kaspersky
expert training

Windows digital forensics

Course
program

№	Track	What you will learn/practice	Lesson	Practice	Evaluation
0	Course overview	• About your trainer • Course objectives • Course road map • Introduction to digital forensics process	Course overview	–	Checkpoint quiz
			Introduction to digital forensics	–	
1	Incident response	• Different steps of incident response process • Where the digital forensics process fits in the full cycle of incident response	Incident response process	–	Checkpoint quiz
2	Case study scenario	• Network topology and case study scenario data for subsequent practice within the training • How to use the environment in virtual lab	Case study scenario	Virtual environment setup	–
			Introduction to the environment in CloudShare		
3	Evidence acquisition	• Different types of evidences • How to ensure the evidence integrity • Best practices for acquiring evidence • Imaging techniques	Evidence acquisition	Challenge: evidence acquisition and triage collection Solution: Evidence acquisition and triage collection	Knowledge check Checkpoint quiz
4	NTFS file system	• Basics about NTFS Files System • How to use timestamps from $MFT file for digital forensics goals • How to analyze of USN Journals	NTFS file system	Challenge: NTFS file system analysis “DOMAIN CONTROLLER” Solution: NTFS file system analysis “DOMAIN CONTROLLER”	Quiz

№	Track	What you will learn/practice	Lesson	Practice	Evaluation
4				Challenge: Exchange triage analysis Solution: Exchange triage analysis	Quiz Checkpoint quiz
5	Live analysis	• How to conduct analysis on a live system	Live analysis and incident response CDs	Challenge: Endpoint live analysis with incident response CDs Solution: Endpoint live analysis with incident response CDs	Quiz Checkpoint quiz
6	Windows artifacts	• How to various Windows artifacts for the benefit of your investigation and to get further leads and findings	RDP connections and RDP cache	Challenge: investigation of RDP-traces Solution: investigation of RDP-traces	Quiz
			Windows events	Challenge: investigation of windows events Solutions: investigation of windows events	Knowledge check
			Event tracing for Windows	—	—
			Powershell logging	Challenge: PowerShell log analysis Solution: PowerShell log analysis	Quiz
				Challenge: analysis of MFT of system partition Solution: analysis of MFT of system partition	Quiz

№	Track	What you will learn/practice	Lesson	Practice	Evaluation
6			Execution history. Windows Prefetch	Challenge: checking Prefetch, SRUM and BAM Solution: checking Prefetch, SRUM and BAM	Knowledge check
			Execution history. Windows SRUM: System Resource Usage Monitor		
			Execution history. Windows BAM: Background Activity Moderator		
			Windows Recycle Bin	Challenge: extraction of the Recycle Bin and parsing a deleted file Solution: extraction of the Recycle Bin and parsing a deleted file	Checkpoint quiz
			Shell items	Challenge: parsing LNK files, examination of Shellbags and Jump list Solution: parsing LNK files, examination of Shellbags and Jump list	—
			Windows Search Database	Challenge: using Thumbcache viewer for extraction of the Windows.edb file Solution: using Thumbcache viewer for extraction of the Windows.edb file	—
			Windows Thumbnail		

№	Track	What you will learn/practice	Lesson	Practice	Evaluation
6			Windows user access logs	—	—
			Windows notification center	—	—
			Windows scheduled tasks	—	—
			USB forensics	Challenge: tracing the history of USB Solution: tracing the history of USB	—
			Compound files	—	—
			WMI-based attacks investigation	—	—
7	Registry analysis	• What is registry to Windows OS • What types of registry hives are there • How to view of registry keys and values • Mapping each hives to its corresponding files in file system	Registry Analysis. Part 1	Challenge: checking the time zone calculation Solution: checking the time zone calculation	Checkpoint quiz
			Registry Analysis. Part 2		
			Execution history in Registry	Challenge: execution history in Registry Solution: execution history in Registry	Quiz
			Registry analysis. User activities	Challenge: user activities analysis in Registry Solution: user activities analysis in Registry	Quiz

№	Track	What you will learn/practice	Lesson	Practice	Evaluation
			Registry analysis. AUTORUN registry keys	Challenge: persistency Solution: persistency	—
8	Browser forensics	• How browsers work • Different browser's artifacts • How to analyze browsing traces effectively	Browser forensics introduction	Challenge: WebCacheV01.dat file analysis Solution: WebCacheV01.dat file analysis	Checkpoint quiz
			Microsoft Edge web browser	Challenge: browsers’ analysis Solution: browsers’ analysis	—
			Mozilla Firefox		
			Google Chrome		
9	E-mail forensics	• Email system structure • Email components • Email clients	Email protocol and email structure	Challenge: parsing the header of a received e-mail message Solution: parsing the header of a received e-mail message	Knowledge check
			Email analysis (Outlook)	Challenge: email investigation Solution: email investigation	Checkpoint quiz
10	Summary	• Trainer's closing remarks	Course summary	—	—
			Thank you!		

Thank you!

kaspersky.com

Discord : kas.pr/g2j8

Help page: kas.pr/ii9f

kaspersky