The State of the Art in Windows Memory Forensics
Introduction
System state is kept in memory

- Processes
- Sockets
- TCP connections
- System functions
- ...
Relevant data is not on disk

Dolan-Gavitt (2008):

- Registry consists of several files (hives).
- Hives (partially) loaded into memory.
- Direct changes to in-memory registry (by-passing the API) not mirrored back to disk.
Key recovery

Kornblum (2008): Bitlocker key material

<table>
<thead>
<tr>
<th>Offset</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>1EE5E000</td>
<td>00</td>
<td>00</td>
<td>07</td>
<td>A4</td>
<td>04</td>
<td>46</td>
<td>56</td>
<td>45</td>
<td>63</td>
<td>2C</td>
<td>FE</td>
<td>D8</td>
<td>83</td>
<td>E0</td>
<td>FE</td>
<td>D8</td>
</tr>
<tr>
<td>1EE5E010</td>
<td>20</td>
<td>E0</td>
<td>E5</td>
<td>82</td>
<td>B0</td>
<td>03</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>1EE5E020</td>
<td>20</td>
<td>04</td>
<td>01</td>
<td>68</td>
<td>02</td>
<td>D5</td>
<td>44</td>
<td>41</td>
<td>AB</td>
<td>E0</td>
<td>AA</td>
<td>47</td>
<td>5B</td>
<td>12</td>
<td>00</td>
<td>63</td>
</tr>
<tr>
<td>1EE5E030</td>
<td>E7</td>
<td>F7</td>
<td>E7</td>
<td>51</td>
<td>EA</td>
<td>AA</td>
<td>AA</td>
<td>A3</td>
<td>1A</td>
<td>50</td>
<td>6A</td>
<td>A2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1EE5E040</td>
<td>B9</td>
<td>0D</td>
<td>D0</td>
<td>F3</td>
<td>53</td>
<td>D7</td>
<td>7E</td>
<td>EE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1EE5E050</td>
<td>1B</td>
<td>0A</td>
<td>8A</td>
<td>C3</td>
<td>48</td>
<td>8E</td>
<td>E4</td>
<td>26</td>
<td>52</td>
<td>5E</td>
<td>8E</td>
<td>82</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1EE5E060</td>
<td>4B</td>
<td>BA</td>
<td>89</td>
<td>C3</td>
<td>03</td>
<td>CE</td>
<td>6D</td>
<td>E3</td>
<td>59</td>
<td>55</td>
<td>FE</td>
<td>77</td>
<td>0B</td>
<td>0B</td>
<td>70</td>
<td>F5</td>
</tr>
<tr>
<td>1EE5E070</td>
<td>70</td>
<td>91</td>
<td>5F</td>
<td>E8</td>
<td>73</td>
<td>5F</td>
<td>02</td>
<td>0B</td>
<td>2A</td>
<td>0A</td>
<td>FC</td>
<td>7C</td>
<td>21</td>
<td>01</td>
<td>6C</td>
<td>09</td>
</tr>
<tr>
<td>1EE5E080</td>
<td>2C</td>
<td>F5</td>
<td>C3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1EE5E090</td>
<td>5E</td>
<td>01</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1EE5E0A0</td>
<td>72</td>
<td>84</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1EE5E0B0</td>
<td>70</td>
<td>52</td>
<td>37</td>
<td>4E</td>
<td>03</td>
<td>7D</td>
<td>C7</td>
<td>E7</td>
<td>04</td>
<td>59</td>
<td>EA</td>
<td>07</td>
<td>23</td>
<td>D7</td>
<td>A0</td>
<td>45</td>
</tr>
<tr>
<td>1EE5E0C0</td>
<td>48</td>
<td>B2</td>
<td>59</td>
<td>68</td>
<td>4B</td>
<td>CF</td>
<td>9E</td>
<td>0F</td>
<td>4F</td>
<td>96</td>
<td>74</td>
<td>88</td>
<td>6C</td>
<td>41</td>
<td>1D</td>
<td>CD</td>
</tr>
<tr>
<td>1EE5E0D0</td>
<td>86</td>
<td>5D</td>
<td>77</td>
<td>F7</td>
<td>5A</td>
<td>D4</td>
<td>22</td>
<td>F2</td>
<td>6C</td>
<td>00</td>
<td>F9</td>
<td>25</td>
<td>73</td>
<td>DE</td>
<td>D2</td>
<td>EE</td>
</tr>
<tr>
<td>1EE5E0E0</td>
<td>00</td>
<td>03</td>
<td>B7</td>
<td>5B</td>
<td>DC</td>
<td>89</td>
<td>55</td>
<td>05</td>
<td>36</td>
<td>D4</td>
<td>DB</td>
<td>73</td>
<td>1F</td>
<td>DE</td>
<td>2B</td>
<td>4B</td>
</tr>
<tr>
<td>1EE5E0F0</td>
<td>22</td>
<td>B2</td>
<td>CB</td>
<td>16</td>
<td>DC</td>
<td>0B</td>
<td>E2</td>
<td>5E</td>
<td>EA</td>
<td>5D</td>
<td>8E</td>
<td>C2</td>
<td>29</td>
<td>0A</td>
<td>F0</td>
<td>9C</td>
</tr>
<tr>
<td>1EE5E100</td>
<td>1C</td>
<td>03</td>
<td>F0</td>
<td>EE</td>
<td>FE</td>
<td>BE</td>
<td>29</td>
<td>40</td>
<td>36</td>
<td>57</td>
<td>6C</td>
<td>8C</td>
<td>C3</td>
<td>57</td>
<td>7E</td>
<td>4E</td>
</tr>
<tr>
<td>1EE5E110</td>
<td>AE</td>
<td>92</td>
<td>7D</td>
<td>E7</td>
<td>4B</td>
<td>D0</td>
<td>9A</td>
<td>A6</td>
<td>C8</td>
<td>E9</td>
<td>45</td>
<td>C4</td>
<td>F5</td>
<td>00</td>
<td>12</td>
<td>C2</td>
</tr>
<tr>
<td>1EE5E120</td>
<td>F0</td>
<td>CD</td>
<td>AB</td>
<td>57</td>
<td>4C</td>
<td>4A</td>
<td>A4</td>
<td>E1</td>
<td>2A</td>
<td>51</td>
<td>9C</td>
<td>62</td>
<td>3D</td>
<td>E9</td>
<td>57</td>
<td>06</td>
</tr>
<tr>
<td>1EE5E130</td>
<td>99</td>
<td>1B</td>
<td>35</td>
<td>2F</td>
<td>BC</td>
<td>87</td>
<td>0F</td>
<td>B6</td>
<td>66</td>
<td>1B</td>
<td>38</td>
<td>83</td>
<td>17</td>
<td>E8</td>
<td>CB</td>
<td>64</td>
</tr>
<tr>
<td>1EE5E140</td>
<td>5A</td>
<td>D3</td>
<td>F1</td>
<td>92</td>
<td>25</td>
<td>9F</td>
<td>3A</td>
<td>99</td>
<td>DA</td>
<td>9C</td>
<td>37</td>
<td>35</td>
<td>71</td>
<td>A3</td>
<td>F3</td>
<td>E7</td>
</tr>
<tr>
<td>1EE5E150</td>
<td>D5</td>
<td>DE</td>
<td>9E</td>
<td>B2</td>
<td>7F</td>
<td>4C</td>
<td>CB</td>
<td>0B</td>
<td>FF</td>
<td>03</td>
<td>0D</td>
<td>AC</td>
<td>3F</td>
<td>C4</td>
<td>D2</td>
<td></td>
</tr>
<tr>
<td>1EE5E160</td>
<td>20</td>
<td>84</td>
<td>01</td>
<td>68</td>
<td>02</td>
<td>D5</td>
<td>44</td>
<td>41</td>
<td>AB</td>
<td>E8</td>
<td>AA</td>
<td>47</td>
<td>5B</td>
<td>12</td>
<td>63</td>
<td>FS</td>
</tr>
</tbody>
</table>
Forensic process

The same process applies to traditional and memory forensics:

1. Acquisition
2. Analysis
3. Presentation
Acquisition
Memory is volatile

- Do NOT pull the plug:
  Without power and clocking, memory contents dissipates within seconds to minutes.
- Examination of the system’s state changes the system’s state.
- Do it right the first time!
Find the right tool

• Several tools and techniques available
• Taxonomy:
  1. Access to main memory
     pure hardware vs. software
  2. Time of installation
     prior to incident vs. post incident
  3. Required privileges
     user vs. administrator
Find the right tool

• Taxonomy (cont.):
  4. Impact on system
     in vivo vs. post mortem
  5. Atomicity of image
  6. Image file format
     raw (“dd-style”) vs. Microsoft crash dump
     not important any longer

• Test it thoroughly!
Select tool: VMware

- Popular virtual machine monitor.
- Simulated “physical memory” can be stored in a file.
- Excellent lab environment, though malware is aware of virtualization techniques.
Select tool: FireWire

- Physical access and IEEE
- Hard though not impossible to counterfeit.
Select tool: KnTTools

- by GMG Systems, Inc. (George Garner)
- Also obtains for later analysis
  - kernel and network driver binaries
  - system status as seen from userland
- Enterprise edition:
  - signed/encrypted jobs and evidence
  - pre-installed or on-demand
Some free tools

- **mdd**
  by Benjamin Stotts, Mantech
  [https://sourceforge.net/projects/mdd/](https://sourceforge.net/projects/mdd/)

- **win32dd**
  by Matthieu Suiche
Analysis
Select tool: KnTList

- by GMG Systems, Inc. (George Garner)
- Extensive output, plain text and XML
- Analyses file cache
- Cross-view examination eases rootkit detection.
Select tool: PoolTools

- by Andreas Schuster
  http://computer.forensikblog.de/files/poolfinder/
- Open source software.
- Generic kernel object carver and utility programs.
- About 40,000 to 80,000 objects per memory dump (depends on system usage).
Select tool: Volatility

- by Volatile Systems
  https://www.volatilesystems.com/default/volatility
- Open source software.
- Supports all major memory image formats.
- Many object viewers.
- Programming framework, pure Python.
Select tool: PyFlag

- by Michael Cohen and David Collett
  [http://www.pyflag.net/](http://www.pyflag.net/)
- Open source software.
- Web-based analysis software:
  - file systems
  - network captures
  - memory images (using Volatility)
- Generates report (“brief of evidence”).
The future: Correlation

• Case et al., 2008

• Automatic correlation of evidence from disk, network, and RAM.

• Proof of concept, Linux.
Conclusion
Conclusion

• Most tools are in a proof-of-concept phase and target a technical audience.
• Memory analysis produces a lot of extra data.
• Integration into forensics process:
  – front-end: pyFlag, EnCase Enterprise, etc.
  – correlation, e.g. FACE
Questions?
Thank you for your attention!

Andreas Schuster
a.schuster@yendor.net
http://computer.forensikblog.de/en/
Acquisition tool taxonomy
Access to main memory

**Software**
- Employs CPU, memory, kernel and drivers.
- Can easily be fooled.
- Easy to deploy and maintain in a corporate environment.
- Costs mainly driven by license.

**Pure Hardware**
- Does not utilize the CPU.
- Trusted access to memory?
- May require extra hardware
- Installation requires significant time (more costs).
Time of installation

Prior to incident
- Usually requires a reboot.
- Does not tamper with evidence.
- Permanently adds (privileged) code to system, increases exposure to attacks.

Post incident
- Installation possible after the incident occurred.
- Could interfere with evidence.
- “Installed” only as long as needed.
Required privileges

Unprivileged
• No (secondary) logon required.
• Minimizes impact on evidence.

Privileged
• Requires either installation prior to incident or (secondary) logon.
• High impact on evidence in case of a (secondary) logon.
Atomicity of image

**Low**
- Inconsistent state; may confuse tools and examiners (e.g. dangling pointers).
- Significant problem for analysis of user data.
- Less impact on analysis of kernel data.

**High**
- Consistent state over whole image.
- Difficult to achieve.
Impact on system

**Low**
- System continues to work.
- Degraded performance during imaging, reverts to normal afterwards.
- Should be safe even on servers.

**High**
- System forced to crash.
- System out of service for time required to obtain the dump and reboot.
- Acceptable only for clients. Generally best choice under lab conditions.
References
References

