Can Digital Evidence Endure the Test of Time?

By

Michael Duren, Chet Hosmer

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2002 USA

Syracuse, NY (Aug 6th - 9th)

Can Digital Evidence Endure the Test of Time?

By Mike Duren
Sr. Vice President, WetStone Technologies, Inc.
&
Chet Hosmer
President, WetStone Technologies, Inc.

As we accelerate our move into the digital age, more and more information is becoming available in digital form. The multitude of systems and processes that generate digital information is vast. The availability of technology has not only provided an effective way for this information to be stored, but has encouraged the growth of the information data set for the world. The rate at which digital information is produced today is incomprehensible, as digital pictures, financial information, communications, phone records, transaction logs, books, and movies are all now increasingly being used in digital form.

These changes in technology and culture are having a profound impact on the forensic sciences, as the likelihood that information pertaining to a crime can be found in digital form is high and ever increasing. As a result, the forensic investigator needs state-of-the-art tools and capabilities for extracting, filtering, and analyzing information that might have an impact on a case. And, once this data is found, there is still the task of preserving it with integrity in order to both perform effective and reliable forensic analysis, and for eventual presentation in a court of law. Although we have begun to see advancements in forensics extraction and analysis tools, there is much work to be done to provide technology that can effectively manage and ensure the integrity of digital evidence.

Fortunately the computer science and information security field has defined integrity as it pertains to digital information and has contributed a multitude of methods for protecting the integrity of digital data – at least in the general case. Digital integrity can be defined as, "the property whereby digital data has not been altered in an unauthorized manner since the *time* it was created, transmitted, or stored by an authorized source". [1] Applying and adapting methods from computer science and information security to the domain of digital evidence is complex and involves technology and the expertise and understanding of what it means to prove the integrity of this digital data that happens to be evidence. The question then is what are we actually trying to prove?

Using hashes (operations done to transform one or more fields into a different arrangement) and other cryptographic methodologies, the contents of a piece of digital evidence can be preserved. Mapping this to the definition for integrity above, these mechanisms provide an almost impenetrable means for ensuring that digital information "has not been altered." Cryptographic hashes can be used to protect evidence from tampering for long periods of time. Using algorithms such as SHA-1 or even the new SHA-2, content integrity can be attested to for many years even under distributed brute force attack. Adding digital signatures to the mix provides a strong and very effective means for proving the "who" of preserved digital data. Thus by applying cryptographic hashes and digital signature technology to the problem of evidence preservation the "who" and "what" of digital data can be maintained with very high levels of integrity.

But what about the “when”?

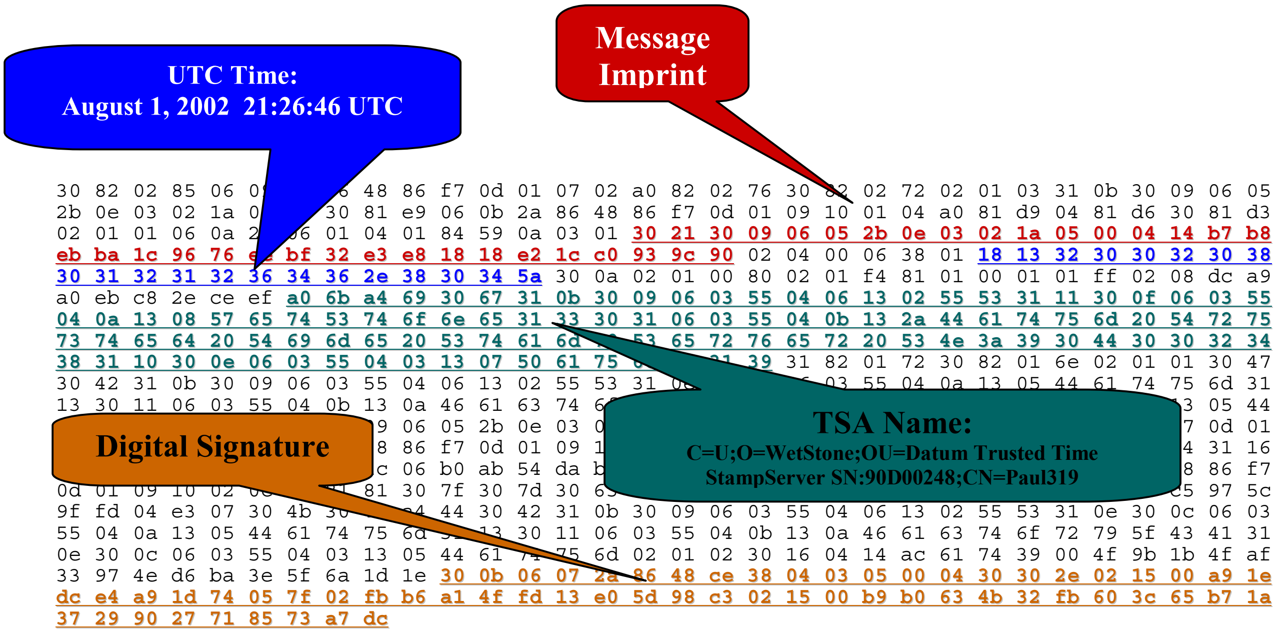
Ensuring the ownership and consistency of digital content using hashes and digital signatures does not guarantee integrity. In addition, application of these mechanisms alone does not meet the forensic requirements for evidence preservation. A key, and often overlooked, component of integrity is *time*. When was the data created? When was it modified? When was data collected as evidence? How long did the collection take place? When was it analyzed? When was the data cataloged? It may seem that these questions would actually be easy to answer, and they are, but being able to verify and prove these answers is another matter altogether. We need to be able to prove the authenticity of the Event Time (ET).

We know that most operating systems and digital storage media allow for the creation date of information to be tracked. In fact, many systems will track creation times, modified times, and last access times of data. However, this information is almost always maintained externally to the actual information itself, and the system clocks that are used by the operating system to provide the time for file creation, modification, and access are unreliable and completely untrustworthy.

Digital Time Stamping

Computer security experts have realized for some time that a major weakness of many security systems is lack of the incorporation of time. Several years ago, the Public Key Infrastructure (pkix) working group of the Internet Engineering Task Force (IETF) embarked on the task of creating a digital time stamping protocol. Their motivation stems from the fact that a key component of a public key certificate is expiration date. In many Public Key Systems (PKS), expiration dates are used to limit the lifetime of public/private key sets and Certificate Revocation Lists (CRLs). Proper enforcement of these expiration dates is critical to the effectiveness of a PKI. The problem is how do you know the time in a certificate or a CRL is trustworthy?

The ITEF pkix working group released RFC 3161 in August of 2001. This Request for Comments (RFC) provides a mechanism to combine the contents of a piece of digital information with a time using a cryptographic hash and a digital signature. The RFC defines an ASN.1 data type called a T*imeStampToken*. [2]


UTC Time:
August 1, 2002 21:26:46 UTC
Message Imprint
TSA Name:
C=U;O=WetStone;OU=Datum Trusted Time StampServer SN:90D00248;CN=Paul319
Digital Signature

```
30 82 02 85 06 0      6 48 86 f7 0d 01 07 02 a0 82 02 76 30 82 02 72 02 01 03 31 0b 30 09 06 05
2b 0e 03 02 1a 0      30 81 e9 06 0b 2a 86 48 86 f7 0d 01 09 10 01 04 a0 81 d9 04 81 d6 30 81 d3
02 01 01 06 0a 2    06 01 04 01 84 59 0a 03 01 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 b7 b8
eb ba 1c 96 76 e   bf 32 e3 e8 18 18 e2 1c c0 93 9c 90 02 04 00 06 38 01 18 13 32 30 30 32 30 38
30 31 32 31 32 36 34 36 2e 38 30 34 5a 30 0a 02 01 00 80 02 01 f4 81 01 00 01 01 ff 02 08 dc a9
a0 eb c8 2e ce ef a0 6b a4 69 30 67 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 11 30 0f 06 03 55
04 0a 13 08 57 65 74 53 74 6f 6e 65 31 33 30 31 06 03 55 04 0b 13 2a 44 61 74 75 6d 20 54 72 75
73 74 65 64 20 54 69 6d 65 20 53 74 61 6d    53 65 72 76 65 72 20 53 4e 3a 39 30 44 30 30 32 34
38 31 10 30 0e 06 03 55 04 03 13 07 50 61 75 6        39 31 82 01 72 30 82 01 6e 02 01 01 30 47
30 42 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 0        03 55 04 0a 13 05 44 61 74 75 6d 31
13 30 11 06 03 55 04 0b 13 0a 46 61 63 74 6                                           3 05 44
                 9 06 05 2b 0e 03 0                                                   7 0d 01
                 8 86 f7 0d 01 09 1                                                   4 31 16
                 c 06 b0 ab 54 da b                                                   8 86 f7
0d 01 09 10 02 0       81 30 7f 30 7d 30 6                                            c5 97 5c
9f fd 04 e3 07 30 4b 30     4 44 30 42 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 0e 30 0c 06 03
55 04 0a 13 05 44 61 74 75 6d       13 30 11 06 03 55 04 0b 13 0a 46 61 63 74 6f 72 79 5f 43 41 31
0e 30 0c 06 03 55 04 03 13 05 44 61 7    75 6d 02 01 02 30 16 04 14 ac 61 74 39 00 4f 9b 1b 4f af
33 97 4e d6 ba 3e 5f 6a 1d 1e 30 0b 06 07 2a 86 48 ce 38 04 03 05 00 04 30 30 2e 02 15 00 a9 1e
dc e4 a9 1d 74 05 7f 02 fb b6 a1 4f fd 13 e0 5d 98 c3 02 15 00 b9 b0 63 4b 32 fb 60 3c 65 b7 1a
37 29 90 27 71 85 73 a7 dc
```

Figure 1. Hex Dump of a Sample Timestamp

The TimeStampToken is a reasonably straightforward ASN.1 data type that is encapsulated into a SignedData type as defined by R. Housley. [3] The hex dump above shows a complete time stamp and then points out a few of the interesting fields.

Once time can be bound to digital information, the next question to ask is, "How can you prove the time of the time stamp was valid when the time stamp was created?" The question really is – do you trust the time in a time stamp? The IETF addressed this issue by defining an entity called a Time Stamp Authority (TSA) and simply stated that the entity must be trusted. There is no defined means for this trust, except to say this should be done through policy.

In order to complete the trust model of digital time stamps, it can be asserted that in order for a time stamp to be trusted, the time in the time stamp must be traceable back to an official source of time. Current practice helps validate this argument as clocks and timepieces (i.e. wrist watches, alarm clocks, and computer system clocks) throughout the world are always being set to the "correct time."

In our daily lives and work habits, however, the concept of showing or proving that the time was correct is never considered or is overlooked. Consider your wristwatch, for example. It's likely that your watch is within several minutes of the officially agreed upon global time or Universal Coordinated Time (UTC). It is also likely that you even know if your watch is a few minutes fast or a few minutes slow. Considering the number of wristwatches in the world, it is astounding to realize how well synchronized all of these watches are. This is in part due to technology that has existed for some time that allows a clock to operate with precision, but it is also due to the cultural evolution that has taken place over centuries as watches and time pieces have become available. Accurate time keeping devices are so prevalent that one assumes that valid or near-valid time can be obtained easily.

On a practical level however, proving the authenticity of time becomes increasingly difficult as the ET we are trying to authenticate moves father into the past. To prove time authenticity, we must prove that the ET was valid; and we must be able to show traceability to official time at that ET. To do this, we will have to define what official time is and then define what it means to be traceable. Then, through the application of hardware systems, software systems, and auditable processes we can create a time stamping system that issues time stamps that are trusted and can be traced back to UTC.

Where does time come from?

From ancient societies to the present day, time has been a function interpreted in many ways. Time essentially is an agreement that allows society to function in an orderly fashion – where all parties are able to easily understand the representation. Several mechanisms for time measurement have been developed and used:

- Earliest calendars were based on the moon because everyone could easily agree on this as a universal measure of time. The Egyptians were the first to understand the solar year and develop a calendar based on the rotation of the earth around the sun. The calendar we use today uses this solar basis to arrive at the number of days in the year.

- In 1582, Pope Gregory XIII introduced his calendar, which is the calendar used today and referred as the Gregorian Calendar.

- In 1967, an international agreement defined the unit of time as the *second,* measured by the decay of Cesium using precision instruments known as atomic clocks.

- In 1972, the Treaty of the Meter (established in 1875) was expanded to include the current time reference known as Coordinated Universal Time (UTC), which replaced Greenwich Mean Time (GMT). More than forty countries running a collection of over two hundred atomic clocks administer UTC. This is where the time reference originates enabling government entities to establish their respective "national time."

UTC time is truly a coordinated time and is not maintained by a single clock. On a regular basis, the UTC contributors all measure their clocks against this reference and then make appropriate adjustments to their own clocks. The process is coordinated in Paris by the International Bureau of Weights and Measures (BIPM). The United States has two organizations that contribute to UTC: the National Institute of Standards and Technology (NIST) and the US Naval Observatory (USNO). These same organizations maintain official time for the US. [4]

Traceability

Traceability has been defined as follows:

> *The property of a result of a measurement or the value of a standard whereby it can be related to stated references, usually national or international standards, through an unbroken chain of comparisons all having stated uncertainties. [5]*

The first step in showing traceability of a time stamp is to show that the clocks used to issue the time stamp are related to and associated with a national or international standard (i.e. NIST or UTC in the case of time). This must be accomplished through an "unbroken chain of comparisons" of that clock showing its offset relative to the reference. In a trusted system, the measurements and resulting audit records must be made and recorded complying with secure protocol procedures. Once you can show traceability of a clock, mapping that into a time stamp in a trustworthy and verifiable fashion is all that is left. In RFC 3161, there is no provision for accomplishing this, however the RFC 3161 approach requires this trust to be implied through the application of policy. Using policy in situations like identity validation might work, but in time keeping where traceability is clearly a requirement and is clearly and well defined, policy is not the correct mechanism.

Traceable Time Stamps

The issues surrounding time and integrity caught the interest of WetStone Technologies several years ago. Since then WetStone has become an expert in the field of Trusted Time Stamping through our work with the IETF/pkix working group, our efforts on our Phase I and II SBIR awards for Trusted Network Time, and our research and engineering contracts with Datum, Inc., where we have advanced the state-of-the-art in secure time stamping, management and distribution protocols. This document represents some of the work that has been performed in researching this problem and defining and building a solution to this problem. Although many different technical approaches to creating traceable time are possible with varying levels of automation, the following describes our approach.

The RFC-3161 time stamp provides an effective means for using digital signatures to bind time and digital content together. To provide traceable time stamps, a time stamping system complying with this protocol must be augmented. Since cryptography is the mechanism whereby time and data are bound together in a trustworthy fashion, it is imperative that the time used as input into the signing process is trusted. This can be accomplished at the timestamp issuing point by combining a timekeeping device and cryptographic keys together on a trusted hardware platform.

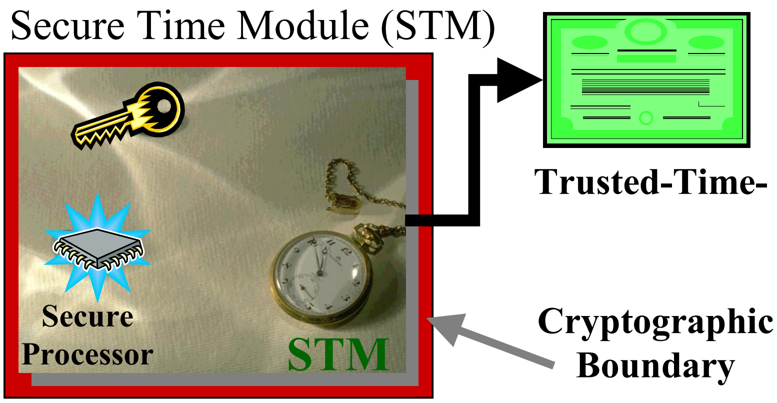


Figure 2. The Secure Time Module

The software on this Secure Time Module (STM) is trusted and runs on the secure processor within the cryptographic boundary of the STM. The hardware module provides a high level of physical security and is certified with NIST at Level 4 of FIPS 140-1. The software adheres to strict requirements for key usage and key management to ensure that all time stamps issued by this device are signed using the appropriate keying material and created using the clock that exists within the cryptographic boundary. This device ensures that the keying material that is used to sign the time stamps is only used to sign time stamps and that the time stamps are only based on this internal clock. This clock, then, must be shown to be traceable to UTC through the "unbroken chain of comparisons" that the traceability definition states.

Traceability of timestamps issued by an STM can be facilitated through a Trusted Third Party (TTP), called a Root Time Authority (RTA), which attests to the time validity of the STM's clock. The RTA plays a role that is similar to that of a Certificate Authority (CA) except that the RTA attests to time validity rather than the validity of one's identity. Using a similar model to an X.509 identity certificate, the RTA issues X.509 Attribute Certificates to an STM based on secure, authenticated measurements of the STM's clock

On a periodic basis (defined by policy taking into consideration stated uncertainties), the RTA securely measures the offset of the remote STM and then produces an Attribute Certificate stating the results of this measurement. The STM then, uses this information to validate its continued operation and to make any clock updates.

In order to issue timestamps, an STM must have two certificates: an identity certificate and a Time Attribute Certificate (TAC). Time stamps that are issued by the STM are based on the RFC 3161 specification and are subsequently a SignedData [3] data type. It is required that the time stamps issued by the STM specify the TAC under which they are operating. Since the time stamp is a SignedData [3] data type and the TAC is a standard X.509 Attribute Certificate, the TAC can be included in the stamp in accordance with standard practice using the Certificates field and the ESSCertID signed attribute. [3,6]

Showing that a clock is traceable back to an RTA does not complete the traceability requirement for "chain of measurements" back to a reference, however. The RTA is responsible for ensuring its auditing clocks are, in turn, traceable to UTC. At Sovereign Time™, an RTA operated by WetStone Technologies, inputs are collected and recorded from multiple National Measurement Institutes to guarantee that traceability to UTC is maintained. In addition, several different mechanisms are used to communicate timing information between Sovereign Time and the National Measurement Institutes (NMIs). Both secure and publicly available, non-secure mechanisms are deployed. Since Sovereign Time acts as a Trusted Third Party, this RTA publishes a set of practices and procedure that it adheres to in its operation. Compliance with these practices is ensured through both internal and external audits of these processes, and of the Sovereign Time records.

Conclusion

It is imperative that we continue to examine the approach that we take to maintain integrity of data with regards to time. In forensics, this issue is critical as the timing of events can be paramount to the results of a case. Protecting digital evidence with time stamps is one application that will directly benefit the forensic community. In addition, the forensics investigator must be aware of the issues with time keeping and the current practices whereby time stamps are maintained within systems. As corporate America begins to see the importance of strong auditing & authentication processes to protect their own interests, the current practices for time integrity will come under closer scrutiny, and stronger forms of time stamping will begin to emerge as the standard business practice.

Further Research

The work that has been performed thus far in digital time stamping has been very successful and productive and has resulted in technology that is being deployed today. However, additional work needs to be performed in two areas: time measurement uncertainty and trusted timekeeping hardware. The uncertainty of time measurements has been studied for some time. The work that David Mills has performed over the years is invaluable in the processes of time synchronization over a network. However, the addition of trust to this process brings up new questions regarding the definition of uncertainty, particularly as it pertains to audits and showing traceability at some later point in time.

The question of time accuracy and precision is often raised when time stamping is discussed. In most cases, high levels of precision are not required; most applications can work well with clocks that are within a few hundred milliseconds or even a second of a reference clock. Accuracy, on the other hand, is an issue. If your need is to have faith that a clock will maintain some level of precision (again even 1 second or more), you must trust that your time keeping hardware can keep that level of precision. Additional research is needed to consider these issues. Clocks for time stamping must also be secure. Custom research into time keeping technology and current tamper resistant techniques could result in dramatic discoveries that would benefit both commercial and government interests.

Bibliography

[1] Vanstone Scott A., Oorschot Paul C. van, Menezes, Alfred J. (1997) Handbook of Applied Cryptography, CRC Press

[2] C. Adams, P. Cain, D. Pinkas, R. Zuccherato, “Internet X.509 Public Key Infrastructure,” RFC 3161, August 2001

[3] R. Housley, "Cryptographic Message Syntax", RFC 2630, June 1999.

[4] NIST, “World Time Scales,” http://physics.nist.gov/GenInt/Time/world.html

[5] Lombardi, Michael A., “Traceability in Time and Frequency,” NIST Time and Frequency Division Publication

[6] P. Hoffman, “Enhance Security Services for S/MIME,” RFC 2634, June 1999