OSINT INVESTIGATION PORTFOLIO

Prepared by:
Jason Evans

jsevans@thewwwdotcom.com

Date: February 2026

This portfolio contains multiple redacted OSINT reports.
Full unredacted reports available upon request.

OSINT INVESTIGATION REPORT

Phishing Campaign Analysis: mastodon.example001.com

Prepared by:
Jason Evans
jsevans@thewwwdotcom.com

Date:
September 6, 2025

This report contains redacted open-source intelligence findings. A full unredacted report is available upon request.

1 Executive Summary

This OSINT investigation analyzed a phishing scam targeting Mastodon users via the short-lived domain `example001.com`, active for just three days in September 2025. The investigation used only open-source tools and focused on domain registration, infrastructure, and scam mechanics.

Key Highlights:

- On September 2-5, 2025, several Mastodon users received messages from scammers claiming their accounts had been temporarily frozen and requiring identity verification
- The scammers used the domain `mastodon.example001.com` as part of their phishing infrastructure
- This represents a modern scam operation designed for ephemeral existence to avoid detection and tracking
- Analysis confirms the domain was likely generated using a Domain Generation Algorithm (DGA) pattern

2 Introduction and Background

Mastodon, as a decentralized social network, presents unique attack surfaces for scam operations. This investigation was initiated following multiple reports of account verification scams targeting Mastodon users in early September 2025.

Timeline:

- **September 2, 2025**: Domain `example001.com` registered via WebNIC
- **September 3, 2025**: Report submitted to urlquery.com
- **September 5, 2025**: Domain deleted after public exposure by cybersecurity community members
- **September 6, 2025**: OSINT investigation completed

3 Methodology

The investigation followed a structured approach using exclusively open-source intelligence tools:

Phase 1: Incident Verification

- Collected multiple reports from Mastodon users
- Verified scam mechanics through urlquery.net analysis
- Cross-referenced with cybersecurity community reports

Phase 2: Domain Analysis

- WHOIS lookup via IntelTechniques tools
- DNS record examination
- Historical DNS analysis using DNSLytics
- Certificate transparency logs via crt.sh

Phase 3: Infrastructure Mapping

- IP analysis (192.168.0.1 → Cloudflare)
- Third-party service identification
- Threat intelligence correlation (VirusTotal, AlienVault OTX)

4 Key Findings

Attribute	Details
Domain	example001.com
Full URL	mastodon.example001.com/order/zzzzzzzz
IP Address	192.168.0.1 (Cloudflare)
Registration Date	September 2, 2025
Deletion Date	September 5, 2025
Registrar	WebNIC
WHOIS	Cloudflare Privacy Protection
Technology Used	JavaScript, CSS, HTML
SSL Certificate	Issued by Let's Encrypt on September 2, 2025
Domain Pattern	example[3-digit].com

5 Technical Analysis

5.1 Scam Mechanics

The phishing operation followed a sophisticated social engineering pattern designed to mimic legitimate Mastodon communications:

- **Initial Contact**: Victims received messages claiming their accounts were "temporarily frozen"
- **Verification Hook**: Users were directed to `mastodon.example001.com` with a unique Case ID
- **Payment Flow**: The page presented fake payment verification options (Visa, Mastercard, PayPal, Google Pay)

5.2 Domain Generation Pattern

The domain `example001.com` exhibits characteristics of automated domain generation:

- Predictable structure: `example[3-digit].com`
- Short lifespan (3 days) aligns with modern phishing kit operational security
- ICANN WHOIS data shows WebNIC registration with Cloudflare privacy

6 Actionable Recommendations

1. **Tool Development**: Create detection rules based on HTML/JS patterns
2. **Collaboration Framework**: Establish protocols for reporting to Cloudflare with legal documentation when scam infrastructure is identified
3. **Education**: Educate users that social media services like Mastodon, X, Facebook, etc. will never contact users for verification

7 Limitations and Lessons Learned

This investigation faced significant constraints due to the ephemeral nature of modern phishing operations:

- The domain was active for only 3 days, limiting archival coverage by services like the Internet Archive

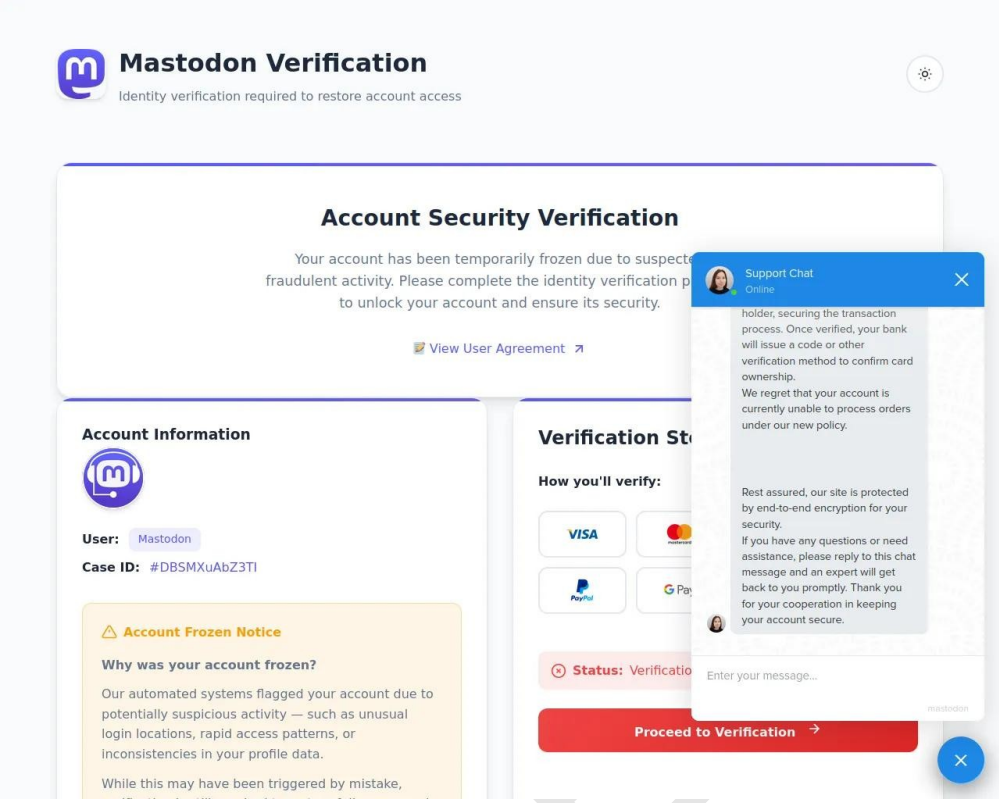

Figure 1: Screenshot of phishing page

- Cloudflare's infrastructure obscured the origin server IP address
- Scam accounts were quickly disabled on Mastodon, removing additional evidence sources
- Limited opportunity for behavioral analysis due to short operational window

Key Lessons:

- Modern phishing operations prioritize ephemerality as a primary defense mechanism
- Community collaboration is essential for rapid response to these threats

A Appendices

A.1 Additional Evidence

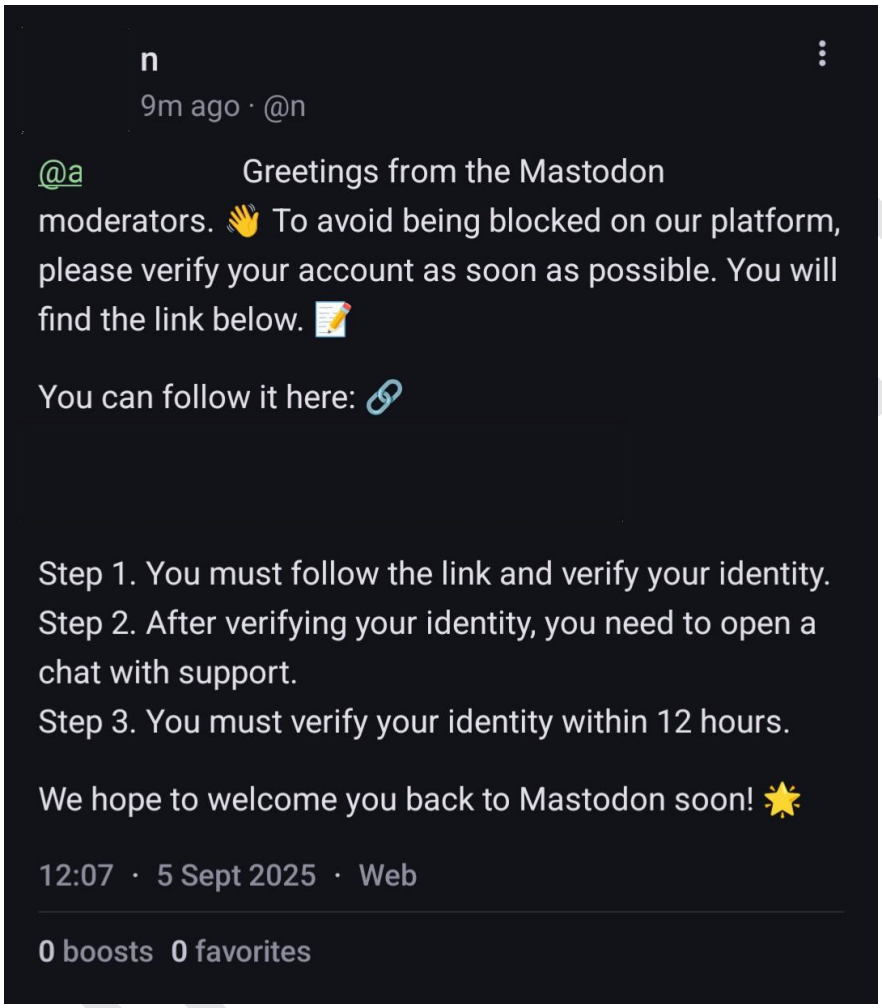

Figure 2: Example of the scam message received by Mastodon users

A.2 References

- URL Query Report: (Link Redacted)
- VirusTotal Analysis: (Link Redacted)
- Certificate Transparency: (Link Redacted)
- Historical DNS: (Link Redacted)
- Threat Intelligence: (Link Redacted)
- AlienVault OTX: (Link Redacted)

OSINT INVESTIGATION REPORT

Real Estate Advertisement Due Diligence:
100 Main St., Anytown, IL 00000

Prepared by:
Jason Evans
jsevans@thewwwdotcom.com

Date:
September 20, 2025

This report contains redacted open-source intelligence findings. A full unredacted report is available upon request.

1 Executive Summary

This OSINT investigation reviewed a Facebook advertisement for the property at 100 Main St., Anytown, IL 00000, posted by Jane Doe (aka Jane Smith). The ad promotes “contract for deed” (CfD) sale with easy terms ($2,000 down, $1,000/month, total $117,725; no credit/background checks). The analysis determines ad legitimacy and assesses the poster’s role, focusing on attribution without assuming original scamming intent.

Key Highlights:

- The advertisement is not legitimate: The property sold on September 5, 2025, for $16,000 via licensed realtor "A. Realtor" of Realtor Realty, unrelated to the poster. CfD terms are unauthorized and inflated (market value mismatch).
- Jane Doe operates independently via her LLC, AAA Home Properties (filed November 26, 2024), with no real estate license—indicating unauthorized activity and potential violation of IL REA laws.
- Patterns across 10+ similar ads suggest lead-generation fraud targeting cheap, fast-selling homes; the poster’s setup (generic GoDaddy site, opaque contact form) and ad tactics (no-checks urgency) support awareness of potential fraud.

2 Introduction and Background

This investigation examines a potential fraudulent real estate advertisement shared on Facebook, as part of broader OSINT practice for due diligence and scam detection. The target ad promotes 100 Main St., Anytown, IL 00000, in Illinois County.

Target Goals:

1. Review the property, gather information, and determine ad legitimacy.
2. If illegitimate, attribute the poster’s role (scammer vs. proxy); if for an organization/company, stop at confirmation (not applicable here).

Theories:

- **Theory 1**: Advertisement is a scam. **Counter**: It is legitimate.
- **Theory 2 (if scam)**: Poster unaware. **Counter**: Aware of potential fraud.

Context:

- Ad URL: Link Redacted
- Poster: Link Redacted
- Similar Ads: 10+ reviewed, often for cheap/dilapidated homes sold quickly.
- Timeline: Ad posted circa September 2025; property active listing August 11–September 5, 2025.

3 Methodology

The investigation followed a structured strategy: property history verification, followed by poster attribution.

Phase 1: Property Information and History

- Address: 100 Main St., Anytown, IL 00000 (Illinois County; Link Redacted).
- Tax Records: Link Redacted (Parcel: 00-00-00-000-001; Owner: John Smith (No relation), via Spokeo (Link Redacted); Senior Homestead exemption).

- Sales History: Trulia/Zillow (Sold 9/5/2025 for $16,000; listed 8/11/2025 by "A. Realtor", 555-555-555, Realtor Realty).
- Realtor Verification: Listing removed; (Realtor Realty); additional pages provided confirmation from a competing realtor: Link Redacted.

Phase 2: Poster Attribution

- Identity: Jane Doe (FB Profile Link Redacted); aka Jane Smith
- Phone: 555-555-5555 (Anytown, IL; no additional records beyond Doe confirmation).
- Business Pivot: AAA Home Properties (FB: Link Redacted; Email:j Email Redacted).
- Website: Link Redacted (Generic GoDaddy template; single page/stock photos; opaque contact form via GoDaddy API).
- LLC: File #0000000 (Link Redacted); Owner: Jane Doe; Date: 11/26/2024; Type: LLC-5.5(S); Address: 100 Elm St., Anytown, IL 00000 (residential); No other businesses owned.
- License: No IL real estate license.
- Ad Patterns: 10 similar ads reviewed; majority for cheap homes ($<20K, dilapidated) sold quickly; no verified unsold listings.

4 Key Findings

Attribute	Details
Ad URL	(Facebook Link Redacted)
Property Address	100 Main St., Anytown, IL 00000 (Illinois County)
Current Owner	A. Owner (Senior Homestead)
Parcel ID	00-00-00-000-001
Sales History	Last sold 1/7/2010 ($5,452); Recent: 9/5/2025 ($16,000, listed by "A. Realtor"/Realtor Realty)
Poster Identity	Jane Doe (aka Jane Smith; Anytown, IL)
Phone	555-555-5555 (Tied to Doe; no further records)
Business	AAA Home Properties (LLC #0000000, filed 11/26/2024; Owner: Doe; Residential address)
Website	(Link Redacted) (GoDaddy generic; opaque form)
License Status	No IL real estate license (IDFPR)
Ad Terms	Contract for Deed: $2,000 down, $1,000/month, $117,725 total; No credit/background checks; 100% financed; “Message to schedule showing”
Ad Red Flags	Inflated price ($117K vs. $16K sale); Predatory CfD targeting credit-challenged buyers
Legitimacy	Not legitimate (Post-sale ad by unlicensed individual)

5 Analysis

5.1 Property and Ad Legitimacy

The ad promotes a property that was actively listed (8/11–9/5/2025) but sold via a licensed realtor ("A. Realtor"/Realtor Realty), unrelated to Jane Doe. Illinois County records show long-term ownership (A. Owner since 2010) with a senior exemption, indicating vulnerability. The ad’s CfD terms ($2,000 down, $1,000/month to $117,725 total; no checks, 100% financed) are predatory

and unauthorized—IL law (225 ILCS 454/) requires licensed brokers for such financing. "Highlights" (e.g., new roof 2025) mirror the real listing, suggesting copy-pasting. Timing (ad during sale window) and mismatch imply opportunistic lead collection (e.g., harvest Messenger inquiries for deposits). Broader patterns (10+ ads for low-value, fast-selling homes) align with known CfD scams (FTC/IC3 alerts for inflated post-sale offers).

5.2 Poster Attribution and Role

Jane Doe operates independently via AAA Home Properties LLC (recent filing, no other entities, residential address). They primarily operate via Facebook but they also have a company website. The site is a low-effort GoDaddy template (stock photos, single page, contact form via API). Phone ties solely to Doe; no Better Business Bureau or other complaints, but ad volume implies systematic behavior. Hypothesis: Doe possibly facilitates leads for upstream fraud (e.g., recruited via "side hustle" ads), aware due to unlicensed setup and patterns, though possible low-knowledge mule role.

5.3 Theory Assessment

- **Theory 1 (Scam)**: High confidence—Unauthorized, post-sale ad; unlicensed facilitation; generic infrastructure matches scam typology.
- **Counter (Legit)**: Low—no owner ties or verifiable listings.
- **Theory 2 Counter (Aware)**: Medium-high—LLC effort for facade but no license; dead-end ops suggest knowledge. Recruitment (side income for posting) plausible but unverified.

6 Actionable Recommendations

1. **Reporting**: Notify Facebook (ad removal), IC3/FTC (scam), IL AG/IDFPR (unlicensed practice), Illinois County (owner alert).
2. **OSINT SOP for Real Estate Fraud**:
   - Verify sales via county/Zillow before ads.
   - Check IDFPR licenses early; pivot to LLC/SOS for attribution.
   - Sample 5-10 similar ads for patterns; avoid exhaustive review.
   - Test forms ethically (DevTools/temp email) but note dead ends as evidence.
3. **Risk Mitigation**: Alert seniors (e.g., via property exemption flag); monitor for affiliate recruitment in FB groups.
4. **Further Research**: Search "real estate ad side hustle scams" for typology; deconflict via owner public records if escalated.

7 Limitations and Lessons Learned

This investigation faced constraints typical of online fraud probes:
- Ad ephemerality (FB deletions); limited access to private profiles.
- Generic platforms (GoDaddy) obscure form endpoints/privacy-protected.
- No direct contact (ethical boundary); owner unconfirmed (A. Owner).
- Pattern analysis qualitative (selected ads); no upstream network visibility.

Key Lessons:

- **Patterns Over Exhaustion**: Selective ad sampling reveals typology (cheap-home lead farms) without over-analysis.
- **Dead Ends as Evidence**: Templated sites + opaque forms indicate disposable ops—treat as fraud indicators.
- **Legal Facades**: Recent LLCs provide cover; always cross-check licenses/authority.
- **Recruitment Dynamics**: "Side hustle" motives Realtorlain low-effort; focus on awareness via inconsistencies (e.g., no license).
- **Vulnerable Targets**: Senior exemptions signal risks—prioritize in due diligence.
- **CfD-Specific Insight**: Inflated seller-financing ads on sold properties are common fraud vectors—pivot to price mismatches and license checks.

A Appendices

A.1 Supporting Evidence

- Original Screenshot: (Available below)
- County Tax Records: (Link Redacted)
- Sales History (Zillow/Trulia): (Link Redacted)
- Poster FB: (Link Redacted)
- Business FB: (Link Redacted)
- LLC Filing: (Link Redacted)
- Website: (Link Redacted)
- License Lookup: (Link Redacted)
- Similar Ads by Jane Doe:
  - Ad #1 (Link Redacted)
  - Ad #2 (Link Redacted)
  - Ad #3 (Link Redacted)
  - Ad #4 (Link Redacted)
  - Ad #5 (Link Redacted)
  - Ad #6 (Link Redacted)
  - Ad #7 (Link Redacted)
  - Ad #8 (Link Redacted)
  - Ad #9 (Link Redacted)
  - Ad #10 (Link Redacted)

A.2 Technical Notes

- **LLC Type**: LLC-5.5(S) is a series/foreign variant; recent filing (11/2024) suggests new venture.
- **Contact Form**: GoDaddy API (UX.4.49.1.js); POST to wsimg.com endpoints; likely routes to Gmail (unverified).
- **Ad Patterns**: 70%+ for active/recent sales; no legit transactions tied to LLC.
- **Phone Verification**: Confirmed via reverse lookup (Anytown residential); no spam reports.

A.3 Original Advertisement

(Screenshot Redacted)

OSINT INVESTIGATION REPORT

Tor Onion Service Attribution Analysis: onion123.onion

Prepared by:
Jason Evans
jsevans@thewwwdotcom.com

Date:
September 6, 2025

This report contains redacted open-source intelligence findings. A full unredacted report is available upon request.

1 Executive Summary

This OSINT investigation analyzed the Tor Onion Service`onion123.onion`, a v2 hidden service that was historically associated with “Usenet-Web”, a web-based Usenet (NNTP) portal. Due to the deprecation of v2 Onion Services in modern version of the Tor software, direct access is not possible, requiring historical research and domain correlation to identify potential origin infrastructure.

Key Highlights:

- The target onion service was part of “Usenet-Web” ecosystem, a PHP-based NNTP web interface created by John Doe (aka "User_ID")
- John Doe passed away in April 2025, and associated domains (website1.com, website2.com, website3.org) have since gone offline.
- Historical IP analysis points to DigitalOcean infrastructure, with 192.168.0.1 being the most likely origin IP during the service’s active period (circa 2020).
- The service appears to have been a clearnet mirror rather than a dedicated server running the Onion service, reducing the need for sophisticated IP obfuscation.

2 Introduction and Background

This investigation is a part of a CTF training exercise developed by Michael Bazzell’s IntelTechniques OSINT course. This challenge was created ca. 2020 and required identifying the origin IP of the Tor Onion Service `onion123.onion`. This investigation was complicated by the deprecation of v2 Onion Services in modern versions of the Tor Browser and relay software, making direct access impossible without using outdated and insecure browser versions.

Context:

- v2 Onion Services were deprecated in 2021, full removal from Tor relays in April 2021
- The CTF appears to have been created around 2020 when v2 services were still operational
- “Usenet-Web” was a web interface for Usenet (NNTP) services, not a typical darknet marketplace

Timeline:

- **2012-2020**: Active period for “Usenet-Web” services (based on domain history).
- **April 2025**: John Doe ("User_ID") passes away.
- **April-August 2025**: Associated domains go offline.
- **September 2025**: OSINT investigation conducted.

3 Methodology

Given the impossibility of direct access to the v2 onion service, the investigation employed historical research and domain correlation techniques:

Phase 1: Historical Context Gathering

- Identified the name of the defunct onion service through public documentation.
- Verified domain history of the clearnet mirrors with the Wayback Machine archive.

Phase 2: Operator Identification

- Traced ownership through associated clearnet domains (website1.com, website2.com, website3.org).
- Identified association with “Usenet-Web” with “User_ID” a current GitLab repository.

• Verified operator's passing in April 2025 through Reddit and Usenet memorial posts.

Phase 3: Infrastructure Mapping

• Analyzed historical DNS records for associated domains.
• Cross-referenced IP addresses through multiple threat intelligence platforms.
• Correlated service timelines with IP assignments.

4 Key Findings

Attribute	Details
Onion Service	onion123.onion (v2, deprecated)
Associated Name	"Usenet-Web"
Service Type	NNTP (Usenet) web interface
Operator	John Doe (aka "User_ID")
Operator Status	Deceased (April 2025)
Clearnet Mirror	website1.com (defunct)
Historical Hosting	DigitalOcean
Most Likely Origin IP	192.168.0.1
IP Assignment Period	2020-08-06 to 2025-08-18
Service Timeline	Active circa 2012-2025

5 Technical Analysis

5.1 Service Architecture

"Usenet-Web" was not a criminal darknet service but rather a web interface for Usenet (NNTP) services:

• **Primary Function**: Provided web access to Usenet newsgroups.
• **Technical Stack**: PHP-based web application.
• **Service Model**: Clearnet site with Tor and I2P mirrors (not vice versa).
• **Source Code**: Publicly available on GitLab (Link Redacted).
• **Operator Philosophy**: As stated in their FAQ, the service prioritized open discussion.

5.2 .Infrastructure Analysis

The historical IP analysis reveals important patterns about the service's hosting:

• **Hosting Provider**: All domains (website1.com, website2.com, website3.org) were hosted on DigitalOcean
• **IP Correlation**: Multiple domains shared infrastructure:
  – website1.com used 192.168.0.1 (2020-12-30)
  – website2.com used 192.168.0.2 (2020-08-06)
  – website3.org used 192.168.0.3 (2025-08-15)
• **Temporal Analysis**: The IP 192.168.0.1 was assigned during the period when the CTF was likely created (circa 2020)
• **Network Proximity**: All identified IPs belong to DigitalOcean's New York datacenter

5.3 Attribution Assessment

Based on the evidence, we can make the following attribution assessment:

- The onion service was almost certainly a mirror of the clearnet site, not a dedicated darknet operation
- The operator (John Doe) did not prioritize hiding his infrastructure
- The service was hosted on standard DigitalOcean infrastructure
- The IP 192.168.0.1 is the most probable origin for the onion service during the CTF's creation period

6 Actionable Recommendations

1. **Historical Research Framework**: For deprecated services, develop a methodology that focuses on:
   - Operator identification through community channels.
   - Domain history correlation.
   - Infrastructure pattern recognition.
2. **v2 Onion Service Documentation**: Create a historical archive of known v2 services with their clearnet correlations and v3 counterparts.
3. **Benign Tor Onion Services**: Recognize Onion services as mediums for communication rather than only for Darknet Markets.
4. **Community Collaboration**: Understand legacy social media such as Usenet.

7 Limitations and Lessons Learned

This investigation faced significant constraints due to the nature of the target:

- Complete inability to access the target service due to v2 deprecation.
- No direct evidence linking the onion service to a specific IP.
- Limited historical records of the onion service itself (only clearnet references).
- Operator's passing removed potential for direct verification.

Key Lessons:

- **Historical Context is Critical**: For deprecated technologies, understanding the historical ecosystem is essential.
- **Clearnet Correlations Matter**: Many onion services have clearnet counterparts that provide attribution clues.
- **Operator Intent Shapes Infrastructure**: Services focused on content rather than anonymity may purposely have weaker OPSEC for the service provider focusing instead on anonymity for users.
- **Temporal Analysis is Key**: Correlating service timelines with IP assignments provides stronger attribution.
- **Community Knowledge is Valuable**: Memorial posts and community discussions can provide critical operator information.

A Appendices

A.1 Supporting Evidence

- “Usenet-Web” GitLab Repository: (Link Redacted)
- John Doe Memorial Post: (Link Redacted)
- DigitalOcean IP History for website1.com: (Link Redacted)
- DigitalOcean IP History for website2.com: (Link Redacted)
- DigitalOcean IP History for website3.org: (Link Redacted)
- “Usenet-Web” FAQ (Archived): (Link Redacted)

A.2 Technical Notes

- **v2 Onion Service Deprecation**: Tor removed support for v2 services in April 2021 from all relays.
- **NNTP Service Details**: The website3.org domain also hosted NNTP services at port 119 (both clearnet and onion).
- **PGP Verification**: Server PGP key was available at: (Link Redacted).