Landscape Study of **Digital Tools to Identify, Capture, and Analyze Digital Evidence in Technology-Facilitated Abuse Cases**

August
2021

NIJ Contact:
Steven Schuetz
Senior Physical Scientist
steven.schuetz@ojp.usdoj.gov

CJTEC Contacts:
Jeri D. Ropero-Miller, PhD, F-ABFT
Project Director, CJTEC
jerimiller@rti.org

Rebecca Shute
Innovation Advisor
rshute@rti.org

Criminal Justice Testing and Evaluation Consortium
A Program of the National Institute of Justice

TABLE OF CONTENTS

This report was authored by RTI International's Innovation Advisors—including Rebecca Shute, Emily Vernon, Rick Satcher, and Michelle Verastegui-Sanchez, with support from Molly O'Donovan Dix, Kristina Cooley, and Jonas Hall—and RTI's Division for Applied Justice Research—including Jeri Ropero-Miller, Michael Planty, and Lynn Langton. CJTEC would like to thank the National Institute of Justice's Steven Schuetz and Martin Novak for their valuable efforts in reviewing the document. We would like to thank Lt. Brendan Hooke of the Fairfax County Police Department for his guidance through the study and Alisa Matlin for her review of this document.

This project was supported by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, through award number 2018-75-CX-K003. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice. The products detailed in this landscape study are intended to show illustrative examples, not serve as an exhaustive list of commercially available products and products approaching market readiness. The inclusion of a product or company in this report does not represent NIJ's or CJTEC's recommendation, endorsement, or validation of product claims.

Suggested Citation:

Shute, R., Vernon, E., Satcher, R., Verastegui-Sanchez, M., Dix, M., & Planty, M. (2021). *Landscape study of digital tools to identify, capture, and analyze digital evidence in technology-facilitated abuse cases*. RTI International. Retrieved from https://cjtec.org/

EXECUTIVE SUMMARY

Landscape Study of Digital Tools to Identify, Capture, and Analyze Digital Evidence in Technology-Facilitated Abuse Cases

This landscape study provides an overview of tools that help the criminal justice community identify, capture, and analyze digital evidence in cases of technology-facilitated abuse (TFA). TFA is defined as crimes committed via digital means to cause emotional and physical harm to victims, such as cyberstalking, nonconsensual pornography, doxing, and swatting.[1] Although closely linked to traditional abuse tactics such as intimidation, threats, and humiliation, TFA happens over digital communication platforms such as websites, social network platforms, dating sites, mobile applications, blogs, online games, text messages, and email.

Technology-facilitated abuse leaves traces of digital evidence that can be captured for criminal investigations, but this evidence is often difficult to find and document. With input from experts in state and local cybercrime practitioners, digital forensics laboratories, and Internet Crimes Against Children (ICAC) task force members, CJTEC profiled tools that can help investigators ultimately collect evidence that leads to fair adjudication of TFA-related crimes. This landscape study covers tools used to capture digital evidence, which may be left by an abuser on community-based platforms or on the victim's or perpetrator's private devices. Beyond capture, these tools also can analyze aggregated data to map interactions, and patterns of activity. This report provides insights on topics and products relevant to TFA, as well as guidance for adopting tools which help in planning, reporting, managing, and presenting evidence in court. Although this is not an exhaustive product landscape, the study is intended to educate decision-makers within law enforcement, forensic crime laboratories, and the legal community about the available tools and considerations for use.

Criminal Justice Testing and Evaluation Consortium (CJTEC)

CJTEC is a program of the National Institute of Justice (NIJ), which uses research-based methodologies to enhance the capabilities of law enforcement, courts, and corrections agencies. As a consortium, CJTEC leverages expertise from varied criminal justice community stakeholders to understand and test technologies and practices in a variety of NIJ's research areas.

RTI International

RTI International is an independent, nonprofit research institute dedicated to improving the human condition. Clients rely on us to answer questions that demand an objective and multidisciplinary approach—one that integrates expertise across the social and laboratory sciences, engineering, and international development. We believe in the promise of science, and we are inspired every day to deliver on that promise for the good of people, communities, and businesses around the world. For more information, visit www.rti.org.

RTI leads CJTEC. CJTEC leverages RTI's expertise in criminal justice, forensic science, innovation, technology application, economics, data analytics, statistics, program evaluation, public health, and information science.

[1] Witwer, A. R., Langton, L., Vermeer, M. J. D., Banks, D., Woods, D., & Jackson, B. A. (2020). *Countering technology-facilitated abuse: Criminal justice strategies for combating nonconsensual pornography, sextortion, doxing, and swatting*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA108-3.html

Thank you to the various criminal justice community stakeholders and practitioners who provided insights and expertise.

Interviews with subject matter experts and end users helped to frame issues, consider solutions, and deliver key insights for decision-makers interested in implementing solutions. CJTEC sought feedback from varied stakeholders, including state and local cybercrime practitioners, digital forensics laboratories, ICAC task force members, and researchers to understand the value of specific tools and the practical implications of adoption and use.

JOSH BRUNTY
Associate Professor Cyber Forensics & Security
Marshall University
Huntington, WV

CHUCK COHEN
Vice President
The National White Collar Crime Center
Glen Allen, VA

JOAN DONOHUE
Director, Technical Solutions
Department of Defense Cyber Crime Center
Linthicum Heights, MD

JIM EMERSON
Chair of Computer Crimes and Digital Evidence Committee
International Association of Chiefs of Police
Alexandria, VA

DAVID FRATTARE
ICAC Commander
Cuyahoga County Prosecutor’s Office
Cuyahoga, OH

BARBARA GUTTMAN
Group Leader Software Quality Group
National Institute of Standards and Technology
Gaithersburg, MD

BRENDAN HOOKE
First Lieutenant
Fairfax County Police Department
Fairfax, VA

MITCH KAJZER
Director, Cyber Crimes Unit
Office of Prosecuting Attorney, St. Joseph County
Notre Dame, IN

CHRISTOPHER W. KELLY
Director, Digital Evidence Laboratory
Office of the Attorney General
Boston, MA

ROBERT KURTZ
Division Chief
Homeland Security Investigations Cyber Division
Washington, DC

TROY LAWRENCE
Sergeant, Digital Laboratory
Fort Worth Police Department
Fort Worth, TX

VANESSA MARTINUCCI
Director
North Carolina State Crime Laboratory
Raleigh, NC

JEFFREY REISING
Federal Bureau of Investigation Baltimore Cyber Task Force
Baltimore, MD

PETER STOUT, PhD
CEO/President
Houston Forensic Science Center
Houston, TX

MICHAEL YU
Detective Sergeant Electronic Crimes Unit
Montgomery County Police Department
Gaithersburg, MD

Key Findings

Technology-facilitated abuse is a growing challenge for investigators.

According to the Criminal Justice Priority Needs Initiative, TFA refers to "acts or courses of conduct facilitated through digital means that compromise the victim's privacy and cause them emotional, physical, or reputational harm."[2] The categorization of abuse includes acts such as cyberstalking, swatting, doxing, nonconsensual pornography, and sextortion. Abusers use technologies such as digital communication platforms and private devices in a way that publicly humiliates their victim, extorts them for money or favors, jeopardizes their safety, or instills fear through monitoring their activities.

TFA is prevalent; nationally representative surveys by the Data & Society Research Institute,[3] the Pew Research Center,[4] and the Anti-Defamation League (ADL)[5] have found that between 40% and 55% of Americans have been subject to some form of harassing behavior online. Although it takes place in a digital realm, this kind of abuse can inflict serious and tangible psychological trauma, harming victims' personal and professional reputation and disrupting relationships with friends, family, and colleagues. Abuse conducted digitally may lead to serious consequences such as in-person violence, self-harm, or even suicide.[6]

TFA may leave behind digital evidence that helps inform investigations.

When individuals abuse victims using technology, law enforcement may be able to capture digital evidence of these interactions to bring abusers to justice. Evidence such as text messages, emails, photos, videos, and social media activity can identify and document interactions between suspected abuser and victim. The use of technology in these crimes, however, can make identification and subsequent evidence collection challenging. TFA investigations are difficult because of the following:

- Despite the presence of case law for collection and admissibility of digital evidence, there is little knowledge about the impacts of the use of digital evidence on prosecutorial outcomes in TFA cases;
- Victims may be reluctant to report these crimes;
- Information stored in the cloud or through social media platforms is difficult to access;
- Access to information stored in the cloud or through social media platforms may be difficult to access;
- The plethora of digital platforms can make finding relevant evidence difficult;
- Cloud-based platforms and digital technologies (including communication platforms) are rapidly evolving, so many tools used in investigations can become obsolete without consistent updates;
- Investigations create large amounts of data, which may require additional resources to accommodate.

[2] Witwer, A. R., Langton, L., Vermeer, M. J. D., Banks, D., Woods, D., & Jackson, B. A. (2020). *Countering technology-facilitated abuse: Criminal justice strategies for combating nonconsensual pornography, sextortion, doxing, and swatting*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA108-3.html

[3] Lenhart, A., Ybarra, M., Zickuhr, K., & Price-Feeney, M. (2016, November). *Online harassment, digital abuse, and cyberstalking in America.* Data & Society Research Institute and the Center for Innovative Public Health Research. https://datasociety.net/wp-content/uploads/2016/11/Online_Harassment_2016.pdf

[4] Duggan, M. (2017, July 11). *Online harassment 2017*. Pew Research Center. https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

[5] Anti-Defamation League. (2019). *Online hate and harassment: The American experience*. https://www.adl.org/onlineharassment#survey-report

[6] Hinduja, S. & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research, 14(III)*, 206-221. https://cyberbullying.org/cyberbullying_and_suicide_research_fact_sheet.pdf

Digital tools can help investigators discover, document, and sift through relevant digital evidence.

There are a variety of tools available to uncover digital evidence in cases of abuse. While some may already be in use for digital forensics investigations, some offer value specific to searching and documenting digital evidence related to technology-facilitated abuse. This document provides an overview and examples of tools and resources as shown in Figure 1.

Digital Tools for Abuse Investigations

Tools to Identify and Capture Digital Evidence from Community-Based Sources

Active Monitoring Tools

- Tip lines and hotlines
- Crawler-based technologies
- Victim-provided evidence

Intelligence Gathering Tools

- Social media investigative tools
- Open-source aggregators
- Evidence documentation tools

Tools to Extract and Identify Digital Traces from Private Devices and Networks

Mobile Device Tools

- Password recovery
- Manual extraction
- Logical extraction
- Physical extraction

Hard Drive Tools

- File carving
- Data imaging

Cloud and Network Tools

Tools to Analyze Digital Evidence for Indicators of TFA

Advanced Searching Tools

Insights Generation Tools

Figure 1: Agencies investigating TFA can leverage tools to capture digital evidence from different sources, such as community platforms and private devices, and analyze the data collected for keywords and patterns.

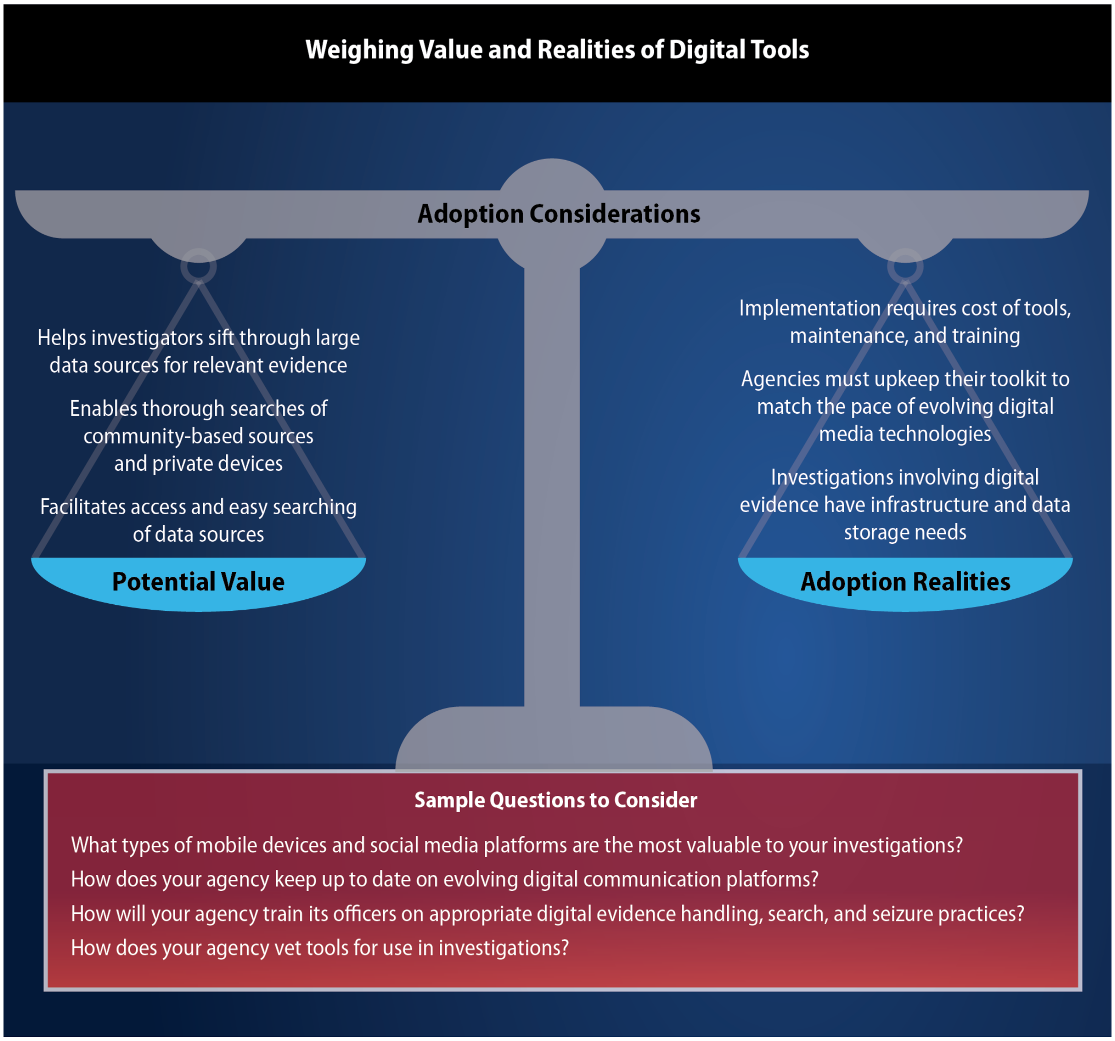
Active monitoring and intelligence-gathering tools help route important publicly available information to law enforcement. These tools are helpful in instances where abusers post content on public forums or online avenues to publicly shame or expose information on their victims. These tools can help identify where and when this abuse is happening, capture evidence of it occurring, investigate and possibly identify a perpetrator, identify potential threats, and help establish probable cause for search and seizure. These tools are often open-source or low-cost products, though some subscription-based aggregator platforms exist; investigators may need multiple products since most only focus on one platform.

Mobile devices, hard drives, and cloud and network access tools can help agencies document relevant digital evidence, identify where and when this abuse is happening, capture evidence of it occurring, investigate and possibly identify a perpetrator, identify potential threats, and help establish probable cause for search and seizure. These tools are helpful in instances where there may be enough preliminary evidence to justify a more thorough investigation of content found on a victim's or suspect's private devices. These tools can gather multiple types of data, including content stored locally or on a cloud-based application, metadata and artifacts indicative of abuse, and internet data and traffic entering and exiting a network. These tools are typically more expensive, and are often part of large digital forensics suites that extract data across computers and mobile device types and analyze in one platform.

Digital evidence investigations often lead to recovery of a large volume of information to sift through. These tools help agencies search large datasets and gather insights by establishing patterns of interactions and activity. Analysis products are useful in situations when an abuser may be harassing a victim multiple times, harassing victims within the same network, or using multiple devices. These tools are usually part of large digital forensic suites that have device extraction capabilities, though there are some photo-focused standalone products. Many of these products can also incorporate and manage evidence gathered from other tools (such as screenshots).

Investigators should plan for digital tool investment and training.

Agencies should weigh the value of these tools against their limitations when considering implementation. Like most digital evidence tools, adopting and implementing new tools for investigations involving TFA requires significant time and resource investments. This landscape study outlines key considerations and practical recommendations for procuring these tools, including testing, training, and ensuring legal capture and use of data, as summarized in Figure 2.



Weighing Value and Realities of Digital Tools

Adoption Considerations

Helps investigators sift through large data sources for relevant evidence

Enables thorough searches of community-based sources and private devices

Facilitates access and easy searching of data sources

Potential Value

Implementation requires cost of tools, maintenance, and training

Agencies must upkeep their toolkit to match the pace of evolving digital media technologies

Investigations involving digital evidence have infrastructure and data storage needs

Adoption Realities

Sample Questions to Consider

What types of mobile devices and social media platforms are the most valuable to your investigations?

How does your agency keep up to date on evolving digital communication platforms?

How will your agency train its officers on appropriate digital evidence handling, search, and seizure practices?

How does your agency vet tools for use in investigations?

Figure 2: Agencies must weigh the value of tools for TFA-related investigations against their limitations in light of considerations that could enable or hinder adoption.

Agencies should understand that...

- There is no "magic bullet" that accomplishes all necessary jobs in a case with digital evidence. Investigators may use a wide variety of tool types during an investigation involving abuse through digital means. Many products have multiple functions or search multiple device types.
- Many tools may provide value for other cases where digital evidence may uncover key clues, and may be already in use in supporting units or crime laboratories.
- Agencies should train users not only on effective use of the tool, but also on writing inclusive warrants, obtaining evidence in a legally defensible manner, and correctly handling seized evidence.
- Tool implementation requires planning for ensuring data integrity, storing data, and vetting or validating the tools.

Landscape Research Methodology

To conduct this study, CJTEC used the following iterative process:

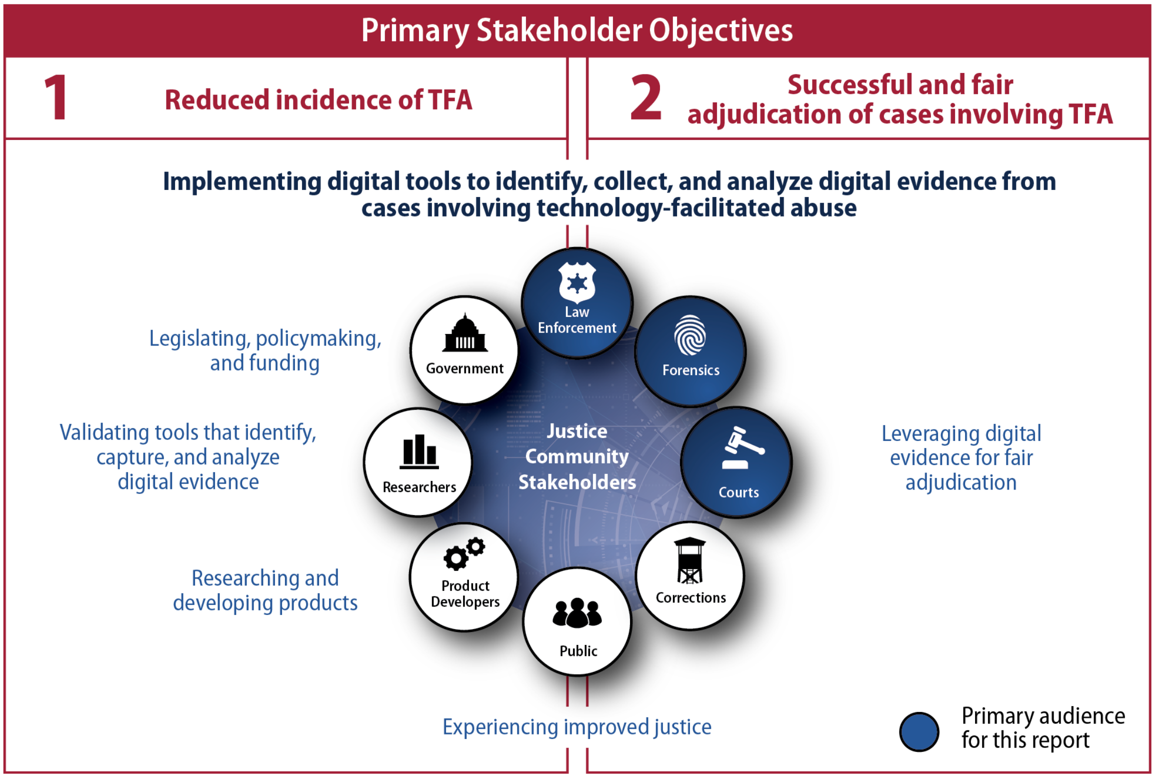
1. Participated in NIJ's Priority Criminal Justice Needs Initiative meeting on identifying and responding to internet-enabled harassment and considered technology-related needs. Following the meeting, CJTEC considered the topics and built forward with additional interviews with key stakeholders.
2. Consulted with experts, practitioners, and other key stakeholders:
   - Discussed categories of tools that capture digital evidence relevant to TFA with end users in law enforcement agency task forces, ICAC units, local and federal digital forensics laboratories, the National Institute of Standards and Technology (NIST), and experts from associations such as the International Association of Chiefs of Police (IACP).
   - Consulted subject matter experts, such as Lt. Brendan Hooke, Fairfax Police Department, and Martin Novak, an NIJ Senior Computer Scientist, to prioritize and organize key tool types used in investigations involving TFA.
3. Scanned extant literature and market:
   - Consulted secondary sources, including literature from NIST's Computer Forensics Tools Testing Program and research publications.
   - Used both secondary and primary research methods to identify tools of interest. Specifically researched relevant tools based on feedback from expert interviews. Considered technology and market knowledge from general digital forensics applications.
4. Consolidated and synthesized information:
   - Synthesized tools outlined by primary and secondary research into categories corresponding to key "jobs" that digital forensic investigators must complete in cases involving TFA, as well as key considerations for appropriate and legally defensible documentation and use of digital evidence.

CJTEC would like to remind decision-makers considering these technologies that implementation should be considered with respect to existing agency policies and procedures, which might not directly align with solutions/products. Standard operating procedures (SOPs) should be reviewed and updated as needed when considering the implementation of new technology. Consulting the IACP Law Enforcement Policy Center to review leading practices may serve as a guide for agencies updating SOPs. This landscape provides examples of products and research efforts as illustrative examples and is not intended to be a comprehensive market summary of available products.

CONTEXT

Technology-facilitated abuse is a growing challenge with serious consequences for its victims.

The advent of digital technologies has transformed the way the world connects and interacts. Through a mobile phone or computer, individuals can communicate with friends, family, and strangers around the world through digital media, using avenues such as software applications, messaging services, and online games. Although digital advances have affected our culture, enterprises, and social lives significantly, they have also changed the way individuals commit crimes. Increased interconnectivity has provided abusers with a means to digitally track, threaten, and harass their victims. As shown in Figure 3, many stakeholders within the criminal justice system play a role in identifying and reducing crimes involving this kind of technology-facilitated abuse.



Primary Stakeholder Objectives

1 Reduced incidence of TFA

2 Successful and fair adjudication of cases involving TFA

Implementing digital tools to identify, collect, and analyze digital evidence from cases involving technology-facilitated abuse

Justice Community Stakeholders
Law Enforcement
Forensics
Courts
Corrections
Public
Product Developers
Researchers
Government
Legislating, policymaking, and funding
Validating tools that identify, capture, and analyze digital evidence
Researching and developing products
Experiencing improved justice
Leveraging digital evidence for fair adjudication
● Primary audience for this report

Figure 3: As digital communication technologies have played an increasing role in cases of abuse, the criminal justice community has responded to address crimes involving TFA.

Abusers can use technology to harm victims in many different ways.

TFA refers to acts carried out by digital means to cause emotional, physical, or reputational harm to a victim.[7] Abusers may leverage technologies such as mobile phones, tablets, or computers and means such as websites, social network platforms, dating sites, web applications, online games, instant messages, and email. TFA includes a variety of crimes such as cyberbullying, cyberharassment, cyberstalking, brigading, cyberthreats, sextortion, nonconsensual pornography, doxing, and swatting. Perpetrators may conduct these crimes to:

- **Humiliate the victim:** Abusers may harm a victim's reputation by disseminating (or threatening to disseminate) embarrassing or sensitive information to the community without their consent. They may also impersonate the victim to cover their tracks or further damage a victim's reputation. This category includes crimes such as cyberbullying and nonconsensual pornography dissemination.
- **Entertain themselves or build their reputation:** Abusers may share cyberbullying content or nonconsensual pornography to establish their status among peers.
- **Instill fear in their victim:** Abusers may cyberstalk their victims, monitoring their activities for the purpose of extortion or exerting control over them.
- **Damage an individual's professional reputation:** Abusers may disseminate information or impersonate an individual in a way that jeopardizes the victim's livelihood, such as leaving false ratings on a review website or swatting them. These tactics may lead to financial losses.
- **Jeopardize a victim's safety:** Abusers may put victims at risk for physical abuse or violence by doxing them and swatting them, whereby an abuser anonymously places a false report to emergency services.
- **Extort the victim:** Abusers may demand money or favors from a victim and threaten to harm the victim physically or emotionally if they fail to comply. This category includes crimes such as sextortion.

Examples of Technology Facilitated Abuse

The following are definitions for the predominant forms of TFA in cases investigated by law enforcement.

Cyberbullying: A form of unwanted, aggressive behavior that generally involves a real or perceived power imbalance, is repeated or has the potential to be repeated over time, and takes place using electronic communications technology.

Cyberstalking: The repeated use of electronic communications technology to stalk a person or group. Cyberstalking is distinguished from cyberharassment in that it poses a credible threat of harm to the victim.

Doxing: The use of electronic communications technology to publish personally identifiable information (e.g., name, address) about an individual without their permission.

Nonconsensual pornography: The distribution of nude/sexually explicit images or videos of an individual without their consent. These images/videos may have been consensually produced or obtained in the context of an intimate relationship, or they may have been nonconsensually produced or obtained (e.g., the use of secret cameras, hacking).

Sextortion: A form of cyber extortion in which offenders demand that victims provide them with sexual images, sexual favors, or other things of value and threaten to harm or embarrass the victim if they fail to comply.

Swatting: The false reporting of an emergency to public safety agencies for the intent of getting a "SWAT team" response to a location where no emergency exists.

Please visit the Glossary section of this report for additional information and resources regarding the types of TFA investigated by law enforcement.

[7] Witwer, A. R., Langton, L., Vermeer, M. J. D., Banks, D., Woods, D., & Jackson, B. A. (2020). *Countering technology-facilitated abuse: Criminal justice strategies for combating nonconsensual pornography, sextortion, doxing, and swatting*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA108-3.html

Abuse in the digital realm has real-world impacts.

Recent studies suggest that abuse using digital media is growing in prevalence.[8, 9] Nationally representative surveys conducted by the Data & Society Research Institute,[10] the Pew Research Center,[8] and ADL[9] over the last few years have found that between 40% and 55% of Americans have been subject to some form of abusive behavior online.

- An estimated 18% to 37% of Americans have experienced severe online harassment, defined to include physical threats, sexual harassment, stalking, and sustained harassment.[9]
- One in eight American social media users has either been threatened with or been the victim of nonconsensual pornography.[11]
- 7% of U.S. adults have had explicit images of themselves shared without their consent.[8]
- 5% of U.S. middle and high schoolers report having been victims of sextortion.[12]
- Swatting incidents are estimated to have risen from around 400 in 2011 to over 1,000 annually in the past three years.[13]
- 20,604 victims in the United States reported online harassment and threats of violence to the Internet Crimes Complaint Center in 2020.[14]

Although criminal activity from this abuse takes place via digital means, the effects on its victims are tangible. Additionally, the abuse can escalate from digital interaction to in-person victimization; however, little is known about the markers of escalation. While just 3% of U.S. internet users report that an online abuser attempted to harm them in person,[10] research suggests that abuse via digital means is not an uncommon tactic in the perpetration of stalking and interpersonal violence.[15, 16] Text message records have played key roles as digital evidence in trials involving intimate partner violence, including those that escalated to suicide.[17] According to the Bureau of Justice Statistics, one in four stalking victims reported being cyberstalked through technology, such as email or instant messaging.[18] The growing, dangerous nature of this abuse necessitates development of tools and resources to address these crimes.

[8] Duggan, M. (2017, July 11). *Online harassment 2017*. Pew Research Center. https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

[9] Anti-Defamation League. (2019). *Online hate and harassment: The American experience*. https://www.adl.org/onlineharassment#survey-report

[10] Lenhart, A., Ybarra, M., Zickuhr, K., & Price-Feeney, M. (2016, November). *Online harassment, digital abuse, and cyberstalking in America*. Data & Society Research Institute and the Center for Innovative Public Health Research. https://datasociety.net/wp-content/uploads/2016/11/Online_Harassment_2016.pdf

[11] Eaton, A. A., Jacobs, H., & Ruvalcaba, Y. (2017). *2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration*. Cyber Civil Rights Initiative, Inc. https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

[12] Patchin, J., & Hinduja, S. (2018). Sextortion among adolescents: Results from a national survey of U.S. youth. *Sexual Abuse: A Journal of Research and Treatment*. https://doi.org/10.1177/1079063218800469

[13] Swatting could become a federal crime. (2019, January 12). *The Economist, 430*(9125), 23, https://www.economist.com/united-states/2019/01/12/swatting-could-become-a-federal-crime

[14] Internet Crime Complaint Center. (n.d.). *2019 internet crime report.* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[15] King-Ries, A. (2011). Teens, technology, and cyberstalking: The domestic violence wave of the future. *Texas Journal of Women and the Law, 20*(2), 131–164.

[16] Marganski, A., & Melander, L. (2018). Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *Journal of Interpersonal Violence, 33*(7), 1071–1095.

[17] Felton, L (2019). In court cases involving domestic violence, text messages can be key—to winning or losing. *The Lily.* https://www.thelily.com/in-court-cases-involving-domestic-violence-text-messages-can-be-key-to-winning-or-losing/

[18] Office of Justice Programs, Bureau of Justice Statistics. (2021). *Stalking victimization, 2016*. https://bjs.ojp.gov/library/publications/stalking-victimization-2016

Technology-facilitated abusers leave behind digital evidence of their activities.

Criminal activities, including abuse carried out via technology, may leave digital evidence of an abuser's actions. Different types of abusive activities leave behind different types of data that may be acquired as digital evidence, as shown in **Figure 4**. Some abusive activities, such as cyberbullying and doxing, are meant to broadcast sensitive or embarrassing information to the public or smaller online communities, whereas interactions specific to cyberstalking or sextortion may only be between a victim and the abuser. Digital evidence can bring these abusers to justice. Akin to traditional crime scene investigators who analyze the physical scene for traces of evidence to understand events that transpired, investigators, digital forensics analysts, and other experts identify, retrieve, store, and analyze electronic data related to TFA. Digital evidence can be any information stored or transmitted in binary form that can be captured for possible use in an investigation.[19] Evidence from text messages, chat rooms, mobile applications, emails, photos, videos, and social media can help identify and document interactions between suspected abuser and victim.

Digital Evidence from Technology-Facilitated Abuse

Type of Abuse	Mode of Abuse	Intent of Abuser	Examples of Digital Evidence
Cyberbullying, Cyberhate, Cyberharassment	• Derogatory, insulting, or threatening posts made in a public or private forum, like social media or content-sharing platforms (Facebook, YouTube) • May include account takeovers, abusers posing as the victim	• Publicly shame and ridicule victims • Cause victims to fear for their personal safety (whether threats are credible or not) and other psychological distress	• Documented interactions on social media sites, public or private forums • Screenshots by victims or witnesses • Fake social media accounts • Text messages, emails
Cyberstalking, Cyberthreats	• Unwanted or unsolicited emails, phone calls, text messages, or other forms of electronic communication directed to a TFA victim that implicitly or explicitly suggests knowledge of the victim's identity or personal life • Use of apps to monitor an individual's location or activities	• Monitor the victim's activities • Create fear for the victim's well-being • Disrupt the victim's personal affairs, relationships, or career • Cause physical harm to the victim	• Phone-based data calls, texts, emails • Social media platform-based messages • Images • Records of transactions of harassment (like sending unwanted solicitors to victims) • Network traffic
Sextortion, Nonconsensual Pornography, Child Pornography[20]	• Extortion, blackmail, sexual abuse, or revenge enabled by the possession of sexually explicit images, obtained through either consensual (in a relationship) or nonconsensual means by the abuser (coercion) • Abusers may also share sexually explicit images of minors	• Cause public shame, damage to the reputation of the victim • Disrupt the victim's personal life • Sexually abuse or assault the victim • Personally gain something (monetary, reputational) • Entertain themselves or their friends	• Images on social media platforms or on physical devices
Doxing, Brigading, Swatting	• Publishing of personally identifiable information (name, address, phone, place of work, etc.) that includes a call to action for other would-be abusers • Putting victims' lives in danger using false pretenses	• Cause physical or psychological harm to, abuse of, harassment of, or death of the victim	• Documented interactions on social media sites

Figure 4: Abusers may leverage technology to humiliate, exploit, instill fear in, or jeopardize the physical safety of their victims. Different types of TFA leave different digital traces that can be captured in an investigation.

[19] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (2021). *U.S. Digital evidence and forensics*, https://nij.ojp.gov/digital-evidence-and-forensics

[20] Child pornography is a serious separate issue from TFA that affects its victims in a different way and requires specific expertise to address. However, CJTEC chose to note this as a potential example because minors may share explicit photos of other minors.

Cases involving TFA pose unique challenges for digital evidence collection.

Investigators working on cases that involve TFA may leverage common tools and processes used in other digital forensics applications. While digital forensics workflows differ by laboratory/agency because of varied capabilities, casework, tools, and resources, investigators typically follow a process similar to NIST's four step procedure, which includes:[21]

1. Identifying, collecting, and preserving the data from the information source
2. Processing the data to flag relevant digital evidence
3. Analyzing to glean insights from relevant keywords, or patterns of activity
4. Reporting results of the analysis

Although abuse via technology is becoming more common, the nature of these crimes makes identification and subsequent collection, processing, and analysis of evidence quite challenging.

Law enforcement has few precedents for recognizing and prosecuting crimes related to abuse via technology.

The criminal justice community, like the rest of the world, is adapting to the impacts of digital technology adoption. The current legal climate is slowly getting up to speed, from court cases to legislation. Although no current federal or state laws address all aspects of TFA, there is a trend of legislation addressing criminal acts via technology. As of 2019, 46 states and Washington, D.C., had passed laws prohibiting dissemination of nonconsensual pornography, 26 states had passed laws prohibiting sextortion, and Kansas had passed an antiswatting law.[22] Federal legislation related to telecommunications (18 U.S.C. 875[c] and 47 U.S.C. 223) has been applied to cyberstalking in federal cases.[23] According to the Cyberbullying Resource Center, at least 30 states have enacted cyberbullying laws that mention electronic forms of harassment.[24] Although case law has helped set legal precedents for the general collection and admissibility of digital evidence, there is little knowledge about the impacts of the use of digital evidence on prosecutorial outcomes in TFA cases.[25]

The journal article "Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration" examines federal criminal cases using computer forensics that have implications for search and seizure, admissibility, and precedents. Of 45,030 federal criminal cases affirmed or reversed between 2010 and 2015, only 147 were directly related to legal issues in digital evidence.

[21] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

[22] Greenberg, P. (2019, August). *Fighting revenge porn and 'sextortion.'* National Conference of State Legislatures, 27(29). https://www.ncsl.org/research/telecommunications-and-information-technology/fighting-revenge-porn-and-sextortion.aspx

[23] Blanch, J. L., & Hsu, W. L. (2016). An introduction to violent crime on the internet. *United States Attorneys' Bulletin, 64*, 2-11. https://www.justice.gov/usao/file/851856/download

[24] Hinduja, S. & Patchin, J. (2018). *State cyberbullying laws: A brief review of state cyberbullying laws and policies.* Cyberbullying Research Center. https://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf

[25] See Lorraine v. Markel American Insurance Company (241 F.R.D. 534) and Riley v. California (573 U.S. 373).

Abuse victims may not recognize the role of digital evidence in cases of TFA.

Law enforcement, as well as the public, is working to better understand and react to cases involving TFA. Victims themselves may not know that law enforcement can help; because these crimes are meant to humiliate or instill fear, victims may be reluctant to report this crime or may not even know that they can receive assistance from law enforcement. Even if they seek assistance, they may not pursue the case to keep the details of this abuse out of the public eye. Victims may lack awareness of best practices to capture evidence of TFA and pursue help; they can be valuable sources of evidence, but harassment victims may delete evidence in an effort to mitigate the abuse. In RAND's Countering Technology-Facilitated Abuse report, an expert panel identified the priority need for trauma-informed resources for victims (and their families) to identify and respond to TFA.

Access to key evidence can be blocked by cloud-based providers, social media platforms, and encryption.

Perpetrators often use commonly available platforms to abuse their victims, such as social media outlets, text messages, and emails. Although some of these data may be available on a victim's or an abuser's devices, most of this information (including deleted information) may be stored by cloud providers employed by the social media platforms. In many circumstances, law enforcement must establish legal authority to access these data, which requires a well-drafted warrant with language that specifically speaks to accessing data stored in the cloud. Even with a warrant, access depends on the cooperation of the companies that use or act as the cloud storage mechanism for the data, and they may not be obligated to comply. These servers may be based outside of the United States, making access in another jurisdiction more complicated. Ensuring a proper chain of custody, verifying authenticity of the data in a multi-user environment, and sifting through large amounts of data make forensic investigations involving cloud-based platforms extremely challenging. The NIST Cloud Computing Forensic Science Working Group has listed some of the key challenges faced by the forensic community responding to incidents in a cloud-computing environment. Some highlighted challenges include the following:

- **Architecture**—Enabling accurate and secure provenance for preserving the chain of custody
- **Data collection**—Locating forensic artifacts in large, distributed, and dynamic systems
- **Analysis**—Correlating forensic artifacts across and within cloud providers
- **Legal**—Identifying and addressing issues of jurisdictions for legal access to data and lack of effective channels for international communication and cooperation during an investigation
- **Standards**—Operating with a lack of minimum/basic SOPs, practices, and tools; lack of interoperability among cloud providers; and lack of test and validation procedures[26]

Data stored by social media platforms are protected under the Stored Communications Act, a federal statute that prohibits electronic communications providers from sharing data about an individual. Although an exception to this prohibition includes disclosure to law enforcement in the case that the electronic communication pertains to a crime, providers may challenge these subpoenas and access may differ by state.[27] For example, in the 2018 California Supreme Court case *Facebook, Inc. v. Superior Court r417 P.3d 725*, 74, the court ruled that the Stored Communications Act exception to law enforcement applied to public posts, not private groups.[28]

[26] National Institute of Standards and Technology. (2020, August). *NIST cloud computing forensic science challenges*. https://csrc.nist.gov/publications/detail/nistir/8006/final

[27] Kentucky Bar Association. (2019). *Text me, maybe? Discovery of electronic communications under the Stored Communications Act*. 2019 KBA Annual Convention. https://cdn.ymaws.com/www.kybar.org/resource/resmgr/2019_convention/materials/tex_me,_maybe_discovery_of_e.pdf

[28] Landis, J., & Page, L. (2020, October 5). *Content with subpoena? CA Supreme Court says yes*. ZwillGenBlog. https://www.zwillgen.com/litigation/content-with-subpoena-ca-supreme-court-says-yes/

Although agencies may be granted access to a suspect's devices through a search warrant, they may be hindered by increasing "warrant-proof encryption" by service providers, device manufacturers, and software applications. During the 2015 San Bernardino terrorist attack, the Federal Bureau of Investigation (FBI) served Apple with a federal court order demanding that Apple lift security restrictions to ultimately access content on the terrorist's iPhone.[29] Apple refused to comply and challenged the matter in court and Congress, and the FBI eventually accessed the data with the help of a third party. As more companies adopt these encryption strategies, law enforcement must consider alternative approaches to accessing data from private devices.

Digital communication platforms are constantly evolving.

Mobile phones, wearables, computers, and cloud-based social media platforms, common tools of TFA, are rapidly evolving and expanding capabilities. For example, today's mobile phones have taken on multiple roles beyond enabling audio calls and serve as a camera, a wearable device, and a way to control other devices connected through the Internet of Things. Constantly evolving technology has provided abusers with even more ways to contact, track, and threaten the safety of a victim.

The digital forensics community has developed technologies to extract data from devices such as mobile phones, tablets, and hard drives, but it has been challenging to keep the pace of development of these tools with the technology advancements of these devices and applications. Forensic tools to retrieve information may be made obsolete with device or application software updates. Vendors that offer forensic tool suites must keep apprised of and react to these updates.

Law enforcement must also maintain awareness of new or popular communication platforms to understand potential sources of digital evidence; understanding how these platforms work, how users interact, and what kinds of data are stored on these applications can help agencies identify and collect evidence more quickly. Maintaining this awareness may require consistent technology and trend monitoring. For example, school resource officers may lean on students or parents to gain an understanding of today's most popular messaging service or content generation platform.

TFA investigations, like other types of digital forensics investigations, may be resource intensive.

The significant data associated with digital investigations may be difficult for agencies to manage. Law enforcement agencies have a finite amount of network storage space that may quickly be consumed by the volume of data in digital investigations. Bandwidth limitations can also hinder the ability of agencies to quickly upload and download data gathered in investigations. These challenges may require additional investment to create more server space or other external storage measures.

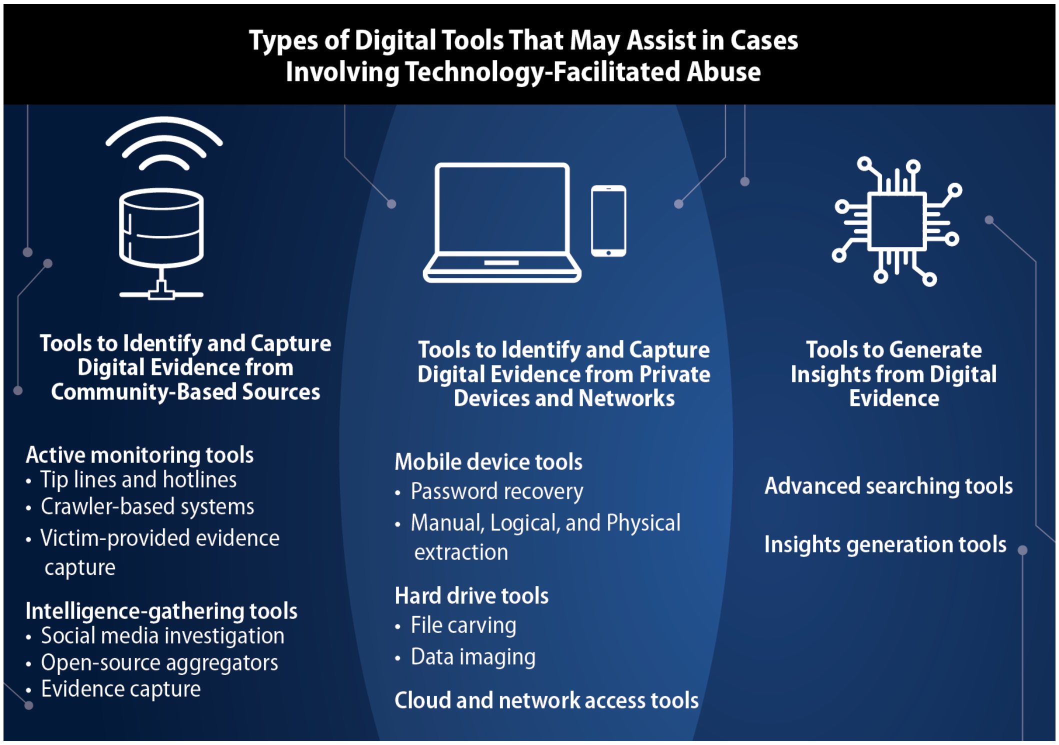
Beyond server space, smaller agencies may not have the ability to dedicate enough personnel to these investigations, which may require sifting through large amounts of data. Training staff on current and new forensics tools and trends in digital communication platforms used by the general public, both of which are evolving constantly, will improve TFA outcomes.

[29] Selyukh, A. (2016, December 3). *A year after San Bernardino and Apple-FBI, where are we on encryption?* All Tech Considered. https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption

TOOL LANDSCAPE

Digital tools can help investigators uncover relevant digital evidence and draw insights from disparate data sources.

In abuse cases, investigators have a responsibility to search for, identify, capture, and analyze potentially relevant traces of interactions between abusers and victims. Digital forensics tools and techniques, which can be used at multiple steps during the digital forensics process, may be able to help investigators find and document this evidence. Many tools highlighted in this landscape study are used in a variety of other digital crimes but also apply to TFA. These tools help investigators find digital evidence in large datasets, capture evidence of abusive interactions between the abuser and victim, and demonstrate a pattern of interactions or activity. Figure 5 profiles the types of tools, and Figure 6 shows how investigators may use these tools collectively in a case involving TFA.



Types of Digital Tools That May Assist in Cases Involving Technology-Facilitated Abuse

Tools to Identify and Capture Digital Evidence from Community-Based Sources

Active monitoring tools
- Tip lines and hotlines
- Crawler-based systems
- Victim-provided evidence capture

Intelligence-gathering tools
- Social media investigation
- Open-source aggregators
- Evidence capture

Tools to Identify and Capture Digital Evidence from Private Devices and Networks

Mobile device tools
- Password recovery
- Manual, Logical, and Physical extraction

Hard drive tools
- File carving
- Data imaging

Cloud and network access tools

Tools to Generate Insights from Digital Evidence

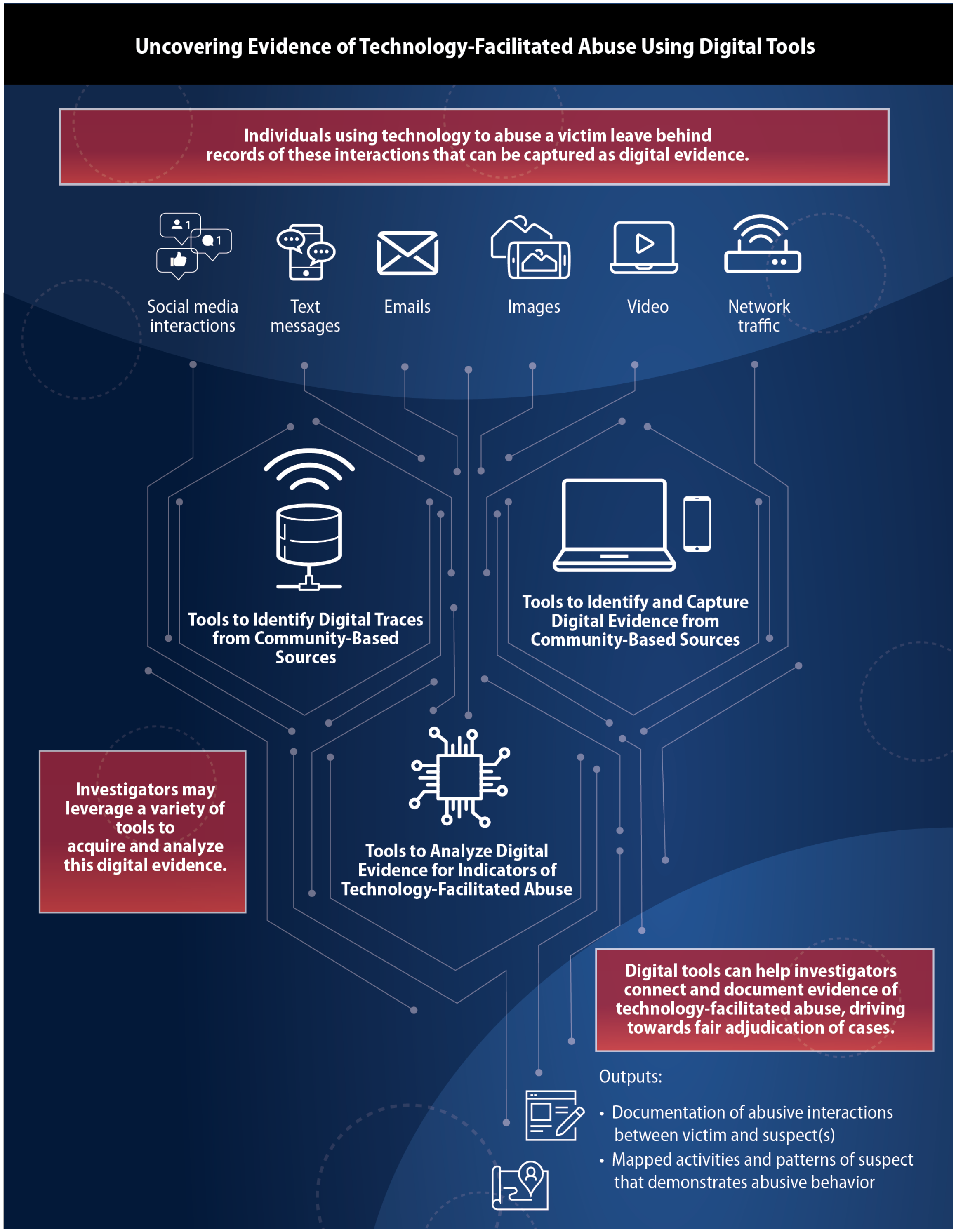
Advanced searching tools

Insights generation tools

Figure 5: Tools can augment an investigator's workflow in TFA-related investigations by identifying and gathering digital evidence from community-based sources or private devices and analyzing the evidence to glean valuable insights for the case.

This report is organized to consider tools that help with community-based platforms, private devices, and analysis; specifically:

- Community-based platforms (e.g., Facebook, Twitter): active monitoring and intelligence-gathering, including online "eyewitnesses" to abusive activity;
- Private devices and connections (e.g., mobile devices, hard drives, and cloud and network access): accessing and capturing digital evidence;
- Analysis: searching large datasets and establishing patterns of interactions and activity.



Uncovering Evidence of Technology-Facilitated Abuse Using Digital Tools

Individuals using technology to abuse a victim leave behind records of these interactions that can be captured as digital evidence.

Social media interactions
Text messages
Emails
Images
Video
Network traffic
Tools to Identify Digital Traces from Community-Based Sources
Tools to Identify and Capture Digital Evidence from Community-Based Sources
Tools to Analyze Digital Evidence for Indicators of Technology-Facilitated Abuse

Investigators may leverage a variety of tools to acquire and analyze this digital evidence.

Digital tools can help investigators connect and document evidence of technology-facilitated abuse, driving towards fair adjudication of cases.

Outputs:

- Documentation of abusive interactions between victim and suspect(s)
- Mapped activities and patterns of suspect that demonstrates abusive behavior

Figure 6: Investigators can leverage a combination of digital tools to identify, document, and gain important insights from digital evidence in cases involving TFA.

Community-based platforms are a rich source of digital evidence.

In cases involving TFA, abusers may intend to harm their victims by posting embarrassing, false, or private information to the public or a community or falsely impersonating them. Communities play a key role in these crimes; abusers may cyberbully their victims to publicly ridicule or shame them or "dox or swat" them by posting personal details such as their address, compromising their security. Intelligence from community-based platforms, such as social media websites, electronic service providers, and public networks, can offer helpful insights to law enforcement. These sources can be used to identify where and when this abuse is happening, capture evidence of it occurring, investigate and possibly identify a perpetrator, identify potential threats, and help establish probable cause for search and seizure.

Investigators can leverage both active monitoring tools, which route investigative leads and relevant community-based information to law enforcement, or intelligence-gathering tools, which can help investigators search for evidence online.

Active Monitoring Tools

Investigators are often working against the clock in TFA cases. The quicker investigators can react, the more likely they will be able to discover or recover key digital evidence. Active monitoring tools, including those profiled in **Figure 7**, serve as channels by which law enforcement can route important information. The various forms include:

Tip Lines and Hotlines

Tip lines leverage and route community, vendor, and law enforcement–gathered intelligence to agencies that can further investigate if needed. Agencies can tap into readily available sources to respond to complaints and can leverage information aggregated from these tip lines to quickly understand and address abuse. These information sources can be real-time information sources, such as 911 or domestic violence hotlines, which enable rapid documentation and response. While serving as an easy method for the community to route important investigative leads, the ease of these systems may also serve as a deterrent for future TFA.

Tip lines can also provide value at the state or local level. Agencies often partner with school systems to monitor cyberbullying, threats, and other forms of TFA. These information sources can be as rudimentary as phone-based systems, where the receiver manually records the information, or as advanced as anonymized reporting through multiple avenues (phone, online portal) that can aggregate information and help identify possible abuse patterns. Tools that enable the community to send documentation of TFA (such as screenshots) are especially helpful.

The investment of setting up a tip line may be worth the dividends in intelligence gathering. Consult the NIJ publication School Tip Line Toolkit: A Blueprint for Implementation and Sustainability for more information.

Crawler-Based Systems

A web crawler is a program that methodically searches the internet, stores the data, and queries it. These programs are part of the fundamental technology behind search engines like Google and Bing, which are valuable tools to an investigator, and can be used to passively search specific sites and search the web for possible abusive content. Agencies can take advantage of search engine web crawlers by using readers for really simple syndication (RSS) feeds to automatically push updates of relevant content from chosen web pages or search parameters. Investigators can use crawlers to identify where an abuser has been impersonating or doxing a victim. These tools automatically search leads given by tip lines, reports, and other information sources to quickly inform investigators of potential leads.

Victim-Provided Evidence Capture Applications

In cases involving TFA, the victim and online eyewitnesses can play a key role in collecting relevant evidence. Properly documented evidence in real time, such as screenshots of abuser activity, can capture evidence of these interactions, even if they are later deleted by an abuser. Agencies can encourage the community to screenshot and save evidence of abuse. Agencies can also recommend software applications to help victims document and share digital evidence. For example, DocuSAFE is a free phone application that serves as a tool to store photos, screenshots, and video documentation of abuse, and share with law enforcement. Developed initially as a tool for victims of domestic violence, DocuSAFE may be helpful for any victims experiencing harassing phone calls, threatening social media posts, or other forms of abuse. In addition to providing these applications to victims, law enforcement should continue educating the public about the importance of documenting these instances of abuse and routing this information to authorities when appropriate.

Tools to Actively Monitor Abuse

Category and Information Gathered	Benefits	Limitations	Example Products
Tip Lines and Hotlines: Community and electronic service provider information that suggests evidence of TFA happening, keeps agencies apprised of crime trends	• Nationwide tip lines can offer key aggregated insights for agencies • They can leverage a wide range of community and nationwide "eyes" on TFA • Participation in nationwide tip lines is free to agencies	• Local lines are often rudimentary • Tip lines may have limited ways to report and be unable to identify patterns of activity	The FBI's IC3 allows victims of internet crimes spanning a wide range of activities, including blackmail and harassment, to file a complaint, which is routed to the appropriate jurisdiction. The National Center for Missing and Exploited Children (NCMEC) offers a CyberTipline for the community and over 1,400 registered electronic service providers to report abusive images, videos, and other files that may contain child sexual exploitation material. This information is routed to the appropriate law enforcement entity.
Crawler-Based Systems: Automatically searches links or web pages for illicit or relevant content	• Semi-automated process frees up time for investigators and notifies user of potential "hits" • They can track specific search terms and help monitor multiple sources for abuser activity	• Many law enforcement–focused technologies are currently in development by research organizations, not quite ready for full community use • Some RSS readers require some coding experience	Free RSS Reader sites such as Feedly, Inoreader, and NewsBlur pull articles from sites directly into a reader, track keywords, and subscribe to social media feeds. Experienced users can write their own crawlers to scrape RSS feeds for particular sites or keywords. The Augmented Visual Intelligence and Targeted Online Research (AviaTor) project automatically crawls online sources for additional information for investigations in accordance with the national legal requirements. The tool triages reports from tip lines to streamline the process for law enforcement and investigate cases more rapidly.
Victim-Provided Evidence Capture Applications: Documented evidence from victims of TFA	These applications can securely document evidence of the TFA directly by the victim	Success depends on compliance from the victim	DocuSAFE is a free application created by the National Network to End Domestic Violence that enables victims to capture documentation of abuse in one location. The app securely shares information with stakeholders such as law enforcement, while providing helpful safety planning resources.

Figure 7: Active monitoring tools serve as channels by which law enforcement can route important information. These tools can rely on participation from the community or can passively search for instances of TFA by leveraging artificial intelligence.

Intelligence-Gathering Tools

Abusers who act to publicly shame or expose information on their victims often post this content on public forums and other online avenues. Investigators must sift through a variety of information sources to identify and capture evidence of TFA. Tools that aid in intelligence gathering help investigations actively sift through community platforms, draw insights about the abuse, and capture them for the investigation. These tools, which are listed in **Figure 8**, confirm the abuse, investigate and possibly identify a perpetrator, and help establish probable cause for search and seizure.

Social Media Investigative Tools

Social media platforms often serve as the primary means of TFA that involve public humiliation or dissemination of a victim's personally identifiable information. These platforms often contain information that is critical to abuse cases, including evidence of the abuse in messages, images, videos, and posts; the relationships between victim and suspected abusers; and patterns of behaviors from suspected abusers. These sites can be key resources for an investigator; however, the investigator may spend hours combing through multiple social media platforms and pages. Access to specific closed communities, private profile information, and private messages is challenging; investigators must go through proper legal processes to obtain the data, but in some cases, the law enforcement exceptions to the Stored Communications Act do not include content in private groups or profiles. To identify and collect relevant social media data, investigators can use two routes: (1) open-source search tools and (2) preservation letters.

> According to a 2012 LexisNexis survey of 1,200 federal, state, and local law enforcement, 67% of respondents believed social media information helps solve crimes, and 80% of respondents used social media information to aid in their investigations.

- **Open-Source Search Tools**—Law enforcement can use free or low-cost tools that make it easier to search social media sites for keywords, profiles, and location tags that may point to abuser activity. TweetDeck, for example, offers a user-friendly way to keep track of particular users, locations, or hashtags. Sowdust Facebook search enables simple searching of profiles, location, employers, keywords, and other fields. These tools are often tailored to the specific social media platform and pull all data that can be accessed in the public domain.
- **Social Media Preservation Letters**—Requesting information from these providers, such as private messages or a profile, requires going through the proper legal process using a preservation request. Many social media platforms have created a portal or means to submit preservation letters for records that are related to criminal investigations within a certain time period, even if the account has been deleted.

Open-Source Aggregators

Searching for relevant information about an individual, location, or keyword can be incredibly time consuming for an investigator. Open-source aggregators mine open-source intelligence sources for relevant people, locations, and keywords—including sources like social media tools, mobile applications, and the dark web—in a fraction of the time it takes to manually search. Cobwebs Technologies, for example, offers a web investigation platform that mines a variety of open-source web layers for insights using machine learning algorithms. These software products create aggregated trends and insights from disparate data sources, such as activity of a particular keyword or hashtag. These tools are usually subscription based.

Evidence Capture Applications

When active searching uncovers key information to an abuse case, investigators must capture this information for their records. Investigators can use screen-capping or video-recording tools to document evidence of the abuse as it happens or capture interactions before they are deleted by the victim or suspects. Investigators may also use website archiving to better preserve the data and metadata on a website, which may be able to paint a clearer picture of digital media interactions between the abuser and the victim.

Tools to Gather Intelligence of Abuse Across Community Platforms

Category and Information Gathered	Benefits	Limitations	Example Products
Open-Source Social Media Investigative Tools: Provide information on specific profiles, hashtags and keywords, and activity by location; can aggregate and download datasets such as follower lists, tagged users, and publicly available insights.	• Simplify searching processes across multiple social media platforms; most tools are free to use	• Searches and queries only publicly available information: must reach directly out to social media platform for private data • Not a "one stop shop": Investigators may need many of these tools to find relevant information • Tools may quickly become obsolete as social media platforms constantly update • Agencies must abide by policies of social media platforms when using these tools	Facebook[30] – Sowdust Facebook Search, IntelligenceX, Facebook Directory List, Netbootcamp Preservation letters: The Facebook Law Enforcement Portal enables investigators to request information about profiles that have been deleted or profiles at a certain time point. Investigators can also reach out to: 1601 Willow Road; Menlo Park, CA 94025; Attention: Facebook Security, Law Enforcement Response Team
			Instagram (A Facebook Company)[31] – Webstagram, Picodash, Netbootcamp Preservation letters: Consult the Facebook Law Enforcement Portal
			Twitter[32] – TweetDeck, TweetBeaver, IntelligenceX, Netbootcamp Preservation letters: Legal request submissions website; more information about Twitter's law enforcement support policies can be found on their help page.
			Snapchat[33] – SnapMap Preservation letters: lawenforcement@snapchat.com; Custodian of Records Snap Inc.; 2772 Donald Douglas Loop; North Santa Monica, CA 90405
			General (across social media sites) – Namechk.com
Open-Source Aggregators: Strings together multiple information sources to create aggregated insights. These may be powered by AI and analyze data from open-source sites across the web and dark web.	• Faster than manually searching open-source sites • May provide analytics/insights	Often subscription-based services that may be expensive	Cobwebs Technologies
Evidence Capture Applications: Capture stills, videos, website data, and metadata that contain information relevant to a case.	• Capture evidence of TFA as it is occurring • Can preserve evidence before the suspect or victim deletes it	• Screencapped evidence may be difficult to defend in court • Social media web page archiving is often done by the platform itself; requires preservation letter	Screencapping tools: QuickTime screen-recording tool Website archiving: Hanzo, WebPreserver

Figure 8: Investigators can leverage intelligence-gathering tools to identify pertinent evidence of TFA on online platforms, aggregate these data into meaningful insights to establish patterns of activity between the victim and suspect, and document the evidence to supplement their investigation.

[30] Wong, K., Lai, A. C. T., Yeung, J. C. K., Lee, W. L., & Chan, P. H. *Facebook forensics*. Valkyrie-X Security Research Group. https://www.fbiic.gov/public/2011/jul/facebook_forensics-finalized.pdf

[31] Riadi, I., Yudhana, A., & Putra M. C. F. (2018). Forensic tool comparison on Instagram digital evidence based on Android with the NIST method. *Scientific Journal of Informatics, 5*(20), 235-247. https://www.researchgate.net/publication/329465962_Forensic_Tool_Comparison_on_Instagram_Digital_Evidence_Based_on_Android_with_The_NIST_Method

[32] Yusoff, M. N., Dehghantanha, A., & Mahmod, R. (2017). Forensic investigation of social media and instant messaging services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as case studies. In K.-K. R. Choo & A. Dehghantanha (Eds.), *Contemporary digital forensic investigations of cloud and mobile applications* (pp. 41-62). Elsevier. https://arxiv.org/ftp/arxiv/papers/1706/1706.08062.pdf

[33] Alyahya, T., & Kausar, F. (2017). Snapchat analysis to discover digital forensic artifacts on android smartphone. *Procedia Computer Science, 109*, 1035-1040.

Case Study

New Hampshire town's sole detective leveraged social media activity as evidence to identify a suspect who was ultimately sentenced to 8 years for cyber stalking.

Starting in 2012, a disturbing pattern began to emerge among high school students in the small New Hampshire town of Belmont. Multiple girls approached the town's sole detective, Rachel Mouldin, with an eerily similar complaint: someone going by the name of "Seth" that the victims had never met in person was pressuring them for explicit photos. When Seth did not get his way, he escalated to verbal abuse and hacking the victim's private social media accounts. Even when the victims blocked Seth on their mobile devices, he would find a way to contact them via new phone numbers or social media. If the victims still refused to comply with Seth's demands, he began creating fake Facebook accounts impersonating the victims and threatened to post any explicit photos the victims did share online or send them to their family members and friends. The continued abuse had an extreme psychological toll on the victims, who felt isolated, helpless, and ashamed from the abuse.

Mouldin knew she had to act quickly to prevent Seth from escalating his pattern of abuse. The first break in the case arose when one of the victims told Mouldin that Seth was able to contact the victims via multiple phone numbers with Text Free, a free online texting service. Mouldin sent Text Free a subpoena to pinpoint the Apple universal identification number corresponding to Seth's phone. Using this universal identification number, Mouldin was able to subpoena Apple and reveal that a Belmont native by the name of Ryan Vallee was connected to "Seth's" universal identification number.

Although this was a great break in the case, Mouldin knew that she needed to gather more evidence to arrest Vallee. Mouldin knew she needed reinforcement to make any progress and escalated the case to the federal level. Shortly after the federal authorities took the lead, the psychological impact on the victims reached a breaking point with one of the victims expressing suicidal ideation. Authorities charged Vallee with extortion, but dropped the case due to time constraints and a lack of evidence. Mona Sedky, an expert prosecutor in computer crimes and cases involving sextortion, joined the team to bring justice to the victims.

Sedky served multiple online platforms with subpoenas including Amazon, Google, and Facebook to obtain Vallee's login IP addresses and time stamps on the online platforms. The investigative team took this information to the internet providers and obtained location data of Vallee's online traffic. Using these location data, the tie between Seth and Vallee started to become clearer; all of the locations Seth had accessed the online platforms had ties to Vallee. Armed with this evidence, the investigative team charged Vallee with computer fraud and abuse, aggravated identity theft, and interstate threats across 10 victims.

As part of Vallee's bail, he was ordered to not use the internet until his trial the next year. Shortly after he was released, one of the victims started to receive harassing messages from a Facebook account named "M.M." The investigative team subpoenaed Facebook to provide the IP address and login time reports daily. One of the investigators took over the victim's Facebook and began interacting directly with M.M. The IP addresses from Facebook indicated Vallee was using a mobile device, which the investigative team was finally able to obtain after a high-speed chase and a search warrant. The phone provided all of the evidence needed to prosecute Vallee for his crimes and brought the victim count up to 23. Vallee was sentenced to 8 years in prison for aggravated identity theft, computer hacking, and cyberstalking.[34]

Technology Insight

Law enforcement could employ active monitoring tools as tip lines to monitor for online abuse similar to Vallee's in the future and web crawlers to search for names or other relevant keywords that could indicate an abuser's activity. Social media preservation letters may help identify one or more of an abuser's accounts, even if they have been deleted; open-source aggregators may be able to help track where abusers like Vallee may be posting abusive information.

[34] Clifford, S. (2019). He cyberstalked teenage girls for years-then they fought back. *Wired*. https://www.wired.com/story/cyberstalked-teen-girls-for-years-fought-back/

Access to private devices and networks enables investigators to locate, extract, and capture evidence.

Intelligence gathering and active monitoring via community-based sources may provide enough preliminary evidence to justify a more thorough investigation of content found on a victim's or suspect's private devices. "Dumping" these data can uncover messages, photos, and network traffic indicating cyberstalking or could demonstrate that the suspect is gathering or posting information meant to cause emotional harm. The three main avenues for obtaining data include: (1) mobile devices, including phones and tablets, (2) computer hard drives, and (3) the victim's or suspect's networks. Multiple types of data can be located, downloaded, and captured, including content stored locally or on a cloud-based application, metadata and artifacts indicative of abuse, and internet data and traffic entering and exiting a network.[35] Investigators must acquire evidence in a deliberate and legally defensible manner to enable efficient and admissible evidence analysis. Appropriate policies and procedures documenting how the evidence is collected will ensure admissibility and preserve the integrity of the evidence. Law enforcement should work closely with courts and prosecutors to determine the proper legal requirements. With proper policies and procedures in place, law enforcement can employ a number of tools and techniques to help extract evidence from electronic devices and capture data residing on a network.

Mobile Device Tools and Techniques

A recent report by Upturn[36] indicated that over 2,000 agencies have purchased tools to search mobile devices. Law enforcement often uses one or more of the following approaches for extracting digital evidence from mobile phones and tablets: password recovery, manual, physical, and hex dumping. Although some agencies may consider use of JTAG, Chip-off, and Micro Read, these approaches are often intrusive or destructive techniques that require advanced training or assistance from a digital forensics laboratory to disassemble the phone. This report focuses on nondestructive tools and techniques that agencies can use, as summarized in **Figure 9**.

Password Recovery

When dumping data from mobile devices, investigators may have full access to the data (e.g., when they gather data from a victim's phone or computer); however, in some cases, suspects may not provide the passcode or biometric data to access the device. Password recovery tools are the first step in accessing encrypted data via manual, logical, or physical extraction processes. Unlocking Apple and Android phones has become increasingly challenging with evolving security features, including more people using strong passwords that contain a combination of letters, numbers, and symbols. Vendor products such as Cellebrite and GrayKey have evolved alongside the increasing security of passwords and encryption methods. Complicating access to devices without a passcode includes legal challenges as illustrated by *Riley v. California*, which held that officers may seize a cell phone from a person as a search incident to arrest but may not search the cell phone's contents without a warrant. Recent case law suggests that with a proper warrant, law enforcement can require an individual to unlock the device, but not to provide the password.[37]

Manual Extraction

Manual Extraction involves simply taking photographs or screen captures of the data, which can be performed in the field or agency's office; however, care must be taken because data can be modified or deleted during examination. Although it is an easy and inexpensive way to access data from a device, this extraction technique is only possible if the device is unlocked.

[35] Although cloud-based platform and network technologies sit at the nexus of public and private data sources, these capabilities typically require a warrant and are thus captured in this section.

[36] Koepke, L., Weil, E., Janardan, U., Dada, T., & Yu, H. (2020, October). *The widespread power of U.S. law enforcement to search mobile phones.* Upturn. https://www.upturn.org/reports/2020/mass-extraction/

[37] Basalla, K. (2020). Smartphones and the fourth amendment: When is access to password-protected information permitted? *University of Cincinnati Law Review*. https://uclawreview.org/2020/01/28/smartphones-and-the-fourth-amendment-when-is-access-to-password-protected-information-permitted/

Logical Extraction

Logical extraction provides access and the ability to copy current files and folders but cannot obtain deleted data. Data collected include photos, audio, video, text messages, contacts, call logs, Global Positioning System (GPS) data, and application data. Both the device and cloud may serve as sources for logical extraction. The process is quick and relatively straightforward; however, tools are expensive. The key benefit is that it can also capture data from social media applications and online file storage services (e.g., Facebook, Google, iCloud, Twitter, Snapchat, WhatsApp, Instagram) where TFA often occurs.

Physical Extraction (Hex Dump)

Hex dumping offers more in-depth analysis of data than logical extraction; hex dumps capture all data, both current and deleted, from flash memory chips. The data are extracted as a raw image in binary format. Decoding of raw data will vary based on the device model. Although hex dumps can provide a more comprehensive view into the TFA offense, tools can be expensive and analyzing the data is time intensive.

Tools to Extract Digital Evidence from Mobile Devices

Tool Category and Information Gathered	Data Acquisition	Benefits	Limitations	Example Products
Password Recovery: Recovers password for access to mobile device	Access to phone for manual extraction of data	Enables access to key information on phone	• Changing legal environment around reasonable expectations of privacy may prevent use of these tools. • Expensive tools • May require frequent updates as security protocols for devices change	Cellebrite Physical Analyzer, GrayShift GrayKey
Manual Extraction: Extracts and views data through the device's touchscreen or keypad	Data such as photographs, texts, emails, application activity documented via photographs	No-cost method of accessing data (other than time/labor)	• Cannot capture metadata and some types of data stored on phone • Data liable to inadvertent manipulation by examiner • Access is limited when devices are encrypted	Camera, handwritten notes, screen scraping tools
Logical Extraction (Mobile Device Data): Recovers data from locked and unlocked devices, including the full file system, decrypted keychain, and process memory	• Call detail records (CDRs) • GPS • App Data • SMS • Photos and Videos	Captures data and metadata from phone in short time; lower-cost tools available	Systems are expensive.	Oxygen Forensic Detective
Logical Extraction (Cloud Data): Recovers data from connected cloud-based storage. Uses tokens on mobile devices that enable apps to function without the need for users to re-enter their login details	Social media data and online file storage services (e.g., Facebook, Google, iCloud, Twitter, Snapchat, WhatsApp, Instagram)	Can capture data from systems where TFA often occurs (e.g., social media platforms)	Legal challenges may limit use of tool: may require express permission and password	MSAB XRY Cloud, ElcomSoft, Magnet Axiom Cloud
Physical Extraction (Hex Dumping): Performs a bit-by-bit copy of the contents of flash memory; enables the collection of live, deleted, and hidden data. Displays the contents of binary files in hexadecimal, decimal, octal, or ASCII	Obtains a complete image of phone data	Captures all data and metadata from phone	Systems can be expensive; there are more data to examine and may be time consuming	ADF Solutions Digital Evidence Investigator, MSAB XRY Physical, Cellebrite Frontliner

Figure 9: Data extraction tools for mobile devices enable investigators to gain access to locked devices and recover and extract data from mobile device storage and cloud-based storage.

Hard Drive Tools and Techniques

Investigators can leverage several tools to access critical information, such as memory keys, from hard drives in computers and other devices. Use of these tools varies by sophistication and availability of law enforcement in-house personnel to perform the techniques. A description of each is provided below and highlighted in **Figure 10**.

File Carving

File carving extracts data from a disc drive or other storage device by reassembling files from raw data that do not contain file system metadata. These metadata may include information about where the file was stored on the device and the type of file (e.g., JPEG, DOC, XLS). The term carving refers to obtaining structured data from raw data. It recovers files in unallocated spaces and is a common procedure used to recover data after a storage device failure or when data have been deleted or partially overwritten.

Data Imaging

Investigators may use data imaging to make a forensic copy of the hard drive. If a 1 TB hard drive has 500 GB of files, a logical copy would only back up the 500 GB. A forensic copy would back up the 500 GB of visible files as well as data in unallocated spaces that contain deleted files, metadata, time stamps, or other residual data that can be used during discovery. Data imaging can also include browser forensic artifacts and vary based on the type and version of a web browser used. Browsers such as Google Chrome can sync information to all computers that a suspect logs into and can include:

- History
- Passwords
- Cache
- Cookies
- Typed URLs
- Sessions
- Most visited sites
- Screenshots
- Form values (searches, autofills)
- Downloaded files (downloads)
- Favorites

Tools to Extract Digital Evidence from Hard Drives

Tool Category and Information Gathered	Data Acquisition	Benefits	Limitations	Example Products
File Carving: A technique of reassembling files from raw data fragments when no file system metadata are available	Finds hidden or deleted files from digital media. A file can be hidden in areas like lost clusters, unallocated clusters and slack space of the disk or digital media	Recovers data that may have been intentionally deleted by an abuser	May not be effective if data are very corrupt	Advanced Carver, BlueBear, EnCase
Data Imaging: Creates a "forensic copy," which includes all visible files and all data, every sector, partition, files, folders, master boot records, deleted files, and unallocated spaces	All data on hard drive	Ensures all data are available for analysis	Challenging to sift through all data on the hard drive	AccessData FTK Imager

Figure 10: Investigators can use file carving or data imaging tools to recover or duplicate data from hard drives.

Network Tools and Techniques

Many network tools, including FileTSAR (shown in Figure 11), are available as open-source programs for use by law enforcement.

Network forensics focuses on the capture, recording, and analysis of internet traffic to secure information about a suspect's activity. Network tools can monitor and collect information relevant to TFA investigations, such as evidence of a suspect monitoring a victim's activities. Although these tools are helping to capture digital evidence for TFA cases, other internet technologies have been developed to mask the identity and location of users accessing and sharing information. The Navy developed the Tor (The Onion Router) browser to provide safer internet access where censorship or repressive regimes prevented internet access.[38] But Tor's ability to encrypt information over several server nodes throughout the internet has made it easy to mask illegal activities. Law enforcement continues to face challenges in accessing data via network forensics. Digital forensics is a burgeoning field, and thus new techniques will emerge to alter suspects' ability to mask their identities.

Tools to Extract Digital Evidence from Network Traffic

Tool Category and Information Gathered	Data Acquisition	Benefits	Limitations	Example Products
Network Traffic Capture Tools: Collects data to reconstruct files from a user's network	Documents (e.g., doc, docx, pdf), images (e.g., jpg, png, gif) email (based on SMTP, IMAP, IMP), and VoIP sessions	• Provides access to data that may be otherwise deleted • Many tools are available as open-source programs	• High volume of data acquired • Representative sample in real time may not contain material relevant to investigation	PCAP, TcpDump, Wireshark, NetworkMiner, FileTSAR

Figure 11: Network traffic capture tools can be used by investigators to access and analyze the internet traffic of suspects to determine patterns of activity related to TFA.

[38] Jardine, E., Lindner, A. M., & Owenson, P. (2020, December). The potential harms of the Tor anonymity network cluster disproportionately in free countries. *Proceedings of the National Academy of Sciences, 117*(50), 31716–31721. https://doi.org/10.1073/pnas.2011893117

Cloud-Based Challenges

Cloud computing uses a network of remote servers hosted on the internet to store, manage, and process data, thus removing the need to store data on a local server or a personal computer. The ubiquitous nature of cloud computing has presented significant challenges in digital forensics due to the difficulty of obtaining data by cloud service providers (CSP) or social media. Data like log information stored by CSPs may reside in different locations (even in different countries), making collection difficult. Service providers hide the physical location of the data, and it is not in their business interest to provide tools and services that help forensic investigators acquire evidence in the cloud. Service-level agreements between the CSP and customer often do not contain terms that would enable a forensic investigation, giving CSPs the rationale that limits access to data. Data can also be lost when a server is shut down or rebooted.

Despite these challenges, several products such as Cellebrite's UFED Cloud Analyzer, Magnet Forensics' AXIOM Cloud, and Oxygen Forensics' Cloud Extractor have developed features that allow law enforcement to extract public domain and private social media data, instant messaging, file storage, web pages, and other cloud-based information from various social media services including Facebook, Twitter, Instagram, and WhatsApp and cloud storage associated with Apple, Google, and Microsoft. Usernames and password combinations or tokens extracted from the mobile device or PC can be used to gain access to cloud storage from these providers. Two-factor authentication is a process that prompts a user to confirm a code sent to an independent device, such as a mobile phone, and is now a key security feature used to prevent unauthorized access to data. Usually, the use of tokens stored on devices keeps two-factor authentication from being triggered. If, however, it is during an investigation, these extractors can provide options to bypass the authentication.

Case Study

Hard drive access played a key role in demonstrating an abuser's predatory behavior.

In 2017, Heriberto Latigo was sentenced to 60 months in prison for cyberstalking and abusing his ex-girlfriend. After their breakup, Latigo's ex-girlfriend experienced unrelenting abuse by Latigo, including sextortion, cyberstalking, and nonconsensual pornography. Latigo threatened to post explicit photos of the victim if she did not comply with his demands. His abuse escalated to threats and harassment via the creation of a fake Facebook page containing personal information about the victim. When the victim would not comply with Latigo's demands, he shared the explicit photos with the victim's family and colleagues. Although the victim did go to her local law enforcement to report Latigo's behavior, the case was complicated by changes in the victim's story because of her fear of Latigo. The case was escalated to the federal level.

FBI took multiple routes to uncover Latigo's pattern of predatory behavior. To avoid loss of evidence online on social media platforms, the investigative team sent social media preservation letters to multiple platforms. The break in the case came with the investigative team seizing Latigo's computer hard drives. From the computer hard drives, the investigative team was able to ascertain that Latigo accessed the social media sites he used to torment the victim from his electronics. The team also found the explicit photographs of the victim that Latigo was using as blackmail. With these overwhelming pieces of evidence, the investigative team had enough to prosecute Latigo. In the course of the investigation, federal authorities uncovered additional cyberstalking and sextortion complaints filed against Latigo, showing a pattern of abusive behavior. Special Agent Christopher Petrowski, a member of the investigative team on the Latigo case, remarked on the importance of taking cases of TFA seriously: "By taking this one guy off the street, we may have prevented countless future sexual assaults."[39]

Technology Insight

Using a combination of cloud network tools, mobile devices, and hardware extraction tools may help demonstrate that an abuser is repeatedly contacting a victim, especially if the individual is in possession of different physical devices.

[39] Federal Bureau of Investigation. (2018). Two federal cases illustrate the consequences of sextortion. *Federal Bureau of Investigation News*. https://www.fbi.gov/news/stories/sentences-in-separate-cyberstalking-cases-103018

Tools to analyze digital evidence often include search capabilities.

Extraction of data often leads to recovery of a large volume of information in a variety of formats—pictures, text messages, emails, relevant metadata—that investigators must sift through, which is often a time-intensive process. Investigators need tools to help them analyze and report insights from the data. Many of these tools are bundled with extraction tools to streamline information flow or can easily interface with product suites. Many are designed with the investigator in mind, with intuitive interfaces and the ability to create useful, shareable reports. Figure 12 provides an overview of tools employed to process this data, such as advanced searching tools and tools for insights generation.

Advanced Searching Tools

Digital forensic practitioners use forensic search tools to search and filter through digital evidence to find search terms, images, or demonstrated interactions between abuser and victim. Advanced tools sort data "dumped" by extraction by file type and location and can automatically search for and extract data such as contacts and ID numbers from the files. Some searching tools leverage hashing technology; these can search the contents of a dataset against a known "library" of hash values from known exploitative material or a specific image the investigator is looking for. Others may use AI tools, which rely on machine learning and computer algorithms to recognize patterns and quickly discover them. For TFA cases, AI tools are often used to search for specific image content—based on a keyword or known location/background—and flag those that may fit this description. This is especially useful in cases involving nonconsensual pornography. AI-powered tools not only significantly decrease the time needed to search large amounts of data, but they reduce exposure of investigators to the sensitive material and may lead to reduction of vicarious trauma and revictimization of victims of TFA.

Insight Generation Tools

Analytical software can help investigators better understand the interactions between an abuser and victim and leverage multiple sources of data and metadata to establish patterns of activity. These tools help create a timeline of activity between two phone numbers or usernames, create a visual network to understand relationships between two or more individuals, and physically map out relevant locations to a case.

Tools That Can Help Develop Insights from Data Gathered in Investigations Involving TFA

Category and Information Gathered	Benefits	Limitations	Example Products
Advanced Searching Tools: Enable investigators to search for specific keywords, files, and images. Some leverage AI or machine learning.	• Sorts information for easy searching • Customized or set search parameters enable quick discovery of relevant images and videos • Can limit vicarious trauma of investigators	• Aggregation and analysis of data may not be included • Some AI-based tools focus on identifying images, which may not be relevant to some TFA investigations	Vound Intella, Truxton Forensics Platform, MSAB XAMN, AccessData Forensic Toolkit, GriffEye Analyze Platform, Cease.ai
Insights Generation: Connects data and metadata to demonstrate activity timeline, connections between two individuals	• High-powered data analysis capabilities to create meaningful insights • Time savings compared to traditional data analysis methods • Are often directly tied to data access tools	Usually part of a forensic tool suite, not "a la carte," and can be quite expensive	Magnet Forensics Digital Investigation Suite, MSAB XAMN, ADF Solutions Digital Evidence Investigator, Cellebrite Physical Analyzer, Oxygen Forensic Detective

Figure 12: To generate insights from the digital evidence left behind in TFA cases, investigators can use analysis tools to search for keywords and establish patterns of abuser activity.

Case Study

Abusers can use dozens of devices which requires sophisticated analysis by law enforcement.

When Francesca Rossi met Juan Thompson in 2014, she could not have predicted how an online romantic interest could have unleashed more than a year of psychological torture via online attacks and other forms of TFA. The two first met via an online dating platform and quickly began a relationship, with Thompson moving into Rossi's apartment in 2016. After Thompson moved in, Rossi began to receive harassing text messages, notices for lawsuits that turned out to be false, and nonconsensual pornography, presumably from ex-boyfriends.

The timing of these attacks and Thompson's move was no coincidence. Rossi consulted a lawyer with expertise in cyberharassment who determined the perpetuator behind these attacks was Thompson. Rossi promptly broke up with Thompson, which only escalated the abuse.

Following their breakup, Thompson mercilessly harassed and cyberstalked Rossi through a variety of platforms, including social media, text messaging, and phone calls, even going so far as harassing her family members. Thompson's abuse did not stop at cyberstalking. He doxed Rossi on a website encouraging men to violently attack women and posted nonconsensual pornography of Rossi online. When reflecting back on her abuse, Rossi stated, "Every time my phone buzzed, I felt sick. I mean, I thought he was going to kill me. I felt like my life was over." Although overwhelming to Rossi, this TFA left digital evidence that was picked up by the investigators.

Rossi did report Thompson's abuse to both her local law enforcement jurisdiction and the FBI, but there was not much traction from either effort; instead, local law enforcement began investigating Rossi as a result of a swatting attack orchestrated by Thompson. Thompson falsely reported that Rossi was planning to stage a shooting at a police station and that she may have been illegally trafficking guns. Even though police received a threat on Rossi's life, and she insisted Thompson was behind all of the harassment, Rossi claimed police officials told her they could not help her until it became worse.

Thompson did not make law enforcement's job easy with this case, using 25 different devices for his coordinated attacks on Rossi and her loved ones. Thompson's use of multiple methods of harassment, including text messaging, social media platforms, and calls, further complicated law enforcement's investigative process. With so many breadcrumbs to follow, law enforcement needed a breaking point in the case to help Rossi.

All of the pieces came together after a coordinated swatting attack was reported on Jewish community centers in 2017 across the United States and Canada. The majority of the threats were attributed to Michael Ron David Kadar, but federal officials attributed a dozen or so of the attacks to Thompson. For one of these attacks on a San Diego Jewish community center, Thompson posed as Rossi and was promptly arrested 4 days later. Finally, Thompson was prosecuted for both his swatting and cyberstalking crimes. During the trial, Rossi stated the need for TFA to be taken as seriously as physical crimes by law enforcement: "The police diminished my abuse because my life-threatening attacks came from phones and computers. This is what domestic violence looks like now." In 2019, Thompson was sentenced to 5 years in prison for his crimes.[40]

Technology Insight

Analysis tools can be used to glean insights from data across multiple sources, for example, the abuser's multiple physical devices to map how an abuser interacts with, monitors, or even impersonates a victim. These data can help determine whether an abuser is in possession of nonconsensual pornography and can demonstrate threatening behavior toward a victim.

[40] Long, C. (2018, February 27). Cyberstalking victim says she feared tormentor would kill her. *The Seattle Times*. https://www.seattletimes.com/nation-world/cyberstalking-victim-says-she-feared-tormentor-would-kill-her/

Digital tools are evolving with communication platforms and abuse tactics.

Tools that help capture and analyze digital evidence must adapt and evolve with digital technologies, and abusers efforts to harm their victims. Current and emerging tools are leveraging the following technology trends and advances to stay on top of TFA trends and fit the changing needs of investigators.

Tools with enhanced capability to sift through large amounts of data

During a TFA investigation, an investigator may need to sift through a large amount of content, whether it be internet pages or content on a hard drive. Finding relevant evidence is a slow process that may consume many man-hours in an investigation, and storage capacities of devices are growing from year to year. Vendors and researchers are leveraging technologies such as AI and crawlers to automatically search through large amounts of data for clues on open-source data and "dumped" data sources. NIJ has funded a sifting collector software that can help identify and capture disk regions of a hard drive that may contain evidence.[41] Grier Forensics' Rapid Forensic Acquisition of Large Media accelerates the analysis of the hard drive by bypassing operating system software and applications not relevant to the investigation. These innovations can help point investigators in the direction of valuable evidence and may play a role in reducing case backlogs.

Tools with the ability to capture data from a variety of devices

Tools and technologies that access information from devices are currently focused on hard drives and mobile devices, which are often primary sources of TFA evidence. However, many devices, such as vehicle entertainment systems, personal assistants such as Amazon Alexa, gaming systems, wearables, and other objects, are connected and may store data locally or in a cloud-based system. Home devices connected by the Internet of Things may indicate network activity and provide information such as call logs. Vendors and researchers are working to understand the value of this data and approaches to extracting data from these devices. Oxygen Forensics, for example, has created a tool called Cloud Extractor that can extract data from cloud-based Amazon accounts, enabling investigators to access Alexa data with login information.[42]

Tools that provide analysis capabilities across cases involving digital evidence

Individuals who commit TFA may be repeat offenders or may operate in different jurisdictions. Digital forensics experts have noted a growing need to analyze data not only gathered for one case, but across a number of cases to identify potential timelines, suspects, or patterns of activity. In the future, investigators may leverage analysis tools to understand trends in TFA and link similar cases. Enhanced data sharing between jurisdictions will be a key need for successful data analysis. Fusion centers, which serve as repositories for state- and regional-level crime data, could leverage these tools to better identify and address TFA cases.

[41] Novak, M., Grier, J., & Gonzales, D. (2018, October). *New approaches to digital evidence acquisition and analysis.* National Institute of Justice Journal https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

[42] Oxygen.Forensics. (2019, February). *Digital assistants the new eye-witness*. https://blog.oxygen-forensic.com/digital-assistants-the-new-eye-witness/

ADOPTION GUIDANCE

Implementation of a toolkit to extract and analyze digital evidence related to abuse cases requires sufficient planning of resource and time investment. The potential sensitivity of materials related to abuse cases, along with the ever-evolving nature of the field of digital forensics, can lead to complexities in adopting tools to aid in conducting investigations. **Figure 13** lists key questions that agencies should consider when implementing these tools for TFA digital evidence identification and analysis.

Challenge	Key Questions to Consider
Strategic Tool Investment	Can your agency afford expenses beyond software products, including necessary hardware, training, and maintenance?
	Which tools can access data from the largest number of sources?
	Which tools interface directly with each other via APIs or other mechanisms, such as suites of tools?
	How does your agency prioritize expensive, time-saving tools vs. inexpensive, time-intensive tools?
Leveraging the Criminal Justice Community	Does your agency have access to technical experts who can help validate or troubleshoot tools?
	Is there a clear distinction of roles between the investigator and digital forensic examiner?
	Can your agency partner with other laboratories or agencies to cost share software licenses?
	Which stakeholders may be affected by adoption of the tool?
	What storage options are available for digital evidence gathered in the investigations?
Training	Is your agency up to date on community platforms and other potential sources of TFA digital evidence?
	Do you understand the capabilities and limitations of these products?
	Do your first responders and investigators know how to protect evidence on a private device?
	Has your agency trained investigators to obtain digital evidence in a legally defensible manner?
	Is your agency aware of professional associations and training resources that can help you use these tools?
Validation	Does your agency consult resources such as NIST's Computer Forensics Tool Testing Program?
	Has your agency developed policies for piloting, implementing, or validating digital forensics tools?
Data Storage	What is your agency's approach to storing digital evidence and data related to cases?
	Is your agency's current data storage capacity sustainable in the next few years?
	What type of digital data can be stored in your network and for how long?

Figure 13: Like any digital forensics product, tools that assist in investigations involving TFA should be holistically considered before implementation. Agencies should understand the resource investments needed for purchase, training, and data storage and also consider the realities of product capabilities and validation.

Consider tool functionality, redundancies, and investment needs prior to implementation.

Although several tools can help agencies capture digital evidence for cases of TFA, specific agency needs depend on factors such as agency size, budget, caseload, expertise, and support. Agencies must consider their limited resources when building their "toolkit."

Balance tool functions with bundling and cost.

Several digital evidence tools can serve multiple roles and accomplish multiple tasks within an abuse investigation or any investigation involving digital communication platforms or devices. For example, some companies offer a product suite that provides mobile device extraction, analysis, and reporting capabilities packaged within the single suite. Although product suites streamline the procurement process and enable simpler workflows with minimal integration between different products, they often come with a hefty price tag that may not be feasible for smaller agencies. Agencies should balance the required tools needed for investigations with the price of available product suites that combine tools or the price of single tools accomplishing only one job.

Consider needs and possible redundancies in tools.

All digital evidence tools are not created equally. Some tools are specialized for a step in the digital evidence examination process, whereas other tools have multiple functions and can broadly be used throughout the investigation. For example, some digital forensic suites like Magnet, MSAB, and Oxygen Forensics toolkits may include multiple functions such as data extraction, searching, and analysis, whereas some open-source tools may be created specifically for searching or gathering data from a specific social media platform. Tools accomplishing the same job may range in their capabilities, such as compatible starting data types. When building a toolkit, compare the functionalities of different tools and the resources needed to implement the tools.

Assess modular software options.

A digital evidence investigator's toolkit will often contain tools from different vendors. When building a toolkit, consider adopting tools that are compatible with each other, such as Griffeye and Magnet Forensics, which may facilitate transfer or analysis of data. Many forensic suites enable interfacing with tools to streamline workflows.

Plan for investment beyond the cost of tools.

Agencies must plan for sufficient allocation of resources to ensure proper use of tools and thereby thorough investigations of cases, even if the tool is free or low cost. Tool implementation includes investment in proper IT infrastructure and support, as well as investigator training, especially if the agency is just beginning to populate its toolkit. Digital media are constantly evolving; to keep up to date with these changes, agencies must invest time to update their tools and periodically search for new open-source and on-market products.

Digital media are constantly changing. Although experts note that data are typically gathered from mobile devices and hard drives in abuse cases, other sources, such as smart watches and doorbell systems, may capture relevant information, leading investigators to widen the scope of the sources of data in cases with digital evidence.

Although an agency could mitigate cost issues by pursuing several smaller, lower-cost products rather than a robust product suite, they may see additional costs related to setup, management, and training. However, products in a suite may automatically update to reflect changes in digital media, whereas open-source tools may become obsolete quickly.

When deciding on a strategy to invest in resources to address abuse cases, agencies should leverage partners within their network to choose appropriate and mutually beneficial tools. Outside of partners within the criminal justice community, agencies could consider leveraging external forensic service providers or consulting firms, such as Vestige or FTI Consulting, to supplement their digital forensic capabilities.

Consider stakeholder roles and cost sharing opportunities for investigations involving digital evidence.

As with any investigation, abuse cases require collaboration and mutual agreement between internal and external stakeholders at a law enforcement agency. When considering which tools to implement to aid in conducting abuse cases, agencies should identify the relevant stakeholders whose workflow may be affected by adopting the tools. Multiple stakeholders may interact with the physical device containing the digital evidence or with the digital evidence itself. Furthermore, patrol officer buy-in may be crucial for extraction tools with field capabilities, which could lead to considerable workflow changes and potential complexities without sufficient training. Gaining leadership buy-in could help agencies implement novel tools with increased capabilities and justify additional resource allocation to improve efficiency with investigating these cases.

Establish clear responsibilities between the investigator and examiner roles in abuse cases.

Whether a law enforcement agency is adopting digital evidence tools for the first time or adopting novel tools to supplement their current digital evidence toolkit, changes in workflow can be expected. With these changes in workflow, law enforcement agencies should consider which jobs should be performed by which stakeholder. For example, agencies should designate whether the extraction step in the investigative process should be performed by a patrol officer, investigator, or forensic examiner (who may be internal to the agency or located in a crime laboratory). The roles and responsibilities assigned to each stakeholder can depend on multiple factors, including the knowledge base of the team and tool capabilities. Defining clear roles for each stakeholder will avoid confusion and mistakes and ensure proper training.

Identify opportunities for agency collaboration.

To alleviate the burden of high caseloads and costs of digital evidence tools, agencies may be able to collaborate, combining both manpower and technical expertise. Some cases involving digital evidence may surpass the capabilities and current toolkit of a law enforcement agency. Therefore, agencies should decide which capabilities will be offered in-house and conducted internally and which capabilities can be outsourced to an external collaborator, such as a forensic crime laboratory. Setting clear boundaries on the capabilities that can be performed in-house will eliminate possible mishandling of evidence because of a lack of proper tools.

Collaborating with external agencies can also provide the option of cost sharing when purchasing new tools for digital evidence that will be used for both agencies. Agencies in close jurisdictions may be able to set up shared tip lines and other tools for gathering intelligence about the abuse. Identifying opportunities to collaborate with other agencies may not only improve the efficiency of an agency in terms of conducting investigations but could also keep agencies up to speed on the practices in use by other members of the digital forensics community.

Prioritize training for effective and legal use of digital evidence tools.

As with any investigation, abuse cases require collaboration and mutual agreement between internal and external stakeholders at a law enforcement agency. When considering which tools to implement to aid in conducting abuse cases, agencies should identify the relevant stakeholders whose workflow may be affected by adopting the tools. Multiple stakeholders may interact with the physical device containing the digital evidence or with the digital evidence itself. Furthermore, patrol officer buy-in may be crucial for extraction tools with field capabilities, which could lead to considerable workflow changes and potential complexities without sufficient training. Gaining leadership buy-in could help agencies implement novel tools with increased capabilities and justify additional resource allocation to improve efficiency with investigating these cases.

Train officers to obtain evidence in a legally defensible manner.

Agencies adopting tools for capture and analysis of digital evidence must be aware of the appropriate procedures for documenting evidence and for legally seizing physical devices and accessing digital evidence on them. Before the seizure of physical items of evidence containing digital evidence, agencies must understand the ramifications of including digital evidence on warrants, especially with mobile devices. As technology continues to advance, agencies must keep up-to-date policies and procedures that address the extraction of data from devices. An NIJ report entitled *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*[43] and *Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations*[44] may help agencies establish proper policies and procedures. Agencies should consider several legal issues:[45]

1. **Search and Seizure:** Fourth amendment rights protect individuals from unreasonable search and seizure. Law enforcement must obtain a search warrant to carry out a search. For data stored on social media platforms or on applications that store information in the cloud, it is often up to the discretion of the vendor to provide the data and may require a subpoena to execute.

The Supreme Court case of *Riley v. California* (decided June 25, 2014) established that the information on a cell phone is not immune from search, but a warrant is needed before such a search, even when a cell phone is seized during the arrest. With modern technology, obtaining a warrant is more efficient; in some cases, officers acquiring the phone at the crime scene can email warrant requests to judges and have a response within 15 minutes.

2. **Documentation:** Proper authentication and chain of custody are essential for pursuing a court case. Authenticating the chain of custody ensures the evidence is preserved in its original form. Documentation includes where and when data were collected, the type of device, from whom it was collected, how it was stored, and who accessed the data. When agencies use criminal intelligence databases and evidence captured from sources such as social media, they must adhere to the appropriate policies and procedures outlined in federal, state, and local laws (such as the Criminal Intelligence Systems Operating Policies 28 CFR part 23 Guideline).

[43] Ashcroft, J., Daniels, D. J., & Hart, S. V. (2004, April). *Forensic examination of digital evidence: A guide for law enforcement*. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[44] Office of Legal Education, Executive Office for United States Attorneys. (n.d.). *Searching and seizing computers and obtaining electronic evidence in criminal investigations*. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

[45] Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence*. Priority Criminal Justice Needs Initiative. https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

3. **Admissibility:** Five criteria have been suggested by the Supreme Court to weigh the admissibility of evidence. The extraction and analysis techniques must be tested, be peer reviewed, have a known error rate, have established standards for operation, and be accepted by the scientific community.
4. **Obligations to the Defense:** Discovery requirements ensure evidence is usable and is provided to the defense with enough time to review and prepare for trial.

Furthermore, agencies should only adopt and use tools that can produce results submittable for use in court and tools that investigators and forensic specialists feel comfortable explaining through court testimony. Agencies may need to consult with legal stakeholders to be aware of the legal complexities associated with digital evidence.

Train field officers to correctly handle seized evidence and identify potential sources of data.

Multiple stakeholders may interact with the physical device containing the digital evidence or with the digital evidence itself. For example, a patrol officer may procure a mobile device from a victim or suspect and, if not properly trained, could unintentionally delete case-sensitive data or lock the device, making downstream processing for investigators or examiners more difficult. In addition to correctly handling evidence to maintain integrity, officers must be trained to recognize potential sources of TFA outside of the obvious sources like text messages and email. Valuable data could be overlooked if officers are not equipped with the right knowledge to thoroughly identify all potential sources of TFA.

Train end users to derive the most value out of the tool.

Digital evidence is a rapidly evolving field of forensic science, due in part to advancements in consumer technologies and improvements in tools used to conduct investigations. These advancements, coupled with the complexity of the field, amplify the importance of training. Training offered by vendors can be tool specific and offered complementarily with the purchase of a tool or as an add-on certification class at an extra cost, such as EnCase's Certified Examiner program. Several vendor-neutral training certifications are offered, including the International Association of Computer Investigative Specialists (IACIS) Certified Forensic Computer Examiner and the Global Information Assurance Certification (GIAC) Certified Forensic Examiner. Regardless of the depth of training, agencies must set aside time and resources to ensure examiners are properly equipped to conduct investigations with digital evidence. Agencies should determine what level of training is needed for both the tools in use and relevant investigations.

Consider validation challenges and resources for emerging digital tools.

TFA investigations are relatively new to agencies and uniquely require cutting-edge tools to keep up with the "arms race" of evolving digital media. Because of the parallel innovation in both consumer technologies and tools to conduct digital evidence investigations, validation of these tools is a long-standing challenge for law enforcement agencies.

As with any tool used in criminal investigations, tools for extracting or analyzing digital evidence must be validated for admission into court. *Daubert v. Merrell Dow Pharmaceuticals* established the legal precedent of the need for expert testimonies to be based in scientifically valid reasoning, which led to a push for validation of tools within every forensic science discipline. Although necessary, validation is a time-consuming process that can be burdensome on already resource-constrained law enforcement agencies. There are ongoing efforts to streamline the validation of digital evidence tools and steps law enforcement agencies can take to ease the process. Agencies should consider several factors when choosing tools.

Adopt tools with a legal precedent.

Emerging technologies may show promise in improving the efficiency of conducting abuse cases or robustness in the data procured and analyzed. Still, the logistical hurdles of validating these tools may outweigh these proposed benefits, because law enforcement agencies may have to rely internally on validation of these tools with no guarantee the validation will hold up in court. Adopting tools with widespread use in the forensic science community, along with legal precedent, may save law enforcement agencies time and money and ensure cases can be fully prosecuted with all of the evidence available. Consider leveraging case law databases such as LexisNexis to assess legal precedents for tools of interest before adoption.

Use available validation protocols from organizations like NIST and SWGDE.

Ongoing efforts by prominent research organizations and working groups within the forensic science community have been addressing the challenge of validating digital evidence tools. Law enforcement agencies should use these publicly available tools to not only facilitate the validation process but also to ensure compliance with industry-accepted standards.

NIST has long been on the forefront of publishing standardized practices for conducting investigations among several forensic science disciplines. The Computer Forensics Tool Testing (CFTT) Program was established by NIST to develop open-source validation protocols for digital evidence tools commonly used by law enforcement agencies. Agencies can download tool testing reports and reference datasets directly from CFTT's website to test a multitude of digital evidence tools that serve multiple jobs to be done. CFTT's Federated Testing Project enables streamlined validation of multiple types of tools within a single test suite. Currently, the Federated Testing suite can test disk imaging, forensic media preparation, forensic string search, hardware write blocking, and mobile forensics data extraction functionalities. Agencies are encouraged to share the reports generated through the testing process to enable open-source collaboration throughout the entire digital forensics community to ensure the best tools are being used for their respective jobs.

The Scientific Working Group on Digital Evidence (SWGDE) is a multidisciplinary working group formed from key stakeholders in the digital forensics community. SWGDE publishes documents capturing best practices for workflows associated with conducting investigations with digital evidence, including validation and testing of tools. Agencies in the process of adopting new digital evidence tools or technologies should refer to the "Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics" and "Recommended Guidelines for Validation Testing."

Plan for data storage complexities.

As with physical evidence, one consideration for agencies conducting investigations with digital evidence is storing the evidence. Although physical evidence storage may require implementation of additional storage units, the storage of digital evidence requires robust servers and data storage systems, both in house and in the cloud. Agencies must consider implementing practices to prevent data compromises, safeguards for sensitive case materials, and systems capable of high-volume data storage.

Establish practices to ensure data integrity.

As with any evidence, compromise of digital evidence can have severe consequences for law enforcement agencies and hinder just outcomes for victims. Many tools used to extract and access data incorporate hashes into the data files as a safeguard. Investigators use hash algorithms to verify that forensic copies are exact duplicates of the original drive. A hash is a string of hexadecimal characters that, when added to digital evidence, creates a digital fingerprint unique to the files. If the data being copied change, the hash will change as well. If the two hashes are equal, the underlying data are identical. In digital forensics, hashing is primarily used for integrity verification and file identification. Scientific Working Group on Digital Evidence recommends hashes be made as early as possible during the collection process, as proper chain of custody starts from collection even before the hash is made and secured. Although the underlying technology often relies on MD5 and Secure Hashing Algorithm (SHA-1) functions, tools like FTK Imager and EnCase have incorporated hashing algorithm functionality in their products.

In addition, agencies need to establish internal practices to monitor data integrity. Digital evidence should be treated the same as physical evidence, with an airtight chain of custody and a record of changes made to the data, especially when using tools for analysis. Agencies may develop best practices and SOPs for tools used in digital evidence investigations, which may help prevent accidental compromises or deletion of data. Access to case-related materials should be limited and monitored to prevent internal or external security breaches.

Implement systems capable of robust data storage.

One of the most prominent challenges in investigating cases with digital evidence is the storage bandwidth required to house the sheer amount of data generated. A single computer hard drive could house multiple terabytes of data and could be only one device out of several within a single case. Agencies investigating multiple cases at once will need to implement sufficient data storage systems to accommodate high volumes of data. Often, agencies store case data on local networks for a set period of time and afterward burn the data onto CDs, which then become the items of evidence. Although this practice frees up space for new case data, it can introduce complexities with evidence management practices, and agencies must ensure physical copies are not compromised. There are many approaches to managing data in digital forensics, and agencies should implement what best suits their needs while protecting the evidence.

GLOSSARY

Brigading

The use of electronic communications technology by an online group to conduct a concerted attack against a targeted individual or group

Cyberbullying

A form of unwanted, aggressive behavior that generally involves a real or perceived power imbalance, is repeated or has the potential to be repeated over time, and takes place using electronic communications technology[46]

Cyberharassment

A course of conduct facilitated through electronic communications technology that causes the targeted individual substantial emotional distress or fear for safety but does not involve a credible threat[47]

Cyberhate

Using electronic communication to attack people based on their actual or perceived race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability, or disease to spread bigoted or hateful messages or information[48]

Cyberstalking

The repeated use of electronic communications technology to stalk a person or group; cyberstalking is distinguished from cyberharassment in that it poses a credible threat of harm to the victim[48]

Cyberthreats

Threatening communications that are conveyed via the internet or other electronic communications technology[49]

Data Imaging

Creating a digital forensic copy, or forensic clone, an exact bit-for-bit copy of a computer hard drive[49]

Digital Evidence

Any information stored or transmitted in binary form that can be captured for possible use in an investigation[50]

Digital Forensics

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal[51]

Doxing

The use of electronic communications technology to publish personally identifiable information (e.g., name, address) about an individual without their permission[49, 52]

File Carving

Searching for and reconstructing files based on content, rather than file system metadata[48]

Hashing

Takes an arbitrary string of binary data from a data object and produces a number, or digest, in a predefined range. The likelihood of two data objects producing the same digest is miniscule; thus, it can be assumed two objects with the same digest are identical. Hashing is a common method to validate the integrity of data and identify known explicit content[53]

[46] U.S. Department of Health and Human Services. (2019, May). *What is bullying*. https://www.stopbullying.gov/what-is-bullying/index.html

[47] Brenner, S.W. (n.d.). *Cyber-abuse: Legal Issues*. National Conference of State Legislatures. https://www.ncsl.org/documents/telecommunications/Brenner.pdf

[48] Anti-Defamation League. (n.d.). *Responding to cyberhate*. https://www.adl.org/education/resources/tools-and-strategies/table-talk/cyberhate

[49] Executive Office for the United States Attorneys. (2016, May). Cyber misbehavior. *The United States Attorneys' Bulletin, 64*(3). https://www.justice.gov/usao/file/851856/download

[50] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (2021). *Digital Evidence and Forensics*. https://nij.ojp.gov/digital-evidence-and-forensics

[51] Palmer G. (2001). A road map for digital forensic research. Technical Report DTR-T0010-01. https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

[52] *Doxing.* (n.d.). Cambridge Dictionary Online. https://dictionary.cambridge.org/us/dictionary/english/doxing

[53] Office of Legal Education, Executive Office for United States Attorneys. (n.d.). *Searching and seizing computers and obtaining electronic evidence in criminal investigations*. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

Logical Extraction

A copy of the logical storage objects (e.g., directories and files) that reside on a logical store (e.g., flash memory) of a mobile device[54]

Manual Extraction

Involves viewing the data on the phone directly as viewed on its screen using the device's keypad and documenting the information manually (e.g., with a digital camera)[55]

Network Forensics

The investigation of network traffic patterns and data captured in transit between computing devices[56]

Nonconsensual Pornography

The distribution of nude/sexually explicit images or videos of an individual without their consent. These images/video may have been consensually produced or obtained in the context of an intimate relationship or they may have been nonconsensually produced or obtained (e.g., the use of secret cameras, hacking)[57]

Physical Extraction (Hex Dump)

A bit-for-bit copy of an entire physical store (e.g., flash memory) of a mobile device[58]

Sextortion

A form of cyber extortion in which offenders demand that victims provide them with sexual images, sexual favors, or other things of value and threaten to harm or embarrass the victim if they fail to comply[57]

Swatting

The false reporting of an emergency to public safety agencies for the intent of getting a "SWAT team" response to a location where no emergency exists[59]

Technology-Facilitated Abuse

Acts or courses of conduct facilitated through digital means that compromise the victim's privacy and cause them emotional, physical, or reputational harm[60]

Web Crawler

A program, software, or programmed script that browses the World Wide Web (or dark web) in a systematic, automated manner[61]

[54] Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence*. Priority Criminal Justice Needs Initiative. https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

[55] U.S. Department of Health and Human Services. (2019, May). *What is bullying*. https://www.stopbullying.gov/what-is-bullying/index.html

[56] Palmer G. (2001). A road map for digital forensic research. Technical Report DTR-T0010-01. https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

[57] Eaton, A. A., Jacobs, H., & Ruvalcaba, Y. (2017). *2017 nationwide online study of nonconsensual porn victimization and perpetration*. Cyber Civil Rights Initiative, Inc. https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

[58] Corez, P. (2015). *Mobile forensics: Where are you going? Where have you been?* Sandia National Laboratories. https://www.osti.gov/biblio/1251554

[59] National 911 Program. (2015, May). *Public safety information on "swatting."* https://www.911.gov/pdf/National_911_Program_Public_Safety_Information_Swatting_2015.pdf

[60] Witwer, A. R., Langton, L., Vermeer, M. J. D., Banks, D., Woods, D., & Jackson, B. A. *Countering technology-facilitated abuse: Criminal justice strategies for combating nonconsensual pornography, sextortion, doxing, and swatting*. RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA108-3.html

[61] Kausar, A., Dhaka, V. S., & Singh, S. K. (2013). Web crawler: A review. *International Journal of Computer Applications, 63*(2). https://research.ijcaonline.org/volume63/number2/pxc3885125.pdf