U-3 (CSDF)

Intro to Digital Forensics.

* Computer Forensic -

- Methodical examination of computer media (hark discs, diskettes, cassettes, etc) evidence is known as computer forensics.
- Involves gathering, preserving, analysing & presenting data relating to computer.

* Use of computer Forensics in Law Enforcement -

- Recovery of deleted files
- Search for unallocated
- To trace artefacts
- To process hidden files
- To run string searches.

* Collection of Evidence -

1) Analysis of evidence
2) Investigating the evidence
3) comparing evidences with a references model
4) Documenting the evidences
5) Maintaining a chain of custody &
6) Resolution

* Computer Forensics Services -

1) Data Seizure
2) Data Duplication / preservation.
3) Data Recovery
4) Document Searches
5) Media Conversion
6) Expert witness services
7) Computer evidence service offices.

* Steps taken by Computer Forensics Specialists.

- Protect subject computer system
- Discover all files
- Recover all deleted data detected
- Reveal contents of secret folders.
- Access the contents of password.
- examine all potentially relevant data discovered
- print on overall study of subject computer system.
- Provide an opinion on system layout, file structure, etc
- provide expert consultation &/or testimony.

* Types of Law Enforcement - Computer Forensic Technology.

- security of evidence
- ecommerce investigation
- Program with two purposes
- search techniques with text
- tools of fuzzy logic used to identify
- Internet Abuse Detection & Identification.
- Memory Resident Programs & Boot Process.

Internet Abuse Detection & Identification.
- Disk structure
- Data Encryption
- Diskette to computer matching
- Data Compression.
- Deleted Files.

* Types of Business Computer Forensic Technology,

1) Remote monitoring of target computers
2) Creating trackable electronic documents.
3) Theft recovery software for laptops & PCs
4) Basic forensic tools & techniques
5) Forensics services available.

* Computer Forensics Evidence & Capture.

- Data Recovery Defined → • highly experienced engineers analyse.
- Data Backup & Recovery → • Backup Obstacles

* Backup Window — • is time span which backups maybe performed
  • non production times → network bandwidth & cause a low throughout system → • Traditional backup methods → I/O bottlenecks.
  * ability of system → being backup.
  * backup servers capacity to accept data.
  * throughout of tape devices onto which data is sent.

shortage of resources.

* Role of Back Up in Data Recovery
  - → storage prices are falling
  - → system must be available at all times
  - → Role of backup has evolved.

* Problem with Today's Back Up.
  - → Network Backup degrades
  - → offline Backup
  - → live backups
  - → Mirroring.

* Data Recovery Solutions.
  - → shrinking Expertise, Growing Complexity
  - → Failures
  - → Downtime & Budgets
  - → Recovery
    - → Automated Recovery
    - → Takes Backup
    - → Make Recovery More Efficient.

U-4th

Forensic Evidence Collection & Data Seizure.

- **Need for collecting evidence –**
  - Prevention in Future.
  - Responsibility
  - To make decisions.
  - To prove or disprove a fact.

- **Types of Evidence –**
  - Real evidence → • one courtroom to another • most powerful evidence
    • show in jury • speaks for itself.
  - Documentary evidence → • written form • server log, email, database, etc
    • authenticated due to fake copies • original doc → more
  - Testimonial evidence → • statement of oath, either in court or deposition
    • helps validate alternative types.
  - Demonstrative evidence → • Recreates or explains diff evidence.
    • Doesn't talk for itself.
    • Demostrate & make previous points.
    • max helpful → technical topic to non-technical audiences.

- **Rules of Evidence –**
  - Admissible → • most basic rule • evidence nature • doesn't hold up in court
    • lost time • allowed guilty individual to go
  - Authentic → • evidence → genuine • investigation → authetication.
    • inquiry → unimportant • evidence → relevant way.

- Reliable - • dependable evidence • validity of expert's decisions.
  • found^{n} → reliable • authenticity & veracity
- complete - • evidence → complete • diff perspective of evidence needed
  • no assumption • unequivocal judgment.
- Believable - • acceptable evidence • conclusn → plain & unambiguous.
  • jury → non tech member • understable evidence.

* Process of Evidence Handling -
  - Identification of Evidence
  - Preservation of Evidence
  - Evidence analysis
  - Evidence presentation.

* collecting & Archiving → • Logs & Logging • Monitoring.

* Methods of collection → • Honeypotting • Freezing the Scene.

* Artifacts → • code snippets, malicous software or attacker nearly leaves behind.
  • impacts of artefacts → out control → unpredictable.

* collection Steps → 1) Find Evidence
  2) Find Relevant data
  3) Establish an order of volatility
  4) Eliminate external source of exchange.
  5) Gather Evidence
  6) Document everything.

Chain of custody →

- documentation of all changes in control, handling, custody & ownership.
- store in tamper proof manner
- trace place of evidence from instant it was collected → judicial court.
- Access evidence safe is controlled by evidence custodians.

Process:

1) Data Collection → • first step • identification labelling, recording & acquisition

2) examination → • info → documented • forensic procedure.
• take ss → process → task completion.

3) Analysis → • result of examination stage • respond to q in case

4) Reporting → • statement about COC
• various tools
• data sources → how analysed
• vulnerabilities
• Addn forensics measure are taken.

- save original files
- photograph → physical evidence
- taking ss → digital evidence
- date, time & other info
- authenticate working clone
- Inject forensic computers.

Duplication & Preservation of Digital Evidence.

- SafeBack → • widely utilised by govt intelligence, military & law.
  • appln → copies & maintains all data stored on hard drive.

- SnapBack → • Bit stream backup appln
  • more expensive
  • every step → evidence backup & restoration procedure.
  • image harddrive → need specialist bitstream backup software.

- Computer Evidence Processing Steps:-
  - Turn Computer off
  - System Hardware setup in writing
  - Transport computer system to a secure location.
  - Create hard disc & floppy disc bit stream backups.
  - Mathematically verify all data.
  - Create a list of key search words.
  - Record system's time & data.
  - Examine Window's Swap file
  - Determine file slack.
  - Examine unallocate space (erased files).
  - search files, file slack & unallocated space for keywords.
  - Document file names, dates & times.
  - Detect irregularities in files, programs & storage.
  - Examine operation of s/w
  - Document your findings
  - Retain copies of s/w used.

- Computer Image Verification & Authentication
  - → Digital IDS & Authentication tool
  - → Authenticode.
  - → Authentication with Verisign Digital IDs.
  - → Public Key Cryptography
  - → Digital ID
  - → certificate Authorities

- Evidence Collection Procedure
  - Incident Coordinator.
  - Evidence Notebook
  - Evidence Collection.
  - Storage & Analysis of Data

U-5
Computer Forensics Analysis & Validation.

✱ Determining what Data to collect & Analyse.

- Type of investigation conducted
- Volume of data to be processed.
- amount of time required to gather, examine & present evidence
- Keep all evidence & discoveries for examination.
- ~~Retain~~ Recover contents of any password protected files
- best to recover root directory of disc.

✱ Data analysis with Access Data Forensic Toolkit

- Microsoft FAT12, FAT16, & FAT32.
- Microsoft NTFS (for windows NT, 2000, XP & Vista)
- Linux Ext2fs & Ext3fs

Validating Forensic Data → Using Hexadecimal Editors for Validation

✱ Addressing Data Hiding techn" & performing Remote Acquisition.

1) Hiding Partitions → consider all evidence drive
   → Using Disk Manager to view a hidden partition.

2) Marking Bad Clusters → sensitive data → disc partition clusters
   → labelling good cluster as bad clusters using disc editor

3) Bit Shifting → ability to programme in assembly language used by certain home computer used allowed them

4) Performing Remote Acquisitions → need to image drive of a computer that is far away from you or don't want a suspect to be aware that an investig" taking place

5) Remote acquisition with Runtime software-
- Disk explorer for FAT
- Disk Explorer for NTFS
- HDHOST

* Identifying Digital Evidence →
- Digital Evidence
- US courts accepts → digital evidence → physical evidence
- set standards for digital evidence.

→ General task Investigators perform when working with digital evidence
1) Identify digital info or artifacts → used as evidence
2) collect, preserve & document evidence
3) Analyze, identify & organize evidence
4) Rebuild evidence of repeat a situation to verify results.

⇒ Processing Law Enforcement Crime Scenes:

Prepare for Search
- Securing a Computer Incident or Crime Scene
- Seizing Digital Evidence at Scene.
- Storing digital evidence
- Obtaining a Digital Hash.
- Reviewing a Case.
  - specify requirement → case
  - Plan your research
  - carry out investigation
  - finishing writing case report
  - Examine art.

U-6.
Current Computer Forensic Tools.

* Computer Forensics Tools Responsibility/Tasks-

a) Acquistion -
- create replica of original drive in intial step
- protects original drive ensure doesn't degrade & harm digital evidence
- example of subfunctions
  - physical & logical copies of data
  - format for acquiring data
  - verification.
  - common line acquision
  - GUI acquistion
  - remote acquistion.

b) Validation & Discrimination → process of verifyg data.
subfunc → Filtering
Hashing
Investigating file headers.

c) Extraction → which recovery work in computer study
subfunc → Data viewing
keyword search
decompression
carving
decryption
book marking

d) Reconstruction

e) Reporting.

Computer Forensics Software Tools-

1) SANS SIFT —
- SANS Investigating Forensic Toolkit (SIFT).
- Ubuntu based Live CD. → conduct indepth forensic
- Incident response investigation.

2) Crowd strike Crowd Response -
- lightweight console application → part of incident response → scenario.
- embedded YARA signatures → scan your host malware & report.

3) Volatility -
- memory forensic framework for incident response & malware analysis
- allows extract digital artefacts from RAM dumps.
- extract info → running processes, open network sockets, etc.

4) The sleuth kit (+Autopsy) -
- open source digital forensics toolkit
- indepth analysis of various file systems
- extract info → running processes.

5) FTK Images -
- Data preview & imaging tool → examine file & folders on local drive.
- Review content of forensic images or memory dumps.
- create SHA1 or MD5 hashes of files.

6) ExifTool -
- Command line application → read, write or edit file metadata info
- fast, powerful & supports a large range of file formats

7) Free Hex Editor Neo -
- Is a basic hex editor → handle very large files.
- additional features → commercial versions of Hex Editor Neo

8) Bulk Extractor -
- computer forensics tools scans a disk image, file or directory of files
- extracted info → output to series of text files.

9) DEFT -
- another linux live CD → free & open source computer forensic tools
- Help with Incident response, Cyber Intelligence & computer forensics

10) Xplico -
- open source Network Forensic Analysis Tool → extract app^n data from internet traffic
- features include support for multitude of protocols

11) Last Activity View -
- Allows you to view what actions → by user & events occurred
- running executable file, opening a file/folder from Explorer

12) DSi USB Write Blocker -
- Is write Blocker is software based → write access → USB devices
- prevent modifying metadata or timestamps

13) Fire Eye Red line -

- Redline offers → perform memory & file analysis of specific host.
- collects info → running processes & drivers from memory.

14) Plain Sight -

- Live CD based on knoppix.
- perform digital forensics tasks such as viewing internet histories.
-

15) HXD -

- one of best, user friendly editor & perform low level editing
- modifying of hard disk & main memory (RAM).
- include searching & replacing, exporting, built file, etc.

16) HELIX 3 Free -

- Is a live CD based on Linux → Incident Response, Computer Forensics & E-Discovery scenarios
- Pack with touch of open source tools.

17) Paladin Forensic Suite -

- Is a live CD based on Ubuntu → wealth of open source forensic tools.
- 80+ tools found on this CD are organized → 25 categories.

18) USB Historian -

- parses USB information, primarily from Windows Registry
- dealing with investigation → data was stolen → moved or accessed.

Computer forensics Hardware Tools -

1) Computers →
2) Cell phones & GPS units
3) cloning units
4) Crime Scene kit.

Validating & Testing Software forensics -

- National Institute of standards & Techology Tools -
  - classification of forensic tools
  - requirements → category
  - create test claims
  - Determine test cases
  - Develop test strategy
  - Report test findings.

Email Investigations -

- role of email in investigations
- exploring roles of Client & Server in Email.
- → POP (Post office Protocol)
  → Internet Message Access Protocol (IMAP)
  → MAPI (Microsoft's Mail API)
  → HTTP
  → SMTP (simple mail transfer protocol).

* Investigate E-mail Crimes & Violations

steps -

1) Examine email message
2) Copy email message
3) Print email message.
4) View mail headers.
5) Examine email headers.
6) Examine attachment if it is there in email
7) Track email.

* Using Specialised E-mail Forensic Tools.

- Data Recovery → • ProDiscover Basic & Access Data FTK.
- FINAL e MAIL for Outlook Express & Eudora.
- R-Tools R-Mail for Outlook & Outlook Express
- Paraben E-Mail Examiner
- Data Viewer → Outlook & Outlook Express
- DBX Extract for Outlook Express.
- Access Data FTK for Outlook & Outlook Express.
- Track Easy Recovery Email Repair for Outlook & Outlook Express.
- Office Recovery Mail Recovery for Outlook, Outlook Expresses Exchange, Exchange Server & IBM Lotus Notes.