
UE15CS615

PES UNIVERSITY

PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

NOVEMBER 2016: END SEMESTER ASSESSMENT
M.TECH. III SEMESTER CSE & SE

UE15CS615: CYBER FORENSICS AND IOT SECURITY

Time: 180 Mins Answer All Questions Max Marks: 100

1		On the basis of the following case study answer the questions that follows. **Case study: Drug Diversion, Brand Protection, Counterfeiting and International Fraud** A pharmaceutical company began receiving complaints from its representatives in certain geographical areas that sales of normally high volume drugs were slowing down considerably. The company's internal security department, as well as the security departments of its major distributors, began an investigation. The results of the investigations led the security professionals to believe a significant amount of the company's product was being diverted from foreign countries into the United States and sold through smaller distributors who specialized in sales to locally, privately owned pharmacies and dispensaries within nursing homes. The diversion activities were immediately reported to the local authorities in the regions, as well as to the FDA. An investigation was immediately launched and millions of dollars of diverted drugs and repackaging equipment was seized from several locations, including the warehouses of fully licensed pharmaceutical distributors. Along with the diverted product, the computers and other electronic equipment were also seized. But majority of communications between the principals of the distribution companies (foreign nationals) and the foreign suppliers was conducted by email. There were also virtually no paper records on site. While the local authorities and the FDA had access to computer forensic labs, both faced similar roadblocks in their investigations; the labs were severely backlogged and the systems were encrypted and fairly complex, as well as being in a foreign language.	
	a)	Investigate the team's suspicions and suggest the team how drugs and other electronic equipment got diverted?	10
	b)	Carry out a detailed email forensics investigation to see whether you can trace the cause of the problems, and prepare a case against the perpetrators.	10
2	a)	What are the techniques used for minimizing footprints as a measure for anti-forensics?	5
	b)	Give 3 commands in linux which can be used for data recovery. Explain.	5
3	a)	What are the components of a sim card? Explain the evidence values of a sim card?	5
	b)	Explain the functions of the following registry HKEYs: i. HKEY_CLASS_ROOT ii. HKEY_CURRENT_USER	10

PTO

		iii. HKEY_LOCAL_MACHINE iv. HKEY_USERS v. HKEY_CURRENT_CONFIG	
4	a)	How is live forensics different from digital forensics? What are the challenges of live forensics? Enumerate the steps for live acquisition?	**10**
	b)	What are the types of data transfers in a USB?	**5**
5	a)	Explain the email architecture?	**5**
	b)	What are the various email forensic investigation techniques?	**10**
6		Companies who recycle their computers by selling them on to someone else will aim to erase all data on their hard drive. However, this may not always be successful.	
	a)	Outline how formatting the disk may not in fact achieve this aim.	**5**
	b)	Outline the possible effects on privacy if all of the data is not erased.	**5**
7	a)	What do we need to conduct an investigation involving Internet abuse? Enumerate the steps for processing of an internet abuse case.	**10**
	b)	Describe the method for performing a remote investigation?	**5**