Netherlands Forensic Institute develops and publishes open source software

The Netherlands Forensic Institute (NFI) recently published its own software, TULP2G, under an open source license. The NFI had already published a software library called Rfile as open source software. The software that was developed by the NFI can now be used and developed further by other organizations. In addition, the reflection of third parties may enhance the quality of the software.

The NFI initiatives are not isolated incidents; corresponding foreign organizations and other governmental organizations frequently publish their own software with an open source license or participate in existing open source projects. In turn, the NFI uses open source software that has been developed by other parties to trace digital tracks. However, an open source code is not a must, and the NFI uses closed software as well. Nevertheless, when doing forensic research there are certain high-quality open source products that can not be ignored by the NFI and its foreign equivalents. The openness of the source code enables the NFI to make additions and to study and check the precise working of the software.

Netherlands Forensic Institute

The NFI (http://www.forensischinstituut.nl) is part of the ministry of Justice and does technical and scientific research to help solve crimes. Since 1985 the NFI has been working with digital evidence, which in the beginning was handled by the department of hand- and machine-writing. In 1995 a new department was founded, which is now known as Digital Technology (DT). Since then, the department has grown from 4 to 35 employees. This rapid growth shows the increasing importance of digital evidence. Among the principals of the department are all Bureaus of Digital Expertise (BDEs) in the Netherlands.

Forensic research and software

With the increasing use of computers for daily communication, the importance of digital evidence is increasing as well. Using information systems leaves many tracks, which can serve as evidence in a lawsuit. Although electronic tracks are relatively easy to find, they are also very sensitive. The date of last entry into a file can be easily changed, and e-mail messages or logfiles can also be forged relatively easy. It is also possible for someone to break into someone else's computer system and place evidence on this system. The sensitivity of digital tracks plays a role in collecting and analyzing the digital evidence. Obviously the evidence should not be changed, and it is important that no evidence is lost.

According to Dutch criminal law, a suspect can only be convicted if the judge can establish his guilt based on legal and convincing evidence. This means that the origin, the reliability and the way of obtaining it determine the value of evidence. This is true for digital evidence as well. The reliability and verifiability of the functioning of a certain forensic software tool is therefore of great importance. The NFI is well aware of this and thoroughly examines both open and closed software tools before using them in forensic investigation.

In addition to this it should be noted that using a software tool is usually part of a more elaborate forensic investigation. The results of an investigation are therefore not based on the information that was obtained with a certain software tool alone, which is part of the reason why an open source code is no strict demand for the NFI.

Open source software does have advantages when it comes to gathering and analyzing digital evidence. The way open source software works can be checked by the NFI in a more simple and thorough way. Because of the openness of the source code it can be verified by everyone, including scientists and suspects, and on all levels. The reliability of closed software on the other hand, can only be established by Black-Box-tests, in which the output for different scenarios is analyzed.

In addition it is easier to check new software versions when the source code is open. By comparing the source code with the previous, already checked version of the software, changes can be recognized relatively easy. In case of closed software changes are not transparent and full Black-Box-tests are required to establish the reliability of the new software.

TULP2G

The NFI developed TULP2G and is publishing the software as open source under the BSD license since September 13th 2004. TULP2G is an abbreviation for Telefoon Uitlees Programma, 2^e generatie (Telephone Outreading Program, 2nd generation). The software offers a forensic frame for reading out and decoding data that is saved on electronic mobile devices, such as mobile phones and PDAs. TULP2G has been designed so that plug-ins can easily be added to the software. The current version already has a number of plug-ins for reading out mobile phones.

TULP2G just reads out the information and uses the open standard XML as saving format. This way other programs can be used for viewing or scanning through the information. TULP2G is not suited for this. The program was written in C# and is currently available for the windows platform only.

The NFI developed the software themselves, because their principals had a need for it, but no such program was available on the market. By publishing the program under an open source license, the NFI wants to offer everyone the possibility to develop additions to or plug-ins for the framework. Moreover, because of the BSD-license, third parties can decide for themselves whether they want to publish these extensions with an open or a closed license. In this way the NFI hopes to stimulate the forensic research in the field of electronic mobile devices and the standardization of procedures in this field. The moment another product reaches the same level as TULP2G in terms of price and quality, the NFI will stop any further development of TULP2G, says Van den Bos. Since the source code is freely available, the development of TULP2G can always be continued by other parties.

By now, several organizations other than the NFI are using TULP2G or considering this. From different parties the NFI has received suggestions for improvement. The last quarter of 2004, TULP2G has been offered to the renowned American organization NIST. This governmental organization tests the working of forensic tools within the Computer Forensics Tool Testing project.

RFile

Rfile is a software library developed by the NFI to open and read different file formats. The library has been published in 2003 under the BSD-license. The German Bundesamt für Sicherheit in der Informationstechnik (BSI) is now using Rfile, and even offers it on its website. Besides the NFI and the BSI, a number of other organizations is now using Rfile as well.

Other Open source software

Several open source products that have not been developed by the NFI can be used for forensic investigations. For making disk images there are md5deep, md5sum, sha1sum, GNU dd, decal-dd, AIR and Odessa. For forensic analysis open source applications such as Foremost, Odessa, Coroner's Toolkit, Sleuthkit and Forensic Browser Autopsy are available. Many of these tools operate under Linux or BSD or are automatically distributed together with these open source operating systems. There are also several open source software tools available for the windows platform. The NFI and its foreign equivalents use a number of the before mentioned products and contribute to their development. The Computer Crimes Division of the American NASA recently published a manual for researchers that want to do forensic research with Linux.

A standard Linux distribution has a number of qualities and tools that can be used for forensic research. Linux, for instance, supports a large number of file-formats including the windows formats FAT and NTFS. In addition Linux can be easily loaded from a CD-ROM. In this way Linux can be used in a read-only mode to investigate a system without affecting this system.

A standard Linux distribution contains the tool GNU Duplicate Disk (GNU dd). This can be used to create an image, an exact copy, of a disc. Its quality has been checked in a test by the American government; the tool proved to be highly accurate and fast. The American Ministry of Defence has developed an extension for this tool.

Linux also offers the so-called Enhanced Loopback Device, which is used to access the above mentioned image. This software was originally developed by NASA.

Another tool, developed by the American Air Force Office of Special Investigations, is Foremost. This open source application can be used to repair damaged files.

Conclusion

What precedes shows that open source software is not only used for generic application, but plays an important role in specialised fields of work as well, such as forensic investigations. Several high-quality open source products are available for forensic investigation. The availability enables the user to check the working of the software, and where necessary to improve it.

The NFI and its foreign equivalents utilize the possibilities offered by open source software. The organization uses open source software that was developed by other parties, and launched two open source projects of its own. Other organizations are now using the NFI's software and are contributing to the improvement of the applications. The NFI's initiatives therefore have a positive effect on international standardization and co-operation in the field of forensic research. The ultimate way of sharing knowledge and innovating!

This document was prepared by David Duijnmayer based on a report by Bart Knubben of the OSOSS programme, which was based on interviews in October and November 2004 with Zeno Geradts and Jeroen van den Bos of the Department of Digital Technology of the Netherlands Forensic Institute.

24 December, 2004