Digital Forensics 2021/22
Written Exam Thrimilce 6th, 2022

The exam must be taken individually. You may use any literature. Literature can be in paper form or on an electronic device that is not connected to other devices.

You may be awarded extra points if you answer all questions at least partially. Although individual questions may be more closely related to a single chapter from the lectures, you will often need to use the knowledge from the other chapters as well. Some questions are intentionally vague and require you to make assumptions to give a precise answer. In such cases, be precise in answering the questions and specifying the assumptions. Precise answers will bring more points. You will not get full points for general answers.

You have 75 minutes to take the test.

May your knowledge bring you success!

TASK	POINTS	MAX. POINTS	TASK	MAX. POINTS	POINTS
1			3		
2			4		

1. task: Basics.

QUESTIONS:

A) To which of the four categories (according to Parker) does a computer, infected with malware that prevents it's user normal work and is at the same time used to attack other computers, belong? Justify your answer.

B) (i.) One of the basic conditions for the admissibility of evidence is its authenticity. What does this mean and how do we ensure it? (ii.) What are the remaining four acceptance conditions for the material?

C) Peter Zmeda would like to replace the log recording program. He uses Debian 9.0. He will switch from `rsyslog` to `syslog-ng`. (i) Where have the logs most likely been (log files) so far? Where will they be after the program change? (ii) How will the log file format change? (iii) Peter has so far collected events from multiple computers running `rsyslog`, right on the computer he is now upgrading. What will he have to do to continue collecting data on the same computer? How will he need to change the settings of other computers?

2. task: File systems.

QUESTIONS:

A) The Butale police have to do a house search at Cefizlj, who is suspected of having something to do with the recent disappearance of Šprinca Maroglja. During the premises search, they found an external disk with the file system `ext2` in the closet and pictures of Šprinca Maroglja on it. They did not find any computer with the operating system `unix`, but they did find a computer with the Windows 10 operating system. Compare file metadata in the `ext2` and `ntfs` file systems. (i.) Which metadata is exists in both file systems and how can we convert it from the format of one file system to the format of the another and vice versa. (ii.) Which metadata exists only in one file system, in which and why do you think it does not in another?

B) Which property is specific to UNIX systems and is not present on Windows/DOS systems but is very important for forensic investigation, since it ensures data on a disk device does not change?

   (a) The possibility of data encryption.
   (b) The possibility of warning before the system tries to change data on a disk device.
   (c) The possibility of mounting a disk device in read-only mode.

(d) The possibility of copying data from a disk device.

C) Peter Zmeda got his hands on a DVD with only one file named *disk.iso*. (i) Peter guesses that *disk.iso* contains a file system. Write a sequence of commands that you can use to check this and see which files it contains. (ii) How would the command sequence change if *disk.iso* contains the `ext4` file system and not *ISO9660*? (iii) Peter suspects that *disk.iso* contains a file system written by Cefizelj that will crash his driver *ISO9660*. What tool or library could Peter use to still scan the file, but still protect himself from such attacks?

3. task: Mobile and network forensics.

QUESTIONS:

A) The only Internet provider in Butale *ButiButi* has a problem. In Tepanje, they found that someone had launched an *DoS* attack on their central website. He carried out the attack by sending a continuous stream of SYN packets from the IP address owned by *ButiButi* for 10 minutes. Peter Zmeda, who manages *ButiButi*, was informed about the attack. *ButiButi* assigns IP addresses to its customers through the DHCP service. (i.) In order to begin the investigation, Peter will need some information from Tepanje – which ones and why? (ii.) What information does he have to record in order to be able to find the attacker? (iii.) How should all the data collected be used to trace the perpetrator?

B) What VPN permits to the attacker? Justify the correct answer by stating why it is correct and why others are incorrect.

(a) Launching their attack from a compromised computer from a distant location to hide their MAC address and geographic location.
(b) Launching their attack from their computer with a forged MAC address to hide their true MAC address and geographic location.
(c) Launching their attack from their computer with a forged IP address to hide their true IP address and geographic location.
(d) Launching their attack from a compromised computer from a distant location to hide their IP address and geographic location.

C) Peter Zmeda somehow managed to get the data stored in the flash memory of a mobile phone running Android 4, in the file `mmcblk0.raw`. (i) Peter knows that there were several partitions on the phone. With which command / how could he find out how many there were and what are their types? (ii) One of the partitions contains the file `data/data/com.android.providers.contacts/databases/contacts2.db`. What tool can he use to view

the content of the file? (iii) Peter was able to extract a section with interesting data. He compressed it into a `.zip` file and sent it to a friend. When a friend received the file, Microsoft Windows informed him that the file contained the *ZergRush* virus. He read on the internet that it is a *privilege escalation exploit and Android 2.0*. Is this file compromising a friend's computer? Justify the answer.

4. task: Investigation.

QUESTIONS:

A) We return to the case described in question A 2. task. Our forensic scientist Peter Zmeda suspects that Cefizelj used a found computer with Windows 10 operating system to read and write from an external disk. (i.) Formulate three essentially different hypotheses by which to confirm Peter's suspicion. (ii.) For each of the hypotheses, write down how you would test if it is true.

B) Peter Zmeda received a server with two hard drives for review. He connected both disks to his computer running Ubuntu 20.04 Desktop. He created copies of disks:

```
dd if=/dev/sdc of=prvidisk.raw
sha512sum /dev/sdc
cat /dev/sdd > drugidisk.raw
sha512sum /dev/sdd
sha512sum prvidisk.raw
sha512sum drugidisk.raw
```

He was given a different checksum each time. He then ran the same commands again. This time, the checksums matched. (i) Apparently he created copies of the discs in two different ways. Which is the right one? (ii) Why could he get different checksums on first start-up? (iii) How would you ensure that the checksums would be the same on first try?

C) What is a Threat Model? Justify the answer.

(a) A model or activity that obfuscates the real attack.
(b) A program that an attacker uses to exploit the target system.
(c) The means by which an attacker gains access to infrastructure.
(d) Detailed description of an exploitable vulnerability in the system.
(e) An action plan with priorities, what will an attacker do, which vulnerabilities will the attack first and what are they hoping to achieve.