

## Real-World Scenario 18-2: Imaging a Hard Drive and Live Data for Forensic Purposes

**Scenario:** You work for a small organization and wear multiple hats: network administrator, cable installer, security administrator, and digital forensic analyst, when required. Upper management is concerned that an employee (who left work suddenly and didn't return) might have been attempting to compromise the organization's secret data. Your task is to document the potential crime scene (the ex-employee's workstation), analyze the data on the computer, and learn whether there is any merit to the organization's concerns.

Name several forensically acceptable software tools you can use to image the hard drive.

Name a forensically acceptable software tool you can use to copy the live data.

Name several LiveCDs that you can use to image the drive (which might or might not be forensically acceptable).

**NOTE** When I use the term *LiveCDs* I mean any Live optical discs or USB flash drives.

## Real-World Scenario 18-2 Solution

The key with a potentially compromised computer is to document everything you see (and can't see). Take photos, write down what you encounter, and of course, use software and hardware tools to image the machine.

For example, to image a hard drive you might use AccessData's Forensic Toolkit or Guidance Software's EnCase. These are commonly used tools that are usually accepted by the courts as forensically sound applications. Of course, these tools come with a price tag (a hefty one), so in some cases a smaller company will go with simply imaging the drive bit by bit, which could be done with cloning software or with a LiveCD (or LiveDVD/Live\_Flash\_Drive) such as Knoppix or BackTrack. The question here is whether these tools (and the resulting hard drive images) will be acceptable to a court of law. Also, you must be very careful not to disturb the original drive when making the image, something that can easily be done when using a tool not designed specifically for the job.

If you were to use a LiveCD—and there are many options—it would be derived from Linux, so a solid knowledge of the command-line would be necessary. For example, if you were to image a drive, you would need to understand the syntax of the `dd` and `nc` commands. Plus, you would need to copy the data from one system to another. Many forensic analysts will use a Linux OS (such as Ubuntu) as the destination computer for the copied image. That system would have a secondary drive that could either be analyzed or booted off of if necessary.

For live data—and we are talking about the RAM and other volatile areas of the computer—you could use Live Response, which might run off of a USB key, and Helix software. That is only if the computer is already powered up when you encounter it. If the computer is off, then volatile areas of storage will most likely be cleared.

Important! Remember your incident response plan phases:

**Phase 1. Preparation:** It all comes down to preparation. Consider a data breach, for example. An organization with no planning

will take much longer to repair the problem and will have a hard time controlling the damage and loss. But an organization with a well-planned incident response procedure in advance, a strong security posture, and a knowledgeable CISO will be able to limit the damage (to data and to the company reputation) by quickly discovering the breach, having an internal response team ready to take action, obtaining forensics data quickly, and beginning a seamless notification process and inquiry response plan.

- Phase 2. Identification:** The recognition of whether an event that occurs should be classified as an incident. Once identified, you might be required to make contact with other groups or escalate the problem if necessary.
- Phase 3. Containment:** Isolating the problem. For example, if it is a network attack, the attacker should be extradited to a padded cell where the attacker can be analyzed and monitored. Or if only one server has been affected so far by a worm or a virus, it should be physically disconnected from the network. The same goes for devices—they should be removed from the network or from a connected computer if the incident concerns them. This phase might also include evidence gathering (in a way that preserves the evidence's integrity) and further investigation so that you can ascertain exactly what happened and why.
- Phase 4. Eradication:** Removal of the attack or threat, quarantine of the computer(s), device removal if necessary, and other mitigation techniques covered previously in this book.
- Phase 5. Recovery:** Retrieve data, repair systems, reenableView servers and networks, reconstitute server rooms and/or the IT environment, and so on. Damage and loss control come into play here; making sure that as much data is recovered as possible can be a very slow process.

**Phase 6.**    **Lessons learned:** The scenario should be reviewed to define what went wrong and why, ultimately defining the lessons to be learned—how the organization can improve. Document the process and make any changes to procedures and processes that are necessary for the future. Damage and loss should be calculated, and that information should be shared with the organization's accounting department. The affected systems should be monitored for any repercussions.

**NOTE** There are no videos or simulations for this real-world scenario.