Introduction to Computer Forensics and Security **6G7Z1009**

Lecturers

- Dr. Majdi Owda – 6 Weeks
  Room: E120
  Email: m.owda@mmu.ac.uk
  Phone: 0161 247 1520

- Dr. Liangxiu Han– 6 Weeks
  Email: l.han@mmu.ac.uk
  Phone: 0161 247 1521

Lectures and Labs

- Weekly 2 hours lecture and 4 hours lab
- Weekly exercises to complete

Assessment

- Assignments 50%
- Exam 50%

Prerequisite

- There are 10 groups of people those who can read binary and those who can’t.

Unit Overview

1. Forensic Process [10%]: Types of investigations, role of investigator, processes, and legal aspects.

2. File System Analysis [30%]: Data acquisition, volume analysis, write blockers, signatures, file systems artefacts, locating and restoring deleted content.

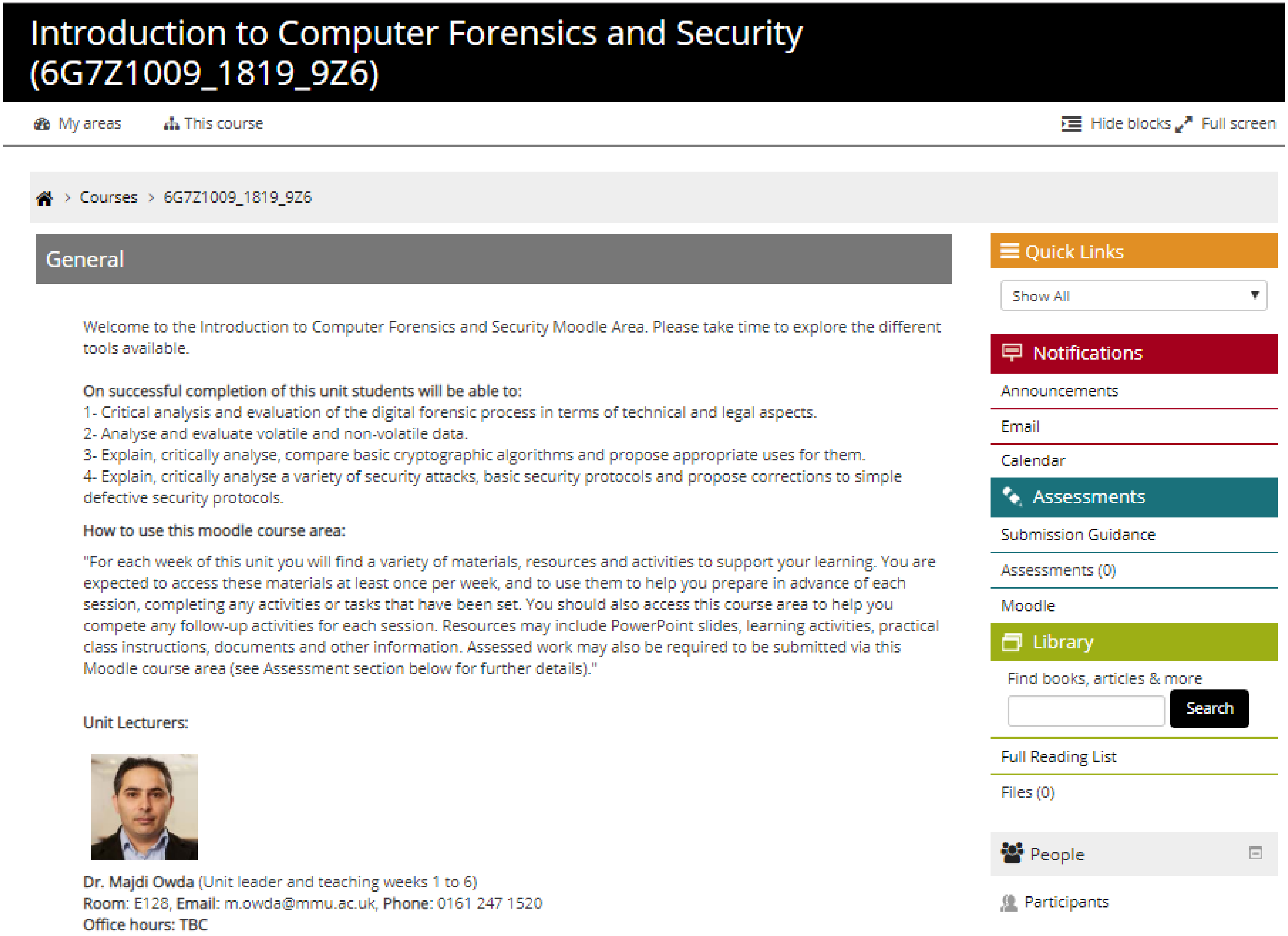
3. Recent Developments and Advances in Digital Forensics [10%]: Topics such as mobile forensics, memory forensics and forensic data mining.

4. Overview of security [15%]: The need for security; Types of security; Threats; Security mechanisms and security services.

5. Introduction to Cryptography [10%] : Attacks on conventional and public key cryptography; Integrity (hash functions and message authentication codes).

6. Access control [25%]: Goals of protocols (Authentication and Authorisation; Key distribution and confirmation); Fiat-Shamir protocol; PKI; Digital certificates; Mediated authentication (Needham-Schroeder protocol); Access control lists and capabilities; Multilevel Security; Multilateral Security; Covert channels; Kerberos.

Moodle – Materials



Introduction to Computer Forensics and Security (6G7Z1009_1819_9Z6)

General

Welcome to the Introduction to Computer Forensics and Security Moodle Area. Please take time to explore the different tools available.

On successful completion of this unit students will be able to:
1- Critical analysis and evaluation of the digital forensic process in terms of technical and legal aspects.
2- Analyse and evaluate volatile and non-volatile data.
3- Explain, critically analyse, compare basic cryptographic algorithms and propose appropriate uses for them.
4- Explain, critically analyse a variety of security attacks, basic security protocols and propose corrections to simple defective security protocols.

How to use this moodle course area:

"For each week of this unit you will find a variety of materials, resources and activities to support your learning. You are expected to access these materials at least once per week, and to use them to help you prepare in advance of each session, completing any activities or tasks that have been set. You should also access this course area to help you compete any follow-up activities for each session. Resources may include PowerPoint slides, learning activities, practical class instructions, documents and other information. Assessed work may also be required to be submitted via this Moodle course area (see Assessment section below for further details)."

Unit Lecturers:

Dr. Majdi Owda (Unit leader and teaching weeks 1 to 6)
Room: E128, **Email:** m.owda@mmu.ac.uk, **Phone:** 0161 247 1520
Office hours: TBC

What is Forensic Computing?

Forensic

Relating to the recovery, examination and/or production of evidence for legal purposes

Computing

Through the application of computer-based techniques

“The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable.”

Objectives

- Understand what constitutes a crime and identify categories of crime
- Understand law enforcement’s authority to investigate information warfare and terrorist threats to national security
- Identify what affects the admissibility of evidence
- Identify what computer forensics tools and techniques can reveal and recover
- Explain the process of discovery and electronic discovery

Introduction

Criminal investigations involve the analysis of ballistic or bloodstain patterns, gunpowder residue, tire tracks, fingerprints, or evidence left by electronic devices. E-evidence is the digital equivalent of the physical evidence found at crime scenes.

Introduction (Cont.)

- The expansion of the Internet provides countless opportunities for crimes to be committed
- Digital technologies record and document electronic trails of information that can be analyzed later
  - E-mail, instant messages (IM), Web site visits
  - PDAs, iPods, smart phones, cookies, log files etc.

Basics of Crimes

- Early cases that illustrate the importance of knowing the law regarding computer crimes
  - Robert T. Morris Jr. (Morris worm)
  - Onel De Guzman (Lovebug virus)
- Computer crimes can be prosecuted only if they violate existing laws

Morris Worm and Lovebug Virus

- Morris was charged with violation of the Computer Fraud and Abuse Act (CFAA)
- Morris sentenced to 3 years probation, 400 hours of community service, and a $10,500 fine
- Lovebug virus did $7 billion in damage in 2000
- De Guzman released because no law in the Philippines made what he had done a crime

Definition of Crime

- A *crime* is an offensive act against society that violates a law and is punishable by the government.
- Two important principles in this definition:
  - The act must violate at least one criminal law
  - It is the government (not the victim of the crime) that punishes the violator.

Crime Categories and Sentencing

- Crimes divided into two broad categories:
  - Felonies—serious crimes punishable by fine and more than one year in prison
  - Misdemeanors—lesser crimes punishable by fine and less than one year in prison
- Sentencing guidelines give directions for sentencing *defendants*

Cybercrime Categories

- The terms *computer crime*, *cybercrime*, *information crime*, and *high-tech crime* are used interchangeably.

- Two categories of offenses that involve computers:
  - Computer as target—computer or its data is the target of the crime.
  - Computer as instrument—computer is used to commit the crime.

Civil vs. Criminal Charges

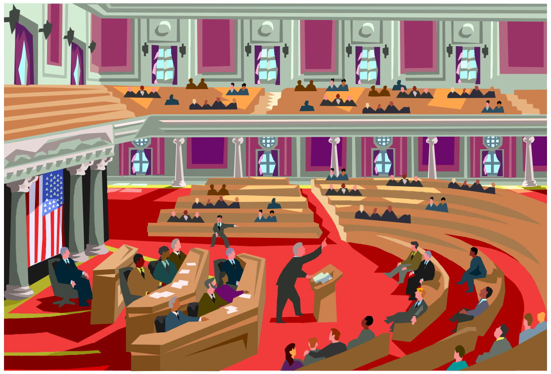
- Civil charges are brought by a person or company.
  - Parties must show proof they are entitled to evidence.
- Criminal charges can be brought only by the government.
  - Law enforcement agencies have authority to seize evidence.

In Practice: Distinction Between Criminal and Civil Cases

- Distinction between civil and criminal violation is not always clear
- In *Werner v. Lewis* case (Civil Court of N.Y. 1992)
  - Lewis inserted a time bomb (malicious computer program) into system (a crime)
  - Werner was awarded damages as in a civil suit

Information Warfare and Cyberterrorism

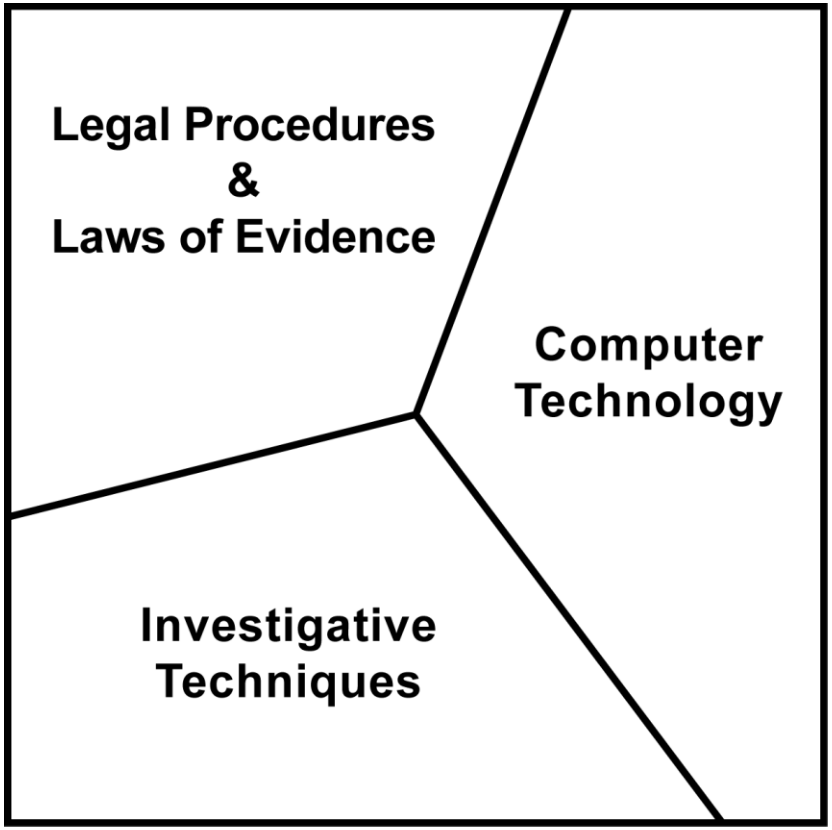
- Information warfare is the extension of war into and through cyberspace



Computer Forensics Skills

- An investigator's success depends on three skill sets.

- Value of recovered evidence depends on expertise in these areas.



Importance of Computer Forensics

- Computer forensics investigations supply evidence for:
  - Criminal cases such as homicide, financial fraud, drug and embezzlement crimes, and child pornography.
  - Civil cases such as fraud, divorce, discrimination, and harassment.
- Computer forensics also used to prevent, detect, and respond to cyber attacks.

Computer Forensics Can Reveal . . .

- Theft of intellectual property, trade secrets, confidential data.
- Defamatory or revealing statements in chat rooms, usenet groups, or IM.
- Sending of harassing, hateful, or other objectionable e-mail.
- Downloading of criminally pornographic material.
- Downloading or installation of unlicensed software.
- Online gambling, insider trading, solicitation, drug trafficking.
- Files accessed, altered, or saved

Computer Forensics Can Recover . . .

- Lost client records intentionally deleted by an employee.
- Proof that an ex-employee stole company trade secrets for use at a competitor.
- Proof of violations of noncompete agreements.
- Proof that a supplier's information security negligence caused costly mistakes
- Proof of a safer design of a defective item in a product liability suit.
- Earlier drafts of sensitive documents or altered spreadsheets to prove intent in a fraud claim.

The Main Point

- Remember

  An experienced forensic examiner once wrote:

  “ Computer Forensic Examiners may get a way without knowing all the legal nuances, but they need to know the principles behind maintaining a proper chain of custody – otherwise, their work product could become irrelevant if its custody is challenged during the litigation” Phil R.

Summary

- E-evidence plays an important role in crime reconstruction.
- Crimes are not limited to cybercrimes; cybertrails are left by many traditional crimes.
- Without evidence of an act or activity that violates a statute, there is no crime.
- Rules must be followed to gather, search for, and seize evidence in order to protect individual rights.

Summary (Cont.)

- Tools used to recover lost or destroyed data can also be used in e-discovery of evidence

Questions?

m.owda@mmu.ac.uk