verjamemo metapodatkom, ustvarjena z mobilnim telefonom. (i.) Opišite kje in kako so verjetno shranjeni omenjeni metapodatki? (ii.) Katere lastnosti slike lahko uporabite, da preverite, ali je bila vsebina slike predelana?

3. Peter Zmeda je v obdelavo prejel star strežnik, na katerem so nameščena Microsoftova Okna XP (Windows XP SP2). Ve, da se je na strežnik nekdo prijavljal, ne ve pa, kdo je to bil. Odločil se je, da bo pregledal dnevnik (log). Na računalniku je tudi precej podatkov - predvsem v `C:\Users`. (i.) Pripravite načrt zajema imenikov, ki jih mora zajeti (skopirati), da bo zajel dnevnik? Dnevnik se nahaja na privzeti lokaciji. (ii.) Če bi rad pregledal vsa sporočila, na kakšne težave lahko naleti in katere dodatne datoteke si mora skopirati s pregledovanega računalnika?