FORENSICS CYBER-SECURITY

MEIC, METI

2022/2023 1st Semester

2nd Exam February 8, 2023 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 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 = 4 points)

1. Consider the so-called Kruse investigation model:

   a. Indicate what authorization level is required in the assessment stage for each investigation type: internal, civil, or criminal investigations.

   b. In the acquisition stage of an investigation, state one advantage of using digital signatures to generate integrity checks instead of using one-way hash functions.

   c. "In the analysis stage, it may be necessary to find evidence of anti-forensic techniques using proper tools. For instance, the tools *scalpel* and *foremost* are particularly useful for finding LSB-encoded content inside images." Do you agree with this statement? Justify your answer.

   d. In the reporting stage, a forensic analyst forgot to attach the case timeline to the documentation submitted to the judge. Will this glitch potentially render the evidence inadmissible?

2. Consider the following investigative scenario:

> Mr. Fellini was under suspicion of consuming and selling child pornography online. After obtaining a search warrant, the police authorities broke into his house to gather relevant evidence for the case. Agent Sharp, the forensic analyst accompanying the police, took over the operations. He found several hardware devices in the house: one Windows desktop computer, one MacBook laptop, five external SDD drives, and two mobile phones (one iPhone and a Samsung Galaxy phone). The desktop computer connected to the Internet, and the screen was off. However, hard disk and network activity were noticeable, given the blinking of the hard disk's and network interface card's LEDs. By the time the police broke into the apartment, Mr. Fellini was sitting at his laptop typing on the keyboard and, startled, became violent. He jumped from his desk, leaving his laptop logged in as before, ran for his mobile phones, and smashed the iPhone against the wall before being arrested by the police. The Samsung phone was protected with a blocking pattern and was running out of battery. Agent Sharp then needed to take proper actions to seize evidence and bring it to the forensic lab for future analysis.

Indicate if you agree with the following actions performed by Agent Sharp. Justify your responses:

a. "Because Agent Sharp wanted to preserve as much evidence as possible, he immediately switched off the desktop computer by pulling the power plug."

b. "Given that the MacBook was unblocked, Agent Sharp created a bitstream image of its disk. He connected one pen drive containing Kali and an external SSD drive and executed Kali's disk imaging tools to save the image on the external drive, computing the respective hash. Then, on his laptop, he replicated the SSD drive to a second SSD drive."

c. "Agent Sharp picked up the wrecked iPhone and sealed it inside an evidence bag. As for the Samsung phone, he switched off the phone and sealed it in a second evidence bag."

d. "He wrote a chain of custody. The complete list of identified items comprises i) the serial numbers and models of all the hardware devices encountered in the house and ii) the serial numbers and models of the two forensic SSD drives containing the MacBook disk image."

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

1. Indicate one benefit of using a dedicated hardware card to perform memory acquisition on a server when compared to software-based approaches.

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

–	A_0	A_1	B_0	B_1	A_2	C_1	C_0	D_0	–	D_1	E_2	F_0	E_1	E_0

The files (and their blocks) are: file A (A_0, A_1, A_2), file B (B_0, B_1), file C (C_0, C_1), file D (D_0, D_1), file E (E_0, E_1, E_2), and file F (F_0). All files are GIFs whose format is as follows:

- GIF: "0x47 0x49 0x46 0x38 0x37 0x61" header, "0x00 0x3B" footer

Answer the following questions and justify your response. (No justification means 0 points)

a. Assuming that we run a single-pass structure-based file carver on this disk image, indicate which files the tool can recover *correctly*.

b. Suppose that we run a modified version of the file carver used in a) returning the following files X_i as output. What specific change was made in this carving algorithm?

$$X_0 \rightarrow A_0, A_1 \quad X_1 \rightarrow B_0, B_1 \quad X_2 \rightarrow C_0, D_0, -, D_1 \quad X_3 \rightarrow F_0 \quad X_4 \rightarrow E_0$$

c. We run an alternative modification of the file carver used in a). This version returns the following files X_i as output. What modification was made in this case?

$$X_0 \rightarrow E_0, E_1 \quad X_1 \rightarrow F_0 \quad X_2 \rightarrow D_0, C_0, C_1 \quad X_3 \rightarrow B_0, A_1 \quad X_4 \rightarrow A_0$$

3. A technique to extract data from a hard disk is to open it and read directly from the platter. Tell (yes/no) if this is effective for each of the following storage technologies and justify.

   (1) Password-protected hard disk against reads/writes (2) Self-encrypted hard disk (3) SSD

4. To analyze an NTFS file system, we executed the command listed below; `0-128` has the form of x-y where x is an index and y is an attribute (128 refers to the `$DATA` attribute).

```
# icat -f ntfs ntfs1.dd 0-128 | xxd
0000000: 4649 4c45 3000 0300 4ba7 6401 0000 0000 FILE0...K.d.....
0000016: 0100 0100 3800 0100 b801 0000 0004 0000 ....8...........
0000032: 0000 0000 0000 0000 0600 0000 0000 0000 ................
0000048: 5800 0000 0000 0000 1000 0000 6000 0000 X...........`...
[REMOVED]
```

   Answer the following questions:

   a. What is the general purpose of the *icat* tool in computer forensics?

   b. Explain the meaning of the value *x* in the above execution of *icat*.

   c. What content is being displayed in this output by calling *icat* with these parameters?

5. Indicate four Windows data structures (excluding NTFS) that can provide valuable sources of evidence for the execution of programs. Be specific.

6. Consider two disks A and B, whose filesystem metadata was destroyed. The disks are used at about 10% and 90% of their capacity, respectively. Which of these cases is digital stratigraphy more likely to give better results in establishing temporal relations between files? Why?

7. The *Ap0calyp0* botnet sends messages from their C&C servers to infected bots using embedded messages starting with `BABA` and terminating in `F0F0`. A network administrator configured the IDS to detect this pattern in his local network (10.0.0.0/8). At some point, the IDS positively flagged one of such messages sent by an external source to the email server. Immediately after receiving that message, the email server pinged several internal IP addresses, one of them being 10.0.1.8. The hex dump below shows the intercepted message:

```
00: 51dc 9a88 7231 d9d2 ad68 326f f6f0 c3c9
10: 791b a37e aeb1 5e83 39a0 addf 9977 8aba
20: ba04 0a00 0180 0a00 0128 0a00 0115 0a00
30: 0108 f0f0 2ac3 50a5 1c55 3e7f 1803 2048
40: ff4f c35f ced2 a1da e7d7 3908 e9e6 6a0b
50: .... .... .... .... .... .... .... ....
```

Answer the following questions. Justify all your answers.

a. What traffic analysis technique is the IDS using to detect these messages?

b. Suggest a possible explanation for the observed sequence of events.

c. Analyse the hex dump and identify all the IP addresses that were pinged by the mail server. Explain your response. (You can present the IPs in hexadecimal notation.)

8. SIEM systems are widely adopted by organizations. Indicate two functions of a SIEM system.

III. (2 + 1 + 0.5 + 0.5 + 0.5 + 0.5 + 0.5 + 1 + 0.5 + 0.5 + 0.5 = 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 email spoofing, the attacker fakes the email address of the receiver.

   b. ____: The IMSI can be used to identify the manufacturer and model of a specific mobile device, but not the identifier of the mobile subscriber.

   c. ____: NATs improve the anonymity of clients in local networks because clients' private IP addresses are masked by a common public IP address.

   d. ____: Botnets usually employ fast flux which consists in rotating the IP addresses of the C&C server.

   e. ____: Examples of anti-dynamic malware analysis techniques include virtualization detection, debugger detection, and anti-virus scanning.

   f. ____: In Bitcoin investigations, the shared spending heuristics is useful to infer if two or more input sources in a transaction belong to the same user.

   g. ____: Placing a mobile phone inside a Faraday bag increases the battery longevity of the device.

   h. ____: In cloud forensics, one of the hardest challenges of multi-tenancy issues is to determine whether information has been stolen via side channels that can bypass virtual machines' isolation.

2. For about one week now, the Humberto Delgado airport has been receiving complaints from travelers reporting stolen credentials while their are located within the airport's premises. A forensics investigator investigated post-mortem traces of the airport's WiFi network. Using Wireshark, he applied the filter `wlan.fc.type_subtype == 0x0c` to the trace. Below, we show a sample packet of the Wireshark output affecting one of the victims:

No.	**Time**	**Source**	**Destination**	**Protocol**	**Length**
`221453`	`58.884717`	`NokiaDan_3d:aa:57`	`Siemens_41:bd:6e`	`802.11`	`26`

Answer the following questions and justify your responses:

a. Considering that the frame subtype `0x0c` identifies a deauthentication frame interpret the output above indicating who the victim is and the potential effects of this frame.

b. Based exclusively on the traces from the past two weeks, how would you proceed to determine if the other affected travelers where attacked by the same actor?

c. Assuming now that you can also collaborate with the ISPs providing mobile network coverage at the airport, how could you leverage their help to locate the attacker?

3. An online store suffered an SQL injection attack. Information was stolen from the users' database, which contains: the usernames, hashed passwords, and cookies of active sessions.

a. What can the attacker immediately do with this information?

b. What recommendation would you give to mitigate further damage?

4. A drug trafficking website was deployed as a Tor hidden service. John establishes a session with it from his Tor browser. Assuming that the police authorities managed to intercept the traffic in the session's rendezvous point in what way can the anonymity be compromised?

5. A server that was suspected of being compromised by a rootkit was immediately replaced without being shutdown. The forensic analysis collected a memory dump of the operating system kernel, saved it in a separate dump file, and then used *volatility* to inspect the content of the system call table. Some entries of the table were modified, namely the following ones:

Interposed System Call	**Interposing Function**
`fork`	`0xfe9f2fb4`
`exec`	`0xfe9f234c`

   a. Indicate if the steps performed by the analyst after collecting the memory sample correspond to static or dynamic analysis. Justify your answer.

   b. Suggest what the malware may try to achieve by modifying the system calls above.

6. Regarding mobile forensics, consider the following statements and indicate whether you agree or disagree with them, justifying your answers:

   a. "Shared preferences are good places to find cached images downloaded by mobile apps."

   b. "Chip-off data acquisition techniques are more destructive than JTAG-based techniques."