An Evaluation Platform for Forensic Memory Acquisition Software

By

Stefan Voemel and Johannes Stuttgen

Presented At

The Digital Forensic Research Conference

DFRWS 2013 USA Monterey, CA (Aug 4th - 7th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http://dfrws.org
Research in memory forensics has mostly focused on analysis-related aspects to date.

The respective base snapshot is frequently assumed to be „sound“ or „reliable“.

But what factors actually affect its „soundness“?

- Once determined, how can we measure those factors?
- To what degree do current acquisition approaches satisfy those factors?
- In this talk: Methods for evaluating software-based imaging solutions.
Acquisition Criteria

Criteria for “Sound” Memory Imaging

- Several criteria have been early identified by different authors
  - Works are mostly descriptive though and primarily illustrate weaknesses of existing technologies
  - More formal definition by Vömel and Freiling (2012)
- Theory: The quality of a forensic memory snapshot is determined by its degree of correctness, atomicity, and integrity
Acquisition Criteria

- Correctness

**Definition 1.** A snapshot is correct with respect to a set of memory regions $R \subseteq \mathcal{R}$ if for all these regions, the value that is captured in the snapshot matches the value that is stored in this region at this specific point of time.

- correctness basically means that the snapshot only contains “true” values
- trivial but necessary requirement
  - for instance, malicious software may try to impede or manipulate the acquisition process
  - errors in imaging applications may lead to incorrect acquisition results
**Acquisition Criteria**

- **Atomicity**

**Definition 2.** A snapshot is atomic with respect to $R$ if the cut through the corresponding space-time diagram is consistent.

Inconsistencies may occur due to concurrent activity.
Acquisition Criteria

- **Integrity**

**Definition 3.** Let $R \subseteq \mathcal{R}$ be a set of memory regions and $\tau \in \mathcal{T}$ be a point in time. A snapshot $s$ satisfies integrity with respect to $R$ and $\tau$ if the values of the respective memory regions that are retrieved and written out by an acquisition algorithm have not been modified after $\tau$.

![Diagram showing memory regions and time points](image)
Evaluation Methodology

- We have developed an evaluation platform to determine the degree of correctness, atomicity, and integrity for Windows-based software imagers.

- Platform is based on a heavily customized version of the Bochs x86 PC emulator.

- White-box testing methodology
  - Acquisition utilities need to be patched.
  - Important events (e.g., start of a page imaging operation) are communicated to the platform via a number of hypercalls.
Overview of the Platform Architecture

Memory acquisition software is executed on the emulated Windows PC and communicates with the instrumentation interface via hypercalls.
Measuring Correctness

- Idea: Create an external memory snapshot in parallel to the acquisition phase
  - match the external snapshot with the image of the acquisition program to identify possible differences
  - permits verifying the size and contents of the created memory image
Measuring Atomicity

- Idea: Use an indirect approach and attempt to quantify the degree of atomicity violations

- requires monitoring the memory operations of all running threads during the acquisition phase

- Problem: We do not know if the individual memory operations are causally related

- Quantify potential atomicity violations as an upper bound
### Measuring Integrity

- **Idea:** Create external snapshots of system memory at specific point of times
  - match the created snapshots in a second step to determine the level of differences
  - permits determining how much memory was changed during the acquisition phase and due to loading the acquisition program into RAM

![Diagram showing timeline of acquisition process with timepoints t1, t2, and t3.](image-url)
Evaluation Procedure

1. Prepare snapshot of the guest in an idle system state
2. Start snapshot
3. Select the acquisition software to assess
4. Perform evaluation
5. Determine atomicity
6. Determine correctness
7. Determine integrity
8. Revert snapshot and restart

- Evaluation of three open source imaging applications
  - win32dd, mdd, WinPMEM
- 90 test runs for each imager
- All tests initially started from an idle system state
- Memory sizes between 512 MB and 2 GB
- Each test required between 6.87 and 22.37 GB of disk space
Correctness Evaluation

- (older, open source version of) *win32dd* and *mdd* initially acquired the physical address space incorrectly
  - regions of device memory were ignored
  - offset mapping is corrupted
- after patching, all three utilities created *correct* snapshots, both in size and contents
  - non-accessible regions are zeroed out

Atomicity Evaluation

- The level of atomicity rapidly decreased with larger memory sizes.

Theory: With longer imaging periods, it gets increasingly difficult to keep the image file free from smearing.

Open research: In how far do inconsistencies truly affect later memory analysis?

Inconsistencies are counter-intuitive to classic perceptions of "forensic soundness" though.
Integrity Evaluation

- the level of integrity slightly increased with larger memory sizes

- Theory: On a system with constant load, proportionally less amounts of space are required with higher memory capacities

- Still: About one fifth of memory is changed during the acquisition phase

- Results are similar to earlier experiments by other authors
Summary and Outlook

- Rigorous testing and evaluation of acquisition solutions has been widely neglected so far.

- We now have a mechanism for verifying the correctness of imaging applications and estimating their level of atomicity and integrity.

- Experiments have been performed under “laboratory” conditions.

- Next step: How reliably do acquisition solutions work in the presence of an intelligent adversary?
In case of any questions, please feel free to contact:

Stefan Vömel
http://www1.informatik.uni-erlangen.de/
stefan.voemel@cs.fau.de
Discussion of the Evaluation Approach

- Evaluation of a software imager requires minor patching
  - white-box testing methodology
  - so far, we have only evaluated open source solutions
- Evaluation is limited to x86 32-bit applications and systems with a maximum memory capacity of 2 GB
  - restrictions are due to the underlying Bochs engine
- Level of atomicity and impact of an acquisition program can only be estimated based on upper bounds