

Trends in Digital Forensics

The traditional approach to digital forensics is changing. More and more companies now have a global presence with offices spread around the world. What's more, these distributed networks have thousands, if not tens of thousands of pc's attached to them. In the past, when someone was suspected of a crime or behavior that was in violation of corporate policy, the typical process would be to seize the hard drive after hours, take a bit stream image, analyze the drive and compile a report. With p/c's spread across the globe, this is becoming an increasingly difficult task.

Forensics is defined as the acquisition and analysis of evidence for presentation to a court whether that court be an arbitration hearing, a civil court or a criminal court. In a corporate environment, employees have been known to get into all kinds of trouble. Things like harassment, fraud and inappropriate use (surfing porn on company time) are commonplace.

The new trend in digital forensics is to be able to use the corporate network to immediately respond to incidents. It allows us to capture and analyze volatile data, including active network sessions and running processes. It even allows us to see what ports and IP addresses these processes are communicating with. It is far better to see what is actually happening as opposed to trying to piece it together after the fact from fragments found across the drive. Much information is lost when a computer is turned off, specifically the Random Access Memory (RAM). More and more we are seeing a sophisticated user that hides ones tracks by using something like a third party email program which is not part of the corporate network and then using a cleansing program to erase any internet history on the hard drive. Although the proxy server will still show entries to this third party email program it does not capture nearly enough information to be useful. By using a product for "live" investigations one can track exactly what is being said and to whom. Let me try to illustrate the scenario with an example. It has been alleged that Sally has been selling narcotics using the corporate network and doing it on company time. She does this routinely during the day. Since Sally works at the corporate headquarters, you wait till Sally goes home and you take a forensic image of her hard drive. Once done you analyze the image and find nothing that will link her to the allegations. You do notice that her internet history is always cleaned at the end of the day. When you use your forensic software to try and recover that internet history, you find that it is gone. What you do find is that Sally has loaded a popular internet history erasing program on her computer and faithfully runs it several times per day. Clearly you are suspicious about why she would be doing this, but you have no evidence to support the allegations. Next you check the internet proxies to see what internet sites she is visiting. You find that she spends a lot of time on hotmail. At this point all you can confront her with is her spending too much time on personal sites (hotmail), but you have nothing to prove the allegation of selling drugs. So, what are your options. You could put a key logging program on her machine, however, she may notice, and besides your current desktop security software detects key loggers so this option doesn't work. You could use an external key catcher (A hardware device that the keyboard is plugged into and then

this device is plugged into the computer effectively catching all of the key strokes from the keyboard). This is problematic in that it could be noticed by the user. These two options also assume that you have access to the computer which may not be the case as the computer could be located on the other side of the world.

Which brings us to the latest trend in digital forensics for security minded corporations. Online digital forensics over the network. Since we suspect strongly that Sally is using hotmail to broker her drug deals we watch the proxy servers for traffic to hotmail. Once we see this traffic starting we then have a look at her machine in real time. In this way we can dump and analyze the memory and find out lots of key information such as the content of the emails, what is in the internet cache files at the time and ip addresses of other machines that she may be communicating with. The good news is that we can do all of this even if the machine is located in another country. Other features include the ability to traverse the registry of the target machines in a live state. Files can also be acquired over the network. The only downside is if you are running on a slow network this can be cumbersome and time consuming to acquire the entire drive. The theory of course is that you are able to narrow your search considerably by doing an online analysis and through this analysis you know what you are looking for. You then acquire the evidence related to the crime.

There are two products in the market who are industry leaders with two different implementation strategies. One is the product from Guidance Software which has a product called Encase Enterprise and the second is WetStone Technologies "LiveWire". Both accomplish the same result in that they both have the ability to dump, search and analyze memory and the files on the remote computer, however LiveWire does it without needing to have a program (service) running on the machine being analyzed. With Encase Enterprise a service must previously be installed and running on the machine in order to allow for the machine to be accessed. This makes the deployment in the corporation not only complex, since any service must co-exist with other services, it also makes it very costly. With LiveWire no such service needs to be running making it extremely useful for a forensic consultant to go to a site, bring their laptop with them, attach to the network and forensically acquire both the memory and the hard drive information of any computer on the network, including servers. All that is required is an administrator userid and password of the machine being targeted. This makes LiveWire extremely useful, easier and far more cost effective than its competitor.

There is also a growing trend to encrypt the data stored on hard drives, particularly portable computers such as laptops and notebooks. Although we as forensic examiners have some tools to get past these encryption schemes they are not always successful. A live investigation allows us to use calls to the operating system of the target machine to extract and decipher the data.

With increasingly complex network infrastructures geographically dispersed across the globe, "live" investigations is the trend we are heading towards.