NetAnalysis™ Foundation Training

DIGITAL DETECTIVE

Course Objectives

The NetAnalysis™ Foundation Course is a 2 day, instructor-led, web browser forensics course designed to provide the student with the necessary skills and knowledge to utilise NetAnalysis™ and HstEx™ effectively within a forensic investigation.

Prerequisites

This course is designed for both corporate and law enforcement forensic examiners who use NetAnalysis™ and HstEx™ for the recovery of web browser evidence. It is suitable for individuals with all levels of experience and is focused towards those who wish to learn how to realise the full potential of our software.

To gain the most from this course, the student should meet the following minimum requirements:

- Read and understand the English language
- Attended basic digital forensic training
- Previous investigative experience in digital forensic case work
- Familiarity with the Microsoft Windows environment and data recovery concepts
- No previous experience of NetAnalysis™ or HstEx™ required

What you will learn

This course will equip the student with the knowledge to recover web browser data and analyse it utilising custom designed SQL searching and filtering. The student will be taught how to identify and bookmark evidence as well as techniques for presenting their findings in an evidential format.

The full functionality of NetAnalysis™ and HstEx™ will be explored using real life scenarios, case studies and hands-on exercises.

Course Dates

The following courses are currently available. To book a place or to discuss hosting a training course: 0845 224 8892.

Date	Venue	Cost
24th - 25th January 2012	Learning Tree International Euston House, 24 Eversholt Street, London, NW1 1AD	£ 830 + VAT Per Person
21st - 22nd February 2012	Learning Tree International Euston House, 24 Eversholt Street, London, NW1 1AD	£ 830 + VAT Per Person
6th - 7th March 2012	Learning Tree International Euston House, 24 Eversholt Street, London, NW1 1AD	£ 830 + VAT Per Person

Introduction

- » Course introduction
- » Prerequisites and background information
- » Course structure and learning materials
- » Housekeeping and policy

Pre-Read Material

- » Review of pre-read material
- » Answers to pre-read knowledge check

Introduction to NetAnalysis™ and HstEx™

- » Overview of NetAnalysis™ and HstEx™
- » Software installation
- » Licence key / USB dongle installation

NetAnalysis™: A Guided Tour

- » Understanding the user interface
- » Understanding NetAnalysis™ columns
- » NetAnalysis™ workspace files
- » Using keyboard shortcuts

Configuring NetAnalysis™

- » Considerations before you start an investigation
- » Time zones
- » Date formats
- » Restricted Date Ranges
- » Case Settings
- » Export Settings
- » Interface Settings

Establishing Time Zones

- » Overview of time zones in forensic analysis
- » Time zone translation and the Windows API
- » Identification of the target system time zone
- » Overview of ControlSets
- » Daylight Saving Time
- » Static and Dynamic DST
- » ActiveTimeBias, Bias, StandardBias, DaylightBias
- » SYSTEMTIME structure
- » NetAnalysis™ time zone configuration

Investigation Techniques and Considerations

- » Importing browser data
- » Recovery of live and deleted data
- » Restrictive data import
- » Overview of web page rebuilding
- » Overview of audit log
- » Evidence continuity (chain of evidence)

Identifying the evidence

- » Filtering, searching, sorting and identifying evidence
- » Keyword highlighting
- » Right click filters
- » Filtering records between dates
- » Tagging
- » Navigating through the workspace

Building and saving SQL queries

- » Searching using the Column Filter Bar
- » Utilising keyword list searching
- » SQL Query Manager
- » Sample SQL queries and keyword lists

Understanding the Evidence

- » URL components and structure
- » URL encoding and obfuscation
- » Interpretation and analysis
- » URL decoding

Web Page Rebuilding

- » Overview of web page rebuilding
- » Understanding a persistent cache
- » Web page objects and components
- » Absolute and relative path structures
- » Exporting / Rebuilding the entire cache
- » Cache files: grouping and analysis
- » Reviewing the page rebuild audit log
- » Evidencing an exported cache
- » Archiving to media

Bookmarking, Reporting and Record Exporting

- » Bookmarking evidence
- » Copying formatted records to the clipboard
- » Understanding and utilising built-in reports
- » Overview of record exporting
- » Customising NetAnalysis™ for bespoke exporting

Recovery of Deleted Data

- » Overview of HstEx™ and its capabilities
- » Recovery from forensic image files
- » Recovery from physical / logical devices
- » Recovery from dd / segmented dd images
- » FBE (File Base Extraction)
- » RBE (Record Based Extraction)
- » Linear / Sequential processing
- » Cluster boundaries
- » Matching recovered data to original evidence