2Secure

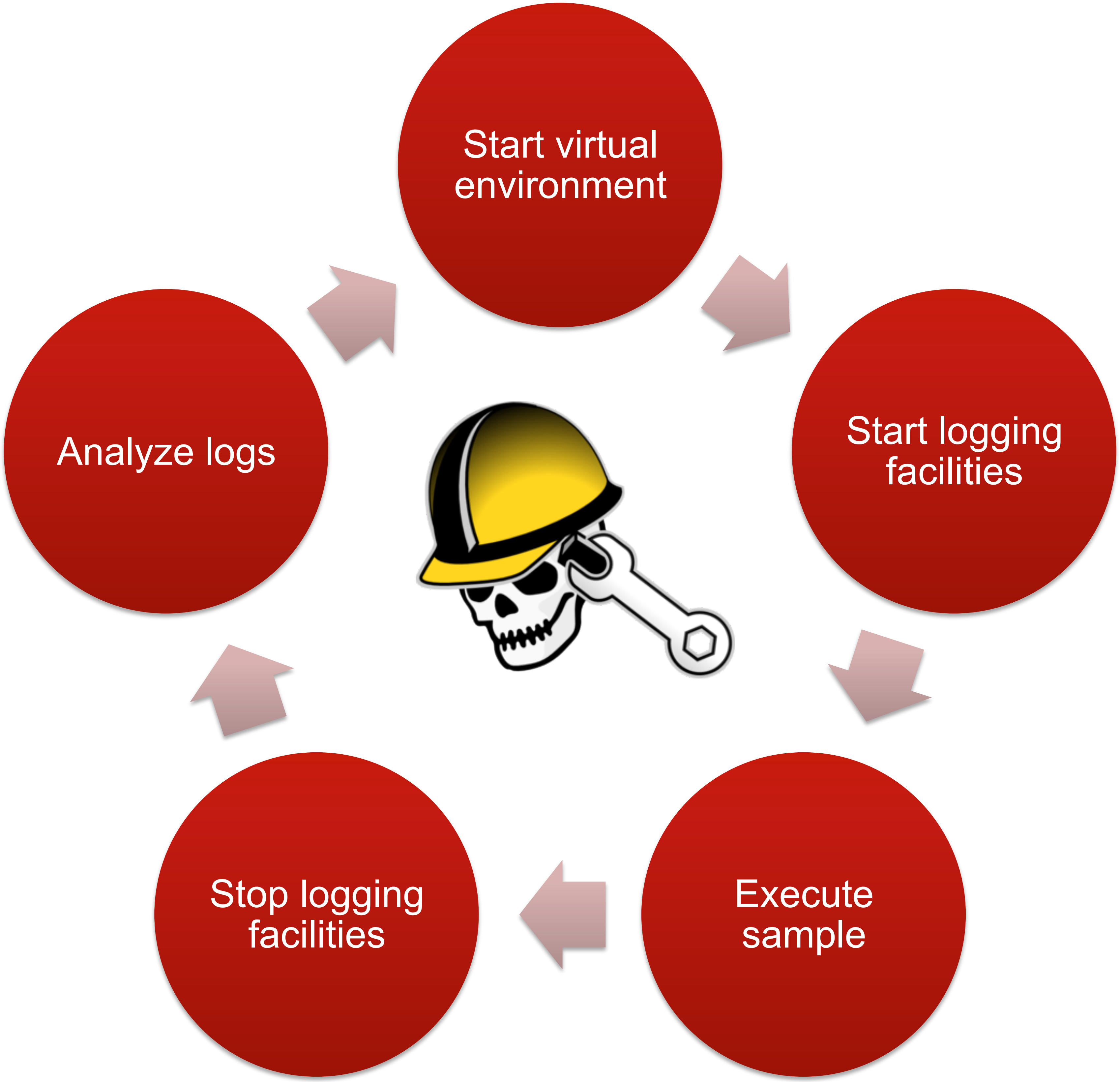
Updated

Malware Analysis on a shoe-string budget

Michael Boman - Security Consultant/Researcher, Father of 5

phillipmartin.info

Why the strange hobby?



Start virtual environment

Start logging facilities

Execute sample

Stop logging facilities

Analyze logs

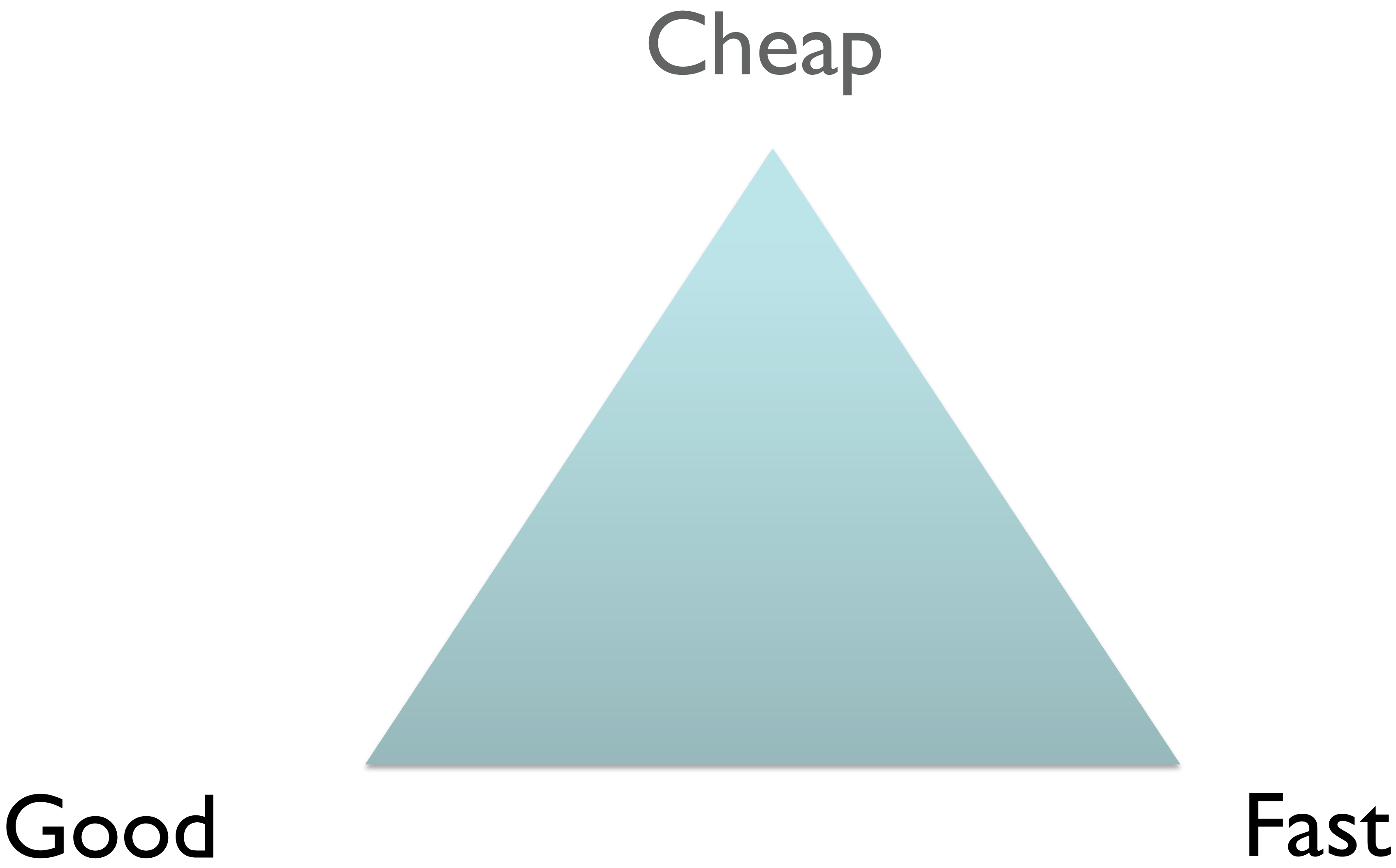
Drawbacks

- Time consuming
- Boring in the long run
  - not all malware are created equal

I don’t have time for this…

I need a (better) system!

Choose any two….

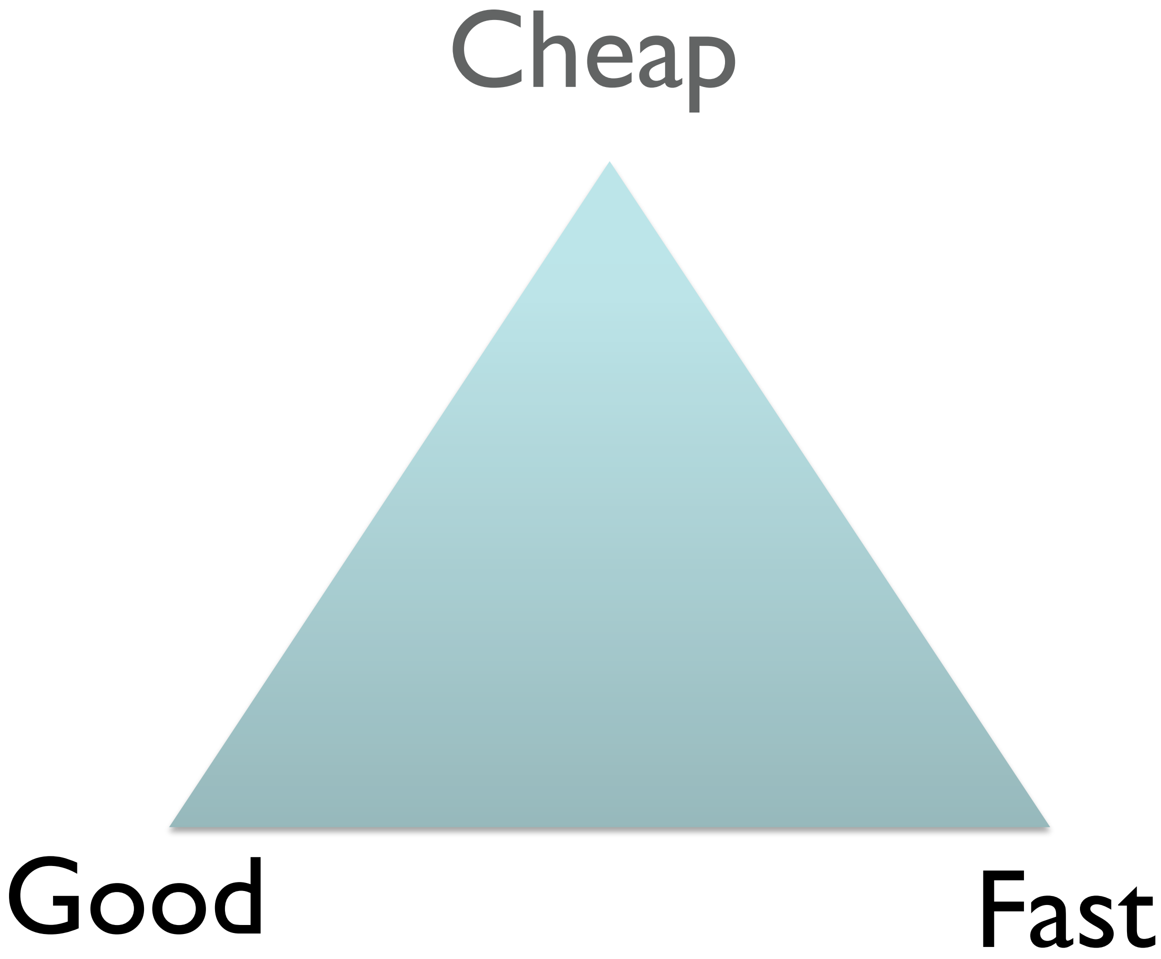


Cheap

Good

Fast

Choose any two?
Why not all of them?


Cheap

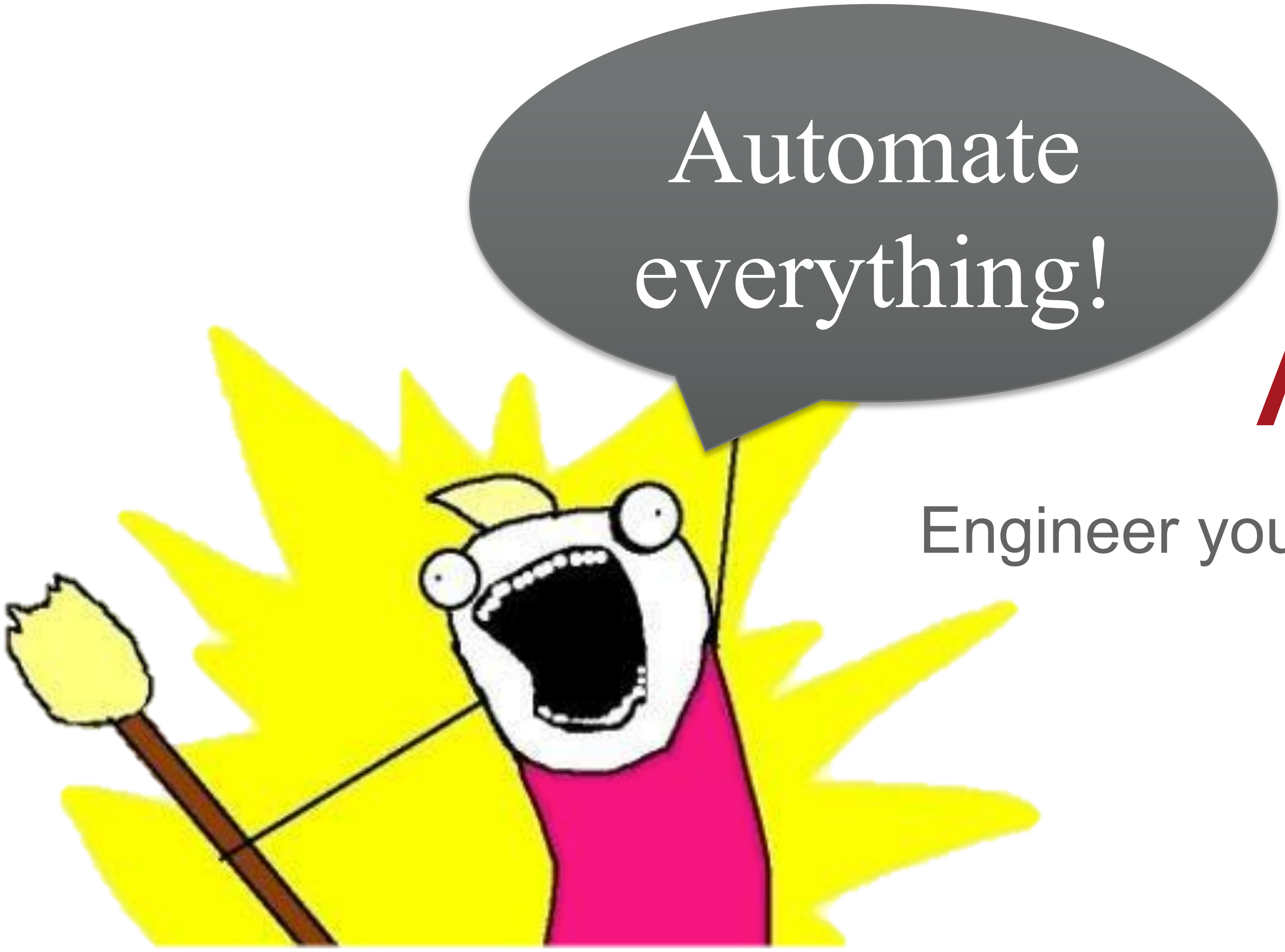
Good

Fast

I can do it **cheaply** (hardware and license cost-wise) - Human time not included.

I can do it **quickly** (I spend up to 3 hours a day doing this, at average even less). An analysis is done in less then 5 minutes…

I get **pretty good** results (quality). Where the system lacks I can compensate for its shortcomings.



Automate

Engineer yourself out of the workflow

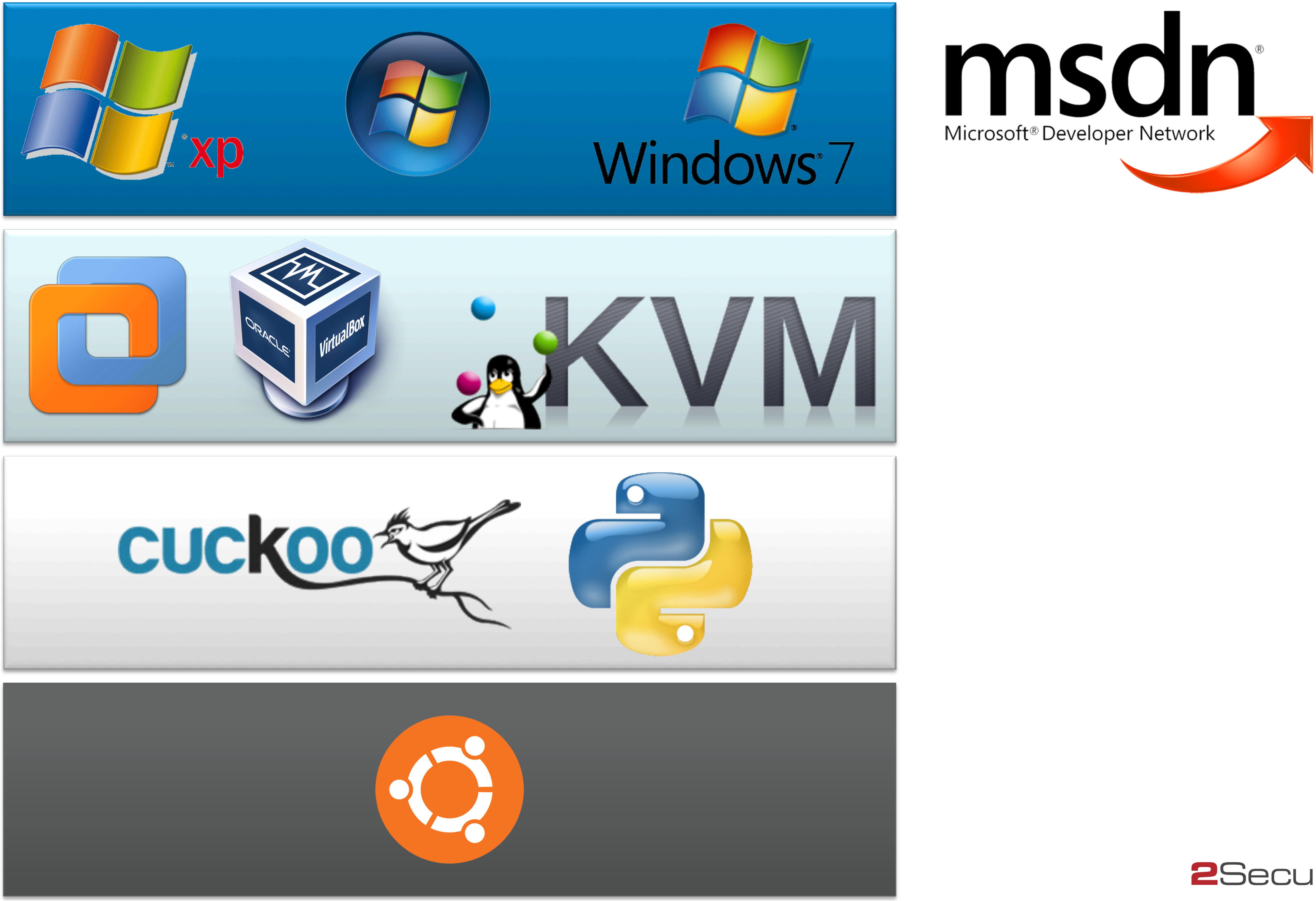
M.A.R.T

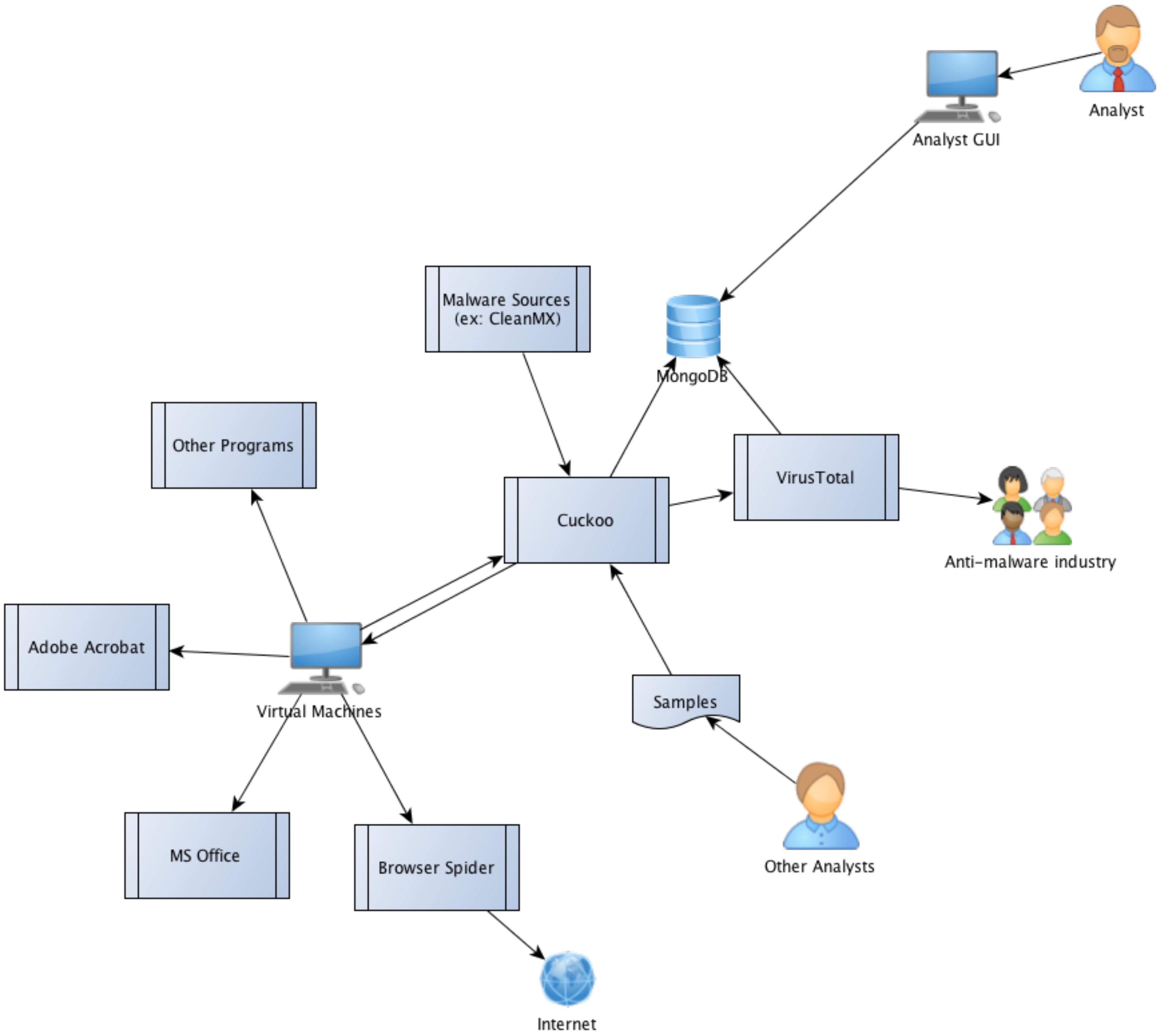
MALWARE ANALYST RESEARCH TOOL

Birth of the MART Project

Malware Analyst Research Toolkit

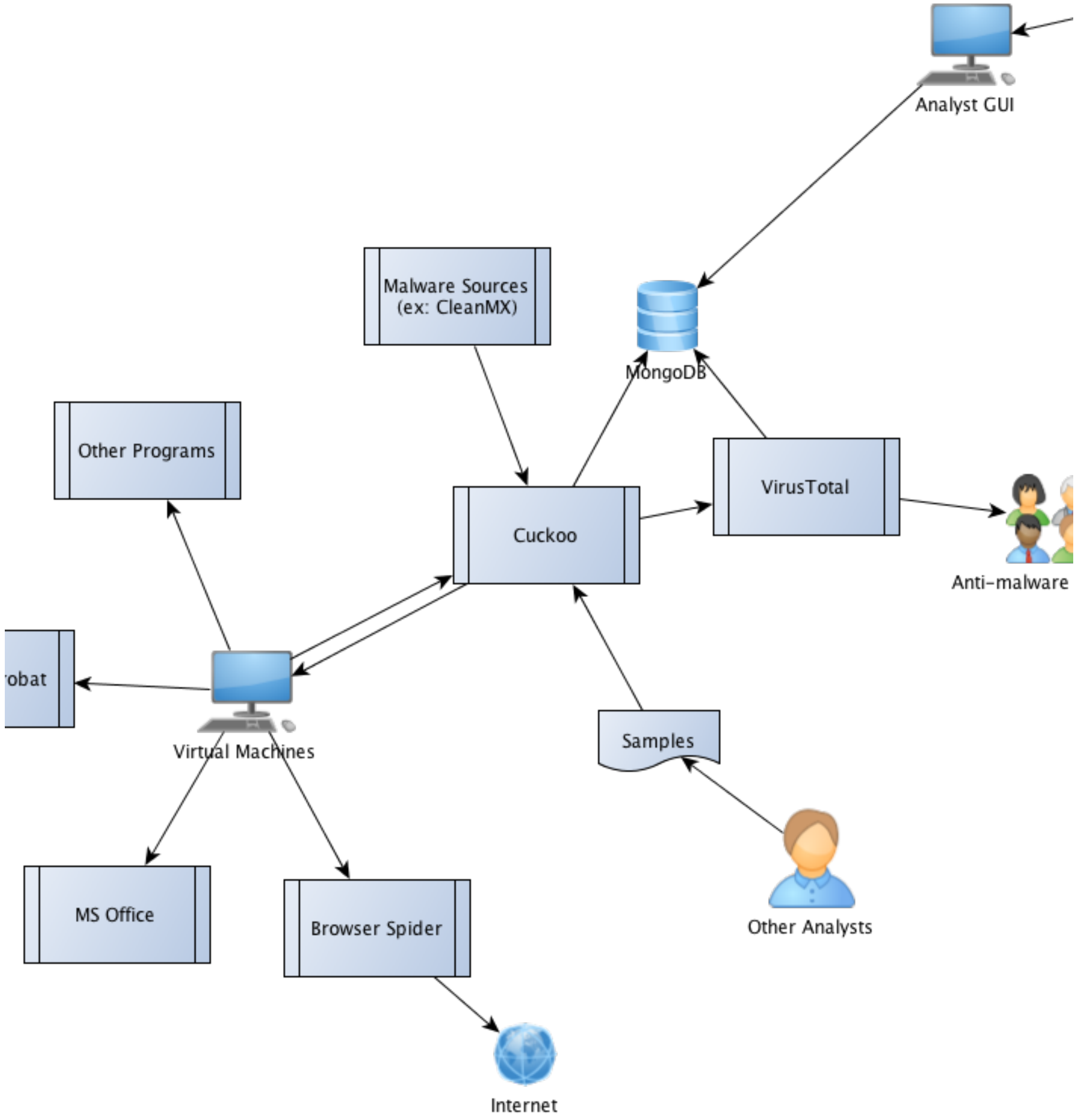
Components


xp
Windows 7
msdn
Microsoft® Developer Network
ORACLE
VirtualBox
KVM
cuckoo


Analyst
Analyst GUI
Malware Sources (ex: CleanMX)
MongoDB
Other Programs
VirusTotal
Cuckoo
Anti-malware industry
Adobe Acrobat
Virtual Machines
Samples
MS Office
Browser Spider
Other Analysts
Internet

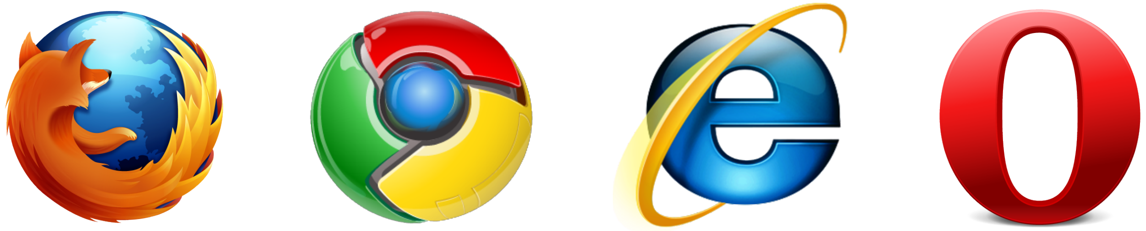
Sample Acquisition

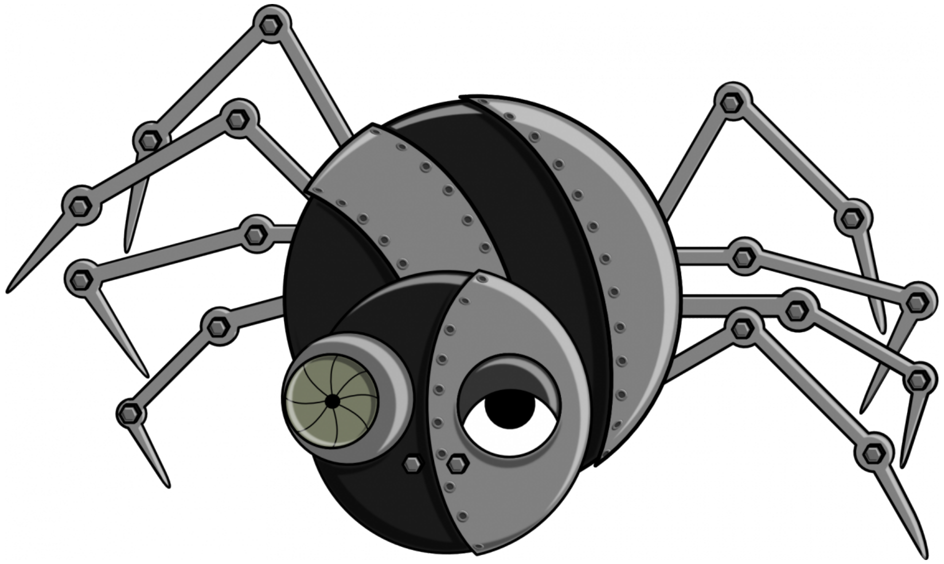
- Public & Private Collections
  - Clean MX
  - Malware.lu
  - Etc.
- Exchange with other malware analysts
  - You know who you are
- Finding and collecting malware yourself
  - Download files from the web
  - Grab attachments from email
  - Feed **BrowserSpider** with links from your SPAM-folder



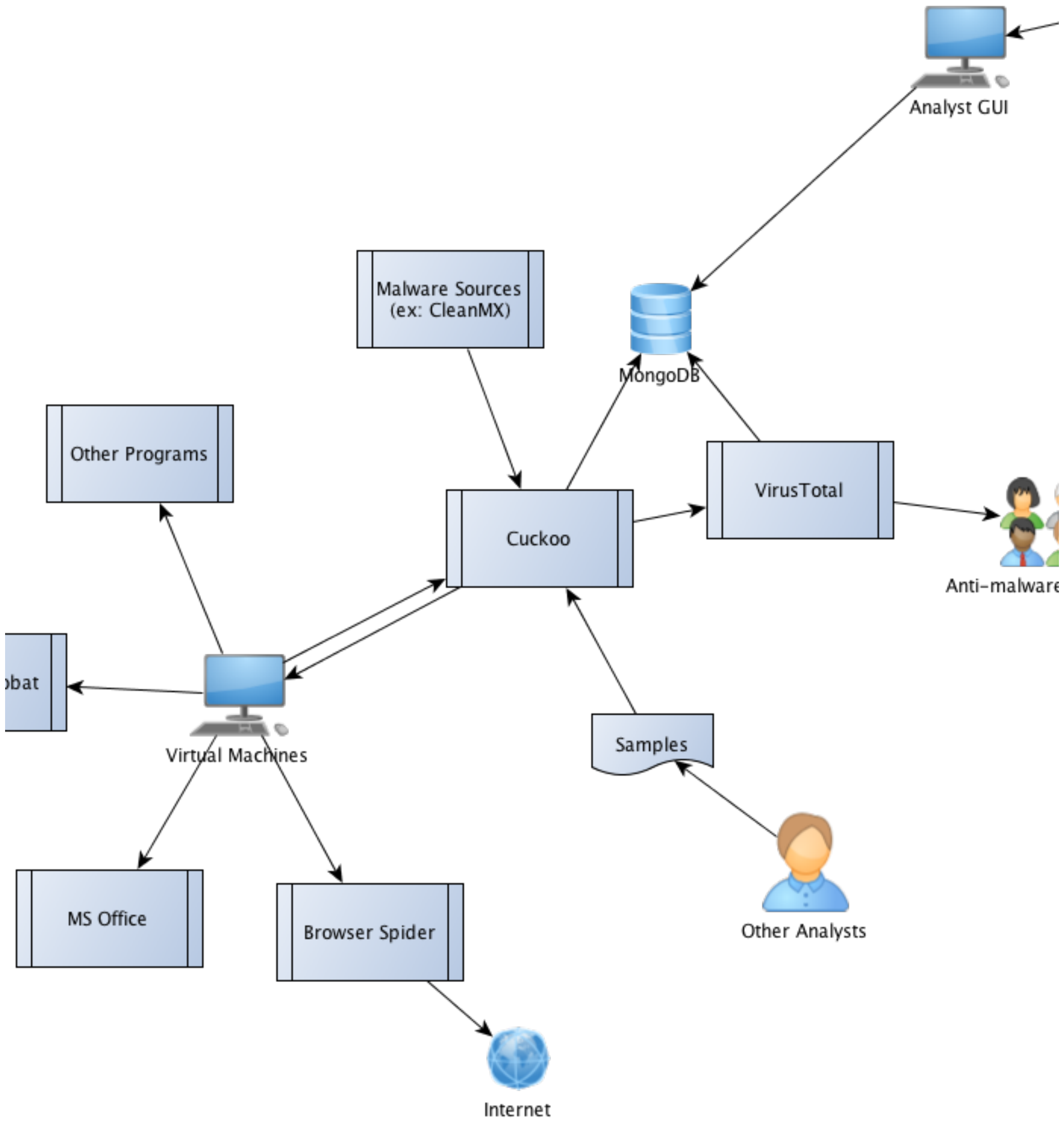
BrowserSpider

- Written in Python
- Using the Selenium framework to control REAL browsers
    - Flash, PDFs, Java applets etc. executes as per normal
    - All the browser bugs exists for real
- Spiders and follows all links seen





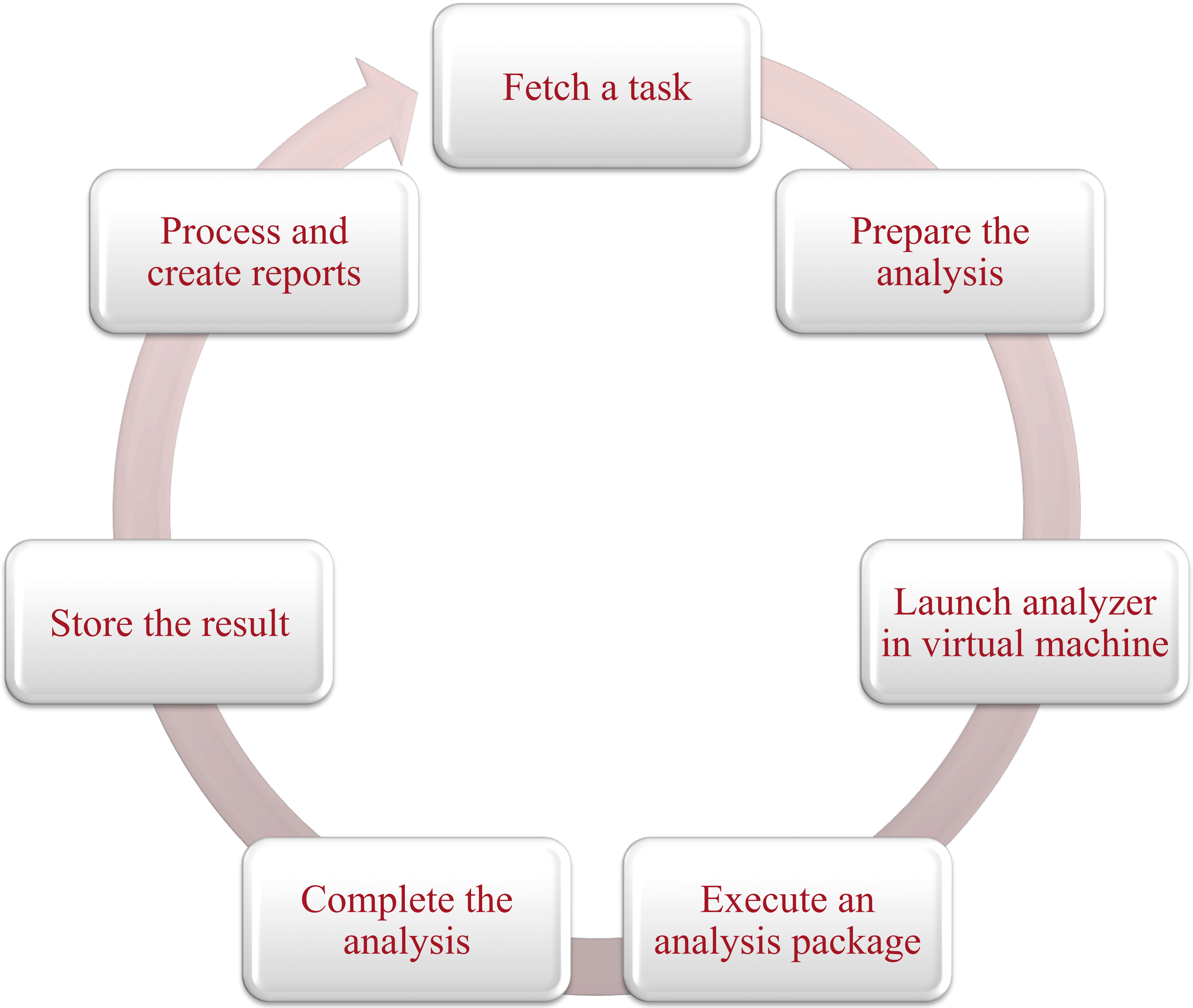
Sample Analysis



- Cuckoo Sandbox
- VirusTotal

DEMO: Submit sample for analysis

A days work for a Cuckoo



Fetch a task

Prepare the analysis

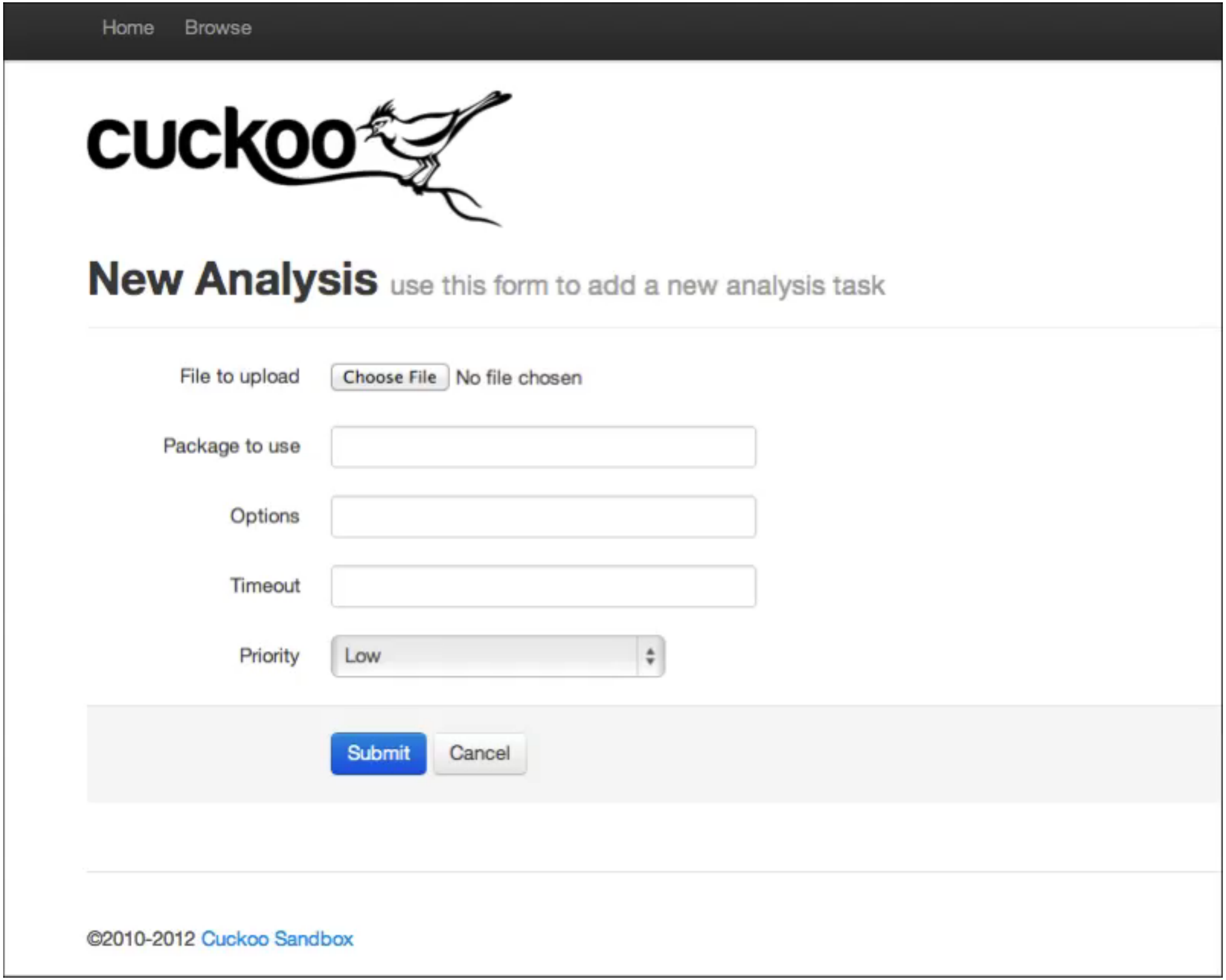
Launch analyzer in virtual machine

Execute an analysis package

Complete the analysis

Store the result

Process and create reports



New Analysis use this form to add a new analysis task

File to upload No file chosen

Package to use

Options

Timeout

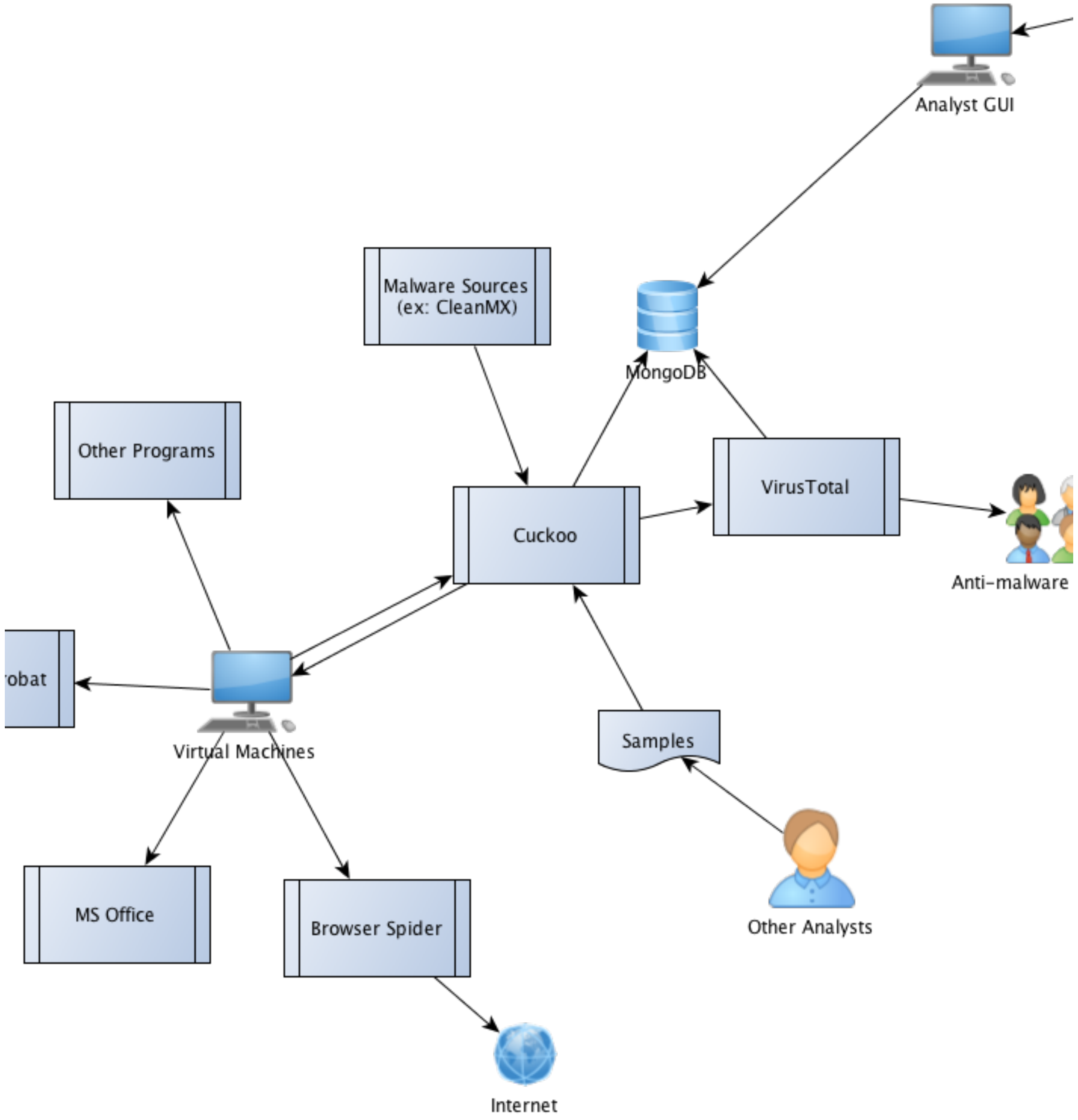
Priority: Low

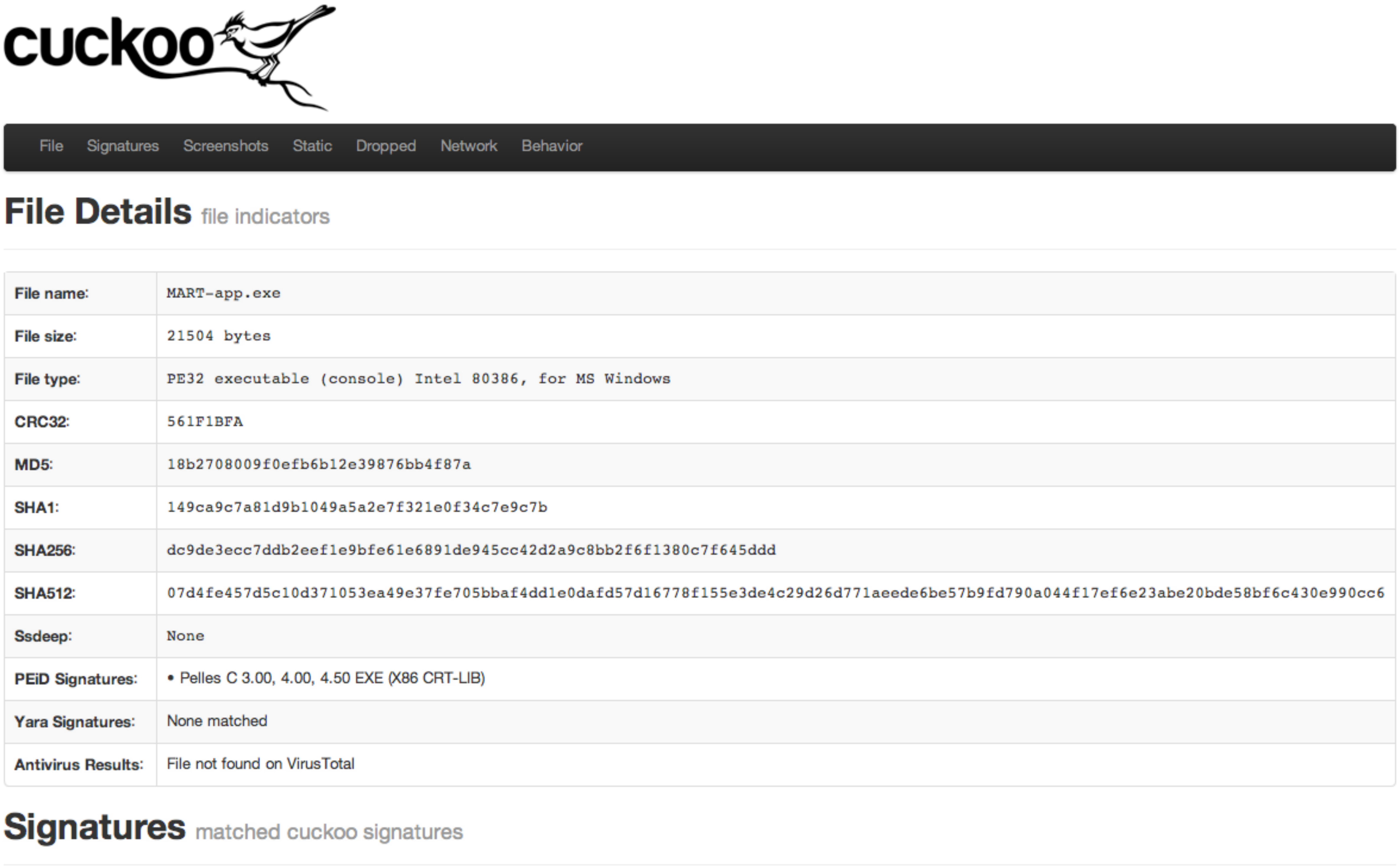
©2010-2012 Cuckoo Sandbox

Sample Reporting

Results are stored in MongoDB (optional, highly recommended)

Accessed using a analyst GUI

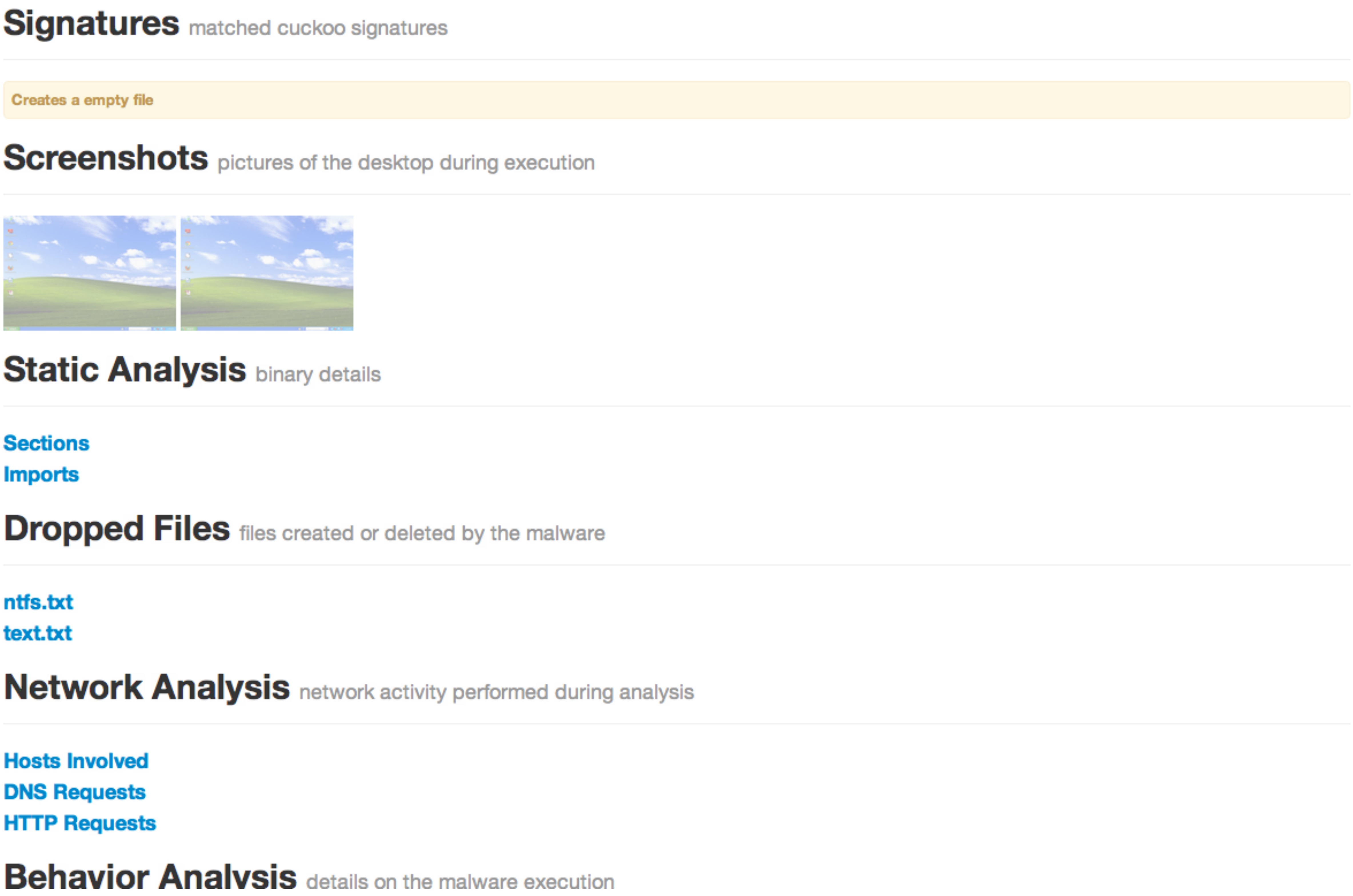




File Details file indicators

File name:	MART-app.exe
File size:	21504 bytes
File type:	PE32 executable (console) Intel 80386, for MS Windows
CRC32:	561F1BFA
MD5:	18b2708009f0efb6b12e39876bb4f87a
SHA1:	149ca9c7a81d9b1049a5a2e7f321e0f34c7e9c7b
SHA256:	dc9de3ecc7ddb2eef1e9bfe61e6891de945cc42d2a9c8bb2f6f1380c7f645ddd
SHA512:	07d4fe457d5c10d371053ea49e37fe705bbaf4dd1e0dafd57d16778f155e3de4c29d26d771aeede6be57b9fd790a044f17ef6e23abe20bde58bf6c430e990cc6
Ssdeep:	None
PEiD Signatures:	• Pelles C 3.00, 4.00, 4.50 EXE (X86 CRT-LIB)
Yara Signatures:	None matched
Antivirus Results:	File not found on VirusTotal

Signatures matched cuckoo signatures



Signatures matched cuckoo signatures

Creates a empty file

Screenshots pictures of the desktop during execution

Static Analysis binary details

Sections
Imports

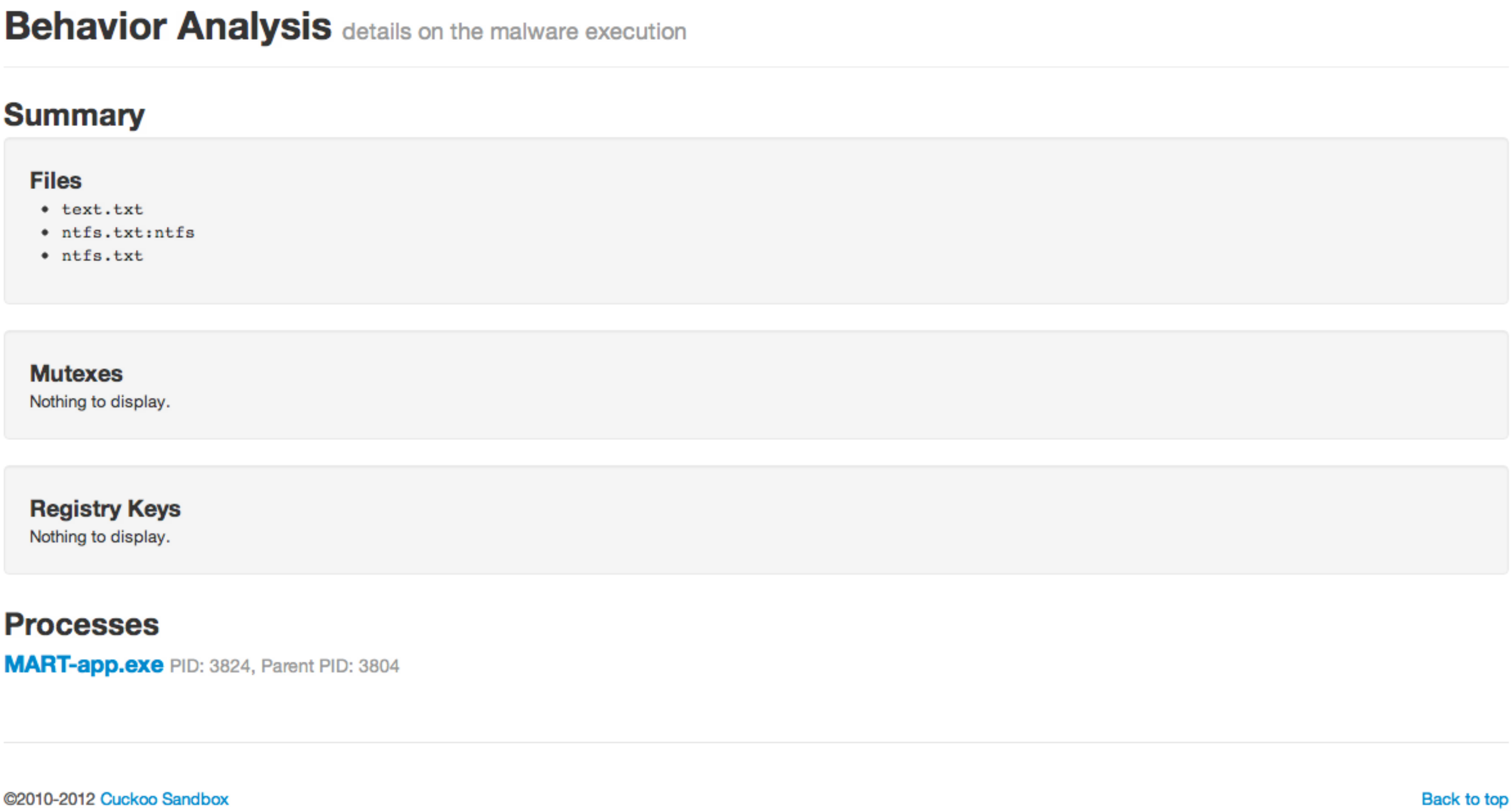
Dropped Files files created or deleted by the malware

ntfs.txt
text.txt

Network Analysis network activity performed during analysis

Hosts Involved
DNS Requests
HTTP Requests

Behavior Analysis details on the malware execution



Behavior Analysis details on the malware execution

Summary

Files

- `text.txt`
- `ntfs.txt:ntfs`
- `ntfs.txt`

Mutexes

Nothing to display.

Registry Keys

Nothing to display.

Processes

MART-app.exe PID: 3824, Parent PID: 3804

©2010-2012 Cuckoo Sandbox

Back to top

Data Mining

Malware attribution

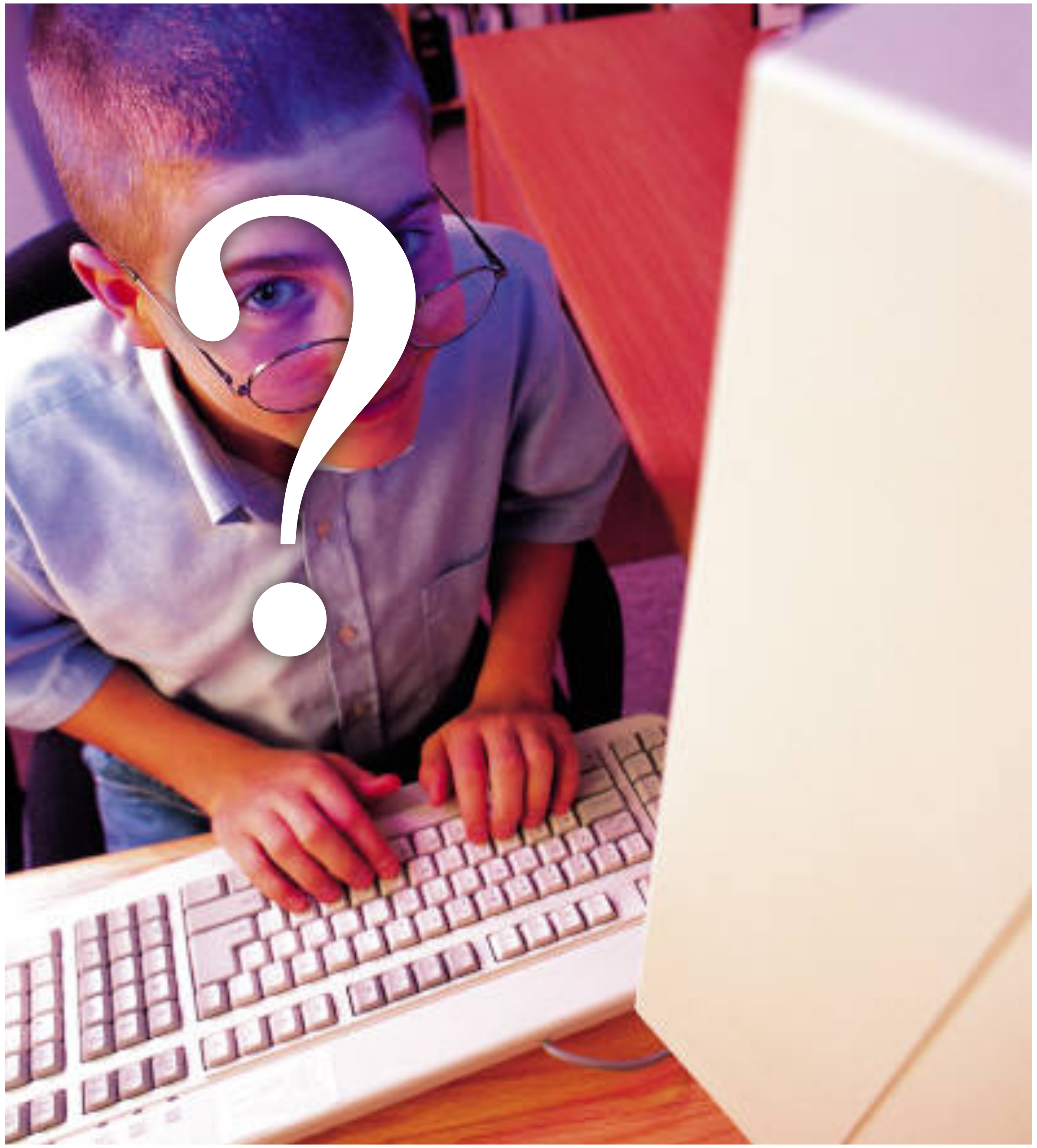
Black Hat USA 2010: Greg Hoglund: Malware attribution and fingerprinting

Where Virtual Machine analysis fails

And what to do about it

Problems

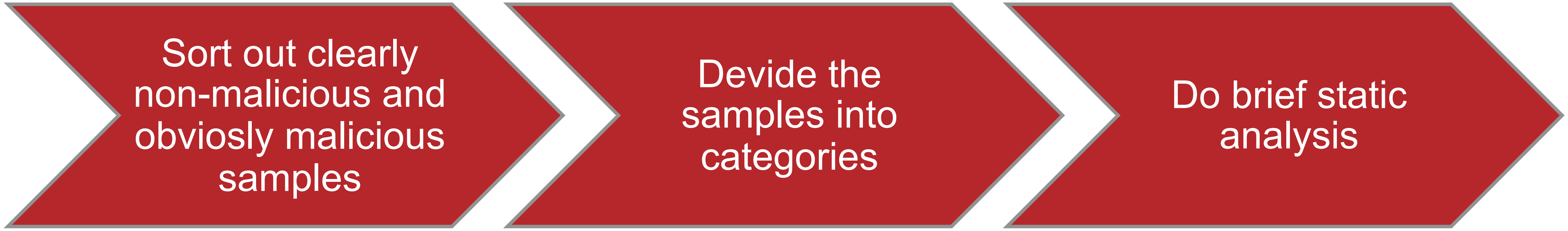
- User-detection
- Sleeping malware
- Multi-stage attacks



Problems

- VM or Sandbox detection
- The guest OS might not be sufficient enough

Iterating automatiation



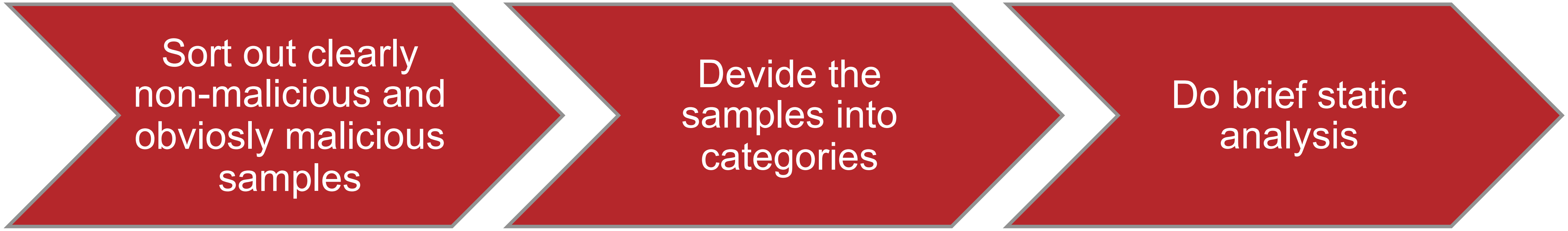
Sort out clearly non-malicious and obviosly malicious samples

Devide the samples into categories

Do brief static analysis

Known Good	Known Bad
Unknown	

Iterating automatiation



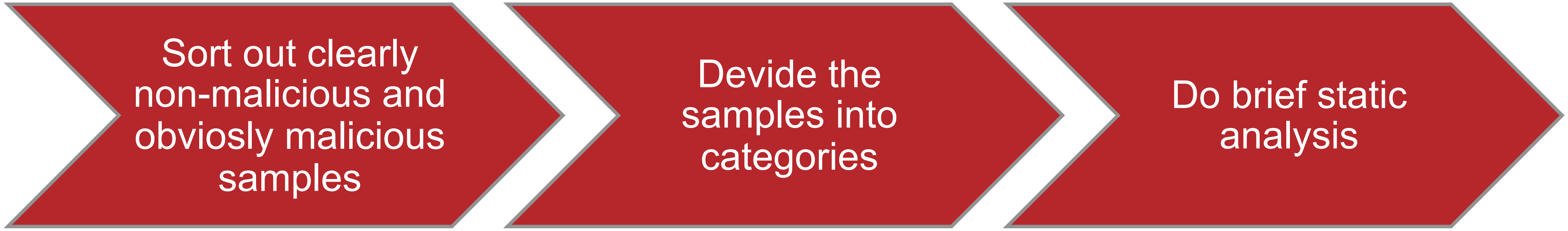
Sort out clearly non-malicious and obviosly malicious samples

Devide the samples into categories

Do brief static analysis

- Does not do anything
- Detects environment
- Encrypted segments
- Failed execution

Iterating automatiation

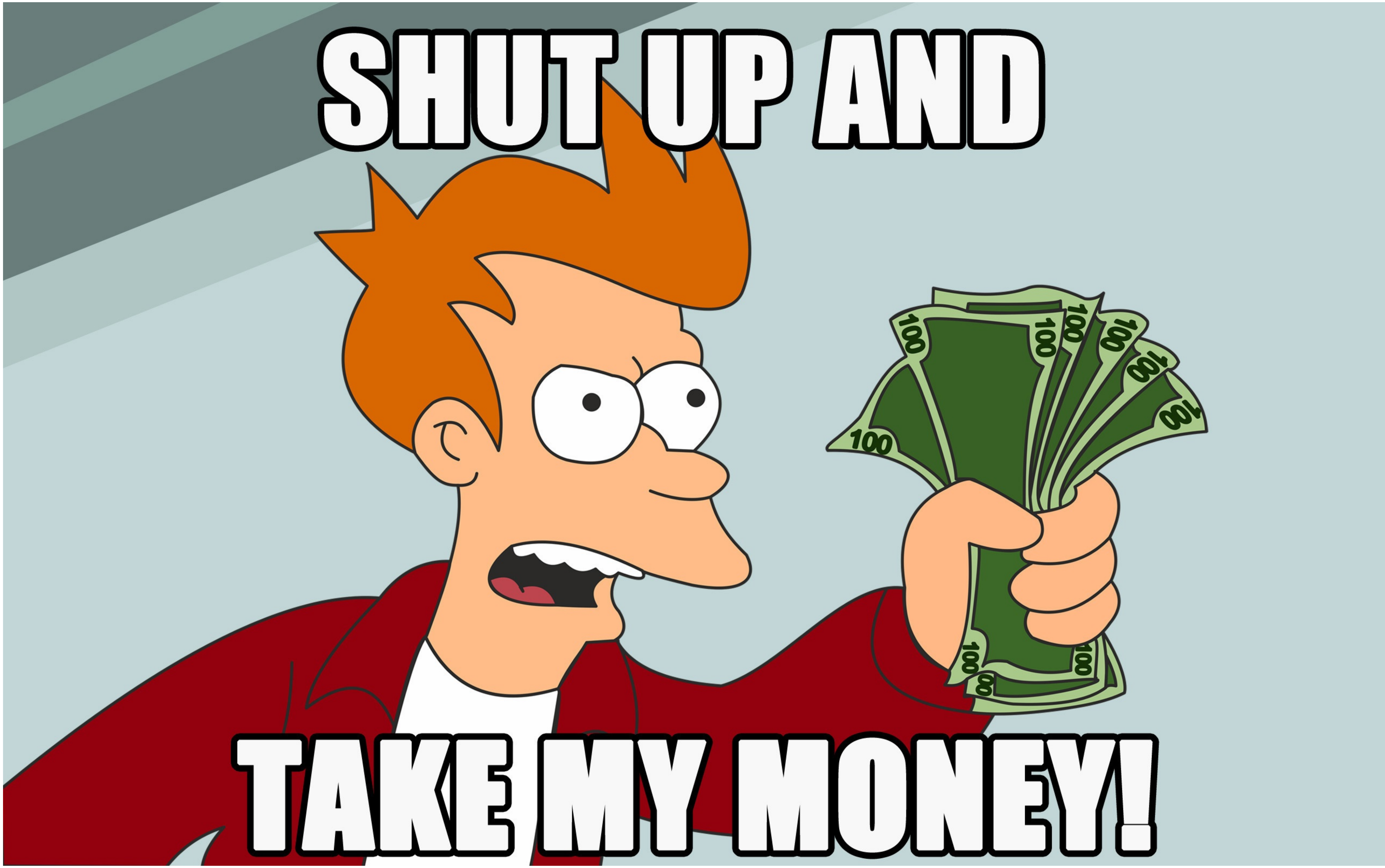


Sort out clearly non-malicious and obviosly malicious samples

Devide the samples into categories

Do brief static analysis

- Run longer
- Envirnoment customization

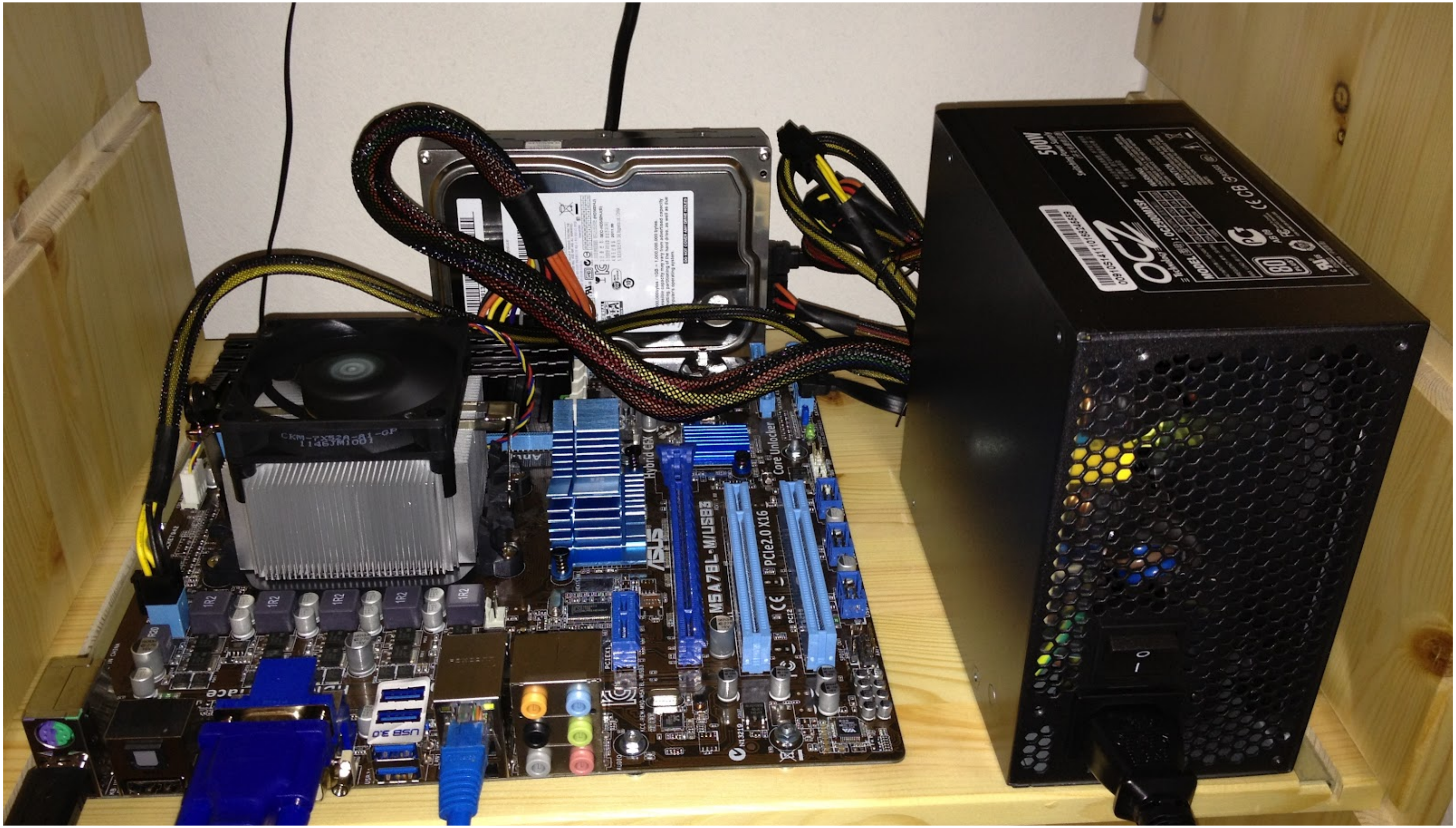

SHUT UP AND
TAKE MY MONEY!
100

Budget

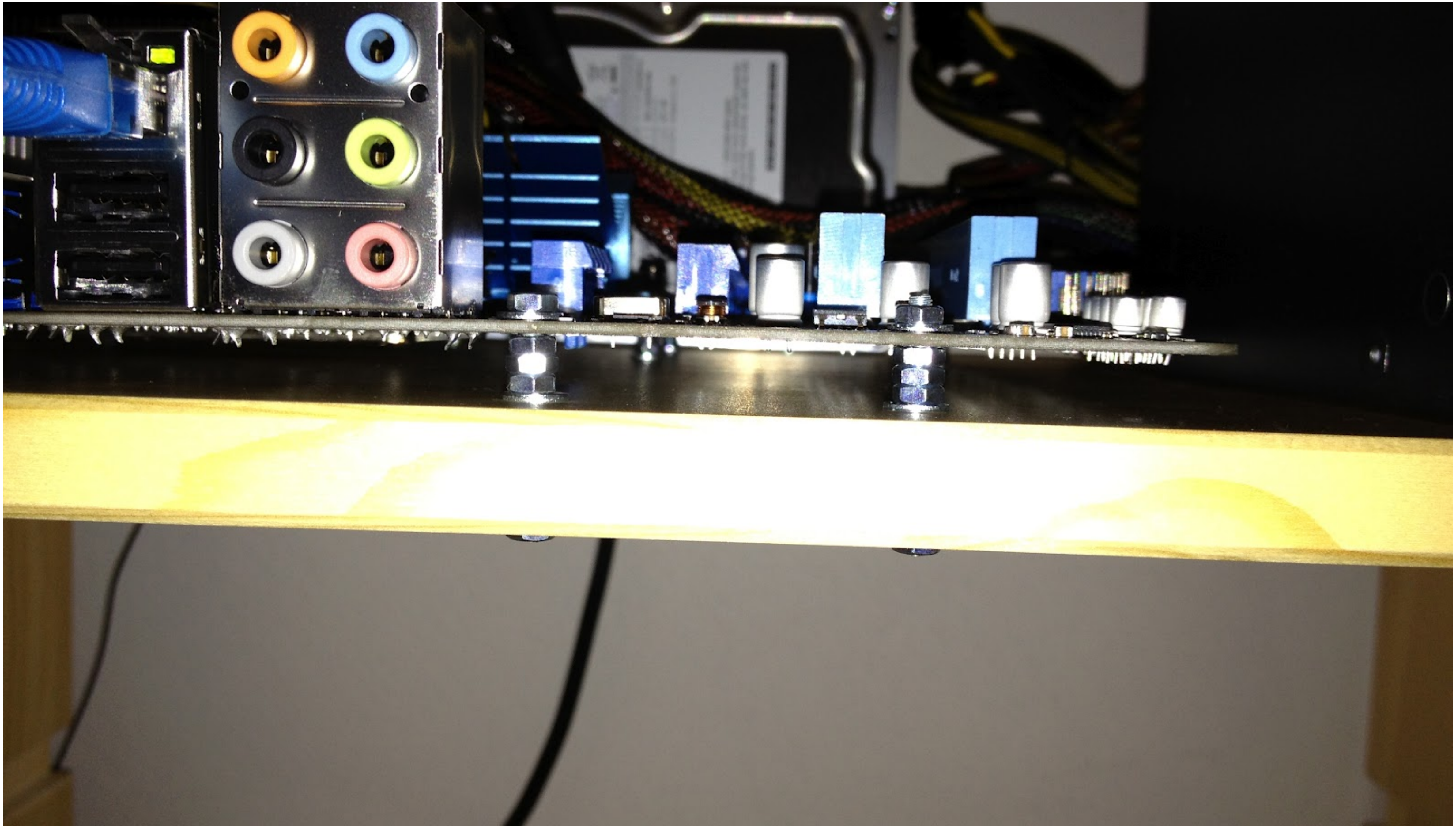
- Computer: €520
- MSDN License: €800 (€590 renewal)
- Year 1 (2012): €1320
- Year N (2013…): €590
- Money saved from stopped smoking (yearly): €2040

Malware Lab

MART Hardware (overview)



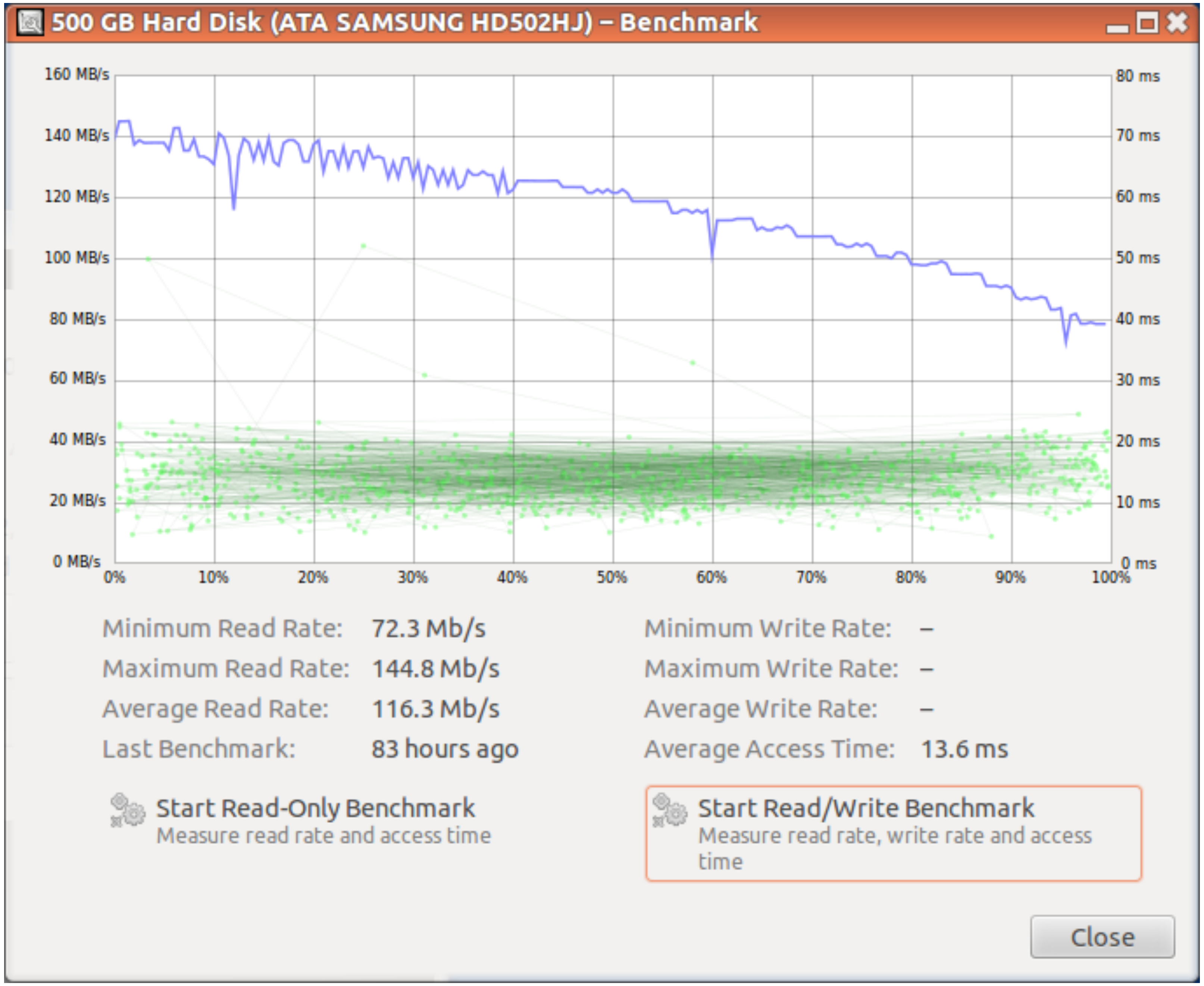
MART Hardware (mounts)



The need for speed

- Original setup couldn’t run more then 2 virtual machines simultaneously
    - Disk I/O couldn’t keep up

MART Hardware (HDD)



500 GB Hard Disk (ATA SAMSUNG HD502HJ) – Benchmark

Minimum Read Rate: 72.3 Mb/s
Maximum Read Rate: 144.8 Mb/s
Average Read Rate: 116.3 Mb/s
Last Benchmark: 83 hours ago

Minimum Write Rate: –
Maximum Write Rate: –
Average Write Rate: –
Average Access Time: 13.6 ms

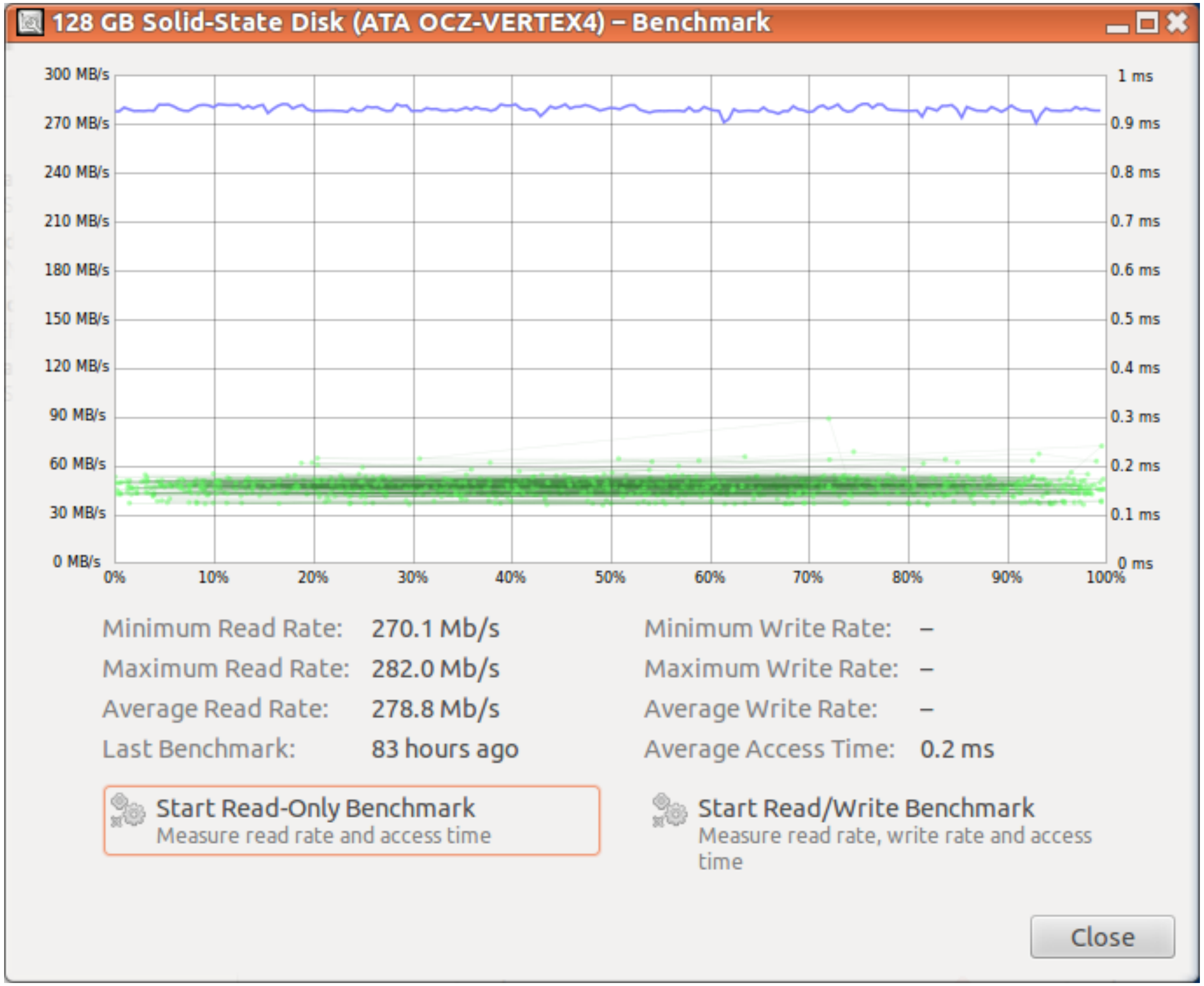
Transfer speed:

72-144 Mb/s

Access time:

13.6 ms

MART Hardware (SSD)



Minimum Read Rate: 270.1 Mb/s
Maximum Read Rate: 282.0 Mb/s
Average Read Rate: 278.8 Mb/s
Last Benchmark: 83 hours ago

Minimum Write Rate: –
Maximum Write Rate: –
Average Write Rate: –
Average Access Time: 0.2 ms

Start Read-Only Benchmark
Measure read rate and access time
Start Read/Write Benchmark
Measure read rate, write rate and access time
Close

Transfer speed:

270-280 Mb/s

2x

Access tim

0.2 ms

68x

Running 3-4 machines simultaneously

Next steps

1. Barebone on-the-iron malware analysis
2. Android platform support
3. OSX platform support
4. iOS patform support

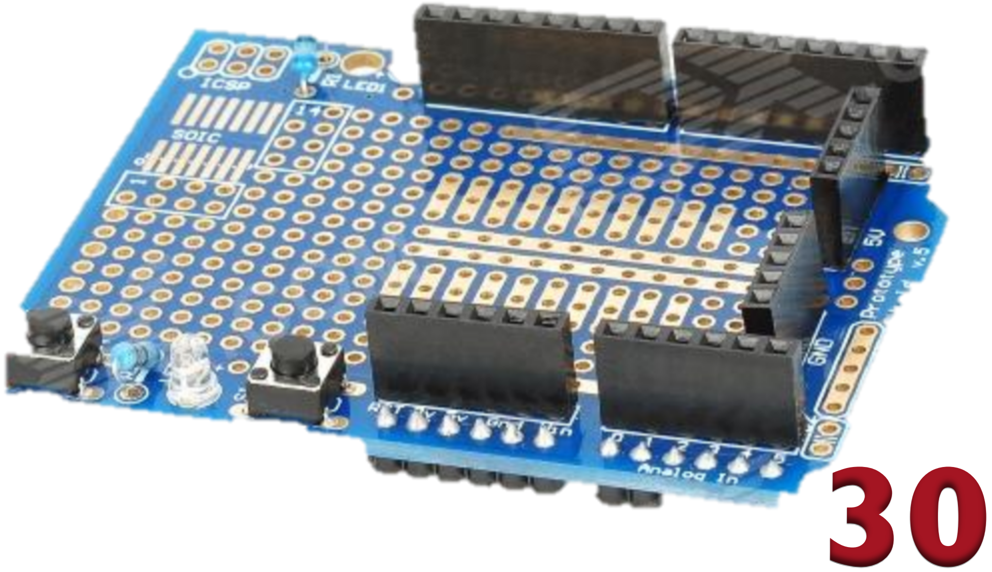
Existing barebone implementations

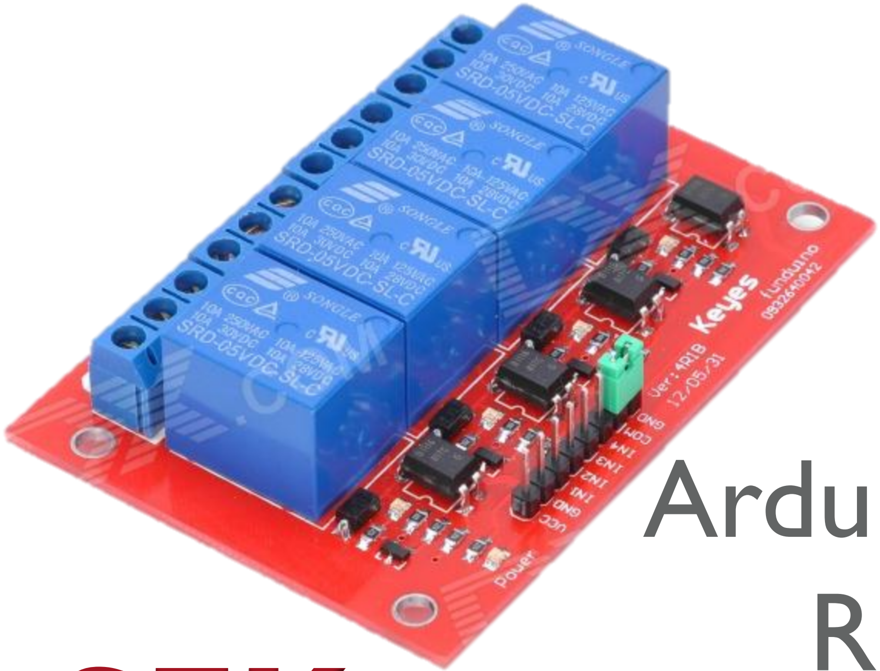
- BareBox
  - BareBox: Efficient Malware Analysis on Bare-Metal
  - Dhilung Kirat, Giovanni Vigna, Christopher Kruegel
  - ACSAC 2011
  - No code has been released

- NVMTrace
  - Entrapment: Tricking Malware with Transparent, Scalable Malware Analysis
  - Paul Royal
  - Blackhat 2012 EUROPE
  - Requires special hardware (Intelligent Platform Management Interface [IPMI])

Proof of Concept hardware

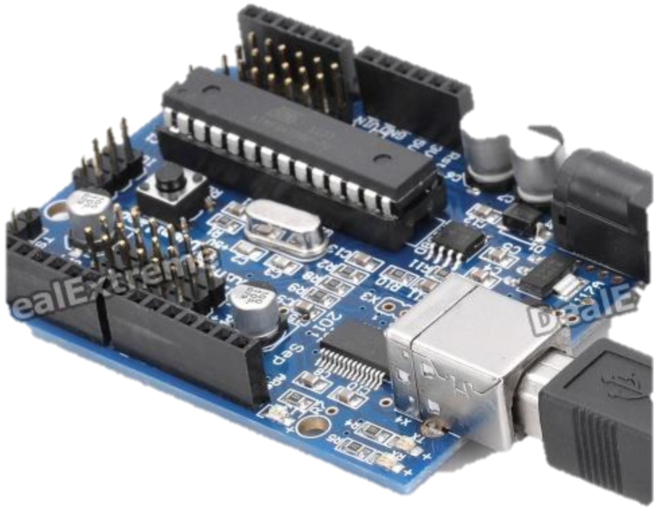
Prototype Shield





Arduino 4-Channel Relay Shield

300 SEK (€~30)



Arduino Duemilanove

Ethernet Shield

Questions?

Michael Boman
michael.boman@2secure.se
http://www.2secure.se

Michael Boman
michael@michaelboman.org
http://michaelboman.org
@mboman