SRN | | | | | | | | | | | |

PES UNIVERSITY

PES University, Bangalore
(Established under Karnataka Act No. 16 of 2013)

UE16CS433

END SEMESTER ASSESSMENT (ESA) B.TECH III SEMESTER- Dec 2019

UE16CS433 – Computer Forensics

Time: 3 Hrs | Answer All Questions | Max Marks: 100

Note: All answers must be precise and to the point.

1	a)	Define computer forensics. How can you differentiate Digital Forensics and Anti Digital Forensics with an example	6 (3+3)
	b)	Consider the scenario wherein you have created a process that opens a file. Then Unlink the file. Answer the following questions below in detail. i. Can you still write to the file? If yes/No, then give the proper explanation. ii. Is the file visible to the "ls" command? If not how do you find them?	5
	c)	Given below are various resources. Analyze carefully and Order them in the order of volatility from most volatile to least volatile 1.Remote logging and monitoring data 2.Temporary File systems 3.Disks 4.CPU Registers and CPU Cache 5.Router table,Kernel Statistics,Process Table 6.Archival Media 7.Physical configuration and Network Topology	6
	d)	What do you think are the challenges in Digital forensics?	3
2.	a)	Below are some of the important commands for collecting volatile data and transfer. Give a one line functional explanation for each of them. 1.cryptcat –l -p 1234 >sample.txt 2.UNAME 3.UPTIME 4.free	4
	b)	Explain in detail the use of the UNIX Utility "dd" . Also give the steps to carve out a portion of data from the source device using various dd options with an example	7
	c)	What is a Master Boot Record? Explain its structure in detail	5
	d)	Assume the suspect's machine is a LINUX/UNIX based computer instead of Windows platform. Do you think if the operating system affects the computer forensic investigation process at all? Give a proper Justification points.	4
3.	a)	What happens when a new file is created in a EXT2 file system? Explain the steps in detail with respect to inodes and superblock entries. Also justify why it is not possible to recover a deleted file in EXT3/4 filesystems.	7

SRN | | | | | | | | | | | |

	b)	Give atleast four differences between a hard link and a soft link on Linux file system with a diagram? Give its syntax and mention about the link count.	5
	c)	i) What is the use of $BITMAP attribute in a master file table? ii) How do you describe REFS file system? Which of the problems of NTFS file system this addresses?	6
	d)	Explain the concept of Registry Hives in Windows?	2
4.	a)	Explain in detail the concept of MAC times in Linux/Unix file systems? Given a sequence of commands Timeline example i) Mon Dec,23 2019 3:30:34 6524 .a. –rwr-wx-wx 0 0 filepath/sample_pes ii) Mon Dec,23 2019 4:10:22 6524 –rwr-wx-wx 0 0 filepath/sample_pes iii) Mon Dec, 23 2019 4:11:32 Then do echo "newdata" >> sample_pes iv) Then do touch –m –d '2012-01-02 06:43:45' sample_pes After executing the timeline commands, echo and touch commands in sequence what will be the modified time, access time and changed time of the file sample_pes?	5
	b)	What are the different modes in which the HELIX3 forensic tool operates on?	3
	c)	Explain the concept of Cold Boot Attack for doing a memory dump on Windows machine. Give a proper flow diagram briefing the steps till the passphrase is obtained.	8
	d)	Why do you think the slack spaces in the Windows system memory are of great importance to forensic investigators? Also briefly describe the "clusters" in any Windows system.	4
5.	a)	i) Briefly explain the FAT File system structure for Windows. ii) What happens to a deleted file in a FAT File System?	6 (3+3)
	b)	What happens when a disk is done a quick format? Give detailed steps. Will you be able to recover the deleted contents? Below are some scenarios. Provide a suitable suggestion whether to go for a quick or a full format? S1:When you want to sell an external 1 TB harddisk on OLX S2:To Clear partition with unnecessary files to free up space S3:The Installation of new Operating system S4: The hard disk is very old and there are many bad sectors on it S5:When your computer is infected with a backdoor malware S6:When your file system is damaged and the OS prompts you to format it before you can use it	8
	c)	What is Steganography and compare it with cryptography with respect to its • Definition • Its Purpose • Data Visibility • Key Explain the LSB Encoding method involved in Substitution technique with an example	6