



# Why Certify?

Doug White

PhD, CCE, CISSP, PI(RI)

ISFCE.ORG

Roger Williams University

# Traditional Reasons

- Daubert vs. Frye
- Daubert allows for experts to be admitted in court based on the trial judge's opinion that they will contribute to the case.
- Daubert doesn't really require anything more so normally widely accepted certifications may qualify you as an expert.

# Modern Ideas

- Today, there is a greater focus on forensics as a skill set than as a traditional expert witness.

# ISACA.ORG

- COBIT Best Practice Guidelines
- G28 – Computer Forensics (all in part)
  - 1.3.2 – The foremost aim of computer forensics is to establish the truth behind a particular situation by immediately capturing data to identify an attacker and establish proof for criminal proceedings to aid law enforcement...
  - 1.3.3 – During the conduct (sic) of computer investigation, it is critical that confidentiality is maintained and integrity is established for data and information gathered and made available to appropriate authorities only...
  - 1.3.4 – Computer forensics involves the detailed analysis of events in cyberspace and collection of evidence...

# So we need to add

- Adherence to professional, ethical, legal behavior in the acquisition, observation, and maintenance of digital evidence.

# The focus on audit

- More frequently, corporate entities are now being scrutinized for IT Security, Practice, and Behavior.
- It is more common to see auditors evaluating individuals credentials to determine their effective skill set
- It is also more common to see individuals wishing to capture their advanced skills via certification for both validation and community.

# Case Example

- I received a contact via my name
- The contact wanted an examination of a variety of systems
- I coordinated this acting as a kind of GP and via the cce board was able to recruit and retain two different specialists to focus on specifics of the problem, e.g a minicomputer and an MACBOOK which needed analysis.

# Certifications Related to Forensics

- Certified Computer Examiner – ISFCE.ORG
- GCFA – SANS.ORG
- CFCE – Certified Forensic Computer Examiner – IACIS.ORG
- There are others, of course

# Some key criteria I like to see

- Vendor Neutral – It seems that if you focus on a product the more the training/skill set is about the product feature set.
  - I don't discourage this, if you are using a tool, being an expert in the tool is absolutely beneficial.
- Ethics Review Boards – I focus on this because it creates a punitive outcome for unethical behavior. This creates a kind of Hippocratic oath situation for professionals that supercedes the organization.

# Key Certification Criteria

- **Skill/Practically Based** – Certifications which focus on the ideas underlying the discipline seem to be more beneficial than terminology and/or simple concepts.
- **Non-Persistent** – Certifications in dynamic fields should focus on continual assessment of skills rather than persistent approval.
- **Strong Community** – This provides both behavior reinforcement and resources to the practitioner.

# So, why certify your specialists?

- Validation -- Provide proof of your skillsets
  - Audit
  - Court
  - Internal Evaluation
- Veracity – Ensure behavior via multiple paths
  - Ethics in both internal and external views
  - Kohlbergian Preconventionalism
- Value Added – Provide resource access via communities of experts

# Peripheral Reasoning

- Privacy
  - State Statutes and Private Investigation Problems
  - Skill/Knowledge Base
  - Ethics again
- Continuous Improvement
  - Retraining/CPE approach

# Slides and Info

- [www.whitehatresearch.com](http://www.whitehatresearch.com)
- [Doug.white@acm.org](mailto:Doug.white@acm.org)
- **(646) 485-5502**