Digital Dumpster Diving
an investigative analysis
So who uses a mobile device?
The real ?? is who does not.
device?
Worldwide population using mobile phones
Not using mobile phones
Probability of a Breach involving MD

• 1/3 of Data Breach
  • 52% data loss involved mobile device theft
  • 21% of breaches in healthcare involving MD affected 51.8% of all records (~2)
  • ~7% likely if a data breach occurs a MD is involved

• Costs
  • ~200-300 per record
  • iOS 64 gb (~62 Gb can be used)
    • ave 65K per doc 9 pg ave = 15,385 / 1Gb * 62 = ~954,000 docs (records) possible
    • Even say 1% are records = $2,862,000 USD
This is our TARGET RIGHT
Selection of solution based on the lowest level of effort

Set of possible solutions to fulfill the need

Defines

User Need

Limits

User Knowledge
Operation: Digital Dumpster Diving
Androids (userdata Partition)
Sanyo 2300
Motorola V3
WYSIWYG

- JPGs, PDFs, DOC
- Email, IM, Applications
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>From</th>
<th>To</th>
<th>Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Well it said on my phone that ur did</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Are u there abby</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Yeah sorry</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Hangin with Seebde</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Oh oh ur ru doing</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Hey firey</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Makin smoothies</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Whoa</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Hey!!!</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Nathan really watchin tv</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Wait ur done</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Nice</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Hiafafa ya u gives</td>
</tr>
<tr>
<td>9/3/2011</td>
<td>12:00</td>
<td>at</td>
<td>+12084517469</td>
<td>+12084517469</td>
<td>Makin a smoothie and watchin tv</td>
</tr>
</tbody>
</table>
Forensic Examination

Deep Dive

- Unallocated
  - Media Types
- SQL Parser
  - iOS/Android
  - SMS
- Browser
Final Statement
SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.
Proof of Concept
Let me know your new number?

For SURE!
Glad you like it!
FULL DOUBLE RAINBOW

WHAT DOES IT MEAN?
We are the frontline, We are the pioneers, We ARE FORENSICATORS.