INVESTIGATION · METHOD AND THE FUTURE

Timeline Analysis: Reconstructing Events

Almost every investigation must establish what happened, in what order and when. This article explains how investigators build timelines from witnesses, documents and digital records, how to judge the reliability of each time source, the common errors that distort reconstructions, and how timelines are used to test hypotheses and present findings.

ModQu research article · 2,653 words · 24 references (APA 7th edition)

Investigations are, at their heart, attempts to reconstruct the past. Whether the question is how a fire started, when a document was created, how a cyber attacker moved through a network, or what happened in the hours before an accident, the investigator must establish a sequence of events and fix them in time. A timeline, or chronology, is the structured record of that sequence. It is one of the simplest tools in investigation and one of the most powerful. A good timeline reveals gaps, contradictions and impossible sequences; it shows which accounts fit together and which do not; and it gives a clear framework for explaining the findings to others.

This article explains the purposes of timeline analysis, how timelines are built from different kinds of source, how to judge and reconcile the times those sources give, the cognitive and technical errors that can distort reconstructions, and how timelines are used to test hypotheses and present conclusions.

Why timelines matter

Investigation guides in many fields recommend building a chronology early and maintaining it throughout. In criminal investigation, timelines help establish opportunity, test alibis and link events (Stelfox, 2009; Tong et al., 2009). In investigative journalism, a master chronology helps reporters organise documents and interviews and spot connections (Hunter et al., 2011). In intelligence analysis, chronologies and timelines are standard structured techniques for organising information and identifying gaps and anomalies (Heuer & Pherson, 2015). In cyber incident response, a timeline of the attacker's actions is the core output of the analysis (Cichonski et al., 2012).

Timelines serve several purposes at once:

- **Organising information.** Placing every event and record in time order brings scattered material together.
- **Revealing gaps.** Periods with no information show where further inquiry is needed.
- **Exposing contradictions.** When two sources place the same event at different times, or when a sequence is physically impossible, at least one source is wrong.
- **Testing hypotheses.** Each explanation of what happened implies a sequence of events, which can be compared with the timeline.
- **Communicating findings.** A clear timeline helps decision-makers, courts and the public understand what happened.

Psychological research suggests that people naturally understand evidence in the form of stories. Pennington and Hastie (1992) found that jurors construct narratives to explain the evidence, and that the narrative they find most coherent strongly influences their verdict. Wagenaar et al. (1993) argued that stories in criminal cases must be "anchored" in evidence at each point, and that persuasive stories can be built on weak anchors. A well-documented timeline is one way of ensuring that each element of the story is anchored in evidence.

Sources of time

Times come from many sources, which differ greatly in precision and reliability.

Sources of time in an investigation

Each source needs to be assessed before its times are combined with others

	Typical precision	Main risks
Witness memory	Hours to days; order often better than time	Telescoping, reconstruction, influence from others
Documents and records	Day or minute, as recorded	Back-dating, errors, time of entry versus event
Device and system logs	Seconds or better	Wrong clocks, time zones, formats, tampering
Video and photographs	Seconds, if clock is checked	Unsynchronised camera clocks; missing frames
Physical evidence	Hours to years	Wide ranges; depends on conditions

Based on Friedman (1993), Casey (2011) and Schatz et al. (2006) ModQu.com

Figure 1. Five kinds of time source. A timeline is strongest where several independent sources agree on the same time. Diagram by ModQu.

Witnesses. People are usually better at remembering the order of events than their exact timing. Friedman (1993) reviewed research on memory for the time of past events and found that people rarely store dates directly; instead they reconstruct them from clues, such as what else was happening, the weather or the day of the week. Errors are common. One well-documented error is "telescoping", in which people place events as more recent than they really were. Neter and Waksberg (1964) found this effect in household surveys about expenditure. Loftus and Marburger (1983) showed that asking people to anchor their memory to a memorable public event reduced such errors, a technique that investigators can use when asking witnesses about timing.

Documents and records. Letters, invoices, minutes, logbooks and receipts carry dates and sometimes times. They are often more reliable than memory, but they can be wrong, back-dated or created later. A further subtlety is the difference between the time an event happened and the time it was recorded: a log entry made at the end of a shift may describe events from several hours earlier.

Digital records. Computers, phones, servers, vehicles and payment systems record time stamps for files, messages, logins, transactions and sensor readings. These can be extremely precise, but their accuracy depends on the device's clock, its time zone settings and how the software records time (Carrier, 2005; Casey, 2011). File system time stamps can be changed by ordinary activity, such as copying or opening a file, and can be altered deliberately (Buchholz & Spafford, 2004).

Video and photographs. Security cameras and phones record time, but camera clocks are often wrong by minutes or hours, and different cameras in the same building may disagree. Investigators check camera clocks against a known reference and record the offset.

Physical evidence. Some physical evidence indicates time, such as the state of decomposition, the growth of plants, the setting of concrete or the weathering of a surface. Such estimates usually give ranges rather than precise times.

Reconciling clocks

When time stamps from different systems are combined, they must first be put on a common basis. Investigators check each device's clock against a reliable reference, record any offset, convert all times to a single time zone, often Coordinated Universal Time (UTC), and use an unambiguous date format. The international standard ISO 8601 provides such a format (International Organization for Standardization [ISO], 2019). Networked computers often synchronise their clocks using the Network Time Protocol (Mills, 1991), but devices that are offline, misconfigured or deliberately altered may drift far from the true time.

Schatz et al. (2006) proposed methods for establishing the reliability of time stamps in digital evidence by correlating them with other sources, such as network logs and external servers whose clocks are known to be accurate. If a computer's log shows that it received an email at 10:02, and the sending server's log shows it was sent at 10:05, the investigator knows that the computer's clock was at least three minutes slow at that time.

Building the timeline

A practical timeline records, for each event:

- **The date and time**, in a standard format and time zone, with an indication of precision (for example "about 14:00" or "14:02:37").
- **A description** of what happened.
- **The source**, such as a witness statement, document reference or log file, with enough detail for someone else to find it.
- **The reliability** of the source and of the time, including any clock correction applied.
- **Links** to related events, such as cause and effect.

Spreadsheets and dedicated software help when there are many events. In digital forensics, "super timelines" combine time stamps from many sources, such as file systems, browser histories, event logs and application records, into a single sequence, which can contain millions of entries. Hargreaves and Patterson (2012) described methods for automatically reconstructing higher-level events, such as "user opened a document" or "program was installed", from these low-level time stamps, making the timeline easier to interpret. Chabot et al. (2014) proposed a formal model for representing timeline events and their relationships to support automated reasoning.

Analysing the timeline

Once built, the timeline is analysed for several features.

Sequence. Does the order of events make sense? Could the alleged cause have preceded the effect? A message cannot be answered before it is sent; a person cannot be in two places at once.

Gaps. Are there periods with no information? Gaps may be innocent, or they may point to missing evidence, deleted records or events that someone has not disclosed.

Clusters. Do events concentrate at particular times? A burst of activity just before a deadline, or immediately after a meeting, may indicate cause or coordination.

Contradictions. Where sources disagree, the investigator must decide which is more reliable, or whether both can be reconciled, for example by a clock offset.

Fit with hypotheses. Each competing explanation implies a timeline. An explanation that requires impossible timings, or that leaves important events unexplained, is weakened.

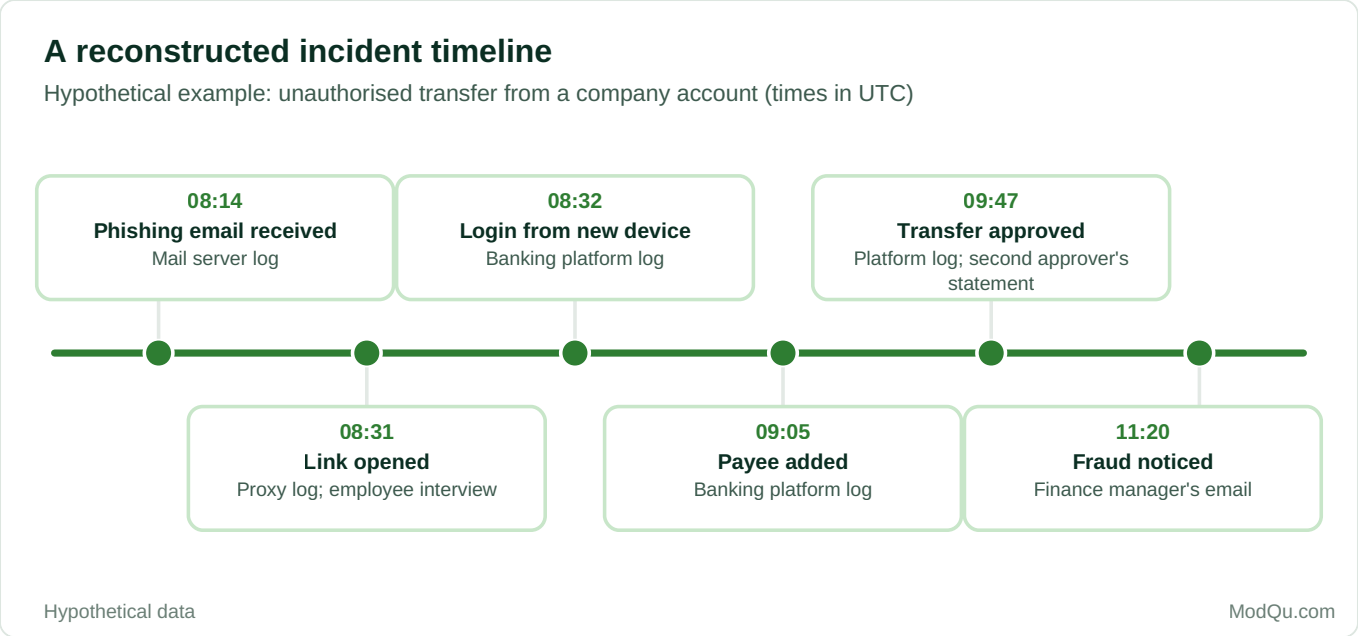


Figure 2. A simplified timeline combining logs, emails and interviews. The 33 minutes between adding the payee and approving the transfer is a key period to examine, because a second approver should have checked the new payee. Diagram by ModQu.

Handling uncertainty

Many events cannot be timed precisely. A witness may say that something happened "in the afternoon", a document may carry only a date, and a physical clue may give a range of several hours. Rather than forcing such events onto a single point, investigators can record them as intervals, with the earliest and latest possible times. Intervals can then be narrowed by reasoning from other events. If a witness saw a door open "some time after lunch", and a security log shows that the door was locked at 15:10 and not unlocked again, the opening must have occurred before 15:10. Such reasoning, applied systematically, can turn vague estimates into useful constraints.

It is equally important to show uncertainty when presenting a timeline. A chart that places every event on a precise point implies a certainty the evidence may not support. Showing ranges as bars, marking approximate times clearly, and noting where times rest on a single source allow readers to judge the timeline's strength for themselves. When the order of two events is critical to a conclusion, the investigator should state explicitly how confident they are in that order and why.

Timelines and interviews

Timelines are also useful during interviews. A draft timeline helps the interviewer identify which periods need to be covered, which accounts conflict and which details could confirm or challenge a witness's account. It should, however, be used carefully. Showing a witness the investigator's timeline, or suggesting times, can contaminate the witness's memory and lead them to adopt details they did not remember. A better approach is to let witnesses give their own

account first, ask them to link events to landmarks they remember, such as a phone call, a meal or a news broadcast, and only then compare their account with the timeline (Loftus & Marburger, 1983). Discrepancies can then be explored openly, without assuming that the witness or the record is the one in error.

Common errors

Timeline analysis can go wrong in several ways.

Clock and format errors. Mixing time zones, misreading date formats (is 03/04 the third of April or the fourth of March?), ignoring daylight saving changes and failing to correct clock offsets are among the most frequent technical errors. A single uncorrected offset can reverse the apparent order of events.

Treating recorded time as event time. A database may record when a transaction was processed rather than when it was requested; a document's "modified" time may reflect when it was copied rather than when it was written.

Overconfidence in precision. Precise-looking times from unreliable sources can give a false impression of certainty. Witness estimates in particular should be recorded as approximate.

Hindsight bias. Once the outcome is known, earlier events can appear to point clearly towards it. Fischhoff (1975) showed that people who know an outcome overestimate how predictable it was. In accident and incident investigation, Dekker (2014) and Woods et al. (2010) warn that hindsight leads investigators to judge people's actions by information they did not have at the time. A timeline should record what each person knew and when, not only what happened.

Confirmation bias. Investigators who already favour an explanation may give more weight to times that fit it and explain away those that do not. Recording the source and reliability of every time, and actively looking for events that contradict the favoured explanation, helps guard against this (Heuer & Pherson, 2015).

Landmark reconstructions

Some of the most important investigations of recent decades have been, in large part, exercises in timeline reconstruction. The 9/11 Commission reconstructed the hijackers' preparations and the events of 11 September 2001 minute by minute, using flight data, radar, air traffic control recordings, telephone records and interviews, and used the timeline to show where opportunities to detect or respond to the attacks had been missed (National Commission on Terrorist Attacks Upon the United States, 2004). The investigation into the loss of Air France flight 447 reconstructed the final minutes of the flight second by second from the flight recorders, revealing how the crew responded to a sequence of failures and alarms (Bureau d'Enquêtes et d'Analyses [BEA], 2012).

The Hillsborough Independent Panel examined hundreds of thousands of documents relating to the 1989 disaster at a football stadium in Sheffield, in which 97 people died. By reconstructing the sequence of events and comparing original statements with later amended versions, the panel showed that police statements had been altered and that the official account had wrongly blamed supporters (Hillsborough Independent Panel, 2012). Its work demonstrates how a careful timeline, built from original sources, can overturn a long-accepted narrative.

Keeping the timeline current

A timeline is a working document, not a one-off product. New evidence arrives throughout an investigation: a further log is recovered, a witness corrects an earlier estimate, a clock offset is discovered. Each change should be recorded with the date it was made and the reason, so that earlier versions of the analysis can be reconstructed if needed. This matters especially when findings are challenged later, because the investigator may need to show what was known at each stage and how conclusions changed. Version control, whether in specialised software or simply in dated copies of a spreadsheet, provides this record and supports the reproducibility of the investigation.

Presenting timelines

Timelines are among the clearest ways to present investigative findings. Good presentations show the key events, indicate the source and reliability of each, highlight gaps and contradictions, and avoid crowding the reader with irrelevant detail. For complex investigations, a summary timeline of key events can be supported by a detailed appendix. Graphical timelines, such as horizontal charts with parallel lanes for different people or systems, help readers see how events in different places relate.

A short example

The following hypothetical case illustrates the method. A company discovers that €85,000 has been transferred from its account to an unknown payee. The finance manager suspects an employee in the accounts team.

The investigator gathers the bank platform's logs, the company's email server logs, the web proxy logs, the employees' calendars and statements from the people involved. All times are converted to UTC, and the clocks of the email server and proxy are checked against an external reference; the proxy's clock is found to be 90 seconds fast and is corrected.

The timeline shows that at 08:14 a phishing email arrived in the accounts employee's inbox; at 08:31 the employee clicked the link; and one minute later the banking platform recorded a login with the employee's credentials from a new device in another country. At 09:05 that session added a new payee, and at 09:47 the second approver, a manager, approved a transfer to that payee. The manager's calendar shows that she was in a meeting from 09:30 to 10:30, and her statement explains that she approved the transfer on her phone during the meeting because the request appeared routine.

The timeline does not support the suspicion of the accounts employee, whose actions are consistent with having been deceived by the phishing email, and who was at a desk in the office at the time of the foreign login. It identifies two weaknesses: the platform allowed a new device to log in without additional verification, and the approval process did not prompt the approver to check new payees. The company's report recommends changes to both.

Conclusion

Timeline analysis brings order to the evidence of an investigation by placing events in sequence and in time. It draws on witnesses, documents, digital records, video and physical evidence, each with its own precision and risks, and it requires careful reconciliation of clocks and formats. Analysed well, a timeline reveals gaps, contradictions and impossible

sequences, and allows competing explanations to be tested against the facts. Its main dangers are technical errors, false precision and the biases that come from knowing the outcome. Built from original sources, with the source and reliability of each entry recorded, a timeline is one of the most reliable tools an investigator has for reconstructing what really happened.

References

Buchholz, F., & Spafford, E. (2004). On the role of file system metadata in digital forensics. *Digital Investigation, 1*(4), 298–309. https://doi.org/10.1016/j.diin.2004.10.002

Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile. (2012). *Final report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro–Paris*. BEA.

Carrier, B. (2005). *File system forensic analysis*. Addison-Wesley.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet* (3rd ed.). Academic Press.

Chabot, Y., Bertaux, A., Nicolle, C., & Kechadi, M.-T. (2014). A complete formalized knowledge representation model for advanced digital forensics timeline analysis. *Digital Investigation, 11*(Suppl. 2), S95–S105. https://doi.org/10.1016/j.diin.2014.05.009

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Dekker, S. (2014). *The field guide to understanding 'human error'* (3rd ed.). Ashgate.

Fischhoff, B. (1975). Hindsight ≠ foresight: The effect of outcome knowledge on judgment under uncertainty. *Journal of Experimental Psychology: Human Perception and Performance, 1*(3), 288–299. https://doi.org/10.1037/0096-1523.1.3.288

Friedman, W. J. (1993). Memory for the time of past events. *Psychological Bulletin, 113*(1), 44–66. https://doi.org/10.1037/0033-2909.113.1.44

Hargreaves, C., & Patterson, J. (2012). An automated timeline reconstruction approach for digital forensic investigations. *Digital Investigation, 9*(Suppl.), S69–S79. https://doi.org/10.1016/j.diin.2012.05.008

Heuer, R. J., Jr., & Pherson, R. H. (2015). *Structured analytic techniques for intelligence analysis* (2nd ed.). CQ Press.

Hillsborough Independent Panel. (2012). *Hillsborough: The report of the Hillsborough Independent Panel* (HC 581). The Stationery Office.

Hunter, M. L., Hanson, N., Sabbagh, R., Sengers, L., Sullivan, D., & Svith, F. T. (2011). *Story-based inquiry: A manual for investigative journalists*. UNESCO.

International Organization for Standardization. (2019). *Date and time — Representations for information interchange — Part 1: Basic rules* (ISO Standard No. 8601-1:2019).

Loftus, E. F., & Marburger, W. (1983). Since the eruption of Mt. St. Helens, has anyone beaten you up? Improving the accuracy of retrospective reports with landmark events. *Memory & Cognition, 11*(2), 114–120. https://doi.org/10.3758/BF03213465

Mills, D. L. (1991). Internet time synchronization: The network time protocol. *IEEE Transactions on Communications, 39*(10), 1482–1493. https://doi.org/10.1109/26.103043

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission report*. W. W. Norton.

Neter, J., & Waksberg, J. (1964). A study of response errors in expenditures data from household interviews. *Journal of the American Statistical Association, 59*(305), 18–55. https://doi.org/10.1080/01621459.1964.10480699

Pennington, N., & Hastie, R. (1992). Explaining the evidence: Tests of the story model for juror decision making. *Journal of Personality and Social Psychology, 62*(2), 189–206. https://doi.org/10.1037/0022-3514.62.2.189

Schatz, B., Mohay, G., & Clark, A. (2006). A correlation method for establishing provenance of timestamps in digital evidence. *Digital Investigation, 3*(Suppl.), 98–107. https://doi.org/10.1016/j.diin.2006.06.009

Stelfox, P. (2009). *Criminal investigation: An introduction to principles and practice*. Willan.

Tong, S., Bryant, R. P., & Horvath, M. A. H. (2009). *Understanding criminal investigation*. Wiley-Blackwell.

Wagenaar, W. A., van Koppen, P. J., & Crombag, H. F. M. (1993). *Anchored narratives: The psychology of criminal evidence*. Harvester Wheatsheaf.

Woods, D. D., Dekker, S., Cook, R., Johannesen, L., & Sarter, N. (2010). *Behind human error* (2nd ed.). Ashgate.