Cuckoo Sandbox

Leonardo De La Rosa

Institute for Financial Services Analytics

University of Delaware

Cuckoo Sandbox

- Automated **malware analysis** system.
- Uses **virtualization** and supports **Bare-metal** environments.

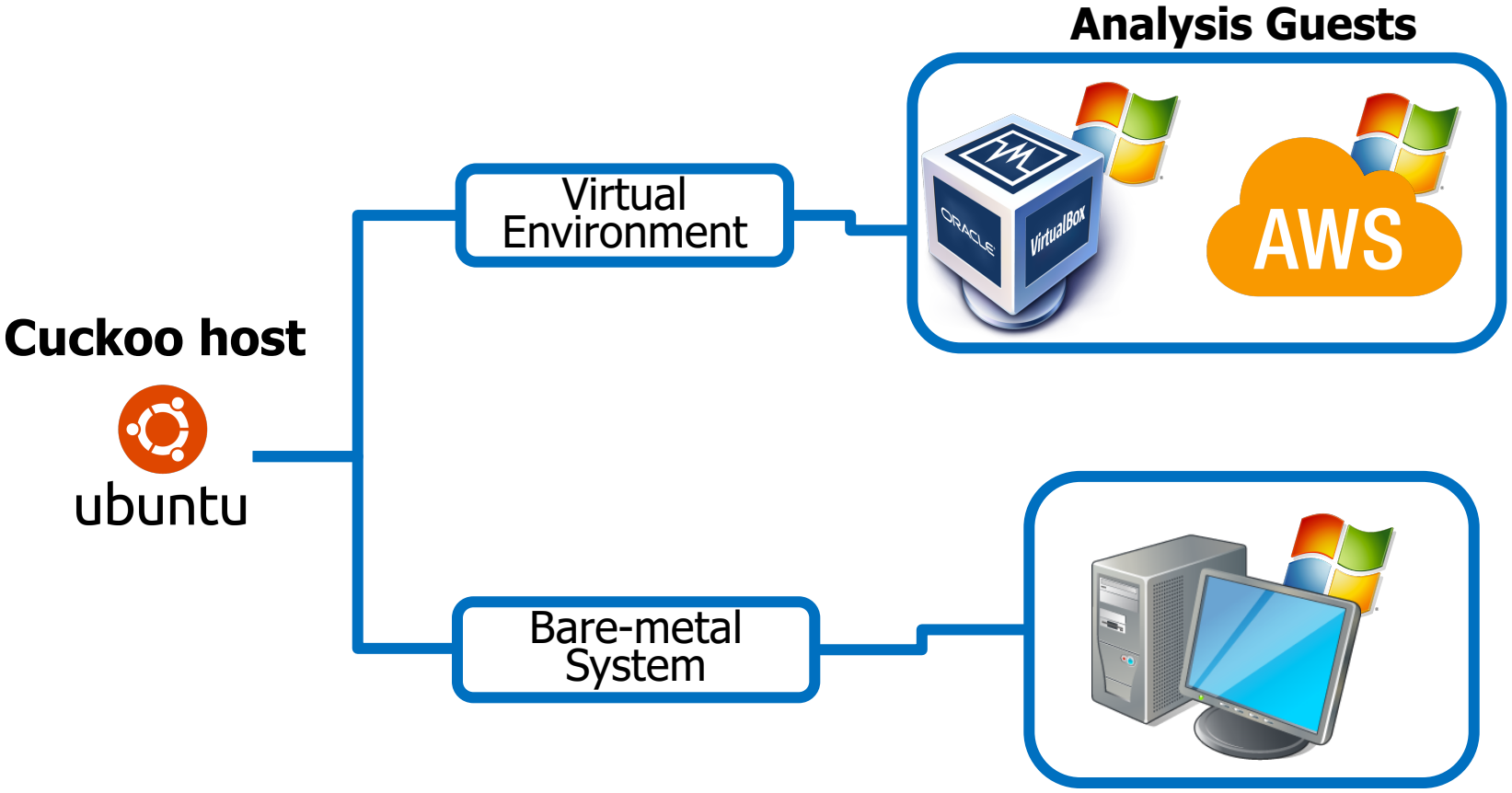
- Analyzes **different** malicious **files**.

- **Python** based. Easy to **customize.**

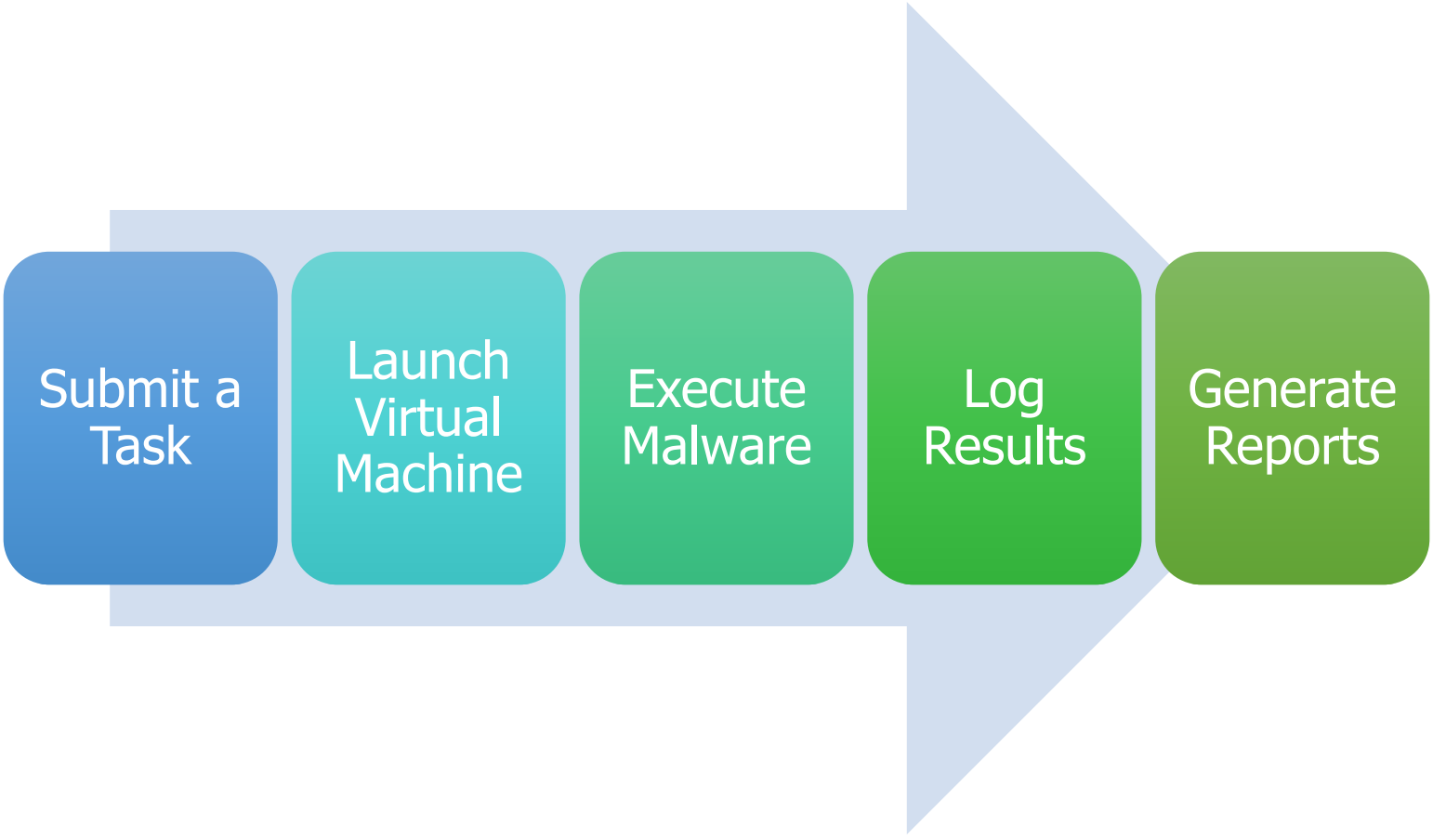
What Cuckoo can do

- Trace **API calls**.
- Generate **Behavioral** profile and **signatures.**
- Dump and analyze **Network Traffic.**
- Capture **file dumps.**
- Take **screenshots** during execution of the analysis.

Cuckoo's Architecture



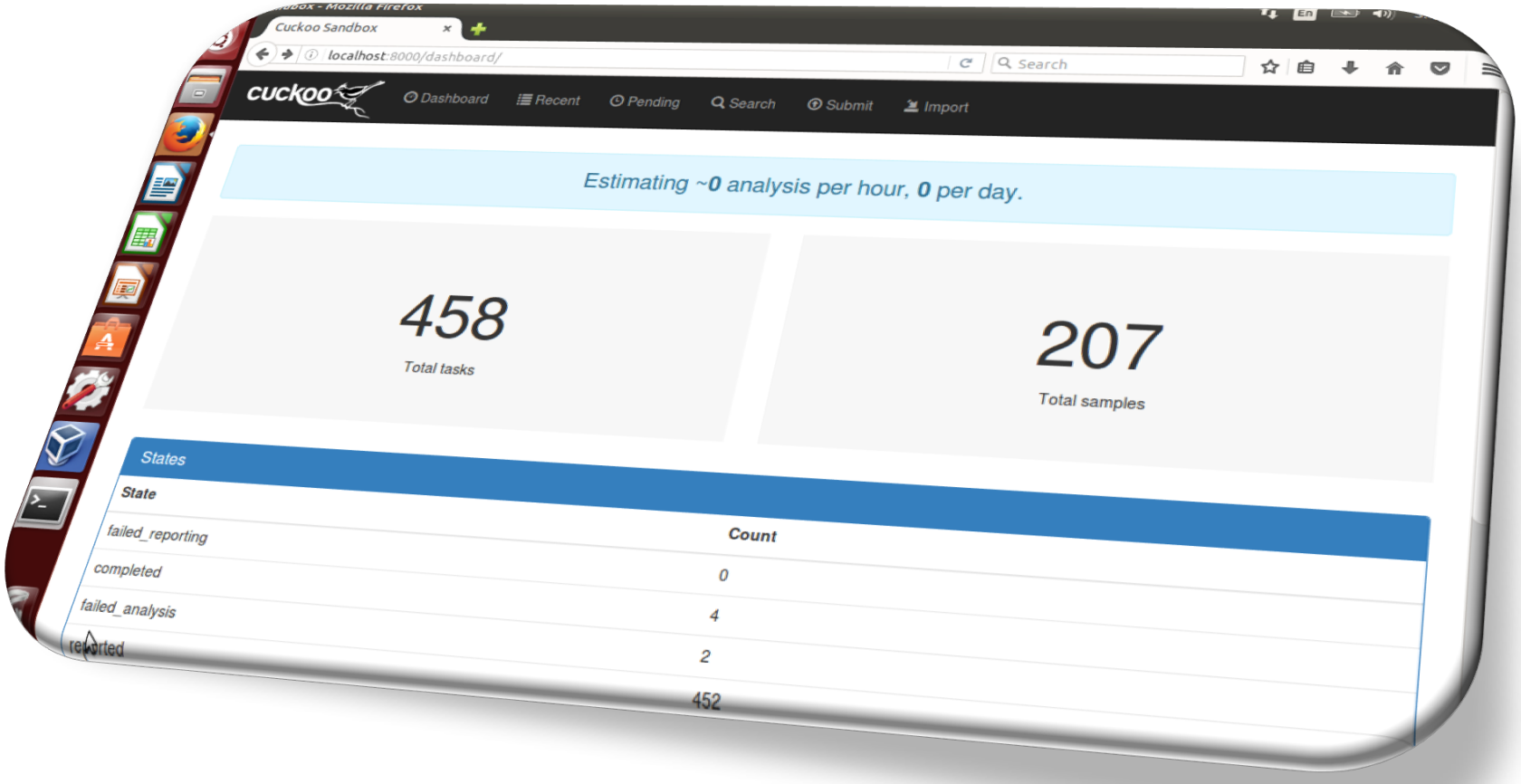
Execution Flow



Drawbacks

- Malware checks for **virtualization software:**
  - Registry keys.
  - Devices (CD-ROM, HDD).
  - Background processes.
  - IP addresses.
- **Evasive techniques:**
  - Time triggers.
  - Extended sleep.
  - User interaction.

Demo


Cuckoo Sandbox
localhost:8000/dashboard/
Search
cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Estimating ~0 analysis per hour, 0 per day.
458
Total tasks
207
Total samples
States
State
Count
failed_reporting
0
completed
4
failed_analysis
2
reported
452