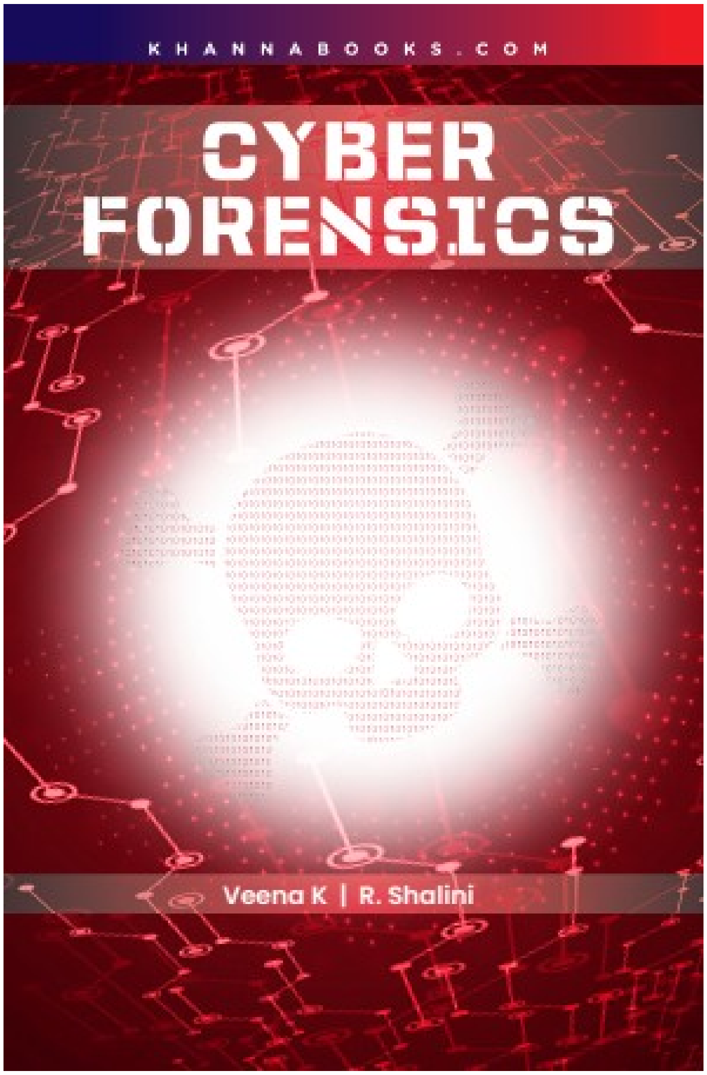
KHANNABOOKS.COM



Cyber Forensics

Author :	R. Shalini
ISBN 13 :	978-93-55385-44-4
ISBN 10 :	93-55385-44-7
E-ISBN 13 :	978-93-55385-44-4
Edition :	First
Pages :	88
Type of book :	Paperback
Year :	2025
Language :	English
Publisher :	Khanna Publishing House
M.R.P :	Rs 148.00
Categories :	Satyabhama Series
Condition Type :	New
Country Origin :	India

Product Description

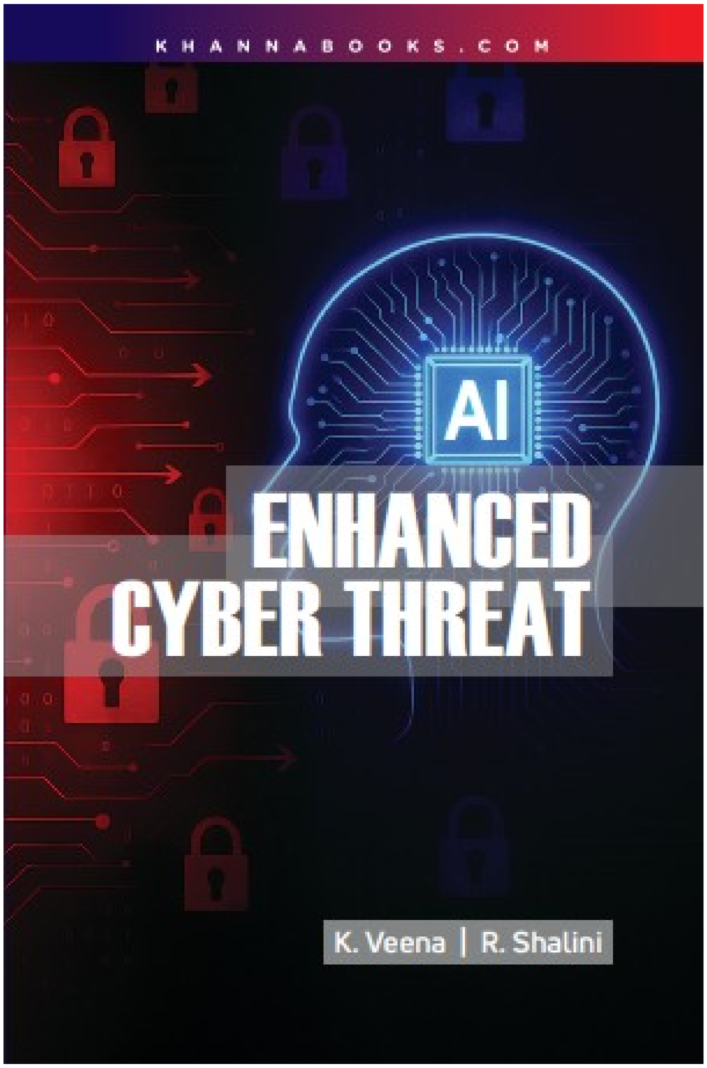
CYBER FORENSICS This book,” CYBER FORENSICS,” serves as comprehensive and essential guide to the rapidly evolving field of digital crime investigation. It is specifically structured to align with the curriculum for BE CSE students specializing in cyber security, but its rigorous methodology makes it indispensable for law enforcement, IT security specialists, and aspiring forensic professionals. The book’s core theme revolves around the systematic process of identifying, collecting, analyzing, and preserving electronic evidence to ensure its integrity and legal admissibility in court. It establishes a robust foundation by detailing the history of computer crime, the critical intersection of technology and law, and the fundamentals of professional forensic methodology. Moving beyond theory, the text provides in-depth coverage of specialized forensic domains, including disk, network, memory, and mobile forensics. Readers gain practical expertise through detailed explorations of advanced topics such as window registry analysis, cloud forensics, and virtual machine forensics. The practical value is significantly enhanced by incorporating hands-on case studies and demonstrating the use of open-source forensic tools. This approach equips readers with the skills needed to navigate the complex challenges of investigative reconstruction, analyze criminal modus operandi, and secure justice in the digital world. **Salient Features:**

- **Foundational Protocols**: covers the history and terminology of computer crime, establishes the investigative process, and details the crucial intersection of technology and law for evidence admissibility.
- **Advanced Domains**: Provides deep dives into specialized areas like memory forensics, cloud storage analysis, and virtual machine forensics, preparing students for complex, modern cyber-investigations.
- **Practical Tools & Techniques**: integrates learning on essential forensic software such as Wireshark, bulk extractor, and YARA through engaging case studies, emphasizing real-world tool application.
- **Evidence Life Cycle**: Emphasizes the forensic methods for identifying, collecting, and preserving electronic data, along with crucial steps like forensic imaging and maintaining the chain of custody.
- **Data Artifact Analysis**: Explores the structure of storage devices, including SSD devices, and teaches the extraction and analysis artifacts, hidden data, and file signatures.
- **Criminal Profiling**: Focuses on investigative reconstruction techniques, analyzing the modus operandi

Table of Contents

Author

Dr. Veena k Associate Professor Dept Of CSE, Sathyabama Institute of Science and Technology **Dr. R Shalini** Associate Professor Dept Of CSE, Sathyabama Institute of Science and Technology



AI Enhanced Cyber Threat

Author :	R. Shalini
ISBN 13 :	978-93-55388-24-7
ISBN 10 :	93-55388-24-1
E-ISBN 13 :	978-93-55388-24-7
Edition :	First
Pages :	100
Type of book :	Paperback
Year :	2025
Language :	English
Publisher :	Khanna Publishing House
M.R.P :	Rs 148.00
Categories :	Satyabhama Series
Condition Type :	New
Country Origin :	India

Product Description

AI Enhanced Cyber Threat In the rapidly evolving digital landscape. Artificial intelligence (AI) presents a double – edged sword. While it serves as the foundation for next-generation defense systems. It is simultaneously being weaponized by adversaries to create sophisticated, adaptive, and highly evasive cyber threats.AI Enhanced cyber threats offers a vital, comprehensive analysis of this critical intersection. This book meticulously explores the emerging methodologies where Ai and Machine Learning are used to launch automated spear-phishing campaigns, craft polymorphic malware, and bypass conventional security measures. Crucially, it provides IT professionals, security analysis, and researchers with actionable, cutting-edge strategies to counter these advanced threats.From implementing adversarial training to fortify defense models to establishing secure deployment practices in complex IoT and cloud environments, this text is the definitive guide to building an intelligent, resilient, and adaptive cybersecurity posture in the AI age. **Salient Features:**

- **Comprehensive threat analysis:** In-depth exploration of how adversaries utilize AI to automate attacks, enhance phishing efficacy, and deploy adaptive malware.
- **Advanced Mitigation Strategies:** Detailed coverage of AI-powered defense mechanisms, including Adversarial training to improve model resilience against attacks.
- **Real-time security implementation:** Focus on deploying AI-powered anomaly detection systems for continuous, real-time monitoring ongoing compliance in modern infrastructure.
- **Secure IoT and cloud deployment:** best practices for secure configuration of cloud services, network segmentation, and ensuring ongoing compliance in modern infrastructure.
- **Data security fundamentals:** Insights on establishing effective patch management processes and conduction regular security audits and risk assessments.
- **Ideal for:** undergraduate and postgraduate students, researchers, cybersecurity professionals, and network administrators seeking to master the principles of AI-driven security.

Table of Contents

Author

Dr. R. Shalini Associate Professor, Dept of CSE, Sathyabama Institute Of Science and technology **Dr. K. Veena** Associate professor, Dept of CSE, Sathyabama Institute Of science and technology