Evolving Standards: Encryption and Protection against Digital Evidence Tampering

By James Wiebe, WiebeTech / CRU DataPort


BACKGROUND

10 Years ago, forensic investigators just gathered evidence and made copies of it.

I've been involved in the digital forensic marketplace for about 10 years. In that time period, investigative methodologies have changed; case storage requirements have evolved from straightforward, simple, and unsecure to a much higher standard: totally secure; encrypted (at the investigator's option), and absolutely inerasable and unalterable, especially as evidenced is transferred from the investigative agency to the defense.

The basic scenario of forensic drive investigation is well understood:

“Computer evidence is data that is harvested from a computer hard drive and utilized in the process of a crime investigation. Because it is relatively easy to corrupt data stored on a hard drive, forensics experts go to great lengths to secure and protect computers that are seized as part of the investigative process. Extracting the data must take place under highly controlled circumstances, and must be accomplished by law enforcement professionals that are specifically trained in the process.” --- wisegeek.com

It was really pretty simple: ten years ago, it was all about capturing the evidence without altering it, which helped us believe that we had good evidence and that we could put the bad guys away. We had this
assurance of good evidence because we used write blockers, and because we had the ability to hash (or verify) the contents of any image or file.

Our customers have continuously provided us with feedback on what they need to have better evidence. They pointed out that they had simple problems, and they wanted us to solve them:

- To avert the risk of evidence being seen by the wrong people, it had to be encrypted. This would prevent problems if evidence was shipped and lost. It also helped cover the intangibles associated with bad circumstances: What if access to evidence was compromised? What if a hard drive containing evidence was lost? How can an agent feel comfortable with physical shipping of digital evidence through common carriers (IE, FedEx and UPS) from city to city? These are such strong possibilities, especially for larger agencies, that encryption is now a requirement.
- Another possible problem and headache was the alteration of evidence by tampering or by mistake, such as when an evidentiary hard drive was given to opposing counsel. A tangent of this worry was that a tampered drive could bring a cloud of suspicion over a case.

**TODAY’S SITUATION:**

CRU’s encryption and WriteBlocking / WriteProtecting technologies allow forensic investigators to safely store and ship evidence, and also prevent its destruction

We have invested significant effort with our design and rollout of two major new technologies for forensic investigators: Encryption, which is very easy to manage and deploy; and drive protection technologies which did not exist even two years ago. These drive protection techniques allow investigators to share case images with defense counsel in a way which ensures the images are not tampered with or accidently deleted.

Let’s take a quick look back at how a forensic investigator might treat a case 10 years ago:

- The investigator would remove the drive from the inside of an old fashioned ‘tower’ style.
- Using a laptop computer and write blockers, he would then make a copy of the suspect hard drive, producing an image.
- The copy would be removed to a laboratory for further analysis.
- At the lab, forensic software would then analyze the copy for evidence of crimes.
- A copy of the digital evidence would likely be shared with defendant's counsel.

Yes, those were simple times.

While that chain of events is still valid for some circumstances, the nuances of today’s laws and procedures offer better protection for the certainty of the data, using just two changes in technique.

- However the evidentiary image is produced, it is eventually copied to a hard drive in encrypted format. This is done in a completely transparent fashion, using CRU's encryption technology. This prevents all problems associated with transport and possible loss or theft of evidence.
- As the evidence is shared with the defense, it is provided in a storage device that provides absolute protection against alteration. This prevents problems associated with accidental or intentional evidence tampering.
Some investigative groups may require encryption; others may require protection against alteration; some may require both. Let’s briefly discuss encryption for the forensic investigator, and then conclude with a brief discussion of evidentiary write protection.

**Encryption from CRU-DataPort**

CRU-DataPort / WiebeTech has innovated by developing an encryption technology that has absolutely no software dependencies and provides total control over encryption keys. This is achieved by using small hardware keys, each containing a completely unique 256 bit key value. Keys may be thought of as being analogous to hardware door keys – copies are possible, easily created, and easily controlled. Any case may have its own set of keys. Keys may be distributed on a per case basis, or by any other criteria deemed important to case management.

Key creation is performed by an inexpensive key programmer, on inexpensive blank keys. ($280 / $7 respectively). This is what sets CRU’s product apart from all competition: 256 bit encryption keys for every case, easily generated on the spot, easily distributed and easily managed.

These products make digital evidence ‘Secure’, and we incorporate that name in our products: ToughTech Secure Q, and ToughTech Secure mini-Q. The mini-Q product utilizes notebook drives in a pocketable aluminum storage enclosure, all with FIPS 140-2 government strength encryption, while the larger ToughTech Secure provides the same technology with larger enclosures and drive sizes. (And the same technology is available in removable drives.)

**Evidentiary Write Protection**

If an investigator wants to provide digital evidence to the defense, it can be irritating if the drive’s data is accidently modified or erased. CRU has solved this problem by developing a technology which eliminates the anxiety of accidental (or intentional) evidence modification. We have a couple of different flavors of this technology, but all provide the same thing, which is elimination of evidence modification. We call it WriteLock™. We provide a Read-only switch for hard drives. This allows the investigator to create a hard drive of evidence, and then by the flip of a switch prevent any alteration to that data.

In other words, WriteLock enables a Read-only feature similar to CD-ROMs and DVDs without the small media size or speed limitations. Once data is on the drive in the desired way, enable WriteLock to prevent further changes. This technology is perfect for situations where data must be distributed to another party and you want to ensure the data is preserved.

Here is how you use WriteLock:

- Use ToughTech in full Read/Write mode with a standard SATA hard drive for as long as required.
- To engage WriteLock mode, press and hold the WriteLock button while ToughTech powers up.
- ToughTech is now in WriteLock mode and ready to share Read Only data.

Once active, no more writes or erasures will be allowed onto the drive. Files cannot be modified and their locations will not be altered. Tampering or accidental data evidence destruction is not possible.

Enclosures with write-lock are designed to be reusable, but by design the reset mechanism is on the inside of
the enclosure. If you accidentally enable WriteLock before you were finished, you can undo the action.

The reset mechanism is in a hard-to-reach spot to add physical security to this feature. Using tamper-evident tape to seal a ToughTech with WriteLock means that in addition to preventing accidental writes, purposeful actions can be detectable.

**SUMMARY**

Ten years ago, life was easy for forensic investigators – copy drives, analyze drives, search for evidence. Loss of evidence was painful and accidental evidence destruction happened, but there weren’t any really good and inexpensive solutions for these problems.

Today, CRU uniquely offers products which solves these problems, and does so with modest purchase price.

It’s easy to see that encryption solves legal issues with evidence loss. CRU’s product family provides offerings that don’t use software and do allow total control over key creation and distribution. These products are inexpensive, transparent, and easy to administer. We call them ‘Secure’ and they are available in a government certified version.

It’s also easy to see that life is better when evidence can’t be tampered with. We offer our WriteLock product, making it impossible to alter or delete the evidence on a hard drive.

In fact, both of these technologies are available in one storage device – our Secure product line, with WriteLock technologies, is encrypted and can be set to be unalterable. This is the best storage technology available to the forensic investigator.

**Strong, Total Disk, Real Time Hardware Encryption.**

**Lock down your evidence with whole-disk write-protection.**