UNIT-3

Identification of Data:

The internet provides access to vast information and facilitates global email communication and file sharing. Law enforcement agencies often encounter computers at crime scenes, which are used to store criminal information and facilitate crimes. Maintaining accurate timestamps is crucial for computer forensics, as it helps in identifying data and investigating incidents involving multiple computers.

Forensic Analysis of Technical Surveillance Devices

Computer forensics is used in both criminal investigations and business expansion.

Corporate Information (CI):

CI involves activities like spying, theft of trade secrets, and intelligence gathering to help executives collect and analyze public information about competitors for strategic planning.

Information Overload:

With the increasing amount of information available, CIOs should focus on supporting their company's CI efforts by recruiting technology executives who can build systems for real-time reactions to competitors and faster responses to customer needs.

Building Teams:

Teams should have diverse skills, combining information organization with technology expertise. Companies should not expect to buy off-the-shelf software for intelligence processes; CIOs need to help build custom solutions.

Reconstructing Past Events:

Reconstructing past events involves more than just recovering electronic data; it's about ensuring that the findings are admissible as evidence. Here's a simplified breakdown:

- **Recovering Data**: Recovering electronic data is the first step. Once you have the data, you need to reconstruct past events to ensure your findings can be used as evidence.
- **Getting Help**: If you're unsure about handling the data, seek help from a litigation support group or other resources within your office.
- **Converting Digital Evidence**: Data can come in various formats like holograms, video, data tapes, Zip disks, CD-ROM disks, and floppy disks. You need to convert this data into a format you can work with.
- **Putting Evidence in a Usable Format**: Once the data is converted into a usable format like word processing, spreadsheet, or presentation files, you can start working with it to reconstruct past events.

Usable File Formats

Even if data appears to be in a familiar format, conversion may still be necessary if it's too new or runs on a different operating system. While simple files can often be opened in a competitor's similar product, complex files may require conversion.

Unusable File Formats

You may need to convert files to a usable format, which can be challenging. This is common with email files, database files from mainframe systems, and ".txt" files containing data from databases. Gathering information about how the files were created and maintained can help facilitate the conversion process.

Converting Files

If you attempt to convert the data yourself, you might be able to use programs like Access or Excel, which have built-in wizards for file conversion.

For ".txt" files, the first line might contain field names, making the conversion simpler.

If necessary information is not in the file, try to obtain it from the party that produced the data.

Some data, like email files, may not be immediately convertible to a usable format.

Destruction Of Email:

Emails are not just casual messages; they're considered formal records by the courts and can be used as evidence in legal cases. Deleting emails doesn't always make them disappear forever; they can still be retrieved from backups or archives. To avoid legal issues, it's important to have a consistent email retention policy:

- Keep all incoming emails on your server for a specific period, like 30-60 days.
- Delete archived emails after an additional specified time.
- Keep email backups separate from other computer backups.
- Automatically delete emails, including backups, after a short period, like 15-30 days.
- Use the same rules for deleting emails on all devices and suspend automatic deletion during investigations or legal matters.

Damaging Computer Evidence :

Protecting Digital Evidence

To ensure the accuracy and reliability of digital evidence, law enforcement and forensic organizations must establish and maintain effective quality systems. Rapid technological changes require regular updates to personnel, training, equipment, and procedures. Case notes and records must be permanent and authenticated. Evidence is valuable only if it can be shown to be accurate, reliable, and controlled.

International Principles for Preserving Computer Evidence

The International Organization on Computer Evidence (IOCE) was established to facilitate international cooperation in computer crime investigation. The

IOCE developed principles for the standardized recovery of computer-based evidence, emphasizing consistency with legal systems, a common language, and confidence in evidence integrity.

Key Principles for Handling Digital Evidence

- Actions taken upon seizing digital evidence should not alter it.
- Only forensically competent individuals should access original digital evidence.
- All activities related to digital evidence seizure, access, storage, or transfer must be fully documented and preserved.
- Individuals are responsible for actions taken with digital evidence while it is in their possession.
- Agencies handling digital evidence are responsible for complying with these principles.

Tools and Procedures for Intrusion Response and Incident Reporting

It's crucial to document and inventory the tools needed for responding to intrusions and data destruction. This includes intrusion detection software, backups, and file-system-recovery tools. Training IT staff on how to deal with intrusions is also important, and this can be done through various courses or custom training programs.

Incident reporting and contact forms are essential for documenting intrusions. They provide an audit trail that can be used in criminal proceedings. These forms should capture as much information as possible, including:

- Contact information for those discovering the problem and responsible parties.
- Details about the systems under attack, such as operating system versions and IP addresses.
- The purpose of the systems under attack, including their importance.
- Evidence of the intrusion, including the method of attack and the source IP address of the attacker.
- A list of parties to notify, including technical contacts, internal legal contacts, and legal authorities.

System Testing and Security Measures

System testing is crucial for ensuring the security of your network. Statistics show that over 82% of successful hacks occur due to the failure to install patches for known bugs. Here are some key areas to focus on:

Domain Name Service (DNS)

- DNS is a critical part of the Internet infrastructure that translates domain names to IP addresses.
- Ensure your DNS software is up to date to protect against vulnerabilities.
- Limit access to port 53 (the DNS port) on your firewalls to prevent unauthorized access.

Services and File Sharing

- Windows computers are often targeted for file sharing attacks.
- Remove unnecessary services to reduce vulnerabilities.
- Configure file shares properly to avoid exposing critical system files.

By implementing these measures and staying vigilant about security updates, you can greatly enhance the security of your network.