Research Project 2: Forensic Challenge

Axel Puppe & Joeri Blokhuis

June 30, 2010

- Founded in 2001, annual meeting
- Advancing digital forensic science
- Target crowd:
  - University researchers
  - Computer forensic examiners
  - Analysts
- Since 2005 annual challenge

- Suspected arms dealer
- Recovered phone from canal (memory dumps)
- Questions:
  - Evidence connecting suspect to the sale of arms
  - Evidence of the receipt of payment
  - Recovery of any other leads: individuals, companies, or bank accounts

- Phone data
  - Log
    - Phone calls
    - Text messages
  - Calendar
    - Appointments
    - Reminders
    - Birthdays
  - Address book
- File data
  - Multimedia files
    - Audio
    - Video
    - Photos
  - Documents
- Internet data
  - Browser
    - History
    - Cache
    - Bookmarks
  - E-mail
    - Sent
    - Received
    - Drafts
    - Deleted
    - Account settings
  - Instant messaging

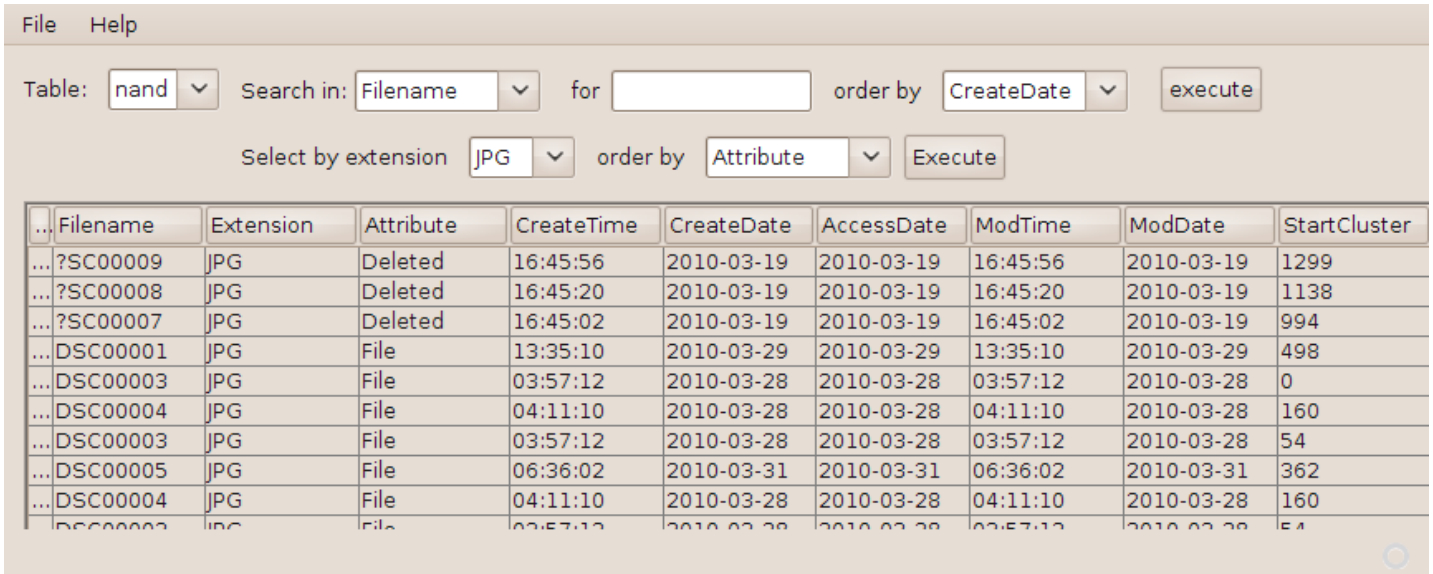
- Standard forensic tools
- Developed forensic tools
  - FAT Walker
  - Xarver

- **Unsuccessful**: Autopsy/Sleuthkit, Encase, FTK, Paraben Cell Seizure, pyflag
- **Beneficial**: Scalpel(carving), Standard Linux commands(strings, file, grep), Google goggles.

Figure: Picture taken and identified by Google goggles

- Extract Directory Table Entries
  - On physical memory dumps
  - Filenames/Extension, MAC times (**Modified/Access/Creation**)
- Benefits for a forensic investigator:
  - Initial research
  - Possible user behaviour on the phone
  - Last created files
  - Build an absolute path (depending on the parent and current directory)

Screenshot



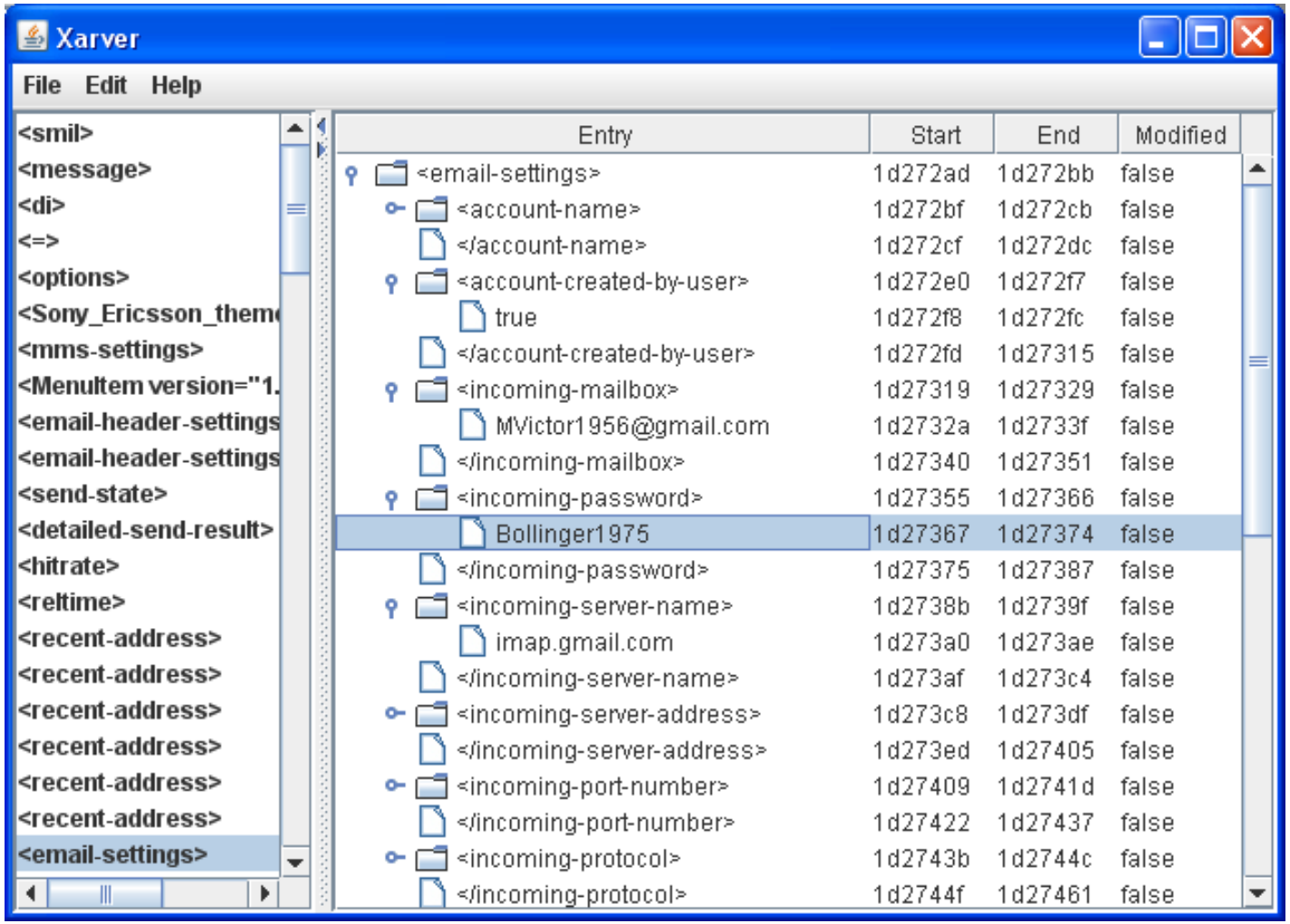
...	Filename	Extension	Attribute	CreateTime	CreateDate	AccessDate	ModTime	ModDate	StartCluster
...	?SC00009	JPG	Deleted	16:45:56	2010-03-19	2010-03-19	16:45:56	2010-03-19	1299
...	?SC00008	JPG	Deleted	16:45:20	2010-03-19	2010-03-19	16:45:20	2010-03-19	1138
...	?SC00007	JPG	Deleted	16:45:02	2010-03-19	2010-03-19	16:45:02	2010-03-19	994
...	DSC00001	JPG	File	13:35:10	2010-03-29	2010-03-29	13:35:10	2010-03-29	498
...	DSC00003	JPG	File	03:57:12	2010-03-28	2010-03-28	03:57:12	2010-03-28	0
...	DSC00004	JPG	File	04:11:10	2010-03-28	2010-03-28	04:11:10	2010-03-28	160
...	DSC00003	JPG	File	03:57:12	2010-03-28	2010-03-28	03:57:12	2010-03-28	54
...	DSC00005	JPG	File	06:36:02	2010-03-31	2010-03-31	06:36:02	2010-03-31	362
...	DSC00004	JPG	File	04:11:10	2010-03-28	2010-03-28	04:11:10	2010-03-28	160

- Memory dump 1:
  - Only two distinct MAC times
- Memory dump 2:
  - Clear gap from 2008 to 2010
  - Top files created since 2010: JPG, BIN, DAT and XML.
- Not updated: Access and Modification time
- Decide possible focus!

```
<?xml version="1.0" encoding="UTF-8" ?>
<Forensics>
    <Unit>
        <Name> The Netherlands Forensic Institute </Name>
        <City> The Hague </City>
    </Unit>
    <Unit>
        <Name> New Scotland Yard </Name>
        <City> London </City>
    </Unit>
</Forensics>
```

- XML Usage:
  - Sim Cards
  - Databases
  - Open Office XML
  - Mobile phone (Android) applications
  - And more...
- Xarver features:
  - Read raw data
  - Build XML tree
  - Deal with damaged XML
  - Gives offsets of original data

Screenshot


Xarver
File Edit Help
<smil>
<message>
<di>
<=>
<options>
<Sony_Ericsson_theme
<mms-settings>
<MenuItem version="1.
<email-header-settings
<email-header-settings
<send-state>
<detailed-send-result>
<hitrate>
<reltime>
<recent-address>
<recent-address>
<recent-address>
<recent-address>
<recent-address>
<recent-address>
<email-settings>
Entry Start End Modified
<email-settings> 1d272ad 1d272bb false
<account-name> 1d272bf 1d272cb false
</account-name> 1d272cf 1d272dc false
<account-created-by-user> 1d272e0 1d272f7 false
true 1d272f8 1d272fc false
</account-created-by-user> 1d272fd 1d27315 false
<incoming-mailbox> 1d27319 1d27329 false
MVictor1956@gmail.com 1d2732a 1d2733f false
</incoming-mailbox> 1d27340 1d27351 false
<incoming-password> 1d27355 1d27366 false
Bollinger1975 1d27367 1d27374 false
</incoming-password> 1d27375 1d27387 false
<incoming-server-name> 1d2738b 1d2739f false
imap.gmail.com 1d273a0 1d273ae false
</incoming-server-name> 1d273af 1d273c4 false
<incoming-server-address> 1d273c8 1d273df false
</incoming-server-address> 1d273ed 1d27405 false
<incoming-port-number> 1d27409 1d2741d false
</incoming-port-number> 1d27422 1d27437 false
<incoming-protocol> 1d2743b 1d2744c false
</incoming-protocol> 1d2744f 1d27461 false

Combining the tools

Xarver

Email	
Subject:	Engine
From:	Mvictor1956@gmail.com
To:	grassyjansen@yahoo.com
When:	2010-03-28 04:12:18
Attachment:	file:///tpa/system/messaging/email/Mv/msg_00005/DSC00004.JPG

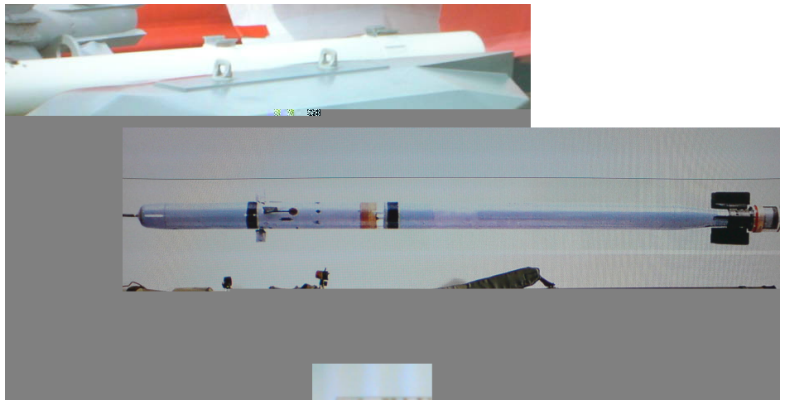
FAT Walker

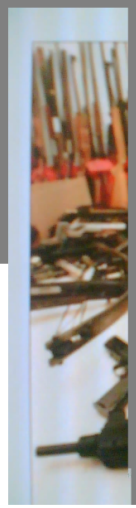
Scalpel

Google Goggles

- MMS
  - Subjects: Look at this, This?, Contact, ...
- Email
  - Subjects: Buy, Engine, Payment, ...
- Email Settings
  - Email address
  - Username
  - Password
  - And more...
- Call log

Pictures





- Evidence connecting suspect to the sale of arms
  - *Found emails + pictures*
- Evidence of the receipt of payment
  - *Suspected email (subject: 'payment')*
- Recovery of any other leads: individuals, companies, or bank accounts
  - *Individuals yes, Companies/Bank account(s) nothing so far...*

Questions?