STRATHMORE UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY
MASTER OF SCIENCE IN INFORMATION SYSTEMS SECURITY
END OF SEMESTER EXAMINATION
MST 8602
Cyber Crime Law and Investigation

DATE: 17 October, 2017 Time: 3 Hours

Instructions: This examination consists of Two Sections; Answer all questions

SECTION A: 70 pts

1) What is Cyber Crime? Define, Describe, and provide examples **(10 points)**

2) Describe in detail how computers can be used to commit cyber-crime **(10 points)**

3) One of the difficulties of prosecuting a cyber-criminal is the borderless nature of cybercrime. If a **Kenyan** commits a cybercrime while in the **US**, using a proxy server in **England** – by what laws should he/she be prosecuted? Be sure to defend your position **(10 points)**

4) Social media has become a major aspect of online activity, and thus an essential part of cybercrime and cyber terrorism-related operation. Using examples please describe:
   a. How social media can be used to **commit** cyber-crime **(10 points)**
   b. Conversely – how social media can be used to **solve** crimes (**10 points)**

5) Should Kenyan police authorities be allowed to pursue and prosecute cyber criminals? Defend your position using specific examples **(10 points)**

6) What are some of the major challenges with protecting children on the Internet **(10 points)**

SECTION B: Case Study (30 pts)

Following reports of customers being missold legal-based documentation, a high-tech investigation was requested by a legal practice.

Arrangements were made to attend the premises of the organization under investigation, legal proceedings meant that the organization had no idea that this was to happen — preventing malicious data destruction. A legal stipulation was enforced, intended to reduce loss of revenue for the business, which meant that digital devices could not be removed from the premises. Pre-search intelligence identified that up to 20 staff worked at the premises at any one time, and the access that was available for the building; including vehicle access routes. No information was available, nor time available, to identify what digital devices may be present.

The following day the premises were attended by both a legal team and a team of high-tech investigators. The scene was initially secured by removing all occupants from the vicinity of all digital devices. A full recording of the site was conducted using digital cameras and sketches and each digital device was identified. A review was made of the potential digital sources to determine their current state: in the main the devices were computers or laptops which had nothing significant running, and were therefore disconnected from power. A server was identified that was currently running, a capture was made of the memory to ensure running processes and connections were recorded, and then the server was shutdown.

Forensic data captures were made of all devices onsite, which in itself took over 12 hours. These captures were then placed into tamper proof evidence bags and returned to the laboratory and analyzed. The background to the investigation provided relevant keywords and file types. These were used to analyze the data which subsequently identified a number of files, emails and documents that were relevant to the investigation, these allowed the legal team to progress their legal proceedings

Use the above case study to answer the following:

1) Evaluate law enforcement's response to the above cybercrime **(10 points)**

2) What measures were taken to protect/preserve the crime scene **(10 points)**

3) What forensic techniques were used to investigate the crime **(10 points)**