DIY Malware Analysis with Minibis

Christian Wojner, L. Aaron Kaplan
({wojner,kaplan}@cert.at)

* who knows minibis
* who uses minibis?

Overview

1. Overview
2. About CERT.at: our tools and services
3. Minibis
4. Minibis Applications
5. Future

Overview

1. last minute schedule change
2. This talk is a **preview** of the Minibis talk at FIRST2011.
3. Minibis 2.1b works, is downloadable for free and we use it ourselves

Overview CERT.at

{wojner,kaplan}@cert.at

2010/11/22

Overview CERT.at

- national CERT for Austria since 2008
- cooperation with chancellory of Austria: GovCERT.gv.at
- “Feuerwehr” (fire brigade) for the Internet of Austria
- CERT.at is a project of NIC.at (AT registry)

Overview CERT.at - Services

CERT.at

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Overview CERT.at - Services

CERT.at

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Overview CERT.at - Services

CERT.at

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

{wojner,kaplan}@cert.at

Overview CERT.at - Services

CERT.at

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓Risk Analysis
- ✓Business Continuity & Disaster Recovery Planning
- ✓Security Consulting
- ✓Awareness Building
- ✓Education/Training
- ✓Product Evaluation or Certification

{wojner,kaplan}@cert.at

Overview CERT.at - Services

CERT.at

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓Risk Analysis
- ✓Business Continuity & Disaster Recovery Planning
- ✓Security Consulting
- ✓Awareness Building
- ✓Education/Training
- ✓Product Evaluation or Certification

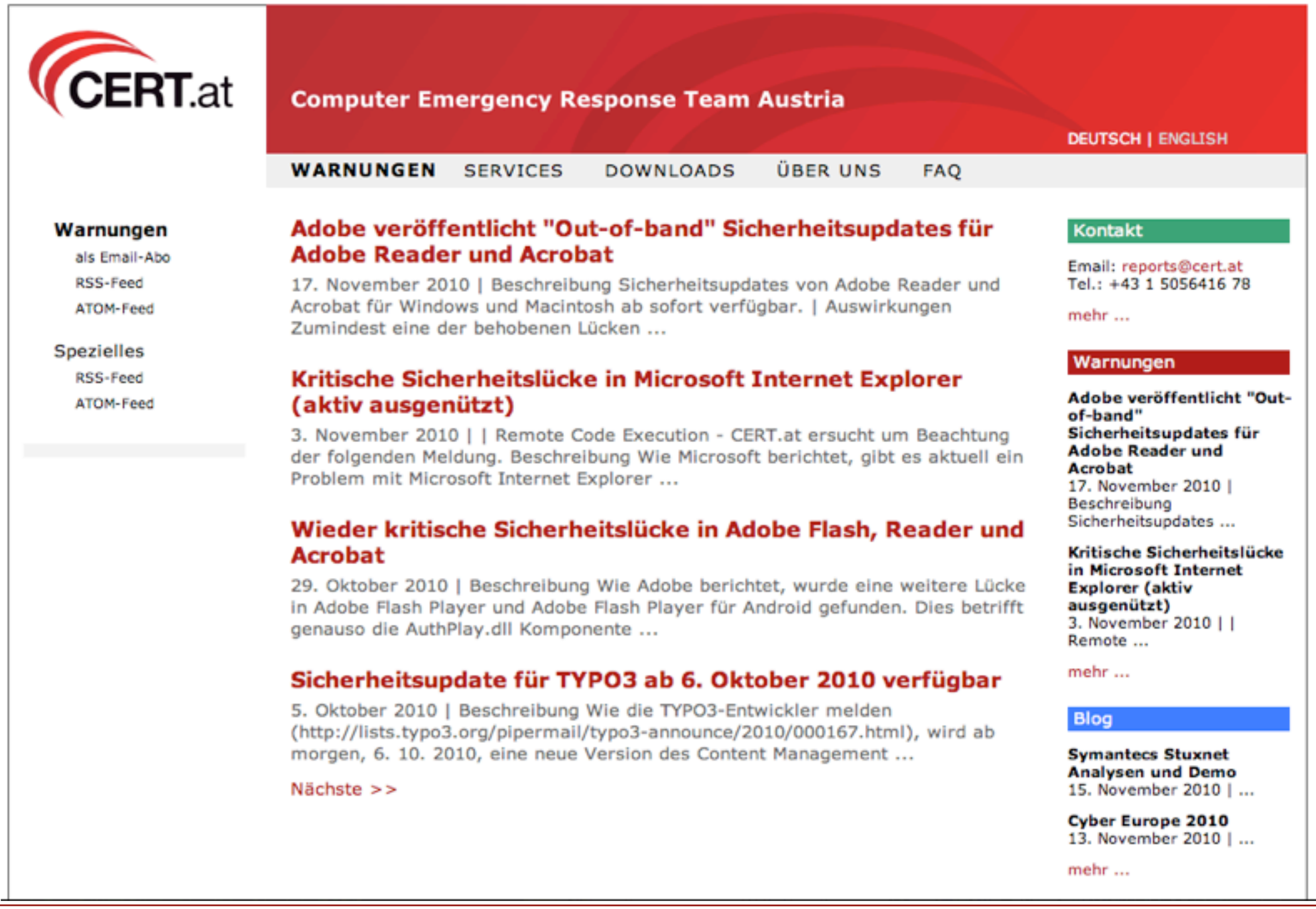
{wojner,kaplan}@cert.at

Overview CERT.at - Services

- regular trainings (TRANSITs, “IT Security Stammtisch”)
- Warning@lists.cert.at ML
- Discuss@lists.cert.at ML

- Purpose: information hub for IT Security incidents
- We are **not the police**

Overview CERT.at - Contact



DYI mass malware analysis with Minibis

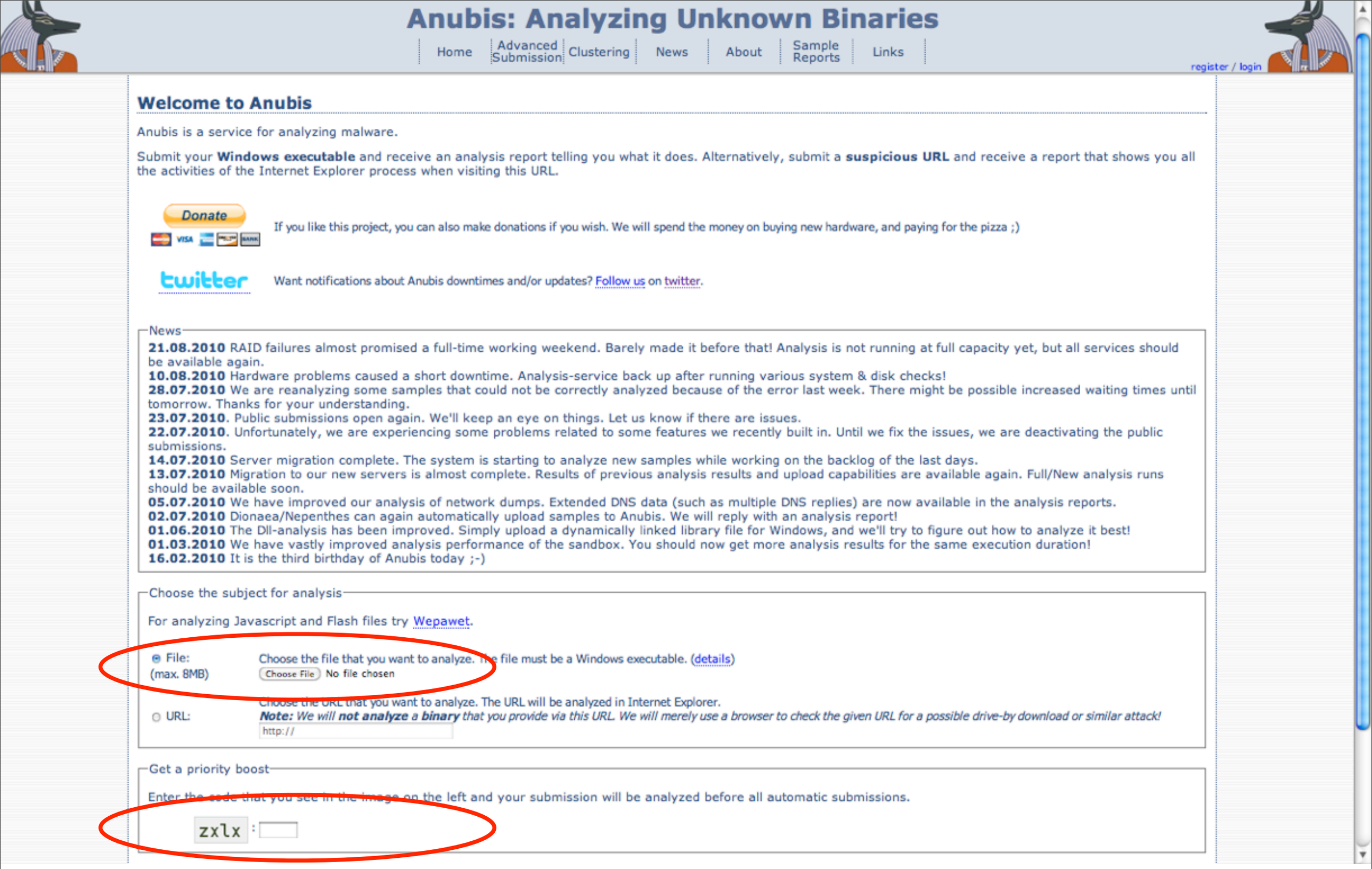
2010/11/22 {wojner,kaplan}@cert.at

Minibis - History

CERT.at

1. Our inspiration:
   Anubis = “**An**alyzing **u**nknown **bi**naries”
2. we needed some **offline** analysis capabilities
3. License costs/time issue

{wojner,kaplan}@cert.at



credits: iseclab

Minibis - Motivation

- Problem: malware can check if it runs on the Anubis server (via IP addr)
- http://avtracker.info
- We run on $IP ;-)
- … or not connected to the network at all
- … or (potentially) connected to a honeynet
- license: ISCL (~ BSD license)
- actually, it was a proof of concept: does malware check for virtualization?

Minibis - Evolution

CERT.at

{wojner,kaplan}@cert.at

Minibis - Evolution

{wojner,kaplan}@cert.at

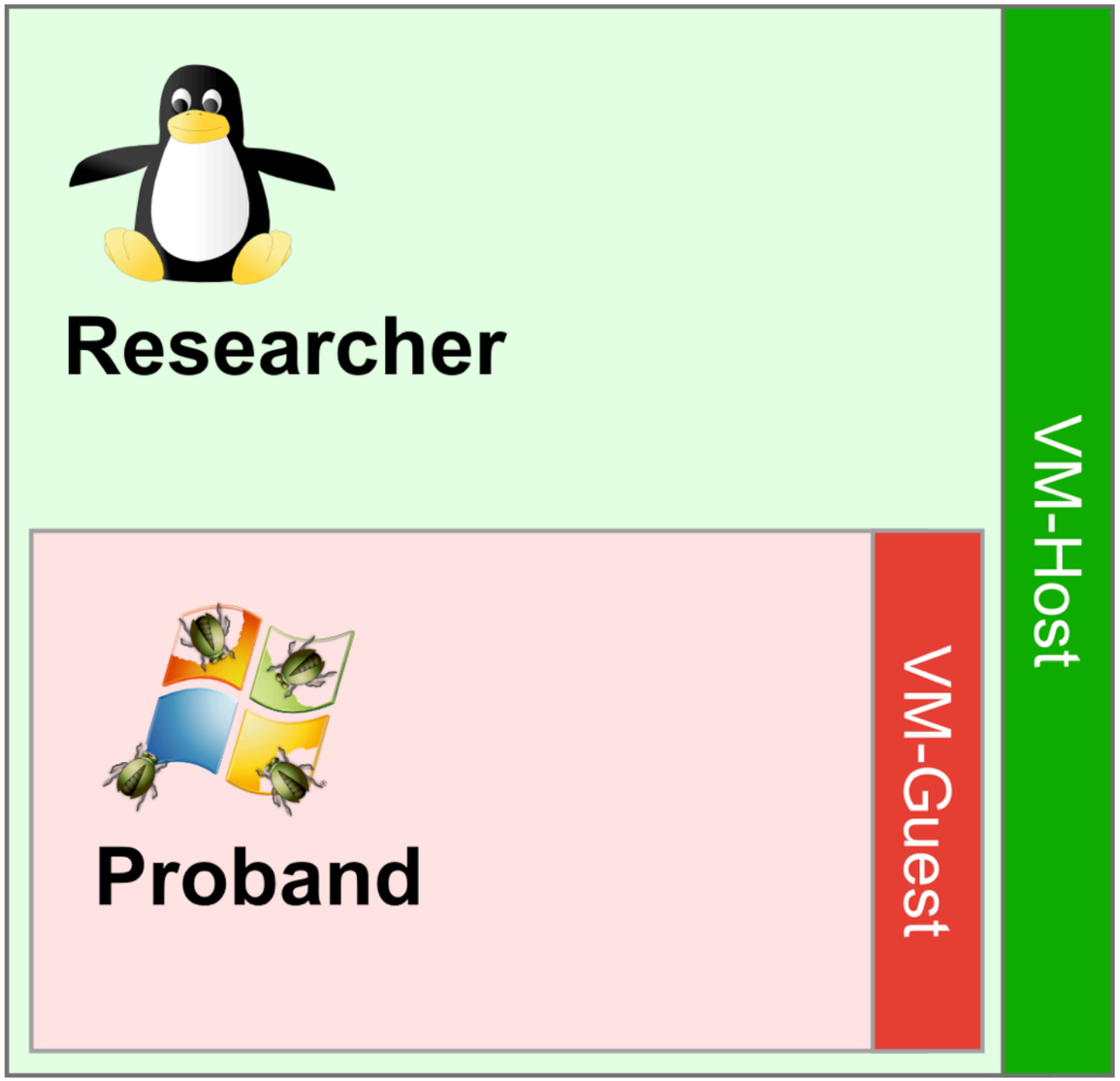
Minibis - Basic Idea

Behavorial Analysis Steps

CERT.at

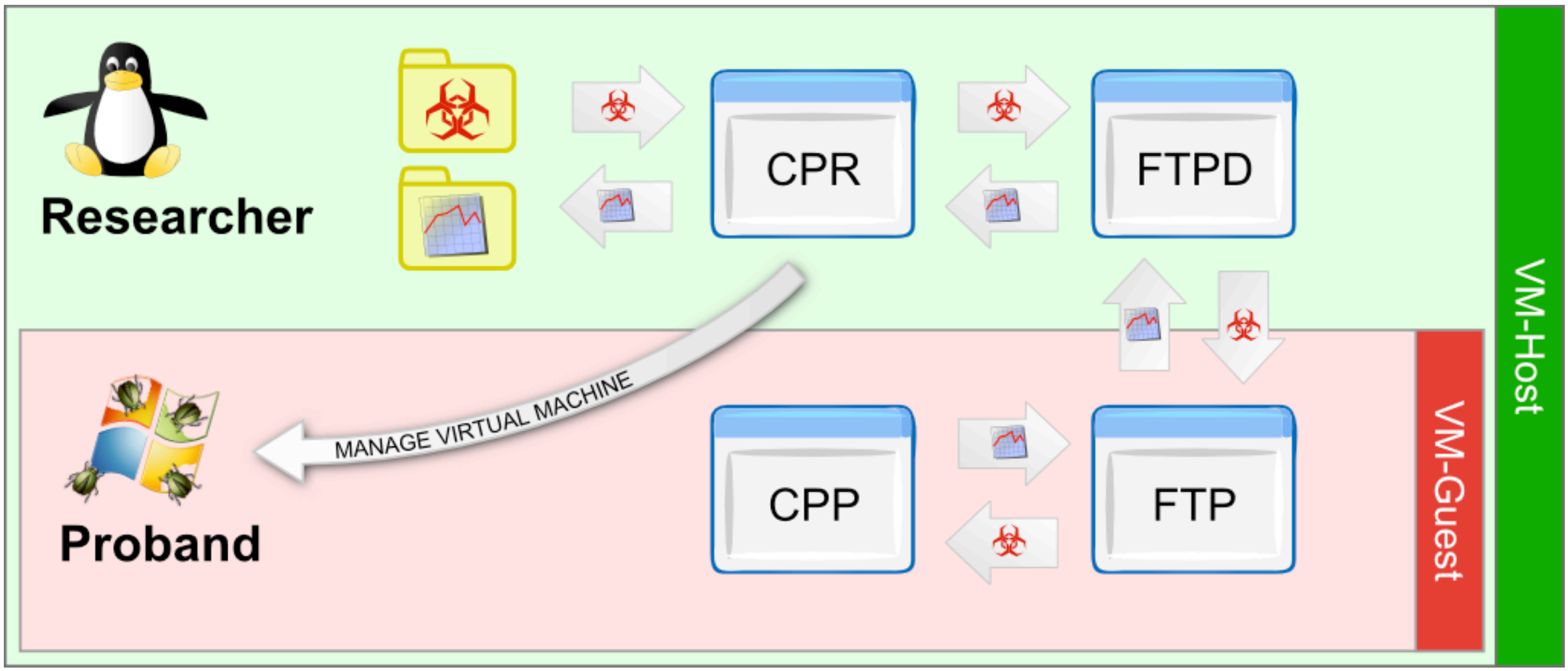
1. Prepare system (virtual machine) with monitoring tools
2. Transfer sample to virtual machine
3. Start up monitoring tools in the VM
4. Run sample
5. Give sample some time to do nasty things
6. Save monitoring logs and transfer them back
7. Analyze logs
8. (Revert VM)

Minibis - Architectural Concept

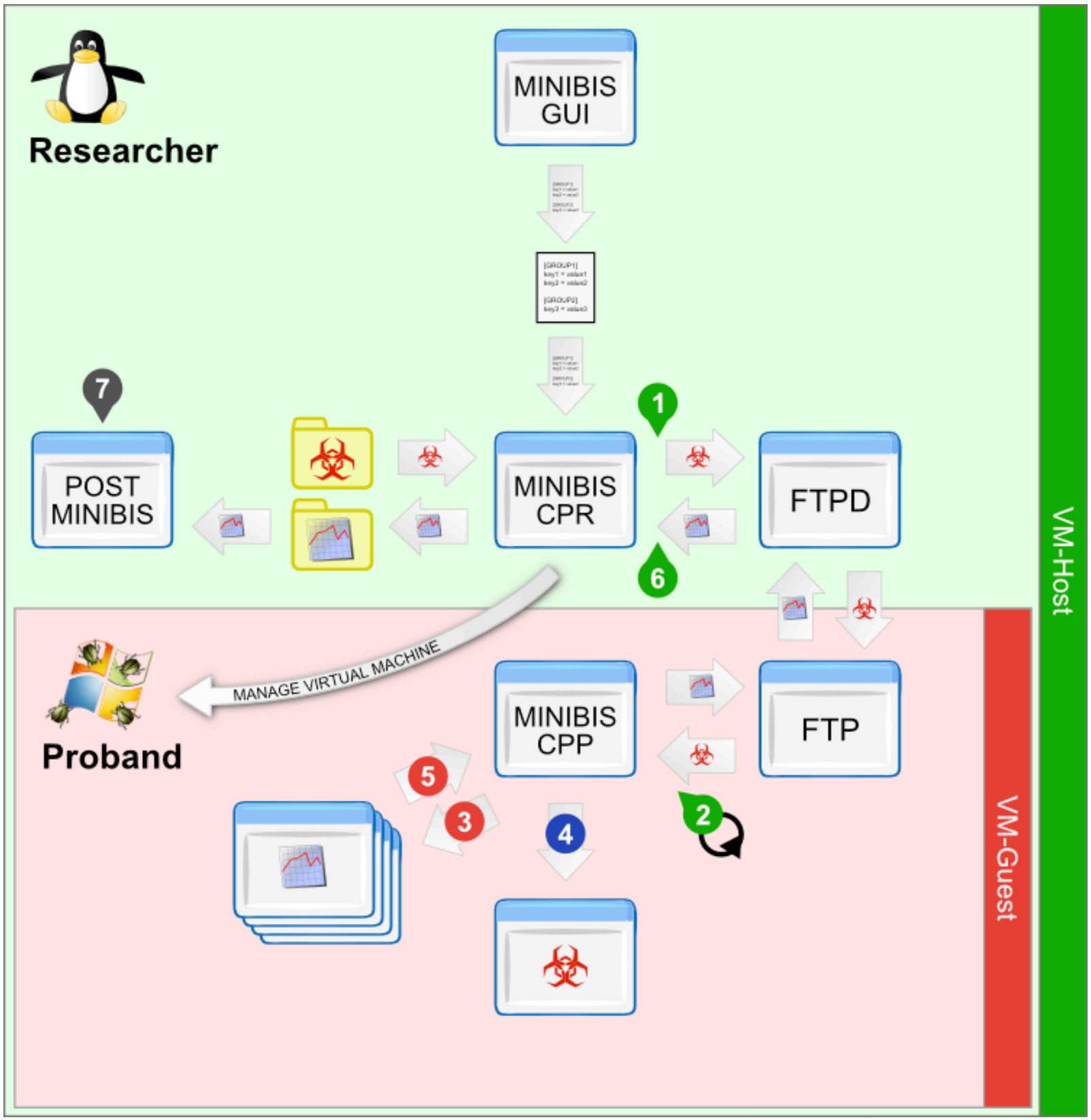


{wojner,kaplan}@cert.at

Minibis - Architectural Concept (2)



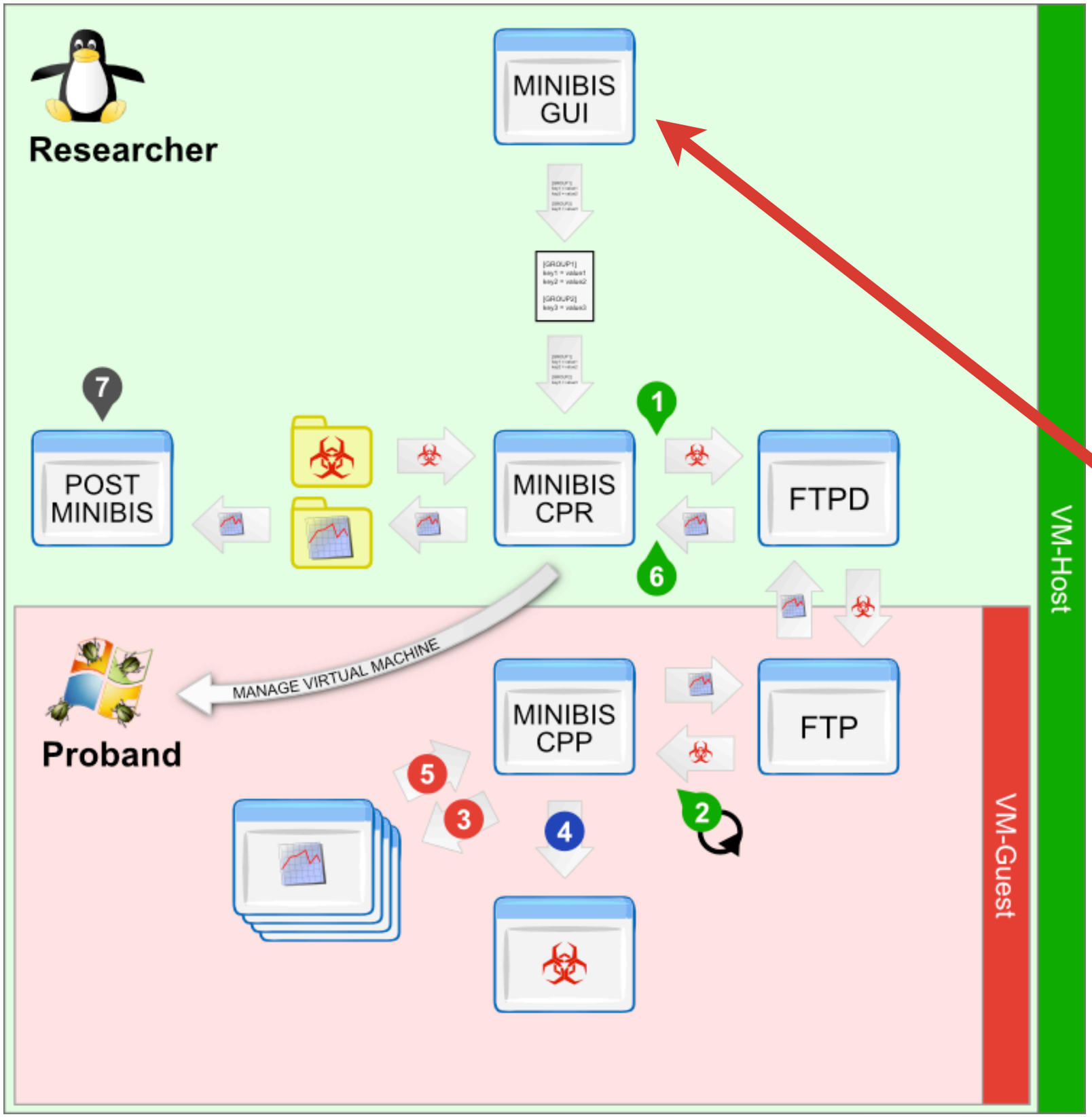
CPR = controller process researcher
CPP = controller process proband



Architectural Concept (3)

color legend:
tab researcher
tab Proband
tab sample type
postminibis plugins

{wojner,kaplan}@cert.at

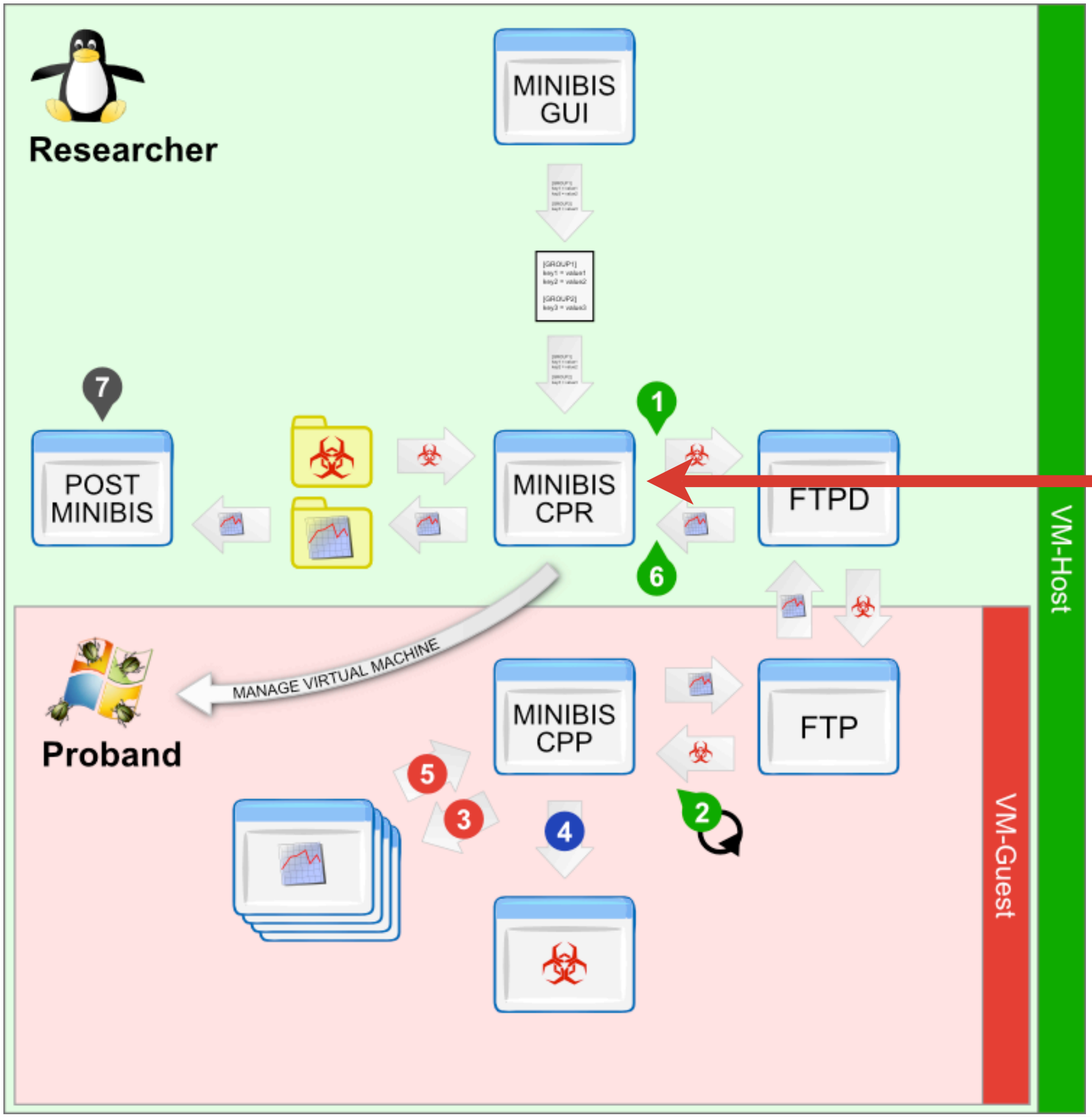


Architectural Concept (3)

minibis-gui: for configuration, progress/status view

color legend:
tab researcher
tab Proband
tab sample type
postminibis plugins

{wojner,kaplan}@cert.at

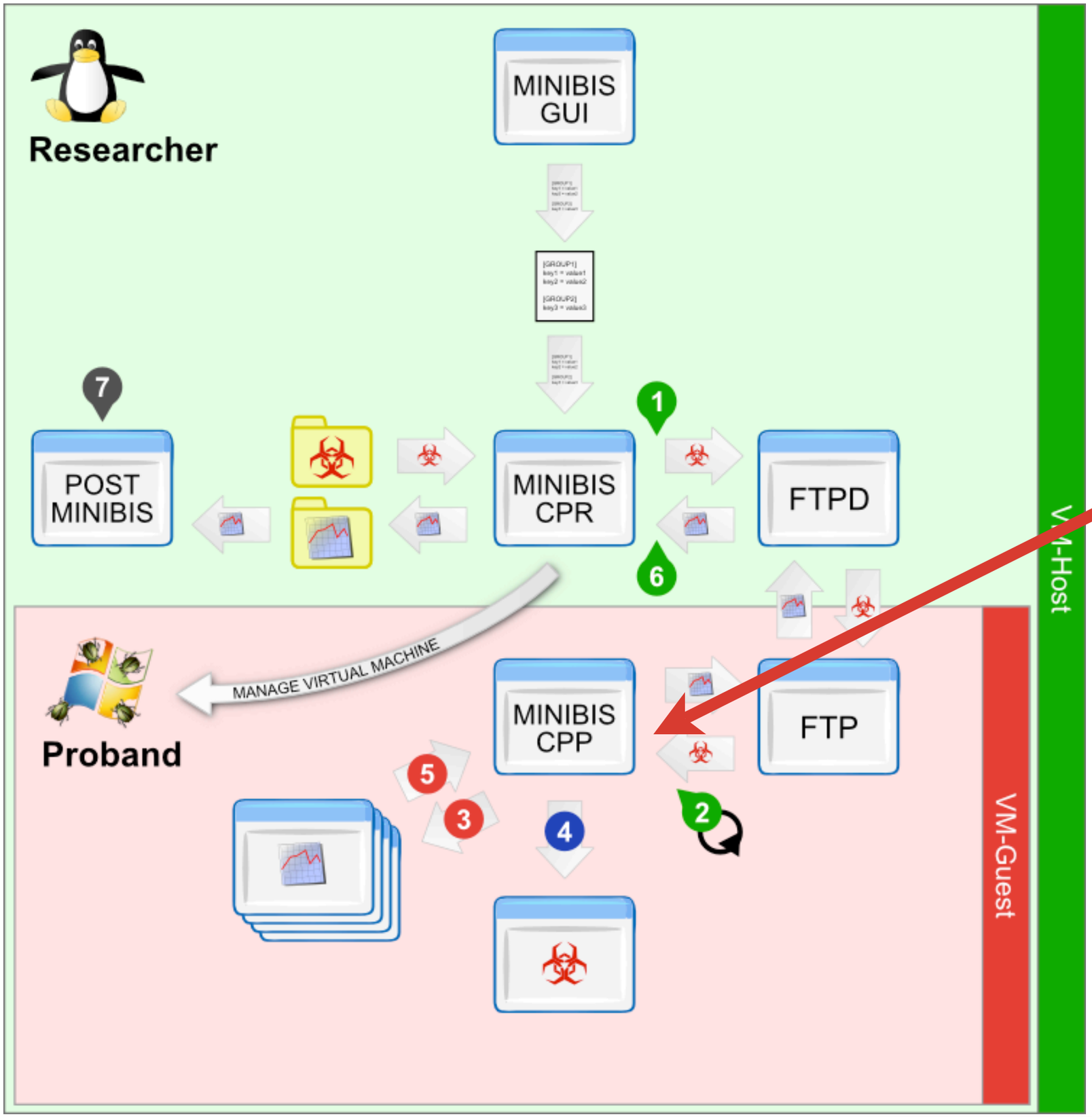


Architectural Concept (3)

minibis-cpr:
“controller process of researcher”

color legend:
tab researcher
tab Proband
tab sample type
postminibis plugins

{wojner,kaplan}@cert.at

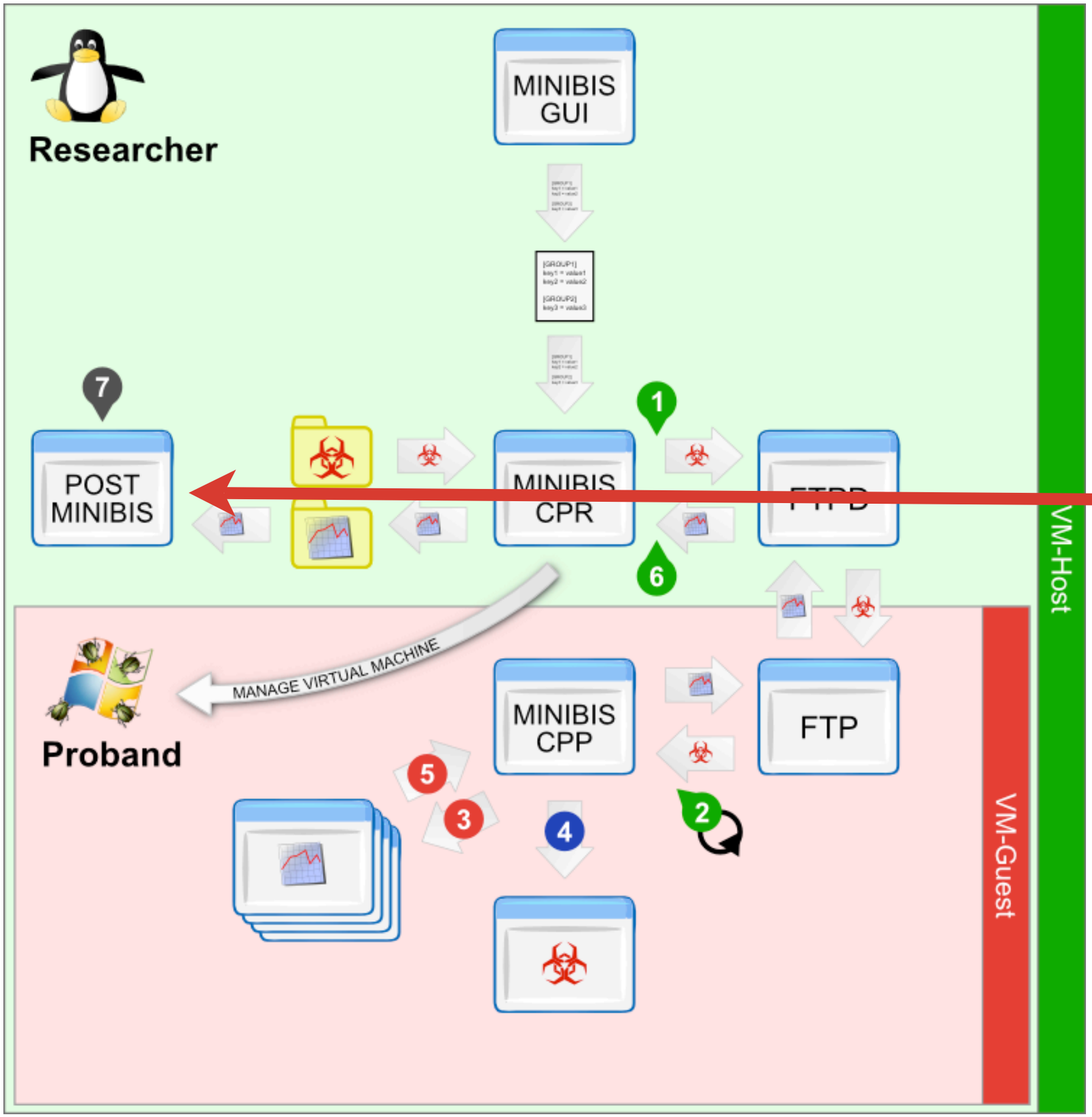


Architectural Concept (3)

minibis-cpp:
“controller process of proband”

color legend:
tab researcher
tab Proband
tab sample type
postminibis plugins

{wojner,kaplan}@cert.at



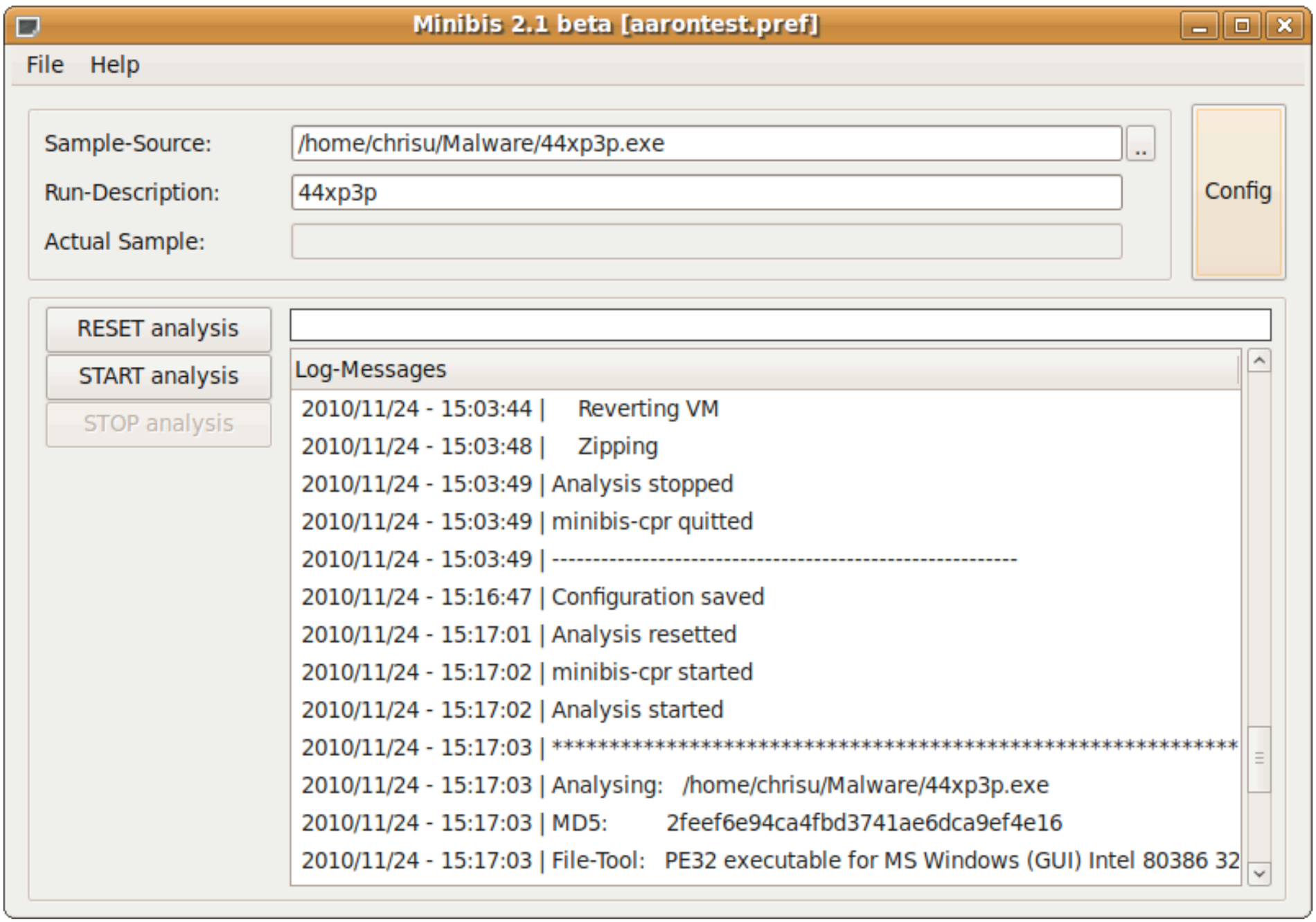
Architectural Concept (3)

postminibis: log file classification/ interpretation

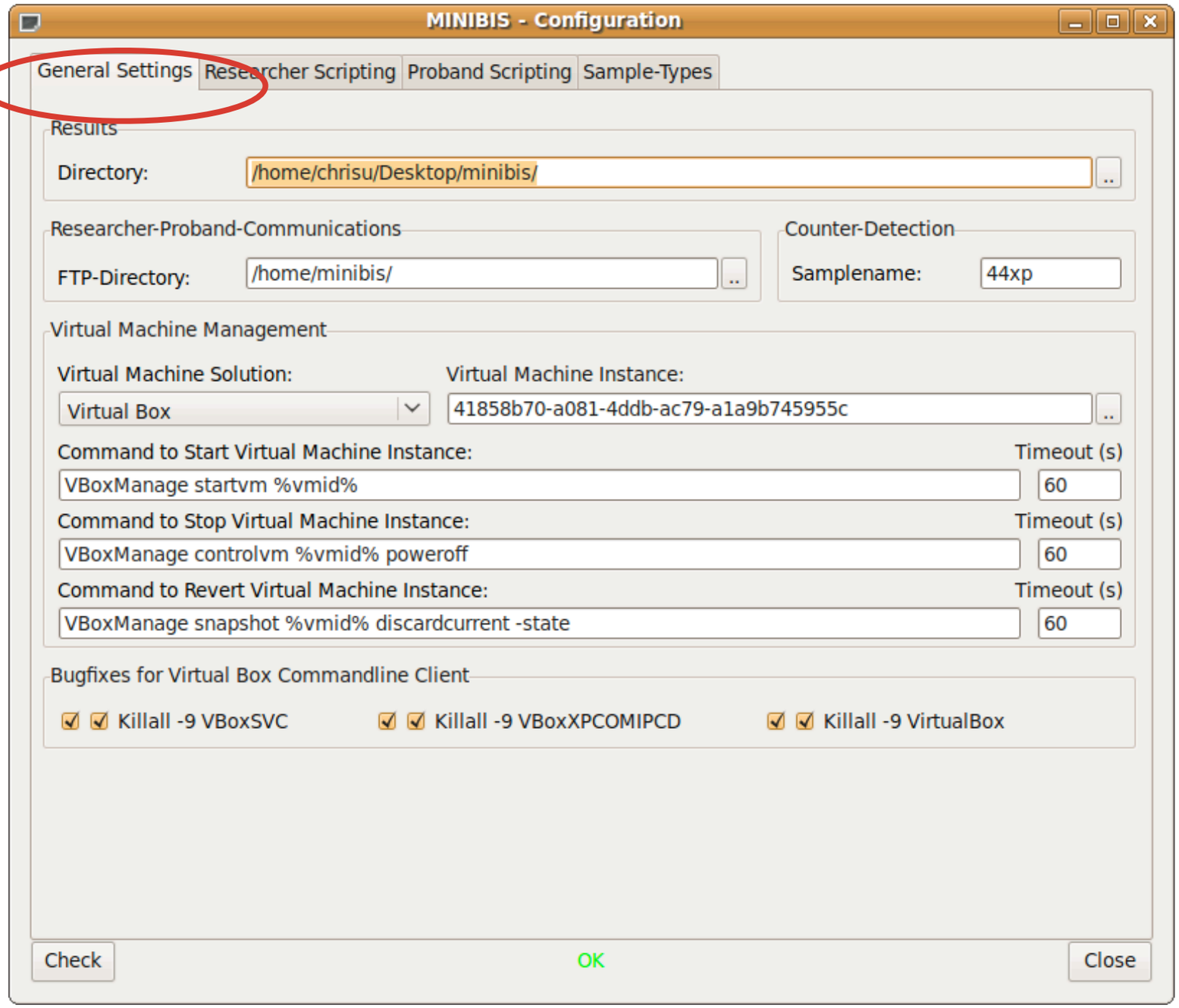
color legend:
tab researcher
tab Proband
tab sample type
postminibis plugins

{wojner,kaplan}@cert.at

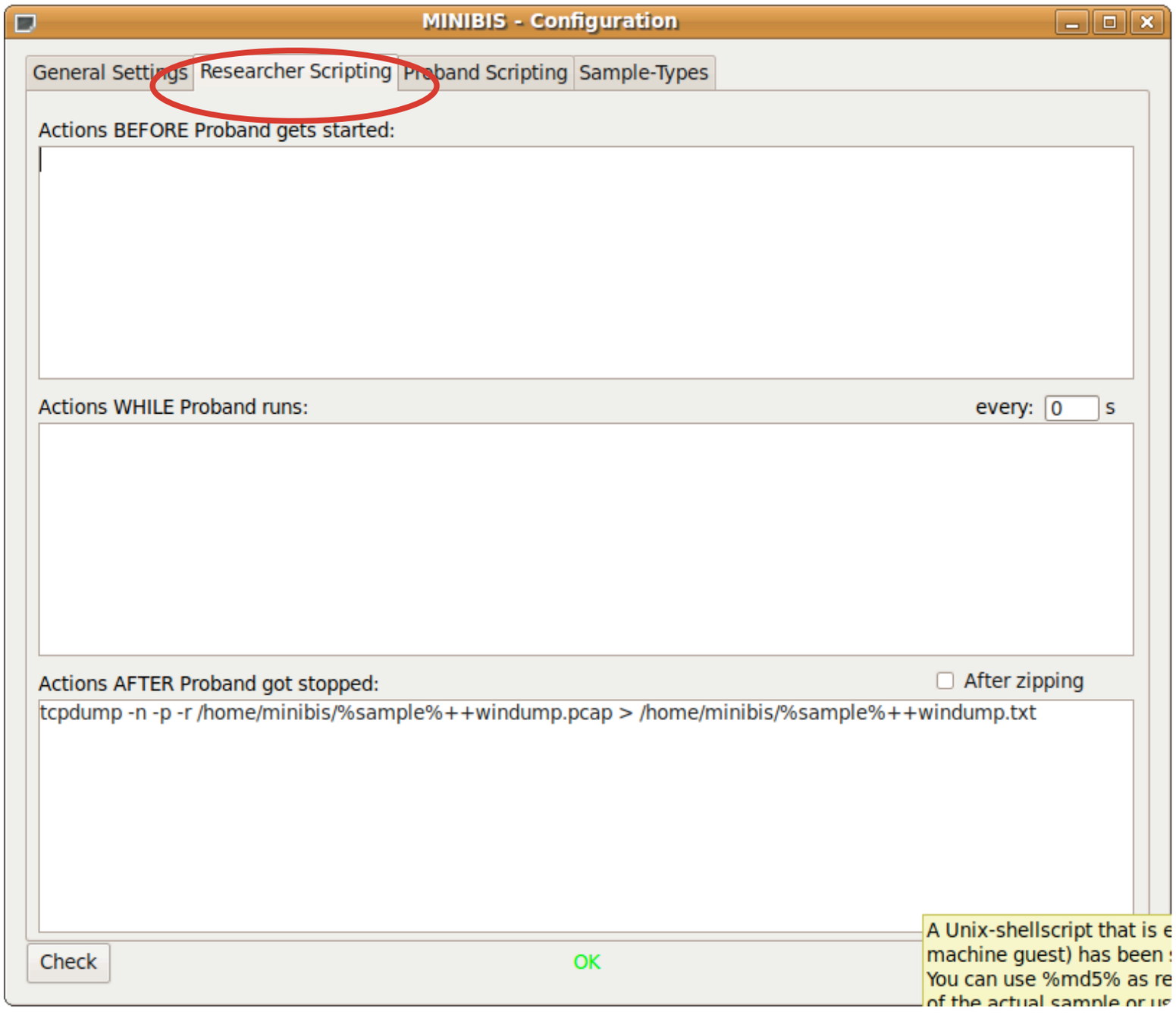
Walkthrough - Main screen



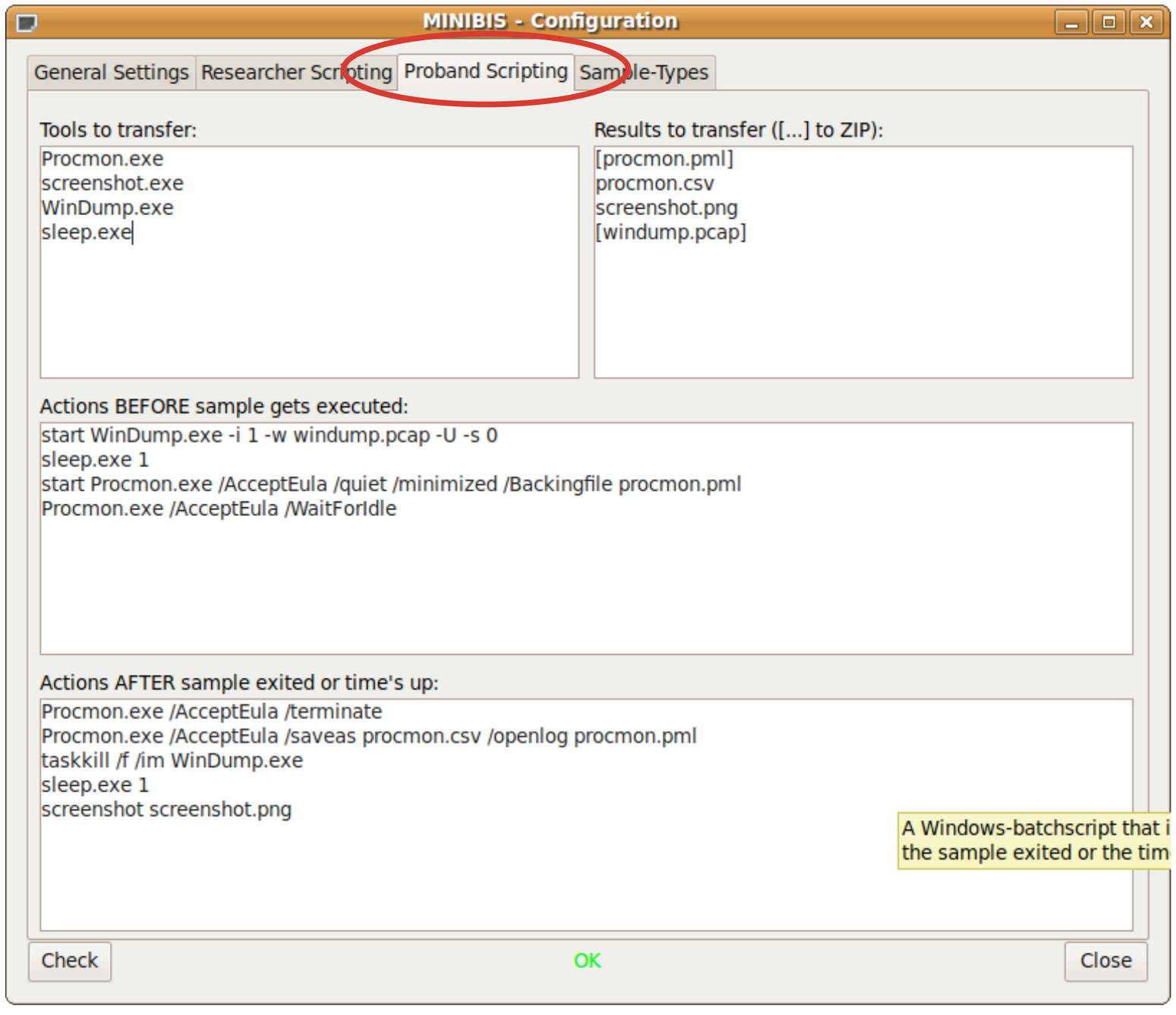
Walkthrough - Config->General



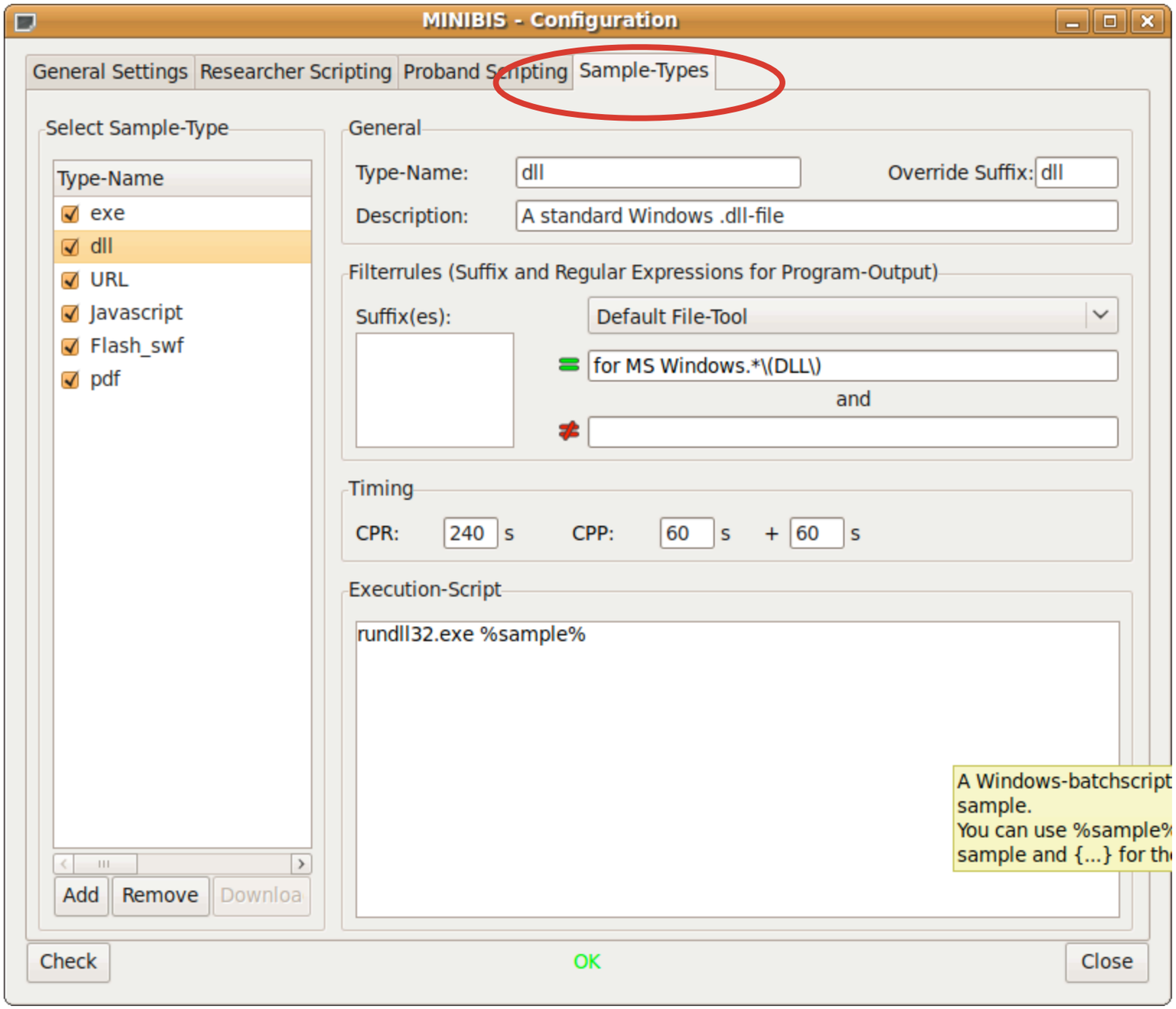
Walkthrough - Config->Researcher



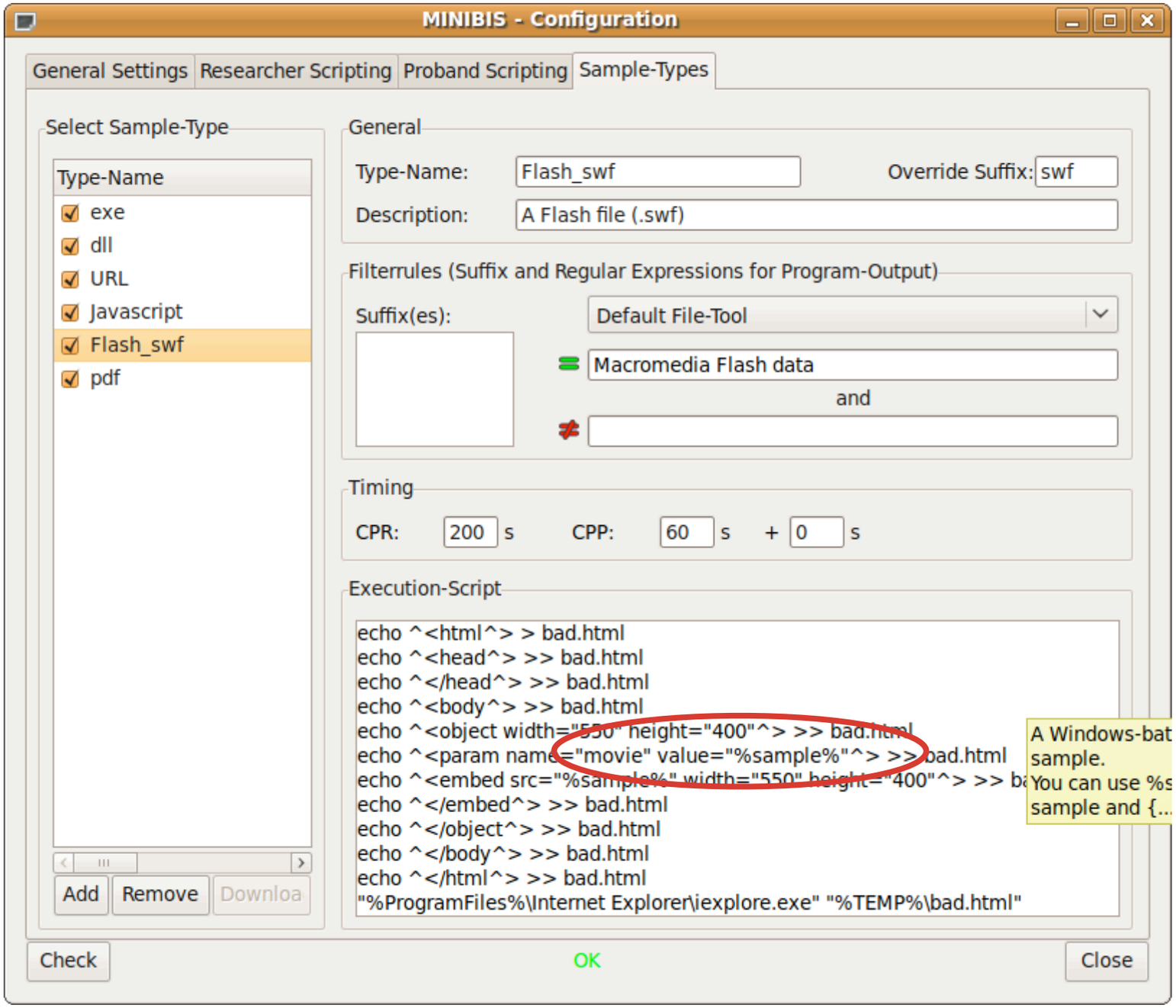
Walkthrough - Config->Proband



Walkthrough - Config->Sample Types



Walkthrough - Config->Sample Types



Output directory organization

filename = “$md5++internal_vmid+sample_type++resultfile

Result folder (based on config)/

|- *YYYY/*

|-- *MM/*

|- *DD/*

|- *HHMISS/*

|- *filename*

postminibis

- Analyse results, classify (alert, warning, info level)
- extensible via shell scripting for any log file coming out of Minibis
- toolset for interpretation of result files

```
$ postminibis \
  /minibis/2010/11/24/171328/| \
   grep ";a;"
```

dient zur analyse der ergebnis files und zur klassifikation der alert/warning/info levels
Weiters: es ist mittels shell script plugins beliebig erweiterbar fuer beliebie analyse output files von minibis
* scriptable
* must parse CSV syntax
* toolset for interpretation of result files

Typical output of postminibis

- d407ebf73d25715050bea07fdbfb76a5;2010/11/24-16:15:27;**;a;Se**
tting autostart-registry-key *"HKLM\SOFTWARE\Microsoft\Windows*
\CurrentVersion\RunServices\Microsoft Update 32"
=> ,"SUCCESS","Type: REG_SZ, Length: 24, Data: *network.exe*"

Typical output of postminibis

- d407ebf73d25715050bea07fdbfb76a5;2010/11/24-16:15:27;**;a;Se**
tting autostart-registry-key *"HKLM\SOFTWARE\Microsoft\Windows*
\CurrentVersion\RunServices\Microsoft Update 32"
=> ,"SUCCESS","Type: REG_SZ, Length: 24, Data: *network.exe*"

Typical output of postminibis

- d407ebf73d25715050bea07fdbfb76a5;2010/11/24-16:15:27;**a;Setting autostart-registry-key** *"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Update 32"*
=> ,"SUCCESS","Type: REG_SZ, Length: 24, Data: *network.exe*"

Typical output of postminibis

• d407ebf73d25715050bea07fdbfb76a5;2010/11/24-16:15:27;**;a;Se**
tting autostart-registry-key *"HKLM\SOFTWARE\Microsoft\Windows*
\CurrentVersion\RunServices\Microsoft Update 32"
=> ,"SUCCESS","Type: REG_SZ, Length: 24, Data: *network.exe*"

Typical output of postminibis

- d407ebf73d25715050bea07fdbfb76a5;2010/11/24-16:15:27;**;a;Se**
tting autostart-registry-key *"HKLM\SOFTWARE\Microsoft\Windows*
\CurrentVersion\RunServices\Microsoft Update 32"
=> ,"SUCCESS","Type: REG_SZ, Length: 24, Data: *network.exe*"

Example for interpreting results

Top-5 of most-used autorun-registrykeys for 3000 samples

```
$./postminibis ~/Minibis/Results/2010/11/10/120000/ | grep
";a;" | grep "registry" | cut -d\; -f 5 | cut -f 2 -d'"' | sort |
uniq - -c | sort -rn

   1161 HKLM\SOFTWARE\Microsoft\Windows\
        CurrentVersion\Run
    887 HKLM\System\CurrentControlSet\
        Services
    113 HKCU\Software\Microsoft\Windows\
        CurrentVersion\Run
    101 HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Userinit
     85 HKLM\Software\Microsoft\Windows\
        CurrentVersion\Explorer\Browser
        Helper Objects
```

Future

- Parallelization
- Diffs over different VM configurations (browser, windows version, etc)
- GUI for postminibis
- Installer
- Support for more VMs (VMWare, Qemu)
- 64 Bit Linux version, OS X version
- Support for physical machines (data recovery cards)
- Support GUI based tools in VM
- More sample scripts
- Community...

Community

CERT.at

minibis

Software and tips to easily build up an automated malware analysis station

Search project

Project Home | Downloads | Wiki | Issues | Source | Administer

Summary | Updates | People

Tip: Project owners, see our Getting Started guide for steps to configure your project. hide

Software and tips to easily build up an automated malware analysis station based on a concept introduced in the paper "Mass Malware Analysis: A Do-It-Yourself Kit".

See also: http://cert.at/downloads/software/minibis_en.html

Star this project

Activity: Low

Code license:
Other Open Source
See source for details

[redacted]

Community

CERT.at

minibis

Software and tips to easily build up an automated malware analysis station

Search project

Project Home | Downloads | Wiki | Issues | Source | Administer

Summary | Updates | People

Tip: Project owners, see our Getting Started guide for steps to configure your project. hide

Software and tips to easily build up an automated malware analysis station based on a concept introduced in the paper "Mass Malware Analysis: A Do-It-Yourself Kit".

See ...

Star this project

Activity: ...

Code license:
Other Open Source
See source for details

http://code.google.com/p/minibis

[redacted]

{wojner,kaplan}@cert.at

Thanks!

{wojner,kaplan}@cert.at