CYBERFORENSICS

UNIT – I

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.

Computer Forensics

- Goal: The goal of computer forensics is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it.
- Computer crime is any criminal offense, activity or issue that involves computers

- ❑Computer misuse tends to fall into two categories
  - ❑Computer is used to commit a crime
  - ❑Computer itself is a target of a crime. Computer is the victim. Computer Security Incident.
- ❑Computer is used to commit a crime
  - ❑ Computer 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, happened at certain

times is used in illegal activities: child examining log

❑Computer security Incident

- ❑Unauthorized or unlawful intrusions into computing systems ❑Scanning

a system - the systematic probing of ports to see which ones are open

- ❑Denial–of–Service designed to disrupt the ability of authorized users to access data

- ❑Malicious Code – any program or procedure that makes unauthorized actions (virus, worm, Trojan horse)

- ❑Computer forensics:
  - ❑Computer Forensic Analysis
  - ❑Electronic Discovery
  - ❑Electronic Evidence Discovery
  - ❑Digital Discovery
  - ❑Data Recovery
  - ❑Data Discovery
  - ❑Computer Analysis
  - ❑Computer Examination

What is Computer Forensics?

❑**Definition:** Involves obtaining and analyzing digital information, often as evidence in civil, criminal, or administrative cases ❑ **Computer forensics**

- ❑Investigates data that can be retrieved from a computer’s hard disk or other storage media

- Task of recovering data that users have hidden or deleted and using it as evidence
- Evidence can be ***inculpatory*** (“incriminating”) or **exculpatory**

- **Examples**
- Recovering thousands of deleted emails
- Performing investigation post employment termination
- Recovering evidence post formatting hard drive
- Performing investigation after multiple users had taken over the system

Computer Forensics Vs Other Disciplines

- Network forensics
    - Yields information about how a perpetrator or an attacker gained access to a network
- Data recovery

- ❑Recovering information that was deleted by mistake, or lost during a power surge or server crash
- ❑Typically you know what you’re looking for

❑Disaster recovery

- ❑Uses computer forensics techniques to retrieve information their clients have lost

❑Investigators often work as a team to make computers and networks secure in an organization

Digital Evidence

- ❑Locard’s principle: “every contact leaves a trace”
- ❑any information, stored or transmitted in digital form, that a party to a court case may use at a trial
- ❑To be accepted in court, digital evidence must meet certain criteria …
  - ❑Admissibility
  - ❑Authenticity

❑Reason for Evidence

❑ **Non-Business Environment:** evidence collected by Federal, State and local authorities for crimes relating to: Theft of trade secrets, Intellectual property breaches, Fraud, Unauthorized use of personal information, Extortion, Forgery, Industrial espionage, Perjury ,Position of pornography, SPAM investigations,

Virus/Trojan distribution , Homicide investigations

❑**Business Environment:** Theft of or destruction of intellectual property, Unauthorized activity, Tracking internet browsing habits, Reconstructing Events, Inferring intentions, Selling company bandwidth, Wrongful dismissal claims, Sexual harassment, Software Piracy

Case study

- In this case, American Express (Amex) claimed that Mr. Vinhnee had failed to pay his credit card debts, and took legal action to recover the money. But the trial judge determined that Amex failed to authenticate its electronic records, and therefore Amex could not admit its own business records into evidence. Among other problems, the court said that Amex failed to provide adequate information about its computer policy & system control procedures, control of access to relevant databases & programs, how changes to data were recorded

  or logged, what backup practices were in place, and how **Amex** could provide assurance of continuing integrity of their records.

- The judge pointed out that, "... the focus is not on the circumstances of the creation of the record, but rather on the **circumstances of the preservation of the record** so as to assure that the document being proffered is the same as the document that originally was created ...”

❑Lesson:

❑Document your access control and backup procedures and policies and test effectiveness of your controls. ❑Have the changes to your databases and content/record management system routinely recorded and logged.

❑Protect your electronic record from post-archival tampering with modern data integrity and trusted time stamping technologies.

❑Document the audit procedures you use to provide assurance of the continuing authenticity of the records.

Who use Computer Forensics?

- ❑Criminal Prosecutors - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- ❑Civil Litigations - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- ❑Insurance Companies - Evidence discovered on computer can be used to mollify costs (fraud, worker's compensation, arson, etc)
- ❑Private Corporations - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases
- ❑Law Enforcement Officials - Rely on computer forensics to backup search warrants and post-seizure handling

- ❑ Individual/Private Citizens - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment

- ❑ **Computer Forensics Services:** Content, Comparison again known data, Transaction sequencing, Extraction of data, Recovering deleted data files, Format conversion, Keyword searching, Decrypting passwords, Analyzing and comparing limited source code

Cyber Crime

❑Crime committed using a computer and the internet to steal a person’s identity or illegal imports or malicious programs. ❑Cybercrime is nothing but where the computer used as an object or subject of crime.

❑Current Scenario: 556 million victims per year,1.5+ Million victims per day, 18 victims per second…

❑In this Tech-savvy world of 21st Century every one is engaged with internet, through whatsapp, twitter, facebook, net banking & lots of other platforms are there.

- ❑Cyber criminal: Person or Group who commits

Cyber

Crime using computers Hackers, criminals groups, hacktivists, virus writers, terrorists

History of cyber crime

- ❑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.

- ❑Mid-1980s

❑Xtree Gold appeared on the market: Recognized file types and retrieved lost or deleted files

❑Norton DiskEdit soon followed: Became the best tool for finding deleted file ❑1987 Apple Mac SE

❑A Macintosh with an external Easy Drive hard disk with 60 MB of storage ❑1990

❑**International Association of Computer Investigative Specialists (IACIS)** ❑IRS created search-warrant programs

❑Expert witness for the Macintosh

❑First commercial GUI software for computer forensics

❑Created by ASR Data

❑Expert Witness for the Macintosh

❑Recovers deleted files and fragments of deleted files

❑Other software – iLook & AccessData Forensic Toolkit (FTK)

Cyber Crime & its Category

❑The Computer as a Target : using a computer to attack other computers. virus/worm attacks, Dos attacks etc. E.g Hacking,

❑The computer as a weapon : using a computer to commit real world crimes. Eg. Cyber terrorism, card Cyber frauds, Child pornography etc..

❑Category: Against Person, Property, Government

- ❑ Against Person: Harassment via email, cyber stalking, email spoofing, carding, assault by threat. The potential harm of such a crime to humanity can hardly be overstated.

- ❑ Against Property: cybercrimes against all forms of property. Unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs,

and unauthorized possession of computerized information.

- ❑Against Government: Cyber terrorism, damaging critical information infrastructure. Damaging gov or mil websites.

Types of Cybercrime

❑Hacking: illegal intrusion or unauthorized access to or control over a computer system or network.

❑DOS attack: attempt to make a machine or network resource unavailable to its intended users

- ❑Virus Dissemination: Malicious s/w attack (Trojan horse, web jacking..)

- ❑Computer Vandalism: Damaging or destroying data rather than stealing.

- ❑Piracy: theft of s/w through the illegal copying of genuine programs

❑Credit card Fraud: Fraudsters might use the information to purchase goods in your name or obtain unauthorized funds from an account.

❑Net Extortion: Copying of someone’s confidential data in order to extort for huge amount.

❑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.

❑Phishing: to request confidential information over the internet or by telephone under false pretenses 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.

❑Cyber Terrorism: Terrorist attacks on the Internet is by distributed DOS attacks, hate websites and hate emails, attacks on sensitive computer networks, etc.

How to tackle these activities?

- ❑ Awareness is the first step in protecting yourself, family and business. Invest in anti virus, firewall and SPAM blocking software for your PC.
- ❑Secure websites when conducting transactions online.
- ❑Don’t respond for unknown emails.

❑Set very tuff passwords.

❑ Cyber Law: There is absolutely no comprehensive law on cybercrime any where in the world.

This is reason that the investigating agencies like FBI are finding the cyberspace to be an extremely difficult terrain.

❑Electronic Transaction act 2061 BS (2005 AD).

❑Information Technology policy – 2000.

Traditional Pbm asso. W. comp. crime

❑Any offence against morality, social order or any unjust or shameful act. ❑"Offence" -in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force.

❑Cyber Crime is emerging as a serious threat.

World wide governments, police departments and intelligence units have started to react.

❑Cyber crime variants:

❑**Hacking** is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year.

❑**Cyber Stalking** is use of the Internet or other electronic means to stalk someone. ❑This term is used interchangeably with online harassment and online abuse. ❑Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property

CYBERCRIME

❑**Cyber Squatting** is the act of registering a famous Domain Name and then selling it for a fortune.

❑**Phishing** is just one of the many frauds on the Internet, trying to fool people into parting with their money.

❑Phishing refers to the receipt of unsolicited emails by customers of Financial Institutions, requesting them to enter their Username, Password or other personal information to access theirAccount for some reason.

❑The fraudster then has access to the customer's online bank account and to the funds contained in that account.

❑ **Vishing** is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward.

❑Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.