

Windows

Windows Events Logs

Hayabusa

- Create json from windows event logs
- Filter → Analyse in visidata

```
<source> docker run -it -v ./:data -v ./output:/output tabledevil/hayabusa
```

```
</source>
```