Review 5

Recenzija po delih / Review by elements

Vsebina / Content:	**4**: (dobra / good) I think that the topic is represented quite well. It tells a little bit about different tools like pegasus that goverment use and later a little bit about app downgrading and retreiving the data from social media. There is report on previous results. The article is talking about one single topic, and does not work on wider problematics. There is no implementation incuded. It is possible to enhance the content, maybe to be a little bit more clear.
Tok predstavitve / Flow of the presentation:	**4**: (dober / good) It seems that it is possible to read the text, but i am a little bit confused. At first i thought that there will be some emphasis on the comparison between the comercial tools and govermental spyware but then i think this wasnt the case. Othervise flow seems quite nice.
Oblika / Form:	**3**: (korektna / adequate) I have no idea about the ACM Reference Format. The students seems not to be from Slovenia so it is possible that this is acceptable format, but sadly the most articles are differently formated. If you are not sure about the format correct please consult with the profesor. There is no references at all. No quotation of image in the text. There is no further comment but i think that this part should be improved.

Predlogi in opažanja / Suggestions and notifications

Dobre strani / Issue that are specially good:	The topic is very interesting and it is well represented. It puts emphasis on the comercial tools that are used and explains very well how the experiment was done. The core thing is quite nice in terms of attracting intrest from the reader.
Predlogi za izboljšave / Suggestions for improvements:	It is quite hard to evaluate the authors understanding of the topic since i dont know what was the original articles name? Probably you should quote image in text and reconsider the format. If the format is already acceptable then fine. I have no knowledge about this.

Splošno / General

Splošna ocena / Overall evaluation:	**3**: (korekten prispevek / adequate contribution) As mentioned previously the article is written quite well but it seems that has some structral issues. The topic is interesting and it tells a little bit about how this tools might be abused but otherwise it is quite readable to me. The only thing i would point out are references and format as mentioned.
Recenzentovo poznavanje tematike / Reviewer's confidence:	**1**: (sploh ne poznam problematike / no knowledge about the topic) I dont have a lot of knowledge about any of the programs used.

Review 3

Recenzija po delih / Review by elements

Vsebina / Content:

3: (korektna / adequate)
The results of the original study are presented in the article. However, many potentially interesting details are missing (such as the list of the mobile devices tested) and it's hard to get a clear picture regarding the extent of the additional testing. The testing itself is not described in great detail and it's also not clear what testing was performed by the authors of the original article and what was done in addition.
However, the article does attempt to describe a view that is a bit more broader than the original article itself, describing some methods of security bypassing etc.

Tok predstavitve / Flow of the presentation:

3: (korekten / adequate)
While the over-arching structure of the text is acceptable, starting from a general introduction of the mobile forensics field and continuing to the experiments step-by-step, the flow of the reading is hampered by a poor separation of topics discussed in some of the chapters.
Specifically, most of the Chapter 3 could be summarized in a sentence or two, or it should perhaps just be a part of the Introduction or Conclusion as it talks very generally about the usefulness of mobile forensics, which should perhaps be instead cited from another article and briefly summarized in this one. Likewise, a large part of the Experiments section could be better used as a conclusion of the article.
Furthermore, the reader sometimes comes across phrases which hint at experimentation described later in the article, but the details never appear to be stated afterwards. Sometimes, "evident" conclusions are mentioned which don't appear to correlate to anything mentioned in the article.

Oblika / Form:

2: (slaba / poor)
First, while the article itself is well-formatted, it appears that a wrong document style was used when compiling the PDF from the Latex source. As I understand it, `sigconf` was the prescribed style, which can be applied using the following command at the top of the tex source file: \documentclass[sigconf]{acmart} - but I may be wrong here.

Sadly, the article seems to be void of any references and citations. Even the original article, which was used as a basis for the article in question, does not appear to be cited. The article frequently makes claims that are unsupported by either the author's own experimentation or citations, leaving the reader wondering whether a claim will be supported by further chapters of the article or if this was something that was already researched. This impacts the credibility of the stated facts. References are a crucial part of publication.

The included image on Page 5 is also without any captions, is not referenced in the article itself and is generally hard to read.

Predlogi in opažanja / Suggestions and notifications

Dobre strani / Issue that are specially good:

The article describes the motivation behind mobile forensics and goes in depth about implications of the availability of various tools to specialists performing forensic investigations.
Additionally, in Chapter 5, the authors list a number of interesting features of a specific forensic tool, giving some additional insight into the current

Predlogi za izboljšave / Suggestions for improvements:

state-of-the-art.
First of all - please provide citations for the claims provided in the article. If this is the first time you are citing existing works in Latex, Google Scholar provides BibTeX snippets for any article, which can be copy and pasted into your project's bibliography.
The third sentence in the introduction is already something that could/should be cited (the one about the number of smartphones used globally), just as an example.

Also make sure to be consistent when using the names of products, specifically MOBILedit - in Section 4.1 and Section 5, you use a different, incorrect capitalization (MobilEdit).

The following suggestions are targeting specific sections of the article.

1. Introduction
> "Even though programs like MOBILedit Forensic Express are available to the general public and have extensive functionality, we found that their capabilities were noticeably different from those of products that are only sold to governments, like Predator."

It is written here that you "found that their capabilities were noticeably different", but this does not appear to be discussed further in the article in detail. The capabilities of government-access-only tools are not listed and not compared to any other tool, including MOBILedit. Please list the mentioned noticeable differences and capabilities.

2. Security Bypassing
> "In our experimentation, we encountered challenges when attempting to access data from various devices, irrespective of their operating systems. Despite utilizing MOBILedit Forensic Express and exploring every possible avenue within the tool, we found that certain security measures on the devices impeded our efforts to extract data without the necessary access credentials. It's important to note that the ability to bypass device security measures may vary depending on factors such as device model, operating system version, and the specific security configurations implemented by the user."

You mentioned "challenges when attempting to access data from various devices", but you failed to mention in the article which devices were used in the testing (manufacturer, model, ...) or whether you tested both popular operating systems. You also mention "exploring every possible avenue within the [MOBILedit] tool", but the Experiment section fails to describe any methods utilized, only what data was recovered from the device.

> "Overall, our experimentation underscored the importance of ethical and lawful practices in digital forensic investigations [...]"

The experimentation did not appear to underscore any such importance since standard forensic tools were used. Please corroborate.

2.1. The importance of rooting for access to secured data
> "This can be crucial in uncovering evidence related to criminal activities,

such as terrorism, fraud, or cybercrime. For example, deleted messages may contain valuable evidence that could be instrumental in solving a case."
This is a claim that can be made for (mobile) forensics in general - perhaps this part should be moved to the Conclusion or the Introduction as it is not specific to the rooting procedure.

2.2. App Downgrading
Unclear section - it is not explained how app downgrading can provide additional data during a forensic investigation.

2.3. Exploring Alternative Paths in Mobile Data Access
> " In the US, the legal landscape regarding the force of use in mobile forensics is evolving."
Unclear sentence, please rephrase.

Additional comment for the entirety of Section 2 - this section is full of great opportunities to cite existing research!

3. Comparison with other tools and stating the purpose of the experiment
This section is way too long and a large part of the text belongs in the Introduction instead. Please shorten the first half of the paragraph to a sentence or two, cite the source of the claims for the state of digital forensics, and move the resulting text to the introduction instead.

> "We set out on a mission to research the effectiveness of mobile forensic tools in retrieving digital evidence from popular messaging apps [...]"
Reword - the word "mission" is rather unfitting. Additionally, you used plural in the phrase "mobile forensic tools" while only a single tool appeared to be researched/used. A better phrasing would perhaps be "[...] to research the effectiveness of MOBILedit in retrieving [...]"

> "We decided to investigate widely used programs in Europe because we wanted to find out how flexible and adaptable MOBILedit Forensic Express and other forensic tools were in various linguistic and cultural contexts."
Apart from MOBILedit no "other forensic tools" were investigated in the article. Omit the phrase.
Additionally, you did not appear to investigate in Section 4 (Experiment) the adaptability of MOBILedit or any other tool in "various linguistic and cultural context".

4. Experiment
I'm missing a better descriptions of the procedures you used. You fail to even mention MOBILedit in the section - the reader has to deduce that you used this program and not also other methods.

> Image
Please add a caption to the image and explain what is displayed. I suspect it is a screenshot from MOBILedit showcasing what kind of data can be extracted from text messaging applications?
Please enlarge the image to enhance its readability. I recommend only

keeping the first 1-2 messages instead of six - this way, it will be easier for you to enlarge the image and display the content clearly.
Also, please reference the image from within the article text.

> WhatsApp bullet point
In the WhatsApp bullet point, you also mistakenly duplicated the entirety of the Telegram bullet point.

> Facebook Messenger bullet point - you wrote a double "r" in the app name in the heading of the bullet point.

> "This was the least secure application that we accessed during our experiment, and the findings highlight the importance of encryption in mobile security, and also the aggressive nature of Meta’s data collection, which has been scrutinized by researchers and legislators."
By what measures was Messenger the least secure application? You mention "findings", but fail to explain any details and how they highlight the importance of encryption.
Also, please cite the researchers who "scrutinized [Meta's data collection]".
It might also be interesting to discuss the data found in WhatsApp, which is also owned by Meta - was the security and privacy on a higher level there?

> "These revelations highlight how crucial it is to use a variety of forensic techniques [...]"
"Revelations" is too strong a word here. Reword.

5. Interesting features of MOBILedit tool
> Password Extractor bullet point
Add the missing space after the colon in the bold bullet point heading.

Splošno / General

Splošna ocena / Overall evaluation:

3: (korekten prispevek / adequate contribution)
While the article made a good attempt at making an overview of the field of mobile forensics and briefly described a handful of state-of-the-art techniques used in the field, the poorly described experiments and the lack of citing throughout the article degrade its quality significantly.
The article text is not consistent from section to section - in some parts, it is claimed that a number of tools were tested while only briefly showing what appear to be testing results for one forensic tool. Also, the authors could focus more on describing the testing procedure, not just the results.

Recenzentovo poznavanje tematike / Reviewer's confidence:

3: (poznam področje / familiar with the topic)
I am experienced in mobile application development and am familiar with the ways apps interact with the operating system, which is knowledge that is also applicable in mobile forensics. I am also familiar with some advanced tools and methods for data extraction from mobile devices.