**Digital Forensics Lab-Tasks**

### 

**Prepared By: Ms.Memoona Sadaf**

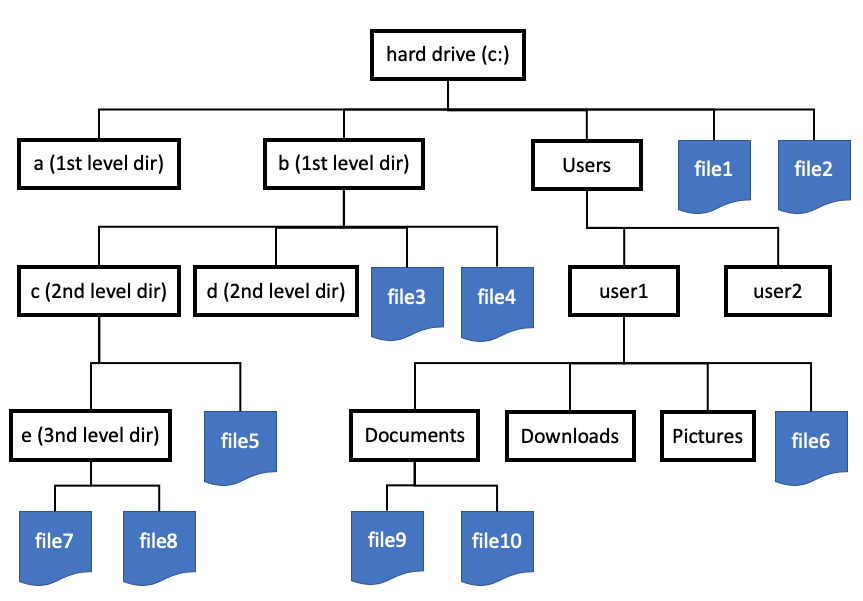
**Instructor: Ms.Memoona Sadaf**

**Lab/Teaching Assistant: Muhammad Ahmad Ali Qureshi**

**Air University Islamabad**

### **Lab Task 1:**

**Total Marks: 10 CLO-2**



1. Write down complete paths for file1-file10 in form of a table.

|  |  |
| --- | --- |
| File1 | Path |

1. Get a USB (recommended size 8-16 GB.) Format it, make a partition of 5

GB in it named (member1.name\_member2.name\_lab). Example:

Memoona\_Sadaf\_lab. You can make another partition for the left space or

keep it unallocated.

{Google is your best and only friend and you are free to ask for help from

it.}

Attach screenshots of work done. {Describe your screenshot in one line

what you have done or what you are showing in this screenshot.}

You will keep this USB with you in your all labs so avoid sharing it or using

someone else’s screenshots (you can share it with your group member).

1. Complete This Basic THM Room of Linux for your understanding also provide the Screenshot of Room Solved with the ***university login***.

<https://tryhackme.com/room/linuxfundamentalspart1>

1. After completing this room you must be able to answer these:

* If we wanted to list all the .log files in the current directory, what command would we use?
* What command can we use to read the contents of the file /etc/group?
* If we wanted to search for the string "Failed" in all files in the /var/log directory, what would our command be?
* What would be the commands to calculate MD5 and SHA1 hashes of the file /etc/passwd?
* Use the file command to determine the type of the file /usr/bin/whoami and explain the output in 2–3 sentences.
* What command can we use to display all printable strings of length ≥ 10 in the file /bin/echo?
* Given the following output of the file command, can you determine what’s wrong with this file?

*$ file image.jpg*

image.jpg: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=3ab23bf566f9a955769e5096dd98093eca750431, for GNU/Linux 3.2.0, not stripped

* If we wanted to find files modified in the last 10 minutes in the /tmp directory, what command would we use?

Hint: Explore how you can use find command to achieve this.

* What command can we use to display all active UDP connections on the system?

Note: Try to give one line/word answer for these! Chat GPT can help you, but there will be no one to help you in VIVA, remember this XD.

***Best of Luck***