Mass Malware Analysis

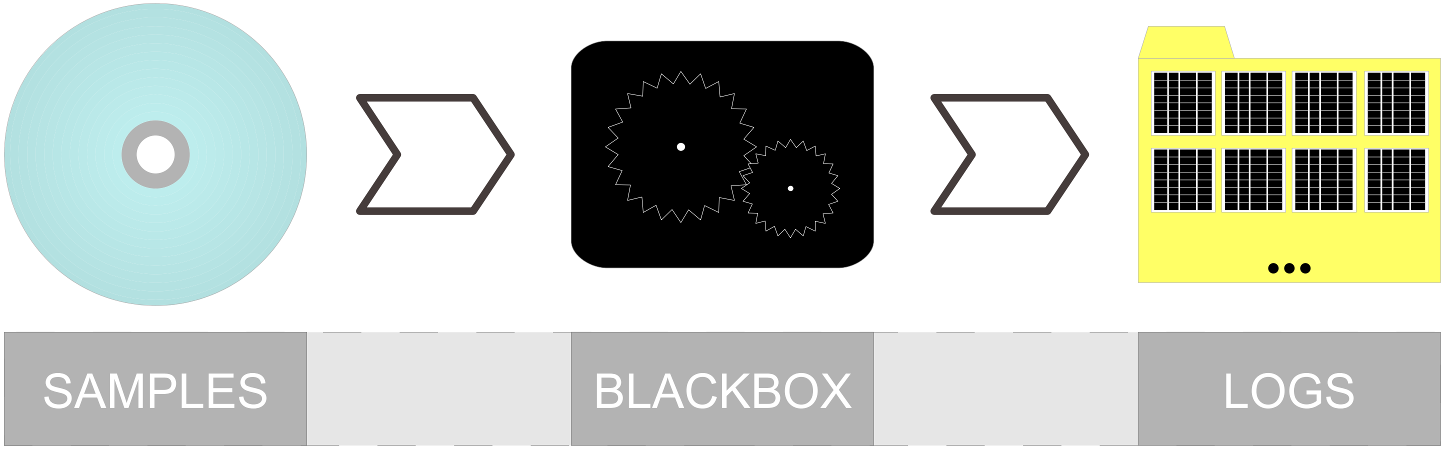
A Do-It-Yourself Kit

Christian Wojner
2010/01/26

The Speaker

- Christian Wojner
  - CERT.at
  - Malware analysis
  - Reverse-Engineering
  - wojner@cert.at

Mass malware analysis needs automation!



Automated Malware Analysis Station

Talk's Outline

- What?
  - Characteristics
- How?
  - General concept
  - CERT.at's implementation
  - Screenshots
- What-For?
  - Example evaluations

What?

Characteristics

- Cheap (mostly free software)
- Autonomic
- Runs on a standard desktop
- Target-OS freely chooseable
- Easy to set up
- Ready for use within a day
- Fully customizable
- Easily evaluateable

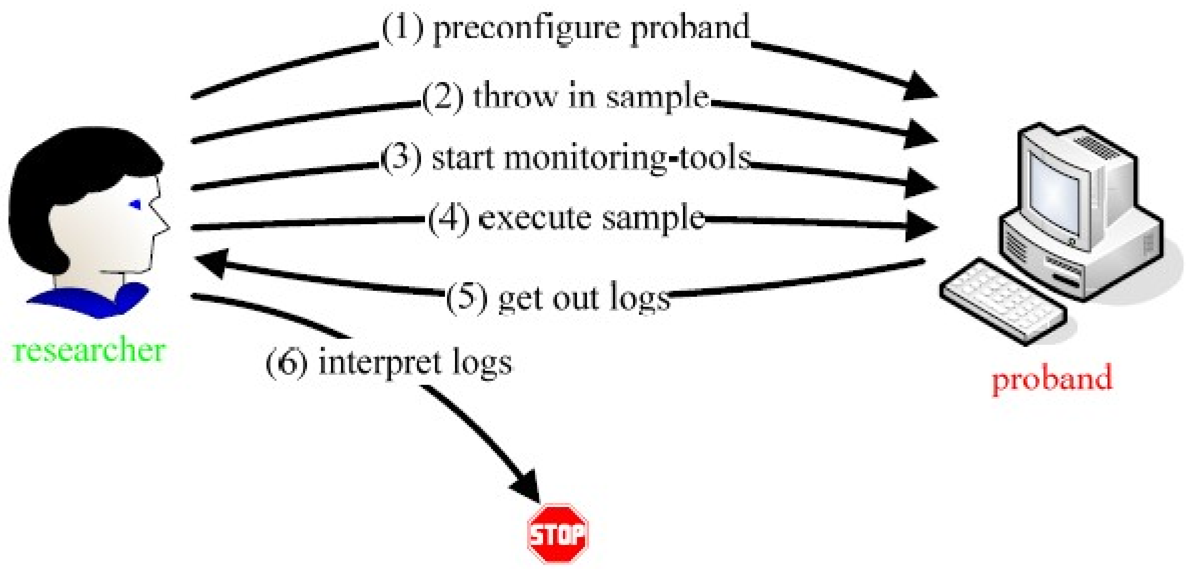
Characteristics

- Runtime-unpacked/-decrypted samples must not be a hurdle
- Data/Analysis/Samples/… kept confidential

How?

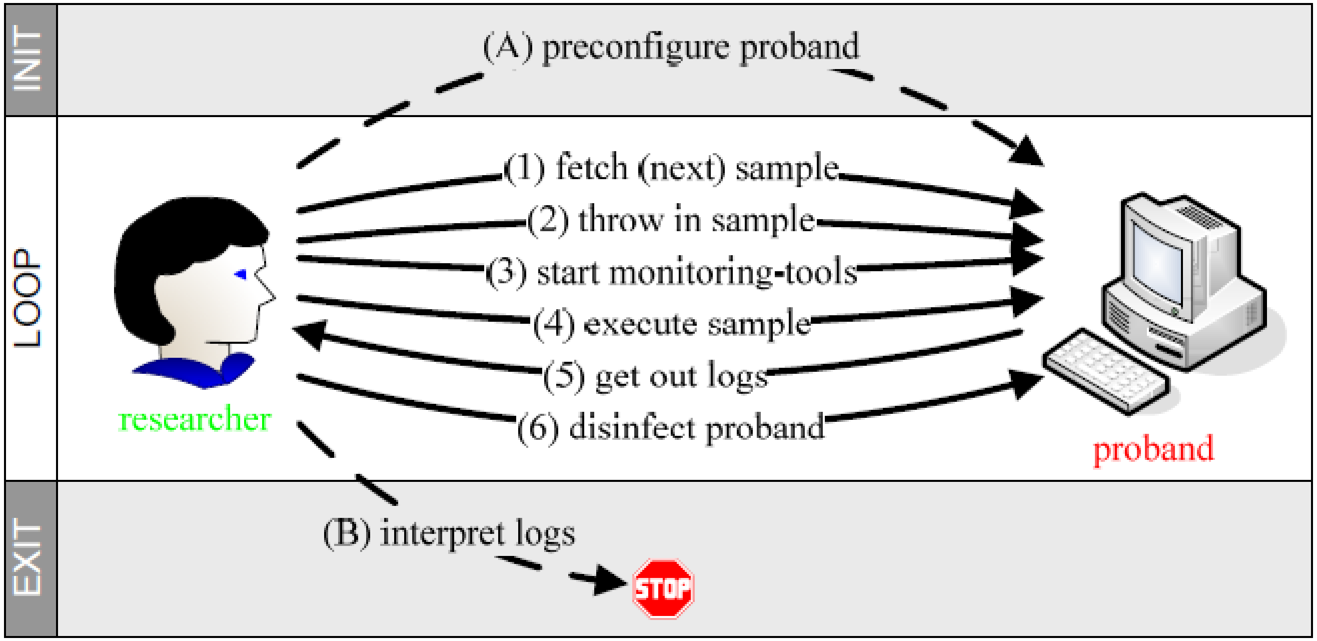
Fundamental Approach

Manual steps to behavorial analyse one sample:



Fundamental Approach

Manual steps to behavorial analyse more than one sample:

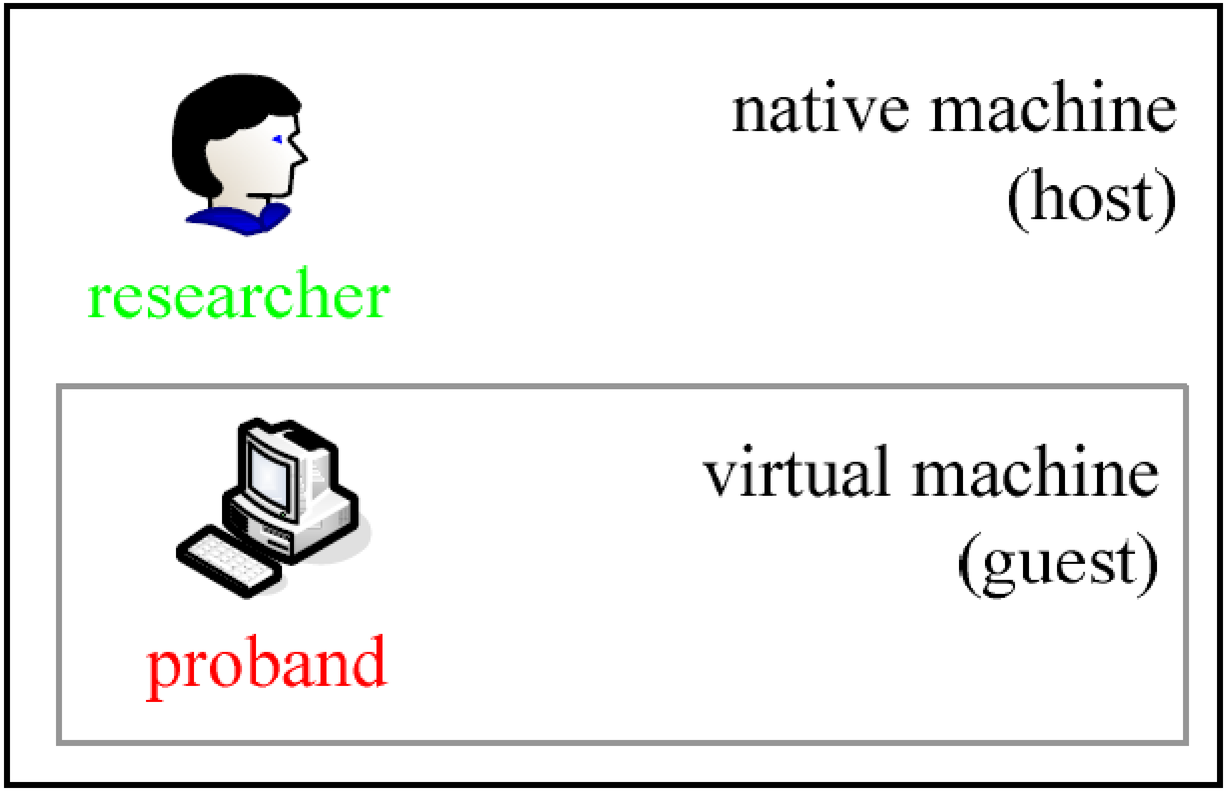


Identifying Components

- Two scopes
  - Researcher
  - Proband

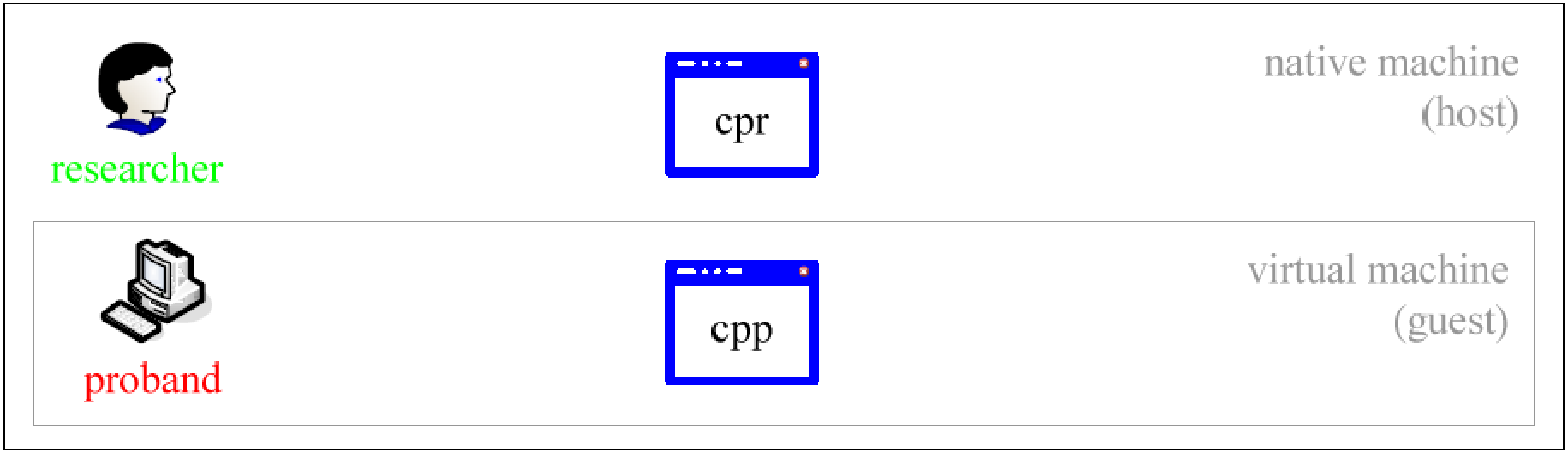
- Virtual machines come in handy
  - Researcher (= native machine)
  - Proband (= virtual machine)

Identifying Components

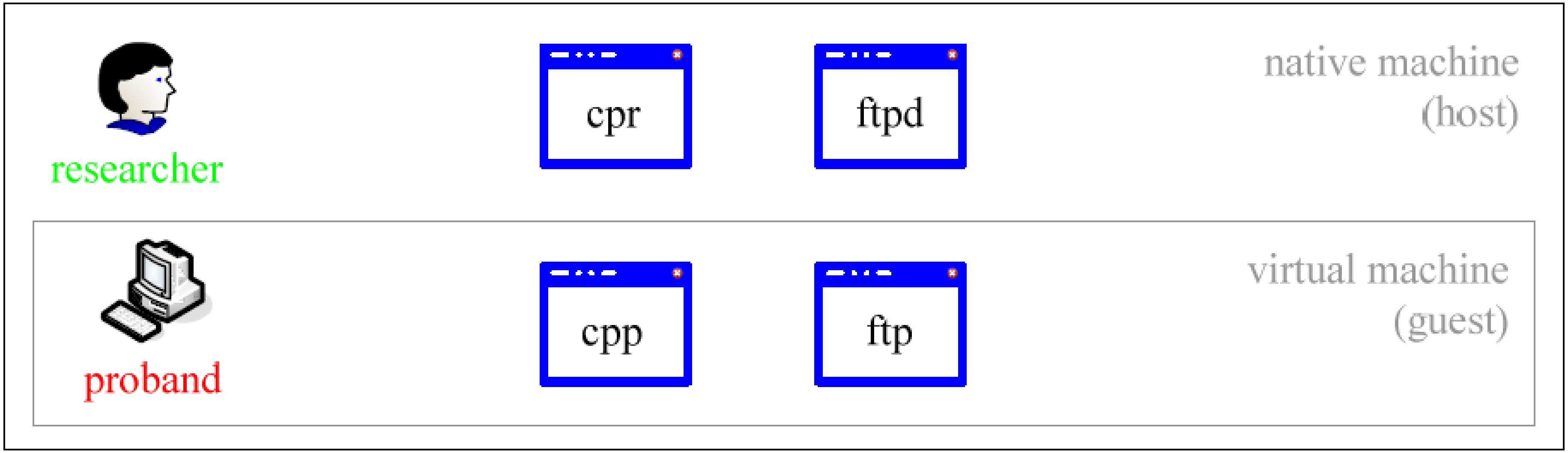


Identifying Components

We need some controller processes:

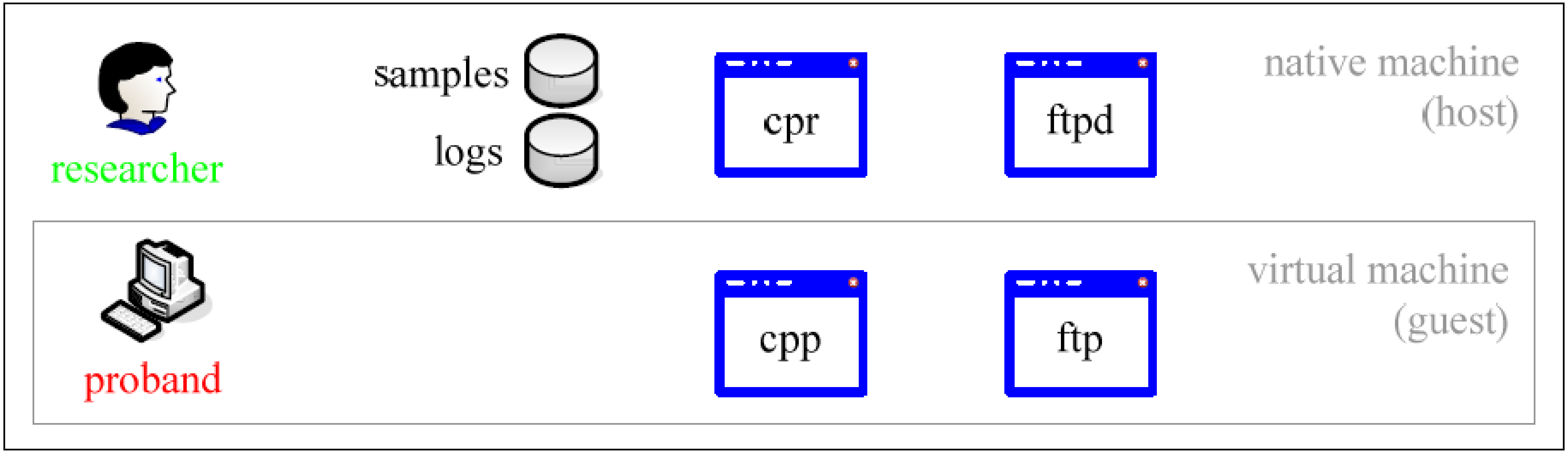


Communications over FTP:

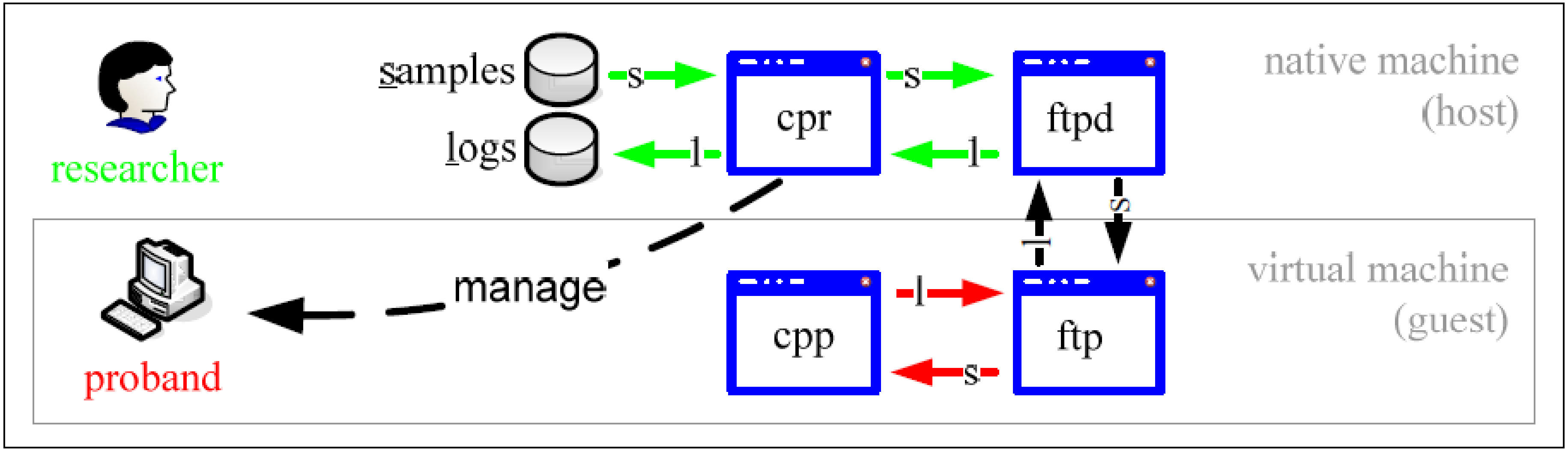


Identifying Components

We need two collections:



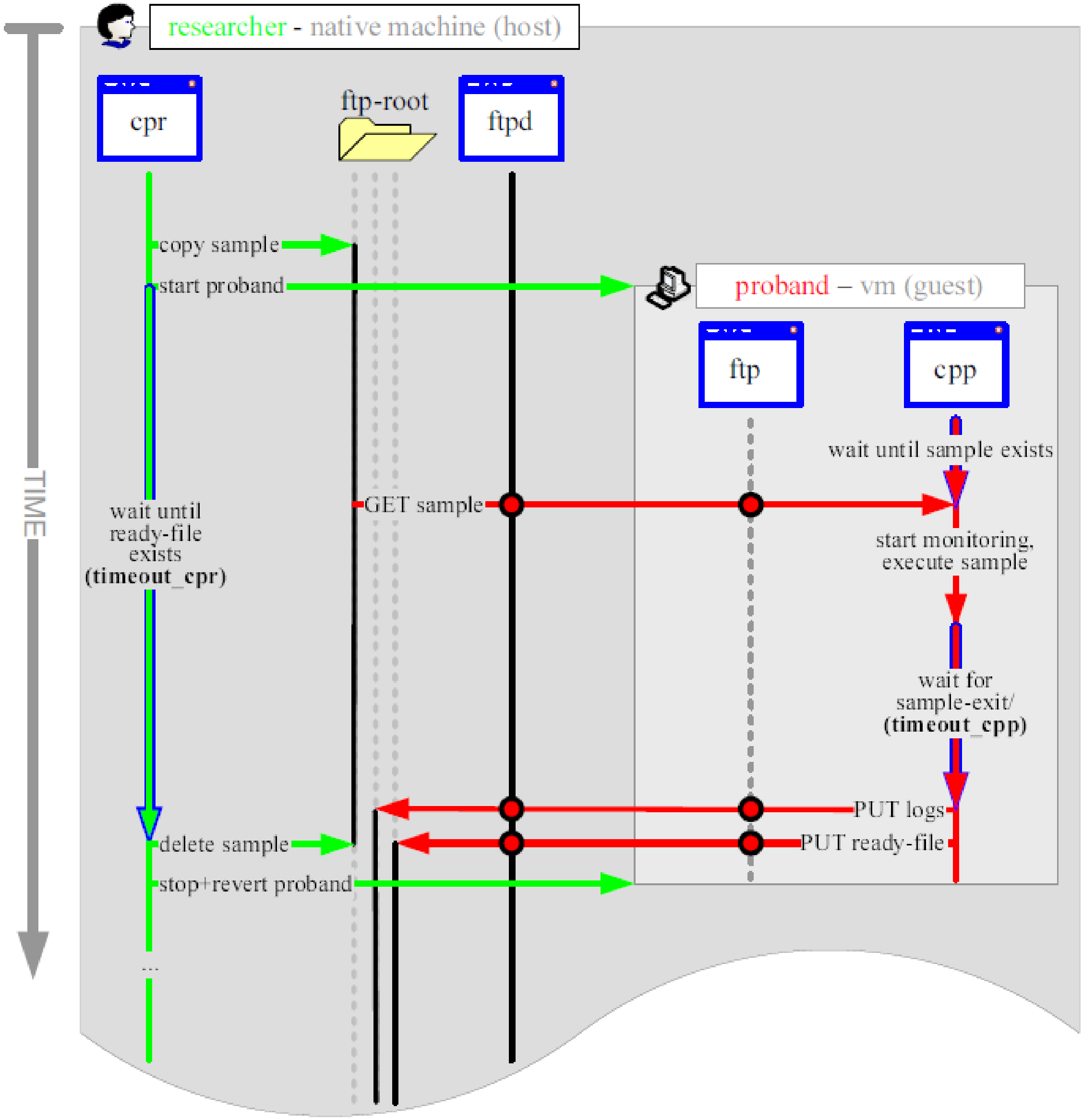
Big picture with communication flow:



Problems Of Automation

- Synchronization
  - Two processes, different machines
  - FTP again
- Timing
  - Deadlocks
  - Timeouts
- Timeouts
  - Best values? – It depends!

Big Picture For Each Sample



Theory => Practice

Controlling The Proband

- VirtualBox (VBox)
  - Commandline tool VBoxManage ...
    - ... list vms
      - Find out your uuid
    - ... startvm uuid
      - Startup virtual machine
    - ... controlvm uuid poweroff
      - Pull out power cable
    - ... snapshot uuid discardcurrent -state
      - Restore to last saved state

CERT.at's Implementation

CERT.at's Implementation

- Hardware
  - Dell OPTIPLEX 745
  - Intel Core 2 Duo 6400
  - 2 Gigs of RAM

CERT.at's Implementation

- Researcher's software
  - Ubuntu-Linux
  - SUN’s VirtualBox
  - Proftpd
  - zip
  - minibis-cpr (home-grown)

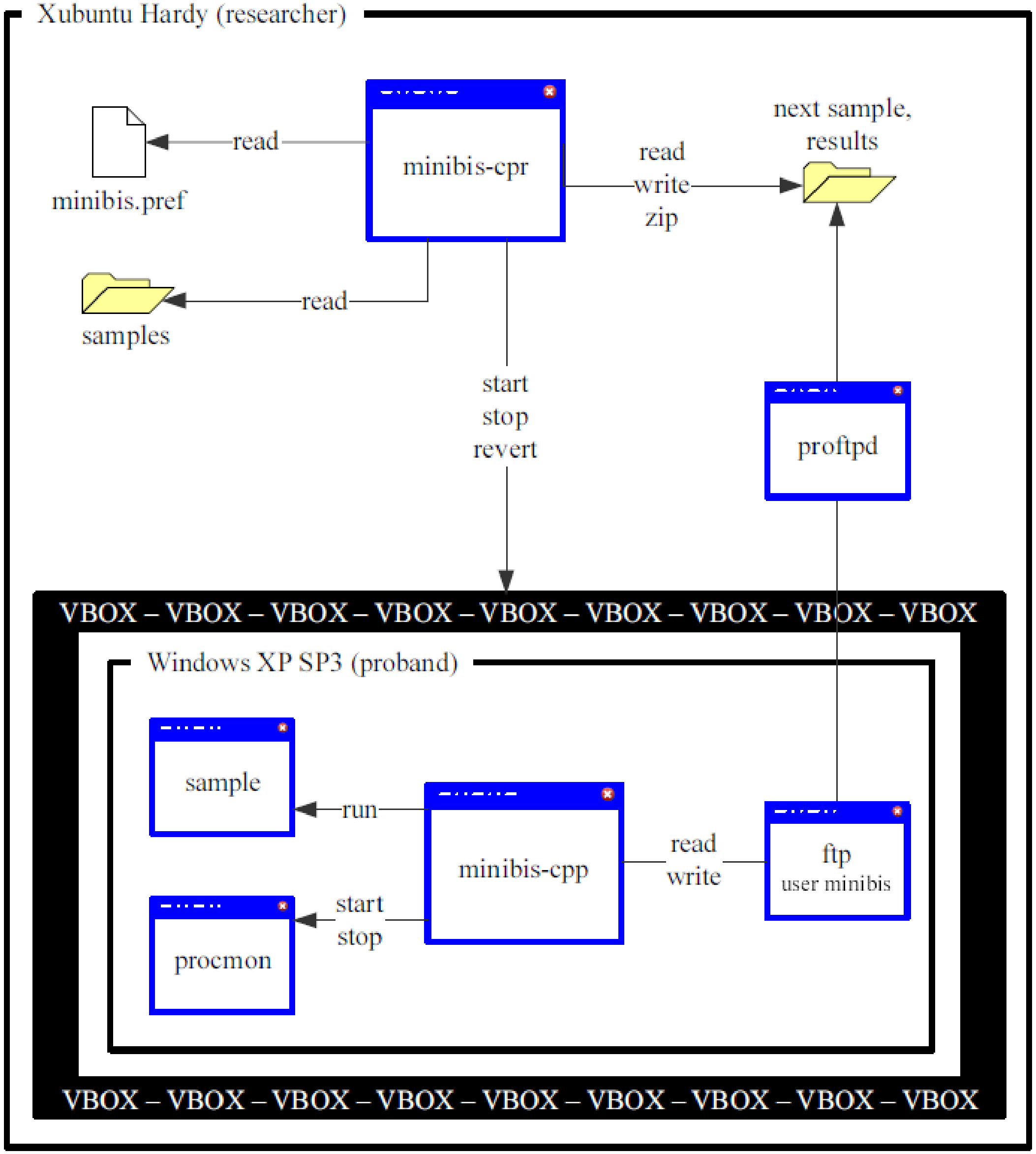
CERT.at's Implementation

- Proband's software
  - Microsoft Windows XP SP3
  - ProcessMonitor (from Sysinternals)
  - minibis-cpp (home-grown)

CERT.at's Implementation

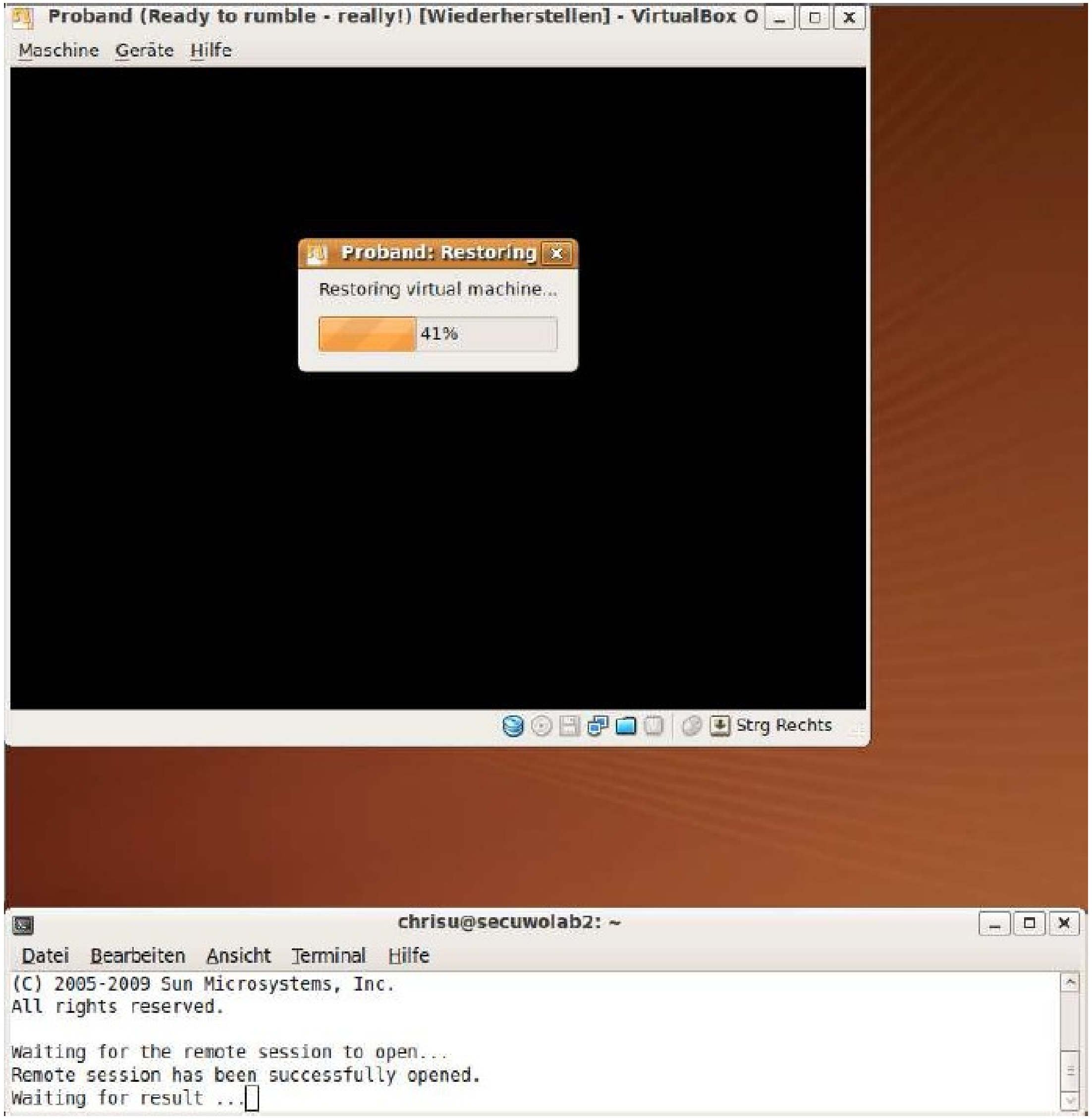
- Features
  - Monitoring activities using ProcessMonitor (Procmon from Sysinternals)
  - Making screenshot on exit
  - .PML-files
  - .CSV-files
  - Compress (ZIP) the returned .PML-files and binaries

Big Picture For CERT.at's Implementation



Screenshots

Screenshots

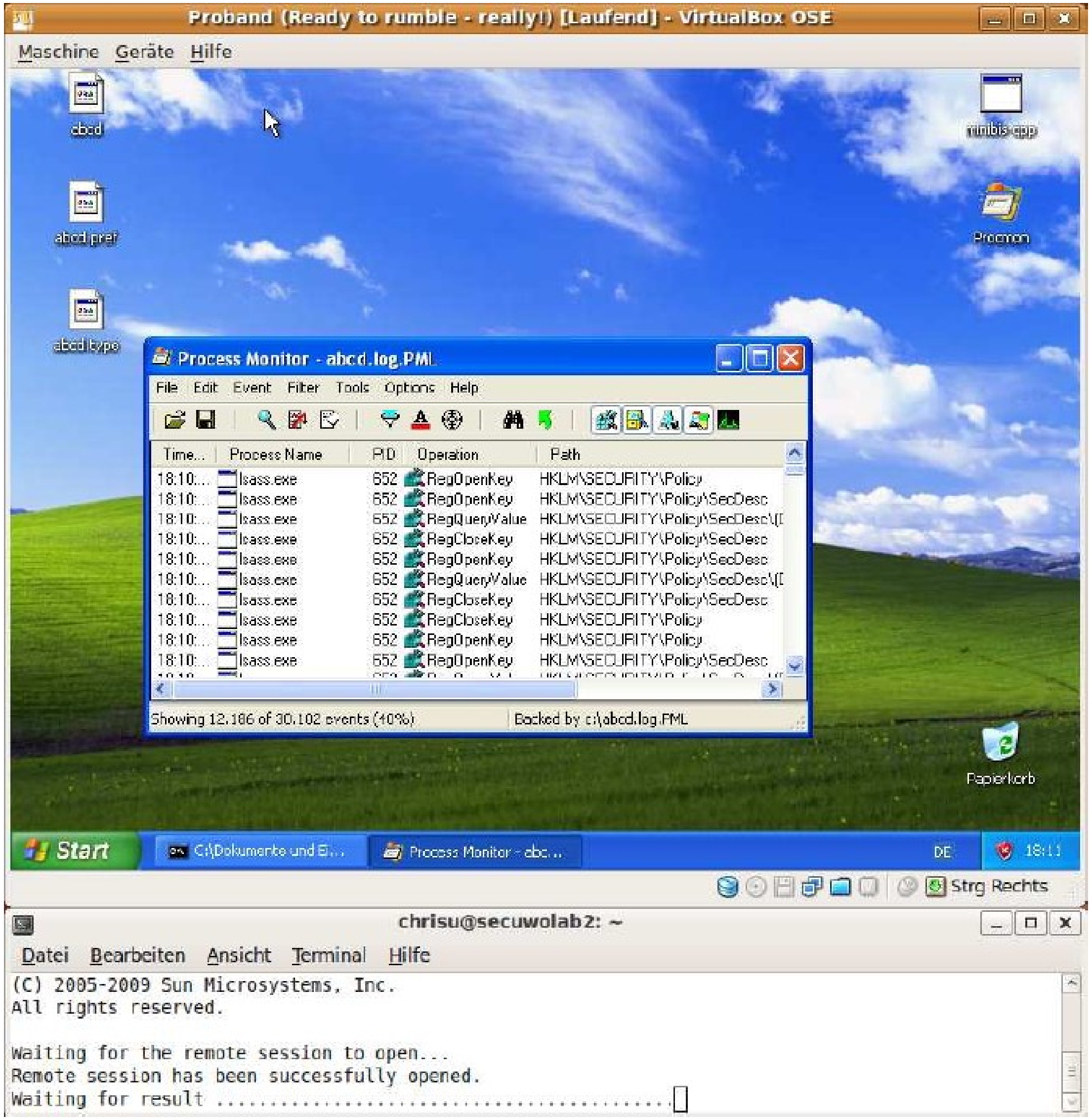

Proband (Ready to rumble - really!) [Wiederherstellen] - VirtualBox O
Maschine Geräte Hilfe
Proband: Restoring
Restoring virtual machine...
41%
Strg Rechts
chrisu@secuwolab2: ~
Datei Bearbeiten Ansicht Terminal Hilfe

```
(C) 2005-2009 Sun Microsystems, Inc.
All rights reserved.

Waiting for the remote session to open...
Remote session has been successfully opened.
Waiting for result ...
```

The virtual machine (proband) is being started.

Screenshots



Proband (Ready to rumble - really!) [Laufend] - VirtualBox OSE
Maschine Geräte Hilfe
abcd
abcd.pref
abcd.type
minibis.cpp
Procmon
Papierkorb
Process Monitor - abcd.log.PML
File Edit Event Filter Tools Options Help
Start
C:\Dokumente und E...
Process Monitor - abc...
DE
18:11
Strg Rechts
chrisu@secuwolab2: ~
Datei Bearbeiten Ansicht Terminal Hilfe

Time...	Process Name	PID	Operation	Path
18:10:...	lsass.exe	652	RegOpenKey	HKLM\SECURITY\Policy
18:10:...	lsass.exe	652	RegOpenKey	HKLM\SECURITY\Policy\SecDesc
18:10:...	lsass.exe	652	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(I
18:10:...	lsass.exe	652	RegCloseKey	HKLM\SECURITY\Policy\SecDesc
18:10:...	lsass.exe	652	RegOpenKey	HKLM\SECURITY\Policy\SecDesc
18:10:...	lsass.exe	652	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(I
18:10:...	lsass.exe	652	RegCloseKey	HKLM\SECURITY\Policy\SecDesc
18:10:...	lsass.exe	652	RegCloseKey	HKLM\SECURITY\Policy
18:10:...	lsass.exe	652	RegOpenKey	HKLM\SECURITY\Policy
18:10:...	lsass.exe	652	RegOpenKey	HKLM\SECURITY\Policy\SecDesc

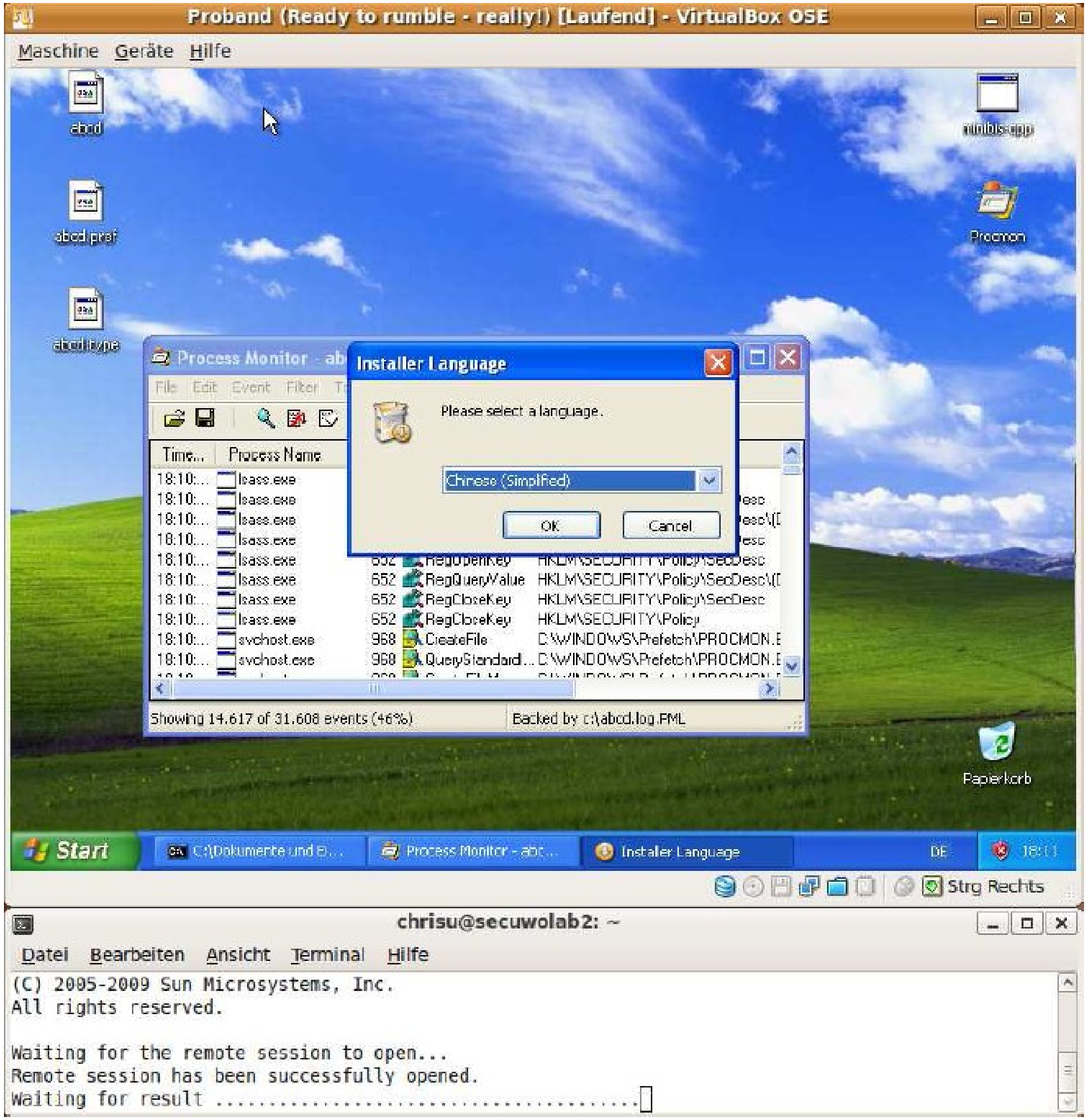
Showing 12.186 of 30.102 events (40%) Backed by c:\abcd.log.PML

```
(C) 2005-2009 Sun Microsystems, Inc.
All rights reserved.

Waiting for the remote session to open...
Remote session has been successfully opened.
Waiting for result ..............................................
```

ProcessMonitor from Sysinternals has just been started.

Screenshots



Please select a language.

Chinese (Simplified)

```
Time...   Process Name
18:10:... lsass.exe
18:10:... lsass.exe                                       esc
18:10:... lsass.exe                                       esc\(
18:10:... lsass.exe                                       esc
18:10:... lsass.exe       652 RegOpenKey      HKLM\SECURITY\Policy\SecDesc
18:10:... lsass.exe       652 RegQueryValue   HKLM\SECURITY\Policy\SecDesc\(
18:10:... lsass.exe       652 RegCloseKey     HKLM\SECURITY\Policy\SecDesc
18:10:... lsass.exe       652 RegCloseKey     HKLM\SECURITY\Policy
18:10:... svchost.exe     968 CreateFile      C:\WINDOWS\Prefetch\PROCMON.E
18:10:... svchost.exe     968 QueryStandard... C:\WINDOWS\Prefetch\PROCMON.E
```

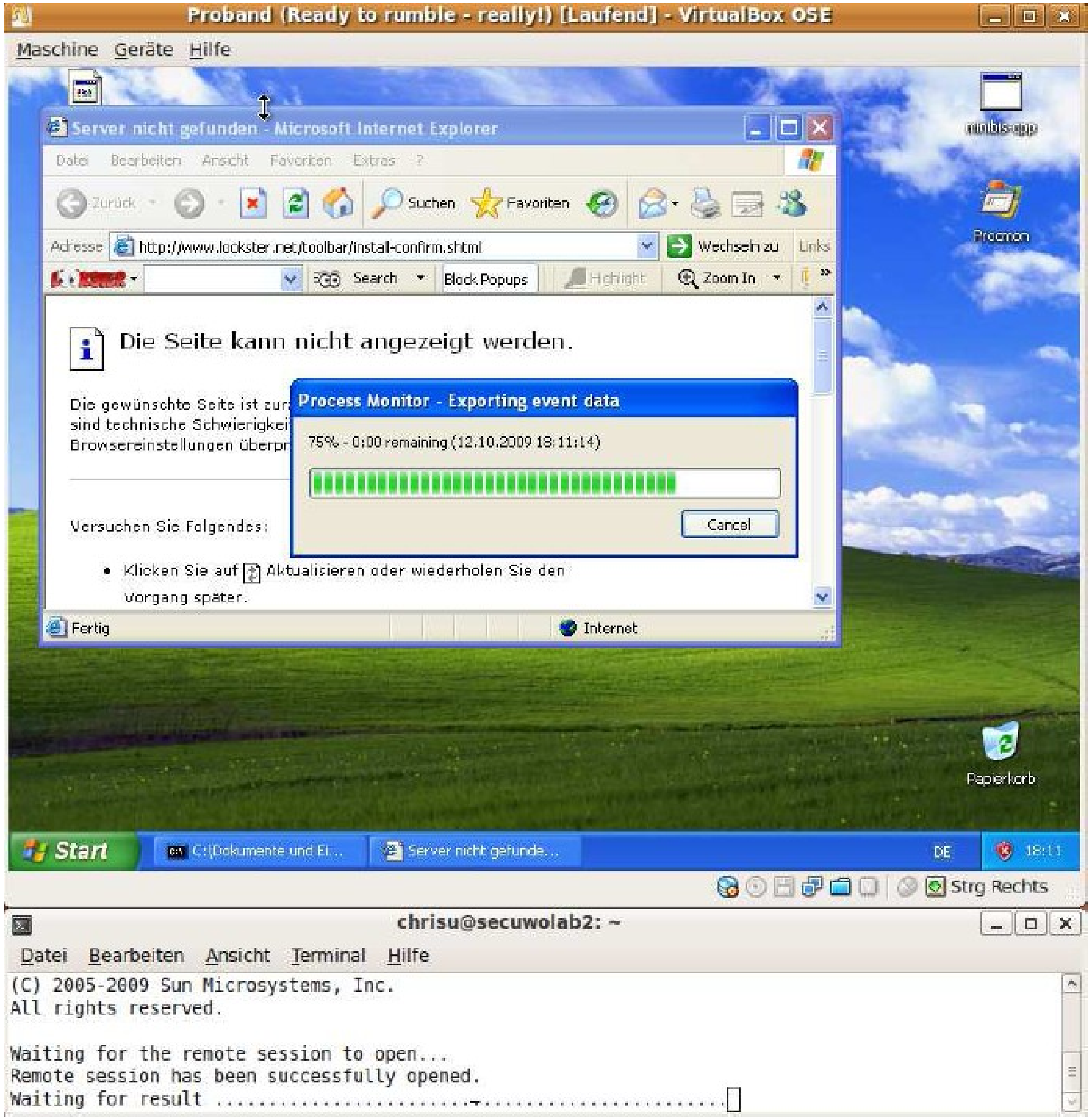
Showing 14.617 of 31.608 events (46%)   Backed by c:\abcd.log.PML

```
(C) 2005-2009 Sun Microsystems, Inc.
All rights reserved.

Waiting for the remote session to open...
Remote session has been successfully opened.
Waiting for result .......................................
```

Just an example of active malware.

Screenshots


Proband (Ready to rumble - really!) [Laufend] - VirtualBox OSE
Maschine Geräte Hilfe
Server nicht gefunden - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse
Wechseln zu Links
Search Block Popups Highlight Zoom In
Fertig
Internet
minbis-cpp
Procmon
Papierkorb
Start
C:\Dokumente und Ei...
Server nicht gefunde...
DE
18:11
Strg Rechts
chrisu@secuwolab2: ~
Datei Bearbeiten Ansicht Terminal Hilfe
Cancel

http://www.lockster.net/toolbar/install-confirm.shtml

Die Seite kann nicht angezeigt werden.

Die gewünschte Seite ist zur
sind technische Schwierigkei
Browsereinstellungen überpr

Versuchen Sie Folgendes:

- Klicken Sie auf Aktualisieren oder wiederholen Sie den Vorgang später.

Process Monitor - Exporting event data

75% - 0:00 remaining (12.10.2009 18:11:14)

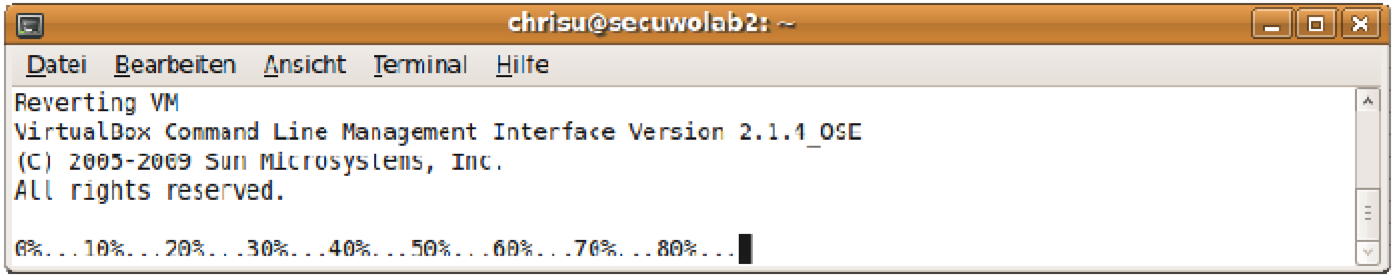
```
(C) 2005-2009 Sun Microsystems, Inc.
All rights reserved.

Waiting for the remote session to open...
Remote session has been successfully opened.
Waiting for result ..........................................
```

The native ProcessMonitor saving format is being converted to CSV.

Screenshots

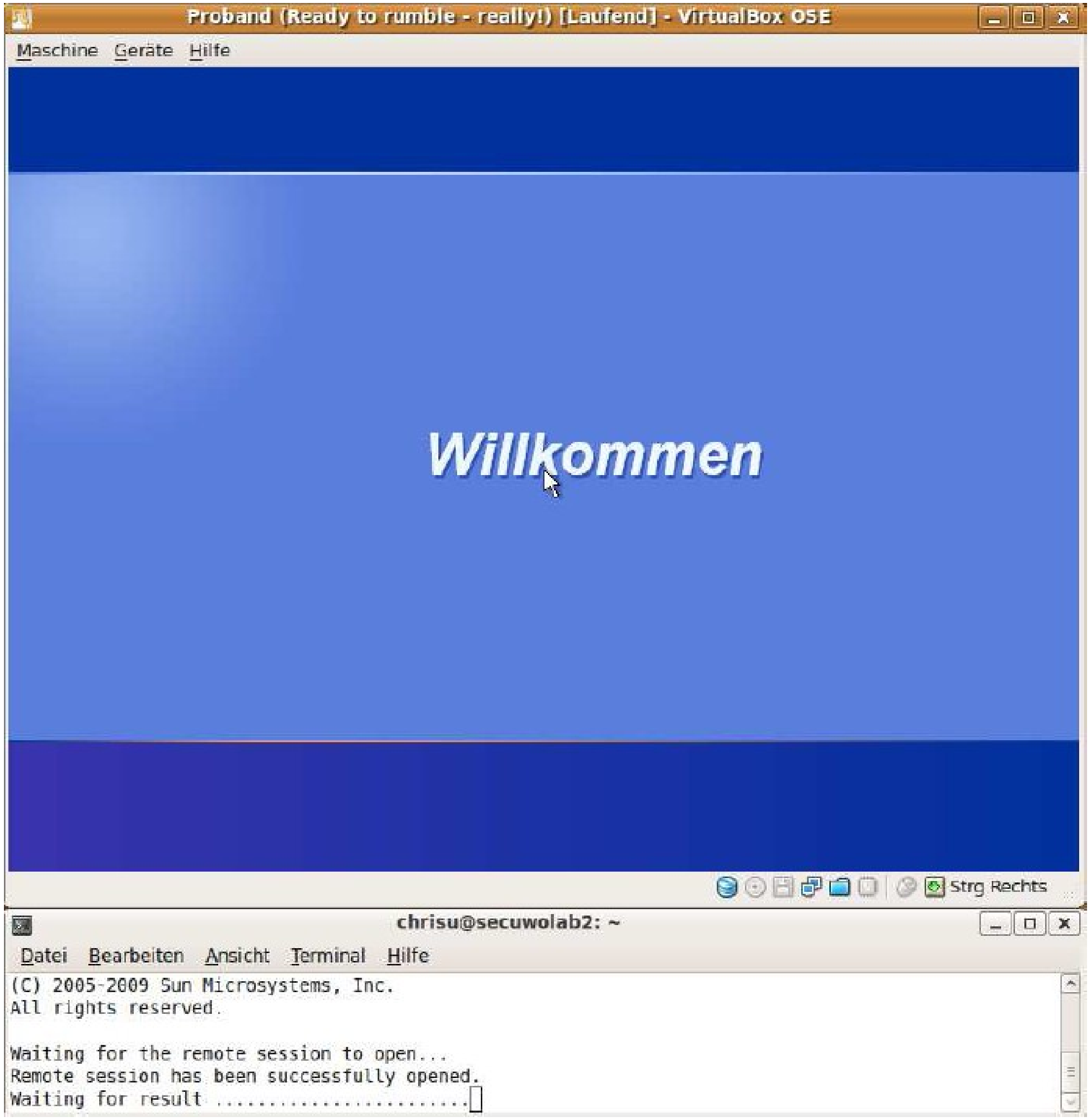
The virtual machine (proband) gets reverted.



```
Reverting VM
VirtualBox Command Line Management Interface Version 2.1.4_OSE
(C) 2005-2009 Sun Microsystems, Inc.
All rights reserved.

0%...10%...20%...30%...40%...50%...60%...70%...80%...
```

Screenshots

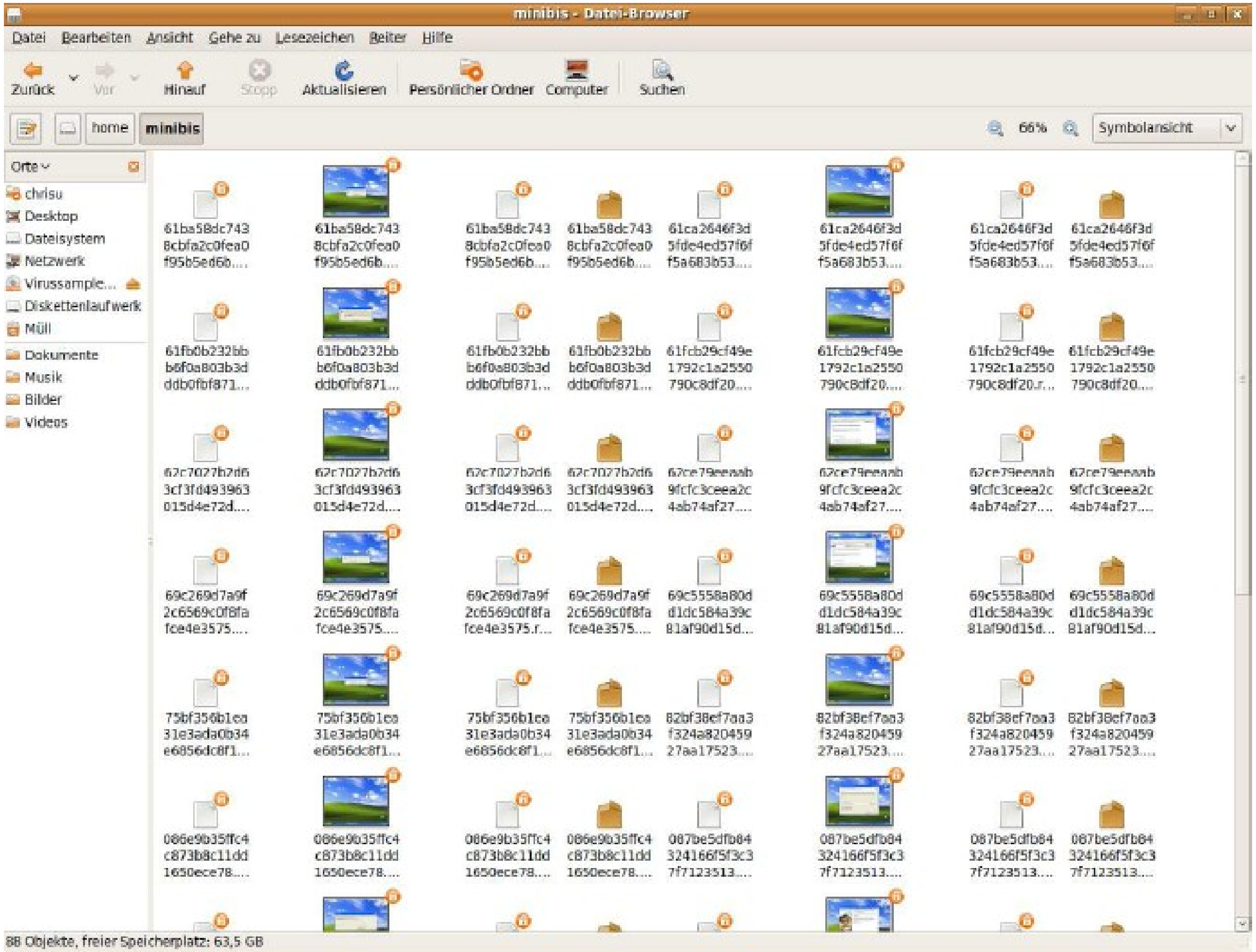

Proband (Ready to rumble - really!) [Laufend] - VirtualBox OSE
Maschine Geräte Hilfe
Willkommen
Strg Rechts
chrisu@secuwolab2: ~
Datei Bearbeiten Ansicht Terminal Hilfe

```
(C) 2005-2009 Sun Microsystems, Inc.
All rights reserved.

Waiting for the remote session to open...
Remote session has been successfully opened.
Waiting for result .......................
```

Malware caused our proband to restart. That's why we need the outer emergency break.

Viewing results after a few samples.


minibis - Datei-Browser
Datei
Bearbeiten
Ansicht
Gehe zu
Lesezeichen
Reiter
Hilfe
Zurück
Vor
Hinauf
Stopp
Aktualisieren
Persönlicher Ordner
Computer
Suchen
home
minibis
66%
Symbolansicht
Orte
chrisu
Desktop
Dateisystem
Netzwerk
Virussample...
Diskettenlaufwerk
Müll
Dokumente
Musik
Bilder
Videos
61ba58dc7438cbfa2c0fea0f95b5ed6b....
61ba58dc7438cbfa2c0fea0f95b5ed6b....
61ba58dc7438cbfa2c0fea0f95b5ed6b....
61ba58dc7438cbfa2c0fea0f95b5ed6b....
61ca2646f3d5fde4ed57f6ff5a683b53....
61ca2646f3d5fde4ed57f6ff5a683b53....
61ca2646f3d5fde4ed57f6ff5a683b53....
61ca2646f3d5fde4ed57f6ff5a683b53....
61fb0b232bbb6f0a803b3dddb0fbf871...
61fb0b232bbb6f0a803b3dddb0fbf871...
61fb0b232bbb6f0a803b3dddb0fbf871...
61fb0b232bbb6f0a803b3dddb0fbf871...
61fcb29cf49e1792c1a2550790c8df20....
61fcb29cf49e1792c1a2550790c8df20....
61fcb29cf49e1792c1a2550790c8df20.r...
61fcb29cf49e1792c1a2550790c8df20....
62c7027b2d63cf3fd493963015d4e72d....
62c7027b2d63cf3fd493963015d4e72d....
62c7027b2d63cf3fd493963015d4e72d....
62c7027b2d63cf3fd493963015d4e72d....
62ce79eeaab9fcfc3ceea2c4ab74af27....
62ce79eeaab9fcfc3ceea2c4ab74af27....
62ce79eeaab9fcfc3ceea2c4ab74af27....
62ce79eeaab9fcfc3ceea2c4ab74af27....
69c269d7a9f2c6569c0f8fafce4e3575....
69c269d7a9f2c6569c0f8fafce4e3575....
69c269d7a9f2c6569c0f8fafce4e3575.r...
69c269d7a9f2c6569c0f8fafce4e3575....
69c5558a80dd1dc584a39c81af90d15d...
69c5558a80dd1dc584a39c81af90d15d...
69c5558a80dd1dc584a39c81af90d15d...
69c5558a80dd1dc584a39c81af90d15d...
75bf356b1ea31e3ada0b34e6856dc8f1...
75bf356b1ea31e3ada0b34e6856dc8f1...
75bf356b1ea31e3ada0b34e6856dc8f1...
75bf356b1ea31e3ada0b34e6856dc8f1...
82bf38ef7aa3f324a82045927aa17523....
82bf38ef7aa3f324a82045927aa17523....
82bf38ef7aa3f324a82045927aa17523....
82bf38ef7aa3f324a82045927aa17523....
086e9b35ffc4c873b8c11dd1650ece78....
086e9b35ffc4c873b8c11dd1650ece78....
086e9b35ffc4c873b8c11dd1650ece78....
086e9b35ffc4c873b8c11dd1650ece78....
087be5dfb84324166f5f3c37f7123513....
087be5dfb84324166f5f3c37f7123513....
087be5dfb84324166f5f3c37f7123513....
087be5dfb84324166f5f3c37f7123513....

88 Objekte, freier Speicherplatz: 63,5 GB

What-For?

Example Evaluations

Some example evaluations on the basis of 3902 .exe samples ...

Example Evaluations

- „Size DOES matter“

● Biggest sample:	16.448.512 bytes
● Smallest sample:	812 bytes
● Average sample:	391.688 bytes

Example Evaluations

- „Browser-History-Junkies“
  - Historydata accessed: 1220 samples
    - Historydata written: 3 samples

Example Evaluations

- „Cookie Monsters“

● Cookies accessed:	118 samples
○ Cookies read:	58 samples
○ Cookies written:	4 samples
○ Cookies created:	3 samples

Example Evaluations

- „Security Center Kings“

Service disabled:	2 samples
Warnings diabled:	3 samples
Firewall disabled:	9 samples
Autoupdates disabled:	1 sample

Example Evaluations

- „Internet Settings“

Read:	1.480 samples
Changed:	1.236 samples

Example Evaluations

- „DNS-Kiddies“

● \etc\Host read:	9 samples
● \etc\Host written:	14 samples

Example Evaluations

- „Desktop Designers“
  - Screensaver changed: 44 samples
  - Wallpaper changed: 46 samples

Example Evaluations

- „Reboot-Fetish“

Pending renames scanned:	112 samples
Pending renames added:	41 samples
Pending renames deleted:	7 samples

Example Evaluations

- „Miscelaneous“

Taskmanager disabled:	446 samples
Other processes forked:	1.486 samples
Multiple threads used:	2.255 samples
ADS used:	3 samples

Example Evaluations

- „Favorite Autstart Method“

1161	**… HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
0887	**… HKLM\System\CurrentControlSet\Services**
0113	… HKCU\Software\Microsoft\Windows\CurrentVersion\Run
0101	… HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
0085	… HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
0063	… HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
0061	… HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
0050	… HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
0030	… \Programs\Startup\
0008	… HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
0007	… HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks
0004	… HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
0002	… HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
0001	… HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls

CERT.at's Implementation

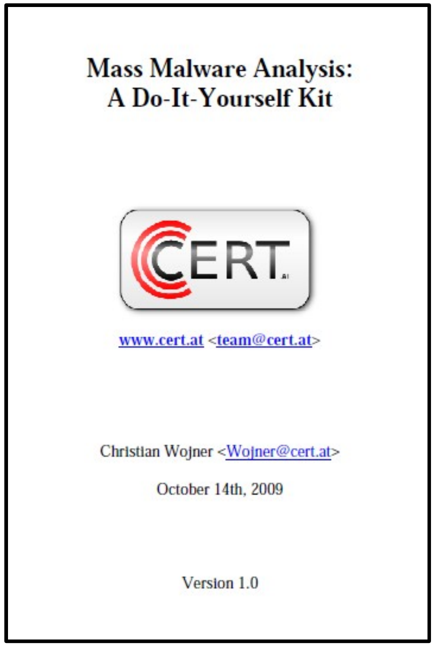
- The underlying paper provides you with
  - more details
  - a step-by-step guide for building CERT.at's implementation
  - and links for downloading our binaries

So, please take a look at it!

Feedback is always appreciated.

Topical Background

Paper from October 14th, 2009



Mass Malware Analysis:
A Do-It-Yourself Kit

www.cert.at <team@cert.at>

Christian Wojner <Wojner@cert.at>

October 14th, 2009

Version 1.0

http://cert.at/downloads/papers/mass_malware_analysis_en.html

Thanks!

Christian Wojner
wojner@cert.at