Activity) End of Section Review, Windows Investigations

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 Explorer	
Windows File Analyzer	

Hint | Check