

**Blue Team Level 1 Certification
(Standard)**☐ TI1) Introduction to Threat Intelligence

7 Topics

☐ TI2) Threat Actors & APTs

6 Topics 2 Quizzes

☐ TI3) Operational Threat Intelligence

7 Topics 1 Quiz

☐ TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

☐ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

☐ TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN☐ DF1) Introduction to Digital Forensics

5 Topics

☐ DF2) Forensics Fundamentals

10 Topics 5 Quizzes

☒ DF3) Digital Evidence Collection

8 Topics 1 Quiz

☒ Section Introduction, Evidence Collection☐ Equipment☐ ACPO Principles of Digital Evidence
Collection & Preservation☐ Chain of Custody☐ Disk Imaging: FTK Imager☐ Live Forensics☐ Live Acquisition: KAPE☐ Evidence Destruction☒ Activity) End of Section Review, Evidence
Collection☐ DF4) Windows Investigations

3 Topics 3 Quizzes

☐ DF5) Linux Investigations

Section Introduction, Evidence Collection

Blue Team Level 1 Certification (Standard) > DF3) Digital Evidence Collection > Section Introdu...

IN PROGRESS

This section is dedicated to artifact collection, and how these should be properly retrieved during a forensic investigation. We will cover the ACPO principles, the tools and equipment used to collect evidence, an insight into live acquisition, how to collect evidence, and how to perform forensically-sound hard drive copies.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand the tools and equipment used to collect digital and physical evidence, and how it should be transported and stored.
- Understand the Association of Chief Police Officers (ACPO) principles for dealing with digital evidence during forensic investigations.
- Understand how artifacts can be retrieved from systems over the network via live acquisition.
- Understand how to collect evidence, and complete a number of practical activities based around real investigation scenarios.
- Understand different types of hard drive copies, and the differences between them.

[Previous Lesson](#)[Mark Complete](#) ✓[Back to Lesson](#)[Next Topic](#) >