UNIVERSITI TEKNOLOGI MARA

MRM810: DIGITAL RECORDS FORENSIC AND E-DISCOVERY

Course Name (English)	DIGITAL RECORDS FORENSIC AND E-DISCOVERY APPROVED
Course Code	MRM810
MQF Credit	3
Course Description	The course is designed for information professional background in understanding the electronic evidence field. Digital Forensic is one aspect of authentication process of information to be used in legal proceeding, apart from the Electronic Discovery which offers skill of drilling into detail of information and records. The skill and knowledge acquired from both domains serve as an important aspect in expending the field of information domain. The course discusses the trends, enforcement functions and also highlights the importance of understanding the various computer devices, forensic processes and techniques as well as forensic tools to counter the threats. Student also will be taught practical aspect of conducting the forensic investigation as well performing electronic discovery
Transferable Skills	Computer Forensic Models & Processes Evidence Analysis Search Skill
Teaching Methodologies	Lectures, Practical Classes, Reading Activity, Problem Based Learning (PBL)
CLO	CLO1 Establish association and integration aspects records management field and digital records forensic discipline as well as to apply the course with with both industry and academic fields. CLO2 Understand forensic processes and techniques, various computer storage and devices, forensic tool selection as well as some legal aspect which applicable throughout the digital records forensic and electronic discovery processes. CLO3 Explain the digital records forensic investigation in accordance to the legal requirements
Pre-Requisite Courses	No course recommendations

Topics
1. 1.0 Subject Introduction 1.1) 1.1 Objective of digital forensic 1.2) 1.2 Terminologies 1.3) 1.3 Records Management and Digital Forensic 1.4) 1.4 Type of computer crimes 1.5) 1.5 Anti Forensic
2. 2.0 Records Management from Malaysia's Forensic perspective 2.1) 2.1 Digital Forensic and E-Discovery from records management's perspective 2.2) 2.2 Digital Forensic: Local perspective 2.3) 2.2.1. Authority and Enforcement 2.4) 2.2.2. Researches
3. 3.0 Digital Forensic Readiness 3.1) 2.1 Benefit of digital forensic readiness 3.2) 2.2 The need for digital forensic investigation readiness 3.3) 2.3 A Forensic Readiness Implementation Guide
4. 4.0 Law and Digital forensic 4.1) 4.1 Court cases 4.2) 4.2 Privacy Issues and computer forensic 4.3) 4.3 European Law 4.4) 4.4 Malaysia Cyber law and computer forensic: An overview
5. 5.0 Digital Forensic Investigation processes & Models 5.1) 5.1 Principles in digital forensic investigation. 5.2) 5.2 Securing computer evidence 5.3) 5.3 Preparation for search 5.4) 5.4 Chain of evidence 5.5) 5.5 Investigation process 5.6) 5.6 Presentation
6. 6.0 Responding to the incident 6.1) 6.1 Procedures 6.2) 6.2 Categories 6.3) 6.3 Challenges
7. 7.0 Understanding Digital Evidence Premises 7.1) 7.1 Volatile 7.2) 7.2 Non-volatile 7.3) 7.3 IOT
8. 8.0 Computer forensic tools 8.1) 8.1 Hard disk 8.2) 8.2 Windows 8.3) 8.3 RAM 8.4) 8.4 Registry 8.5) 8.5 Mobile 8.6) 8.6 Open Source 8.7) 8.7 Database
9. 9.0. Computer Memory 9.1) 9.1 Magnetic Tape 9.2) 9.2 Portable (PDA), Memory card, Flash memory, USB Flash drive, SSD, RRAM etc
10. 10. Future in Computer Forensic challenges 10.1) 10.1 Current Challenges 10.2) 10.1.1 Encryption 10.3) 10.1.2 Cloud forensic 10.4) 10.1.3 Tiage/volume of data 10.5) 10.1.4 Legal challenge 10.6) 10.1.5 Growth in digital crime 10.7) 10.1.6 Lack of resources 10.8) 10.1.7 Cross-border cooperation 10.9) 10.1.8 New Application 10.10) 10.1.9 Lack of new forensic tools
11. 11.0 Balancing E-discovery Challenges with Legal and IT Requirements 11.1) 11.1 Practises 11.2) 11.2 Tools and techniques in the market 11.3) 11.3 Industry evolves with their new methodologies, inventions, and ideas 11.4) 11.4 Legal Gap
12. 12. Special Topics 12.1) 12.1 Cyberpsychology and Computer Forensic 12.2) 12.2 Media Social Forensic Investigation 12.3) 12.3 Covert Espionage 12.4) 12.4 Windows Forensics

Assessment Breakdown	%
Continuous Assessment	100.00%

Details of Continuous Assessment

Assessment Type	Assessment Description	% of Total Mark	CLO
Assignment	This assignment utilizes the public response (Crowd Sourcing) on the relevant internet forums on the pre-determined topic of students choice. Student firstly proposes a topic/scope to venture in, present for the lecturer consent, post on the internet forum and produce knowledge discovery in mind map format.	20%	CLO1
Assignment	Anti Forensic This assignment offers student an competitive advantage over the data manipulation to in avoid conviction from the authority	20%	CLO2
Final Project	Project varies shoud demonstrate the students' comprehension of a combination of subject content and the academic/Legal/innovation/Business aspect	30%	CLO3
Online Quiz	Test to measure comprehension the lessons taught throughout the semester	30%	CLO3

Reading List

This Course does not have any book resources

Article/Paper List

Recommended Article/Paper Resources

- **Dauda Sule 2014, Importance of Forensic Readiness, *ISACA Journal*, ISACA Journal Volume 1, 2014** https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/JOnline-Importance-of -Forensic-Readiness.aspx
- **Alastair Irons 2006, Computer forensics and records management – compatible disciplines, *Records Management Journal*, Vol. 16 Issue: 2,, pp.1** http://www.emeraldinsight.com/doi/pdfplus/10.1108/09565690610677463
- **David Lillis, Brett A. Becker, Tadhg O'Sullivan and Mark Scanlon 2016, CURRENT CHALLENGES AND FUTURE RESEARCH AREAS FOR DIGITAL FORENSIC INVESTIGATION, v1 [cs.CR] 13 Apr 2016**
- **TIMOTHY M. OPSITNICK, JOSEPH M. ANGUILANO AND TREVOR B. TUCKER 2017, Using Computer Forensics to Investigate Employee Data Theft, *law Journal Newsletter*** http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/05/01/usin g-computer-forensics-to-investigate-employee-data-theft-2/?slreturn=20170810222042
- **Forensic Focus 2016, Current Challenges In Digital Forensics, *Forensic Focus-For Digital Forensic and Discovery Professional*, MAY 11, 2016** https://articles.forensicfocus.com/2016/05/11/current-challenges-in-digital-fore nsics/

Other References

- **Book Gerard Johansen 2020, *Digital Forensics and Incident Response Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition*, PacktPublishing, Birmingham, UK**

