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

PES

PES UNIVERSITY, BANGALORE

UE17CS543

(Established under Karnataka Act No. 16 of 2013)

END SEMESTER ASSESSMENT (ESA) M.TECH II SEMESTER- MAY 2018

UE17CS543 – CYBER FORENSICS and IOT SECURITY

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

1.	a)	Evidentiary files and data relating to Internet searches and websites visited are more readily available while the computer is turned on - Justify	05
	b)	What is a file slack? Suppose you have an NTFS drive with 512 byte sectors, 8 sectors per cluster and the size of a cluster is 4096 bytes. Further, you have stored a file of 5100 bytes long on the disk. What is the file slack in this case? Note: NTFS systems works on clusters and not sectors and 20 bytes is RAM slack.	05
	c)	Assume that you have a Windows XP, Vista, 7 / 8 / 10 system and you try to explore Windows File Registry using regedit, then a Registry Editor dialog box displays with five hives. Discuss the contents of these five hives.	05
	d)	Discuss the terms journaling and alternate data stream wrt NTFS file systems.	05
2.	a)	What is Global System for Mobile Communications? Discuss about recent two standards associated with it. From the forensics perspective what challenge does it pose?	06
	b)	Back in October of 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN. This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to login, infecting them with malware. These devices were things like digital cameras and DVR players. List any four IoT security lessons that businesses can take from the incident.	04
	c)	A smart city is one in which traffic lights and parking sensor technologies improve traffic patterns and reduce both parking issues and the carbon dioxide emissions caused by them. Smart trash cans inform the city when they need to be emptied, smart water pipes can measure quality, leakage, and more, and bus and train stops let passengers know when their ride is set to be there, in real-time. Identify an IoT vulnerability associated with each of them discussed.	04
	d)	Discuss how SMS can act as evidence in mobile device and sim forensics	06
3.	a)	Bring out the significance of Dynamic Host Configuration Protocol. Discuss the three essential attributes / information provided by DHCP server to its client.	05
	b)	List the UNIX / LINUX commands for displaying routing table, arp table, network status, network interface and hosts	05
	c)	What is SYN Flood attack? Which layer of OSI model is it associated with? Suggest a tool that can be used to monitor it.	06
	d)	Assume that you and your friends are traveling from Bengaluru to Chennai by road (your car). After driving for about 100 kms you have stopped at a popular café for breakfast. During breakfast your friend receives a message for payment of his postpaid mobile connection and he decides to connect to free wifi provided by the café. The café itself has cyber lounge and your friend also has his laptop. Which would you suggest for your friend for net-banking either his laptop or desktop owned by café?	04

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

4.	a)	What is preservation order of evidence? Discuss the role of service provide w.r.t the same.	05
	b)	During the investigation, documenting the investigation plays a vital role. Assume that you are investigating a digital crime at a University and you have been assigned the task of collecting evidence w.r.t RAID systems available in the university. What details do you capture about RAID systems?	04
	c)	With a suitable example narrate why documenting chain of custody is crucial in computer forensics.	06
	d)	You have been called to the residence of a suspected drug dealer. At the residence, you are informed that there is a Sony Vaio laptop and a Samsung Galaxy S4. Outline the steps you will take in the possible onsite examination of these devices. You should note how to properly document and handle these devices based on published guidelines for law enforcement. Describe what other hardware present at the home could be of evidentiary value to the investigator.	05
5.	a)	Consider the two phrases: "Email evidence is in the email itself" and "Email evidence is left behind as the email travels" – Comment	05
	b)	Highlight on the features of the following tools to document an investigation: Network Analyzer and the Cop App	05
	c)	With suitable examples explain how LINUX / UNIX commands can be used to image individual disk partitions or entire disk of the victim / suspect.	05
	d)	With a suitable example, illustrate why digital evidence admissibility is difficult in law.	05

****