0. **Install sublime3** (from repo/ubuntu):

wget -qO - https://download.sublimetext.com/sublimehq-pub.gpg | sudo apt-key add -

sudo apt-get install apt-transport-https

echo "deb https://download.sublimetext.com/ apt/stable/" | sudo tee /etc/apt/sources.list.d/sublime-text.list

sudo apt-get update  
sudo apt-get install sublime-text

1. Forensics vs. IR ??!!

… SAME PROFESSION, DIFFERENT TIME CONSTRAINTS …

2. “TOOLS OF THE TRADE”

* analysis env. … (not KALI/SIFT …)
* linux shell
* fs analysis.. sleuthkit (30 linux cmd’s)
* “supertimelines” … plaso (python script)
* mem analysis.. volatility (strings)
* YARA ..
* ELK (efficient log search)
* OSquery (if we have time)