FORENSICS CYBER-SECURITY

MEIC, METI

2020/2021 1st Semester

2nd Exam February 9, 2021 Duration: 2h00

- Use a pen only; no extra material is allowed, such as calculator, scratch paper, etc.
- Write your answers in the free space after each question.
- The exam can be answered in Portuguese or in English.
- Identify all sheets; **unidentified pages will not be graded!**

I. (0.5 + 0.5 + 1 + 0.5 + 0.5 + 0.5 + 0.5 = 4 points)

1. Producing admissible evidence is one of the most fundamental goals of digital forensics.

   a. Consider a case where a forensic investigator collected child pornography photos from a suspect's computer while searching for evidence on drug-related activities. The photos have been considered inadmissible in court. Explain on what basis they have been excluded.

   b. The credibility guideline implies the exclusion of hearsay evidence. Indicate two exceptions to the hearsay rule.

2. High-quality forensic tools have several desired properties. Consider two memory dump analysis tools: $m1$ and $m2$. What does the following statement mean?

   "$m1$ is more comprehensive than $m2$".

3. Consider the following investigative scenario:

> InSure is an insurance company that is being investigated for fraud. The forensic team identified four important computers operating in different conditions. A *mail server* that contained the email of the company. It was up and running and connected to the Internet. The system administrator informed you that the mail server was running Windows and the disk volume was encrypted using BitLocker. A *backup server* that was used to store backups. The backup server contained four 1TB hard disks and it was powered on. You were told the root password, then you logged in, and discovered that that the disks had been formatted in the previous day. A *file server* that was dedicated to storage of the company's working documents. This was a Linux server equipped with a single 500GB hard disk and it was powered on. You realized it was running CleanSweep, a popular application for erasing files. A *Windows workstation* owned by the company's CEO. You moved the mouse and saw that it was not password-protected. You also noticed that it had been unplugged from the Ethernet socket, but some of the led indicators of the built-in wireless network card were blinking.

Explain how you would proceed to deal with each of these four computers. Justify your responses:

a. Mail server.

b. Backup server.

c. File server.

d. Windows workstation.

II. (1 + 1 + 0.5 + 1 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 1 = 8 points)

1. Kelly wants to hide a secret message inside a cover photo using a steganographic tool. The cover photo consists of a 24-bit RGB image with the resolution of 1440×1080 pixels. The tool applies a LSB-1 encoding scheme to each color channel using a password protection algorithm. The algorithm that tells which pixels contain the encoded data is:
   * the first pixel (p_0) to encode bits is given by: $p_0 =$ password *mod* 4;
   * the next pixels are found by: $p_i = p_{i-1} + 4$;
   * pixel numbering begins in 0, i.e., the index of the first pixel of an image is 0.

   What is the maximum size of the secret message that can be hidden inside that cover photo? (You can provide the mathematical expression.)

2. Consider the following unallocated disk space containing the blocks of six deleted files. The empty blocks filled with zeros are indicated with the symbol "−":

−	A_0	−	B_1	B_0	C_0	C_1	D_0	D_1	C_2	−	E_0	E_1	−	F_1	F_0

   The files (and respective blocks) are listed below according to their file formats:
   - GIF: file A (A_0), file C (C_0, C_1, and C_2), file D (D_0, and D_1), and file F (F_0, and F_1)
   - JPEG: file B (B_0, and B_1), and file E (E_0, and E_1)

   The formats of these files are as follows:
   - GIF: "0x47 0x49 0x46 0x38 0x37 0x61" header, "0x00 0x3B" footer
   - JPEG: "0xFF 0xD8" header and "0xFF 0xD9" footer

   Your job is to recover the deleted files using two file carving tools. Each tool implements a different file carving technique: single-pass structure-based and bifragment gap carving.

   a. Write the blocks produced by each tool for each file (use "×" if no output is generated):

File	Single-pass structure-based carving tool	Bifragment gap carving tool
A		
B		
C		
D		

   b. "File C is likely to be older than file D." Based on the disposition of blocks in the unallocated disk space, do you agree with this statement? Justify. (No justification: 0 points)

3. Consider a memory dump that contains a full memory snapshot of the execution state of a Linux computer. At the moment the memory snapshot was taken, 12 processes were running in the system. Describe an algorithm of a hypothetical forensics tool that: i) reads the the memory dump, and ii) writes the contents of each of the 12 processes in an independent file.

4. TSK is a powerful digital forensics framework. Do you agree with these statements? Justify.

   a. "When starting to analyze a disk image, it is normally a good practice to extract general information about the disk partitioning scheme. For that purpose we use the *dcat* tool."

   b. "Tools such as *icat* or *istat* are adequate to obtain information in the meta-data category."

   c. "The *fls* tool has the ability to list both allocated and unallocated file names of a given folder. This information is obtained from the folder's inode."

   d. "The TSK tools operating in the content category cannot recover the journaling information of an Ext3 file system."

5. Give two examples of digital artifacts from the Windows Registry that might be relevant to investigate the execution of programs on a computer. Explain what those digital artifacts are.

6. A network administrator detected abnormal traffic targeting their file server (turbina). Reading server's `/var/log/auth.log`, he could see thousands of lines like the following ones:

```
Jan 12 11:27:10 turbina sshd[8423]: Failed password for
    invalid user admins from 172.25.1.1 port 44216 ssh2
Jan 12 11:27:13 turbina sshd[8425]: Failed password for
    invalid user phoenix from 172.25.1.1 port 20532 ssh2
Jan 12 11:27:17 turbina sshd[8428]: Failed password for
    invalid user piglet from 172.25.1.1 port 24492 ssh2
Jan 12 11:27:22 turbina sshd[8430]: Failed password for
    invalid user rainbow from 172.25.1.1 port 46591 ssh2
Jan 12 11:27:25 turbina sshd[8432]: Failed password for
    invalid user runner from 172.25.1.1 port 57129 ssh2
Jan 12 11:27:34 turbina sshd[8434]: Failed password for
    invalid user sam from 172.25.1.1 port 11960 ssh2
Jan 12 11:27:37 turbina sshd[8437]: Failed password for
    invalid user abc123 from 172.25.1.1 port 5921 ssh2
Jan 12 11:27:40 turbina sshd[8439]: Failed password for
    invalid user passwd from 172.25.1.1 port 21208 ssh2
...
```

   a. Suggest an explanation for the observed events.

   b. Does a modern network IDS like Snort have the ability to detect traffic such as this and fire an alarm accordingly? Justify your answer. (Unjustified answers get 0 points.)

7. Protocol analysis aims to understand how a particular communication protocol works and how to identify it. Provide two examples of protocol identification techniques.

III. (2 + 0.5 + 0.5 + 0.5 + 0.5 + 1 + 0.5 + 0.5 + 0.5 + 0.5 + 1 = 8 points)

1. For each of the following statements, indicate whether it is true (T) or false (F). Each correct answer is awarded 0.25 points; each wrong answer is penalized by subtracting 0.10 points.

   a. ____: In the specialized search engine Shodan, some content cannot be found due to several limitations of the URL traversal techniques.

   b. ____: In centralized botnet architectures, the IRC protocol is normally used for the communication between the zombies and the C&C servers.

   c. ____: In order to hide their presence, many rootkits replace commands like *ps* by hooking into the Linux kernel.

   d. ____: In the Bitcoin system, the transaction records preserved by the blockchain contain precious information about the IP address of the transaction issuers.

   e. ____: The IMSI of an Android device can be modified by rooting the device.

   f. ____: Browser fingerprinting is based on the systematic collection of browser information such as the user agent and installed plugins.

   g. ____: The received field in the header of an email provides precious information about the recipient of the email.

   h. ____: Virtual Machine Introspection is not adequate for detecting the presence of malware on guest virtual machines.

2. Consider the following email header, and answer the questions below. Justify all your answers. (Unjustified answers get 0 points.)

```
Delivered-To: abdullah.yousouf@gmail.com
Received: by 10.194.119.165 with SMTP id kv5csp2398913wjb;
        Wed, 21 Oct 2015 07:59:40 -0700 (PDT)
Return-Path: <atest_2000@yahoo.com>
Received: from nm16-vm3.bullet.mail.ne1.yahoo.com
    (nm16-vm3.bullet.mail.ne1.yahoo.com. [98.138.91.146])
    by mx.google.com with ESMTPS id v29si1732890ioi.35.2015.10.21.07.59.39
    for <Abdullah.yousouf@gmail.com>;
    Wed, 21 Oct 2015 07:59:40 -0700 (PDT)
Received: from [98.138.100.115] by nm16.bullet.mail.ne1.yahoo.com
    with NNFMP; 21 Oct 2015 14:59:39 -0000
Received: from [98.138.88.234] by tm106.bullet.mail.ne1.yahoo.com
    with NNFMP; 21 Oct 2015 14:59:38 -0000
Received: from [127.0.0.1] by omp1034.mail.ne1.yahoo.com
    with NNFMP; 21 Oct 2015 14:59:38 -0000
Received: (qmail 83569 invoked by uid 60001); 21 Oct 2015 14:59:38 -0000
Received: from [41.32.28.249] by web310605.mail.ne1.yahoo.com
    via HTTP; Wed, 21 Oct 2015 07:59:38 PDT
Message-ID: <1445439578.66136.YahooMailBasic@web310605.mail.ne1.yahoo.com>
Date: Wed, 21 Oct 2015 07:59:38 -0700
From: atest_2000 <atest_2000@yahoo.com>
Subject: Our 0ffers
To: Abdullah.yousouf@gmail.com
```

   a. What is the source IP address of this email?

   b. What is the protocol used my the email client for sending the email?

   c. Based on this header alone, can you reconstruct the full path of the email?

3. Provide two examples of different tools installed by typical rootkits on a victim's computer.

4. The police apprehended the mobile phone of a suspect and hired you to help them access the suspect's bitcoin accounts. These accounts are managed by a bitcoin wallet app installed on the phone. What is the critical piece of information that you need to extract from the phone?

5. A suspect malicious binary was analyzed using the *strace* tool. Below you find an excerpt of *strace*'s execution:

```
time(NULL) = 1207931463
getppid() = 1
brk(0) = 0x804e000
brk(0x806f000) = 0x806f000
open("/usr/dict/words", O_RDONLY) = -1 ENOENT (No such file or directory)
open("/home/alice/dict/words", O_RDONLY) = -1 ENOENT (No such file or directory)
open("/home/alice/dict/words.old", O_RDONLY) = -1 ENOENT (No such file or directory)
```

   a. Is the usage of *strace* considered to be a static or a dynamic analysis technique? Justify.

   b. Suggest a hypothesis for what the malware may be attempting to do.

   c. Indicate one precaution that is recommended to forensic analysts prior to the employment of dynamic analysis techniques.

6. What is the specific anonymity property that the Tor hidden services can provide to users when compared to vanilla Tor circuits?

7. Give two examples of relevant evidence that can be collected from wireless access points.