

Digital forensics research

SVEIN YNGVAR WILLASSEN AND STIG FRODE MJØLSNES



Svein Yngvar Willassen is PhD student at the Norwegian University of Technology and Science, Trondheim, Norway



Stig Frode Mjølunes is Professor at the Norwegian University of Technology and Science, Trondheim, Norway

Digital Forensics is the field of analysing and evaluating digital data as evidence. Time stamps stored on digital media play a crucial role in evidence analysis, but digital time stamps may not be correct for various reasons. A more scientific understanding of digital time stamps in digital forensics is therefore needed.

In this paper we present the emerging field of digital forensics, and take the first steps toward a methodology of digital time stamps in an evidential context.

1 Digital forensics

Digital forensics can be defined as the practice of scientifically derived and proven technical methods and tools toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of *after-the-fact* digital information derived from digital sources for the purpose of facilitating or furthering the reconstruction of events as forensic evidence.

Examples of digital sources include VLSI chips, hard disks, mobile phones, digital cameras, computers, printers, copiers, backup tape, CDs, DVDs and network routers, as well as software and communication protocols. Digital forensics must be based on the science of ICT within the requirements and interpretation of law [1]. Data can be recovered even if deleted from a user's point of view. Techniques for recovery of deleted information are therefore central to digital forensics [9]. Digitally stored information can easily be manipulated, so great care has to be taken when handling digital evidence, in order to be able to prove the origin of the information.

The practice of digital forensics is new. When computers became common in homes and businesses, the police more and more often came across computers which contained forensic evidence. Thus, police organizations saw the need of establishing special police units to handle electronic evidence. USA was first when the FBI established the Computer Analysis and Response Team (CART) in 1984. Later, a similar unit was established at Scotland Yard in UK.

The need for standardization and dissemination of knowledge in this area was first recognized during the 1990s. Meetings between police units in different countries were arranged in 1991, 1993 and 1995. As a result, several international organisations for standardisation of computer forensic techniques were established [5]. Interpol European Working Party on Information Technology Crime [3], a workgroup within Interpol, was established in 1993. The Interna-

tional Organisation on Computer Evidence was established in 1995. This organisation is a meeting place for computer forensic units in law enforcement all over the world, and work with standardization of digital evidence analysis.

In Norway, a process was started in 1993 that led to the establishment of a "computer crime team" at ØKOKRIM in 1995 [4]. This team had from the start a responsibility for computer forensics and investigation of computer crime cases. The computer crime team became the National Computer Crime Center (PDS) in 2002, taking on the national responsibility for digital forensics at the Norwegian Police. The national Police Academy has since 1996 given educational courses in digital forensics in cooperation with ØKOKRIM. Therefore, several local police districts have a certain capability for performing digital forensics. Still, many cases are solved with assistance from the National Computer Crime Center.

At the commercial side, the company Ibas AS has performed computer forensic analysis on behalf of businesses and governmental institutions since the late 1990s. From 2001, digital forensics was organized as a business area within Ibas. Ibas now exports this service from Norway to most countries in Europe.

The scientific ICT community has taken an interest in the field of digital forensics only recently. As a result, digital forensics has been and still is ad-hoc practice-driven procedures which may be lacking scientific foundation. In response to very apparent public needs, direct requests from the government authorities, and realizing that incident investigation is a vital part of efficient protection against computer crime, the ICT security community has taken interest in providing a scientific approach to digital forensics. In 1998 the Scientific Work Group on Digital Evidence (SWGDE) was established in USA. The research communities established the *International Journal on Digital Evidence* in 2002.

Digital forensics practice is currently performed in three stages:

- *Securing of evidence.* Securing involves the process of producing exact copies of the seized digital medium, so-called imaging. The copies must be exact, and cryptographic hashing techniques are used to be able to prove that the copy contains the exact same information as the original. This phase is very important to ensure that the evidence is admissible in court [2].
- *Analysis of evidence.* Analysis involves the enumeration of evidence items in the data set. This process may be difficult as the data set is usually very large and it is unknown which pieces of information may have value as evidence.
- *Evaluation.* Evaluation is the process of assessing what implications the enumerated evidence items have in the investigation. What does the evidence tell us about the use of the computer and the actions of the user? As the goal of any investigation is to provide evidence of a chain of events, the evaluation phase is very important.

Up till now, most scientific effort has been put into the problems of the first phase. As a result, sound methods exist today for image copying and other securing of digital evidence, including scientifically evaluated software packages for forensic imaging [7, 8]. However, little effort has been spent on the analysis and evaluation phases yet. These are going to be the important areas for digital forensics research in the near future.

2 The challenge of time stamps

The Department of Telematics at NTNU has established the research project “TID – Time stamps in Digital Forensics”, with funding from the Norwegian Research Council. The project is an important part of ongoing research within Norwegian digital forensics, and within NTNU Research Programme for Information Security it will be carried out in cooperation with internationally renowned research institutions within digital forensics.

2.1 Problem definition

A digital time stamp is a date/time stored or communicated by an electronic medium. The digital time stamp can take many different formats and resolutions. Computer systems store time stamps in many different ways and according to various rules. In most file systems, time stamps are stored whenever a file is created, written or accessed. Most computer systems also have logging functions which log activities on

the computer with time stamps. There may also be different file formats which include time stamps. These may be operating system specific formats such as executables and configuration files. It may also be application specific formats, such as documents and spreadsheets. Time stamps are also stored on other electronic media, such as mobile phones, PDAs and flash memories. Protocol messages and packets include time stamp fields that are important to the functionality and security of networks and networked systems.

Digital time stamps are very important within digital forensics because establishing the correct sequence of events and time spans are a fundamental method to activity reconstruction during case investigation and in court. Knowledge of when an action was committed is often of vital importance as evidence. With credible digital time stamps, an investigator can determine when executables were run, or when documents were written, or when emails were sent.

Based on time stamps carried by a digital medium, the investigator can construct a *timeline of activities*. The ability to prove not only what has happened, but also when it happened is crucial in the evaluation of digital evidence. A timeline is necessary to tie the chain of events that can be found on a digital medium to the chain of events that has taken place in the real world. In most cases, it is also necessary to tie the chain of events in a digital source to a specific user [10].

Time stamps exist in many formats. Although international standards for date and time representations exist [15, 17], the implementers of common file systems, applications and devices have mostly chosen not to use the standardized formats. We all remember the Y2K problem of format, representation and use.

The information security community has traditionally met the challenge of time stamp analysis by asserting the need for network base synchronisation of time sources. [15, 16] This is a valid solution if the computer at any time is in a controlled environment. In digital forensics however, it is usually the case that the digital source was not in a controlled environment. An investigator must question what previous actions have been done to the time source of a computer or digital device.

Forensic examiners who wish to use time stamps as evidence are experiencing the following deficits:

- There is little systematic documentation on time stamp formats available.

- There is a lack of documentation of the use of time stamps and time zones in systems.
- Reference systems including different calendars, leap years and leap seconds vary.
- It is unclear how time stamps in file systems are handled at different operations on different operating systems.

In addition the investigator will encounter more fundamental problems regarding the use of digital time stamps as evidence. Computer programs can manipulate most time stamps. Time stamps are related to a time source, often a clock or a network service. Clocks can be unreliable, not working, or not synchronized.

These obstacles present great challenges to computer forensic investigators. The reason is the nature of investigations digital forensics is a part of. If the timeline cannot be established beyond reasonable doubt, the evidence may be worthless since it cannot be established who was using the computer at a particular time. In several recent court cases, it has been alleged that the timeline cannot be established *beyond reasonable doubt*, since the time source may be manipulated or time stamps may be manipulated by computer programs. Such allegations may create reasonable doubt on computer usage and may lead to incorrect acquittals or convictions.

2.2 Properties of time and clocks

Starting our examination of time stamps in an evidential context, it is important to understand some properties of time. We define here *Real Time* as an abstract concept of an ideal clock always representing the real and correct time. Such a clock does not exist, but close approximations do, and these serve as the original time source for most other clocks.

Real Time can be viewed as a mathematical relation on the set of points of time with two important properties. The first, *anti-symmetric*, implies that it is impossible from any given point in time to “go back” to a previous point in time. This is a fundamental property that is consistent with how most people perceive time. Although clocks can be adjusted back and forth, the underlying concept of Real Time is a constant directed current, where time travel backwards is impossible. The other important property is the property of *transitivity*. Transitivity implies that any given point B in time, that comes after another point A in time, must also come after all other points that A comes after. With the definition of Real Time as a transitive relation, we may have all time points placed somewhere on a linear time axis, and therefore have a

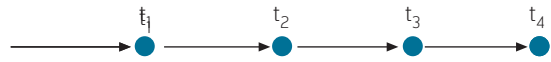


Figure 1 Real time considered as a mathematical relation with the properties of reflexivity, anti-symmetry and transitivity

relation to all other time points as either *happened-before* or *happened-after*. If a point in time is concurrent with another point in time, it is the same point. Events however, may be concurrent, since they may stretch over a period of time.

A Clock is a device that can be defined to be a device that gives an approximation of Real Time. A clock can be adjusted at any time, by actions of the user or by failure. For convenience, we do not consider the case where a clock stops working. For our purposes, we define this as a situation with continuous adjustments of a clock.

In practice, most clocks are periodically synchronized with other clocks. This adjustment can be manual or automatic, such as when using time adjustment protocols. In most cases, clocks are adjusted from a time source that represents a closer approximation to Real Time than the clock that is being adjusted. In addition, the adjustment in itself also introduces an error in most cases. This is in turn true when considering the time source, and so on all the way to the root. Taking this into account, a way to view a clock is therefore to see it as the sum of approximations to Real Time, where each has been made in the path from the clock back to the root time source. [18] Provided that a clock is adjusted often enough to a valid source, and the error introduced at adjustment is

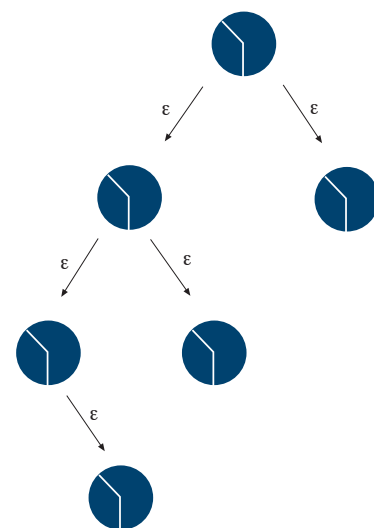


Figure 2 Clocks are adjusted from a source – Error introduced at each step

fairly small, most clocks will approximate Real Time to a level that is sufficient for everyday life.

A clock that is a few minutes off to either side will normally not be a problem in everyday life. In the Digital Forensics context, the same would be true. A few minutes off will likely not be crucial to the facts of the investigation. The problem arises where a clock shows a larger error due to lack of adjustment, failure or malicious adjustment.

2.3 Time stamps, events and causality

A time stamp is a representation of a state of a clock and that is somehow related to an event. Informally one may say that the generation of a time stamp was caused by an event. An event is something that occurred that changed the state of the world. Since changes cannot happen instantly, the definition of an event must be such that events are allowed to span over time. We define an event as a change that occurred over a time span. The start and end of an event are points in Real Time. With our definition of Real Time, an event can be said to have happened before another if the end point of the first event happens before the start point of the next event. If the time span of two events overlap, the events can be said to be concurrent.

Now, a time stamp can be said to be the representation of the local clock at some point in Real Time between the starting point and ending point of the event that caused it.

Having defined the time span of an event, we now turn to look at the change in the state of the world that an event produces. All events have necessary prerequisites. In order for an event to make a particular change in the state of the world it is necessary for the state of the world to be such that the particular event is possible. Say for instance that I pour coffee in a mug. In order for this event to occur, the state of the world must be such as to allow this event. For instance, I must have a cup and I must already have brewed coffee. This introduces the concept of causality. When an event starts, the state of the world must be such that it is allowed to happen. But the state of

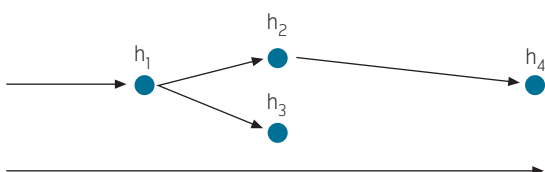


Figure 3 Causality – Some events are necessary for others to occur

the world at a particular time is just the sum of all previous events plus (possibly depending on one's religious beliefs) a starting condition. Thus, an event is only allowed to happen if previous events that led the world to the necessary starting state have already happened.

It is common in a computer system that all time stamps are recorded according to the same time source, a local clock according to the definitions above that may deviate from Real Time. If such a system records time stamps for events that are causally connected, the system can be analyzed for changes in the relationship between the local clock and Real Time.

2.4 The time stamp context

The key to the solution of the time stamp challenge lies in the understanding of the context where time stamps live in computer systems, and the causal relationship between the events that caused them. Fortunately, common digital systems record a large amount of time stamps with clear patterns of causal connections. A file system is a very good example of this.

2.5 Time stamps in file systems

Most file systems contain time stamps for each file. On a normal workstation, these time stamps amount to hundreds of thousands of causally interconnected events. The most common file system time stamps are:

- *Last Written*: An event that caused the file content to change;
- *Last Read*: An event that caused the file to be read;
- *File Created*: An event that created the file at its current location;
- *Entry Modified*: An event that caused file metadata to change.

Already from these definitions, several causal connections can be postulated:

- If a file is created at a new location, its metadata must change.
- If a file is read, it must first have been created.

Taking into account the organisations of file systems, and even operating systems, more causal connections spring to mind:

- A file is created in a directory; thus the directory must already have been created. This must hold for all files and directories in a file system.
- Files cannot be created in a file system unless the file system has already been created.
- Files cannot partially overwrite other files unless those files were there already.
- If a file is created or deleted in a directory, the system must change the directory.
- If a file is read, the system must read the directory first.
- If a program is run, files that it depends on must be installed first.

If all time stamps are related to the local clock, a change in the relationship between the local clock and Real Time is bound to be reflected in the observed time stamps. This will lead to inconsistencies.

Analysing time stamps in file systems is only one example of where important time stamps can be found to determine the time stamp consistency. Many other sources exist, both in terms of actual time stamp existence, and as sources of interrelations.

2.6 The development of a framework for time stamp analysis

By analysing causal relationships between events in a computer system that produce time stamps, one can therefore detect changes in the local clock caused by failure or malicious adjustment. With the modelling of more causal interconnections, it becomes less likely that changes will be undetected. Due to the high number of time stamps and interconnections, analysis of causal relationships as defined here should be automated. It is therefore proposed to define a logical framework for the analysis of causal relationships between events and the time stamps resulting from them. The framework will be a foundation of implementations of causal analysis in software, a system that will be of great importance in digital forensic investigations.

3 Conclusion

Time stamps are vital elements in Digital Forensics, since they are the only entities that can relate evidence found on digital media to events that have taken place in the real world. Time stamps may be wrong for various reasons. We have shown that it is possible to improve the evidential quality of time stamps by correlating time stamps that occur on an

evidence medium. Before such correlation can be done on a large scale, it is necessary to define a logical framework for time stamps analysis. The development of such a framework is one important goal in the TID research project funded by the NFR IKT SOs research programme.

4 References

- 1 Vacca, J. *Digital forensics – Computer Crime Scene Investigation*. Charles River Media, 2002.
- 2 Prorise, C, Mandia, K, Pepe, M. *Incident Response and Digital forensics*. McGraw-Hill, 2003.
- 3 Interpol. *Interpol Computer Crime Manual, 1993–2004*.
- 4 Lilleng, S. *Datakriminalitet (Computer Crime)*. ØKOKRIM skriftserie, 1995.
- 5 Assosiation of Chief Police Officers. *Good Practice Guide for Computer Based Evidence*. June 1999.
- 6 *EnCase, software package*. June 16, 2005. [online] – URL: <http://www.encase.com/>
- 7 National Institute of Justice. *Test Results for Disk Imaging Tools: EnCase 3.20*. June 2003.
- 8 National Institute of Justice. *Test Results for Disk Imaging Tools: dd Provided with FreeBSD 4.4*. Jan 2004
- 9 Willassen, S. Forensics and the GSM Mobile Telephone System. *International Journal on Digital Evidence*, 2 (2), 2003.
- 10 Vatis, M. *Law Enforcement Tools and Technologies for Investigating Cyber Attacks*. Dartmouth College, June 2002.
- 11 Casey, E.. Error, Uncertainty and Loss in Digital Evidence. *International Journal on Digital Evidence*, 1 (2), 2002.
- 12 Hosmer, C. Proving the Integrity of Digital Evidence with Time. *International Journal on Digital Evidence*, 1 (1), 2002.
- 13 Weil, M. Dynamic Time & Date Stamp Analysis. *International Journal on Digital Evidence*, 1 (2), 2002.

- 14 Boyd, C, Forster, P. Time and Date issues in forensic computing – a case study. *Digital Investigation*, 1, Jan 2004.
- 15 Klyne, G, Newman, C. *Date and Timestamps of the Internet*. IETF, July 2002. RFC 3339.
- 16 Rousseau, L. Secure Time in a Portable Device. *Proc. of GemPlus Developer Conference*, Paris, France, June 20–21, 2001.
(<http://www.gemplus.fr/smart/rd/publications/pdf/Rou01heu.pdf>)
- 17 International Standardization Organisation. *Data elements and interchange formats – Information interchange – Representation of dates and times*. 2004. ISO 8601:2004.
- 18 Stevens, M. Unification of relative time frames for digital forensics. *Digital Investigation*, 1, 2004.

Svein Y. Willassen has a *Siv.ing.* degree in Telematics from the Norwegian University of Science and Technology (NTNU). He has worked as a special investigator at the Norwegian National Computer Crime Center and as Computer Forensic Investigation Manager at Ibas AS. Willassen is currently working on a PhD within Digital Forensics in the research project “Time Stamps in Digital Forensics” at NTNU.

email: svein@willassen.no

Stig Frode Mjølshes received his *Siv.ing.* degree in Physical Electronics in 1980, and *Dr.Ing.* degree in Telecommunications in 1990, both at the Norwegian Institute of Technology, Trondheim. He has on several occasions served as security technology expert on Norwegian governmental committees in security and privacy, such as health privacy, and cryptographic policy. Just recently, he was asked to write the initial draft of a new national research programme in information security. He was called as expert witness in several legal cases, including the rather famous DVD DeCSS prosecution. He has worked on engineering analysis and design with respect to conditional access control in digital satellite television broadcast. Scientifically, he has maintained an interest in the technical approach of cryptographic protocols to help solve parts of the challenges of commercial access rights to digital content. Starting 2003, he holds a full professorship in information security at NTNU (Department of Telematics).

Stig Frode Mjølshes is appointed committee executive manager of “NTNU Research Programme for Information Security” in the strategic focus area of ICT, and is also the manager of the research project “Time Stamps in Digital Forensics”.

email: sfm@item.ntnu.no