Course Title:	**Digital Forensics Tools and Techniques**
Course Code:	**COMP832**
Descriptor Start Date:	**15/07/2024**
POINTS:	**15.00**
LEVEL:	**8**
PREREQUISITE/S:	**None**
COREQUISITE/S:	**None**
RESTRICTION/S:	**None**

LEARNING HOURS

Hours may include lectures, tutorials, online forums, laboratories. Refer to your timetable and course information in Canvas for detailed information.

Total learning hours: 150

PRESCRIPTOR

Evaluates and assesses a range of forensic tools and techniques used for abstracting low-level detail and engaging in a structured approach to the analysis and presentation of digital evidence. Researches the underlying low level details behind each tool and the ethical aspects related to their application in order to provide the necessary advanced technical understanding required from technical expert witnesses.

LEARNING OUTCOMES

1. Demonstrate high level understanding of the different types and uses of forensic digital media
2. Demonstrate a high level of practical knowledge of the tools and other software used to examine digital media
3. Demonstrate critical awareness of techniques used to analyse digital media
4. Demonstrate knowledge of acceptable professional and legal practices involving acquiring, analysing and presenting of digital forensic evidence
5. Demonstrate advanced ability to apply computer forensics to practical investigation of case studies
6. Prepare and present a technical report on forensic analysis

CONTENT

Forensic Investigation Processing including acquisition, analysis and presentation of evidence. The student shall develop advanced understanding of:
- malware;
- file retrieval & analysis;
- imaging, forensic bridges, hashing and decryption techniques
- inculpatory and exculpatory evidence
- court-ready presentation of evidence
- rules of evidence

LEARNING & TEACHING STRATEGIES

Each lecture session will be followed by workshops and practical laboratories designed to provide students with hands-on experience of various digital forensic tools and techniques. Case studies will be used for acquiring practical analytical skills. Students will present a technical report on the application of digital forensic tools.

A problem-based learning (PBL) approach is adopted for the technical assignment. The students will be given case study material requiring forensics analysis that they will process forensically. The student will need to recover the relevant artefacts following crime scene management procedures and produce the appropriate forensic analysis documentation. Activities will focus on extracting and analysing evidence in order to build a report of forensic evidence suitable for a court setting. The assignment will be assessed through this portfolio submitted by each student. A separate assignment will require the student to research an aspect of digital forensics and present a research report on their findings. The assessments shall be submitted by the student electronically.

ASSESSMENT PLAN

Assessment Event	Weighting %	Learning Outcomes
Technical Report	50.00	4-6
Report on Research	50.00	1-3

Grade Map **MAP1**

A+ A A- Pass with Distinction
B+ B B- Pass with Merit
C+ C C- Pass
D Fail

Overall requirement/s to pass the course:

To pass a course, students must attempt all assignments, and achieve a minimum overall grade of C-.

LEARNING RESOURCES

A recommended reading list will be provided.

For further information, contact: Te Ara Auaha - Faculty of Design & Creative Technologies

Principal Programme:	**AK1324, Master of Cyber Security and Digital Forensics**
Related Programme/s:	**AK1329** **AK3745** **AK3746** **ICE1** **INEXCH1** **SABRD1**

Disclaimer: Course descriptors may be amended between teaching periods/semesters