Sven Kälber
Chair of Computer Science I
email: sven.kaelber@cs.fau.de

Forensic Application-Fingerprinting...

... based on File System Metadata

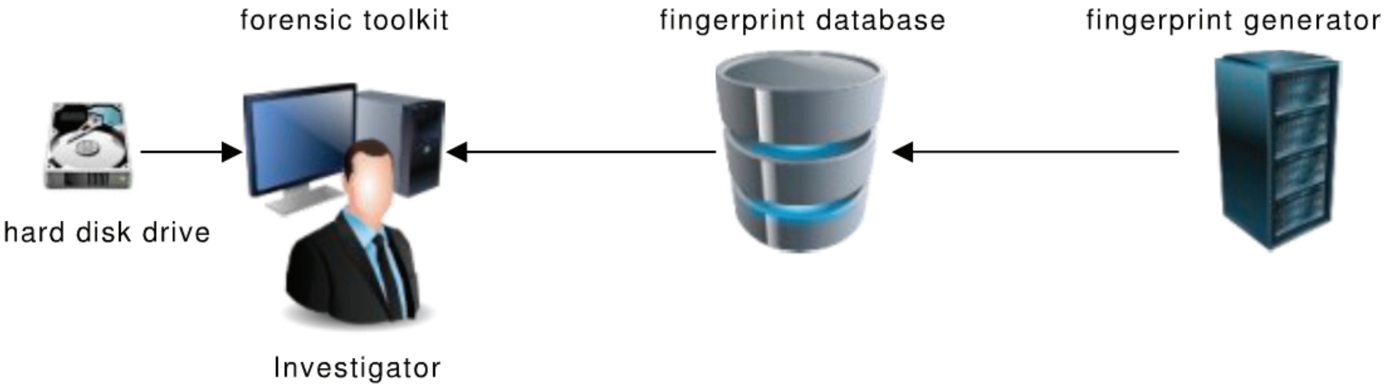
Motivation

- Event reconstruction is a key factor in digital forensic investigations.
- Investigators are facing a remarkable increase in the amount of cases as well as the data volume to be processed.
- Today, event reconstruction still is a mainly manually performed process, which leads to very time consuming investigations.

Motivation (cont'd)

Automating the important steps in the event reconstruction phase results in cost and time savings for the investigator.

How can the degree of automation for event reconstruction be increased?



Digital Evidence

Typically digital evidence can be found in:

- File contents
- Logfiles
- Browser cache and cookie files
- Deleted files
- File system metadata (timestamps)
- ...

No need for individual parsers or analysis tools for application specific files and data → allows for a generic approach!

File System Metadata

- In general, file systems store different timestamps for each file

- Example NTFS:
  - atime : last accessed timestamp
  - mtime: modified timestamp
  - crtime: created timestamp
  - ctime: MFT* entry modified timestamp

- Assumption: timestamps are faithfully updated by the operating system
  - NTFS only updates atime every 60 minutes
  - atime is enabled in pre-Vista Windows systems (XP, 2000, NT)
  - atime is disabled by default in Vista and Windows 7

* MFT = Master File Table of NTFS filesystems

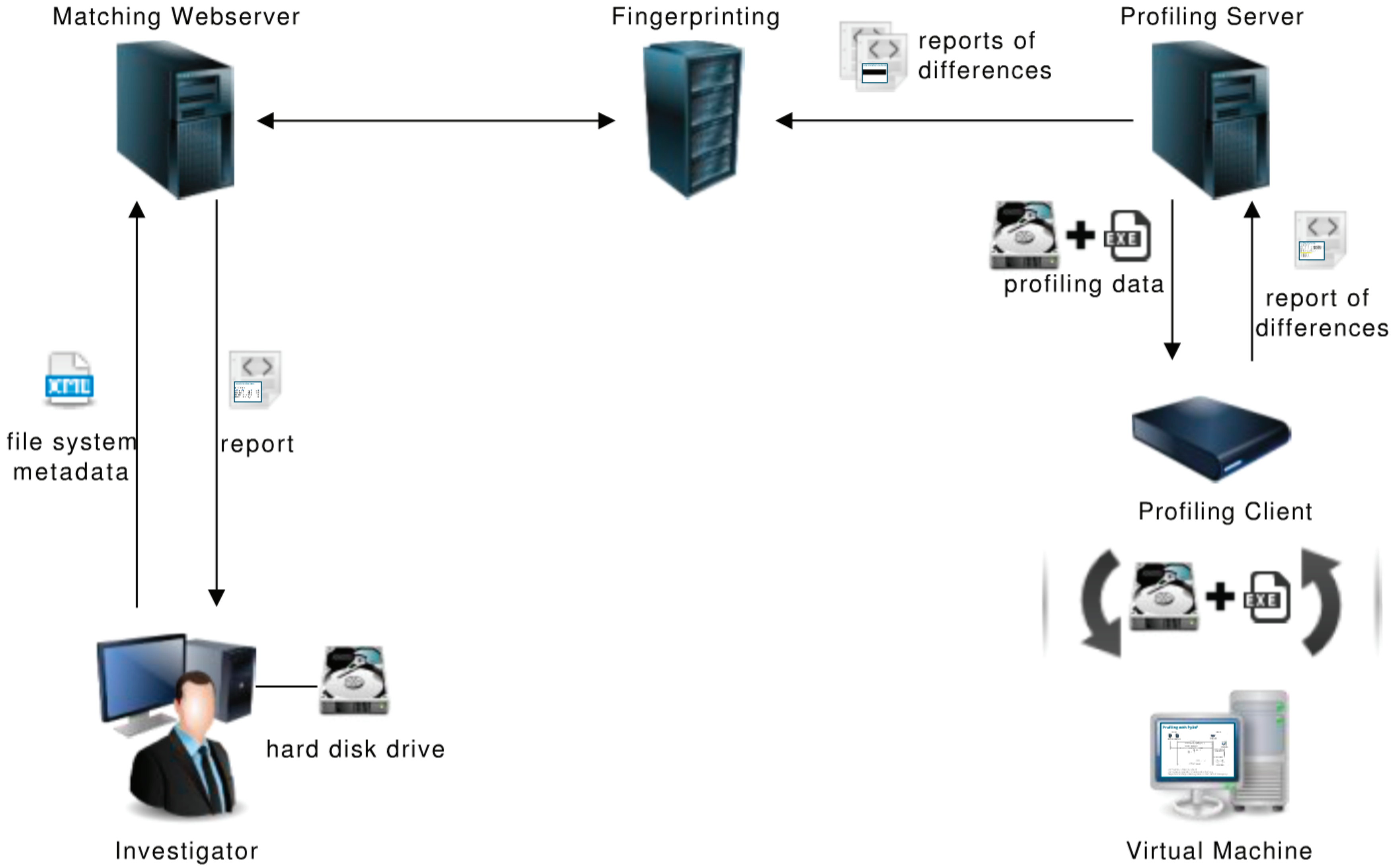
Inferring the Past

- Whenever an action is executed, multiple timestamps are changed; atime, mtime, ctime and crtime of:
  - Binaries
  - Libraries (DLLs)
  - Logfiles
  - Data files

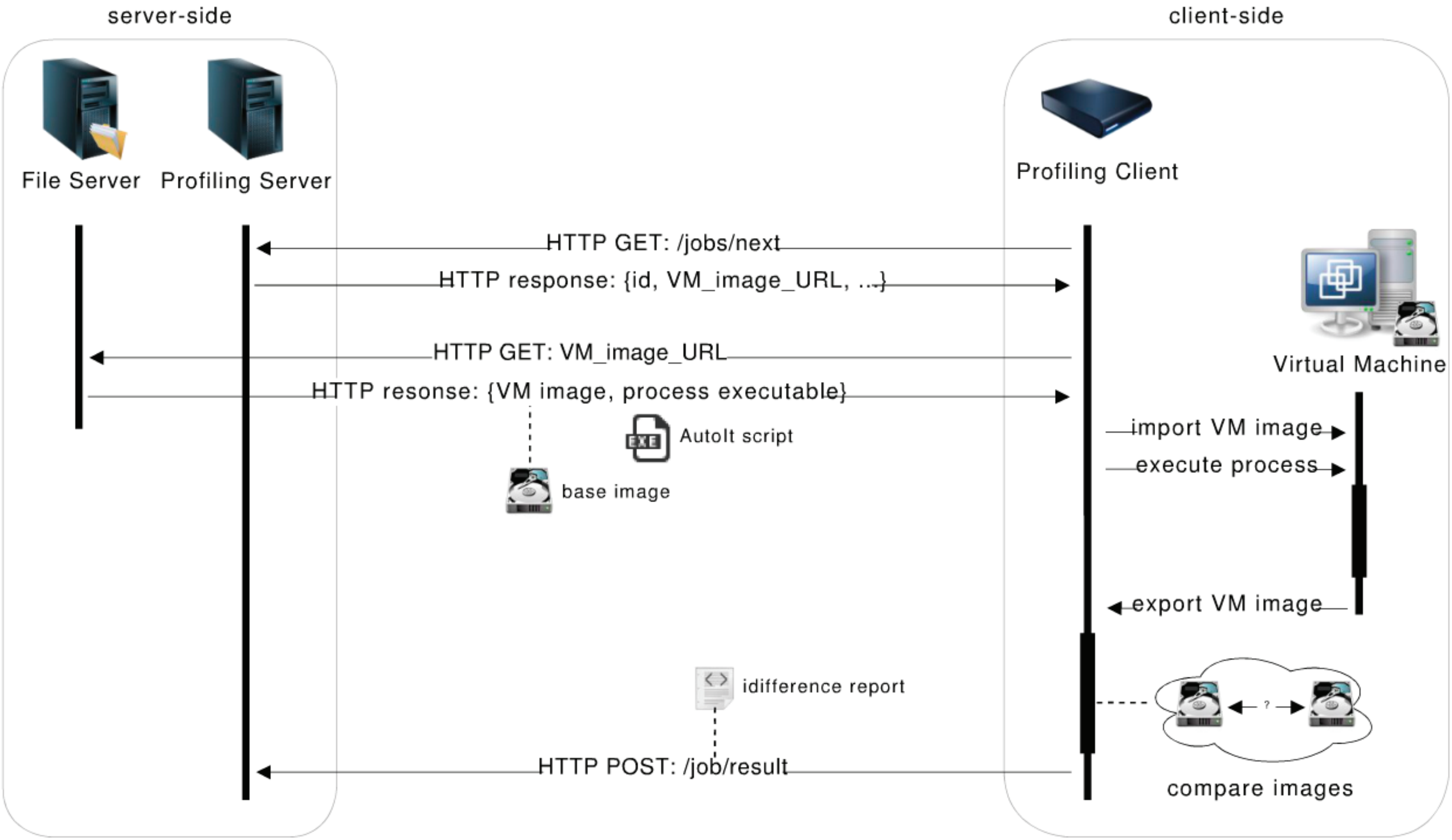
What can timestamps tell you about previously performed actions?

- Example: What happens (timestamp-wise) if you receive a new message in your ICQ instant messenger application?

System Overview: Py3xF



Profiling with Py3xF

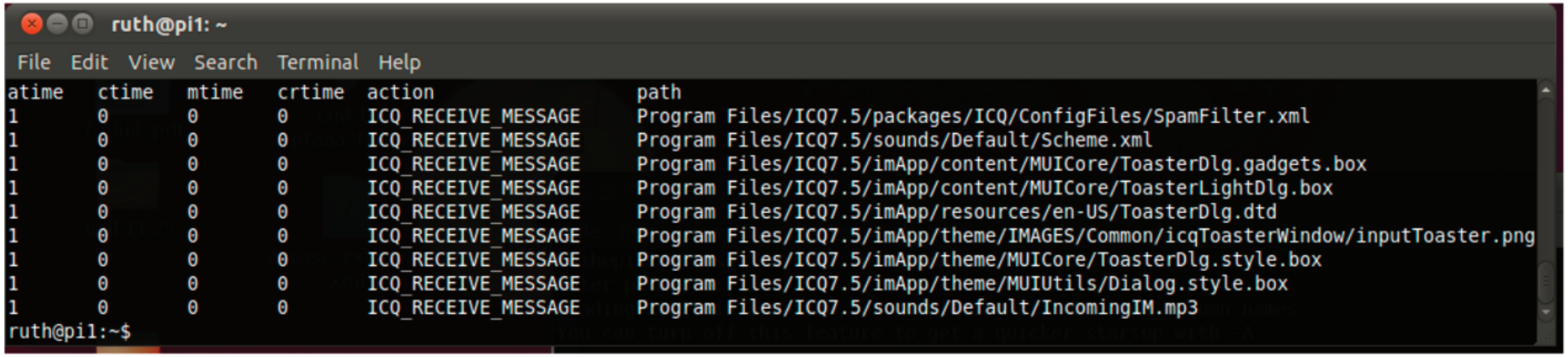


- profiling process is completely automated
- profiling requires a prepared virtual machine and an AutoIt script
- comparison of disk images is done using Simson Garfinkel's fiwalk idifference.py script

Receiving an ICQ Message

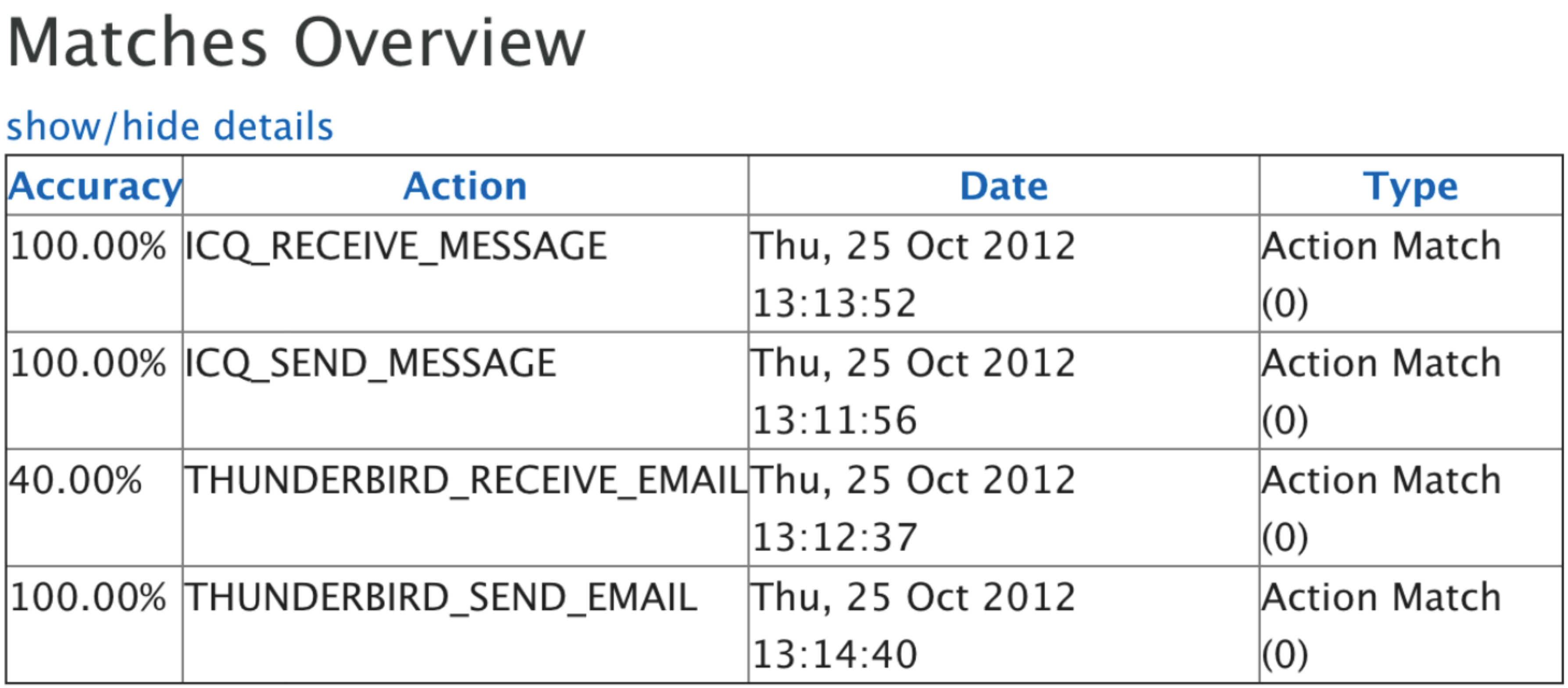
```
…
WINDOWS/system32/config/system.LOG:mtime_changed = 1
WINDOWS/system32/devenum.dll:atime_changed = 1
WINDOWS/system32/jscript.dll:atime_changed = 1
WINDOWS/system32/ksuser.dll:atime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/Content/04AFA8793E5CDC4A81C6CD4554A30707:ctime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/Content/04AFA8793E5CDC4A81C6CD4554A30707:mtime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/Content/D4F348B882DF3F205ECCB6243795CB3A:ctime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/Content/D4F348B882DF3F205ECCB6243795CB3A:mtime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/MetaData/04AFA8793E5CDC4A81C6CD4554A30707:ctime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/MetaData/04AFA8793E5CDC4A81C6CD4554A30707:mtime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/MetaData/D4F348B882DF3F205ECCB6243795CB3A:ctime_changed = 1
Documents and Settings/user/Application Data/Microsoft/CryptnetUrlCache/MetaData/D4F348B882DF3F205ECCB6243795CB3A:mtime_changed = 1
Program Files/ICQ7M/imApp/content/MUICore/ToasterDlg.gadgets.box:atime_changed = 1
Program Files/ICQ7M/imApp/content/MUICore/ToasterLightDlg.box:atime_changed = 1
Program Files/ICQ7M/imApp/resources/en-US/ToasterDlg.dtd:atime_changed = 1
Program Files/ICQ7M/imApp/theme/IMAGES/Common/icqToasterWindow/inputToaster.png:atime_changed = 1
Program Files/ICQ7M/imApp/theme/MUICore/ToasterDlg.style.box:atime_changed = 1
Program Files/ICQ7M/imApp/theme/MUIUtils/Dialog.style.box:atime_changed = 1
Program Files/ICQ7M/packages/ICQ/ConfigFiles/SpamFilter.xml:atime_changed = 1
Program Files/ICQ7M/packages/german/language/de-DE/ToasterDlg.dtd:atime_changed = 1
Program Files/ICQ7M/sounds/Default/incomingIM.mp3:atime_changed = 1
Program Files/ICQ7M/sounds/Default/Scheme.xml:atime_changed = 1
WINDOWS/system32/devenum.dll:atime_changed = 1
WINDOWS/system32/ksuser.dll:atime_changed = 1
WINDOWS/system32/l3codecx.ax:atime_changed = 1
WINDOWS/system32/msdmo.dll:atime_changed = 1
WINDOWS/system32/quartz.dll:atime_changed = 1
WINDOWS/system32/vbscript.dll:atime_changed = 1
WINDOWS/system32/l3codecx.ax:atime_changed = 1
WINDOWS/system32/quartz.dll:atime_changed = 1
WINDOWS/system32/security.dll:atime_changed = 1
WINDOWS/system32/vbscript.dll:atime_changed = 1
WINDOWS/system32/wbem/wmipcima.dll:atime_changed = 1
…
```

Example Fingerprint generated by Py3xF



```
atime   ctime   mtime   crtime  action                  path
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/packages/ICQ/ConfigFiles/SpamFilter.xml
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/sounds/Default/Scheme.xml
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/imApp/content/MUICore/ToasterDlg.gadgets.box
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/imApp/content/MUICore/ToasterLightDlg.box
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/imApp/resources/en-US/ToasterDlg.dtd
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/imApp/theme/IMAGES/Common/icqToasterWindow/inputToaster.png
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/imApp/theme/MUICore/ToasterDlg.style.box
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/imApp/theme/MUIUtils/Dialog.style.box
1       0       0       0       ICQ_RECEIVE_MESSAGE     Program Files/ICQ7.5/sounds/Default/IncomingIM.mp3
ruth@pi1:~$
```

Example Matching Report

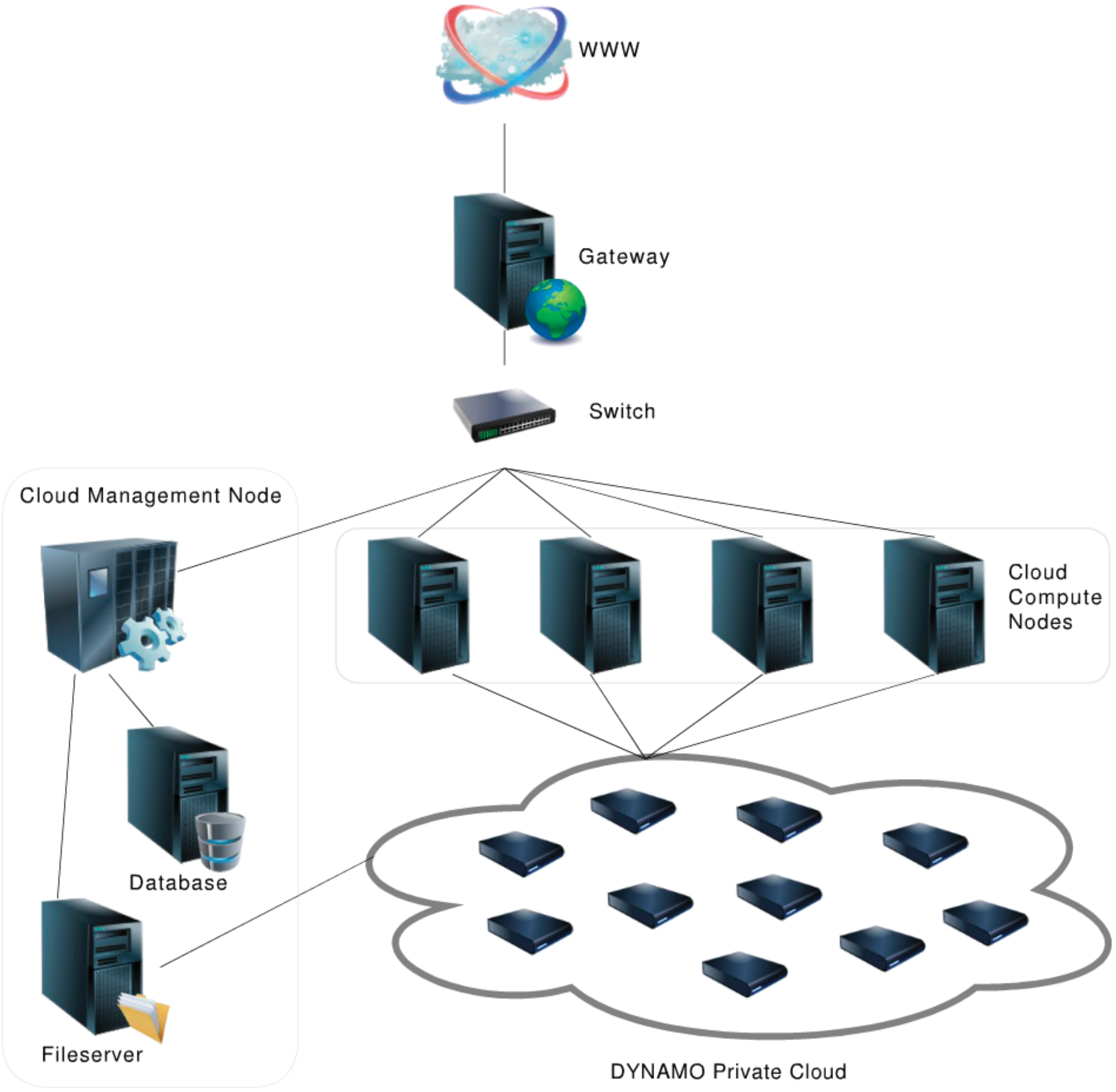


Matches Overview

show/hide details

Accuracy	Action	Date	Type
100.00%	ICQ_RECEIVE_MESSAGE	Thu, 25 Oct 2012 13:13:52	Action Match (0)
100.00%	ICQ_SEND_MESSAGE	Thu, 25 Oct 2012 13:11:56	Action Match (0)
40.00%	THUNDERBIRD_RECEIVE_EMAIL	Thu, 25 Oct 2012 13:12:37	Action Match (0)
100.00%	THUNDERBIRD_SEND_EMAIL	Thu, 25 Oct 2012 13:14:40	Action Match (0)

Hardware Setup



Case Study: Sending & Receiving Mails and Instant Messages

13:11 - THUNDERBIRD_SEND_EMAIL

13:12 - ICQ_SEND_MESSAGE

13:12 - THUNDERBIRD_RECEIVE_EMAIL

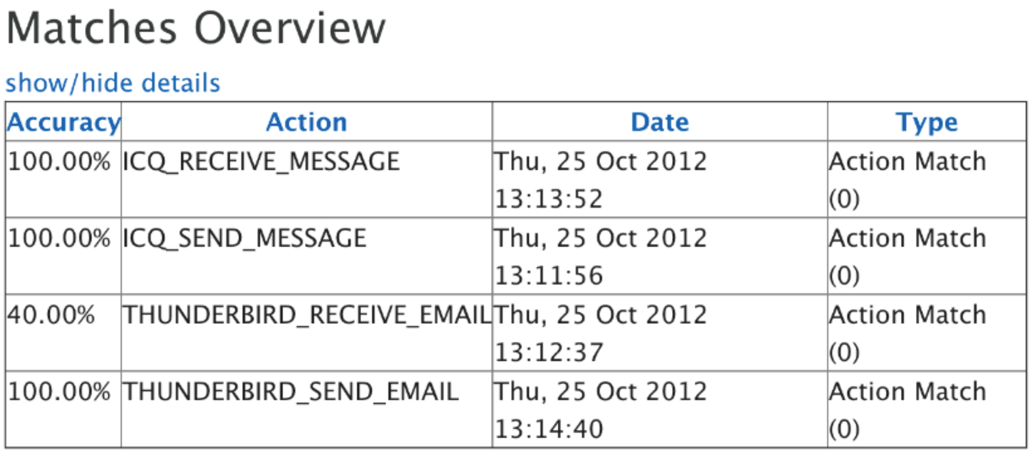
13:13 - ICQ_RECEIVE_MESSAGE

13:13 - THUNDERBIRD_SEND_EMAIL

13:15 - ICQ_SEND_MESSAGE

13:16 - ICQ_RECEIVE_MESSAGE

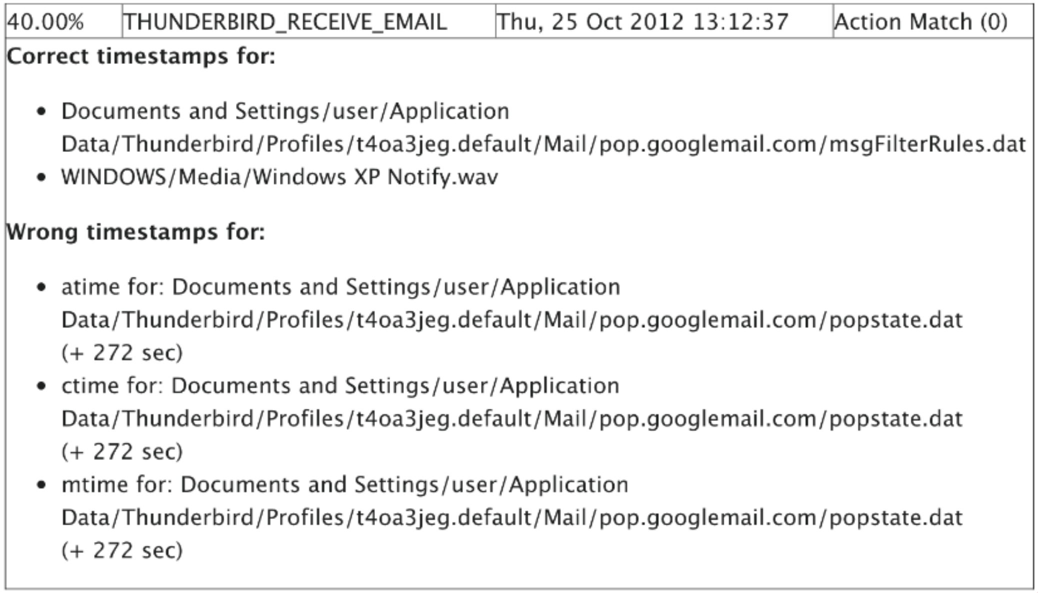
13:16 - THUNDERBIRD_RECEIVE_EMAIL



Matches Overview

show/hide details

Accuracy	Action	Date	Type
100.00%	ICQ_RECEIVE_MESSAGE	Thu, 25 Oct 2012 13:13:52	Action Match (0)
100.00%	ICQ_SEND_MESSAGE	Thu, 25 Oct 2012 13:11:56	Action Match (0)
40.00%	THUNDERBIRD_RECEIVE_EMAIL	Thu, 25 Oct 2012 13:12:37	Action Match (0)
100.00%	THUNDERBIRD_SEND_EMAIL	Thu, 25 Oct 2012 13:14:40	Action Match (0)



40.00%	THUNDERBIRD_RECEIVE_EMAIL	Thu, 25 Oct 2012 13:12:37	Action Match (0)

Correct timestamps for:

- Documents and Settings/user/Application Data/Thunderbird/Profiles/t4oa3jeg.default/Mail/pop.googlemail.com/msgFilterRules.dat
- WINDOWS/Media/Windows XP Notify.wav

Wrong timestamps for:

- atime for: Documents and Settings/user/Application Data/Thunderbird/Profiles/t4oa3jeg.default/Mail/pop.googlemail.com/popstate.dat (+ 272 sec)
- ctime for: Documents and Settings/user/Application Data/Thunderbird/Profiles/t4oa3jeg.default/Mail/pop.googlemail.com/popstate.dat (+ 272 sec)
- mtime for: Documents and Settings/user/Application Data/Thunderbird/Profiles/t4oa3jeg.default/Mail/pop.googlemail.com/popstate.dat (+ 272 sec)

Limitations

- Fingerprints generated by Py3xF are prone to timestamp manipulation.
- Path and files with temporary or differing names prevent a fingerprint generated by Py3xF from being matched on different machines (e.g. C:\Users\[username]\...).
- Fingerprints are generated by comparing all already profiled actions, thus creating new profiles might have impact on existing fingerprints.
- Py3xF's fingerprinting functionalities were only tested with Windows operating systems, which are running based on the NTFS filesystem (XP and 7)

Future Work

- Profile and fingerprint various actions of multiple applications in different Windows versions.
- Overcome the issue of temporary path and file names by applying machine learning techniques instead of simple string comparison operations.
- Extend Py3xF to operate on journal data provided by journaling file systems like NTFS to also match previously performed actions instead of only the last one.
- Extend Py3xF for the usage with smartphone apps by adding support for Android and iOS file systems

Thank you for your attention!

Questions?