derived from them, their evidential value would be too low to justify a conviction.

In the case of integrity and atomicity a closer look is needed. A tool that produces a snapshot with low integrity overwrites more parts of the memory than a tool that produces a snapshot with a higher degree of integrity. Therefore, loss of information in the memory snapshot is more likely if less integrity can be achieved. As the presented evidence should also be as authentic as possible (Fröwis et al., 2020) the method that extracts memory snapshots with higher integrity should be chosen if it also produces correct ones.

Because less atomic snapshots are also more likely to have inconsistencies than more atomic snapshots, the reliability and completeness of the results of an analysis of such a snapshot can be questioned. Therefore, in trying to adhere to the quality requirements of evidence used in court decisions, the more atomic method should be chosen if possible. It should also fulfill the requirements regarding correctness and integrity. Another influencing factor on the evidential value of results based on less atomic memory snapshots would be how likely it is that inconsistencies in memory snapshots lead to analysis results that suggest the presence of incriminating evidence even though it never existed in memory. To the best of the authors' knowledge no research has been published about this topic.

Tools with atomicity guarantees, be they instantaneous, quasi-instantaneous or causal consistency, can often not be used due to the technical circumstances of the investigation and time constraints. If a tool without atomicity guarantees is used, many inconsistencies might occur. The information how likely their occurrence is for a specific snapshot is helpful because investigators or expert witnesses who present the results of a technical analysis need to explain the likeliness of errors or missing information to the court. The court should also be enabled to evaluate how likely different hypotheses based on the presented evidence are and if the evidence is reliable (Fröwis et al., 2020). While it is possible to find some inconsistencies by examining the data structures of the operating system, thereby enabling analysts to report them exactly, others might not be visible. Therefore indicators for the likeliness of the occurrence of inconsistencies, like for example suggested by Pagani et al. (2019), should be made available by the memory snapshoting tool to the analyst. This would enable analysts to provide founded estimates about the likeliness of the analysis results being incomplete or the possibility of wrong results due to inconsistencies.

9. Conclusions and Future Work

The new notions of atomicity and integrity wish to clarify the conditions under which snapshots of storage can be considered as "good". The definitions assume a synchronous system but cover any form of storage which cannot be "frozen" and where individual memory regions have to be acquired sequentially.

The measurement approach described in Section 5 needs to be evaluated in future work. The question remains how the results for a subset of memory regions can be transferred to the quality of the complete memory snapshot. Therefore, it will be necessary to perform an evaluation of the method itself before testing different memory dumping tools. To evaluate the method, the same steps as for a tool evaluation can be performed. Memory snapshots are created while the test program is running and, with the help of vector clocks, atomicity violations are identified. Then, other indicators for inconsistencies, like those described by Pagani et al. (2019), need to be examined. A ground truth of the memory state might be helpful to identify further inconsistencies. The ground truth could be created in a virtualized environment by taking atomic snapshots from the hypervisor. Identifying as many indicators for inconsistencies as possible and creating a big data set of analyzed memory snapshots is another challenge. Indicators can be identified from the related literature.

The creation of a big data set requires the automation of memory snapshot creation and the analysis of memory snapshots, and the organization of the analysis results. A big data set enables statistical analysis with which it can be evaluated, e.g., if the number of atomicity violations in a subset of memory can be used to extrapolate the occurrence of other inconsistency indicators in other memory areas. Another question that seems worth examining is if scenarios can be observed in which inconsistencies lead to false conclusions that create incriminating evidence where none is present.

Acknowledgments

We thank Nicole Scheler and Ralph Palutke for helpful comments on previous versions of this paper. Work was supported by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) as part of the Research and Training Group 2475 "Cybercrime and Forensic Computing" (grant number 393541319/GRK2475/1-2019).

References

Campbell, W., 2013. Volatile memory acquisition tools – A comparison across taint and correctness, in: Proc. 11th Australian Digital Forensics Conference.

Carrier, B., 2005. File System Forensic Analysis. Addison-Wesley.

Case, A., Richard III, G.G., 2017. Memory forensics: The path forward. Digital Investigation 20, 23–33.

Chase, C.M., Garg, V.K., 1998. Detection of global predicates: Techniques and their limitations. Distributed Comput. 11, 191–201. URL: https://doi.org/10.1007/s004460050049, doi:10.1007/s004460050049.

Chu, C., Brockmeyer, M., 2008. Predicate detection modality and semantics in three partially synchronous models, in: Lee, R.Y. (Ed.), 7th IEEE/ACIS International Conference on Computer and Information Science, IEEE/ACIS ICIS 2008, 14-16 May 2008, Portland, Oregon, USA, IEEE Computer Society. pp. 444–450. URL: https://doi.org/10.1109/ICIS.2008.95, doi:10.1109/ICIS.2008.95.

Cooper, R., Marzullo, K., 1991. Consistent detection of global predicates, in: Miller, B.P., McDowell, C.E. (Eds.), Proceedings of the ACM/ONR Workshop on Parallel and Distributed Debugging, Santa Cruz, California, USA, May 20-21, 1991, ACM. pp. 167–174. URL: https://doi.org/10.1145/122759.122774, doi:10.1145/122759.122774.

Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C., Pesch, P., 2020. Safeguarding the evidential value of forensic cryptocurrency investigations. Forensic Science International: Digital Investigation 33, 200902.

Gärtner, F.C., Kloppenburg, S., 2000. Consistent detection of global predicates under a weak fault assumption, in: 19th IEEE Symposium on Reliable Distributed Systems, SRDS'00, Nürnberg, Germany, October 16-18, 2000, Proceedings, IEEE Computer Society. pp. 94–103. URL: https://doi.org/10.1109/RELDI.2000.885397, doi:10.1109/RELDI.2000.885397.

Gruhn, M., Freiling, F.C., 2016. Evaluating atomicity, and integrity of correct memory acquisition methods. Digital Investigation 16, S1–S10.

Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W., 2009. Lest we remember: cold-boot attacks on encryption keys. Commun. ACM 52, 91–98. URL: https://doi.org/10.1145/1506409.1506429, doi:10.1145/1506409.1506429.

Hannich, R. (Ed.), 2019. Karlsruher Kommentar zur Strafprozessordnung: StPO - mit GVG, EGGVG und EMRK. 8. ed.

Heinson, D., 2016. IT-Forensik und Beweisrecht, in: DGRI Jahrbuch 2015. Verlag Dr. Otto Schmidt, pp. 109–130.

Inoue, H., Adelstein, F., Joyce, R.A., 2011. Visualization in testing a volatile memory forensic tool. Digital Investigation 8, S42–S51.

Kiperberg, M., Leon, R., Resh, A., Algawi, A., Zaidenberg, N., 2019. Hypervisor-assisted atomic memory acquisition in modern systems, in: International Conference on Information Systems Security and Privacy, SCITEPRESS Science And Technology Publications.

Lamport, L., 1978. Time, clocks, and the ordering of events in a distributed system. Commun. ACM 21, 558–565. URL: https://doi.org/10.1145/359545.359563, doi:10.1145/359545.359563.

Lempereur, B., Merabti, M., Shi, Q., 2012. Pypette: A platform for the evaluation of live digital forensics. Int. Journal of Digital Crime and Forensics 4, 31–46.

Martignoni, L., Fattori, A., Paleari, R., Cavallaro, L., 2010. Live and trustworthy forensic analysis of commodity production systems, in: International Workshop on Recent Advances in Intrusion Detection, Springer. pp. 297–316.

Mattern, F., 1989. Virtual time and global states of distributed systems, in: Proceedings of the International Workshop on Parallel and Distributed Algorithms, pp. 215–226.

Nisbet, A., Lawrence, S., Ruff, M., 2013. A forensic analysis and comparison of solid state drive data retention with trim enabled file systems, in: Proc. 11th Australian Digital Forensics Conference, pp. 103–111.

Pagani, F., Fedorov, O., Balzarotti, D., 2019. Introducing the temporal dimension to memory forensics. ACM Transactions on Privacy and Security (TOPS) 22, 1–21.

Palutke, R., Ruderich, S., Wild, M., Freiling, F., 2020. Hyperleech: Stealthy system virtualization with minimal target impact through dma-based hypervisor injection, in: 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020), pp. 165–179.

Schwarz, R., Mattern, F., 1994. Detecting causal relationships in distributed computations: In search of the holy grail. Distributed Comput. 7, 149–174. URL: https://doi.org/10.1007/BF02277859, doi:10.1007/BF02277859.

Stoller, S.D., 2000. Detecting global predicates in distributed systems with clocks. Distributed Comput. 13, 85–98. URL: https://doi.org/10.1007/s004460050069, doi:10.1007/s004460050069.

Vömel, S., Freiling, F.C., 2012. Correctness, atomicity, and integrity: defining criteria for forensically-sound memory acquisition. Digital Investigation 9, 125–137.

Vömel, S., Stüttgen, J., 2013. An evaluation platform for forensic memory acquisition software. Digital Investigation 10, S30–S40.

Yu, M., Qi, Z., Lin, Q., Zhong, X., Li, B., Guan, H., 2012. Vis: Virtualization enhanced live forensics acquisition for native system. Digital Investigation 9, 22–33.

Zheng, X., Garg, V.K., 2019. An optimal vector clock algorithm for multithreaded systems, in: 39th IEEE International Conference on Distributed Computing Systems, ICDCS 2019, Dallas, TX, USA, July 7-10, 2019, IEEE. pp. 2188–2194. URL: https://doi.org/10.1109/ICDCS.2019.00215, doi:10.1109/ICDCS.2019.00215.

CRediT authorship contribution statement

Jenny Ottmann: Conceptualization, Methodology, Investigation, Writing - Original Draft, Writing - Review and Editing. **Frank Breitinger:** Conceptualization, Writing - Review and Editing, Supervision. **Felix Freiling:** Conceptualization, Methodology, Investigation, Writing - Original Draft, Writing - Review and Editing, Supervision.