

COMPUTER FORENSICS

Dr. H. Shaheen

(Associate Professor, CSE Department)

St. Peter's Engineering College, Hyderabad, (Telangana), INDIA

Dr. Rajasekar Rangasamy

(Professor, CSE Department)

St. Peter's Engineering College, Hyderabad, (Telangana), INDIA

Dr. T. Sreenivasulu

(Professor, CSE Department)

St. Peter's Engineering College, Hyderabad, (Telangana), INDIA

Mr. T. Vijaykanth Reddy

(Assistant Professor, CSE Department)

St. Peter's Engineering College, Hyderabad, (Telangana), INDIA

COMPUTER FORENSICS

Copyright © : Dr. H. Shaheen
Publishing Right (P) : VSRD Academic Publishing
A Division of Visual Soft India Private Limited

ISBN-13: 978-93-87610-23-1

FIRST EDITION, SEPTEMBER 2018, INDIA

Printed & Published by:

VSRD Academic Publishing

A Division of Visual Soft India Private Limited

Disclaimer: The author(s) are solely responsible for the contents compiled in this book. The publishers or its staff do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the Authors or Publishers to avoid discrepancies in future.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the Publishers & Author.

Printed & Bound in India

VSRD ACADEMIC PUBLISHING

A Division of Visual Soft (India) Pvt. Ltd.

REGISTERED OFFICE

154, Tezabmill Campus, Anwarganj, KANPUR – 208 003 (UP) (INDIA)
Mob.: +91 9899936803 || Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

MARKETING OFFICE

340, First Floor, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI – 400 053 (MH) (INDIA)
Mob.: +91 9956127040 || Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

PREFACE

This book entitled “**Computer Forensics**” has been written in accordance with the syllabus prescribed by the ‘JNTUH R2013 ’ for the Final Year, B.Tech students of Engineering colleges affiliated to JNTUH.

This book comprises of five chapters which covers Jawaharlal Nehru Technological University ,Hyderabad syllabus. The main emphasis of the book is to explain in a simple manner, the logical concepts that will enable even the beginners to understand them without difficulty.

Systematic care has been taken to support the topics with necessary illustrations and relevant diagrams to make learning much easier. It is believed that this book shall serve all the requirements of Final Year Engineering students.

It covers all the important questions that have appeared in the previous years of Jawaharlal Nehru Technological University, Hyderabad Examinations. University questions for regulations R2013 are given at the end.

Your suggestions are most welcome

✍ Dr. H. Shaheen

✍ Dr. Rajasekar Rangasamy

✍ Dr. T. Sreenivasulu

✍ Mr. T. Vijaykanth Reddy

ACKNOWLEDGEMENT

We sincerely thank the Almighty for being with us through all stages of the preparation of this book.

Firstly, we would like to express our sincere gratitude to the **The Chairman T.Bala Reddy, St.Peters Engineering College** for the continuous support motivation, and immense knowledge.

Special Acknowledgement is due to our **Secretary Mr. T.V. Reddy, St.Peters Engineering College** for his continuous support for the successful completion of this book.

We thank **Dr. M. Narendra Kumar, Principal, St.Peters Engineering College** for his source of inspiration.

We thank **Dr. M. Saradha Varalakshmi, Head of the Department**, who have always supported and motivated us to accomplish this incredible work.

Our Special thanks to all our Friends and Colleagues for their encouragement and support in various stages of writing this book.

We express our sincere thanks to our publisher **VSRD Academic Publishing (A Division of Visual Soft India Private Limited)**, for their help and co-operation in publishing this book.

✍ Dr. H. Shaheen

✍ Dr. Rajasekar Rangasamy

✍ Dr. T. Sreenivasulu

✍ Mr. T. Vijaykanth Reddy

CONTENTS

CHAPTER 1 : COMPUTER FORENSICS FUNDAMENTALS, TYPES, EVIDENCE AND CAPTURE.....	1
1.1. WHAT IS COMPUTER FORENSICS?	1
1.2. ELECTRONIC OR DIGITAL OR COMPUTER EVIDENCE	1
1.3. ROLE OF A COMPUTER IN A CRIME.....	2
1.4. SOME IMPORTANT POINTS REGARDING COMPUTER FORENSICS.....	3
1.5. COMPUTER FORENSICS ASSISTANCE TO HUMAN RESOURCES/ EMPLOYMENT PROCEEDINGS.....	4
1.6. COMPUTER FORENSICS SERVICES	5
1.7. BENEFITS OF PROFESSIONAL FORENSIC METHODOLOGY	7
1.8. TYPES OF MILITARY COMPUTER FORENSIC TECHNOLOGY	7
1.9. COMPUTER FORENSIC EXPERIMENT-2000 (CFX-2000).....	7
1.10. TYPES OF LAW ENFORCEMENT COMPUTER FORENSIC TECHNOLOGY	8
1.11. TYPES OF BUSINESS COMPUTER FORENSIC TECHNOLOGY.....	10
1.12. REFINING AND MODIFYING THE INVESTIGATION PLAN.....	13
1.13. SEARCH AND REPORT FUNCTIONS OF ACCESS DATA FORENSIC TOOLKIT (FM).....	13
1.14. TOOL COMPARISONS.....	17
1.15. TASKS PERFORMED BY COMPUTER FORENSICS TOOLS	19
1.16. COMPUTER FORENSICS EVIDENCE AND CAPTURE	20
1.17. THE ROLE OF BACK-UP IN DATA RECOVERY	22
1.18. THE DATA RECOVERY SOLUTION	24
CHAPTER 2 : EVIDENCE COLLECTION AND DATA SEIZURE, DUPLICATION AND PRESERVATION OF DIGITAL EVIDENCE, COMPUTER IMAGE AND VERIFICATION AND AUTHENTICATION	27
2.1. WHY COLLECT EVIDENCE?.....	27
2.2. COLLECTION OPTIONS	27
2.3. OBSTACLES IN COLLECTING EVIDENCE.....	28
2.4. TYPES OF EVIDENCE	28
2.5. DUPLICATION AND PRESERVATION OF DIGITAL EVIDENCE.....	33
2.6. COMPUTER EVIDENCE PROCESSING STEPS	33
2.7. LEGAL ASPECTS OF COLLECTING AND PRESERVING COMPUTER FORENSIC EVIDENCE.	35
2.8. EVIDENCE COLLECTION PROCEDURE	36
2.9. COMPUTER IMAGE VERIFICATION AND AUTHENTICATION	38

2.10.	ILLUSTRATIVE EXAMPLE USING MICROSOFT AUTHENTIC + VERISIGN DIGITAL SIGNATURES	42
2.11.	TIME STAMPING	43
2.12.	SECURITY CONSIDERATIONS	45

CHAPTER 3 : COMPUTER FORENSICS ANALYSIS AND VALIDATION, NETWORK FORENSICS, PROCESSING CRIME AND INCIDENT SCENES..... 46

3.1.	DETERMINING WHAT DATA TO ANALYZE AND COLLECT.....	46
3.2.	VALIDATING FORENSIC DATA	47
3.3.	LIVE ACQUISITIONS	49
3.4.	PROCESSING AND HANDLING DIGITAL EVIDENCE	66

CHAPTER 4 : CURRENT COMPUTER FORENSIC TOOLS, EMAIL INVESTIGATIONS, CELL PHONE AND MOBILE DEVICE FORENSICS ... 69

4.1.	CURRENT COMPUTER FORENSIC TOOLS	69
4.2.	EVALUATING COMPUTER FORENSICS TOOL NEEDS	69
4.3.	TASKS PERFORMED BY COMPUTER FORENSICS TOOLS.....	70
4.4.	ACQUISITION	70
4.5.	VALIDATION AND DISCRIMINATION	71
4.6.	EXTRACTION	71
4.7.	RECONSTRUCTION	72
4.8.	PRO DISCOVER.....	73
4.9.	COMPUTER FORENSICS SOFTWARE TOOLS.....	76
4.10.	EMAIL INVESTIGATION	81
4.11.	EXPLORING THE ROLE OF E-MAIL IN INVESTIGATIONS.....	83
4.12.	GUIDELINES.....	96
4.13.	SECURITY OF MOBILE DEVICES.....	97

CHAPTER 5 : WORKING WITH WINDOWS AND DOS SYSTEMS 99

5.1.	UNDERSTANDING DISK DRIVES.....	99
5.2.	EXAMINING FAT DISKS.....	102
5.3.	EXAMINING THIRD-PARTY DISK ENCRYPTION TOOLS	111
5.4.	UNDERSTANDING THE WINDOWS REGISTRY	111
5.5.	STARTUP IN WINDOWS NT AND LATER	113
5.6.	UNDERSTANDING MS-DOS STARTUP TASKS	114

QUESTION PAPERS..... 115