

S&P Column for “Privacy Matters”.

DIGITAL “EVIDENCE” MAY NOT BE “EVIDENCE” AT ALL.

AN EDITORIAL¹

Michael A. Caloyannides

Unlike conventional analog data, such as the shade of grey or the subjective recollection of a witness, digital data which takes one of two very unambiguous values (zero or one) is misperceived by the average person as being endowed with intrinsic and unassailable truth.

In fact, quite the opposite is true. Unlike conventional, analog, data and evidence whose tampering can often be detected by experts with the right equipment, digital data can be manipulated at will and, depending on the sophistication of the manipulator, the alteration can be undetectable regardless of digital forensics experts’ competence and equipment. The potential for miscarriage of justice is vast, given that many defense lawyers, judges and juries are unaware of the technical details of computer science. This “dirty little secret” about digital “evidence” is conveniently soft-pedaled by the computer forensics industry and by the prosecution, both of which focus on those *other* aspects of the process of collecting, preserving and presenting digital data evidence which are indeed unassailable, such as the “chain of custody” portion of handling digital evidence.

Let’s take a common example of “computer evidence”. A suspect’s hard disk is confiscated, subjected to forensics analysis and a report is generated for the court which states that the hard disk contained this or that file, and that these files dates’ were this and that, that these files were re-named or printed on this and that date, thereby negating the suspect’s claim that he did not know of the existence of these files, etc.

A typical judge or jury will accept these facts at face value. It should not, for the following reasons:

1. The data found in someone’s hard disk (or other mass storage media) could indeed have entered that hard disk through any one or more of the following ways

¹ This is not a research paper but an editorial based on the author’s experience and background. This editorial will not review the state of the art in computer forensics. The field of computer forensics has far too many references to be cited in this brief editorial. The interested reader may wish to review, for example, “Computer Forensics and Privacy”, Artech House Publishers, 2001, ISBN 1-58053-283-7, and “Desktop Witness”, John Wiley Publishers, 2002, ISBN 0-471-48657-4, both by this author.

without the suspect's knowledge, let alone complicity. All of these paths for surreptitious data entry are very commonplace and occur on a daily basis.

- a. The hard disk was not new when the suspect purchased it, and contained files from before the suspect took custody of it. This applies even in the case of purchases of "new" computers because they could have been resold after being returned by a previous buyer. Even if that hard disk had been "wiped" (i.e. overwritten) by the seller and the software reinstalled, there is no physical way to guarantee that some data were not left behind; this is why the classified community will never allow a disk to leave a secure installation but will physically destruct it.
- b. A large amount of software packages today (referred to as "ad-ware" and "spy-ware", take it upon themselves to secretly install unadvertised files and a capability for the software-maker to snoop on the individual's computer through the Internet or other network. If this "snooping" capability is exploited by a third party hacker who routinely scans computers for this "back door entry", then files can be inserted on the suspect's computer at will.
- c. Over the years, a large assortment of malicious software, such as "Back Orifice", "Back Orifice 2000" and numerous others, when installed (remotely or inadvertently by the user) on unsuspecting users' computers, have been demonstrated to allow hackers to take over these unsuspecting user's computer and modify, delete, or install files in them.
- d. Obtaining full control of anyone's computer through the Internet does not even require that such "ad-ware", "spy-ware" or any hacking tools like the above to have been installed. Microsoft has been admitting to numerous existing security flaws in its operating systems and applications, especially its Internet Explorer, that allow anyone to gain full control of anyone else's Internet-connected computer and insert files in it without the victimized computer's owner knowing anything about it. Other operating systems have had their share of comparable weaknesses but their impact is not anywhere near as large simply because most computers today use Windows. Discoveries of new online "back door entries" to anyone's computer have been appearing at an average rate of at least one every month for the last several years.
- e. When any of us "browses" the Internet, it is not uncommon to mistype and end up inadvertently and unintentionally on a web site which is often an adult site. Even without mistyping at all, however, one can still end up at an incriminating site for the following reason: hackers have often doctored up entries in the domain name servers (DNS)², which amounts to

² The Internet does not "understand" names such as www.cnn.com and only understands addresses in number form, such as 123.456.789.012; the translation from a name to a number is done each and every

doctoring-up the directory which is accessed every time we type the name of a web site we want to see.

- f. Unlike “cookies”, the short datastreams inserted by remote web sites into our hard disks that, over time, paint a picture of one’s web browsing history, which are fairly well known, “web bugs” are more insidious. An email, a Usenet Newsgroup posting, or even any file that supports HTML, may (and often does) contain invisible single pixel white dots; the html-enabled software will dutifully try to connect one’s computer to the Internet address (the “URL”) referenced in this html code of the single pixel in order to retrieve this single pixel image. This is done behind the computer user’s back. If this URL being visited is one that a court would view as inappropriate and if the user has not taken specific steps to disable this automated Internet access, a user could end up with a record of repetitive visits to potentially incriminating Internet sites that the user really had nothing to do with.
- g. Even in the absence of any of the foregoing, the fact of life is that the Internet is largely free to the user; since nothing in life is really free, the revenue source for many “free” web sites we visit on the Internet comes from advertising in the form of pop-up ads, scrolling text, images, etc. Often these advertising images are not ones of facial crèmes and vacation packages but of unclad underage persons. While one can rapidly go to a different web site, the fact is that, unless one has gone to the trouble to change the web browser’s default settings (of storing web pages on the disk) to not storing anything, these offensive images get stored (“cached”) in one’s hard disk drives. Over a period of time, enough to them collect in any of our computers and an overzealous prosecutor can claim that there is an “obvious pattern or proclivity that stretches over a few years”. A hapless defendant will have a very difficult time convincing a technology-challenged judge or jury that he/she knows nothing about how those images got there.
- h. Unless one lives by oneself and never admits anyone to his/her house, chances are that one’s sons, daughters, spouse, or some friend or relative will use one’s computer during a computer’s typical lifetime of a few years. In that case, it is not inconceivable at all that such other persons could have visited web sites that you or I would not have patronized.
- i. Unsolicited email is as common as the air we breathe. Many of them peddle get-rich-quick schemes, pyramid schemes, sex, and just about everything else. Most people ignore them; many delete them. But here is the problem: aside from the fact that deleting does not delete anything (it

time we type a URL name (such as www.cnn.com) by the Domain Name Server network (DNS) which is a network of computer servers around the world that does just that for a living.

merely tells the computer that the space on the disk occupied by that file or email, which is in fact not erased at all, can be used in the future if the computer feels like it), hardly any of us goes to the trouble to delete *attachments* that often come with such unsolicited email; and even if we did, the attachment would still remain on our hard disks for the same reasons. Perhaps nobody, other than computer experts, will go to the trouble of *overwriting* the offensive attachment, because Windows does not include any provision to overwrite anything; one has to buy special software for this and most people don't. And even if one did go to the heroic step of overwriting a file with specially purchased software, the name of the file, which could be quite incriminating in and by itself, and which is stored in a different location than the file itself in our hard disks would not be overwritten, to the delight of the forensics investigator who has a vested interest in finding something incriminating. Again, the hapless defendant will have a very hard time convincing a non-technical jury that such offensive files were not solicited (or even tolerated). Even if one went to the heroic steps of overwriting unsolicited email attachments and their separately stored names (nobody does that), fragments of these incriminating files may still be found by forensics investigators in the swap file.

- j. The Wi-Fi (802.11a,b,g,x) route. Wireless access in the US is increasing at an explosive rate. It can be found at McDonald's, Starbuck Coffee, many airports, many hotels, and most important to this discussion, in our homes where we may like to access our high speed Internet connection from anywhere in the house without running wires all over the place. The literature is full of the technical details of how insecure this "standard" is; "out of the box", Wi-Fi are configured to require no password, no encryption, and no security at all; most users do not tinker with those default settings. Now, radio travels over far larger distances than what these boxes claim, and it is not uncommon for a home Wi-Fi to be accessed a full 5 miles away if one builds a directional antenna and drives around town looking for other people's home Wi-Fi's to connect to, a practice known as "war driving". Once connected, which is trivial since there is no security, the "war driver" has full access to the victim's computer *and* Internet connection. This means that files can be placed into or removed from the victim's computer, and it also means that the war-driver can leave a long trace of illegal Internet activity in the victim's Internet Service Provider's records. Now imagine the very common situation where the victim is at home, is the only person at home, and the war-driver uses the victim's computer to engage in any one or more of the multitude of illegal activities that can be conducted over the Internet. The finger will be pointed at the victim as being the "obvious" perpetrator; good luck convincing an uninformed Court that the victim was a victim and not the perpetrator.

- k. Computers crash sooner rather than later. The typical course of action for one is to take the computer to some repaid person in an effort to be able to access one's prized personal and business data. While computer repairmen use special diagnostic software, test the computer's Internet functionality, and have every opportunity –though hardly any motivation– to place data into the repaired computer. A few years later, the owner of the computer is likely to have forgotten about the repair altogether and never bring it up in his/her defense.
2. Computer forensics examiners like to substantiate their findings by pointing out the time/date stamp associated with different computer files as if those time/date stamps were kept in a vault that is inaccessible by mere mortals. This is patently false. The date/time stamp, as well as every single bit of data in a computer's magnetic media can be altered undetectably just as readily and any other data in one's data storage media, so that the "evidence" found by the forensics investigator will substantiate what one wants it to. All it takes is a disk editor, which is openly available (e.g. in Norton Utilities), to change any metadata (data about data, such as who did what and when) in a computer, whether date/time, or anything else.
3. Unlike conventional film-based photography where a competent investigator can usually determine if it has been doctored, digital images (such as those taken by any surveillance camera) can be altered in a manner that no expert can detect, if the alteration was done professionally enough. Noise and blur can be digitally added to the end result to further hide any digital tinkering that might have been detectable at the individual pixel level by even an expert. "Pictures don't lie" is a lie.
4. As with digital photography, so with digitized sounds and even plain old documents. Unlike analog sounds of yesteryear (e.g. the infamous gap in the tape recordings of Nixon's office), where a careful study of the background noise can detect alterations of analog recordings), digitized files of sounds can be altered at will; if the alteration is done professionally enough, it will be undetectable by even a forensics examination of the digital file.

In summary, we are witnessing a new phenomenon in today's courtrooms. All of us store in our computers more and more information about our lives and activities. This has resulted in an explosive increase in computer forensics on confiscated or subpoenaed computers on the incorrect assumption that "what is in the computer is what we put in it". An entire cottage industry of computer forensics investigators, some more qualified and

competent than others, has sprung up to service the insatiable appetite for such services by all.

The legal and societal problem with this social phenomenon is that most individuals in the legal and law enforcement professions are unaware of at least some of the many ways I summarized above whereby the data they present as evidence is really not evidence of anything because it is routinely placed in one's computer without the knowledge or complicity of the owner of the computer.

Independently, "evidence" presented which is based on one's Internet Service Provider's records is, similarly, evidence of nothing because one's Internet account can be (and routinely has been) accessed by third parties without one's awareness or complicity, even if one was the only person at home when the alleged Internet access occurred.

A few months ago, a British youth was acquitted of some computer-related charges after the court accepted that some "Trojans", (one of malicious code) in his computer could have been used by unknown third parties to perpetrate the act of which that youth had been accused. This acquittal has alarmed some law enforcers.

Defense lawyers and judges should get urgently needed remedial education in digital forensics. Digital evidence should be viewed with extreme suspicion, regardless of the competence or qualifications of the computer forensics expert witness. While the "chain of custody" portion of the rules of evidence may have been impeccable, the raw digital data itself on which a forensics analysis was done can be easily and undetectably tampered with by anyone with the right background. Digital evidence is often evidence of nothing.