OPEN SOURCE FORENSIC CASE MANAGEMENT

Sarah Holmes
About Me

- Computer Science BSc Hons
- Forensic Informatics MSc
- Advanced Professional Certificate in Investigative Practice
- AccessData Certified Examiner
- Certified Malware Investigator
- Currently work in Threat Management at RBS
- Previously a Senior Forensic Analyst at RBS
- Forensic Investigator at Morgan Stanley

www.lowmanio.co.uk
Open-Source Forensic Case Management
Contents

- What is Forensic Case Management
- The Problem
- Current Systems
- Introducing my Solution
- Conclusions
Forensic Case Management

- Organises case lifecycle
- The processes and procedures around how cases are created, divided up in the team, worked on and then delivered
The Problem

- Many companies don’t have a specific or tailored forensics case management solution. Why?
- There aren’t many forensics specific software solutions out there
- They decide to use a system already used within their organisation
- Many forensics teams were not built from scratch – morphed from IT teams
- Case management software doesn’t look like it adds value compared to actual forensic software
“Doesn’t Add Value”

- Evidence Tracking
- Case & Task tracking
- Reporting
- Secure
- Audit trails
- Role based permissions & administration
- Centralised database
Alternatives

- A spreadsheet used as database to map many-to-one relationships
  - Manual reporting
  - No audit trail – override data
  - One file, easy to corrupt
- Using a generic ticketing system
  - Forensic Report generation
  - Evidence tracking
  - Secret need-to-know cases
Current Systems

- Intraforensics Lima
- Blackthorn Case Management
- AccessData AdLabs

Open-Source Forensic Case Management
Lima

Open-Source Forensic Case Management
Blackthorn Case Management
AccessData AdLabs
Problem with these solutions

- Expensive
- Closed source
The most important part of a new project is coming up with a good name
Foreman
Open-Source Forensic Case Management
Foreman

/ˈfoʊmən/
noun
noun: foreman; plural noun: foremen
1.
A worker who supervises and directs other workers.
synonyms: supervisor, overseer, superintendent, manager, manageress, boss, team leader, line manager, controller; foreperson; chargehand, captain, ganger; griev: induna; maistry; informal chief, head honcho, governor, super; informal gaffer, guv'nor; informal ramrod, straw boss; informal pannikin boss; overman "the foreman was left in charge of the printing works"

2.
(in a law court) a person who presides over a jury and speaks on its behalf.
Foreman Details

- Open Source – available on BitBucket
- Written in Python
- Web-based system
- Database backend (SQLite & Postgres supported)

www.foreman-forensics.org
Foreman Overview

Users
- Requester
- Case Managers
- Investigator
- QA
- Admin

Cases
- Created
- Open
- Closed
- Archived

Tasks
- Created
- Allocated
- Forensics in Progress
- QA
- Delivery
- Complete
- Closed

Evidence

Task

Case

Open-Source Forensic Case Management
Tasks for Nybble Lowman

Outstanding Tasks as principle Forensic Investigator

<table>
<thead>
<tr>
<th>Case Name</th>
<th>Task Name</th>
<th>Task Type</th>
<th>Task Created</th>
<th>Status</th>
<th>Principle Forensic Investigator</th>
<th>Secondary Forensic Investigator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lantern</td>
<td>Lantern_02-1</td>
<td>User Personal Drive Capture</td>
<td>10 Jun 2014 22:03:58</td>
<td>Allocated</td>
<td>Nybble Lowman</td>
<td>None</td>
</tr>
<tr>
<td>L - Kemp</td>
<td>L - Kemp_02-2</td>
<td>Instant Messenger Search</td>
<td>10 Jun 2014 22:03:59</td>
<td>Forensics in Process</td>
<td>Nybble Lowman</td>
<td>None</td>
</tr>
<tr>
<td>Maetoic</td>
<td>Maetoic_03-3</td>
<td>Email Search</td>
<td>10 Jun 2014 22:03:59</td>
<td>Allocated</td>
<td>Nybble Lowman</td>
<td>None</td>
</tr>
</tbody>
</table>

Outstanding Tasks as secondary Forensic Investigator

None.

All Open Tasks

<table>
<thead>
<tr>
<th>Case Name</th>
<th>Task Name</th>
<th>Task Type</th>
<th>Task Created</th>
<th>Status</th>
<th>Principle Forensic Investigator</th>
<th>Secondary Forensic Investigator</th>
</tr>
</thead>
<tbody>
<tr>
<td>L - Kemp</td>
<td>L - Kemp_03-3</td>
<td>User Browser History</td>
<td>10 Jun 2014 22:03:59</td>
<td>Queued</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>L - Meteor</td>
<td>L - Meteor_01-2</td>
<td>User Browser History</td>
<td>10 Jun 2014 22:03:59</td>
<td>Forensics in Process</td>
<td>Steven W Holmes</td>
<td>None</td>
</tr>
<tr>
<td>Laveer</td>
<td>Laveer_02-1</td>
<td>Fax Search</td>
<td>10 Jun 2014 22:03:58</td>
<td>Forensics in Process</td>
<td>Sarah Holmes</td>
<td>None</td>
</tr>
<tr>
<td>Maitre</td>
<td>Maitre_03-4</td>
<td>Networked Drive Search</td>
<td>10 Jun 2014 22:03:58</td>
<td>Allocated</td>
<td>Pixel F Lowman</td>
<td>None</td>
</tr>
<tr>
<td>Laveer</td>
<td>Laveer_01-2</td>
<td>Malware Analysis</td>
<td>10 Jun 2014 22:03:58</td>
<td>Queued</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Latvia</td>
<td>Latvia_01-6</td>
<td>Mobile Image</td>
<td>10 Jun 2014 22:03:58</td>
<td>Queued</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Latvia</td>
<td>Latvia_02-7</td>
<td>User Browser History</td>
<td>10 Jun 2014 22:03:58</td>
<td>Queued</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Latvia</td>
<td>Latvia_03-8</td>
<td>Email Archive Search</td>
<td>10 Jun 2014 22:03:58</td>
<td>Queued</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Latvia</td>
<td>Latvia_04-9</td>
<td>Windows Event Log Analysis</td>
<td>10 Jun 2014 22:03:58</td>
<td>Allocated</td>
<td>Steven W Holmes</td>
<td>None</td>
</tr>
</tbody>
</table>
Case L - Kemp

Case Background

Laurent Gbagbo, born on 31 May 1945, in the Mama village of the Ouragahio sous-préfecture, Gagnoa department in Côte d’Ivoire. He is an Ivorian national and former President of Côte d’Ivoire.

Laurent Gbagbo allegedly bears individual criminal responsibility, as indirect co-perpetrator, for four counts of crimes against humanity:

- murder,
- violence,
- persecution
- other inhuman acts; allegedly committed in the context of post-electoral violence in the territory of Côte d’Ivoire between 16 December 2010 and 12 April 2011

Details

<table>
<thead>
<tr>
<th>Reference</th>
<th>HERFDHDF45777</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Files Location</td>
<td>C:\Users\Sarah\Programming\Foreman</td>
</tr>
<tr>
<td>Private</td>
<td>Yes</td>
</tr>
<tr>
<td>Case Created</td>
<td>10 Jun 2014 22:03:40</td>
</tr>
<tr>
<td>Status</td>
<td>Open</td>
</tr>
<tr>
<td>Case linked to</td>
<td>Latreen</td>
</tr>
<tr>
<td>Case linked from</td>
<td>Latreen</td>
</tr>
<tr>
<td>Principle Case manager</td>
<td>Neil Armstrong</td>
</tr>
<tr>
<td>Secondary Case manager</td>
<td>None assigned</td>
</tr>
<tr>
<td>Requester</td>
<td>Lucy Campbell</td>
</tr>
</tbody>
</table>

Tasks

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task Created</th>
<th>Task Type</th>
<th>Status</th>
<th>Principle Forensic Investigator</th>
<th>Secondary Forensic Investigator</th>
<th>Principle QA Investigator</th>
<th>Secondary QA Investigator</th>
</tr>
</thead>
<tbody>
<tr>
<td>L-Kemp_03</td>
<td>10 Jun 2014 22:03:59</td>
<td>User Browser History</td>
<td>Queued</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>L-Kemp_01</td>
<td>10 Jun 2014 22:03:59</td>
<td>Chat Room Search</td>
<td>Complete</td>
<td>Pixel F Lowman</td>
<td>None</td>
<td>None</td>
<td>Sarah Holmes</td>
</tr>
</tbody>
</table>

Evidence

Add Evidence

1. SCH-20140228-HDD_004
2. SCH-20140228-HDD_005
L - Kemp: Task L - Kemp_02-2

Task Description

Please investigate the users with log ids: LOMASSNM, GGHDDE & SGLDCPPL. I require:

* All their instant messages between the dates of 15th March 2013 and 18th April 2014
* Instant messages between the three custodians with the keywords "Laurent" OR "Gbagbo"

Case Details

<table>
<thead>
<tr>
<th>Case</th>
<th>L - Kemp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Created</td>
<td>10 Jun 2014 22:03:40</td>
</tr>
<tr>
<td>Case Status</td>
<td>Open</td>
</tr>
<tr>
<td>Principle Case Manager</td>
<td>Neil Armstrong</td>
</tr>
<tr>
<td>Secondary Case Manager</td>
<td>None assigned</td>
</tr>
<tr>
<td>Requester</td>
<td>Lucy Campbell</td>
</tr>
</tbody>
</table>

Task Details

| Task Created | 10 Jun 2014 22:03:59 |
| Task Status | Forensics in Process |
| Task Type | Communications Retrieval > Instant Messenger Search |
| Task Files Location | C:Users/SarahProgramming/Foreman |
| Principle Forensic Investigator | Nybble Lowman |
| Principle QA Investigator | Pied F Lowman |
| Secondary QA Investigator | Sarah Holmes |

Notes

Date & Time | Author | Hash of note |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>14 Jun 2014 11:58:48</td>
<td>Nybble Lowman</td>
<td>4014574fa12bc4c54a30e9b6bea8f878cabb9d7d570172c191f820ef7159b0</td>
</tr>
</tbody>
</table>

Started the investigation by going through all the documentation given.

OMASSNM
Instant message to OR from user id OMASSNM
Date start: 15/03/2013
Date end: 18/04/2014

GGHDDE
Instant message to OR from user id GGHDDE
Instant message from all
Date start: 15/03/2013
Work on L - Kemp: Task L - Kemp_02-2

Request QA

To Pixel F Lowman

Message Subject QA for L-Kemp_02_02

Message body

Hi,
Completed the searches and notes updated. Can you check my results please?
Thanks!

Submit
Work on L - Kemp: Task L - Kemp_02-2

Case Notes

Export the notes to PDF, RTF, and spreadsheet.

14 Jun 2014

Date & Time: 21 Jun 2014 11:48:14  Author: Nybble Lowman

Results downloaded and are ready for delivery.

Hash of note: a98f0398144beb720e22311a359b311bcc4f395afec34eacc436c4c9be4882dd

Update Case Notes

Notes
Evidence SCH-20140228-HDD_004

Details

<table>
<thead>
<tr>
<th>Case</th>
<th>L - Kemp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Evidence Added</td>
<td>2014-06-10 22:03:59.174000</td>
</tr>
<tr>
<td>Evidence Type</td>
<td>USB Hard Drive</td>
</tr>
<tr>
<td>User who added evidence</td>
<td>Stuart Chambers</td>
</tr>
<tr>
<td>Originator</td>
<td>PC McNaddy</td>
</tr>
<tr>
<td>Bag Number</td>
<td>B000196</td>
</tr>
<tr>
<td>Storage Location</td>
<td>Main Evidence Cabinet</td>
</tr>
<tr>
<td>Current status</td>
<td>In storage</td>
</tr>
<tr>
<td>Comments</td>
<td>Hard drive from Joe's main machine</td>
</tr>
</tbody>
</table>

Chain of Custody

<table>
<thead>
<tr>
<th>Record Date</th>
<th>User</th>
<th>Date of Movement</th>
<th>Custodian</th>
<th>Action</th>
<th>Comment</th>
<th>Attachments</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Jun 2014</td>
<td>Stuart Chambers</td>
<td>10 Jun 2014</td>
<td>Sherlock Holmes</td>
<td>Evidence checked in</td>
<td>Initial check in to the storage cabinet</td>
<td></td>
</tr>
<tr>
<td>22:03:59</td>
<td>22:03:59</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Check out the evidence

Photographs
Future Improvements

- Shiny pretty pages
- Requester page
- Reporting
- Customising the reports
- Encryption & digital signatures
- Android / iOS/ Blackberry App for Evidence Tracking
The Future of Foreman

☐ I’d love to see Foreman adopted in universities / teaching world

☐ Community & small forensics companies

☐ Hosted solutions
I need help with...

- Development
- Design improvements
- Testing
- Promotion
Thanks for listening

www.foreman-forensics.org

sarah@lowmanio.co.uk