

Re: FileCopy overwrites the existing file

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-12/msg00197.htm>

- *From:* "David J. Craig" <Dave@xxxxxxxxxxxxxx>
 - *Date:* Tue, 5 Dec 2006 21:32:42 -0800
-

I would not say that with the assurance you seem to have. I would ask in the ntdev newsgroup where two people who work for a hard drive company read and post. I am certain that the hard drive companies have done this and don't forget the data recovery people. Also you can't get any information about this, but do you think the "No Such Agency" hasn't already done it.

There are some theoretical attacks on SmartCards using a microwave oven that had not been successfully done, but I also heard some of the SmartCard manufacturers were engineering their new cards to protect against it. Just because you haven't heard of it being done doesn't mean it hasn't been. I don't work at a company where I have access to a class 100 or better clean room which would be required for the hard drive attack.

"anton bassov" <soviet_bloke@xxxxxxxxxxxx> wrote in message
<news:1165349136.522972.114120@xx>

To understand it you'll need to go much lower level than most computer scientists do, ie below NAND gates and ask yourself what really binary 0 and 1 is. On electronic level 0s and 1s are determined by measuring voltage. When you overwrite former 0 by 0 and former 1 by 0 you'll get different voltage measurements (same with overwriting by 1). Of course both of these will be read as logical 0 (1) by the hardware. But now you can already imagine that a specially tuned hardware will be able to distinguish between those, thus recover the former value.

Exactly – this is what speculation about the possibility of recovering overwritten data is based upon. From the logical standpoint, the task in itself is **THEORETICALLY** feasible – no one argues about it. However, AFAIK, in practice no one has yet demonstrated how to do it in more or less reliable way. This is the reason why no data recovery company gives you 100% guarantee of success – if data has been actually overwritten, there is a very good chance that it is gone forever.....

Re: FileCopy overwrites the existing file

Anton Bassov

Grzegorz Wróbel wrote:

anton bassov wrote:

if you refer US
Department of Defence they, depends on how documents are
classified
recommends up to 7 times rewriting with random data (if I
remember
well).

Three times is the actual standard. Indeed, there was a *SUGGESTION*
that overwriting data up to 7 times may be needed, but, again, this is
just a speculation.
Concerning classification, AFAIK, top-secret data is still destroyed
only by disk incineration.....

I recall reading some newer document stating 3-times overwrite is
required for documents classified as CONFIDENTIAL and 7-times write for
documents classified as SECRET. I can't find it on my hardrive though ;)

Recovering overwritten data is NOT a speculation, it can be
done and
any
good software recovering company will do it without
problems if the
data
was overwritten only once (we're talking about magnetic data
storage
disk here).

AFAIK, they deal only with such things as disaster (i.e mechanical or
electrical damage to the disk) recovery, formatted disks, accidentally
deleted files, etc, and still they never guarantee that absolutely all
data will be recovered – when it comes to recovering data that has been
actually overwritten, they are out of luck (unless they are able to
find a copy of it somewhere on the disk, which happens quite
often).....

I wrote a data destruction utility some time ago. I was quite confident
that one-pass overwrite will be enough if you chose a good random number

Re: FileCopy overwrites the existing file

generator (large seed and enormous period). I realized much later I was wrong, because not only choosing good pseudo-random number generator is critical, but multiple overwrite as well. To understand it you'll need to go much lower level than most computer scientists do, ie below NAND gates and ask yourself what really binary 0 and 1 is. On electronic level 0s and 1s are determined by measuring voltage. When you overwrite former 0 by 0 and former 1 by 0 you'll get different voltage measurements (same with overwriting by 1). Of course both of these will be read as logical 0 (1) by the hardware. But now you can already imagine that a specially tuned hardware will be able to distinguish between those, thus recover the former value.

What is worse you can't tell how much times you should really overwrite the data to make it unrecoverable, since whether it will be recoverable or not depends on given hardrive characteristic. That is why (or at least one of the reasons), what I believe, documents classified as TOP-SECRET are not to be destroy this way.

--

Grzegorz Wróbel

<http://www.4neurons.com/>

677265676F727940346E6575726F6E732E636F6D