LNJN National Institute of Criminology & Forensic Science
NFSU Delhi Campus

M. Sc. Digital Forensics and Information Security 1st Semester
Term Assessment I (TA-I)

Date of Examination: 21/12/2021

Subject Code & Name: CTMSDFIS SI P2; Cyber Security Audit and Compliance

Time: 45 Minutes **Maximum Marks: 5X5=25**

Answer any **FIVE** questions:

Q1. Define Compliance and name any one existing compliance framework. Also, justify the need for maintaining IT compliance as an ongoing program.

Q2. Differentiate between IT Security Assessment and IT Audit.

Q3. With the help of a case, discuss the possible consequences of non-compliance with regulatory standards.

Q4. Discuss briefly the seven domains of a typical IT infrastructure.

Q5. Write down a few measures that an organization can take to be in compliance.

Q6. What are the various types of audits? Define IT auditing.

LNJN National Institute of Criminology & Forensic Science
NFSU Delhi Campus

TERM ASSESMENT-1
SEMESTER 1 [~~MA CRIMINOLOGY~~] MSc (DFIS)

CTMS DFIS S1 P5

Paper Code: ~~MACR-S1-P3~~
Time: 45 minutes **Maximum Marks: 25**

Note: Attempt all the questions. All questions carry equal marks.

Q1) How Forensic Science helps the Criminal justice system elaborate with example. And also classify various Divisions under Forensic Science Umbrella and their major role in criminal justice system.

Q2) Discuss various principles of forensic science and elaborate with example.

Q3) Demonstrate the Locard'sexchangeprinciplewithexample.

Q4) Discuss thehistory of Forensic Science laboratories in India.

Q5) Explainbrieflyaboutthe following

a) **ForensicAnthropology**
b) **ForensicEntomology**
c) **ForensicPsychiatry**
d) **ForensicOdontology**

LNJN National Institute of Criminology & Forensic Science
NFSU Delhi Campus

M. Sc. Digital Forensics and Information Security 1st Semester
Term Assessment I (TA-I)

Date of Examination: 22/12/2021

Subject Code & Name: CTMSDFIS SI P4- Python and Scripting

Time: 45 Minutes **Maximum Marks: 5X5=25**

Answer any**FIVE** questions:

1. What is a shell? List the name of different Shells available in Linux.
2. Define Shell Variable. Write a script that takes variable input from the user and displays.
3. Compare two values and check if one is greater than other value. Write below script in compare.sh file.
4. Write a script to create a file and check whether the file exists or not.
5. Write a shell script to get the current date, time, username, and current working directory.
6. Perform numeric comparisons in Linux.
   a. <eq>
   b. <ge>
   c. <gt>
   d. <le>
   e. <ne>

LNJN NICFS NFSU DELHI CAMPUS

Term Assessment 1

Subject Name: Computer Forensics **Max Marks: 25**

Subject Code: MSDF SI P1

All Questions are compulsory and carry 01 mark each

1. Convert Binary to octal: 1110100010
   a. 1644
   b. 1642
   c. 1668
   d. None of the above

2. Convert 1100110011011 to hexadecimal
   a. 1990
   b. 199A
   c. 199B
   d. 199C

3. James wants to use a device that enables data to be acquired from a hard disk without modifying the disk data. Which device should he choose
   a. Disk copier
   b. Disk imager
   c. Write Blocker
   d. None of the above

4. This document refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases.
   a. Custody document
   b. FIR
   c. Chain of Custody
   d. None of the above
5. Tina's computer is running very slow. Which memory of the computer is used to speed up the computer processing
   a. RAM
   b. Cache Memory
   c. ROM
   d. None of These

6. Which among the following is not defined as a stage in Computer Forensics as per NIST guidelines.
    a. Repair
    b. Collection
    c. Analysis
    d. Examination

7. Which among the following can be called a volatile memory
    a. ROM
    b. RAM
    c. BIOS
    d. PROM
8. In a binary number, the bit furthest to the left is called the
    a. LSB
    b. MSB
    c. Neither LSB nor MSB
    d. Both LSB and MSB

9. "What are the difficulties in handling Digital Evidence?
    a. Easy to destroy
    b. Easy to sustain
    c. Hard to get
    d. Both a and c

10. "In forensic science, which principle holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.
    a. Henry's Principle
    b. David's Principle
    c. Locard's Priciple
    d. None of these

11. The four phases involved in Forensic process as per NIST guidelines are
    a. Collection, Analysis, Examination and Reporting
    b. Collection, Examination, Analysis and Reporting
    c. Identification, Examination, Analysis and Reporting
    d. None of the above

12. Which type of evidence is likely to be found in all modern-day crime scenes with maximum investigative value.
    a. Traditional evidence
    b. Physical evidence
    c. Digital evidence
    d. None of the above

13. Which of the following is not a type of volatile evidence
    a. RAM data
    b. Log file
    c. Pagefile
    d. ROM

14. Convert decimal to binary: 65
    a. 1000001
    b. 1001001
    c. 1000101
    d. 1000011

15. The group of people who respond to variety of computer security incidents are called
    a. IT Professionals
    b. Forensic Investigators
    c. Incident Handlers
    d. All of the above

16. Subtract using 2's complement. 110101 - 101010
    a. 100100
    b. 100001
    c. 100010
    d. 100110

17. What is the most significant legal issue in computer forensics?
    a. Admissibility of Evidence
    b. Preserving Evidence
    c. Seizing Evidence
    d. Discovery of Evidence

18. Do the binary addition of two nos 100100101+001001001. The result should be in binary format.
    a. 110010010
    b. 101101010
    c. 101011110
    d. 101101110

19. When the least significant bytes are stored before the most significant bytes then that format is called
    a. Big Endian
    b. Little Endian
    c. Red Endian
    d. White Endian

20. Volatile data can be found in
    a. Registry
    b. Cache
    c. RAM
    d. All of the above

21. Using swap space significantly _____ system performance
    a. Decrease
    b. Increase
    c. Maintain
    d. Does Not affect

22. NIST stands for
    a. National Institute of Surfing and Transition
    b. National Institute of Standards and Technology
    c. National Institute of Studies and Technology
    d. None of the above

23. When capturing online evidence what data is of importance
    a. Network forensics
    b. Volatile data
    c. Both a and b
    d. None of the above

24. NIST guidelines are made keeping forensics in mind from which perspective
    a. IT view
    b. Law Enforcement view
    c. Investigation view
    d. All of the above

25. A write blocker is any tool that permits
    a. Read-only access to data storage devices
    b. Does not compromise the integrity of the data
    c. Can guarantee the protection of the data chain of custody
    d. All of the above