



**UNIVERSITY EXAMINATIONS: 2013/2014**  
**EXAMINATION FOR THE MASTER OF SCIENCE IN**  
**DATA COMMUNICATIONS**  
**MDC 6403 COMPUTER FORENSICS**

**DATE: AUGUST, 2014**

**TIME: 2 HOURS**

---

**INSTRUCTIONS: Answer Question One and Any Other Two Questions**

---

**QUESTION ONE: [20 Marks]**

The following are observations about the digital world, tools, software, digital crimes and digital tools users.

- Every passing year, the number of digital crimes being committed is on the increase worldwide.
- As technology evolves, software changes, and users become digitally savvy, the crimes they commit are becoming more sophisticated.
- Law enforcement is in a perpetual race with these criminals to ensure that the playing field remains level. Part of this race includes developing tools that have the ability to systematically search digital devices for pertinent evidence.
- As more devices become digitalized, the tool development should also progress to include these as well.
- More crucial in this race, is the development of a methodology in digital forensics that encompasses the forensic analysis of all genres of digital crime scene investigations. Here, we have had the classical method for digital forensics investigations that may include identification, preparation, preservation, collection, examination, analysis to reporting/documentation etc. Apparently, this approach is simply too technology specific.

**Required:**

- a) Briefly outline some of the shortcomings of the classical methods used in digital forensics.

(10 Marks)

- b) Highlight the direction that digital forensic research is taking as regards redefining digital forensics investigation models. (10 Marks)

### **QUESTION TWO (15 MARKS)**

New forensics certifications are constantly being offered by diverse organizations.

- (a) Briefly detail these organization(s), and the certifications they offer. (8 Marks)
- (b) Discuss the kind of background/experience it takes to make a good digital forensic expert. (7 Marks)

### **QUESTION THREE (15 MARKS)**

By referring to Daubert's Guidelines, Discuss the admissibility of Open Source Software tools in Court of Law.

### **QUESTION FOUR (15 MARKS)**

- a) Using specific examples, distinguish between Digital Forensics and Computer Forensics. (5 Marks)
- b) Discuss the generic types of Digital Evidence that one can encounter while investigating digital crimes. (5 Marks)
- c) Highlight some of the emerging trends in digital forensics practice in the last decade. (5 Marks)