

Computer Forensics workshop

Duration:

2 day workshop

Target Group:

Everyone with an interest in networking. Some knowledge of TCP/IP is expected.

Goals:

Give a basic understanding of Computer Forensic tools and methods. Participants are expected to be able to carry out simple to advanced investigations of their own equipment after the course.

Content:

The participants will learn methods and tools to carry out structured analysis of hacked systems, including gathering of information about deleted files from hard disc images.

After this course the students will be able to bring a compromised system securely back into a consistent state that can be used productively using best-practice methods and a minimum of costs: time, money and other resources.

In this workshop we will go through the techniques behind computer forensics and methods to perform structured analysis from hard discs and networks. The workshop method will include carrying out attacks on vulnerable systems using available tools and operating systems - in the same way a hacker would do.

In this work shop the starting point is available open source tools including [sleuthkit](#), Autopsy and foremost.

Tools are primarily executed using UNIX but knowledge of UNIX is not a prerequisite for this course. The examples used are from both UNIX and Windows.