



E-Discovery & Fraud, Abuse Details

Randy Marchany, VA Tech IT Security Office

10/9/2009



Background

- We've become a litigious society
- Criminal and civil lawsuits require “evidence” that needs to be collected and analyzed
 - We've had a lot of practice ☹️
- Need to clearly define who “collects” and who “analyzes”



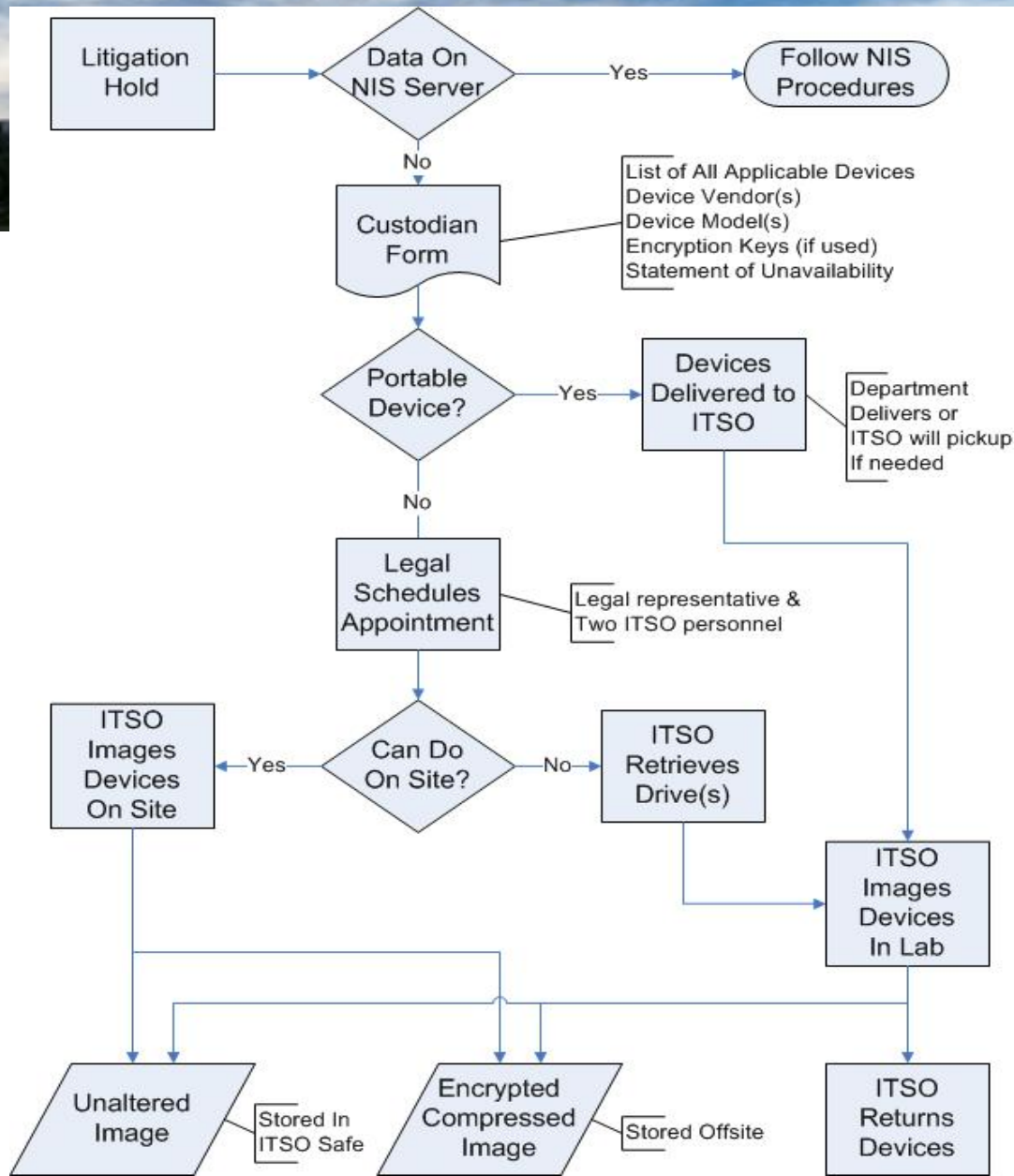
Who Wants the Data?

- University Legal
 - E-discovery for pending or potential lawsuits
 - Data from desktop or laptops only, no analysis done by ITSO
 - Data sent to Servient for processing
 - Data on Central NAS collected by Systems Group
 - Data sent to Servient for processing



Who Wants the Data?

- University Internal Audit
 - Fraud and Abuse investigations
 - Data collection from laptops, desktops only
 - Some forensic analysis based on IA requests
 - Results sent to IA





Get a Clue (Plan)

- Preservation and Collection
 - Locate potentially relevant docs
 - Need data and metadata (file creation, attributes, etc.)
 - Answers the “who knew what & when”
 - Quarantine them
 - Group them together for analysis
 - Throw out what you don’t need



Get a Clue (Plan)

- Processing Stage
 - Use keywords, dates, ownership to reduce the # of files required
- Review & Production
 - Tag the documents for review
 - Most important
 - Most expensive



E-Discovery Preparation

- Legal memo asking specific info for ITSO
 - [Data Custodian Form](#)
 - list all computer and storage devices that Legal wants
 - Vendor, model
 - Provide any encryption keys
 - Statement of Unavailability
 - Systems will be unavailable for up to 2 days



E-Discovery Preparation

- Systems will be powered off
- Disk Image rough time estimate: **1GB/minute**
- Drop off instructions
- Laptops, storage devices or portables
- Dept person drops this off hand delivers to ITSO
- Desktop, Server
- ITSO visits to assess what needs to be done.



Disk Imaging Checklists

- [Offline Hard Disk Imaging Checklist](#)
- [IT-SOP-Data-Collection-Diagram](#)



Data Collection & Preservation

- **1. Introduction**
- **A. Purpose & Scope**
 - This document denotes the recommended “Standard Operating Procedures” (SOP) to be used by Virginia Tech I.T staff involved in data collection and preservation activities related to regulatory or litigatory compliance and/or for personnel actions.
- **B. Definitions**
- **C. Responsibility for document**
- **D. Frequency of publication**
- **E. Information Technology Security Office**



DC&P Guide

- **2. Information Technology Guidelines for collecting electronic data**
 - Data for e-discovery and litigation purposes
 - First Steps
 - Details
 - IT Security Office Data Collection Flowchart
 - Litigation Flowchart
 - Internal Audit or H.R. Policies Chart
 - Criminal Investigations Chart



DC&P Guide

- **3. Policy Links**
- **4. Centrally Managed Storage and Backup Systems**
- **5. Glossary of Terms**
 - **Appendix A: Authorization to Release Information form**
 - **Appendix B: Sample Interview Questions**
 - **Appendix C: Equipment Retrieval Form**
 - **Appendix D: Disk Imaging Form**
- [VT IT SOP for Data Collection Guide](#)



ITSO Fraud & Abuse Process

- IT Security Office primary contact
- Some forensic analysis
 - Recover deleted files
 - Search for specific files
- Coordinates with E-discovery group



ITSO Fraud & Abuse Process

- [Imaging Request Form](#)
- [Equipment receipt form: \(equipment dropoff and pickup\)](#)
- [Image in Progress Form](#)
- [Disk Image Analysis Form](#)

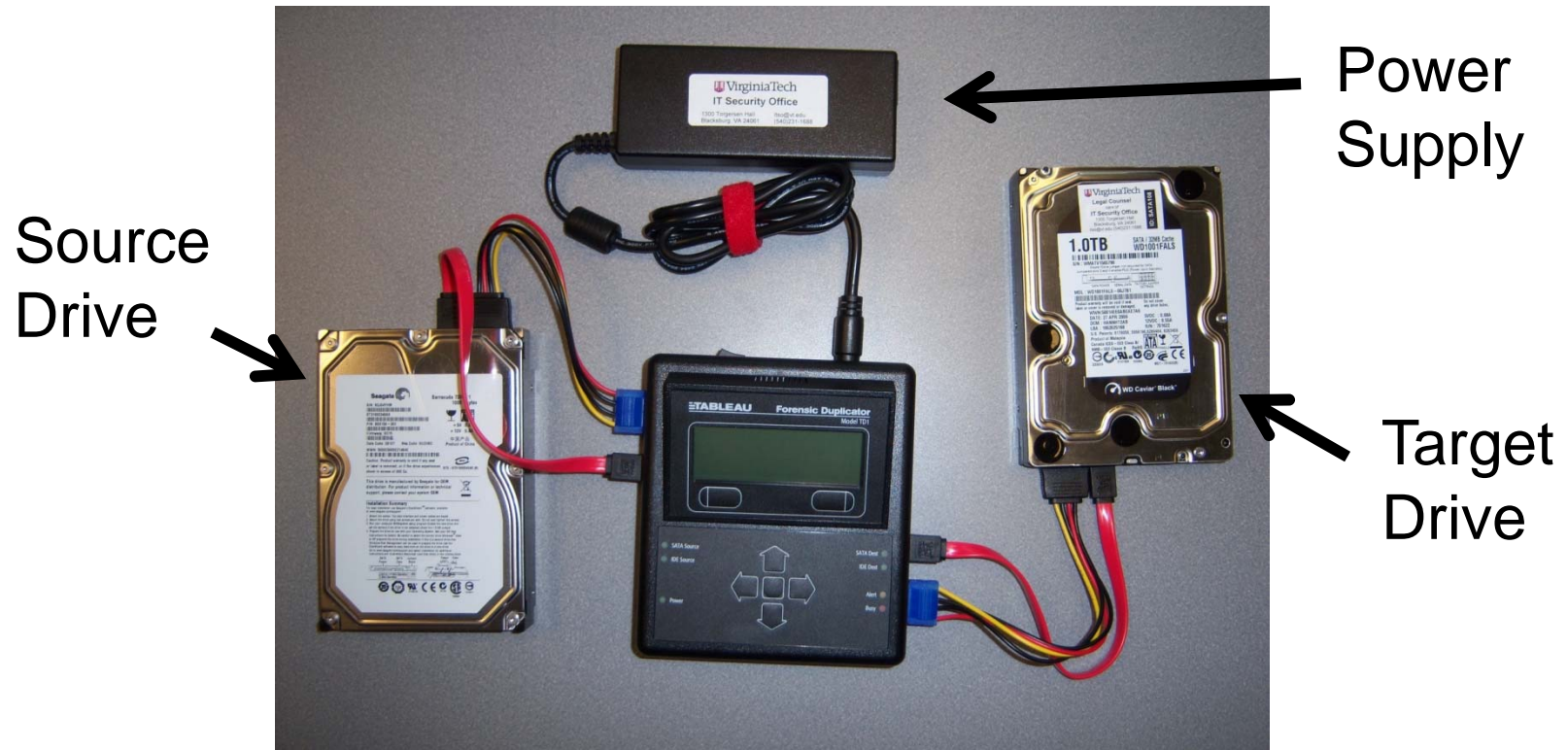


Some Statistics

- ITSO
 - 19 e-discovery
 - Some with analysis
 - 4 fraud & abuse investigation
 - 1 required overnight stay
 - Analysis: recover deleted files or search for specific filetypes
- Systems Group
 - ~200 E-discovery (4/16/07 related)
 - ~50 E-discovery (other)



Disk Imaging Hardware





Disk Image HW Travel Case



Adapters

- IDE
- Serial ATA



Incident Response Jump Kit

- Write-blocking Set & following adapters
 - Parallel ATA: 3.5”, 2.5”, 1.8” hard drives
 - Serial ATA
 - SCSI: 50-pin, 68-pin, 80-pin
 - USB drives
 - Firewire
 - Memory cards
 - Read / write ATA adapter for target drive
 - Blank 250GB ATA (IDE) 3.5” hard drive



IR Jump Kit Contents

- Dual boot Laptop PC (Windows, Linux)
 - 2GB memory
 - Common software installed such as Office and networking tools
 - Network data logger
 - ATA, SATA, 2.5” hard drive to USB adapter (read / write)
 - Multiple format memory card reader (read / write)



IR Jump Kit Contents

- 10/100 Ethernet tap
- Ethernet cables – short and long
- 120GB 2.5” USB drive
- 1GB USB flash drive
- USB floppy drive
- USB DVD±RW d



IR Jump Kit Contents

- Surge Protector
- Portable printer with battery
- Hand tool kit
- 8-port Ethernet hub (repeater)
- AUI – 10BaseT transceiver



IR Jump Kit Software

- Encase
- Helix CD, BackTrack CD, SANS 504 CD
- Ghost CD, Nero CD, printer driver CD
- Blank CDRs and DVDRs



Passive Ethernet Tap



Network Data Logger





Thoughts & Observations

- E-discovery consumes all
 - **TIME** consuming
 - **Resource** consuming
 - Unknown # of systems: 1-150+
 - Staff time, disk drives
 - **Unpredictable** scheduling
 - We never know when a request comes in
 - Legal Counsel sensitive to this dilemma



Thought & Observations

- Internal Fraud & Abuse
 - **TIME** consuming
 - **Resource** consuming
 - Disk drives, staff time
 - **Unpredictable** Scheduling
 - May require overnite stays at remote sites
 - High priority

A wide-angle photograph of the Virginia Tech campus. In the center, the iconic Campanile tower stands tall against a blue sky with light clouds. The foreground is filled with green grass and several trees with autumn-colored leaves in shades of yellow, orange, and red. Other campus buildings are visible in the background.

Thoughts & Observations

- Prepare checklists
- Train your staff
 - Get certified, for example GIAC GCFA
- Develop rapport with Internal Audit, University Legal, Campus Police



Contact Info

- Randy Marchany
 - Director of IT Security Lab,
marchany@vt.edu
- William Dougherty
 - Director of Systems Support and
E-Discovery, william@vt.edu
- <http://security.vt.edu>



What do we do

- Legal counsel gives us a list of targets
 - We make disk images of their computers
- We give the imaged drives to Legal
- We do NO analysis
 - We just copy the bits



E-Discovery: Org Chart

- Data can be on individual hosts or central NAS
- William Dougherty – Director of E-discovery
 - Lead for e-discovery operations
 - ITSO provided some support