1. Detailed questionnaires and interview guidelines

For the review process, we decided to include all materials in the appendix to be available for the reviewer. In case this paper gets accepted, all data will be made available via a common data repository/archive and removed from here.

2. Pre-tampering questionnaire

Below, we provide the full transcript of the pre-tampering questionnaire. Note: Coding rules and question types are marked in gray (not visible to respondents).

- [Q0 - Short free text] Participation in exercise 1 is done in an anonymous fashion to prevent bias caused by grading. To connect the results of a particular participant we will use a personal pseudonym that is calculated according to the following algorithm: Third letter of the first name of your mother, example: MARIA MÜLLER = R; Last digit of the house number of your address, example: Street 119 = 9; Sum of the day and month of your birthday, example: birthday is 14.9.1982 = 14 + 9 = 23. The pseudonym of the example is therefore S923. Please note down your pseudonym for later use. We will repeat the algorithm whenever you are instructed to use your pseudonym. What is your pseudonym (calculated according to the above algorithm)?
- [Q1 - Single choice question] What is your course of study?
  (a) Computer Science
  (b) Information and Communication Technology
  (c) Computational Engineering
  (d) Other
- [Q2 - Single choice question] What is the degree of your course of study?
  (a) Master of Science
  (b) Master of Arts
  (c) Bachelor of Science
  (d) Bachelor of Arts
  (e) Other
- [Q3 - Single choice question] Which semester are you in within your current degree?
  (a) 1
  (b) 2
  (c) 3
  (d) 4
  (e) 5
  (f) 6
  (g) 7
  (h) 8
  (i) 9
- [Q4 - Single choice question] Towards which degree are you following this course?
  (a) Bachelor
  (b) Master
- [Q5 - Single choice question] I am motivated to participate in this experiment. (1 = strongly agree, 5 = strongly disagree)
  (a) 1
  (b) 2
  (c) 3
  (d) 4
  (e) 5
- [Q6 - Single choice question] How many other courses are you following in this semester next to [this forensic lecture]?
  (a) None
  (b) 1
  (c) 2
  (d) 3
  (e) >4
- [Q7 - Single choice question] Which percentage of your weekly working time do you plan to invest into this experiment during the time that the experiment runs?
  (a) 0-10
  (b) 10-20
  [...]
  (i) 80-90
  (j) 90-100
- [Q8 - Single choice question] Did you attend the introductory lecture [on digital forensics]?
  (a) Yes
  (b) No
- [Q9 - Single choice question] In case you attended [the digital forensic lecture], did you submit at least one expert witness report as part of the exercise of that course?
  (a) Yes
  (b) No
  (c) Did not attend
- [Q10 - Single choice question] In case you attended [the digital forensic lecture] and took the exam, in what region was your grade [blinded for review]?
  (a) [range 1]
  (b) [range 2]
  (c) [range 3]
  (d) [range 4]
  (e) Did not pass
  (f) Did not attend
- [Q11 - Multiple choice question] Which other courses of the IT security infrastructures lab have you attended [blinded for review]?
  (a) [lecture 1]
  (b) [lecture 2]
  (c) [lecture 3]
  (d) [lecture 4]
  (e) [lecture 5]
  (f) [lecture 6]
  (g) [lecture 7]
  (h) [lecture 8]
  (i) Others
- [Q12 - Single choice question] How many disk images have you analyzed forensically until today? If you don't know the number exactly, please estimate the number as good as you can.
  (a) 0-2
  (b) 3-6
  (c) more than 6
- [Q13 - Single choice question] On how many of these disk images was Windows installed?
  (a) 0-2
  (b) 3-6
  (c) more than 6
- [Q14 - Single choice question] In how many tampering experiments have you participated before?
  (a) 0
  (b) 1
  (c) 2
  (d) more than 2

- [Q15 - Single choice question] How many working hours do you plan to invest into this experiment on average per week during the time that the experiment runs?
  (a) 0
  (b) 0,5
  (c) 1
  (d) 1,5
  (e) 2
  (f) 2,5
  (g) 3
  (h) 3,5
  (i) 4
  (j) >4

3. Post-tampering questionnaire

Below, we provide the full transcript of the post-tampering questionnaire. On LimeSurvey, each subsection corresponded to one questionnaire page (e.g., Section 2 subsection III Tampering process). Students were not allowed to check their answers on previous pages. Note: Coding rules and question types are marked in gray (not visible to respondents).

Part 0: Pseudonym

- [C0 - Short free text] Please give your personal pseudonym used in the experiment. You can calculate it according to the following algorithm: Third letter of the first name of your mother, example: MARIA MÜLLER = R; Last digit of the house number of your address, example: Street 119 = 9; Sum of the day and month of your birthday, example: birthday is 14.9.1982 = 14 + 9 = 23. The pseudonym of the example is therefore S923.

Section 1: experiences before the tampering task

I. Design and original ideas.
Consult your project log book and reposition yourself at the start of the experiment.

- [Q1 - long free text] What were your initial thoughts when starting with the exercise? Please explain your strategy and plan of action.
- [Q2 - long free text] How did you prepare (literature review, experiments)?

II. Initial assessment of the sources of timing information.
How did you initially judge the following sources of timing information? If you learned about this source during the experiment, please answer "No" to the following questions.

- [Q3 - array question] I knew of this source.
  Row options: each item in 1.
  (a) Yes
  (b) No
  (c) I am not sure
  (d) I do not remember

Now, considering only the sources of timing information you indicated you knew. Please, answer the following questions.

- [Q4 - array question] I found this source of timing information relevant to solving the upcoming tampering task.
  Row options: [Sources in Q3 marked as "Yes"] .
  (a) Yes
  (b) No
  (c) I do not remember

Layers	Sources
Application	Files internal metadata
	Firefox cache files
	Firefox cookies
	Firefox history and downloads database
	Microsoft Edge cache files
	Microsoft Edge history and downloads database
	OneDrive synchronization logs
	Thunderbird Inbox file
	Thunderbird Global database
OS	Amcache (registry)
	Bam (registry)
	Jumplists
	LNK files
	OpenSavePIDMRU / LastVisitedPIDMRU (registry)
	Prefetch files
	`setupapi.dev.log`
	Shellbags (registry)
	ShimCache (registry)
	USB/USBSTOR (registry)
	UserAssist (registry)
	Windows Event Logs
	Windows timeline database
File system	`$LogFile`
	`$MFT`
	`$RECYCLE.BIN`
	`$USNjrnl`

Table 1: Catalog of Windows artifacts derived from Plaso parsers.

- [Q5 - array question] I planned to manipulate this source.
  Row options: [Sources in Q3 marked as "Yes"] .
  (a) Yes
  (b) No
  (c) I do not remember
- [Q6 - array question] How hard did you think it was to manipulate that source?
  Row options: [Sources in Q3 marked as "Yes"] .
  (a) Easy
  (b) Medium
  (c) Hard
  (d) I do not remember
- [Q7 - single choice question] Are there any sources of timing information that you planned to manipulate but are missing from the above list?
  (a) Yes
  (b) No
- [Q7b if Q7=="Yes" - long free text] Please explain which ones and how you planned to manipulate them.

Now, considering the sources of timing information you indicated you had planned to manipulate.

- [Q8 - ranking] Given the following list of sources of timing information, please sort them according to the *perceived difficulty* of tampering. Arrange the sources of timing information in descending order of difficulty for tampering, placing the most challenging source at the top right and progressing towards the less challenging ones.
  Ranking options: [Sources in Q5 marked as "Yes"] .
- [Q9 - ranking] Given the following list of sources of timing information, please sort them according to the *priority in which you wanted to tamper* with them. Arrange them in descending order of priority, with the highest priority at the top right and descending towards the lower ones.
  Ranking options: [Sources in Q5 marked as "Yes"] .
- [Q10 - array (text)] Please give a short statement of how you had planned to manipulate these sources of timing information (e.g., process, tools, ...).
  Row options: [Sources in Q5 marked as "Yes"] .

Section 2: experiences during the tampering task

III. Tampering process.
Consult your project log book and reposition yourself during the experiment.

- [Q11 - long free text] Which of the planned manipulations went according to plan? Which ones failed and why?
- [Q12 - single choice question] Did you adapt your strategy from the beginning?
  (a) Yes
  (b) No
- [Q12b if Q12=="Yes" - long free text] What did you change in your strategy?
- [Q13 - single choice question] Did you attempt to remove any traces of your activities (indirect traces)?
  (a) Yes
  (b) No
- [Q13b if Q13=="Yes" - long free text] How did you remove the traces of your activities?
- [Q14 - single choice question] Did you do some form of quality control of your activities?
  (a) Yes
  (b) No
- [Q14b if Q14=="Yes" - long free text] How did you do the quality control of your activities?

Part 3: experiences after the tampering task

IV. Final assessment of the sources of timing information
Now, after completing the experiment, how do you rejudge the following sources of timing information? Note that you gave the following answers in part 1: [array of answers in Q3].

- [Q15 - array question] I now know of this source. Note that this may include the sources you selected in part 1. For example, if I knew of the $MFT before starting the task, and discovered the existence of the $USNjrnl during/after the task, I select "yes" for both sources of timing information.
  Row options: [$LogFile, $MFT, $RECYCLE.BIN, $USNjrnl, Amcache (registry), Bam (registry), Files internal metadata, Firefox cache files, Firefox cookies (cookies.sqlite), Firefox history and downloads database (places.sqlite), Jumplists, LNK files (.lnk files), Microsoft Edge cache files, Microsoft Edge history and downloads database (History), OneDrive synchronization logs, OpenSavePIDMRU/LastVisitedPIDMRU (registry), Prefetch files (.pf files), setupapi.dev.log, Shellbags (registry), ShimCache (registry), USB/USBSTOR (registry), UserAssist (registry), Thunderbird emails (Inbox file), Thunderbird Global Database (global-messages-db.sqlite), Windows Event Logs (.evtx files), Windows timeline database]
  (a) Yes
  (b) No
  (c) I am not sure
  (d) I do not remember

Now, considering only the sources of timing information you indicated you know. Please, answer the following questions.

- [Q16 - array question] I now find this source of timing information relevant to solving the tampering task.
  Row options: [Sources in Q15 marked as "Yes"] .
  (a) Yes
  (b) No
  (c) I do not remember
- [Q17 - array question] I manipulated this source in the image I submitted.
  Row options: [Sources in Q15 marked as "Yes"] .
  (a) Yes
  (b) No
  (c) I do not remember

Now, considering the sources of timing information you indicated you had manipulated.

- [Q18 - array question] How hard did you think it was to manipulate that source?
  Row options: [Sources in Q17 marked as "Yes"] .
  (a) Easy
  (b) Medium
  (c) Hard
  (d) I do not remember
- [Q19 - single choice question] Are there any sources of timing information that you planned to manipulate but are missing from the above list?
  (a) Yes
  (b) No
- [Q19b if Q19=="Yes" - long free text] Please explain which ones and how you manipulated them.
- [Q20 - ranking] Given the following list of sources of timing information, please sort them according to the *perceived difficulty* of tampering. Arrange the sources of timing information in descending order of difficulty for tampering, placing the most challenging source at the top right and progressing towards the less challenging ones.
  Ranking options: [Sources in Q17 marked as "Yes"] .
- [Q21 - ranking] Given the following list of sources of timing information, please sort them according to the *order you tampered* with them. Arrange them in descending order, with the first source you tampered with at the top right and descending towards the lower ones.
  Ranking options: [Sources in Q17 marked as "Yes"] .
- [Q22 - array (text)] Please give a short statement of how you manipulated these sources of timing information (e.g., process, tools, ...).
  Row options: [Sources in Q17 marked as "Yes"] .

4. Interviews

Below, we provide the full transcript of the semi-structured interview guidelines.

Welcome
Welcome and thank you for taking the time to participate in our interview. [Introduction of the interviewer(s)]

Research project
In this research project, we are interested in understanding your approach to the tampering task and evaluating the difficulty of tampering with different sources of timing information. The idea is to identify the factors that render one source of timing information more difficult to tamper with compared to another. For this purpose, it is important for us to gain insights from the perspective of individuals manipulating data to hide their activities.

Duration
30-40 minutes.

Process
The interview will be recorded. You can stop this interview at any moment without any disadvantages as a result. Throughout the interview, we will ask you some questions about your work and experiences in regard to the tampering experiment. The questionnaire provided us with a deeper insight into your approach to the task. Our focus now is understanding the 'why' behind your decisions — specifically, the factors that influenced your design choices and tampering approach.I will be referring to some of your earlier responses. Thank you for investing your time in completing it; it was really interesting to read your answers. Please remember, that there are no right or wrong answers in your responses. We are interested in understanding your thought process and considerations.

Data usage
Information shared will be treated confidentially; results will be anonymized (no reference to individuals). All data will be used solely for the research project. Before any publication, we will provide you with the results of the interview and questionnaire. You can then inform us whether you agree with

the form of these results or if parts should be omitted.

Consent
Are you in agreement with the interview being recorded so that it can be transcribed and evaluated later?

Other
Do you have any questions before we start the recording?

Thematic 1: prior experiences
I would like to begin the interview by discussing your prior experiences and interests.

1. How familiar are you with the Windows operating system?
   (a) Was your unfamiliarity with Windows a downside to performing this task?
   (b) If yes, can you explain why?
2. Do you have any personal interests or prior experiences related to digital forensics outside the formal teaching curriculum?

Thematic 2: strategy
According to the questionnaire, your plan for this task was to modify either A2 or A3. In the end, you chose to manipulate [Thunderbird (A2)/Firefox (A3)].

1. Could you briefly describe again the approach you took in the process?
   (a) What was the main motivation(s) behind your choice of manipulating [Thunderbird (A2)/Firefox (A3)]?
   (b) What potential problems or issues might arise from manipulating [Thunderbird (A2)/Firefox (A3) (choice not taken)]?
   (c) Do you think that there were other possible strategies? If yes, can you provide an example and explain in which sense your strategy is better (or not)?
   (d) What were your main concerns while performing the task?
   (e) Did you follow a specific order of manipulations?
   (f) What factors influenced the order in which you tampered with the sources of timing information?

Thematic 3: perceived difficulty
In the questionnaire, we asked you to express "how hard a source was to manipulate" (easy/ medium/ hard/ I do not remember).

1. In your opinion, what makes a source of timing information more easy to tamper with than another?
2. In your questionnaire, you mentioned that [Source 1] was more difficult to tamper with compared to [Source 2]. What are the factors that make this source more difficult to tamper with?
3. How did the perceived difficulty influence your strategy, in particular the order in which you proceeded?

Thematic 4: effort

1. How would you describe your motivation level?
2. How many working hours did you put into the task? (estimation)

Thematic 5: conclusion
[Brief summary of the discussion]

1. If you had the opportunity to start again the experiment with your current knowledge, is there anything that you would do differently?
2. If you were in the position of Albert, would you think that your manipulations would be sufficient to make it look "as if" A3 happened before A2 to an investigator?
3. Is there anything else that you would add or discuss?

Thank you for participating in the interview!