2Secure

# Malware Analysis as a Hobby

Michael Boman - Security Consultant/Researcher, Father of 5

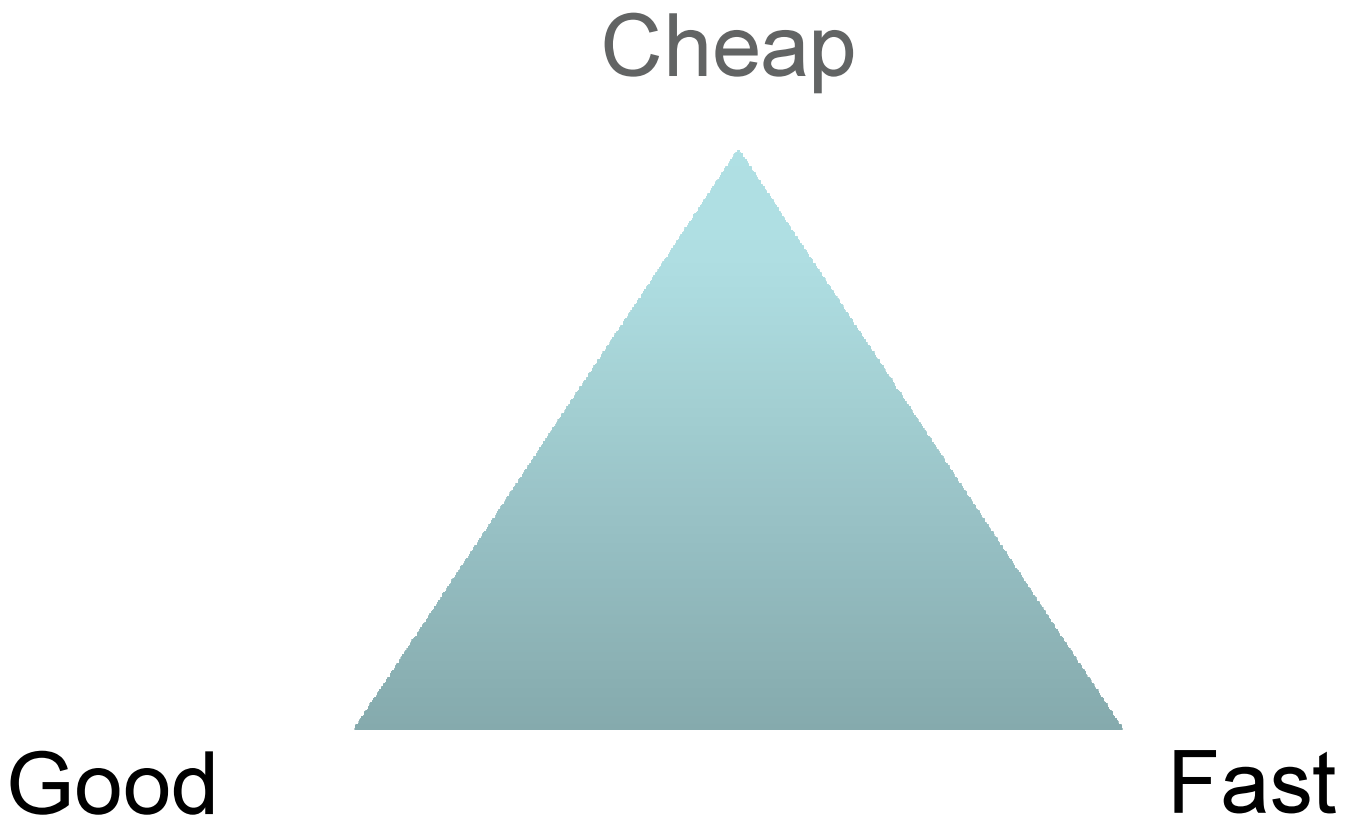
# Why the strange hobby?

1. Start virtual environment
2. Copy sample
3. Start logging facilities
4. Execute sample
5. Stop logging facilities
6. Analyze logs

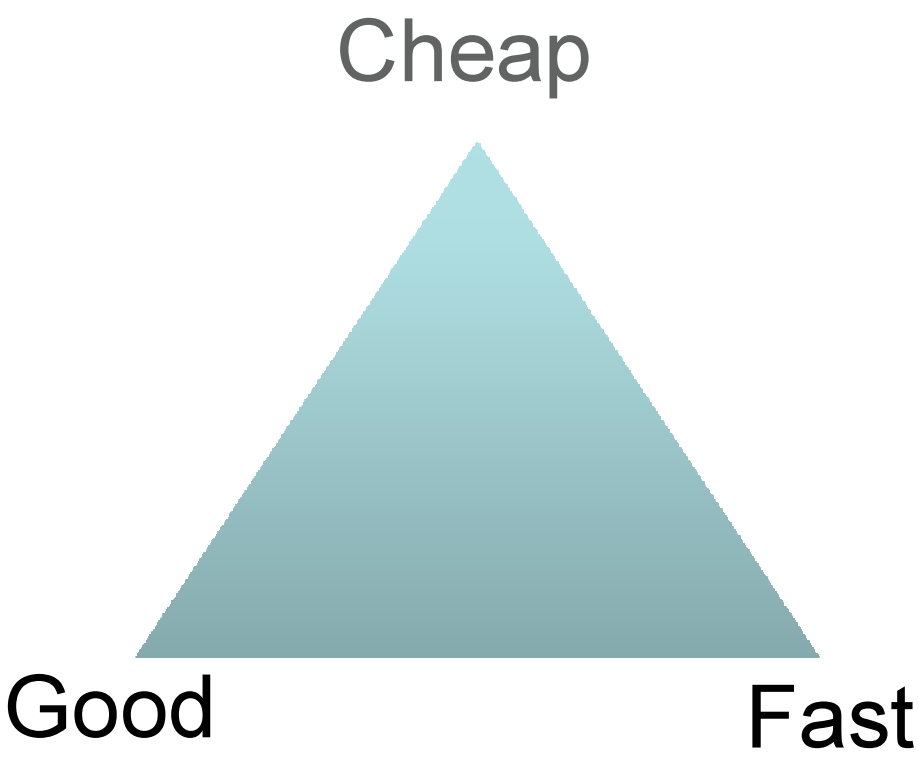
# Drawbacks

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

# Choose any two….



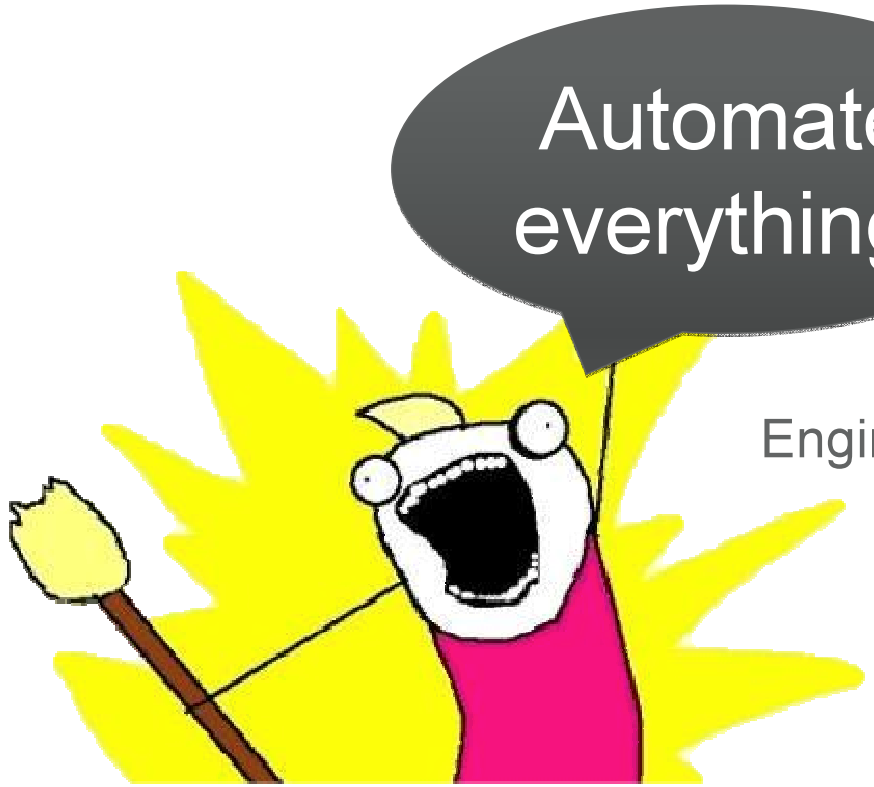
Choose any two?
Why not all of them?




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).

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




# Automate

Engineer yourself out of the workflow

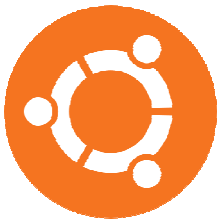
M_A_R_T

MALWARE ANALYST RESEARCH TOOL

# Birth of the MART Project

Malware Analyst Research Toolkit

2Secure




ORACLE
VirtualBox

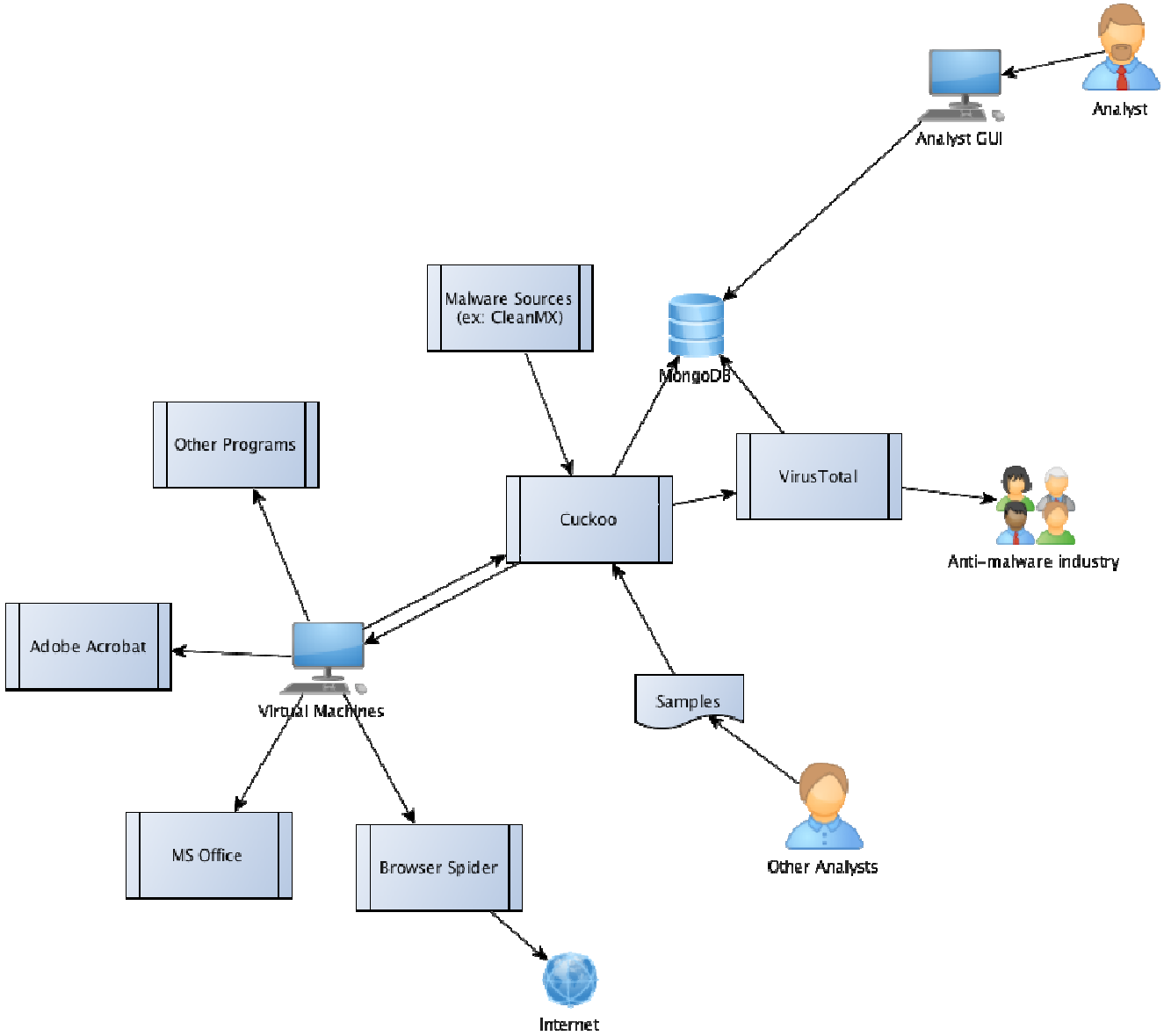

cuckoo


msdn
Microsoft® Developer Network

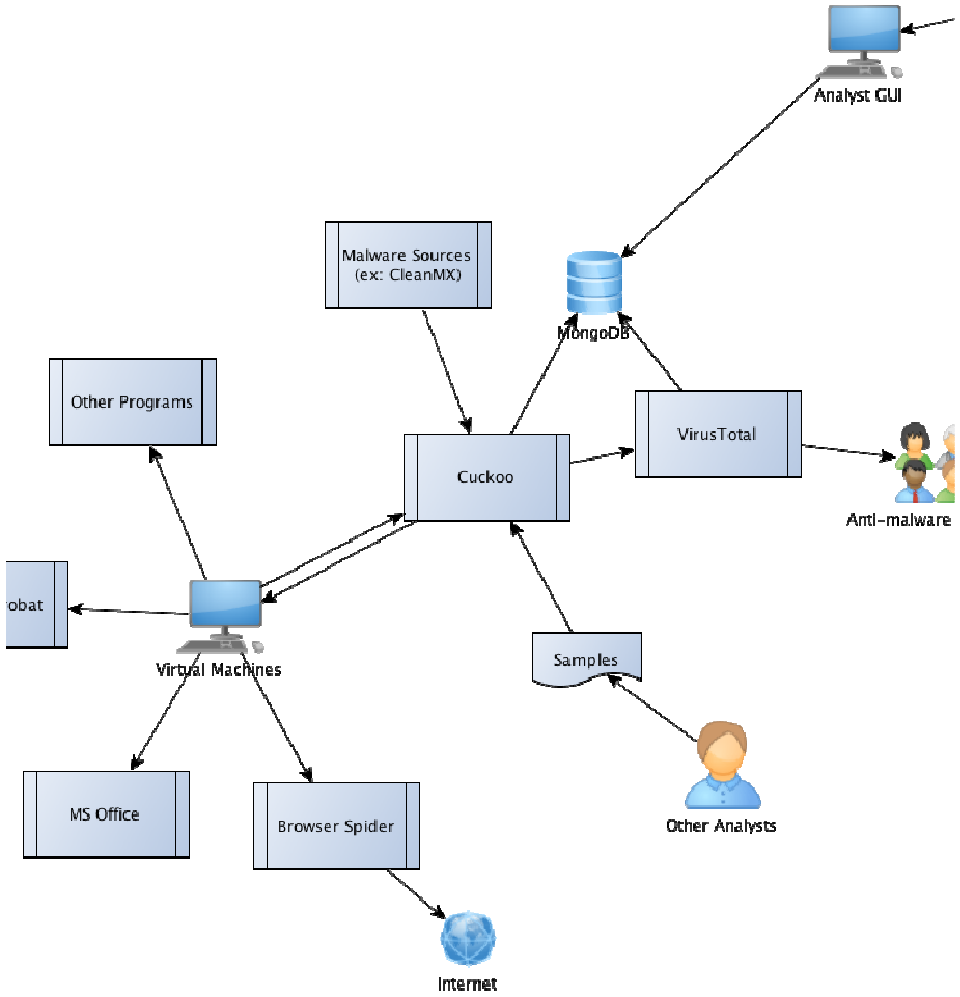

xp

# Components


Windows 7

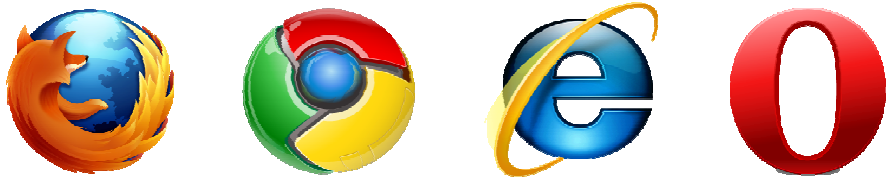

Analyst
Analyst GUI
Malware Sources
(ex: CleanMX)
MongoDB
Other Programs
VirusTotal
Cuckoo
Anti-malware industry
Adobe Acrobat
Virtual Machines
Samples
MS Office
Browser Spider
Other Analysts
Internet

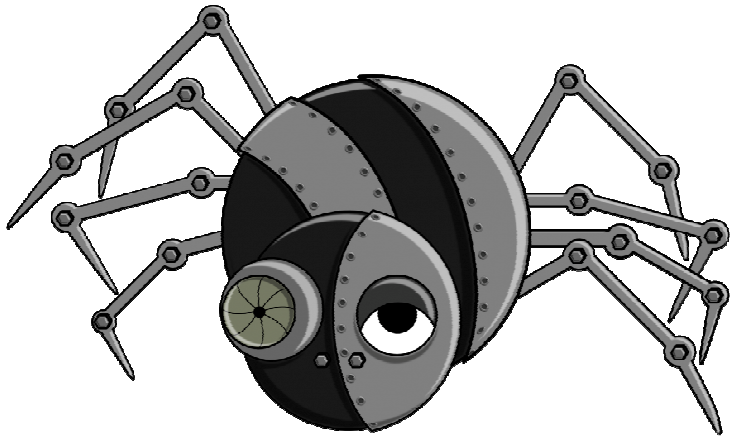
- Public & Private Collections
- Exchange with other malware analysts
- Finding and collecting malware yourself
  - Download files from the web
  - Grab attachments from email
  - Feed BrowserSpider with links from your SPAM-folder



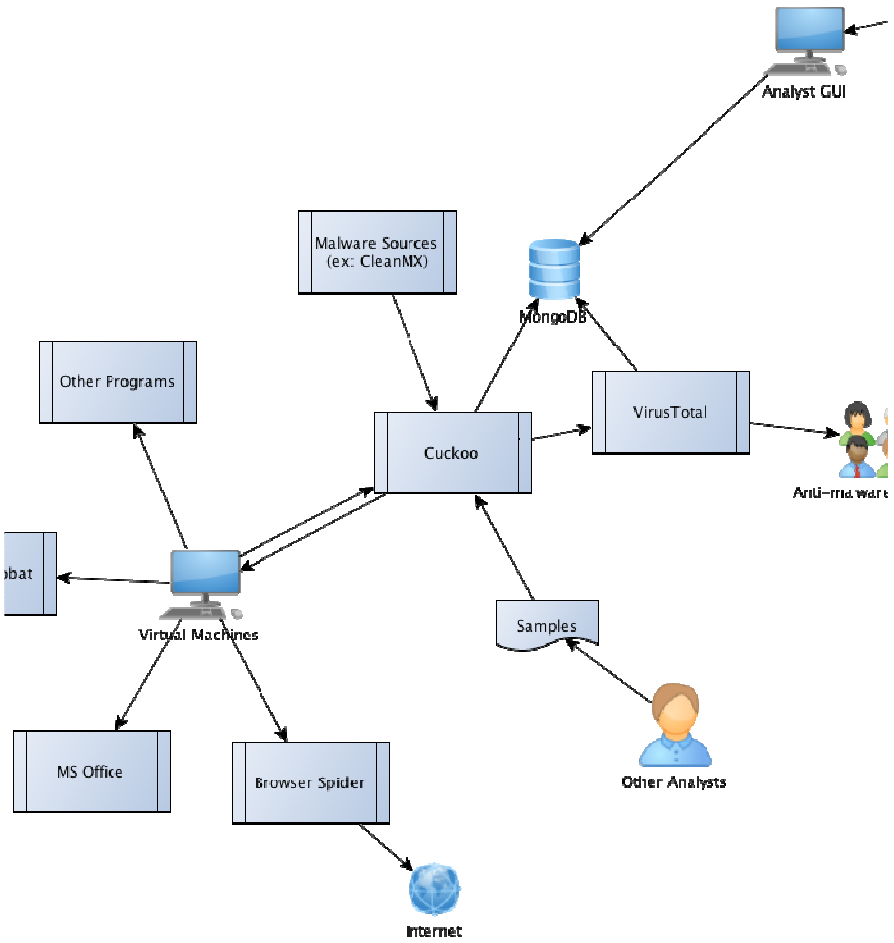
# BrowserSpider

- 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



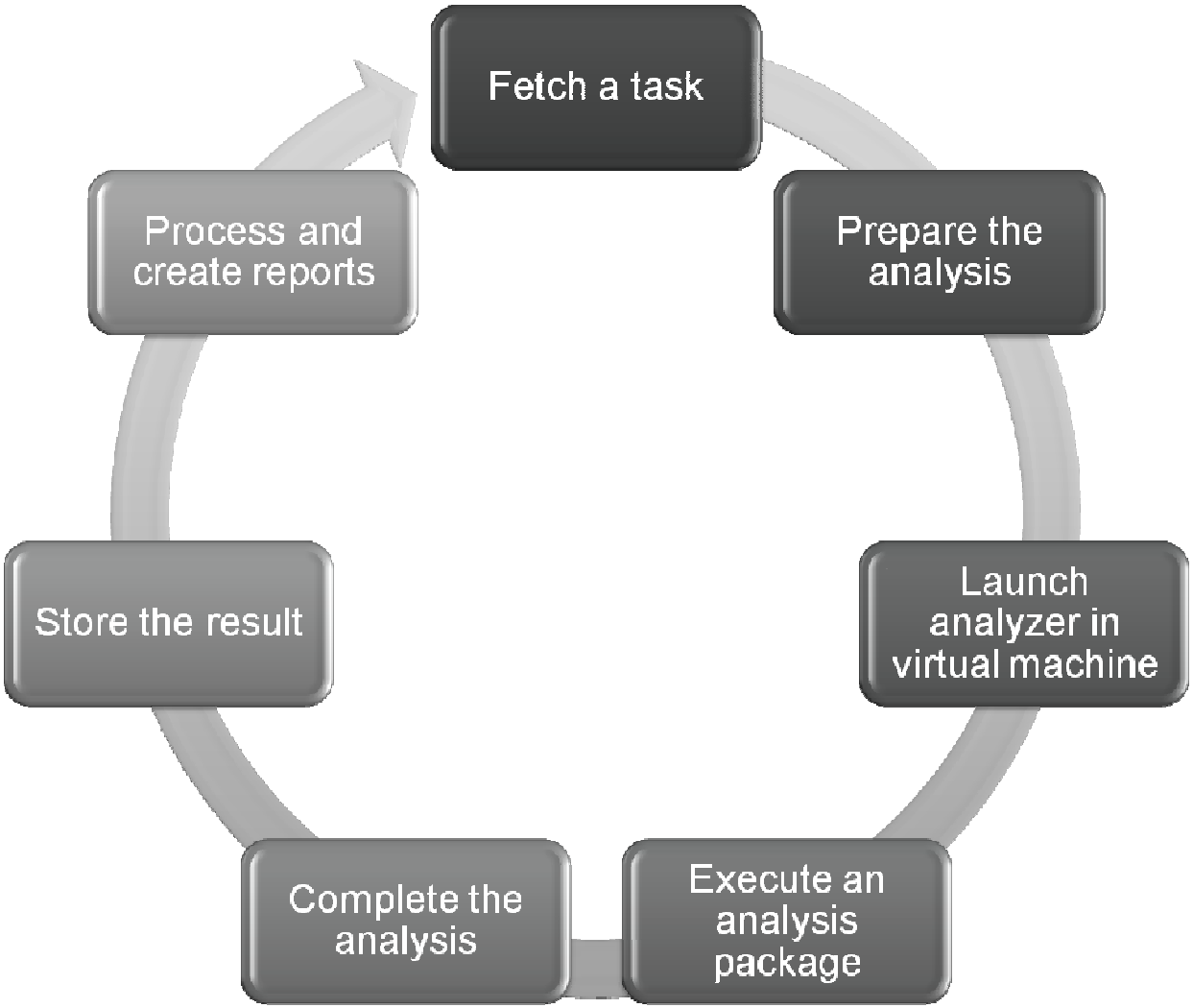


# Sample Analysis

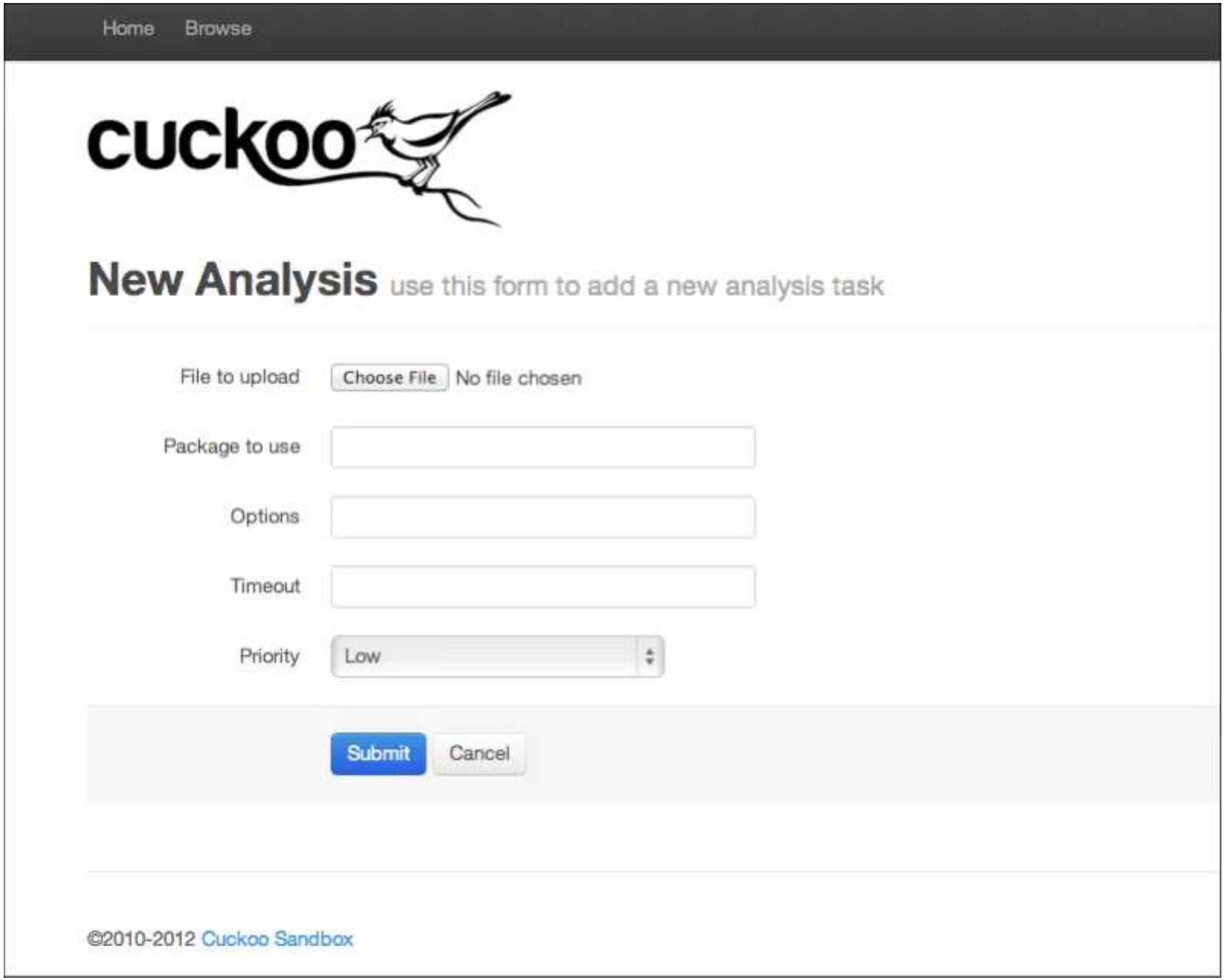



- Cuckoo Sandbox
- VirusTotal

# A days work for a Cuckoo



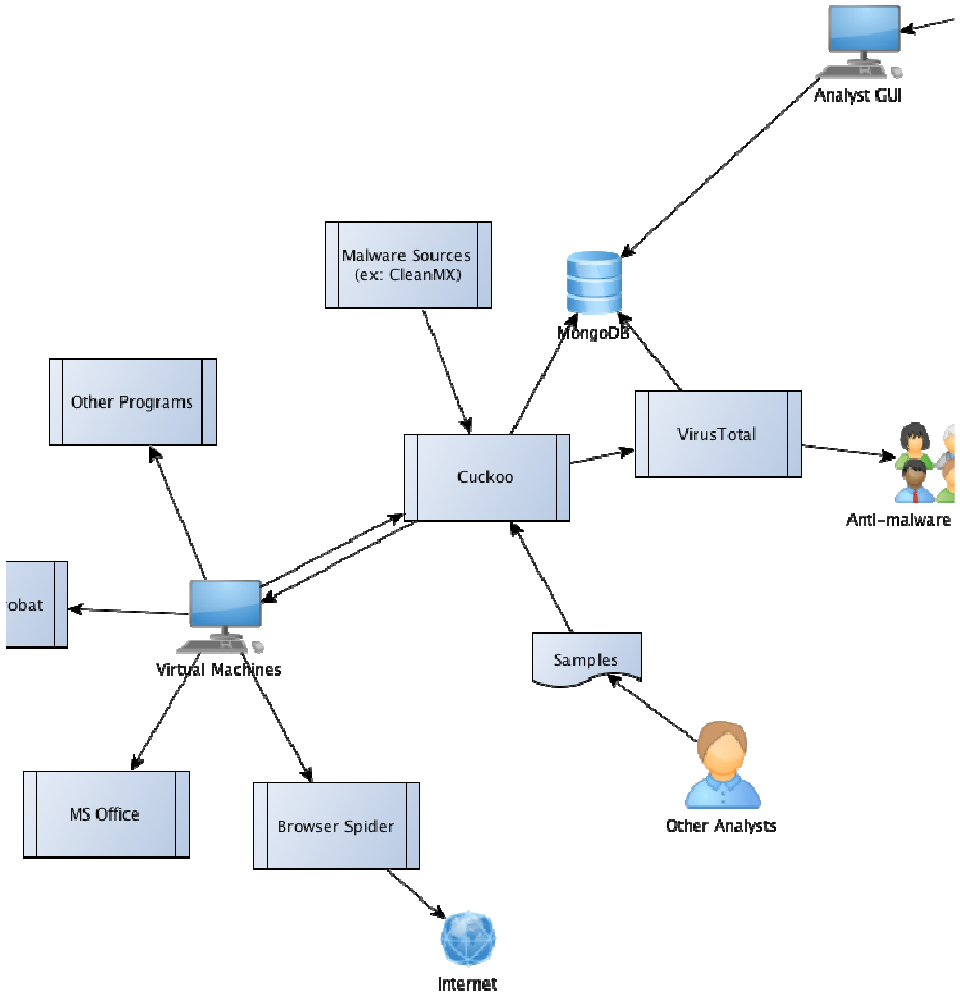
# DEMO: Submit sample for analysis


Home
Browse
cuckoo
New Analysis
use this form to add a new analysis task
File to upload
Choose File
No file chosen
Package to use
Options
Timeout
Priority
Low
Submit
Cancel
©2010-2012 Cuckoo Sandbox

# Sample Reporting

Results are stored in MongoDB (optional, highly recommended)

Accessed using a analyst GUI




File Signatures Screenshots Static Dropped Network Behavior

# File Details file indicators

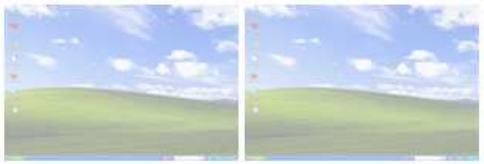
| | |
|---|---|
| **File name:** | MART-app.exe |
| **File size:** | 21504 bytes |
| **File type:** | PE32 executable (console) Intel 80386, for MS Windows |
| **CRC32:** | 561F1BFA |
| **MD5:** | 18b2708009f0efb6b12e39876bb4f87a |
| **SHA1:** | 149ca9c7a81d9b1049a5a2e7f321e0f34c7e9c7b |
| **SHA256:** | 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



Back to top

# Data Mining

# Where Virtual Machine analysis fails

And what to do about it

# Problems

- Cuckoo is easly bypassed
- User-detection
- Sleeping malware

# Problems

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

# Iterating automatiation

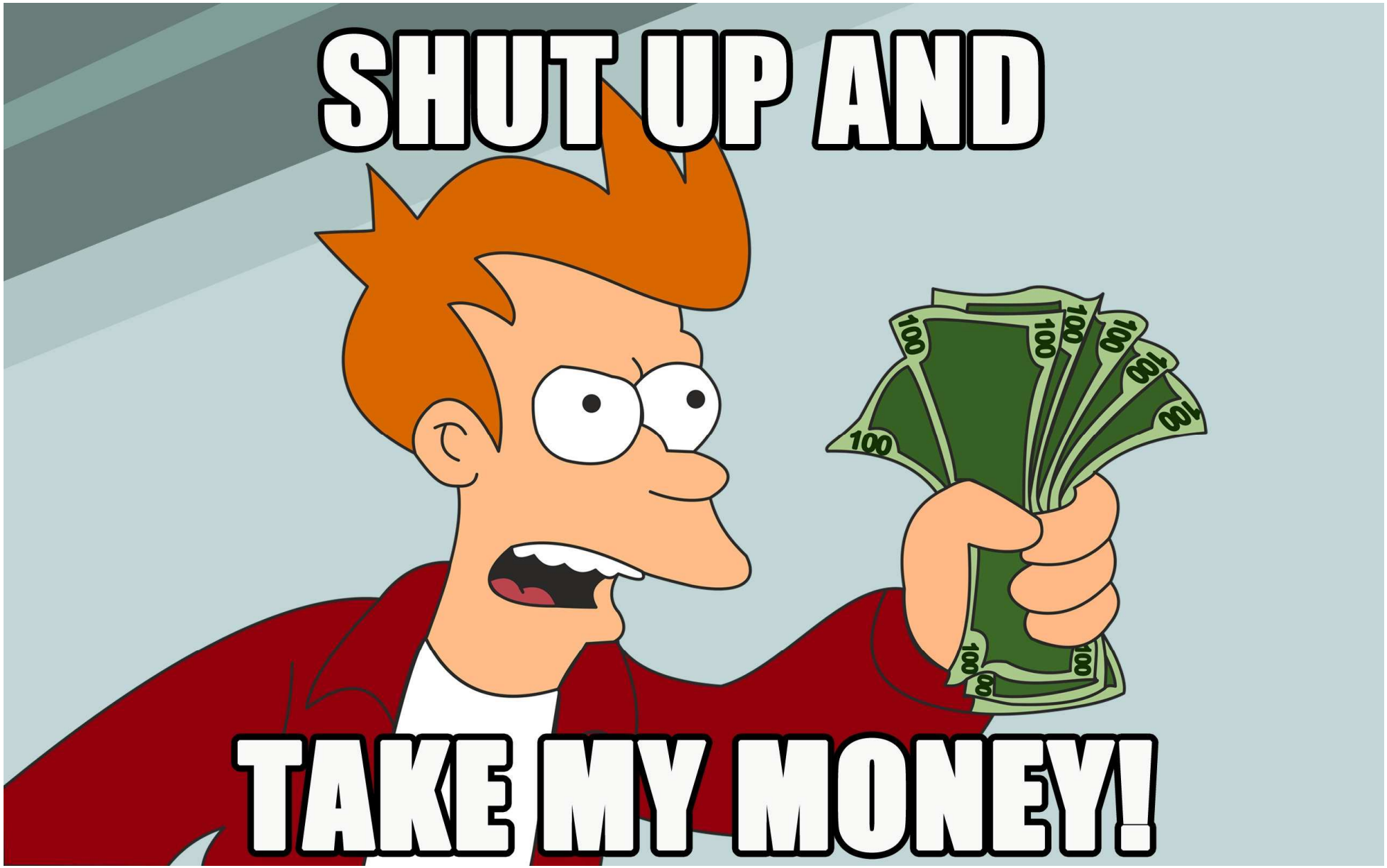

| Known Good | Known Bad |
|---|---|
| Unknown | |

# Iterating automatiation


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

# Iterating automatiation


- Run longer
- Envirnoment customization

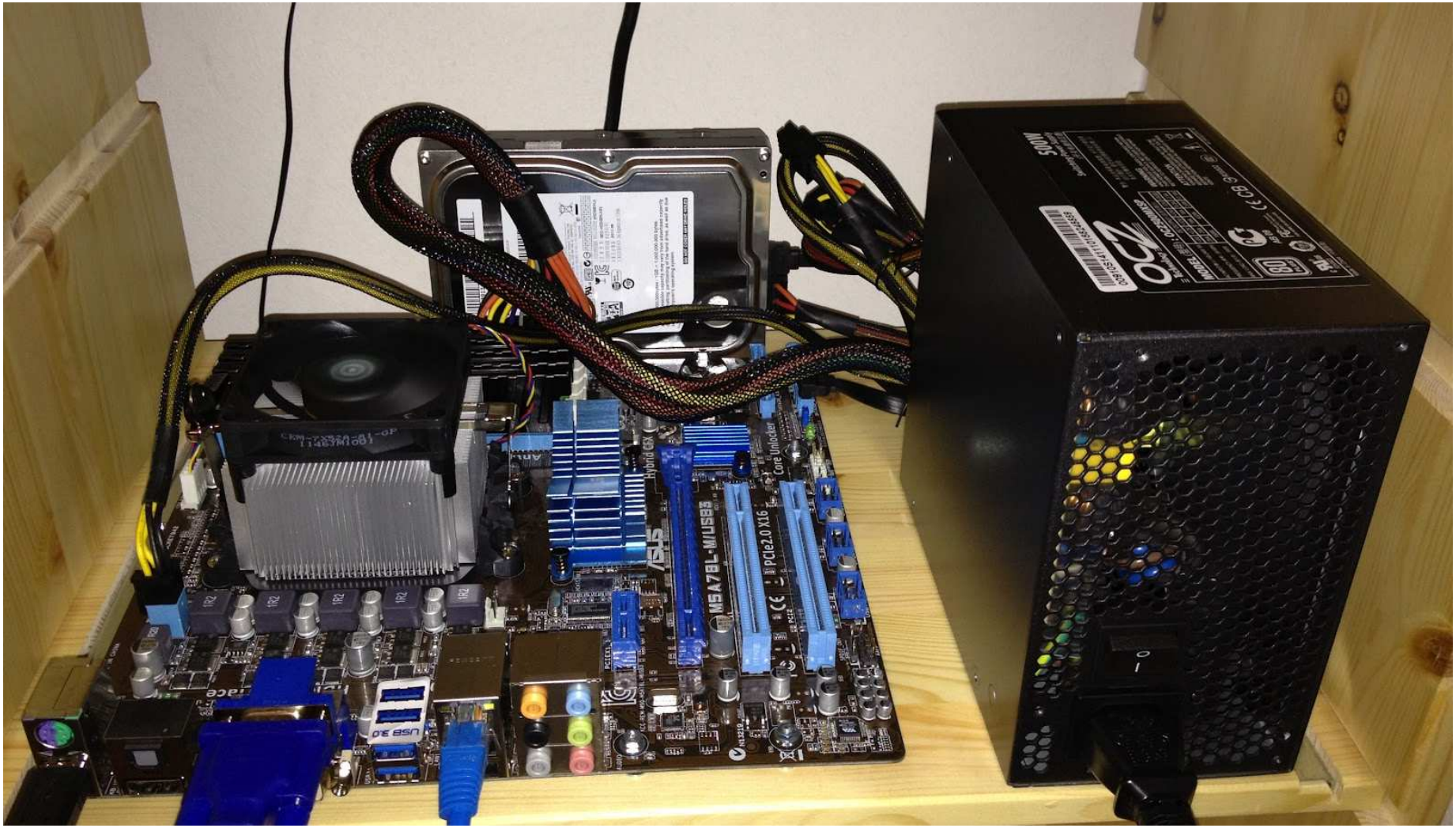

SHUT UP AND
TAKE MY MONEY!

# Budget

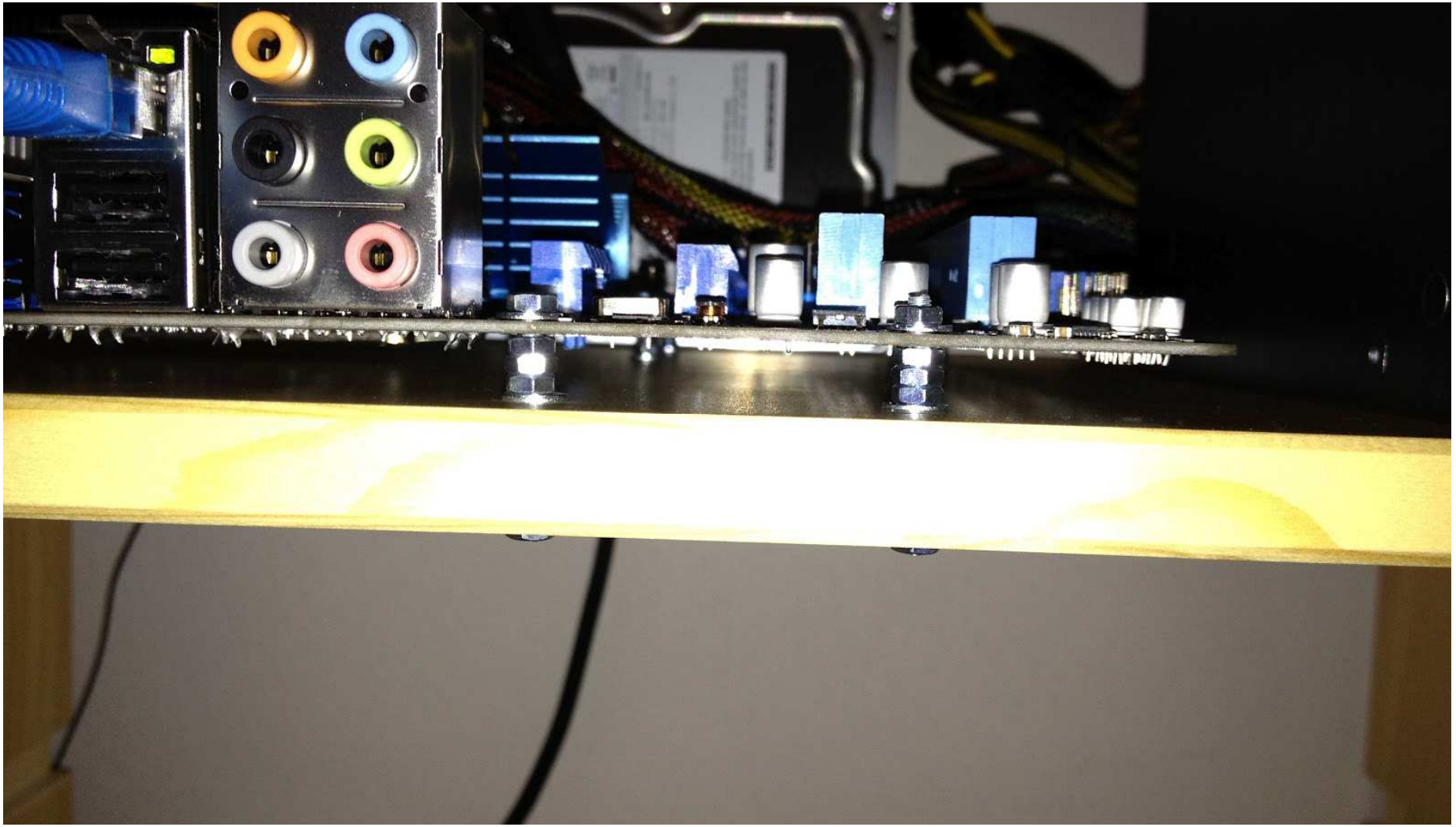
- Computer: €520
- MSDN License: €800 (€590 renewal)
- Year 1: €1320
- Year N: €590
- Money saved from stopped smoking (yearly): €2040

# Malware Lab

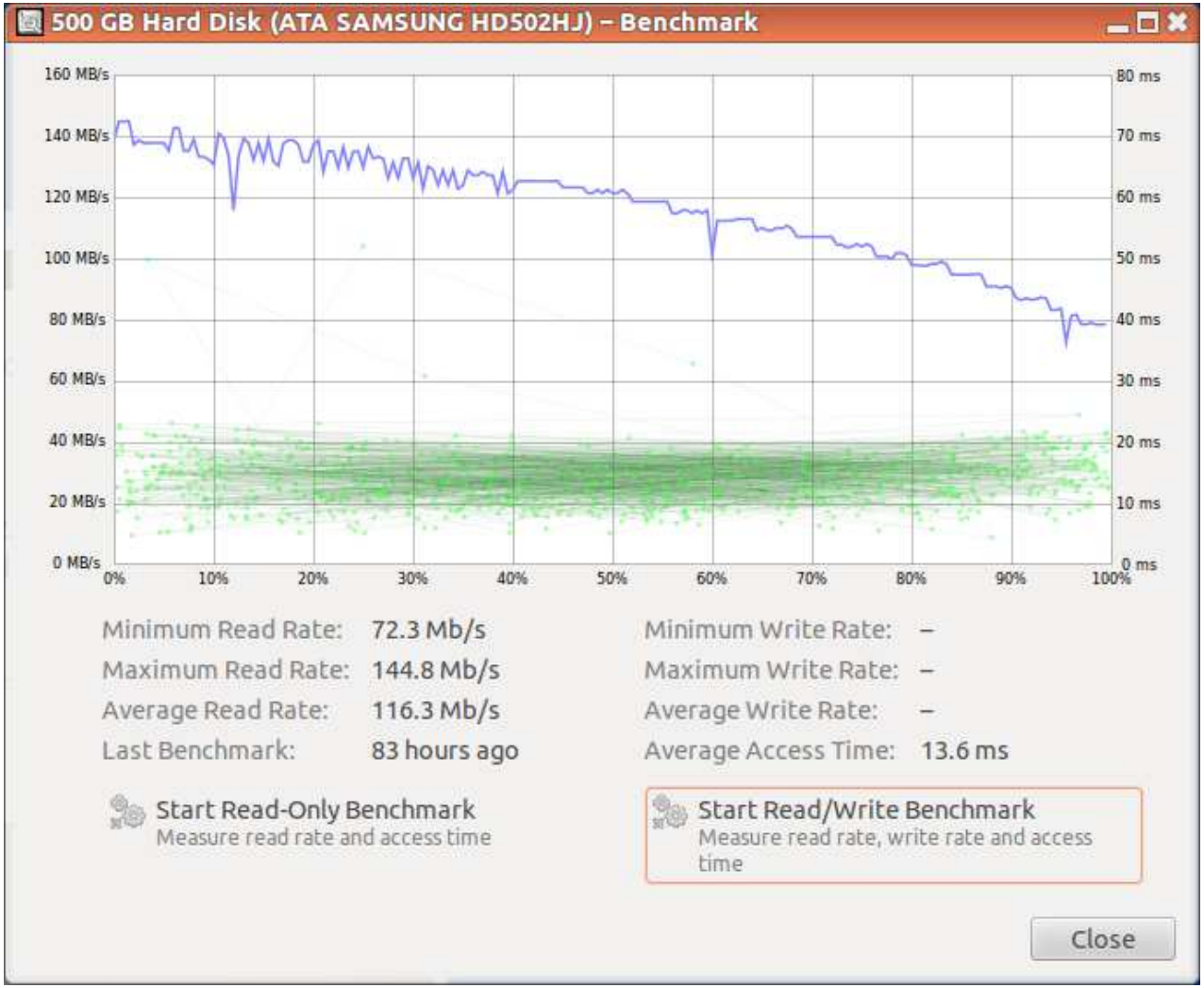
# MART Hardware (overview)



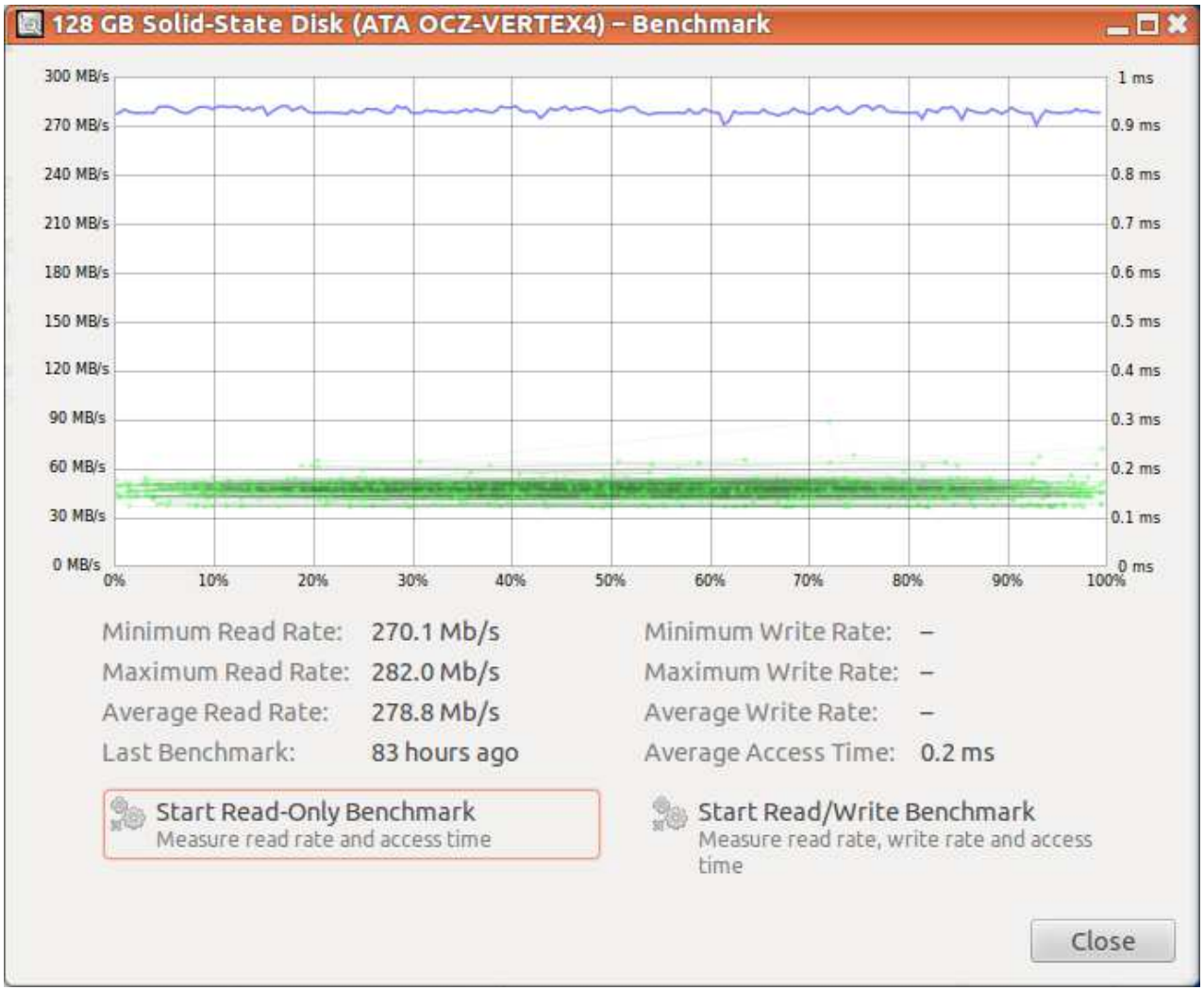
# MART Hardware (mounts)



# MART Hardware (HDD)



# MART Hardware (SSD)

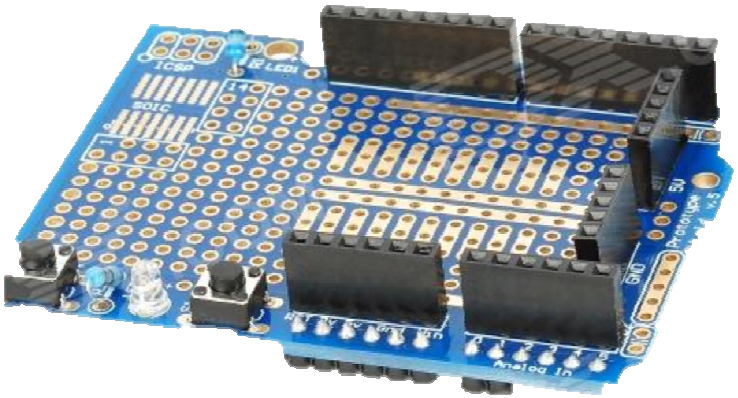


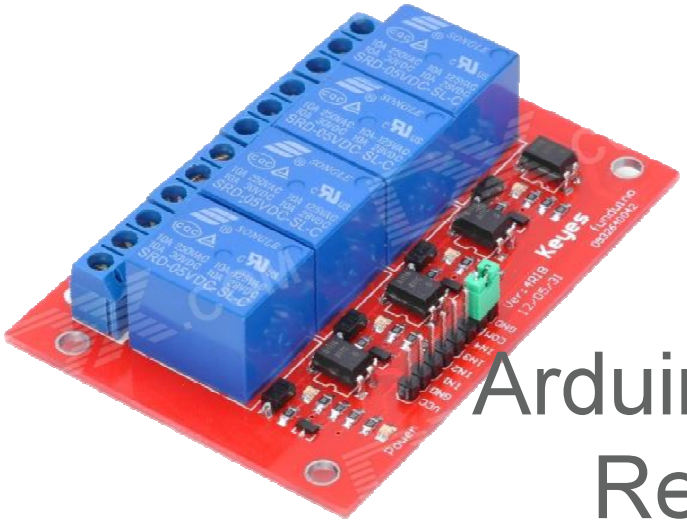
# Next steps

- Barebone on-the-iron malware analysis
- Android platform support
- OSX platform support
- iOS patform support

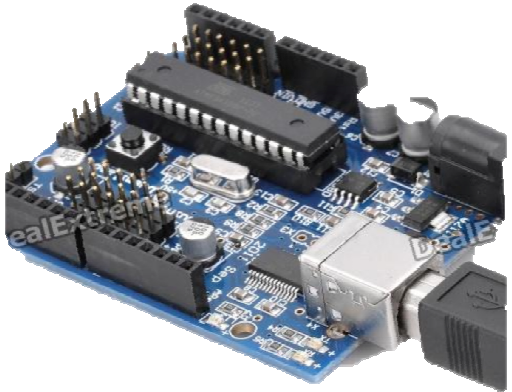

# Proof of Concept hardware

Prototype Shield

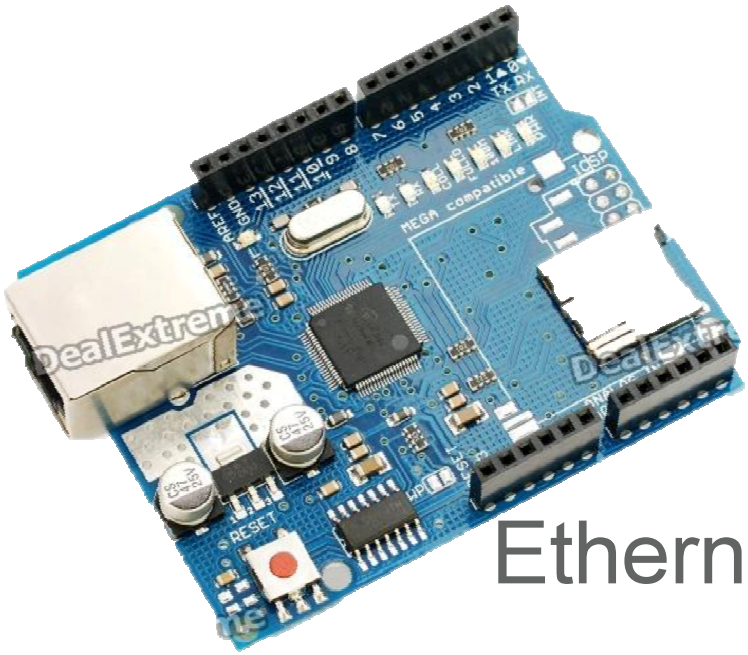




Arduino 4-Channel Relay Shield



Arduino Duemilanove



Ethernet Shield

2Secure

# Questions?

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

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