Malware Forensics Field Guide for Windows Systems

Digital Forensics Field Guides

Cameron H. Malin
Eoghan Casey
James M. Aquilina

Curtis W. Rose, Technical Editor

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

SYNGRESS.

Contents

5. File Identification and Profiling

6. Analysis of a Malware Specimen