Course Code:	DFxxxxx
Course Name:	DIGITAL FORENSIC INVESTIGATION
Course Credit:	Three (3) Units
Course Prerequisites:	(---)
Objectives:	General

Gain knowledge and skills that are required to effectively carry out digital forensic investigation and examination by understanding the fundamentals of computing, cybersecurity and issues, setting up of laboratory and toolkit, ability to navigate and identify multitude of equipment and applications presented and utilized, analysis of gathered data and its presentation to concerned stakeholders.

Specific

Cognitive
At the end of the term, participants should be able to:

- Understand the general idea and concepts about forensic and scientific discovery and link as well as apply them to computer forensic effort
- Effectively distinguish digital forensic and computer security requirements and how the latter can be used to operate and/or handle investigation
- Learn how to effect skills based on need and of sound forensic investigation and examination

Psychomotor
At the end of the course, the student will be able to:

- Develop and/or customize toolkit necessary in responding computer incidents and forensic investigation
- Apply knowledge and skills in conjunction with digital forensic requirements including working out which technology might be effective to fulfill a purpose, function as well as organizational policies and rule of law
- Establish sound forensic laboratory
- Prepare forensically sound report for stakeholders including but not limited to the court of law

COURSE OUTLINE

Week 1
Specific Objective/s

- Refresh if not introduce participants to the required computing and technological knowledge in preparation to the digital forensic course.

Module 1	House rules and course introduction
Module 2	Brief review and prerequisites: Fundamentals and principles of computer and internetworking
Module 3	Basic Input Output System (BIOS)
Module 4	Typical idea in computer security
Module 5	Computer storage interface and controllers
Module 6	Small computer systems interface (SCSI)

Week 2
Specific Objectives

- Emphasize the importance of understanding and practical usage of storage controllers and interfaces.
- Discuss the possibilities of security incidents, why and how it happened and what must be done to preserve the integrity of security mechanism—associating to the need of digital forensics.

Module 7	ATA and SCSI comparison
Module 8	Hard disk drive
Module 9	Direct memory access
Module 10	File systems management
Module 11	Occurrences of security incidents
Module 12	Verity of security

Week 3
Specific Objectives

- Introduce basic definitions and principles of forensic practice in general, what may be required in the conduct of investigation and how it is relevant and its applicability to digital forensics.
- Explore what can be pursued through digital forensic efforts as against cyber crimes.

Module 13	Forensic basic definitions and principles
Module 14	Investigation comprises Laboratory exercise: Data acquisition
Module 15	Containment of environment Laboratory exercise: Monitoring of events
Module 16	Basic of digital forensics
Module 17	Digital forensic history

Module 18 Cyber crime

Week 4
Specific Objectives

- Identify mechanism and technological requirements in setting up a sound forensic laboratory.
- Discuss how explicit equipment and toolkit are used to effectively assist in the achievement of digital forensic goal.

Module 19	Computer forensic laboratory Laboratory exercise: Computer and network attacks
Module 20	Computing forensic processes
Module 21	Evidence handling Laboratory exercise: Identification and numbering of evidences and toolkit
Module 22	Network computers
Module 23	Equipment preparation
Module 24	Forensic analysis and examination

Week 5
Specific Objectives

- Demonstrate how variant of advance technologies are use to facilitate crime and how to counter it with forensic investigation and analysis.
- Recall information management principles and standards and link their relevance to the techniques used in digital forensics.
- Discuss the significance of using industry standards and practices and how it can get along in the processing, assessing and presentation of evidence to stakeholders including the court of law.

Module 25	Forensic of non-tradition computer technologies
Module 26	Information management
Module 27	Processing, review and analysis
Module 28	Presentation Laboratory exercise: Evidence presentation
Module 29	EDRM standards
Module 30	Early data assessment

Week 6
Specific Objectives

- Discuss about acceptable processes in evidence collection as well as archiving.
- Echo the imperativeness of investigator's qualification.
- Emphasize acceptable practices, especially in court of law, the labeling of toolkit and evidences.

Module 31 Best practice management summary

Module 32	Evidence collection and archiving Laboratory exercise: Customization and application of independent utility to collect and archive evidence
Module 33	Computer evidences
Module 34	Qualification of investigator
Module 35	Volatile data retrieval
Module 36	Labeling toolkit media

Week 7
Specific Objectives

- Identify why it is necessary to take on computer incidents right away and what can be gathered by doing so.
- Discuss volatile data which can serve a very important piece of the puzzle and of the evidence collection process.
- Introduce advance technologies can be a source of cyber crime and is necessary to understand each of their capacity.

Module 37	Live response Laboratory exercise: Volatile data retrieval and live response
Module 38	Collecting and analyzing volatile RAM Laboratory exercise: Volatile data retrieval and live response continuation
Module 39	Live response methodologies
Module 40	Investigative uses of advance technology
Module 41	Investigative uses of advance technology continuation
Module 42	Investigation and analysis. Platform-based

Week 8
Specific Objectives

- Understand platforms' file systems and what can be dealt with it especially during data acquisition, analysis and examination of evidence.

Module 43	Examination of Windows file systems Laboratory exercises: Examination of Windows file systems
Module 44	Examination of Windows file systems continuation
Module 45	Windows New Technology File Systems (NTFS)
Module 46	NTFS on-disk file format
Module 47	Master file table
Module 48	Alternate data streams

Week 9
Specific Objectives

- Learn how processes and content from volatile devices can assist in the pursuit of computer crime and what to do with them to further the investigation effort.

Module 49	Windows process memory

Module 50	Alternative approaches to dumping RAM content Laboratory exercise: Dumping volatile RAM content or recovering data from blue screen of death
Module 51	Windows registry
Module 52	Registry evidence
Module 53	Local Security Authority (LSA)
Module 54	Unix-like file systems

Week 10
Specific Objectives

- Understand the differences and capabilities of various file systems existed or used in a number of platforms or operating systems.
- Introduce how next generation file system(s) can affect hard disk drive format and its effect to master boot records of each of the different operating systems.

Module 55	Unix-like file system group descriptors
Module 56	ext2
Module 57	ext3/4
Module 58	stat
Module 59	Macintosh file system
Module 60	Macintosh forensic, GPT

Week 11
Specific Objectives

- Apply toolkit in data acquisition and analysis of forensically sound evidence.

Module 61	Macintosh HFS internals
Module 62	Macintosh HFS internals and B*tree
Module 63	Hard disk drive forensics Laboratory exercise: Byte-by-byte data acquisition, image and noncompressed
Module 64	Digital and optical media
Module 65	Bootstrap process evolution
Module 66	Boot sector

Week 12
Specific Objectives

- Identify the different application of boot processes and their requirements to deal with each effectively.
- Recall what is being generated when browsing the Internet and visiting various websites.
- Learn what has been very interesting with smartphones not only how consumers love their functionalities but how security and forensic practitioners and intruders—exploiting—are doing to take advantage of their capabilities.

Module 67	Volume boot record
Module 68	GUID Partition Table (GPT)

Module 69	Windows 8 and Unix-like boot processes
Module 70	Laboratory exercise: Identification of boot processes and collection of available data
Module 71	Investigation and analysis. Application-based
Module 72	Smartphone

Week 13
Specific Objectives

- Examine the acquisition of learning, the entire understanding of the subject and the ability to deliver effectively in incident response and forensic investigation and how they may assist law enforcement in replicating processes used in data acquisition and reconstructing of the crime scene, if any.

Module 73-75 Laboratory exercise: Computer and smartphone data acquisition
Module 76-78 Written and/or practical final examinations

Textbook:

Sources/references:

Books:
Operating Systems Concepts, Eight Edition
Computer Architecture
Hacking Expose Computer Forensics, Second Edition
Incident Response and Computer Forensics, Second Edition
Windows Forensic Analysis
iOS Forensic Analysis

Instruction Strategies:
Lectures and discussions, Hands-on exercises (individual), Group/team assignments and applications, Basic research, Written and practical examinations

Grading Systems:

Major examinations	30%
Quizzes	20%
Recitation	15%
Assignment	15%
Practical	10%
Regular class participation	10%
Total	**100%**
Passing mark	**70%**