Mahatma Gandhi University
Kottayam

Programme	**BSc (Hons) Cyber Forensics**				
Course Name	**INTRODUCTION TO DIGITAL FORENSICS AND TOOLS**				
Type of Course	DSC A				
Course Code	MG1DSCCFS100				
Course Level	**100-199**				
Course Summary	The course is about preserving evidence, identifying criminals, protecting corporate interests, assisting in cyber crime investigations, and facilitating legal proceedings.				
Semester	I	Credits		4	Total Hours
Course Details	Learning Approach	Lecture	Tutorial	Practical	Others
		3	0	1	0	75
Pre-requisites, if any					

COURSE OUTCOMES (CO)

CO No.	Expected Course Outcomes upon completion of this course , the students will be able to:	Learning Domains *	PO No
1	Understand the role and uses of digital forensics in criminal investigations.	Understand	1,2
2	Understand how data are collected as evidence and analyse windows system artifacts	Understand	1,2
3	Analyse image files and artifacts using appropriate tools.	Analyse	3
4	Undertake basic digital forensic investigation, by using a variety of digital forensics tools.	Apply	3,4
Remember (K), Understand (U), Apply (A), Analyse (An), Evaluate (E), Create (C), Skill (S), Interest (I) and Appreciation (Ap)			

COURSE CONTENT

Content for Classroom transaction (Units)

Module	Units	Course description	Hrs	CO No.
1	1.1	Introduction to Digital Forensics, Forensic Science, Uses of Digital Forensics	3	1
	1.2	Procedure of digital evidence-Identification, Collection and Preservation	3	1,2
	1.3	Lab tools-Forensic laboratories, virtual labs, lab security	4	2
	1.4	Evidence Storage, Policies and Procedures	3	2
2	2.1	Collecting Evidence: Crime Scenes and Collecting evidence, Documenting the scenes	5	2
	2.2	Chain of custody, Live system vs Dead System, Hashing, Report	4	2
	2.3	Windows System artifacts: Registry, Deleted data, Hibernation file	5	1,2
3	3.1	Introduction to Anti-forensics: hiding data, Password attacks, Steganography, Data Destruction	3	1,3
	3.2	Network Forensics: Fundamentals, types, attacks	2	1,3
	3.3	Legal: Basics of law, the fourth amendment, Criminal law, Searching with a warrant, e Discovery	4	1,3
	3.4	Apply theoretical knowledge through hands-on labs and practical – Identification and collection-Autopsy	5	3,4
	3.5	Registry Analysis – Reg-ripper	4	3,4

		Data Preservation tool – Guymager		
4	4.1	Introduction to data carving tools- Analyse an image -FTK	10	1,4
	4.2	Analyse an image file using - Pro Discover	10	4
	4.3	Data carving tool- FDAC, Foremost, Scalpel, Steganography - steghide	10	4
5	5.1	Teacher Specific content. This can be either class room teaching, practical session, field visit etc as specified by the teacher concerned. Evaluation is internal.		

Teaching and Learning Approach	**Classroom Procedure (Mode of transaction)** **Lecture and Practical**
Assessment Types	**MODE OF ASSESSMENT** **A. Continuous Comprehensive Assessment (CCA) 25 Marks** **Written Test / Seminar / Viva/ Assignments** **Practical 15 Marks**
	B. Semester End examination 50 Marks **Written test** **Practical Examination 35 Marks**

References

1. Digital Forensics with Kali Linux Enhance your investigation skills by performing network and memory forensics with Kali Linux 2022.x, 3rd Edition (Kindle Edition)Shiva V. N. Parasram
2. The Basics of Digital Forensics The Primer for Getting Started in Digital Forensics John Sammons Technical Editor Jonathan Rajewski
3. Cyber Forensics - Concepts and Approaches, Ravi Kumar & B Jain,2006, ICFAI University press
4. Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, John R. Vacca, Charles River Media, 2005