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.

Introduction to Identity Theft & Fraud

- What is Identity theft?
- Someone steals your personal information
- Uses it without permission
- Can damage your finances, credit history and reputation
- How do you know if your identity was stolen?
- mistakes on accounts or your Explanation of Medical benefits
- regular bills go missing

- calls from debt collectors for debts that aren't yours
- notice from the IRS
- calls or mail about accounts in your minor child's name
- How does identity theft happen?

- steal information from trash or from a business
- trick you into revealing information
- take your wallet or purse
- pretend to offer a job, loan, or apartment to get your information

Reduce the Risk

- Identity protection means treating your personal information with care. Make it a habit.
  - like buckling your seatbelt, or
  - locking your doors at night
- Read your bank, credit and account statements,

and
- Explanation of Medical benefits.

- Look for charges you didn’t make.

- Be alert for bills that don't arrive when you expect them.
- Follow up if you get account statements you don't expect.
- Protect Your Personal Information.
- Keep your important papers secure.
- Be careful with your mail.
- Shred sensitive documents.
- Don't over share on social networking sites.

Reduce the Risk

- Respond quickly to notices from the Internal Revenue Service.

- If someone has used your Social Security number on
- a tax return, contact IRS's Specialized Identity Theft
- Protection Unit 1-800-908-4490
- Be alert to online impersonators.
- Do you know who is getting your personal information?
- Don't click on links in emails.
- Contact customer service.
- Protect your computer.

❑Use anti-virus software, anti-spyware software, and a firewall. ❑ Create strong passwords. Lock up your laptop.

❑Keep your computer's operating system, browser, and security up to date. ❑Encrypt your data.

❑Be wise about wi-fi.

❑Read privacy policies.

19

What to do if someone has stolen identity?

❑Act fast to limit the damage.

❑Take these steps immediately.

❑STEP 1: Place an initial fraud alert on your credit report. ❑

Contact any one of the three nationwide credit reporting companies. ❑

Equifax 1-800-525-6285 Experian 1-888-397-3742 TransUnion 1-800-680-7289 ❑

Step 2: Order your credit reports.

- ❑Contact each of the three credit reporting companies.
- ❑ID theft victims get a copy of their reports for free.
- ❑Read your reports carefully and correct any errors.

- Step 3: Create an Identity Theft Report.
  - Gives you rights that help you to recover more quickly.
  - File a complaint with the FTC.
  - This will become your FTC Affidavit.
  - File a police report.

TYPES OF CYBER FORENSICS

- Military Computer Forensic Technology

- Law Enforcement Computer Forensic
- Business Computer Forensic

TYPES OF CYBER FORENSICS

- Military Computer Forensic Technology
- Key objectives of cyber forensics include rapid discovery of evidence, estimation of potential impact of the malicious activity on the victim, and
- assessment of the intent and identity of the perpetrator.

- National Law Enforcement and Corrections Technology Center (NLECTC) - demonstrate New Methodology
- National Institute of Justice (NIJ) sponsors research and development or identifies best practices to address those needs.
- Possible to accurately determine the motives, intent, targets, sophistication, identity, and location of cyber criminals and cyber terrorists Synthesizing Information from Forensic Investigations (SI-FI) integration environment supports the collection, examination, and analysis processes employed during a cyber-forensic investigation

- Integrated forensic analysis framework

- SI-FI prototype uses digital evidence bags (DEBs) – investigators can seal & Authorized user can reopen the DEBs

TYPES OF CYBER FORENSICS

- Law Enforcement Computer Forensic
- Computer Evidence Processing Procedures
- Preservation of Evidence
- Disk Structure : evidence can reside at various levels within the structure of the disk

❑Data Encryption : should become familiar with different forms ❑Matching a Diskette to a Computer: use special software tools to complete this

❑Data Compression

❑Erased Files

❑Internet Abuse Identification and Detection

❑The Boot Process and Memory Resident Programs

TYPES OF CYBER FORENSICS

- Business Computer Forensic
- Remote Monitoring Of Target Computers - Data Interception by Remote Transmission (DIRT)
- Creating Trackable Electronic Documents - intrusion detection tool
- Theft Recovery Software For LaptopsAnd PCs

Forensics Services Available

❑Tracking and location of stolen electronic files ❑Honey pot sting operations

❑Location and identity of unauthorized software users ❑Theft recovery software for laptops and PCs ❑Investigative and security software creation ❑Protection from hackers and viruses