

Computer Forensics In the Inspector General Environment



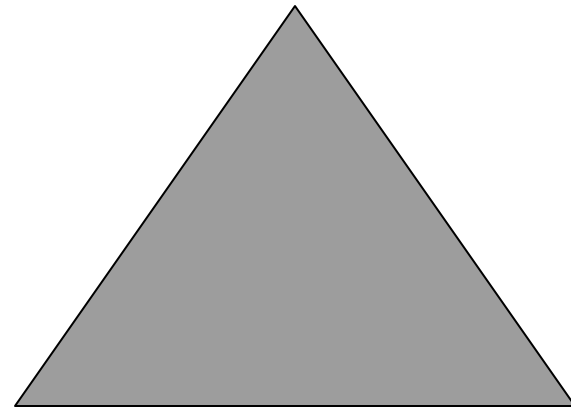
Inspector General

What is it?



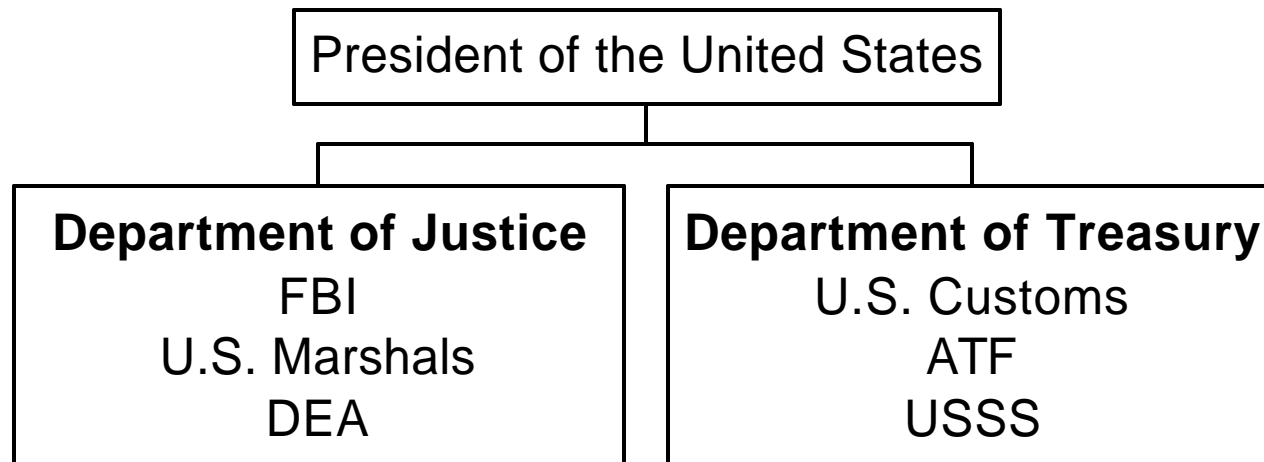
United States Government

- Three Branches
 - Executive
 - Legislative
 - Judicial



Executive Branch

- Departments
 - Agencies



- Each agency is responsible for elements of the United States Code of Laws (Jurisdiction).
- No one watching the overall Department
- Major multi-hundred million dollar fraud against a federal department in early 1970's



Congress passed
The Inspectors General Act
in 1978



Inspector General Investigations

- Fraud
- Waste
- Abuse, and
- Mismanagement



United States Postal Service

- 800,000+ Employees
- 32,000+ Facilities in the States and Territories
- Annual Revenue \$63 billion
- Extensive use of computers and digital equipment in all phases of operation
- The use of computers and digital equipment will continue to increase



**Investigations in our
environment tend to
generate large data sets
from multiple computers
and/or storage arrays.**



Time is the Enemy!

- Services must be timely in order to add value to the investigation
- Speed the processing and analysis of data sets with automated tools and processes



Computer Forensic Tools

- Commercial (COTS) Tools
 - “All-in-One” Tools
 - Guidance Software’s Encase
 - iLook
 - AccessData’s FTK



Computer Forensic Tools

- Restricted Access Tools
 - “All-in-One” Tools
 - FBI ACES



Computer Forensic Tools

- Commercial (COTS) Tools
 - “Specialty” Tools
 - NTI (New Technology Inc.) Tools
 - Maresware Tools
 - AccessData Tools
 - Data Sniffer



Computer Forensic Tools

- Restricted Access Tools
 - RCMP Utilities
 - Hashkeeper



Computer Forensic Processes

- Self contained processes
 - “All-in-One” Tools
- Constructed processes
 - Developed using a mixture of specialty tools and “all-in-one” tools



Computer Forensic Processes

- USPS-OIG constructed process
 - On the restored image
 - Identify and separate to specific folders on the “storage drive”
 - data in unallocated space
 - data in slack space
 - data in swap file(s)
 - Using NTI programs



Computer Forensic Processes

- USPS-OIG constructed process
 - Using a restored image
 - Calculate the MD5 hash of all files using Maresware program
 - Identify matching and non-matching files using Hashkeeper program
 - Remove matching files using Maresware program to reduce size of data set



Computer Forensic Processes

- USPS-OIG constructed process
 - Using a restored image
 - using Maresware programs within a single batch file
 - copy files (based on file extension) to “category” folders on the storage drive with complete paths
 - catalog all files copied
 - remove copied files from restored image



Computer Forensic Processes

- USPS-OIG constructed process
 - Using a restored image
 - using Maresware programs within a single batch file
 - copy remaining files to “remain” folder on the “storage” drive with complete paths
 - catalog all files copied
 - remove copied files from restored image



Computer Forensic Processes

- USPS-OIG constructed process
 - Using a restored image
 - using Maresware programs within a single batch file
 - a final catalog is run on the restored image to insure all files have been copied and removed from the restored image



Computer Forensic Processes

- USPS-OIG constructed process
 - analysis of results
 - “all-in-one” tools are then used to analyze the files on the “storage” drive
 - “keyword” searches are completed



Computer Forensic Processes

- USPS-OIG constructed process
 - analysis of results
 - files such as word processing, spreadsheet, graphic, and html are exported to CD and forwarded to case agent for review



Computer Forensic Processes

- USPS-OIG constructed process
 - analysis of results
 - specialty programs are run on the unallocated space, slack and swap data



Computer Forensic Processes

- USPS-OIG constructed process
 - Advantages
 - quickly eliminates files that do not require analysis
 - reduces data sets to more manageable sizes



Computer Forensic Processes

- USPS-OIG constructed process
 - Advantages
 - allows offloading of some files for review by case agents
 - have better knowledge of case



Computer Forensic Processes

- USPS-OIG constructed process
 - Disadvantages
 - requires ownership of several programs in addition to “all-in-one” program
 - time (+/-)



Computer Forensic Processes

- USPS-OIG constructed process
 - Planned future enhancements
 - Porting the entire process to a Linux based platform
 - enhancement to the new “Linux Deluxe” to allow for operation on Alpha 64 bit processors



QUESTIONS



Computer Forensics

Michael P. Everitt

Special Agent

United States Postal Service

Office of Inspector General

703-248-2387

meveritt@uspsoig.gov

www.uspsoig.gov

