B19 Look Ma! No Wires: Challenges Wireless Networking Presents to Investigators

Walter T. Hart, MBA, 149 Hamerton Avenue, San Francisco, CA 94131*

After attending this presentation, attendees will gain an understand of the scope of wireless networking technology, potential problems it creates for investigators, and what methods can be employed to help account for the presence of wireless networking technology in the field.

This presentation will impact the forensic science community by providing a basic understanding of the principles and challenges faced by investigators because of the widespread use of wireless networking technology.

Wireless networking is everywhere around us from our phones, our computers, our printers, our storage devices, and even our cars. While this makes life for most very convenient, it presents many challenges to network security managers and to investigators of wrongdoing using digital devices. In virtually all types of digital investigations, investigators must plan for, and account for the presence of wireless devices. These devices provide vulnerability, opportunity, as well as possible defenses to allegations of wrongdoing involving digital evidence. Wireless technology provides both a way in and a way out of what might otherwise be a controlled network environment. Many businesses both large and small, households, and government installations, may have wireless access points. Many of these may have multiple wireless access points with varying levels of security on each. While this makes access to the network resources, including the internet, very easy, it also provides possible access to unauthorized persons or organizations to internal resources and/or the internet. Securing a network while providing a convenient level of wireless access has proved to be challenging, even for experienced network administrators. Many home users, unaware of the need to secure their home network, do not even attempt to do so, leaving themselves at risk to the loss of personal data and/or unauthorized access to their resources.

Additionally, many resources within a network can now be accessed wirelessly such as printers, scanners, phone systems, and internal data servers. While convenient to be able to use these resources without having physical infrastructure in place, this also provides an opportunity for data compromise.

Basic examples will be given of wireless network scanning resources, how they can be utilized, when they might be utilized, and precautions and pitfalls to using these tools. This will include mapping of the wireless network environment while conducting an investigation. The manufacturing of inexpensive wireless network scanning equipment that can be utilized in investigations as well as an introduction to the capabilities of some commercially available equipment will be briefly discussed. While an effective wireless investigators kit may not require any of these, some basic understanding of the capability is beneficial. Examples will be given of the use of this technology in investigations as well as investigations where it was not employed, but might have been.

A brief discussion about wireless security in the home, home office, and/or small business environment will highlight the basics of what might be done to help secure these networks. Some typical wireless installation options for common home or home office type wireless equipment will be used as examples. This will allow an investigator to possibly ask better probative questions during interviews of network administrators, home office users, and/or subjects of the investigation.

Wireless, Network Vulnerability, Wi-Fi

