Forensic Challenges in the Courtroom

Larry E. Daniel
Larry@Guardiandf.com

SANS INSTITUTE

Question Answered By Larry Daniel

- 27 years experience in programming, IT support, networks and servers, data recovery and network security.
- 7 years full time in computer forensics and cell phone forensics
- Specialization in criminal defense cases.
  - 20+ capital murder cases.
  - Over 200 cases in the last seven years. Mostly as the expert for the defense in criminal cases.
- Author of the Ex Forensis blog: www.exforensis.blogspot.com and the Digital Forensics Tool Reviews blog: www.digitalforensicstools.blogspot.com
- Host of the Talk Forensics internet radio show: www.blogtalkradio.com/talkforensics

Question

- IF YOU WERE WORKING THE DEFENSE ON A CASE, WHAT WOULD YOUR BASIC STRATEGY BE TO CREATE DOUBT IN THE PLAINTIFF'S DIGITAL EVIDENCE?

Answer

- Things to remember when working for the defense in a case:
  - Examiner expertise varies widely. (Julie Amero case)
  - Everyone makes mistakes.
  - Assume that if you can find it, they can find it. Don't get cocky.
  - Work closely with the attorney in the case to get the full story.
  - Get all of the discovery and READ IT THOROUGHLY.
    - This is especially critical in complicated criminal cases.
  - Take the role of scientist-educator when working with your attorneys.
  - Verify EVERYTHING.

Answer

- Things to avoid when working for the defense
  - The SODDI (Some other dude did it) defense.
    - This is weak and difficult to prove.
  - The Trojan Horse defense.
    - Puts the burden of proof on the defense. Should only be used when you are confident you can prove it.
  - Forgetting the principal of Occam's Razor.
    - The simple answer is probably the correct one.
    - Don't make up elaborate scenarios.
  - Attacking the other examiner instead of the evidence.
    - Shows that you have a weak case.
    - Can blow up in your (attorney's) face pretty fast.

Answer

- IF YOU WERE WORKING THE DEFENSE ON A CASE, WHAT WOULD YOUR BASIC STRATEGY BE TO INSTILL DOUBT IN THE PLAINTIFF'S DIGITAL EVIDENCE?
  - Always work the case like you are the primary examiner.
  - Never assume anything.
  - Check all the points in the case where mistakes are normally made:
    - Chain of custody.
    - Examination standard procedures.
      - RTC verified for all evidence containing clocks.
      - Evidence handling at the scene.
      - Was everything examined.
    - Claims made in the forensics report.
      - Pay particular attention to keyword search results, internet history results, link files, etc.
      - Placing the defendant at the computer.