

1. Record Nr.	UNINA9910971364803321
Autore	Anson Steve
Titolo	Mastering windows network forensics and investigation // by Steve Anson and others
Pubbl/distr/stampa	Indianapolis, : John Wiley & Sons, 2012
ISBN	9786613662262 9781118721612 1118721616 9781118236086 1118236084 9781280685323 1280685328 9781118226148 1118226143
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (698 p.)
Collana	Sybex serious skills. Mastering Windows network forensics and investigation
Disciplina	ELECTRONIC BOOK
Soggetti	Computer crimes: investigation Computer networks: security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Network investigation overview -- The Microsoft network structure -- Beyond the Windows GUI -- Windows password issues -- Windows ports and services -- Live-analysis techniques -- Windows filesystems -- The registry structure -- Registry evidence -- Introduction to malware -- Text-based logs -- Windows event logs -- Logon and account logon events -- Other audit events -- Forensic analysis of event logs -- Presenting the results -- The challenges of cloud computing and virtualization.
Sommario/riassunto	An authoritative guide to investigating high-technology crimes Internet crime is seemingly ever on the rise, making the need for a comprehensive resource on how to investigate these crimes even more dire. This professional-level book--aimed at law enforcement personnel, prosecutors, and corporate investigators--provides you with

the training you need in order to acquire the sophisticated skills and software solutions to stay one step ahead of computer criminals. * Specifies the techniques needed to investigate, analyze, and document a criminal act on a Windows computer or network * Places a special emphasis on how to thoroughly investigate criminal activity and now just perform the initial response * Walks you through ways to present technically complicated material in simple terms that will hold up in court * Features content fully updated for Windows Server 2008 R2 and Windows 7 * Covers the emerging field of Windows Mobile forensics Also included is a classroom support package to ensure academic adoption, Mastering Windows Network Forensics and Investigation, 2nd Edition offers help for investigating high-technology crimes.
