A Controlled Experiment in Digital Investigation

Felix Freiling       Christian Zoubek
How do they (classical) crime investigators work?
How do they do it?

• Established inventory of methods and evidence types
• Clear separation of duties between investigator and forensic scientist
• Documented experience that is systematically used in criminalistics education
How do digital investigators work?
How do they do it?

• Unclear role of “digital forensic scientist”
• Hardly any (peer reviewed) literature on how digital investigators work
• We know how to teach technical skills, but how do we teach investigative skills?
Overview

1. Research questions
2. The experiment
3. Experimental results
4. Conclusions
1. Research Questions
Terminology

• “Case”
  • Description of case context and investigative goals
  • A collection of digital evidence

• “Participant” and “Group”
  • Human who participated in the experiment
  • Multiple participants

• “Effort”
  • Time in minutes spent on solving the case
  • “Individual effort” vs. “group/total effort”

• “Quality”
  • Percentage/amount of correctly interpreted digital evidence
Different Types of Work (Task Types)

• T1: conceptual work with pen and paper, including documentation

• T2: group meetings, discussion

• T3: programming new tools, interfacing with old tools, automating investigative/analysis steps

• T4: applying tools, doing the actual investigation
Research Questions

• Is there a difference between the total effort to solve different cases?
• Do groups use different strategies when trying to solve different cases?
• Is the distribution of task types different for different cases and groups?

• What factors correlate with total effort per case?
• What factors can predict total effort?
• What factors correlate with result quality?
• What factors can predict result quality?
2. The Experiment
The Setting

• Course „Forensik II“, October 2015-February 2016
• Almost 40 students, all of them with basic forensics education from earlier course
• Split up into 10 groups of investigators
• 3 (arguably realistic) cases
• Pre-study questionnaire, final investigative report
• Mandatory documentation of effort by every participant

• In total we used data from 34 participants
The Cases

• ARPspoof
  • Sysadmin gets access to passwords via ARP spoofing

• Terror
  • Terrorists coordinate bombing attack on embassy in a web forum trying to hide their traces

• Malware
  • Distribution of malware over a an infected website, infection of clients, keylogging

• At least three disk images to analyse in a stepwise fashion
• One false false trail in each case description
Experimental Design
Timeline

- 2nd meeting w. prosecutor, exhibit 3
- Delivery report
- Debriefing

Cohort #1: Blue
Cohort #2: Orange

Timeline:
- 08.12.15
- 15.12.15
- 22.12.15
- 29.12.15
- 05.01.16
- 12.01.16
- 19.01.16
- 26.01.16
3. Experimental Results
Figure 6: Total effort per case (plot of average and standard deviation).
Figure 7: Total effort per task type (plot of average and standard deviation).
Figure 9: Real total effort per student vs. motivation.
Figure 10: Grade vs. effort per group.
Figure 11: Grade vs. total motivation per group.
Figure 12: Result quality/grade vs. grade of basic course.
Previous Grades vs. Quality

• Quality correlates positively with grade in introductory forensics course

• Previous grades are a good predictor of future grades
4. Conclusions
Interpretation of Results

- Bounded (well-specified) investigation goals reduce effort
- Effort is more important than motivation for good quality
- Use quality of previous work to select good people
Future Studies

• Focus more on measurements of individuals than on groups

• Formulate precise hypotheses and calculate statistical significance with more (100+) participants

• Case comparison is hard, can this be done better?

• Data available online:
A Controlled Experiment in Digital Investigation

Felix Freiling  Christian Zoubek