RAM Forensics against Cyber Crimes Involving Files

Mohammed I. Al-Saleh and Ziad A. Al-Sharif

Jordan University of Science and Technology
Outline

• Background and Problem
• Investigation Model
• Experiments
• Results
• Conclusions
Background and Problem

• The Internet
  – An essential part of people’s daily lives
  – Communication, business, education, research, and social networks

• However, people with malicious intention misuse it.
  – Stealing information, eavesdropping, spamming, phishing, impersonation, etc.
Background and Problem

• Digital Forensics
  – Extract digital crime evidences
  – Inspect networks, hard drive, flash memory, and RAM.

• Among others, inspecting the RAM is very appealing
  – All operations need to go through the RAM
Background and Problem

• Many Internet operations explicitly or implicitly involve files
  – Ex., opening a website implicitly involves saving different files into the machine.

• Those files might stick in the RAM (called artifacts)

• Forensics analysts are interested in such artifacts
  – More specifically, this research is all about the the artifacts of files in the RAM.
Problem and Background

• Searching for files in the RAM
  – Need to know
    • How files are mapped into the RAM!
Paging

Virtual address space

60K–64K  X
56K–60K  X
52K–56K  X
48K–52K  X
44K–48K  7
40K–44K  X
36K–40K  5
32K–36K  X
28K–32K  X
24K–28K  X
20K–24K  3
16K–20K  4
12K–16K  0
8K–12K   6
4K–8K    1
0K–4K    2

Virtual page

Physical memory address

28K–32K
24K–28K
20K–24K
16K–20K
12K–16K
8K–12K
4K–8K
0K–4K

Page frame
File Page Alignment Possibilities in the RAM

a- File page is aligned to RAM page

b- File page is spanned to next RAM page

1 2

1 2

c- File page is spanned to arbitrary RAM page
File Page Alignment Possibilities in the RAM

First Choice

a- File page is aligned to RAM page

b- File page is spanned to next RAM page

c- File page is spanned to arbitrary RAM page
Investigation Model

- RAM Pages
  - File Portion 1
  - File Portion 2
  - File Portion 3

- Criminal/Violator
- File Location
- Investigator

Directly downloaded
Viewed in browser
Downloaded via BitTorrent
Copied from external storage

Get File

Activities
Experiments

Ubuntu 10.04/Windows 7

*Downloading a file*
*Viewing a file in Firefox and IE*
*Downloading a file using BitTorrent*
*Copying a file from a flash memory*
*Viewing a pic using a pic viewer*

512 MB RAM

Host/Fedora 16, Intel(R) Core(TM) i5 CPU, 8 GB RAM
## Results

### Copy from flash memory

<table>
<thead>
<tr>
<th></th>
<th>Linux</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Pages</td>
<td>118</td>
<td>118</td>
</tr>
<tr>
<td>Found Pages</td>
<td>118</td>
<td>118</td>
</tr>
<tr>
<td>Not Found Pages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Avg Search Time (Sec)</td>
<td>11.83</td>
<td>7.94</td>
</tr>
<tr>
<td>Avg Time Per Page (Sec)</td>
<td>0.10</td>
<td>0.07</td>
</tr>
</tbody>
</table>

### Download from the Internet

<table>
<thead>
<tr>
<th></th>
<th>Linux</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Pages</td>
<td>118</td>
<td>118</td>
</tr>
<tr>
<td>Found Pages</td>
<td>118</td>
<td>118</td>
</tr>
<tr>
<td>Not Found Pages</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Avg Search Time (Sec)</td>
<td>13.31</td>
<td>12.30</td>
</tr>
<tr>
<td>Avg Time Per Page (Sec)</td>
<td>0.11</td>
<td>0.10</td>
</tr>
</tbody>
</table>
## Results

### View a Pic in a Browser

<table>
<thead>
<tr>
<th></th>
<th>Linux</th>
<th>Windows</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Pages</td>
<td>186</td>
<td>186</td>
<td></td>
</tr>
<tr>
<td>Found Pages</td>
<td>185</td>
<td>185</td>
<td></td>
</tr>
<tr>
<td>Not Found Pages</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Avg Search Time (Sec)</td>
<td>14.97</td>
<td>15.04</td>
<td></td>
</tr>
<tr>
<td>Avg Time Per Page (Sec)</td>
<td>0.08</td>
<td>0.08</td>
<td></td>
</tr>
</tbody>
</table>

### Download a File with Torrent

<table>
<thead>
<tr>
<th></th>
<th>Before Delete</th>
<th>After Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Pages</td>
<td>429</td>
<td>429</td>
</tr>
<tr>
<td>Found Pages</td>
<td>341</td>
<td>7</td>
</tr>
<tr>
<td>Not Found Pages</td>
<td>88</td>
<td>422</td>
</tr>
<tr>
<td>Avg Search Time (Sec)</td>
<td>36.65</td>
<td>87.01</td>
</tr>
<tr>
<td>Avg Time Per Page (Sec)</td>
<td>0.09</td>
<td>0.20</td>
</tr>
</tbody>
</table>
Results

Open a Picture with a Viewer

<table>
<thead>
<tr>
<th></th>
<th>Search for a Page in a Paged RAM</th>
<th>Search for a Page in a Flat RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Pages</td>
<td>66</td>
<td>66</td>
</tr>
<tr>
<td>Found Pages</td>
<td>0</td>
<td>63</td>
</tr>
<tr>
<td>Not Found Pages</td>
<td>66</td>
<td>3</td>
</tr>
<tr>
<td>Avg Search Time (Sec)</td>
<td>12.77</td>
<td>66.84</td>
</tr>
<tr>
<td>Avg Time Per Page (Sec)</td>
<td>0.19</td>
<td>1.01</td>
</tr>
</tbody>
</table>
Conclusion

• Many criminal activities might be thought of as if they explicitly or implicitly involve files
• Files are mapped in page granularity by the OS to the RAM page frames
• Searching for such files is reduced to searching for the file pages in the RAM frames
• Such search is effective and efficient
Acknowledgements

• Jordan University of Science and Technology for the financial support
Thanks