Majmaah University

College of Computer and Information Science (CCIS)

Department of Information Technology

Proposed Program

MS in Cybersecurity and Digital Forensics (CSDF)

ماجستير الأمن السيبراني والأدلة الرقمية

كلية علوم الحاسب والمعلومات

قسم تقنية المعلومات

MS in Cybersecurity and Digital Forensics (MS in CSDF)

Introduction

The Department of Information Technology in the College of Computer and Information Science (CCIS) at Majmaah University (MU) offers a MS degree in Cybersecurity and Digital Forensics (CSDF) that is cross-disciplinary and includes technology, management, compliance, and legal issues available in the Kingdom of Saudi Arabia.

Foundations Digital Forensics

Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law.

Foundations of Cyber security

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access.

Program details

Program title	**MS in Cybersecurity and Digital Forensics**
Title abbreviation	MS in CSDF
Program type	Master's Degree by Coursework and Research Project
Status	Proposed to open 1st Semester 2018-2019
Administered by	College of Computer and Information Sciences
Intake periods	First semester
Attendance type	Full-time
Credit hours required	30 credit hours
Standard program duration	2 years full-time
Maximum Time Limit	4 years
Delivery mode	In-class
Locations	Main Campus, Majmaah University
Language of instruction	English
Pre-Requisites	BS or BSc degree in Computing domain, such as CS, IT, IS, CE, or a related field (degree in other field is accepted only if candidate has either previous work experience or in-service training in IT, with)
Program Coordinator(s)	Dean of CCIS
Contact details for program information	Department of Information Technology, College of Computer and Information Science

Program Overview

Computers are central to all aspects of our daily lives; as industries ranging from communications to banking have come to rely on them, the need for improved computer security has never been greater. This Program focuses on two aspects, Cybersecurity and Digital Forensics.

Students joining the Program will gain an understanding of the nature of the security threats that face computer systems and the type of information that is stored on digital devices (and how it can be extracted from them). They will benefit from a broad and varied array of state-of-the-art tools and technologies.

In the MS in Cybersecurity and digital forensics at CCIS, MU student can gain the capability to help organizations and law enforcement detect data breaches, cyber-attacks, and digital crime. Learn how to determine whether a digital system has been attacked or compromised as well as how to uncover, preserve, and present evidence for legal prosecution.

Coursework in the Cybersecurity and digital forensics master's degree can help student gain the technical competencies and knowledge needed to investigate system security breaches and recover lost or compromised data. Our curriculum features hands-on learning experiences that use the same evidence and scenarios encountered in real-world investigations.

Program Description

The Master's degree of Cybersecurity and Digital Forensics (CSDF) is a postgraduate award offered by the CCIS at Majmaah University. It is designed for postgraduate scholars and professional managers with appropriate undergraduate qualifications in IT, computer science, electrical, computer or systems engineering or a related discipline and/or extensive relevant professional experience who wish to gain a more detailed understanding of the technical skills and expertise relevant to the technical implementation and leadership of the Cybersecurity and Digital Forensics function.

The MS in CSDF program offers a balance of practice and theory through study in Information Technology, law and criminal justice. The goal is to produce professionals qualified as digital forensic scientists who can apply and sustain their expertise as new technological and societal challenges emerge, who understand the scientific, legal and criminal justice context of high technology crime, and who can effectively communicate their knowledge to others.

College Mission Statement

The mission of the College of Computer & Information Sciences is to provide distinguished educational programs based on latest developments in computer and

and to develop highly scientific and academic qualified graduates ,information sciences .and successful competitors in the labor market to contribute to the national development

Department Mission Statement

Prepare qualified national graduates with high skills and enough experience to join and engage into labor market of the different fields of Information Technology by providing and strong moral values to serve ,advanced skills ,the graduates with the latest knowledge the kingdom of Saudi Arabia

Program Educational Objectives (PEOs)

Program educational objectives define the characteristics of our graduates a few years after they have graduated and are employed or undertaking graduate studies .The program will produce graduates who :

1. Practice as computing professionals in areas of Cybersecurity and Digital Forensics with an appropriate combination of theoretical knowledge and hands-on skills.
2. Enhance their skills in wide aspects of the security of information systems and specialized skills in computer security incidents and crime evidence and master new computing technologies through self-directed professional development or conduct research in Cybersecurity and Digital Forensics field.
3. Follow a career path toward leading positions in the Cybersecurity and Digital Forensics field.

Student Outcomes (SOs)

The program has documented measurable outcomes that are based on the needs of the program's constituencies .The program enables students to achieve ,by the time of graduation:

a) An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline
b) An ability to analyze a problem ,and identify and define the computing requirements appropriate to its solution
c) An ability to design ,implement ,and evaluate a computer-based system ,process , component ,or program to meet desired needs
d) An ability to function effectively on teams to accomplish a common goal
e) An understanding of professional ,ethical ,legal ,security and social issues and responsibilities
f) An ability to communicate effectively with a range of audiences
g) An ability to analyze the local and global impact of computing on individuals , organizations ,and society

h) Recognition of the need for and an ability to engage in continuing professional development
i) An ability to use current techniques ,skills ,and tools necessary for computing practice.
j) An ability to use and apply current technical concepts and practices in the core information technologies .
k) An ability to identify and analyze user needs and take them into account in the selection ,creation ,evaluation and administration of computer-based systems .
l) An ability to effectively integrate IT-based solutions into the user environment .
m) An understanding of best practices and standards and their application .
n) An ability to assist in the creation of an effective project plan .

Needs for the MS in Cybersecurity and Digital Forensics (CSDF) program degree in KSA:

As Cybercrime continues to escalate, **corporations, government agencies and organizations** are seeking Cybersecurity experts to develop innovative tools and techniques to safeguard information, information systems and infrastructures, and to respond to computer security breaches and attack.

The need for Cybersecurity experts spans all industries, from **financial services, manufacturing and utilities to healthcare and retail.**

Cybersecurity jobs also are plentiful in the KSA government market. The Statistics predicts that careers in Cybersecurity and digital forensics will grow at least 30 percent by 2018.

Some of Careers in this field include:

1. Information Security Crime Investigator/Forensics Expert
2. System, Network, and/or Web Penetration Tester
3. Security Architect / Security Analyst
4. Application Penetration Tester and Incident Responder
5. Software / Application Development Security
6. Disaster Recovery/Business Continuity Analyst/Manager

Program Specific Requirements

Students requirements

1. BS or BSc degree in Computing domain, such as CS, IT, IS, CE, or a related field (degree in other field is accepted only if candidate has either previous work experience or in-service training in IT, with coordinator's approval)
2. Grade-Point average (GPA) of at least 3.50 on a scale of 5.00 or equivalent.

3. Proof of English, Completion of TOEFL with minimum Score of 520 (PBT), 190 (CPT), or 68 (IBT)
4. At least two letters of Recommendations.
5. One motivation letter

Prerequisite courses:

BS or BSc degrees in other related fields will be accepted if the candidate has the required academic background (foundation of Computer Science or IT). Otherwise students must take the following foundation courses in Computer Science or IT before starting the MS in CSDF.

Students complete the following five courses:

1. Computer Programming (such as C++, Java, etc.)
2. Data Structure
3. Operating System
4. Database System
5. Data Communications and Networking

Program Contents

All students will take the modules which are designed to give a comprehensive introduction to this specialist field. They will cover basic digital forensics and security. Dealing with digital evidence in a professional manner (that includes adhering to appropriate legal guidelines) is also covered.

The course offers the opportunity to examine a variety of tools available on the open market, and the use of forensic tools to retrieve data from electronic sources. It will also consider the analysis of professional and ethical issues relating to computer security and forensics, and the development of professional competencies, such as report writing and presenting evidence in court.

Curriculum

The program adopts a practical approach, which sees students undertake a research project and get many hands-on labs experience. The curriculum primarily covers key areas from Cybersecurity and Digital Forensics domains, such as (but not limited to)

Cybersecurity

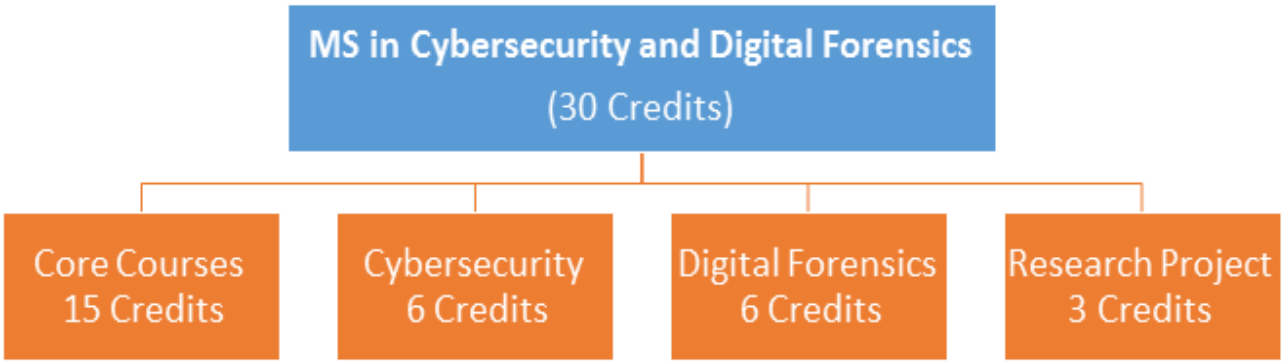
1. Information & Network Security
2. Web, Software, Mobile, Hardware, Data, People, etc. Security
3. Cybersecurity Governance & Management

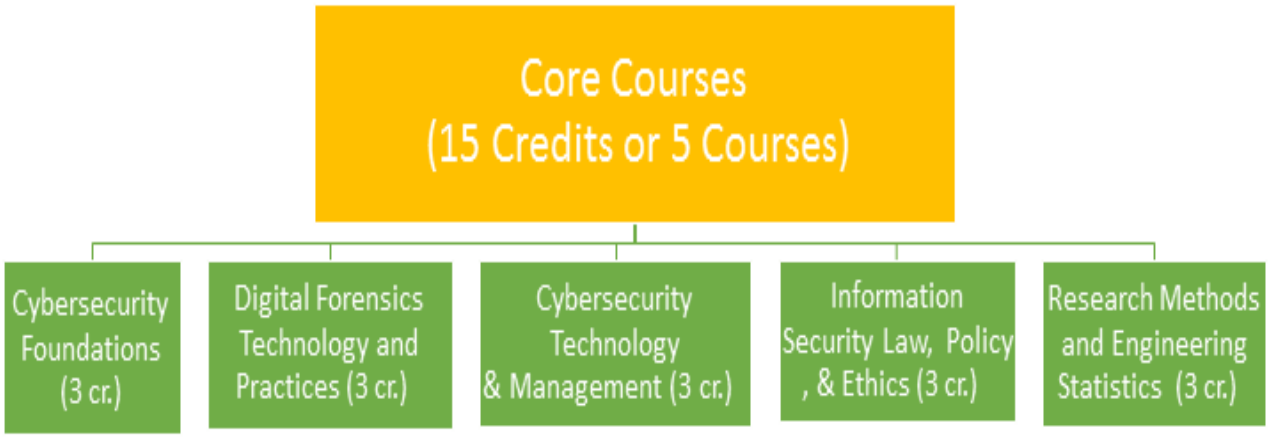
4. Cybercrime & Response
5. Cyber Law, Compliance & Ethics
6. Ethical Hacking and Penetration Testing

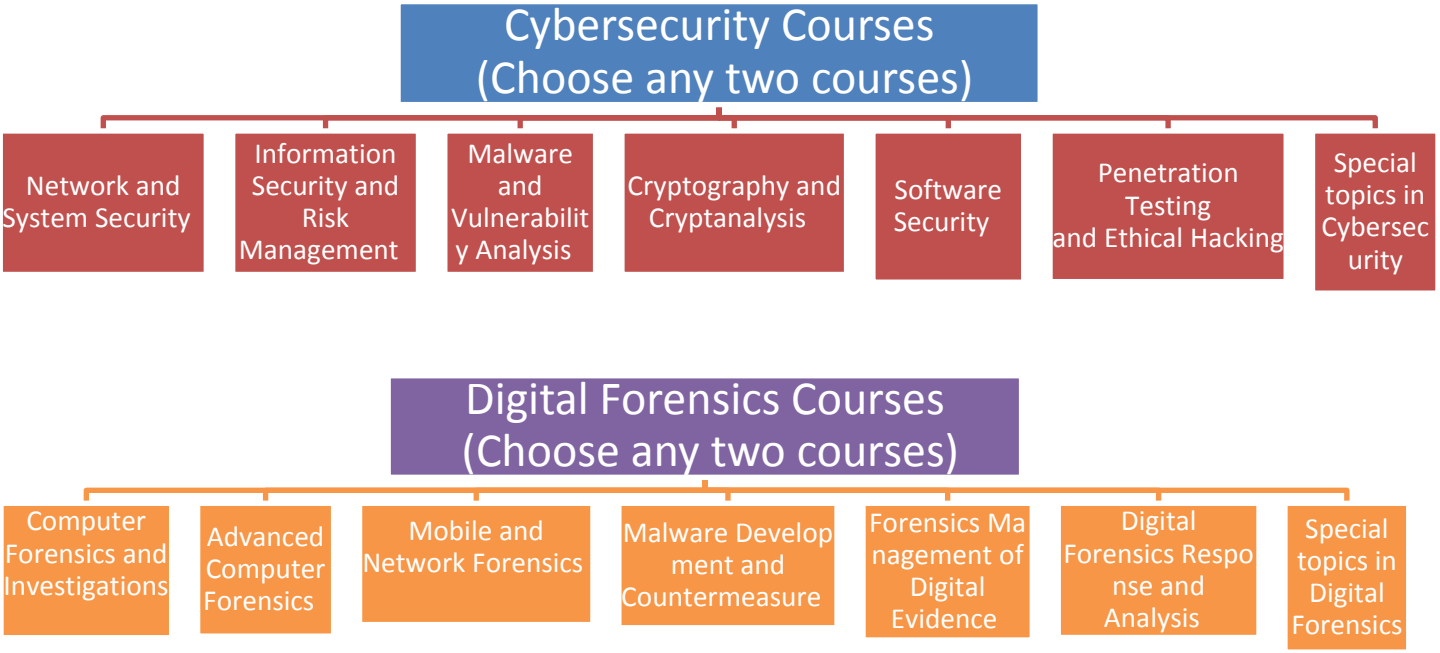
Digital forensics

1. File Systems, Disks, Devices, Data, Hardware, OS, etc. Forensics
2. Network and Mobile Forensics
3. Forensic data analysis and Investigation
4. Evidence collection, processing, analysing, and reporting
5. Malware development and countermeasures

The MS in CSDF degree is comprised of 30 credits hours of graduate study which include 15 credits core courses, six credits from Cybersecurity or related domains, six credits from digital forensics or related domains, and three credits Research Project.







Core Courses (15 credits)

Students study five Core Courses (15 credits) for the MS in CSDF degree program. These courses are mandatory for students. Students would require to pass a comprehensive exam based on these course contents to earn their MS degree. Core courses focuses on Cybersecurity and Digital Forensics' foundation, Laws, Policies, Ethics, Available Tools & Technology as well as some basic research practices and statistics. Students will require to **study the following five core courses**.

1. Cybersecurity Foundations ..... (3cr)
2. Digital Forensics Technology and Practices ..... (3cr)
3. Cybersecurity Technology and Management ..... (3cr)
4. Information Security Law, Policy, and Ethics..... (3cr)
5. Research Methods and Engineering Statistics .....(3cr)

Group A (6 credits):

The MS in CSDF program will offer several courses in the Cybersecurity and related domains. Students will choose two courses from the Cybersecurity domain. Cybersecurity domain will primarily focus on Cybercrime & Response, Security Threats and Defences, Risk Management, and so on.

Cybersecurity Courses (Students choose two courses)

1. Network and System Security ……..(3cr)
2. Malware and Vulnerability Analysis ……..(3cr)
3. Cryptography and Cryptanalysis ……..(3cr)
4. Software Security ……(3cr)
5. Penetration Testing and Ethical Hacking ……(3cr)
6. Special Topics in Cybersecurity ……..(3cr)

Group B (6 credits):

The MS in CSDF program will offer several courses in the Digital Forensics and related domains. Students will choose two courses from the Digital Forensics domain below.

Digital Forensics Courses (Students choose two courses)

1. Computer Forensics and Investigations …….. (3cr)
2. Advanced Computer Forensics ……...(3cr)
3. Mobile and Network Forensics .....(3cr)
4. Malware Development and Countermeasure .....(3cr)
5. Forensics Management of Digital Evidence ……(3cr)
6. Digital Forensics Response and Analysis .....(3cr)
7. Special Topics in Digital Forensics …….. (3cr)

Research Project (3 credits):
College of Computer and Information Science (**CCIS**), *Majmaah University* program offers an innovative learning experience where students work on innovative projects. Student projects are mentored by CCIS faculty who guide the progress and ensure that in addition to learning it, students can do it.

The MS in CSDF program students will choose the graduate research project option. Students will conduct research under a supervisor and submit a graduate research paper. Student will need to complete a graduate research project (e.g. Development a InfoSec Tool, Conduct a comparison study using tools, etc.) worth three credit hours and deliver the final product. With the appropriate permission, Program Chair, students may substitute their graduate research project with relevant Capstone project or real-world industry project.

Projects are not only a great learning experience, but they also help in job interviews. By the time our students graduate, they can share with interviewers their participation in several successful projects which can help them get the job and be prepared to become innovators, entrepreneurs, and leaders of the future.

Proposed Course Plan (Time-line, Two Years):

Semester 1			
Code	Course	Cr.	P.R
IT 601	Cybersecurity Foundations	3(2, 0, 2)	N/A
IT 602	Digital Forensics Technology and Practices	3(2, 0 ,2)	N/A

IT 603	Information Security Law, Policy, and Ethics	3 (3, 0, 0)	N/A
	Total Semester Credits	**9**	

Semester 2			
Code	Course	Cr.	P. R
IT 604	Cybersecurity Technology and Management	3 (3, 0, 0)	N/A
IT 6XX	Elective- Group A	3(3, 0, 0)	IT 601
IT 6XX	Elective- Group B	3(3, 0, 0)	IT 602
	Total Semester Credits	**9**	

Semester 3			
Code	Course	Cr.	P.R
IT 605	Research Methods and Engineering Statistics	3 (3, 0, 0)	IT 604
IT 6XX	Elective- Group A	3(3, 0, 0)	N/A
IT 6XX	Elective- Group B	3(3, 0, 0)	N/A
	Total Semester Credits	**9**	

Semester 4			
Code	Course	Cr.	P. R
IT 650	Research Project	3(0, 0, 6)	IT 605
	Total Semester Credits	**3**	

Course Descriptions

Core Courses

1. **IT 601 Cybersecurity Foundations**

This course provides fundamental overview of Cybersecurity and lays a foundation for subsequent topical courses in the area of Cybersecurity systems Topics covered include: Cyber Security Fundamentals, Microsoft Windows Security Principles, Attacker Techniques, Exploit Tools, Self-Replicating Malicious Code, Evading Detection, Virtual Machine Detection, Stealing Information, Exploitation and Defense and Analysis Techniques, Memory Forensics, Intrusion Detection System.

2. **IT 602 Digital Forensics Technology and Practices**

This course provides overview of digital forensic. Topics covered includes, introduction to digital forensic, digital forensic process, digital forensic tools, investigative

methodology ,current techniques and tools for forensic examinations & Analysis ,Digital investigations, Electronic Discovery ,Intrusion Investigation , Anti-forensics, Windows Forensic Analysis ,Embedded Systems Analysis &Network Evidence and Investigations.

3. IT 603 Information Security Law, Policy, and Ethics

This course provides in depth analysis of information security laws in many jurisdictions, and needs to understand the overall framework of legal security requirements, so it can evaluate how local law fits in, and what it might do to become generally legally compliant in many jurisdictions and under many laws. This course also provides an concise overview of the traditional ethical frameworks that can guide our analysis of the moral dilemmas and social problems that rise in cyberspace. Discussions on Saudi securities laws are also appended.

4. IT 604 Cybersecurity Technology and Management

This course provides issues in cyber security technology and practice. This course explores practical solutions to a wide range of cyber-physical and IT infrastructure protection issues. This course also aims at managing the cyber-attacks on the critical IT infrastructure computer networks.

5. IT 605 Research Methods and Engineering Statistics

Studying of the research methods and processes applicable to engineering/technology to emphasis on defining research problems, collecting, analysing, recording, and interpreting data. Students should learn number of academic research methods. Students will be required to conduct a research project.

Group A: Cybersecurity Courses (Students choose two courses, one in Semester II and one in Semester III)

1. IT 611: Network and System Security

This course includes basic concepts of network and system security, with an emphasis on the threats and countermeasures relevant to computer programs and Internet applications. Students will be prepared to evaluate the security of real network systems, and to develop strategies to detect and defend against attacks. In additional to the traditional security technologies, this course will also include discussions on problems of current research in network and system security.

2. IT 612: Malware and Vulnerability Analysis

This Course provides important aspects of malicious codes and the technical skills required to identify, analyse, and exploit software vulnerabilities, focusing on application-level issues which includes Code auditing, reversing, memory corruption, fuzzing, Post-Exploitation, Webapp Hacking, Reversing, Reverse Engineering, Client-side attacks and Web Hacking on android and smart devices. This will form the basis of a

methodological approach for identifying and analyzing software vulnerabilities and to design secure systems and defend against intrusion.

3. IT 613: Cryptography and Cryptanalysis

This course provides fundamental overview of Cryptography & cryptanalysis and lays a foundation for subsequent topical courses in the area of Computer Security. Topics covered include; Security Concepts, Attacks, Block Ciphers, Block Cipher Operation, Cryptanalysis, Number Theory, Public-Key Cryptography, Factoring and Discrete Algorithms, Linear Cryptanalysis. &Differential Cryptanalysis, Cryptographic Hash and MAC Functions, User Authentication Protocols.

4. IT 614: Software Security

This course will provide students to understand the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis. Students will study, in-depth, vulnerability classes to understand how to protect software and how to develop secure software. This course will also cover various analysis and design techniques for improving software security. We will also discuss the technical trends affecting software security.

5. IT 615: Penetration Testing and Ethical Hacking

Students will learn the ethical hacking techniques commonly used to breech and exploit corporate networks and can identify how and when they are used. This course enables students to uncover vulnerabilities in operating systems, applications and IT networks and provides advice in applying appropriate countermeasures. This course teaches penetration testing techniques that quickly, efficiently and most importantly methodically uncover vulnerabilities in operating systems, applications and networks. Students will learn core skills and techniques that every pentester needs. Using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, they will run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite.

6. IT 616: Selected topics in cyber security

This course will focus on future trends in technology in the field of cyber security; as well discuss contemporary Cybersecurity policy problems, economy and politics, and how those are affecting Cybersecurity policy. Topics may include Routing security and next-generation Internet, Privacy and Anonymous communication: attacks and designs, Cloud security, End-to-end (E2E) security: practical attacks and defences etc.

Group B: Digital Forensics Courses (Students choose two courses, one in Semester II and one in Semester III)

1. **IT 621: Computer Forensics and Investigations**

This course gives students a solid foundation to the methods of computer forensics and investigations. It provides an in-depth knowledge of the criminal justice system, Computer hardware and software systems, investigative and evidence gathering protocols. The topics covered will enable the students to possess the knowledge, skills and experience to conduct complex, data-intensive forensic examinations involving various operating systems, platforms and file types.

2. **IT 622: Advanced Computer Forensics**

This course is designed as an advanced course in computer forensics, focusing on Windows systems. It is estimated that Windows comprises over 85% of the operating systems used worldwide. This course focuses on advanced topics in Windows operating system analysis, including advanced file system analysis, web and email, as well as a comprehensive final case involving a moot court exercise.

3. **IT 623: Mobile and Network Forensics**

This course aims to provide mobile and network forensic investigations that are legal, ethical, and highly effective using the detailed information contained in this practical guide. This course will explain the latest tools and methods along with features, examples, and real-world case studies. Students will find out how to assemble a mobile and network forensics lab, collect prosecutable evidence, uncover hidden files, and lock down the chain of custody. This comprehensive resource shows not only how to collect and analyze mobile device and network data but also how to accurately document your investigations to deliver court-ready documents.

4. **IT 624: Malware Development and Countermeasure**

This course aims to provide malware development strategies such as delivery mechanisms, self-protection and malicious framework engagement. In addition to these this course also provides defense strategies against malware development such as threat modelling, static application security testing, Dynamic application security testing and benefits of the 360 approach.

5. **IT 625: Forensics Management of Digital Evidence**

This course covers digital evidence as it applies to any crime and its management. It includes forensic examination methods of computer components and computer networks within the legal framework. It covers wide ranging topics such as legal issues relating to digital evidence and computer crime, language of computer crime investigation, court room dealings of digital evidence and forensic examinations.

6. **IT 626: Digital Forensics Response and Analysis**

This course deals with computer investigation and forensic analysis techniques in the interests of determining potential legal evidence in cybercrime situations. It covers

significant topics related to identification, collection, preservation, and analysis of computer evidence such as the incident response process, data collection in Windows/Unix based system, data analysis techniques and preparation of forensic analysis reports.

7. **IT 627: Special Topics Digital Forensics**

This course will focus on future trends in technology in the field of Digital Forensics and current forensic research directions and argues that to move forward the community needs to adopt standardized, modular approaches for data representation and forensic processing; Topics may include Semantic based DNS forensics, Information Forensics and Security, Deniable Encryption ,Sequence detection of overlapping latent fingerprints etc.

Program Lab Descriptions

IT 601: Cyber Security Foundation

In the lab students are;

1. Solve Problems with Window Messages and Create the Process Object
2. Implement Tunnelling Techniques
3. implement SQL Injection
4. Design, implement and evaluate Malicious Code Analysis Systems

IT 602: Digital Forensics Technology & Practices

In the lab students are;

1. Analyze computer evidence including audio & video evidences
2. Investigate digital evidence in a Windows and Linux environment.
3. Investigate Network Evidence

Textbook and References

Core Courses

1. IT 601 Cybersecurity Foundations

Reference 's Name	Author	Publisher	Publication year
Essentials of Cyber Security Paperback ISBN-13: 978-0692218006	Dr Gurpreet S Dhillon		2014
Cyber Security Essentials ISBN-13: 978-	James Graham Richard Howard Ryan Olson	Auerbach	2010

1439851234			
Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives ISBN-13: 978-8126521791	Nina Godbole and Sunit Belpure	Wiley	2011

2. IT 602 Digital Forensics Technology and Practices

Reference 's Name	Author	Publisher	Publication year
1.The Basics of Digital Forensics, ISBN-13: 978-0128016350	John Sammons	Syngress	2014
2.Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, , , ISBN 9780123742681	Eoghan Casey	Academic Press	2011
3.Handbook of Computer Crime Investigation: Forensic Tools and Technology, ISBN: 0121631036,.	Eoghan Casey	Butterworth Heinemann	2002

3. IT 603 Information Security Law, Policy, and Ethics

Reference 's Name	Author	Publisher	Publication year
Information Security Law: The Emerging Standard for Corporate Compliance · ISBN-10: 1905356668	Thomas J. Smedinghoff	IT Governance Publshing	2016

Cyberethics: Morality and Law in Cyberspace ISBN-10: 1284081397	Richard Spinello	Jones & Bartlett Learning	2016
Saudi Securities Law ISBN-10: 0615431704	Michael O'Kane	Al-Andalus Publishing	2015

4. IT 604 Cybersecurity Technology and Management

Reference 's Name	Author	Publisher	Publication year
Cyber Security and IT infrastructure protections · ISBN-10: 0124166814	John Vacca	Syngress, First Edition	2013

5. IT 605 Research Methods and Engineering Statistics

Reference 's Name	Author	Publisher	Publication year
Research Methods for Engineers ISBN-10: 1107610192	David V. Thiel	Cambridge University Press	2014
Research Methods for Postgraduates ISBN-10: 1118341465	Tony Greenfield	Wiley	2016

Group A: Cybersecurity Courses (Students choose two courses, one in Semester II and one in Semester III)

1. IT 611: Network and System Security

Reference 's Name	Author	Publisher	Publication year
Hacking – The art of exploitation (2nd edition)	Jon Erickson	O Reilly Media	2017

Secure Programming with Static Analysis.	Brian Chess and Jacob west	Pearson	2016

2. IT 612: Malware and Vulnerability Analysis

Reference 's Name	Author	Publisher	Publication year
Android Security: A Survey of Issues, Malware Penetration and Defenses	ParvezFaruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur	IEEE Communications Surveys & Tutorials PP(99):29 · December 2014	2014
Evolution, Detection and Analysis of Malware for Smart Devices	Guillermo Suarez-Tangil, Juan E. Tapiador, Pedro Peris-Lopez, and Arturo Ribagorda	IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 2, SECOND QUARTER 2014 961	2014

3. IT 613: Cryptography and Cryptanalysis

Reference 's Name	Author	Publisher	Publication year
Modern Cryptography: Applied Mathematics for Encryption and Information Security (Networking & Communication - OMG) , ISBN-13: 978-1259588082,	Chuck Easttom	McGraw-Hill Education	2015
Modern Cryptanalysis: Techniques for Advanced Code Breaking ISBN: 978-0-470-13593-8,	Christopher Swenson	WILEY	2008
Cryptography and Network Security: Principles and Practice (7th	William Stallings	Prentice Hall	2014

Edition) ISBN-13: 978-0134444284, 2016			

4. IT 614: Software Security

Reference 's Name	Author	Publisher	Publication year
Cyber Security Engineering: A Practical Approach for Systems and Software Assurance (SEI Series in Software Engineering) 1st Edition	Nancy R. Mead and Carol Woody	Addison-Wesley Professional	2017
Principles of Computer Security, Fourth Edition	Wm. Arthur Conklin and at el.	McGraw-Hill Education	2015
Computer Security: Art and Science (2 Volume Set) 1st Edition	Matt Bishop	Addison-Wesley Professional	2015
Core Software Security: Security at the Source 1st Edition	James Ransome and Anmol Misra	Auerbach Publications	2013
Fundamentals of Information Systems Security, 2nd Edition	David Kim and Michael G. Solomon	Jones & Bartlett Learning	2014

5. IT 615: Penetration Testing and Ethical Hacking

Reference 's Name	Author	Publisher	Publication year
Advanced Penetration Testing: Hacking the World's Most Secure Networks, 1st Edition	Wil Allsopp	Wiley	2017
CEH v9: Certified Ethical Hacker Version 9 Study Guide 3rd Edition	Oriyano	Sybex	2016

Penetration Testing: A Hands-On Introduction to Hacking 1st Edition	Georgia Weidman	No Starch Press	2014

6. IT 616: Special Topics in Cyber security

Group B: Digital Forensics Courses (Students choose two courses, one in Semester II and one in Semester III)

1. IT 621: Computer Forensics and Investigations

Reference 's Name	Author	Publisher	Publication year
Guide to Computer Forensics and Investigations	Bill Nelson , Amelia Phillips, Christopher Steuart	Cengage Learning, 4th Edition	2010
Handbook of Digital Forensics and Investigation	Eoghan Casey	Elsevier Academic Press	2010

2. IT 622: Advanced Computer Forensics

Reference 's Name	Author	Publisher	Publication year
Windows Forensic Analysis, DVD Toolkit	Harlan Carvey Harlan Carvey	Elsevier	2012
UNIX and Linux Forensic Analysis DVD Toolkit	Chris Pogue Cory Altheide Todd Haverkos	Elsevier	2008

3. IT 623: Mobile and Network Forensics

Reference 's Name	Author	Publisher	Publication year
Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation (required)	Lee Reiber	McGraw-Hill Education	2016
Network Forensics(required)	Ric Messier	Wiley	2017
Computer Forensics: Investigating Network Intrusions and Cybercrime	EC-Council	Course Technology	2016

(CHFI), 2nd Edition (optional)			
Practical Mobile Forensics - Second Edition (optional)	Heather Mahalik, Rohit Tamma and Satish Bommisetty	Packt Publishing	2016

4. IT 624: Malware Development and Countermeasure

Reference ‘s Name	Author	Publisher	Publication year
Managed code rootkits: hooking into Runtime Environments	Erez Metula	Elsevier	2011

5. IT 625: Forensics Management of Digital Evidence

Reference 's Name	Author	Publisher	Publication year
Digital Evidence and Computer Crime – Forensic Science, Computers and Internet	Eoghan Casey	Elsevier, 3rd Edition	2011
Computer Forensics: Evidence Collection and Management	Robert C. Newman	Auerbach Publications	2007

6. IT 626: Digital Forensics Response and Analysis

Reference 's Name	Author	Publisher	Publication year
Incident response and Computer Forensics	Jason Luttgens, Matthew Pepe and Kevin Mandia	McGrawHill, Third Edition	2014
File System Forensic Analysis	Brian Carrier	Addison Wesley Professional (Pearson ed)	2005

7. IT 627: Special Topics Digital Forensics