PANEL: LAW ENFORCEMENT

Ken Privette – Special Agent in Charge
Digital Evidence Services
USPS Office of Inspector General
Kprivette@uspsoig.gov
703.248.2173

Question

What is the biggest challenge facing law enforcement in digital forensics? How would you overcome this challenge?

Answer

Challenge – Digital Evidence Volume!

Question Answered by Ken Privette

- Ken serves as the Special Agent in Charge of Digital Evidence Services (DES), a component of the USPS Joint Mission Support Center. His team provides computer crime and digital forensics support to more than 2000 investigators from the United States Postal Service Office of Inspector General and Postal Inspection Service. He and his team of forensic examiners have pioneered state-of-the-art initiatives such as remote forensics and the development of forensic tools such as eInvestigator – an online forensic collaboration environment for sharing, parsing and searching digital evidence.
- Ken spent much of his professional life as a Special Agent with the Naval Criminal Investigative Service both overseas and state-side conducting investigations involving computer crime, terrorism, and counterintelligence matters. He has worked in assignments at the Department of Defense CERT and served as an instructor for the SANS Institute.

An Ocean of Data…

- Law Enforcement now deals with an Ocean of potential evidence
- Vast number of data formats
- Data may be dispersed
- More parameters to seizing the data
- The Game Changer – Encryption

Cultural Evolution –Triage Tradeoff

- Better Preparation for Search Warrants
- Compromises at the Search Site
- More Onsite Tools for Triage
- Remote Imaging – Triage real time

Cultural Evolution –Triage Tradeoff

- Greater Collaboration – Customer and Examiner
- Share out low level data
- Need Surge Capacity
- Need Online Environment – with low Training overhead