Research Project 2: Forensic Challenge

Axel Puppe & Joeri Blokhuis

June 30, 2010
Introduction

Method

FAT Walker

Xarver

Investigation

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

- 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
What information can be expected in a mobile phone?

- **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
Standard Forensic tools

- **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](image)
► 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)
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
Axel Puppe & Joeri Blokhuis
Research Project 2: Forensic Challenge
Combining the tools

Xarver

<table>
<thead>
<tr>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject:</td>
</tr>
<tr>
<td>From:</td>
</tr>
<tr>
<td>To:</td>
</tr>
<tr>
<td>When:</td>
</tr>
<tr>
<td>Attachment:</td>
</tr>
</tbody>
</table>

FAT Walker

Google Goggles

Scalpel

Axel Puppe & Joeri Blokhuis
Research Project 2: Forensic Challenge
- MMS
  - Subjects: Look at this, This?, Contact, ...

- Email
  - Subjects: Buy, Engine, Payment, ...

- Email Settings
  - Email address
  - Username
  - Password
  - And more...

- Call log
Axel Puppe & Joeri Blokhuis
Research Project 2: Forensic Challenge
▶ 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?