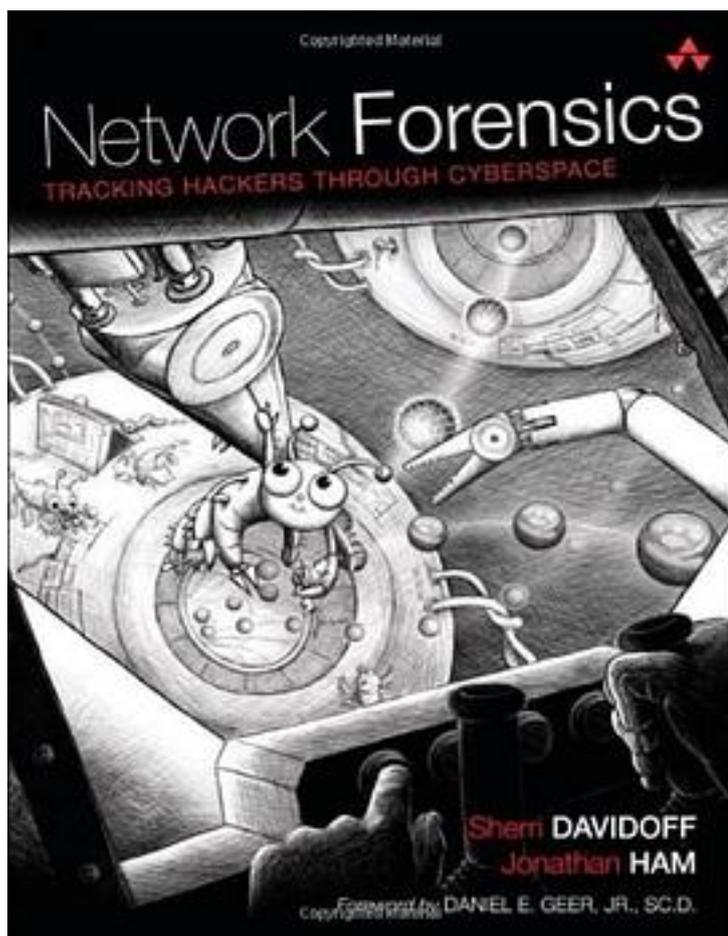


# Network Forensics



[Network Forensics\\_ 下载链接1](#)

著者:Davidoff, Sherri; Ham, Jonathan;

出版者:

出版时间:2012-6

装帧:

isbn:9780132564717

"This is a must-have work for anybody in information security, digital forensics, or involved with incident handling. As we move away from traditional disk-based analysis into the interconnectivity of the cloud, Sherri and Jonathan have created a framework

and roadmap that will act as a seminal work in this developing field." - Dr. Craig S. Wright (GSE), Asia Pacific Director at Global Institute for Cyber Security + Research. "It's like a symphony meeting an encyclopedia meeting a spy novel." -Michael Ford, Corero Network Security On the Internet, every action leaves a mark-in routers, firewalls, web proxies, and within network traffic itself. When a hacker breaks into a bank, or an insider smuggles secrets to a competitor, evidence of the crime is always left behind. Learn to recognize hackers' tracks and uncover network-based evidence in Network Forensics: Tracking Hackers through Cyberspace. Carve suspicious email attachments from packet captures. Use flow records to track an intruder as he pivots through the network. Analyze a real-world wireless encryption-cracking attack (and then crack the key yourself). Reconstruct a suspect's web surfing history-and cached web pages, too-from a web proxy. Uncover DNS-tunneled traffic. Dissect the Operation Aurora exploit, caught on the wire. Throughout the text, step-by-step case studies guide you through the analysis of network-based evidence. You can download the evidence files from the authors' web site (lmgsecurity.com), and follow along to gain hands-on experience. Hackers leave footprints all across the Internet. Can you find their tracks and solve the case? Pick up Network Forensics and find out.

作者介绍:

目录:

[Network Forensics\\_ 下载链接1](#)

标签

Security

计算机网络

网络取证

analysis

Wireshark

Tools

2012

评论

-----  
[Network Forensics\\_下载链接1](#)

书评

-----  
[Network Forensics\\_下载链接1](#)