THE MANCHESTER METROPOLITAN UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING, MATHEMANTICS AND DIGITAL TECHNOLOGY

ACADEMIC YEAR 2015-2016:

MIDSEMESTER SESSION

Examination for
MSc Computer and Network Security

UNIT 6G7Z1009: Introduction to Computer Forensics and Security

Duration: 3 hour(s)

Instructions to Candidates

Please answer **FOUR** questions (**Two** questions each from both **Section A** and **Section B**)

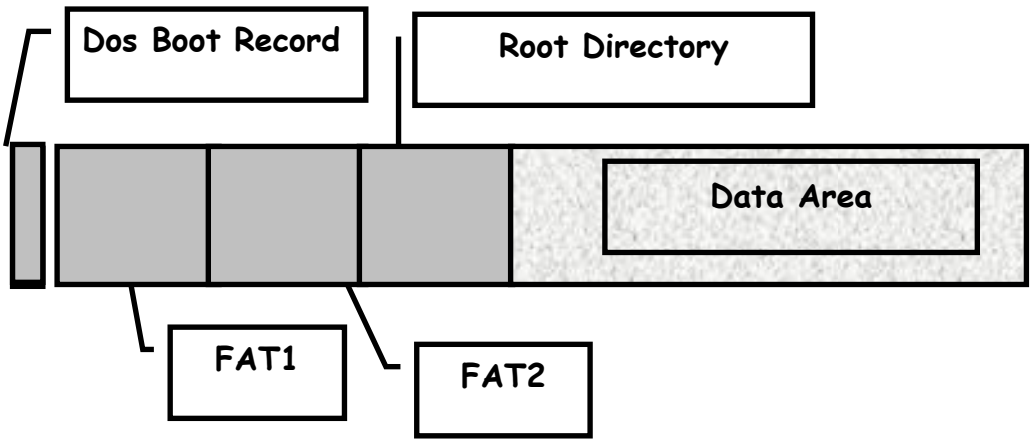
Each question carries 25 marks.

Students are permitted to use their own calculators subject to the standard Faculty conditions.

Section A Questions (1 - 3):

1. (a) You are a digital forensic investigator in a forensic team. The team has been asked to go to a suspect scene. Briefly describe the five steps of the forensic computing process you are going to conduct. [11]

(b) The following figure shows the main parts of FAT12 filesystem; what is the role of FAT1; what information can be found in the DOS Boot Record; what is the role of the Root Directory; and give an example how file slack could occur. [8]



(c) What is meant by the following terms: MD5 hash, search warrant, and hearsay evidence? [6]

Continued

2. Figure 2.1 shows a basic directory entry structure and the hexadecimal data associated from a windows OS based machine uses Intel processor, find out the following:

FIGURE 2.1: Basic directory entry structure and Hex. data associate.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
E5	**4F**	**50**	**20**	**20**	**20**	**20**	**20**	**54**	**58**	**54**	**20**	**18**	**84**	**82**	**70**	**9F**	**2D**	**9F**	**2D**	**00**	**00**	**F1**	**71**	**9F**	**2D**	**16**	**02**	**80**	**00**	**00**	**00**
Status	File Name							Extension			Attributes	Reserved		Created				Date Accessed		Unused		Written			Cluster	Starting	File Size						
														Time		Date						Time											

(a) What is the file system type this directory entry structure is part of? [2]

(b) Briefly explain what the starting cluster section contains and how it is used? [4]

(c) What is the status of the file; and how did you identify it? [2]

(d) What is the logical file size and how did you identify it? [5]

(e) When was the file created; including date and time; show your calculations? [12]

Continued

3. (a) A hard disk has 16 heads, 512 cylinders and 63 sectors per track, suppose each sector contains 512 bytes and the block size is 2 sectors. Calculate the following:

(i) Hard disk size in bytes.

(ii) The minimum physical file size in bytes.

(iii) The slack space size in bytes for a file size 912 bytes.

Fully explain your answer and include all calculation details.

[6]

(b) Explain the key features of the NTFS file system. Your answer should include information concerning:-- the master file table, character sets, resident and nonresident attributes, and $Bitmap. [9]

(c) Highlight the forensic importance of each of the following files in the Windows XP Operating System:

(i) FileName.LNK;

(ii) FileName.SPL;

(iii) Thumbs.DB;

(iv) NTUSER.DAT;

(v) PAGEFILE.SYS.

[10]

Section B Questions (4 - 6):

4. a) Define the following security related concepts: Security attacks/threats, Security services, security mechanism. [16]

b) Describes how many types of security and give one example cryptographic algorithm used for each type of security. [9]

5. a) Explain the block cipher and stream cipher. [10]

b) Explain the use of public key cryptography as a means of authentication and discuss the major problem associated with its use for this purpose.

[4]

c) i) Explain symmetric ciphers

ii) Use symmetric ciphers to encrypt message “secure” and decrypt message “WANT”. [11]

Continued

The representation of characters in modulo 26 is described as follows:

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The mathematical equations for encryption and decryption can be described as follows:

$$\text{Encryption } E_{(k)} : i \; ! \quad i + k \bmod 26$$

$$\text{Decryption } D_{(k)} : i \; ! \quad i - k \bmod 26$$

i represents the messages (plaintext or cipher), k represents a symmetric key. In this case k=10.

6. a) Describe a method that can provide integrity. [2]

b) Define KDC (key distribution center) and describe the types how the keys are distributed. [8]

c) i) Explain how Needham Schroeder Protocol operates and use the diagram to assist your analysis. [10]

ii) Explain the vulnerability in Needham-Shroeder protocol and how to overcome it? [5]

END OF QUESTIONS

Continued