Revealing the Expected

A Survey about Memory Forensic in Practice

Lisa Rzepka, Benedikt Mader, Zinaida Benenson, Harald Baier

Motivation

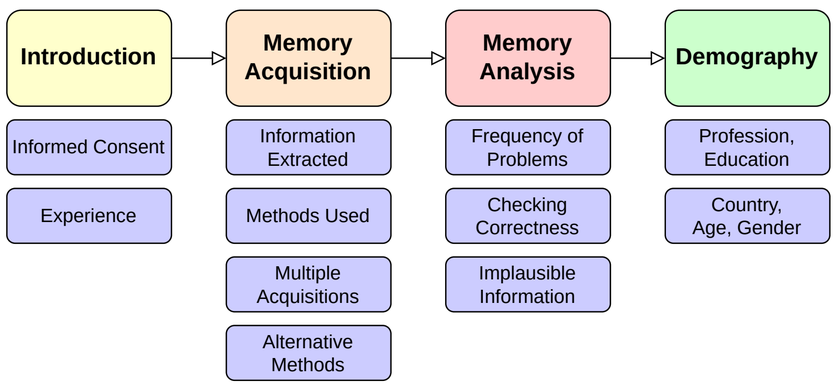

Figure 1: Structure of the conducted survey.

- Memory forensics is essential to detect stealthy attacks like fileless malware, but acquiring memory is a complex task which leads to inconsistencies
- Latest surveys focus on digital forensics in general [1] or have a different aim [2][3][4]
- Goal of this survey (Figure 1): Gain insights in *actual usage* of memory forensics in practice, as this is currently missing in the forensic community
- Understand *strengths and limitations* of memory forensics

Survey and Demographics

- Survey aimed at people with experience in memory forensics, so participants must have acquired memory at least once in order to participate
- 31 participants
- Recruitment: social media, personal contacts, snowball recruiting
- From at least 7 countries, majority male, between 30 and 50 years old
- Highest education mostly Master's degree, followed by PhD
- Main employment evenly split between public and private sector, roles depicted in Figure 2

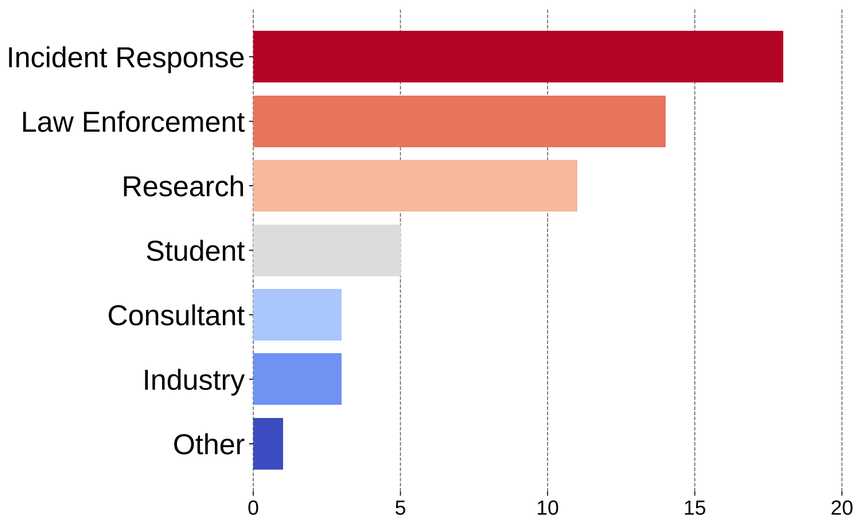

Figure 2: Different role categories. Multiple choice question.

Memory Acquisition and Extracted Information

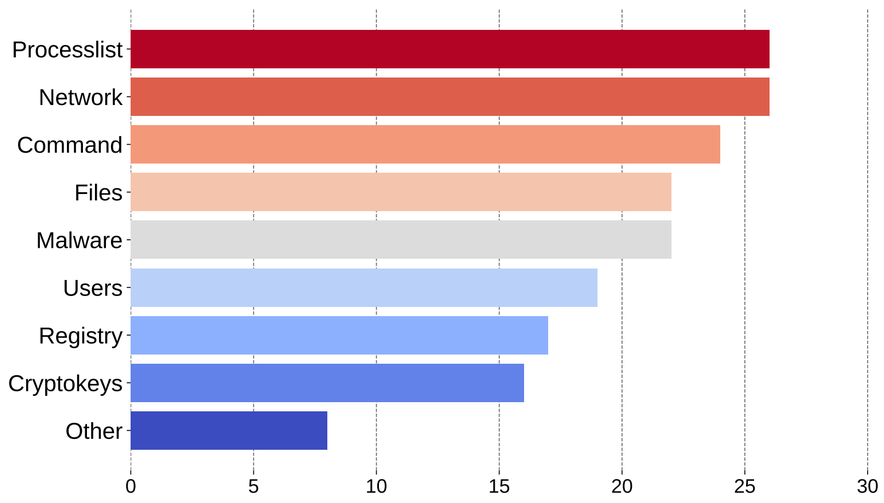

Figure 3: Memory forensic use cases. Multiple choice question.

- Most common use case for memory forensics are extraction of running processes and network information (Figure 3)
- Most common acquisition methods are software tools and hypervisor-based methods
- Memory acquisition is rarely done multiple times for the same case
- Alternative methods include disk forensics and live analysis

Problem frequency during Memory Acquisition

- Problems (depicted in Figure 4) occurring during acquisition and analysis are typically infrequent, but play nevertheless an important role, e.g., regarding reliability of evidence
- The study highlights the need for *reliable* memory forensic tools

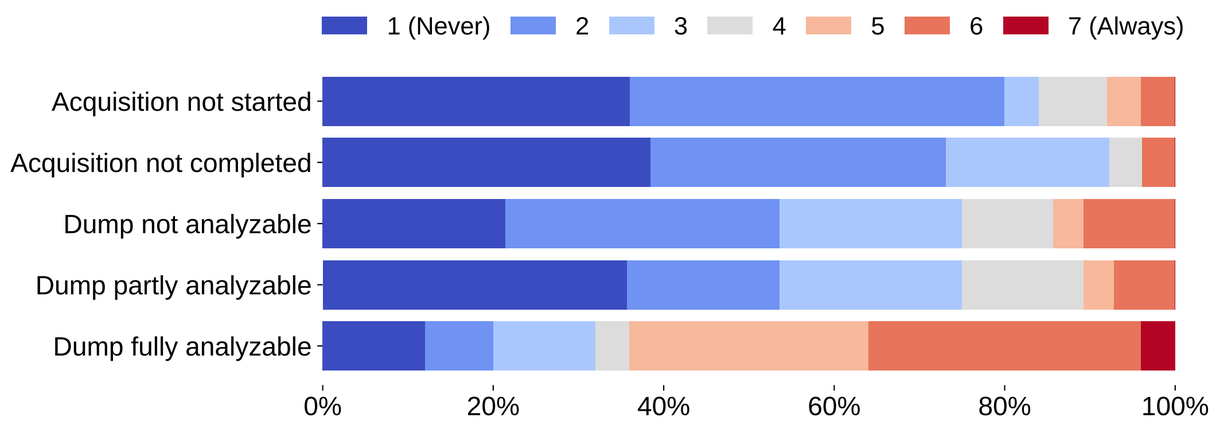

Figure 4: Problems occurring during acquisition and analysis. Answered on Likert scale (1=never to 7=always). Responses were checked regarding plausibility, 4 participant answers were removed.

[1] Hargreaves, C. et. al, 2024. DFPulse: The 2024 digital forensic practitioner survey. FSI:DI 51.
[2] Sanchez, L. et. al, 2019. A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM). FSI:DI 29.
[3] Franqueira, V. N. L. et. al, 2018. Investigation of Indecent Images of Children cases: Challenges and suggestions collected from the trenches.FSI:DI 24.
[4] James, J. I. et. Al, 2016. A survey of mutual legal assistance involving digital evidence. FSI:DI 18.