Onion Services in the Wild: A Study of Deanonymization Attacks

Pascal Tippe
FernUniversität in Hagen
Hagen, Germany
pascal.tippe@fernuni-hagen.de

Adrian Tippe
Hochschule für Technik und Wirtschaft Berlin
Berlin, Germany
adrian.tippe@student.htw-berlin.de

ABSTRACT

Tor, the leading anonymization network, routes traffic over multiple relays to ensure client anonymity. Its Onion Services allow users to host services within the Tor network without revealing their location. While these techniques are crucial for users in authoritarian regimes and whistleblowers, they are also exploited by criminals. This paper diverges from the common focus on the technical vulnerabilities of the Tor protocol and instead explores the practical aspects of deanonymizing Onion Service users and operators. Despite Tor's robust security mechanisms, human errors in its usage and operation frequently lead to deanonymization. This study models law enforcement agencies as powerful attackers and evaluates documents from 136 court cases to determine investigative methods. We find that investigators employ different methods depending on the offense, with user mistakes being the dominant angle. Technical attacks, though comparatively rare, are highly effective and can potentially impact a large number of users simultaneously. Attacks on the well-researched Tor protocol are exceptionally rare, but their impact is even more significant. We argue that the human aspect of using Tor is the most critical deanonymization angle and that tailored guidelines for ethical users can help protect them from oppressive retaliation while still enabling the prosecution of criminal activity.

KEYWORDS

Tor, Tor study, Onion Service, deanonymization, court case analysis

1 INTRODUCTION

Tor [6] has emerged as the leading anonymization network, ensuring fundamental rights such as freedom of expression and privacy. It serves as an invaluable tool for whistleblowers and political activists worldwide [2] and offers uncensored internet access to users in authoritarian regimes. Tor is open-source software that relies on currently over 7,500 volunteer relays [25] to route user traffic over multiple hops, concealing the traffic's origin and destination. This prevents local adversaries from eavesdropping and conceals the origin IP address of users, enabling anonymity. Onion Services, another feature of the Tor network, allow users to set up anonymous services operating inside the Tor network. This feature enables the hosting of anonymous websites and other services, making them resistant to censorship and providing a secure platform for whistleblowers to highlight grievances. However, criminals also exploit Tor to evade law enforcement detection, with Onion Services sometimes acting as enablers of crimes and central coordination points. Law enforcement agencies have to use sophisticated technical attacks to identify operators and halt their operations.

Academic research primarily focuses on technical vulnerabilities of the Tor protocol and analyzes several angles to break the Tor anonymization and potential countermeasures. Prominent examples are fingerprinting attacks where local eavesdroppers could identify the destination of encrypted Tor traffic by matching patterns or including malicious Tor relays in the network to engage in traffic analysis attacks, linking the origin and destination of Tor traffic and effectively deanonymize users. The practical impact of many vulnerabilities is challenging to quantify as experiments are usually limited to test environments. Larger field tests are not carried out due to potential harm to affected Tor users. Also, complex attacks require a large budget, access to highly qualified personnel, and they are still potentially detectable in the privacy-focused Tor community.

While academic research has significantly improved the technical security of Tor and Onion Services, the users remain a less-explored area. Despite the robust protection offered by the default Tor browser, it is not easy to use or operate Onion Services without making mistakes that could allow attackers to deanonymize them. Comprehensive guidelines or orientation are currently lacking, which severely affects users from censored regions facing retaliation from authoritarian regimes. Attackers can exploit this and focus on human mistakes from users and operators rather than developing complex scenarios. Less powerful attackers might also be restricted to relatively more straightforward attacks due to insufficient resources. For our analysis, we assume that law enforcement agencies model powerful attackers and use court cases to analyze how users and operators of Onion Services are deanonymized. The rationale is that they are legally constrained, but they are well-resourced and persistent in identifying criminals. We formulated the following research questions:

- Which techniques do law enforcement agencies use to deanonymize users and operators of Onion Services?
- How commonly are these techniques utilized?
- What are common mistakes of users and operators of Onion Services?
- Are the investigative methods dependent on the investigated offense?

With these research questions, we focus on Onion Service users and operators and systematically analyze the influence of human behavior on their security. This knowledge can assist in creating new guidelines for ethical and secure Onion Service usage. Results from the analysis can also assist law enforcement in systematizing investigative methods and potentially underutilized angles. We take their perspective into account and aim to create guidelines that

Proceedings on Privacy Enhancing Technologies 2024(4), 291–310

https://doi.org/10.56553/popets-2024-0117

benefit ethical users and operators of Onion Services while still allowing effective investigations of criminal activities.

The remainder of this paper is structured as follows: Section 2 provides a brief overview of Tor and the Onion Service protocol. Section 3 discusses related work on Onion Services and classifies common attack vectors. These help to understand ongoing academic research on Onion Services and Section 4 provides background for understanding the following court case analysis. In Section 5, we present our methodology of data collection and analysis of the court cases. Section 6 details the results from the data collection that are subsequently analyzed in Section 7. We discuss the ethical implications, main findings, recommendations, limitations and future work in Section 8, while Section 9 concludes.

2 TOR ONION SERVICES

The Tor network is designed to provide a low-latency anonymity network that prevents attackers from linking communication parties [6]. It is a decentralized network, made up of volunteer servers that act as Tor relays, forwarding data for other participants. Clients select multiple Tor relays, typically three, and incrementally establish a connection. The first relay they connect to is known as the entry guard which is instructed to contact the next relay. This process continues until the circuit includes the last relay, referred to as the exit relay. Clients then send and receive traffic over the circuit, with each node only aware of its direct predecessor and successor. Recipients, such as internet websites, only see that the traffic originates from the exit relay. To prevent relays from observing the traffic content, clients negotiate symmetric encryption keys with each involved relay using asymmetric handshakes. Clients encrypt the 512-byte fixed-size cells multiple times with the symmetric keys, allowing each relay to peel off one layer until the exit relay handles the cleartext cell. For incoming cells destined for the client, each relay adds another encryption layer until the client removes all layers.

Onion Services [26], a feature of the Tor network, enable servers to maintain anonymity and provide anonymity for clients connecting to them. For instance, operators can provide websites or SSH remote access over Tor to protect server and client anonymity. Initially, Onion Services select multiple Tor relays as introduction points and establish circuits to them. They then publish service descriptors which include identifiers for the selected introduction points together with cryptographic keys. These service descriptors are stored in a distributed hash ring constituted by Tor relays with a directory flag. Random values are used to prevent attackers from precisely placing malicious Tor relays to observe or block descriptor fetches. Clients can fetch the service descriptor by querying the .onion address of the targeted Onion Services, which is derived from the master identity key. Subsequently, clients select a relay to act as a rendezvous point and build up a circuit to it. They then contact the introduction points from the Onion Service with information about the rendezvous point, a cookie and a partial handshake. The introduction points forward the connection requests to the Onion Service which then establishes a circuit to the rendezvous point and delivers the cookie. Finally, the rendezvous point connects the two circuits from the client and Onion Service based on their cookie allowing them to complete the handshake. As a result, both parties can communicate without revealing their location. However, it's important to note that while Tor provides a transparent reverse proxy for Onion Services that obfuscates the IP addresses, it doesn't affect the traffic content. This leaves servers vulnerable to a large number of potential attack vectors that could potentially deanonymize them. Therefore, these servers need to be substantially more secure than regular web servers, as identifiers that would not affect normal websites could endanger the operators.

Central directory relays, called directory authorities, act as trustworthy authorities. They vote each hour to create a consensus document describing the state of the network. It includes, inter alia, signed descriptions about relays, statistics, and recommended parameters. A naive Tor relay selection algorithm chooses new relays from the consensus for each new circuit. Attackers can inject malicious Tor relays, called Sybils, into the Tor network since volunteers run it decentrally. Compromising the entry and exit relay enables attackers to deanonymize clients via traffic analysis. Øverlier and Syverson [44] described a feasible attack on Onion Services. The central idea is that attackers can force an Onion Service to create new circuits and check via timing analysis if the target uses a compromised entry guard. Currently, clients choose a fixed set of Tor relays for a prolonged time period and use them as entry guards. That decreases the likelihood of Sybil attacks enormously. For the middle and exit relays, clients select randomly from the consensus based on bandwidth and bandwidth-weight. Directory authorities help clients selecting appropriate relays by voting about flags of Tor relays in the consensus, and they can flag malicious relays as bad. Major protocol revisions have been made since inception, and the specification remains subject to change. Current protocols still contain legacy options due to the slow adaptation of changes [5].

3 RELATED WORK

Various publications have identified vulnerabilities in the Tor protocol that affect Onion Services. In addition, operators can also make mistakes that are not directly related to Tor but indicate a lack of operational security and misconfigurations. Since the range of possible attack vectors is very large, presented related work is limited to risks that specifically apply to Onion Services. Since Onion Services utilize the same software as internet services, they are generally vulnerable to the same vulnerabilities. Next to the vulnerabilities, we also describe existing guidelines from the Tor project website.

3.1 Tor Deanonymization

Operational security Matic et al. present an automized tool, Caronte [14], to extract information about Onion Services. They automatically search the website and certificates for potentially identifying information, for example, IP addresses or DNS names on the error page. This potentially allows attackers to connect different information if it appears elsewhere. Al Jawaheri et al. [1] crawled Onion Services to collect Bitcoin addresses combined with a manual collection. They identified a few users by combining public data from Twitter and other social media platforms. Attackers can try to trace money flows which must take place safely to protect the Onion Service and donors. Me et al. [15] scrape PGP public keys

from vendors on Onion Service markets, extract signatures and consult key servers to conduct a social network analysis showing actors with their connections. In [22], 22 court cases were briefly analyzed to generate an overview of vulnerabilities for Onion Services.

Technical attacks Panchenko et al. [19] simulate a website fingerprinting attacker who listens to the link between the client and the entry guard. In two phases, they determine if a client connects to an Onion Service and then compare traffic features to identify the visited service from a candidate set. Yang et al. [43] present an active fingerprinting attack that delays HTTP requests to improve the detection rate. Kwon et al. [12] show how duration, initialization sequences, number of cells, and direction leak information about the circuit type. Iacovazzi et al. [10] developed a watermarking technique that exploited a vulnerable traffic congestion mechanism in Tor and TCP. It induces a pattern of silent communication periods that entry guards of Onion Services can detect. Chen et al. [3] deployed malicious relays, called Sybils, to observe Onion Service circuits initiated by malicious clients. Combined with watermarks, they could identify entry guards for Onion Services if their Sybil is a middle relay in an initiated circuit. Iacovazzi et al. [9] exploited the congestion control mechanism in Tor with *SENDME* control cells. Ling et al. [13] exploit protocol-level behavior. The client-side inserts a corrupt package into the circuit that forces the Onion Service to close the connection. By correlating timing and cells, attackers can deanonymize Onion Services. Protocol violations lead to the termination of streams, thus leaving conspicuous traces. Murdoch [17] induced workload on Onion Services via traffic leading to slightly different clock skews. A server in a preselected candidate set could be deanonymized by comparing timestamps from TCP probes. Simioni et al. [21] correlate the uptime of an Onion Service with public availability information to identify servers among a candidate set.

3.2 Security Guidelines

The Tor Project provides a set of basic guidelines [24] for securely hosting Onion Services, currently consisting of six bullet points with additional references. These references [16] primarily detail the technical setup and how to counter advanced technical attacks, such as those involving malicious Tor relays, traffic analysis, and fingerprinting attacks. One reference [20] provides advice on avoiding common misconfigurations and cautions users against revealing identifying information. Another page warns users about the risks of clicking links, opening attachments, and emphasizes the importance of using strong passwords. However, upon further internet searches for guidelines tailored to whistleblowers, general Tor users, and Onion Services, we found that advice is scattered and sometimes counterproductive, such as recommendations to combine VPNs with Tor [7], or references to outdated Tor versions. We were unable to locate a comprehensive guideline for whistleblowers or other ethical Tor users on how to navigate Tor securely. Information specifically about Onion Services is even more scarce.

4 U.S. CRIMINAL COURT PROCESSES

For the purpose of this paper, U.S. court documents will be analyzed and referenced, warranting a basic understanding of the U.S. court system. In the United States, the criminal justice system [18] is a structured process initiated by law enforcement agencies that conduct investigations. Upon gathering sufficient evidence, the case is handed over to the prosecution, which then decides whether to file charges. This critical decision often involves a grand jury, tasked with evaluating the evidence to ascertain if it justifies a trial. During the trial, the prosecution bears the burden of proof and is required to prove the defendant's guilt beyond a reasonable doubt. Judges are instrumental throughout this process, diligently ensuring the integrity of the proceedings by enforcing the rules of evidence and legal procedures. They are responsible for determining the admissibility of evidence and instructing the jury on the legal standards to be applied, all while maintaining a fair and impartial trial environment. In the case United States v. DeFoggi [33], the presiding judge described to the jury their role as follows:

> *It will be your duty to decide from the evidence whether the defendant is guilty or not guilty of the crimes charged. From the evidence, you will decide what the facts are. You are entitled to consider that evidence in the light of your own observations and experiences in life. You may use reason and common sense to draw deductions or conclusions from facts established by the evidence.*

Defendants have the right to file motions to suppress evidence, which, if granted, would prevent the evidence from being presented to the jury, or to dismiss the case altogether. Judges have considerable discretion in ruling on these motions. It is important to note that court documents from the trial are strictly factual and do not contain personal opinions from either the judge or the jury, as the jury's deliberations are conducted in private. Following a guilty verdict, the judge imposes a sentence guided by established guidelines, taking into account any mitigating or aggravating factors. While these considerations may reflect the judge's personal judgment, they are grounded in the facts and outcomes of the trial.

5 METHODOLOGY

While academic literature often explores theoretical attack vectors, practical experiments are limited to ensure the preservation of Tor network participants' anonymity. This cautious approach, while necessary, leaves a gap in our understanding of real-world deanonymization strategies and their frequency of successful application. It is crucial to comprehend the practical attacks that users and operators are likely to encounter. However, discerning the modus operandi of attackers is a complex task. Attackers typically maintain secrecy around their methods to prevent targets from adapting their defenses. For a comprehensive analysis, we require systematic and verifiable information, which is often lacking in sources like blog posts, newspaper articles, and YouTube videos. These sources frequently overlook technical investigative details, and the diverse range of authors, often with little background information, makes it challenging to assess the reliability of the information.

This study addresses these challenges by examining U.S. court documents related to cases involving illegal activities conducted through Tor Onion Services. These documents serve as a proxy to investigate real-world deanonymization techniques. Law enforcement agencies are obligated to explain their methods of identifying suspects to secure a conviction in court. Although these documents

may not fully detail all investigative methods, they offer valuable insights. Despite the legal constraints they operate under, U.S. law enforcement agencies have substantial budgets and access to resources, making them formidable adversaries compared to hacking groups or intelligence services in oppressive countries. While U.S. court documents are generally publicly accessible, some may be sealed or partially redacted, for instance, to protect ongoing investigations.

5.1 Data Collection

First, we collected potential court cases for further examination. Since there is no full-text search available for court cases, we queried the U.S. Department of Justice website for press releases and documents using their integrated search engine. This introduces a bias, as only court cases related to press releases are analyzed. However, we consider these cases to have more public attention and likely more investigative resources allocated to them. This approach also improves the sampling, as rare circumstances like apprehending operators will not be overshadowed by the larger number of more common offenses. During an initial search, we examined the structure and terminology of the press releases, noting that the terminology is less precise compared to academic notations. We noticed that prosecutors use a consistent wording for describing cases involving Tor and Onion Services and adapted our key words accordingly. The term Darknet is primarily associated with Tor, and the former name for Onion Services, "hidden services," is still prevalent. Subsequently, we selected three key phrases to filter relevant results mentioning Tor or Tor Onion Services:

- "Darknet"
- "hidden service"
- "Tor network"

To ensure the consistency and accuracy of our data, we conducted the search on the same day and saved the results for subsequent manual inspection. Press releases may contain supplementary resources and can simultaneously mention defendants from multiple separate court cases. We incorporated all supplementary resources into our analysis and recorded the defendants' names and the district court for each case. If a press release referred to another as supplementary material, we included this in our analysis. For results that linked to documents, we noted the case number and the district court. We observed that the number of returned results varied significantly between the key phrases. In particular, the key phrase "Darknet" yielded a large number of offenses related to drugs. To manage the volume of data and balance the dataset, we decided to limit the number of included results for this phrase to the first ten pages, while processing the complete result list for the other two phrases.

We utilized the Public Access to Court Electronic Records system (PACER) to locate corresponding court cases by querying the defendants' names and district court from the press releases. If a document was provided, we used the case number. We then examined the case docket, which contained the attached documents, and downloaded those that were relevant. Many of these documents were brief, spanning one or two pages, and often indicated procedural events such as the attendance of individuals or announcing deadlines. To minimize the inclusion of irrelevant documents, we concentrated on criminal complaints or indictments that supported the charge, pretrial motions that requested the court to decide on issues before the trial commenced, and sentencing memorandums that argued about the appropriate sentence. For cases that concluded with a plea agreement, we analyzed the stated facts. For cases that proceeded to trial, we examined trial transcripts and motions filed during and after the trial had concluded. If a case did not yield sufficient useful information due to sealed or redacted documents or an early plea agreement, we sought additional court documents published by journalists by searching for the case number and the name of the defendants. If the court case still yielded insufficient or too few investigative facts, we excluded it from the analysis.

After collecting the relevant court case documents, we proceeded with their preliminary analysis and applied predefined selection criteria to filter out irrelevant court cases. Based on our initial research questions, we determined that a court case is relevant if at least one of the following three points apply:

- Defendant was running an Onion Service
- Investigation started on an Onion Service
- Significant part of the the crime relied on Tor

5.2 Offenses and Investigative Methods

Our methodology started with a focus on potential investigative techniques and the variety of offenses encountered. Two reviewers, both with expertise in IT security, began by examining 30 randomly selected court cases. They independently annotated these documents, which facilitates their understanding of the legal language and structure. Given the diversity of investigative techniques and offenses, we adopted an iterative, inductive strategy, incorporating both open and selective coding processes. During three rounds of open coding, the reviewers independently identified and extracted text segments detailing the methods law enforcement employed to deanonymize Tor users. These segments allowed us to maintain the context of the investigation, with key terms highlighted to aid in the organization of the data. Subsequent discussions allowed the reviewers to deconstruct complex statements into sub-statements and categorize them into distinct clusters. For example, a crawled "*public PGP key indicated that this key was registered to Babadjov@***.com. A social media search for Babadjov@***.com resulted in the discovery of a Facebook account*"[35]. This comprises public information (the PGP key), extracting the associated email address (metadata), and linking the email address to another service (linking pseudonyms).

As the discussion rounds progressed, a third reviewer with a non-specialist background in IT security was brought in to validate the accuracy of the representation. This reviewer did not engage with the full court cases but rather focused on the synthesized statements and annotations provided by the primary reviewers. After the third iteration, with only minor adjustments observed between the second and third round, open coding was concluded. The reviewers then proceeded to define and name the hierarchies within the clusters, which formed the basis for categorizing the offenses and investigative methods. The two expert reviewers concluded a high level of agreement, and one proceeded to apply selective coding to the remaining documents. Throughout this process, any unusual

Table 1: Overview of investigative methods.

Method	Explanation
Surveillance	
Physical	Surveillance of physical movements
Online	Surveillance of online activities
Linking information	
Pseudonyms	Linking pseudonyms across platforms
Cryptographic keys	Linking cryptographic keys across platforms
Private information	Linking non-public data
Public information	Linking publicly available information
Metadata	Linking metadata
Associated accounts	Linking associated accounts
Shared characteristics	Linking other information
Crypto tracing	Tracing cryptocurrency movements
Undercover infiltration	Infiltrating with undercover agents or confidential informants
Malware	Unmask Tor users with malware
Witnesses	
Third party	Information from a third party
Co-Conspirator	Information from a co-conspirator
Misconfigurations	Misconfigurations that bypass Tor
Tor protocol attacks	Protocol attacks that break the Tor anonymity
Physical search	Investigating physical items

terms or phrases encountered in the court documents were discussed with the other expert reviewer. In one instance concerning the private information method, the third reviewer was consulted again.

The offenses were then categorized based on the established clusters. For instance, CSAM refers to individuals involved with child sexual abuse materials, while drug vendors and other vendors represent those selling substances and various goods on Onion Service marketplaces. The category of Onion Services includes those managing and securing the infrastructure, whereas employees encompass moderators and administrators who facilitate the operation without controlling and organizing the physical infrastructure. Onion Service customers are those purchasing illicit items such as drugs, poisons or engaging in murder-for-hire services. The hacking category covers ransomware infrastructure and hacking collectives, and a single case involves espionage. For CSAM cases, we specifically noted associations with larger operations.

For each case, we marked the identifying lead deanonymizing the defendants by searching for explicit statements within the court documents. This often pinpointed the breakthrough in the investigation. Table 1 lists the investigative techniques with explanations and examples. When documents provided vague details, we inferred the most likely method used and checked if other documents or press releases provided further hints. If a single explanation was plausible, we adopted it; otherwise, we refrained from drawing conclusions and excluded the information. Not all cases disclosed the initial identifying lead, and some involved multiple agencies concurrently investigating the defendants. If a case has multiple defendants with separate identifying leads, we marked the identifying lead for each defendant. If interconnected cases revealed methods used in related cases, we counted the technique for all associated cases.

5.3 Further Case Information

After a thorough analysis of the court documents for investigative methods and considering external feedback, we have broadened our research questions and extended our codebook. Our aim is to incorporate legal dimensions such as the status of cases, the handling of digital evidence, and the role of foreign law enforcement agencies in the investigations. The resulting research questions are as follows:

- To what extent do investigative methods detailed in U.S. court documents reflect the practices of international law enforcement?
- In what ways do defendants challenge digital evidence in court?
- What legal issues arise from the investigative methods employed?

Utilizing their notes from the initial analysis, the expert reviewers deductively introduced new categories, supported by examples, into the revised codebook. To validate these additions, the experts selected 20 court cases that had generated extensive notes during the initial coding phase. They then independently reviewed these cases over two rounds, engaging in discussions between rounds to refine the newly added categories. The final version of the codebook is detailed in Appendix A and B. This phase also provided an opportunity to assess the inter-rater reliability of our codebook. We distributed 10 randomly chosen court cases among all three reviewers and compared their coding outcomes. The agreement among reviewers was quantified using Krippendorff's alpha coefficient [11], resulting in the value $\alpha \approx 0.82$, indicating a high level of consensus. Subsequently, one expert reviewer continued the selective coding of the remaining court documents. The third reviewer, who was directly exposed to the court documents for the first time, reported challenges in understanding the language and structure of the documents, as well as navigating the docket system. This reviewer's lack of a strong IT security background further complicated the ability to identify methods that were not explicitly stated but implied, as highlighted in one comment during a discussion:

"*My knowledge of Coinbase didn't lead me into crypto tracing.*"

In our analysis, we recorded instances where defendants contested the evidence, either by seeking to suppress parts of it or by moving to dismiss the entire case. Legal challenges were noted when evidence was argued to have been obtained unlawfully, such as through inadequately supported search warrants, warranting its exclusion. Technical challenges refer to disputes over the authenticity of forensic examinations or the scientific standards of the methods used. We also documented instances of appeals against court decisions. The trial outcomes were categorized as follows: plea agreements, verdicts (jury, bench, or default judgment), ongoing cases, unknown outcomes, trials conducted abroad, and other outcomes. To account for co-defendants tried abroad and extradition processes, we introduced two separate categories. When extradition was not explicitly mentioned in court documents, we sought additional information from newspaper articles detailing extradition processes for defendants residing outside the U.S. The involvement of foreign law enforcement agencies (FLAs) was tracked, noting whether they participated in or initiated the investigation.

6 DATA COLLECTION

Table 2: Results of the collection process.

Key phrase	*Search results*	*Extended results*	*Not Tor*	*Already done*	*Court cases*	*Evaluated court cases*
Darknet	200	255	63	/	94	65
"hidden service"	171	171	4	10	37	30
"Tor network"	283	291	10	35	53	41
	654	717	77	45	184	136

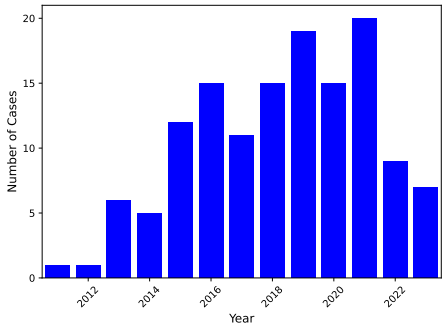

Figure 1: Number of analyzed court cases by year.

Table 3: Case number per offenses separated by key phrases.

Key phrase	*CSAM*	*Drug vendor*	*Employee*	*Espionage*	*Hacking*	*Onion Service customer*	*Onion Services*	*Other vendors*
Included court cases								
Darknet	9	43	/	1	1	5	4	1
"hidden service"	11	9	3	/	1	/	6	1
"Tor network"	13	11	4	/	1	/	6	6
	33	**63**	**7**	**1**	**3**	**5**	**16**	**8**
Excluded court cases								
Darknet	1	28	/	/	/	/	/	1
"hidden service"	3	/	1	/	/	/	1	1
"Tor network"	8	1	/	/	2	/	/	1
	12	**29**	**1**	**/**	**2**	**/**	**1**	**3**

Table 2 presents the results of our queries on the U.S. Justice Department website, conducted on September 1, 2023, using the three key phrases outlined in the methodology. We initiated the search with the *"Darknet"* key phrase, followed by *"hidden service"* which yielded nine pages of results, and then *"Tor network"* which yielded 15 result pages. The *Search results* column shows the initial number of returned results. The *Extended results* column includes instances where some press releases detailed multiple court cases or referred to other press releases. Subsequently, we filtered out cases not involving Tor and court cases that were already identified by previous key phrases. The order of key phrases affects these numbers. The *Court cases* column presents the number of court cases for each key phrase, and the *Evaluated court cases* column excludes court cases with too little evaluable information. Notably, the first key phrase, *"Darknet"*, brought up many unrelated court cases and had the most sealed and redacted documents. This is due to larger operations where law enforcement agencies did not fully disclose their procedures to avoid alerting other investigated suspects. The other two key phrases were more targeted, and the relative number of evaluated court cases was larger.

Table 3, as presented in this paper, categorizes offenses by keyword and provides an overview of cases that were excluded from our analysis. The largest number of cases involved drug vendors, followed by those involving CSAM. Interestingly, operators of Onion Services, which host the platforms where these offenses occur, constituted the third largest group with 16 cases. This may reflect the increased scrutiny these platforms receive due to their role in enabling a significant number of users to commit crimes, and the technical expertise required to set them up. The trend in the excluded cases was similar, although the number of cases involving Onion Services was lower. This could be due to the heightened public interest in these cases, leading to more scrutiny of associated court documents. A notable observation was that in the included court cases, CSAM producers made up 2 out of 33 cases, while in the excluded cases, the ratio was 4 out of 12. This discrepancy could suggest that law enforcement agencies are more cautious in revealing their investigative methods in cases involving CSAM producers.

7 ANALYSIS

The dataset encompasses 38 out of 94 district courts in the U.S. The three district courts with the highest number of cases are the Eastern District of California, the Eastern District of Virginia, and the Central District of California, with 15, 15, and 14 cases respectively. The number of inhabitants per district court varies, and it is plausible that different jurisdictions have differing resources for investigations. Additionally, some may provide fewer announcements on the U.S. Justice Department website. The earliest case in the dataset was filed in 2011, and the most recent in 2023. From 2011 onwards, the number of cases per year generally increased, despite occasional setbacks. The Playpen operation identified numerous defendants simultaneously, resulting in 4 cases filed in 2015, 9 in 2016, and 2 in 2017. This suggests that investigations can span a prolonged period and continue to yield new cases even two years after the deployment of the malware. The recent decrease in cases does not necessarily indicate a downward trend, as case proceedings can be lengthy and press releases often announce verdicts rather than new cases. Therefore, ongoing cases may appear on the U.S. Justice Department website with some delay.

7.1 Investigative Method Analysis

Table 4 provides detailed statistics on the utilized investigative methods and shows the percentage of how often they were applied. The second number in parentheses indicates how often this investigative method was the identifying lead. Both values are rounded

Table 4: Investigative method analysis by offense, first number represents percentage of cases where investigative method was used and number in parentheses shows percentage of identifying leads for the case category both rounded to the first decimal place.

	Surveillance		Linking information										Witnesses				
Number of cases	*physical*	*online*	*Pseudonyms*	*Cryptographic keys*	*Private information*	*Public information*	*Metadata*	*Associated accounts*	*Shared characteristics*	*Crypto tracing*	*Undercover infiltration*	*Malware*	*Third party*	*Co-conspirator*	*Misconfigurations*	*Tor protocol attacks*	*Physical search*
Offense type: Drug vendor																	
63	92.1 (36.5)	20.6 (1.6)	55.6 (3.2)	30.2 (0)	42.9 (4.8)	42.9 (1.6)	30.2 (6.3)	52.4 (3.2)	66.7 (6.3)	28.6 (0)	77.8 (4.8)	0 (0)	39.7 (6.4)	27 (15.9)	0 (0)	0 (0)	74.6 (4.8)
Offense type: Onion Services																	
16	25 (0)	37.5 (6.2)	31.2 (0)	31.2 (0)	0 (0)	56.2 (0)	78.8 (18.8)	100 (6.2)	25 (0)	68.8 (6.2)	100 (0)	0 (0)	0 (0)	18.8 (0)	37.5 (37.5)	6.2 (6.2)	62.5 (0)
Offense type: CSAM (Playpen)																	
15	0 (0)	100 (0)	6.7 (0)	0 (0)	0 (0)	13.3 (0)	0 (0)	6.7 (0)	13.3 (0)	0 (0)	6.7 (0)	100 (100)	13.3 (0)	0 (0)	0 (0)	0 (0)	93.3 (0)
Offense type: CSAM																	
13	23.1 (0)	23.1 (7.7)	15.4 (0)	0 (0)	30.8 (0)	38.5 (15.4)	53.8 (0)	38.5 (0)	38.5 (0)	0 (0)	38.5 (0)	0 (0)	38.5 (0)	23.1 (7.7)	15.4 (15.4)	0 (0)	100 (15.4)
Offense type: Other vendors																	
8	87.5 (25)	0 (0)	37.5 (0)	12.5 (0)	50 (12.5)	25 (0)	12.5 (0)	50 (0)	25 (0)	12.5 (12.5)	75 (12.5)	0 (0)	25 (0)	37.5 (12.5)	0 (0)	0 (0)	12.5 (12.5)
Offense type: Employees																	
7	42.9 (0)	14.3 (0)	57.1 (14.3)	14.3 (0)	71.4 (0)	57.1 (0)	28.6 (0)	28.6 (0)	42.9 (0)	0 (0)	57.1 (14.3)	14.3 (14.3)	28.6 (0)	28.6 (14.3)	0 (0)	28.6 (28.6)	71.4 (0)
Offense type: Onion Service customers																	
5	60 (20)	0 (0)	40 (0)	0 (0)	40 (0)	20 (0)	20 (0)	100 (0)	60 (0)	60 (20)	60 (20)	0 (0)	60 (0)	20 (20)	0 (0)	0 (0)	60 (0)
Offense type: CSAM (Torpedo)																	
3	0 (0)	100 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	100 (0)	100 (100)	0 (0)	0 (0)	0 (0)	0 (0)	100 (0)
Offense type: Hacking																	
3	0 (0)	33.3 (0)	66.7 (33.3)	0 (0)	33.3 (0)	33.3 (0)	33.3 (0)	100 (33.3)	33.3 (33.3)	33.3 (33.3)	66.7 (0)	0 (0)	33.3 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Offense type: CSAM (Welcome to Video)																	
2	50 (0)	0 (0)	0 (0)	0 (0)	50 (0)	50 (0)	0 (0)	100 (0)	0 (0)	100 (100)	0 (0)	0 (0)	50 (0)	0 (0)	0 (0)	0 (0)	100 (0)
Offense type: Espionage																	
1	100 (100)	100 (0)	0 (0)	0 (0)	0 (0)	0 (0)	100 (0)	100 (0)	0 (0)	0 (0)	100 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	100 (0)
All cases																	
136	58.8 (19.9)	31.6 (2.2)	39.7 (2.9)	19.1 (0)	32.4 (2.9)	38.2 (2.2)	31.6 (5.1)	52.9 (2.9)	45.6 (3.7)	26.5 (4.4)	66.2 (4.4)	14 (14)	30.1 (2.9)	21.3 (10.3)	5.9 (5.9)	2.2 (2.2)	72.8 (4.4)

to the first decimal number. In the 136 analyzed court cases, the most commonly used investigative methods, present in more than 50 % of all cases, resemble traditional methods that can also be applied outside of online investigations. While associated accounts mostly refer to mail or other online accounts, they are similar to subpoenaing business records. This shows that online investigations share some characteristics with traditional methods. Out of these methods, only physical surveillance generates around 19.9 % of identifying leads for investigations, while the others are used to continue leads or collect additional evidence to secure a conviction. The low number of identifying leads for undercover infiltration is surprising, as social engineering is a common attack vector. However, either law enforcement didn't fully make use of it, or the defendants were careful in their interactions. Linking pseudonyms, shared characteristics, metadata, public information, and private information were also commonly used, with percentages between roughly 30 % and 45 %. Individually, they rarely generate the identifying lead, but cumulatively they account for 16.8 %, with metadata and shared characteristics providing slightly more identifying leads. This is likely because these methods are rather indirect compared to pseudonyms or public information and therefore harder to conceal. Generally, the more data users leave, the easier it is to tie it to a person. Online surveillance is used in roughly one-third of all cases but is primarily used to collect additional evidence with pen traps indicating Tor traffic, tracking phone locations tied to criminal acts, or tracking user accounts on platforms. Crypto tracing is an exclusive method for digital investigations that affects all actions involving digital currencies; however, the percentage values are quite low. Likely, the use of mixing services or privacy-preserving cryptocurrencies makes investigations harder, while when the wallets of suspects are known, it is possible to indicate suspicious transactions for a wallet as circumstantial evidence. Hints from third parties and co-conspirators are used in 30.1 % and 21.3 % of all cases, respectively. The former helps to further confirm suspicions, while defendants rarely get identified with it. Co-conspirators are more effective in this situation, with 10.3 % of identifying leads showing that law enforcement agencies can crawl through criminal networks after apprehending individuals. Cryptographic keys are the least common technique from the linking information category and, as the only method, provide zero identifying leads. Still, they helped associate accounts or posts with each other, and the containing metadata or public information from key servers aided investigators. The three least common techniques are decidedly different from the others because they involve technical attacks, and each time they were applied, they also provided the identifying lead. Malware and misconfigurations are comparatively rare methods, with 14 % and 5.9 % respectively, but are highly effective. These methods require more technical preparation, so the percentage is still surprisingly high and is likely due to the increased public attention to the results in the data collection process. While the previous two technical attacks did not affect the Tor protocol but are rather the result of user behavior and technical configuration, the Tor protocol attacks break the Tor anonymization and affect all users. Only in three cases was this method used, and all go back to the same deanonymization attack on the Tor network, demonstrating that this attack is rare.

7.2 Investigative Method Analysis by Offense

Table 4 also groups the statistics about the investigative methods by offenses. CSAM is further divided into subcategories because there were three major operations that all followed a common pattern, deviating from the remaining cases. The Playpen and Torpedo cases identified all defendants by deploying malware on CSAM websites and confirming this with physical searches. Online surveillance, in the form of tracking activities on these websites, helped to collect additional evidence for the prosecution. In some cases, investigators collected additional evidence by linking pseudonyms, public information, undercover infiltration, and third-party witnesses. For the two Welcome to Video cases, investigators seized the CSAM website and tracked the cryptocurrency payments to identify the defendants and conduct physical searches. The low number of cases does not allow any other inferences other than the general strategy. The remaining general CSAM cases show a larger variety. Misconfigurations, physical searches, and linking public information were the most effective, each providing 15.4 % of the identifying leads, followed by online surveillance and co-conspirators, each with 7.7 %. Interestingly, all other methods did not provide any identifying leads, showing that these offenses involve fewer physical activities and also fewer cryptocurrency payments to track. Linking information and surveillance support the investigations.

Drug vendors have the largest case number, and it becomes clear that the physical activities involved in shipping drugs are the dominant sources for identifying leads, followed by information from co-conspirators. All methods from the linking information category help investigators, especially to link drug vendors across multiple platforms and even accounts. Undercover infiltration is another common method that mainly consists of buying drugs to generate further leads and become aware of the crime. Technical attacks are non-existent in this sample, showing that it is rather a continuous task not requiring vulnerabilities. Crypto tracing is used in 28.6 % of the cases but provides no identifying leads, which could be because of the use of Tor Onion Service platforms that obfuscate cryptocurrency flows.

Onion Services have a high rate of misconfigurations, with 37.5 % that, when utilized, always provided the identifying lead. This shows that these platforms offer a larger attack surface for misconfigurations and require more technical knowledge compared to solely using these platforms. Searching through associated accounts is always included, likely because records from the hosting provider will already provide additional leads. Undercover infiltration is also used in all cases, indicating that law enforcement agencies dedicate more resources to these platforms as this method requires human effort and is less standardized. Metadata is another rich source used in 78.8 % of the Onion Service cases and provides the identifying lead in 18.8 %, running these services requires some effort and configurations that are prone to unwanted metadata, especially IP addresses in logs. Cases in the other vendors category show similar patterns to drug vendors, but involve fewer physical searches and crypto tracing provides more identifying leads, which is because some deals are done outside of established Onion Service platforms with integrated protection mechanisms. The employee cases include a comparatively high number of technical attacks and successful undercover infiltration, which could show that law enforcement agencies focused more on them and also utilized rather expensive methods. The pseudonym linking could be because the employees have to maintain an online reputation if they are hired without personally knowing the administrators of Onion Services.

The remaining categories have too few cases to make meaningful inferences. Overall, the cases resemble highlighted cases from the justice department that might have attracted more investigative resources, and some cases have been excluded due to incomplete information, but still, some strategies are observable and they differ for the offense type. Physical surveillance and shared characteristics like fingerprints on packages or sending packages from the same post office are more common due to the physical nature of the offense, while other offenses stay more in the digital sphere. For the different CSAM categories, law enforcement conducted some operations using technical attacks to catch a larger number of users at once, which might be because criminals leave fewer observable traces.

7.3 Notable Technical Attacks

To further understand the threat of technical attacks and their effects, we describe the large operations in this subsection. The Playpen case started with the case United States v. Chase [40] and is a significant example of how Onion Service investigations are conducted, demonstrating how the FBI utilized technical attacks to unmask users' identities. Playpen, an Onion Service dedicated to CSAM, was already under the FBI's radar, with undercover agents regularly visiting the site. The breakthrough occurred when

> *a foreign law enforcement agency advised the FBI that it suspected IP address [...] to be associated with the TARGET WEBSITE [Playpen. The] FBI verified that the TARGET WEBSITE was hosted from the previously referenced IP address*

This is a clear misconfiguration since Onion Services should only be accessible via the Tor network, not directly from the internet. Upon obtaining a search warrant, investigators copied the server contents and discovered "*the actual Playpen administrator account was logged into directly from an IP address that could be traced.*" The associated hosting account revealed additional IP addresses and payment information, which were linked to further accounts. Physical surveillance at the locations registered to these IP addresses, along with queries to the private driver's license database, identified the suspects. Online surveillance of the suspects' internet connections indicated connections to the Tor network, and public social media posts were consistent with this surveillance. A subsequent search warrant authorized a physical search of the defendants' homes. The element of surprise allowed the FBI to take administrative control of the Playpen server. A co-conspirator later testified against the defendant in court. Following the takeover, law enforcement utilized a Network Investigative Technique, a form of malware that sends identifying information, including the unmasked IP address and session ID, directly to their server. The case of United States v. Sparks [36] is a classic example of the resulting cases:

> *According to data obtained from logs on "Website A," monitoring by law enforcement and the deployment of a NIT [malware], the user "CRAZYCATS" engaged in*

> *the following activity on "Website A" from IP address [...] law enforcement agents executed a search warrant at SPARKS's residence*

While assembling and analysing our dataset, we identified three additional operations involving law enforcement takeovers and subsequent malware deployment. Several cases, including United States v. Cottom [32] between November 18, 2012, and December 2, 2012, involved the infiltration of other CSAM Onion Services. Law enforcement used malware contained in a flash application to extract the IP address, operating system information, and session ID. During the investigation in United States v. Marques [31] in 2013, an IP address was identified that linked back to the Freedom Hosting Onion Service, which offered anonymous hosting for Onion Services. After analyzing the associated hosting account and checking further associated accounts linked to the payment address and method, law enforcement followed up on connected IP addresses and "*forwarded information regarding that [linked postal] address in Dublin, Ireland to Irish law enforcement for further investigation*". Physical surveillance conducted by Irish law enforcement confirmed that the defendant resided at the reported address. After copying the server, they cracked the encryption password and linked connection logs and cryptographic keys to the defendant. A physical search at his residence in Ireland allowed them to assume control over the infrastructure and plant malware to identify users of hosted services. Interestingly, not only CSAM-related Onion Services were targeted, but also a number of mail accounts on an Onion Service as seen in the search warrant application [30]. The third case United States v. Falte [38], from 2017, involved several connected CSAM Onion Services. Court documents did not provide a clear picture, only indicating that these services were connected, and one administrator was caught by tracing cryptocurrency used to pay for the server. Additional media coverage [4, 8] provided comprehensive details of the investigations, which began with identifying a moderator and assuming their online identity. Later, likely due to a misconfiguration, law enforcement identified an IP address for an Onion Service and traced cryptocurrency payments for the hosting provider to the operator. After arresting and taking administrative control, malware was again used to identify users.

Our analysis found only one attack on the Tor protocol. All other investigative methods could be mitigated by adapting behavior or secure technical configurations, which makes attacks on Tor particularly devastating. Three cases in our dataset were affected. In United States v. Farrell [41], documents show that in July 2014 "*the defendant's IP address was identified by the Software Engineering Institute ('SEI') of Carnegie Mellon University ('CMU') when SEI was conducting research on the Tor network*". A Tor security advisory [23] from July 30 details that a number of rogue Tor relays modified Tor protocol headers to conduct traffic analysis attacks, revealing unmasked IP addresses from Onion Services and users navigating on them. A press release [28] mentions that during this operation, more than 400 Onion Services were affected and seized. This highlights the extensive impact these Tor Protocol attacks can have, but also that they require well-resourced attackers. The effort for pursuing cases without technical attacks is lower, but technical attacks can potentially sweep more users and Onion Services at once.

Table 5: Distribution of trial outcomes across different offenses.

Offense	Trial outcome in percent						
	Number of cases	*Plea*	*Verdict*	*Ongoing*	*Unknown*	*Trial abroad*	*Other*
Drug vendor	63	88.9	0	7.9	1.6	0	1.6
Onion Services	16	31.3	12.5	6.3	6.3	25	18.8
CSAM (Playpen)	15	73.3	26.7	0	0	0	0
CSAM	13	76.9	15.4	7.7	0	0	0
Other vendors	8	100	0	0	0	0	0
Employees	7	71.4	14.3	0	14.3	0	0
Onion Service customers	5	80	20	0	0	0	0
CSAM (Torpedo)	3	100	0	0	0	0	0
Hacking	3	33.3	33.3	33.3	0	0	0
CSAM (Welcome to Video)	2	100	0	0	0	0	0
Espionage	1	100	0	0	0	0	0
All cases	136	77.9	8.1	5.9	2.2	2.9	2.9

Table 6: Legal analysis outcomes by offense type: number of cases is absolute and other numbers as percentage, rounded to the first decimal number.

Number of cases	Challenges							
	Legal	*Technical*	*Appeal*	*Crime mainly outside US*	*Extradition*	*Trial abroad*	*FLA involved*	*FLA initiated*
Offense type: Drug vendor								
63	14.3	0	12.7	0	0	3.2	7.9	1.6
Offense type: Onion Services								
16	37.5	25	12.5	68.8	12.5	37.5	75	18.8
Offense type: CSAM (Playpen)								
15	86.7	26.7	66.7	0	0	0	100	0
Offense type: CSAM								
13	23.1	15.4	15.4	7.7	0	0	7.7	23.1
Offense type: Other vendors								
8	12.5	0	0	0	0	12.5	37.5	0
Offense type: Employees								
7	57.1	42.9	42.9	28.6	0	14.3	14.3	57.1
Offense type: Onion Service customers								
5	0	0	80	0	0	0	0	0
Offense type: CSAM (Torpedo)								
3	100	66.7	66.7	0	0	0	0	100
Offense type: Hacking								
3	0	0	0	0	33.3	0	66.7	0
Offense type: CSAM (Welcome to Video)								
2	50	50	50	0	0	0	100	0
Offense type: Espionage								
1	0	0	100	0	0	0	0	100
All cases								
136	29.4	11.8	24.3	10.3	2.2	7.4	30.1	11

7.4 Trial Outcome and Challenges

Tables 5 and 6 present the outcomes of our legal analysis. Plea agreements emerge as the predominant outcome, offering defendants a sentence reduction in exchange for saving prosecutorial resources and ensuring a conviction. The frequency of plea agreements varies across offenses, with Onion Services notably diverging from the trend. This difference suggests that defendants facing charges for more common offenses, such as drug vending or CSAM, are more

inclined towards plea agreements, likely due to the prosecution's extensive experience and the precedent of convictions in similar cases. Additionally, the prospect of lengthy sentences may influence defendants' decisions, prompting some to pursue acquittals through substantial legal defense or being afraid of too lengthy sentences. Conversely, in Onion Service cases, characterized by their complexity and the voluminous evidence from lengthy investigations, defendants are more inclined to proceed to trial. Three of the Onion Service cases fall into the 'other' category due to defendants either committing suicide or becoming fugitives. Remarkably, our analysis revealed no instances of not guilty verdicts, which may reflect a selection bias in our sample towards selecting cases with a high likelihood of public interest and conviction.

Legal challenges were more frequently encountered than technical challenges, often contesting the validity of search warrants due to insufficient probable cause or other procedural errors, such as jurisdictional issues or lack of specificity. A notable legal challenge involved a defendant in a CSAM case disputing the probable cause cited in the search warrant affidavit by questioning the association between two specific usernames. While some challenges resulted in the suppression of parts of the evidence, particularly defendants' oral statements made before being informed of their rights, none decisively altered the evidentiary status. An appellate court opinion [27] underscored the modest threshold for probable cause, emphasizing that it merely requires

"*only 'a fair probability,' that 'contraband or evidence of a crime will be found in a particular place.' [...] Probable cause is therefore 'not a high bar.'*"

This explains the predominance of unsuccessful legal challenges. The analysis indicates that legal challenges are less common in the relatively standardized cases of drug and other vendors, as well as CSAM, compared to Onion Services and Employees. The latter categories, due to their uniqueness or access to better legal defense, exhibit a higher frequency of challenges. Cases stemming from the Playpen operation notably featured a high volume of legal challenges, likely driven by the operation's high profile and the legal community's interest.

Technical challenges were raised in 11.8 % of all cases, aiming either to suppress evidence directly or to undermine its credibility during trial. None of these motions were granted by the courts, and no challenge presented in front of a jury resulted in a not guilty verdict. Technical challenges typically targeted the authenticity and chain of custody of evidence, questioned the reliability of investigative methodologies, or posited alternative controllers of the accused devices. Despite defendants' efforts, courts consistently ruled in favor of the prosecution, attributing sufficient credibility to the evidence to warrant a conviction. Appeals were relatively evenly distributed among cases involving drug vendors, Onion Services, and CSAM, rarely resulting in significant relief for defendants beyond minor adjustments to supervised release conditions. The Playpen cases, however, stood out with a notably high appeal rate, likely attributed to the abundance of legal challenges and the potential for appellate success. Plea agreements often include waivers of certain appeal rights, which may account for the overall lower incidence of appeals.

7.5 International Law Enforcement Collaboration

Table 6 illustrates the necessity of international cooperation in addressing crimes facilitated by Tor. It is evident that certain crimes, such as those committed by drug vendors and other vendors, often leave traces that domestic law enforcement can pursue. These cases typically serve a local market, diminishing the need for extensive international collaboration, as foreign agencies may prioritize their resources elsewhere. However, inside these offenses, the landscape changes with crimes that have a broader impact, such as international trafficking of weapons and drugs. In these instances, cross-border cooperation is more common to track shipments and identify suspects. A notable case [34] involved a U.S. resident selling poison internationally. After apprehension, data about customers was shared with FLAs leading to additional arrests, underscoring the international collaboration in high-impact cases. The infiltration of the Playpen and Torpedo cases exemplifies the successful outcomes of international efforts, which were crucial for the identification and infiltration of the associated Onion Services. Interestingly, cases involving CSAM and employees of Onion Services often see FLAs taking the initiative in investigations, rather than joining after U.S. agencies have started the investigation. This contrasts with technical attacks during large operations, where suspects are identified by international efforts. Individual users like CSAM users do not require international searches or comprehensive data sharing as it is likely that one law enforcement agency conducts the identification individually and then notifies another one if the suspects reside in a different country. Also, law enforcement agencies might allocate their resources to other crimes like employees who facilitate a range of offenses. This is reflected in the higher incidence of extraditions and the fact that these crimes are frequently committed outside U.S. jurisdiction. For Onion Service cases, 68.8 % were primarily conducted outside the U.S., with 37.5 % involving extradition processes and 12.5 % resulting in trials abroad. These numbers highlight the significant resources U.S. law enforcement dedicates to investigating international defendants. The location of suspects is often initially unknown, requiring at least one agency to identify suspects facilitating crimes internationally. Although local convictions may not always be achieved, the substantial harm caused by Onion Services as facilitators justifies the concerted effort to mitigate their impact. Consequently, 93.8 % of Onion Service cases and 71.4 % of employee cases result from international law enforcement collaboration. This demonstrates that the investigative approaches to these global offenses are collective efforts, with agencies likely exchanging expertise and best practices.

7.6 Notable Legal Issues

Defendants occasionally raise technical challenges, but many such challenges are not fully addressed, either due to plea agreements or specific legal requirements. For instance, in the Silk Road case, United States v. Ulbricht [39], the defense argued that log files provided by the government contained implausible information and that recorded packet streams were not preserved. However, this challenge was dismissed on the grounds that "*Ulbricht has not conceded that he created Silk Road, or that he administered or oversaw its operations, [..] attesting to any personal privacy interest*

that he may have in any of the items searched and/or seized". Among all technical challenges presented, only one remains unresolved, questioning the reliability of crypto tracing services, specifically Reactor, in the case United States v. Sterlingov [29] involving a Bitcoin mixing service. The court allowed the evidence, stating:

> *The defense contends that Reactor is "junk science," [...] as a result, any testimony based on Reactor is not "the product of reliable principles and methods," [...] substantial evidence supports the government's submission that the software is highly reliable [...] The defense, of course, remains free to challenge the accuracy and reliability of Reactor before the jury.*

This illustrates the difficulty defendants face in dismissing technical evidence, compounded by the vast amounts of data law enforcement can accumulate during investigations. The cost of expert assessments for legal strategy further skews the advantage towards the prosecution, which tends to have significant resources at its disposal. In a CSAM case linked to the Torpedo operation, a technical challenge from the defendant was dismissed, noting that only the compiled version of the malware's source code was preserved by law enforcement [32]. The Playpen cases, in particular, underscored significant legal issues, revealing varying legal interpretations across courts. Some courts initially suppressed malware-derived evidence, while others justified its use. Two primary issues emerged: jurisdictional concerns regarding the scope of search warrants across districts and debates over the disclosure of malware code, balancing the defense's need for scrutiny against the prosecution's desire to protect its investigative tools. During our analysis, we found in a referenced case United States v. Michaud [42] that the court suppressed the evidence resulting from the Playpen malware because the government was unwilling to provide the defendant confidential access to the source code. During appeals, jurisdictional disputes were often settled by circuit courts invoking the good faith exception, which allows evidence obtained with an invalid warrant to be used if the warrant was issued in good faith. The case of United States v. Falte [38] highlighted potential legal complications arising from international law enforcement collaboration. Media coverage [8] suggested that the operation was strategically moved to a jurisdiction in Australia with fewer legal constraints. This approach enables the sharing of information with agencies that might otherwise be restricted from using certain investigative methods, potentially encouraging a shift in operations abroad to circumvent local legal limitations. The analyzed court cases demonstrate the challenges of succeeding with technical and legal challenges in court, suggesting a possible incentive for law enforcement to pursue operations in jurisdictions with more favorable legal frameworks.

7.7 General Remarks

The dataset began with an initial 717 results, which yielded 184 associated court cases after following related links and resources. This indicates that multiple press releases and documents exist for some cases. Most of these provided sufficient information to infer investigative methods, but 48 were discarded, suggesting a desire from law enforcement to keep some methods undisclosed. Large operations, which often involve comprehensive criminal enterprises and sophisticated attacks affecting many users, tend to attract more public interest. In three out of four large operations within the dataset, documents were initially sealed but later unsealed due to pressure from defendants and the public. One operation in the dataset could not be evaluated, but media coverage provided detailed insights. The keywords used showed a difference in found offenses, especially in drug distribution cases, indicating varying terminology in press releases and documents. Drug vendors, with 63 cases, make up the majority of cases, followed by 33 CSAM cases. This aligns with content studies showing that these categories are the most popular ones on Onion Services [2]. The 16 cases for Onion Services demonstrate that investigators can take down these platforms despite the protection offered by Tor. With this high number, it is likely that they are oversampled in the dataset because they enable cybercrime and require more resources to take down, as shown by the high rate of identifying leads from technical misconfigurations and metadata.

During the search for associated documents, we queried search engines and found various online sources, such as newspaper reports or press releases from Europol. We confirmed our assumption in the methodology that these sources generally do not provide enough background information for a systematic study. Large operations like Playpen or the Tor Protocol attack received significant attention, likely contributing to the unsealing of case files. Only in two cases did we find articles that contained information we could not find in available documents. These include one CSAM case where face recognition software was used and one CSAM Onion Service that we described in the notable technical attacks.

8 DISCUSSION

In this section, we discuss ethical considerations, main findings from our analysis, derived practical recommendations, limitation and potential future work.

8.1 Ethical Considerations

In the course of our research, we examined a significant number of court cases that involved personal data such as names, addresses, and even mentions of medical conditions in sentencing memorandums to influence the sentencing outcome. Our focus was solely on evaluating the investigative methods that linked the defendants to the crimes, and we noted their occurrences for the cases. All the documents we processed were available via the PACER system or published in media outlets, allowing unrestricted access. For media documents, we excluded sentencing memorandums and did not reference URLs. Our results only contribute to the count of the investigative methods that appeared. While it is possible that criminals could utilize our findings to adapt their behavior and evade law enforcement action, our research does not provide guidelines for avoiding prosecution. Instead, we merely evaluate public documents. Furthermore, during our analysis, we found several documents indicating that criminals already search through PACER to find cases that affect them or their modus operandi. A few court documents state that on Onion Services related to illegal goods and CSAM, some operational security guidelines were shared by operators, and users could discuss further precautions. Meanwhile, ethical Tor users with restricted internet access may lack a technical

background and are unlikely to first access Onion Services related to criminal content to improve their security. Tailored guidelines can help protect ethical users while not entirely preventing law enforcement actions.

8.2 Main Findings

Based on our analysis, we distilled six main findings that answer our initial research questions.

Investigative methods vary by offense The analysis, categorized by offense type, reveals that investigators employ diverse methods depending on the offense. Factors such as the nature of the offense and the traces it leaves behind influence this. For instance, drug vendors often leave physical clues that investigators can exploit. Cryptocurrency flows, often obfuscated by platforms, hinder law enforcement from pursuing this angle. Despite drug vendors and other vendors constituting the majority of cases, none were affected by malware or Tor protocol attacks, suggesting that investigators selectively target other offenses with these methods.

Users make mistakes The analysis indicates that in most instances, defendants could have evaded detection with modified behavior, barring rare cases where defendants were identified by coincidences or Tor protocol attacks. The prevalent use of linking information, physical searches, and crypto tracing suggests that users could enhance their security without alterations to the Tor protocol. The Onion Service cases demonstrate that even operators managing servers and large platforms make avoidable misconfiguration errors.

Technical attacks affect many users simultaneously The four operations included in the dataset illustrate law enforcement takeovers of platforms, leading to malware distribution to users. Unlike other methods requiring labor-intensive investigations on individual users, these attacks generate a multitude of identifying leads that can be pursued with fewer investigative resources. The Tor protocol attack exemplifies this, with the takedown of over 400 Onion Services. However, these attacks attract significant attention, rendering them ineffective after a short duration. Attackers can only utilize this method under limited circumstances.

Tor Protocol attacks are exceptional We found only one Tor protocol attack with devastating impact. Public interest and media coverage would quickly escalate if defendants in court cases were affected by this method. The FBI did not execute this attack, but seized records from a research institute, enabling them to locate the defendants. It is likely that only well-funded attackers with access to research resources can conduct similar attacks, especially since academic research has significantly improved Tor's security since 2014.

International collaboration is essential for high-impact cases The presence of international law enforcement collaboration is particularly evident in cases with broader implications, such as Onion Services facilitating crimes. Such collaboration has led to apprehension of defendants, including the identification and infiltration of Onion Services. For other crimes, international collaboration during the investigation is more rare, but hints are shared among agencies. This underscores the applicability of U.S. law enforcement investigative methods on a global scale, despite legal constraints potentially limiting or extending specific employed techniques. It confirms that they serve as a strong attack model as private hacking groups or isolated oppressive regimes typically lack international collaborations.

Legal defense for Tor users is challenging For individuals utilizing Tor, mounting a legal defense, at least in U.S. courts, proves to be a formidable challenge, as the likelihood of successfully contesting charges is notably low. Especially technical evidence is hard to dispute with the vast amounts of data collected by law enforcement during investigations, various legal interpretations that can differ between courts and international collaboration introducing additional legal complexities. For instance, the use of malware by foreign law enforcement agencies and strategic jurisdictional moves can complicate the defense's ability to challenge the reliability of investigative methods or their legality. These unresolved issues cast a shadow of uncertainty over Tor users. Moreover, even users residing in jurisdictions with different evidentiary rules might find themselves affected, as some defendants—mainly those involved with Onion Services—have been extradited to the U.S.

8.3 Practical Recommendations

As briefly mentioned in the ethical considerations, our systematic study can assist in creating tailored guidelines for ethical Tor users seeking to avoid prosecution in authoritarian regimes. Additionally, our study can provide law enforcement with potential strategies to structure investigations and utilize additional angles.

Ethical Tor users The need for criminal prosecution and support for ethical users should be balanced with tailored guidelines that do not entirely impede law enforcement. We believe these guidelines are necessary for ethical users and should be more prominently displayed, as many of these users likely lack a technical background and are prone to human errors that could endanger their lives. In our discussions, we generated numerous ideas to potentially enhance the security of Tor users and Onion Services. However, we consistently encountered the challenge that additional protective measures often introduce complexity, which can increase risks, given the difficulty of securing even a single server. We opted for generating basic recommendations that are easy to understand for different target groups and specific enough for users to potentially adapt their behavior. We offer some suggestions for different Tor users, which are not exhaustive but provide a starting point. The detailed recommendations are given in Appendix C. For Tor beginners, we give mainly behavioural advice that should be easy to implement even without a technical background like choosing privacy-focused providers in favorable jurisdictions. Meanwhile, advanced Tor users should configure technical things, maintain a small online footprint and are advised to use privacy-preserving cryptocurrencies. Onion Service operators received separate advice as it is a specific scenario. In our analysis, law enforcement agencies used different investigative methods depending on the offense. Similarly, ethical Tor users should consider their specific scenarios and select suitable measures individually.

The devastating impact of technical attacks underscores the need to protect all Tor users. While Tor protocol attacks are not preventable by design, further research can reduce their likelihood. More importantly, malware is more prevalent, and hardening the Tor browser by default could help prevent user infections. One

possibility could be to disable scripts in the Tor browser for Onion Services by default, while enabling them on regular websites to minimize the impact on usability. This makes targeted attacks on Onion Service users more difficult.

Law enforcement The investigative methods analyzed provide a range of potential approaches. Additionally, the distinction between case types can indicate which methods might be more effective. Starting with less resource-intensive methods like linking pseudonyms, and progressing to more costly ones like malware, can help conserve valuable resources and address low-hanging fruits. In the analysis, undercover infiltration was surprisingly often used, but provided the identifying lead in only 4.4 % of all cases. Social engineering is a prevalent threat on the internet, and criminals are likely susceptible to it as well, therefore developing this method might generate more identifying leads. This method allows investigators to be proactive, rather than passively following leads, without requiring sophisticated technical techniques. It can be used to gain entry into criminal networks. Focusing resources on large platforms can also prove efficient, as these platforms enable crime and potentially hoard enormous amounts of data. A speculative angle might be to take down or impersonate mixing services in combination with cryptocurrency analysis. Standardizing international collaboration is necessary to tackle global crime facilitators and creating comparable investigative framework can help to authenticate technical evidence and ensure its admissibility in court.

8.4 Limitations and Future Work

Our study's methodology, which relies on press releases issued by the U.S. Department of Justice, may introduce bias. These releases tend to emphasize cases of greater public interest or importance, potentially omitting cases where a dismissal or not guilty verdict is anticipated by the government. Additionally, the dynamic nature of legal language and investigative methods requires periodic updates to our codebook. While we believe that reviewers with a basic cybersecurity background can effectively evaluate documents, the involvement of experts is crucial for these updates. Our analysis did not include a legal expert, which means that our legal interpretation may not encompass all nuances and exceptions, remaining potentially superficial. Nevertheless, we maintain that our study's technical focus justifies a less detailed legal examination.

The reliance on U.S. court documents also limits the generalizability of our findings. Although international law enforcement cooperation may standardize investigative methods to some extent, legal constraints and available resources vary by country. The U.S. is likely to have significant resources, as evidenced by extradition processes and investigations into crimes such as CSAM or Onion Service offenses, where the location of suspects is not immediately apparent. However, the legal challenges arising from investigative methods and the evaluation of technical evidence are expected to differ considerably internationally, given the unique characteristics of jury trials and the variability of criminal law. Moreover, while the analyzed court documents may not disclose all investigative methods, the number of included cases helps mitigate this concern. Our methodology assumes the integrity of the information in these documents, but there is a possibility that law enforcement officials may present fictional evidence or engage in parallel construction. For instance, in the Silk Road case [39], allegations of parallel construction were not entirely resolved due to legal procedures. The exclusion of improperly obtained evidence and the potential for sanctions are intended to deter such practices from law enforcement officials. In our document analysis, we did not encounter significant concerns regarding the authenticity of the technical evidence presented.

Future research could take several directions. One approach is to examine court documents from other countries to determine whether law enforcement strategies are consistent. Additional data sources, such as online posts from targeted Tor users or interviews with threat actors, could refine our attacker model, though the reliability of such information poses a challenge. Recommendations for users could be enhanced through in-depth interviews with practitioners and user studies. Software redesigns, such as modifications to the Tor browser, could increase user awareness of potential risks and encourage more secure behavior. One possible step could be to disable scripts by default for Onion Services in the Tor browser. A significant area for future inquiry is the legal acceptability of information obtained through international collaboration, the verification of such information according to local evidence admission rules, and the permissibility of investigative methods, particularly those involving controversial technical attacks.

9 CONCLUSION

Our analysis reveals that despite the academic focus on them, Tor protocol attacks are exceptionally rare. Even criminals, who have a vested interest in maintaining their anonymity, often make simple mistakes such as reusing pseudonyms. Similarly, operators administering large Onion Services, despite their technical knowledge, make avoidable configuration mistakes, such as making their services directly available over the IP address or leaking the IP through the Onion Service. Currently, the advice from the Tor project is insufficient, and valuable guidance is hard to find amidst the fragmented, sometimes counterproductive or outdated advice available. While criminals share guidelines in forums, ethical users, especially in censored regions, are effectively cut off from suitable advice. Guidelines tailored to ethical use cases will vary, as the analysis by offense type shows. We argue that it is possible to design guidelines that take law enforcement interests into account, and we provide some examples. Newspapers or similar organizations could distribute these to potential sources. Furthermore, some court cases demonstrated legal issues with investigative methods and how technical evidence can be authenticated. Lastly, the significant impact of technical attacks underscores the need to protect users from malware and to continue academic research to prevent attacks on the Tor protocol. While the results may not yield visible results, they are nonetheless important. Proper handling of Tor research data is crucial, as a single mistake can put many lives in danger, as shown with the simultaneous take down of over 400 Onion Services.

ACKNOWLEDGMENTS

We express our sincere gratitude to Maria Tarczewska for her contribution as a third reviewer, meticulously assessing the court documents and providing insightful perspectives. We are grateful to

the anonymous reviewers for their thoughtful and constructive feedback, which led to significant improvements in our work. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

[1] Husam Al Jawaheri, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. 2020. Deanonymizing Tor hidden service users through Bitcoin transactions analysis. *Computers & Security* 89 (Feb. 2020), 101684. https://doi.org/10.1016/j.cose.2019.101684

[2] Alex Biryukov, Ivan Pustogarov, Fabrice Thill, and Ralf-Philipp Weinmann. 2014. Content and Popularity Analysis of Tor Hidden Services. In *Proceedings of the 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW '14)*. IEEE Computer Society, USA, 188–193. https://doi.org/10.1109/ICDCSW.2014.20

[3] Muqian Chen, Xuebin Wang, Jinqiao Shi, Yue Gao, Can Zhao, and Wei Sun. 2019. Towards Comprehensive Security Analysis of Hidden Services Using Binding Guard Relays. In *Information and Communications Security: 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers*. Springer-Verlag, Berlin, Heidelberg, 521–538. https://doi.org/10.1007/978-3-030-41579-2_30

[4] Joseph Cox and Lorenzo Franceschi-Bicchierai. 2016. Newly Uncovered Tor Browser Exploit Targeted Dark Web Child Porn Site. https://www.vice.com/en/article/9a3mq7/tor-browser-zero-day-exploit-targeted-dark-web-child-porn-site-giftbox

[5] Roger Dingledine and Nick Mathewson. 2023. Tor Protocol Specification. https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt

[6] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The Second-Generation Onion Router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13 (SSYM'04)*. USENIX Association, San Diego, USA, 21 pages. https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router

[7] Alexander Færøy. 2020. TorPlusVPN. https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN

[8] Håkon F. Høydal, Einar Otto Stangvik, and Natalie Remøe Hansen. 2017. BREAKING THE DARK NET: WHY THE POLICE SHARE ABUSE PICS TO SAVE CHILDREN. https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en

[9] Alfonso Iacovazzi, Daniel Frassinelli, and Yuval Elovici. 2019. The DUSTER Attack: Tor Onion Service Attribution Based on Flow Watermarking with Track Hiding. In *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*. USENIX Association, Chaoyang District, Beijing, 213–225. https://www.usenix.org/conference/raid2019/presentation/iacovazzi

[10] Alfonso Iacovazzi, Sanat Sarda, and Yuval Elovici. 2018. Inflow: Inverse Network Flow Watermarking for Detecting Hidden Servers. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. IEEE Press, Honolulu, HI, USA, 747–755. https://doi.org/10.1109/INFOCOM.2018.8486375

[11] Klaus Krippendorff. 2019. *Content Analysis: An Introduction to Its Methodology*. SAGE Publications, Inc., Thousand Oaks, CA. https://doi.org/10.4135/9781071878781

[12] Albert Kwon, Mashael AlSabah, David Lazar, Marc Dacier, and Srinivas Devadas. 2015. Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, D.C., 287–302. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/kwon

[13] Zhen Ling, Junzhou Luo, Kui Wu, and Xinwen Fu. 2013. Protocol-level Hidden Server Discovery. In *2013 Proceedings IEEE INFOCOM*. IEEE, Turin, Italy, 1043–1051. https://doi.org/10.1109/INFCOM.2013.6566894

[14] Srdjan Matic, Platon Kotzias, and Juan Caballero. 2015. CARONTE: Detecting Location Leaks for Deanonymizing Tor Hidden Services. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (Denver, Colorado, USA) *(CCS '15)*. Association for Computing Machinery, New York, NY, USA, 1455–1466. https://doi.org/10.1145/2810103.2813667

[15] Gianluigi Me, Liberato Pesticcio, and Paolo Spagnoletti. 2017. Discovering Hidden Relations Between Tor Marketplaces Users. In *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*. IEEE, Orlando, FL, USA, 494–501. https://doi.org/10.1109/dasc-picom-datacom-cyberscitec.2017.93

[16] mikeperry-tor. 2023. The Vanguards Onion Service Addon. https://github.com/mikeperry-tor/vanguards

[17] Steven J. Murdoch. 2006. Hot or not: Revealing hidden services by their clock skew. In *Proceedings of the 13th ACM Conference on Computer and Communications Security* (Alexandria, Virginia, USA) *(CCS '06)*. Association for Computing Machinery, New York, NY, USA, 27–36. https://doi.org/10.1145/1180405.1180410

[18] Administrative Office of the U.S. Courts. 2024. Criminal Cases. https://www.uscourts.gov/about-federal-courts/types-cases/criminal-cases

[19] Andriy Panchenko, Asya Mitseva, Martin Henze, Fabian Lanze, Klaus Wehrle, and Thomas Engel. 2017. Analysis of Fingerprinting Techniques for Tor Hidden Services. In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society* (Dallas, Texas, USA) *(WPES '17)*. Association for Computing Machinery, New York, NY, USA, 165–175. https://doi.org/10.1145/3139550.3139564

[20] Riseup. 2023. Best Practices for Hosting Onion Services. https://riseup.net/en/security/network-security/tor/onionservices-best-practices

[21] Marco Simioni, Pavel Gladyshev, Babak Habibnia, and Paulo Roberto Nunes de Souza. 2021. Monitoring an anonymity network: Toward the deanonymization of hidden services. *Forensic Science International: Digital Investigation* 38 (Oct. 2021), 301135. https://doi.org/10.1016/j.fsidi.2021.301135

[22] Pascal Tippe. 2024. A Study of Deanonymization Attacks of Onion Services. In *Sicherheit 2024*. Gesellschaft für Informatik e.V., Bonn, 281–287. https://doi.org/10.18420/sicherheit2024_021

[23] Tor Project. 2014. Tor security advisory: "relay early" traffic confirmation attack. https://blog.torproject.org/tor-security-advisory-relay-early-traffic-confirmation-attack/

[24] Tor Project. 2023. Operational Security. https://community.torproject.org/onion-services/advanced/opsec/

[25] Tor Project. 2023. Tor Metrics. https://metrics.torproject.org/

[26] Tor Project. 2023. Tor Rendezvous Specification - Version 3. https://gitweb.torproject.org/torspec.git/tree/rend-spec-v3.txt

[27] U.S. Court of Appeals for the Fourth Circuit. 2019. United States v. Bosyk. No. 18-4302 (4th Cir. 2019).

[28] U.S. Department of Justice Office of Public Affairs. 2014. More than 400 .Onion Addresses, Including Dozens of 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on Tor Network. https://www.justice.gov/opa/pr/more-400-onion-addresses-including-dozens-dark-market-sites-targeted-part-global-enforcement

[29] U.S. District Court for the District of Columbia. 2021. United States v. Sterlingov. 1:21-cr-00399.

[30] U.S. District Court for the District of Maryland. 2013. United States v. The computers that access the e-mail accounts described in Attachment A, incorporated herein. 8:13-mj-01746.

[31] U.S. District Court for the District of Maryland. 2019. United States v. Marques. 8:19-cr-00200.

[32] U.S. District Court for the District of Nebraska. 2013. United States v. Cottom. 8:13-cr-00108.

[33] U.S. District Court for the District of Nebraska. 2013. United States v. DeFoggi. 8:13-cr-00105.

[34] U.S. District Court for the District of New Jersey. 2014. United States v. Korff. 3:14-cr-00471.

[35] U.S. District Court for the Eastern District of California. 2016. United States v. Babadjov. 1:16-cr-00204.

[36] U.S. District Court for the Eastern District of California. 2016. United States v. Sparks. 2:16-cr-00095.

[37] U.S. District Court for the Middle District of Florida. 2017. United States v. Lueck. 6:17-cr-00008.

[38] U.S. District Court for the Middle District of Tennessee. 2017. United States v. Falte. 3:17-cr-00044.

[39] U.S. District Court for the Southern District of New York. 2013. United States v. Ulbricht. 1:14-cr-00068.

[40] U.S. District Court for the Western District of North Carolina. 2015. United States v. Chase. 5:15-cr-00015.

[41] U.S. District Court for the Western District of Washington. 2015. United States v. Farrell. 2:15-cr-00029.

[42] U.S. District Court for the Western District of Washington. 2015. United States v. Michaud. 3:15-cr-05351.

[43] Ming Yang, Xiaodan Gu, Zhen Ling, Changxin Yin, and Junzhou Luo. 2017. An active de-anonymizing attack against tor web traffic. *Tsinghua Science and Technology* 22, 6 (Dec. 2017), 702–713. https://doi.org/10.23919/tst.2017.8195352

[44] Lasse Øverlier and Paul Syverson. 2006. Locating Hidden Servers. In *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, Berkeley/Oakland, CA, USA, 114–129. https://doi.org/10.1109/SP.2006.24

A INITIAL CODEBOOK

The initial codebook comprised two distinct sections. Table 7 defined the various investigative techniques employed by law enforcement agencies. Table 8 provided a systematic framework for determining the classification of offenses in court cases. To mark the identifying lead, we formatted the investigative method separately. To calculate the Krippendorff's alpha coefficient, we treated

the identifying lead as an additional column with nominal values representing the investigative methods.

B EXTENDED CODEBOOK

As detailed in Section 5.3, we developed further research questions concerning the legal dimensions of court cases. Consequently, we expanded the original codebook to include Table 9. In our analysis, we categorize challenges to evidence into two types: legal and technical. Below, we illustrate each category with a quote from court documents.

Legal Challenges to Evidence: An exemplary instance of a legal challenge is presented in the case United States v. Lueck [37] where the defendant intended to have the charges dismissed on the grounds of the government's conduct, which he argued was a violation of his due process rights. The motion filed by the defendant is summarized by the court as follows:

> *Defendant seeks dismissal based on the United States' allegedly outrageous conduct, arguing that the Government's conduct violated his due process rights under the Fourth and Fifth Amendments to the United States Constitution as well as Federal Rule of Criminal Procedure 12(a)(3). Defendant argues that the Government acted outrageously when it maintained control over Playpen for a twelve-day period. Defendant contends this conduct was outrageous because by assuming administrative control over Playpen, the Government allowed vast amounts of child pornography to be disseminated without any restrictions or limitations, despite the Government's ability to place controls on the website. Defendant also argues that allowing such widespread distribution of child pornography caused the victims to be repeatedly harmed and also asserts that the Government failed to take any steps to reduce the resulting harm to the victims*

Technical Challenges to Evidence: An example of a technical challenge is highlighted in the case United States v. Chase [40] during a trial where the defense argued in front of the jury that the defendant could not be held responsible for actions taken using his device or account, suggesting that an external party had control. This argument is in the following excerpt from the trial transcript:

> *We know that he was either hacked, somebody was using his information. There's no indication that he knew that was happening. There be no reason for him to go back and look. But for some of that information it's really not going to be clear who did it; for some of it, it will be absolutely clear that he did not and it was other people*

C RECOMMENDATIONS

Our dataset is populated by criminal cases from the U.S., so it's possible that ethical Tor users are endangered by other investigative methods. We believe that powerful attackers would at least try to reuse methods that are established in criminal investigations. Also, in the attached paper, we found that the offense determines investigative methods. While drug dealers are not ethical Tor users, activists who ship printed materials might be. CSAM offenders have in common with journalists/activists that they share pictures, albeit with vastly different content and intent. The espionage case has parallels for potential whistleblowers. Failures from Onion Service operators and their employees should be directly transferable as they offer platforms where the concrete theme/offense does not largely impact their attack surface. This is shown by the high values for identifying leads from misconfigurations (37.5 %), metadata (18.8 %) and other independent attack vectors in Table 4.

In our discussions, we generated numerous ideas to potentially enhance the security of Tor users and Onion Services. However, we consistently encountered the challenge that additional protective measures often introduce complexity, which can increase risk, given the difficulty of securing even a single server. Conducting user studies to test potential guidelines is challenging in an environment where users highly value privacy. Therefore, we aim to provide recommendations that are directly linked to the investigative methods we analyzed, striking a balance between offering valuable advice that is neither too specific nor too general.

To serve to the diverse needs of Tor users, we drafted three separate sets of guidelines that can be seen in the following tables. Table 10 offers basic advice for all Tor users. Table 11 provides advanced advice for more experienced users who may require enhanced security, and Table 12 is specifically tailored to Onion Service operators, who face many technical challenges that do not affect regular users. These guidelines are grounded in our findings from the court cases, focusing on practical advice rather than potential technical attacks. Therefore, the column *Investigative method* maps the advice to the investigative methods used in our paper.

Table 7: Part of the codebook categorizing investigative methods with binary coding.

Code	Description and examples*	Example quotes
Physical	Surveillance of physical activities * Package interception * Camera recordings * Surveillance by agents * Surveillance by confidential informants * Audiorecordings from hidden devices * Community supervision (parole, supervised release, probation) * Meetup with disguised agents * Suspicious package	*A selection of photographs taken during the surveillance are included below:* *Law enforcement subsequently observed BURGAMY walking with what appeared to be multiple United States Postal Service mailing envelopes* *The Postal Inspector then conducted physical surveillance of the Post Office in Cumming, Georgia, on or about August 6, 2020.*
Online	Surveillance of online activities * Live monitoring of accounts * Wiretapping calls * Identifying BitTorrent clients * Pen trap * Network monitoring * GPS tracking * Phone ping	*a court in the Netherlands authorized a wiretap of the computer assigned to the IP address ending in 247, which began on or about May 24, 2016. United States authorities received a copy of the wiretap data…* *a pen register order for the Buchta Comcast Account was issued in the Northern District of Illinois, and thereafter renewed three times. The pen register collection reflected extensive communication between the Buchta Comcast Account and IP addresses ending in …* *Pursuant to a Pen Register/Trap and Trace authorized by the Honorable Judge John F. Anderson for PAGAN's home internet on December 18, 2020, records show network connections from PAGAN's home internet to TOR nodes on multiple days which indicates the use of TOR which is needed to connect to the darkweb.*
Pseudonyms	Linking pseudonyms across platforms * Usernames, mail addresses and other identifiers	*During the course of this investigation, investigators reviewed darknet marketplaces and observed vendor accounts with the moniker addy4cheap offering drugs for sale on the Empire Market and Cryp0nia* *Addy4cheap offered Adderall for sale on the Empire Market and Cryp0nia for quantities ranging from one to over 1000*
Cryptographic keys	Linking cryptographic keys across platforms * DSA login keys * Crypto (hardware) wallets * GPG/PGP keys * Certificates * SSH keys	*The PGP public keys listed for H00k3d on all of the aforementioned sites were identical* *It was discovered that the "SafeServe" accounts on all of these markets used the same PGP key, indicating that the same individual or individuals operated each of the accounts.*
Private information	Information normal persons cannot access * Drivers license register * Jail records * Vehicle registration * Information from confidential informants * Information from other investigations (seized servers, seized devices) * Postal records * Tax databases * Biometric databases * Employment records * Law enforcement databases * Company records without account	*A search of the Colorado Department of Motor Vehicle revealed Gregory Lopez, DOB-XX-XX-1993 with a reported home address in Colorado Spring, Colorado.* *The photo of the male provided by HSI Newark appeared to be the same individual in the driver's license photo of the defendant.* *A review of U.S. Postal Service ("USPS") business records indicated that the aforementioned indivual had received three packages* *Based upon reviews of law enforcement databases*
Public information	Information normal persons can access * Online platforms accounts (i.e. StackOverflow, Instagram, Reddit) * Open source databases * Company registers (which companies exists, who owns them etc.) * Online platform posts and information * Key databases to link cryptographic keys * Public pictures or videos	*An open source review of the Facebook.com website for Gerren Johnson located a Facebook page for user "GREENJOHNSON88."* *Through additional social media research, pictures of PERSON were located on PERSON'S mother's Facebook page* *I was able to observe that it has been a vendor account since November 16, 2016 and has 531 confirmed sales of MDMA.*
Associated (non-government) accounts	Information from associated (non-government) accounts * Online platform accounts (i.e. cloud, email, social media) * Crypto exchange accounts * Prepaid cards * Physical accounts/registration (i.e. bank, post box, storage unit)	*The Twitter records also reflect the following different communications…* *According to subscriber information provided by Google* *Records obtained from Coinbase revealed that the account is subscribed in the name of*
Shared characteristics	Linking other information/ behavioral information * Fingerprint on letter * Linguistic expressions * Political views * Shared password across contexts * Similar package shipping style * Similar posting style * Timings fit to defendants schedule/ travel plans * Similar behavior	*I also reviewed the language in the terms and conditions and the refunds and dispute sections of the addy4cheap profile. The language was identical for addy4cheap's profile on both the Empire Market and Cryptonia* *H00k3d used the same avatar, a fish with a hook in it as depicted below, on at least the Dms Apollon, Avaris and Darkode*
Crypto tracing	Tracing cryptocurrency movements * Tracing crypto payments (i.e. Bitcoin)	*An analysis of Bitcoin transactions available via the public Blockchain reflects that the user of the MIMM Silk Road Account withdrew Bitcoins credited to the MIMM Silk Road Account to certain Bitcoin addresses (the "Ellingson Intermediary Bitstamp Bitcoin Addresses"). On several occasions in or about October 2013 and February 2014, Bitcoins were then transferred from the Ellingson Intermediary Bitstamp Bitcoin Addresses to the Ellingson Bitstamp Account.* *Based on a review of records available on the public blockchain, as well as a review of the Coinbase records, on January 6, 2020, approximately 16 minutes after receiving the deposit from the FBI undercover employee*
Undercover infiltration	Infiltrating with undercover agents or confidential informants * Agents crawling Onion Services * Agents buying products * Agents impersonating other entities (i.e. customers, money launderer) * Phishing and social engineering * Taking over accounts from criminals	*In or about mid-2014, an FBI online covert employee (the "OCE") assumed an online Dark-Web identity, which had previously been used by a trafficker in illicit materials, including, among other things, biological toxins* *Throughout the investigation, I, and other law enforcement agents, including the HSI-UC, have visited Silk Road 2.0 using undercover user accounts* *I have been involved in undercover purchases of narcotics from the website through an undercover account, which were ordered to and received in the Southern District of New York*

Code	Description and examples*	Example quotes
Malware	Unmask Tor users with malware * Network investigative techniques * Video files pinging home * JavaScript exfiltrating information	*accessed a post containing child pornography from Playpen, at which point the NIT was deployed to the activating computer.*
Third party	Information from a third party * Post office employees * Landlord * Victim * Users	*FBI agents interviewed an individual residing in Fairfax County, Virginia within the Eastern District of Virginia who was suspected of being a darknet drug recipient. [...] The individual stated that he had on multiple occasions purchased Adderall through a DM known as the Empire Market from a vendor using the moniker addy4cheap. [...] The inidividual provided agents with the tracking number from his most recent purchase from addy4cheap on the Empire market*
Co-conspiritor	Information from co-conspirators * Employees * Money launderer * Vendor	*CW-1 has been charged with federal crimes for his participation and involvement with Silk Road, and is cooperating with law enforcement in the hopes of obtaining a cooperation agreement with the Government, and ultimately leniency at the time that CW-1 is sentenced.*
Misconfigurations	Misconfigurations that bypass Tor * IP address leaked * Onion Service directly reachable by IP address * Link opened in normal browser * Revealing mail header * Insufficiently protected accounts on Onion Service infrastructure	*In December 2014, Playpen's administrator misconfigured the website. As a result, when the user entered a valid e-mail address, the user received a confirmation e-mail sent over the regular Internet, not the Tor network*
Tor protocol attacks	Protocol attacks that break the Tor anonymity * Traffic confirmation attacks	*The record demonstrates that the defendant's IP address was identified by the Software Engineering Institute ("SEI") of Carnegie Mellon University (CMU") when SEI was conducting research on the Tor network which was funded by the Department of Defense ("DOD"). The government previously produced information to the defense that Farrell's IP address was observed when SEI was operating its computers on the Tor network. This information was obtained by law enforcement pursuant to a subpoena served on SEI-CMU.*
Physical search	Investigating physical items from the defendant * Searching through defendants home/car/ trash in the garden * Search warrant for sent packages	*A search warrant was subsequently executed on the Defendant's home, resulting in the seizure of electronic devices.*

Table 8: Offense classification schema from the codebook with mandatory single-category assignment for each case.

Category	Description and examples*	Example quotes
CSAM	Crimes related to CSAM (Child Sexual Abuse Material) * CSAM users * CSAM distributors * CSAM producers	*Access or Attempt to Access Child Pornography* *Distribution of Child Pornography*
CSAM (Playpen)	CSAM cases related to Playpen/Operation Pacifier	*Defendant was first identified through an FBI investigation into a child pornography website known as "Playpen."*
CSAM (Torpedo)	CSAM cases related to Operation Torpedo	*The United States [...] alleges that a website, known as an image board, that allowed its users to view and upload images of children being sexually exploited ("Website A") was operated from August to December of 2012 in Bellevue, Nebraska. [...] The computer server that hosted the website was seized by law enforcement officers on November 15, 2012, and they monitored activity on the site from November 19, 2012, to December 9, 2012. Each of the defendants is alleged to have viewed child pornography during that time period*
Drug vendor	Crimes related to distributing drugs online * Users selling fentanyl on Onion Services * Users selling illegal drug derivatives on Onion Services	*Conspiracy to Distribute Controlled Substances*
Other vendor	Crimes related to distributing illegal items/services online * Poison vendor * Gun vendor * Money laundering * Hitman services	*aided and abetted by each other, knowingly Engage in Dealing in Firearms without a License, knowingly Smuggle Goods the United States and knowingly Failed to Declare Firearms to a Common Carrier* *Selling Firearms Without a License*
Onion Services	Operating an illegal Onion Service * CSAM forums * Darknet marketplace (DNM, DM) * Cryptocurrency tumbler	*Silk Road 2.0, a platform underground for drug dealers around the world to sell a wide variety of substances*
Employees	Assisting operators maintaining/creating Onion Services * Forum moderators * Technical programmers/admins	*the defendant, who served as a trusted advisor of Ulbricht* *including customer support staff representatives and several computer programmers*
Onion Service customers	Customers buying goods/services on Onion Services * Poison customers * Muder-for-hire customers	*which criminalizes the use of interstate commerce facilities in the commission of murder-for-hire,* *Attempted Acquisition of a Biological Toxin*
Hacking	Crimes related to hacking * Ransomware infrastructure * Hacking groups * DDoS groups	*the Hive administrators set up a network of servers to run their online criminal business. The public-facing side or "frontend" of the network consists of four Tor-accessible websites*
Espionage	Obtaining and selling classified documents	*a current employee of the United States Navy, has passed, and continues to attempt to pass, Restricted Data [...] to a foreign government,*

Table 9: Expanded codebook detailing legal aspects of court cases.

Code and values* (if not binary)	Description	Indicators
Legal challenges to evidence	Suppression of evidence based on legal grounds	- Motion for suppression in docket based on, for example, illegal searches - Attempting to suppress evidence during appeals
Technical challenges to evidence	Suppression of technical evidence due to unreliability or questioning its validity	- Motion for suppression in docket based on unreliable method - Questioning the reliability of technical evidence in front of the jury - Presenting alternative interpretations for technical evidence to the jury
Trial outcome * Plea * Verdict * Ongoing * Unknown * Trial abroad * Other	How the trial concluded - Plea, if at least one defendant entered a plea agreement and no other defendants received a verdict - Verdict, if at least one defendant was tried - Cases with at least one defendant sentenced in the U.S., with others pending extradition or tried abroad, were categorized based on the outcomes of the U.S. defendants - Ongoing describes cases without a judgement/sentence - Unknown refers to cases where the court docket lacks clear documentation or indication how the case concluded - Trial abroad, if no defendant has a trial in the US - Others includes cases where defendants became fugitives or preliminary deaths occurred before conclusion	- Visible as an entry in the docket - Judgement document can include this information - Entry "Change of Plea"/"Plea hearing" in docket contains information - Verdict requires trial transcripts and further preparation documents - If no activity, check for newspaper articles if defendants are living abroad or are fugitives
Appeal	If the defendant appealed a court decision	- Appeals can be visible in the docket - Query defendant and case number for appellate documents
Crime mainly committed outside the U.S.	Was the crime mainly committed outside the US?	- Two conditions should apply: 1. The defendants were mainly residing outside of the US 2. The crime was not targeted towards the US
Extradition process	At least one defendant arrested outside of the U.S. and an extradition process started	- Check if extradition is mentioned in the court documents - If defendants resided abroad, check for newspaper articles
Trial abroad	At least on defendant was tried or has an ongoing trial process outside the U.S.	Check if both of the following conditions apply and then check for newspaper articles: 1. No trial/judgement documents are visible in the docket after a prolonged time 2. Defendants were not U.S. citizens or residing outside of the U.S.
FLA involved	At least one FLA assisted during the investigation	- FLA provided information during the investigation - Often in the form of mutual legal assistance treaties (MLAT) - Typically providing server images, physical surveillance, or executing search warrants
FLA initiated	The investigation started from information provided by a FLA	- FLA provided crucial information that initiated the investigation - Typically identified IP addresses, servers or results from undercover infiltrations are shared

Table 10: Essential advice for Tor beginners.

Advice	Details	Investigative method
Create robust and unpredictable passphrases	- Passphrases should not be predictable and sufficiently long - Avoid using easily discoverable personal information or common phrases - Remember, writing down your passphrase can pose a risk if discovered by others	Misconfigurations, linking information
Stay vigilant about metadata in files	- Be mindful that files, including images and documents, can carry hidden data such as creation dates, locations, and device information - Cryptographic keys might contain sensitive information in comment fields or associated email addresses - Metadata can inadvertently reveal personal details - When sharing files, consider using tools or methods to strip or anonymize metadata to protect your privacy	Linking information
Use safe Tor browser settings	- Refrain from installing additional plugins in the Tor browser - Opt for the safest settings that deactivate JavaScript - While this may alter the appearance of websites, enabling JavaScript can introduce vulnerabilities that might compromise your anonymity	Malware, misconfigurations
Choose privacy-focused providers in favorable jurisdictions	- Opt for service providers known for their commitment to privacy - Ensure they operate within jurisdictions with transparent privacy laws and a strong stance on free speech - This approach can help reduce stored personal data - It also limits the likelihood and impact of data requests by authorities and breaches	Linking information, surveillance
Exercise caution with third-party interactions	- Be aware that third parties may attempt to collect information or deceive you into revealing your real identity - Approach interactions with skepticism to safeguard your anonymity	Linking information, undercover infiltration
Implement end-to-end encryption	- Be aware of the fact that platforms, such as email services or forums, could be compromised, allowing unauthorized access to your messages - End-to-end encryption is crucial for protecting the content of your communications - End-to-end encryption does not conceal sender-receiver relations or other metadata	Linking information, surveillance

Table 11: Advanced security practices for experienced Tor users.

Advice	Details	Investigative method
Secure your devices with encryption	- Utilize secure encryption software like LUKS to encrypt your file storage devices - Be aware that if you only encrypt certain files, systems may store temporary files in unencrypted locations	Physical search
Maintain separate identities for different contexts	- To avoid linking different contexts (like private social media and blogging), avoid reusing existing information - This includes pseudonyms and cryptographic keys	Linking information, crypto tracing
Understand that cryptocurrencies aren't inherently anonymous	- Consider using privacy-focused cryptocurrencies like Monero - If you use pseudonymous cryptocurrencies like Bitcoin, which allow third parties to see the flow of funds, use decentralized mixing protocols like CoinJoin to obfuscate transaction flows	Crypto tracing
Handle downloaded files with caution	- As a general rule, avoid downloading files - If necessary, you can reduce the attack surface by opening downloaded files in a separate offline environment - Digital signatures can help to verify the integrity and authenticity of files	Malware, misconfigurations
Maintain a small online footprint	- Be mindful that attackers can use your public information to link to your identity - Remember that private information could also be leaked or hacked by attackers	Linking information
Use Tor bridges with pluggable transports to obfuscate Tor usage	- Tor bridges with pluggable transports can help to disguise Tor usage from your Internet Service Provider or third-parties in your local network	Surveillance, Tor protocol attacks (fingerprinting)
Diversify behaviors and characteristics across different identities	- Avoid linking different user profiles together by varying login times, linguistic expressions, and other identifiable characteristics - It's essential to consciously vary your behaviors and the details you share across different services or profiles	Linking information
Be mindful of your physical environment	- Stay aware of your physical surroundings and avoid behavior that might attract unwanted attention	Witnesses, surveillance

Table 12: Advice for Onion Service Operators.

Advice	Details	Investigative method
Tunnel all traffic through Tor	- It's crucial to route all traffic through the Tor network to prevent accidental bypasses - Any traffic that doesn't go through Tor could potentially expose the server's real IP address or other identifying information	Misconfigurations
Implement secure log management	- Log files can contain sensitive information that could potentially expose user identities or other confidential data - It's essential to manage these files securely and implement policies that limit the amount of sensitive information logged	Misconfigurations, physical search
Access your Onion Service exclusively through Tor	- Directly accessing your Onion Service without using Tor can link the service to your personal internet connection, potentially compromising your anonymity and the security of the service	Surveillance, misconfigurations
Avoid reusing configurations and software code across multiple Onion Services	- Shared characteristics, such as special configurations or reused software code, can potentially link several onion services together - This could compromise the anonymity of the services and their operators	Shared characteristics, linking information
Limit information disclosure	- Configure software to minimize the amount of information it provides to clients - This includes disabling or altering services that reveal software versions and disabling unnecessary debugging information - Remove or anonymize identifiers	Linking information, misconfigurations