

---

# **INVESTIGATING BY COMPUTER SECOND EDITION**

---



Association of Certified Fraud Examiners

GLOBAL HEADQUARTERS • THE GREGOR BUILDING  
716 WEST AVE • AUSTIN, TX 78701-2727 • USA

TABLE OF CONTENTS

**I. INTRODUCTION**

Learning Objectives .....1  
About the Supplemental Documents .....1

**II. INVESTIGATING WITH THE INTERNET**

What Is the Internet? .....3  
    Brief History of the Internet .....3  
    Glossary of Terms .....6  
Accessing Information Online .....9  
    Pitfalls of Conducting Investigations on the Internet .....10  
    Using Internet Search Engines to Find Information .....10  
    People and Username Search Sites .....13  
    Advanced Search (Boolean) Operators .....14  
    Using Online Directories to Find Information .....18  
    Using the Deep Web to Find Information .....18  
    Using the Internet Archives to Find Web Pages That Have Been Deleted or Revised .....19  
    Using Social Media Sites to Find Information .....20  
    Video .....22  
    Messaging Sites or Applications .....25  
    Using Nontraditional Methods for Finding Information on the Internet .....26  
    Online Communities .....28  
    Image Searching .....29  
    Utilizing Online Maps .....31  
Review Questions .....34

**III. SOURCES OF INFORMATION**

Public Versus Nonpublic Records .....37  
    Public Records .....37  
    Nonpublic Records .....39  
Common Types of Public Records .....40  
    Local Records .....40  
    Property Records .....42  
    Video .....42  
    Court Records .....44  
    Corporate Records .....47  
    Other Agency Records .....49  
    Video .....52  
Nonpublic Records .....52  
    Types of Nonpublic Records .....52  
    Gaining Access to Nonpublic Records .....56  
    Laws Governing Access to Certain Types of Information .....57  
Review Questions .....58

**IV. ACCESSING PUBLIC RECORDS ONLINE**

Sources of Public Records .....63  
    Government Sources .....63  
    Commercial Public Record Database Vendors.....63  
    Investigative Service Companies.....68  
    Video .....69  
Using Online Sources to Conduct Specific Types of Searches.....69  
    Finding Assets Using Online Records.....69  
    Search for Asset Potential Using Online Records.....72  
    Locating People Using Online Records .....72  
    Finding Legal Records Online .....73  
    Conducting Background Checks Online.....74  
    Finding Corporate Records Online .....76  
    Video .....77  
Review Questions .....80

**V. INVESTIGATING WITH DATA ANALYSIS TOOLS**

Introduction.....83  
    Video .....83  
    Big Data .....84  
    Structured Versus Unstructured Data .....84  
    Database Management Systems.....85  
Data Mining .....85  
    Video .....87  
Data Analytics and Fraud.....87  
    Applying Fraud Knowledge to Data Analysis .....88  
    Effective Approaches to Data Analysis.....88  
    Advantages of Using Data Analytics to Detect Fraud .....88  
    Barriers to Using Data Analytics to Detect Fraud .....89  
The Data Analysis Process .....93  
    Video .....94  
    Planning Phase.....94  
    Preparation Phase.....95  
    Testing and Interpretation Phase .....98  
    Post-Analysis Phase .....99  
Using Data Analysis Software .....100  
    Advantages of Using Data Analysis Software.....100  
    Data Analysis Software Functions .....101  
    Video .....108  
    Examples of Data Analysis Queries.....112  
    Data Analysis Checklist .....114  
    Advanced Data Analytics.....115  
Textual Analytics.....117  
    Textual Analysis Techniques .....118  
    Textual Analytics Implementation Challenges.....122

**V. INVESTIGATING WITH DATA ANALYSIS TOOLS (CONT.)**

Visual Analytics..... 122

- Bar Graphs..... 122
- Timelines ..... 123
- Flow Charts..... 124
- Pie Charts..... 124
- Heat Maps..... 125
- Link Analysis..... 125
- Geospatial Analysis..... 126
- Word Clouds..... 127

Evaluating Data Analysis Software ..... 127

- Evaluating Data Analytics Software..... 127
- Tailoring Data Analytics Software for Your Organization..... 128
- Evaluating Data Mining Consultants..... 129
- Video ..... 129

Types of Data Mining and Analysis Software..... 129

- Galvanize..... 130
- CaseWare IDEA..... 130
- Excel..... 131
- ActiveData for Excel..... 131
- AutoAudit..... 132
- Altair Monarch ..... 133
- Arbutus..... 134
- Oversight ..... 134
- SAS..... 134
- Tableau..... 135
- IBM Analytics ..... 135

Spreadsheet Software..... 135

- Spreadsheet Basics ..... 135
- Video ..... 136
- Limitations of Spreadsheet Software..... 137

Reporting and Case Management Software..... 137

- IBM’s i2 Analysis Product Line..... 138
- CaseMap by LexisNexis..... 138
- Actimize Enterprise Risk Case Manager ..... 139
- Xanalys Suite ..... 139
- World-Check..... 140
- GlobalVision Systems..... 140
- NetReveal ..... 140
- i-Sight Case Management Software..... 140
- Navex Global’s EthicsPoint Issue and Event Manager ..... 141

Review Questions..... 142

**VI. INVESTIGATING WITH DIGITAL FORENSICS**

Digital Forensics Versus Digital Investigations.....	149
Digital Forensic Experts.....	150
Video .....	153
Digital Evidence.....	153
Volatility of Digital Evidence .....	153
Video .....	155
Understanding File Systems.....	156
Types of File Systems.....	157
Locating Relevant Data .....	159
Computer Systems.....	159
Workstations .....	170
Networks.....	172
Smartphones.....	173
Cloud Environments.....	176
Hash Values .....	176
Email Forensics.....	177
Web-Based Email .....	177
Email Archives.....	177
Tracing Emails.....	178
Digital Forensic Investigations .....	183
Planning .....	184
Seizing.....	185
Imaging .....	196
Processing.....	197
Analyzing .....	198
Reporting and Testifying.....	199
Investigating in the Cloud.....	199
Challenges of Cloud Forensics .....	199
Conclusion.....	202
Mobile Forensic Investigations.....	203
Plan .....	204
Seize.....	205
Extract .....	206
Analyze .....	207
Document .....	208
Report and Testify .....	208
Digital Forensics Software.....	208
Keystroke Logging .....	208
EnCase Forensic.....	210
Forensic ToolKit.....	210
Password Recovery Toolkit.....	211
ProDiscover Forensics .....	211
StegoHunt Suite .....	212
E3 from Paraben.....	212

**VI. INVESTIGATING WITH DIGITAL FORENSICS (CONT.)**

X-Ways Forensic from X-Ways Software Technology.....	212
Open-Source Forensic Products.....	213
Mobile Device Forensic Tools.....	213
Review Questions.....	215

**VII. LEGAL ISSUES AFFECTING COMPUTER INVESTIGATIONS**

Introduction.....	219
Laws Governing Access to Information.....	219
Privacy Rights.....	220
Employees' Privacy Rights.....	220
Sector-Specific Privacy Laws.....	220
Invasion of Privacy Laws.....	220
Human Rights Legislation in the European Union.....	221
Data Privacy Laws.....	221
International Data Transfers.....	226
Privacy and Social Media.....	228
U.S. Laws Governing Access to Information.....	228
Video.....	236
U.S. Laws Related to Computer Crimes.....	240
Admissibility of Digital Evidence.....	242
Common Law Versus Civil Law Legal Systems.....	242
Requirement of Relevance.....	243
Requirement of Authentication.....	243
Chain of Custody.....	247
The Best-Evidence Rule.....	249
Review Questions.....	251

**VIII. PRACTICAL EXERCISES**

Internet Exercises.....	255
Newspaper Sites.....	255
University and Library Databases.....	255
Business and Individual Searches.....	256
Maps.....	256
Search Engine and Directory Searches.....	257
Legal Information.....	257
Government Websites.....	257
Vital Records.....	258
Using Your Spreadsheet.....	259
Formula Exercise.....	260
Sorting Exercise.....	261
Using a Spreadsheet for Horizontal and Vertical Analysis.....	263
Vertical Analysis Discussion.....	266
Horizontal Analysis Discussion.....	266

<b>IX. NELSON BUILDING COMPANY CASE</b> .....	267
<b>X. APPENDIX A: VIDEO TRANSCRIPTS</b> .....	289
<b>XI. APPENDIX B: USEFUL WEBSITES</b> .....	303
<b>XII. SOLUTIONS TO REVIEW QUESTIONS</b>	
II. Investigating with the Internet.....	305
III. Sources of Information .....	312
IV. Accessing Public Records Online .....	321
V. Investigating with Data Analysis Tools .....	325
VI. Investigating with Digital Forensics.....	338
VII. Legal Issues Affecting Computer Investigations.....	346
<b>XIII. SOLUTIONS TO NELSON BUILDING COMPANY CASE</b> .....	353
<b>XIV. INVESTIGATING BY COMPUTER FINAL EXAMINATION</b> .....	E-1
<b>XV. INDEX</b> .....	I-1