Paper Code : A

SUNBEAM INSTITUTE OF INFORMATION TECHNOLOGY
Hinjewadi
Module End Lab Exam – Cyber Forensics

Course Name:	PG – DITISS	**Batch :**	AUG - 25
Module Name:	Cyber Forensics	**Date:**	04/11/2025
Max. Marks:	20	**Duration :**	1:30 Hours
		Group:	_____
Name :	_____	**Roll No. :**	_____

Instructions :

1. Create folder by the name CF_RollNo_FirstName in your home directory.
2. After successful completion of any part, tick mark √ the stage/step in the following self-declaration column. Take appropriate screenshots in above folder.
3. After evaluation compress/zip your folder (named CF_RollNo_FirstName and upload it on EMIS.

Evaluation of Lab Exam should be based on the following criteria :

Self-declaration for Paper Code – A

Sr. No.	Points to cover	Tick Mark by student	Max Marks	Marks by Evaluator
1.	Recover Partitions	☐	6	
2.	Half part of password	☐	1	
3.	Find the information	☐	10	
4.	Browser forensics	☐	3	
			Total : 20	_____

_____ **Signature of Student**

_____ **Signature of Evaluator**

Paper Code : A

The password for the exam1.zip file is -- *CF-exam1@25*

Q.1. The **exam1-part.vmdk** is a SATA hard disk. An employee has deleted the partitions from the hard disk before leaving the job. The employee has saved part of his password in one of the files on this hard disk. Thus recover the partitions and files in it. [6 Marks]

The half part of the password is ---------- [1 Mark]

Q.2. The **exam1.vmdk** is a Linux hard disk (SATA). This machine was used by the above employee. The remaining part of the password is in one of the files on this hard disk. Connect to your forensics vm and mount it in **/cf1** directory. Find following information from it. [10 Marks]

Hint: *sudo vgchange -ay rl*
sudo mount -t xfs /dev/rl/root /c1

A. Name of the computer	1 Mark
B. Usernames and their UID's	1 Mark
C. Users with the sudo permissions	2 Marks
D. Which user installed nmap application	1 Mark
E. Which user created, formatted and mounted partitions	1 Mark
F. Which user created the web1 user	1 Mark
G. Which user deleted the ditiss1 user	1 Mark
H. Which operating system is installed? Kernel Version	1 Mark
I. Part of the password	1 Mark

Q.3. Perform the browsing analysis on the given sqlite files and find out the 6 websites the user has visited. The sqlite files are stored in the **/exam1 (/c1/exam1)** directory in the above hard disk. [3 Marks]

---------- ALL THE BEST ----------