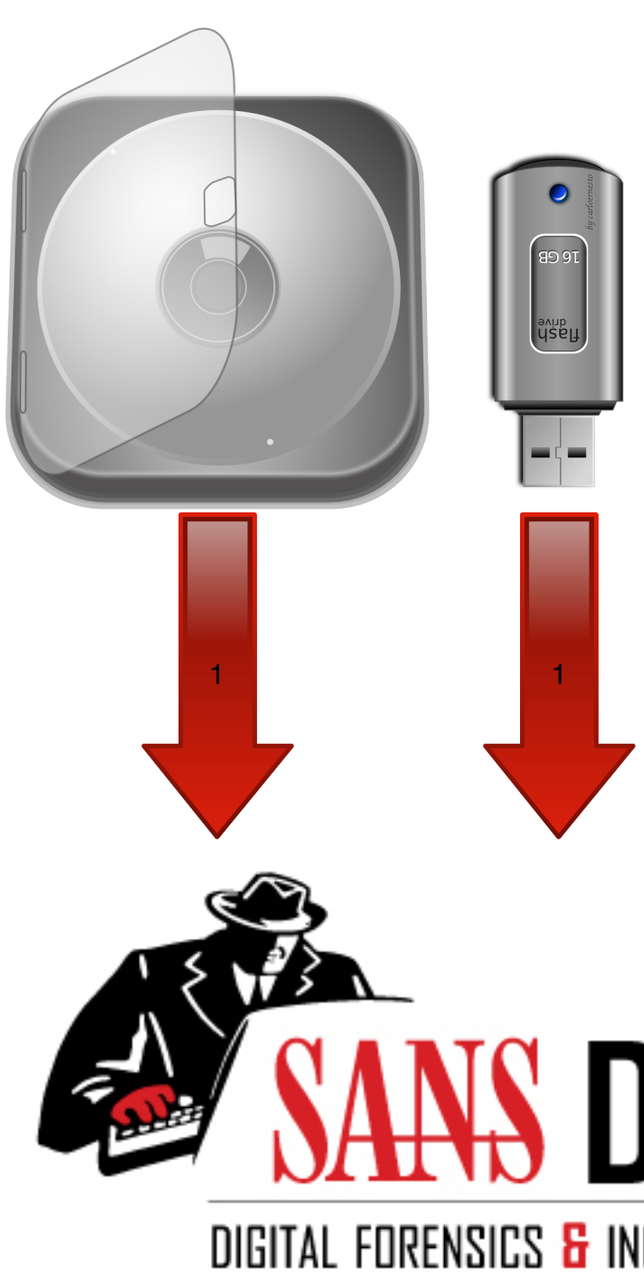
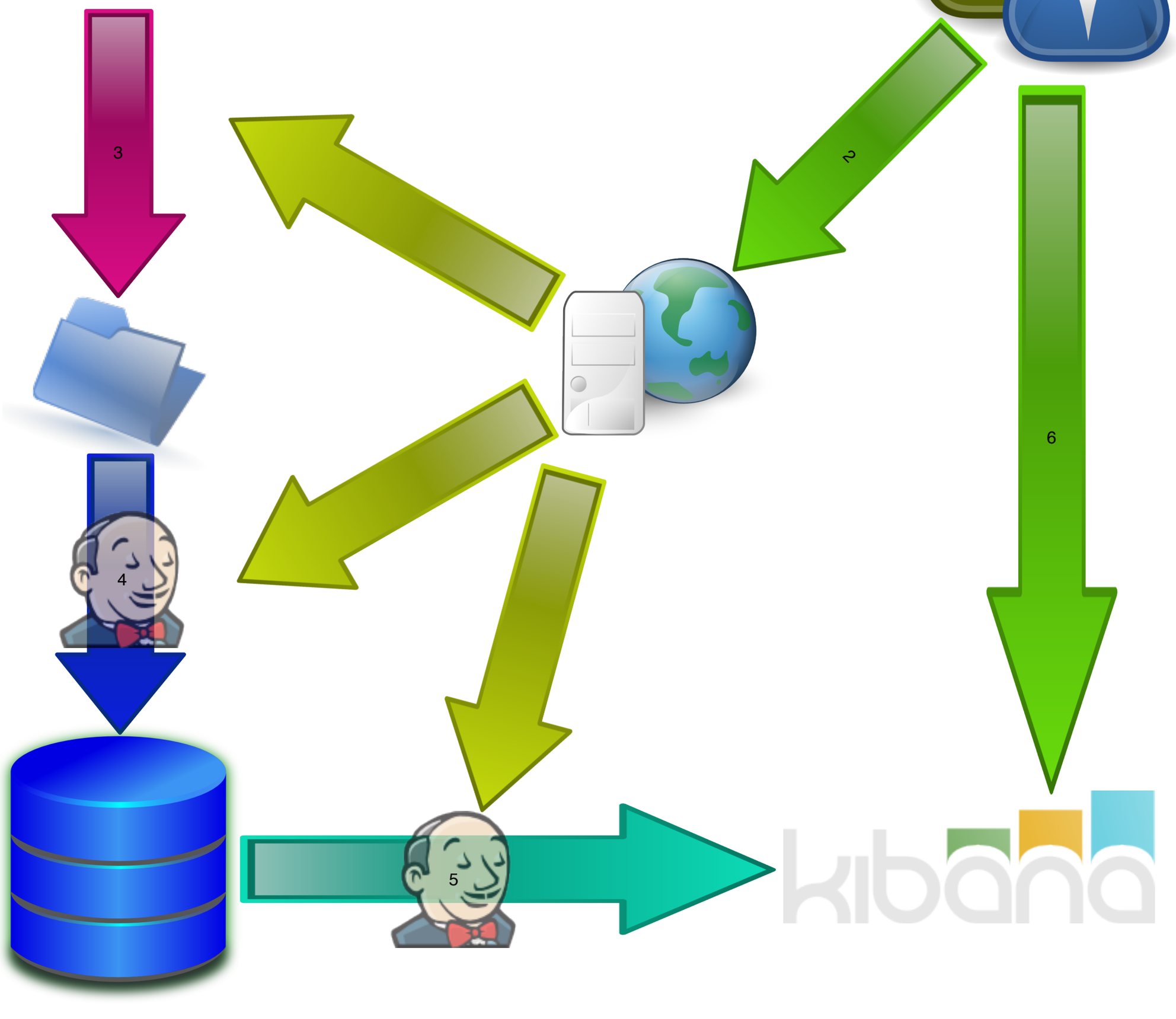


1

1

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE



kibana

1 Data is transferred onto SIFT workstation

2 SIFT user browses http://<SIFT-ip>/ffate/

3 SIFT user creates a case

4 Jenkins jobs “Find Evidence”

5 Jenkins transfers data from plaso to Elasticsearch

6 SIFT user views data in Kibana, browsing http://<ELK-ip>:9292/index.html#/dashboard/file/plaso.json