National Commission on Forensic Science

Digital & Multimedia Evidence Panel

Accreditation - State/Local Perspective

Jim Dibble, President

International Association of
Computer Investigative Specialists

CERTIFIED FORENSIC COMPUTER EXAMINER
IACIS

IACIS
The International Association of
Computer Investigative Specialists

CERTIFIED FORENSIC COMPUTER EXAMINER
IACIS

International Association
of
Computer Investigative Specialists

Introduction

- 20 years US Army Criminal Investigation Command (Warrant Officer)
- 22 years Washington State Gambling Commission (Special Agent)
- 36 years law enforcement
- 12 years digital forensic examiner
- Certifications:
  - Certified Forensic Computer Examiner (CFCE)
  - Seized Computer Evidence Recovery Specialist (SCERS)
  - Cellebrite Certified Logical Operator (CCLO)
  - Cellebrite Certified Physical Analysts (CCPA)
  - Certified Fraud Examiner (CFE)

What problem are we trying to solve?

Why has Digital Evidence been swept up in the accreditation of traditional sciences?

- 2009 NAS Report
- Are DF examiners actually performing a scientific or an investigative activity?
- At what point does investigative activity become a scientific (forensic) procedure?

What problem are we trying to solve?

Are current digital forensic units doing an improper job of handling and reporting data?

If so, would any of the “issues” have been prevented if the examiners were in an accredited lab?

What remedies already exist?

- Organizational Policies/Procedures
- Legal System
- Certification

ASCLD-LAB’s Digital Evidence

Sub-Disciplines

Computer Forensics

Forensic Video

Image Analysis

Forensic Audio

Define Digital Evidence?

- Mobile phone extraction and analysis?
- Automobile infotainment system data?
- DDOS attacks to businesses or critical infrastructure?
- Manufacture and distribution of Child Pornography?
- Cyber intrusion and Intellectual Property theft?
- E-mail threats?

Mandatory Accreditation

Positives:

- Force examiners to develop and adhere to written policies regarding handling and processing digital evidence
- Mandate continuing professional education
- Provides the “appearance” of quality, credible work

Mandatory Accreditation

Negatives:

- Technical review for “one examiner” forensic units difficult if not impossible
- Does not necessarily address training or examiner qualifications

  This is up to each lab – does not guarantee quality examiners
- Those who believe accreditation will increase public confidence are only getting a false sense of protection. Accreditation does little (if anything) to enhance or ensure the examiners skills.

State & Local Perspective

- 12,501 Local Police Departments
- 3,063 Local Sheriff's Departments
- IACIS has over 1900 current certified examiners
  - 500+ are single police/sheriff examiners
- Majority of digital forensic exams done in 1-2 person digital forensic units

Accreditation Issues

- Labs write their own policies and training requirements

- If DF units aren’t trusted to do their job now (thus the need for accreditation), can they be trusted to develop their own policies?

Accreditation Issues

Personnel Selection

- Sworn vs Civilian
- Full-time vs Part-Time

Accreditation Issues

- Significant policy/procedure variations between DFU
- Onerous costs of implementing/maintaining accreditation
- Current evidence turnaround time

Accreditation Issues

There will be fewer departments processing digital evidence

- Backlogs on state (accredited) labs will grow exponentially
- Dramatic increase in turnaround time

Many supporters of accreditation come from large or regional labs.

- Different perspective from smaller agencies
- Accreditation can be invaluable, it just isn’t appropriate for all departments

Federal legislation will be pushed to state/local labs

- Grants withheld (ICAC/Economic Crimes Task Forces)
- State legislatures tend to emulate federal requirements

How to Strengthen Digital Evidence?

- Focus on minimum training standards for all examiners.
- Focus on minimum certification standards for all examiners
  - Vendor neutral, published competencies, code of ethics, periodic re-certification requirements
- Establish curriculum for undergraduate/graduate degrees
- Focus on the individual performing the examination and not the facility or organization where the examination is performed.

How to Strengthen Digital Evidence?

If accreditation is mandated:

- Consider suitable alternatives to ISO 17025:
  - ISO – 17020 ?
  - ISO – 27035 ?
  - ISO – 27041 ?
  - ISO – 27042 ?
  - ISO – 27050 ?

Recommend NCFS task the SME's to develop a digital evidence accreditation standard that truly reflects the digital forensic discipline?

How to Strengthen Digital Evidence?

If accreditation is mandated:

- Implement limitations:
  - Larger labs/units (10 or more examiners)
    - Organizations that can absorb the resource/overhead costs

How to Strengthen Digital Evidence?

If accreditation is mandated:

Smaller labs/units (Less than 10 examiners)

- Accreditation optional
- Training requirements based on core competencies
- Certification required
  - Vendor-neutral certification to core competencies
  - Periodic recertification, professional education and proficiency testing
  - Accredited “independent” certifying bodies

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

IACIS
The International Association of
Computer Investigative Specialists

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

International Association
of
Computer Investigative Specialists