The BEST Forensic Technique... Ever!

Christopher E. Pogue, CISSP, CEH, CREA, QSA
cepogue@trustwave.com
Incident Response Panel
The Question?

- What techniques do you use in incident response that are the most reliable at helping solve cases?
Who am I?

- Senior Security Consultant, Trustwave SpiderLabs
- Former US Army Warrant Officer
- 11 + years of administrative and security experience
- Master’s degree in Information Security
- CISSP, CEH, CREA, QSA
- Author, “Unix and Linux Forensic Analysis”, Syngress
- Member of the HTClA Board of Governors
The Founder of the Feast

• Edmund Locard (1877 – 1966)
  – French forensic scientist (1877 – 1966)
  – Considered to be the “father” of modern forensics
  – Worked in the same lab with Forensic pioneer, Alexandre Lacassange in Lyon, France.
  – Techniques proved to be extremely to French Secret Service during World War I (1914 – 1918).

• Locard’s Exchange Principle
  – Summarized, states that when two items come into contact with one another, materials from each become visible on one another.
  – The is the inverse of the cause – effect principle.
  – Learn it, live it, love it!
Keep It Simple Stoopid

- The “Alexiou Principle”
- What question are you trying to answer?
- What data do you need to answer that question?
- Where does that data reside?
- What does the data tell you?
The BEST Forensic Tool EVER!!!
Questions???

cepogue@trustwave.com