B.E/B.TECH. DEGREE EXAMINATIONS, September 2020

Eighth Semester

IT16013 – CYBER FORENSICS

(Regulation 2016)

Time: Three Hours **Maximum : 80 Marks**

Answer **ALL** questions

PART A - (8 X 2 = 16 Marks)

		CO	RBT
1.	_____ is an encryption tool that was introduced with the Ultimate and Enterprise editions of Microsoft Windows Vista, which allows for encryption at the file, folder, or drive level and _____ is a tool that produces a bit-for-bit copy of original media, including files marked for deletion. a) Bitlocker, Bit image tool b) Datalocker, Bit state imaging tool c) Bitlocker, Bitstream imaging tool d) Datalocker, Bit image tool	1	2
2.	Which of the following functions can be used to verify the integrity of the time data that is stored in the computer? (Choose all that apply) a) SHA256 b) MD5 c) AES d) S/MIME	2	2
3.	In a Linux shell, which of the following command can be used to acquire data from the drive /svce/hd along with its sha256 hash value? a) dcfldd if=/svce/hd split=2M of=hd_image.img hash=sha256 b) dcfldd if=/svce/hd split=2M of=hd_image.img hash=md5 c) dcfldd if= hd_image.img split=2M of=/svce/hd hash=sha256 d) dcfldd if= hd_image.img split=2M of=/svce/hd hash=md5	2	2
4.	E-mail headers contain which of the following information? (Choose all that apply) a) The sender and receiver e-mail addresses b) Username and password c) Server logs d) The e-mail servers the message travelled through to reach its destination	3	3
5.	How automatic defragmentation is not helpful for the forensic investigators? Justify your answer.	2	4
6.	Analyse how 16 bits are enough to represent the time in a computer system instead of 17 bits?	4	2
7.	Justify the need of RAID in computers.	3	4
8.	How is pharming different from spoofing in network attacks?	5	4

PART B - (4 X16 = 64 Marks)

9.	(a)	(i)	Decode the following message: 496E666F726D6174696F6E207365637572697479206973206D616E6461746F7279	**(8)**	1	**3**
		(ii)	You work for a mid-size corporation known for its inventions that does a lot of copyright and patent work. You're investigating an employee suspected of selling and distributing animations created for your corporation. Describe the process of copying the data from the suspect's drive using any one of the forensic tool.	**(8)**		
			(OR)			
	(b)	(i)	Calculate the RAM, Drive and File Slack for the following: Cluster with 1000 sectors each of size 4096 bytes, File of size: 0.5Mb is stored	**(8)**	1	**3**
		(ii)	Calculate the RAM, Drive and File Slack for the following: Cluster with 200 sectors each of size 2048 bytes, File of size: 5000 bytes is stored	**(8)**		
10.	(a)	(i)	As part of the duties of a digital forensics examiner, creating an investigation plan is a standard practice. Write a paper that describes how you would organize an investigation for a potential fraud case. In addition, list methods you plan to use to validate the data collected from drives and files, such as Word and Excel, with hashes. Specify the hash algorithm you plan to use, such as MD5 or SHA1.	**(16)**	2	**3**
			(OR)			
	(b)	(i)	Your digital forensics company has been hired to verify the local police department's findings on a current case. Tension over the case is running high in the city. What do you need to ask the police investigator for, and what procedures should you follow? You should also take date and time values into consideration as part of your opinion on the files' validity. In addition, give an opinion on any legal correspondence you found in this examination.	**(16)**	2	**3**
11.	(a)	(i)	You're a detective for the local police. Thomas Brown, the primary suspect in	**(16)**	3	**4**

a murder investigation, works at a large local firm and is reported to have two windows computers at work in addition to one at home. What do you need to do to gather evidence from these computers, and what obstacles can you expect to encounter during this process?

(OR)

(b)	(i)	You're investigating a case involving a 2 GB drive that you need to copy at the scene. Write one to two pages describing various file formats for generating the disk image of the drive accurately. Be sure to include your software and media choices.	**(16)**	3		**4**
12.	(a)	(i)	A cloud customer has asked you to do a forensics analysis of data stored on a CSP's server. The customer's attorney explains that the CSP offers little support for data acquisition and analysis but will help with data collection for a fee. Elucidate the steps in acquiring the data from the cloud storage in detail.	**(16)**	4	**4**

(OR)

(b)	(i)	You have acquired the mobile device of the suspect from the crime scene. It has a pattern lock enable to protect the contents from being exposed. One of your colleagues has a licensed version of Oxygen Forensics and OS Forensics. How will you examine the data using both the tools?	**(16)**	5		**4**