MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

1.	Name of Course	Digital Forensics
2.	Course Code	TDF 3241
3.	Status of Course [Applies to (cohort)]	Specialisation Core for B.IT Security Technology
4.	MQF Level/Stage Note : *Certificate – MQF Level 3* *Diploma – MQF Level 4* *Bachelor – MQF Level 6* *Masters – MQF Level 7* *Doctoral – MQF Level 8*	Bachelor – MQF Level 6
5.	Version (State the date of the Senate approval – history of previous and current approval date)	Date of previous version: - Date of current version: June 2014
6.	Pre-Requisite	TCS2251 Computer Security
7.	Name(s) of academic/teaching staff	Ho Yean Li Ooi Shih Yin
8.	Semester and Year offered	Trimester 2, Year 3
9.	Objective of the course in the programme: This course exposes students to the forensics tools, methods, and procedures used for investigation of computers, techniques of data recovery and evidence collection, protection of evidence, expert witness skills, and computer crime investigation techniques.	
10.	Justification for including the course in the programme: Digital forensics is one of the major domains in computer security study, where it is most often associated with the investigation of a wide variety of computer crimes.	

11.	Course Learning Outcomes :	Domain	Level
	LO1 Apply and discover various forensic tools employed by computer forensics experts.	Cognitive	3
	LO2 Examine and analyze the forensic evidences from the seized digital devices.	Cognitive	4
	LO3 Compile and summarize the forensic evidences into the investigative reports.	Cognitive	5
	LO4 Evaluate the digital evidences.	Cognitive	6
12.	Mapping of Learning Outcomes to Programme Outcomes :		

MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

	Learning Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9
	LO1	X						X	X	
	LO2	X						X	X	
	LO3	X						X	X	X
	LO4	X						X	X	X

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Mid Test	Written test	10%
Laboratory	Practical work and report	30%
Quizzes	Written quizzes	10%
Final Examination	Written examination	50%

14. Mapping of assessment components to learning outcomes (LOs)

Assessment Components	LO1	LO2	LO3	LO4
Mid Test		14.29	14.29	14.29
Laboratory	100			
Quizzes		14.29	14.29	14.29
Final Examination		71.42	71.42	71.42

15. Details of Course

Topics	Mode of Delivery (eg : Lecture, Tutorial, Workshop, Seminar, etc.) Indicate allocation of SLT (lecture, tutorial, lab) for each subtopic	
	Lecture	Lab
1 **Computer Forensics and Investigation Processes** Understanding computer forensics, preparing for computer investigations, maintaining professional conduct.	2	2
2 **Understanding Computing Investigations** Preparing a computer investigation with systematic approach, procedures for corporate high-tech investigations, understanding data recovery workstations and software	2	2
3 **The Investigator's Office and Laboratory**	2	2

	Understanding forensics lab certification requirements, determining the physical requirements for a computer forensics lab, selecting a basic forensic workstation, building a business case for developing a forensics lab.		
	4 **Data Acquisitions** Understanding storage formats for digital evidence, determining the best acquisition model, contingency planning for image acquisitions, using forensics acquisition tools, validating data acquisitions.	2	2
	5 **Processing Crime and Incident Scenes** Identifying digital evidence, collecting digital evidence, processing law enforcement crime scenes, securing a computer incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash	2	2
	6 **Working with Windows and DOS Systems** Understanding file systems, exploring Microsoft file structures, examining NTFS disks, understand whole disk encryption, understanding the Windows registry	2	2
	7 **Current Computer Forensics Tools** Evaluating current forensics tools, validating current forensics tools, hardware forensics tools, software forensics tools	2	2
	8 **Macintosh and Linux Boot Processes and File Systems** Understanding the Macintosh file structures and boot process, examining UNIX and Linux disk structures and boot process	2	2
	9 **Computer Forensics Analysis** Determining the data to collect and analyze, validating the forensics data, addressing data-hiding techniques, performing remote acquisition.	2	2
	10 **Recovering Graphics Files** Recognizing a graphics file, understanding data compression, identifying unknown file formats,	2	2

SUMMARY OF INFORMATION ON EACH COURSE

	understanding copyright issues with graphics		
	11 **Virtual Machines, Network Forensics, and Live Acquisitions** Virtual machines overview, network forensics overview, performing live acquisitions, using network tools	2	2
	12 **E-mail Investigations** Exploring the role of email in investigation, investigating email crimes and violations.	1	1
	13 **Cell Phone and Mobile Device Forensics** Understanding mobile devices forensics, understanding acquisition procedures for cell phones and mobile devices	1	1
	14 **Report Writing for High-Tech Investigations, Expert Testimony in High-Tech Investigations** Understanding the importance of reports, generating report findings with forensics software tools	1	1
	15 **Ethics and High-Tech Investigations** Preparing for testimony, testifying in court, preparing for a deposition or hearing, preparing forensic evidences for testimony.	1	1
	Total	**26**	**26**

	Total Student Learning Time (SLT)	Face to Face / Guided Learning	Independent Learning
	Lecture	26	26
	Tutorials	0	0
	Laboratory/Practical	26	13
	Presentation	0	0
	Assignment	0	0
	Mid Term Test	1	3
	Final Exam	2	20
	Quizzes	3 times	3
	Sub Total	55	65
	Total SLT	**120**	
16.	Credit Value	**120/40 = 3**	

MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

17. Reading Materials :

Textbooks

Bill Nelson, Amelia Phillips, Christopher Steuart (2015). Guide to Computer Forensics and Investigations, Fifth Edition, ISBN-13: 978-1285060033. Cengage Learning

Reference Material (including 'Statutes' for Law)

Eoghan Casey BS MA (2011). Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet, ISBN-10: 0123742684.
Eoghan Casey BS MA (2009). Handbook of Digital Forensics and Investigation, ISBN-10: 0123742676

Appendix (to be compiled when submitting the complete syllabus for the programme) :

1. Mission and Vision of the University and Faculty
2. Programme Objectives or Programme Educational Objectives
3. Programme Outcomes (POs)
4. Mapping of POs to the 8 MQF domain
5. Summary of the Bloom's Taxonomy's Domain Coverage in all the Los in the format below :

Subject	Learning Outcomes (please state the learning 0utcomes)	Bloom's Taxonomy Domain		
		Affective	Cognitive	Psychomotor
ABC1234	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			
DEF5678	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			

6. Summary of LO to PO measurement
7. Measurement and Tabulation of result for LO achievement
8. Measurement Tabulation of result for PO achievement