

**Blue Team Level 1 Certification
(Standard)**

7 Topics 1 Quiz

☐ T15) Strategic Threat Intelligence

5 Topics 1 Quiz

☐ T16) 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

☐ DF4) Windows Investigations

3 Topics 3 Quizzes

☒ DF5) Linux Investigations

4 Topics 2 Quizzes

☒ Section Introduction, Linux
Investigations☐ Linux Artifacts – Passwd and Shadow☐ Activity) Password Cracking☐ Linux Artifacts – /Var/Lib and /Var/Log☐ Linux Artifacts – User Files☐ Activity) End of Section Review, Linux
Investigations☐ DF6) Volatility

3 Topics 1 Quiz

☐ DF7) Autopsy

4 Topics 1 Quiz

**SECURITY INFORMATION AND EVENT
MANAGEMENT DOMAIN**

Section Introduction, Linux Investigations

Blue Team Level 1 Certification (Standard) > DF5) Linux Investigations > Section Introduction, Li...

IN PROGRESS

This section of the Digital Forensics domain is going to focus specifically on conducting digital forensics work on systems running Linux-based operating systems. This includes the artifacts that forensic investigators may try to retrieve, the tools that can be used, and we'll provide you with some activities for you to try yourself.

LEARNING OBJECTIVES

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

- Understand the different artifacts that can be retrieved from systems running Linux-based operating systems.
- Explain why these artifacts could provide value to a digital investigation, or incident response process.
- Conduct activities to develop a practical understanding of conducting basic investigations on a system running Linux-based operating systems.

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