



Creating Digital Advantage™

Forensics Investigation

With John Auman

Steps for a Successful Forensic Acquisition and Examination

- Plan
- Acquire data
- Analyze
- Report



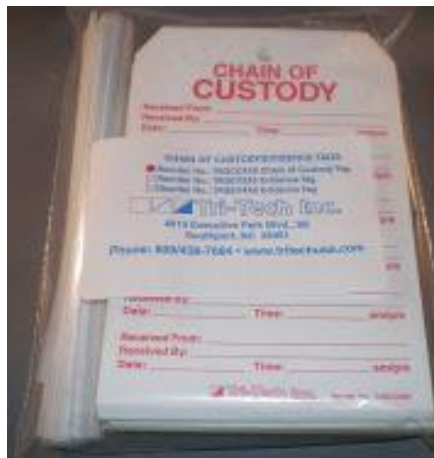
Planning

- Preparation
 - Prepared storage media, equipment, scope of work
- Processes
 - Digital Forensics - an applied science, repeatable results
 - Proven methods, will withstand scrutiny
- Hardware/Software
 - Specifically designed for Forensics work
 - Encase, Forensics Tool Kit, Solo-III



Acquisition

- Preparation
 - Computer literacy
 - Legal authority
 - Tool capability
 - Availability of people and equipment
- Preservation
 - Checking for activity
 - Shutdown
 - Physical exam and documentation
 - Packing, storage and transport
 - CHAIN OF CUSTODY



Acquisition Continued

- Duplication
 - Authenticate Original Evidence (MD5 Hash)
 - Duplicate Evidence
 - Authenticate Duplicate
 - Re-authenticate Original Evidence
- Document
- Working Image Copy



Support Role in E-Discovery

- Export
- Processing
- Review
- Production
- Information Governance



Examination

- Pre-Examination
 - Forensic workstation preparation
 - Image verification
 - Image conversion
 - Recover/Undelete files
 - Verify file signatures



Examination Continued

- Owner
- User identification
- User agreements
- Recovery of deleted files/folders
- User profile and registry settings
- Timeline of events
- Internet history and artifacts
- System log files
- Installed applications

Examination Continued (2)

- Data wiping activity
- File review
- E-mail
- Attached devices
- Keyword searching
- Custom scripting
- Export of relevant files and/or artifacts

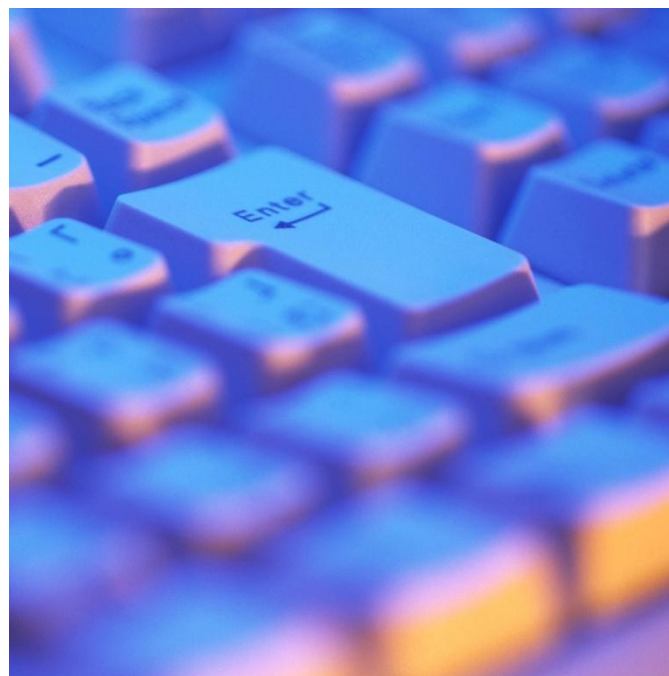


Reporting

- Who conducted the acquisition and examination
- What information is thought to be contained in the evidence items
- What items of evidence were examined
- Which tools were used to conduct exam
- What digital evidence, proving or disproving the allegation, was found

Keys to Success

- Documentation throughout the process is paramount
 - Imaging
 - Chain of Custody
 - Exam report
- Knowledge
- Experience
- Defensible process
- Usefulness of results



Example-Project Book

- Publishing company
- IPO within 1 month
- Concern surfaces that sales is “padding” numbers
- VERY confidential matter

Project Book

- 20 laptops
- Covert operation
- Worked with General Counsel and outside Investigator on needs of the investigation
- Determined no padding occurred
- Sales force never knew what happened
- IPO went off without a hitch

Need Information?



411 N Central Ave, Suite 170
Phoenix, AZ 85004
602.992.3600

