Windows

Windows Events Logs

Hayabusa

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

```
# in folder with evtx
# --user 1001:1001
docker run -rm -it -v ./:/data -v ./output:/output tabledevil/hayabusa
```