A Brief History of Digital Forensics at the Florida Department of Law Enforcement

Since the early 1980's when the IBM 5150 home computer was released, people have become increasingly dependent on computers to organize, manage, enhance, and influence their lives. Law enforcement, recognizing the power of technology, has harnessed these devices and the data that they store to investigate criminal activities. FDLE has been no exception to this endeavor.

The early 1990's saw the advent of new communication and storage technologies. Widespread consumer use of the Internet began at this time and changed the way information was shared. Zip disks and flash memory cards hit the market as new storage media that increased storage capacity while decreasing in physical size. Around this time, FDLE was organizing its mission to analyze the contents of personal computers. In 1993, the FDLE Crime Laboratory System certified the first person, Special Agent Jeff Herig, in the Computer Evidence Recovery (CER) section. One year later, Mike Forche became the second person certified in this area through the FDLE Crime Laboratory System. This new CER section had the ability to recover data from hard drives and other data storage media like floppy diskettes, Zip disks, and DAT tapes.

At the turn of the century, many exciting technological developments were occurring. 1999 saw the birth of the first Blackberry phone, Napster hit the scene as a notorious file sharing platform that caught the attention and the ire of the music industry, and wireless networking standard 802.11b was released that allowed users to connect to the internet without any cables. In 2000, the first digital camera phone was released by Sharp, and USB flash drives hit the market, making data storage more robust and convenient. FDLE's CER section was changing as well. By this time, the Tallahassee Regional Operation Center (TROC) and Tampa Bay Regional Operation Center (TBROC) had established CER sections in each region. By 2001, around the time that the first Apple iPod was released, TROC had three dedicated analysts assigned to CER and TBROC had four dedicated analysts assigned to CER. These analysts were tasked with recovering data from hard drives, as well as the various data storage devices from the past, and the newer devices using USB technology.

The early 2000s were full of innovations that allowed people to participate in online communities. MySpace, mainstreaming social networking, and Skype, revolutionizing video chat, were founded in 2003. Facebook was founded in 2004. In response to the changing technology and the way that people were communicating, in 2005, FDLE's CER sections added analysis of cell phones to their capabilities. This was two years before Apple introduced the iPhone, and three years before the first Android phone was sold.

Around 2011, FDLE began to phase Video Enhancement into CER as a subdiscipline. Though Digital Video Recorder security systems had been available since the mid 1990's, it took several years for consumers and businesses to adopt the equipment. As video surveillance moved from analog storage (i.e. VHS and Hi-8 tapes), to digital storage (i.e. DVRs and NVRs), FDLE began to move Video Enhancement from the Crime Scene section where it originated, to the CER section. Currently, Video Enhancement is only offered in TROC, and three analysts are trained in this sub-discipline.

Video Enhancement wasn’t the last expansion of CER. In 2013, the CER section began offering hardware based advanced data recovery for mobile devices. These techniques allow the analyst to recover data from damaged or locked devices when they are otherwise inaccessible. Damaged devices can be repaired so that data can be extracted from them. JTAG (Joint Test Action Group) and ISP (In System Programming) allow analysts to recover information from stored memory through wires connected to the circuit board. Chip-off methods allow analysts to remove the chip that stores data so that the data can be recovered directly from the chip. These advanced techniques have evolved over the years to expand to vehicle infotainment centers and Internet of Things devices.

Somewhere along the way, FDLE dropped the section title “Computer Evidence Recovery” and transitioned to the more fitting title, “Digital Evidence”, to more accurately reflect the broad nature of all that the discipline can do. FDLE currently has four full-time analysts in TBROC and five full-time analysts in TROC. Research is under way to expand the types of devices that can be analyzed and to expand the repair capabilities to an even broader range of devices. With all that the future holds for technological advances and discoveries, FDLE’s Digital Evidence section will continue to learn, adapt, and rise to the challenge of recovering data no matter how it is stored.