FORENSICS CYBER-SECURITY

MEIC, METI

2019/2020 1st Semester

1st Exam January 8, 2019 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. A fundamental goal of digital forensics is to produce admissible evidence.

   a. Indicate the four main guidelines for admissibility of digital evidence in court.

   b. Indicate one challenge in preserving admissibility in the phase of data acquisition.

2. Discuss one advantage and one disadvantage of using the airplane mode in order to guarantee network isolation when dealing with mobile devices.

Number: ______________ Name: ____

2. Consider the following investigative scenario:

> Bonnie and Clyde have become suspects of conspiring to steal corporate trade secrets from the pharmaceutical company where they work. Motivated by unusual traffic patterns detected periodically in the company's network – taking place every Friday at midnight – the police authorities were called to perform a search in their work places on January 3^{rd} 2020 around that time. Aided by the local system administrator, you were given access to their workstations, to a file server where most secrets were stored, to a VPN server, and to the NetFlow logging system. The file server was accessible only within the local network via SSH. The VPN server provided external authenticated access to the local network. Bonnie and Clyde had credentials to access the VPN server and the file server. Bonnie's workstation is a Linux computer. It was password-protected, and it was exchanging substantial traffic with a remote computer. Clyde's workstation is a Windows computer and it was not locked, which means you have login access to the system. No network activity was reported involving this computer.

Answer the following questions and justify your responses:

a. What relevant evidence would you be looking for? Provide a few examples.

b. What artifacts would you collect from Bonnie's computer and how?

c. What artifacts would you collect from Clyde's computer and how?

d. What artifacts would you collect from other relevant sources and how?

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

1. There are three steganalysis approaches for detection of hidden content. Explain them briefly.

2. A full memory dump was extracted from a running computer. Four processes were executing at the time of extraction. Four files were open: A, B, C, and D. Each file was opened by one of the four processes. The files were memory-mapped and loaded entirely into the memory address space of each process. The diagram below depicts a segment of the physical memory illustrating the pages that contain the chunks of each file. This segment is divided into blocks, each of them represents a physical memory page. Memory addresses grow from left to right:

   * HTML files: file A (A_0, A_1)
   * JPEG files: file B (B_0, B_1), file C (C_0, C_1), and file D (D_0, D_1, D_2)

	C_1	C_0	D_0	D_1	D_2		B_0	B_1	A_0	A_1	B_2	

   The following list provides relevant details about the file formats of each file:

   * HTML: no header and no footer, content follows the syntax of the HTML language
   * JPEG: “0xFF 0xD8” header and “0xFF 0xD9” footer, content must be decoded

   Answer the following questions:

   a. A file carving tool was executed in order to recover files from this memory segment. The tool managed to recover *correctly* the files: B, C, and D. Based on the output of the tool, which of the following strategies is implemented by the tool: structure-based carving, content-based carving, or bifragment gap carving? Justify. (No justification: 0 points)

   b. Assuming you can analyze the full memory dump, would it be possible to correctly recover all files and discover which process was responsible for opening each file? How?

3. Consider the following output of the *istat* tool when applied to the forensic image `disk.dd` containing an ext2 file system partition. The goal is to inspect the state of inode 10090.

```
# istat -o 10260 disk.dd 10090
inode: 10090
Not Allocated
Group: 5
Generation Id: 3534950782
uid / gid: 4 / 7
mode: rrw-r--r--
size: 3591
num of links: 0

Inode Times:
Accessed: 2003-08-10 00:18:36 (EDT)
File Modified: 2003-08-09 00:11:12 (EDT)
Inode Modified: 2003-08-10 00:29:58 (EDT)
Deleted: 2003-07-08 00:29:58 (EDT)

Direct Blocks:
5184 5185 5184 5187
```

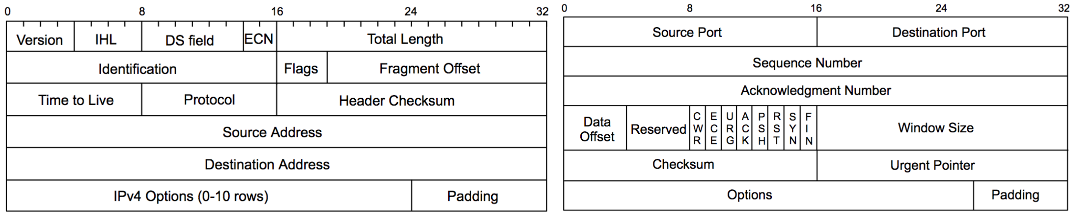
a. What is the meaning of the output “Not Allocated” for this particular case?

b. Identify two existing inconsistencies in this inode and describe their consequences to the correct forensic interpretation and recovery of data.

4. You were called to obtain evidence about the execution of programs on a Windows desktop. For each of the following artifacts, indicate whether or not it can be useful for that purpose: Recycle Bin, prefetch files, RunMRU, Thumbs.db. Why? (Unjustified answers get 0 points)

5. A network administrator identified a sudden spike of incoming traffic overwhelming their web server. The IP address of the web server is 146.193.41.40. All packets look exactly the same. A packet sample is shown below in hex notation. The IP and TCP header layouts are depicted on the left and right, respectively; big endian is used.

```
 0: 4500 002c 08b8 4000 ff06 9997 8b85 d96f
16: 92c1 2928 9005 1F90 1f48 d03f 7214 f114
32: 6002 2238 a92c 0000 0204 05b4
```



a. Analyze the packet above and extract these values: source IP, destination port, and TCP flags. Values can be provided in hex notation. (Hint: the IP header size is 20 bytes.)

b. What can be inferred about the source and purpose of this traffic? Justify your answer.

6. Suggest specific traffic patterns that can be used by an IDS in order to automatically flag network scanning attempts performed using these techniques: *port scans* and *ping sweeps*.

7. Indicate whether or not you agree with this statement: "If the `Received` fields of an email header are internally consistent and complete, then they can always be trusted in conveying the precise path traveled by an email." Justify your answer. (Unjustified answers get 0 points.)

III. (2 + 1 + 0.5 + 0.5 + 0.5 + 1 + 0.5 + 1 + 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. ____: Specialized search engines like Shodan can discover publicly connected devices by randomly picking an IP address out of all the IPs that exist.

   b. ____: Fast flux is an evasion technique implemented by botnets that involves the constant modification of the IP address of a compromised host.

   c. ____: In order to hide their presence, many rootkits deploy their own versions of userland commands, replacing *ps* in order to hide the rootkit's files.

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

   e. ____: To launch an evil twin attack, the rogue AP aims at emitting a stronger wireless signal than a legitimate AP.

   f. ____: Android applications can store structured data inside SQLite databases, which allow data to be retrieved by a dedicated backup service running on the device.

   g. ____: In the NTFS file system, the MFT data structure allocates an entry for each and every file that exists in the system.

   h. ____: The multi-tenancy features of cloud platforms only create serious obstacles for forensic analysis in the cases where the customers' data is encrypted.

2. The network logging system of a given organization recorded a sequence of periodic DNS name resolution queries issued from a local workstation with a time interval of about 5 hours between each query. These queries are listed below on the left. With the exception of the entries marked with *, all other DNS queries returned an error from the DNS server.

DNS query
eqxdowsn.info
ggegtugh.info*
hqute.org
rpacw.net
oumaac.com
eersmhdhb.org*
rzziyf.info
...

   a. Suggest an explanation for the phenomena being observed?

   b. Describe how you would proceed to further investigate this traffic.

3. Mr. Black is being investigated for financial fraud involving large money transfers facilitated by the Bitcoin system. He performs Bitcoin transactions through his phone using a Bitcoin wallet software. His mobile device was seized. Describe how you would proceed with the investigation of Mr. Black's Bitcoin transactions in the following two cases:

   a. The mobile device was unlocked (i.e., it was not password protected), and you can access the full state of the wallet software.

   b. The mobile device was locked, you do not know the lockscreen password pattern, and the device was not rooted.

4. Static and dynamic analysis techniques are commonly used for malware forensic analysis:

   a. Compare static and dynamic analysis indicating two important differences between them.

   b. Describe one anti-static analysis technique and one anti-dynamic static analysis technique commonly employed by malware.

5. An ISP managed to deanonymize a Tor circuit that was used by a subscriber to access a hidden service. Through the use of traffic analysis techniques, the ISP was able to link the subscriber's IP address (156.132.5.23) to the IP address (21.42.102.86) of the destination pointed by the circuit's exit node. Is the IP address 21.42.102.86 the address of the server accessed by the subscriber? Justify your answer. (Unjustified answers earn 0 points.)

6. Sam wanted to remove potential evidence from the disk of his Windows desktop, so he installed and executed a wiping tool. This tool writes zeros in the entire NTFS partition except in: the boot section, the MFT, and the MFT backup copy. Will it still be possible to recover the content of some previously existing files? Justify your answer. (No justification: 0 points)