[U19CS012]

Department of Computer Science and Engineering - SVNIT, Surat

Mid Semester Examinations, March - 2023

B.Tech. IV (Semester-VIII)

Course: Cyber Law and Forensics(CS402)

Date: 10-03-2023 **Time: 2.00PM to 3.30PM** **Marks: 30**

Instructions:

1.Write your admission number and other details clearly on your answer sheet and also write your admission number on the questions paper.

2.Be precise and clear in answering the questions.

3.Support your answer with necessary diagrams and examples.

Q1 Answer the following: **[04]**

1 What is the name of a Windows artifact used to identify recently opened files?

2 List down any two tools used for RAM acquisition. dc dd

3 What is the path of the SYSTEM registry hive? dc

4 What is the full form of MFT?

- Belkasoft Live RAM Capture
- Dump It
- magnet

dd fid

c:\users\system32\config

FTK Imager

x registry
x prefetch
Shellbags
→ LNK files x
→ JumpList

Q2 Answer the following in brief (Any three): **[06]**

dd dc

1 What is spoofing? Explain with examples.

2 Differentiate between imaging and cloning.

3 Explain the forensic importance of the write blocker device.

(DBT) [4] List down only names of artifacts that can be analyzed from the Windows registry.

Q3 Answer the following in detail (Any two): **[10]**

1 Explain any five different types of cybercrime.

- phishing

2 Explain following windows artifacts:

a. Prefetch run →
b. Shellbags
c. LNK Files

Windows vista

\R
\MRU

3 Explain the process of crime scene management.

Q4 Answer the following:

ECID

1 What is digital evidence? Point out four challenges that traditional Indian Laws are facing in relation to cybercrime cases. **[03]**

2 Write a short note on the International convention on cybercrime or BUDAPEST Convention. **[02]**

CBSS

3 Explain the meaning of GDPR and highlight its provision and applicability. **[03]**

Data Protection

4 Fill in the blanks: **[02]**

a. The Information Technology Act came into force since _(exact date)_ 17 Oct 2009

b. The Information Technology [Amendment] Act 2008 came into force since _(exact date)_ 27/10/2009