The Digital Forensics World

In the information protection space, a lot of progress has been made of late in many areas. While long ago I was concerned at the lack of people interested in the field, I am now often concerned at the number of people involved relative to their expertise. Nowhere is this more to the point today than in the area of digital forensics.

Digital forensics is ultimately about understanding and describing what took place at an earlier time in a digital system, to a standard adequate for use in a legal setting. It often involves complex sequences of events occurring between multiple systems and involving many people and things; and there are usually many possibilities that have to be considered. Since peoples' lives may depend on the outcomes, there is a need for a high degree of certainty and known degree of precision and accuracy with regard to the assertion of facts and opinions.

Unfortunately, as widely practiced today by companies and independent consultants, too little care is taken, inadequate training and expertise is applied, and results vary widely. In case after case, so-called forensics experts come up with results that are just plain wrong (and can be demonstrated wrong by experiment), express beliefs that are not in correspondence with reality (for example, making claims that turn out to not be factually correct), and draw conclusions without adequate – or in some cases any – basis.

Tools in the market place

Tools for digital forensics are rarely used, even more rarely used right, and don't provide the mechanisms required in order to do the hardest parts of working on forensics issues. This is because of generally ignorance of their existence and their application, and because the field is relatively new and still emerging.

The only areas where tools work well today are in select types of content duplication (often called forensic imaging) and simplistic searches for select types of content within specific sorts of files and devices.

- In the area of imaging, there are hardware devices designed to make forensically sound copies of disks. You plug the original evidence disk into one slot and the destination disk into another, and the image is generated automatically at reasonably high speed, and with a cryptographic checksum generated to allow validation of image integrity. There are also hardware locks to lock out changes to a hard disk drive that can help prevent accidental spoliation and software tools that are used for forensics often do duplication, but at lower surety. There are network-based forensic tools that, with some loss of integrity, can image remote disks or files, or otherwise allow duplication of much of the content of interest to forensic investigation and application. For network imaging there are also select tools that provide covert imaging of network traffic, and many enterprises use more overt tools for similar purposes. These have various limitations, but most operate reasonably well within the limits of their specification.

- In the area of simple searches, tools typically provide the ability to enter a string, a regular expression, or some other similar sort of search term and generate listings of locators of the desired target information within the searched media. There are variations on this theme that do cryptographic checksums of areas of disks or files and compare them to known checksums to identify known contraband, tools that look within certain classes of documents, look at different parts of disks or disk images, and tools that piece together parts of disks like deleted file fragments or blocks that look like headers of particular types.

For cases where someone is duplicating a system disk, then looking for a user identity in a log file, and then searching the files they own for specific content, this works reasonably well. Almost anyone can be trained to use these tools quickly and with reasonably reliability and, with a good laboratory environment, procedures, paper trails, policies, management, and other similar things, a reliable system of duplicating content and searching it for certain classes of content can be largely regularized and reliably undertaken.

Four types of business approaches

There are four types of business structures involved in this sort of work today:

1. These activities can be carried out by any enterprise of sufficient size and with adequate volume to justify the cost, if so desired. But in practice, only the largest enterprises undertake to do this in a significant manner.
2. The combination of these tools and an organization allows the basic forensic functions to be performed in volume appropriate to the current need for the front end forensic processes in many cases today. If augmented with some additional expertise, such as that available to most systems administrators, perhaps 80% of the most obvious work can be done at relatively low cost. As a result, there are emerging commercial companies that do this for other enterprises that are unable to do so themselves.
3. The most advanced of these companies, also have reasonably strong staff that have significant law enforcement or other similar experience, systems and network administrators, and other similar expertise that allow them to do a rudimentary job of analysis for relatively simple scenarios. They may also have investigative staff that can understand the issues in a case, follow legal procedures, and are licensed to do investigations. With competent investigators having proper training, they can then carry out searches over networks, locate people and things at a distance, and work toward a capability to handle entire cases that have only limited disputed issues. These then form the relatively small number of elite forensics investigation firms, and they are often housed within companies that do other sorts of investigations, intelligence activities, or other similar functions.
4. The fourth type of approach is the highly skilled digital forensics expert. There are a relatively small number of these individuals and most of them work in their own small businesses. They tend to work on at most a few cases at a time, and they tend to have special expertise in select areas where they can drill down to a level where opposing experts do not have adequate understanding to delve.

Which to use and when

Internal forensics staff are suitable only to large enterprises that specialize in a particular aspect of information protection that include digital forensics as part of their internal purpose. Some of these companies sell the tools and maintain internal staff to support the tools, are owned or operated by experienced investigators, or otherwise have some special link into the forensics community and a desire to operate in this space for their internal investigations. For other companies, the cost of operating internal staff for these purposes usually exceeds any benefit.

Companies that do imaging and searching in volume and don't have specialized expertise are find for many situations in which companies have to secure large volumes of evidence for some large-scale legal matter, assuming that the company operates in a reasonable manner and that there is confidence that they can do the job required for the nature of the case at hand. They are most often called in at the beginning of a large volume evidence case or because of a corporate link or personal relationship between insiders and the outside company. Increasingly, service providers are starting to try to enter this space to handle large volume business for legal actions, and many law firms are starting to either outsource this function or provide internal staff to do this part of the work.

The top end companies of this sort are most often used by law firms, large enterprises who have more complex cases, in international cases where a combination of many different issues drive the need for the larger and more diverse expertise of a larger high-end firm or in cases where wealthy individuals are involved and they want to get a higher quality specialist on their side out of concern for liability or a desire to make more certain of the quality of the results.

Finally, the highly skilled experts, who are few and far between, operate on a case by case basis for anyone who decides to seek them out. They are more often than not unknown to the world at large, and their reputation spreads through the legal community as they are involved in case after case. They should be sought out and used in cases where a lot is on the line and where the top experts are likely to make the difference.

Summary and conclusions

The field of and market in digital forensics is in its earliest stages, with only rudimentary tools that serve only a limited part of the process. There is a long growth path ahead in this industry, and it will take a long time to make significant progress. As an industry, it is only being born, and it will be many years before it starts to mature in any meaningful way.

It seems likely that, over time, this field will become a profession, with doctorate level experts at the top, certification processes mandates, professional standards applied, and regularly published refereed scientific journals forming the basis for analysis and presentation of materials in court. But for now, like the Wild West that was the Internet and is not yet well settled today, the area of digital forensics will continue to be a territory for innovation, exceptional individuals, major missteps by players here and there, and a lack of clear direction for the foreseeable future.

