Total No. of Questions: 6 *Total No. of Printed Pages:2*

Enrollment No......................................

Faculty of Engineering

End Sem (Odd) Examination Dec-2019

IT3EI02 Cyber Security & Forensics

Programme: B.Tech. Branch/Specialisation: IT

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d.

Q.1 i. Which is the legal form of hacking based on which jobs are provided in IT industries and firms? 1

(a) Cracking (b) Non ethical Hacking
(c) Ethical hacking (d) Hactivism

ii. According to the CIA Triad, which of the below-mentioned element is not considered in the triad? 1

(a) Confidentiality (b) Integrity
(c) Authenticity (d) Availability

iii. What is the most significant legal issue in computer forensics? 1

(a) Preserving Evidence
(b) Seizing Evidence
(c) Admissibility of Evidence
(d) Discovery of Evidence

iv. When a forensic copy is made, in what format are the contents of the hard drive stored? 1

(a) As compressed images (b) As bootable files
(c) As executable files (d) As operating system files

v. The ability to hide data in another file is called 1

(a) Encryption (b) Steganography
(c) Data parsing (d) Both (a) and (b)

vi. Computer memory files written to the hard drive are called ______ 1

(a) Metadata (b) Swap files (c) Spool files (d) User profiles

vii. What is IMSI stands for? 1

(a) Internet Mobile Subscriber Identifier
(b) International Mobile Subscriber Identity
(c) Internet Machine Subscriber Identity
(d) International Machine Substitute Identifier

P.T.O.

viii. Which number is commonly printed on the SIM cards? 1

(a) IMSI number (b) ICCID Number
(c) Both (a) and (b) (d) None of these

ix. UDID stands for 1

(a) Unique Device Identifier
(b) Unique Data Intercepting Device
(c) Unique Device Intercepting Data Module
(d) None of these

x. As per cyber security professionals what is primary role of cyber security expert? 1

(a) Security records (b) Imaging records
(c) Moving records (d) Avoiding threats on records

Q.2 i. Explain the need of cyber security in cyber space. **3**

ii. Justify the role of "CIA" triad in gaining trust for cyber security. **7**

OR iii. Explain the importance of security standards in network security. **7**

Q.3 i. What are the various sources of digital evidence? **3**

ii. Compare digital evidence with physical evidence on various parameters (minimum 3 parameters) using table or diagram. **7**

OR iii. Explain in detail about imaging process. What are the different file formats of disk imaging? **7**

Q.4 i. Justify the need of cyber forensics tools. **3**

ii. How Cyber forensics can help data recovery mechanism. Explain using example. **7**

OR iii. Explain various phases in cyber forensics investigation using diagram. **7**

Q.5 i. Compare live analysis and dead analysis using example. **4**

ii. Differentiate between network forensics and mobile forensics. (minimum 3 parameters) **6**

OR iii. Explain role of SIM forensics in detecting financial fraud. **6**

Q.6 Write short note on (any two)

i. Role of cyber forensics investigator **5**

ii. Application of digital forensics **5**

iii. Cyber investigation at society level **5**

******

Marking Scheme
IT3EI02 Cyber Security & Forensics

Q.1	i.	Which is the legal form of hacking based on which jobs are provided in IT industries and firms?		**1**
		(c) Ethical hacking		
	ii.	According to the CIA Triad, which of the below-mentioned element is not considered in the triad?		**1**
		(c) Authenticity		
	iii.	What is the most significant legal issue in computer forensics?		**1**
		(c) Admissibility of Evidence		
	iv.	When a forensic copy is made, in what format are the contents of the hard drive stored?		**1**
		(a) As compressed images		
	v.	The ability to hide data in another file is called		**1**
		(d) Both (a) and (b)		
	vi.	Computer memory files written to the hard drive are called ______		**1**
		(b) Swap files		
	vii.	What is IMSI stands for?		**1**
		(b) International Mobile Subscriber Identity		
	viii.	Which number is commonly printed on the SIM cards?		**1**
		(b) ICCID Number		
	ix.	UDID stands for		**1**
		(a) Unique Device Identifier		
	x.	As per cyber security professionals what is primary role of cyber security expert?		**1**
		(d) Avoiding threats on records		
Q.2	i.	Need of cyber security in cyber space.		**3**
	ii.	Role of “CIA” triad in gaining trust for cyber security		**7**
		Confidentiality	1 mark	
		Integrity	1 mark	
		Availability	1 mark	
		Trust factor with importance of trust	4 marks	
OR	iii.	Importance of security standards in network security		**7**
		Security standard	5 marks	
		Network security parameters	2 marks	
Q.3	i.	Evidences available at multiple sources		**3**
	ii.	Digital evidence with physical evidence Minimum three parameters		**7**
		2 marks for each (2 marks *3)	6 marks	
		Table or diagram	1 mark	
OR	iii.	Imaging process		**7**
		Disk imaging	5 marks	
		File format	2 marks	
Q.4	i.	Need of cyber forensics tools.		**3**
	ii.	Data recovery mechanism	4 marks	**7**
		Example	3 marks	
OR	iii.	Various phases in cyber forensics investigation	5 marks	**7**
		Diagram	2 marks	
Q.5	i.	Live analysis	1.5 marks	**4**
		Dead analysis	1.5 marks	
		Example	1 mark	
	ii.	Differentiate between network forensics and mobile forensics.		**6**
		Minimum 3 parameters 2 marks for each	(2 marks * 3)	
OR	iii.	Explanation SIM forensics	4 marks	**6**
		Financial fraud aspect	2 marks	
Q.6		Write short note on (any two)		
	i.	Role of cyber forensics investigator		**5**
	ii.	Application of digital forensics		**5**
	iii.	Cyber investigation at society level		**5**

******