1. Record Nr. UNINA9910865263503321

Autore	Easttom Chuck
Titolo	Windows Forensics : Understand Analysis Techniques for Your Windows / / by Chuck Easttom, William Butler, Jessica Phelan, Ramya Sai Bhagavatula, Sean Steuber, Karely Rodriguez, Victoria Indy Balkissoon, Zehra Naseer
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2024
ISBN	979-88-6880-193-8
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (484 pages)
Altri autori (Persone)	ButlerWilliam PhelanJessica Sai BhagavatulaRamya SteuberSean RodriguezKarely Indy BalkissoonVictoria NaseerZehra
Disciplina	5,268
Soggetti	Microsoft software Microsoft .NET Framework Microsoft
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record. Registry Explorer
Nota di contenuto	Chapter 1: Introduction to Windows -- Chapter 2: Forensics Concepts -- Chapter 3: Creating Forensic Images Using OSForensics, FTK Imager, and Autopsy -- Chapter 4: Windows File Artifacts -- Chapter 5: Windows Registry Part 1 -- Chapter 6: Windows Registry Part 2 -- Chapter 7: Windows Shadow Copy -- Chapter 8: Windows Memory Forensics -- Chapter 9: PowerShell Forensics -- Chapter 10: Web Browser Forensics -- Chapter 11: Windows Email Forensics -- Chapter 12: Microsoft Azure and Cloud Forensics -- Chapter 13: Data-Hiding Techniques in Windows -- Appendix A: Volatility Cheat Sheet -- Appendix B: Windows Registry Cheat Sheet.
Sommario/riassunto	This book is your comprehensive guide to Windows forensics. It covers

the process of conducting or performing a forensic investigation of systems that run on Windows operating systems. It also includes analysis of incident response, recovery, and auditing of equipment used in executing any criminal activity. The book covers Windows registry, architecture, and systems as well as forensic techniques, along with coverage of how to write reports, legal standards, and how to testify. It starts with an introduction to Windows followed by forensic concepts and methods of creating forensic images. You will learn Windows file artefacts along with Windows Registry and Windows Memory forensics. And you will learn to work with PowerShell scripting for forensic applications and Windows email forensics. Microsoft Azure and cloud forensics are discussed and you will learn how to extract from the cloud. By the end of the book you will know data-hiding techniques in Windows and learn about volatility and a Windows Registry cheat sheet. What Will You Learn Understand Windows architecture Recover deleted files from Windows and the recycle bin Use volatility and PassMark volatility workbench Utilize Windows PowerShell scripting for forensic applications.