Working with Law Enforcement Panel

SA Paul J. Vitchock, Federal Bureau of Investigation, Washington Field Office

paul.vitchock@ic.fbi.gov

(703) 686-6760

Question

- What types of criminal cases involving digital evidence are you seeing a high number of?
- Why do you think that is?

Question Answered by Paul Vitchock

- Special Agent assigned to criminal cyber squads in Pittsburgh (2003-2006) and Washington (2006-present)
- Specializes in criminal computer intrusion investigations with current focus on Eurasian Cyber OC, but has worked Internet fraud, child pornography, and intellectual property rights
- Before FBI, spent 9 years in Washington, DC area working as a network infrastructure and security consultant and manager
- CISSP

Answer

- Child Pornography
  - Hard drives, thumb drives, CDs, DVDs
  - Highest number of evidentiary pieces and total storage capacity
- Why
  - Pedophiles are collectors
  - Warrant and consent are obtainable

Answer

- Botnets: Infected computers → C&C servers
  - First lead/IP: victim computer (bot)
  - Analysis: leads to C&C
- Why
  - Low risk, high reward $$$$
  - Point and click

Answer

- Parties to terrorist communications
  - Computers that are end or relay point
  - Majority IT
- Why
  - Priority, we are looking for it
  - Preference – security, anonymity