Traveling in time
from past to future
Time travel

- Ideally, a Frankenstein-like experiment.
- Reconstruct sequences of past events.
- Correlate information from different sources.
- Time machine - a look into the future.
who - active user snapshot

- Username.
- Terminal (or window).
- Start of session.
- Origin if remote (often truncated, easily masked).

```
% who
wietse    console    Jul 25 15:05    (:0)
wietse    pts/1      Jul 28 19:59    (beukel.porcupine.org)
wietse    pts/5      Jul 25 15:06
```

- Files: /etc/utmp, /var/run/utmp, /var/adm/utmp(x).
  Easy to forge, easy to unremove.
last - past login activity

- Username.
- Terminal (or window).
- Session start/end/duration.
- Origin if remote (often truncated).
- Logout times scatter, making output hard to interpret.

```
% last
  dbtpto   tty03   SVRC05  Thu Feb 21 12:48 - 12:52  (00:03)
tgtawb   tty02   SVRC05  Thu Feb 21 12:44   still logged in
rcsamw   :0                   Thu Feb 21 12:29 - 13:13  (00:44)
```

- Files: /var/adm/wtmp, /var/log/wtmp, /var/adm/wtmpx.
  Easy to forge, easy to unremove.
lastlog - time of last login

- One entry per user, indexed by numerical userid.
- Terminal port.
- Time of login.
- Origin if remote (often truncated).


- Files: /var/adm/lastlog, /var/log/lastlog.
  Easy to forge, hard to unremove.
## Login/time correlations

### What users had access to the system around 13:15?

<table>
<thead>
<tr>
<th>User</th>
<th>Terminal</th>
<th>Host</th>
<th>Date/Time</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>wmsorrng</td>
<td>tty06</td>
<td>SVRC05</td>
<td>Wed Feb 20 12:58 - 13:24</td>
<td>(00:25)</td>
</tr>
<tr>
<td>rcbajvl</td>
<td>tty05</td>
<td>SVRC05</td>
<td>Wed Feb 20 12:30 - 13:34</td>
<td>(01:04)</td>
</tr>
<tr>
<td>bdbert</td>
<td>tty03</td>
<td>SVRC05</td>
<td>Wed Feb 20 12:26 - 13:27</td>
<td>(01:01)</td>
</tr>
<tr>
<td>rcstack</td>
<td>tty02</td>
<td>SVRC05</td>
<td>Wed Feb 20 12:19 - 13:44</td>
<td>(01:24)</td>
</tr>
<tr>
<td>rcmart</td>
<td>ttyp1</td>
<td>rwc.urc.tue.nl</td>
<td>Wed Feb 20 11:49 - 16:15</td>
<td>(04:25)</td>
</tr>
</tbody>
</table>

### What is the usage pattern of a specific account?

<table>
<thead>
<tr>
<th>User</th>
<th>Terminal</th>
<th>Host</th>
<th>Date/Time</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>wsbsym@wsinfo01</td>
<td>ttyp8</td>
<td>rw8.urc.tue.nl</td>
<td>Mon Jun 15 15:33 - down</td>
<td>(00:27)</td>
</tr>
<tr>
<td>wsbsym@wsinpa01</td>
<td>ttyp2</td>
<td>wsinfo01</td>
<td>Mon Jun 15 14:14 - 14:24</td>
<td>(00:10)</td>
</tr>
<tr>
<td>wsbsym@wsinfo01</td>
<td>ttyp8</td>
<td>wsinfo01</td>
<td>Mon Jun 15 14:11 - 14:11</td>
<td>(00:00)</td>
</tr>
<tr>
<td>wsbsym@wsinfo01</td>
<td>ttyp2</td>
<td>rw8.urc.tue.nl</td>
<td>Mon Jun 15 13:58 - 14:24</td>
<td>(00:26)</td>
</tr>
</tbody>
</table>
ps - process status snapshot

- Username.
- Terminal (or window).
- Start time.
- Memory and CPU usage.
- Command line (easily forged).
- Process status (running, sleeping, suspended, dead).
- Other utilities of interest: top, lsof (both freeware).
- Files: /vmunix, /dev/kmem, /proc
lastcomm - past process activity

- Command (easy to forge).
- Status: abnormal exit, privilege change.
- Username.
- Terminal (or window).
- CPU usage.
- Start time + elapsed time (elapsed not shown).

```
w    wsingus  ttyp9      0.61 secs Mon Mar 11 13:46
ps   wsingus  ttyp9      0.33 secs Mon Mar 11 13:46
rn   wsingus  ttyp9      1.91 secs Mon Mar 11 13:44
w    wsingus  ttyp9      0.61 secs Mon Mar 11 13:44
rm   wsingus  ttyp9      0.06 secs Mon Mar 11 13:44
```


Easy to forge records.
Process/time correlations

- All commands executed by a specific user.
- All commands within a specific login session.
- Successive instances of a (resident) process.
- (Sequences of) specific commands by any user.
- All processes running during some time window.
- Resident process started long after boot time.
tcp wrapper - network connections

- Date and time.
- Target host.
- Network process name and ID.
- Client host (optional: client user).
- Relies on connection information supplied by client.

May 20 01:04:42 tuegate: 14498 systatd: connect from litp.ibp.fr
May 20 01:10:19 tuegate: 14536 systatd: connect from monk.rutgers.edu
May 20 01:23:49 tuegate: 15040 systatd: connect from monk.rutgers.edu

May 20 13:02:45 tuegate: 27048 systatd: connect from litp.ibp.fr
May 20 14:04:51 tuegate: 27668 systatd: connect from litp.ibp.fr
May 20 14:08:53 tuewsd in.fingerd[7075]: connect from litp.ibp.fr
tcp wrapper/time correlations

- All connections from a specific site.
- All connections for specific services, for example finger and systat.
- Sequences of specific connections from any site, for example, finger followed by login attempt.
- All connections made in a specific time window.
File m/a/c times

- Significant amount of information: with $10^5$ files on a typical single-user UNIX box, 10 MBytes of data.

- If available, as easy to read as footsteps in fresh snow.
  Example: compiling a "hello world" program.
Time machine

- Correlating by time-aligning data from different sources.
- It slices and dices time into frames.
- Unification of data gathering tools.
- And you thought that SATAN+Netscape was a pig...
- Guaranteed to be Year 2000 compliant.