Some Issues from Current Cases in DF

Doug White, PhD, CISSP, CCE, PI
Secure Technology, LLC.
dwhite@whitehatresearch.com

Objective Today

- Discuss Key Issues in US Courts for DFs framed by some current cases

What is the Hacker Defense?

- Suppose you need to suppress evidence
- Let's introduce the idea that the suspect is being wronged by a third party (e.g. The One Armed Man).

Evidence and the Hacker Defense [HD]

- Physical vs. Digital Evidence
  - Rule 401 – Relevant evidence means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.
- Admissibility
- The 4th Amendment
- US. V. Richardson 583 F. Supp. 2d 694 (W.D. PA 2008)
  - The Hacker Defense – "It couldn't have been me?"

Policy

- Netstumble the site
  - Be sure and document the available networks and security restrictions
- Seize wireless nodes to review configurations
- Ask the suspect if there is a wireless network on the premises.
- HKEY_LOCAL_MACHINE\Software\Microsoft\WZCSVC\Parameters Disable WPA = 1 means they were using WPA.

Warrants

- U. S. v. Carter 549 F. Supp. 2d (D. Nev. 2008)
- Suppress the warrant due to the possibility of spoofing the IP or MAC.
- Suppress due to “sharing” of nodes or connections.
- Key Statements here:
  - “The fact that an outside computer user can gain access to the internet through the internet service subscriber’s wireless connection and IP address, with or without his knowledge, or that computer users can use software to ‘spoof another person’s assigned IP address or MAC address’, are certainly possibilities that diminish the likelihood that the Internet transmission emanated from the subscriber’s premises.

Policy

- Be sure and show that the IP on the system was in use at key times during the events being questioned.
- Have a good explanation ready for how IP addressing works.
- PAT and/or NAT is particularly a problem in these cases and can be introduced as a HD as well.

Key CP Issues

- Remember:
  - Rule §3509 (Adam Walsh Act) limits defense access to drives and other evidence except in Federal Custody.
  - Ashcroft v. Free Speech Coalition (535 U.S. 234 (2002) (Kennedy, J.))
    - If the image is not a child but a digitally altered adult it is not CP.

Due Process

- State v. Dingman 202 P 3d 388 (WA 2009)
- *Boyd,* 160 Wash.2d at 430 (finish)
- Defense claimed that Encase images were not easily accessible by their forensics expert.
- Defense was denied access to the original media due to the state being concerned that the evidence would be damaged since it hadn't been started in a long time.
- The defendant won on appeal.

The Point

- The Boyd Test:
  - The state must **show** – rather than claim or allege– that is it restricting access to protect the evidence.
  - Boyd strikes down some of the §3509 provisions
- Bottom Line:
  - Make evidence available in discovery
  - Provide DD copies or instructions for conversion of Encase formats to other usable formats.

And then there is you

- Daubert
  - (WILLIAM DAUBERT, ET UX., ETC., ET AL., PETITIONERS V. MERRELL DOW PHARMACEUTICALS, INC.)
  - Credentials
- The Great PI Debate