

## COURSE OUTLINE

# DIGITAL FORENSICS

## Certified Linux Forensic Practitioner (CLFP)



**SPECIALIST-LEVEL COURSE**

**Cost: £2,600.00 + VAT**

**Duration: 4 days**

This specialist-level course is for experienced forensic investigators who want to acquire the knowledge and skills to navigate, identify, capture and examine data from Linux-based systems. You will develop knowledge and skills to identify, collect, analyse and interpret data from Linux systems.

### COURSE OVERVIEW

Linux is an increasingly popular operating system. This course will provide you with a practical understanding from a forensic perspective of how to deal with a Linux system, and requires no previous Linux knowledge. This will be demonstrated and applied to reinforce understanding using both a Linux environment and Windows based forensic software.

### THE SKILLS YOU WILL LEARN

Upon completion of the course you will have used a Linux System to:

- Become familiar with both Linux GUI and command line environments
- Demonstrate how Linux can be used for forensic imaging
- Capture RAM and basic volatile data from a live Linux system (Note: this doesn't include network discovery or traffic capture).

You will have used Windows based forensic software to:

- Examine ext3 and ext4 file system structures
- Identify core system information
- Explore system log files for artefacts including; boots, logins and device connection
- Examine user artefacts including; recent activity, thumbnails and printing

### KEY BENEFITS

On this course, you will:

- Develop confidence when faced with a Linux system
- Learn effective techniques to identify and collect data from a Linux environment
- Understand the data structures associated with the 'ext' file systems
- Develop knowledge and skills to examine and process data from a Linux system
- Improve your ability to respond effectively to a wider range of forensic incidents

### WHO SHOULD ATTEND

Forensic practitioners, systems administrators and cyber investigators who want to extend their experience from Window-based systems to the Linux environment.

### PREREQUISITES

Completion of the PA CFIP course is highly recommended. Alternatively you will need an understanding of digital forensic principles and practices.

No Linux experience is necessary.

### WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Linux Forensic Practitioner (CLFP) qualification.



**To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email [cybereducation@paconsulting.com](mailto:cybereducation@paconsulting.com)**

## COURSE OUTLINE

# DIGITAL FORENSICS

## Certified Linux Forensic Practitioner (CLFP)



**SPECIALIST-LEVEL COURSE**

**Cost: £2,600.00 + VAT**

**Duration: 4 days**

*“Very good course, well paced and provided a good understanding of the Linux platform and analysis.”*

**CLFP Delegate**

**Huron Consulting**

### SYLLABUS

- 1. What is Linux? Brief history, marketplace and distributions**
- 2. Key differences between Windows and Linux forensics**
- 3. Linux concepts: Devices and user privileges**
- 4. Understanding disk and partition mounting**
- 5. Linux partitions and core directories**
- 6. The Linux Command line: navigation and utilities**
- 7. Imaging using Linux tools and forensic distributions**
- 8. Live RAM and other volatile data collection**
- 9. Understanding ext file systems:**
  - a) The evolution of the ext file systems
  - b) Volumes and block groups
  - c) Directories, inodes and data storage
  - d) Forensics: Evidence of file deletion and problems with data carving
- 10. Examination of a Linux system:**
  - a) Identifying system information
  - b) File timestamps
  - c) Log files
  - d) Network and device connections
  - e) User accounts and passwords
  - f) Printing and Trash
  - g) User navigation, program executions and file access
- 11. Introduction to memory analysis**
- 12. Web-servers and log analysis**
- 13. Cygwin and Windows sub-system for Linux**

PA Consulting  
Global Innovation & Technology Centre Back Lane,  
Melbourn  
Herts, SG8 6DP, United Kingdom  
tel: +44(0) 1763 285285  
email: [cybereducation@paconsulting.com](mailto:cybereducation@paconsulting.com)  
[www: cybereducation.paconsulting.com](http://www.cybereducation.paconsulting.com)



**To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email [cybereducation@paconsulting.com](mailto:cybereducation@paconsulting.com)**