

**SWG-DE**

Scientific  
Working Group -  
Digital Evidence

# SWG-DE Mission:

**The mission of the Scientific Working Group - Digital Evidence is to establish and promulgate accepted forensic guidelines and definitions for the handling of digital evidence.**

**(SWG-DE 6/16/98)**

# Goals

- Standards for exchange of evidence
- Development of standard vocabulary
- Seek to prevent conflict between disciplines

# Digital evidence:

- is information of probative value stored or transmitted in digital form (SWG-DE 7/14/98)
- is acquired when information and/or physical items are collected and stored for examination purposes. (SWG-DE 8/18/98)

# Evidence types

- **Original digital evidence** - physical items and all the associated data objects at the time of acquisition

## Evidence types cont.

- **Duplicates** - an accurate reproduction of all data objects independent of the physical item
- **Copy** - an accurate reproduction of the information contained in the data objects independent of the physical item.

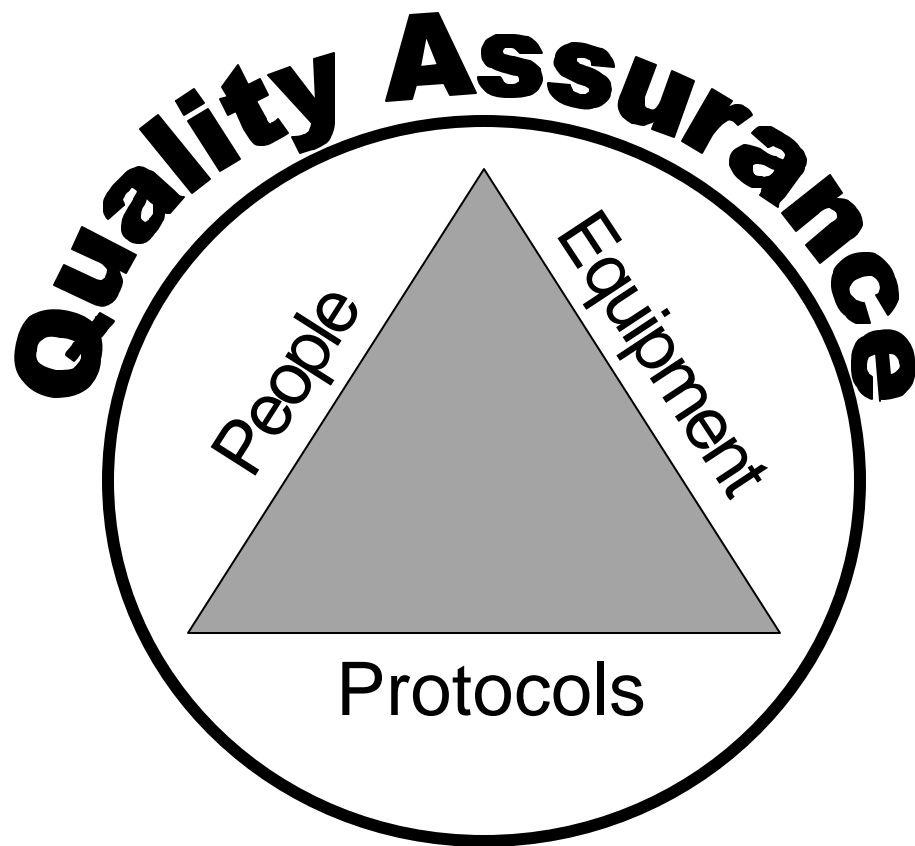
# Evidence Handling

- ANY action which has the potential to alter, damage or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner (SWG-DE 3/12/99)

# SWG-DE

- Is discipline independent
- Seeks to promote the forensic handling of digital evidence
- Encourages the development of sound systems of forensic practice and service

# Forensic Model



# Accomplishment: Outreach

- 1999 IAFS Meeting
  - 1st Digital Evidence Section
  - SWGDE Workshop “Developing a Digital Evidence Program”
- SWGDE Principles Presented to IOCE
- Jan 2000/June 2000 SWGDE Road Shows
- Feb. 2000 AAFS Workshop
- Sept. 2000 ASCLD Workshop
- Fall 2000 ASCLD/LAB Accreditation Discussion

# Accomplishments: Standards

- 1998 SWGDE Definitions
- 1999 SWGDE Digital Evidence Principles published in [www.fbi.gov/fsc/backissu/april2000/swgde.htm](http://www.fbi.gov/fsc/backissu/april2000/swgde.htm)
- 2000 ASCLD/LAB Accreditation Format
- 2000 Digital Evidence Glossary (cross-discipline)

# What standards?

- Definitions
- Principles
- Processes
- Outcomes
- Common language

# Works in Progress

- Glossary of Digital Evidence Terms
- Standard Format for Seizure/Examination Requests and Returns
- Development of examination protocol standards
- Proficiency test criteria

# Works in Progress

- NIJ Software Reference Library
- NIJ Forensic Software Validation Project
- Forensic Software Developers Symposia in Conjunction with 6th IOCE

# National Cybercrime Training Partnership (NCTP)

- US Department of Justice (DOJ)
- Computer Crime and Intellectual Property Section (CCIPS): Manages NCTP
- National White Collar Crimes Center (NW3C) : Operational Support
- Courses in Basic and Advanced Data Recovery; Internet as an Investigative Tool

## For further info:

- Mark Pollitt FBI (202) 324-9307
- [mpollitt@leo.gov](mailto:mpollitt@leo.gov)
  
- Carrie Whitcomb, (407) 823-6469
- [whitcomb@mail.ucf.edu](mailto:whitcomb@mail.ucf.edu)
- NCTP [www.cybercrime.org](http://www.cybercrime.org)