Menu

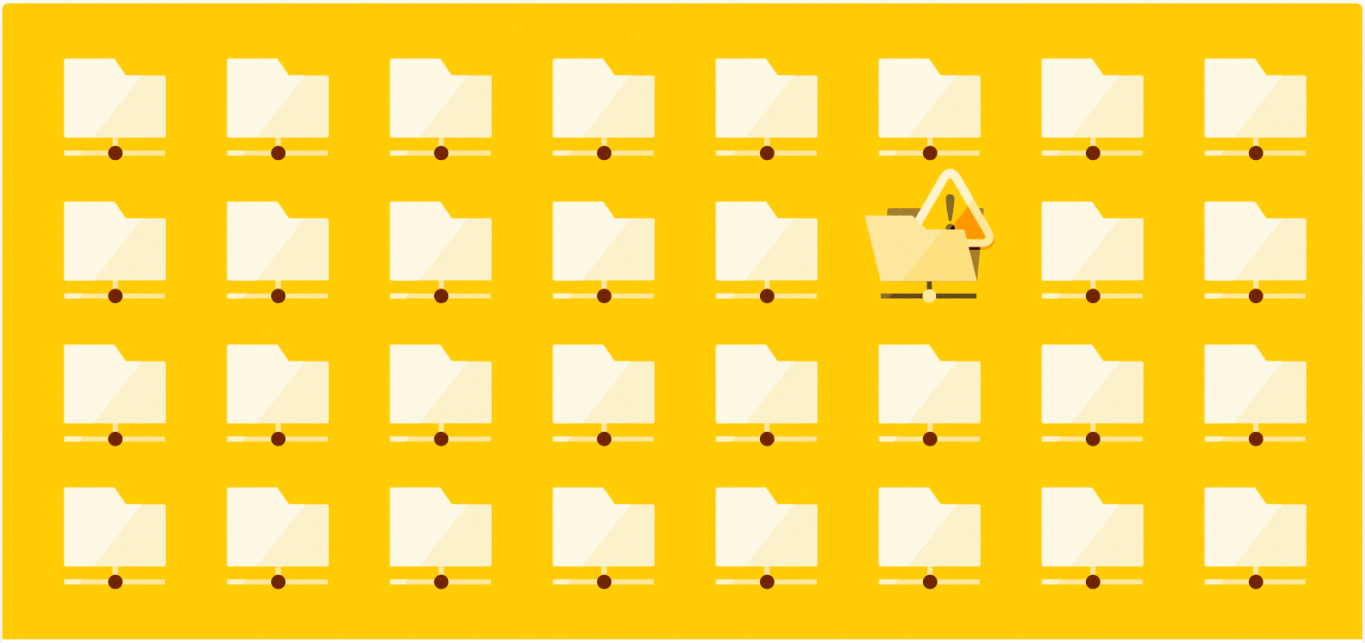
What Can You Learn From a “Wiped” Computer With Digital Forensics?

1,662 people reacted

2 4 min. read

SHARE

By Michael Savitz
May 27, 2021 at 12:00 AM
Category: Unit 42, Unit 42
Tags: Exposed Data, insider threats, Unit 42, vulnerabilities, wiped



This post is also available in: 日本語 (Japanese)

Executive Summary

It’s easy to assume deleting data from a computer is comparable to burning paper documents – what’s gone is gone. But is it?

There are many scenarios in which individuals would like data to be truly gone, potentially to hide a trail of criminal behavior. Yet others hope it’s recoverable, perhaps to piece together a trail of evidence.

Consider the following scenario:

An employee resigns and joins a competitor working on a similar product. The company suspects the employee shared proprietary information with her new company before resigning. However, the employee returned her laptop “wiped” of user data. In this state, what can the company learn about how the computer was used?

The question is whether digital evidence can be effectively and completely deleted or obfuscated. While some still assume otherwise, it’s becoming more widely understood that merely “deleting” data doesn’t necessarily mean it’s truly gone. Indeed, there are tools available that go beyond simple deletion to truly securely delete or wipe data.

To further muddy the waters, the term “wipe” can take on very different meanings. It might refer to simple deletion, reformatting a drive – or securely overwriting data numerous times, such that it is truly not recoverable.

Below, we look at how digital forensics can be used to determine the extent to which data has been wiped, as well as to recover digital evidence.

Using Digital Forensics to Recover Wiped Data

As digital forensic examiners, we have learned to always dig a little deeper when a computer is reported to have been “wiped.” There are often relevant answers or information our analysis can provide, even if only confirming when and how the wiping occurred. In many cases, however, we can recover deleted data and evidence of additional activity that helps reveal significant clues about how a computer was used.

In its simplest form, digital forensics is the collection, preservation, examination and analysis of data stored on digital media. A digital forensic examiner uses forensic methodologies that are reliable, repeatable and as minimally invasive to the data as possible, so that all actions and processes can stand up in a court of law.

Every action a user takes on a computer can leave a digital footprint. Digital forensics experts use tools and techniques to uncover these traces by looking at the data at its physical, or disk, level. For example, forensic analysis can pinpoint the time a user connected to a coffee shop’s WiFi, uncover chat history between two colleagues, identify external storage devices attached in the past and other actions. Forensics tells the story of how a user interacted with their device, especially when that user took steps to hide their tracks or delete data. In the digital world, what’s gone is often not truly gone.

Examples of Digital Forensics in Data Recovery Operations

Let’s look at two examples we encountered of how digital forensics told the story and uncovered malicious acts.

Example 1: Data Recovery Reveals Extensive Coverup of IP Theft

In the scenario described in the executive summary, digital forensics ultimately uncovered the theft of intellectual property and destruction of data. A forensics expert recovered fragments of previously deleted files and other essential forensic artifacts from the ex-employee’s laptop. Among the key findings, the forensic expert identified evidence that code reviews, rollout plans and other proprietary information were accessed from thumb drives while the laptop was connected to the network of a competitor (and the ex-employee’s new employer) days after she resigned.

The most damaging revelation was that digital forensics uncovered the considerable lengths to which she went to mass-delete files and cover her tracks. Just days prior to returning her laptop to her former

employer, the ex-employee installed a remote access tool and received an incoming connection from an IP address that resolved to the remote location of an outsourced technician of the company, who was suspected of being a co-conspirator. Seconds after the successful incoming connection, mass deletions occurred on the laptop. Without the use of digital forensics, the company would never have found out about the illicit acts carried out by their ex-employee and the outsourced technician.

Example 2: Digital Forensics Proves File Theft

In another matter, a company suspected that a recently departed employee stole intellectual property right before he left, but they had no way to prove it. An initial review of the user’s Mac laptop found that most files and folders had been deleted. However, digital forensics proved that this ex-employee connected his work laptop to his personal iCloud account, synchronized several folders containing proprietary data and then deleted those same folders from the laptop just days before resigning. Experts analyzed forensic artifacts and system logs that captured historical records of those folders, the approximate time of the iCloud synchronization and subsequent deletions from the laptop. Forensic evidence revealed that the data was backed up to a personal time capsule around the same time. These findings supported the company counsel’s legal basis to request an examination of this ex-employee’s personal devices.

Conclusion

As these examples illustrate, just because data appears to be gone doesn’t mean that it really is. Digital forensics was used to recreate the story of how each of these individuals stole information from their employer and then took steps to destroy data and cover their tracks. It is likely that in both cases the perpetrators didn’t realize a forensic expert had the ability to retrace those footprints and uncover the truth.

Unit 42’s Incident Response team can help with data breaches and other cases that may require digital forensic analysis and investigations.