Welcome to my web page! I've been a web developer for several years, and I'm excited to share my knowledge with you. Here are some examples of projects I've worked on:

- Project A: A web application for managing customer orders.
- Project B: A mobile app for tracking fitness goals.
- Project C: A social media platform for connecting with friends.

I'm also passionate about teaching web development. If you're interested in learning more, feel free to reach out to me on LinkedIn or through my email address.
Chapter 3 TRADITIONAL COMPUTER CRIME: EARLY HACKERS AND THEFT OF COMPONENTS  

I. Introduction 52
II. Traditional Problems 52
III. Recognizing and Defining Computer Crime 54
IV. Three Incidents 55
V. Phreakers: Yesterday's Hackers 59
   a. What Is Phreaking? 59
   b. The War on Phreaking 60
VI. Hacking 61
   a. Defining Hacking 62
   b. Evolution in the Hacking Community 62
   c. Contemporary Motivation 63
   d. Hierarchy of Contemporary Cybercriminals 65
VII. Computers as Commodities 67
   a. Hardware 67
VIII. Theft of Intellectual Property 69
   a. Software 69
   b. Film Piracy 71
XI. Conclusions 71
   Discussion Questions 72 • Recommended Reading 72 • Web Resources 72 • Endnotes 73

Chapter 4 CONTEMPORARY COMPUTER CRIME 74

I. Web-Based Criminal Activity 75
   a. Interference with Lawful Use of Computers 76
II. Malware 77
   a. Viruses and Worms 78
   b. DoS and DDoS Attacks 80
   c. Botnets and Zombie Armies 80
Chapter 5 IDENTITY THEFT AND IDENTITY FRAUD 114

I. Introduction 115

II. Typologies of Identity Theft/Fraud 116
   a. Assumption of Identity 117
   b. Theft for Employment and/or Border Entry 118
   c. Criminal Record Identity Theft/Fraud 119
   d. Virtual Identity Theft/Fraud 120
   e. Credit Identity Theft/Fraud 121

III. Prevalence and Victimology 122
   a. Victims and the Costs Associated with Victimization 123
   b. Future Increases 125

IV. Physical Methods of Identity Theft 126
   a. Mail Theft 126
   b. Dumpster Diving 127
   c. Theft of Computers 128
   d. Bag Operations 129
   e. Child Identity Theft 130
   f. Insiders 131
   g. Fraudulent or Fictitious Companies 131
   h. Card Skimming, ATM Manipulation, and Fraudulent Machines 132

V. Virtual or Internet-Facilitated Methods 132
   a. Phishing 133
   b. Spyware and Crimeware 135
c. Keyloggers and Password Stealers 136
d. Trojans 137

VI. Crimes Facilitated by Identity Theft/Fraud 138
   a. Insurance and Loan Fraud 139
   b. Immigration Fraud and Border Crossings 139

VII. Conclusions and Recommendations 141
    Discussion Questions 143 • Recommended Reading 143
    • Web Resources 144 • Endnotes 144

Chapter 6 TERRORISM AND ORGANIZED CRIME 146

I. Terrorism 147
   a. Defining Terrorism 148
   b. Classification Through Motivation 149
   c. Roots of Contemporary Terrorism 150
   d. Terrorism as a Stage 151
   e. Cyberterrorism as a Concept 152

II. Terror Online 153
    a. Propaganda, Information Dissemination, Recruiting,
       and Fundraising 154
    b. Training 156
    c. Research and Planning 157
    d. Communication 158
    e. Attack Mechanism 159

III. Terrorism and Crime 164
    a. Criminal Activities 164
    b. Criminalizing Terrorist Acts 164
    c. Government Efforts 165
    d. Conclusions 165

IV. Organized Crime 167
    a. Defining Organized Crime 167
    b. Distinguishing Organized Crime from Cybergangs 172

V. Organized Crime and Technology 174
    a. Extortion 175
    b. Cargo Heists and Armed Robbery 175
    c. Fraud 176
    d. Money Laundering 177
    e. The Sex Trade 177
    f. Confidence Scams 178
    g. Fencing of Stolen Property 179
    h. Data Piracy and Counterfeit Goods 179
    i. Human Smuggling 181

VI. Confronting Contemporary Organized Crime 182

VII. The Intersection of Organized Crime and Terrorism 182
    Discussion Questions 184 • Recommended Reading 184
    • Web Resources 185 • Endnotes 185
Chapter 7 AVENUES FOR PROSECUTION AND GOVERNMENT EFFORTS 187

I. Introduction 188

II. Traditional Statutes 189

III. The Evolution of Computer-Specific Statutes 189
   a. Computer Fraud and Abuse Act of 1986 191
   b. National Information Infrastructure Protection Act of 1996 (NIIPA) 193

IV. Evolving Child Pornography Statutes 193

V. Identity Theft and Financial Privacy Statutes 195
   a. Identity Theft and Assumption Deterrence Act of 1998 195
   b. The Financial Modernization Act of 1999 195
   c. Fair and Accurate Credit Transactions Act (FACTA) 2003 196
   d. Identity Theft Penalty Enhancement Act of 2004 197
   e. Identity Theft Enforcement and Restitution Act of 2008 198
   f. Additional Efforts to Protect Personal Information 198

VI. Federally Funded Initiatives and Collaborations 199

VII. Law Enforcement Operations and Tools in the United States 201
   a. Packet Sniffers and Key Loggers 202
   b. Data Mining 202
   c. Collaborations and Professional Associations 206

VIII. International Efforts 207
   a. OECD and the Select Committee of Experts on Computer-Related Crime of the Council of Europe 208
   b. Council of Europe’s (CoE) Cybercrime Conventions 209

IX. Conclusions 212

Discussion Questions 213 • Recommended Reading 213
• Web Resources 213 • Endnotes 214

Chapter 8 APPLYING THE FIRST AMENDMENT TO COMPUTER-RELATED CRIME 215

I. Introduction and General Principles 216

II. Obscenity in General 216

III. Traditional Notions of Decency 217

IV. Emerging Statutes and the Availability of Obscene Material to Children 218

V. Traditional Attempts to Criminalize Child Pornography 220

VI. Applying Case Law to Traditional Child Pornography Statutes 220
   a. New York v. Ferber 221
   b. Osborne v. Ohio 222
VII. Technology-Specific Legislation—Contention in the Courts 224
   a. Child Pornography Prevention Act 224
   b. Ashcroft v. Free Speech Coalition 225
   c. Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act (PROTECT) 227
   d. U.S. v. Williams 228

VIII. Internet Gambling 228
   a. Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) 229
   b. Case law on Internet Gaming Statutes 229
   c. Lack of International Cooperation and the WTO 230

IX. Future Issues and Conclusions 231
   Discussion Questions 232 • Recommended Reading 232 • Web Resources 232 • Endnotes 232

Chapter 9 THE FOURTH AMENDMENT AND OTHER LEGAL ISSUES 234

I. The Fourth Amendment 235
   a. Probable Cause 236
   b. Reasonable Suspicion 236

II. Warranted Searches and Computers 237
   a. Particularity 237
   b. Seizure of Evidence 239
   c. Third-Party Origination 240
   d. Other Arguments Used in Warranted Searches 241

III. Warrantless Searches 242
   a. Consent 242
   b. Exigent Circumstances and Emergency Situations 242
   c. Incident to Arrest 244
   d. Plain View 244
   e. Border Searches 245
   f. Other Warrantless Searches 246

IV. Exclusionary Rule 246

V. Electronic Surveillance and the Right to Privacy 247
   a. Types of Recognized Privacy 247

VI. Private versus Public Sector Searches 248

VII. Application of Ortega to E-mail: The Cases of Simons and Monroe 249

VII. The Electronic Communications Privacy Act and The Privacy Protection Act of 1980 250
   a. Electronic Communications Privacy Act of 1986 250
   b. Three Titles under ECPA 251
   c. Privacy Protection Act 253
   d. Defining Interception under ECPA and the PPA 254
Chapter 10 COMPUTER FORENSICS: TERMINOLOGY AND REQUIREMENTS 267

I. Computer Forensics—An Emerging Discipline 268

II. Traditional Problems in Computer Investigations 269
   a. Inadequate Resources 270
   b. Lack of Communication and Cooperation among Agencies 270
   c. Over-reliance on Automated Programs and Self-proclaimed Experts 271
   d. Lack of Reporting 271
   e. Evidence Corruption 271

IV. Disk Structure and Digital Evidence 272
   a. Disk Structure and Data Storage 273
   b. Partition Table 275
   c. File Systems 276
   c. Firmware—Operating Instructions 277
   e. Data Integrity 279

V. Developing Computer Forensic Science Capabilities 279

VI. Minimum Housing Requirements 281

VII. Minimum Hardware Requirements 282

VIII. Minimum Software Requirements 285
   a. Data Preservation, Duplication, and Verification Tools 285
   b. Data Recovery/Extraction Utilities 287
   c. Data Analysis Software 290
Chapter 11 SEARCHING AND SEIZING COMPUTER-RELATED EVIDENCE 302
I. Traditional Problems Associated with Finding Digital Evidence 303
II. Pre-search Activities 304
a. Warrant Preparation and Application 306
b. Plan Preparation and Personnel Gathering 308
c. Preparing a Toolkit 311
d. Traditional Equipment 311
e. Computer-Specific Equipment and Materials 312
III. On-scene Activities 314
a. Knock, Notice, and Document 315
b. Securing the Crime Scene 315
c. Determining the Need for Additional Assistance 316
d. Scene Processing 316
e. Locating Evidence 320
f. Seizure and Documentation of Evidence 322
g. Bagging and Tagging 324
h. Interviewing Witnesses 326
i. Scene Departure and Transportation of Evidence to Lab 327
IV. Conclusions 327
Discussion Questions 328 • Recommended Reading 328 • Web Resources 328 • Endnotes 329

Chapter 12 PROCESSING OF EVIDENCE AND REPORT PREPARATION 330
I. Aspects of Data Analysis 336
a. Establish Forensically Sterile Conditions 336
b. Ensure Legitimacy and Capabilities of Analysis Tools 338
c. Physical Examination 338
d. Creation and Verification of Image 339
e. Jumping the CMOS Password 340
f. Short-Circuiting the Chip 340
g. Pulling the Battery 341
h. Recovering Passwords 342
i. Image Verification 342
j. Logical Examination 343
k. Restoration of Files 343
I. Listing of Files 344
  m. Examine Unallocated Space for Data Remnants 345
  n. Unlocking Files 345
  q. Examination of User Data Files 347
  r. Piping of Evidence 347
  s. Examination of Executable Programs 347
  t. Evidence from Internet Activity 348
II. Non-Windows Operating Systems 351
  a. Macintosh Operating System 351
  b. Linux/Unix Operating Systems 352
III. Smart Phones and GPS Forensics 353
    a. Smartphones 353
IV. A Sample of Popular Products 354
V. Navigation Systems 355
VI. Report Preparation and Final Documentation 356
VII. Conclusions 357
  Discussion Questions 357 • Recommended Reading 357
  • Web Resources 358 • Endnotes 358

Chapter 13 CONCLUSIONS AND FUTURE ISSUES 359
I. Traditional Problems and Recommendations 360
  a. Establishing Technology-Neutral Legislation 360
  b. Establishing Accountability for Internet Users 360
  c. Increasing Public Awareness and Research Capabilities 361
  d. Increasing Interagency and Intradepartmental Cooperation 361
  e. Developing Relationships between Investigative Agencies and the Private Sector 362
  f. Developing International Cooperation 362
  g. Standardization of Accreditation or Expertise 363
  h. Miscellaneous 364
II. Additional Approaches to Internet Crime 364
III. Future Trends and Emerging Concerns 366
  a. Wireless Communications 367
  b. Data Hiding: Remote Storage, Encryption, and the Like 367
  c. Governing Decency and Virtual Pornography 368
  d. Data Mining and Increased Interoperability 369
IV. Conclusions 371
  Discussion Questions 372 • Web Resources 372
  • Endnotes 372

Bibliography 373
Index 383