

Digital Forensics - Not Just for Cops

Discuss in Forums {mos_smf_discuss:Opinions}

By Michael Roberts, Founder and President of Mile2

Having been involved in the IT Security Education space for some time I have found that it is a common misconception that Computer Forensics training is only for Law Enforcement. On the contrary, the FBI is currently so backlogged with computer related criminal cases related to terrorism and big crime that they will often pursue only serious felony cases. If the FBI decides to take on a felony case it can be subsequently shut down by their local US Attorney whose case load is so heavy that they cannot handle additional cases despite FBI's willingness to pursue.

Our team experienced this exact scenario two months ago despite unimpeachable evidence of unauthorized access by an individual to a bank account which resulted in a wire fraud of more than \$100,000 as well as illegal interceptions from an "efax.com" fax service and unauthorized access to Yahoo Briefcase accounts. This only leaves local or county law enforcement authorities who, despite best intentions, often do not have the sophistication or skills required to prosecute a computer crime case, and if they do, lack of quality training can result in the evidence being corrupted due to improper chain of evidence procedures.

These problems leave the frontline network administrators in a frustrating situation with obvious crimes often going unpunished. Whereas, if organizations invested modestly in basic "first response" training for their network staff, then evidence can be preserved and documented in such a way that it can be admissible in criminal or civil actions. Successful actions serve further as a deterrent to would be hackers who will often choose "soft targets."

Legal actions are the most obvious benefits of effective Computer Forensics training, and effective forensics capability can be built in-house for a very reasonable investment. These skills can contribute significantly to effective security policies and implementation for a given enterprise because the knowledge gained can better identify "what went wrong" in any IT problem, whether it is caused as a result of malicious actions from within or without, or from an innocent glitch or rash action.

I would like to invite new visitors to this site to become members of ethicalhacker.net for a chance to win a free seat in our computer forensics training which is a combination Introduction/Advanced Forensics Boot Camp.

Michael Roberts is the founder and President of Mile2 which has offices in USA, Australia, Malaysia, Singapore, United Kingdom and Europe. He first became involved in Information Assurance as an Investigator with the Australian Telecommunications Commission in the 80's and now lives between the United States and Europe where he coordinates Mile2's partner activities. Mile2's penetration testing courses have become the de facto standard for the US Military with dedicated classes being delivered at US Air Force bases as well as US Marines, US Army and National Guard. Mile2 has also taught personnel from the United Nations, NATO, foreign Military and Government personnel and a large number of Fortune 100 companies. Traditionally, student participation has also come from a wide spectrum ranging from charities, banking, insurance, health, communications, transport, law enforcement and education to almost any sector imaginable.