

Chapter 1

HYPOTHESIS BASED INVESTIGATION OF DIGITAL TIMESTAMPS

Svein Yngvar Willassen

Abstract Timestamps stored on digital media play an important role in digital investigations. Unfortunately, timestamps may be manipulated, and also refer to a clock that can be erroneous, failing or maladjusted. This reduces the evidentiary value of timestamps. This paper takes the approach that historical adjustments to a clock can be hypothesized in a clock hypothesis. Clock hypotheses can then be tested for consistency with stored timestamps. A formalism for the definition and testing of a clock hypothesis is developed, and test methods for clock hypothesis consistency are demonstrated. With the number of timestamps found in typical digital investigations, the methods presented in this paper can justify clock hypotheses without having to rely on timestamps from external sources. This increases the evidentiary value of timestamps, even when the originating clock has been erroneous, failing or maladjusted.

Keywords: digital investigation, timestamps, causality, hypothesis based

1. Introduction

A timestamp is a recorded representation of a specific moment in time. In digital computing, a timestamp is a recorded representation of a specific moment in time in a digital format. This representation is either stored on a medium storing digital data, or transmitted on a network designed to convey digital data. Timestamps play an important role in digital investigations. Traditionally, they are used to place the event generating the timestamp at a specific moment in time, thereby facilitating event reconstruction. The identification that a certain event on a computer took place at a specific time makes it possible to correlate the event with events occurring outside the computer system. This can be events that occurred in another digital system, or in the physical world. A hard drive of a Windows system, investigated in typical digital

investigations, usually contains tens or even hundreds of thousands of timestamps.

1.1 Error and uncertainty in timestamps

For a number of reasons, stored timestamps may not accurately reflect the time of the generating event. A timestamp always depends on the adjustment of the clock from which it is generated. Since the timestamp is a function of the clock, it is always relative to the setting of the clock. Unfortunately, clocks are not fully reliable. Clocks may drift, thereby generating timestamps gradually more different from those generated from other clocks. Clocks may also fail, and produce completely incorrect timestamps. Further, clocks on most systems may be adjusted at any time by the user of the system to show a different date and time than civil time. The consequence is that a timestamp is relative not only to the clock it was generated from in general, but also to the particular adjustment of the clock at the time the timestamp was generated. Therefore, even timestamps generated from the same clock cannot be reliably compared unless it can be justified that the adjustment of the clock is unchanged between creations of timestamps. In order to reliably compare timestamps from different clocks, the difference between the clocks must be found, and it must be justified for all clocks that their adjustment has not changed.

The uncertainty associated with digitally stored timestamps implies that timestamps in general cannot be relied upon as evidence without justification of the factors that can lead to errors. In particular, it cannot be blindly assumed that timestamps are based on a clock that is adjusted to civil time. Further, it cannot be assumed that timestamps generated by different clocks are relative to the same clock. Not even when timestamps are based on the same clock, can one be absolutely certain that the time difference between the two events is equal to the difference between the timestamps. These uncertainties are worrying for investigators. If timestamps cannot be relied upon, then it is in many cases not possible to reconstruct the events in the case reliably.

1.2 Timestamps and causality

New methods are required for digital investigation of timestamps and use of digitally stored timestamps as evidence. This work takes the approach that time stamps and their evidence value can be tested in the hypothesis based investigation model suggested by Carrier. [2] In this model, the history of the medium under investigation is the complete set of configurations, states and events that has occurred during the lifetime

of the medium. The data direct observable by the investigator is the final state of the medium. This includes observations of all timestamps stored on the medium and the clock. These timestamps are all functions of the computer clock at some previous state in the history, and any subsequent events that affect them. This paper uses these properties to develop a formalism for clock hypothesis definition and tests that can be used to test it for consistency with observed evidence.

1.3 Related work

Being recognized as a research challenge, the problem of timestamp interpretation in digital investigation has been studied by a few researchers during recent years. Schatz et al demonstrated the problem of clock drift by observing clock synchronization on a network of computers in a small business. [3] Schatz suggests mitigating the problem by correlating the timestamps in web cache stored on the computer with records obtained from the web servers. Weil and Boyd et al suggest similar correlation methods, by using timestamps stored on the investigated computer coming from other clocks, such as timestamps in dynamically generated web pages. [1, 4] Such methods would provide correlation for the period for which cached data exist on the investigated computer only. These methods may be able to confirm or refute hypotheses about the clock in the period for which correlation material exists. They may not be able to provide reasonable evidence to refute a hypothesis that timestamps have been changed or the clock has been adjusted during the period for which no correlation material exist. Correlation with server records is only possible when such records actually exist, and the investigator has legal access to them.

Gladyshev studied the use of causality properties for establishing boundaries on period of time in which an event may have occurred. [5] In his approach, time bounding can be established when an event that occurred at an unknown or uncertain time is causally preceded and succeeded by events with known time occurrence. In order to perform time bounding, it is then required to know events of known time causally connected to the investigated events. When used to investigate a computer system, these events of known time must come from external sources. This approach differs from the approach taken in this work, where no time references from external sources is assumed. The concept of causality is used in this work as well as in Gladyshev's. Although the happened-before relation is defined differently, its use to correlate timestamps bears resemblance.

2. Hypothesis based timestamp investigation

2.1 Causality

Informally, causality is the relationship between cause and effect. This relationship can be expressed as a relation between events. In previous works, causality has been defined by means of the *happened-before* relation \rightarrow . The happened-before relation was first used by Lamport, who defined the relation by ordering events happening in a process and sending and receiving messages between processes. [6] This definition was generalized by Fidge to encompass process creation and termination as well as both synchronous and asynchronous message passing. [7]

For use in digital investigation, Gladyshev proposed an extended definition of happened-before. In Gladyshev's version it is defined that $e_1 \rightarrow e_2$ if e_2 uses the result of e_1 or e_1 precedes e_2 in the usual course of business of some organisation or during the normal operation of a machine. [5] In this definition, the meaning of happened-before is extended beyond computers. This extension is useful, since digital investigation requires the reconstruction of events, both within computers and outside them. Gladyshev's definition might however create doubt about exactly what happened-before means, since it is debatable what exactly constitutes the *normal operation* of a machine and the *usual course* of a business.

Definition. Let \rightarrow be the *happened-before* relation. If $e_1 \rightarrow e_2$, then the occurrence of e_1 is necessary for e_2 to occur because e_2 depends on the effects of e_1 .

Important examples of causality per this definition of the happened-before relation include:

- e_1 produces an item that is necessary input for e_2

This is equivalent to Gladyshev's definition " e_2 uses the result of e_1 ". The definition of happened-before in terms of message sending and reception used by Lamport and Fidge also fall within this example.

- e_1 and e_2 are events in a computer program, where e_2 uses data produced by e_1 .

Since events in computer programs use items produced by other events in the same program, such as variables, data stored in memory, registers and stack pointers, many events occurring in computer programs will be related by happened-before. This is a special case of " e_1 produces an item that is necessary input for e_2 ". The definition of happened-before in terms of events occurring in a

process used by Lamport and Fidge falls within this example, with the exception of events that do not use the result of each other. This exception makes the definition suitable for modern computer systems, in which the execution order of a computer program can be rearranged by compilers and processors when the instructions do not depend on the results of each other.

2.2 Time and time values

In this work, time is considered to be a fundamental quantity. As a fundamental quantity, time is not itself defined in terms of other quantities, but it is measurable by means of comparison with periodic events, such as the periodic events occurring in clocks. Such periodic events may for example be the swinging of a pendulum (a pendulum clock), the movement of earth (a sundial) or microwave emission from certain materials (an atomic clock). We consider events to have a moment in time associated with them, and assume that these moments in time can be ordered in time by relations $<$ and $=$.

Definition. Let E be the domain of events. Let e be an event. Events are considered to be instantaneous. Let T be the domain of time. Let $t(e)$ be a function $E \mapsto T$, representing the moment in time at which event e occurred.

Further, we assume that *causality is preserved in time*. With the preservation of causality in time, we mean that no event can causally depend on an event occurring at the same time or a later time than itself. This can be expressed explicitly with the happened-before relation as:

$$t(e_i) \leq t(e_j) \Rightarrow e_j \not\rightarrow e_i \quad (1)$$

This assumption corresponds to the intuitive understanding of the relationship between causality and time. If such causal relations were allowed, then events in the future would be allowed to affect events in the past, something that has not been shown to occur in the real world.

For two events related by the happened-before relation, Equation (1) implies that:

$$e_i \rightarrow e_j \Rightarrow t(e_i) < t(e_j) \quad (2)$$

The above imposes an ordering in time on events ordered by the happened-before relation \rightarrow . It does not however imply any ordering in time for events not ordered by \rightarrow . Also, $t(e_i) < t(e_j)$ does not imply that $e_i \rightarrow e_j$. Events may happen at different moments in time without being related by \rightarrow . On the other hand, if two moments in time $t(e_1)$ and $t(e_2)$ are ordered such that $t(e_1) < t(e_2)$, events occurring at those

moments in time cannot be causally connected in reverse, such that the $e_2 \rightarrow e_1$.

2.3 Clocks

A clock is a device designed to give the owner an approximation of time that is sufficiently coherent so as to allow the owner to measure and compare time periods and sufficiently consistent with other clocks so as to allow the owner to perform actions concurrent with other clock owners without continuous coordination. Clocks are in other words designed to give an approximation of time. The definition of a clock should be able to reflect the possibility of clock drift and adjustment mentioned in Section 1.2.

Definition. Let V be the domain of time values produced by a clock. $c(t)$ is a clock function $T \mapsto V$

The definition of a clock function does not impose any restrictions on the clock values as a function of time. For example, even if $t_1 < t_2$ it may well be the case that $c(t_1) > c(t_2)$. And even if $t_1 < t_2 < t_3$, it may be the case that $c(t_1) = c(t_2) = c(t_3)$. The latter situation may for example occur if the events occurring at t_1, t_2, t_3 are so close together in time that the clock is unable to differentiate between them.

2.4 Timestamped events

A timestamped event is an event for which there exists a timestamp value in domain V . The timestamp value can be represented as a function on the event. Timestamps are created when an event makes a copy of the value provided by a clock. All timestamps in a set of timestamped events are not necessarily related to the same clock.

Definition. Let E be a set of timestamped events and V a domain of time values. $\tau_c(e)$ is a function $E \mapsto V$ such that $\tau_c(e_i) = c(t(e_i))$. $\tau_c(e_i)$ represents the timestamp associated with the event e_i relative to clock c .

In this definition, a timestamp is the value of the producing clock at the time of the event. The timestamp reflects the clock's representation of time at that particular moment. The definition of timestamps as a function of events and clocks provides a possibility to reason over timestamps and clocks.

2.5 Ideal and non-ideal clocks and their properties

It is useful to introduce the concept of *ideal clocks* and *non-ideal clocks*. An ideal clock is a clock which can only go forward.

Definition. Let I be the set of ideal clocks. An ideal clock $c(t) \in I$ is a clock which satisfies

$$\begin{aligned}\forall i \forall j (t(e_i) < t(e_j) &\Rightarrow c(t(e_i)) \leq c(t(e_j))) \\ \forall i \forall j (t(e_i) = t(e_j) &\Rightarrow c(t(e_i)) = c(t(e_j)))\end{aligned}$$

An ideal clock is a clock function on time which has the property that the value provided in the function from time is monotonically increasing. While having a monotonically increasing value, the values $c(t(e_i))$, $c(t(e_j))$ produced from two different moments in time $t(e_i)$ and $t(e_j)$ where $t(e_i) < t(e_j)$ may be equal. Many clocks represent moments in time as discrete values. In a discrete clock with limited resolution, two moments close in time will be represented by the same clock value.

Theorem 1. For all ideal clocks $c \in I$, produced timestamps satisfies

$$e_i \rightarrow e_j \Rightarrow \tau_c(e_i) \leq \tau_c(e_j)$$

Proof for the theorem is given in the Appendix.

The monotonic property of ideal clocks guarantee that two causally connected events timestamped by the same ideal clock have timestamps where the timestamp of the latter event is always equal or higher than the timestamp of the first.

2.6 Clock hypotheses

In order to be able to test if a certain theory about the clock holds, one must be able to formulate a hypothesis about the clock function. A hypothesis about the clock function is a possible theory about the clock function during the computer history. That hypothesis can then be tested against the set of observed timestamps. In the following, a clock hypothesis will be denoted $c_h(t)$.

Definition. A clock function $c(t)$ can be divided into two components, one function $b(t)$ which is an ideal clock and one function $d(t)$ representing the deviation from the ideal clock.

$$c(t) = b(t) + d(t)$$

In this scheme, the clock ($c(t)$) is divided into components: $b(t)$ is a base clock which must be an ideal clock. $d(t)$ is the difference between

the base clock and the investigated clock. By selecting a common base, two or more clocks can be compared by comparing the deviation only. It is sometimes useful to express the time of an event in terms of the base clock. This can be done by subtracting $d(t)$.

$$b(t) = c(t) - d(t) \quad (3)$$

2.7 Observed event sets and correctness

During a digital investigation of a computer, the investigator will observe a number of timestamped events that all come from the same clock. Some of these events will be causally connected. This set of observed timestamped events is called the *observation set*.

Definition. An observation set O , is a set of timestamped events, in which all timestamps are related to one clock $c_o(t)$.

In an observation set, there will typically be a large amount of timestamped events. The number of causal connections may also be large. The data in an observation set can be used to determine if a clock hypothesis holds or not.

Definition. A clock hypothesis $c_h(t)$ for an observation set O is *correct* if the value of $c_o(t)$ is equal to the value of $c_h(t)$ for all t .

$$\begin{aligned} c_o(t) &= c_h(t) \\ &\Downarrow \\ \forall e_i (\tau_{c_o}(e_i) &= c_h(t(e_i))) \end{aligned}$$

If a clock hypothesis is correct, then all occurrences of timestamps must match the value predicted by the hypothesis. The correctness property can therefore be utilized to find techniques for testing if a clock hypothesis is correct or not.

Theorem 2. *In a correct clock hypothesis $c_h(t)$, the timestamps of all causally connected events $e_i \rightarrow e_j$ in an observation set O must be such that the timestamp of the first event minus the deviation from a common base has value less than or equal to the timestamp of the latter event minus the deviation from a common base.*

$$e_i \rightarrow e_j \Rightarrow \tau_{c_o}(e_i) - d_h(t(e_i)) \leq \tau_{c_o}(e_j) - d_h(t(e_j))$$

Proof for the theorem is given in the Appendix.

Conversely, if the property examined in Theorem 2 does not hold, then the hypothesis is not correct.

Theorem 3. (Test-A theorem). *If a pair of causally connected events $e_i \rightarrow e_j$ exist in an observation set O , for which the timestamp of e_i minus the hypothesis deviation from a common base has a higher value*

than the timestamp of e_j minus the hypothesis deviation from a common base, then the clock hypothesis is incorrect. This is called Test-A.

$$\exists e_i \exists e_j ((e_i \rightarrow e_j) \wedge (\tau_{c_o}(e_i) - d_h(t(e_i)) > \tau_{c_o}(e_j) - d_h(t(e_j)))) \Rightarrow c_o(t) \neq c_h(t)$$

Proof for the theorem is given in the Appendix.

Example 1. Consider the *default clock hypothesis*, where it is assumed that the clock of the investigated computer has always been equal to civil time, say UTC. Then $c_h(t) = b_h(t)$ and $d_h(t) = 0$. Now, let the observed set consist of timestamps for four events $e_1 - e_4$, where:

$$\begin{aligned} \tau_{c_o}(e_1) &= \text{Jan 12, 2003, 12:46:34} \\ \tau_{c_o}(e_2) &= \text{Apr 21, 2004, 10:22:38} \\ \tau_{c_o}(e_3) &= \text{Feb 9, 2003, 22:16:04} \\ \tau_{c_o}(e_4) &= \text{Dec 12, 2002, 02:46:32} \end{aligned}$$

And where $e_1 \rightarrow e_2$ and $e_3 \rightarrow e_4$. If we now apply Test-A for $i = 3$ and $j = 4$, we see that

$$(e_3 \rightarrow e_4) \wedge (\tau_{c_o}(e_3) > \tau_{c_o}(e_4))$$

And since $d_h(t) = 0$, the test fails. Thus, the default hypothesis is not correct for this observation set.

The result can be explained informally as follows: Since e_4 must have happened after e_3 and the timestamp of e_4 is at an earlier time than the timestamp of e_3 , it cannot be the case that the clock has not been adjusted between these two events.

Theorem 4. (Test-B theorem). *In a clock hypothesis $c_h(t)$, for values c' of $c_h(t)$ for which $c_h(t) = c'$ has no solution, the existence of any timestamps in the observation set O with value $\tau_{c_o}(e_i) = c'$, implies that $c_h(t)$ is incorrect. This is called Test-B.*

Proof for the theorem is given in the Appendix.

2.8 Clock hypothesis consistency

The results in Theorem 3 and Theorem 4 are useful, because they can be used to refute a clock hypothesis for observation set O , from observations of the timestamps on events in O . In Test-A, a clock hypothesis is incorrect when observations of timestamps for two causally connected events are not ordered correctly by the clock hypothesis. In Test-B, a clock hypothesis is incorrect if observations of timestamps exist that

cannot be produced by the clock hypothesis, because it is a discontinuous function. These theorems provide methods for testing if a clock hypothesis is incorrect. By iterating over all events and pair of events, each timestamp can be checked for consistency with Test-A and Test-B.

The result of testing all timestamps in the observation set will be either that the clock hypothesis is incorrect or that it is not incorrect. The tests can refute the clock hypothesis, but they can not prove it correct. This leads to the following definition of a consistent clock hypothesis.

Definition. Given a set of tests Z , a clock hypothesis is *consistent under Z* with an observation set O if no test $z \in Z$ shows that the hypothesis is incorrect for O . A clock hypothesis is *inconsistent under Z* with an observation set O if it is not consistent under Z with O .

The distinction that follows from the definitions of correct and consistent is useful in the context of digital investigations. In a correct clock hypothesis all possible time values are always equal to the investigated clock. A correct clock hypothesis can only be derived if the investigated clock has been observed at every moment in its history. Establishing a correct hypothesis about the investigated clock is inconceivable in a real investigation. All the investigator can hope to do is to establish a consistent clock hypothesis. In such a hypothesis there is no evidence available that refutes the hypothesis. Specifically, none of the timestamps of events in the observation set O as applied in tests in the test set Z show that the hypothesis is incorrect. If there is a large number of timestamps and causally connected events present in the observation set O , these requirements impose strict constraints on a consistent hypothesis. This can lead to the justification of the hypothesis. The more data available in O to be fed into the tests in Z , the more justified the clock hypothesis can be. As long as the clock hypothesis is consistent, the data in O is evidence supporting the hypothesis.

2.9 The clock hypothesis as a scientific hypothesis

In the hypothesis based investigation model proposed by Carrier, a digital investigation is a process that formulates and tests hypotheses to answer questions about digital events or the state of digital data. [2] Carrier proposes that the investigation process is scientific if the hypothesis is scientific and then tested through conducting experiments. Carrier cites Popper in that the “criterion of the scientific status of a theory is its falsifiability, or refutability, or testability”.

The question here is then if the method for clock hypothesis formulation and testing the set of observed timestamps adhere to these criteria.

From the previous discussion, a clock hypothesis is a theory that is falsifiable and therefore testable. The clock hypothesis theory described in the previous sections adheres to the requirements of a scientific theory. The hypothesis forbids certain things to happen; the occurrence of timestamp configurations as described in Test-A and Test-B. The described tests examine the evidence for refutation of the theory. They do not look for confirmation, but examine the available evidence for inconsistency with the theory. When the tests have been applied, and found not to refute the hypothesis, the tests count as serious but unsuccessful attempts to falsify the theory and therefore as confirming evidence.

3. Concluding remarks

This paper has presented a formalism for the definition of a clock hypothesis and testing it for consistency with evidence in the form of observed timestamps. When the number of timestamps is high, and many of them are causally related, these tests will put a clock hypothesis under close scrutiny. This is the typical situation when investigating digital media like hard drives. In order to test hypotheses on large number of stored timestamps, the tests can and should be implemented in software. The tests can then be used in digital investigations, typically by testing alternative clock hypotheses, such as alternative hypotheses provided by a plaintiff and a defendant. When a clock hypothesis is justified by these methods, the evidentiary value of the investigated timestamps is increased; the real time when a timestamp was created can now be found by using the clock hypothesis.

References

- [1] C. Boyd and P. Forster, "Time and date issues in forensic computing - a case study," *Digital Investigation*, vol. 2004:1, pp. 18-23, 2004.
- [2] B. Carrier, "A hypothesis-based approach to digital forensic investigations," Center for Education and Research in Information Assurance and Security, Purdue University Tech Report 2006-06, 2006.
- [3] B. Schatz, G. Mohay, and A. Clark, "A correlation method for establishing provenance of timestamps in digital evidence," *Digital Investigation*, vol. 2006:3S, pp. 98-107, 2006.
- [4] M. C. Weil, "Dynamic Time & Date Stamp Analysis," *International Journal of Digital Evidence*, vol. 1:2, 2002.
- [5] P. Gladyshev and A. Patel, "Formalising Event Time Bounding in Digital Investigations," *International Journal of Digital Evidence*, vol. 4:2, 2005.

- [6] L. Lamport, "Time, Clocks and the Ordering of Events in a Distributed System," *Communications of the ACM*, vol. 21:7, pp. 558-565, 1978.
- [7] C. Fidge, "Logical Time in Distributed Computing Systems," *Computer*, vol. 24:8, pp. 28-33, 1991.

4. Proofs

Theorem 1.

Claim: For all ideal clocks $c \in I$, produced timestamps satisfies

$$e_i \rightarrow e_j \Rightarrow \tau_c(e_i) \leq \tau_c(e_j)$$

Proof: By definition an ideal clock satisfies:

$$\forall i \forall j (t(e_i) < t(e_j) \Rightarrow c(t(e_i)) \leq c(t(e_j)))$$

That is, for events e_i and e_j occurring at times $t(e_i)$ and $t(e_j)$ we have:

$$t(e_i) < t(e_j) \Leftrightarrow c(t(e_i)) \leq c(t(e_j))$$

By replacing we now obtain:

$$e_i \rightarrow e_j \Rightarrow c(t(e_i)) \leq c(t(e_j))$$

And then, $\tau_c(e_i) = c(t(e_i))$, which gives:

$$e_i \rightarrow e_j \Rightarrow \tau_c(e_i) \leq \tau_c(e_j)$$

□

Theorem 2.

Claim: In a correct clock hypothesis $c_h(t)$, the timestamps of all causally connected events $e_i \rightarrow e_j$ in an observation set O must be such that the timestamp of the first event minus the deviation from a common base has value less than or equal to the timestamp of the latter event minus the deviation from a common base.

$$e_i \rightarrow e_j \Rightarrow \tau_{c_o}(e_i) - d_h(t(e_i)) \leq \tau_{c_o}(e_j) - d_h(t(e_j))$$

Proof: Let $c_h(t)$ be a correct clock hypothesis. Let $b(t)$ be a common base for $c_h(t)$ and $c_o(t)$. Then

$$b(t) = c_h(t) - d_h(t)$$

$$b(t) = c_o(t) - d_o(t)$$

Thus,

$$c_h(t) - d_h(t) = c_o(t) - d_o(t)$$

And since $c_h(t)$ is correct we have $c_h(t) = c_o(t)$. Therefore

$$\begin{aligned} d_h(t) &= d_o(t) \\ b(t) &= c_o(t) - d_h(t) \end{aligned}$$

And inserting definition yields

$$b(t(e)) = \tau_{c_o}(e) - d_h(t(e))$$

Now, $b(t)$ shall be an ideal clock. From Theorem 1 we know that ideal clocks satisfy

$$e_i \rightarrow e_j \Rightarrow c(t(e_i)) \leq c(t(e_j))$$

And then, inserting $b(t)$ gives

$$\begin{aligned} e_i \rightarrow e_j &\Rightarrow b(t(e_i)) \leq b(t(e_j)) \\ e_i \rightarrow e_j &\Rightarrow \tau_{c_o}(e_i) - d_h(t(e_i)) \leq \tau_{c_o}(e_j) - d_h(t(e_j)) \end{aligned}$$

□

Theorem 3.

Claim: *If a pair of causally connected events $e_i \rightarrow e_j$ exist in an observation set O , for which the timestamp of e_i minus the hypothesis deviation from a common base has a higher value than the timestamp of e_j minus the hypothesis deviation from a common base, then the clock hypothesis is incorrect.*

$$\exists e_i \exists e_j ((e_i \rightarrow e_j) \wedge (\tau_{c_o}(e_i) - d_h(t(e_i)) > \tau_{c_o}(e_j) - d_h(t(e_j)))) \Rightarrow c_o(t) \neq c_h(t)$$

Proof: The proof is by contradiction. Let $c_h(t)$ be a clock hypothesis and O an observation set with clock $c_o(t)$. Let (e_a, e_b) be a pair of events in O such that $e_a \rightarrow e_b$ and $\tau_{c_o}(e_a) - d_h(t(e_a)) > \tau_{c_o}(e_b) - d_h(t(e_b))$. Assume that $c_h(t)$ is correct, $c_h(t) = c_o(t)$. If $c_h(t)$ is correct we have from Theorem 3 that

$$e_i \rightarrow e_j \Rightarrow \tau_{c_o}(e_i) - d_h(t(e_i)) \leq \tau_{c_o}(e_j) - d_h(t(e_j))$$

But for $i = a$ and $j = b$, we have assumed that,

$$(e_a \rightarrow e_b) \wedge (\tau_{c_o}(e_a) - d_h(t(e_a)) > \tau_{c_o}(e_b) - d_h(t(e_b))) \quad (4)$$

This contradicts the result from Theorem 3. Therefore, if (4) holds, then $c_h(t)$ cannot be correct. There have been no assumption or restriction on the events a and b. a and b could therefore have been any event in the observation set O . The result is that for any event e_i and e_j , if (4) holds, $c_h(t)$ cannot be correct.

$$\exists e_i \exists e_j ((e_i \rightarrow e_j) \wedge (\tau_{c_o}(e_i) - d_h(t(e_i)) > \tau_{c_o}(e_j) - d_h(t(e_j)))) \Rightarrow c_o(t) \neq c_h(t)$$

□

Theorem 4.

Claim: *In a clock hypothesis $c_h(t)$, for values c' of $c_h(t)$ for which $c_h(t) = c'$ has no solution, the existence of any timestamps in the observation set O with value $\tau_{c_o}(e_i) = c'$, implies that $c_h(t)$ is incorrect.*

Proof: The proof is by contradiction. Let $c_h(t)$ be a clock hypothesis and O an observation set with clock $c_o(t)$. Let e_a be an event in O and $\tau_{c_o}(e_a) = c'$ the timestamp of e_a . Let c' have a value such that $c_h(t) = c'$ has no solution. Assume that $c_h(t)$ is correct, $c_h(t) = c_o(t)$. If $c_h(t)$ is correct we have

$$\forall e_i (\tau_{c_o}(e_i) = c_h(t(e_i)))$$

Which means that for $i = a$

$$\tau_{c_o}(e_a) = c_h(t(e_a))$$

This is a contradiction since $\tau_{c_o}(e_a) = c'$ and $c_h(t) = c'$ has no solution. Therefore if $\tau_{c_o}(e_a) = c'$ and $c_h(t) = c'$ has no solution, then $c_h(t)$ cannot be correct.

□