



Initial Open Source Intelligence

By

Ray Massie - Fleet Forensics Ltd

Course Description

The initial open source intelligence course is designed to equip students the skills necessary to safely and lawfully gather information from a variety of sources, found on the Internet. During the course students will learn a structured methodology, enabling them to present any of information they find, to an evidential standard which is demanded by UK criminal and civil courts.

The 3 day course is interactive offering students a hands on learning experience throughout. They will be taught a range of skills, from understanding different protocols of the Internet through to how data is sent and stored. This will increase their knowledge of where to look for information, how best to capture it and then present it at hearings. Students will build their own toolkit and use free on line resources to enhance their investigations. Throughout they will adopt a method of recording what they do and give that work integrity, which is designed to withstand legal challenge at court or tribunal.

This course provides students with the essential foundation knowledge which is a prerequisite to the 4 day Advanced Open Source Intelligence Gathering course offered in partnership with CSI Tech Ltd. The Advanced course is delivered through the same interactive methods but focuses on the more technical aspects of open source intelligence gathering.

Course Goals

1. Develop understanding of the Internet as an open source asset
2. Develop an individuals skill in open source research
3. Develop techniques necessary to present a product to an evidential standard
4. Provide essential foundation knowledge as a prerequisite to more advanced study.

Course Content

The Internet & Networks

History
Scale of the Internet & architecture
Internet protocols
Networks and IP addressing
Hardware
Domain Name Service (DNS)
Internet registries
Communication Service providers

World Wide Web

Browsers
Search Engines
Keywords
Cached Pages
Archives
Web Pages linked & unlinked

Content from other sites
Page Source
HTML
Traces, cookies, web logs & servers
Criminal use of the WWW

Open Source resources

Search & Meta Search Engines
Categories of Open Source
People search
Data Sources
Places
Closed source information

Capture, Presentation and Investigation

Still & moving capture
Downloading a website
Note taking
Software sources
Build your own tool kit
Provenance & attribution
Evaluating open source
Complete methodology - product integrity, evidence or intelligence
Evidence handling

Tools & Techniques

Advanced Searching
Boolean searching
URL manipulation

Email headers
Basic commands
Work station issues
Private browsing, anonymous surfing & proxies

Social Networking

What are they?
Searching within social networks
Use as an investigative tool
Twitter

Internet Relay Chat (IRC)

What is it?
How it works
Criminal use of IRC
Evidence from IRC

Legal Issues

Law enforcement and corporate

Requirements

The student should have a basic understanding of how to use a computer and ideally be able to download and install software.

Cost

Total cost - £1248 + VAT including manual & USB key to store software and electronic tools. Lunch, tea, coffee and snacks also included.