MIDTERM PROGRESS TEST

Course name: Digital Forensics

Course code: FRS301

Class:IA1602

|  |  |
| --- | --- |
| Student name: | Trần Thanh Tuấn |
| Student ID: | SE161095 |

Part 1: Multiple choice (20 questions) (7 marks)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| A |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| B |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| C |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| D |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. The primary component of storage in the personal computer is the:

A) NIC.

B) hard disk drive.

C) zip disk.

D) media card.

2. A set of instructions compiled into a program that performs a particular task is known as:

A) central processing unit.

B) software.

C) motherboard.

D) hardware.

3. How many characters are defined by ASCII?

A. 255

B. 256

C. 128

D. 94

4. Headers and footers can be used to

A) identify the file as well as mark its beginning and end.

B) records the date and time a particular file

C) All of the mentioned

D) None of the mentioned

5. The header of the generic JPEimage file is

A) FF D8

B) FF D9

C) FF DA

D) FF DB

6. Areas of files and disks that are not apparent to the user, and sometimes not even to the operating system, is termed:

A) hidden data.

B) missing data.

C) latent data.

D) exceptional data.

7. The most common storage device for the personal computer is the:

A) USB thumb drive.

B) zip disk.

C) floppy disk.

D) hard disk drive.

8. The volatile memory of the computer is known as:

A) CPU.

B) BIOS.

C) ROM.

D) RAM.

9. Which of the following devices may contain log files?

A) Servers

B) Routers

C) Firewalls

D) All of the mentioned

10. The items to examine in Digital forensic?

A) Laptop and desktop computers

B) Mobile devices

C) Networks

D) All of the mentioned

11. What following statement is true about RAM.

A) RAM is volatile, so data be lost when power goes off.

B) RAM is nonvolatile, so data be lost when power goes off.

C) RAM remains data without power.

D) None of the mentioned.

12. Which of the following evidence is not contained on RAM?

A) Instant messages

B) Network connections

C) Running processes

D) time-stamps

13. Purpose of cloning:

A) Examine a copy, not the original

B) You can recover from mistakes

C) A properly authenticated forensic clone is as good as the original in court

D) All of the mentioned

14. RAM may contain:

A) IP Addresses

B) Trojans

C) Passwords in cleartext

D) ALL of the mentioned.

15. Which of the following shutdown options keeps data in RAM?

A) Sleep

B) Hibernate

C) Soft shutdown

D) Hard shutdown

16. Which of the following commands will enable Hiberation?

A) powercfg -h on

B) hibercfg -h on

C) sleep -h on

D) None of the mentioned

17. What is metadata?

A) Metadata is most often defined as data about data.

B) Metadata is most often defined as bigdata.

C) Metadata is most often defined as relative data.

D) None of the mentioned

18. Which of the follwowing methods will make real obstacles to forensic examiners?

A) Delete cookies

B) Clear temporary internet files

C) Clear history

D) Encryption

19. Anti-forensic prevents \_\_\_\_

A) Forensic investigation process

B) Attacker to attack

C) Security threats

D) Malicious attacks

20. Isolate the phone may prevents:

A) inbound emails, texts, and calls, which could overwrite evidence

B) the battery charge

C) The password requirment

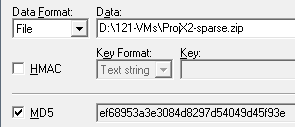
D) None of the mentioned

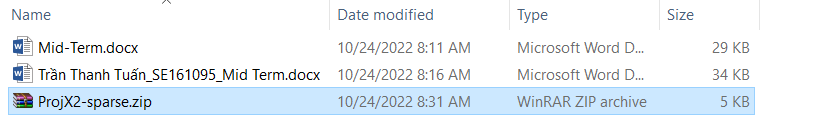
**Part 2: Static Acquisition** (3 marks)

## What You Need for This Project

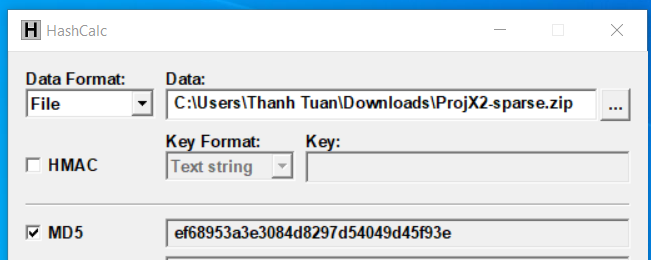
* VMware Workstation
* Any other tools you choose to use

## Getting the Evidence File

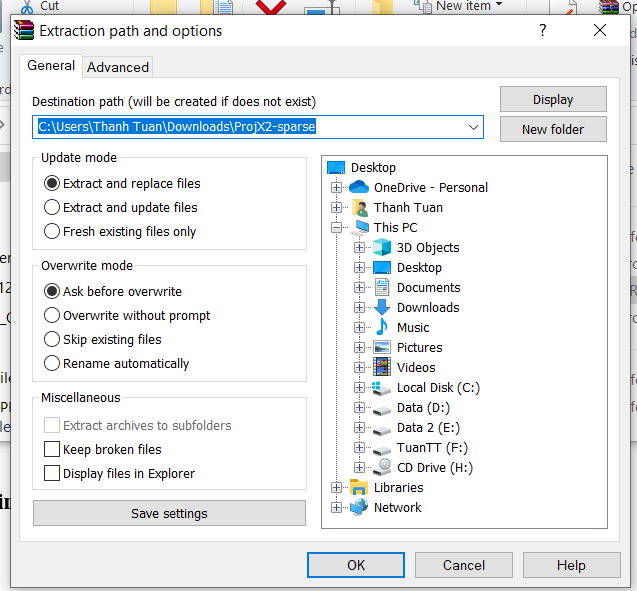
1. Download **ProjX2-sparse.zip** file



1. Calculate the MD5 hash of the file and verify that it matches the value shown to the right on this page.

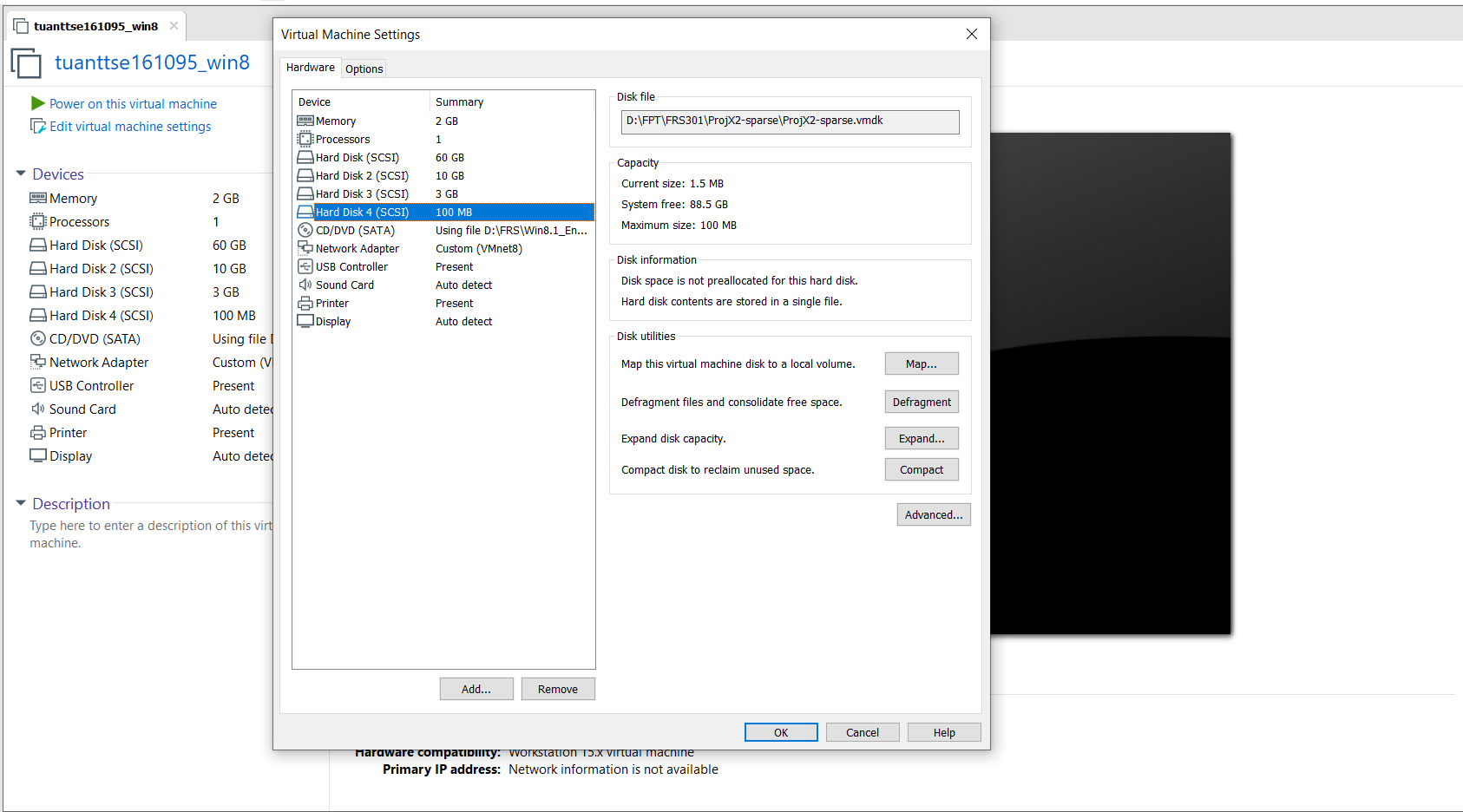


1. Unzip the file to extract the virtual hard disk inside.

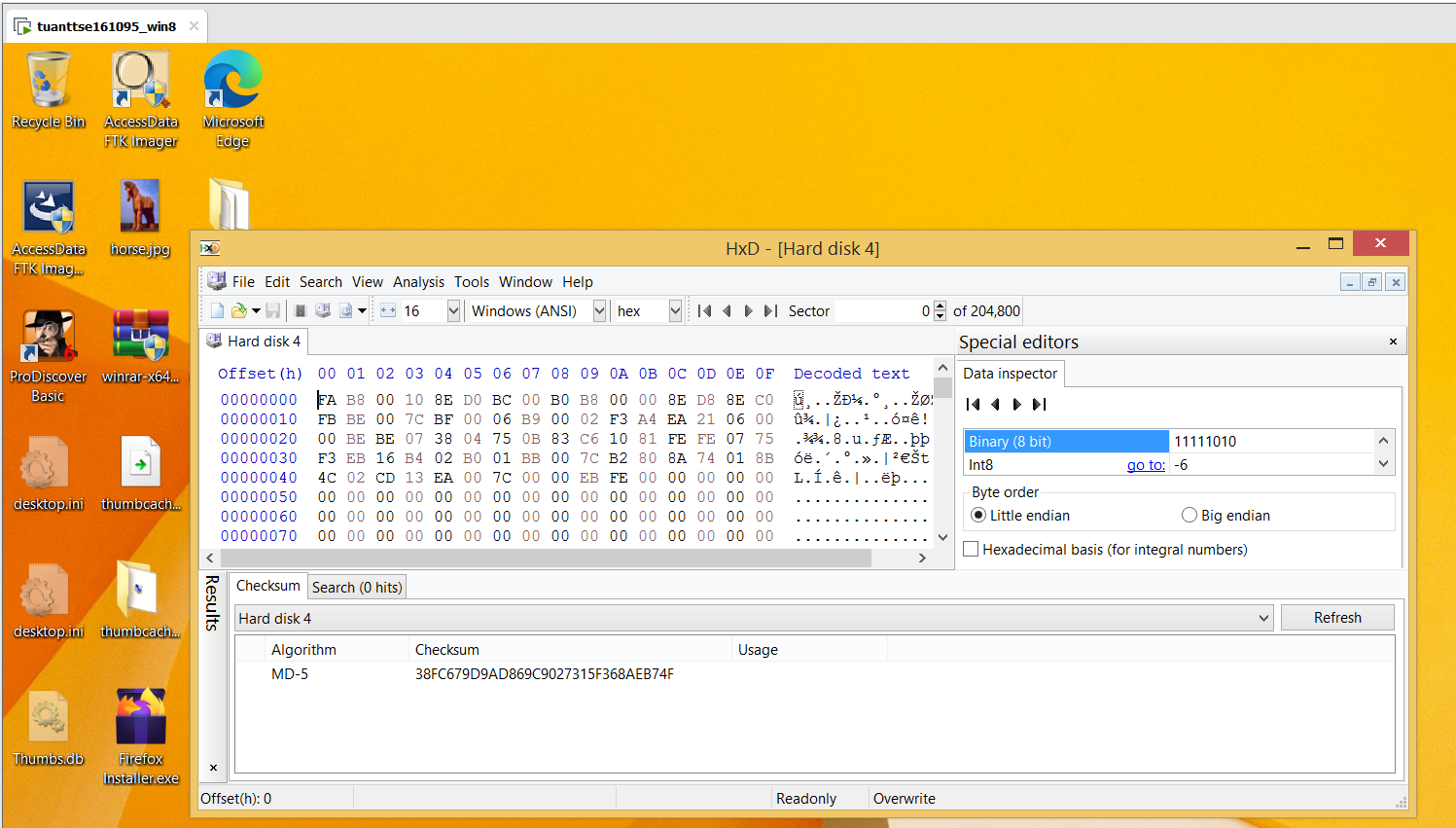


## Imaging the Evidence Drive

1. Mount the evidence drive in an appropriate virtual machine.



1. Use any technique you like to make a correct forensic image of the drive.
2. Calculate the MD5 hash of your forensic image.



## Saving a Screen Image

1. Make sure your screen shows the MD5 of the image, from whatever tool you chose to use.