UNIVERSITY OF MALTA
FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
Department of Computer Information Systems

January/February 2015 Assessment Session

CIS3089 Digital Forensics **15th January 2015**

09:15-12:15

Calculators are NOT allowed

General instructions:

Candidate must attempt all questions in section A. Furthermore the students shall answer two other questions from section B. The total marks in this paper are 100. The weight of each question section is there to guide you.

State any assumptions made. Your writing, drawing and coding should be clear and concise.

Section A – Student to attempt all

1 Some files have been deleted from the file system (assume a MS Windows FS). Plan and explain the actions required to identify, gather, and present this incident.

[5 marks]

2 We have a 250 GB Hard Disk to make a copy of. Describe how one can by using a well-known tool, e.g. NETCAT, copy the Hard Disk data to another storage.

[5 marks]

3 Give five characteristics of digital evidence.

[5 marks]

4 a) What does non-repudiation investigation in digital forensic entail?

[2 marks]

b) Management is worried on the increasing incidence of employees claiming their accounts have been hacked. Could you suggest two techniques to monitor and possibly identify an illegitimate log-on?

[3 marks]

5 a) Explain the possible use of MS Windows registry in digital forensics investigations.

[3 marks]

b) Explain the key and its value in forensic investigation shown in figure 1.

[2 marks]

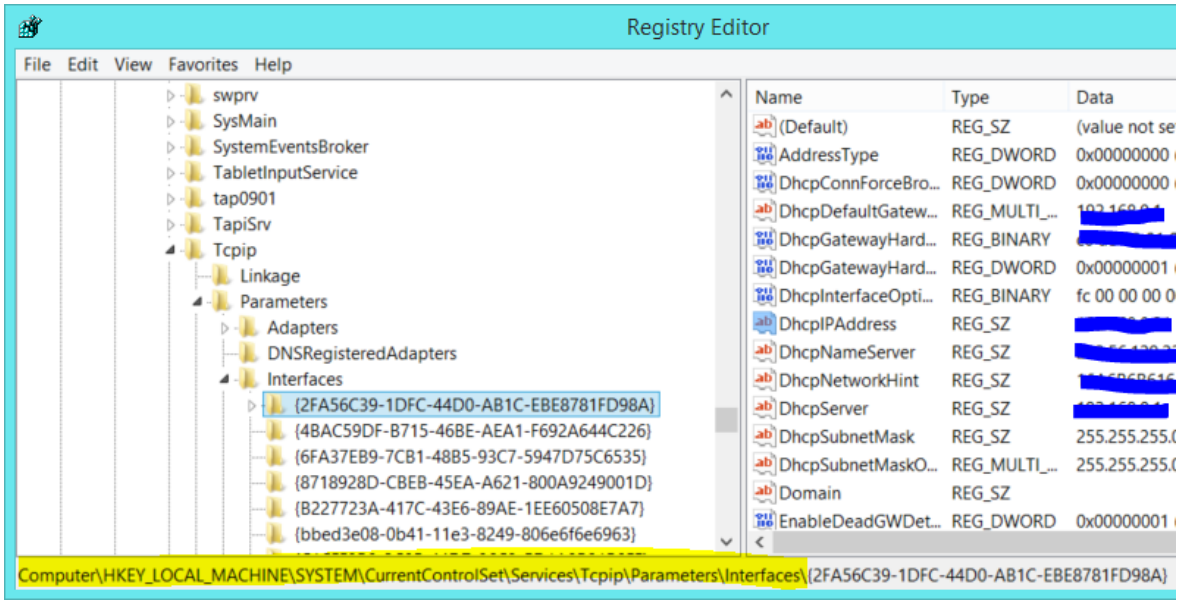

Figure 1: Registry screen dump

6 a) List the order of volatility of digital evidence in live forensics.

[3 mark]

b) List six Malware Code Types which you are aware of.

[2 mark]

7 It is known that data on a hard disk drive (HDD) is encrypted using the *Blowfish* block-cipher with a 50-bit key. It is your job to decipher this data for a complete forensic study of the HDD. Estimate how many computers are required to decipher this data in one week. You may assume that a single block of data can be decrypted in 0.3µs. State any further assumptions.

[5 marks]

8 Would the data on a hard disk drive be encrypted using a symmetric or a public-key cipher or both? Justify your answer.

[5 marks]

Section B – student to choose any two

9 a) i) In Cryptography, explain what is meant by Kerchoff's Principle and why this is important.

[5 marks]

ii) Briefly describe the four modes of attacks on a cryptosystem.

[4 marks]

b) i) Explain what is meant by perfect secrecy.

[5 marks]

ii) Can perfect secrecy be achieved in practice? If so, explain one technique that can achieve this. In any case, justify your answer.

[5 marks]

c) A Linear Feedback Shift Register (LFSR) may be used together with a stream cipher to encrypt data.

i) Explain how this system works with the help of a block system diagram.

[5 marks]

ii) What is the main weakness of this system?

[3 marks]

iii) How can this weakness be addressed? Are there other problems with your proposed solution?

[3 marks]

10 a) Define the terms: *live forensics* and *network forensics*,

[4 marks (2-Per term)]

b) How would you go about preserving live evidence? List the detailed steps involved, giving attention to live data and which tools would be needed.

[26 marks (20-Steps;6-Tools)]

11 a) Give a detailed logical design (in ERM notation) of the data requirements for a custody information system. Limit and specialise the database for recording details of wood artefacts and wood samples found in criminal cases.

i) ERM entities including attributes.

[10 marks]

ii) ERM relationships (including cardinalities and participation constraints)

[12 marks]

b) Describe two processes over the above database related with a digital forensic investigation.

[8 marks]

12 File carving is a process to extract purged files from a filing system without access to their meta data.

a) Describe a file carving attempt that although file is not entirely reconstructed, it's still useful.

[3 marks]

b) Give an example of a deep carving.

[3 marks]

c) View figure 2. What's the cause of this banding in the figure?

[4 marks]

d) What challenges does a file fragmentation brings to file carving?

[8 marks]

e) Describe a file reassembly procedure that is based on a graph path traversal technique.

[12 marks]

Figure 2: A recovered file