5

Digital Evidence

Designing a Trusted Third Party Service for Securing E-vidence

Nicklas Lundblad
Swedish Research Institute for Information Technology

Abstract: The evolution of an information society is accompanied by the growth of digital materials and transactions. It is in some cases necessary to use these digital materials and transactions as evidence in legal processes. The value of digital evidence is, however, hard to determine. In this paper some basic requirements and suggestions for a trusted third party model that can be used to secure digital evidence is given. A first sketch of a general typology of digital evidence is offered and discussed.

1. INTRODUCTION

1.1 The nature and growth of digital evidence

There is no single definition of what constitutes digital evidence, and it might be problematic to try to define, crisply, what is and what isn't digital evidence. If an e-mail has been printed out, for example, it might be considered to be a kind of digital evidence, since it originated from a digital original.

There are, however, some attempts at defining digital evidence. One such definition (SWGDE 1999) is interesting and might prove valuable: "*Digital Evidence:* Information of probative value stored or transmitted in digital form". It is far to early to say what different new technologies might change the evidentiary landscape.

It suffices to say that digital evidence is something that is used as evidence in a court of law and that is avaliable primarily in digital format. By enumerating different kinds of digital evidence the definition will be made clearer later on.

There are several reasons to examine digital evidence form a legal standpoint. Some of the most important are:

- Digital evidence is easy to manipulate. The integrity of the material being used as evidence is open to different forms of attack. Files, screen dumps, documents and other digital materials are easy to fabricate or modify.
- Digital evidence is more anonymous than regular evidence. An e-mail, or a web page, is less attached to a person than is a physical letter or a statement in some other kind. The change of medium, from paper to computer, increases the number of possible senders or originators.
- Digital evidence is highly technological. The form and content are interwoven and must be considered as a whole in deciding the evidentiary value of the material in question. Consider the fact that digital evidence often will be encrypted or hidden. (Denning and Baugh 2000)
- Digital evidence is hard to submit to court. The actual processes of submitting the digital evidence is extremely open to attack, and the general level of knowledge in court when it comes to these kinds of evidence is low.

The legal system is not used to handling this kind of evidence. There are, however, good reasons to assume that digital evidence will become a more and more frequent means of proving facts in cases pertaining to electronic commerce. This implies that we have to learn more about digital evidence and find ways of securing digital evidence in satisfactory ways.

1.2 Digital evidence –some introductory remarks

There exists – today – commercial firms that work with *existing* digital evidence and offer services in the area. One such firm, Digital Evidence, offers pre-trial assistance and evidence acquisition (Digital Evidence 2001):

> At Digital Evidence Inc., we are experts in a wide variety of computer investigation techniques. We can assist you by examining a large assortment of computer platforms and media to locate information which is important to your case.

The services offered by Digital Evidence are services tailored to help the police, lawyers or other actors after the fact. In contrast to this we could discuss how to pre-emptively design systems so that they capture evidence during the transaction. The perspectives differ slighly from each other. In the first case the aim is to evaluate and restore digital material that can be used in court. In the second case the objective is to create processes and systems such that evidence or material of evidentiary value (potential evidentiary value) are created when using the system. The TTP-services drawn up in this paper are pre-emptive in the sense that they try to capture evidence in new and safe ways. This suggests two different categories of digital evidence: constructed and recovered.

Digital evidence is going to become more complex. Most of what we consider today is static evidence – pictures, email et cetera – but it is far from unlikely that

we will need to secure processes or sessions in the future. This new kind of dynamic evidence will require much more from the securing party. This also suggests two different categories: time stamp evidence (which would be evidence gathered at a certain point in time) and session evidence (which would be evidence that is arranged into sequences and timelines).

The field can be divided into an empirical perspective and a constructive perspective. The first perspective studies how we can handle what we find today as digital evidence, and deals with complicated issues on how to decrypt data that has been encrypted to hide evidence, how to intercept email, filter data et cetera. (Eoghan 2000) The second deals with designing systems that generate essentially new kinds or stronger kinds of digital evidence. This paper mainly deals with the second perspective.

This paper works with what is a distinctly Swedish legal perspective. In Sweden evidence law is not designed to be statutory, i.e. formal in any way. Anything might be entered as evidence and the court then has to decide what the value of the evidence presented is. We will thus speak about evidentiary value as an analogue variable. In some systems the opposite will hold true; evidence laws will be designed to admit only certain kinds of pre-defined categories of evidence. Practice will look different in those legal systems.

2. TYPES OF DIGITAL EVIDENCE

2.1 Introduction

The process of securing digital evidence can almost always be referred to as a form of *printing,* where the document is put through a process where it is time stamped and secured/signed in it's present form. Secure printing is a main theme of the service this paper describes. We often will refer to signing and encrypting documents without considering the method of doing so. This does not mean that the form of signing and encryption is, in itself, unimportant – quite the contrary – but it falls besides the main theme of the paper. The TTP-service/services described in this paper will presumably coexist with an advanced public key infrastructure.

Generally, however, there are some qualities that all systems that collect or construct digital evidence must share. These systems must be trusted, in the sense that their technical architecture and design must comply with accepted security standards. Pfleeger (1997) and Camp (2000) discuss in greater detail what this means for systems handling any kind of material that needs to be trusted. It should be noted that these requirements also apply to systems securing digital evidence.

2.2 Web pages

Regular web pages are, of course, the subjects of legal examination quite often. The reasons are many: copied text, unlawful links, illegal pictures, or content that in any other way violates a law, contract or other legal enforceable rules might necessitate an exmination. If the examiner decides that the material is in any way unlawful it might be necessary to submit web pages as evidence.

Web pages are, by themselves, hardly secure. It is easy to alter the content of a web page and any judge that is given a web page should reasonably ask him or herself what the value of that piece of digital evidence is. If the submitting party can then not show that the evidence was produced in a secure and trusted way the evidentiary value assigned to the web page should be close to zero.

How can web pages then be secured? One possible way would be to develop a browser plugin that stores the web page and encrypts it with a timestamp. Such a program might also save the page in multiple places and media, at once, ensuring redundancy. It would work as a sort of camera, taking 'pictures' of the web and then storing them in a way as to ensure their security. The material stored could, among other media, be printed out in a relatively safe format such as the portable document format (pdf), to ensure that it is not tampered with.

The repository can easily be distributed and the browser can be one or more – depending on the level of security desired. The page is then signed with a collection of data pertaining to the page, it's IP-number, time viewed, author metadata et cetera.

There will have to be a certain, safe storage solution behind the entire concept. This goes for all the following types of digital evidence and is, in itself, a problem of some magnitude. It is important to note that if the material, once secured, is not kept safe, the evidentiary value will be heavily reduced.

2.3 Digital documents

In the growing number of cases where digital documents are the only documents that exist in a certain case it is necessary to submit them as evidence. Here we can deal with everything from carefully formatted XML-documents to Microsoft Word documents, or even simple ASCII text messages (S2ML 2001).

Again the process of printing these (in the form of screen dumps or any other form) to a safe format, like pdf, with some amendment, time-stamps and other additions might serve the purpose of generating medium-safe evidence.

2.4 E-mail

That e-mail can be used as evidence in court is something that everyone familiar with the Microsoft Trial is aware of. A company's email is in fact often a liability.

The evidential value of e-mail, however, should really be considered small to non-existent if the company itself submits it. There are however models that remedy this.

The methods available to secure email are many. Three seem especially important:

- The BCC-plugin model (BCC here stands for Blind Carbon Copy, and is a mode of sending e-mail).
- The Dual SMTP model
- The Dual POP/IMAP model

The first two secures mail that has been sent. The third secures mail that arrives to a certain address.

The BCC-plug in model is a simple add-on program that allows the user to send a copy of all outgoing mail to a secure storage solution. In this way a record of all sent mail is drawn up, and questions concerning what was and was not said can authoratively be laid to rest.

This plug-in might easily be configured to allow the user to choose what mail is copied, or it can be locked, so that all e-mail is copied. The configuration will of course affect the value of the evidence.

The Dual SMTP solution works in much the same way, but it does not utilise the secure link between TTP and Sender that is assumed to exist in the BCC Plug In case. The Dual POP/IMAP solution is likewise merely a device that copies all incoming mail to a locked account for future reference. This, also, can be accomplished at both server and client level. The choice will of course affect the security achieved.

2.5 Log files

Another important form of evidence is a log file. These files might very well be used to prove unlawful computer break-ins or hacking crimes. Log Ffiles can be used to construct evidence in several different ways. The deposition of log files is one way, and then the log file basically works as any kind of digital document. A stronger form of evidence is generated if the log file is outsourced to a TTP, and the logs actually handled by the TTP.

2.6 Digital payments and receipts

In a world where the number of digital payments and receipts grow rapidly there is a need for a way to create evidential value for these new forms of payment. Everything from e-cash to electronic invoices require careful thinking when it comes to how we strengthen their evidentiary values.

The existing secure standards in this field are interesting subjects of study in this field.(Westland and Clark 2000).

2.7 Procurement processes

Aside from the pure static digital phenomena described above – where they all have in common that they are *files* – we might also see the need for a new kind of evidence: evidence of a recorded process, such as a procurement process. The reasons may be varying: we might want to ensure that a public procurement has been performed according to legal protocol, or we might be anxious to see that all bids were opened at the same time, or, indeed, opened at all. We might not settle for data about single files here, but instead require recordings of processes. It is interesting to note that these recordings will then be log files and subsequently handled as such. Public procurement is one especially interesting area here, and the issue is undergoing study in Sweden.

3. A SKETCH OF A DIGITAL EVIDENCE STANDARD

3.1 Standard architecture in general

This first sketch of a standard architecture is made up of three layers: legal, organisational and technological. The thought behind this division is quite simple. It is necessary to understand that none of these levels alone is enough to ensure good evidence. Legal formalities might be useless against sloppy technology or an unsecured organisation, and vice versa. A service designed to secure evidence must consist of careful design on all three levels.

3.1.1 Legal Layer

The legal layer consists of rules of evidence, the structure of evidence and the lawful capture of evidence. There are several different factors that have to be taken into account here:

- What counts as evidence? Are there formal requirements or does the system allow for a free test of evidence?
- What, usually, is interesting in the evidence? That is, what does the evidence consist of? How are these parts digitally rendered?
- Are there formal requirements on the collection of evidence? What if it has been collected unlawfully?

These, and many other questions forces the service provider to establish a legal checklist that he must use in all cases where he collects evidence. Such a checklist is a necessary tool in a service that aims to deliver high value digital evidence. The checklist should also be anchored in courts and responsible authorities, and be made

public, preferrably by displaying it on the web site. The issue of public display is important in that it gurantees that flaws in the checklist are illuminated by the public eye.

3.1.2 Organisational

Firstly it should be mentioned that the organisational layer differs heavily in the two cases where the TTP is a private actor, and where the TTP is a public actor. Here we will primarily deal with the first case. Should public TTPs be established it is to be expected that they will be provided with due instructions from the constituting actors.

The organisational level is more complicated than the legal. What is needed is the equivalence of what is called Certification Practice Statements in regard to the issuing of digital certificates. An *Evidence Securing Statement* (ESS) is required. This should describe, amongst other things:

- How a request for the securing of evidence is received and acted upon
- How evidence is secured, by whom and by what means
- How evidence is stored and redundancy in storage ensured
- What aspects of evidence are ensured and in what order
- Liability limits
- Education and selection of evidence securing staff

The ESS should also be made public and used to create a widespread trust in the service. It is furthermore important to open these processes for review, certainly by allowing lawyers to request review into log files and technology solutions under a set of given circumstances.

The organisational layer also encompasses the different forms of evidence a securing party is ready to offer, which in essence determine the service structure. There are many different forms of evidence, and it should be obvious that the business model of the trusted third party should be constructed to offer the highest possible degree of flexibility. Several variations are possible:

- **Time.** It should be possible to secure evidence for a limited time, for, say two weeks, and then have it erased. It should also be possible to secure evidence a number of times (i.e. every week at different hours) in a sequence, to show that certain content on a web site was posted for a certain time.
- **Security level.** It should be possible to secure evidence with different levels of security. The processes and methods used can vary, for example, and the number of samplings can vary as well. The evidence can be collected in real time with legal counsel present.
- **Redundancy.** This is in part also a matter of security, but if the service secures screen dumps from a hundred different servers or simply from one, this matters. The level of redundancy in the system is also something that effects the strength of the evidence collected.

– **Media.** It is of course also possible to print the material on paper, burn CDs and or save the material in digital format only.

These issues, the construction of the business model of the service, should also be openly published, since they affect the evidentiary value.

3.1.3 Technological

The technological layer requires a careful design of an *Evidence Securing Infrastructure* (ESI) – an infrastructure that technologically allows for the safest and most efficient securing of evidence possible.

Elements in this infrastructure and process should be:

– **A sound amount of redundancy in collecting evidence.** It should not be possible to fool the system by showing a certain page for a certain IP-number, for example. The system should use distributed securing servers, so that the securing process is untraceable as such. This is an important requirement. The securing of evidence should normally not be discernable from regular use.
– **Timestamp technologies that are tamper proof.** Software needs to be developed that signs screen dumps or e-mail immediately in a way that no one should be able to change.
– **Safe storage utilities.** The storage and saving of material should be a) distributed and b) time resistant. Safe server parks and other means might be necessary to use in certain cases.
– **Encryption technologies.** To ensure that someone who does not have access rights does not access evidence, all collected evidence should be stored in encrypted form.
– **Sampling technology.** Technology that can vary collection point in the network (i.e. from what IP-number the evidence is collected, or what server) and that is capable of securing evidence at random times.

These technologies offer a good beginning of the technological layer's construction, but this needs to be tested and prototyped.

3.2 Two Cases

The best way to illustrate what a evidence-securing TTP service would do is to offer to sample cases. The cases offered below are intentionally chosen to show normal and non-spectacular problem situations where digital evidence might be useful.

3.2.1 Intellectual property issues

The owner of digitalpets.com notices that his competitor, analoguepets.com seems to have copied digitalpets.com web site layout and a few useful search

functions that digitalpets.com has developed. He seeks legal advice and the lawyer submits a request for the securing of three kinds of digital evidence: a screen dump, a saved web page and a session in the search functions for both sites.

The submission reaches the Trusted Third Party that immediately registers it in it's log file. Then two certified evidence clerks starts to work. The screen dump is secured by the use of *Secure Screen Dump* – a software that timestamps the screen dump by pinging a number of atomic clocks on the Internet, and then encrypts the file and a signature made of the file for storage in the Trusted Third Party's secure server park. A web page is saved the same way, through another tool, and then a session is recorded in the search tool, and safely stored.

The evidence receipt is sent to the legal counsel, who then puts together a letter to the would-be offender and states that digital evidence has been secured by a trusted third party, and that they would like to see him immediately desist in using the layout and search tools used by digitalpets.com.

If the matter goes to court the evidence is collected from the third party, and then submitted in accordance with due process.

3.2.2 Digital contracts

The earlier example was quite simple, and the evidence easily collected. In this case we will describe a more complex situation, where a contract is negotiated and signed, and subsequently deposited with the Trusted Third Party. Company A starts negotiations with Company B on a large contract. To ensure that all evidence is secured they sign an initial agreement in which they specify that all negotiations will take place on a trusted third party platform and that they will not consider themselves legal obligated until a contract has been deposited with aforementioned trusted third party.

The negotiations consist of carefully phrased email that is sent via a special mail server that copies, and timestamps all communications via the trusted third party. The material is then gathered and saved. When the draft of a contract becomes finalised both parties electronically sign it and deposit it with the trusted third party. The contract's evidentiary value is thus strengthened immensely compared to if it only had been accessible to the parties involved. The TTP then also signs the contracts and submits it to safe storage. It might be necessary to make this storage blind – to ensure that the companies suffer no extra security exposure in storing the information with the TTP.

4. POTENTIAL PROBLEMS

4.1 Legal

In the legal layer we find many of the hardest problems we need to solve. In this subsection we will discuss issues of intellectual property rights and privacy.

4.1.1 Intellectual property rights

Consider the first case offered above. What if the party being sued replies with a counter claim stating that the screen dump a web page copying indeed constitutes illegal copying and an infringement of his/her intellectual property rights? How should such a claim be met?

It could be argued that evidence never is subject to counter claims like this, but if the trusted third party is a private actor or organisation the problem suddenly becomes more complex. We then have to take into account the various IPR laws and try to see if there are exceptions under which securing evidence might be subsumed.

This is a real problem, even if it seems simple enough, and with IPR-laws being revised we need to think about instances like the sampling of digital evidence where a form of fair use exemption would be in order.

4.1.2 Privacy

One particularly interesting problem – in the European Union at least – is how the collection and securing of evidence is viewed under the European Data Protection Directive.[13] The provisions of this directive put heavy demands on the collection of evidence that contains personal data. The articles and rules state quite clearly that several prerequisites must be fulfilled. Not only must such a collection comply with the basic requirements in article 6 of the directive, he or she must also fulfill the consentoriented criteria offered in article 7. Both articles are too long to quote here.

Consider both cases above: the negotiation material, as well as the screen dumps might contain personal data (names, telephone numbers, e-mail addresses et cetera). How should then a claim to the effect that the collection of such evidence is illegal under the data protection directive be handled?

There is a provision in the directive that might be applicable here, in article 7 p f). The balancing of legitimate interests of the individual and the third party. It might be argued here that the interest of securing evidence supersedes the interest of the

[13] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Hereinafter: the data protection directive.

individual. The problem, however, is not a trivial one. Indeed: if the directive would be interpreted literally many of the services described would not be possible. Many of the provisions in both article 6 and 7 put severe limitations on the collection of evidence that contains personal data.

4.1.3 Liability

The chief problem for an actor deciding to act as a trusted third party is, of course, liability. Given that all other issues resolves well, this one is still enough to dissuade a private organisation from taking the role of trusted third party, and to secure evidence.

We see a growing number of phenomena today where liability might very well slow the development of much needed services. This goes for the traditional certificate authority role as well as the more differentiated trusted third party role. This must be solved. In part the problem can be solved with insurance solutions, but it is also important to look at disclaimers and contractual limitations of liability.

Today, however, the problem remains largely unsolved.

4.1.4 Company secrets

When acting as a trusted third party an organisation will run the risk of storing and accessing what must be regarded as company secrets. It is therefore necessary to develop blind systems, where the TTP can store and secure evidence without having access to it, or without knowing what the evidence consists of. Such blind solutions might take some time to develop, but the technology is available today (see Brands, 2000).

4.2 Organisational

There are also organisational problems that need to be solved. These often deal with business issues that remain unsolved, since the TTP-market in all essentials is new.[14]

4.2.1 Bankruptcy

If the TTP is a private organisation or an actor, he or she will risk bankruptcy. The issue will then arise of what to do with the data/evidence collected. This issue must be resolved by creating a back-up plan for these kinds of actors in case of bankruptcy, but they can also be solved by choosing suitable actors – actors with

[14] Even if it is possible to argue that it bears a strong resemblance to earlier services in the field of trust that we have seen such as *Notarius Publicus.*

staying power and well-established trust services, such as the Chambers of Commerce or certain bank federations.

4.2.2 Sales of data

Another issue that needs to be resolved is the ownership of the evidence collected. This is a relatively small issue, but it deserves to be mentioned. The matter could probably be solved by contractual provisions.

4.3 Technological

Among the technological problems that must be solved we find the usual important issues of security, integrity, non-repudiation, redundancy et cetera. It is worth mentioning however that the technological problems are the least pressing in the design of an evidence-securing service.

4.3.1 System weaknesses

One issue that however deserves mentioning is the possible existence of system weaknesses. If it turns out that the evidence provided by the TTP is vulnerable to a certain attack, all previous evidence must and can be called into question. This is a nightmare eventuality for the designers of services like this, but it must be taken into consideration.

5. FUTURE DEVELOPMENTS

A service of the kind described here is quite simple and still also quite useful. It is interesting to reflect on the evolution of this kind of service, and how the evidence situation at large might develop. In this section three different scenarios will be considered.

5.1 Secure zones

One likely and interesting scenario features what we might call secure zones. Instead of securing single pieces of evidence, we might visualise systems that record and monitor all activity in certain well-defined logical subnets. These subnets – secure zones – might then be regarded as evidence safe, i.e. that all that happens can be introduced as evidence in court.

The development of business webs and secure extranets offer us prototypes of how this might look in the future. There is no question: we need secure sub nets. The question is how secure they can become.

5.2 Evidence markup languages and automatic dispute resolution

Another interesting scenario is one where XML and other mark-up languages might be used to generate evidence templates that can be used to standardise on-line evidence. These templates might then be used in highly automatic dispute resolution systems, where claims and counter claims can be automatically evaluated. Such a dispute resolution might be binding or merely used to indicate where a true process would end, but it would still be interesting to use and see.

6. REFERENCES

Brands, Stefan A Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy (MIT Press 2000)

Camp, L Jean Trust and Risk in Internet Commerce (MIT Press 2000)

Denning, Dorothy E and Baugh, William E "Hiding Crimes in Cyberspace" in Cybercrime: Law Enforcement, Security and Surveillance in the Information Age (Routledge: New York 2000)

Digital Evidence web site http://www.digital-evidence.com [2001-02-13]

Digital Evidence: Standards and Principles Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE) October 1999 in Forensic Science Communications April 2000 vol 2 number 2, http://zeraw.nbase.com/programs/lab/fsc/backissu/april2000/swgde.htm [2001-02-13]

Eoghan, Casey Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Academic Press, 2000)

Pfleeger, Carles P. Security in Computing 2nd ed (Prentice Hall 1997)

Security Services Markup Language http://www.s2ml.org/index.cfm [2001-02-13]

Stephenson, Peter Investigating Computer-Related Crime (CRC Press 1999)

Westland, J. Christopher and Clark, Theodore H.K. Global Electronic Commerce: Theory and Case Studies (MIT Press 2000)