A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)

By

Laura Sanchez, Cinthya Grajeda, Ibrahim Baggili, Cory Hall

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2019 USA

Portland, OR (July 15th - 19th)

A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)

* Laura Sanchez, Cinthya Grajeda, Ibrahim Baggili, Cory Hall

* Graduate Researcher, UNHcFREG member

Presenting @ DFRWS 2019
Portland, Oregon

University of New Haven
Cyber Forensics Research & Education Group

Agenda

- Introduction
- Previous Work
- Survey
- Results
- Challenges
- Future Work
- Acknowledgements

Problems

- The investigative process:
  - Individual investigations may deal with terabytes of data, containing millions of still images and hundreds of hours of video, and multiple devices (Quick and Choo, 2014)
  - Examining such large volumes of data can be a long, unmanageable, and unproductive process
    - Contributes to lost time in cases and backlogs

Problems, continued

- Impact on investigators and victims:
  - Due to exposure to explicit content, investigators may experience a physical and emotional impact on self and home, intrusive images and thoughts about the viewed content, and a heightened protectiveness or paranoia regarding the safety of children (Burns et al., 2008).
  - Victims may also be further traumatized and re-victimized as a permanent record of their abuse exists and may be viewed by others

Previous Work

- *Psychological Aspect/Trauma*
  - Burns et al (2008)
  - Powell et al (2015)
  - Bourke and Craun (2013)
  - Seigfried-Spellar (2017)
- *Tools, Techniques, and Automation*
  - Powell et al. (2014)
  - Sae-Bae et al. (2014)
  - Ulges and Stahl (2011)
  - de Castro Polastro and da Silva Eleuterio (2010)
- *Triaging*
  - Rogers et al. (2006)
  - Shaw and Browne (2013)
  - Marturana and Tacconi (2013)
  - Baggili et al. (2014)
- *Articial Intelligence (AI)*
  - Peersman et al. (2016)
  - Mahadeokar and Pesavento (2016)
  - PhotoDNA Cloud Service, n.d.
  - Vitorino et al. (2018)
  - Anda et al. (2018),

Contributions

- First comprehensive study to explore practitioner assigned value of current CSAM investigative tools
- First comprehensive survey to study current use of Data Science techniques and technologies in CSAM investigations
- Explores and identifies what investigators deem to be acceptable false positives and false negatives in CSAM investigative technologies

Survey

- Motivation: improve workflow, shorten the amount of time of an investigation, and limit investigative exposure to CSAM content
- The questions focused on what tools and technologies are utilized by CSAM investigators and how they feel about these tools and technologies.
- Consisted of 49 questions:
  - 7 Likert Scale
  - 11 Multiple-Choice
  - 7 Multiple-Selection
  - 6 Free Response
  - 2 Rank
  - 1 Drop Down List
  - 15 Numerical Sliders

Survey, continued

- Question Categories:
  - Demographic
  - Tools – Processing
  - Tools – Detection
  - Technology – Implementation and Usage
  - Technology – Value, Ranking, and Preference
  - Technology – False Positives and Negatives
  - Workflow
  - Tool Processing Times - Acquisition, Processing, Analysis, & Reporting Time
  - Tool Processing Times - Acquisition Processing Times for Android Phones
- 106 participants

Results – Demographics

- Majority of the sample population → white (93.40%) males ranging from ages 35-54 (65.10%) with at least a high school diploma.
- Highest level of education → Bachelor's Degree (41.51%) with most related to the fields of technology and law
- Respondents indicate being most competent in Digital Forensics (99%); 41% neither agrees nor disagrees on being competent in Data Science
- 69% have received formal training to investigate CSAM cases

Tools – Processing

- Two questions, presented in a multiple-answer format, asked participants to identify all the tools they use to process CSAM images and videos.
- Unsurprisingly, for both questions the results indicated that commercial tools appear to be utilized more than free or open-source tools.
- Limitations:
  - Feature/capability related (62%) → lacking filtering, safe-viewing, carving, photo enhancement, photo grouping, accuracy, user-friendliness

Tools - Detection

- Usage of currently available technology to automatically detect pornographic content:
  - iCOP/iCAC COP → 50%
  - Yahoo NSFW → 2.56%
  - Both → 1.28%
  - Neither → 46.15%
- Benefits → quickness (22.92%)
- Limitations → able to identify only known or hashed content (25%)

Technology –Implementation and Usage

- Respondents were asked if the following technologies are implemented by their image and video processing tools:
  - Skin tone detection
  - Face recognition
  - Face detection
  - Age estimation
  - Child nudity detection
  - Object detection
  - Face presentation
  - Nudity blocker

Technology – Implementation Results

	Count	Percentage
Technology Implemented by Image Processing Tools		
Skin Tone Detection	76	56.30%
Face Recognition	6	4.44%
Face Detection	16	11.85%
Age Estimation	1	0.74%
Gender Estimation	1	0.74%
Child Nudity Detection	8	5.93%
Object Detection	5	3.70%
Face Presentation	1	0.74%
Nudity Blocker	3	2.22%
None of the above	13	963%
I do not use tools	5	3.70%
Technology Implemented by Video Processing Tools		
Skin Tone Detection	80	56.34%
Face Recognition	6	4.23%
Face Detection	16	11.27%
Gender Estimation	1	0.70%
Child Nudity Detection	10	7.04%
Object Detection	8	5.63%
Face Presentation	1	0.70%
Nudity Blocker	3	2.11%
None of the above	13	9.15%
I do not use tools	4	2.82%

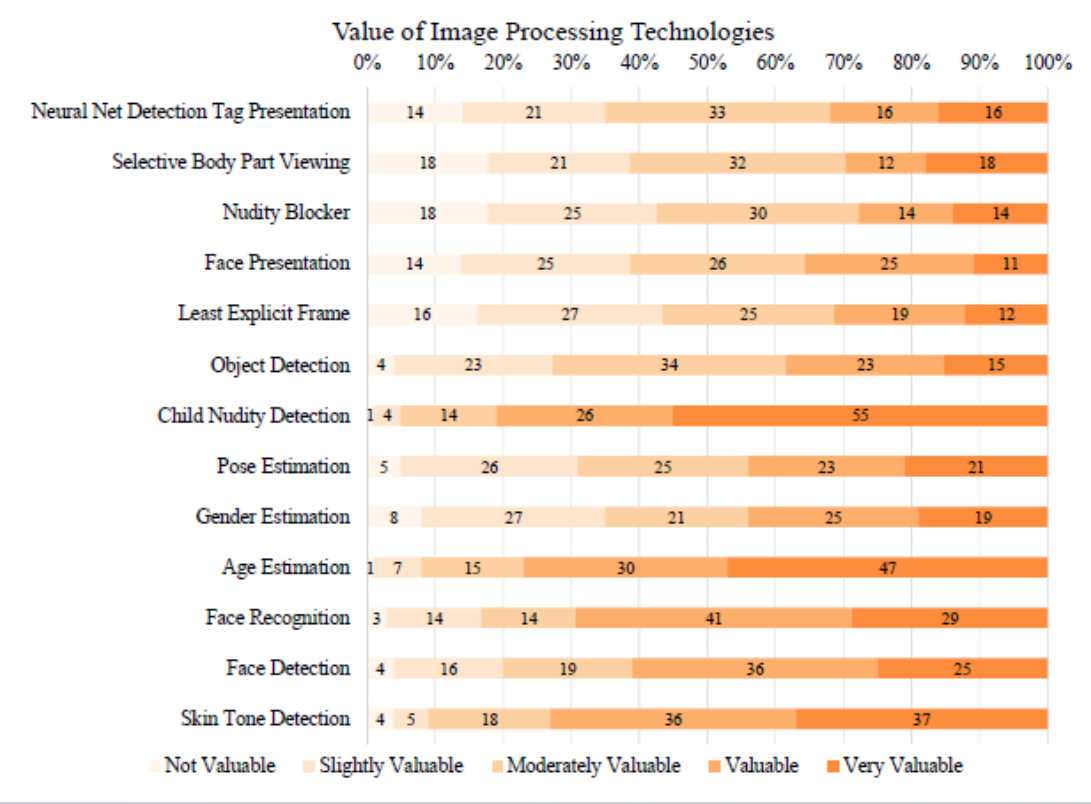
Technology – Usage Results

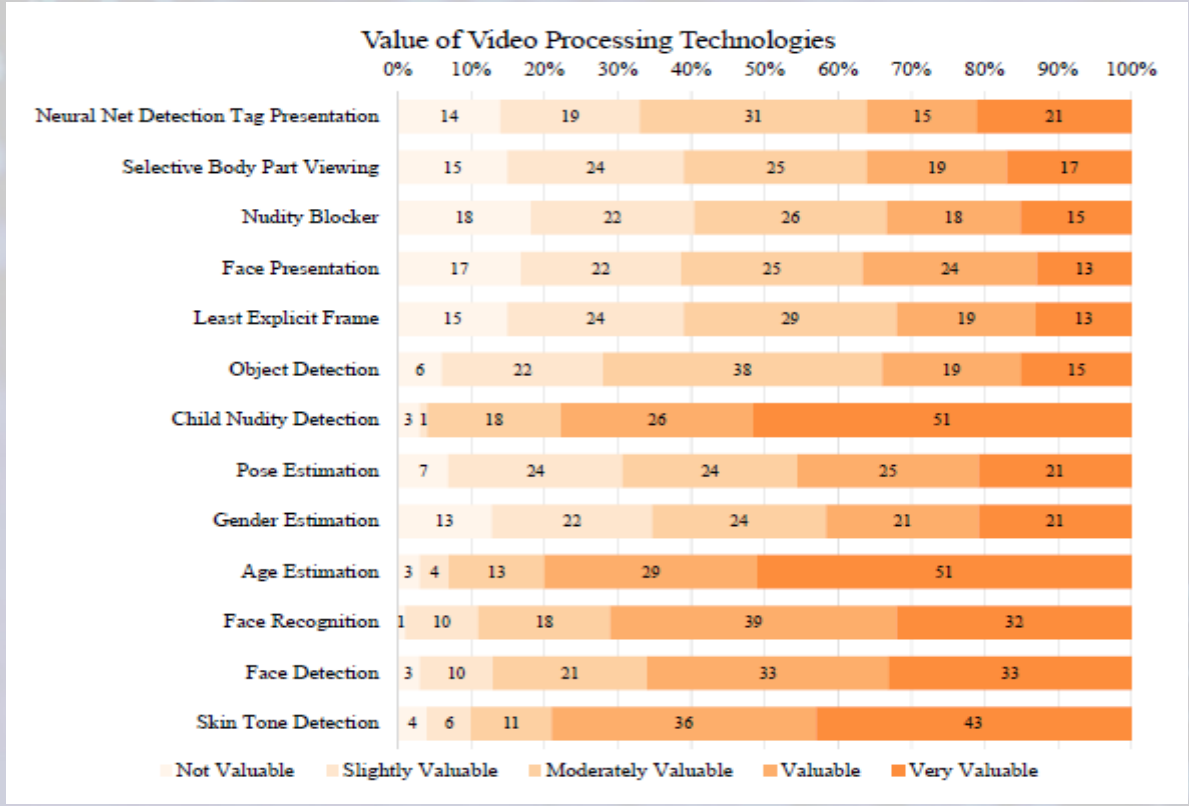
Technology Utilized by Respondents to Process Images		
Skin Tone Detection	67	52.34%
Face Recognition	7	5.47%
Face Detection	10	7.81%
Age Estimation	1	0.78%
Gender Estimation	1	0.78%
Child Nudity Detection	5	3.91%
Object Detection	6	4.69%
Face Presentation	1	0.78%
Nudity Blocker	3	2.34%
None of the options provided	16	12.50%
I do not use any technologies	11	8.59%
Technology Utilized by Respondents to Process Videos		
Skin Tone Detection	57	46.34%
Face Recognition	5	4.07%
Face Detection	9	7.32%
Age Estimation	1	0.81%
Gender Estimation	1	0.81%
Child Nudity Detection	6	4.88%
Object Detection	6	4.88%
Nudity Blocker	2	1.63%
None of the options provided	25	20.33%
I do not use any technologies	11	8.94%

Technology – Value, Ranking, and Preference

UNHcFREG

- Results indicate the implementation of filtering technologies have a higher value than safe-viewing technologies





Results - Workflow

- Limitations of current workflow →
  - Current tools and technology (28.77%)
  - Workload (20.55%)
  - Time (17.81%)
  - Resources (10.96%)
- Participant suggestions:
  - More resources (36.14%), better tools and technology (33.73%)
  - Adding more CSAM hash databases, make it possible for investigators to share hash values
  - More training for management, implement policies and standards that reflect current workflows

Results – Workflow, continued

- Valuable → 44.93%
- Very valuable → 34.78%
- Slightly to moderately valuable → 18.84%

Results – Workflow, continued

UNHcFREG

Type	Suggestion	Count	Total Count	Percentage
Resources	More analysts/examiners/investigators	2	3	16.67%
	More computers	1		
Time	Limit work hours of exposure to CSAM	1	1	5.56%
Tools & Technology	Ability to process large datasets faster	1	11	61.11%
	Add explanation of how automated process generated its result to check for false positives	1		
	Add report options	1		
	After rapid analysis, provide encryption and file hiding analysis to discover steganography attempts	1		
	Assign priority levels to cases based on known presence of CSAM	1		
	Automatically categorize and extract the content of any device (hard drive, usb key, etc.)	1		
	Faster acquisition and analysis	1		
	Implement safer presentation at an earlier stage	1		
	Quickly generate a report	1		
	Retain explicit format and safe presentation	1		
	Utilize reporting software with efficient filters to manually input the data necessary for a case	1		
Other	Availability of an expert witness to testify on behalf of the tool	1	3	16.67%
	System/workflow should allow for division of work into manageable tasks and collaborative/multi-user effort	1		
	Workflow should address data storage, network security, data retention and disposal, granular access and audit trail	1		

Challenges

- The number of participants responding to questions was not the same across the board due in part to intentional skipping of questions and early drop-out rates.
  - Resulted in questions having varying response counts
- Wording may have caused some questions to be misinterpreted by participants.
  - Non-related answers were provided by respondents.
- Some respondents were not consistent in their answers

Recommendations

- Include courses on AI, software design, engineering, and data science in academic DF programs
- Support research of CSAM investigations via a continuous funding model
- Encourage development and use of CSAM centered open source tools
- Establish and implement an up-to-date, standardized workflow
- Encourage non-practitioners to engage in training to better understand the work entailed in CSAM investigations, and the resources needed

Recommendations, continued

- Moving away from hash value identification, utilizing AI techniques to accurately identify CSAM
- Focus research on age estimation
- Develop technology that can identify and group images/video of the same victim and apply age estimation
- Employ novel filtering techniques beyond skin tone detection
- Leveraging novel techniques (e.g. object detection) to provide leads
- Develop technologies allowing for newly identified CSAM to be added to a shared repository between practitioners while adhering to laws

Acknowledgments

- MITRE for providing us the opportunity to work on this incredible endeavor. RESEARCH AGREEMENT NO. 121329
- Special thanks to:
  - All the digital forensic practitioners that took part in this study, sharing their experiences and insight.
  - Ahmed Alhishwan for his time and help designing the survey.
  - UNHcFREG students who assisted in the testing phase.
- Article Authors:
  - Laura Sanchez, Cinthya Grajeda, Ibrahim Baggili, and Cory Hall
- DFRWS:
  - For the opportunity to present this work, and a scholarship to make it possible

Contact Information & Questions?

Laura Sanchez lsanc3@unh.newhaven.edu

Cinthya Grajeda cgraj1@unh.newhaven.edu

Ibrahim Baggili ibaggili@newhaven.edu

Cory Hall clhall@mitre.org

http://www.unhcfreg.com/
https://www.mitre.org/