1.	Record Nr.	UNINA9910827532403321
	Autore	Carvey Harlan A
	Titolo	Windows forensic analysis : DVD toolkit, / / Harlan Carvey
	Pubbl/distr/stampa	Burlington, MA, : Syngress Pub., c2007
	ISBN	1-281-11265-8
		9786611112653
		0-08-055644-2
	Edizione	[1st ed.]
	Descrizione fisica	1 online resource (386 p.)
	Disciplina	363.25/0968
		363.250968
	Soggetti	Computer crimes - Investigation - United States - Methodology
		Computer networks - Security measures
		Internet - Security measures
		Computer security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	"Incident response and cybercrime investigation secrets"--Cover.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Cover; Contents; Preface; Chapter 1: Live Response: Collecting Volatile Data; Introduction; Live Response; What Data to Collect; Nonvolatile Information; Live-Response Methodologies; Chapter 2: Live Response: Data Analysis; Introduction; Data Analysis; Chapter 3: Windows Memory Analysis; Introduction; Dumping Physical Memory; Analyzing a Physical Memory Dump; Collecting Process Memory; Chapter 4: Registry Analysis; Introduction; Inside the Registry; Registry Analysis; Chapter 5: File Analysis; Introduction; Event Logs; File Metadata; Alternative Methods of Analysis
		Chapter 6: Executable File AnalysisIntroduction; Static Analysis; Dynamic Analysis; Chapter 7: Rootkits and Rootkit Detection; Introduction; Rootkits; Rootkit Detection; Index
	Sommario/riassunto	The only book available on the market that addresses and discusses in-depth forensic analysis of Windows systems. Windows Forensic Analysis DVD Toolkit takes the reader to a whole new, undiscovered level of forensic analysis for Windows systems, providing unique information and resources not available anywhere else. This book covers both live and post-mortem response collection and analysis methodologies,

addressing material that is applicable to law enforcement, the federal government, students, and consultants. This book also brings this material to the doorstep of system administrators, who