Fundamentals of Digital Forensics
Overview and Audience

Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications presents and discusses the fundamental building blocks of computer forensics in a practical and accessible manner. Building on Guide to Digital Forensics: A Concise and Practical Introduction, it presents a theoretical background discussing forensic methods, artifacts, and constraints primarily relating to computer forensic examinations in the context of crime investigations. Furthermore, it discusses artifacts and methodologies, in a practical manner, that introduce forensic tools commonly used in forensic examinations in law enforcement as well as in the corporate sector.

This book was written to fulfill a need for a book that introduces forensic methodology and sound forensic thinking combined with hands-on examples for common tasks in a computer forensic examination. The author of Fundamentals of Digital Forensics has several years of experience as a computer forensic examiner with the Swedish Police and is certified as an AccessData examiner. He currently works as a university-level lecturer and researcher in the domain and as a forensic consultant. To further ensure that the content provided in this book is relevant and accurate in the real world, the book has been developed in close relation with the Skövde Office of the Swedish Police in general and with Jan-Åke Pettersson in particular, for which the author is extremely thankful. Fundamentals of Digital Forensics is intended for students that are looking for an introduction to computer forensics and can also be used as a collection of instructions for practitioners. The aim is to describe and explain the steps taken during a forensic examination with the intent of making the reader aware of the constraints and considerations that apply during a forensic examination in law enforcement and in the private sector. Upon reading this book, the reader should have a proper overview of the field of digital forensics and be able as well as motivated to start the journey of becoming a computer forensic expert!

Following the first edition of this book, this second edition has been updated with more material covering incident response practices and tasks. It has also been partly
rewritten following student feedback, and on that note, a special thanks to Marcus Birath for the much appreciated proofreading!

**Motivation and Features**

This is a book written for the sole reason that when I wanted to hold a course on digital forensics, I could not find a textbook that seemed to fulfill my requirements. What I needed a book to cover was the following:

- Sound forensic thinking and methodology
- A discussion on what computer forensics can assist with
- Hands-on examples

My answer to my own needs was, well, to write my own book. It has become obvious to me that writing a book that fulfills those demands is not a very easy task. The main problem lies within making proper hands-on examples. For that reason, I decided to put emphasis on what digital forensics is at its very core, and to make this piece of literature relevant worldwide, I have tried to omit everything that only seems relevant in a certain legislation. That being said, this is the book for you if you want to get an introduction to what computer forensics is and what it can and cannot do. It did feel good to use some sort of well-known forensic software for the examples in this book. Since forensic software can be quite expensive, I decided to use two options interchangeably. The first collection of tools are the proprietary AccessData Forensic Toolkit, which was chosen for the sole reason that AccessData provided the ability to get certified, free of charge, at the time of writing. Using the predecessor of this book in teaching shows that this book can in fact be used to prepare for the AccessData certification test. Further, this book uses a collection of various open source or otherwise free tools that can accomplish the same as the proprietary AccessData tools.

This book begins with setting the stage for forensics examinations by discussing the theoretical foundation that the author regards as relevant and important for the area. This section will introduce the reader to the areas of computer forensics and forensic methodology as well as will discuss on how to find and interpret certain artifacts in a Windows environment. The book will then take a more practical turn and discuss hows and whys about some key forensic concepts. Finally, the book will provide a section with information on how to find and interpret several artifacts. It should at this point be noticed that the book does not, by far, cover every single case, question, or artifact. Practical examples are rather here to serve as demonstrations of how to implement a forensically sound way of examining digital evidence and use forensic tools. Throughout the book, you will find real-world examples applicable in a real-world setting.

Since most computers targeted for a forensic examination are running some version of Windows, the examples and demonstrations in this book are presented in a Windows environment. Being the most recent version of Windows, Windows
10 was used. However, the information should to a very large extent be applicable for the previous version of Windows.

In this second volume, more content describing digital forensics in the corporate secure has been added, introducing incident response work in a reasonable manner. Furthermore, the chapters on memory analysis have been greatly rewritten to include more practices and tools.

Also, most chapters in this book come with a “Questions and Tasks” section. Some are questions with a right or wrong answer, and some are of more exploratory nature. Whatever the case, answers or discussions are found in Appendix A—Solutions. Complementing the book, there are video lectures covering most of the book content in YouTube: https://www.youtube.com/playlist?list=PLEjQDF4Fr75pBnu8WArpeZTKC9-LrYDTI.

Happy reading!

Skövde, Sweden

Joakim Kävrestad
Part I  Theory

1  What Is Digital Forensics? .......................................................... 3
   1.1  A Forensic Examination ....................................................... 4
   1.2  How Forensics Has Been Used ........................................... 6
   1.3  Questions and Tasks .......................................................... 7
       References ........................................................................... 7

2  Ethics and Integrity ................................................................. 9
   2.1  Tracing Online Users ......................................................... 10
   2.2  Key Disclosure Law(s) ........................................................ 11
   2.3  Police Hacking ................................................................. 12
   2.4  Ethical Guidelines ............................................................. 13
   2.5  Questions and Tasks .......................................................... 15
       References ........................................................................... 16

3  Computer Theory .................................................................. 17
   3.1  Secondary Storage Media ................................................... 17
   3.2  The NTFS File Systems ....................................................... 18
   3.3  File Structure .................................................................... 19
   3.4  Data Representation .......................................................... 20
   3.5  User Accounts in Windows 10 ............................................ 21
   3.6  Windows Registry .............................................................. 22
   3.7  Encryption and Hashing ...................................................... 25
   3.8  SQLite Databases ............................................................... 27
   3.9  Memory and Paging ........................................................... 28
   3.10 Questions and Tasks .......................................................... 28
       References ........................................................................... 29

4  Notable Artifacts ................................................................. 31
   4.1  Metadata ............................................................................ 31
   4.2  EXIF Data ......................................................................... 32
   4.3  Prefetch ............................................................................ 33
   4.4  Shellbags ........................................................................... 34
   4.5  .LNK Files ........................................................................ 35
4.6 MRU-Stuff ........................................ 36
4.7 Thumbcache ........................................ 38
4.8 Windows Event Viewer ................................ 39
4.9 Program Log Files ..................................... 42
4.10 USB Device History .................................... 42
4.11 Questions and Tasks .................................... 44
References ................................................ 45

5 Decryption and Password Enforcing ......................... 47
5.1 Password Theory ........................................ 47
5.2 Decryption Attacks ....................................... 50
5.3 Password Guessing Attacks ................................ 51
5.4 Questions and Tasks ....................................... 55
References ................................................ 55

Part II The Forensic Process

6 Cybercrime, Cyber Aided Crime, and Digital Evidence ........ 59
6.1 Cybercrime ........................................... 60
6.2 Cyber Aided Crime ...................................... 60
6.3 Crimes with Digital Evidence ............................ 61
6.4 Questions and Tasks ....................................... 62
References ................................................ 62

7 Incident Response .......................................... 63
7.1 Why and When? ......................................... 63
7.2 Establishing Capabilities .................................. 64
7.3 Incident Handling ........................................ 66
7.4 Questions and Tasks ....................................... 68
References ................................................ 68

8 Collecting Evidence .......................................... 69
8.1 When the Device Is Off .................................. 70
8.2 When the Device Is On ................................... 71
8.3 Live Investigation: Preparation ............................ 72
8.4 Live Investigation: Conducting ............................ 74
8.5 Live Investigation: Afterthoughts ......................... 77
8.6 Questions and Tasks ....................................... 77
References ................................................ 78

9 Triage ...................................................... 79
9.1 Specific Examinations ..................................... 79
9.2 White and Blacklisting .................................... 81
9.3 Automated Analysis ....................................... 81
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4</td>
<td>Field Triage</td>
<td>82</td>
</tr>
<tr>
<td>9.5</td>
<td>Questions and Tasks</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>83</td>
</tr>
<tr>
<td>10</td>
<td>Analyzing Data and Writing Reports</td>
<td>85</td>
</tr>
<tr>
<td>10.1</td>
<td>Setting the Stage</td>
<td>85</td>
</tr>
<tr>
<td>10.2</td>
<td>Forensic Analysis</td>
<td>87</td>
</tr>
<tr>
<td>10.3</td>
<td>Reporting</td>
<td>90</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Case Data</td>
<td>91</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Purpose of Examination</td>
<td>92</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Findings</td>
<td>94</td>
</tr>
<tr>
<td>10.3.4</td>
<td>Conclusions</td>
<td>95</td>
</tr>
<tr>
<td>10.4</td>
<td>Final Remarks</td>
<td>97</td>
</tr>
<tr>
<td>10.5</td>
<td>Questions and Tasks</td>
<td>98</td>
</tr>
</tbody>
</table>

**Part III  Get Practical**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Collecting Data</td>
<td>101</td>
</tr>
<tr>
<td>11.1</td>
<td>Imaging</td>
<td>101</td>
</tr>
<tr>
<td>11.2</td>
<td>Collecting Memory Dumps</td>
<td>106</td>
</tr>
<tr>
<td>11.3</td>
<td>Collecting Registry Data</td>
<td>108</td>
</tr>
<tr>
<td>11.4</td>
<td>Collecting Network Data</td>
<td>109</td>
</tr>
<tr>
<td>11.5</td>
<td>Collecting Video from Surveillance</td>
<td>110</td>
</tr>
<tr>
<td>11.6</td>
<td>Process of a Live Examination</td>
<td>111</td>
</tr>
<tr>
<td>11.7</td>
<td>Questions and Tasks</td>
<td>113</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>113</td>
</tr>
<tr>
<td>12</td>
<td>Indexing and Searching</td>
<td>115</td>
</tr>
<tr>
<td>12.1</td>
<td>Indexing</td>
<td>115</td>
</tr>
<tr>
<td>12.2</td>
<td>Searching</td>
<td>117</td>
</tr>
<tr>
<td>12.2.1</td>
<td>Questions and Tasks</td>
<td>121</td>
</tr>
<tr>
<td>13</td>
<td>Cracking</td>
<td>123</td>
</tr>
<tr>
<td>13.1</td>
<td>Password Cracking Using PRTK</td>
<td>124</td>
</tr>
<tr>
<td>13.2</td>
<td>Password Cracking Using Hashcat</td>
<td>129</td>
</tr>
<tr>
<td>13.3</td>
<td>Questions and Tasks</td>
<td>133</td>
</tr>
<tr>
<td>14</td>
<td>Finding Artifacts</td>
<td>135</td>
</tr>
<tr>
<td>14.1</td>
<td>Install Date</td>
<td>135</td>
</tr>
<tr>
<td>14.2</td>
<td>Time Zone Information</td>
<td>136</td>
</tr>
<tr>
<td>14.3</td>
<td>Users in the System</td>
<td>136</td>
</tr>
<tr>
<td>14.4</td>
<td>Registered Owner</td>
<td>138</td>
</tr>
<tr>
<td>14.5</td>
<td>Partition Analysis and Recovery</td>
<td>138</td>
</tr>
<tr>
<td>14.6</td>
<td>Deleted Files</td>
<td>141</td>
</tr>
<tr>
<td>14.6.1</td>
<td>Recovering Files Deleted from MFT</td>
<td>141</td>
</tr>
<tr>
<td>14.6.2</td>
<td>File Carving</td>
<td>142</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>14.7</td>
<td>Analyzing Compound Files</td>
<td>143</td>
</tr>
<tr>
<td>14.8</td>
<td>Analyzing File Metadata</td>
<td>143</td>
</tr>
<tr>
<td>14.8.1</td>
<td>NTFS Time Stamps</td>
<td>144</td>
</tr>
<tr>
<td>14.8.2</td>
<td>EXIF Data</td>
<td>145</td>
</tr>
<tr>
<td>14.8.3</td>
<td>Office Metadata</td>
<td>145</td>
</tr>
<tr>
<td>14.9</td>
<td>Analyzing Log Files</td>
<td>146</td>
</tr>
<tr>
<td>14.10</td>
<td>Analyzing Unorganized Data</td>
<td>148</td>
</tr>
<tr>
<td>14.11</td>
<td>Analyzing SQLite Databases</td>
<td>150</td>
</tr>
<tr>
<td>14.12</td>
<td>Questions and Tasks</td>
<td>152</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>153</td>
</tr>
<tr>
<td>15</td>
<td>Some Common Questions and Tasks</td>
<td>155</td>
</tr>
<tr>
<td>15.1</td>
<td>Was the Computer Remote Controlled?</td>
<td>155</td>
</tr>
<tr>
<td>15.1.1</td>
<td>Analysis of Applications</td>
<td>156</td>
</tr>
<tr>
<td>15.1.2</td>
<td>Scenario Testing</td>
<td>157</td>
</tr>
<tr>
<td>15.2</td>
<td>Who Was Using the Computer?</td>
<td>158</td>
</tr>
<tr>
<td>15.3</td>
<td>Was This Device Ever at Site X?</td>
<td>160</td>
</tr>
<tr>
<td>15.4</td>
<td>What Device Took the Picture and Where?</td>
<td>160</td>
</tr>
<tr>
<td>15.5</td>
<td>Where Were the Documents Created?</td>
<td>162</td>
</tr>
<tr>
<td>15.6</td>
<td>Application Analysis: The Windows Firewall</td>
<td>164</td>
</tr>
<tr>
<td>15.7</td>
<td>Questions and Tasks</td>
<td>167</td>
</tr>
<tr>
<td>16</td>
<td>FTK Specifications</td>
<td>169</td>
</tr>
<tr>
<td>16.1</td>
<td>FTK: Create a Case</td>
<td>169</td>
</tr>
<tr>
<td>16.2</td>
<td>FTK: Preprocessing</td>
<td>172</td>
</tr>
<tr>
<td>16.3</td>
<td>FTK: Overview</td>
<td>176</td>
</tr>
<tr>
<td>16.4</td>
<td>Registry Viewer: Overview</td>
<td>182</td>
</tr>
<tr>
<td>17</td>
<td>Open-Source or Freeware Tools</td>
<td>189</td>
</tr>
<tr>
<td>17.1</td>
<td>Prefetch Parser by Erik Zimmerman</td>
<td>189</td>
</tr>
<tr>
<td>17.2</td>
<td>Shellbags Explorer by Erik Zimmerman</td>
<td>189</td>
</tr>
<tr>
<td>17.3</td>
<td>.lnk File Parser by Erik Zimmerman</td>
<td>191</td>
</tr>
<tr>
<td>17.4</td>
<td>Thumbcache Viewer</td>
<td>191</td>
</tr>
<tr>
<td>17.5</td>
<td>USBDevview by NirSoft</td>
<td>191</td>
</tr>
<tr>
<td>17.6</td>
<td>Autopsy</td>
<td>193</td>
</tr>
<tr>
<td>17.6.1</td>
<td>Get Going</td>
<td>194</td>
</tr>
<tr>
<td>17.6.2</td>
<td>Autopsy Overview</td>
<td>197</td>
</tr>
<tr>
<td>17.6.3</td>
<td>The Image Gallery</td>
<td>202</td>
</tr>
<tr>
<td>17.6.4</td>
<td>Communications</td>
<td>203</td>
</tr>
<tr>
<td>17.6.5</td>
<td>Timeline</td>
<td>204</td>
</tr>
<tr>
<td>17.7</td>
<td>Registry Explorer</td>
<td>205</td>
</tr>
</tbody>
</table>
Now that the book has kept you interested this far, it is time to discuss what digital forensics actually is. This will be done in a very theoretical manner, but I have tried to keep it short. This part begins with an overview of what digital forensics and cybercrime is, before discussing some ethical aspects of forensic examinations and crime prevention in the digital world. Then, some computer theory that is necessary for a forensic examiner to be familiar with will be presented. The part ends with a chapter that introduces how to find and interpret forensic artifacts that the author deems to be common and important.
What Is Digital Forensics?

So then, what is digital forensics? Well, the simplest explanation could be that it is the examination of digital storage and digital environments in order to determine what has happened. “What has happened” in this context could be whether or not a crime was committed, whether or not someone remote controlled a certain computer, when a picture was taken, or if a computer was subject to intrusion. That being said, it can be basically anything.

However, looking at the target of some actual forensic investigations, it is evident that saying “What has happened” is not covering the entire field of computer forensics since forensic examiners also look into what is currently happening. There have, for instance, been several cases in Sweden and globally were forensic examiners monitored network traffic in order to capture data that was later used to identify sexual predators. There are also situations when forensic examiners, during house searches, record what is currently happening on a computer. The case of using digital forensics to monitor activity in real time may be even more apparent in the corporate world where it is common to examine intrusion attempts and malware behaviors as it is happening.

Looking to the scientific community, Reith et al. (2002) described digital forensics in the following way:

Digital forensics is a relatively new science. Derived as a synonym for computer forensics, its definition has expanded to include the forensics of all digital technology, whereas computer forensics is defined as “the collection of techniques and tools used to find evidence in a computer”

Today, this definition seems a bit old, but it does hold a few key aspects. To begin with, it describes that computer forensics is a collection of techniques and tools. While those are defiantly two important aspects, this definition does not fit my personal beliefs as it kind of omits the methodology and mind-set that, for me, is the foundation of digital forensics. However, it does capture that digital forensics
extends to all digital technology, and that is an important aspect as today, important evidence may be found in everything from thumb drives to computers or the cloud.

A more recent description is found on [www.forensiccontrol.com](http://www.forensiccontrol.com) (2017):

Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. Computer forensics follows a similar process to other forensic disciplines, and faces similar issues.

What is noticeable in this description is that it determines the tasks involved during a forensic investigation: collecting, analyzing, and reporting. It also describes that computer forensics is comparable to other forensic disciplines, and that does suggest that methods used and conclusions drawn during a computer forensic investigation should face the same scrutiny as an analysis of a fingerprint or DNA test. The rest of the section will discuss each of these, beginning with establishing a model that could be used to describe a digital forensic examination.

### 1.1 A Forensic Examination

As we just established, the foundation of digital forensics is that it is the practice of collecting, analyzing, and reporting on digital data. It does, for sure, also impose that there is some data that we target for examination and a reason for the examination. It does also impose that, unless we do the examination for the fun of it, there is someone that we should report back to. I have collected those aspects and formed the very abstract model shown in Fig. 1.1 that attempts to summarize the named aspects in a graphical way.

Figure 1.1 reflects the discussed processes and the inputs or outputs that should be present in each process. From top to bottom, Collect should be the process of collecting digital evidence. I would also say that in this process you do target a person or a data source, which would commonly be a device.

Having a person as a target would be the normal state in a criminal investigation where you have someone that is suspected of a crime. You would then, after getting a search warrant, start searching for devices that belong to the suspect. In a corporate setting, it could be more common to target a device rather than a person, and it would all depend on the reason for doing the investigation.

In this process, it is important to mention that in order to collect the correct data, you need a proper order. The order in this case would include the target person or devices to collect data from, but it should also include the reason for the investigation, at least on an abstract level. This is because you would look for vastly different data sources if you are investigating a suspected malware attack of a child abuse case. It is also important to know if you should prepare to collect information from volatile data sources such as memory circuits or if you only need to care about static media such as hard drives. Another technical consideration is if you should expect encrypted data or not. While there will be a more detailed technical discussion on data collection later in this book, in Chap. 3, it is important to mention that you need...
to come prepared. The preparation steps should help you determine what to expect and should at least include figuring out the reason for the forensic examination and a background check on the person from whom you are collecting data.

The process of Analyzing data is more concerned with finding out what has happened in a digital environment or what was done using a digital device. In a corporate environment, a forensic expert would normally be quite free to conduct whatever examinations she wants, guided of course by agreements. However, with a precise question, the examination will without doubt be more efficient. It is worth mentioning that the input to this phase is commonly found in a discussion between the person ordering the examination and the forensic expert. Also, it is common that new questions and follow-up questions will arise during the investigation. As one example, during an investigation of a computer during a drug case, the initial request was to find out if the computer had been involved in any activities related to selling drugs online. The investigation clearly showed that it had been, but a large portion of the evidence was found in folders shared among several computers. In this case, a follow-up question was to determine who, more than the computer owner, had

Fig. 1.1 Overview of forensic processes
access to the folders in question. As a final note, it is important to mention that, in a criminal investigation, depending on the local legislation, the questions that are taken as input to this process may be more or less important in setting the rules of what the forensic expert is allowed to do.

In the final process, Reporting, the findings from the analysis are reported. The purpose of this step is mainly to report well-grounded answers to the questions given to the examiner in the previous step. In this step, it is very common that new questions will arise in light of the provided answers, and for that reason, the last two steps are commonly iterative. It is also worth mentioning that it is of great importance that the conclusions drawn in this step are actually conclusions that are backed up by the findings during the examination. Each of the phases and considerations relating to each phase will be discussed in greater detail in part 2 of this book.

1.2 How Forensics Has Been Used

To deepen the introduction on the concept of digital forensics, this final section of the first chapter is dedicated to describing two criminal cases and one corporate case that the author has been involved with. The intention is to continue the introduction to the area with some examples of how digital forensics and forensic methods have been used in reality.

The first case was a case where a person (A) got suspected of computer intrusion by having tricked the victim (B) into giving up the credentials to his Web site. A had then used the credentials to modify B’s Web site in malicious ways and later destroy it completely. This case started with a report to the police, and since B has very good indications of the actual identity of A, a house warrant was issued, A got arrested, and his computers got seized. In this case, the forensic examination was done by the author of this book. What is interesting about this case is that the police investigators did not know anything about computer crimes and the forensic examiner had to assume the role of co-investigator. In the first interrogations with A, it became evident that A had been in contact with B using chat clients. As such, the first forensic task was to map the communication between A and B by searching for usernames related to B. The result of this process was that it became evident that A had contacted B and said that he was a Web designer who offered to aid B with his Web site. After some communication, A managed to trick B into giving away the credentials to said Web site.

The second step in the forensic examination was to actually find evidence of A being involved in the malicious modifications to B’s Web site. In this case, searching for URLs and HTML code related to B’s Web site revealed that there were modified versions of B’s Web site located on A’s computer. Moreover, one of the modifications to B’s site involved including pictures with sexual content on the Web site. By using forensic tools to search for identical pictures, it was revealed that the pictures did not only reside on A’s computer but was also taken with A’s iPhone, resulting in A being convicted of computer intrusion.

Another criminal case where the forensic involvement was much smaller but played an important role was in a murder case where the suspect had shot a person. There were some pieces of evidence pointing to the suspect, but he was given alibi
by his girlfriend who said that he was at home at the time of the crime. Home in this case was about 90 min away from the murder site, by car. In this case, the suspect’s telephone was examined, and the IMEI number of the phone was identified. It was then possible to get records displaying what IMEI numbers had been connected to the mobile towers in close proximity to the murder site at the time of the murder. Turning out, the suspect’s phone was connected to a mobile tower very close to the murder site, at the time when he said that he was at home. This was a key piece of evidence that led to the suspect being sentenced to lifetime in prison for murder.

A final example from the corporate sector was a case when an employee of a company was suspected of placing a Trojan horse in the company network. The employment had been terminated, and the suspicion was that the employee had placed a Trojan horse to get back at the company for sacking him. The Trojan horse was detected and analyzed by the company’s IT department, and it was evident that it was configured to send information to an IP address located close to where the former employee lived. Since search warrants and tracing IP addresses are off limits for companies, other actions had to be taken. After careful examination of how the Trojan horse got inserted into the network, it seems as if it had been copied from a USB stick. It was also possible to determine the unique identifier for the USB stick.

A USB device that was issued by the company and used by the employee was examined, and the unique identifier was the same as for the USB stick that was used to distribute the malware. When the employee was confronted with the evidence, he admitted to having injected the Trojan horse, and a civil lawsuit was filed.

1.3 Questions and Tasks

Here are the questions for the first chapter, and for these questions, you may benefit from answering them in a group discussion!

1. Consider in what types of criminal investigations that computer forensic experts may be involved and in what way.
2. Consider when a computer forensic expert may be needed in a corporate environment.
3. Brainstorm on what types of devices may be interesting to a computer forensic expert.
4. To whom are the findings of a computer forensic examination of interest?

References

As you will come to understand during this book, any forensic examination is essentially about digging around in the data on some digital device that belongs to somebody. Seeing as how we spend more and more time online using various devices, a person’s whole life can exist in their device. Thus, any forensic examination is a breach of privacy. This privacy breach is commonly motivated by the need of solving crimes or investigating computer-related incidents, and perhaps rightfully so. However, while we need to conduct forensic examinations in many situations, we shall do so while understanding how what we do affect the people concerned. In a short sentence, forensic examinations should be carried out with integrity in mind and following reasonable ethical guidelines. This chapter provides a short discussion on ethical considerations in regard to digital forensics and highlights some contemporary examples where crime prevention and integrity are in direct conflict. The chapter concludes with suggestions for ethical guidelines derived from ethics in research and the forensics community.

While it is easy, and quite common, to adopt a “suit yourself” approach to the integrity of suspects, that mind-set is very narrow and problematic in reality. As a very important and first rule of thumb, almost any democratic country adopts an “innocent until proven guilty” approach in their legal systems. As such, anyone that is being investigated should be treated as an innocent up to the point when a verdict is expressed in court. It is therefore important to maintain the integrity of any suspect during the course of an investigation. There have been numerous examples throughout the world where, for instance, the name of a suspect has been disclosed to the public, even if the suspect was later declared innocent. At several such occasions, the consequences for the suspect have been dire; there are examples of suspects even being killed. Moving away from the suspects, one should also understand that a criminal investigation is commonly extended to cover not only devices owned by the suspects but also devices belonging to others. Depending on the nature of the case, devices owned by relatives and friends to the suspects or even witnesses that happened to be in the wrong place at the wrong time may have their devices seized. Those devices can hold anything from social media account, chat with loved ones,
medical history, or pictures of all sorts. Having that material looked at by someone unknown is a huge breach of privacy and should not be taken lightly by the forensic examiners.

We have been discussing ethics of digital forensics as a topic of importance in criminal investigations. It is, of course, equally important in corporate forensics. In a corporate environment, it is more common to employ forensic techniques to examine a computer intrusion or perhaps a corporate espionage. That does not change the fact that the devices that are being examined will be devices that are used by someone and very likely to contain personal data. A company may or may not employ policies against personal use of company resources. However, even if such a policy is in place, one can assume to find personal information originating from social media, online banking, or whatever. Very well, to summarize, any forensic examination is by definition a breach of someone’s privacy. While that breach is sometimes necessary, it should not be taken lightly by forensic examiner. The rest of this chapter will exemplify how different societies see the trade-off between crime prevention capabilities and integrity and conclude with a discussion on ethical guidelines.

2.1 Tracing Online Users

The first example is concerned with tracing online users or rather the ability of law enforcements to track the user of an IP address. A little bit simplified, computers use addresses whenever communicating online, and those are called IP addresses. Any device that communicates online must have a unique IP address, and it is often possible to learn the IP address behind an action online, such as an e-mail, online purchase, or chat message. Thus, a very common entry point for the police is an IP address tied to a suspected crime, and if the police can find the user of the IP address, it is a good start on the road toward solving the crime. All good so far, however there is a caveat. Internet is to a very large extent built on IPv4 addressing that can provide a bit over four billion addresses, but there are more devices than that. Since every device needs a unique address, that is cause for a problem. The problems are solved using various techniques called NAT (Network Address Translation) that essentially lets several users use the same IP address and effectively setting the uniqueness out of play and limiting the police’s ability to track the user behind an IP address.

One way of managing the issue can be to force all Internet service providers (ISP) to keep track of the actual user behind an IP address. In technical terms, log when the shared IP address is used and by who. If that is done, the police can simply ask the ISP who used the IP address at a particular point in time, and case is closed. This approach was previously used in Sweden but was declared invalid by the European court in 2016 (The European Court 2016). To back the tape a bit, the Swedish approach was to force ISP’s to store the information needed for tracing IP addresses for 6 months. The information that was stored included information about what user that used an IP address and at what time. The reasoning behind the court’s ruling was that storing information about every uses was a breach of integrity that could not be
motivated with the benefits for law enforcement. What is true and correct is not a discussion to be held in this book, so this example will end here.

### 2.2 Key Disclosure Law(s)

Encryption, further described in REFTEXT, is the act of making data unreadable without the correct key. As such, it is a widely used technique that makes forensic examinations very hard (Vincze 2016). While using various attacks on seized devices is widely accepted as forensic techniques, and asking the owner of a device to give up the keys willingly is common practice, several governments are designing laws to force suspects to give up their encryption keys or face prosecution for the act of keeping the data encrypted and out of the authorities’ reach. There are several different ways to implement this kind of law where one is to force a suspect to give up encryption keys and another is to force the suspect to decrypt encrypted data.

While a key disclosure law would, undeniably, be helpful for law enforcement, it is not blindly accepted by the public. Looking at recent debates, in, for instance, Australia, there are at least three big objections. First, and perhaps most relevant from an ethical perspective, critics claim that a key disclosure law is in conflict with the right to not self-incriminate that is used as a fundamental legal principle in many democratic countries. Essentially, the right to not self-incriminate means that a suspect should not be forced to actions that can generate evidence against her, or as everyone heard from American police series such as the CSI or Miami Vice:

> You [the suspect] have the right to remain silent. Anything you say or do can and will be held against you in a court of law (FANDOM 2019).

Other objections are the very real possibility of someone forgetting their passwords; what would happen in that case? Or what would happen if a suspect just refuses to hand out his password? A concrete example can be found in Crimes Act 1914 by the Australian Government (2015) that states that a police can get magistrate’s order to make someone give out encryption keys. Failing to comply with such an order can result in imprisonment for 2 years. The consequence is worth contemplating on: what would happen if someone that actually committed a murder and the evidence is on his encrypted computer is given such an order? He would most likely accept his 2 years in prison and move on in happiness. The moral of the argument is that a common objection is that having minor consequences will lead to a law that is only efficient against low rank crimes and is therefore unnecessary. And again, what will happen if the key is just forgotten? It would seem harsh to get 2 years in prison for forgetting a password.

Before leaving the topic of key disclosure laws, it should be mentioned that Australia quite recently took a step further. With a new law, the Australian government can now order companies to create technical functions that can give them access to encrypted user information without the user’s knowledge. To exemplify, services such as Apple’s iCloud allow a user to store data on Apple’s servers and that
data can (AND SHOULD!) be encrypted. Using the new act from 2019, Australia can force Apple to create a backdoor into the user’s data without the user knowing about it (BBC 2018). While the implications on integrity for the targeted user are obvious, this act brings yet another concern as introducing backdoors into a service is a security issue that concerns any user of that service. Well, taking a stance and judging what is right is left to you as a reader, and thus ends this example.

2.3 Police Hacking

The final example concerns governmental spyware or other forms of what some refer to as police hacking. While that headline may sound a bit intimidating, it concerns various ways for the government to spy on what a suspect does on his or her computer using technical aids. As described by Škorvánek et al. (2019) as well as Ohm (2017), laws that allow the police to hack into suspects’ computers or plant malware in them have been introduced and discussed in several countries in recent times. It goes without saying that this is an action that is highly intrusive and carried out without the knowledge of the suspect. While those in favor of police hacking highlight that it is a tool that can be a very effective way to gather evidence, the con side talks about the obvious privacy concerns.

Looking at the technical aspect of police hacking, it is essentially about hacking. Even if the hacking operations carried out by the police would be attacks that are performed with the government’s good mind, it is still hacking using the same tools and conditions as an evil hacker that wants to destroy the world. The reason for why that insight is important is that any police hacker would face the same challenges that an evil hacker would—security measures. There are two sides to this coin, which is sometimes proclaimed by those that are against police hacking. First, one can argue whether or not it is reasonable for governmental agencies to hunt for vulnerabilities and exploits. Since they would be used to solve crimes, it would be unlikely that the vulnerabilities discovered would be disclosed so that they can be fixed. The other side would be that if police hackers need to deface security measures, they will have a hard time and may have a slim chance of succeeding. The question becomes: Is it reasonable to use highly intrusive techniques with only slim chances of succeeding? Well, the author’s opinion will remain hidden and the reader can form his own.

As a final note, before discussing ethical guidelines, there is a pattern in different measures that needs to be highlighted. There are measures that the suspect will be aware of and measures that the suspect will not be aware of. In terms of integrity, this difference is important. If you are aware of an action that will be taken against you, you have a chance to appeal. Something that all actions that are happening without the suspect being aware of have in common is that they are effectively impossible to appeal since, well, the suspect does not know that they are happening. It could also be mentioned that, as of today, democratic legislation does not typically let the forensic expert of police officer to rampart with the powers just described. Rather, most action will, in most legislations, require approval from an attorney, judge, or court.
2.4 Ethical Guidelines

The author of this book is not a moral philosopher or someone who can claim the title of an expert in ethics, privacy, or integrity. But it still seems important to conclude this chapter with some ethical compass that could, and perhaps should, be used when conducting forensic work. So based on experience as a forensic expert and information security research, here comes a discussion on ethical guidelines for forensic examinations.

Ethics in digital forensics is indeed an interesting topic. Whether you are doing forensics in a corporate environment or criminal investigation, you are doing something that is breaching privacy of someone, at least very likely. There will of course be regulations to follow, and those will serve as the first rule. Regulation in this sense can be local laws (in criminal investigations) or agreements such as nondisclosure agreements (common in the corporate world). However, regulations may say what you can do, but do they also say what you should do? That may not always be the case; for instance, a bachelor thesis from the University of Skövde concluded that the integrity of those subject to forensic examinations in criminal investigations, in Sweden, is to a large extent up to the people involved in investigation of the case (Olsson 2019). The same thesis concluded that solving crimes is prioritized over the integrity of someone whose devices are seized.

Looking at the research community, Schrittwieser et al. (2013) discuss the following four guidelines for information security research:

- **Do not harm humans actively.**
  While the intent of this guideline was to make researchers avoid studies where someone got harmed during the study, it works for forensics as well. For a forensic examiner, this guideline could be interpreted as “Do not do more harm than you must” and could, for instance, include making sure not to include personal data of someone that is not of interest in an examination when writing a report.

- **Do not watch bad things happen.**
  This guideline essentially says that if you see something bad and have the power to fix it—fix it. One could argue that the forensic interpretation would be to stop crimes or illicit activity as soon as you can rather than to wait for something to play out to get more evidence. It could also mean that if you find something that is illicit but not in the scope of what you are asked to do, you should report it to a supervisor.

- **Do not perform illegal activities to harm illegal activities.**
  Well, one should avoid doing anything illegal and follow local laws and regulations.

- **Do not perform undercover research.**
  This guideline says that you should not do anything to unknowing subjects. As we previously explored in this chapter, such actions are in conflict with integrity. However, they are perhaps necessary at times but should be used with caution.
Bassett et al. (2006) discuss ethics specifically in regard to digital forensics and can be summarized in the following bullets:

- Avoid irrelevant information.
  This bullet basically states that you should avoid information that is not relevant to your task. This could involve information about inappropriate behaviors, medical history, or basically anything.
- Be honest about your errors.
  This bullet depicts that if a forensic expert makes errors, he should own up to them. As you will notice, a forensic examination is a process where it is possible to well, screw up, and in some legislations that will lead to results being questioned. However, it is very important that a forensic examiner reports on what happened during an examination, even if that means that errors are reported.
- Be objective.
  This bullet says that a forensic examiner cannot be biased. A forensic examination should be carried out with an open objective mind and aim at uncovering the truth.

Finally, the International Society of Forensic Computer Examiners, a private organization concerned with forensic training and certification, provides a code of ethics that can be summarized as follows (The International Society of Forensic Computer Examiners 2019):

- Be objective and accurate in all investigations.
- Always be truthful about your findings.
- Be truthful about your competence and training.
- Base examinations on established and validated principles.
- Examine all evidence in the scope of the task.
- Never do anything that could appear to be a conflict of interest.
- Never withhold any evidence or express opinion on guilt.

While compiling a granular list of bullets for everyone to follow is a job that is hard and should perhaps be performed by some organizations with influence over the entire world, the aim of this chapter is to highlight some aspects of ethics and privacy in forensic examinations with the purpose of making the reader, you, aware of them. Such a list would also be impossible since there are different rules in different regulations. For instance, you may or may not gather data from cloud services, depending on where you work. However, there are some abstract boundaries that should never be overstepped. They will conclude this chapter:

- Follow local regulations and law.
  First and foremost, the law is the law and should be followed. After the law come directives and agreements that should also be followed. However, while the law must always be obeyed, one could think of a situation where an agreement
would break the rest of the ethical guidelines. Will your ethical compass allow you to sign it?

- Be objective and thorough.
  
The task of a forensic expert is to find out what happened in a digital environment, not to build a strong case. As such, all examinations should be thoroughly executed with an objective mind.

- Be honest about your competence, training, and mistakes.
  
  A forensic expert should not lie about his or her competence or mistakes. A report should include what happened during an examination. And on the topic of competence, the task of the forensic expert is to be truthful about competence and findings and let other judge their value.

- Present all facts, but no verdicts.
  
  A forensic expert should present all findings from a forensic examination. Even if tasked with finding evidence of a crime, all evidence in favor and against that crime should be presented. The judging is the task for the court.

- Ignore irrelevant data and treat it as confidential.
  
  If data that is irrelevant for the case is encountered, that data should be ignored and treated as confidential. That means that the forensic examiner should not discuss that data with anyone. A reasonable time to step away from this rule would be if the irrelevant data is actually evidence of another crime; in such a case, it would be reasonable to discuss what to do with it with a supervisor.

- Never put yourself in a conflict of interest situation.
  
  A forensic examiner is dependent on his or her reputation. Never put yourself in a situation that could be seen as a conflict of interest. That will impact your credibility and make you seem unprofessional.

### 2.5 Questions and Tasks

Ethics and legal matters are often points of discussion. Thus, the end of chapter tasks are oriented as such. Consider the following questions in class:

1. In your jurisdiction, is it ok for the police to hack into your computer or cell phone to acquire the data that is on it?
2. In your jurisdiction, is it ok for the police to require that an Internet service provider discloses who the user of a certain IP address is?
3. Should the police be allowed to place malware in suspects’ digital devices to track what they are doing?
References


Olsson A (2019) Hantering av integritetsperspektiv inom IT-forensik: En kvalitativ intervjustudie med rättväsandets aktörer

Schrittwieser S, Mulazzani M, Weippl E (2013) Ethics in security research which lines should not be crossed? Security and Privacy Workshops (SPW), 2013 IEEE. IEEE 1–4


Up until this point, we introduced what computer forensics is and pretty much concluded that it is about examining and deducing what happened on a computer or in a computer system. That is all well and good, but to move on further, you do need a bit of background knowledge. The intent of this book is not to provide you with a summary of computer science. Rather, the book expect you to have a fair “know-how” on computer stuff. But there are a few areas that the author found that IT people commonly do not know that much about, but that are important to a computer forensic expert. Those areas are covered, in brief, here. Note that each subsection is an overview. For a complete understanding, follow the references!

### 3.1 Secondary Storage Media

Secondary storage media refers to media where data is stored for long-term preservation. This is in contrast to primary memory, which includes random-access memory and cache memories, which is used for short-term storage. Secondary storage includes hard drives, CD/DVD, USB flash drives, and memory cards. This discussion refers mainly to hard drives but is also (commonly) applicable for USB flash drives and memory cards.

The first thing that is important to know is the physical size of the storage media. This is because it is important to know that you can account for all the storage area on a computer. Say that you find a computer that appears to have a “C:\” partition of 200 GB but a physical examination of the hard drive reveals that it is supposed to be able to house 250 GB of data. This could mean that there is another hidden partition present on the hard drive or that the hard drive was reformatted. Either way, the remaining 50 GB may contain valuable evidence.

This is also a good place to comment on how hard drive formatting is commonly handled by the operating system. It is easy to assume that if you repartition your hard drive, the existing data is overwritten. That is, most times, not the case. Rather, the hard drive is made up from sectors and clusters that can be allocated to a file or a