Digitalna forenzika 2014/15
Pisni izpit 3. mali srpan 2015

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 90 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.

1. Izmed petih osnovnih pravil, ki opredeljujejo ali je gradivo sprejemljivo na sodišču kot dokazno gradivo, sta dve a.) gradivo niso govorice in b.) gradivo je najboljše možno (dokazno) gradivo. Za vsako od naštetih pravil (i.) utemeljite kako zagotavlja sprejemljivost dokaznega gradiva in (ii.) podajte primer gradiva, ki pravilu ne zadošča ter zakaj tedaj ni sprejemljivo (dokazno) gradivo.

2. Peter je nekje na disku našel naslednja dva programa. Prvi program:

```
mov si, konec
msgloop:
    lodsb
    and al,al
    jz konec
    mov ah,0Eh      ; TTY output
    mov bh,[046ch]  ; Current page
    mov bl,07h
    int 10h
    jmp msgloop
konec:
    db 'PETER', 13, 10, 0
    mov es, $a000
    xor cx, cx
    mov dx, 81h
    mov ah, 03h
    mov al, 00h
```

in še drugi program:

```
msgloop:
    lodsb
    and %al,%al
    jz konec
    mov $0x0E, %ah
    mov (0x046c), %bh
    mov $7, %bl
    int $16
    jmp msgloop
konec:
    .ascii "PETER\r\n\0"
    mov 0xa000, %es
```

```
xor %cx, %cx
mov $0x81, %dx
mov $0x03, %ah
mov $0x00, %al
```

(i.) Kaj počneta? (ii.) V čem (če sploh) se razlikujeta, kar zadeva funkcionalnosti? (iii.) S katerim ukazom bi prevedli prvega, s katerim drugega?

3. Ali so digitalni dokazi lahko neposredni (vzpostavijo dejstva) ali so zgolj posredni (namigujejo na dejstva)? Utemeljite odgovor.

2. naloga: Pomnilniški mediji in iskanje podatkov po njih.

VPRAŠANJA:

1. Peter je dobil v roke disk, na katerem sumi, da je Cefizelj skril sliko tepanjske podmornice. Ve še to, da je slika bila shranjena v jpg obliki. Ne ve pa, kje je slika, če sploh še je; niti tega ne ve ali je v samostojni datoteki. Napišite tri hipoteze, kje boste iskali sliko ter nato za vsako od hipotez opišite postopek kako boste iskali sliko. Mesta omenjena v hipotezah morajo biti bistveno različna.

2. Peter je dobil v pregled sliko tipičnega diska z Microsoftovimi Okni. Njegova naloga je bila, da poišče gesla vseh uporabnikov na računalniku. Na žalost je na sliki diska nekaj datotek manjkalo - predvsem so bili uničene vse datoteke v C:\Documents and Settings. Na srečo je dobil celoten imenik C:\Windows. (i.) Kateri panj (*hive*) registra je Peter izgubil? (ii.) Kateri imenik dejansko potrebuje, da bo lahko prišel do gesel uporabnikov? (iii.) Kateri kos programske opreme lahko za to uporabi? (iv.) Od česa še je odvisno, ali bo gesla dobil ali ne?

3. Osrednja struktura, ki se uporablja na datotečnih sistemih ufs in ext je inode tabela. Skicirajte strukturo diska in predvsem na njej označite, kje se nahaja tabela z inode vnose.

3. naloga: Mobilne naprave in omrežna forenzika.

VPRAŠANJA:

1. Sistemski inženir v podjetju VseImamo opazuje IP pakete, ki prihajajo na njegov strežnik. Tako je opazil, da imajo paketi, ki prihajajo z naslova uprava.tepanje.gov, kar precej različne vrednosti TTL (*time to live*) značke. Napišite vsaj dva možna razloga, zakaj je to možno in ju opišite.

2. Peter je premeten možak. Da bi nikdar ne pozabil gesla, je spisal program za beleženje pritiskov na tipke, ki podatke o pritiskih beleži s pomočjo syslog. Ker uporablja razpored tipk Dvorak, je prepričan, da je varen. (i.) Utemeljite, zakaj se moti. (ii.) Kako se običajno shranjujejo gesla pod Linuxom?

3. Špela Štimana je nova sistemska administratorka v Butalah. V dnevniških zapisih je našla sumljiv zapis:

```
69.164.212.61 - - [29/Apr/2014:22:55:36 +0200]
"POST //%63%67%69%2D%62%69%6E/%70%68%70?%2D%64+%61%6C
%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+
%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+
...
%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%64+
%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D
%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%6E
HTTP/1.1" 404 209 -" -"
```

   Odločila se je poklicati lastnika domene, od koder je prišel obiskovalec strani. Opišite korake, ki jih naj izvede, da bo prišla do telefonske številke lastnika domene.

4. naloga: Izvajanje preiskave.

VPRAŠANJA:

1. Eden od postopkov, ki jih uporabimo v forenzični preiskavi je *triaža*. (i.) Kaj je to triaža in (ii.) kdaj jo izvedemo. (iii.) Opišite konkreten primer, ko izvedemo triažo in zakaj.

2. Peter je pred mesecem padel v nakupovalno mrzlico. Kupil si je tri diske po 1.5TB. Na njih je ustvaril en sam datotečni sistem velikosti 4TB. Potem je ugotovil, da je toliko prostora preveč in da bo enega od diskov prek oglasa prodal. Seveda noče zavreči že ustvarjenega datotečnega sistema, na katerem zaseda le 2TB prostora. (i.) Katero tehnologijo je moral uporabiti, da lahko to stori? (ii.) Ali na svojih diskih lahko uporablja MBR? Utemeljite odgovor?

3. Naštejte in opišite tri namene preiskave elektronske naprave po Zakonu o kazenskem postopku?