**Tipe Koleksi: eBook - Sains & Teknologi**

# UNIX and Linux Forensic Analysis DVD Toolkit

Pogue, Chris



---

Abstrak

If you know anything about Linux you know that there are a lot of commands that accomplish the same task. To borrow the motto of Perl, a very popular scripting language with a long *nix history: “There’s more than one way to do it.” It is possible that no two people will do the same thing the same way, yet get the same results.
In our book, we have used what we feel is the quickest and easiest way to accomplish the task at hand. We understand that you may find a way that works better for you, and if that is the case, go with it, and please let us know so we can incorporate it in a later revision of this book. In Chapter 2 of this book, you will learn about the most common file systems used with Linux, how the disk architecture is configured, and how the operating system interacts with the kernel (at a high level). In Chapter 3 of this book, you will learn how to acquire both the volatile and persistent data from a Linux system, using a Linux forensic system. In Chapter 4 of this book, you will learn how to analyze the data you have just acquired. In Chapter 5 of this book, you will learn about the Top 10 most commonly used tools in Linux hacking, either as the launch point or the target. You will also learn what these tools look like when they are installed, how they are used, and what kind of artifacts they may leave behind. In Chapter 6 of this book, you will learn about the /proc filesystem and what
important data you have to collect from it before powering a system down. In Chapter 7 of this book, you will learn about the various file types that should be analyzed and how to analyze them. In Chapter 8 of this book, you will learn about malware as it exists in Linux
machines, and what kinds of signatures they leave.