Principles, Practices, and Procedures: an Approach to Standards in Computer Forensics

By
Mark M. Pollitt
Special Agent
Federal Bureau of Investigation
Baltimore, Maryland

This paper was presented in connection with the Second International Conference on Computer Evidence held at Baltimore, Maryland, April 10-15, 1995. The contents are the opinions of the author and do not represent the official position of the Federal Bureau of Investigation. The ownership and rights of any Copyright or Trademark holders is expressly recognized. Specific software mentioned in this paper are for example only, and their mention does not constitute a recommendation for, or approval of, their use.

Introduction:

For a number of years now, law enforcement agencies have been seizing computers and other electronic devices. In some cases, the machines and associated storage media have been seized as contraband or as the instrumentality of a crime. But, in most cases, they have been seized for evidentiary purposes. Seizing the media is but the first step in being able to use what is contained on the storage media. For this discussion, we will refer to the process by which this "raw material" becomes evidence in a criminal prosecution as "computer forensics".

Investigators and others have, by trial and error, evolved methods which will allow the discovery of evidence from storage media that will satisfy the twin requirements of science and law. Under almost all legal systems, scientific evidence offered in court must meet guidelines that speak to both the origin of the evidence and it's objective validity. Law enforcement has been, and continues to be faced with a wide variety of media types, formats, and standards. The use of electronic storage has impacted many kinds of crimes. The tools available to search for evidence are changing as well. The net effect is that there is not a singular process that will work in all cases. In fact, what works in one case, may not even be appropriate in another. Factor in the differing legal constraints from jurisdiction to jurisdiction, and there would not appear to be much chance of developing standards. However, this is not the case.

Standards - The Arguments For and Against

Standards are both a blessing and a curse. Standards serve to ensure quality. They should describe that which is the minimum acceptable level of performance. Setting higher standards can result in higher performance. Standards are necessary to ensure proper training of examiners. If there are no standards, then how can we qualify examiners? Standards serve as a guarantee, to those not involved, of reliable results. Standards serve to limit liability for actions by the examiner and his organization. Courts have been more willing to accept scientific evidence where there have been standards accepted by the pertinent scientific community. It is a matter of time before standards for forensic examination will be demanded.

However, standards can serve to impede progress and limit creativity. As new problems and new tools become available, new methods of solving forensic problems will be created. Although most physical sciences are evolving, their basic, underlying basis is not changing. Certainly not with the vigor that has been the hallmark of the computer industry. Unless care is taken to build in flexibility, any computer related standards are doomed to failure. How then, should we proceed?

During the last five years, this writer has been associated with many other law enforcement persons who have developed their own way of doing computer forensics. Each has found ways of successfully conducting examinations of electronic media. Each has found software and hardware tools which work for them. They have each developed a general procedure which they apply in most cases. To my knowledge, no one has developed a system which works in all cases. A review of their techniques reveals some striking similarities in their approach, rather than in their actions.

The Three-Tiered Approach

All computer forensic examiners share some common principles which guide the conduct of an examination. They use these principles as a framework for developing methods that will conform to these principles. Most adopt sets of methodologies in conducting examinations which consists of desirable practices. These practices are not absolute, but serve as a preferred methodology. And lastly, most examiners tailor the precise steps for each examination. These steps may be referred to as procedures. This suggests a three tiered approach to standardization of computer forensics.

Virtually all professional examiners will agree on some overriding principles. For example: that evidence should not be altered, examination results should be accurate, and that examination results are verifiable and repeatable. These principles are universal and are not subject to change with every new operating system, hardware or software. While it may be necessary to occasionally modify a principle, it should be a rare event.

Practices are the general process which guide the examiner in conducting the examination. These practices derive from the efficient application of tools and techniques and are bounded by the principles. Practices may be operating system or hardware dependant. While there may be many ways to conduct examinations, generally, they will work best if done in a certain order. It not only makes sense to document the physical and logical structure of the media before viewing files, but is a much more efficient and effective way to conduct the examination. While all examiners will not apply every practice for each examination, most will agree that there are certain "good practices".

Procedures are the step by step techniques and tools that are used to conduct an examination. Here, there are few hard and fast rules. Rarely, will two examiners conduct examinations using the same hardware and software in exactly the same way. Further, there are legitimate reasons that the procedures should be tailored to each individual examination. As a result, agreement on standards concerning the exact method to apply to a given examination will likely never occur.

A Proposal for Implementation

If we accept this three tiered model, then we can formulate a basis for standards. A body, comprised of agencies that conduct forensic examinations of computer evidence could agree on Principles. Likewise, Practices could be approved as acceptable. Multiple Practices could be approved for a given problem. It would likely prove counter-productive to attempt to standardize Procedures or techniques. Acceptance of these Principles and Practices would not be binding upon any particular agency, but would represent the consensus of the body. Agencies would be free to adopt alternative and/or supplementary Principles or Practices.

Individual law enforcement agencies set their own standards either by their practice or by regulation. If an agency puts standards down on paper, then the members of that agency are bound to these standards. As long as these rules have an objective basis, then any questions that might arise from the courts, are defensible. By having standards, we protect the individual by sanctioning his or her actions. If the standards are wrong, then it is the organization that is responsible.

Agencies will find it much easier to defend their standards if they are in conformance with the accepted practice of other agencies and independent bodies. This standardization is what has allowed the almost universal acceptance of fingerprints, for example. Failure to set standards will certainly complicate, if not slow, the acceptance of computer evidence. With the huge and increasing proliferation of computer evidence, we must find a way to ensure it's continued and expanded use in the criminal justice system.

If the proposed, three tier approach is not acceptable to the international community, then we must strive to find other common ground that will allow all agencies to use our collective strength.