**KING’S OWN INSTITUTE***

**Success in Higher Education**

# ICT741 DIGITAL FORENSICS T325 BRIEF

All information in the Subject Outline is correct at the time of approval. KOI reserves the right to make changes to the Subject Outline if they become necessary. Any changes require the approval of the KOI Academic Board and will be formally advised to those students who may be affected by email and via Moodle.
Information contained within this Subject Outline applies to students enrolled in the trimester as indicated.

## 1. General Information

### 1.1 Administrative Details

| Associated HE Award(s) | Duration | Level | Subject Coordinator |
|---|---|---|---|
| Master of Information Technology (MIT)<br>Master of Information Systems (MIS) | 1 trimester | Postgraduate | Dr MD Badiuzzaman<br>md.bodi@koi.edu.au<br>P: +61 (2) 9283 3583<br>L: 7-11, 11 York Street.<br>Consultation: via Moodle or by appointment. |

### 1.2 Core/Elective

This subject is
- an elective subject for the Master of Information Technology (MIT)
- an elective subject for the Master of Information Systems (MIS)

### 1.3 Subject Weighting

Indicated below is the weighting of this subject and the total course points.

| Subject Credit Points | Total Course Credit Points |
|---|---|
| 4 | MIT (64 Credit Points); MIS (64 Credit Points) |

### 1.4 Student Workload

Indicated below is the expected student workload per week for this subject

| No. Timetabled Hours/Week* | No. Personal Study Hours/Week** | Total Workload Hours/Week*** |
|---|---|---|
| 3 hours/week plus supplementary online material | 7 hours/week | 10 hours/week |

* Total time spent per week at lectures and tutorials
** Total time students are expected to spend per week in studying, completing assignments, etc.
*** Combination of timetable hours and personal study

1.5 **Mode of Delivery** Classes will be face-to-face or hybrid. Certain classes will be online (e.g., special arrangements).

**1.6 Pre-requisites** ICT722 Information Security

### 1.7 General Study and Resource Requirements

- Students are expected to attend classes with the weekly worksheets and subject support material provided in Moodle. Students should read this material before coming to class to improve their ability to participate in the weekly activities.
- Students will require access to the internet and their KOI email and should have basic skills in word processing software such as MS Word, spreadsheet software such as MS Excel and visual presentation software such as MS PowerPoint.
- Computers and WIFI facilities are extensively available for student use throughout KOI. Students are encouraged to make use of the campus Library for reference materials.

*Software resource requirements specific to this subject:* Office 365, MS Imagine, VMware, Forensic Tools on book CD, Autopsy.

### 1.8 Academic Advising

Academic advising is available to students throughout teaching periods including the exam weeks. As well as requesting help during scheduled class times, students have the following options:

- Consultation times: A list of consultation hours is provided on the homepage of Moodle where appointments can be booked.
- Subject coordinator: Subject coordinators are available for contact via email. The email address of the subject coordinator is provided at the top of this subject outline.
- Academic staff: Lecturers and Tutors provide their contact details in Moodle for the specific subject. In most cases, this will be via email. Some subjects may also provide a discussion forum where questions can be raised.
- Head of Program: The Head of Program is available to all students in the program if they need advice about their studies and KOI procedures.
- Vice President (Academic): The Vice President (Academic) will assist students to resolve complex issues (but may refer students to the relevant lecturers for detailed academic advice).

## 2. Academic Details

### 2.1 Overview of the Subject

Digital forensics refers to the science of the recovery and investigation of data from digital devices. It is most often used in dealing with computer crime, but can be used in other instances such as data recovery. This subject introduces students to the emerging and evolving field of digital forensics with hands-on labs and practical exercises. Students will learn about data acquisition and validation processes in relation to investigating networks, files, operating systems, email, mobile devices and web services. Professional issues such as ethical responsibilities and legislative requirements will be examined. Students will be introduced to presenting forensic reports and testimony as an expert witness.

### 2.2 Graduate Attributes for Postgraduate Courses

Graduates of postgraduate courses from King's Own Institute will achieve the graduate attributes expected from successful completion of a postgraduate degree under the Australian Qualifications Framework (2$^{nd}$ edition, January 2013). Graduates at this level will be able to apply advanced body of knowledge from their major area of study in a range of contexts for professional practice or scholarship and as a pathway for further learning.

King's Own Institute's generic graduate attributes for a master's level degree are summarised below:

| | KOI Postgraduate Degree Graduate Attributes | Detailed Description |
|---|---|---|
| 📖 | Knowledge | Current, comprehensive and coherent knowledge, including recent developments and applied research methods |
| 💡 | Critical Thinking | Critical thinking skills to identify and analyse current theories and developments and emerging trends in professional practice |

| | | |
|---|---|---|
| 💬 | Communication | Communication and technical skills to analyse and theorise, contribute to professional practice or scholarship, and present ideas to a variety of audiences |
| 🌐 | Research and Information Literacy | Cognitive and technical skills to access and evaluate information resources, justify research approaches and interpret theoretical propositions |
| ⊐ | Creative Problem Solving Skills | Cognitive, technical and creative skills to investigate, analyse and synthesise complex information, concepts and theories, solve complex problems and apply established theories to situations in professional practice |
| 🌍 | Ethical and Cultural Sensitivity | Appreciation and accountability for ethical principles, cultural sensitivity and social responsibility, both personally and professionally |
| ✴ | Leadership and Strategy | Initiative, leadership skills and ability to work professionally and collaboratively to achieve team objectives across a range of team roles<br>Expertise in strategic thinking, developing and implementing business plans and decision making under uncertainty |
| 📜 | Professional Skills | High level personal autonomy, judgement, decision-making and accountability required to begin professional practice |

Across the courses, these skills are developed progressively at three levels:

- **Level 1 Foundation –** Students learn the skills, theories and techniques of the subject and apply them in stand-alone contexts
- **Level 2 Intermediate –** Students further develop skills, theories and techniques of the subject and apply them in more complex contexts, beginning to integrate the application with other subjects
- **Level 3 Advanced** – Students have a demonstrated ability to plan, research and apply the skills, theories and techniques of the subject in complex situations, integrating the subject content with a range of other subject disciplines within the context of the course

Generally, skills gained from subjects in the Graduate Certificate and Graduate Diploma are at levels 1 and 2 while other subjects in the Master's degree are at level 3.

### 2.3 Subject Learning Outcomes

Listed below, are key knowledge and skills students are expected to attain by successfully completing this subject:

| Subject Learning Outcomes | Contribution to Graduate Attributes |
|---|---|
| a) Apply procedures, theories and techniques of digital forensics | 📖 💡 ⊐ |
| b) Demonstrate forensic examination skills on a variety of devices, operating systems, and technologies | 📖 💡 ⊐ 🌐 📜 |
| c) Compare the effectiveness of digital forensic tools based on the requirements of the digital crime | 📖 💡 ⊐ 🌐 |
| d) Assemble forensic reports based on digital evidence according to the digital security practices in industry | 📖 💡 ⊐ 💬 📜 |

| | |
|---|---|
| e) Evaluate ethical and legal considerations involved in the profession of computer forensics | 📖 💡 ⊐ 🌐 |

## 2.4 Subject Content and Structure

Below are details of the subject content and how it is structured, including specific topics covered in lectures and tutorials. Reading refers to the text unless otherwise indicated.

*Weekly Planner:*

| Week (beginning) | Topic covered in each week's lecture | Reading(s) | Expected work as listed in Moodle |
|---|---|---|---|
| Week 1<br>27 Oct | Introduction to digital forensic investigation and lab requirements | Chs. 1, 2 | Discuss review questions on digital forensic investigation procedures and conduct.<br>Formative not graded |
| Week 2<br>03 Nov | Data acquisition | Ch. 3 | Discuss review questions on storage format and data acquisition methods.<br>Tutorial submission graded |
| Week 3<br>10 Nov | Processing crime and incident scenes, and computer forensic tools | Chs. 4, 6 | Discuss review questions on storing and securing evidence, search preparation, and forensic hardware and software tools.<br>Tutorial submission graded |
| Week 4<br>17 Nov | Working with windows and command line interface systems | Ch. 5 | Discuss review questions on file systems, file structure, windows registry, and virtual machines.<br>Tutorial submission graded |
| Week 5<br>24 Nov | Linux and Macintosh file systems and recovering graphic files | Chs. 7, 8 | Discuss review questions on file structures, Linux forensic tools, graphic file forensics, data compression, and file formats<br>Tutorial submission graded<br>**Assessment 2: due** |
| Week 6<br>01 Dec | Digital forensic analysis and validation | Ch. 9 | Discuss review questions on data collection, analysis, validation, and data hiding techniques<br>Tutorial submission graded |
| Week 7<br>08 Dec | Virtual machine forensics, live acquisitions, and network forensics | Ch. 10 | Discuss review questions on forensic procedures for Type 2 and Type 2 Hypervisor, live acquisition, and procedures for network forensics.<br>Tutorial submission graded |
| Week 8<br>15 Dec | E-mail and social media investigation | Ch. 11 | Discuss review questions on Email crimes and violations, Email and social media communication forensic tools. |

| Week (beginning) | Topic covered in each week's lecture | Reading(s) | Expected work as listed in Moodle |
|---|---|---|---|
| | | | Tutorial submission graded<br>**Assessment 3: Report due** |
| Week 9<br>05 Jan | Mobile device forensics and the Internet of Things | Chs. 12, 13 | Discuss review questions on mobile device forensics and IOT<br>Tutorial submission graded<br>**Assessment 3: Presentation due** |
| Week 10<br>12 Jan | Report writing for high-tech investigation | Ch. 14 | Discuss review questions on importance and types of reports, report writing guidelines, and use of tools for writing reports<br>Tutorial submission graded |
| Week 11<br>19 Jan | Expert testimony and ethics for the expert witness | Chs. 15, 16 | Discuss review questions on preparation and guidelines for expert testimony, and ethics and code for expert witness<br>Tutorial submission graded<br>**Assessment 4: Report due** |
| Week 12<br>27Jan (Tue) | Revision | | Discuss review questions from week 1 to 11<br>Formative not graded<br>**Assessment 4: Presentation due** |
| Week 13<br>02 Feb | Study review week and Final Exam Week | | |
| Week 14<br>09 Feb | Examinations<br>Continuing students - enrolments for T126 open | | Please see exam timetable for exam date, time and location |
| Week 15<br>16 Feb | Student Vacation begins<br>New students - enrolments for T126 open | | |
| Week 16<br>23 Feb | ● Results Released<br>● Review of Grade Day for T325 – see Sections 2.6 and 3.2 below for relevant information.<br>● Certification of Grades<br>NOTE: More information about the dates will be provided at a later date through Moodle/KOI email. | | |
| **T126 2 Mar 2026** | | | |
| Week 1<br>02 Mar | Week 1 of classes for T126 | | |

### 2.5 Teaching Methods/Strategies

Briefly described below are the teaching methods/strategies used in this subject:

- *Lectures* (1 hours/week) are conducted in seminar style and address the subject content, provide motivation and context and draw on the students' experience and preparatory reading.
- *Tutorials* (2 hours/week) include class discussion of case studies and research papers, practice sets and problem-solving and syndicate work on group projects. Tutorials often include group exercises and so contribute to the development of teamwork skills and cultural understanding. Tutorial participation is an essential component of the subject and contributes to the development of many of the graduate attributes (see section 2.2 above). Tutorial participation contributes towards the assessment in many subjects (see details in Section 3.1 for this subject). Supplementary tutorial material such as case studies, recommended readings, review questions etc. will be made available each week in Moodle.
- *Online* teaching resources include class materials, readings, model answers to assignments and exercises and discussion boards. All online materials for this subject as provided by KOI will be found in the Moodle page for this subject. Students should access Moodle regularly as material may be updated at any time during the trimester
- *Other contact* - academic staff may also contact students either via Moodle messaging, or via email to the email address provided to KOI on enrolment.

### 2.6 Student Assessment

Assessment is designed to encourage effective student learning and enable students to develop and demonstrate the skills and knowledge identified in the subject learning outcomes. Assessment tasks during the first half of the study period are usually intended to maximise the developmental function of assessment (formative assessment). These assessment tasks include weekly tutorial exercises (as indicated in the weekly planner) and low stakes graded assessments (as shown in the graded assessment table). The major assessment tasks where students demonstrate their knowledge and skills (summative assessment) generally occur later in the study period. These are the major graded assessment items shown in the graded assessment table.

Final grades are awarded by the Board of Examiners in accordance with KOI's Assessment and Assessment Appeals Policy. The definitions and guidelines for the awarding of final grades are:

- *HD High distinction* (85-100%): an outstanding level of achievement in relation to the assessment process.
- *D Distinction* (75-84%): a high level of achievement in relation to the assessment process.
- *C Credit* (65-74%): a better than satisfactory level of achievement in relation to the assessment process.
- *P Pass* (50-64%): a satisfactory level of achievement in relation to the assessment process.
- *F Fail* (0-49%): an unsatisfactory level of achievement in relation to the assessment process.
- *FW:* This grade will be assigned when a student did not submit any of the compulsory assessment items.

Provided below is a schedule of formal assessment tasks and major examinations for the subject.

| Assessment Type | When Assessed | Weighting | Learning Outcomes Assessed |
|---|---|---|---|
| Assessment 1:<br>Weekly Tutorials | Week 2 – Week 11 | 20% | a, b, c, d and e |
| Assessment 2:<br>Research Project – Individual (1500 words) | Week 5 | 15% | c and e |
| Assessment 3:<br>Digital Forensic Principles - Individual (2000 words) | Report: Week 8<br>Presentation: weeks 9 | 25% | a and b |

| Assessment Type | When Assessed | Weighting | Learning Outcomes Assessed |
|---|---|---|---|
| Assessment 4:<br>Group report on professional computer forensic plan and demonstration (2500 words report) | Report: Weeks 11<br>Demonstration: Week 12 | Group – 20%<br>Demonstration – 10%<br>Presentation – 10%<br>Total - 40% | a, b, c, d, and e |

*Requirements to Pass the Subject:*

To gain a pass or better in this subject, students must gain a *minimum of 50%* of the total available subject marks.

### 2.7 Prescribed and Recommended Readings

Provided below, in formal reference format, is a list of the prescribed and recommended readings.

***Prescribed Text:***

Nelson, B., Phillips, A. and Steuart, C. (2024) Guide to Computer Forensics and Investigations. 7th edn. Mason, OH: Cengage Learning US. Available at: ProQuest Ebook Central

***Recommended Readings:***

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C. (2022) Cybercrime and digital forensics: An introduction. Abingdon: Routledge.

Gogolin, G. (2021) Digital forensics explained. Boca Raton, FL: CRC Press.

Johansen, G. (2020) Digital forensics and incident response. 2nd edn. Birmingham: Packt Publishing.

Kävrestad, J. (2020) Fundamentals of digital forensics. Cham: Springer International Publishing.

Sachowski, J. (2018) Digital forensics and investigation: People, process, and technology to defend the enterprise. 1st edn. Boca Raton, FL: CRC Press.

***Suggested Conference/ Journal Articles:***

Horsman, G. (2024) 'Sources of error in digital forensics', Forensic Science International: Digital Investigation, 48, p.301693.

Kebande, V.R. and Awad, A.I. (2024) 'Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions', ACM Computing Surveys, 56(5), pp.1-37.

Xiao, N., Wang, Z., Sun, X. and Miao, J. (2024) 'A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things', Alexandria Engineering Journal, 86, pp.631-643.

Sibe, R.T. and Kaunert, C. (2024) 'Digital Evidence, Digital Forensics, and Digital Forensic Readiness', in Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria. Cham: Springer Nature Switzerland, pp.57-83.

Ashawa, M., Mansour, A., Riley, J., Osamor, J. and Owoh, N.P. (2024) 'Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation', Cloud Computing and Data Science, pp.140-156.

Cook, M., Marnerides, A., Johnson, C. and Pezaros, D. (2023) 'A survey on industrial control system digital forensics: challenges, advances and future directions', IEEE Communications Surveys & Tutorials.

Brunty, J. (2023) 'Validation of forensic tools and methods: A primer for the digital forensics examiner', Wiley Interdisciplinary Reviews: Forensic Science, 5(2), p.e1474.

Yaacoub, J.P.A., Noura, H.N., Salman, O. and Chehab, A. (2022) 'Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations', Internet of Things, 19, p.100544.

Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M. and Patsakis, C. (2022) 'Research trends, challenges, and emerging topics in digital forensics: A review of reviews', IEEE Access, 10, pp.25464-25493.

Al-Dhaqm, A., Ikuesan, R.A., Kebande, V.R., Abd Razak, S., Grispos, G., Choo, K.K.R., Al-Rimy, B.A.S. and Alsewari, A.A. (2021) 'Digital forensics subdomains: the state of the art and future directions', IEEE Access, 9, pp.152476-152502.

***Useful Websites:***

The following industry websites are useful introductory sources covering a range of information useful for this subject.

- https://www.justice.gov/criminal/criminal-ccips
- https://www.htcia.org/
- https://nij.ojp.gov/topics/forensics
- https://www.isfce.com/

***Suggested Periodicals:***

- The Journal of Digital Forensics, Security and Law: https://www.jdfsl.org/
- Digital Investigation: https://www.journals.elsevier.com/digital-investigation
- Journal of Digital Forensic Practice: https://www.tandfonline.com/loi/udfp20

**Software Installation Links:**

- How to install Autopsy on MAC: https://app.box.com/s/s0m91m707kuujbo8asvnaorv9e8mqm88
- Remote Acquisition with F-Response: https://www.f-response.com/software/collect

***Conference/ Journal Articles:***

Students are encouraged to read peer reviewed journal articles and conference papers. Google Scholar provides a simple way to broadly search for scholarly literature. From one place, you can search across many disciplines and sources: articles, theses, books, abstracts and court opinions, from academic publishers, professional societies, online repositories, universities and other web sites.