# Research team finds disk encryption foils law enforcement efforts

November 21 2011, by Bob Yirka

(PhysOrg.com) -- A joint U.S./UK research team has found that common encryption techniques are so good that law enforcement, from local to highly resourceful federal agencies, are unable to get at data on a computer hard disk that could be used to prove the guilt of people using the computer to perpetuate crimes. In looking at the current technology, the team, as they describe in their paper published in *Digital Investigation*, find that if criminals use commonly available hard drive encryption software, law enforcement very often is unable find anything that can be used against them.

Contrary to what we all see in the movies and on television, cracking an encrypted drive is not a simple thing; in fact, it's so difficult that if

someone has encrypted their hard drive, there is apparently little law enforcement (or anyone else) can do read the data on the drive. Adding to the frustration, at least on the part of law enforcement, is the fact that they can't force people to give up their passwords.

The authors of the report suggest there are some things law enforcement can do, but they all must happen prior to a drive being buttoned up by encryption. Specifically, they say that law enforcement should stop turning computers off to bring them to another location for study, doing so only causes the need for a password to be entered to read the encrypted data. Also, in some cases, doing so causes the data to be automatically destroyed. Fortunately, there are some tools forensics experts can use to gather data if it sits untouched, such as copying everything in memory to a separate disk. The team also suggests that law enforcement look first to see if the drive has been encrypted before scanning it with their own software, as doing so will likely result in a lot of wasted time.

The unfortunate bottom line though, is that the authors openly admit that once the drive is encrypted, there is little to nothing to be done, which a lot of criminals are surely going to be really pleased to hear. The team suggests that the government embark on a research mission of its own to figure out a way to subvert encrypted drives or it will find itself with little reason to bother confiscating computers used by criminals to commit crimes in the future.

**More information:** The growing impact of full disk encryption on digital forensics, *Digital Investigation*, In Press.
doi:10.1016/j.diin.2011.09.005

**Abstract**
The increasing use of full disk encryption (FDE) can significantly hamper digital investigations, potentially preventing access to all digital

evidence in a case. The practice of shutting down an evidential computer is not an acceptable technique when dealing with FDE or even volume encryption because it may result in all data on the device being rendered inaccessible for forensic examination. To address this challenge, there is a pressing need for more effective on-scene capabilities to detect and preserve encryption prior to pulling the plug. In addition, to give digital investigators the best chance of obtaining decrypted data in the field, prosecutors need to prepare search warrants with FDE in mind. This paper describes how FDE has hampered past investigations, and how circumventing FDE has benefited certain cases. This paper goes on to provide guidance for gathering items at the crime scene that may be useful for accessing encrypted data, and for performing on-scene forensic acquisitions of live computer systems. These measures increase the chances of acquiring digital evidence in an unencrypted state or capturing an encryption key or passphrase. Some implications for drafting and executing search warrants to dealing with FDE are discussed.