FORENSIC CHALLENGES IN THE COURTROOM PANEL:

GARY C. KESSLER
CHAMPLAIN COLLEGE
VERMONT ICAC
+1 802-865-6460 (office)
+1 802-238-8913 (mobile)
gary.kessler@champlain.edu
http://msdim.champlain.edu
http://www.garykessler.net

Question

- Rank order the following digital forensic attributes: analysis skills, acquisition skills, data recovery skills, report writing skills, law enforcement background, computer science background, problem solving skills, integrity, caution. Which one is most important/least important? Why did you rank them this way?

Question Answered By Gary C. Kessler

- B.S., Mathematics; M.S., Computer Science; Ed.S., Computing Technology in Education; CCE; CISSP
- Associate Professor and Program Director, M.S. in Digital Investigation Management program
  - Started undergraduate programs in Computer & Digital Forensics (2003) and Information Security (2005)
- Member of Vermont Internet Crimes Against Children (ICAC) Task Force since 2000
  - Primary role is mobile device examinations, public outreach, and law enforcement training
- El Presidente y conserje, Gary Kessler Associates
  - Computer forensics (civil) and information security consulting and training
- Frequent speaker at conferences and other events (HTCIA, Techno, DoD Cybercrime, MFW)
- Two book & >70 articles and papers
- *Journal of Digital Forensics, Security and Law; Journal of Digital Forensic Practice; Digital Investigation*

Answer

- Choices provided:
  - analysis skills
  - acquisition skills
  - data recovery skills
  - report writing skills (which I will expand to *communication skills*)
  - law enforcement background
  - computer science background
  - problem solving skills
  - integrity
  - caution
- Choices that I added:
  - *curiousity*
  - *technical astuteness*
  - *tenacity*

Answer

Here's a rank ordering because Rob told me to:

1. integrity
2. *technical astuteness*
3. *curiousity*
4. problem solving skills
5. analysis skills
6. *tenacity*
7. report writing skills/*communication skills*
8. acquisition skills
9. data recovery skills
10. caution

11. computer science background
12. law enforcement background

Answer

Here's *some* rationale...

- Good computer forensics examiners need to be smart, technically capable, able to think like their adversary, aware of their limitations, persistent, and creative
- DF examiners need to be naturally inquisitive and life-long learners
- Good DF examiners need to be analytical, honest, and understand process
- Good DF practitioners need to able to communicate what they did, how, and why
  - We spend a lot of time "training" prosecutors, investgators, lawyers, judges, and juries
- Way too much is made about what people did before
  - Investigators and computer scientists are made, not born!!!
- Tenacity and curiousity are good attributes!
  - "I don't know, so I'm done" mentality vs. "I don't know, so I need another day or two" mentality