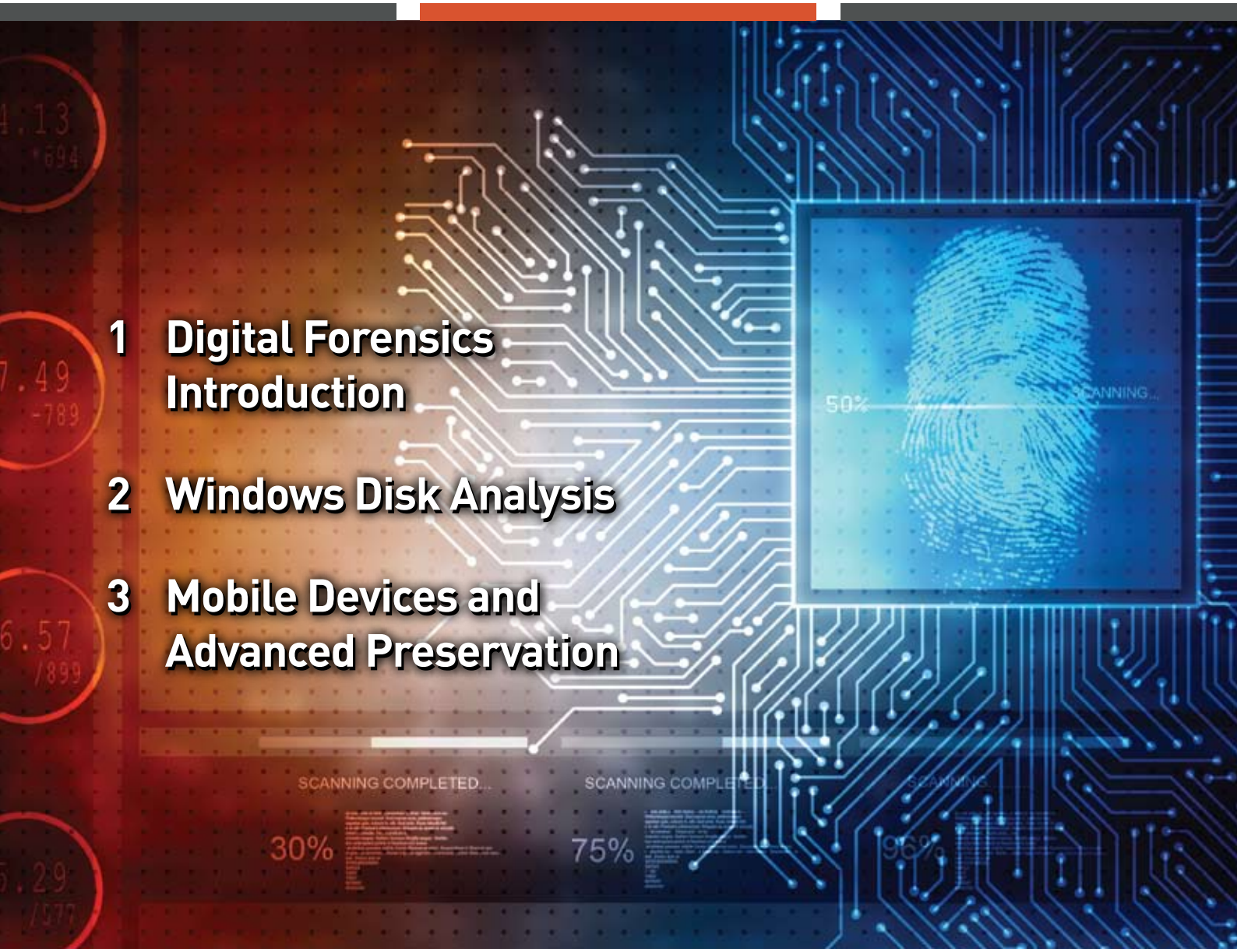
Digital Forensics
Fundamentals

"The essential course for anyone getting started with handling and investigating **Digital Evidence**"



VIEW COURSE INFORMATION >

AUSTRALIA'S NUMBER ONE SECURITY TRAINING PROVIDER

Cyber Security

Sydney | Melbourne | Canberra

Brisbane | Perth

www.alccyber.com.au

Digital Forensics

FUNDAMENTALS

Get Started with Handling and Investigating Digital Forensics

This 3-day Digital Forensics Fundamentals course is designed to provide a solid and practical introductory coverage of the principles of identifying, preserving and analysing digital evidence, such as computers, mobile phones, and online sources.

Learning Objectives

By the end of the course participants will understand:

- Industry best practice when conducting forensic analysis of electronic devices
- End-to-end process and legal requirements for chain of evidence and chain of custody
- Recognising potential sources of digital evidence
- Requirement for identification of evidence
- Introductory techniques for examining evidence
- How to correctly handle and preserve evidence in a forensically sound manner
- Commonly relied on evidence artefacts
- Gain experience with several tools for forensic analysis
- Report structure and format on the analysis of evidence

Who Should Attend

The course is targeted at:

- Investigators
- Would-be digital evidence examiners
- Law-enforcement personnel
- Information security professionals
- Anyone wanting to get started with handling and investigating digital evidence

Course Contents

Day 1 Digital Forensics Introduction

- Digital forensic process
- Identification of evidence
- Evidence handling principles
- Order of volatility
- Evidence preservation
- Imaging basics
- Analysis basics with Autopsy and X-Ways

EXERCISES

- Imaging using a write blocker, live CD, forensic duplicator
- Mounting disk images
- Examination with Autopsy

Day 2 Windows Disk Analysis

- Introduction to file system forensics
- Techniques for filtering and searching
- Mapping of investigative questions to artefacts
- Carving deleted content
- Email activity
- Web browsing historical activity
- Chat rooms and activity
- Evidence of access and execution
- Tracking USB storage and file movement

EXERCISES

- Carving of deleted content
- Tracking web browser history
- Identifying files accessed

Day 3 Mobile Devices and Advanced Preservation

- Volatile memory acquisition
- Gleaning evidence from pagefiles and Random Access Memory (RAM)
- Identifying and dealing with encryption
- Identifying and preserving cloud services
- Reporting
- Managing the case lifecycle

EXERCISES

- Acquisition and analysis of a phone
- Acquisition and analysis of volatile memory
- Extraction of chat and other artefacts from volatile memory