UNIVERSITY COLLEGE TATI

UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET	
COURSE CODE	: BNS 3243
COURSE	: CYBER LAW AND ETHICS
SEMESTER/SESSION	: 1-2023/2024
DURATION	: 3 HOURS

Instructions:

1. This booklet contains 5 questions. Answer **ALL** questions.
2. All answers should be written in answer booklet.
3. Write legibly and draw sketches wherever required.
4. If in doubt, raise your hands and ask the invigilator.

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE TOLD TO DO SO

THIS BOOKLET CONTAINS 6 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

a) Discuss **ONE (1)** unique case regarding on first attempt on how cyber law and ethics exist. (4 marks)

b) Describe **THREE (3)** distinct perspectives of applied ethics. (6 marks)

c) Distinguish between Normative and Descriptive terms. (4 marks)

d) Suppose a programmer discovers that a software product she has been working on is about to be released for sale to the public, even though it is unreliable because it contains "buggy" software. Should she 'blow the whistle'? (3 marks)

e) Justify **THREE (3)** reasons why Don Gotterbarn argued that all genuine computer ethics issues are *professional ethics* issues? (3 marks)

QUESTION 2

a) Explain **ONE (1)** specific task done by these following govern bodies;

i. World Wide Web Consortium (2 marks)

ii. Internet Engineering Task Force (2 marks)

iii. Internet Society (2 marks)

b) Describe **ONE (1)** statement about the top down approach. (2 marks)

c) Identify **THREE (3)** factors that make social networking sites popular also make govern bodies difficult to control. (3 marks)

d) Analyze **THREE (3)** important characteristics of the Internet. (6 marks)

e) Domain name is an identification string that defines a realm of administrative autonomy, authority or control within the Internet. State **THREE (3)** examples of domain names. (3 marks)

QUESTION 3

a) Give **FOUR (4)** types of offensive speech which is prohibited on Internet. (4 marks)

b) In your opinion, justify **FOUR (4)** reasons on why spam is considered harmful to user. (8 marks)

c) Blogs are often interactive and include sections at the bottom of individual blog posts where readers can leave comments. Interpret **TWO (2)** issues on blog related to information integrity. (4 marks)

d) Relate **TWO (2)** statements on how to become a good blogger. (4 marks)

QUESTION 4

a) Distinguish between Extrinsic loss of freedom and Intrinsic loss of freedom. (4 marks)

b) Describes **TWO (2)** ways on how actually data come from in the Internet. (4 marks)

c) Analyze the content of Malaysian Cyber Law in following;

i. Seditious Act 1948 (2 marks)
ii. CMA 1998 Section 3 (2 marks)
iii. CMA 1998 Section 6 (2 marks)
iv. CMA 1998 Section 211(1) (2 marks)
v. CMA 1998 Section 211(2) (2 marks)
vi. Defamation Act 1957 (2 marks)

QUESTION 5

a) There are two types of defamation in Malaysia which are libel and slander. Differentiate between them. (4 marks)

b) Examine the **TWO (2)** ways of conditions to solve the deleted file in computer forensics. (4 marks)

c) Critique the following case. (Mention the status and supportive of case, also analyze the law that meet the case).

i. **CASE 1** (4 marks)
Staff Access Inappropriate Material

The Scenario:

One of the UK's most successful providers of airline support services, suspected a member of staff of accessing pornography contrary to policy. The suspicion had been triggered by the re-occurrence of a virus known to originate on these types of sites.

The client enlisted Cyber Forensics analysts to conduct an investigation to determine if the user had intentionally accessed inappropriate material.

Analysts Actions:

Analysts attend the clients' site. A forensic image copy was made of the hard drive from the suspect computer. A forensic analysis of the image copy was then undertaken using specialist software tools. The incident was managed to meet all legal and evidential regulations with the likelihood of the findings being used in a disciplinary hearing or court proceedings. As part of the investigation, analysts reviewed the clients existing company policies. This was done in order to ascertain the existing regulations and to understand if the company recognized the breach as a disciplinary offence. All computer evidence was gathered using the latest computer forensic tools and methodology, ensures continuity of evidence.

Findings:

The investigation identified the offender, the actions committed, and how they were carried out.

The findings were documented and presented to the HR department who had the responsibility for any disciplinary action. Analysts evidential report was used as part of the disciplinary process. The offender was dismissed.

ii. **CASE 2** (4 marks)

You are a forensic examiner and have been hired by a private company to investigate the apparent theft of a very large sum of money by an employee, Kamil. The company owner, Idris, said that he fired Kamil last week. Kamil took his laptop computer with him, but Idris said that he found a diskette in Kamil' desk after he left. Idris said that he carefully write protected the diskette that he found and he then looked at it. He saw that one of the documents, "C.doc" looked phony. He thinks that Kamil backdated that document. Idris wants you to examine the diskette and determine if the "C.doc" had been backdated. If you can prove that "C.doc" was backdated, Idris says that he can sue Kamil and attempt to freeze his assets in order to recover his money. You accepted a RM1000 retainer to start the job.

End case scenario.

Actions, Results and Conclusions:

The first thing noted was that the Volume Label "DEMO-1" was created 9/28/02 at 5:46PM. There were 4 MS Word documents located on the diskette. They were:

Doc Name	Last Accessed	Last Written	Created
"A.doc"	10-01-02	9-28-02 4:54 PM	10-01-02 5:15:02 PM
"B.doc"	10-01-02	9-29-02 4:54 PM	10-01-02 5:14:58 PM
"C.doc"	10-01-02	8-28-02 5:06 PM	10-01-02 5:15:00 PM
"D.doc"	10-01-02	9-30-02 5:10 PM	10-01-02 5:14:56 PM

First issue - since there only have a floppy diskette and not the computer where you could check the system clock for accuracy, how can you be sure that the system clock is not failing and providing bad or incorrect date information?

One curious issue appears to be that the files were last accessed and created after they were last written to. How could that be? The directory entry dates are notoriously unreliable.

The strongest indication on the authenticity of the "C.doc" is by examining the compound document (sometimes called "metadata") information contained within the document and not to rely solely on a single or more volatile indicators. MS Word documents store a lot of information within the document that is not normally visible to a user. One method to access this information is through the "Properties" tab on a document. Using the "Properties" information and other software that goes deeper that the "properties" information, we were able to establish that "A.doc" was created as an original document on 9-28-02 at 4:52 PM and last saved at 4:54 PM. We were able to establish that "B.doc" was a revision of "A.doc" created on 9-29-02 at 4:54 PM and saved at 4:54 PM. We were able to establish that "C.doc" was a revision of "B.doc" and was backdated approximately 44,638 minutes to 8-28-02 at 5:04 PM. We were also able to establish that "D.doc" was a revision of the "B.doc" created and last saved on 9-30-02 at 5:10 PM.

Based upon the establishment of the system clock accuracy, the explanation for the Create/Accessed date being after the file was last written to, and the compound document data, we concluded that the "C.doc" file was backdated.

d) How Mitnick and Shimomura establish their first conviction on attacks? (4 marks)

----------End of question----------