

Blue Team Level 1 Certification
(Standard)

100) 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

Section Introduction, Windows
Investigations

Windows Artifacts - Programs

Lab) Windows Investigation 1

Windows Artifacts - Internet Browsers

Lab) Windows Investigation 2

Activity) End of Section Review,
Windows Investigations

DF5) Linux Investigations

4 Topics 2 Quizzes

DF6) Volatility

3 Topics 1 Quiz

DF7) Autopsy

4 Topics 1 Quiz

SECURITY INFORMATION AND EVENT
MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics 1 Quiz

SI2) Logging

6 Topics 2 Quizzes

SI3) Aggregation

2 Topics 1 Quiz

SI4) Correlation

6 Topics 1 Quiz

SI5) Using Splunk

5 Topics 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

Activity) End of Section Review,
Windows Investigations

Blue Team Level 1 Certification (Standard) > DF4) Windows Investigations > Activity) End of Section Review, Wi...

Digital Forensics Domain
END OF SECTION REVIEW

Congratulations on completing this section of the Digital Forensics domain! This knowledge review is designed to test what you have learned about detecting and analyzing security incidents to collect information such as Indicators of compromise, and an understanding of what actions the malicious actor has taken. You will be able to re-take the quiz as many times as you like, but will need a score of 70% or above to pass. It is important that you feel confident answering these questions to ensure that you can complete tasks within the BTL1 exam and pass to become certified. If you get stuck, use the **Hint** feature!

Good luck!

KNOWLEDGE REVIEW

[1/5] Match the Windows artifact with the tool we can use to analyze it.

Sort elements

Windows Prefetch files.

Windows Jump List files.

Windows.LNK files.

PECmd.exe

JumpList
ExplorerWindows File
Analyzer

Hint

Check

Privacy & Cookies Policy

