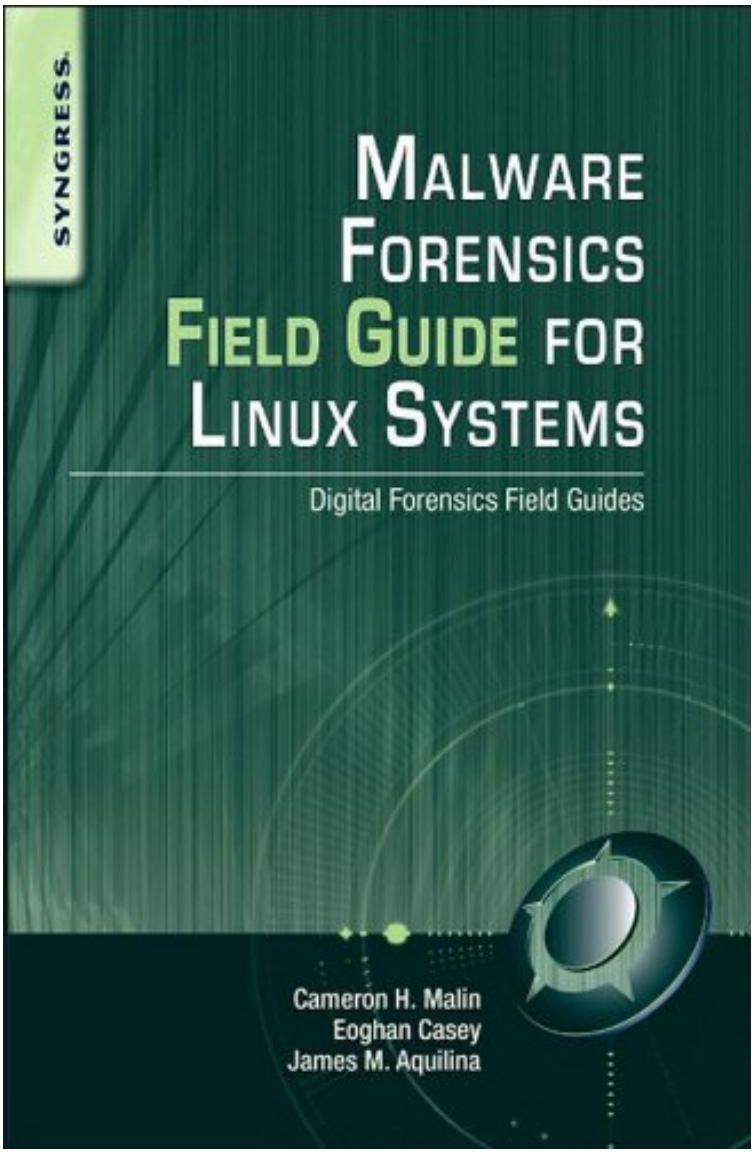
Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides

Von Cameron H. Malin, Eoghan Casey, James M. Aquilina
**Download PDF | ePub | DOC | audiobook | ebooks*



Produktinformation -Verkaufsrang: #544671 in eBooksVerffentlicht am: 2013-12-07Erscheinungsdatum: 2013-12-07File Name: B00HCIC722 | File size: 59.Mb

Von Cameron H. Malin, Eoghan Casey, James M. Aquilina : Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides before purchasing it in order to gage whether or not it would be worth my time, and all praised Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. wirklich

zu empfehlen fuer Linux-AnwenderVon Carl-Valentin Schmittfuer diejenigen Linux-Anwender die schon laenger sich mit Linux auskennen undihr System (Netzwerk) sicherer machen wollen, ist dieses Buch momentandas beste Buch, das alles erklaert in Bezug auf Loesungen gegen malwareund wie man Angriffe zurueckverfolgt.

KurzbeschreibungMalware Forensics Field Guide for Linux Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Linux-based systems, where new malware is developed every day. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Linux system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Linux systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Linux system; and analysis of a suspect program. This book will appeal to computer forensic investigators, analysts, and specialists.A compendium of on-the-job tasks and checklistsSpecific for Linux-based systems in which new malware is developed every dayAuthors are world-renowned leaders in investigating and analyzing malicious codePressestimmen""Malin et al. demonstrate how to preserve volatile data on a Windows system during a malware incident and how to analyze physical and process memory dumps for malware artifacts. The practical handbook also provides formalized methodologies for conducting forensic examinations of Windows systems, profiling a suspect file, and identifying the nature and purpose of a suspect program."--Reference and Research Book News, February 2013""..".a useful companion for law enforcement and the forensic community, as it will enhance their capability to deal with cases involving malware on Linux systems." "-""Computing s, "Oct 08, 2014..".a useful companion for law enforcement and the forensic community, as it will enhance their capability to deal with cases involving malware on Linux systems." -Computing s, Oct 08, 2014-...a useful companion for law enforcement and the forensic community, as it will enhance their capability to deal with cases involving malware on Linux systems.- -Computing s, Oct 08, 2014KurzbeschreibungMalware Forensics Field Guide for Linux Systems is a handy reference that shows students the essential tools needed to do computer forensics analysis at the crime scene. It is part of Syngress Digital Forensics Field Guides, a series of companions for any digital and computer forensic student, investigator or analyst. Each Guide is a toolkit, with checklists for specific tasks, case studies of difficult situations, and expert analyst tips that will aid in recovering data from digital media that will be used in criminal prosecution. This book collects data from all methods of electronic data storage and transfer devices, including computers, laptops, PDAs and the images, spreadsheets and other types of files stored on these devices. It is specific for Linux-based systems, where new malware is developed every day. The authors are world-renowned leaders in investigating and analyzing malicious code. Chapters cover malware incident response - volatile data collection and examination on a live Linux system; analysis of physical and process memory dumps for malware artifacts; post-mortem forensics - discovering and extracting malware and associated artifacts from Linux systems; legal considerations; file identification and profiling initial analysis of a suspect file on a Linux system; and analysis of a suspect program. This book will appeal to computer forensic investigators, analysts, and specialists.A compendium of on-the-job tasks and checklistsSpecific for Linux-based systems in which new malware is developed every dayAuthors are world-renowned leaders in investigating and analyzing malicious code