

PC FORENSICS

FIRST RESPONDER AND BEYOND

Kelly Tipton – Mike Duncan
Wright State University

Intended Audience

⦿ Technicians Why?

- Often first at scene, “stumble upon” a case
- First sent/requested to check suspicious activity
- Familiar with users, easier rapport; Less intimidating than new/unknown “investigator”

Intended audience

⦿ Managers Why?

- Often first point of contact from outside entities
- Must often play interference for technician
- Management Buy-In:
 - Inherent conflicts with “normal” activities
 - “Need-to-Know” can be difficult for managers at all levels to accept

Case Histories

Case #1

- ⦿ Local business, worker accused of selling corporate secrets.
 - Company initiated
 - Law enforcement involved
 - Email held evidence; discussions, attachments
- Employee terminated, later convicted.

Case #2

- ⦿ University, Student assistant suspected of downloading massive amounts of pornography on campus computer; Department requests assistance to:
 - Rule out illegal (child) pornography
 - Discipline student for misuse of campus resources and productivity issues associated with obvious hours spent with “non-work” activity
 - continued

Case #2 (continued)

- ◎ System retrieved, data confirmed that:
 - No illegal/child pornography found
 - Number and size of files = HOURS spent doing so

BUT....

Files were CONSISTENTLY downloaded, moved etc. During hours of the day when Student was not present. Student A was exonerated, Student B confessed and was disciplined by department supervisor.

Case #3

- ◎ University Department Server: Network activity maxed and sustained.
 - Initial response indicates system was hacked from outside the network and turned into a porn server.
 - Law Enforcement (FBI) becomes involved, but department requested server be quickly returned to service, so drive was wiped and rebuilt.
 - FBI was not happy about that.

Case #4

- University employee arrested for public indecency and possession of child-porn. Two counties involved (arrest site and employee's home county, where more evidence was found)
 - IT department received two requests; Law Enforcement to gather more possible evidence, and the employee's department to ensure university systems are free of any illegal data.

Case #4 (continued)

- ◎ Several shared-PC's checked:
 - No illegal files found

Local Law Enforcement was saddened to be left out of the high-profile case, but the University department was glad to be uninvolved.

Case #5

- ◎ Network engineers detects possible “port scanning” on University network.
Chain of events:
 - Technician visits location of suspect PC.
 - When he requests user enter screensaver password to look at “virus” activity, user hurriedly unplugs PC, shutting down the scan.
 - When technician asks user’s supervisor for permission to check the PC, the user becomes argumentative, Tech leaves area.

Case #5 (continued)

- User's supervisor later delivers PC to IT department, but user had reformatted the drive.
- Technician begins data-copy for possible investigation.
- While the technician is out for another call, User comes to IT department, successfully demanding return of the PC.

Investigation halted, possible hacking attempt unresolved.

What have we learned?

Forensics is inherently a HIGH-STAKES game.

This is IT at it's most personal.

Everything else is data, money, time....

But **Forensics can ruin lives.**

ANY weak-link can cause the system to fail, especially in the beginning.

Case can start several ways, but must begin "best practice" as early as possible.

Issues of Concern

⦿ Security

- Physical
- Legal
 - Personal Liability
 - University Liability
- Career
 - “stepping on toes”
 - IT department politics

Security; Legal

- Obtain proper authorization through University Legal Office before each step.
 - All correspondence IN WRITING; Email or hardcopy.
 - Make no assumptions. Stay within authorized power. If in doubt, ask for clarification.
 - Personal Legal concerns. If in doubt, confer with an independent lawyer or refrain from action. There is no Nuremberg Defense!

Security; Legal

⦿ Liability issues

- Need-to-know; Gossip can create it's own legal problems, regardless of original case.
- Right-to-Privacy; Precedents have gone both ways
- Personal Liability must be considered a completely separate concern from University Liability!

Document everything (covered more later)

Security; Physical

- ⦿ Visiting suspect-site:
 - NEVER stay any longer than necessary; take system to secure location
 - Follow Need-to-Know practices
 - 2 technicians ALWAYS!
 - Do not hesitate to bring Law Enforcement if necessary
 - If situation escalates, leave the area

Security; Physical

- ⦿ Controlled work-environment
 - Limited access
 - Unpublished location
 - Secure storage of system and documentation

Security; Career

- ⦿ Because of the high-stakes nature of Forensics, it flies against everything we normally desire in IT; timeliness, transparency, convenience and the regular “chain of command” of management control.
- ⦿ Technicians may have to snub managers, managers may have to snub their superiors or other department managers.

Security; Career

- Need for Universal Buy-In. Everyone in the process MUST agree to established roles, responsibilities and (most importantly) restrictions.

Keys to Success: Forensic Best-Practices

- Consistent methods established by Experts in the field, have been successfully used in courtroom prosecution and legal defense.
- Changes occur regularly as technology, crime and legal precedents evolve.

Best Practices

Equipment

Documentation

Method

⦿ Equipment

- Write-blocker
 - Hardware adapter
 - Prevents ALL write actions
 - (Modified date etc)
- Forensics Utilities
 - Linux and windows
- Secure storage
 - Safe
 - Evidence bags
 - Locking cabinet
- Secure work area
 - Limited and *accountable* access
 - Free from internal and external interference

Best Practices

Equipment

Documentation

Method

- ⦿ Documentation: “Your Best Friend”
- ⦿ Pre-made:
 - Initial Request Forms
 - Release Forms
- ⦿ Log Books
 - COMPLETE Chronology
 - Date, Time, Contact, Actions, Results
 - Mistakes, Re-tries, Deviations from standards are still OK as long as actions and reasons are fully accounted for.

Best Practices

Equipment

Documentation

Method

- ◎ This Page Unsuccessfully Left Blank.

Method

- ⦿ Disclaimer- this is the WSU established practice. Each University should consult their own Legal Office for approval.
- ⦿ Step 1: Request is made for investigation.
 - Regardless of source (IT, Department Chair, Law Enforcement) the request must be referred to Legal Office for approval.

Method

- ◎ Legal Office approves request in writing.
 - Approval documented and secured
 - Approval should note; Reason for request, sources to obtain, personnel involved, actions to pursue.
 - Resources may include:
 - Personal Computer
 - External Drives
 - Network files and/or email history

Method

- ◎ Step 2: Obtain Objects of Investigation
 - 2 technicians (plus Law Enforcement?)
 - Keep it short, keep it quiet
 - “soft-sell” and “need-to-know” during visit
 - Get signed release form from controlling authority if appropriate
 - Document everything, tag all items taken

Method

- ① Step 3 and Beyond... Investigating.
- ① Create complete image of the hard drive to use for data search
 - Create images for all resources (CD's, Thumb-drives etc.)
 - Original drives etc. promptly locked in safe
 - Images can be used over and over without danger to original evidence.

Method

- ① Use images to search for evidence
 - Document everything done, everything found
 - Relevant file names, locations
 - Dates (created, modified etc.)
- ① Forensics Utilities can find hidden files, deleted files, file fragments; Beyond the scope of this presentation!

Method

- Wrap-up: Present findings to authorized parties and Legal Office.

*May be asked to perform later duties:
Affidavit, Court summons etc.

Reference

- ◎ SANS training institute
 - Training, Journals, Forums
 - Sans.org
- ◎ Infragard
 - FBI, national infrastructure
 - Networking and information sharing
 - Many local chapters
 - Infragard.net

- ◎ Thank you!