PES UNIVERSITY, BANGALORE
(Established under Karnataka Act No. 16 of 2013)

UE16CS615

END SEMESTER ASSESSMENT (ESA) M.TECH. III SEMESTER- Dec. 2017
UE16CS615 - CYBER FORENSICS AND IOT SECURITY

Time: 3 Hrs	Answer All Questions	Max Marks: 100

1.	a)	Photographs have even greater importance today than they did 20 years ago – Comment	05
	b)	Detail the process that occurs when the power button on a personal computer is pressed to start a system.	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)	Assume that you are working as an investigator in Forensics Science Lab and have been assigned to a cyber crime investigation. The suspect worked as the team lead of product development for a software company based in Bangalore. The suspect was questioned about a number of expensive international telephone calls. Further inspection of the suspect's telephone records revealed that the suspect had been calling a software development competitor based in China with office in Bengaluru. When confronted, the suspect stated the need for consultation with lawyer and had no further comment. The suspect did not turn up to office the next day. The local police were contacted the following day by the company. The suspect was caught trying to board a one-way flight to Beijing two days after being questioned. Detail the types of digital evidence you will need for this investigation.	05
2.	a)	The rapid expansion of IoT technology brings with it an array of exciting and imaginative ways to make our products smarter and our lives easier. But the growth of this emerging technology also brings with it huge gaps in security. However, IoT is plagued with vulnerabilities with a potential to disrupt infrastructure. Discuss few of the significant IoT vulnerabilities.	05
	b)	In what ways could the cellphone carrier assist you in your investigation?	05
	c)	What are the two stages in Android boot loader?	04
	d)	Discuss how SMS can act as evidence in mobile device and sim forensics	06
3.	a)	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?	05
	b)	Bring out the legal dimension of cloud forensics.	05
	c)	Discuss the main functionalities of DHCP server and SMTP server.	·05
	d)	Bring out the significance of packet sniffer from forensic perspective.	05

4.	a)	Assume that you have been assigned the task for doing a live forensics examination of a crime scene. Narrate the steps that you to take to succeed in your task.	05
	b)	With a suitable example narrate why documenting chain of custody is crucial in computer forensics.	05
	c)	What is preservation order of evidence? Discuss the role of service provide w.r.t the same.	05
	d)	Narrate how email headers can serve as evidence for forensics investigator.	05
5.	a)	Trial Courts of Limited Jurisdiction are limited to hearing certain types of cases. What are the different courts included under this category?	08
	b)	Discuss the three primary bodies of law that exist in the United States.	06
	c)	With a suitable example, illustrate why digital evidence admissibility is difficult in law.	06

****