Code No: 56053 **Set No. 1**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

III B.Tech. II Sem., II Mid-Term Examinations, April – 2014

COMPUTER FORENSICS

Objective Exam

Name: _____ Hall Ticket No. | | | | | | A | | | | |

Answer All Questions. All Questions Carry Equal Marks.Time: 20 Min. Marks: 10.

I Choose the correct alternative:

1. Which of the following step is most important while computing investigations [ ]
   a. Preparing for a computer search and seizure b. Securing a computer incident
   c. Storing digital evidence d. Identify digital evidence

2. The DOS program command *com* is altered by changing which of the following commands [ ]
   a. Dir command to Deltree command b. Tree command to Deltree command
   c. Deltree command to Dir command d. Dir command to tree command.

3. Which of the following analysis tool has the capability to analyze image files [ ]
   a. ProDiscover b. EnCase c. ILook d. All the above

4. Which of the following is not a sub function of reconstruction [ ]
   a. Partition-to-partition copy b. Disk-to-disk copy
   c. Image-to-image copy d. Image-to-disk copy

5. What is the e-mail storage format in Novell evolution [ ]
   a. MAPI b. mbox c. MIME d. PDF

6. What type of computer architecture is used while accessing e-mail [ ]
   a. Domain b. Client/server c. Mainframe and mini computers d. None

7. Which of the following DOS commands creates a subdirectory [ ]
   a. Vol b. Rd c. Md d. Cd

8. Sectors typically contains how many bytes [ ]
   a. 256 b. 512 c. 1024 d. 2048

9. Which of the following tools can examine files created by WinZip [ ]
   a. Registry viewer b. SMART c. FTK d. Hex workshop

10. Which function of computer forensics tools perform hashing, filtering and file header analysis [ ]
    a. Validation and discrimination b. Acquisition c. Extraction d. Reporting

Cont……2

II Fill in the blanks

11. FOIA stands for_____

12. The SATA cable and evidence log forms are found in an _____ field kit.

13. _____ are developed to prevent data writes to a disk drive.

14. The primary hash NSRL uses is _____

15. Phishing emails are in _____ format.

16. Phone store system data in_____

17. _____ is used to access Autosy's tools.

18. _____ tools are commonly used to copy data from a suspects disk drive to an image file.

19. The _____ structure makes the GroupWise folder and file structure complex

20. The troubleshooting log is also known as a _____

-oOo-

Code No: 56053 **Set No. 2**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

III B.Tech. II Sem., II Mid-Term Examinations, April – 2014

COMPUTER FORENSICS

Objective Exam

Name: _____ Hall Ticket No. | | | | | | A | | | | |

Answer All Questions. All Questions Carry Equal Marks.Time: 20 Min. Marks: 10.

I Choose the correct alternative:

1. Which of the following is not a sub function of reconstruction [ ]
   a. Partition-to-partition copy b. Disk-to-disk copy
   c. Image-to-image copy d. Image-to-disk copy

2. What is the e-mail storage format in Novell evolution [ ]
   a. MAPI b. mbox c. MIME d. PDF

3. What type of computer architecture is used while accessing e-mail [ ]
   a. Domain b. Client/server c. Mainframe and mini computers d. None

4. Which of the following DOS commands creates a subdirectory [ ]
   a. Vol b. Rd c. Md d. Cd

5. Sectors typically contains how many bytes [ ]
   a. 256 b. 512 c. 1024 d. 2048

6. Which of the following tools can examine files created by WinZip [ ]
   a. Registry viewer b. SMART c. FTK d. Hex workshop

7. Which function of computer forensics tools perform hashing, filtering and file header analysis [ ]
   a. Validation and discrimination b. Acquisition c. Extraction d. Reporting

8. Which of the following step is most important while computing investigations [ ]
   a. Preparing for a computer search and seizure b. Securing a computer incident
   c. Storing digital evidence d. Identify digital evidence

9. The DOS program command *com* is altered by changing which of the following commands [ ]
   a. Dir command to Deltree command b. Tree command to Deltree command
   c. Deltree command to Dir command d. Dir command to tree command.

10. Which of the following analysis tool has the capability to analyze image files [ ]
    a. ProDiscover b. EnCase c. ILook d. All the above

Cont……2

II Fill in the blanks

11. The primary hash NSRL uses is _____
12. Phishing emails are in _____ format.
13. Phone store system data in_____
14. _____ is used to access Autosy's tools.
15. _____ tools are commonly used to copy data from a suspects disk drive to an image file.
16. The _____ structure makes the GroupWise folder and file structure complex
17. The troubleshooting log is also known as a _____
18. FOIA stands for_____
19. The SATA cable and evidence log forms are found in an _____ field kit.
20. _____ are developed to prevent data writes to a disk drive.

-oOo-

Code No: 56053 **Set No. 3**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

III B.Tech. II Sem., II Mid-Term Examinations, April – 2014

COMPUTER FORENSICS

Objective Exam

Name: _____ Hall Ticket No. | | | | | | A | | | | |

Answer All Questions. All Questions Carry Equal Marks.Time: 20 Min. Marks: 10.

I Choose the correct alternative:

1. What type of computer architecture is used while accessing e-mail [ ]
   a. Domain b. Client/server c. Mainframe and mini computers d. None

2. Which of the following DOS commands creates a subdirectory [ ]
   a. Vol b. Rd c. Md d. Cd

3. Sectors typically contains how many bytes [ ]
   a. 256 b. 512 c. 1024 d. 2048

4. Which of the following tools can examine files created by WinZip [ ]
   a. Registry viewer b. SMART c. FTK d. Hex workshop

5. Which function of computer forensics tools perform hashing, filtering and file header analysis [ ]
   a. Validation and discrimination b. Acquisition c. Extraction d. Reporting

6. Which of the following step is most important while computing investigations [ ]
   a. Preparing for a computer search and seizure b. Securing a computer incident
   c. Storing digital evidence d. Identify digital evidence

7. The DOS program command *com* is altered by changing which of the following commands [ ]
   a. Dir command to Deltree command b. Tree command to Deltree command
   c. Deltree command to Dir command d. Dir command to tree command.

8. Which of the following analysis tool has the capability to analyze image files [ ]
   a. ProDiscover b. EnCase c. ILook d. All the above

9. Which of the following is not a sub function of reconstruction [ ]
   a. Partition-to-partition copy b. Disk-to-disk copy
   c. Image-to-image copy d. Image-to-disk copy

10. What is the e-mail storage format in Novell evolution [ ]
    a. MAPI b. mbox c. MIME d. PDF

Cont……2

II Fill in the blanks

11. Phone store system data in_____

12. _____ is used to access Autosy's tools.

13. _____ tools are commonly used to copy data from a suspects disk drive to an image file.

14. The _____ structure makes the GroupWise folder and file structure complex

15. The troubleshooting log is also known as a _____

16. FOIA stands for_____

17. The SATA cable and evidence log forms are found in an _____ field kit.

18. _____ are developed to prevent data writes to a disk drive.

19. The primary hash NSRL uses is _____

20. Phishing emails are in _____ format.

-oOo-

Code No: 56053 **Set No. 4**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

III B.Tech. II Sem., II Mid-Term Examinations, April – 2014

COMPUTER FORENSICS

Objective Exam

Name: _____ Hall Ticket No. | | | | | | A | | | | |

Answer All Questions. All Questions Carry Equal Marks.Time: 20 Min. Marks: 10.

I Choose the correct alternative:

1. Sectors typically contains how many bytes [ ]
   a. 256 b. 512 c. 1024 d. 2048

2. Which of the following tools can examine files created by WinZip [ ]
   a. Registry viewer b. SMART c. FTK d. Hex workshop

3. Which function of computer forensics tools perform hashing, filtering and file header analysis [ ]
   a. Validation and discrimination b. Acquisition c. Extraction d. Reporting

4. Which of the following step is most important while computing investigations [ ]
   a. Preparing for a computer search and seizure b. Securing a computer incident
   c. Storing digital evidence d. Identify digital evidence

5. The DOS program command *com* is altered by changing which of the following commands [ ]
   a. Dir command to Deltree command b. Tree command to Deltree command
   c. Deltree command to Dir command d. Dir command to tree command.

6. Which of the following analysis tool has the capability to analyze image files [ ]
   a. ProDiscover b. EnCase c. ILook d. All the above

7. Which of the following is not a sub function of reconstruction [ ]
   a. Partition-to-partition copy b. Disk-to-disk copy
   c. Image-to-image copy d. Image-to-disk copy

8. What is the e-mail storage format in Novell evolution [ ]
   a. MAPI b. mbox c. MIME d. PDF

9. What type of computer architecture is used while accessing e-mail [ ]
   a. Domain b. Client/server c. Mainframe and mini computers d. None

10. Which of the following DOS commands creates a subdirectory [ ]
    a. Vol b. Rd c. Md d. Cd

Cont……2

II Fill in the blanks

11. _____ tools are commonly used to copy data from a suspects disk drive to an image file.
12. The _____ structure makes the GroupWise folder and file structure complex
13. The troubleshooting log is also known as a _____
14. FOIA stands for_____
15. The SATA cable and evidence log forms are found in an _____ field kit.
16. _____ are developed to prevent data writes to a disk drive.
17. The primary hash NSRL uses is _____
18. Phishing emails are in _____ format.
19. Phone store system data in_____
20. _____ is used to access Autosy's tools.

-oOo-