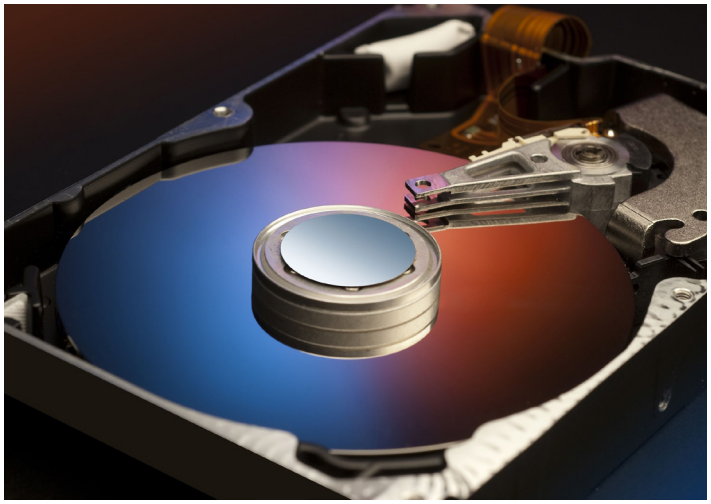
Protecting
Your Data™

Hard Drive Security Study

INTRODUCTION



The purpose of this paper is to promote personal hard drive security, and to discuss why everyone should think about what happens to their old hard drive when upgrading to a new computer.

This paper includes the study of a purchase of 20 used hard drives on eBay, looking for data that was accidentally sold along with them.

This is the third paper in the last seven years that has studied used disk drives purchased from eBay. In all three studies, we found data that would be considered extremely valuable to their owners–including complete tax records, privileged attorney/client information, scans of completed federal forms, and more.

Finally, this paper discusses how to properly erase a hard drive and highlights some common ineffective methods.

WHO WE ARE

CRU is a maker of hard drive storage systems and digital forensic tools. In 2008 CRU acquired WiebeTech, maker of computer forensic hardware. Since then, CRU has continued to advance forensic hardware technology and has created innovative new products for government and corporate security and eDiscovery, such as the Ditto Forensic FieldStation.

YOU HAVE DATA THAT A BAD GUY WANTS

Most people use their computers for more than "just email". We use computers to help us with our taxes, buy goods online, interact with our banks, pay our bills, connect to social media, and store our personal photos. This means that our hard drive is likely to record our social security numbers, income, address, credit card numbers, personal account information, and keeps photos of ourselves, our friends, and family members. A modern hard drive paints—and stores—a fairly complete picture of our lives.

One common myth we hear is "I'm not important enough to be interesting to a data thief." There are many types of valuable data that are on your hard drive right now. Even if someone only uses a computer for email, an email address book is worth money. Combined with demographic information, email addresses become even more valuable.

An identify thief, armed only with a compromised email account, can impersonate a victim and obtain increasing levels of access to other accounts. Many online accounts/institutions often consider ownership of an email address to be a valid form of identification. A password to an email account grants access to social media sites, for example, where the attacker may learn answers to personal security questions, such as "mother's maiden name" or "favorite pet"—information that can then be used to gain access on "more secure" websites, such as banks.

WHAT DID WE FIND ON THE DRIVES IN THIS YEAR'S STUDY?

We found everything a bad guy would want: Credit card numbers, Social Security numbers, tax records, addresses, birth certificates, college registration information, personal photos, and more.

It's lucky for the former owners of these drives that we're the good guys. These drives and all copies of the data on them were securely erased after the examination.

THE LAWYER'S DRIVE

Of all of the drives in the 2014 study, one stood out from the rest. The original owner of the drive was a lawyer, and we have no doubt that his clients would be upset to learn that the person they hired and trusted to keep their information private and secure failed to do so. The lawyer, in turn, would likely be upset that the PC shop that had his hard drive, sold it without erasing it properly.

A lot of the data on this hard drive was about the lawyer's family and legal business, but it also included documents about clients and their legal cases.

On the first attempt, this hard drive appeared to be non-functional—the drive would click instead of mounting. We found that the drive would function properly only if oriented upside-down; when a hard drive is having a hardware failure it can help to return it to the orientation it was most used in in order to recover data.

Here's a brief list of what we found on that one hard drive:

- The lawyer's wife's W2s—including SSNs and income information
- His completed, signed, and scanned 1040 tax return
- A signed—but otherwise blank—power of attorney form
- A scan of a police-issued ticket to the lawyer's son on possession of marijuana
- Records indicating his son's commitment to a rehabilitation center, including bills, receipts, and detailed weekly progress reports
- Scans of handwritten letters from the son back to home
- Debt reduction information with a certain bank, including detailed lists of assets, such as specific stock holdings, owned by the hard drive owner
- Scans of the drive owner's driver license
- The drive owner's credit card numbers (with expiration

date and CSV) on hand-written and scanned documents

- And finally, volumes of client data (judge orders, motions filed, etc.) in more than 500 PDFs and 500 word documents

A majority of this drive went unchecked, as there was no point to continue—clearly there was a lot of damning information.

THE FAMILY LAPTOP

Another interesting drive came from a laptop shared by members of a wealthy family, who clearly enjoyed cars and travel; this family would thus be an excellent target for an identity thief. This was one of two drives in the study to mount with data intact. At first glance it appeared that there was no attempt (not even a failure of an attempt) to erase personal data. The contents were completely unencrypted, and so it was easy to go into Windows users' directories and look at how they used the computer. Within moments we could find a home address, maps to their house, and credit information.

There were four Windows user accounts: One for each parent, and one for each of the two college-aged sons. The sons used the hard drive more than the parents, and in their directories we found many files.

No attempt was made by the drive user or the drive seller to erase the following files:

- Homework (architecture and computer science) and resumes
- A single document titled "DADS CREDIT CARD INFORMATION.doc." which contained a MasterCard number with CSV, and date of expiration.
- 1,243 commercial MP3s (5.46 GB)
- 3,484 JPGs—photos of their cars, house, family members, friends, vacations, etc (1.79 GB)
- At least one feature-length pirated movie and several TV shows (AVIs)

We looked into the "RECYCLER" directory for each account. Most were empty, but one had data—including scans of a user's driver license along with personal self portraits that most people would have intended to stay private and would be justifiably mortified to learn that anyone else saw them.

Next we ran a recovery application to look for "deleted" files—

files no longer used by an application or were "deleted" by way of the Window's Recycle Bin. We found many more files:

- Hundreds of additional college work papers, syllabi, and university information (including addresses to dorm rooms)
- 13,849 JPGs—social media image thumbnails, personal pictures taken at dorm parties (with accompanying videos), and trails of surfing the internet for pornography.

SOME STATISTICS ABOUT WHAT WE FOUND THIS YEAR

20 used hard drives were purchased on eBay in September 2014.

- 3 of the 20 (15%) were initially considered dead on arrival, but with effort we were able to perform full ranges of recovery on each
- 7 of the 20 (35%) were wiped with a repeating pattern
- 2 of the 20 (10%) were encrypted, wiped with a random/non-repeating pattern, or part of a RAID set
- 2 of the 20 (10%) were not erased properly but no interesting data was found after recovery—for example we found default OS files, but do not count them as interesting
- 9 of the 20 (45%) had discernable, interesting data

We define interesting data as: personally identifiable information, or valuable data, in the form of tax returns, legal client info, MP3 collections, software license keys, personal photos, videos, email, or web history that reveals information

about the user.

Of the nine that had interesting data:

- Five contained enough information to personally identify the primary user (it's possible that with additional effort, the remaining 4 could have as well)
- Four contained pornography (either of the hard drive users themselves or collections/web cache)
- Four had commercial MP3 collections
- Seven were reformatted or repartitioned in a way that didn't wipe most of the hard drive
- Two mounted and immediately allowed access to interesting files before recovery was attempted; in both cases even more interesting data was found after recovery was used

METHODS OF RECOVERY AND HOW WE CHOSE WHICH DRIVES TO BUY

The methods used to discover data are methods readily available to anyone. We used free and inexpensive data recovery applications on both Mac OS X and Windows platforms to recover files from the hard drives. Unlike a normal drive recovery situation (where someone lost their hard drive and didn't back up), the data thief can obtain useful information even from corrupted files.

We did what a data thief can do easily—we looked for used hard drive listings on eBay that did not specifically describe the drive as "wiped." It should be mentioned that many eBay listings did in fact list a drive as "wiped." However, this only made it easy to know which drives to avoid. Our goal wasn't to test if they wiped a drive if they said they did, but to seek data in the way that a data thief would. We would buy a drive if it said "formatted," "tested," or otherwise didn't state what they had done to the drive.

For easy access to the bare drives we connected them to our computers with a WiebeTech Forensic ComboDock v5. This dock allows a read/write mode as well as a write-block mode. This is the same hardware write-blocker used by all levels of local and federal government for forensic examination of hard drives.

After the discovery process all found files were permanently deleted and the hard drives were wiped correctly with a

HISTORY OF DRIVE PURCHASES FROM EBAY

On three separate occasions, we purchased used hard drives on eBay to see what data were being left on them after sale. We quickly found tax documents from (with salary, SSN, address, etc.), legal records (including a lawyer's drive, with information about clients), vast amounts of email and personal photos, and trails of web surfing. When a drive contained data, it often contained information about several people (and email addresses of their contacts). By viewing the data we can often determine the drives' original owners—they were a range of corporate, legal, and end user.

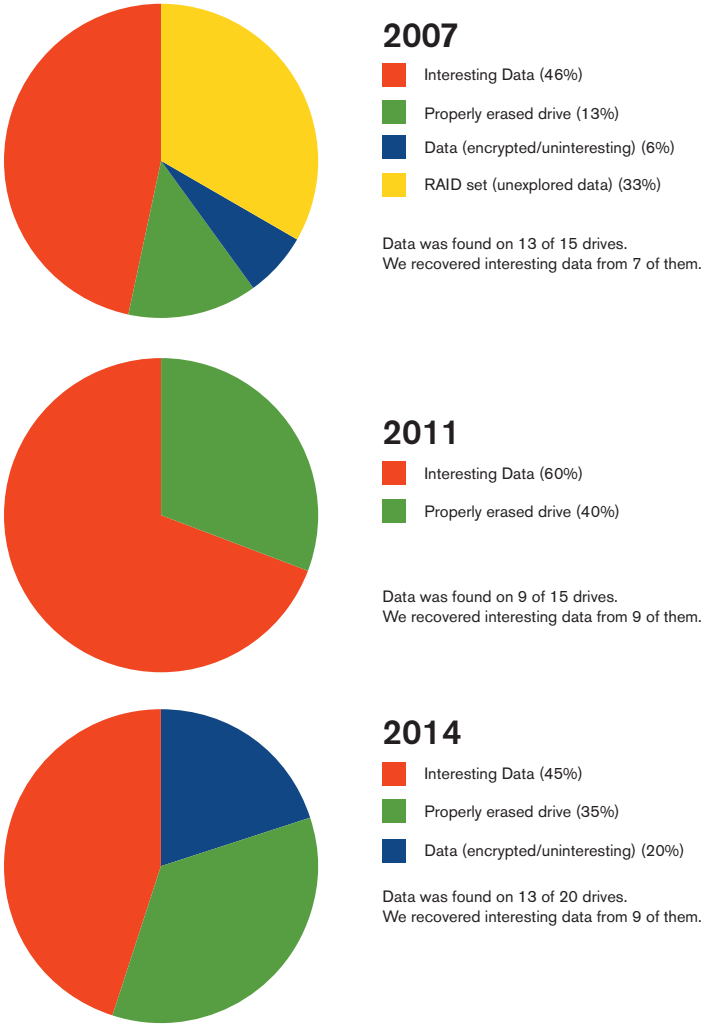


Figure 1
While the amount of encrypted (or otherwise unuseful) data has increased, our third buy shows that a majority of the drives we purchased aren't being erased properly, and that it's still easy to discover data on a used hard drive.

CRU Drive eRazer Ultra, a stand-alone hardware device that correctly wipes and sanitizes hard drives.

HOW OUR RESULTS COMPARED WITH OUR PREVIOUS STUDIES

This year's results are in line with previous years' results. While we found more encrypted data than ever before, and several drives were uninteresting (such as partitions with nothing but a basic Windows install), we did not find a significant change in "properly erased" data from any previous study. We also didn't see much of a change in the percentage of interesting data from previous years. (See Figure 1.)

WHAT IS STANDING IN THE WAY OF HARD DRIVE USERS TO PROPERLY DELETE DATA?

- People don't know they should
- People don't know that what they're doing is ineffective
  - Dragging everything to the trash/recycle bin
  - Formatting or reformatting the drive
  - "Repartitioning" or removing the partition table from a drive
- People think that an "effective method" is so difficult to achieve, that they do nothing
  - Physically obliterating the drive into small particle sizes
  - Performing more than one wipe, in some cases, people think they need to erase 32 or more times.

The improper erasure methods outlined above don't actually erase the files themselves—just the index that tells you where to find your data. Imagine a card catalog system that knows where books are located in a library: If you destroy the card catalog, the books themselves never moved from the shelf. You can still walk to the shelf and get the book. Likewise, when you erase only the index of a hard drive with one of the above methods, software can still read the file itself from the hard drive—this process is called file recovery.

WHAT IS THE CORRECT WAY TO ERASE A HARD DRIVE?

This has a very simple answer. With a dedicated software or hardware tool that is meant for the task, write over the entire hard drive. It doesn't matter if you write over it with a "zero" in every bit (known as zeroing out the drive), a "one" in every bit, some other pattern, or completely random data. The hard drive has only one job: to store, for later retrieval, exactly what you last wrote to it.

It's our position that hardware, such as the CRU Drive eRazer Ultra is better suited for the task of performing bulk erasures. A stand-alone, hardware drive erasure product offers advantages:

- Operates without tying up a computer
- Erases as fast as the drive will allow (with no chance of interference from other apps)
- Proper handling of hidden areas of the drive—such as Host Protected Areas and Device Configuration Overlays (HPAs and DCOs)—a valuable feature not available on many software products
- Performs a quick verification that the erasure was successful
- No need to create and maintain external boot media

Many organizations, especially governmental agencies, have their own policies that dictate their own methods of drive erasure and disposal that may go above and beyond the one-pass recommendation. We understand these policies extend beyond protecting from possible file recovery, but also protects from breaches in internal protocols as well. We also recognize that government agencies with potentially top

secret data must take additional security steps—up to and including complete destruction of the hard drive.

SHOULD A USER WRITE OVER OR ERASE A DRIVE MULTIPLE TIMES?

Because some people are concerned that previous generations of data stored on a hard drive can be retrieved in a laboratory or other state-of-the art setting, they believe they must write over each bit on a drive multiple times.

The reality is that hard drives are quite varied and complex in their designs and operation. For example, data writing patterns on drives are often striped between platters (which will change by manufacturer and model)—meaning the physical location of each bit is information itself, and bit sizes are physically small and shrink every year. An identity thief, even one with advanced skills, will not have the sophisticated technology or laboratory equipment that would be necessary to recover data that has been sequentially overwritten via available software or hardware products.

CONCLUSION

With today's used hard drive market, it is still easy for a data thief to target and recover valuable data—about as easy as it has been since our first study in 2007. Half of the drives that we purchased for all three studies combined contained interesting data.

Even though the solution is simple—to perform a complete one-pass write over the hard drive (called a wipe), there continues to be reasons why people don't do it.

We believe the reasons are threefold:

- Lack of awareness about where old hard drives go when they're not needed any more—many IT shops may resell them
- A socially lax attitude: i.e. "old data isn't important anymore"
- Lack of knowledge about how to erase a drive properly

Selling a used hard drive can be a good idea. For that to be considered a "safe" practice, there needs to be an increased level of awareness among users and vendors alike. Every computer user has a responsibility to make sure their drives are wiped correctly before they sell it. A common way drives are sold without being wiped occurs when users fail to know what a PC repair technician does when they "recycle" old equipment. In cases like these, users should ask what the policies about used hard drives are, and consider performing a proper erasure themselves.

For more information, visit the CRU web site.

cru-inc.com
sales@cru-inc.com