Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Science
End Sem Examination May-2024
FS3EL12 Mobile Forensic

Programme: B.Sc. (Hons.) Branch/Specialisation: Forensic Science

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. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. When was the first commercially available mobile phone introduced? **1**
(a) 1960 (b) 1975 (c) 1983 (d) 1995

ii. What does SIM stand for? **1**
(a) System Information Module
(b) Subscriber Identification Module
(c) Secure Internet Module
(d) Service Information Module

iii. What was the first commercially available Android device? **1**
(a) Samsung Galaxy S
(b) HTC Dream (T-Mobile G1)
(c) Google Nexus One
(d) Motorola Droid

iv. What mechanism does Google use to distribute periodic updates to the Android operating system? **1**
(a) Over-the-air (OTA) updates
(b) Manual downloads from the website
(c) USB transfers
(d) Bluetooth updates

v. What is the default file system used by Android devices? **1**
(a) NTFS (b) FAT32 (c) ext4 (d) HFS+

vi. Which technique involves making an exact copy of all data stored on an Android device for forensic analysis? **1**
(a) Data wiping (b) Imaging
(c) Rooting (d) Encryption

vii. Which software acquisition method involves extracting data from a running or live system without altering its state? **1**
(a) Forensic imaging (b) Live acquisition
(c) Logical acquisition (d) Physical acquisition

viii. What is the primary challenge associated with cloud acquisitions? **1**
(a) Limited access to data
(b) Security and privacy concerns
(c) High cost of acquisition tools
(d) Slow data transfer speeds

ix. Which analysis technique involves examining file metadata, timestamps, and access permissions on an Android device? **1**
(a) File carving (b) File system analysis
(c) Keyword searching (d) Data carving

x. What is the primary purpose of keyword searching in Android forensic analysis? **1**
(a) To identify deleted files
(b) To recover deleted data
(c) To locate specific information of interest
(d) To analyze file system metadata

Q.2 i. Explain the characteristics of handheld devices. **2**
ii. What are SQLite databases? **3**
iii. Explain the concept of SIM card forensics in detail. **5**
OR iv. Write a note on "History of mobile devices." **5**

Q.3 i. What is android market? Explain its characteristics. **3**
ii. What are the different types of android devices? Explain their update mechanism. **7**
OR iii. Write a note on "History and evolution of android." **7**

Q.4 i. Explain the following: **4**
(a) Directory structure (b) File system

ii. Describe the process of conducting a forensic investigation on an android device. **6**
OR iii. Explain the differences between logical and physical imaging techniques. **6**

Q.5 i. What is the difference between software acquisition and hardware acquisition? **4**
ii. Explain the chip-off technique in android forensics. **6**
OR iii. Describe JTAG and ISP methods used for extracting data from Android devices. **6**

Q.6 Attempt any two:
i. Describe the imaging process of an android device. **5**
ii. Explain the role of SQLite in Android forensic investigations. **5**
iii. What are the common analysis techniques used in android forensic investigations to extract evidences? **5**

******

Marking Scheme

Mobile Forensic(T)- FS3EL12(T)

Q.1	i)	c	**1**
	ii)	b	**1**
	iii)	b	**1**
	iv)	a	**1**
	v)	c	**1**
	vi)	b	**1**
	vii)	b	**1**
	viii)	b	**1**
	ix)	b	**1**
	x)	c	**1**

Q.2	i.	Four characteristics of handheld devices.	**2**
	ii.	Any Three Characteristics	**3**
	iii.	SIM card forensics methodology in detail	**5**
OR	iv.	history of mobile devices. 5 -7 points	**5**

Q.3	i.	definition android market, three characteristics.	**1, 2**
	ii.	types of android devices 4 marks, update mechanism 3 marks.	**4, 3**
OR	iii.	history and evolution of android. 7 points	**7**

Q.4	i.	1. Directory structure. 2 Marks 2. File system. 2 Marks	**2, 2**
	ii.	process of conducting a forensic investigation on an Android device. 6 points- 1 Mark each	**6**
OR	iii.	differences between logical and physical imaging techniques. 6 points	**6**

Q.5	i.	difference between software acquisition and hardware acquisition- 4 differences- 1 Mark each	**4**
	ii.	chip-off technique in Android forensics. Introduction- 2 Marks Procedure- 4 Marks	**6**
OR	iii.	JTAG – 3 Marks. ISP – 3 Marks	**6**

Q.6

i.	imaging process of an android device.	**5**
ii.	SQLite introduction and role in details	**5**
iii.	analysis techniques used in android forensic investigations to extract evidences.	**5**

******