Masc Forensic Investigations Academy

MASC FORENSIC INVESTIGATIONS ACADEMY

DIPLOMA IN COMPUTER & DIGITAL FORENSICS

REGULATIONS

1.0 PREAMBLE

1.1. These regulations are to be read in conjunction with the General Academic Regulations of the Harare Institute of Technology Diplomas and in accordance with the School of Business and Management Sciences regulations governing academic programmes.

Diploma in Computer & Digital Forensics is designed to develop Accountants, Auditors and Investigators, with knowledge, skills and attitudes required to satisfy the needs of corporate organisations in handling and conducting Digital Forensic Investigations, evidence collection and presentation in an internationally acceptable manner. It deals with how accountants can investigate and document forensic crimes, how security personnel/investigators can investigate crime and it fully equips participants on how to detect and deal with forensic crimes.

2.0 PROGRAMME OBJECTIVES

The objectives of the programme are to:

2.1. Provide Computer and Digital Forensic services of any nature.

2.2. Describe standard data storage devices.

2.3. Identify some common software & hardware acquisition tools

2.4. Use various Computer Forensic Tools to gather forensic evidence.

2.5. Write and present forensic reports that are grounded on forensically sound evidence and research.

2.6. Provide expertise in collection, analysis and presentation of evidence.

3.0 ENTRY QUALIFICATIONS

3.1. Candidates must comply with Diploma General Academic Regulations;

3.2. Entry requirements for acceptance into this programme are:

3.2.1. A minimum of TWO A 'level passes which must include Computing and Mathematics

OR

3.2.2. A Certificate in Information Technology from a recognised institution, plus Five "O" Levels including English Language and Mathematics passed at Ordinary Level with grade C or better and any other three subjects.

4.0 GRADUATE COMPETENCES

The graduates should be able to:

4.1. Use Computer Forensic Tools to investigate various fraud & criminology schemes and recommend suitable corrective action.
4.2. Prepare court ready expert forensic investigative reports.
4.3. Collect, analyse and present digital evidence.
4.4. Testify as an expert witness
4.5. Design internal control systems that are cybercrime fraud –proof.

5.0 GRADUATE ATTRIBUTES

5.1. Professionalism
5.2. Ethical
5.3. Creative and analytical thinker.
5.4. Detail oriented
5.5. Sound professional judgement

6.0 CAREER PROSPECTS

The graduates of this programme may be employed among others as:

6.1. Computer & Digital Forensic investigators
6.2. Forensic Auditors
6.3. Fraud Risk Officers.
6.4. Cyber-Fraud Crimes Managers
6.5. Compliance Professionals.
6.6. Fraud and Forensics Academics and Researchers.

7.0 PROGRAMME STRUCTURE

Diploma in Computer & Digital Forensics is a one -year programme offered as a Block-Release/Part Time Programme.

8.0 ASSESSMENT PROCEDURE

8.1 Practical Course Assessment

Assessment of practical courses is based on the weighted aggregate of**:**

- Written Examination 60%
- Continuous Assessment 40%

The mark for the coursework assessment in a practical course consists of the following weighted components:

- Written assignment/Presentations and test 15%
- Practical Work (Laboratory Practicals/Field Trips/Industrial Visits Reports 25%

8.2 Non- Practical Course Assessment

Assessment of non-practical courses consists of the following weighted components:

- Written Examination 75%
- Continuous Assessment 25%

9 . Course Work And Attendance

9.1. A candidate is allowed to sit for an examination provided he/she has attained a coursework mark that is not less than 55% in that course. Lectures, tutorials, practicals and industrial visits are compulsory unless otherwise stated. A student who fails to attend 80 % of scheduled lectures , tutorials, laboratory practicals, field trips, industrial visits, seminars and workshops is not eligible to sit for examinations in that course.

9.2. Students of the Diploma in Computer & Digital Forensics Investigations programme cannot graduate without obtaining a weighted average mark of 55% of all attempted courses.

10. RE-WRITES

Re-write(s) should conform to current course structure.

1.1.1 Candidates should pass at least two thirds of the course to qualify for a referral.

1.1.2 Any candidate who fails to pass at least two thirds of the course should repeat the whole course, including the subjects they would have passed.

1.1.3 There is no time limit for which to re-write a failed examination.

1.1.4 There is no aggregation for re-writes.

1.1.5 All re-writes should pass on performance in the examination.

1.1.6 If a candidate fails coursework he/she repeats the subject.

11. EXEMPTIONS

11.1 There are no exemptions for this Diploma

12. IRREGULAR PRACTICES

12.1 Cheating in continuous assessment and or examinations will result in disqualification from the whole course. The candidate will be suspended indefinitely from undertaking any of our courses.

12.2. The penalty for plagiarism shall be as in 12.1

13. DIPLOMA CLASSIFICATION

The following Classification Scheme shall be adopted for all courses:

Mark	Class	Symbol	Decision
90 – 100%	Distinction	D	Pass
80 – 89%	Merit	M	Pass
70 – 79%	Credit	C	Pass
55 -69	Pass	P	Pass

54 and Below	Fail	F	Fail

14.1. DIPLOMA WEIGHTING

Semester I - 55%
Semester II - 55%

15. COURSE SYNOPSIS

DCFIT *Fundamentals of Information Technology*

The course aims to provide students with basic knowledge of computers. By the end of the course, the student should be able to: appreciate the latest technologies and reduce considerable time in solving computer related problems. It takes them through the basic fundaments of computers through applications of information technology. Essentials to be covered include; Evolution of Computers, Computer Generations, Classification of Computers as well as Computer Applications. Computer Organization, Memory and Storage, Basic Computer Organization, Input Devices, Output Devices, Central, Processing Unit,The System Bus Architecture, Memory or Storage Unit, Internet Evolution, Basic Internet Terminology, Data over Internet, Modes of Data Transmission, Types of Networks, Types of Topologies, Protocols used in the Internet, Getting Connected to Internet Applications, Internet Applications, Computer Ethics, and Emerging Trends in IT.

DCF/CFIP Computer Forensics Investigation Process

The course aims at providing students with knowledge, skills and values to understand all aspects of Computer Forensic Investigation Process, the mapping process between the processes/activities and output for each phase in Digital Forensic Investigation Framework (DFIF). Existing digital forensic frameworks will be reviewed and then the mapping is constructed.

The topics includes ; Computer Forensic Tools, Computer investigation and analysis techniques, Procedures for Gathering Evidence, Computer Forensics Procedures, Tools, and Digital Evidence.

DCF/DAP Data Acquisition and Preservation

The course aims at providing students with knowledge, skills and values to understand all aspects of **computer evidence handling methods** to obtain information for crime investigation. It basically covers three parts: **Data acquisition**: is the secure process to obtain data from the original source without damaging or modifying it using the correct tools; **Data preservation**: how to preserve the acquired digital evidence in its original state, using cryptographic hash algorithms and D**ata analysis**: Making sense of the data acquired by analysing it and extracting information from it, identifying partitions, MAC times and others.

DCF/FDAV Forensic Data Analysis and Validation

The purpose of this course is to equip students with the knowledge and expertise to carry out forensic data analysis and validation. By the end of the course the student should be able to: apply the Principles of Forensic Data Analysis & validation (**volatile and not volatile)** to get useful information of the data when carrying out forensic assignments, Adapt the investigative Process,

Understand the Legal issues in Forensic Auditing & Investigations, Identify Sources of Information/Data for evidence collection during investigations, Understand Challenges, Issues, and Trends in Forensic Auditing & Examination and Document & protecting the case (the **chain of custody**).

The topics includes; Determine what data to analyze in a computer forensics investigation; Tools used to validate data, Common data-hiding technique, Methods of performing a remote acquisition

DCF/NF Network Forensics

Through this course students will gain well rounded and systematic knowledge and understanding of how to monitor and analyse computer **network** traffic for the purposes of information gathering, legal evidence, or intrusion detection. A person credited with this module will be able to search for data that points towards human communication, manipulation of files, and the use of certain keywords for example.

DCF/MF Mobile Devices Forensics

The purpose of this course is to provide students with detailed knowledge, skills and values to Identify the fundamental concepts and technologies involved in mobile forensics and implement proper incident response procedures. Students accredited with this module should be able to identify primary technologies used in mobile devices, acquire evidence from mobile devices, analyze extracted evidence, collect evidence from other sources and Report findings using various data analysis & reporting tools.

DCF/AFT Anti-Forensics Techniques

The purpose of this course is to give an understanding of how Anti-Forensics (AF) tools and techniques frustrate Computer Forensic Tools (CFTs) by erasing or altering information; creating "chaff" that wastes time and hides information; implicating innocent parties by planting fake evidence; exploiting implementation bugs in known tools; and by leaving "tracer" data that causes CFTs to inadvertently reveal their use to the attacker. Students will understand primary goals for anti-forensics and how to evaluates the effectiveness of these AF tools for defeating CFTs, strategies for their detection, and countermeasures.

Topics to be covered include:- Overwriting data and metadata, Cryptography, steganography, and other data hiding approaches, Memory injection and Syscall Proxying, Live cds, bootable USB tokens and virtual machines, Anonymous identities and storage. Failure to validate data , Denial of service attacks, Fragile heuristics, AFTs that detect CFTs , Countermeasures.

DCF/FIE Forensic Investigator, An Expert Witness & Ethics

This course will enlighten the student of a litigator's guide for working with forensic expert witnesses. Topics to be covered include: The Necessary Tasks, Qualifications of an Expert Witness, Getting to Know the Expert, Testing and Observing the Methods, Reviewing Other Works, The Testing Phases, Working with the Lawyer. The topics to be covered include: **Report Writing (**Guidelines for Writing Reports, Generating Report Findings with Forensics Software Tools), **Expert Testimony** (Preparing for Testimony, Testifying in Court, Preparing for a Deposition or Hearing, Preparing Forensics

Evidence for Testimony) **Ethics for Expert Witness** (Applying Ethics and Codes to Expert Witnesses, Ethical Difficulties in Expert Testimony, Organizations with Codes of Ethics)