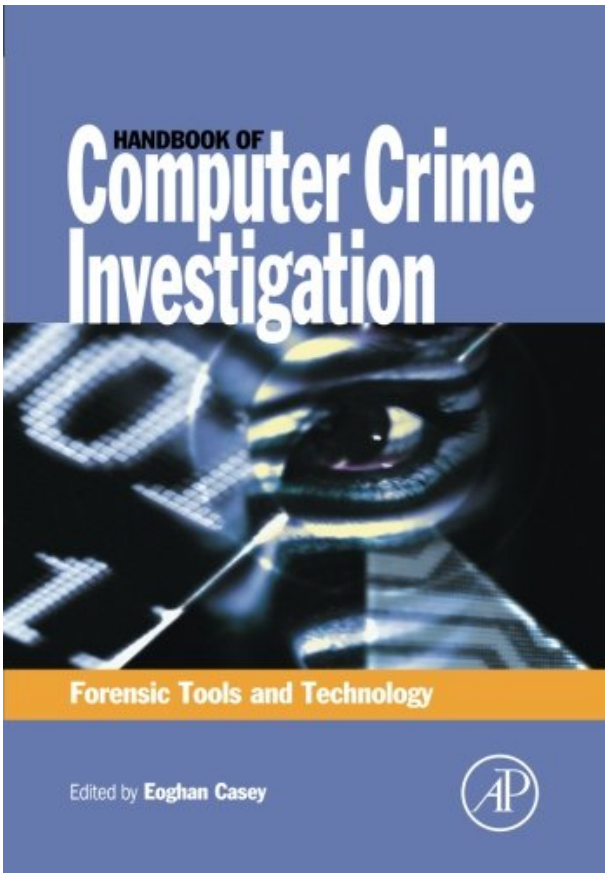
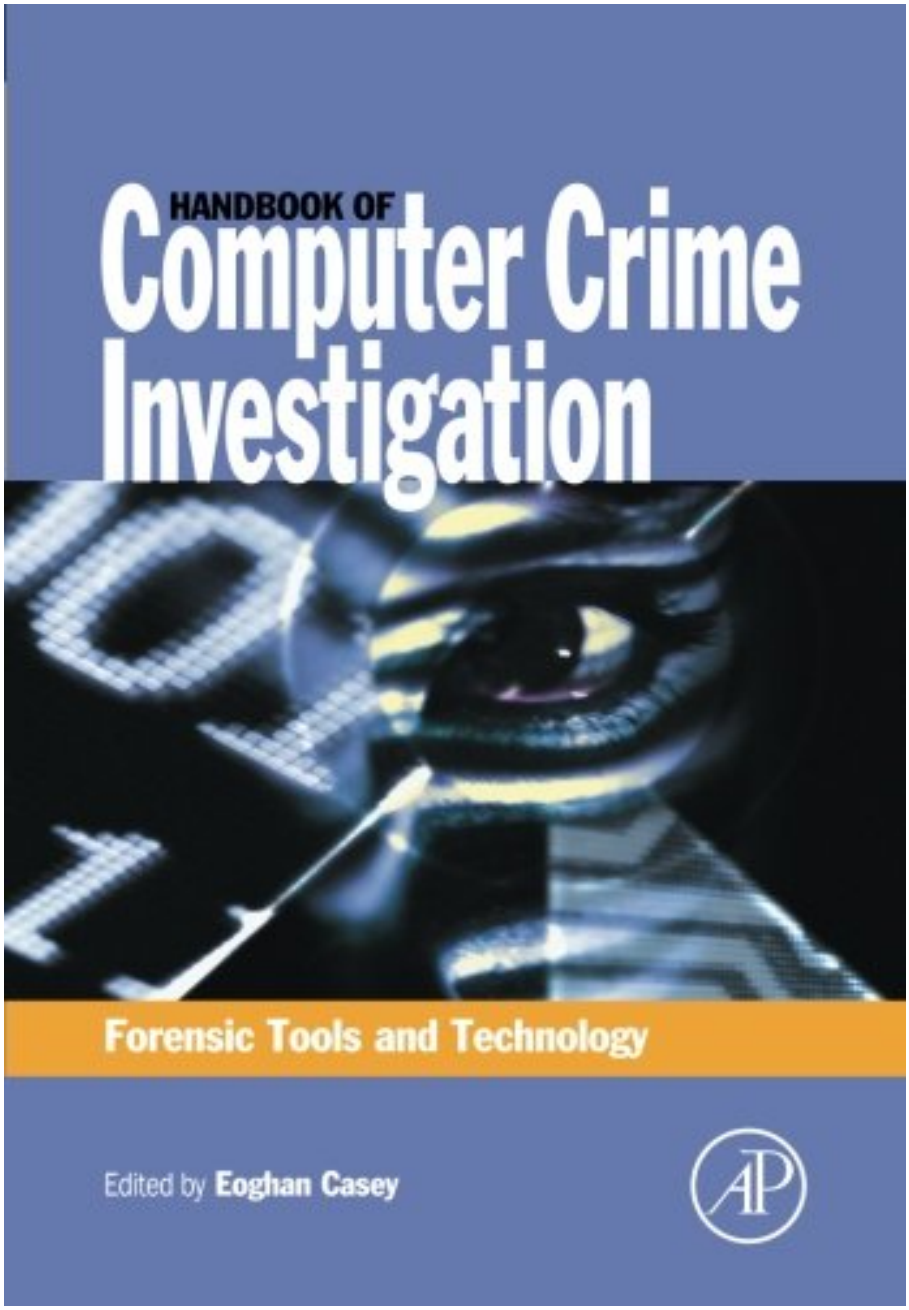
HANDBOOK OF COMPUTER CRIME INVESTIGATION: FORENSIC TOOLS AND TECHNOLOGY FROM ACADEMIC PRESS





HANDBOOK OF COMPUTER CRIME INVESTIGATION: FORENSIC TOOLS AND TECHNOLOGY FROM ACADEMIC PRESS PDF

Poses now this *Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press* as one of your book collection! However, it is not in your bookcase compilations. Why? This is guide Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press that is provided in soft documents. You can download and install the soft file of this magnificent book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press now as well as in the web link offered. Yeah, different with the other people that try to find book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press outside, you could obtain less complicated to pose this book. When some individuals still stroll into the establishment and also look guide Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press, you are below only stay on your seat as well as get the book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press.

Review

The audience for this book is obviously the legal and law enforcement communities, so any library serving them would find this an excellent introduction. Any law firm looking to get into the field would do well to start here. - E-Streams

Academic law, business or computer science collections will, however, find this book a useful introduction to an increasingly important field - even large public libraries will find an eager audience in an uncertain world. - E-Streams

From the Back Cover

Computers can be used in virtually any type of crime, ranging from cyberstalking and child pornography to financial fraud, espionage and terrorism. The Handbook of Computer crime investigation presents detailed technical information that can be used to help solve these crimes.

Following on the success of his introductory text, Digital Evidence and Computer Crime, Eoghan Casey has brought together an expert panel of authors to create this detailed guide for professionals who are already familiar with digital evidence. This unique handbook explains how to locate an utilize evidence in computer hard drives, shared networks, wireless devices, or embedded systems. The use of currently available high-tech tools is discussed and real case examples are provided.

To provide individuals with a deeper understanding of the forensic analysis of computer systems, three primary themes are treated:

Tools: Software and hardware for collecting and analyzing digital evidence are presented and their strengths and limitations are discussed. The section provides details on leading hardware and software programs-such as EnCase, Dragon, and ForensiX-with each chapter written by that product's creator.

Technology: This section provides the technical "how to" information for collecting and analyzing digital evidence in common situations, starting with computers, and Windows and Unix operating systems, progressing to network, wireless and embedded systems.

Case examples: These actual situations demonstrate the technical, legal, and practical challenges that arise in real computer investigations.

The Handbook of Computer Crime Investigation is an essential technical reference and on-the-job guide for professionals in computing, security and investigation, forensic science, legal and law enforcement communities.

About the Author

Eoghan Casey is an internationally recognized expert in data breach investigations and information security forensics. He is founding partner of CASEITE.com, and co-manages the Risk Prevention and Response business unit at DFLabs. Over the past decade, he has consulted with many attorneys, agencies, and police departments in the United States, South America, and Europe on a wide range of digital investigations, including fraud, violent crimes, identity theft, and on-line criminal activity. Eoghan has helped organizations investigate and manage security breaches, including network intrusions with international scope. He has delivered expert testimony in civil and criminal cases, and has submitted expert reports and prepared trial exhibits for computer forensic and cyber-crime cases.

In addition to his casework and writing the foundational book Digital Evidence and Computer Crime, Eoghan has worked as R&D Team Lead in the Defense Cyber Crime Institute (DCCI) at the Department of Defense Cyber Crime Center (DC3) helping enhance their operational capabilities and develop new techniques and tools. He also teaches graduate students at Johns Hopkins University Information Security Institute and created the Mobile Device Forensics course taught worldwide through the SANS Institute. He has delivered keynotes and taught workshops around the globe on various topics related to data breach investigation, digital forensics and cyber security.

Eoghan has performed thousands of forensic acquisitions and examinations, including Windows and UNIX systems, Enterprise servers, smart phones, cell phones, network logs, backup tapes, and database systems. He also has information security experience, as an Information Security Officer at Yale University and in subsequent consulting work. He has performed vulnerability assessments, deployed and maintained intrusion detection systems, firewalls and public key infrastructures, and developed policies, procedures, and educational programs for a variety of organizations. Eoghan has authored advanced technical books in his areas of expertise that are used by practitioners and universities around the world, and he is Editor-in-Chief of Elsevier's International Journal of Digital Investigation.

HANDBOOK OF COMPUTER CRIME INVESTIGATION: FORENSIC TOOLS AND TECHNOLOGY FROM ACADEMIC PRESS PDF

Book fans, when you require an extra book to read, discover the book **Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press** below. Never ever worry not to find just what you need. Is the Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press your required book now? That's true; you are truly a great user. This is an excellent book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press that comes from excellent writer to show to you. Guide Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press supplies the best encounter as well as lesson to take, not only take, but also learn.

Getting guides *Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press* now is not kind of difficult means. You could not just going with publication store or collection or borrowing from your buddies to review them. This is a very straightforward way to precisely obtain the publication by on the internet. This online e-book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press can be one of the options to accompany you when having extra time. It will certainly not lose your time. Believe me, guide will certainly reveal you new point to review. Merely spend little time to open this on-line book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press as well as review them anywhere you are now.

Sooner you obtain guide Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press, quicker you could delight in reviewing guide. It will be your count on maintain downloading the publication Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press in given web link. By doing this, you could truly making a decision that is worked in to obtain your personal publication on-line. Right here, be the very first to get the publication entitled Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press and also be the first to know how the author suggests the notification as well as expertise for you.

HANDBOOK OF COMPUTER CRIME INVESTIGATION: FORENSIC TOOLS AND TECHNOLOGY FROM ACADEMIC PRESS PDF

Following on the success of his introductory text, Digital Evidence and Computer Crime, Eoghan Casey brings together a few top experts to create the first detailed guide for professionals who are already familiar with digital evidence. The Handbook of Computer Crime Investigation helps readers master the forensic analysis of computer systems with a three-part approach covering tools, technology, and case studies.
The Tools section provides the details on leading software programs, with each chapter written by that product's creator. The section ends with an objective comparison of the strengths and limitations of each tool.

The main Technology section provides the technical "how to" information for collecting and analyzing digital evidence in common situations, starting with computers, moving on to networks, and culminating with embedded systems. The Case Examples section gives readers a sense of the technical, legal, and practical challenges that arise in real computer investigations.

The Tools section provides details of leading hardware and software
·
The main Technology section provides the technical "how to" information
· for collecting and analysing digital evidence in common situations
Case Examples give readers a sense of the technical, legal, and practical
· challenges that arise in real computer investigations

- Sales Rank: #1552339 in Books
- Published on: 2001-11-12
- Released on: 2001-10-29
- Original language: English
- Number of items: 1
- Dimensions: 9.61" h x 1.05" w x 6.65" l, 2.23 pounds
- Binding: Paperback
- 448 pages

Review
The audience for this book is obviously the legal and law enforcement communities, so any library serving them would find this an excellent introduction. Any law firm looking to get into the field would do well to start here. - E-Streams

Academic law, business or computer science collections will, however, find this book a useful introduction to an increasingly important field - even large public libraries will find an eager audience in an uncertain world. - E-Streams

From the Back Cover
Computers can be used in virtually any type of crime, ranging from cyberstalking and child pornography to

financial fraud, espionage and terrorism. The Handbook of Computer crime investigation presents detailed technical information that can be used to help solve these crimes.

Following on the success of his introductory text, Digital Evidence and Computer Crime, Eoghan Casey has brought together an expert panel of authors to create this detailed guide for professionals who are already familiar with digital evidence. This unique handbook explains how to locate an utilize evidence in computer hard drives, shared networks, wireless devices, or embedded systems. The use of currently available high-tech tools is discussed and real case examples are provided.

To provide individuals with a deeper understanding of the forensic analysis of computer systems, three primary themes are treated:

Tools: Software and hardware for collecting and analyzing digital evidence are presented and their strengths and limitations are discussed. The section provides details on leading hardware and software programs-such as EnCase, Dragon, and ForensiX-with each chapter written by that product's creator.

Technology: This section provides the technical "how to" information for collecting and analyzing digital evidence in common situations, starting with computers, and Windows and Unix operating systems, progressing to network, wireless and embedded systems.

Case examples: These actual situations demonstrate the technical, legal, and practical challenges that arise in real computer investigations.

The Handbook of Computer Crime Investigation is an essential technical reference and on-the-job guide for professionals in computing, security and investigation, forensic science, legal and law enforcement communities.

About the Author
Eoghan Casey is an internationally recognized expert in data breach investigations and information security forensics. He is founding partner of CASEITE.com, and co-manages the Risk Prevention and Response business unit at DFLabs. Over the past decade, he has consulted with many attorneys, agencies, and police departments in the United States, South America, and Europe on a wide range of digital investigations, including fraud, violent crimes, identity theft, and on-line criminal activity. Eoghan has helped organizations investigate and manage security breaches, including network intrusions with international scope. He has delivered expert testimony in civil and criminal cases, and has submitted expert reports and prepared trial exhibits for computer forensic and cyber-crime cases.

In addition to his casework and writing the foundational book Digital Evidence and Computer Crime, Eoghan has worked as R&D Team Lead in the Defense Cyber Crime Institute (DCCI) at the Department of Defense Cyber Crime Center (DC3) helping enhance their operational capabilities and develop new techniques and tools. He also teaches graduate students at Johns Hopkins University Information Security Institute and created the Mobile Device Forensics course taught worldwide through the SANS Institute. He has delivered keynotes and taught workshops around the globe on various topics related to data breach investigation, digital forensics and cyber security.

Eoghan has performed thousands of forensic acquisitions and examinations, including Windows and UNIX systems, Enterprise servers, smart phones, cell phones, network logs, backup tapes, and database systems. He also has information security experience, as an Information Security Officer at Yale University and in

subsequent consulting work. He has performed vulnerability assessments, deployed and maintained intrusion detection systems, firewalls and public key infrastructures, and developed policies, procedures, and educational programs for a variety of organizations. Eoghan has authored advanced technical books in his areas of expertise that are used by practitioners and universities around the world, and he is Editor-in-Chief of Elsevier's International Journal of Digital Investigation.

Most helpful customer reviews

20 of 20 people found the following review helpful.
Computer Crime Investigation...Cookbook!
By Marco De Vivo
What is your real interest?
If you have a strong background on computer networks, and want to know about 'true' computers forensic, then you should consider books like 'Know your Enemy' or 'Intrusion Signatures and Analysis'. Else, if you are not a computer networks expert or not even a computer professional, and want to have some knowledge about computers forensic, then this can be your book: very comprehensive, not too depth, rich of examples, and, as a bonus, covering several emerging security issues like Wireless Network Analysis and Embedded Systems Analysis.
Note, however that:
- It is not a traditional book, but rather a set of 'essays'.
- The contained material is quite biased, since several explanations seem to be more oriented toward promoting tools than to discuss the areas they are intended for.

15 of 17 people found the following review helpful.
You'll find something to like in this collection of essays
By Richard Bejtlich
I am a senior engineer for network security operations. I bought "Handbook of Computer Crime Investigation" (HoCCI) to expand my knowledge of incident response and digital forensics. While "Incident Response" by Mandia, Prosise, and Pepe remains my top pick, HoCCI contains enough original material to qualify as recommended reading.

HoCCI is a collection of 14 distinct chapters written by 17 authors. The book's main audience appears to be law enforcement personnel, and Academic Press markets the book as a title in its "Forensic Science" catalog. The introduction states the book is written for "forensic examiners" who testify in court, although anyone performing digital forensics will find useful sections.

Some of HoCCI's strengths include numerous case studies. Ch. 2 offers examples of "ineffective" and "effective" disclosure and production of digital records in legal proceedings. Chs. 12, 13, and 14 are dedicated to factual legal and incident response scenarios. Reading these anecdotes, I perceived most of the 17 authors to be extremely familiar with their field.

Beyond helpful case studies, HoCCI provides several strong technical chapters. Bob Sheldon's Windows section (ch. 7) is excellent, and Ronald van der Knijff's embedded systems essay (ch. 11) explains the cutting edge of digital forensics. His discussions of directly reading FLASH and EEPROM memory, and using power analysis to break passwords, are impressive. I enjoyed Steve Romig's explanation of using Cisco NetFlow logs in ch. 4, and found the descriptions of wireless systems in ch. 10 to be useful.

HoCCI is not without faults. Several chapters seem like product advertisements; EnCase is the focus of ch. 3, while NFR's IDS appears in ch. 5. The network analysis section (ch. 9) repeats the much-quoted myth that TCP sequence numbers count packets; they actually count bytes of application data.

Overall, HoCCI is a useful supplement to Foundstone's "Incident Response." HoCCI may spend too many pages describing how to search hard drives for remnants of illicit images, illegal software, or harassing emails. Fortunately, its technical content distinguishes it from "Computer Forensics" by Kruse and Heiser and "Incident Response: A Strategic Guide" by Schultz and Shumway.

2 of 2 people found the following review helpful.
Hands-on, immediately applicable to our real-world cases
By Jeff T. Parker
Eoghan Casey's text is immediately useful. It's not theory, it's practical. It's not biased to one operating system, but covers several technologies. Finally, Eoghan and the book's contributors do not gloss over today's most offensive topics, they address them with vigor and solutions.

I would share one concern: the chapter-long product/vendor discussion. Some reviewers label it marketing; other reviewers don't mention it at all. I'll just forewarn you that you will learn much more about EnCase or NFR than about their competitors.

As a security consultant for Hewlett-Packard, it seems my bookshelf fills up entirely too easily, especially as of the last few years. Therefore, I've gotten fairly selective with new book purchases (until I can get a new bookshelf). However, Casey's text is DEFINITELY worth getting - worth knocking another book off to make room. :)

I hope you enjoy this comprehensive text at least half as much as I do.

See all 8 customer reviews...

HANDBOOK OF COMPUTER CRIME INVESTIGATION: FORENSIC TOOLS AND TECHNOLOGY FROM ACADEMIC PRESS PDF

It will certainly believe when you are visiting choose this e-book. This impressive **Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press** publication can be reviewed completely in specific time depending upon how commonly you open and also review them. One to remember is that every e-book has their very own manufacturing to get by each reader. So, be the great reader and be a better individual after reading this publication Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press

Review
The audience for this book is obviously the legal and law enforcement communities, so any library serving them would find this an excellent introduction. Any law firm looking to get into the field would do well to start here. - E-Streams

Academic law, business or computer science collections will, however, find this book a useful introduction to an increasingly important field - even large public libraries will find an eager audience in an uncertain world. - E-Streams

From the Back Cover
Computers can be used in virtually any type of crime, ranging from cyberstalking and child pornography to financial fraud, espionage and terrorism. The Handbook of Computer crime investigation presents detailed technical information that can be used to help solve these crimes.

Following on the success of his introductory text, Digital Evidence and Computer Crime, Eoghan Casey has brought together an expert panel of authors to create this detailed guide for professionals who are already familiar with digital evidence. This unique handbook explains how to locate an utilize evidence in computer hard drives, shared networks, wireless devices, or embedded systems. The use of currently available high-tech tools is discussed and real case examples are provided.

To provide individuals with a deeper understanding of the forensic analysis of computer systems, three primary themes are treated:

Tools: Software and hardware for collecting and analyzing digital evidence are presented and their strengths and limitations are discussed. The section provides details on leading hardware and software programs-such as EnCase, Dragon, and ForensiX-with each chapter written by that product's creator.

Technology: This section provides the technical "how to" information for collecting and analyzing digital evidence in common situations, starting with computers, and Windows and Unix operating systems, progressing to network, wireless and embedded systems.

Case examples: These actual situations demonstrate the technical, legal, and practical challenges that arise in real computer investigations.

The Handbook of Computer Crime Investigation is an essential technical reference and on-the-job guide for professionals in computing, security and investigation, forensic science, legal and law enforcement communities.

About the Author
Eoghan Casey is an internationally recognized expert in data breach investigations and information security forensics. He is founding partner of CASEITE.com, and co-manages the Risk Prevention and Response business unit at DFLabs. Over the past decade, he has consulted with many attorneys, agencies, and police departments in the United States, South America, and Europe on a wide range of digital investigations, including fraud, violent crimes, identity theft, and on-line criminal activity. Eoghan has helped organizations investigate and manage security breaches, including network intrusions with international scope. He has delivered expert testimony in civil and criminal cases, and has submitted expert reports and prepared trial exhibits for computer forensic and cyber-crime cases.

In addition to his casework and writing the foundational book Digital Evidence and Computer Crime, Eoghan has worked as R&D Team Lead in the Defense Cyber Crime Institute (DCCI) at the Department of Defense Cyber Crime Center (DC3) helping enhance their operational capabilities and develop new techniques and tools. He also teaches graduate students at Johns Hopkins University Information Security Institute and created the Mobile Device Forensics course taught worldwide through the SANS Institute. He has delivered keynotes and taught workshops around the globe on various topics related to data breach investigation, digital forensics and cyber security.

Eoghan has performed thousands of forensic acquisitions and examinations, including Windows and UNIX systems, Enterprise servers, smart phones, cell phones, network logs, backup tapes, and database systems. He also has information security experience, as an Information Security Officer at Yale University and in subsequent consulting work. He has performed vulnerability assessments, deployed and maintained intrusion detection systems, firewalls and public key infrastructures, and developed policies, procedures, and educational programs for a variety of organizations. Eoghan has authored advanced technical books in his areas of expertise that are used by practitioners and universities around the world, and he is Editor-in-Chief of Elsevier's International Journal of Digital Investigation.

Poses now this *Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press* as one of your book collection! However, it is not in your bookcase compilations. Why? This is guide Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press that is provided in soft documents. You can download and install the soft file of this magnificent book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press now as well as in the web link offered. Yeah, different with the other people that try to find book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press outside, you could obtain less complicated to pose this book. When some individuals still stroll into the establishment and also look guide Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press, you are below only stay on your seat as well as get the book Handbook Of Computer Crime Investigation: Forensic Tools And Technology From Academic Press.