# Digital Forensic Timeline Report

This report summarizes the SSH-related system activity captured and processed by the Digital Forensic Timeline Builder. The source data originates from SSH log entries on the Kali Linux system and has been normalized into a chronological event timeline.

**Total events:** 193
**First event:** 2025-08-05 09:52:40
**Last event:** 2025-11-21 13:42:40

## Methodology

Log entries were collected from the SSH logging source on the Kali Linux virtual machine and written to a text file. Each line was parsed to extract the timestamp, host, and message fields. Timestamps were converted to a consistent datetime format and sorted chronologically. The resulting normalized records were stored in a CSV file (*ssh_timeline.csv*), which serves as the basis for this report.

## Sample Timeline Entries

| Datetime | Host | Message |
|---|---|---|
| 2025-08-05 09:52:40 | kali | systemd[1]: regenerate-ssh-host-keys.service - Regenerate SSH host keys was skip |
| 2025-08-05 09:52:43 | kali | systemd[659]: Starting gcr-ssh-agent.socket - GCR ssh-agent wrapper... |
| 2025-08-05 09:52:43 | kali | systemd[659]: Starting gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-age |
| 2025-08-05 09:52:43 | kali | systemd[659]: Starting ssh-agent.socket - OpenSSH Agent socket... |
| 2025-08-05 09:52:43 | kali | systemd[659]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper. |
| 2025-08-05 09:52:43 | kali | systemd[659]: Listening on ssh-agent.socket - OpenSSH Agent socket. |
| 2025-08-05 09:52:43 | kali | systemd[659]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh |
| 2025-08-05 10:12:17 | kali | systemd[841]: Starting gcr-ssh-agent.socket - GCR ssh-agent wrapper... |
| 2025-08-05 10:12:17 | kali | systemd[841]: Starting gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-age |
| 2025-08-05 10:12:17 | kali | systemd[841]: Starting ssh-agent.socket - OpenSSH Agent socket... |
| 2025-08-05 10:12:17 | kali | systemd[841]: Listening on gcr-ssh-agent.socket - GCR ssh-agent wrapper. |
| 2025-08-05 10:12:17 | kali | systemd[841]: Listening on gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh |
| 2025-08-05 10:12:17 | kali | systemd[841]: Listening on ssh-agent.socket - OpenSSH Agent socket. |
| 2025-08-05 10:12:18 | kali | gpg-agent[989]: using fd 4 for ssh socket (/run/user/1000/gnupg/S.gpg-agent.ssh) |
| 2025-08-05 10:12:18 | kali | gpg-agent[989]: listening on: std=3 extra=5 browser=6 ssh=4 |
| 2025-08-05 10:12:18 | kali | gpg-agent[994]: using fd 4 for ssh socket (/run/user/1000/gnupg/S.gpg-agent.ssh) |
| 2025-08-05 10:12:18 | kali | gpg-agent[994]: listening on: std=3 extra=5 browser=6 ssh=4 |
| 2025-08-05 10:12:27 | kali | systemd[659]: Closed gcr-ssh-agent.socket - GCR ssh-agent wrapper. |
| 2025-08-05 10:12:27 | kali | systemd[659]: Stopping gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-age |
| 2025-08-05 10:12:27 | kali | systemd[659]: Stopping ssh-agent.socket - OpenSSH Agent socket... |
| 2025-08-05 10:12:27 | kali | systemd[659]: Closed gpg-agent-ssh.socket - GnuPG cryptographic agent (ssh-agent |
| 2025-08-05 10:12:27 | kali | systemd[659]: Closed ssh-agent.socket - OpenSSH Agent socket. |

| | | |
|---|---|---|
| 2025-08-05 14:37:59 | kali | systemd[1]: Listening on sshd-unix-local.socket - OpenSSH Server Socket (systemd |
| 2025-08-05 14:37:59 | kali | systemd[1]: Listening on sshd-vsock.socket - OpenSSH Server Socket (systemd-ssh- |
| 2025-08-05 14:37:59 | kali | systemd[1]: Reached target ssh-access.target - SSH Access Available. |

## Findings and Observations

The timeline shows the sequence of SSH-related events in the system, including authentication attempts and general SSH daemon activity. By reviewing the timestamps and messages, an analyst can identify patterns such as repeated failed login attempts, unusual login times, or bursts of activity that may warrant further investigation.