

IAZOV 1	Kako IT može podržati mlade u romskoj zajednici da se izbore za svoja prava i prevaziđu strah od narušavanja ravnoteže zajednice, što znači da se zlostavljanje ponavlja kroz generacije, takođe kao i da prepoznaju znakove nasilja.
IAZOV 2	Žene u romskoj zajednici nemaju bezbedan pristup informacijama i ako ih nađu ne znaju kako da ih koriste (Postoje informacije o pravima i podršci za ostvarivanje tih prava, ali žene im ne pristupaju ili ne znaju gde da dobiju prave informacije ili starešine zajednica i počinioci nasilja im zabranjuju pristup.)
IAZOV 3	Žene u nasilnim situacijama su često su izolovane od svake podrške (Potrebno im je da imaju mesto da pronađu i pruže podršku jedna drugoj i da stvore zajednicu koja će upozoravati i podržavati druge)
IAZOV 4	Devojke prisiljene na dečji brak i druge žene u nasilnim situacijama ne znaju da kažu ne porodici ili tradiciji (Žene i devojke bi trebalo da se osećaju podržano i da znaju gde da dobiju podršku – bilo da je to od drugih u istoj situaciji ili od zakona)
IAZOV 5	Kako IT može podržati prikupljanje podataka, razmenu informacija, kreiranje zajednice i izveštavanje za žrtve rodno zasnovanog nasilja? Žene žrtve nasilja na mreži ne znaju kako da prikupe dokaze koje bi dostavile policiji. Ženama su potrebni alati koji će im pomoći da prikupe dokaze koji se mogu koristiti za krivično gonjenje i bazu podataka za razmenu jedni sa drugima i organima za provođenje zakona, kako bi počinioci krivičnih dela bili poznati i podaci mogli da se prikupljaju i koriste za zaustavljanje i sprečavanje nasilja (Zakonska pravila u Srbiji na dnu).
IAZOV 6	Smanjenje porasta broja nasilja nad ženama u javnom prostoru, pogotovu na ulici, parkovima, autobusima itd....
IAZOV 7	Seksualna (ne) edukacija - informisanje dece i tinejdžere o tome šta je seksualno uznemiranjia među vršnjacima i od strane odraslih, šta je pristanak u odnosima, kako da se štite, kome da se obrate

Istraživanja domaća

[Zašto žene ne prijavljuju nasilje](#)

https://www.womenngo.org.rs/images/pdf/Convention_Serbian.pdf.pdf

https://www.osce.org/files/f/documents/7/5/419756_1.pdf

https://www.instagram.com/p/C7EfryXo8De/?img_index=2

Organizacije

[Autonomni ženski centar](#)

[Roma daje](#)

Primeri stranih aplikacija i rešenja

Sound of Soul <https://apps.apple.com/us/app/sound-of-soul/id1532902689> - domaća aplikacija

Calculator Vault

<https://play.google.com/store/apps/details?id=ezttools.calculator.photo.vault&hl=en&gl=US>

Noonlight <https://www.youtube.com/watch?v=cEX388mt6pA>

Hide it pro <https://apps.apple.com/us/app/hide-photos-video-hide-it-pro/id523488488>

myPlan <https://myplanapp.org/>

HeHope <https://www.eib.org/en/stories/domestic-violence-evidence-app>

Circleof6 <https://www.circleof6app.com/>

Watch over me <https://watchovermeapp.com/>

Safetipin <https://safetipin.com/>

Bright sky app <https://www.hestia.org/brightsky>

MyPlan app <https://myplanapp.org/>

Sophia chat <https://sophia.chat/>

Strani Hakatoni

- Spotlight Initiative - Kazakhstan - IT VS VIOLENCE
- StartEgypt, the National Council for Women (NCW), and UN Women - "Fighting Violence Against Women Using Technology" - Hakaton na društvenim mrežama
- The United Nations Development Programme (UNDP) in Ukraine, UN Women and the

United Nations Population Fund (UNFPA) - Hack for Locals 3.0: "Together against violence"

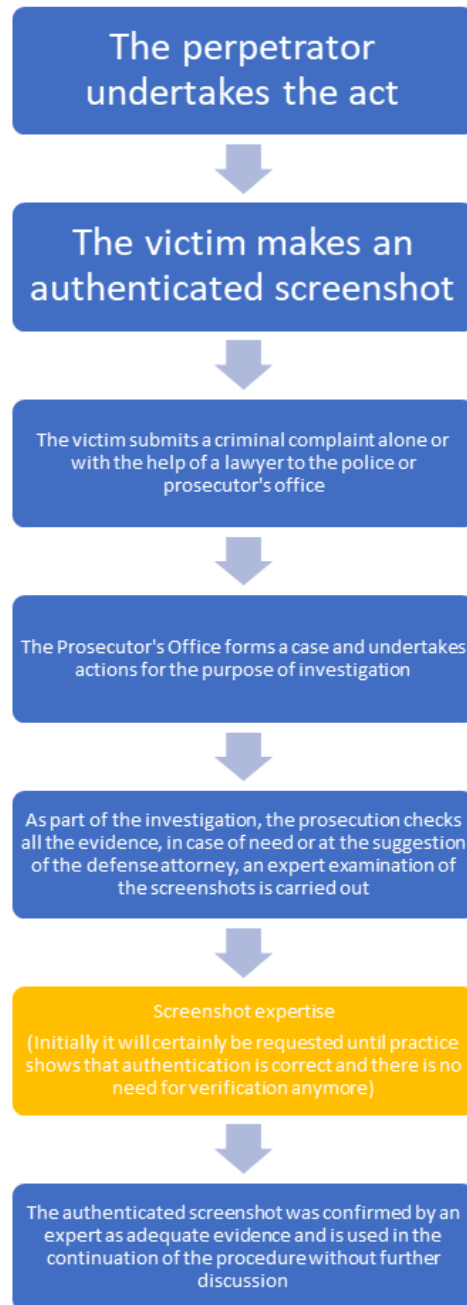
- Woman in Tech Hackathon to tackle Gender Based Violence Snake Nation partnered with CPUT
- Spring act - <https://springact.org/>

IZAZOV 5 detaljnije

What is the proof?

Although in the procedural sense there is a functional separation of the prosecutor's office that deals with crimes committed using the Internet or related to the Internet (Prosecution for high-tech crime - VTK), the Criminal Code does not make such a division. Thus, various criminal acts can be committed using the Internet and social networks. We will take as an example the one that is the most common when it comes to crimes committed through social networks, which is the offense provided for in Article 138 of the Criminal Code - Endangering security and it reads: "Whoever threatens the safety of a person by threatening to attack the life or body of that person or of a person close to him, will be punished with a fine or imprisonment for up to one year." What is necessary in the procedure is to find out who is endangering the safety of a person, in what way, and that the injured party has fear in relation to the assault that threatened his life or the body of that person or a person close to him. The victim submits a criminal complaint with all the evidence he has, including a screenshot of the screen. The image of the screen can be questioned at any time in the procedure (whether in the investigative stages, before the prosecution and the police or later before the court), and then the image would be examined or the device itself would be examined. In this sense, the authentication of the screenshot would shorten that procedure and could continue further, which is the collection of personal data related to the perpetrator of the act (IP address, details of the account from which it was sent, first and last name, etc...). The screenshot itself can be initially expertized (most likely at the suggestion of the defendant's counsel) in order to determine whether the authentication is legitimate, however, I believe that after the practice is established, it will no longer be necessary to perform an expert opinion). In addition to the screenshot of the act itself, the screenshot in this way could also take a picture of the data available to the injured party, e.g. Social network profile, profile picture, phone number and the like.

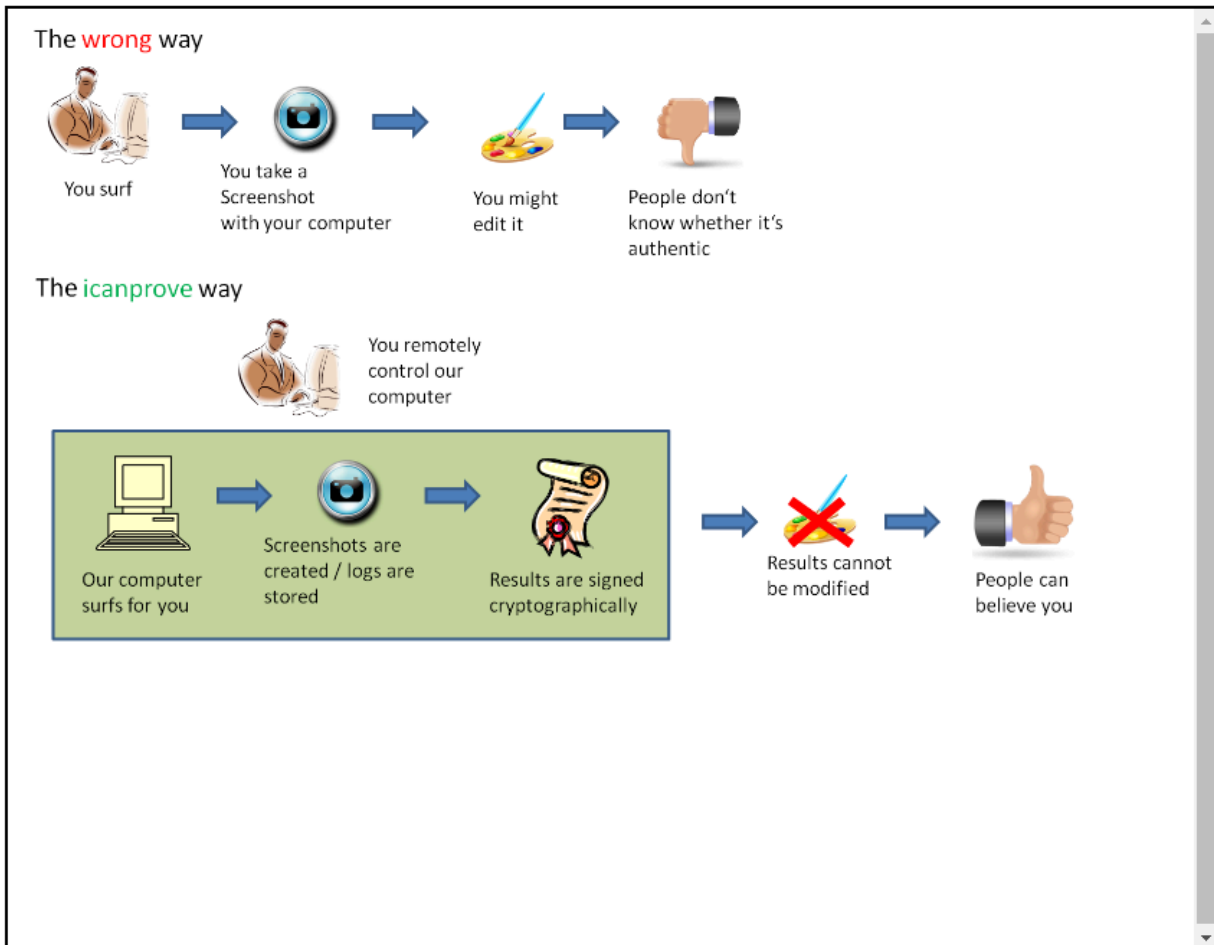
Source: <https://digfor.ftn.uns.ac.rs/>



My research:

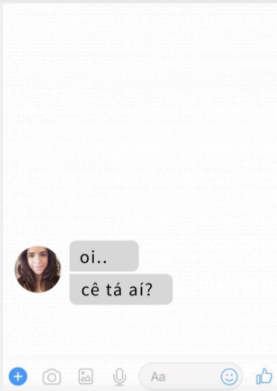
- screenshots do not have any metadata such as EXIF

- For this to work perfectly the output has to contain one screenshot for every single pixel that changes on the screen, e.g. during scrolling or JavaScript animations. Maybe a video format would be more suitable in those cases than PDF as it encodes frames differentially.
- <http://www.icanprove.de/en/>



- metadata could be downloaded and produced?
- in order to use them to provide irrefutable evidence in court it is essential to prove that what is presented is exactly the same as what was originally collected.
- To maintain integrity a detailed log is kept of the transportation, handling, and examination of the evidence including who, when, where, and why possession was taken.
- For a screenshot to be effective as a piece of evidence, it is essential it can be authenticated by the testimony of a witness who has seen the original subject matter and can therefore verify the content of the screenshot.

- The main benefit of using blockchain to prove the authenticity of a screenshot is that it is [immutable](#), meaning no one can change it at a later stage. The immutable nature of blockchain, along with the time/date stamp of the block, proves that the content of the screenshot could not have changed since the time it was committed to the blockchain. Example <https://www.lifehash.com/post/lifehash-releases-evidential-chain-to-improve-security-and-transparency-around-the-handling-of-legal-evidence>
- But is the blockchain evidence for a court or still overkill?
- Video evidence - screen recording rather than just a picture in the app directly
- Another innovative tech use to address risks of sextortion and online harassment, is an AI-powered chatbot and fictional character, developed by [Caretas](#) in Brazil. The platform brings to life the story of 21-year-old Fabi Grossi, who discovers her ex-boyfriend has posted an intimate video of her online. The Facebook page and Messenger chatbot allow the user to interact with Fabi, listen to her story and learn from her experiences. Plan International has released chatbot [Maru](#) supporting girls and women who are experiencing, witnessing or tackling online harassment by providing real advice and resources from experts and activists.



How it works

In the story created, Fabi Grossi is a 21-year-old girl who has an intimate video leaked by her ex-boyfriend on the internet and asks Internet users for help.

To talk to the character, people need to have a Facebook account and access the [Caretas Project Fanpage](#). In it, there are videos, texts and images that simulate the page of a common user.

The public contacts Fabi through Messenger, Facebook's chat space. Through chat, the young woman gives details of the situation she has been experiencing and asks for advice. The conversation is fueled by multimedia content, such as images and audio shared by Fabi, simulating a real conversation between young people in digital media. There are seven stages of interaction, which begin with the character's report on the leak of the intimate video, go through the questioning of the issue in Brazil until reaching the solution and empowerment of the young woman.

The page also provides information about the project, confirms that it is a piece of fiction, and gives instructions on how to get started. Actress Kathia Calil plays Fabi Grossi. If they no longer want to participate, Internet users just need to stop interacting with Fabi or use the STOP command. At the end, everyone is invited to answer some questions for an evaluation of the project.