Computer Forensics

Christoffer Ramqvist
christoffer.ramqvist.4669@student.uu.se

Par Stenhall
par.stenhall.6501@student.uu.se

24 oktober 2006

1 Introduction

Forensics is about using science to answer questions of interest to the legal system, which may be because of a crime. One of the earliest and most classic examples of forensics is using fingerprints to establish identities in crime scene investigations, which have been used for centuries. Forensics has since then evolved into a broad spectrum of sciences including Computer Forensics which is the most recent one. Computer Forensics focuses on finding digital evidence on data storage devices like hard drives and other types of memory concerning illegal activities.

When computer forensics is applied to an crime investigation the following steps are taken:

1. Acquire and preserve the evidence.
2. Analyze the evidence.
3. Present the findings.

Computer crimes can be divided into two categories. One category is criminal activities that *involves* using a computer to commit a crime, for example when people communicate using e-mail to coordinate criminal activities. The other category is criminal activities that has a computer as a target, for example hacking into a company network and stealing secret information. Both types however always leave tracks, and its just a matter of finding them. But it is not always easy since computers and computer networks are getting more complicated each day and computer crime techniques are getting more sophisticated. It's very difficult however for a criminal to completely erase his tracks, even if he tries.

2 Data Recovery

One big part of computer forensics is the art of data recovery. These divide into three main branches:
Recovering deleted data and recovering data from logically or physically damaged media.

When trying to recover deleted data the first thing you should do is to do a raw-image of the media. Either by writing the sectors to a image-file or by writing them to another physical media i.e. to clone the media. When the cloning is done you should run at least two hash-functions over the file system to ensure that it really is a exact copy.
When you have the copy of the media that you want to try to recover files from you store the original in a safe place, that is so that you always have the originals intact, it could be used as evidence if the data you recover is illegal in some way.
So when you have stored the original you want to start recovering, if you have a image you could mount it with a read-only option to your file system so that you don't unintentionally compromise the data. If you have a cloned media you could use some hardware that allows you to connect the it to your system in a

read-only mode.
When everything is set up you run some data-recovery program. This program then analyses the file system on the media to see if it can find any deleted data. This is possible because when data is deleted it really is not, the data is just marked as free in the file system. How this works depends on what file system the media has. This also means that it is not always possible to recover data, as the space is marked as free it can be partially or completely overwritten by other data and then it is really lost.
When you have recovered the files you copy then to another media for further analysis.

If you have a media with a logical damage to the file system you have to try to reconstruct it or extract the raw data before you can try to recover files. A file system can be damaged if the power is cut to the media before the cache is written back to the media. This can cause the file system to not be updated at all or to be partially updated.
There are two very different techniques for trying to repair a damaged file system. One is to traverse the whole file system and compare it against the specification. This method can also rebuild a broken file system to a working state. However it is possible that you do not recover everything when using this method.
The other method is slower and can not be used to reconstruct file systems, it can however recover separate files from a very damaged file system that the first method could not do anything with. The approach used is that you scan the whole drive and record every clue about it. Then you compare your clues to a file system of the same kind and that way you can extract files or segments of files.
When the logical damage is fixed you can use the first method to try to recover files.

The third branch is recovering data from physically damaged media. How you recover data differs greatly between different types of media but in all cases you try to extract as much of the file system and raw data as you can. Depending on how a media is damaged you might be able to recover anything from nothing to almost everything. A physically damaged media is often also logically damaged. So if you are able to extract data from a physically damaged device, you have to fix the logical damage before you can read any files from it. And if the files where deleted before the media was damaged then you also have to try to recover them using the first method.

The conclusions you can derive from this is that if you really want to erase data you should use all three methods. Start with deleting and overwriting the disk over and over. Then you damage the file system so that you can not read the data directly. And last physically destroy the media. One good way to destroy disk drives is to heat them to over 770 degrees centigrade because then the metal loses all its magnetic abilities.

3 Data Retention

Data retention has become a hot subject in the recent years in Europe because of the Data Retention Directive (Datalagringsdirektivet) which would make it mandatory throughout EU. Data retention refers to storing records of telephone and internet traffic and by analysing the retained data governments can identify the locations of individuals, an individual's associates and the members of a group such as political opponents and use it as hard evidence in a crime investigation. The information stored includes part of the e-mail headers, and a log of all telephone calls made. It is often argued that data retention is necessary to combat terrorism but it has been opposed heavily by people who think that it is an invasion of privacy and does not prevent terrorism at all, it just makes it easier to find the criminals and their associates after an attack has already taken place.

One of the strongest supporters of the directive is Sweden, and the directive has been rejected and rewritten several times since it was proposed after the Matrid bombings in 2004 where mobile phones were used to detonate the bombs. But earlier this year the directive was voted through. Accorning to the directive all EU countries must store information including the date, destination and duration of communications and make it available to the law enforcement authorities for between 6-25 months. Service providers will have to bear the costs of the storage themselves. EU countries will now have until August 2007 to implement the directive.

4 References

- References: Silberschatz, Galvin and Gagne: Operating System Concepts Sixth Edition
- http://en.wikipedia.org/wiki/Computer_forensics, 20061023
- http://en.wikipedia.org/wiki/Data_recovery, 20061023
- http://news.com.com/Europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html