Digital Forensics 2023/2
Written Exam Eostremonath 30th, 2024

The exam must be taken individually. Literature in a paper form or on disconnected computer. If you successfully solve all tasks at least partially, you might get extra points. Although individual questions may be more tied to a specific topic, it is necessary to use knowledge from other topics. Some questions require assumptions for an accurate answer. Be precise with them because accuracy earns more points. Principle answers do not bring all the points.

The time for writing the exam is 60 minutes.

May your knowledge bring you success!

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

NAME AND SURNAME: _____

STUDENT ID: _____

DATE: _____

SIGNATURE: _____

Task 1. *Basics.*
QUESTIONS:

1. Digital evidence can be altered or destoyed either accidentally during collection or maliciously by offenders, without leaving any obvious sign of distortion. Which features of digital evidence mitigate this problem? Justify the answer.

(a) When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of.
(b) Digital evidence is difficult to destroy with simple deletion or formatting and can be recovered.
(c) All of the listed.
(d) Digital evidence can be duplicated exactly and a copy can be examined as if it were the original.
(e) With the right tools, it is very easy to determine if digital evidence has been modified or tampered with by comparing it with the original copy.

2. A digital device can be an object or a subject of a crime. (i.) Why is it important in what role does it act? (ii.) Give an example when it acts as an object and justify that it is indeed an object.

3. Peter installed the latest Debian GNU/Linux. He installed `slapd`. Since his LDAP server is not working, he would like to fix it. Unfortunately, `/var/log/syslog` does not exist on his system! (i) Why is there no `syslog` file? (ii) How could he review the events on the system? Were they even logged? Justify your answer. (iii) Write a sequence of commands that makes the system able to use `syslog` again.

Task 2. *File systems.*
QUESTIONS:

1. Forensic Peter Zmeda suspects that there is a picture of the place where Cefizelj hid stolen Butale's salt on the seized disk. (i.) He hypothesized that there are two partitions on the disk. How can he check this? (ii.) In none of the file systems that were in the partitions, he found no image files. Was his suspicion unjustified? Explain your answer. (iii.) Compare file system time metadata in NTSC and *ext-3*.

2. What is the largest number of partitions a personal computer can have? Justify the answer.

(a) 16
(b) 4
(c) It depends on the partitioning scheme.
(d) 13

3. Peter Zmeda received two discs for analysis. After all, they were on the same computer before. He heard that the owner of the computer may have been using RAID. (i) What special care must Peter take so as not to spoil the evidence? (ii) If GNU/Linux and a normal RAID0 were used on the computer, what sequence of commands can be used to access the data on the file

system? (iii) If RAID0 was not used on the disks, and Peter knows that there was only one huge file system on the computer, what other technology(s) could the computer owner have used? List at least 3 options.

Task 3. *Mobile and network forenzics.*
QUESTIONS:

1. Peter is having network problems on one of his computers - the computer does not receive an IP address. All other computers on the network work normally. The problematic computer works on other networks. Peter suspects that the problem lies with the DHCP server. Which files on the server should he inspect and why (what do they contain)?

1. `/etc/dhcp/dhcpd.conf`, `/etc/services`, `/etc/rc.local`, `/var/log/syslog`, `/var/log/dhcp.log`
2. `/etc/dnsmasq.conf`, `/var/log/syslog`, `/var/db/dnsmasq.leases`, `/var/run/dhcp/dhcpd.leases`
3. `/etc/dnsmasq.conf`, `/var/log/syslog`, `/var/run/dnsmasq/dnsmasq.leases`, `/var/run/dhcp/dhclient.leases`
4. `/etc/dhcp/dhcp.conf`, `/etc/init`, `/var/log/syslog`, `/var/lib/dhcp/dhclient.leases`

2. Detective Naočnik made the following queries on an unknown computer (abbreviated print):

```
Nula-Nula> arp -an
? (192.168.126.187) at 48:65:ee:11:f7:49 on alc0 expires in 210 seconds
? (192.168.126.2) at 54:04:a6:94:54:0b on alc0 permanent
? (192.168.126.1) at 0c:c4:7a:c0:df:ee on alc0 expires in 823 seconds
Nula-Nula> netstat -rn
Routing tables
Internet:
Destination        Gateway            Flags     Netif Expire
default            192.168.126.1      UGS        alc0
127.0.0.1          link#2             UH          lo0
Nula-Nula> ifconfig
alc0: flags=8843<UP,...,MULTICAST> metric 0 mtu 1500
        options=c3198<VLAN_MTU,...,LINKSTATE>
        ether 54:04:a6:94:54:0b
        inet 192.168.126.2 netmask 0xffffff00 broadcast 192.168.126.255
Nula-Nula> ping -c 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=60 time=10.636 ms
```

(i.) Write down the hypothesis of how `Nula-Nula` can access the Internet. (ii.) How would you verify this hypothesis? (iii.) How can he find out which organization (domain) `Nula-Nula` belongs to?

3. Peter Zmeda is investigating data from a mobile phone. It's an Android phone, and Peter got an image of the entire flash memory. (i) Which partitions are usually found on Android phones? Where can we find user data? (ii) Which tool can be used to review the contact database? (iii) To review the data, Peter tried:

```
1   select * from view_contacts
2   No such collation sequence: PHONEBOOK
```

How can he bypass the error?

Task 4. *Investigation.*
QUESTIONS:

1. In which phase of criminal proceedings digital forensics does not participate and why not?

(a) Pre-trial proceedings.
(b) The main hearing.
(c) Assesment of the issuance of a search warrant.
(d) No answer from other answers is correct.

2. The police wants to inspect Cefizel's computer. (i.) In what two cases can it do this? (ii.) In both cases, an individual's privacy is violated. What is the key difference between the two infringements?

3. Peter Zmeda received a server with two hard drives for review. He connected both drives to his computer, on which he runs Ubuntu 22.04 Desktop. It created copies of the disks:

```
1  dd if=/dev/sdc of=prvidisk.raw
2  sha512sum /dev/sdc1
3  cat /dev/sdd > drugidisk.raw
4  sha512sum /dev/sdd1
5  sha512sum prvidisk.raw
6  sha512sum drugidisk.raw
```

Each time he got a different hash value. Then he tried the following commands:

```
1  mount -o ro prvidisk.raw /mnt
2  mount -o ro drugidisk.raw /mnt
```

The computer told him that there was no known file system in the image. (i) Why did he get different hash values? (ii) Was his procedure correct? If so, why? If not, what data did he lose? (iii) How can the filesystems be on both disks with as little extra copying as possible?
