Hiding plain text data on a hard disk

Title: Data Hiding and Concealment – A simple experiment with serious implications

Research by: Data Clinic Ltd (UK)

Aim of Experiment: To conceal a non-encrypted, sequentially written, visible text string on a hard disk and, without modifying the text in any way, hide it so that it cannot be detected by conventional forensic data recovery methods.

Procedure:

1. Take any hard disk and sanitize it by writing zeros (00 hex, or any value) to it
2. At a random location on the hard disk write some text – this is a non - encrypted, plain text, sequential string of visible ASCII characters. (eg. the text we used was “Karl Jamieson”)
3. Use forensic tools (such as EnCase and Xways) to search for the data and verify its existence on the hard disk
4. Without modifying the text in any way, hide the text.
5. Repeat Step 3.
6. Make a ‘100% copy’ (or clone) of the original hard disk and repeat Step 3 on the clone.

Results:

1. Before the text was hidden, its’ existence on the hard disk was successfully verified using EnCase and Xways forensic tools.
2. Once hidden, the text was **undetectable** to the same forensic tools on both the original and the clone hard disk.
3. While the text existed in a non - modified state on the original hard disk, it was **not copied** to the clone drive.

Implications:

1. Using knowledge of internal hard disk operations it is possible to hide the data on a hard disk without modifying the data in any way
2. This experiment demonstrates that imaging programs and investigative procedures currently in use by many forensic investigation organisations are flawed.

Conclusion: The test was a success – see Further Notes (below)

Further Notes:

1. This document is deliberately written in a simple and clear way so as not to obfuscate or mislead. No steps have been concealed or purposefully left open to interpretation.
2. With an in-depth knowledge of hard disk workings and data recovery techniques, individuals should be able to correctly figure out how we did this.
3. This is a simple procedure. Other experiments we have conducted with the same non-encrypted, sequentially written, visible text string successfully hide the data in more ingenious ways. Again these experiments rely on the capabilities of the hard disk and do not use encryption or steganography techniques.
4. We welcome your comments.

Release Date: 18/11/04
Document Notes: Overview Only – for further information contact Data Clinic.