FORENSICS PANEL:

Mark McKinnon
RedWolf Computer Forensics
Mark.McKinnon@RedWolfComputerForensics.com
Twitter: Markmckinnon

Question

- What are 2-3 major challenges that investigators now face or will face in the near future?

Question Answered By Mark McKinnon

- 19+ years in IT
- Masters of Science in Computer Science Emphasis in Software Engineering
- CCE
- Owner RedWolf Computer Forensics
  - Provide 15+ Programs used by Forensic Examiners around the world
    - Drive Prophet
    - Skype Log Parser
    - CSC Parser
    - Chrome, Firefox, Flock Browser Parsers
    - Etc…
- Blog – http://cfed-ttf.blogspot.com
- Twitter – markmckinnon
- The "Tool" – Quoted by Rob Lee, Forensic 4Cast Podcast Episode 16

Answer

- *New Technology (Hardware and Software)*
  - *Game Consoles (Nintendo Wii, Dsi, Ps3)*
  - *Google Wave*
  - *Windows 7 and Vista*
    - *Windows Search*
    - *Shadow Volume*
    - *Etc….*
  - *Cell Phones*
    - *Android*
    - *iPhone*
  - *Browsers*
    - *Incognito Mode or Private Mode*
  - *Social Networking*
  - *Upgrades of Existing Programs*

Answer

- *Understanding of Technology (New and Old)*
  - *How does something work*
    - *What does it mean to my investigation*
    - *What data points exists*
    - *What are the data points telling me or not telling me*
    - *Do the data points contain other data points*
      - *What do these mean to me*
      - *What are the data points telling me or not telling me*
      - *Enter Recursive mode here*
    - *Can I explain it*

Answer

- *Automation and Triage Tools*
  - *Size of Hard Drives Increasing*
  - *looking for data in pre-defined usually stable places is going to be paramount.*
    - *Internet History*
    - *Registry*
    - *Types of documents*
  - *Provide information useful to your investigation early.*
    - *Do not have to wait to load and do initial process of case*
    - *Help to ask intelligent questions before you leave the scene or make sure all the evidence has been identified/collected*
  - *Triage Tools*
    - *Pirl – Ovie Carroll*
    - *Drive Prophet*
    - *WFT – Windows Forensics Toolchest*
    - *Cofee – Computer Online Forensic Evidence Extractor*

Answer

- *Time and Complexity*
  - *Size of Hard Drives*
    - *More time for examinations*
  - *More complex programs*
    - *More time for examinations*
    - *Examinations become more complex*