USING ELECTRONIC EVIDENCE IN CYBERCRIME INVESTIGATIONS

U.S. Department of Justice

Understanding Digital Evidence

- Investigators and prosecutors must know:
  - When is digital evidence important?
  - Where is digital evidence found?
  - How is digital evidence collected?
  - What do you do with digital evidence?

- Don’t forget traditional investigative tools: witness interviews, suspect interviews, etc.

Networks and the Internet

Computers rarely stand alone

ALL DIGITAL INFORMATION IS AT A PHYSICAL LOCATION

Collecting digital evidence

- Computer crime is a worldwide challenge, but domestic laws establish procedures for obtaining digital evidence, and:
  - Enable successful investigation and prosecution
  - Rules of evidence to ensure fair trials
  - Improve international legal cooperation
- These rules generally include ways for law enforcement to protect the confidentiality of an investigation
- Countries generally seek to balance law enforcement interests with a respect for human rights

Crimes Create Digital Evidence

- Any crime can create digital evidence

- Cybercrimes - Computer used to commit crime
  - Illegal access to computer systems – "hacking"
  - Interference with data or computer systems
  - Online identity theft
  - Cellphone records, including location records

CRIMINALS MAY NOT KNOW ABOUT
THE DIGITAL EVIDENCE THEY CREATE

Examples of Digital Evidence

- Computer used to store evidence of crime
  - Child pornography photographs
  - Pirated movies and other intellectual property
  - Records of criminal transactions – drug sales
- Computer used for communication about or during crime
  - Email
  - Social networking
  - Voice and video communications
  - Location information
  - Forensic recovery of deleted files
  - System files created by computer use

What Are You Proving?

- Attribution is the primary issue in most cybercrime cases: *who* was at the computer?
- Generally easy to show that a computer was involved in the crime
  - The computer is the "crime scene"
  - Proof will almost always depend on some type of circumstantial evidence
- Absent direct evidence, rely on circumstantial evidence of
  - Access
  - Knowledge
  - Opportunity
  - Motive
  - State of Mind
- Proof in other cases

The Virtual Investigation

- Digital “Fingerprints”
  - IP Address/Phone Number
- Stored data
  - Subscriber data
  - Traffic data
  - Content data
- Real-time data collection
  - Traffic data
  - Content data
- Computer forensics

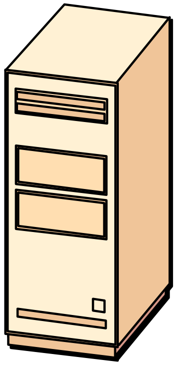
Stored Traffic Data and Subscriber Info

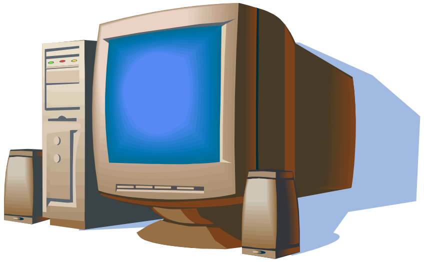
- Service providers are between suspects and the rest of the world
- Service Providers control important digital evidence
  - Customer subscriber information
  - Traffic data (Logs)
  - Computer data (Copies)

Content of Stored Communications

- Production Order for stored email
- Get suspect’s email from Service Provider

Production Order



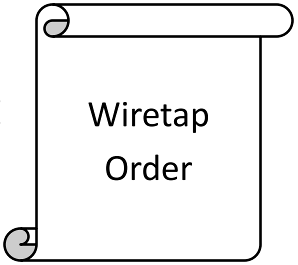


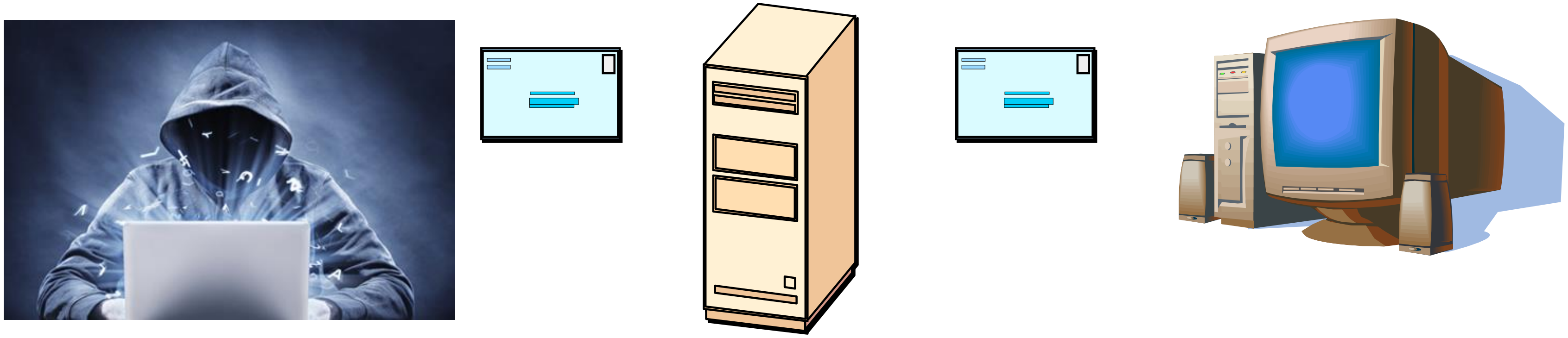
Locate the Suspects: Real-time Traffic Data

- Real-time collection of
  - the source and destination IP address
  - to: and from: email addresses
  - Ports
  - Attachments
  - Other “header” (non-content) information

Interception of Communications

- Interception, “wiretap”
- Sends copies of all content to law enforcement





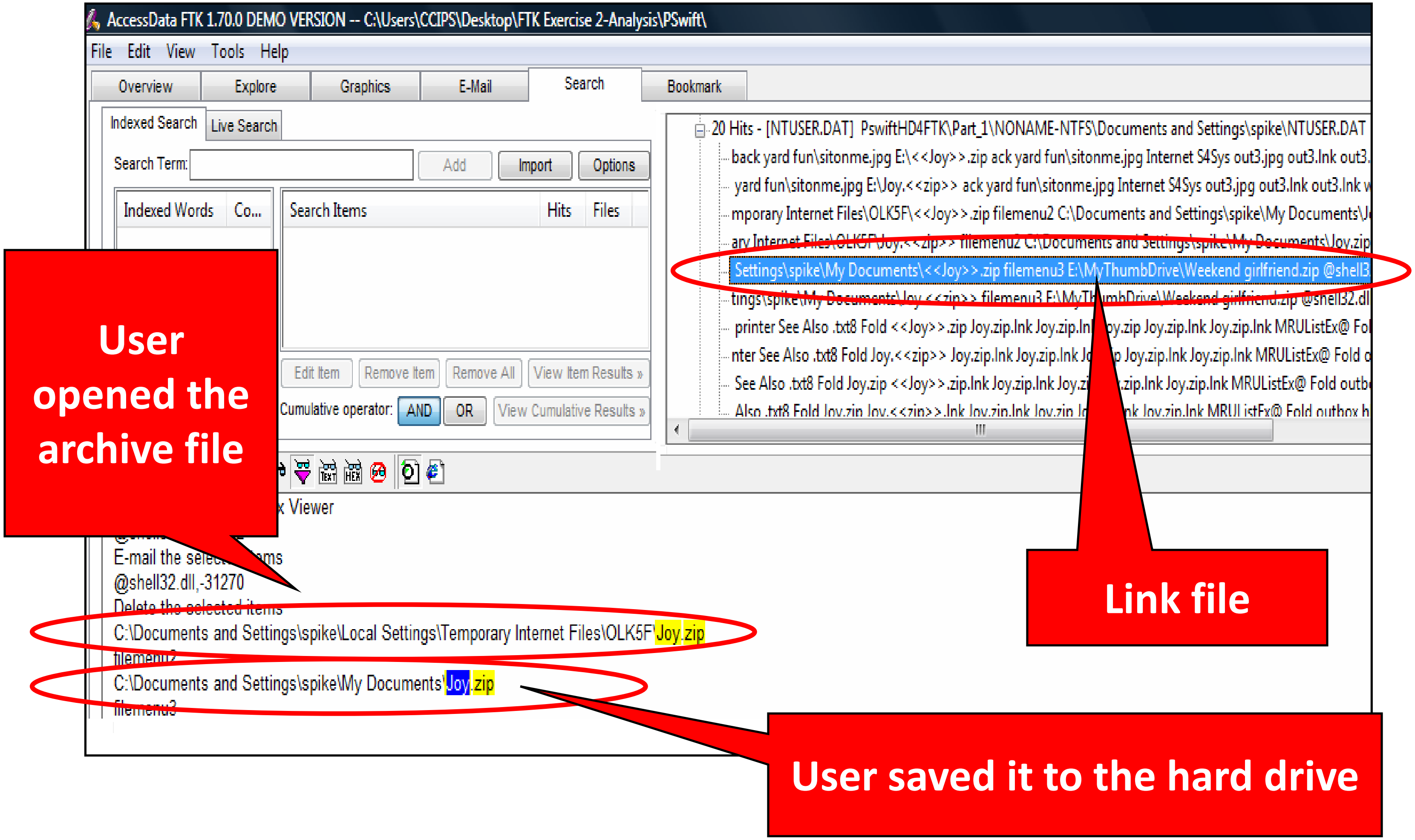
Computer Forensics

- The forensic examination process
  - Forensic request
  - Preparation/extraction
  - Identification
  - Analysis
- Work with the forensic examiner to translate evidence requests to forensic requests

Forensic Analysis Examples

- Data analysis (continued)
  - Chat logs
  - Registry entries and internet cache
  - Link files
  - Web history
  - Unallocated space
  - Installed programs
  - Metadata

Registry and internet cache


AccessData FTK 1.70.0 DEMO VERSION -- C:\Users\CCIPS\Desktop\FTK Exercise 2-Analysis\PSwift\
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Indexed Search Live Search
Search Term:
Add Import Options
Indexed Words Co...
Search Items Hits Files
Edit Item Remove Item Remove All View Item Results »
Cumulative operator: AND OR View Cumulative Results »
x Viewer

```
20 Hits - [NTUSER.DAT]  PswiftHD4FTK\Part_1\NONAME-NTFS\Documents and Settings\spike\NTUSER.DAT
back yard fun\sitonme.jpg E:\<<Joy>>.zip ack yard fun\sitonme.jpg Internet S4Sys out3.jpg out3.lnk out3.
 yard fun\sitonme.jpg E:\Joy.<<zip>> ack yard fun\sitonme.jpg Internet S4Sys out3.jpg out3.lnk out3.lnk w
mporary Internet Files\OLK5F\<<Joy>>.zip filemenu2 C:\Documents and Settings\spike\My Documents\J
ary Internet Files\OLK5F\Joy.<<zip>> filemenu2 C:\Documents and Settings\spike\My Documents\Joy.zip
Settings\spike\My Documents\<<Joy>>.zip filemenu3 E:\MyThumbDrive\Weekend girlfriend.zip @shell3
tings\spike\My Documents\Joy.<<zip>> filemenu3 E:\MyThumbDrive\Weekend girlfriend.zip @shell32.dl
 printer See Also .txt8 Fold <<Joy>>.zip Joy.zip.lnk Joy.zip.ln oy.zip Joy.zip.lnk Joy.zip.lnk MRUListEx@ Fol
nter See Also .txt8 Fold Joy.<<zip>> Joy.zip.lnk Joy.zip.lnk Jo p Joy.zip.lnk Joy.zip.lnk MRUListEx@ Fold o
 See Also .txt8 Fold Joy.zip <<Joy>>.zip.lnk Joy.zip.lnk Joy.zi .zip.lnk Joy.zip.lnk MRUListEx@ Fold outb
 Also .txt8 Fold Joy.zip Joy.<<zip>>.lnk Joy.zip.lnk Joy.zip l nk Joy.zip.lnk MRUListEx@ Fold outbox h
```

```
E-mail the sele ms
@shell32.dll,-31270
Delete the selected items
C:\Documents and Settings\spike\Local Settings\Temporary Internet Files\OLK5F\Joy.zip
filemenu2
C:\Documents and Settings\spike\My Documents\Joy.zip
filemenu3
```

User opened the archive file

Link file

User saved it to the hard drive

Other forensic evidence

- Web history
  - Internet browsers are set by default to collect, or log, browsing activity
  - Even if this recorded activity is deleted by the user, it can sometimes be found in “unallocated space”
- Unallocated space
  - These are the areas on a storage device that are not currently storing data that is part of the logical file system
  - When users delete information from a computer, the space is usually not overwritten

Other forensic evidence

- Metadata
  - Almost all files have created and modified dates (although these can be unreliable)
  - Software can also embed certain additional information inside of the files it produces
    - Digital cameras often embed the time, date, and camera type inside of files
    - Microsoft Word by default embeds the author and last user who saved file
- System Files
  - Records behavior of a user, including files created/opened, applications used, external media attached