



START FREE TRIAL

# Timeline Analysis for Incident Response

When a forensics team is called to investigate, one of the most important techniques they can deploy is to create a timeline of the events. The breach is often the result of several different failures or weaknesses and the timeline allows investigators to gather all of the evidence in a single chart.

Collecting all of the details in one coherent data structure can improve analysis. While some breaches have obvious causes, some can only be understood after all of the failures can be analyzed together. Timelines make it easier to understand causality and the relationships between the many moving parts of a modern enterprise stack.

The timelines can also be essential for legal responses. When a firm wants to contact law enforcement or start its own legal proceedings, a solid timeline can explain what happened to the lawyers, judges and juries.

The approach can also help teams work together and synchronize their often disparate roles. The timeline brings all of their work together in one consistent data model. Each part of the team can work independently yet understand the larger picture.

All of these reasons make constructing a thorough timeline essential for any forensic team. It should be the first responsibility when an investigation begins.

## How to gather evidence for your timeline



START FREE TRIAL

Investigators must also take into account the severity of the incident and the need for the best possible evidence. If the consequences are severe or there is a strong demand for a thorough investigation, then the best physical isolation of the systems is essential. Shutting them down and taking the purest image of the drives is essential.

If the demand is not as high or there would be too much loss caused by shutting down the system, then the information from the data on the system may be collected by copying the essential log files.

Some of the best tools for gathering essential data are open source packages like [Autopsy](#) or professional tools like [CyberTriage](#). Both can capture complete images of computer systems and analyze them to determine the extent of any cyber attack.

Try Cyber Triage's timeline analysis [for free today](#).

## Log files: A valuable source of information

Operating systems and software packages regularly record data during operations to help with debugging and generate statistics about usage to help tune performance. These log files are often invaluable sources of information for constructing the timelines of an attack.

The entries in log files are usually coded with the time of the event. The Firewall logs, for instance, record when someone, perhaps the attacker, unsuccessful attempts to enter your network. The database logs track when data was added or changed and may even record when someone asked for copies. These can make a rich collection of detail to include in any timeline.

Some of the most useful log files are:

- Operating System Event Logs: Many of the common household chores, like scanning the disk for viruses or auditing many services, are recorded in the logs of the operating system. Some errors, like a full disk or a failed IO process, can also offer useful clues.
- Applications Logs: Some application packages also maintain their own logs to track errors or common usage patterns.



START FREE TRIAL

- IDS/IPS Logs: Special intrusion detection and prevention systems (IDS/IPS) can detect and follow malicious traffic. Their logs are especially valuable – if the attacker hasn't evaded the systems.
- Web Server Logs: When the attack targets a web presence, the logs of the web server can reveal the time and type of attack.  
Database Logs: Database logs reveal queries have been run against your database, as well as the IP addresses of the users who ran them. This shows what data the attacker wanted to access.

## Other clues that can help you build a timeline

The log files aren't the only source of information. Some attacks against some systems can produce useful information, either directly or indirectly.

The direct information is the most obvious. Some systems will generate warning emails or pages when something suspicious or problematic happens. For example, if the file system gets too full, some servers send out a warning. The same happens for a suspicious login.

Indirect evidence can be more subtle but it can be just as useful. The performance may start to degrade during an attack and so any complaints from users about the slow or non-existent services can be a good indicator. If the attack is using the network to move large blocks of data, timed out services will indicate that something was happening.

Time stamps on some files can also be useful. If an attacker changes the permissions on a file to gain access, this will be recorded in the last time the file was written. Some files that are normally inconsequential may have timestamps that were changed during the attack.

Sometimes the best time estimates come from events that didn't happen just like the dog barking that didn't happen in Sherlock Holmes's tale, "The Hound of the Baskervilles." Did the regular crontab email alerts not go out? Was the cache not rebuilt in the middle of the night? Did the backups fail? All can indicate that



START FREE TRIAL

When a timeline is finished, extracting insights is a mixture of simple and sophisticated analysis. Some events are obvious. An entry in the network logs showing a large block of data was exfiltrated at 2am is probably evidence that the cyberattacker took sensitive information. A non-standard query for personal information that's in the database logs is pretty clear evidence that someone was searching for personal data.

Other parts of the analysis require deeper understanding of the operating system and how cyberattackers may function. Details like changes in the access permissions for certain files may be small parts of a trail of clues. The incident response team can use their domain skills to identify the type of attack and the probable extent.

The analysis can reveal what data was compromised and how it was done. The first part can guide any response to what's already happened. The second part is a guide for fixing the system to prevent future attacks.

## What specific insights can a timeline reveal?

Each timeline is as different as each attack but there are some facts that a well-constructed timeline can deliver. Some of the most common insights are:

1. Start of the attack – This is the first moment that the attackers began exploring your system. This is very useful for establishing what data might be exposed. Data that was known to be on the system before this moment is vulnerable.
2. End of the attack – When was the last time that the attacker successfully entered the system? Any data created after this moment can't be revealed in this attack.
3. Amount of data that was exfiltrated – When the network logs show that only a few thousand bytes were delivered to the attacker, then large files were not removed in their entirety. The attacker, though, may have looked up individual records or small sections.
4. The systems that were affected. If the details show that all of the attack was concentrated on one isolated system, then only that data on that system is of concern.



START FREE TRIAL

## forged.)

Timeline analysis is not necessarily perfect. It depends on the quality and reliability of any data. In many cases, the information gathered from the log files and other sources is completely reliable, but it can't always be guaranteed. Some attackers are able to gain enough access to also edit the log files and destroy any evidence of their attack.

Good system security makes this more difficult. If the details from the log files are stored on an isolated system without general access, the chances an attacker was able to edit them is much smaller. Still, it can't be completely ruled out.

A thorough timeline analysis takes note of the possibility that the data was either corrupted accidentally or edited deliberately. This can guide anyone using the timeline analysis to make a decision.

## How can a timeline be used in legal proceedings?

If an incident proves to be serious enough to require involving the court system, the timeline can be a useful tool for convincing police investigators, prosecutors and ultimately the judge and jury members. The timeline arranges the events in a simple chronological order that makes it easier to understand.

Skilled forensic scientists understand some of the best techniques for enhancing the value of a timeline in legal proceedings. They can extract disk images and create digital signatures at the beginning to ensure that the data was not changed. This provides a strong chain of control that allows the opposing team a chance to examine and challenge the evidence fairly.

Each of the moments in the timeline can be made stronger with better evidence collection and preservation. Tools like [Autopsy](#) and [CyberTriage](#) are designed to support investigations, both through careful curation of evidence, and also by providing a central repository of hash function values for known dangerous files.

[START FREE TRIAL](#)

security. When the investigation establishes how a breach may have occurred, the team should change procedures and improve technological barriers to prevent something similar happening in the future.

What can't be found on the timeline can also be helpful. If it's impossible to reconstruct some details because of poor record keeping, non-existent log files, or gaps in the record, the holes in the timeline can be an impetus to improve. If there's not enough known, it can motivate investing in new systems that monitor the network, the databases or other critical infrastructure.

## What are the Key Takeaways for IT Leadership?

- Develop a plan to move quickly to assemble a timeline after discovering an incident has occurred.
- Install a solid foundation for creating any timeline by investing in logging and detection technology.
- Invest in training for using forensic technology in order to speed the response immediately after the incident.

FEATURES	BENEFITS	COMPANY
Workflow	Overview	About
Collect	Internal IR	Blog
Prioritize	Consultants	Contact
Recommend	Law Enforcement	Webinars
Collaborate	Pricing	Videos
Versions		Try Cyber Triage
Integrations		

[Platform ▾](#)   [Use Cases ▾](#)   [Pricing ▾](#)**CYBER TRIAGE**[Resources ▾](#)[About ▾](#)[START FREE TRIAL](#)