Efficient Smart Phone Forensics Based on Relevance Feedback

Saksham Varma, Robert J. Walls, Brian Lynn, Brian Neil Levine

Supported in part by the Office of Naval Research (N00244-12-1-0057)
Forensic Triage:

Acquire evidence quickly, accurately, and often on-scene.

> Done before a full examination
Phone Triage

Recovery Engine

DEC0DE

BulkExtractor

Strings

SMS Text Messages

<table>
<thead>
<tr>
<th>Address Book</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert</td>
<td>Walls</td>
<td>443-380-2823</td>
</tr>
<tr>
<td>Erik</td>
<td>Learned-Miller</td>
<td>505-309-3769</td>
</tr>
<tr>
<td>Brian</td>
<td>Levine</td>
<td>718-774-8034</td>
</tr>
<tr>
<td>William</td>
<td>Enck</td>
<td>714-206-4569</td>
</tr>
<tr>
<td>David</td>
<td>Wagner</td>
<td>276-251-8823</td>
</tr>
<tr>
<td>Ian</td>
<td>Goldberg</td>
<td>909-994-6768</td>
</tr>
<tr>
<td>Phone Model</td>
<td>Pages</td>
<td>True Pages</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td>HTC Desire HD</td>
<td>228,860</td>
<td>1,834</td>
</tr>
<tr>
<td>Samsung Galaxy Y</td>
<td>175,873</td>
<td>600</td>
</tr>
<tr>
<td>Motorola XT701</td>
<td>144,618</td>
<td>207</td>
</tr>
<tr>
<td>HTC Evo 4g</td>
<td>78,680</td>
<td>3,178</td>
</tr>
<tr>
<td>Samsung Galaxy Y Duos</td>
<td>60,422</td>
<td>3,612</td>
</tr>
<tr>
<td>HTC Wildfire</td>
<td>55,759</td>
<td>137</td>
</tr>
<tr>
<td>Samsung Galaxy Mini</td>
<td>53,456</td>
<td>1,390</td>
</tr>
<tr>
<td>Sony Xperia x10</td>
<td>30,063</td>
<td>16</td>
</tr>
<tr>
<td>Dell XCD35</td>
<td>20,494</td>
<td>221</td>
</tr>
<tr>
<td>Dell XCD28</td>
<td>17,932</td>
<td>118</td>
</tr>
<tr>
<td>HTC Legend</td>
<td>10,238</td>
<td>19</td>
</tr>
<tr>
<td>Huawei Ideos</td>
<td>8,829</td>
<td>667</td>
</tr>
<tr>
<td>Huawei 8500</td>
<td>6,305</td>
<td>3</td>
</tr>
</tbody>
</table>
Phone Triage

Phone Triage Diagram:

1. Recovery Engine
2. DEC0DE
3. BulkExtractor
4. Strings
5. SMS Text Messages
   - Robert Walls 443-380-2823
   - Erik Learned-Miller 505-309-3769
   - Brian Levine 718-774-8034
   - William Enck 714-206-4569
   - David Wagner 276-251-8823
   - Ian Goldberg 909-994-6768
Phone Triage

Recovery Engine

DEC0DE

BulkExtractor

Strings
Only the investigator can tell us what is important.
# Relevance Feedback

<table>
<thead>
<tr>
<th></th>
<th>Phone Number</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brian</td>
<td>(413) 555-0123</td>
<td>08/05/14 1:00 PM</td>
</tr>
<tr>
<td>Yuriy B.</td>
<td>(413) 555-7823</td>
<td>08/05/14 10:02 AM</td>
</tr>
<tr>
<td>samsung Xkdjfi</td>
<td>(214) 322-9888</td>
<td>01/23/04 4:00 AM</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>1 (800) 555-5555</td>
<td></td>
</tr>
</tbody>
</table>
Liftr: prioritizing information recovered from phones

Liftr

Initial Ranking

ranked pages

Relevance Feedback

Ranked Results

Recovery Engine

DEC0DE

BulkExtractor

Strings

rjwalls@cse.psu.edu

forensics.umass.edu
Liftr: Initial Sorting

1. Group fields by NAND page

2. Score each field using combination of features:
   A. Text quality
   B. a priori
   C. Filename (guess)

3. Score page using weighted sum of field scores

4. Rank by page scores
Liftr: Feedback Stage

1. Select a page
2. Investigator labels relevant fields
3. Update scores for other pages
4. Repeat
Page Feedback

• Fields split into tokens by whitespace and punctuation

• Fields with shared tokens have score increased using the Inverse Document Frequency

• Blacklist tokens:
  A. Common words
  B. Android keywords
  C. Previously marked tokens

• Each token is only scored once
Liftr: Evaluation

• Obtained physical images from 13 previously owned Android phones
• Focused on names, phone numbers, and email addresses
• Input from different recovery engines:
  1. Strings
  2. Bulk Extractor
  3. DEC0DE
<table>
<thead>
<tr>
<th>Device</th>
<th>Pages</th>
<th>True Pages</th>
<th>Fields</th>
<th>True Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTC Desire HD</td>
<td>228,860</td>
<td>1,834</td>
<td>6,247,115</td>
<td>12,275</td>
</tr>
<tr>
<td>Samsung Galaxy Y</td>
<td>175,873</td>
<td>600</td>
<td>4,594,060</td>
<td>2,954</td>
</tr>
<tr>
<td>Motorola XT701</td>
<td>144,618</td>
<td>207</td>
<td>3,049,543</td>
<td>869</td>
</tr>
<tr>
<td>HTC Evo 4g</td>
<td>78,680</td>
<td>3,178</td>
<td>1,853,638</td>
<td>22,850</td>
</tr>
<tr>
<td>Samsung Galaxy Y Duos</td>
<td>60,422</td>
<td>3,612</td>
<td>1,530,630</td>
<td>21,399</td>
</tr>
<tr>
<td>HTC Wildfire</td>
<td>55,759</td>
<td>137</td>
<td>1,019,033</td>
<td>837</td>
</tr>
<tr>
<td>Samsung Galaxy Mini</td>
<td>53,456</td>
<td>1,390</td>
<td>1,329,715</td>
<td>4,031</td>
</tr>
<tr>
<td>Sony Xperia x10</td>
<td>30,063</td>
<td>16</td>
<td>855,464</td>
<td>154</td>
</tr>
<tr>
<td>Dell XCD35</td>
<td>20,494</td>
<td>221</td>
<td>594,469</td>
<td>1,621</td>
</tr>
<tr>
<td>Dell XCD28</td>
<td>17,932</td>
<td>118</td>
<td>495,099</td>
<td>841</td>
</tr>
<tr>
<td>HTC Legend</td>
<td>10,238</td>
<td>19</td>
<td>198,873</td>
<td>121</td>
</tr>
<tr>
<td>Huawei Ideos</td>
<td>8,829</td>
<td>667</td>
<td>170,143</td>
<td>6,799</td>
</tr>
<tr>
<td>Huawei 8500</td>
<td>6,305</td>
<td>3</td>
<td>116,524</td>
<td>41</td>
</tr>
<tr>
<td>DEC0DE</td>
<td>Bulk Extractor</td>
<td>Strings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pages</td>
<td>True Pages</td>
<td>Fields</td>
<td>True Fields</td>
<td>Pages</td>
</tr>
<tr>
<td>228,860</td>
<td>1,834</td>
<td>6,247,115</td>
<td>12,275</td>
<td>518</td>
</tr>
<tr>
<td>175,873</td>
<td>600</td>
<td>4,594,060</td>
<td>2,954</td>
<td>263</td>
</tr>
<tr>
<td>144,618</td>
<td>207</td>
<td>3,049,543</td>
<td>869</td>
<td>118</td>
</tr>
<tr>
<td>78,680</td>
<td>3,178</td>
<td>1,853,638</td>
<td>22,850</td>
<td>2,689</td>
</tr>
<tr>
<td>60,422</td>
<td>3,612</td>
<td>1,530,630</td>
<td>21,399</td>
<td>2,150</td>
</tr>
<tr>
<td>55,759</td>
<td>137</td>
<td>1,019,033</td>
<td>837</td>
<td>118</td>
</tr>
<tr>
<td>53,456</td>
<td>1,390</td>
<td>1,329,715</td>
<td>4,031</td>
<td>1,329</td>
</tr>
<tr>
<td>30,063</td>
<td>16</td>
<td>855,464</td>
<td>154</td>
<td>20</td>
</tr>
<tr>
<td>20,494</td>
<td>221</td>
<td>594,469</td>
<td>1,621</td>
<td>90</td>
</tr>
<tr>
<td>17,932</td>
<td>118</td>
<td>495,099</td>
<td>841</td>
<td>27</td>
</tr>
<tr>
<td>10,238</td>
<td>19</td>
<td>198,873</td>
<td>121</td>
<td>26</td>
</tr>
<tr>
<td>8,829</td>
<td>667</td>
<td>170,143</td>
<td>6,799</td>
<td>81</td>
</tr>
<tr>
<td>6,305</td>
<td>3</td>
<td>116,524</td>
<td>41</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DECODE</strong></td>
<td></td>
<td><strong>Bulk Extractor</strong></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------</td>
<td>----------------------</td>
<td>--------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>Pages</td>
<td>True Pages</td>
<td>Fields</td>
<td>True Fields</td>
</tr>
<tr>
<td>HTC Desire HD</td>
<td>228,860</td>
<td>1,834</td>
<td>6,247,115</td>
<td>12,275</td>
</tr>
<tr>
<td>Samsung Galaxy Y</td>
<td>175,873</td>
<td>600</td>
<td>4,594,060</td>
<td>2,954</td>
</tr>
<tr>
<td>Motorola XT701</td>
<td>144,618</td>
<td>207</td>
<td>3,049,543</td>
<td>869</td>
</tr>
<tr>
<td>HTC Evo 4g</td>
<td>78,680</td>
<td>3,178</td>
<td>1,853,638</td>
<td>22,850</td>
</tr>
<tr>
<td>Samsung Galaxy Y Duos</td>
<td>60,422</td>
<td>3,612</td>
<td>1,530,630</td>
<td>21,399</td>
</tr>
<tr>
<td>HTC Wildfire</td>
<td>55,759</td>
<td>137</td>
<td>1,019,033</td>
<td>837</td>
</tr>
<tr>
<td>Samsung Galaxy Mini</td>
<td>53,456</td>
<td>1,390</td>
<td>1,329,715</td>
<td>4,031</td>
</tr>
<tr>
<td>Sony Xperia x10</td>
<td>30,063</td>
<td>16</td>
<td>855,464</td>
<td>154</td>
</tr>
<tr>
<td>Dell XCD35</td>
<td>20,494</td>
<td>221</td>
<td>594,469</td>
<td>1,621</td>
</tr>
<tr>
<td>Dell XCD28</td>
<td>17,932</td>
<td>118</td>
<td>495,099</td>
<td>841</td>
</tr>
<tr>
<td>HTC Legend</td>
<td>10,238</td>
<td>19</td>
<td>198,873</td>
<td>121</td>
</tr>
<tr>
<td>Huawei Ieodos</td>
<td>8,829</td>
<td>667</td>
<td>170,143</td>
<td>6,799</td>
</tr>
<tr>
<td>Huawei 8500</td>
<td>6,305</td>
<td>3</td>
<td>116,524</td>
<td>41</td>
</tr>
<tr>
<td>Device</td>
<td>DECODE</td>
<td>Bulk Extractor</td>
<td>Strings</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pages</td>
<td>True</td>
<td>Fields</td>
<td>True</td>
</tr>
<tr>
<td>HTC Desire HD</td>
<td>228,860</td>
<td>1,834</td>
<td>6,247,115</td>
<td>12,275</td>
</tr>
<tr>
<td>Samsung Galaxy Y</td>
<td>175,873</td>
<td>600</td>
<td>4,594,060</td>
<td>2,954</td>
</tr>
<tr>
<td>Motorola XT701</td>
<td>144,618</td>
<td>207</td>
<td>3,049,543</td>
<td>869</td>
</tr>
<tr>
<td>HTC Evo 4g</td>
<td>78,680</td>
<td>3,178</td>
<td>1,853,638</td>
<td>22,850</td>
</tr>
<tr>
<td>Samsung Galaxy Y Duos</td>
<td>60,422</td>
<td>3,612</td>
<td>1,530,630</td>
<td>21,399</td>
</tr>
<tr>
<td>HTC Wildfire</td>
<td>55,759</td>
<td>137</td>
<td>1,019,033</td>
<td>837</td>
</tr>
<tr>
<td>Samsung Galaxy Mini</td>
<td>53,456</td>
<td>1,390</td>
<td>1,329,715</td>
<td>4,031</td>
</tr>
<tr>
<td>Sony Xperia x10</td>
<td>30,063</td>
<td>16</td>
<td>855,464</td>
<td>154</td>
</tr>
<tr>
<td>Dell XCD35</td>
<td>20,494</td>
<td>221</td>
<td>594,469</td>
<td>1,621</td>
</tr>
<tr>
<td>Dell XCD28</td>
<td>17,932</td>
<td>118</td>
<td>495,099</td>
<td>841</td>
</tr>
<tr>
<td>HTC Legend</td>
<td>10,238</td>
<td>19</td>
<td>198,873</td>
<td>121</td>
</tr>
<tr>
<td>Huawei Iideos</td>
<td>8,829</td>
<td>667</td>
<td>170,143</td>
<td>6,799</td>
</tr>
<tr>
<td>Huawei 8500</td>
<td>6,305</td>
<td>3</td>
<td>116,524</td>
<td>41</td>
</tr>
</tbody>
</table>

**Relevant (True) Page:** Contains at least one relevant field
Evaluation

- Ground truth from contacts and SMS databases
- Two combinations of initial ranking features
  1. *a priori*: 5 random ground truth tokens
  2. Filesystem labeling: only possible for some phones
- Measured ranking quality of top $k$ pages using *normalized discounted cumulative gain* (NDCG)
- Considered up to 20 rounds of feedback
Evaluation: Ranking

![Graph showing evaluation results for Decode, a priori and Decode, FS labeling. The x-axis represents the number of pages labeled, and the y-axis shows the average normalized discounted cumulative gain. The graph includes lines for different cutoff values (20, 50, 1000).]
Evaluation: Ranking

![Graph showing the comparison between Decode, a priori and Decode, FS labeling methods in terms of Avg. Norm. Discounted Cumulative Gain. The x-axis represents the number of pages labeled, ranging from Initial to 20, and the y-axis represents the average normalized discounted cumulative gain. The graph compares the performance at different cutoff points: 20, 50, and 1000. The graph illustrates how the performance improves as more pages are labeled.]
Evaluation: Ranking

![Graph showing cumulative gain for Decode, a priori and Decode, FS labeling]
Evaluation: Ranking

Average Normalized Discounted Cumulative Gain vs. Number of Pages Labeled

- Decode, a priori
- Decode, FS labeling

Cutoffs: 20, 50, 1000
DEC0DE with a priori input (k=1000)
Evaluation

- Initial ranking gives NDCG of 0.73 for all engines (k=50)
- Top ranking better than end ranking
- FS info not as useful as expected
- Feedback leads to sharp score increase
- Positive examples help more than negative examples
- Evaluation takeaway:
  1. We need both components
  2. We don’t have to ask many questions
Evaluation: Work

- Investigator time spent per page:
  - Only label relevant fields
  - 5 seconds per relevant field
  - On average 7 per page
  - ~11 minutes to complete 20 pages
- Label by page to speed up the process?
Evaluation: Work

Too many false positives per page for page-level marking to work.
Open Questions

- What is the best:
  - presentation order?
  - field grouping?
  - field features?
- How do we best apply these techniques to other sources?
- How do we correlate information across different devices?
Summary

- Liftr addresses an important limitation of current techniques: only a fraction of results are relevant to an investigation.
- Liftr uses investigator feedback to quickly pinpoint relevant information.
- We tested LIFTR with three different recovery engines on 13 pre-owned Android phones.
- Feedback on as few 20 NAND pages is more than sufficient to identify the top 100 most relevant pages out of the hundreds of thousands of recovery results.
A small amount of investigator feedback goes a long way toward improving triage results.
Efficient Smart Phone Forensics Based on Relevance Feedback

Robert J. Walls
rjwalls@cse.psu.edu
http://www.cse.psu.edu/~rjwalls/
http://forensics.umass.edu

Supported in part by the Office of Naval Research (N00244-12-1-0057)
Writes at page level
Deletes at block level