COMPUTER FORENSIC CAPABILITIES

Outline to accompany the slide presentation; this outline does not exactly follow the slides

1. Agenda

   - What is computer forensics?
   - Where to find computer evidence
   - Forensic imaging
   - Forensic analysis

2. What is "computer forensics"?

   - The preservation, identification, extraction, analysis, and interpretation of digital data, with the expectation that the findings will be introduced in a court of law

3. Capabilities

   - Reveals direct evidence on the machine
   - Associates a machine with data
   - Provides investigative leads
   - Reveals evidence that corroborates or refutes allegations or alibis
   - Reveals behavioural evidence

4. Relationship between the case agent and the forensic examiner

   - The case agent and forensic examiner must work as a team
   - Case agent
     - Involves examiner early
     - Explains case
     - Provides focused requests
   - Forensic examiner
     - Educates and advises investigator
     - Explains results and limitations

5. Where to find computer evidence

   - Seize items specified in the search warrant.
     - Computers, laptops, network equipment (hubs and switches)
     - Peripherals: CDR, DVD-R, digital cameras, PDA
     - External media: CD, floppy disk, USB thumb drive
     - Paper notes, documentation and manuals, post-it notes.
   - Document computer equipment and peripherals prior to removal
     - Digital pictures, diagrams

6. What is forensic imaging?

- Obtained by a method which does not, in any way, alter any data on the drive being duplicated
- Duplicate must contain a copy of every bit, byte, and sector of the source drive
- Duplicate will not contain any data except filler characters (for bad areas of the media) other than that which was copied from the source media
- Accurate, verifiable, reproducible

7. Value of forensic imaging

- Incident response/forensic imaging is the most important step in the entire electronic investigation
- Failure can invalidate or make inadmissible all further information gathered from the digital evidence

8. The imaging process

9. Physical write blocks

- Physical device that prevents writes to the evidence drive
- Best method of imaging

10. Attaching write block

11. Hardware imager

12. Software imaging

- Bootable CDs or floppies
- Control computer so it only issues read commands to the drive, never write
- Examples:
- FTK Imager
- EnCase
- DD
- Ghost
- Others

13. Physical vs. Logical

- Physical data structure refers to the actual organization of data on a storage device Physical imaging gets all the zeros and ones possible from the device
- Logical data structure refers to how the information appears to a program or user as seen through the operating system; logical imaging misses data from areas not seen by the operating system

14. What can the examiner find?

- Deleted files
- Text fragments
- Enhanced metafiles (previously printed files)
- Enhanced metadata (embedded information)
- Date/time stamp information
- E-mail messages and chat logs
- Internet usage information (history)
- Archived and compressed files (zip)
- Encoded e-mail attachments
- Images (active and deleted)
- And more...

15. Forensic request from case agent

- Example: kidnapping assault of Heather Miller
    - Evidence of defendant's involvement with abduction
    - Search for victim's name
    - Pictures of victim
    - Evidence of threatening letter sent to victim
    - Evidence of references to date rape drugs
    - Evidence of conspirator
    - Activity on the computer during time of crime
    - User attribution

16. Getting started

- Keyword searches
- Drawbacks to key word searches
    - Adobe PDF documents
    - Faxes
    - Excel
    - Registry
    - Compound/compressed files
    - Several others

17. Graphics review

17. Email review

18. Email headers

19. Types of email metadata

- When created
- How created
- When sent
- When received
- Who sent/received
- Route
- Reply email

20. Time analysis

21. Graphic analysis

22. Application logs

23. Internet cache

24. Chat logs

25. Metadata

26. Using online search engines

27. Web history

- Identify web surfing session
- Where/when did they open browser?
- How did they get to the significant finding?
- Web mail
- Other activities?
- All goes toward user attribution

28. Summary

- Electronic evidence is everywhere
- Case agents must work closely with examiners
- Forensic examiners must look beyond the "single file"
- Metadata can be critical to establishing user attribution
- Even if evidence itself has been deleted/destroyed, numerous artifacts can be found

End