

DIY Malware Analysis with Minibis

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

2010/11/22

1

* who knows minibis

* who uses minibis?

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

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

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

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	

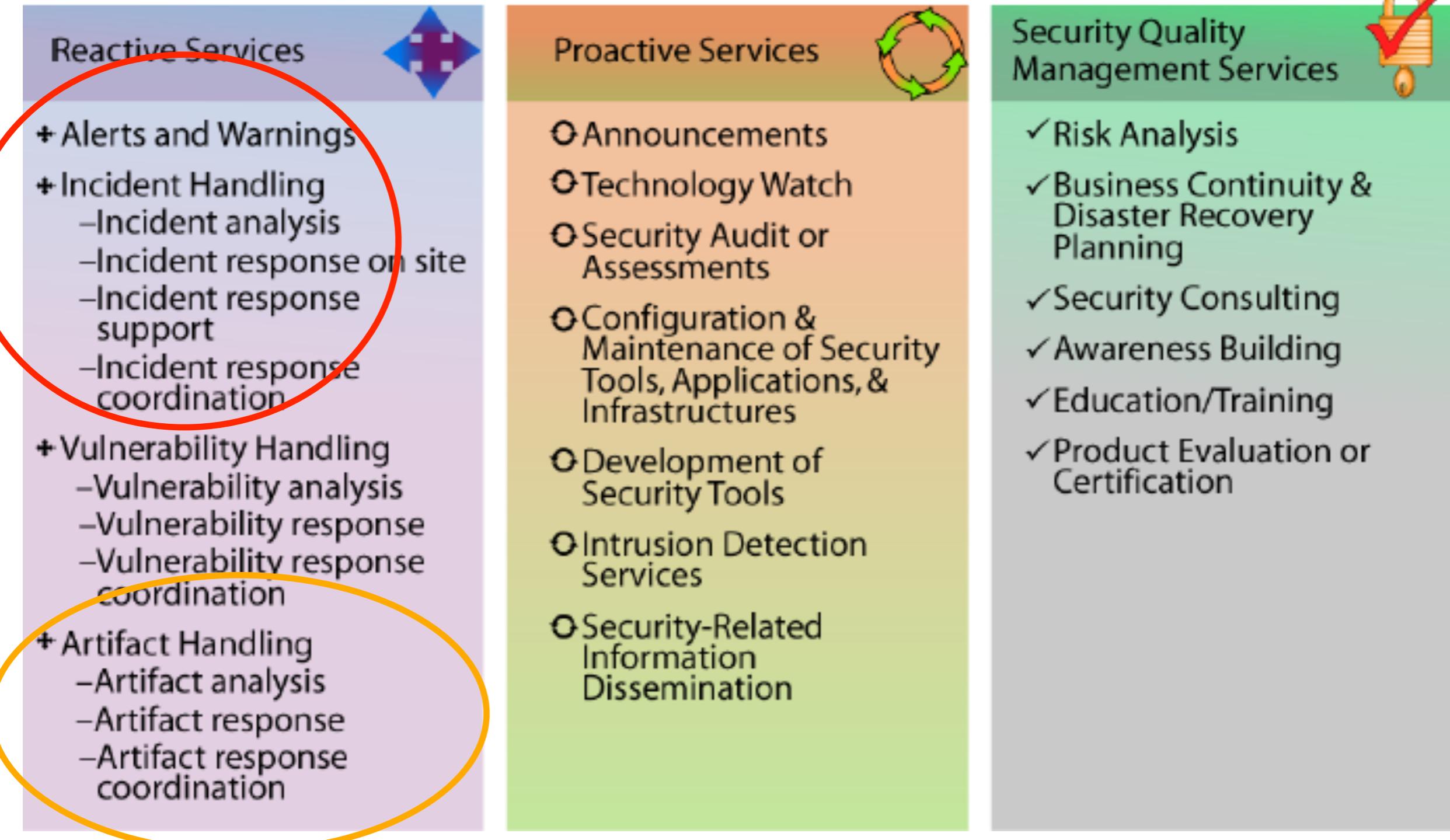
Overview CERT.at - Services

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

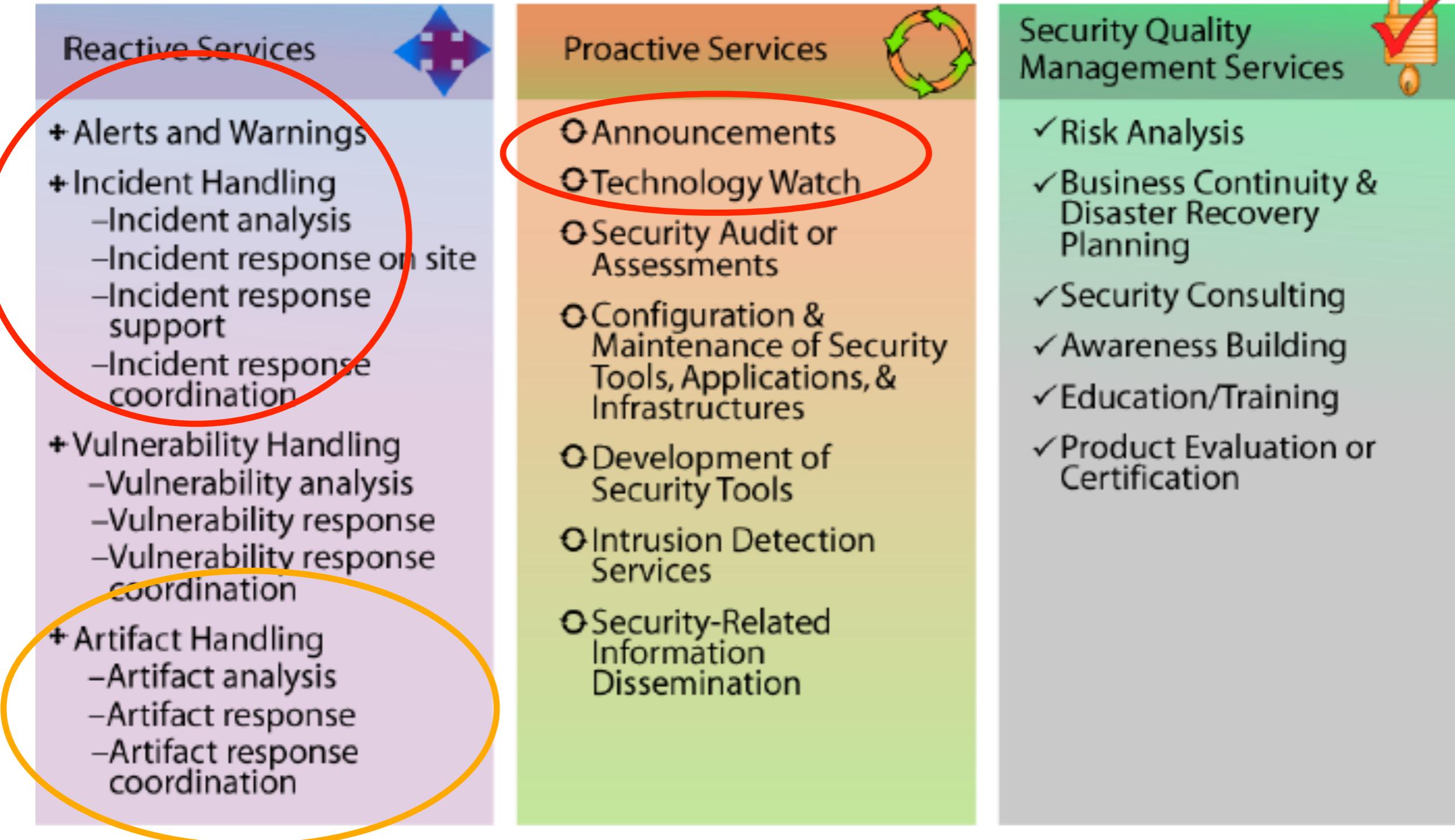
Proactive Services
○ Announcements
○ Technology Watch
○ Security Audit or Assessments
○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
○ Development of Security Tools
○ Intrusion Detection Services
○ Security-Related Information Dissemination

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

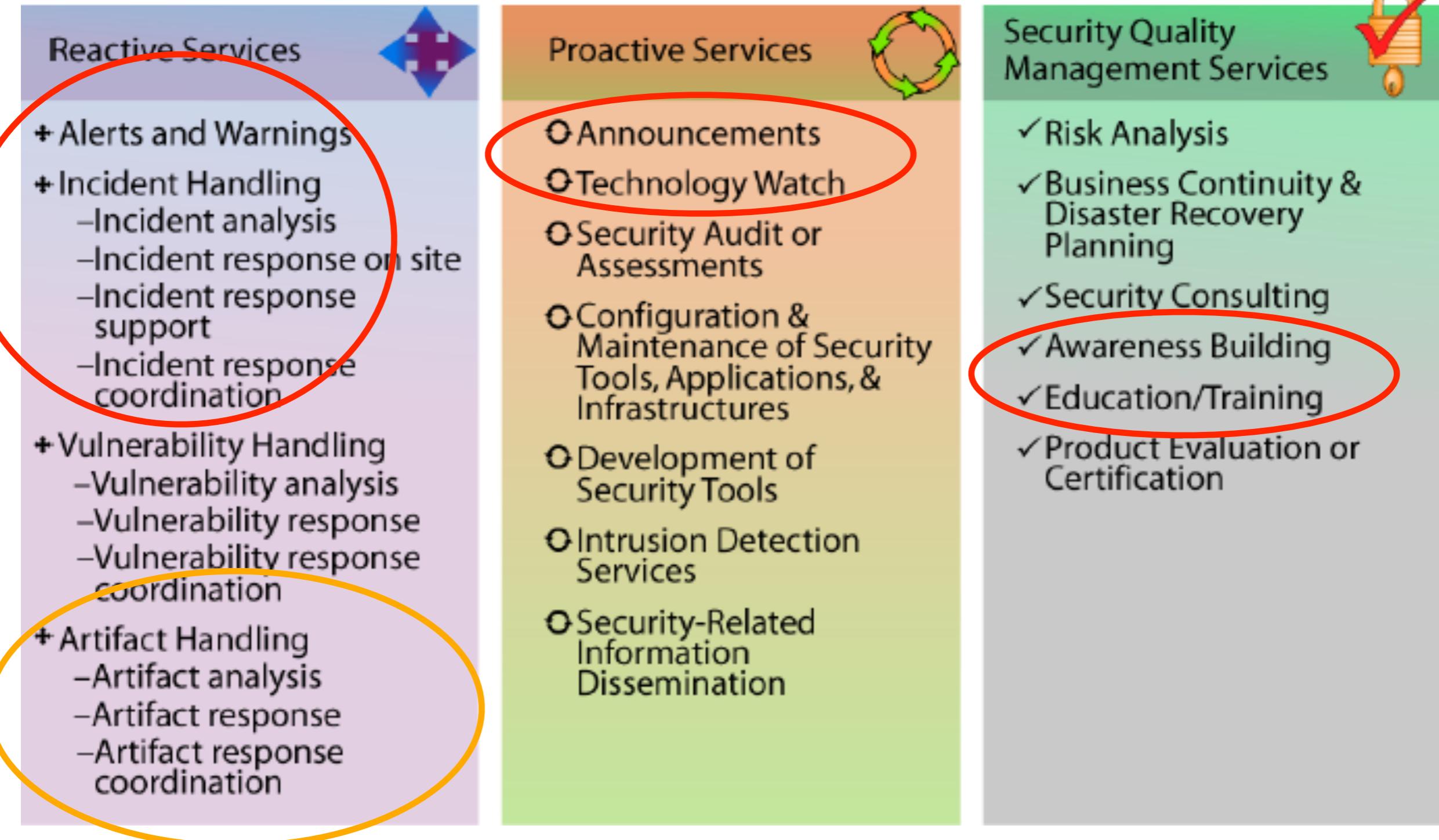
Overview CERT.at - Services



Overview CERT.at - Services



Overview CERT.at - Services



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



CERT.at

Computer Emergency Response Team Austria

DEUTSCH | ENGLISH

WARNUNGEN **SERVICES** **DOWNLOADS** **ÜBER UNS** **FAQ**

Warnungen

als Email-Abo
RSS-Feed
ATOM-Feed

Spezielles

RSS-Feed
ATOM-Feed

Adobe veröffentlicht "Out-of-band" Sicherheitsupdates für Adobe Reader und Acrobat

17. November 2010 | Beschreibung Sicherheitsupdates von Adobe Reader und Acrobat für Windows und Macintosh ab sofort verfügbar. | Auswirkungen Zumindest eine der behobenen Lücken ...

Kritische Sicherheitslücke in Microsoft Internet Explorer (aktiv ausgenützt)

3. November 2010 | Remote Code Execution - CERT.at ersucht um Beachtung der folgenden Meldung. Beschreibung Wie Microsoft berichtet, gibt es aktuell ein Problem mit Microsoft Internet Explorer ...

Wieder kritische Sicherheitslücke in Adobe Flash, Reader und Acrobat

29. Oktober 2010 | Beschreibung Wie Adobe berichtet, wurde eine weitere Lücke in Adobe Flash Player und Adobe Flash Player für Android gefunden. Dies betrifft genauso die AuthPlay.dll Komponente ...

Sicherheitsupdate für TYPO3 ab 6. Oktober 2010 verfügbar

5. Oktober 2010 | Beschreibung Wie die TYPO3-Entwickler melden (<http://lists.typo3.org/pipermail/typo3-announce/2010/000167.html>), wird ab morgen, 6. 10. 2010, eine neue Version des Content Management ...

[Nächste >>](#)

Kontakt

Email: reports@cert.at
Tel.: +43 1 5056416 78
[mehr ...](#)

Warnungen

Adobe veröffentlicht "Out-of-band" Sicherheitsupdates für Adobe Reader und Acrobat
17. November 2010 | Beschreibung Sicherheitsupdates ...

Kritische Sicherheitslücke in Microsoft Internet Explorer (aktiv ausgenützt)
3. November 2010 | Remote ...

Blog

Symantecs Stuxnet Analysen und Demo
15. November 2010 | ...

Cyber Europe 2010
13. November 2010 | ...

[mehr ...](#)

DYI mass malware analysis with Minibis



Minibis - History



1. Our inspiration:
Anubis = “Analyzing unknown binaries”
2. we needed some
offline analysis
capabilities
3. License costs/time
issue



Welcome to Anubis

Anubis is a service for analyzing malware.

Submit your **Windows executable** and receive an analysis report telling you what it does. Alternatively, submit a **suspicious URL** and receive a report that shows you all the activities of the Internet Explorer process when visiting this URL.



If you like this project, you can also make donations if you wish. We will spend the money on buying new hardware, and paying for the pizza ;)



Want notifications about Anubis downtimes and/or updates? [Follow us on twitter](#).

News

- 21.08.2010** RAID failures almost promised a full-time working weekend. Barely made it before that! Analysis is not running at full capacity yet, but all services should be available again.
10.08.2010 Hardware problems caused a short downtime. Analysis-service back up after running various system & disk checks!
28.07.2010 We are reanalyzing some samples that could not be correctly analyzed because of the error last week. There might be possible increased waiting times until tomorrow. Thanks for your understanding.
23.07.2010 Public submissions open again. We'll keep an eye on things. Let us know if there are issues.
22.07.2010 Unfortunately, we are experiencing some problems related to some features we recently built in. Until we fix the issues, we are deactivating the public submissions.
14.07.2010 Server migration complete. The system is starting to analyze new samples while working on the backlog of the last days.
13.07.2010 Migration to our new servers is almost complete. Results of previous analysis results and upload capabilities are available again. Full/New analysis runs should be available soon.
05.07.2010 We have improved our analysis of network dumps. Extended DNS data (such as multiple DNS replies) are now available in the analysis reports.
02.07.2010 Dionaea/Nepenthes can again automatically upload samples to Anubis. We will reply with an analysis report!
01.06.2010 The Dll-analysis has been improved. Simply upload a dynamically linked library file for Windows, and we'll try to figure out how to analyze it best!
01.03.2010 We have vastly improved analysis performance of the sandbox. You should now get more analysis results for the same execution duration!
16.02.2010 It is the third birthday of Anubis today ;-)

Choose the subject for analysis

For analyzing Javascript and Flash files try [Wepawet](#).

File:
(max. 8MB)

Choose the file that you want to analyze. The file must be a Windows executable. ([details](#))

[Choose File](#) No file chosen

URL:

Choose the URL that you want to analyze. The URL will be analyzed in Internet Explorer.

Note: We will *not* analyze a binary that you provide via this URL. We will merely use a browser to check the given URL for a possible drive-by download or similar attack!

<http://>

Get a priority boost

Enter the code that you see in the image on the left and your submission will be analyzed before all automatic submissions.

zxlx :

credits: iseclab

- 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



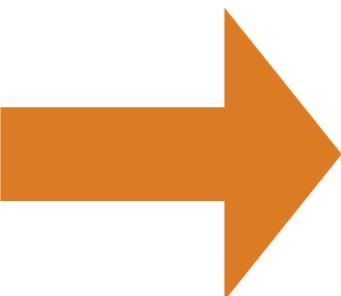
2010/11/22

{wojner,kaplan}@cert.at



2010/11/22

Minibis - Evolution



{wojner,kaplan}@cert.at

CERT.at

Minibis - Basic Idea

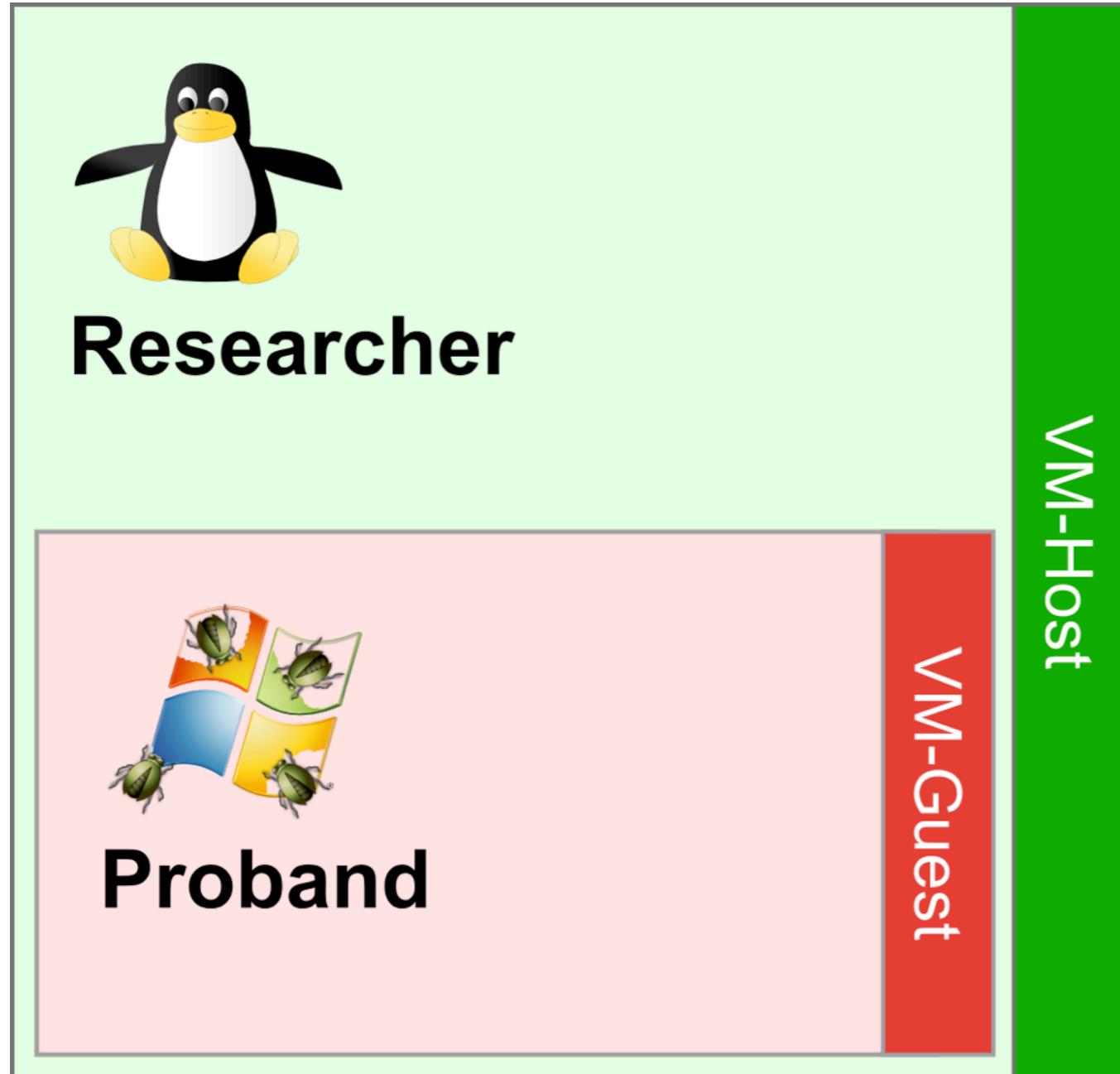


Behavioral Analysis Steps

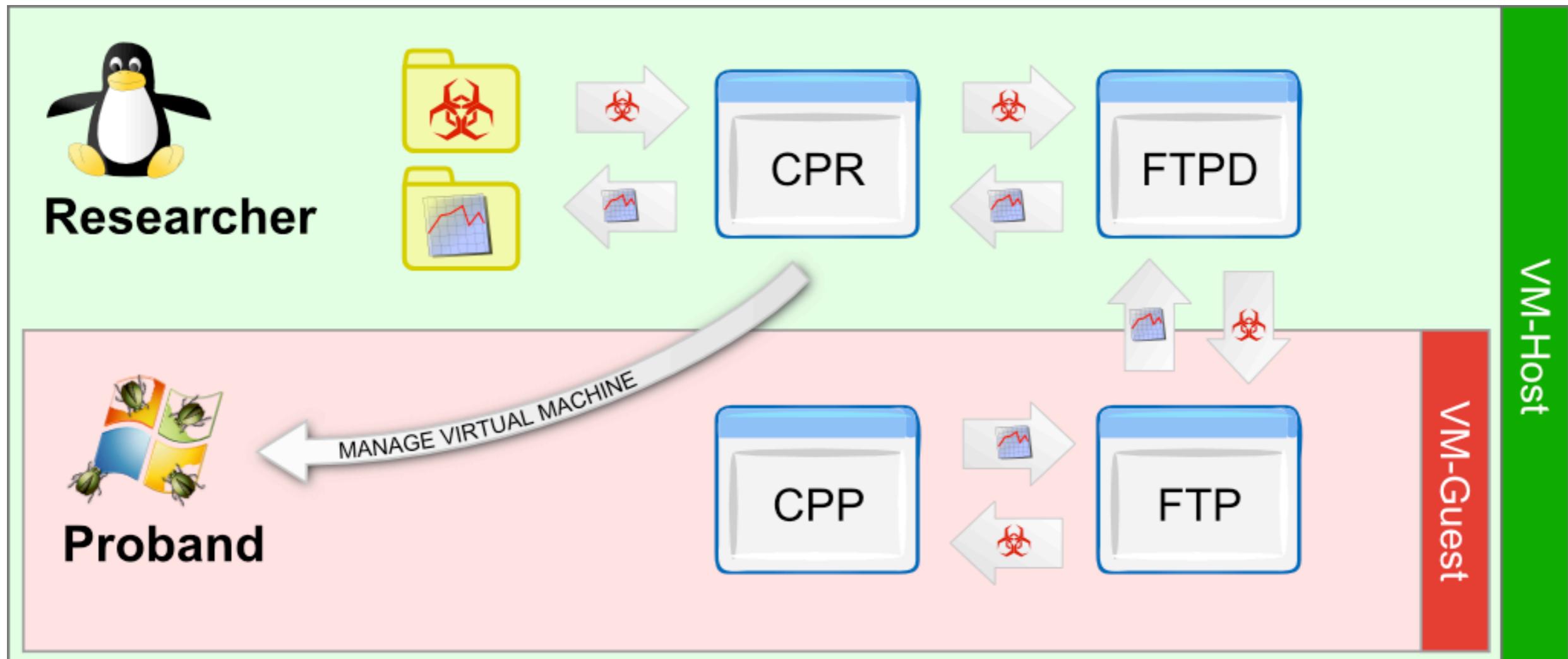


1. Prepare system (virtual machine) with monitoring tools
2. Transfer sample to virtual machine
3. Start up monitoring tools in the VM
4. Run sample
5. Give sample some time to do nasty things
6. Save monitoring logs and transfer them back
7. Analyze logs
8. (Revert VM)

Minibis - Architectural Concept



Minibis - Architectural Concept (2)



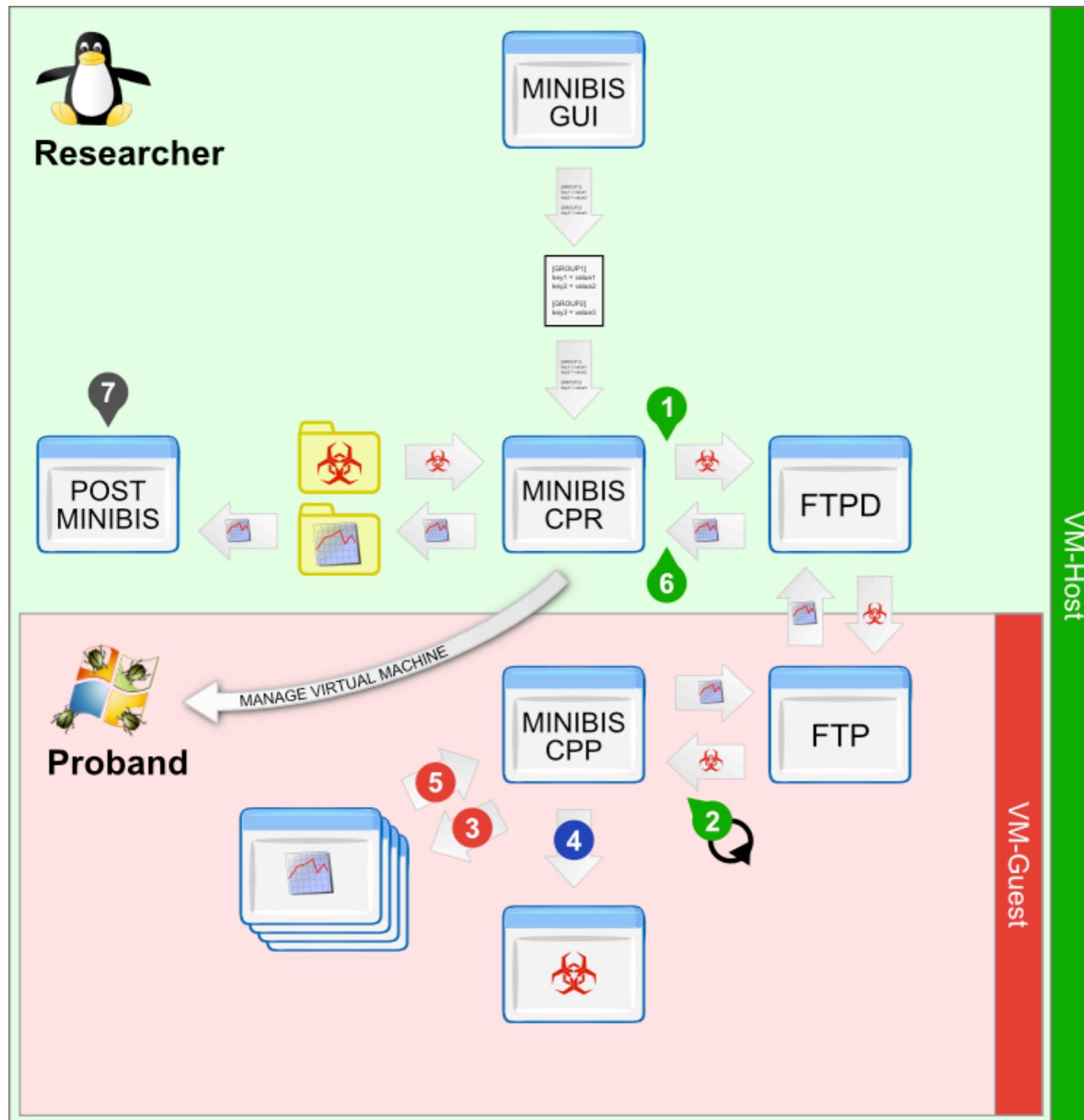
2010/11/22

{wojner,kaplan}@cert.at

CPR = controller process researcher

CPP = controller process proband

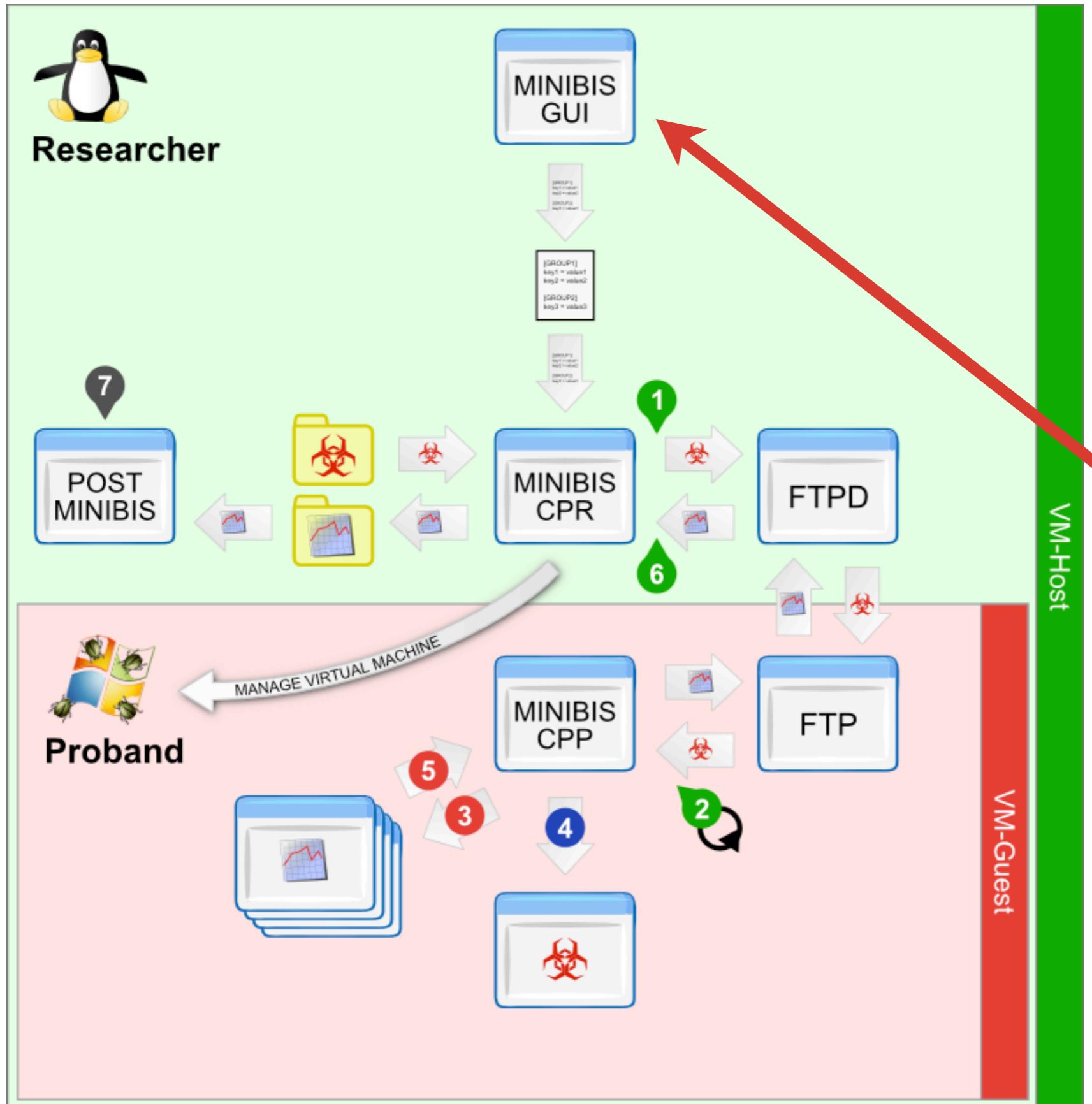
Architectural Concept (3)



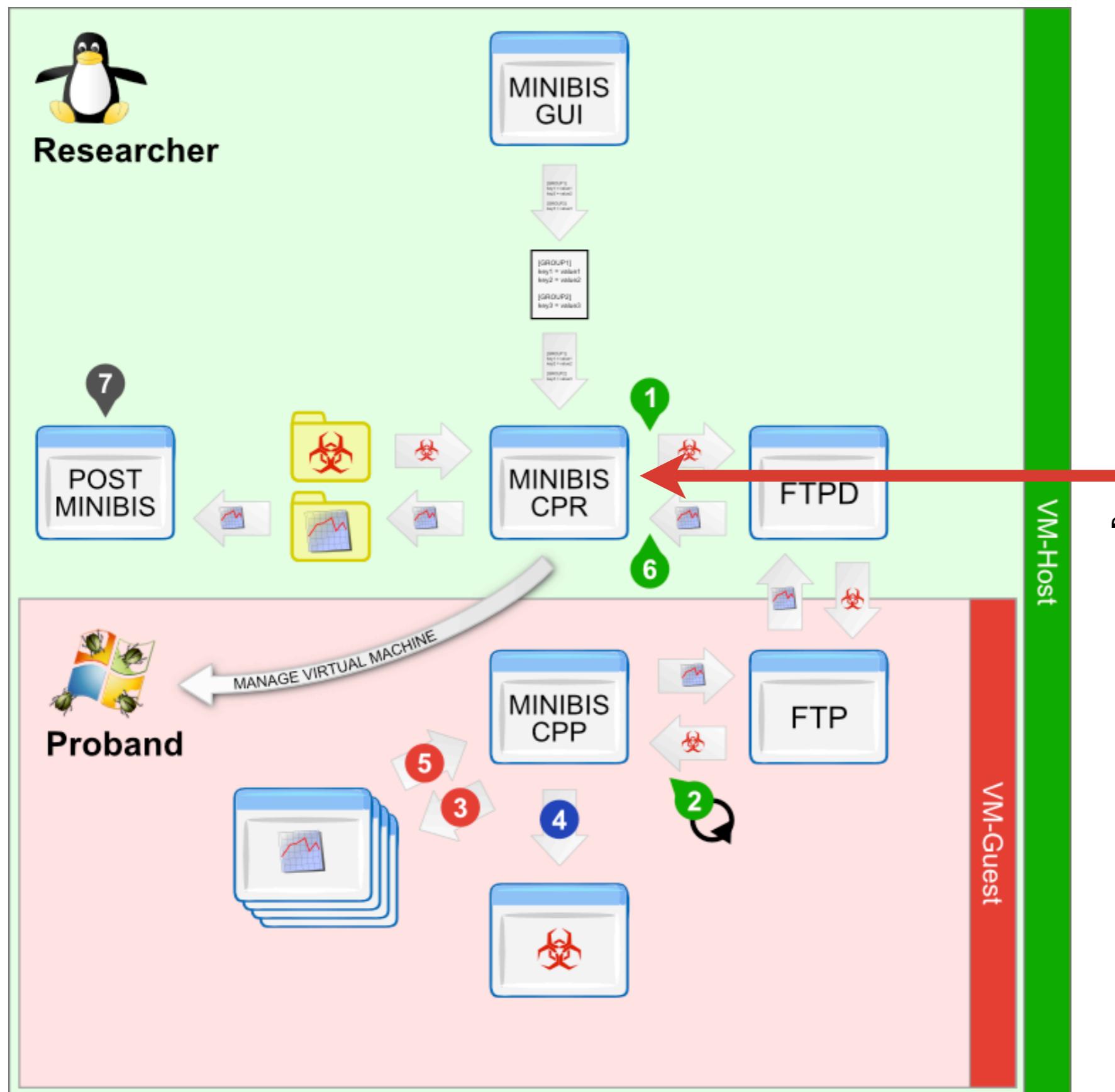
Architectural Concept (3)

minibis-gui: for configuration, progress/status view

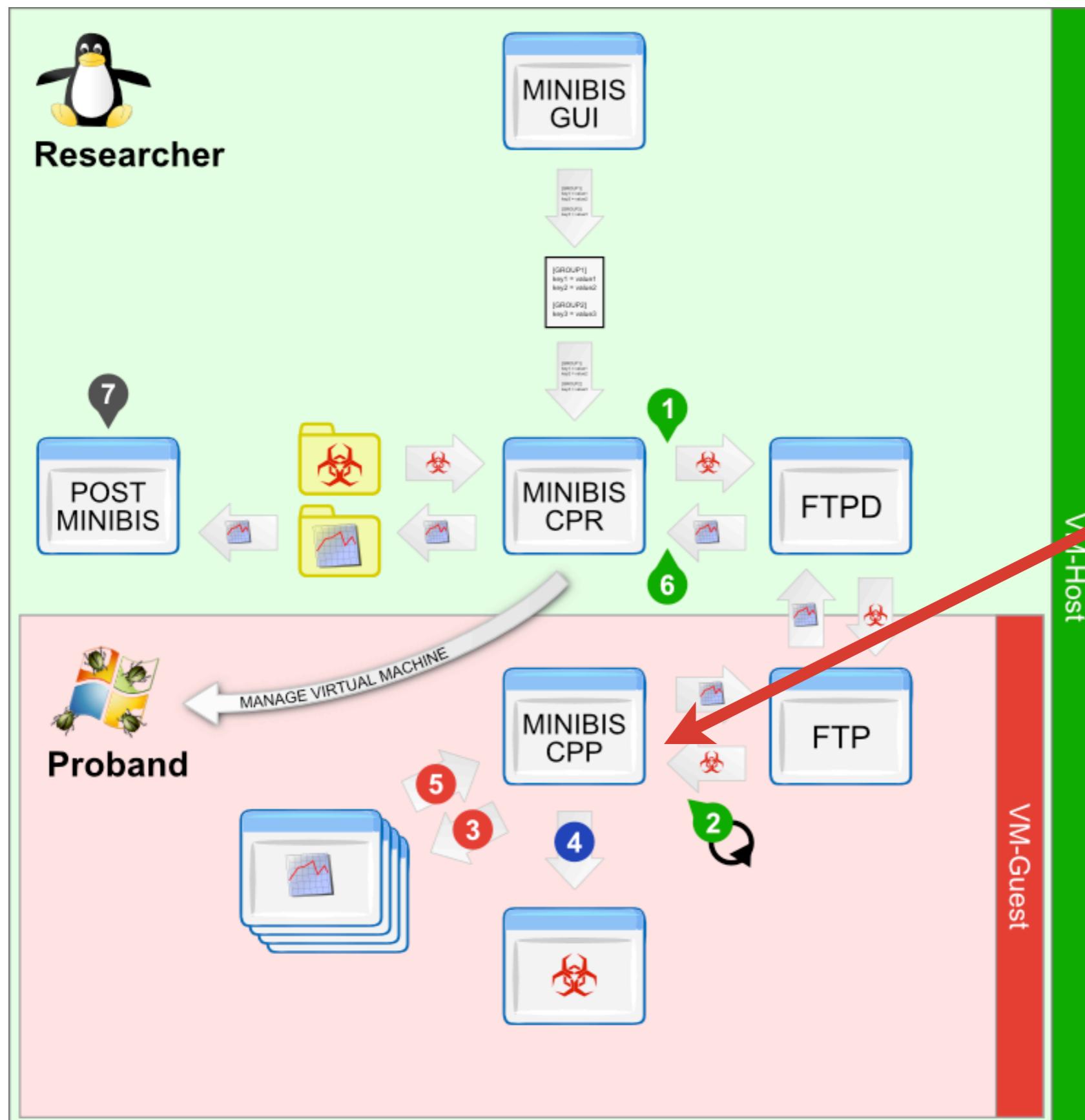
color legend:
 tab researcher
 tab Proband
 tab sample type
 postminibis plugins



Architectural Concept (3)



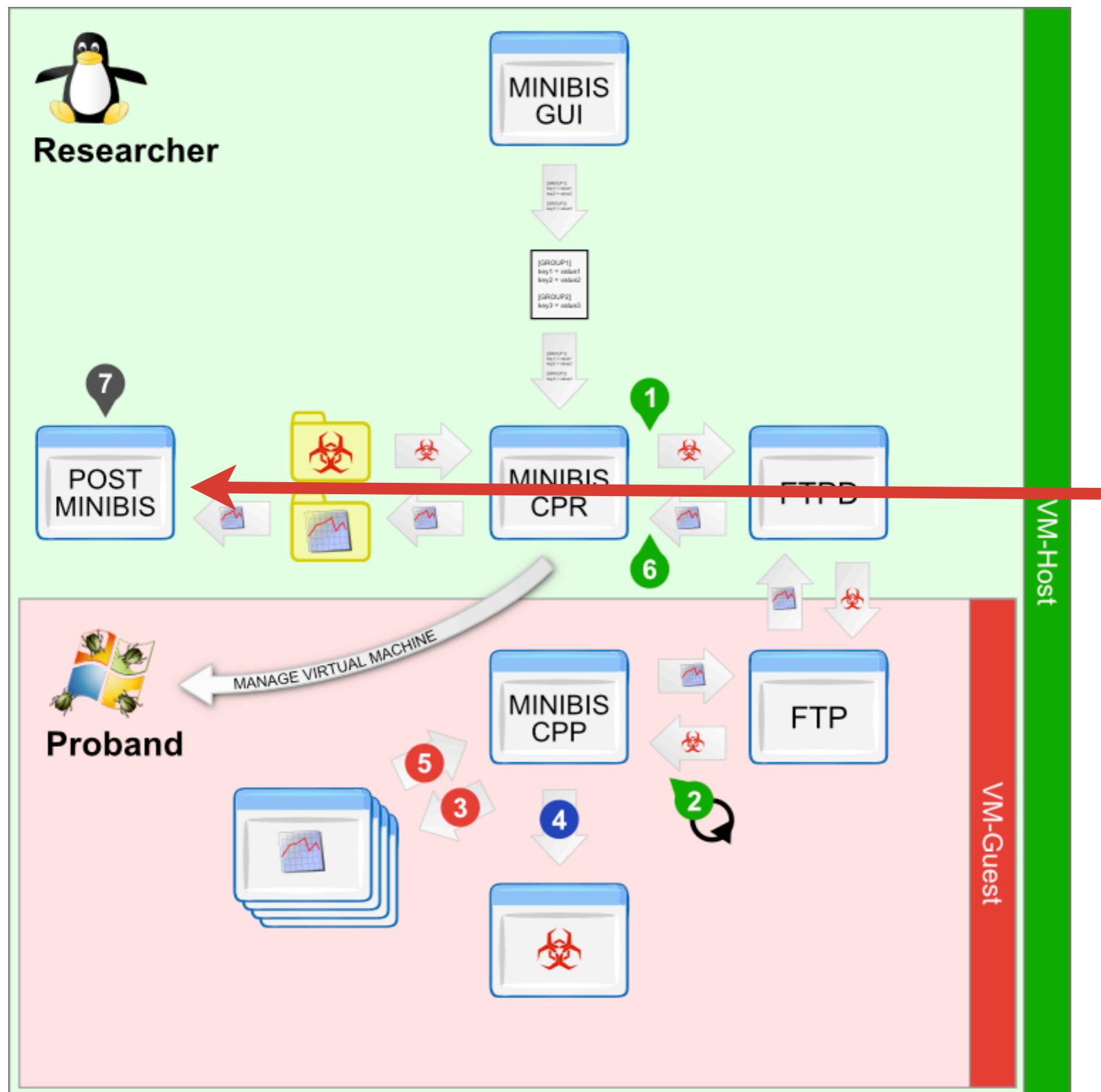
Architectural Concept (3)



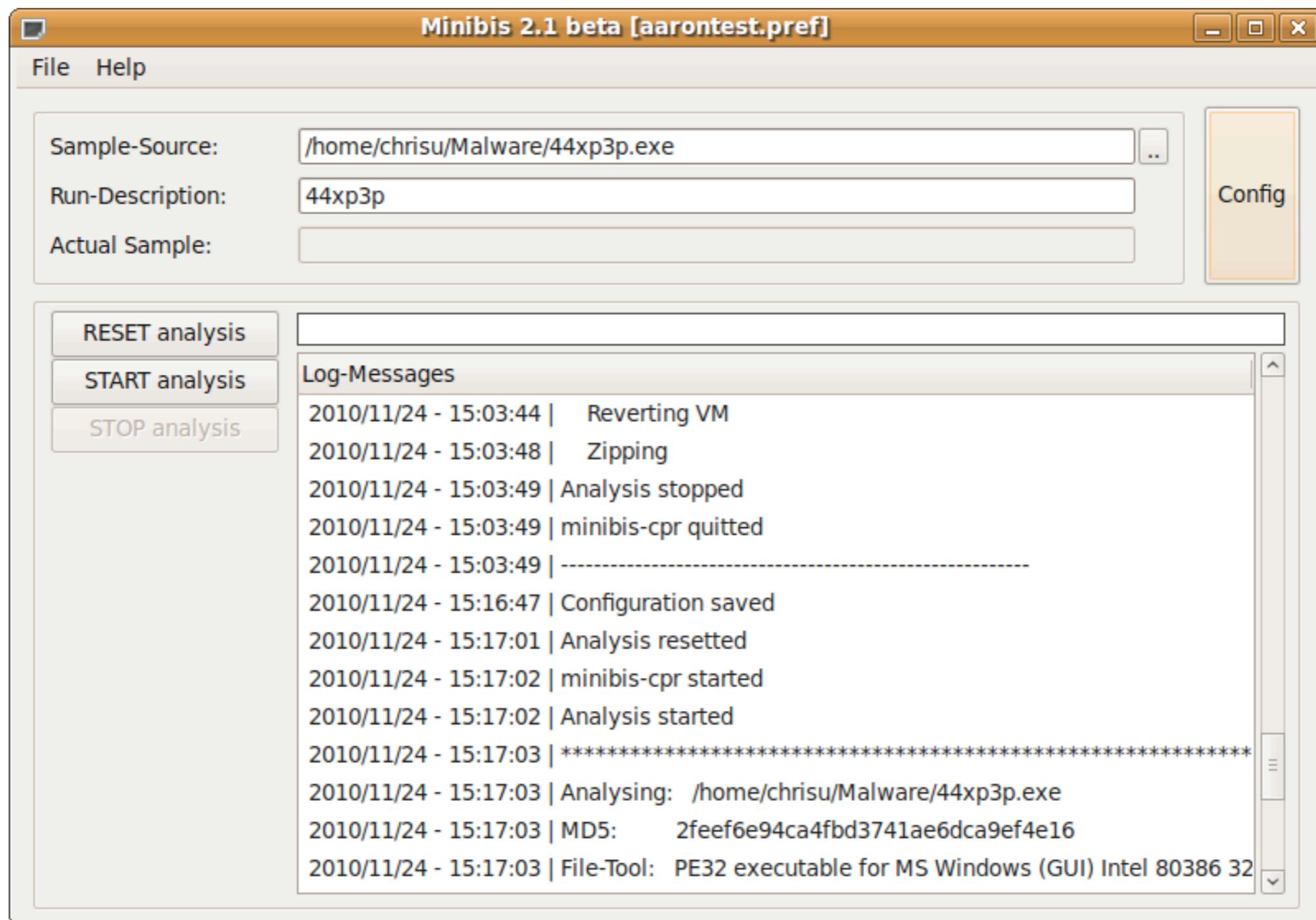
minibis-cpp:
“controller process of
proband”

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

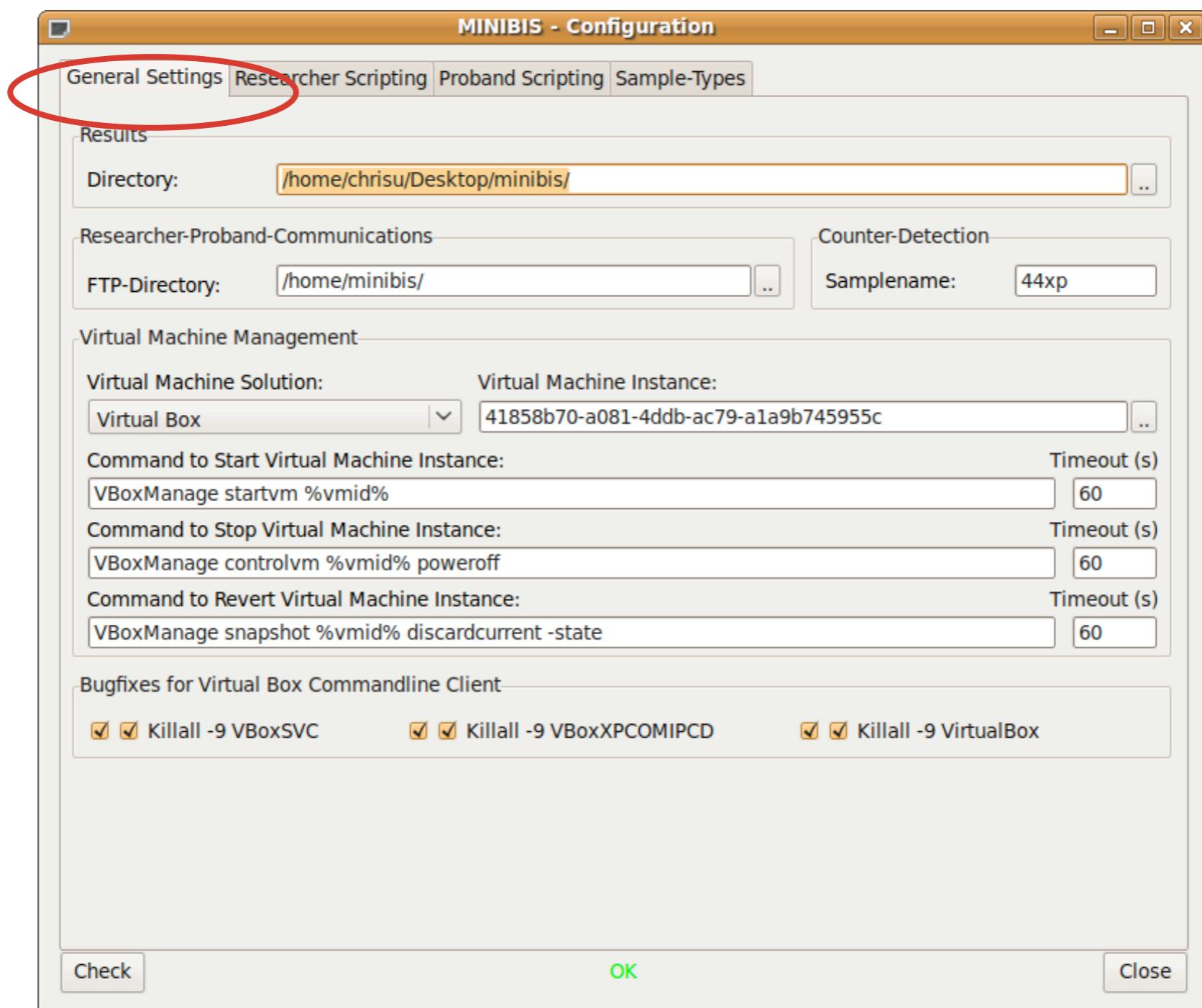
Architectural Concept (3)



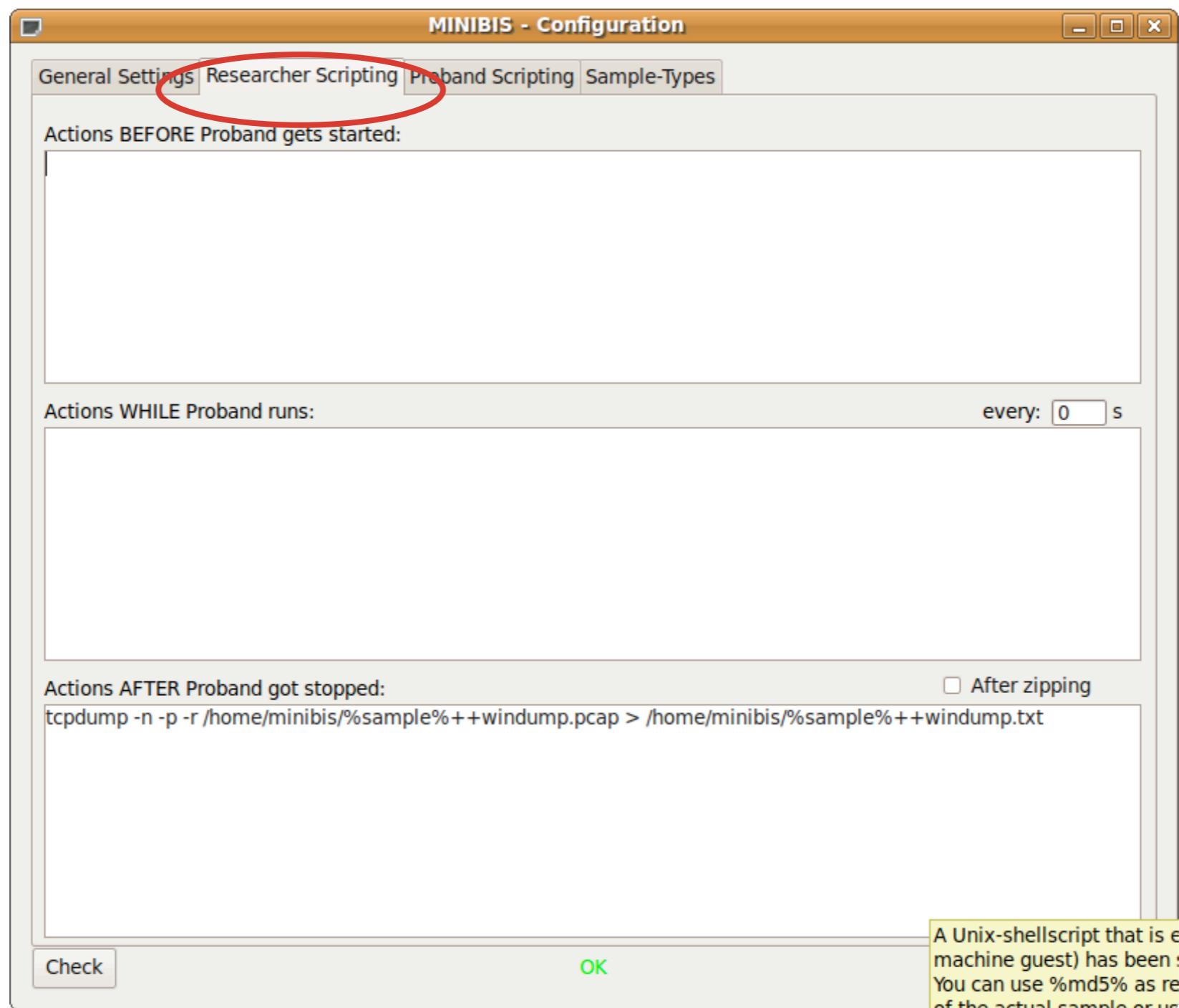
Walkthrough - Main screen



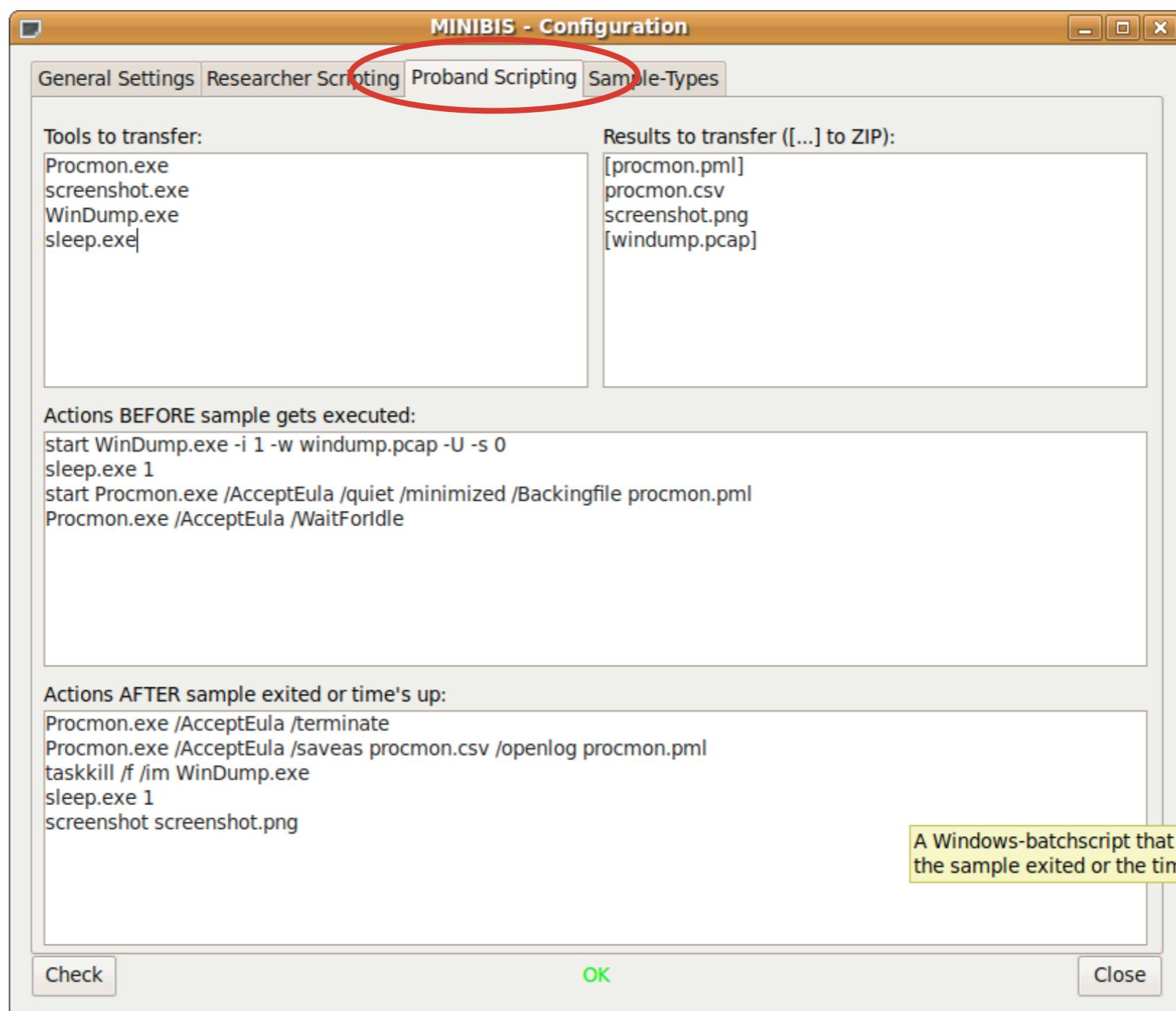
Walkthrough - Config->General



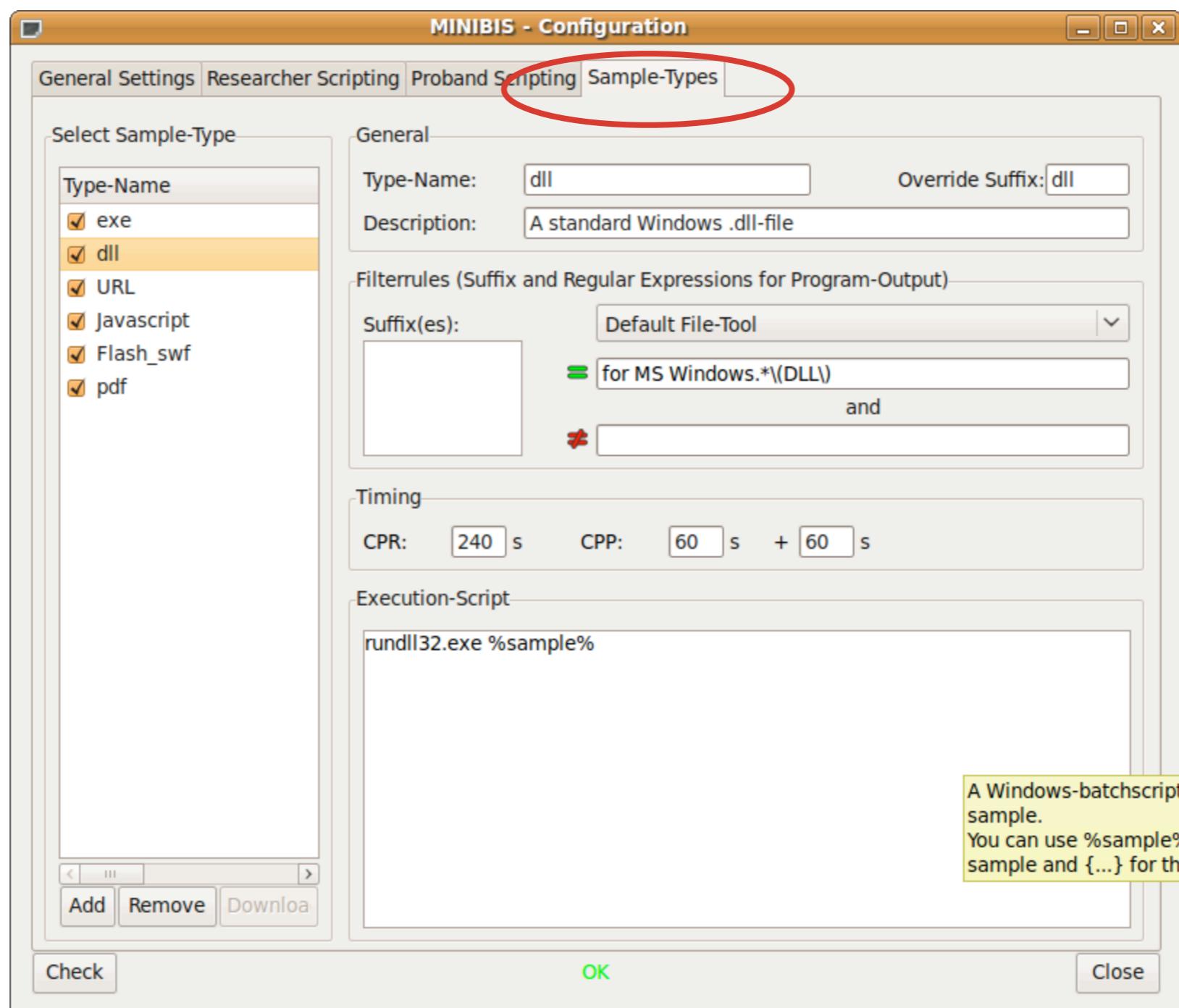
Walkthrough - Config->Researcher



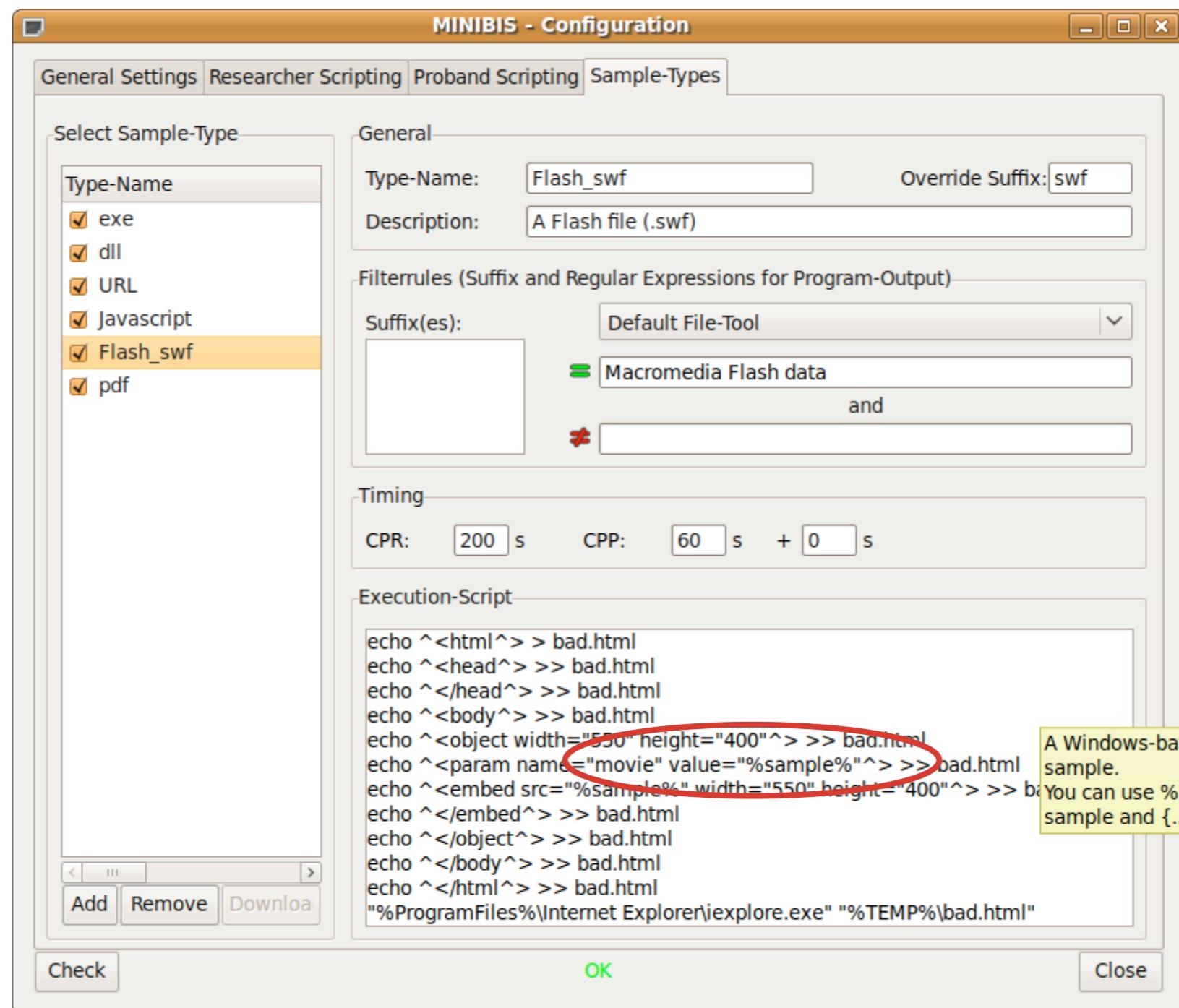
Walkthrough - Config->Proband



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/*

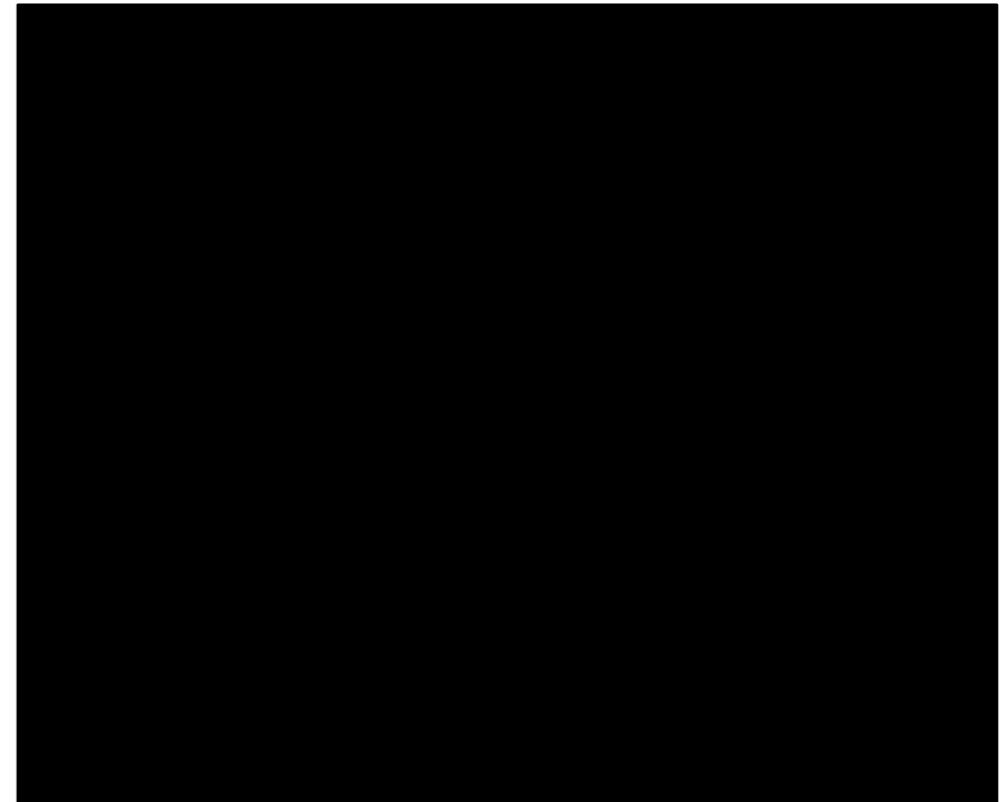
 |- *filename*

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;"
```



2010/11/22

{wojner,kaplan}@cert.at

dient zur analyse der ergebnis files und zur klassifikation der alert/warning/info levels

Weiters: es ist mittels shell script plugins beliebig erweiterbar fuer beliebige analyse output files von minibis

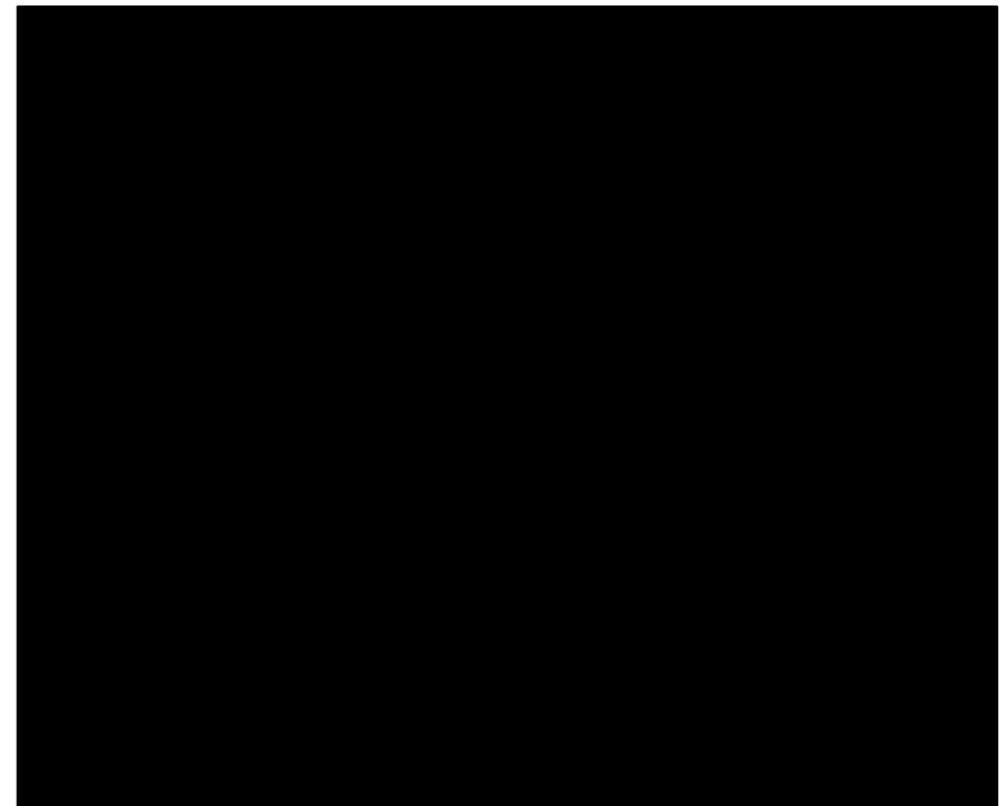
* scriptable

* must parse CSV syntax

* toolset for interpretation of result files

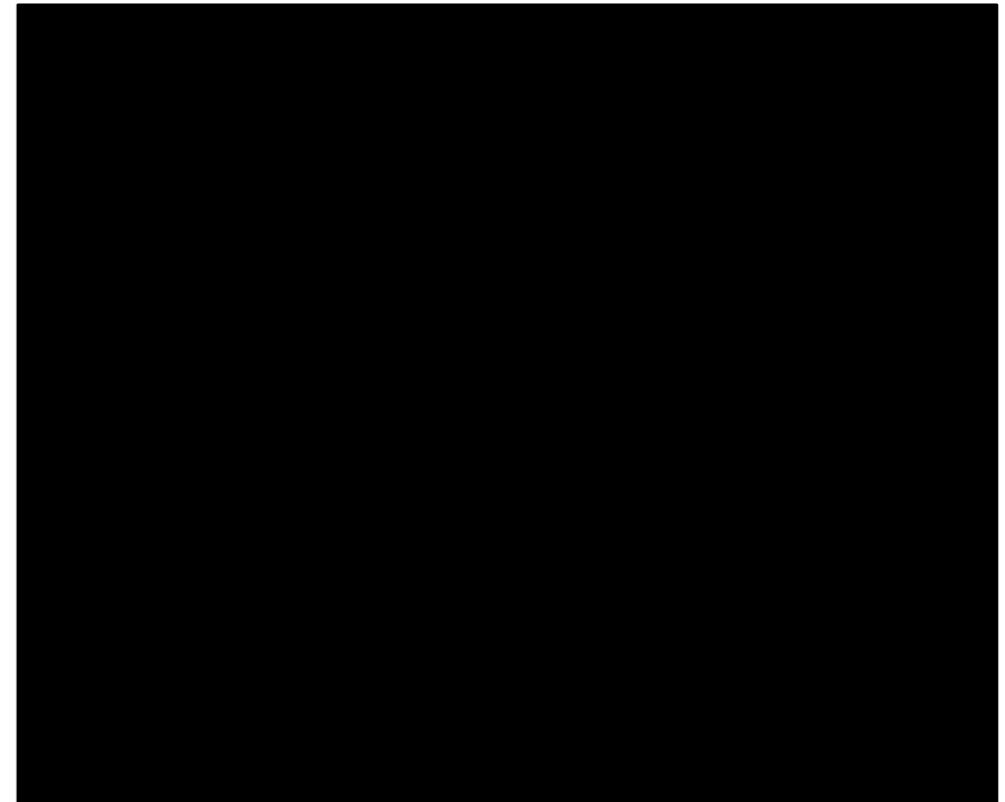
Typical output of postminibis

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



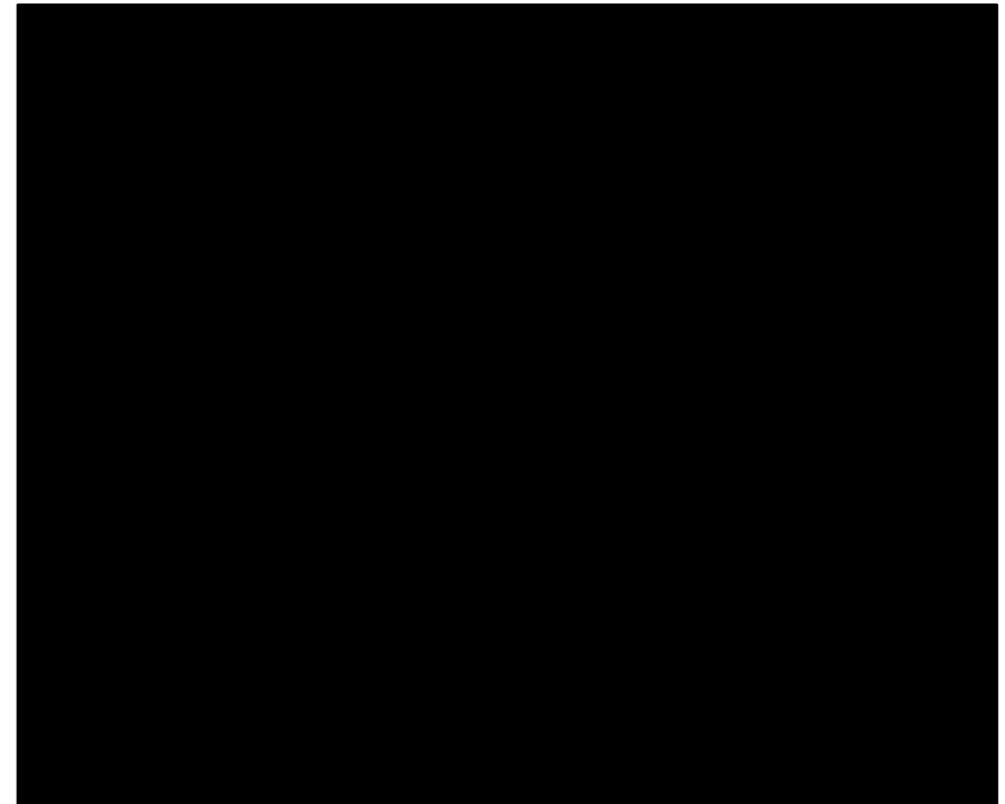
Typical output of postminibis

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



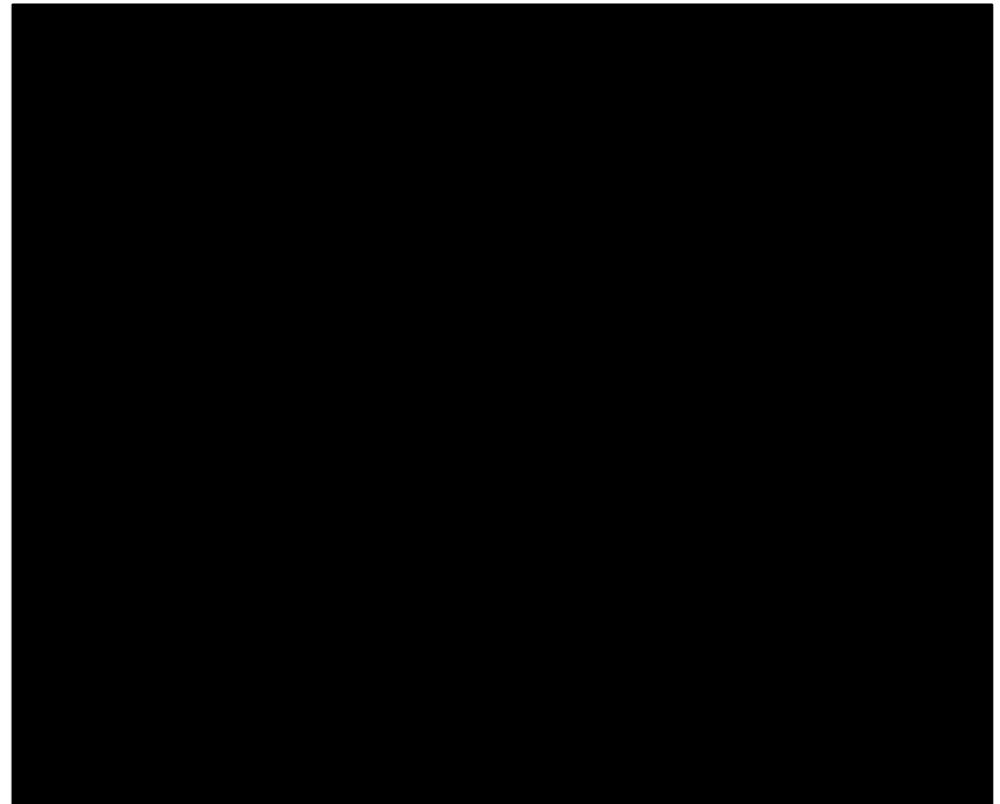
Typical output of postminibis

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



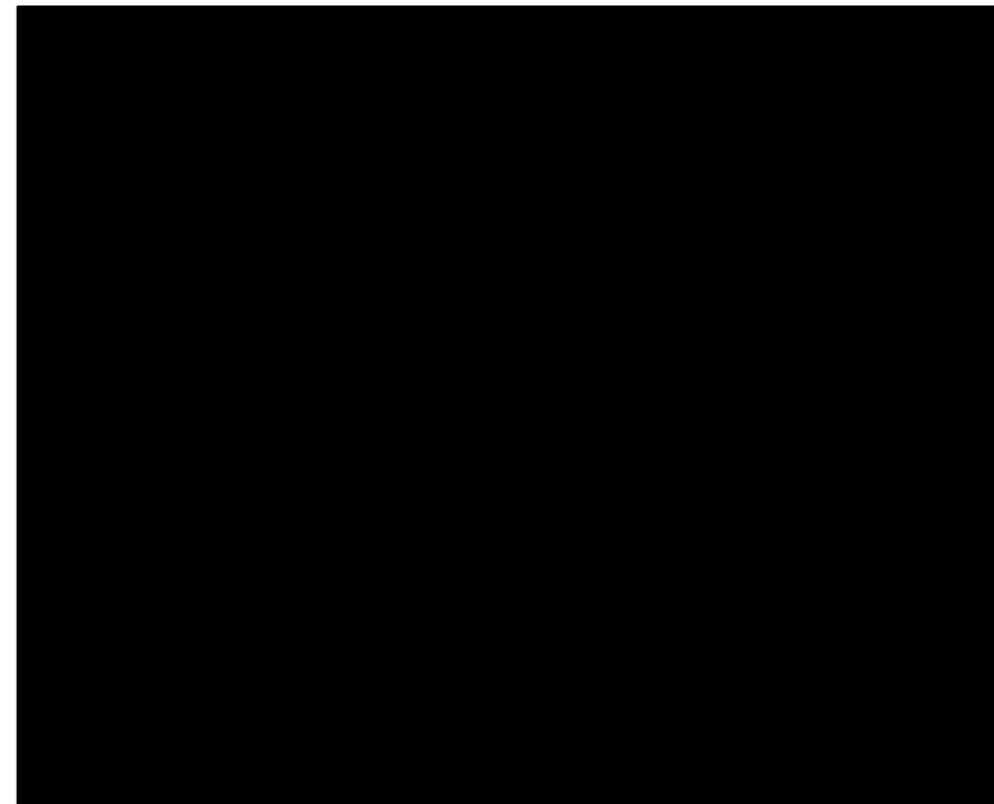
Typical output of postminibis

```
• d407ebf73d25715050bea07fdbfb76a5;2010/11/24-16:15:27;;a;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;Setting 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
```

Count	Registry Key
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



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

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](#)

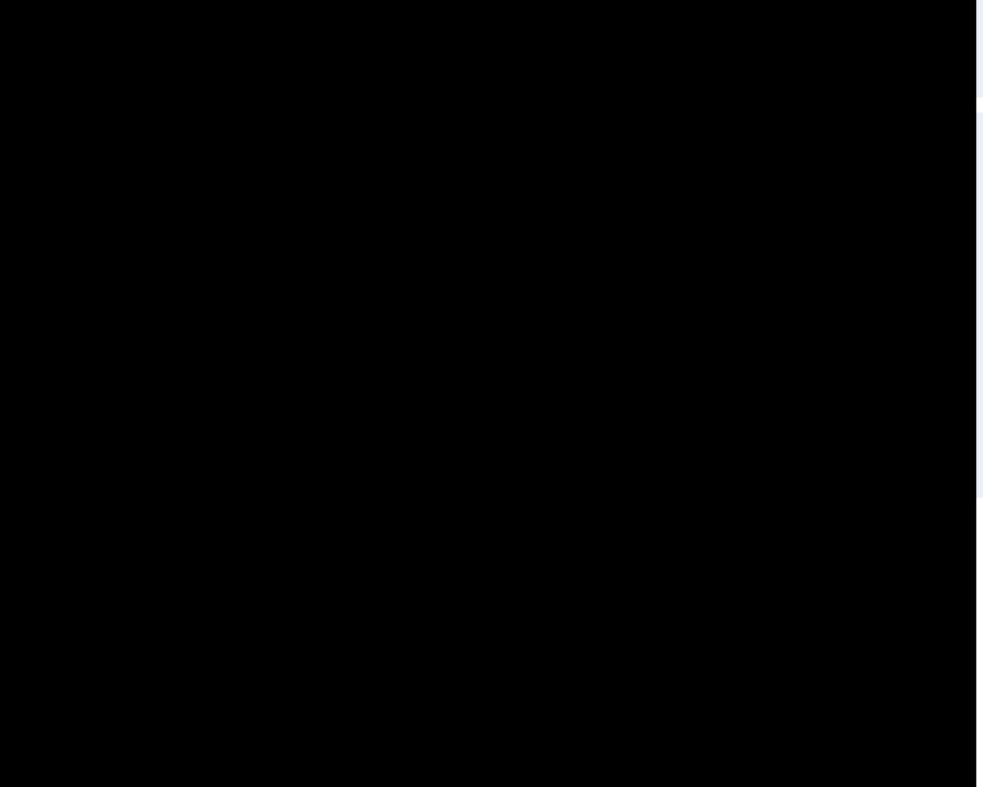
Software and tips to easily build up an automated malware analysis station based on a concept introduced in the paper "Mass Malware Analysis: A Do-It-Yourself Kit".

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

 Star this project

Activity:  [Low](#)

Code license:
[Other Open Source](#)
[See source for details](#)



2010/11/22

{wojner,kaplan}@cert.at

Community



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

Project Home Downloads Wiki Issues Source Administer
Summary | [Updates](#) | [People](#)

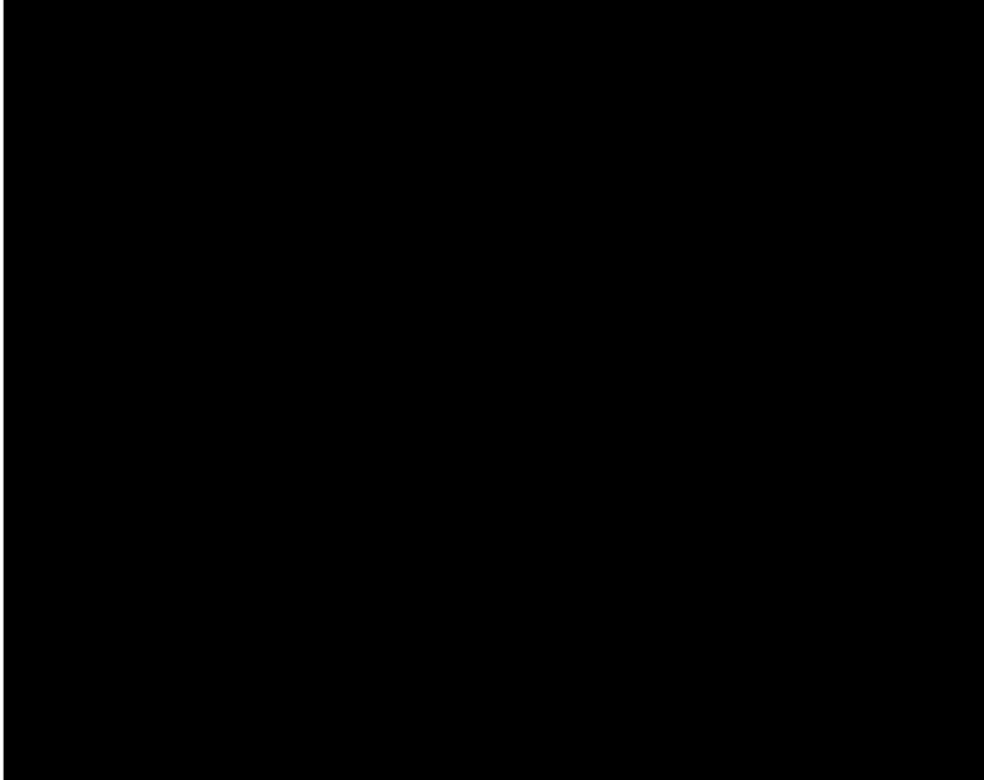
Tip: Project owners, see our [Getting Started](#) guide for steps to configure your project. [hide](#)

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 <http://www.cert.at/downloads/software/minibis.html>

[Star this project](#)
Activity: 
Code license: [Other Open Source](#)
[See source for details](#)

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



2010/11/22

{wojner,kaplan}@cert.at



Thanks!

