Unit III

INTRODUCTION TO COMPUTER FORENSICS

Unit III - INTRODUCTION TO COMPUTER FORENSICS

- Introduction to Traditional Computer Crime
- Traditional problems associated with Computer Crime
- Introduction to Identity Theft & Identity Fraud
- Types of CF techniques
- Incident and incident response methodology
- Forensic duplication and investigation
- Preparation for IR: Creating response tool kit and IR team
- Forensics Technology and Systems
- Understanding Computer Investigation
- Data Acquisition

History

- The first recorded cyber crime took place in the year 1820
- The first spam email took place in 1978 when it was sent over the Arpanet
- The first VIRUS was installed on an Apple computer in 1982

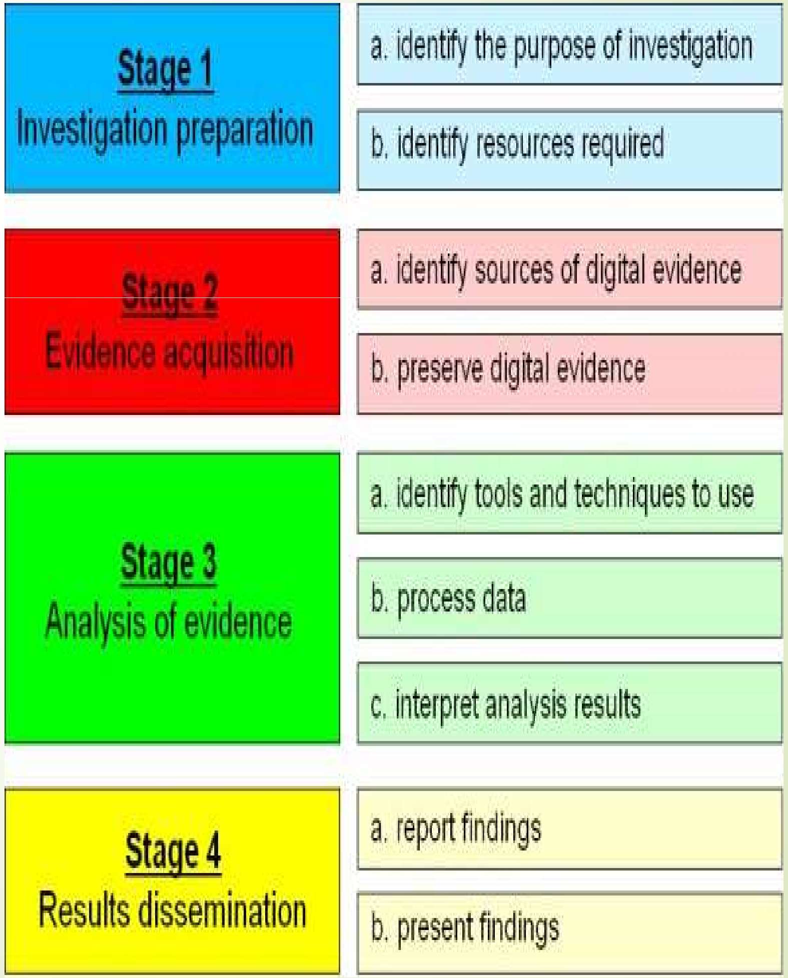
Computer forensics

- Computer forensics involves
  - obtaining and analyzing digital information
  - Preserving and documenting digital information
  - for use as evidence in civil, criminal, or administrative cases
- The goal is to
  - Do a structured investigation
  - Find out exactly what happened on a digital system
  - Who was responsible for it

Computer forensics

- Multiple methods
  - Discovering data on computer system
  - Recovering deleted, encrypted, or damaged file information
  - Monitoring live activity
  - Detecting violations of corporate policy

- CF steps



Stage 1
Investigation preparation

a. identify the purpose of investigation

b. identify resources required

Stage 2
Evidence acquisition

a. identify sources of digital evidence

b. preserve digital evidence

Stage 3
Analysis of evidence

a. identify tools and techniques to use

b. process data

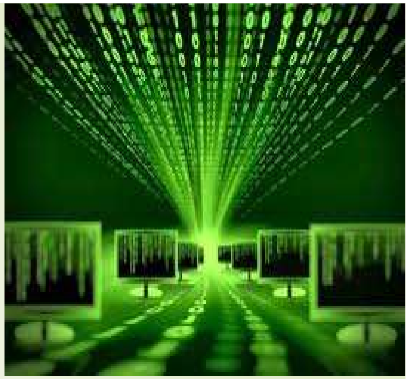
c. interpret analysis results

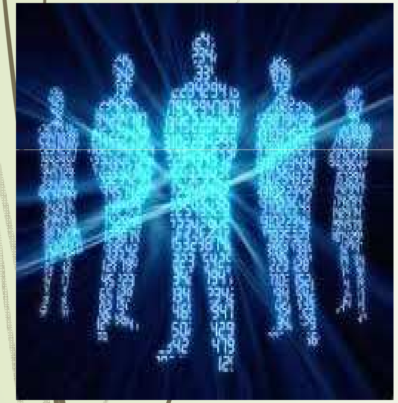
Stage 4
Results dissemination

a. report findings

b. present findings

Computer forensics





- Federal Rules of Evidence (FRE) has controlled the use of digital evidence since 1970
- The FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle the increasing number of cases involving digital evidence
- By the late 1990s, CART had teamed up with the Department of Defence Computer Forensics Laboratory (DCFL) for research and training

Introduction to traditional computer crime

Computer Crime

- Computer crime is any criminal offense, activity or issue that involves computers
- Computer misuse
  - Computer is used to commit a crime
  - Computer itself is a target of a crime (victim)
- Three general categories of computer crime
  - Target
  - Mean
  - Incidental
- Launched
  - Against Person
    - Harassment via emails, cyber stalking, email spoofing, carding,
  - Against Property
    - Trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information
  - Against Government
    - Cyber Terrorism, Damaging critical information infrastructures

Computer Crime

- Computer is used in illegal activities:
  - Child pornography, threatening letters, e-mail spam or harassment, extortion, fraud and theft of intellectual property, embezzlement
- All these crimes leave digital tracks
- Investigation into these types of crimes include
  - Searching computers that are suspected of being involved in illegal activities
  - Analysis of gigabytes of data looking for specific keywords
  - Examining log files to see what happened at certain times

Cyber Crime

- Crime committed using a computer and the internet
  - To steal a person's identity or illegal imports or malicious programs
- Computer used as an object or subject of crime

Cyber Criminals

- Person or Group who commits Cyber Crime using computers
  - Hackers, criminals groups, hacktivists, virus writers, terrorists
- Traditional criminals leave physical evidence like wise the technological counter part
- They hinder discovery (like mask, gloves)
- Investigators are not properly prepared to conceptualize similarity
- Often potentiality of criminals are overlooked

Traditional Problems

- Identification of actual location(Vicinage)
- Utilization of anonymizer
- Spoofing
- Encryption, steganography
- Rate of change in technology
- Jurisdictional disputes
- Lack of international guideline

Traditional Computer Crime

- Focuses on the areas of Computer crimes such as
  - Early hackers
  - Components of theft
- Focused on
  - The criminal behaviours
  - define who they are and how they are shaped

Traditional Computer Crime

- The things around us are developing faster and faster
  - Example
    - Flip phones to a touch phone
    - Back camera to a front camera
- Things that evolve around us develop every minute
- But in a way the new technology is a disadvantage because, more and more crimes are occurring

Traditional computer crime

- Pheakers
- Hacking
- Computer as commodities
- Theft of Intellectual Property

Traditional Computer Crime

- Phreaking
  - It involves the manipulation of telecommunication carriers to gain knowledge of telecommunications
  - Action of hacking through phone calls
  - The use of phreaking is illegal
  - Phreakers are the precursors of today's computer hackers
  - Phreakers would build "Bridges" illegal conference calls of numerous individuals around the world billed to someone else

Traditional Computer Crime

- Hacking
  - An illegal intrusion or unauthorized access to or control over a computer system and/or network
  - Use of computer to gain access to unauthorized data information
  - Computers are intended target of a criminal or may represent cybercrime in a form
  - Snooping neighbour computer to search top secret gov. database

Traditional Computer Crime

- Hacking
  - Contemporary Motivation
    - BORDEM - Informational Voyeurism
    - INTELLECTUAL CHALLENGE - Mining of Knowledge (Pure Hackers)
    - REVENGE- Insider, Employees
    - SEXUAL GRATIFICATION - Stalking, Harassment
    - ECONOMIC - Criminal
    - POLITICAL - Spies, Terrorist

Traditional Computer Crime

- Hacking
  - Hierarchy of Contemporary Cyber-Criminals
    - Script Kiddies
      - a person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own
    - Cyber Punks
      - Individuals intent on wreaking havoc via internet
    - Hacker/Crackers
      - Sophisticated computer criminals capable of writing code and breaching complex systems
      - Hackers has no economical motive
      - Crackers employ their knowledge for personal gain
    - Cyber Criminal organization
      - Group of criminal minded individual – use internet to communicate. Collaborate and facilitate cyber crime

USE PUBLICLY AVAILABLE ATTACK TOOLS MADE BY OTHERS
GET LABELED A 'SOPHISTICATED' THREAT

Traditional Computer Crime

- Piracy Identification
  - Counterfeit hologram
  - Absence of reserve label and polygraphic packing
  - Absence of Copyright and adjacent Rights protection sign
  - Anomalies in packaging material
  - Absence of high quality image on the CD

- Computer as commodities
  - Hardware theft
    - Quite popular as components are become smaller and more valuable
    - Felicitated by Black Market, Gray market, Internet based auction

- Theft of Intellectual Property
  - Software Piracy
    - Data piracy – reproduction, distribution and use of software without permission
    - Due to lack of knowledge regarding software licensing
    - Impossible to stop
    - One solution Shareware – pay on monthly basis and use
    - WareZ- Popular site to get software illegally

Traditional Computer Crime

- DOS (Denial of Service)
  - Act by the criminal
  - They floods the bandwidth of the victims network
  - Internet servers are flooded with continuous requests so as to crash the server
  - Its an attempt to make a machine or network resource unavailable to its intended users

Traditional Computer Crime

- Malicious software
  - Small piece of code that attaches itself to other software
    - Virus
    - Worms
    - Trojan Horse
    - Web jacking
    - E-mail bombing

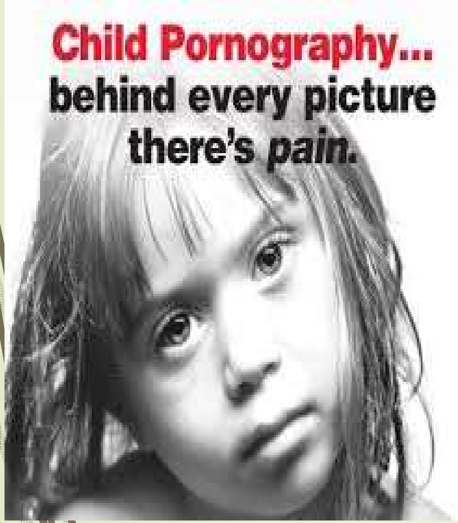
Traditional Computer Crime

- Computer Vandalism
  - Damaging or destroying data rather than stealing
  - Transmitting virus to destroy system files
- Software Piracy
  - Theft of software through the illegal copying of genuine programs
  - The counterfeiting and distribution of products intended to pass for the original

Traditional Computer Crime

- Credit Card fraud
  - Personal information stolen from a card, or the theft of a card itself, can be used to commit fraud
  - Fraudsters might use the information to purchase goods in your name or obtain unauthorized funds from an account
- **Ransomware**
  - Type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid

Traditional Computer Crime



- Phishing
  - To request confidential information over the internet or by telephone under false pretences in order to fraudulently obtain credit card numbers, passwords, or other personal data
- Child Pornography
  - The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide

Traditional Computer Crime

- Cyber Terrorism
  - Use of Internet in terrorist activities
  - Terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc
  - Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt
- Net Extortion
  - Copying of someone’s confidential data in order to extort for huge amount
  - Nowadays demanding of ransom after kidnapping also done through **internet** via e-mail

Traditional Problems associated with computer crime

Traditional Problems associated with computer crime

- Criminals have the ability to adapt to changing technologies, environments and life styles
- Makes law enforcement difficult – failed to recognize the criminal potentiality of emerging technologies
- Earliest computer crime were non technological – theft of computer component, software piracy
- Law enforcement community
  - Experiencing uncertainty and ineffectiveness
  - Lack technological knowledge

Traditional Problems associated with computer crime

- Physicality and Jurisdictional Concerns
- Perceived Insignificance, Stereotypes and Incompetence
- Prosecutorial Reluctance
- Lack of Reporting
- Lack of Resources
- Jurisprudential Inconsistency

Traditional Problems associated with computer crime

- Physicality and Jurisdictional Concerns
  - Increase in Computer crime is due to
    - Lack of Physical boundaries
    - Multinational crime – able to commit crime in one country while sitting in other
    - There is no need of extensive tools, vehicular transportation, storage to commit crime
    - Crime moved from real to virtual environment – It insulate the criminal from law enforcement
    - Lack of cooperation, funding, politic

Traditional Problems associated with computer crime

- Perceived Insignificance, Stereotypes and Incompetence
  - Investigators and administrators show great reluctance to pursue computer criminals
  - Lack of knowledge and interest
  - Insider attack – hiding identity

Traditional Problems associated with computer crime

- Prosecutorial Reluctance
  - Law enforcement prosecutor lack knowledge and experience
  - Lack of interest, corporation, training and resources
  - Focusing towards headline catching case
  - Low priority to electronic crime

Traditional Problems associated with computer crime

- Lack of Reporting
  - Only 17% of victimizations were reported to law enforcement authorities
  - Number of Incidents reported to CERT has increased six fold from 2000 to 2003
  - Reason that business fail to report is to assure consumer of data security
  - Business do their investigation internally and if prosecution is needed then they share their report
  - Due to the perception that reporting will not result in capture of suspect
  - Many intrusions are detected long after violation occurred – making investigation difficult

Traditional Problems associated with computer crime

- Lack of Resources
  - Law enforcement and corporate entity should cooperate with each other
  - Corporate has resources to combat computer crime
    - They have administrators to monitor communication and system activity
    - They can establish policies with oversight
    - They have the ability to gather evidence through logs
    - They have fund for investigation
  - These resources are not available with law enforcement
    - They need economical support
    - They need training (Upgrading technologies) support
    - Need support for
      - personnel – salary, recruiting as needed
      - Hardware – advancing, need to remain consistent with technology
      - Software – Upgrade –os: tools for data capture, analysis, recovery, preservation; password cracking
      - Housing – need to set lab
- Jurisprudential Inconsistency

Traditional Problems associated with computer crime

- Jurisprudential Inconsistency
  - Establish a legality standard
  - Very difficult
  - Need Global cooperation