DR. JOSEPH MAGUIRE

CYBER SYSTEM FORENSICS

University of Glasgow

OVERVIEW

- overview of cyber system forensics and what sort of topics will be explored in the course.
- aim of the course and intended learning outcomes of the course.
- consider the demographic of the audience and motivation for taking the course.
- assessment approach covered as well as general housekeeping.

COURSE COORDINATOR

- Dr. Joseph Maguire
- Email address: **joseph.maguire@glasgow.ac.uk**
- Office 410, Sir Alwyn Williams Building
- Office hours appointment can be booked through course Moodle.

CYBER SYSTEM FORENSICS

CYBER SYSTEM FORENSICS

CYBER SYSTEM FORENSICS

CYBER SYSTEM FORENSICS

CYBER SYSTEM
FORENSICS

CYBER SYSTEM FORENSICS

PRE-HISTORY

- consider the transformation of cyber system forensics from hobbyist concern to profession.
- comprehend the shaping of forensics from roots in financial crimes and child exploitation.
- understand the events that have influenced the development of cyber system forensics.
- appreciate the perceived impending crisis and challenges for cyber system forensics.

INVESTIGATIVE PROCESS

- understand that evidence can be categorised in terms of legal and investigative uses.
- comprehend the difference between digital investigation and digital forensic investigations.
- consider the different investigative models and how they relate to traditional crime scene model.
- consider the privacy implications from any digital investigative procedure.

DATA RECOVERY

- understand the importance of the file system and concept of slack space in recovering data.
- appreciate different allocation strategies and how these impact on data recovery.
- process of reconstructing files based on structure and content, instead of meta-data.
- comprehend the different types of file carving and appropriate use.

HASHING

- understand the important attributes of one-way hash functions.
- appreciate the importance of hashing in the chain of custody and the potential concerns of different approaches.
- comprehend the different types of hash, such as piecewise hash, rolling hash and context-triggered piecewise hash.
- appreciate the potential use of different hashing approaches beyond chain of custody and how it may support in digital investigation.

ANTI-FORENSICS

- consider some techniques that are used as counter measures to forensics analysis.
- appreciate the use of encryption and decryption to hamper digital investigations.
- comprehend the concept of data hiding and using files as a vessel for valuable data.
- understand the role redundancy plays in hiding data within other files.

TOOLS OF THE TRADE

- comprehend the different common tools that can be used in a digital investigation.
- appreciate the strengths and weakness of different tools for a given context.
- articulate appropriate tools and approaches for a given context to suits needs of investigation.
- critically evaluate cyber system tools and approaches for a given context.

COURSE SPECIFICATION

INTENDED LEARNING OUTCOMES

- understand the nature of countermeasures against forensic analysis.
- predict potential ethical, legal and regulatory concerns from gathered forensic evidence.
- effectively communicate complex outcomes from a forensic investigation to a non-technical audience, e.g. court-room.
- critically consider cyber system approaches for a given context.

COHORT DEMOGRAPHIC

- individuals that have **knowledge and experience in other disciplines**, but know little of computing science.
- individuals that have **industrial insight and experience of computing science**, but have little specialist knowledge or insight.
- individuals that have **solid computing science knowledge**, but lack specialist knowledge.
- most will have **little to no knowledge or experience of forensics**.

MOTIVATION

- develop knowledge and insight into the cyber system forensics and digital investigation.
- consider the aspects of cyber system forensics that inform development of 'forensic-ready' systems.
- appreciate the ethical and social concerns of the digital investigation process and forensics.
- generate future research and/or industrial products that have some cyber system forensic thinking to them.

RESEARCH LINKAGE

- research in the areas of forensics and cyber security are considered within the course.
- students will typically be expected to read and consider a research paper each week.
- team exercise expects students to consider research and emerging thinking in the area.

LECTURE SLIDES

- Slides will be available via course Moodle.

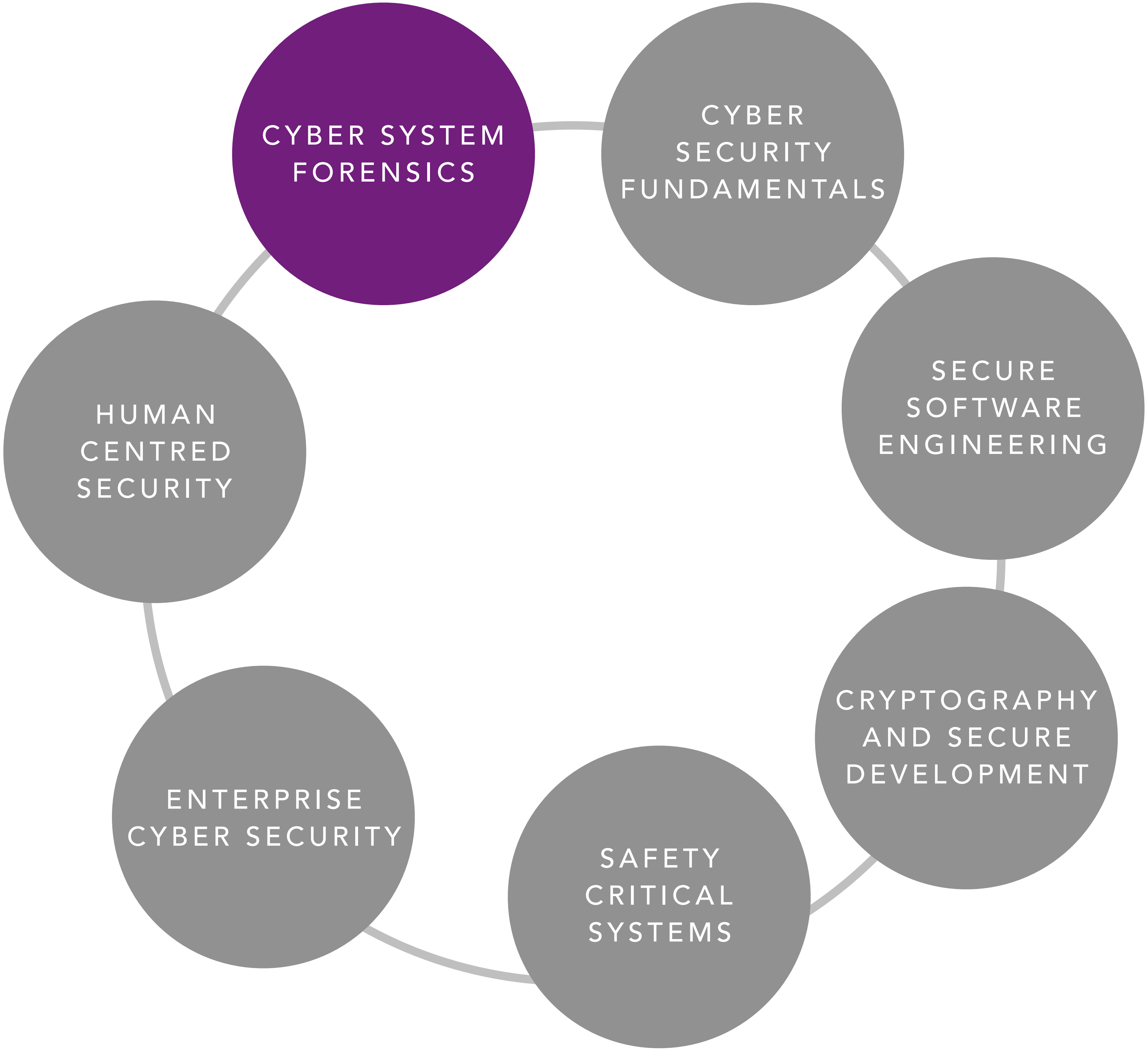
READING LIST

- reading list is accessible via the course Moodle.
- where possible the resources point to digital copies that many students should be able to access.
- reading list material is not a replacement for lectures, but supplementary to them.

AUDIENCE

- criminal activity and laws will be discussed and when expressing yourself, be mindful of your peers.
- international audience, varying opinion and law.
- mindful of the topics and the debate, we will discuss law and criminal activity, but such discussions should not be interpreted as advocacy for specific activities.

WHERE DOES THE SUBJECT FIT WITHIN THE SECURITY OPTIONS?



CYBER SYSTEM FORENSICS

CYBER SECURITY FUNDAMENTALS

SECURE SOFTWARE ENGINEERING

CRYPTOGRAPHY AND SECURE DEVELOPMENT

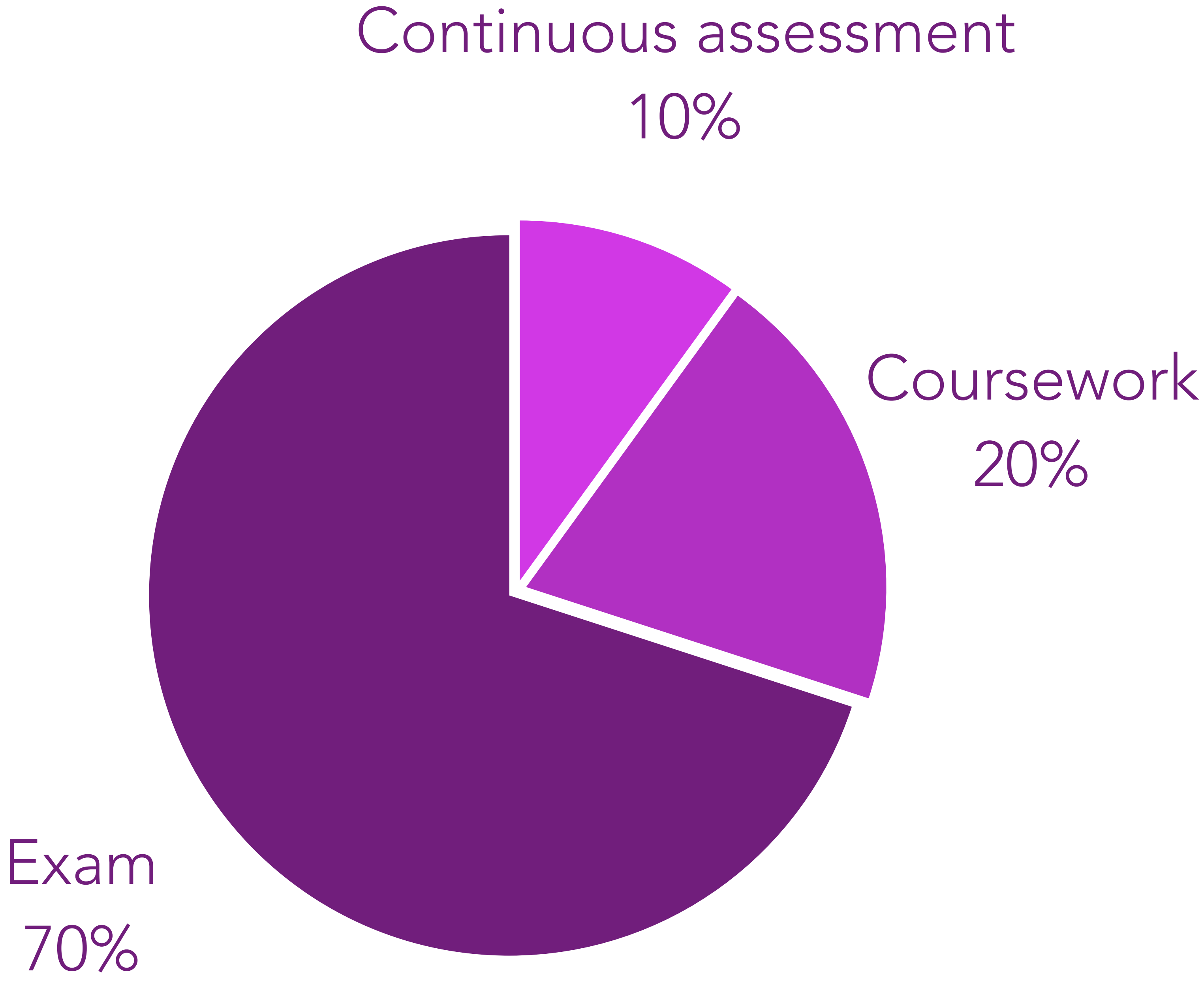
SAFETY CRITICAL SYSTEMS

ENTERPRISE CYBER SECURITY

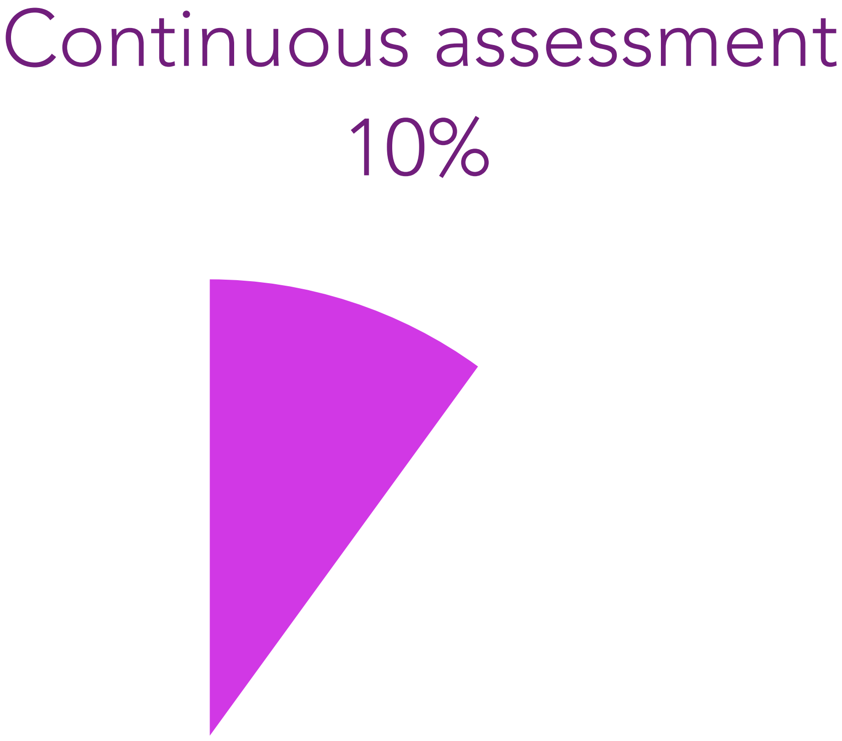
HUMAN CENTRED SECURITY

ASSESSMENT

ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



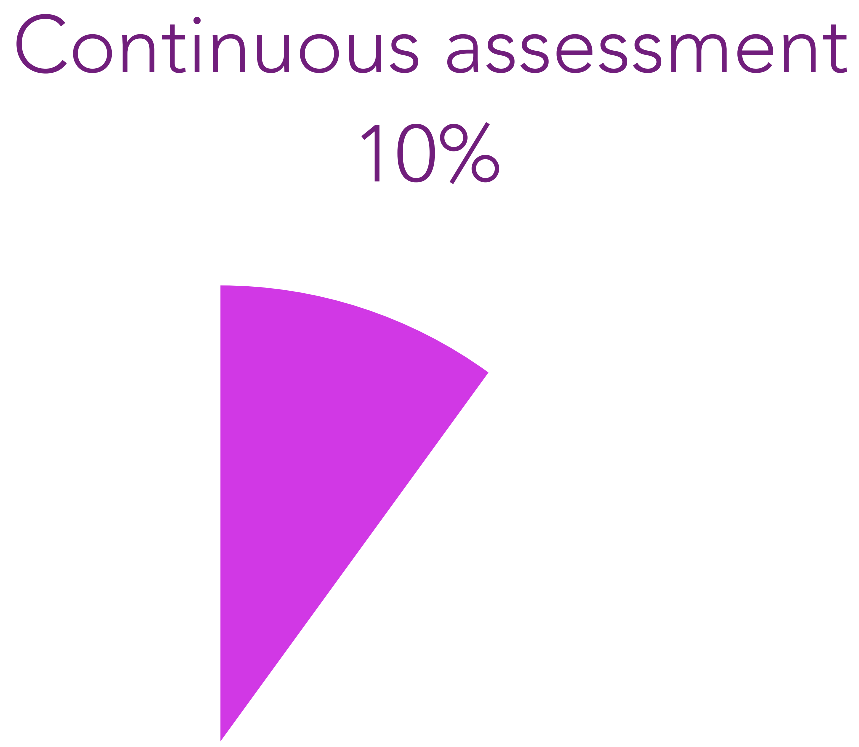
CONTINUOUS ASSESSMENT

- 10% of the individual final grade will be gained from continuous assessment.
- takes the form of a weekly quiz that probes research paper(s) reading.
- research paper(s) will be issued via Moodle and students are expected to prepare for a quiz the following week.
- research paper(s) may also prove a valuable resource for answering exam questions.

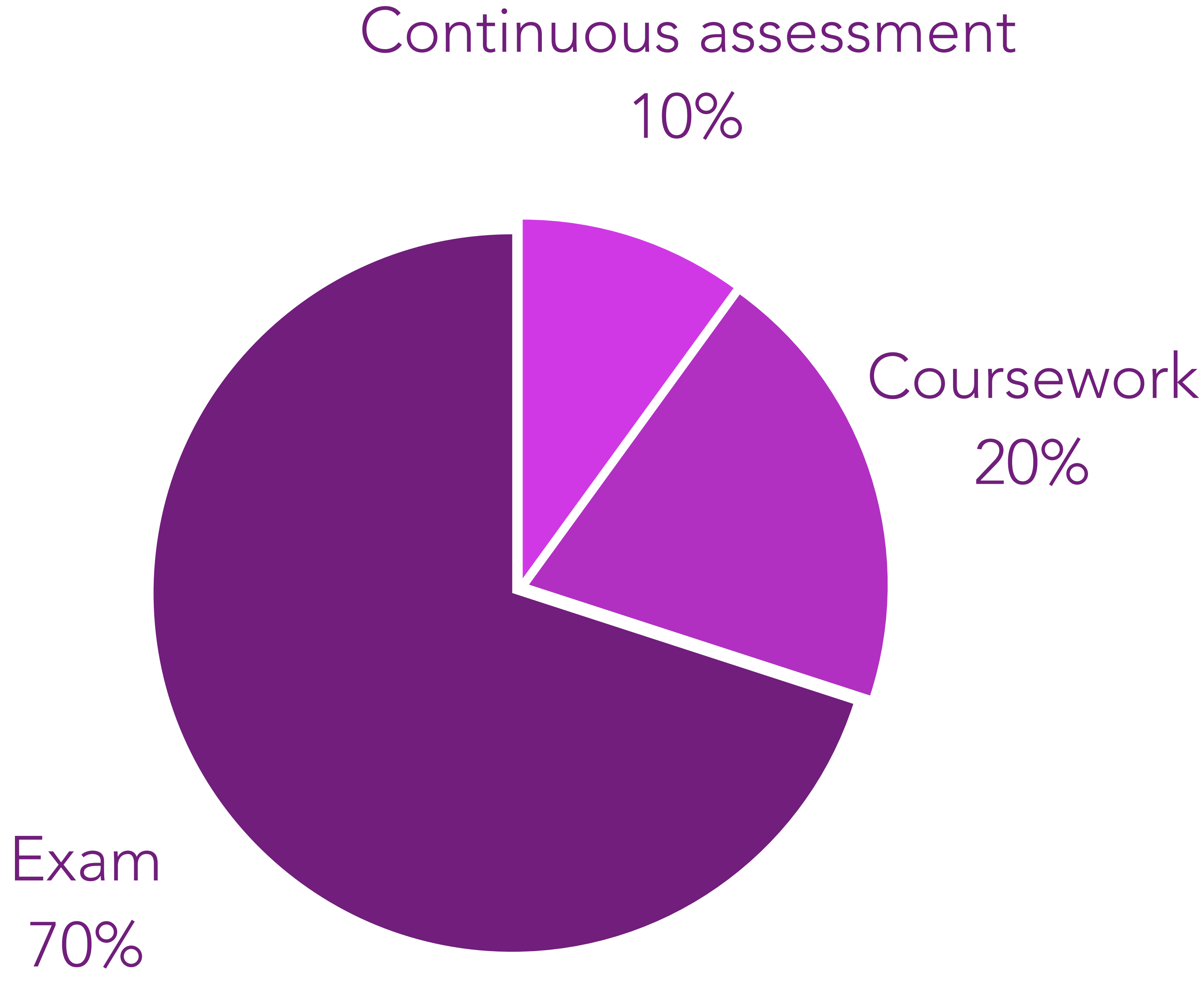
MOODLE QUIZ

- available from 12 noon the day before each teaching session, until 09:30 on each teaching day.
- one mark for each correct question, half-mark for each incorrect response and no mark for not answering a question.
- reading list of research papers available now on course Moodle.

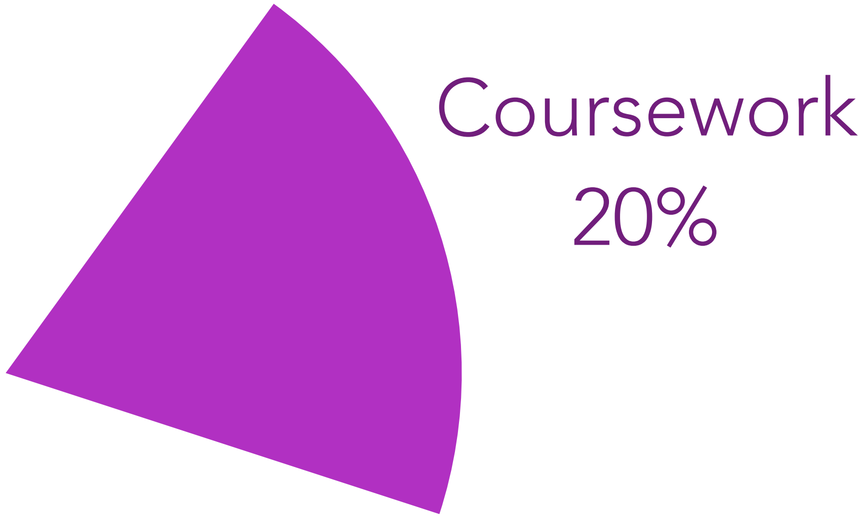
ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



TEAM COURSEWORK

- research countermeasures against forensics analysis and communicate that to a non-technical audience through a report and presentation.
- teams decide route as coursework has both **non-programming** and **programming** routes.
- assessed specification will be released shortly via Moodle.

TEAM COURSEWORK

- 20% gained through individual performance on a group coursework.
- teams are **self-organising** and task can be completed by no more than three members.
- teams submit workload report and personal assessment of contribution that is used to generate the **final individual grade** for coursework.
- every team member must submit by **4.30pm on Monday the 16th of March 2018.**

ASSESSMENT WEEK

- the week prior to the submission of the team assessed exercise the class will not meet.
- teams can use the time to finish work on the assessed exercise.
- no session during assessment week

DELIVERABLES

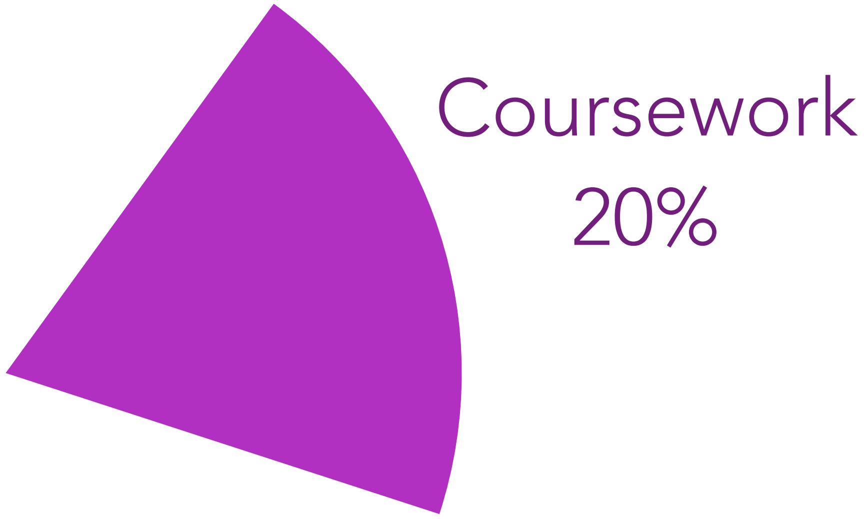
DELIVERABLES

- **presentation**, generated as a team and submitted via Moodle using team submission link.
- **report**, generated as a team and submitted via Moodle using team submission link.
- **workload record**, generated as a team and submitted with report and presentation..
- **personal assessment of contribution**, generated individually and submitted separately.
- depending on the route followed teams may be required deliver additional content.

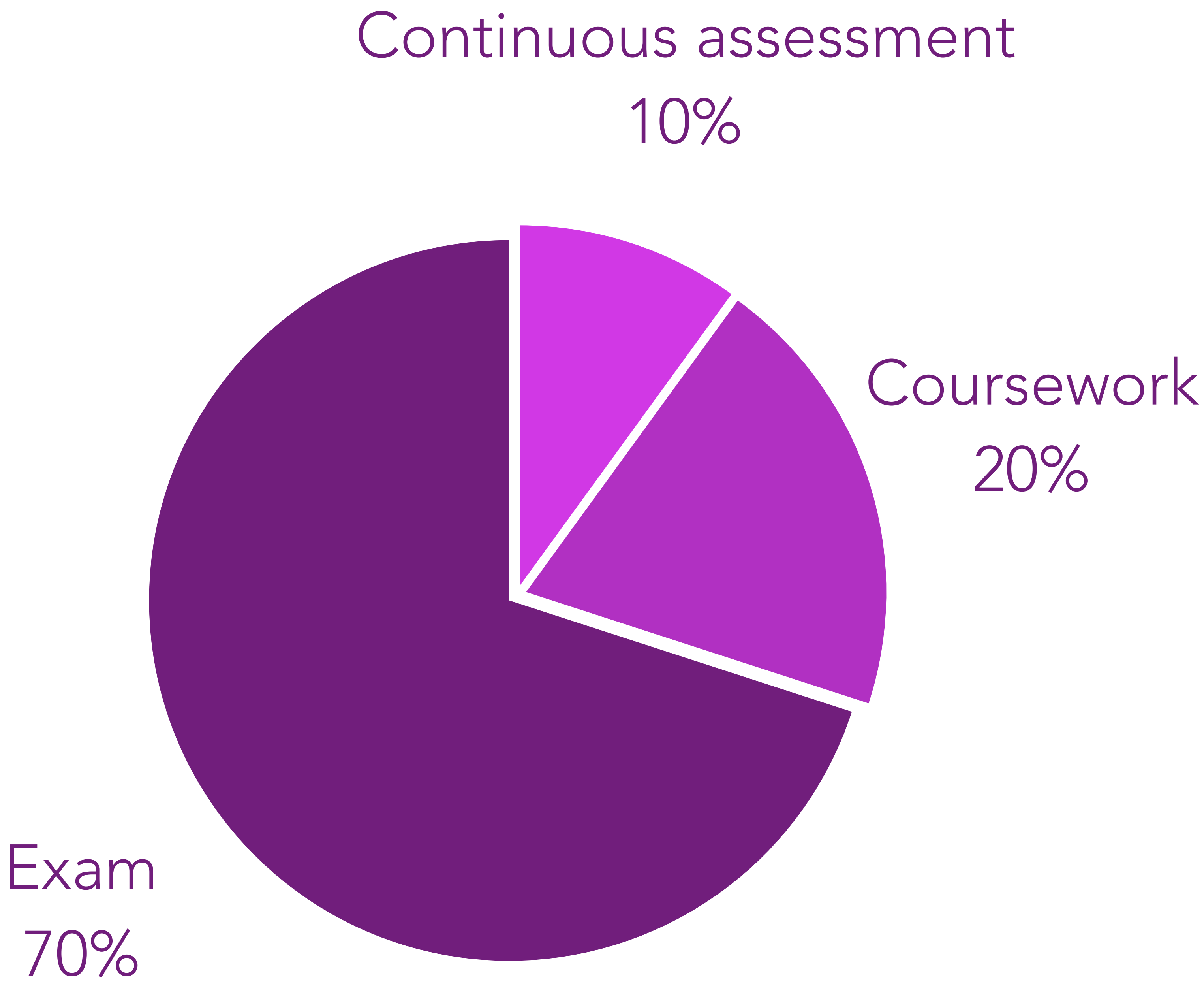
TIMETABLE

DATE	MILESTONE
TUESDAY 14TH OF JANUARY	ASSESSED EXERCISE ANNOUNCED
FRIDAY 24TH OF JANUARY	TEAMS CONFIRMED VIA MOODLE
TUESDAY 10TH OF MARCH	ASSESSMENT WEEK (NO CLASS) (TBC)
MONDAY 16TH OF MARCH	WORKLOAD RECORD AND PERSONAL ASSESSMENT OF CONTRIBUTION
	REPORT AND PRESENTATION

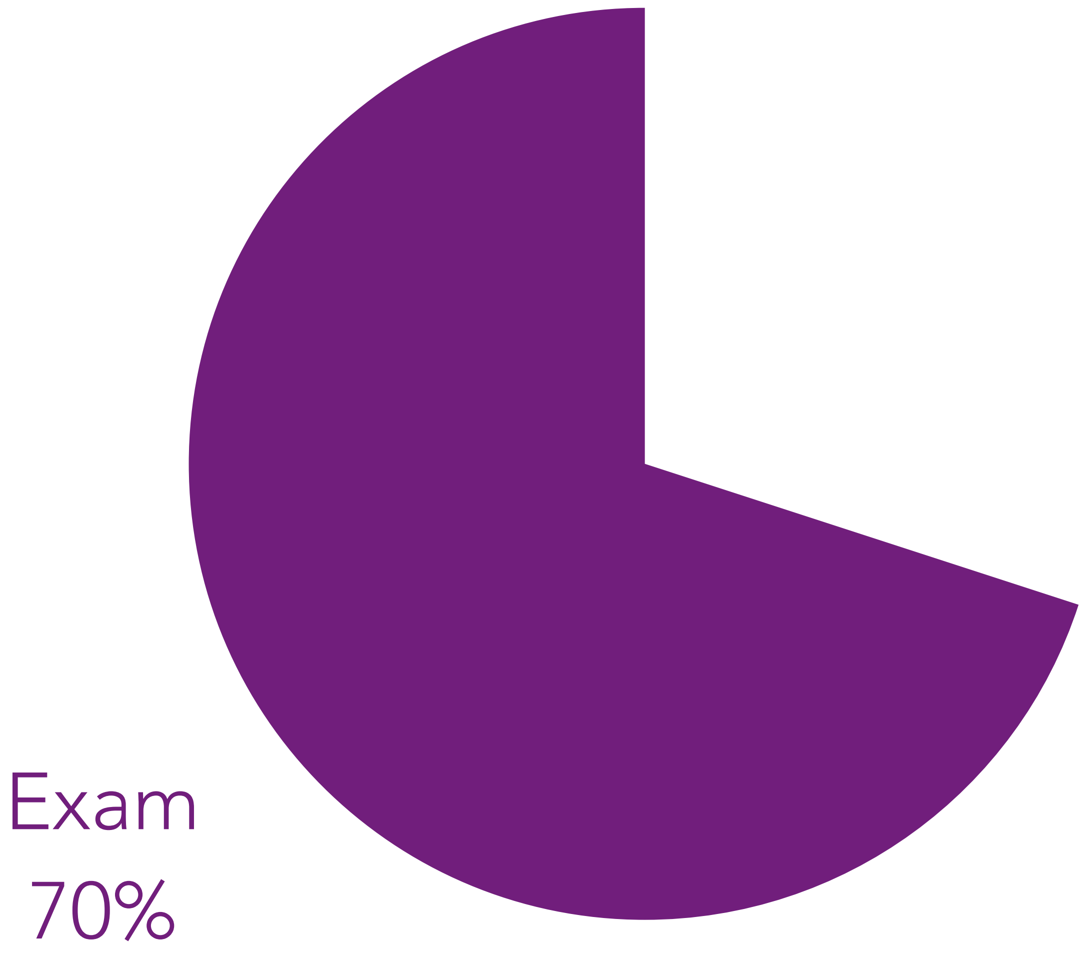
ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



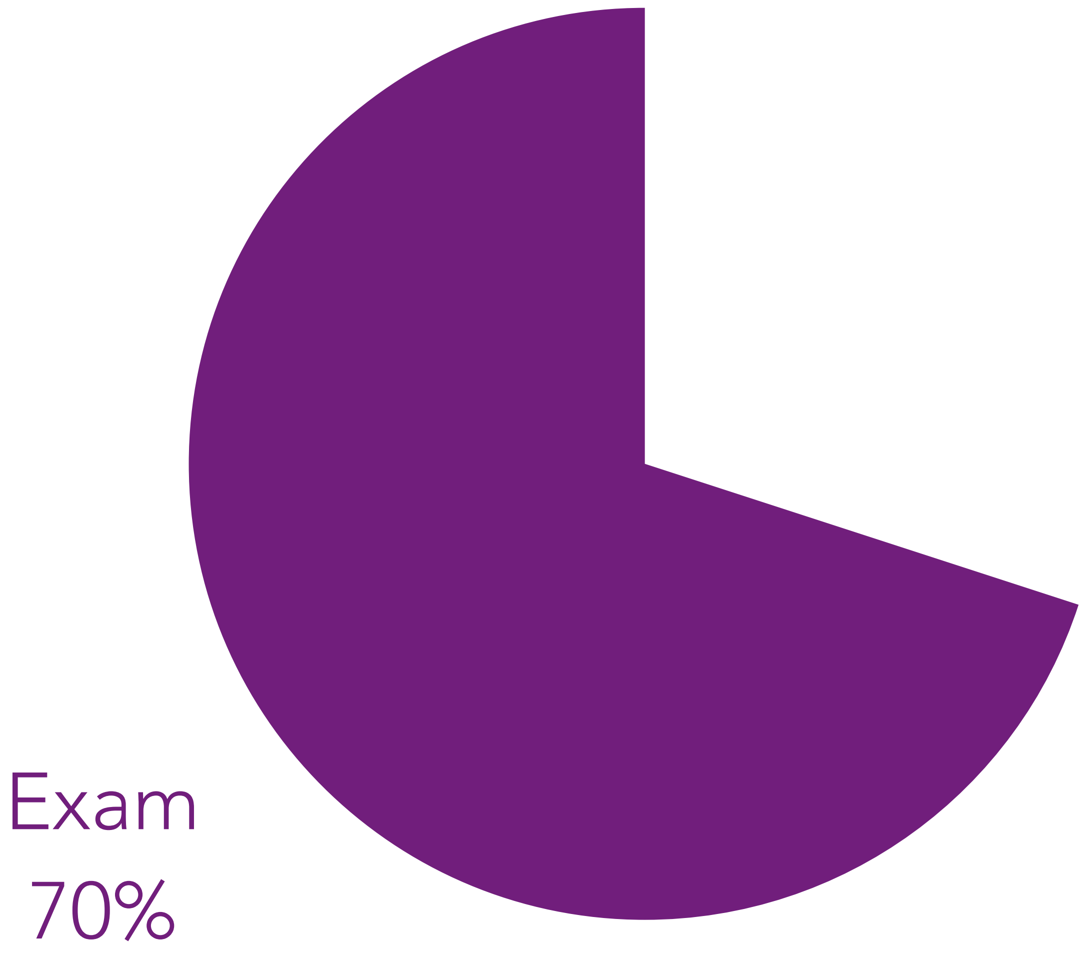
EXAM

- 70% of grade will be gained from individual performance on summer exam.

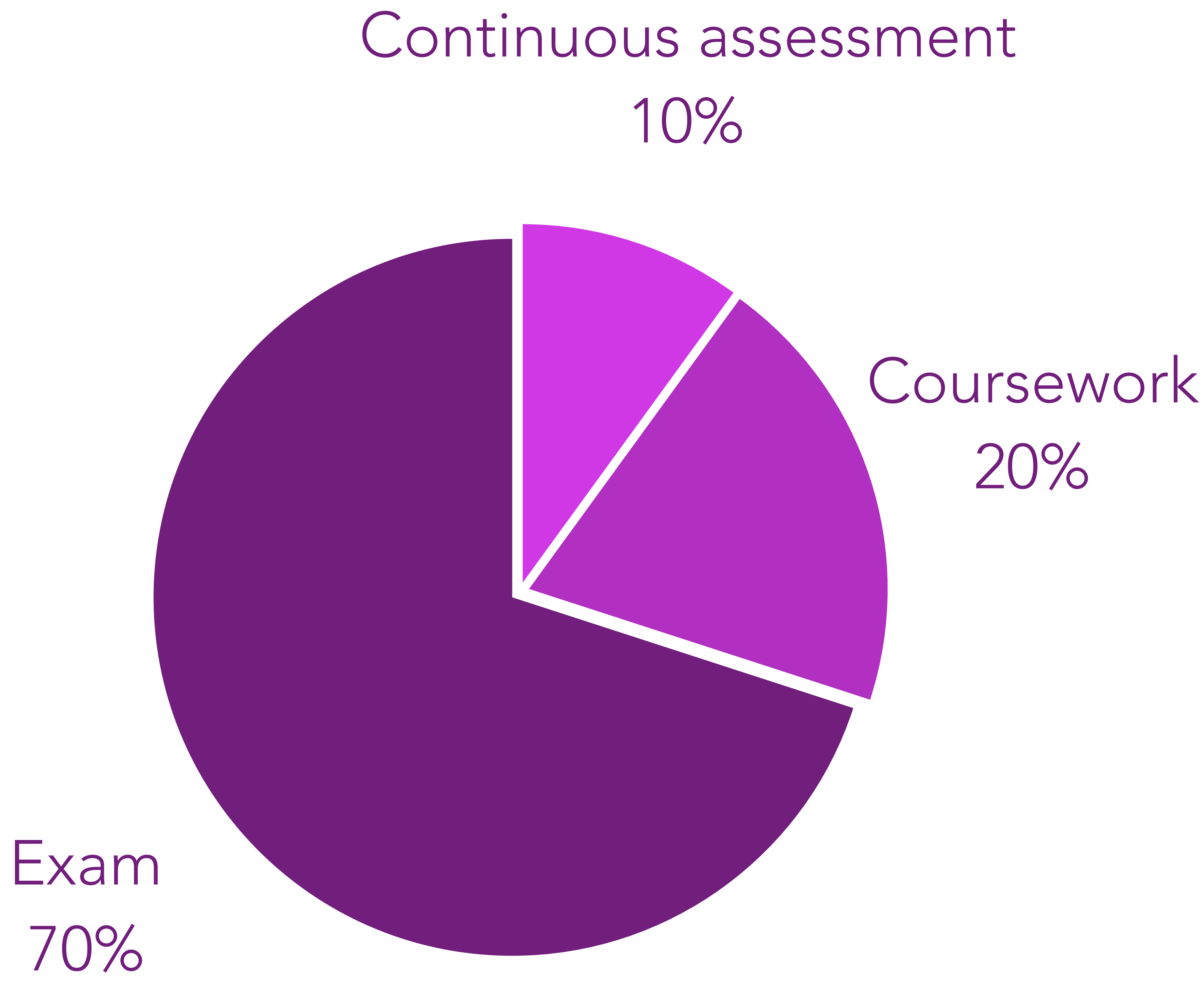
- individuals must attempt at least 80% of course to obtain final grade.

- revision session typically offered nearer the end of course.

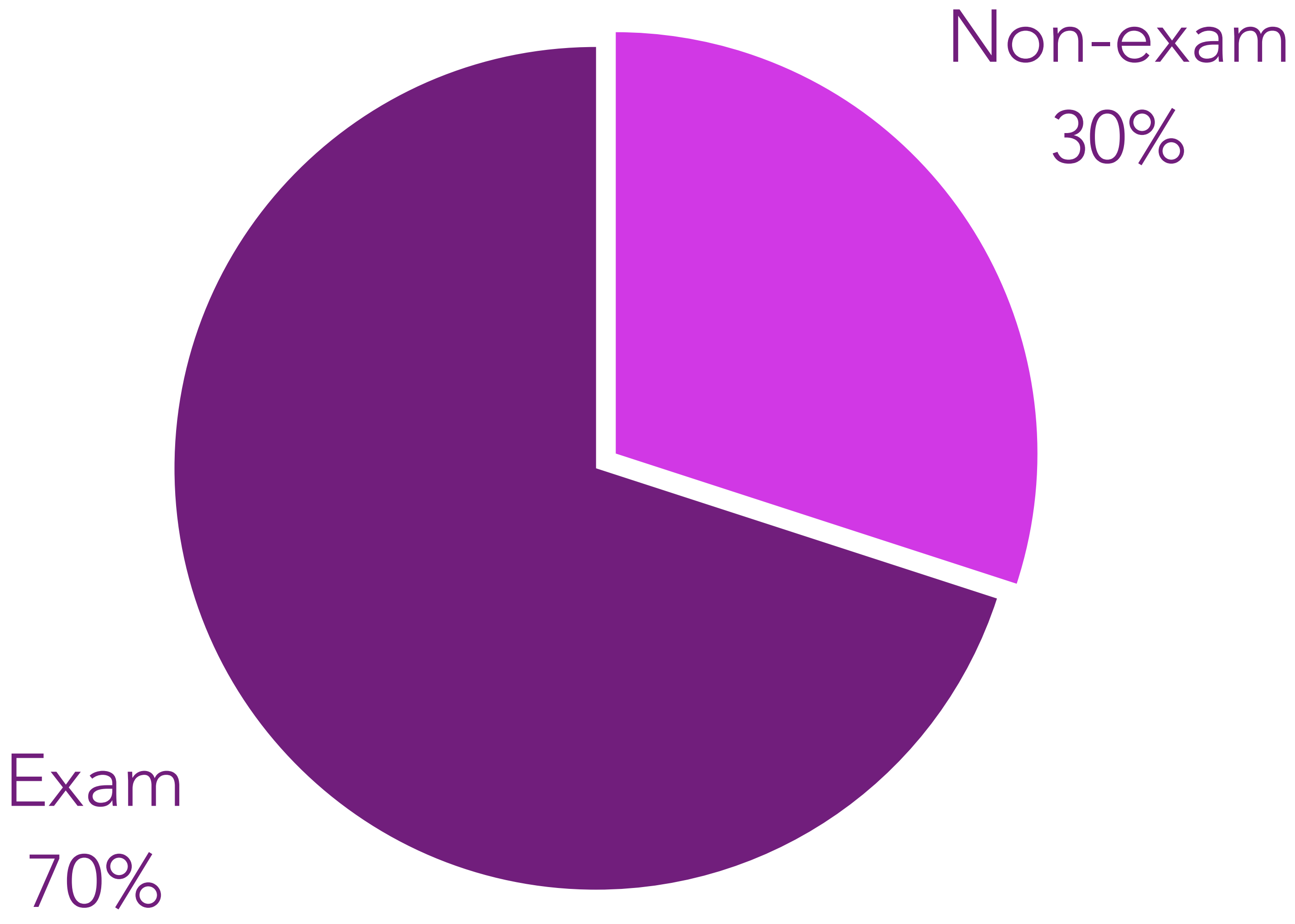
ASSESSMENT OVERVIEW



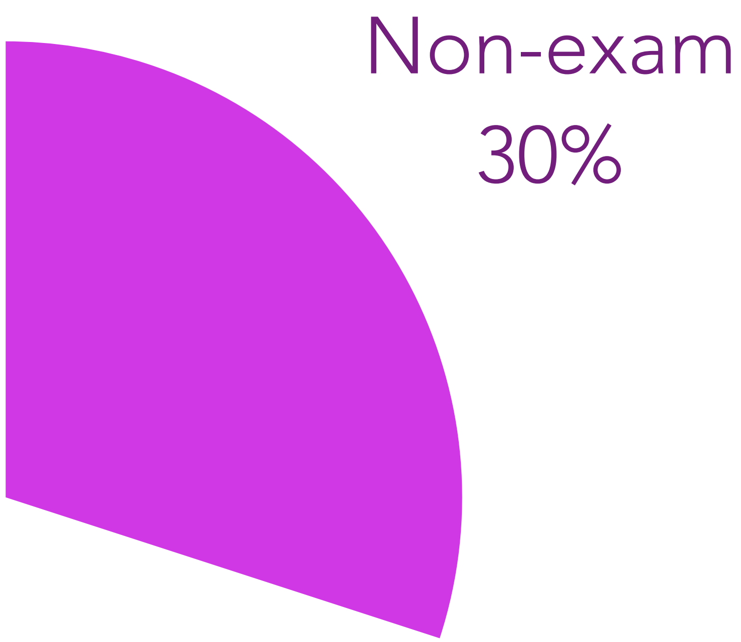
ASSESSMENT OVERVIEW



ASSESSMENT OVERVIEW



MINIMUM REQUIREMENT FOR THE AWARD OF COURSE CREDIT



WELCOME QUIZ

SUMMARY

- defined cyber system forensics and what sort of topics will be explored in the course.
- outlined the aim of the course and intended learning outcomes of the course.
- considered the demographic of the audience and motivation for taking the course.
- covered the assessment approach as well as general housekeeping.

DR. JOSEPH MAGUIRE

CYBER SYSTEM FORENSICS

University of Glasgow