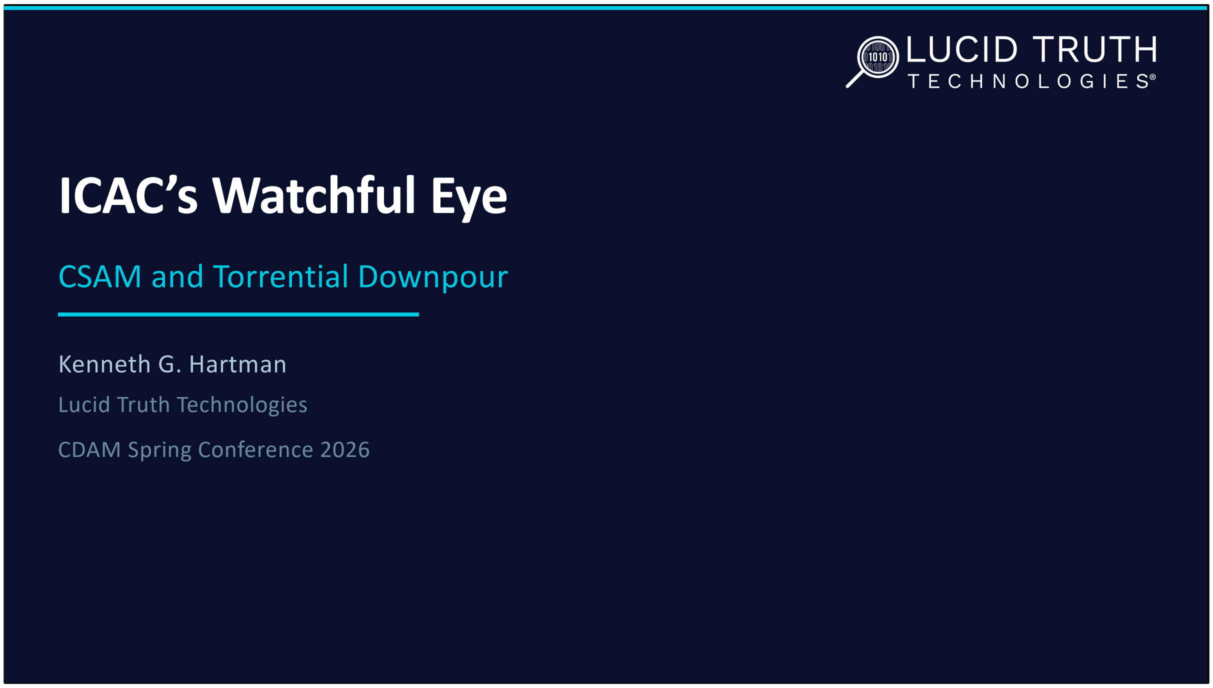


LUCID TRUTH TECHNOLOGIES®

ICAC’s Watchful Eye

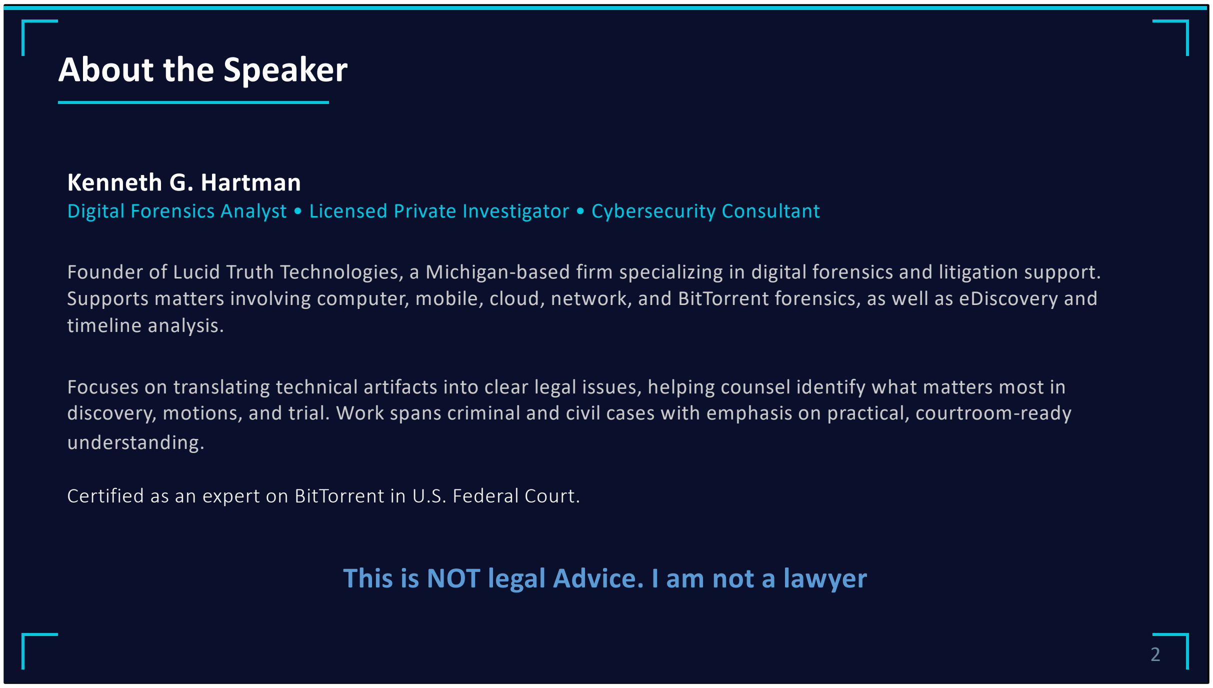
CSAM and Torrential Downpour

Kenneth G. Hartman

Lucid Truth Technologies

CDAM Spring Conference 2026

Kenneth G. Hartman is a digital forensics analyst, licensed private investigator, and founder of Lucid Truth Technologies. This presentation provides defense attorneys with a practical understanding of how CSAM cases are built from BitTorrent evidence using Torrential Downpour and similar ICAC tools, with a focus on actionable courtroom strategy.



About the Speaker

Kenneth G. Hartman

Digital Forensics Analyst • Licensed Private Investigator • Cybersecurity Consultant

Founder of Lucid Truth Technologies, a Michigan-based firm specializing in digital forensics and litigation support. Supports matters involving computer, mobile, cloud, network, and BitTorrent forensics, as well as eDiscovery and timeline analysis.

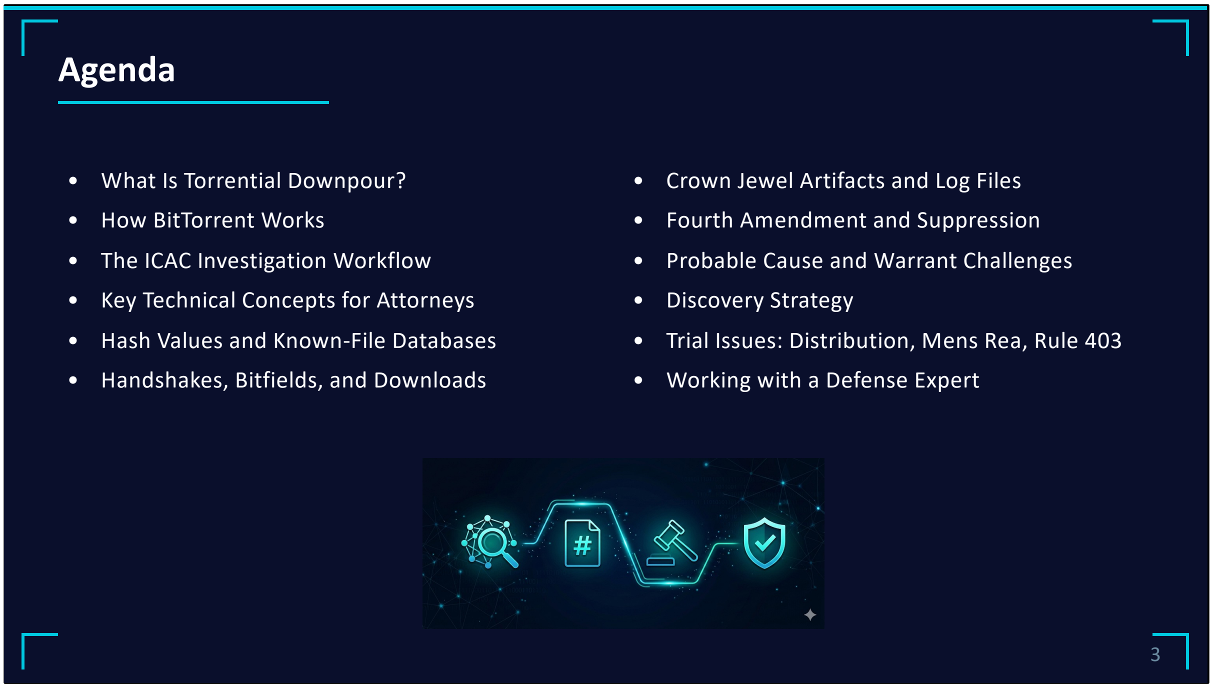
Focuses on translating technical artifacts into clear legal issues, helping counsel identify what matters most in discovery, motions, and trial. Work spans criminal and civil cases with emphasis on practical, courtroom-ready understanding.

Certified as an expert on BitTorrent in U.S. Federal Court.

This is NOT legal Advice. I am not a lawyer

2

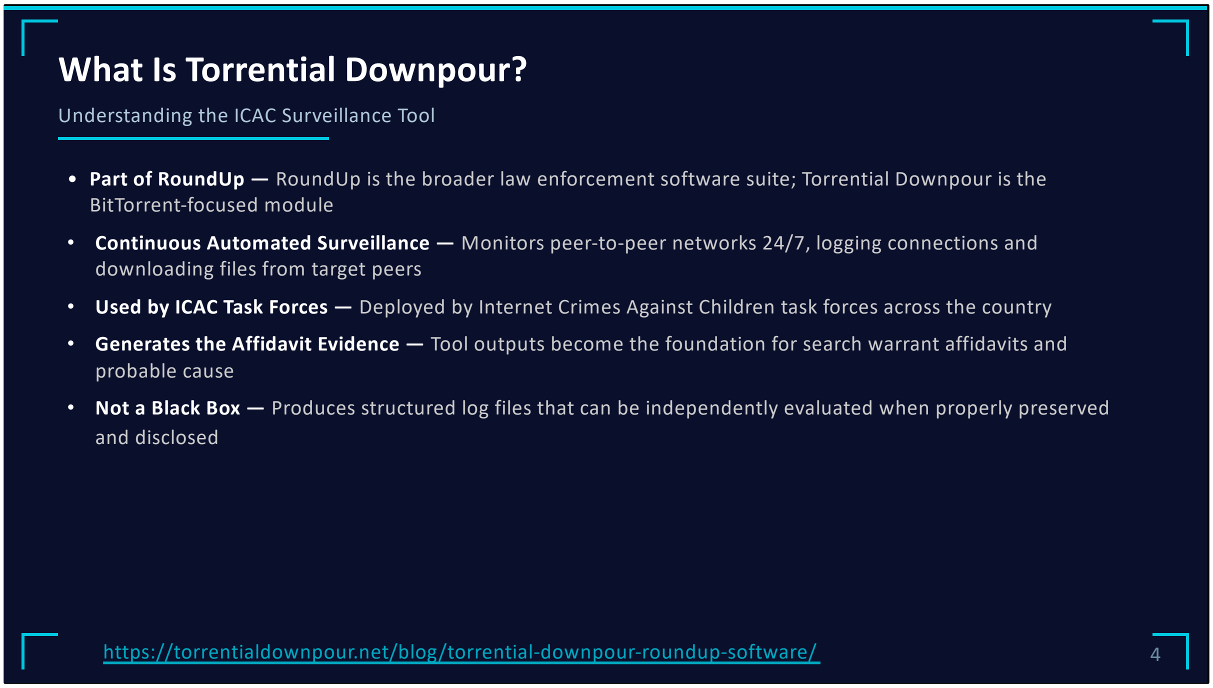
Kenneth G. Hartman brings extensive practical experience supporting defense attorneys with digital evidence interpretation, specializing in BitTorrent forensics. His work focuses on helping attorneys effectively evaluate and challenge this type of evidence through independent forensic analysis.



Agenda

- What Is Torrential Downpour?
- How BitTorrent Works
- The ICAC Investigation Workflow
- Key Technical Concepts for Attorneys
- Hash Values and Known-File Databases
- Handshakes, Bitfields, and Downloads
- Crown Jewel Artifacts and Log Files
- Fourth Amendment and Suppression
- Probable Cause and Warrant Challenges
- Discovery Strategy
- Trial Issues: Distribution, Mens Rea, Rule 403
- Working with a Defense Expert

This presentation is organized into two main sections. The first half covers the technical foundation — key concepts attorneys need to recognize without becoming forensic experts. The second half focuses on litigation strategy: Fourth Amendment arguments, warrant challenges, discovery, and trial issues. Throughout, technical concepts are connected to specific courtroom applications.



What Is Torrential Downpour?

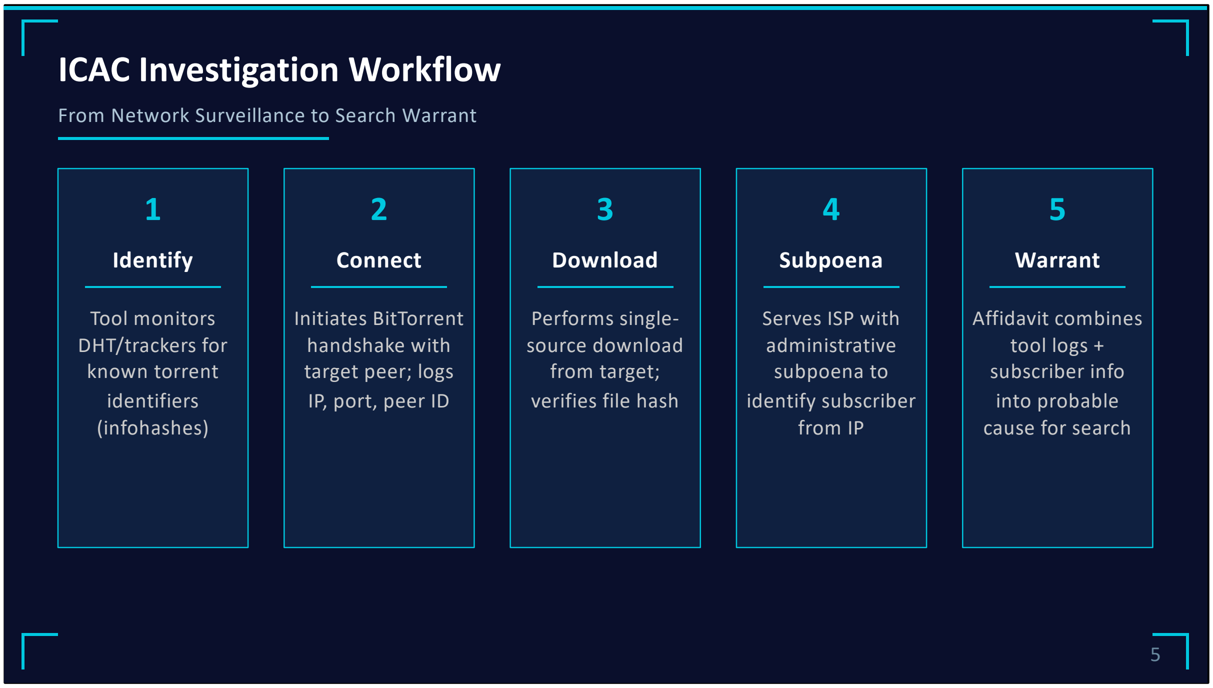
Understanding the ICAC Surveillance Tool

- **Part of RoundUp** — RoundUp is the broader law enforcement software suite; Torrential Downpour is the BitTorrent-focused module
- **Continuous Automated Surveillance** — Monitors peer-to-peer networks 24/7, logging connections and downloading files from target peers
- **Used by ICAC Task Forces** — Deployed by Internet Crimes Against Children task forces across the country
- **Generates the Affidavit Evidence** — Tool outputs become the foundation for search warrant affidavits and probable cause
- **Not a Black Box** — Produces structured log files that can be independently evaluated when properly preserved and disclosed

https://torrentialdownpour.net/blog/torrential-downpour-roundup-software/

4

Torrential Downpour is a module within the RoundUp law enforcement suite, specifically designed to monitor BitTorrent networks for CSAM distribution. The tool produces structured artifacts (log files, XML records) that can and should be independently evaluated. These outputs are not self-validating — they require interpretation, and that interpretation can be challenged. Understanding what the tool actually does versus what an affidavit says it does is the foundation of effective defense work. Blog: https://torrentialdownpour.net/blog/torrential-downpour-roundup-software/



ICAC Investigation Workflow

From Network Surveillance to Search Warrant

1
Identify
Tool monitors DHT/trackers for known torrent identifiers (infohashes)

2
Connect
Initiates BitTorrent handshake with target peer; logs IP, port, peer ID

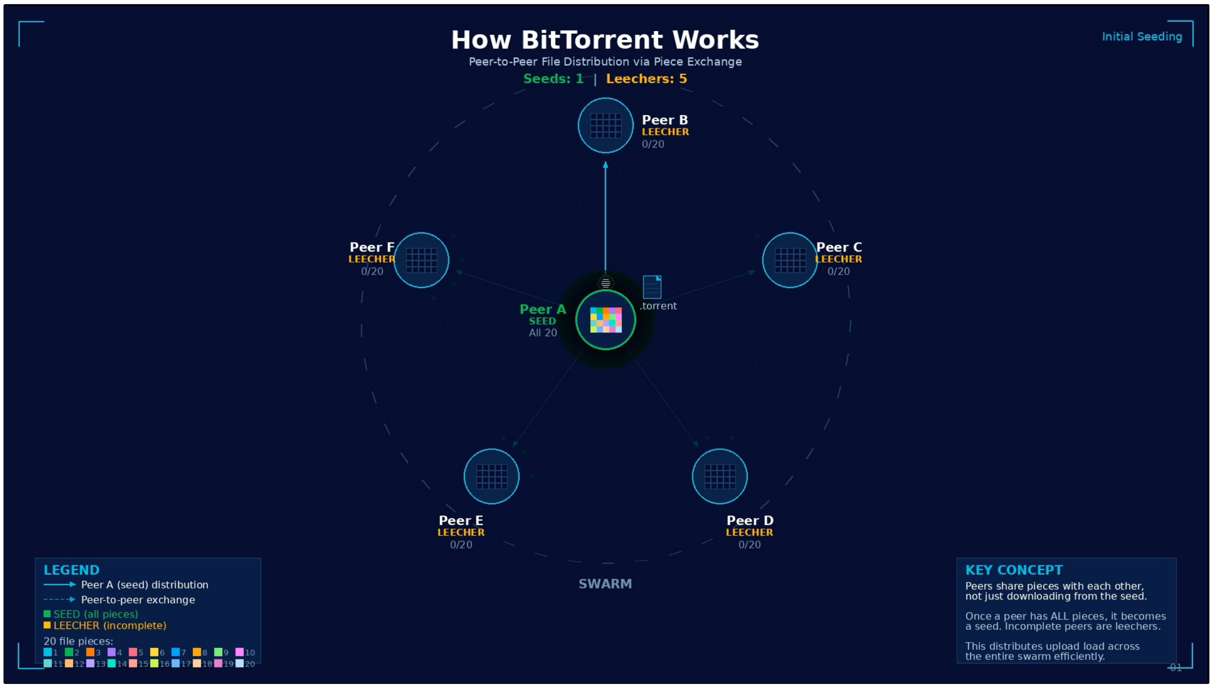
3
Download
Performs single-source download from target; verifies file hash

4
Subpoena
Serves ISP with administrative subpoena to identify subscriber from IP

5
Warrant
Affidavit combines tool logs + subscriber info into probable cause for search

5

The five-stage ICAC investigation workflow: (1) The tool monitors for known infohashes on the BitTorrent network. (2) It connects to the target peer via the BitTorrent handshake protocol. (3) It performs a download, often described as 'single-source.' (4) Law enforcement subpoenas the ISP to map the observed IP address to a subscriber. (5) All evidence is combined into a search warrant affidavit. Each stage produces artifacts that defense counsel should request, and each involves assumptions and potential points of failure that can be challenged. Blog: https://torrentialdownpour.net/blog/torrential-downpour-roundup-software/



How BitTorrent Works

Peer-to-Peer File Distribution via Piece Exchange

KEY CONCEPT

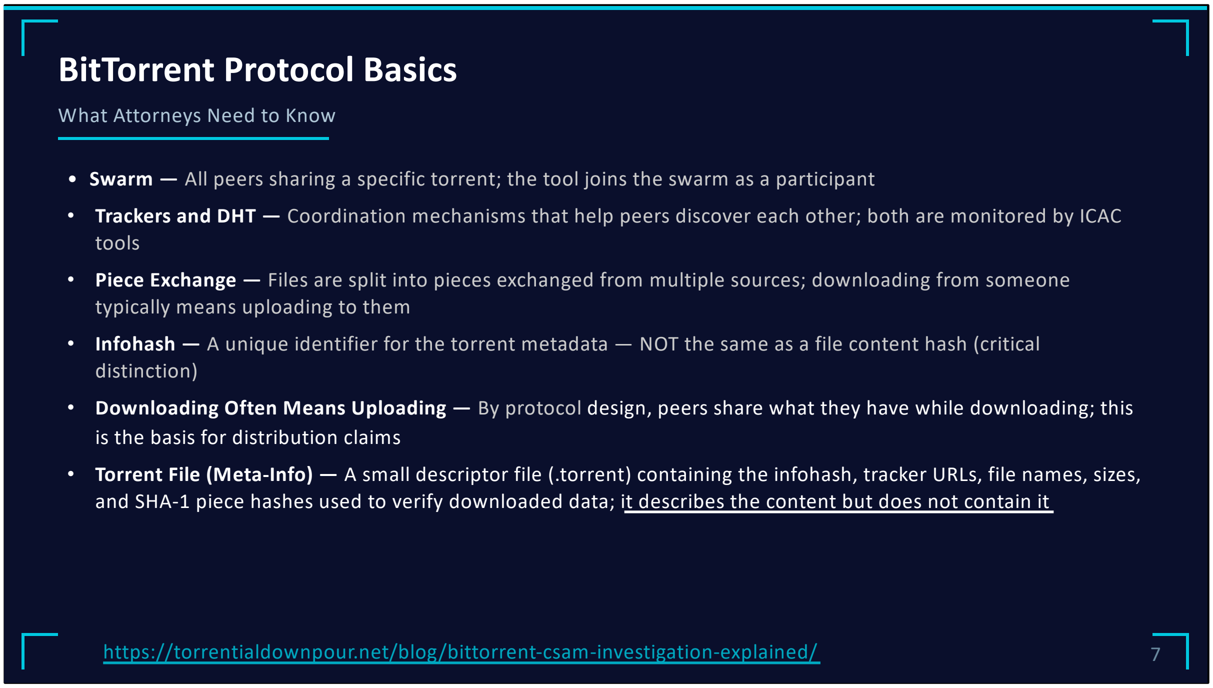
Peers share pieces with each other, not just downloading from the seed.

Once a peer has ALL pieces, it becomes a seed. Incomplete peers are leechers.

This distributes upload load across the entire swarm efficiently.

Key BitTorrent concepts:

- A swarm consists of all peers sharing a particular torrent.
- Trackers are central coordination points (servers) that help peers find each other (but do not contain torrent content),
- DHT (Distributed Hash Table) provides decentralized peer discovery.
- Files are split into pieces that are exchanged between peers.
- Seeders have complete files; leechers are still downloading.
- Importantly, downloading from a peer typically means simultaneously uploading to them — this bidirectional transfer is the protocol basis for distribution charges.



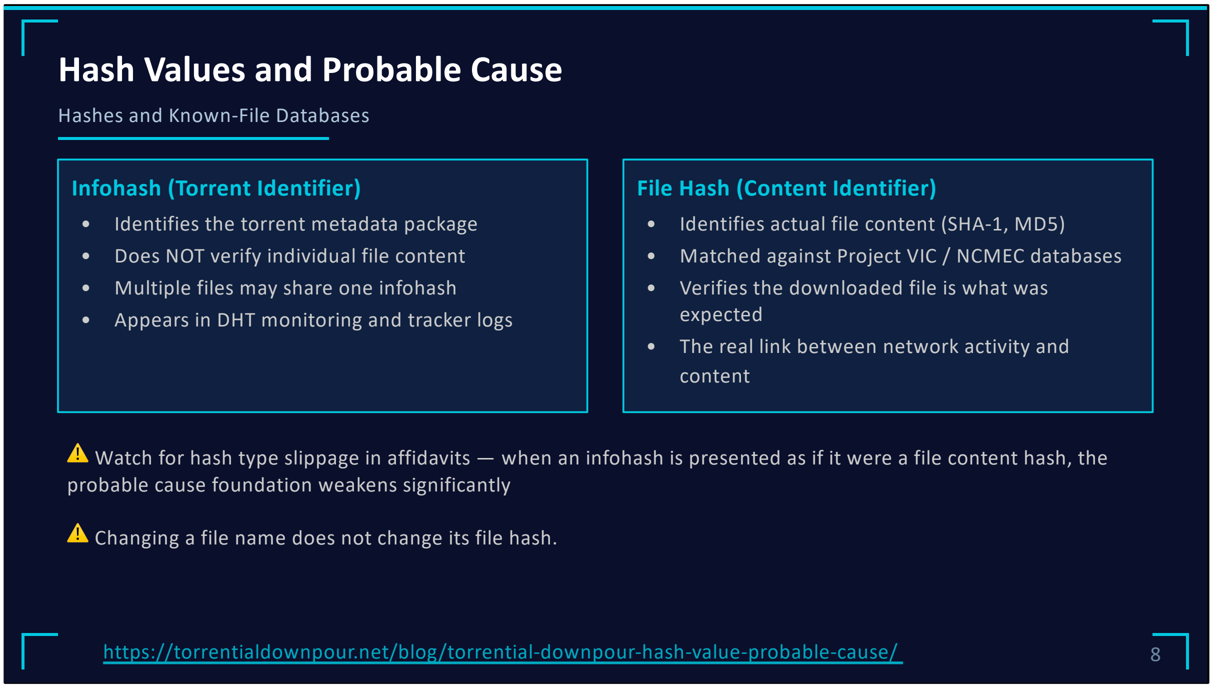
BitTorrent Protocol Basics

What Attorneys Need to Know

- **Swarm** — All peers sharing a specific torrent; the tool joins the swarm as a participant
- **Trackers and DHT** — Coordination mechanisms that help peers discover each other; both are monitored by ICAC tools
- **Piece Exchange** — Files are split into pieces exchanged from multiple sources; downloading from someone typically means uploading to them
- **Infohash** — A unique identifier for the torrent metadata — NOT the same as a file content hash (critical distinction)
- **Downloading Often Means Uploading** — By protocol design, peers share what they have while downloading; this is the basis for distribution claims
- **Torrent File (Meta-Info)** — A small descriptor file (.torrent) containing the infohash, tracker URLs, file names, sizes, and SHA-1 piece hashes used to verify downloaded data; it describes the content but does not contain it

https://torrentialdownpour.net/blog/bittorrent-csam-investigation-explained/

Essential BitTorrent terminology for legal professionals: The most important concept is that BitTorrent is architecturally designed so that downloading simultaneously means uploading. This creates the legal exposure for distribution charges — not necessarily any deliberate decision by the user to distribute. The infohash identifies a torrent's metadata (which torrent is being shared), while a file hash (SHA-1, MD5) verifies actual file content. This distinction between infohash and file hash is critical and recurs throughout the forensic analysis. Blog: https://torrentialdownpour.net/blog/bittorrent-csam-investigation-explained/



Hash Values and Probable Cause

Hashes and Known-File Databases

Infohash (Torrent Identifier)

- Identifies the torrent metadata package
- Does NOT verify individual file content
- Multiple files may share one infohash
- Appears in DHT monitoring and tracker logs

File Hash (Content Identifier)

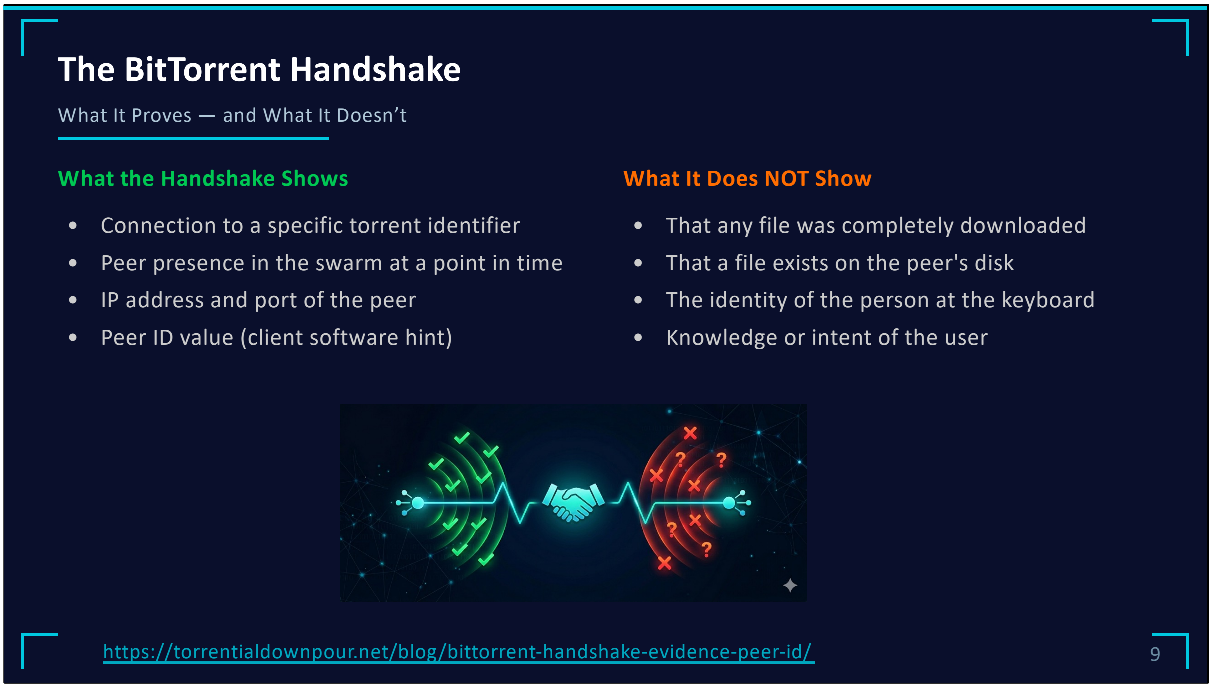
- Identifies actual file content (SHA-1, MD5)
- Matched against Project VIC / NCMEC databases
- Verifies the downloaded file is what was expected
- The real link between network activity and content

⚠ Watch for hash type slippage in affidavits — when an infohash is presented as if it were a file content hash, the probable cause foundation weakens significantly

⚠ Changing a file name does not change its file hash.

https://torrentialdownpour.net/blog/torrential-downpour-hash-value-probable-cause/

This is one of the most important technical distinctions in BitTorrent forensics. An infohash identifies the torrent metadata — it confirms which torrent was being shared but does not verify that any particular file was actually received or that the content matches a known CSAM image. A file hash (SHA-1, MD5) verifies actual file content by matching against databases like Project VIC. Affidavits sometimes blur these two types, presenting an infohash match as equivalent to a file content match. This conflation is a potential Franks challenge target. The key question: did the tool verify the actual file content via hash, or only confirm the torrent identifier? Blog: https://torrentialdownpour.net/blog/torrential-downpour-hash-value-probable-cause/



The BitTorrent Handshake

What It Proves — and What It Doesn’t

What the Handshake Shows

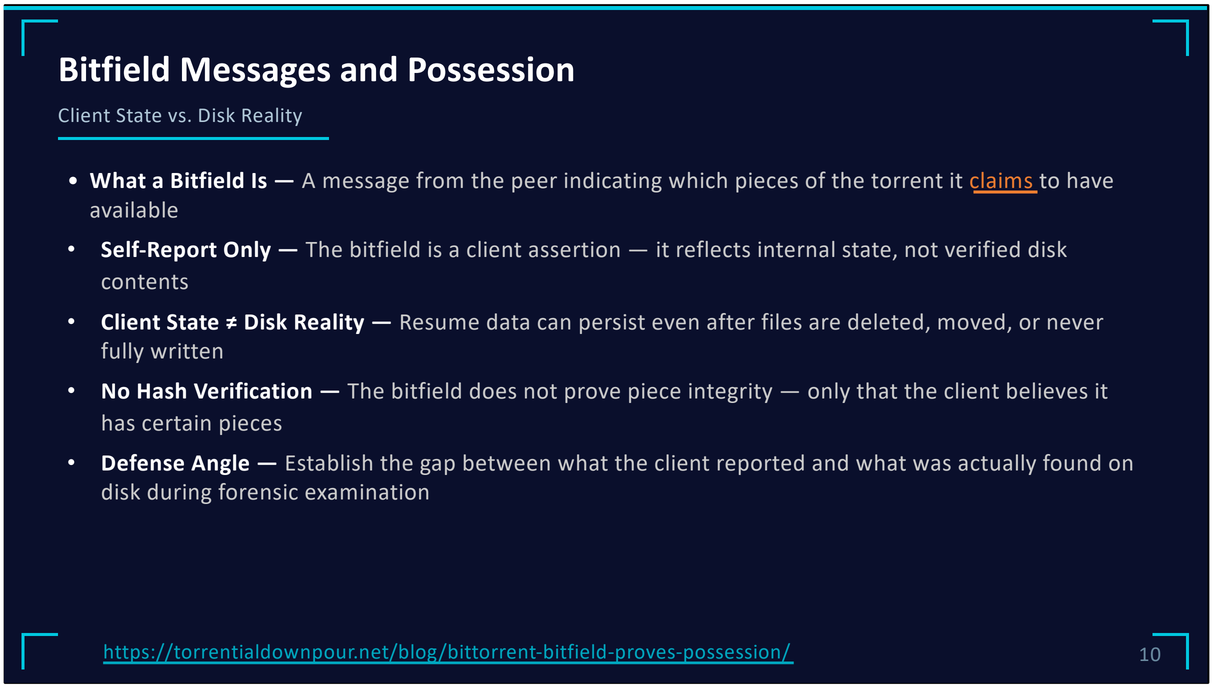
- Connection to a specific torrent identifier
- Peer presence in the swarm at a point in time
- IP address and port of the peer
- Peer ID value (client software hint)

What It Does NOT Show

- That any file was completely downloaded
- That a file exists on the peer's disk
- The identity of the person at the keyboard
- Knowledge or intent of the user

https://torrentialdownpour.net/blog/bittorrent-handshake-evidence-peer-id/

The BitTorrent handshake is the first step in any connection between peers. It confirms that two peers are communicating about the same torrent. What the handshake proves: that a connection existed between the tool and the target IP at a specific time for a specific torrent. What it does NOT prove: that any file was downloaded, that any file exists on disk, or who was using the computer. The peer_id field may indicate which BitTorrent client software was used (e.g., uTorrent, qBittorrent) but cannot identify the person operating it. For cross-examination purposes: establish what the handshake actually demonstrated, then highlight what was assumed beyond the evidence. Blog: https://torrentialdownpour.net/blog/bittorrent-handshake-evidence-peer-id/



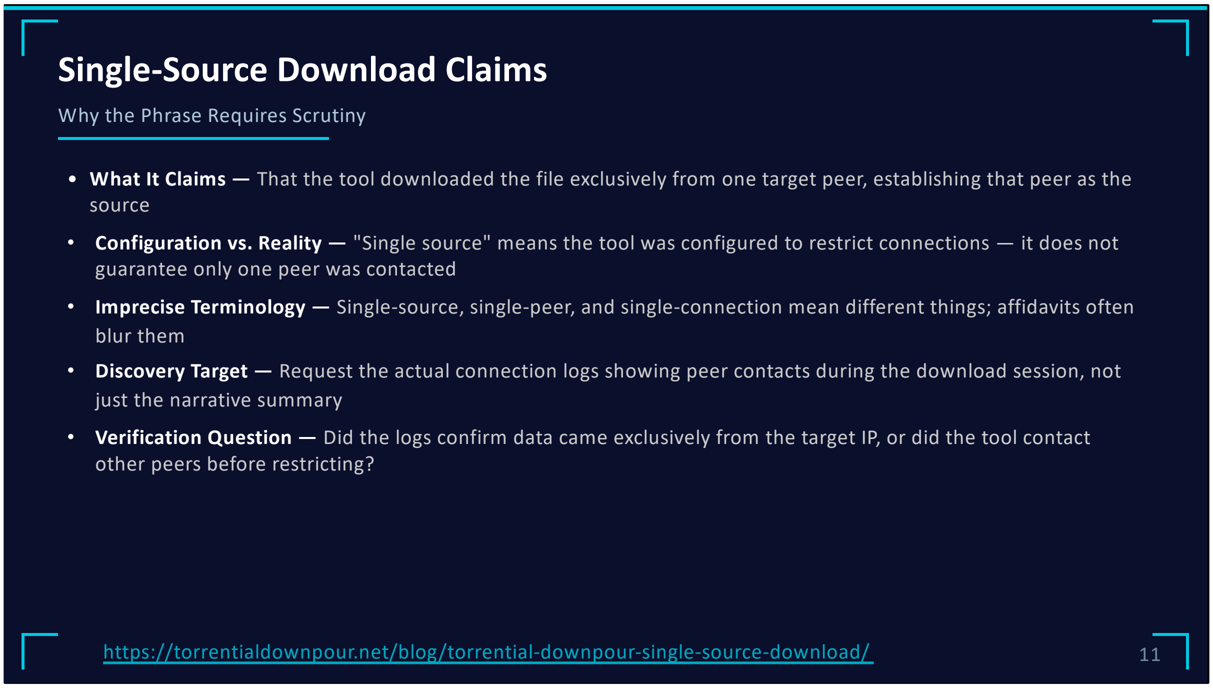
Bitfield Messages and Possession

Client State vs. Disk Reality

- **What a Bitfield Is —** A message from the peer indicating which pieces of the torrent it claims to have available
- **Self-Report Only —** The bitfield is a client assertion — it reflects internal state, not verified disk contents
- **Client State ≠ Disk Reality —** Resume data can persist even after files are deleted, moved, or never fully written
- **No Hash Verification —** The bitfield does not prove piece integrity — only that the client believes it has certain pieces
- **Defense Angle —** Establish the gap between what the client reported and what was actually found on disk during forensic examination

https://torrentialdownpour.net/blog/bittorrent-bitfield-proves-possession/ 10

The bitfield is often cited as evidence of file possession, but it is fundamentally a self-report from the BitTorrent client software — not a verified inventory of what actually exists on disk. Key limitation: client resume data can persist even after the underlying files have been deleted or were never fully written to disk. A bitfield showing '100% complete' means only that the client's internal state data indicates all pieces were received; it does not confirm the file is present on the storage device. If the forensic examination found the file on disk, the bitfield is redundant evidence. If the file was NOT found on disk, the bitfield alone does not establish possession. Blog: https://torrentialdownpour.net/blog/bittorrent-bitfield-proves-possession/



Single-Source Download Claims

Why the Phrase Requires Scrutiny

- **What It Claims** — That the tool downloaded the file exclusively from one target peer, establishing that peer as the source
- **Configuration vs. Reality** — "Single source" means the tool was configured to restrict connections — it does not guarantee only one peer was contacted
- **Imprecise Terminology** — Single-source, single-peer, and single-connection mean different things; affidavits often blur them
- **Discovery Target** — Request the actual connection logs showing peer contacts during the download session, not just the narrative summary
- **Verification Question** — Did the logs confirm data came exclusively from the target IP, or did the tool contact other peers before restricting?

https://torrentialdownpour.net/blog/torrential-downpour-single-source-download/

11

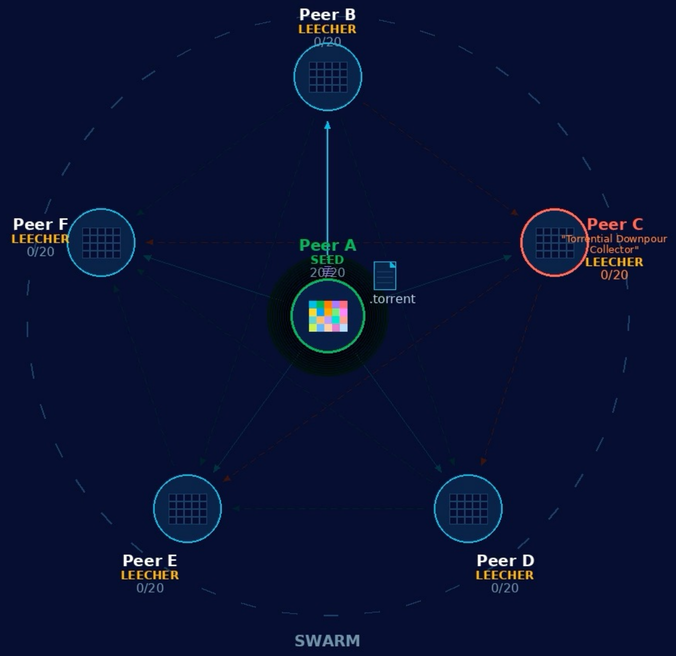
Affidavits routinely describe a 'single-source download' from the suspect's IP address, but this phrase is often imprecise. It typically means the tool was configured to restrict download sources to one target, but the actual connection logs may show that other peers were contacted before the restriction took effect. The critical defense question: was the data actually received exclusively from the target, or could pieces have come from other peers? The connection logs (netstat.txt, details.txt) should be requested and examined to verify exclusivity. If the tool contacted multiple peers before restricting to the target, the single-source characterization is weakened. Blog: https://torrentialdownpour.net/blog/torrential-downpour-single-source-download/

Initial Seeding

How Single Source Download Works

Leeching and the Choking Algorithm

Seeds: 1 | **Leechers: 5**



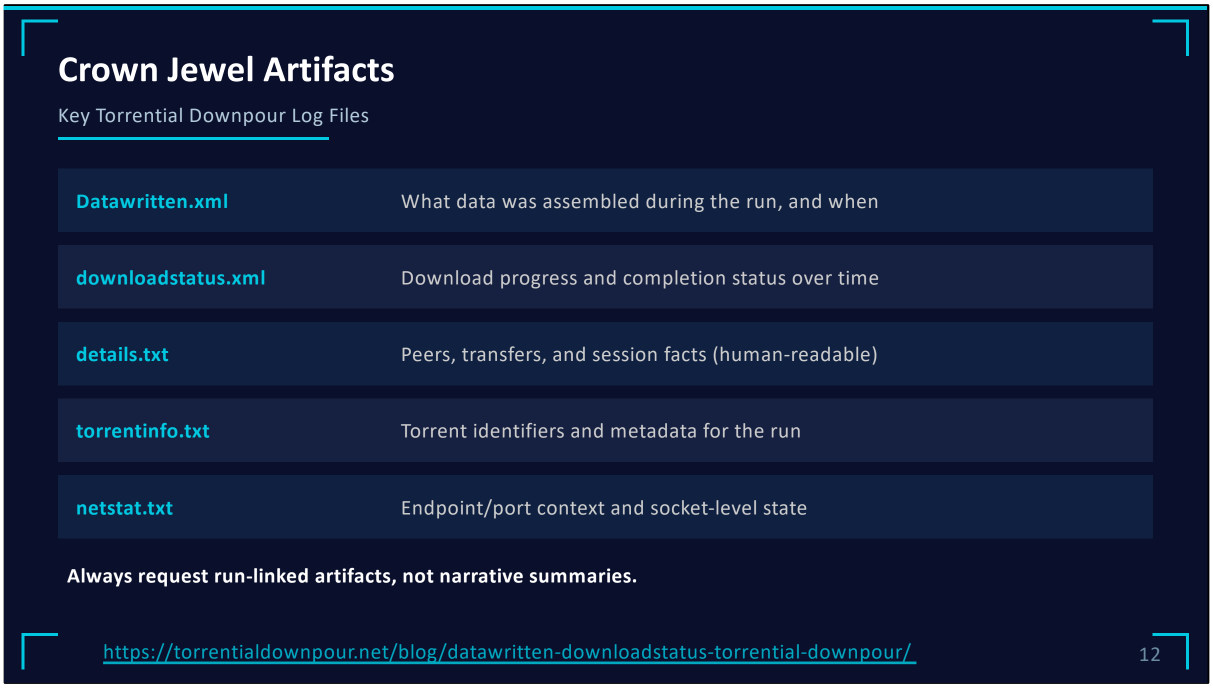
LEGEND

- → Seed distribution
- ⇢ Cooperative peer exchange
- ✕ Choked (not sharing back)
- - - - Optimistic unchoke (rare)

Only 8 of 20 pieces in swarm
(seed left before full distribution)

INITIAL SEEDING

The seed distributes pieces to peers in the swarm. But this seed will leave after sharing only 8 of 20 pieces...



Crown Jewel Artifacts

Key Torrential Downpour Log Files

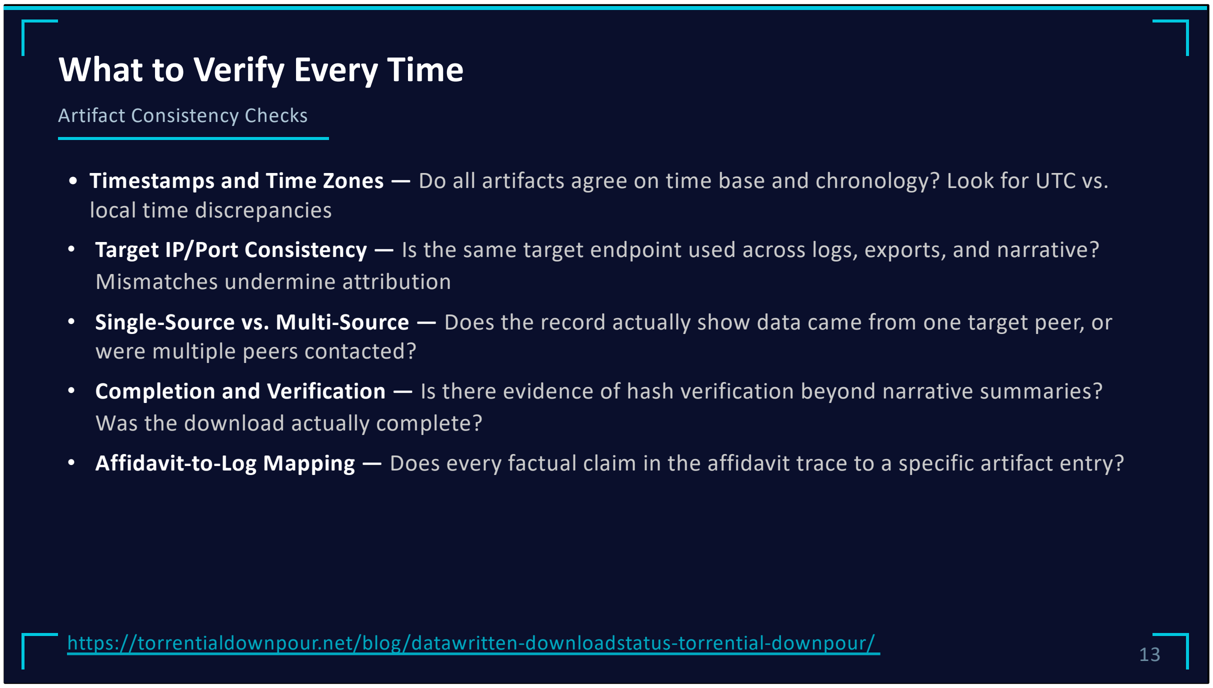
Datawritten.xml	What data was assembled during the run, and when
downloadstatus.xml	Download progress and completion status over time
details.txt	Peers, transfers, and session facts (human-readable)
torrentinfo.txt	Torrent identifiers and metadata for the run
netstat.txt	Endpoint/port context and socket-level state

Always request run-linked artifacts, not narrative summaries.

https://torrentialdownpour.net/blog/datawritten-downloadstatus-torrential-downpour/

12

Key Torrential Downpour artifacts that defense counsel should request in every case: Datawritten.xml and downloadstatus.xml are the most important — they document what was actually written to disk and the download progression over time. Details.txt provides peer and transfer specifics. Torrentinfo.txt confirms which torrent was targeted. Netstat.txt shows network connection state during the operation. Always request the structured log files themselves, not just the detective's narrative summary or report. The narrative is an interpretation; the artifacts are the underlying data that allows independent evaluation of every claim in the affidavit. Blog: https://torrentialdownpour.net/blog/datawritten-downloadstatus-torrential-downpour/



What to Verify Every Time

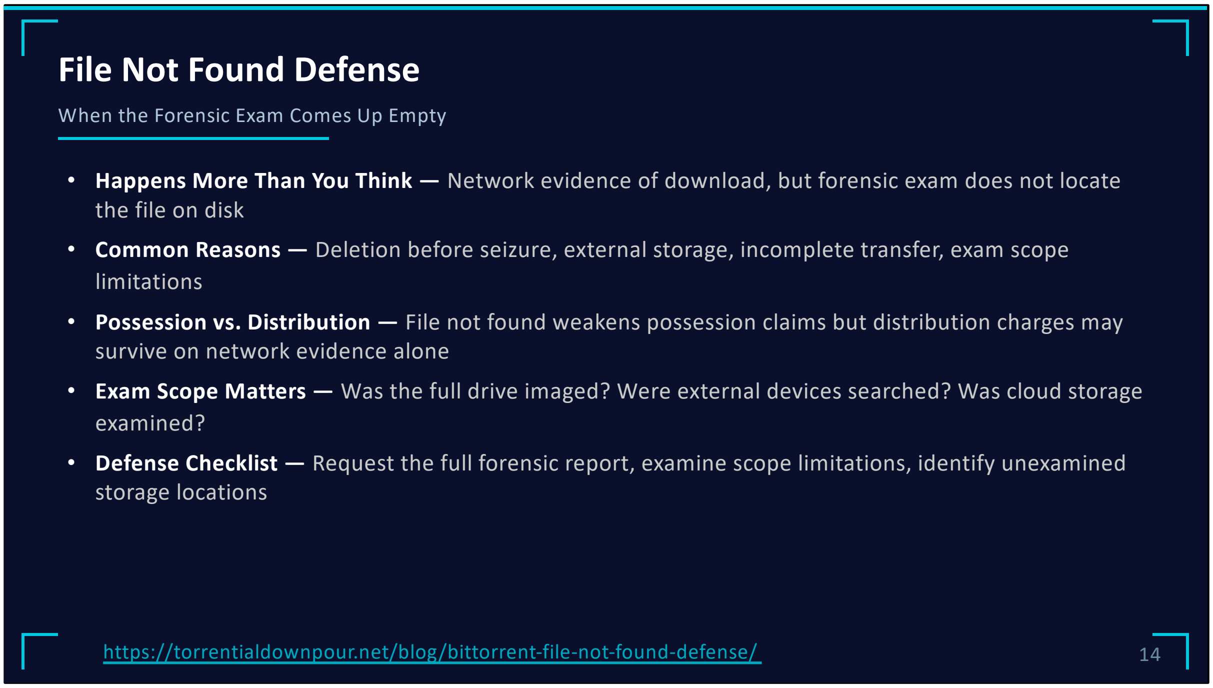
Artifact Consistency Checks

- **Timestamps and Time Zones —** Do all artifacts agree on time base and chronology? Look for UTC vs. local time discrepancies
- **Target IP/Port Consistency —** Is the same target endpoint used across logs, exports, and narrative? Mismatches undermine attribution
- **Single-Source vs. Multi-Source —** Does the record actually show data came from one target peer, or were multiple peers contacted?
- **Completion and Verification —** Is there evidence of hash verification beyond narrative summaries? Was the download actually complete?
- **Affidavit-to-Log Mapping —** Does every factual claim in the affidavit trace to a specific artifact entry?

https://torrentialdownpour.net/blog/datawritten-downloadstatus-torrential-downpour/

13

Artifact verification checklist for defense experts: Timestamps — if the tool uses UTC but the affidavit reports local time without noting the conversion, that is a potential overstatement. IP/port — the target IP in the handshake log must match the IP in the download log, the ISP subpoena, and the affidavit; any discrepancy is a problem. Single-source — verify from actual connection logs, not the narrative summary. Completion — confirm whether hash verification was performed, or whether the affidavit simply states the file was 'downloaded.' The methodology: map every claim in the affidavit to a specific log entry. Any claim that cannot be traced to an artifact is unsupported. Blog: https://torrentialdownpour.net/blog/datawritten-downloadstatus-torrential-downpour/



File Not Found Defense

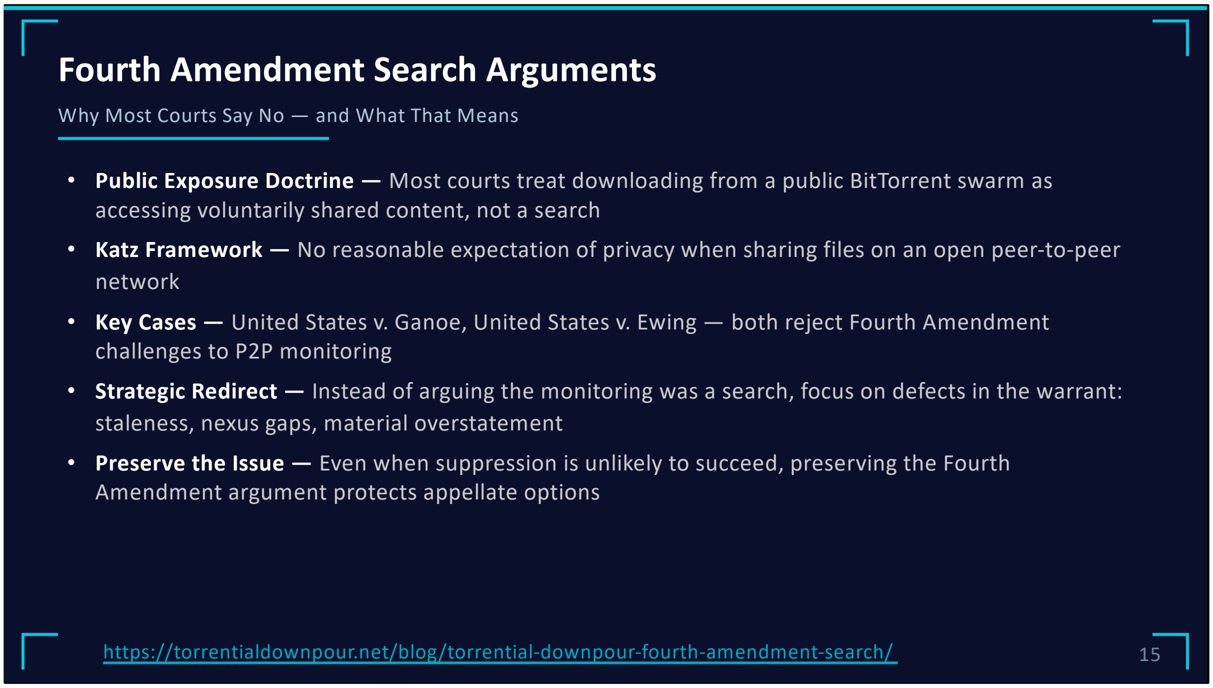
When the Forensic Exam Comes Up Empty

- **Happens More Than You Think** — Network evidence of download, but forensic exam does not locate the file on disk
- **Common Reasons** — Deletion before seizure, external storage, incomplete transfer, exam scope limitations
- **Possession vs. Distribution** — File not found weakens possession claims but distribution charges may survive on network evidence alone
- **Exam Scope Matters** — Was the full drive imaged? Were external devices searched? Was cloud storage examined?
- **Defense Checklist** — Request the full forensic report, examine scope limitations, identify unexamined storage locations

https://torrentialdownpour.net/blog/bittorrent-file-not-found-defense/

14

When Torrential Downpour logs show a download from the suspect's IP but the forensic examination does not find the file on the seized device, different defense opportunities arise depending on the charges. For possession charges, file not found is a strong defense position. For distribution charges, the network evidence (controlled download from the IP) may be sufficient even without finding the file on disk. Key questions to investigate: What was the scope of the forensic examination? Was the full drive imaged? Were all connected devices examined? Were external drives, USB devices, and cloud storage considered? Was the time gap between the logged activity and device seizure significant enough for deletion to have occurred? Blog: https://torrentialdownpour.net/blog/bittorrent-file-not-found-defense/



Fourth Amendment Search Arguments

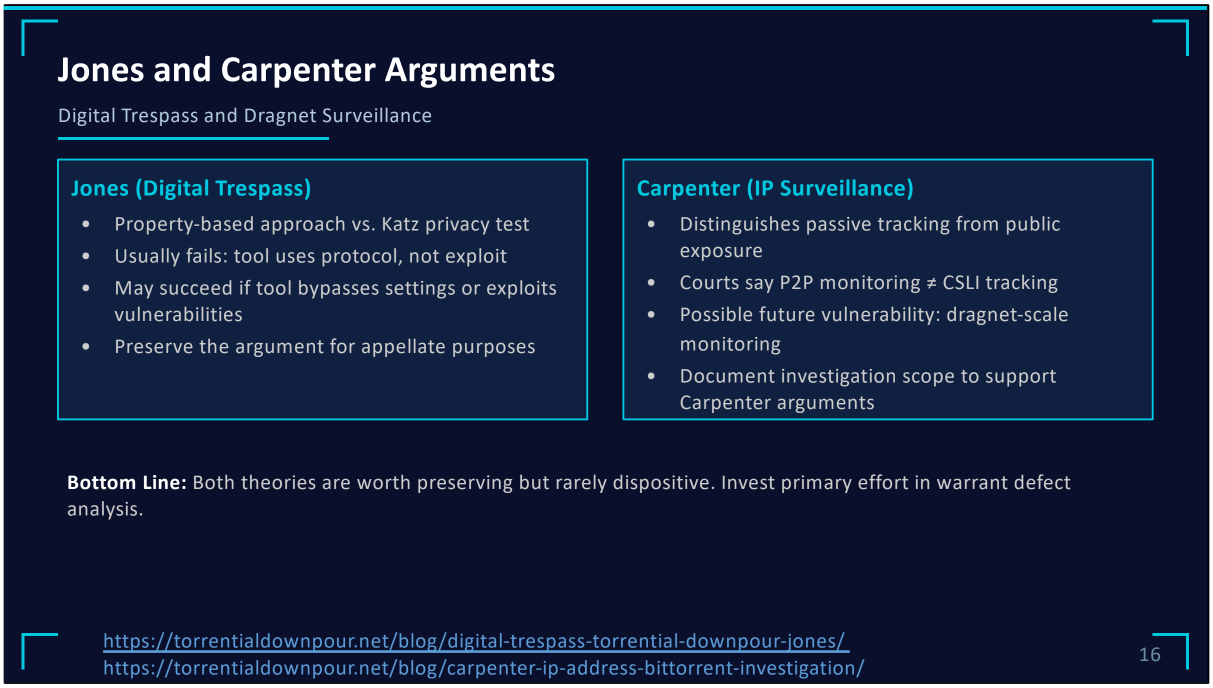
Why Most Courts Say No — and What That Means

- **Public Exposure Doctrine —** Most courts treat downloading from a public BitTorrent swarm as accessing voluntarily shared content, not a search
- **Katz Framework —** No reasonable expectation of privacy when sharing files on an open peer-to-peer network
- **Key Cases —** United States v. Ganoe, United States v. Ewing — both reject Fourth Amendment challenges to P2P monitoring
- **Strategic Redirect —** Instead of arguing the monitoring was a search, focus on defects in the warrant: staleness, nexus gaps, material overstatement
- **Preserve the Issue —** Even when suppression is unlikely to succeed, preserving the Fourth Amendment argument protects appellate options

https://torrentialdownpour.net/blog/torrential-downpour-fourth-amendment-search/

15

Most federal and state courts hold that sharing files on BitTorrent eliminates any reasonable expectation of privacy because the protocol is designed for public distribution — the tool joins the swarm as any peer would. Broad Fourth Amendment suppression motions based on this theory face unfavorable case law. More effective strategies focus on challenging the warrant itself: staleness (how old is the network evidence relative to the warrant application?), nexus (how many inferential leaps exist from IP address to a specific device in the home?), and material overstatements in the affidavit. These defect-focused arguments have a better track record than broad suppression theories. The Fourth Amendment issue should always be preserved for appeal regardless of the trial court outcome. Blog: https://torrentialdownpour.net/blog/torrential-downpour-fourth-amendment-search/



Jones and Carpenter Arguments

Digital Trespass and Dragnet Surveillance

Jones (Digital Trespass)

- Property-based approach vs. Katz privacy test
- Usually fails: tool uses protocol, not exploit
- May succeed if tool bypasses settings or exploits vulnerabilities
- Preserve the argument for appellate purposes

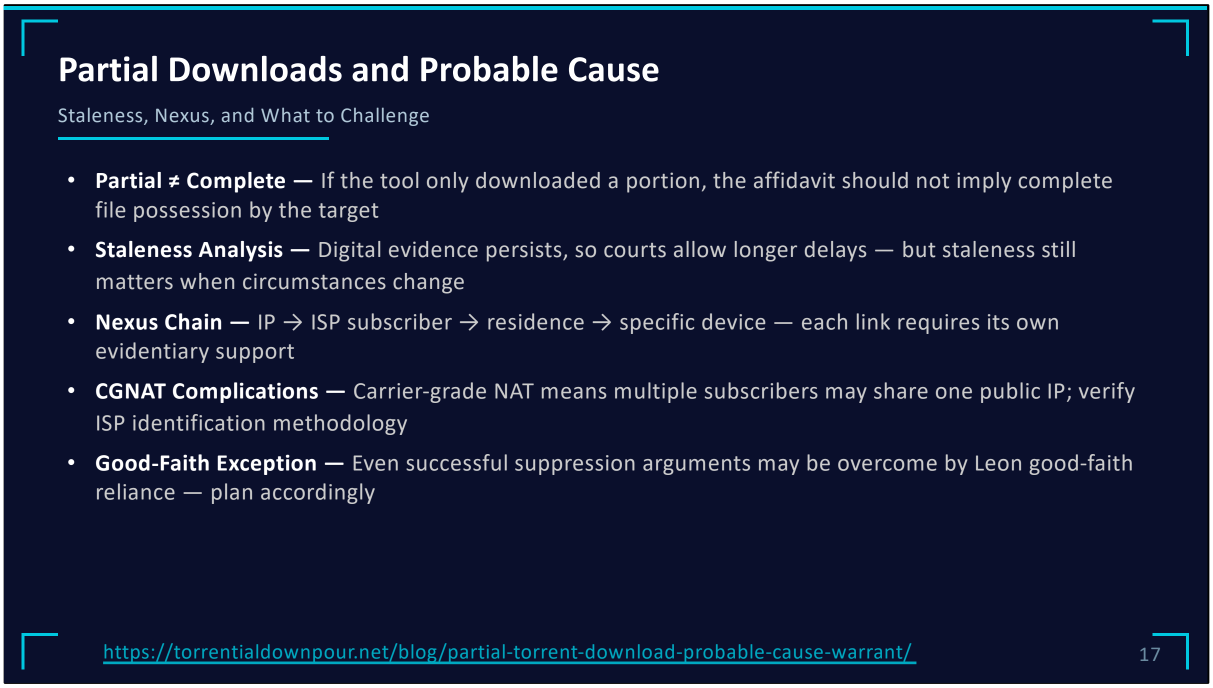
Carpenter (IP Surveillance)

- Distinguishes passive tracking from public exposure
- Courts say P2P monitoring ≠ CSLI tracking
- Possible future vulnerability: dragnet-scale monitoring
- Document investigation scope to support Carpenter arguments

Bottom Line: Both theories are worth preserving but rarely dispositive. Invest primary effort in warrant defect analysis.

https://torrentialdownpour.net/blog/digital-trespass-torrential-downpour-jones/
https://torrentialdownpour.net/blog/carpenter-ip-address-bittorrent-investigation/

Two emerging constitutional theories: The Jones-based digital trespass argument contends that the tool's connection to the peer constitutes a property intrusion. This typically fails because Torrential Downpour uses the standard BitTorrent protocol without exploiting vulnerabilities or bypassing security. However, if evidence shows the tool went beyond normal protocol behavior, the argument gains traction. The Carpenter argument draws an analogy between long-term automated IP surveillance and the cell-site location data at issue in Carpenter v. United States. Courts have generally rejected this because P2P file sharing is viewed as voluntary exposure, unlike passive cell tower tracking. However, evidence of dragnet-scale monitoring of many IP addresses over extended periods makes Carpenter arguments more compelling. Blog: https://torrentialdownpour.net/blog/digital-trespass-torrential-downpour-jones/ and https://torrentialdownpour.net/blog/carpenter-ip-address-bittorrent-investigation/



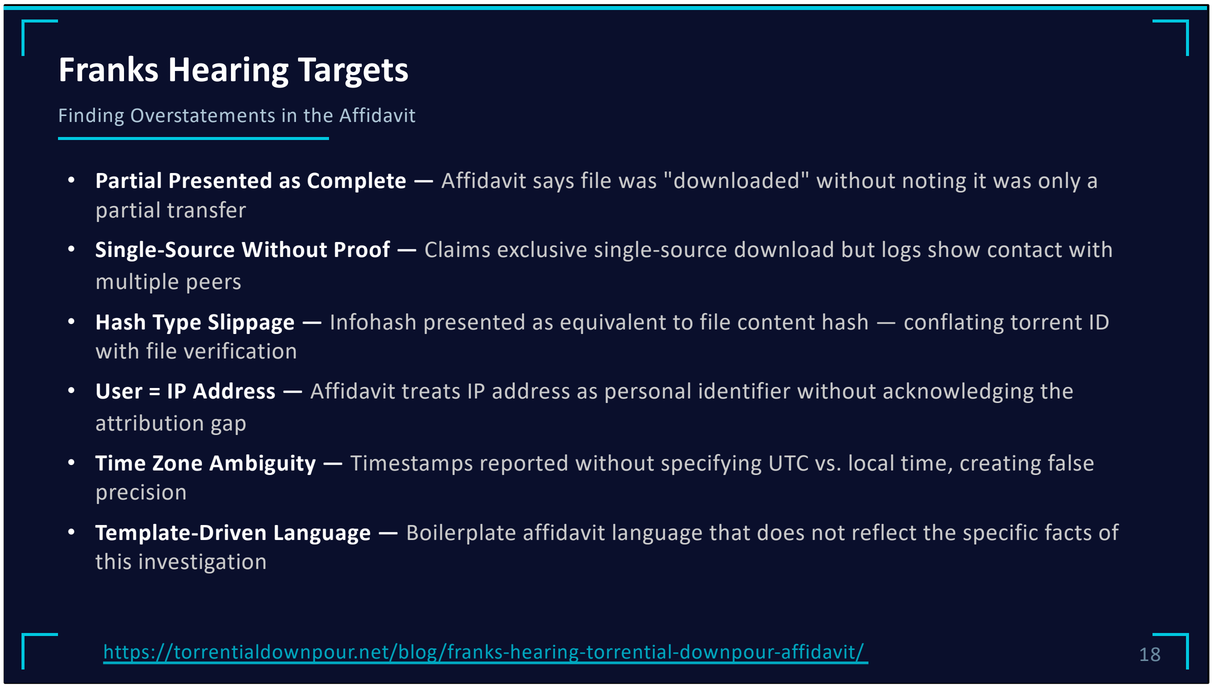
Partial Downloads and Probable Cause

Staleness, Nexus, and What to Challenge

- **Partial ≠ Complete —** If the tool only downloaded a portion, the affidavit should not imply complete file possession by the target
- **Staleness Analysis —** Digital evidence persists, so courts allow longer delays — but staleness still matters when circumstances change
- **Nexus Chain —** IP → ISP subscriber → residence → specific device — each link requires its own evidentiary support
- **CGNAT Complications —** Carrier-grade NAT means multiple subscribers may share one public IP; verify ISP identification methodology
- **Good-Faith Exception —** Even successful suppression arguments may be overcome by Leon good-faith reliance — plan accordingly

https://torrentialdownpour.net/blog/partial-torrent-download-probable-cause-warrant/

Partial downloads create specific defense opportunities. If the tool only received some pieces of the file, the affidavit should accurately reflect that — presenting a partial download as a complete download is a potential Franks challenge target. Regarding staleness, courts generally allow longer delays for digital evidence because files tend to persist on storage devices, but staleness still matters when circumstances have changed (new residents, new ISP, device changes). The nexus chain from IP address to subscriber to residence to specific device requires evidentiary support at each step. CGNAT (carrier-grade NAT) is an emerging issue — if the ISP uses it, multiple subscribers may share one public IP address, weakening identification. Important tactical consideration: even if suppression succeeds under Franks, the Leon good-faith exception may preserve the warrant. Blog: https://torrentialdownpour.net/blog/partial-torrent-download-probable-cause-warrant/



Franks Hearing Targets

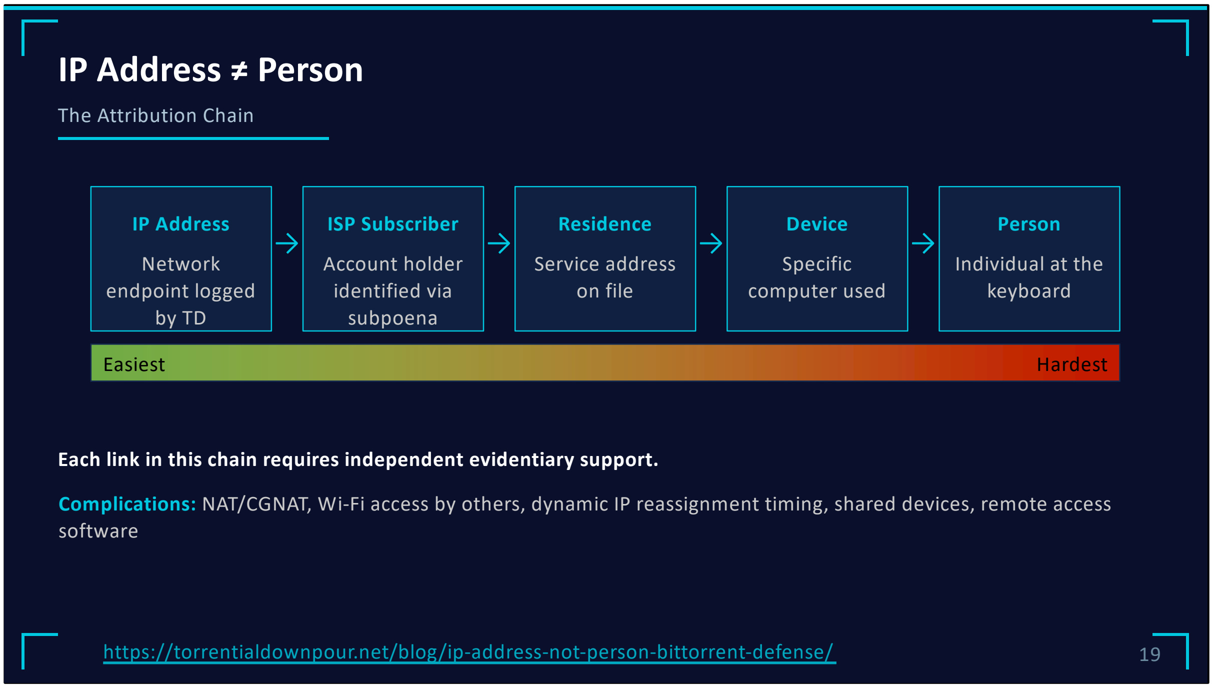
Finding Overstatements in the Affidavit

- **Partial Presented as Complete —** Affidavit says file was "downloaded" without noting it was only a partial transfer
- **Single-Source Without Proof —** Claims exclusive single-source download but logs show contact with multiple peers
- **Hash Type Slippage —** Infohash presented as equivalent to file content hash — conflating torrent ID with file verification
- **User = IP Address —** Affidavit treats IP address as personal identifier without acknowledging the attribution gap
- **Time Zone Ambiguity —** Timestamps reported without specifying UTC vs. local time, creating false precision
- **Template-Driven Language —** Boilerplate affidavit language that does not reflect the specific facts of this investigation

https://torrentialdownpour.net/blog/franks-hearing-torrential-downpour-affidavit/

18

Common affidavit overstatements that constitute concrete Franks v. Delaware targets: treating a partial download as complete, claiming single-source exclusivity without verification from connection logs, blurring infohash and file hash identification, treating an IP address as personal identification, and failing to specify time zones for timestamps. The methodology: map every factual claim in the affidavit to the underlying Torrential Downpour artifacts. Where a claim is not supported by the artifacts, or where the artifacts contradict the affidavit, a potential Franks issue exists. Template-driven affidavits are especially vulnerable because detectives may use standardized language that does not accurately describe the particular investigation. Blog: https://torrentialdownpour.net/blog/franks-hearing-torrential-downpour-affidavit/



IP Address ≠ Person

The Attribution Chain

IP Address — Network endpoint logged by TD → **ISP Subscriber** — Account holder identified via subpoena → **Residence** — Service address on file → **Device** — Specific computer used → **Person** — Individual at the keyboard

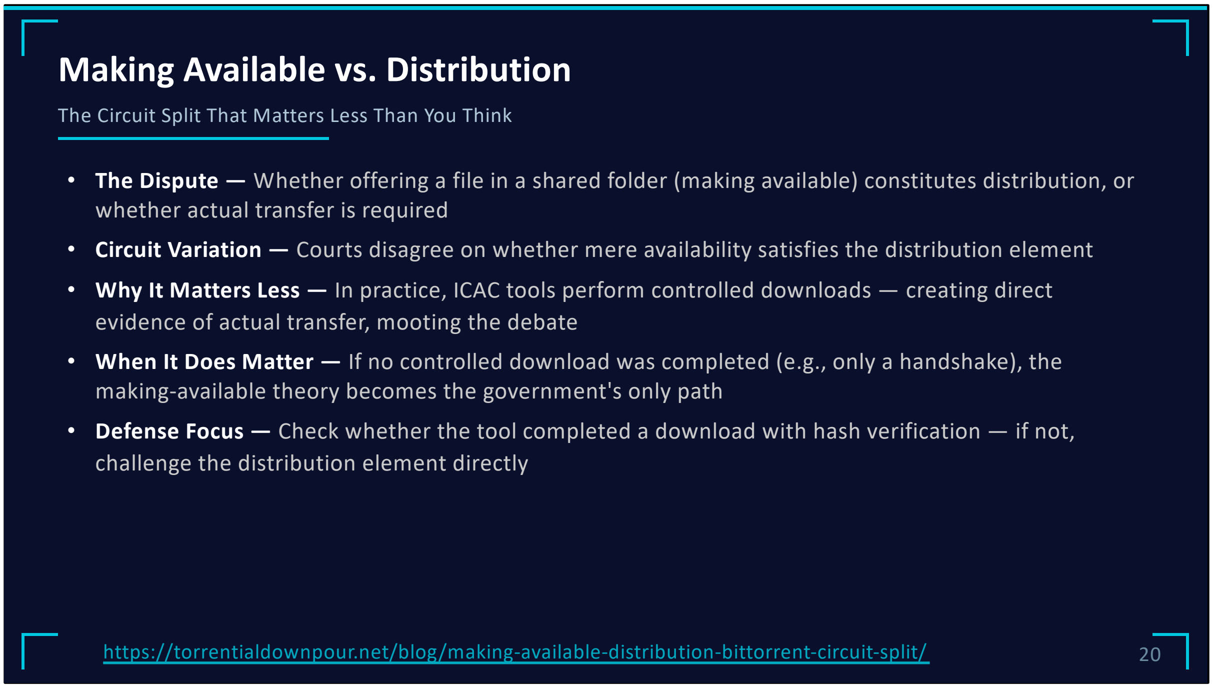
Easiest — Hardest

Each link in this chain requires independent evidentiary support.

Complications: NAT/CGNAT, Wi-Fi access by others, dynamic IP reassignment timing, shared devices, remote access software

https://torrentialdownpour.net/blog/ip-address-not-person-bittorrent-defense/

The fundamental attribution problem in every BitTorrent case: Torrential Downpour identifies an IP address; the ISP subpoena identifies the subscriber; but the subscriber is not necessarily the person who used the computer. The attribution chain has five links, each requiring independent evidentiary support. Complications at each stage: NAT means multiple internal devices share one public IP. CGNAT means multiple subscribers may share one public IP. Wi-Fi access means neighbors, guests, or unauthorized users could be responsible. Dynamic IP assignment means the timing of the ISP lookup must precisely match the logged activity. Shared household devices mean the subscriber is not the only potential user. Each link is an investigation target for defense counsel and forensic experts. Blog: https://torrentialdownpour.net/blog/ip-address-not-person-bittorrent-defense/



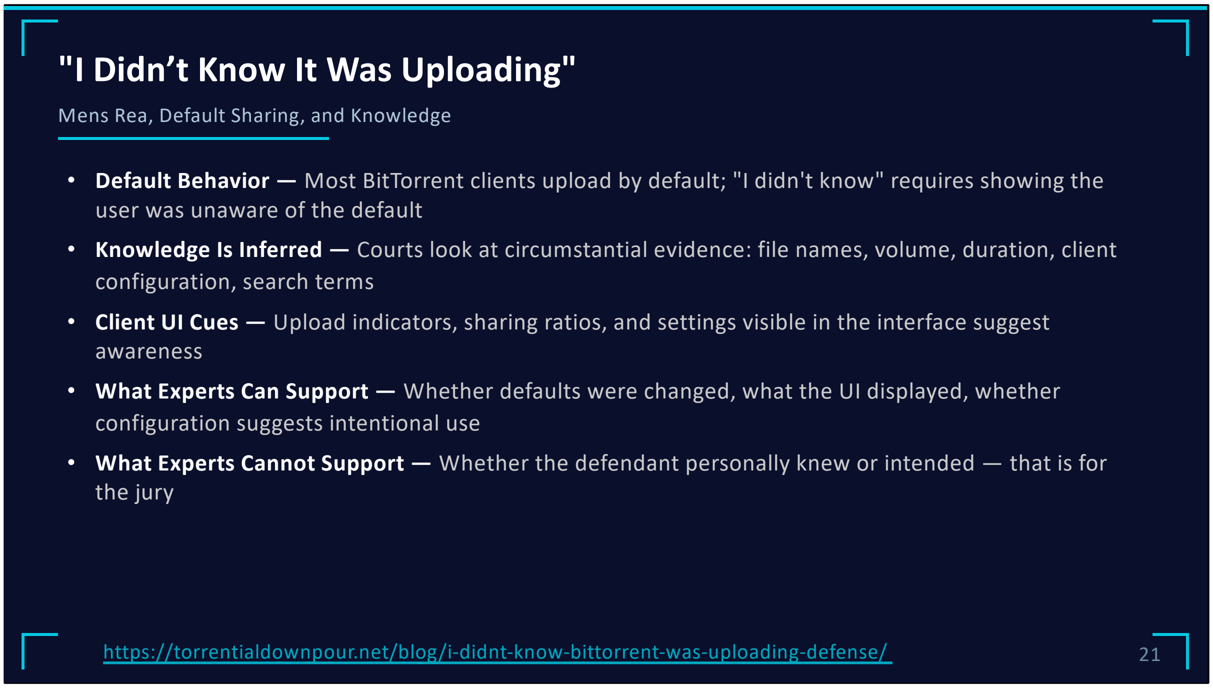
Making Available vs. Distribution

The Circuit Split That Matters Less Than You Think

- **The Dispute —** Whether offering a file in a shared folder (making available) constitutes distribution, or whether actual transfer is required
- **Circuit Variation —** Courts disagree on whether mere availability satisfies the distribution element
- **Why It Matters Less —** In practice, ICAC tools perform controlled downloads — creating direct evidence of actual transfer, mooting the debate
- **When It Does Matter —** If no controlled download was completed (e.g., only a handshake), the making-available theory becomes the government's only path
- **Defense Focus —** Check whether the tool completed a download with hash verification — if not, challenge the distribution element directly

https://torrentialdownpour.net/blog/making-available-distribution-bittorrent-circuit-split/

The making-available theory receives significant attention in legal scholarship, but in practice its impact varies by case. Because ICAC tools perform controlled downloads (connecting to the target and downloading the file), there is usually direct evidence of actual transfer, making the making-available debate secondary. The circuit split becomes critical when the tool did NOT complete a download — for example, if only a handshake and bitfield exchange occurred. In that scenario, the government must rely on the making-available theory, and the defense has a stronger position in circuits that require proof of actual transfer. The threshold question: did the tool complete a download with hash verification? If yes, the making-available debate is largely academic. If no, it becomes central to the case. Blog: https://torrentialdownpour.net/blog/making-available-distribution-bittorrent-circuit-split/



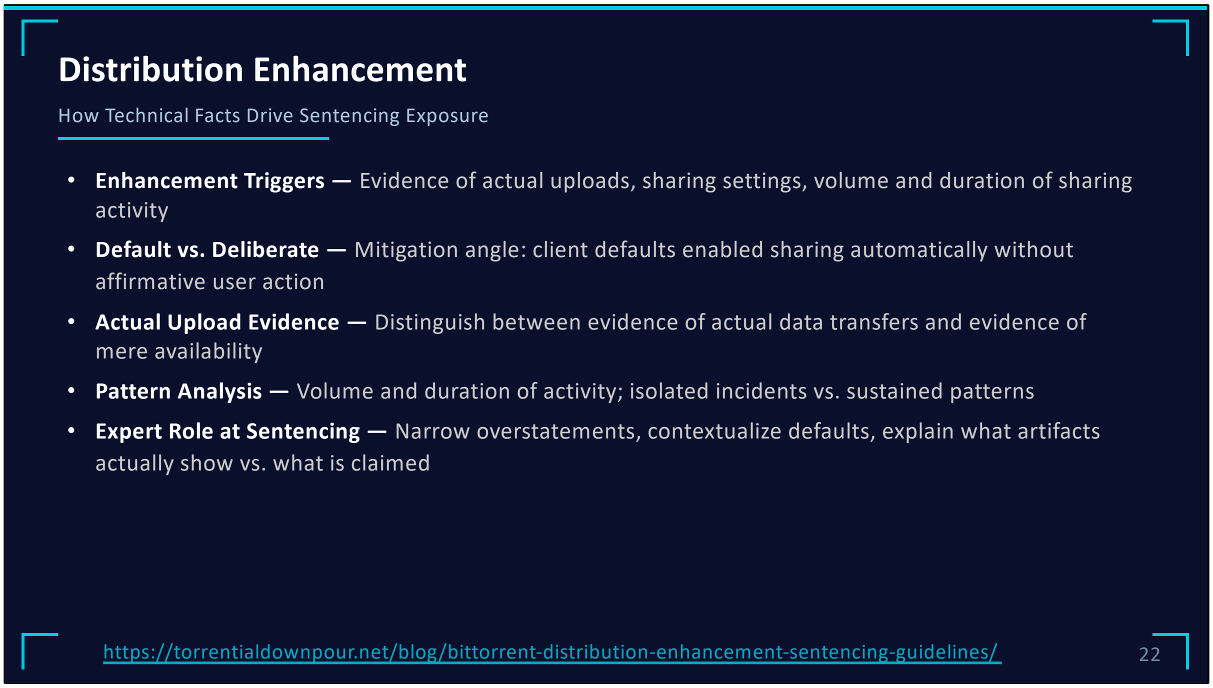
"I Didn’t Know It Was Uploading"

Mens Rea, Default Sharing, and Knowledge

- **Default Behavior** — Most BitTorrent clients upload by default; "I didn't know" requires showing the user was unaware of the default
- **Knowledge Is Inferred** — Courts look at circumstantial evidence: file names, volume, duration, client configuration, search terms
- **Client UI Cues** — Upload indicators, sharing ratios, and settings visible in the interface suggest awareness
- **What Experts Can Support** — Whether defaults were changed, what the UI displayed, whether configuration suggests intentional use
- **What Experts Cannot Support** — Whether the defendant personally knew or intended — that is for the jury

https://torrentialdownpour.net/blog/i-didnt-know-bittorrent-was-uploading-defense/

The 'I didn't know it was uploading' defense is common but difficult to sustain. Most BitTorrent clients upload by default, and courts infer knowledge from circumstantial evidence: the volume and duration of sharing activity, the specificity of file names (suggesting deliberate searching), any configuration changes to the client, and what the client interface displayed during use. A defense expert can testify about default settings, what the client interface would have shown the user, and whether the configuration suggests intentional versus casual use — but cannot credibly testify about the defendant's personal knowledge or intent, which is a jury question. Practical assessment: if the evidence shows minimal activity with default settings and generic file names, the unknowing defense is more viable. Extensive activity with specific names and modified settings points toward other defense strategies. Blog: https://torrentialdownpour.net/blog/i-didnt-know-bittorrent-was-uploading-defense/



Distribution Enhancement

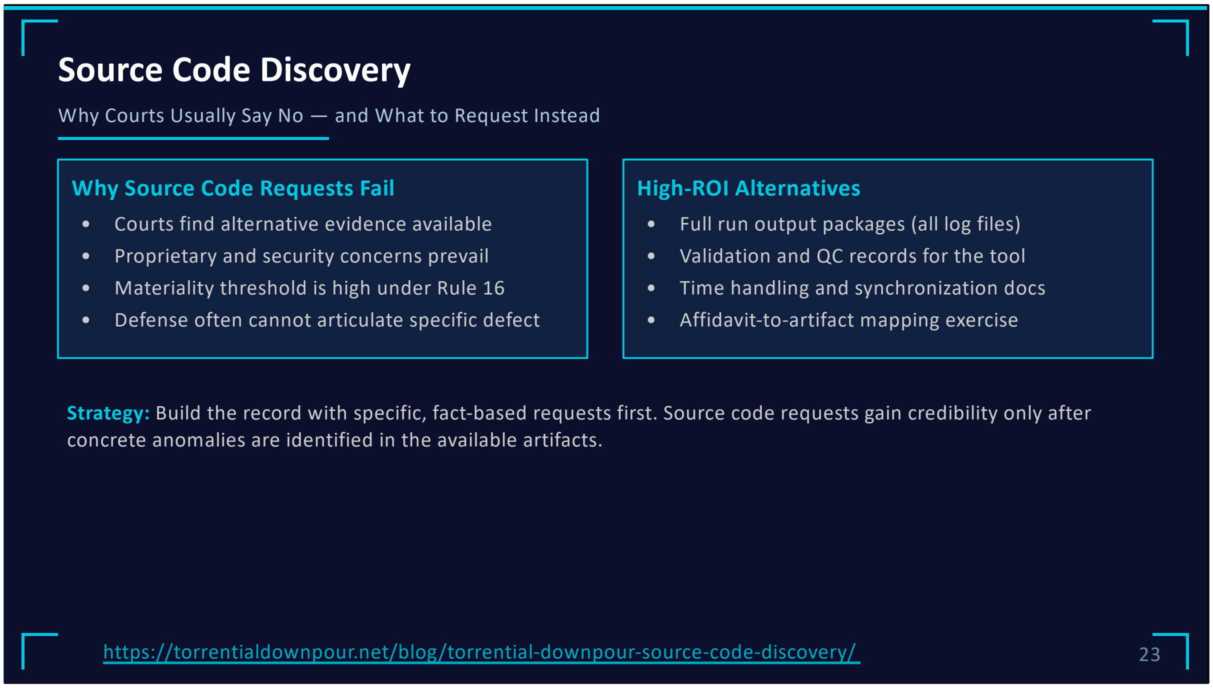
How Technical Facts Drive Sentencing Exposure

- **Enhancement Triggers —** Evidence of actual uploads, sharing settings, volume and duration of sharing activity
- **Default vs. Deliberate —** Mitigation angle: client defaults enabled sharing automatically without affirmative user action
- **Actual Upload Evidence —** Distinguish between evidence of actual data transfers and evidence of mere availability
- **Pattern Analysis —** Volume and duration of activity; isolated incidents vs. sustained patterns
- **Expert Role at Sentencing —** Narrow overstatements, contextualize defaults, explain what artifacts actually show vs. what is claimed

https://torrentialdownpour.net/blog/bittorrent-distribution-enhancement-sentencing-guidelines/

22

Even after conviction or plea, the technical facts remain relevant at sentencing. The distribution enhancement significantly increases exposure and turns on factual questions that defense counsel can challenge. Key mitigation consideration: if sharing was enabled by default client settings rather than affirmative user configuration, that context is relevant to the sentencing determination. It is important to distinguish between evidence of actual upload transfers and mere file availability in a shared folder. Pattern analysis also matters: an isolated incident with default settings presents differently than sustained high-volume sharing over months. A defense expert can help narrow overstatements at sentencing by explaining what the artifacts actually demonstrate versus how the government characterizes them. Blog: https://torrentialdownpour.net/blog/bittorrent-distribution-enhancement-sentencing-guidelines/



Source Code Discovery

Why Courts Usually Say No — and What to Request Instead

Why Source Code Requests Fail

- Courts find alternative evidence available
- Proprietary and security concerns prevail
- Materiality threshold is high under Rule 16
- Defense often cannot articulate specific defect

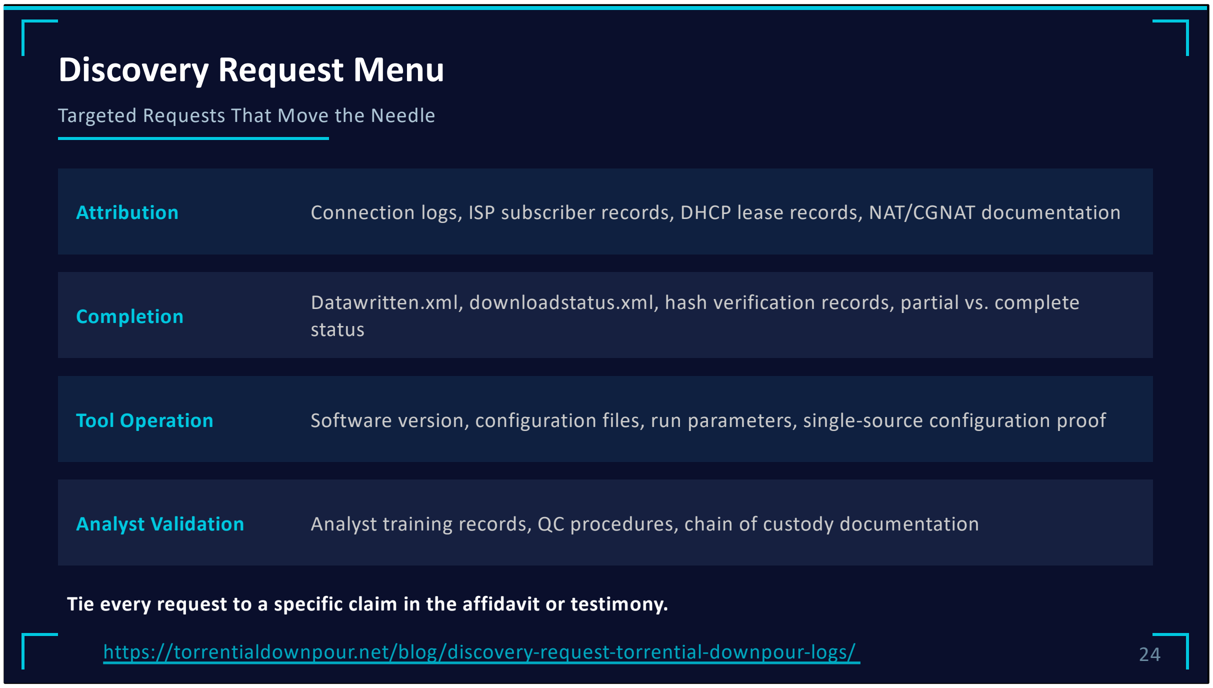
High-ROI Alternatives

- Full run output packages (all log files)
- Validation and QC records for the tool
- Time handling and synchronization docs
- Affidavit-to-artifact mapping exercise

Strategy: Build the record with specific, fact-based requests first. Source code requests gain credibility only after concrete anomalies are identified in the available artifacts.

https://torrentialdownpour.net/blog/torrential-downpour-source-code-discovery/

Source code discovery for Torrential Downpour is an appealing theory but rarely succeeds in practice. Courts typically deny these requests because: (1) alternative evidence exists in the form of the tool's output artifacts; (2) the government raises proprietary and security concerns; and (3) the defense cannot articulate a specific defect that only source code review would reveal. A more effective strategy: request the full run output packages (all log files, not just the narrative), validation and QC records, and time-handling documentation. Use an affidavit-to-artifact mapping exercise to identify concrete discrepancies first. Once specific anomalies are documented, a source code request becomes more credible because it can point to a specific issue requiring code-level investigation.
Blog: https://torrentialdownpour.net/blog/torrential-downpour-source-code-discovery/



Discovery Request Menu

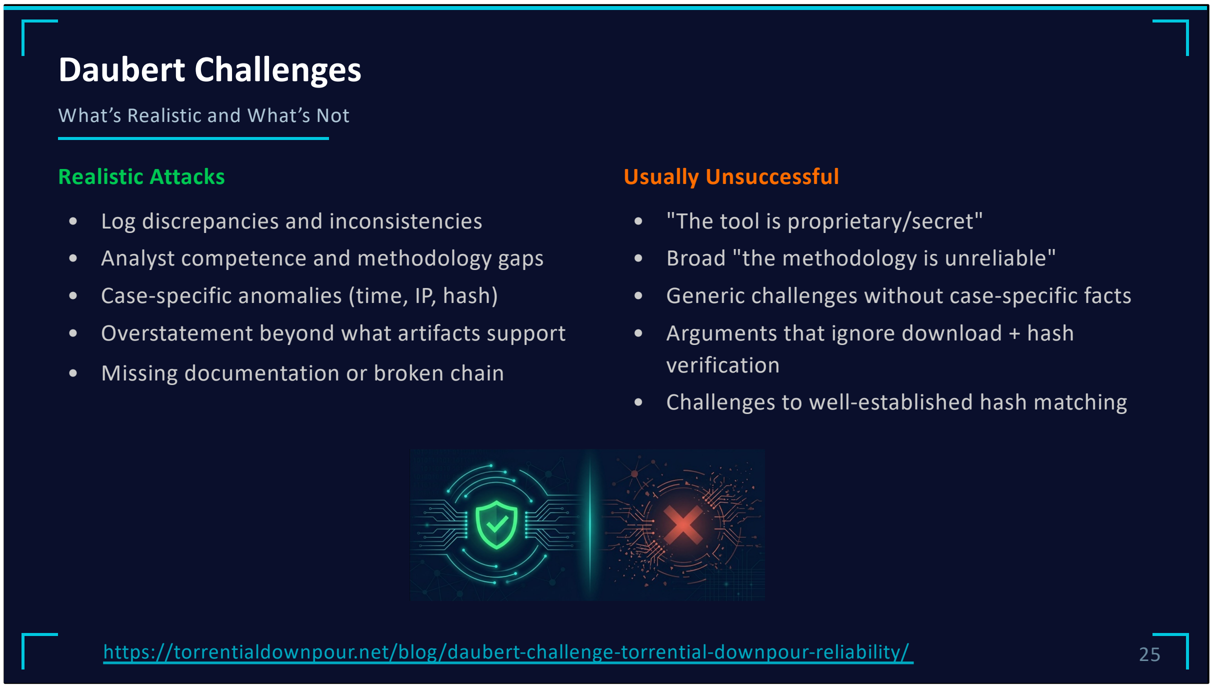
Targeted Requests That Move the Needle

Attribution	Connection logs, ISP subscriber records, DHCP lease records, NAT/CGNAT documentation
Completion	Datawritten.xml, downloadstatus.xml, hash verification records, partial vs. complete status
Tool Operation	Software version, configuration files, run parameters, single-source configuration proof
Analyst Validation	Analyst training records, QC procedures, chain of custody documentation

Tie every request to a specific claim in the affidavit or testimony.

https://torrentialdownpour.net/blog/discovery-request-torrential-downpour-logs/ 24

Practical discovery requests organized by purpose: Attribution — connection logs, ISP subscriber records, DHCP lease records, and any NAT/CGNAT documentation affecting IP-to-subscriber mapping. Completion — Datawritten.xml and downloadstatus.xml files, hash verification records, and documentation of whether the download was partial or complete. Tool operation — specific software version used, configuration files, run parameters, and proof that the single-source configuration was applied. Analyst validation — analyst training records, QC procedures, and chain of custody documentation. Strategic approach: tie every request to a specific claim in the affidavit or anticipated testimony. A focused request stating 'you claimed X in paragraph Y of the affidavit; produce the artifact that supports that claim' is far more effective than a broad discovery demand. Blog: https://torrentialdownpour.net/blog/discovery-request-torrential-downpour-logs/



Daubert Challenges

What’s Realistic and What’s Not

Realistic Attacks

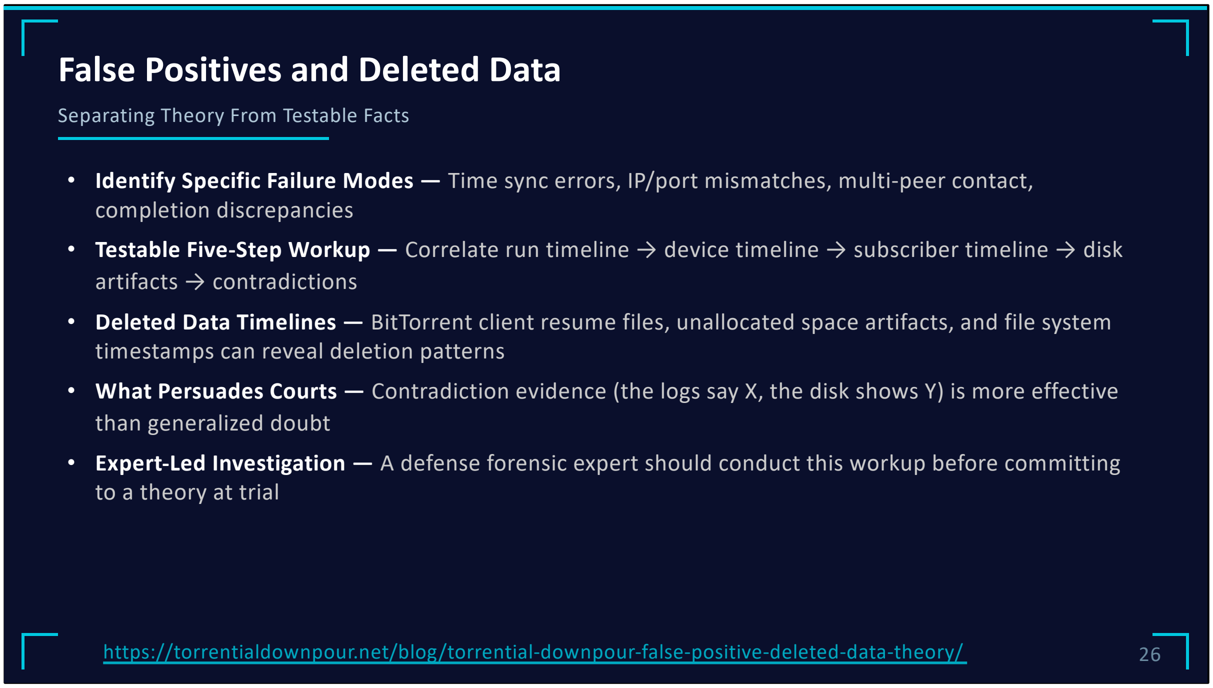
- Log discrepancies and inconsistencies
- Analyst competence and methodology gaps
- Case-specific anomalies (time, IP, hash)
- Overstatement beyond what artifacts support
- Missing documentation or broken chain

Usually Unsuccessful

- "The tool is proprietary/secret"
- Broad "the methodology is unreliable"
- Generic challenges without case-specific facts
- Arguments that ignore download + hash verification
- Challenges to well-established hash matching

https://torrentialdownpour.net/blog/daubert-challenge-torrential-downpour-reliability/

Daubert challenges to Torrential Downpour evidence need to be targeted to succeed. The realistic path is case-specific: identify concrete problems in the investigation's artifacts (log discrepancies, timestamp problems, analyst methodology issues, overstatements beyond what the data supports). Courts treat download plus hash verification as strong functional validation, so broad arguments that 'the tool is secret' or 'the methodology is unreliable' without case-specific evidence generally fail. The most effective Daubert challenges combine: (1) specific artifact anomalies identified through independent analysis; (2) gaps in the analyst's methodology or documentation; and (3) overstatement in testimony beyond what the artifacts support. The standard remains reliable methods applied reliably to the specific case. Blog: https://torrentialdownpour.net/blog/daubert-challenge-torrential-downpour-reliability/



False Positives and Deleted Data

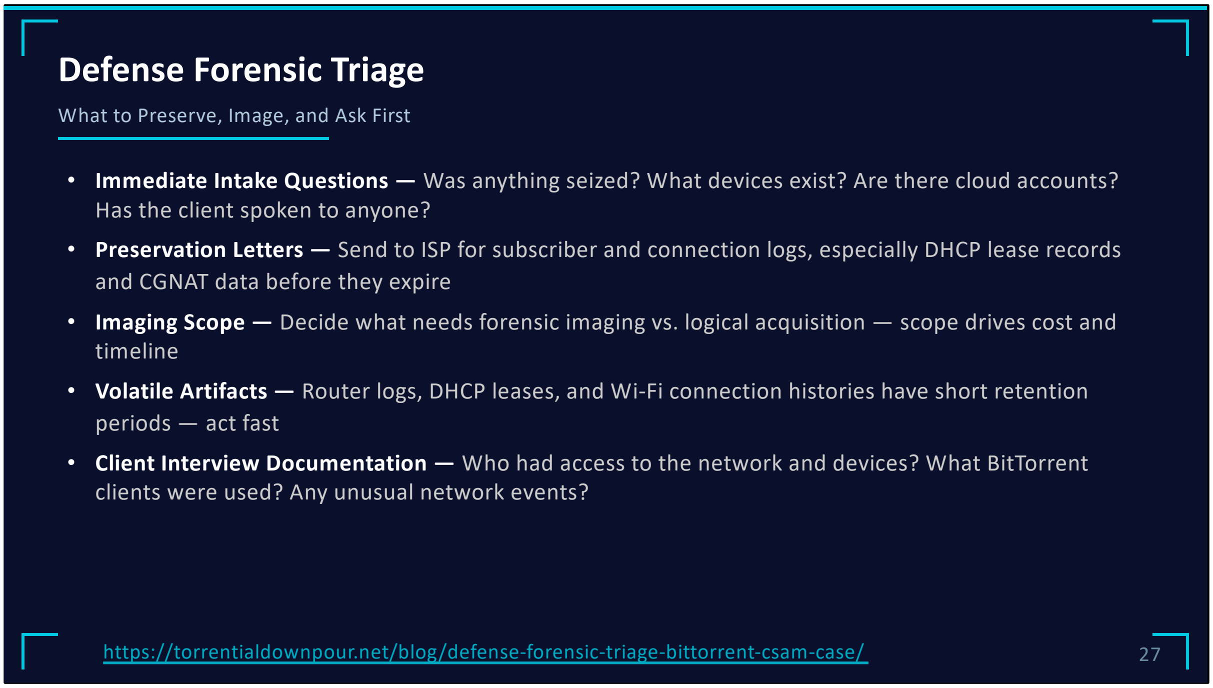
Separating Theory From Testable Facts

- **Identify Specific Failure Modes** — Time sync errors, IP/port mismatches, multi-peer contact, completion discrepancies
- **Testable Five-Step Workup** — Correlate run timeline → device timeline → subscriber timeline → disk artifacts → contradictions
- **Deleted Data Timelines** — BitTorrent client resume files, unallocated space artifacts, and file system timestamps can reveal deletion patterns
- **What Persuades Courts** — Contradiction evidence (the logs say X, the disk shows Y) is more effective than generalized doubt
- **Expert-Led Investigation** — A defense forensic expert should conduct this workup before committing to a theory at trial

https://torrentialdownpour.net/blog/torrential-downpour-false-positive-deleted-data-theory/

26

False positive arguments must be grounded in testable facts, not generalized doubt. The strongest defense position identifies a specific failure mode: time synchronization error between the tool and ISP records, IP/port mismatches between the handshake log and download log, evidence of multi-peer contact undermining single-source claims, or completion discrepancies between what the tool logged and what was found on disk. Five-step verification workup: (1) Map the Torrential Downpour run timeline. (2) Map the device forensic timeline. (3) Map the ISP subscriber timeline. (4) Examine disk artifacts for consistency. (5) Identify contradictions between these timelines. Courts are persuaded by specific contradiction evidence ('the logs indicate X but the disk shows Y') rather than theoretical 'it could have been a false positive' arguments. Blog: https://torrentialdownpour.net/blog/torrential-downpour-false-positive-deleted-data-theory/



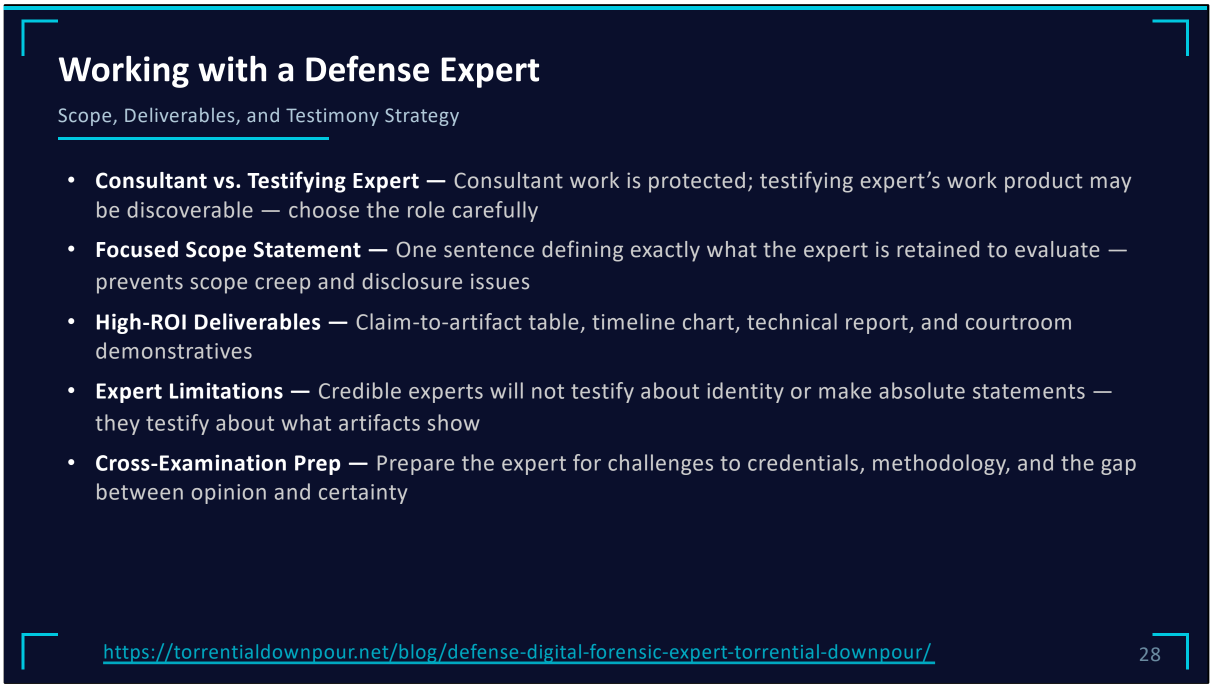
Defense Forensic Triage

What to Preserve, Image, and Ask First

- **Immediate Intake Questions** — Was anything seized? What devices exist? Are there cloud accounts? Has the client spoken to anyone?
- **Preservation Letters** — Send to ISP for subscriber and connection logs, especially DHCP lease records and CGNAT data before they expire
- **Imaging Scope** — Decide what needs forensic imaging vs. logical acquisition — scope drives cost and timeline
- **Volatile Artifacts** — Router logs, DHCP leases, and Wi-Fi connection histories have short retention periods — act fast
- **Client Interview Documentation** — Who had access to the network and devices? What BitTorrent clients were used? Any unusual network events?

https://torrentialdownpour.net/blog/defense-forensic-triage-bittorrent-csam-case/

Practical triage checklist for the first days of a BitTorrent CSAM case: Time-sensitive items — ISP records and DHCP lease data have limited retention periods; send preservation letters immediately. Router logs are volatile and may be lost if the router is rebooted or replaced. Client interview priorities — document who had access to the network and devices, what BitTorrent software was used, whether any devices were disposed of, and whether there were unusual network events (power outages, ISP changes). Imaging scope decisions affect cost and timeline: full forensic imaging of every device may not be necessary, but critical devices must be preserved. Coordinate with a defense forensic expert early to guide preservation, discovery, and strategic decisions. Blog: https://torrentialdownpour.net/blog/defense-forensic-triage-bittorrent-csam-case/



Working with a Defense Expert

Scope, Deliverables, and Testimony Strategy

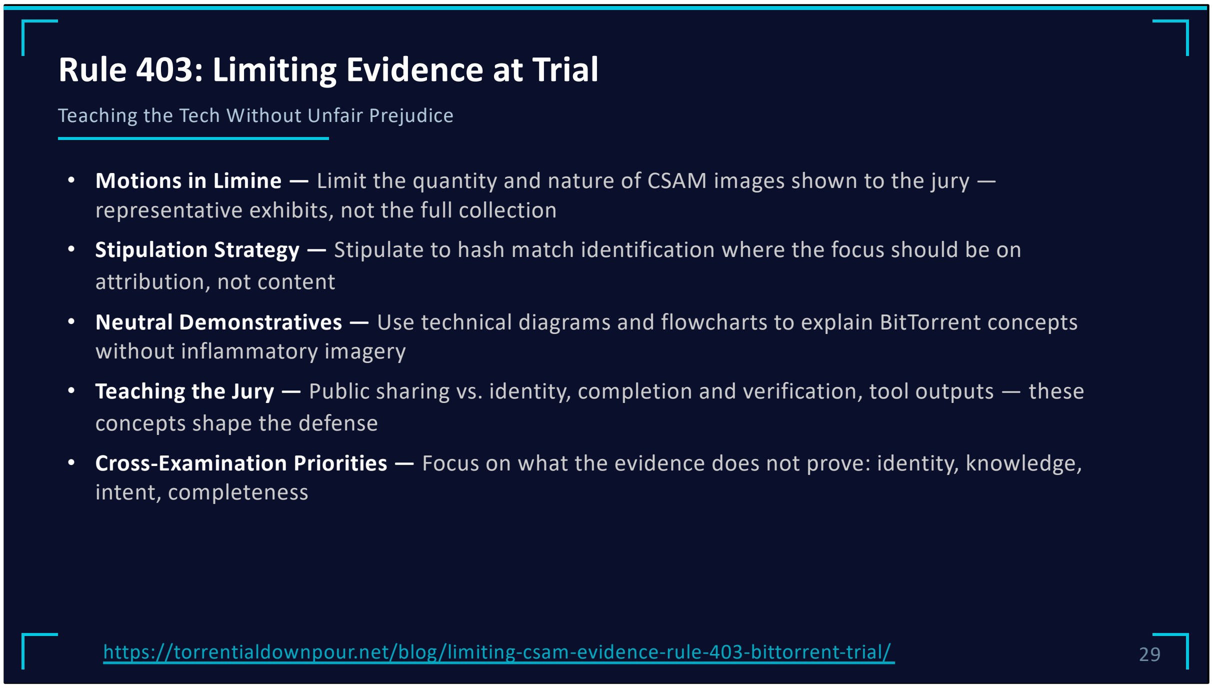
- **Consultant vs. Testifying Expert —** Consultant work is protected; testifying expert's work product may be discoverable — choose the role carefully
- **Focused Scope Statement —** One sentence defining exactly what the expert is retained to evaluate — prevents scope creep and disclosure issues
- **High-ROI Deliverables —** Claim-to-artifact table, timeline chart, technical report, and courtroom demonstratives
- **Expert Limitations —** Credible experts will not testify about identity or make absolute statements — they testify about what artifacts show
- **Cross-Examination Prep —** Prepare the expert for challenges to credentials, methodology, and the gap between opinion and certainty

https://torrentialdownpour.net/blog/defense-digital-forensic-expert-torrential-downpour/ 28

Effective expert engagement begins with role definition. A consulting expert can review everything under work product protection, while a testifying expert's work may be discoverable. Many cases benefit from starting with a consulting engagement, converting to testifying only if the evidence supports it. Recommended scope statement: 'Evaluate whether the Torrential Downpour artifacts support the factual claims in the search warrant affidavit.'

Highest-ROI deliverables:

(1) Claim-to-artifact table mapping each affidavit claim to supporting evidence.
(2) Timeline chart correlating tool activity with device activity.
(3) Technical report suitable for the court.
(4) Courtroom demonstratives explaining technical concepts to non-technical audiences. Credible experts testify about what the artifacts show and do not show — they do not identify who was at the keyboard or make absolute claims about attribution.



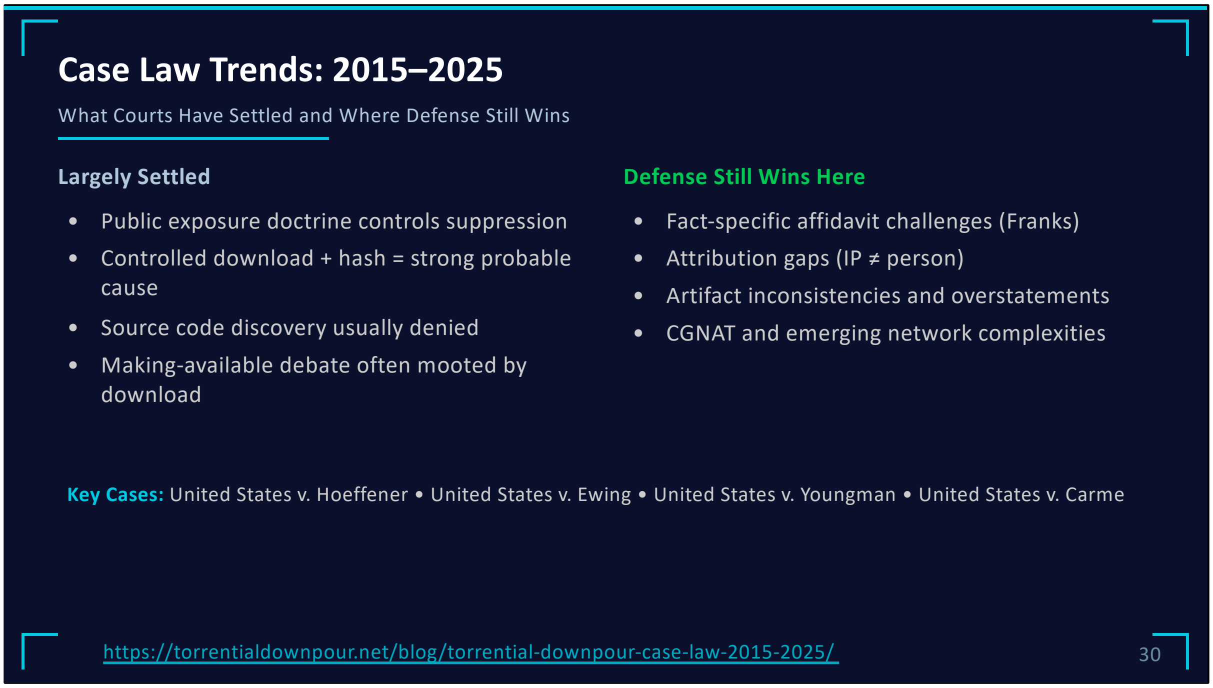
Rule 403: Limiting Evidence at Trial

Teaching the Tech Without Unfair Prejudice

- **Motions in Limine** — Limit the quantity and nature of CSAM images shown to the jury — representative exhibits, not the full collection
- **Stipulation Strategy** — Stipulate to hash match identification where the focus should be on attribution, not content
- **Neutral Demonstratives** — Use technical diagrams and flowcharts to explain BitTorrent concepts without inflammatory imagery
- **Teaching the Jury** — Public sharing vs. identity, completion and verification, tool outputs — these concepts shape the defense
- **Cross-Examination Priorities** — Focus on what the evidence does not prove: identity, knowledge, intent, completeness

https://torrentialdownpour.net/blog/limiting-csam-evidence-rule-403-bittorrent-trial/ 29

If the case goes to trial, Rule 403 motions are critical for limiting prejudicial impact. The core argument: the probative value of displaying numerous CSAM images to the jury is substantially outweighed by the danger of unfair prejudice, especially when the contested issues are technical (attribution, completion, knowledge) rather than content-based. Stipulation strategy: if the defense is not contesting that the files constitute CSAM, stipulate to that fact and focus the trial on attribution and technical evidence. Neutral demonstratives — clean, professional diagrams explaining how BitTorrent works, how Torrential Downpour operates, and where evidence gaps exist — help the jury understand the technology without being overwhelmed by disturbing images. Cross-examination priorities: establish what the government's witnesses cannot prove — who was at the keyboard, whether the user knew about uploading, and whether the download was complete. Blog: https://torrentialdownpour.net/blog/limiting-csam-evidence-rule-403-bittorrent-trial/



Case Law Trends: 2015–2025

What Courts Have Settled and Where Defense Still Wins

Largely Settled

- Public exposure doctrine controls suppression
- Controlled download + hash = strong probable cause
- Source code discovery usually denied
- Making-available debate often mooted by download

Defense Still Wins Here

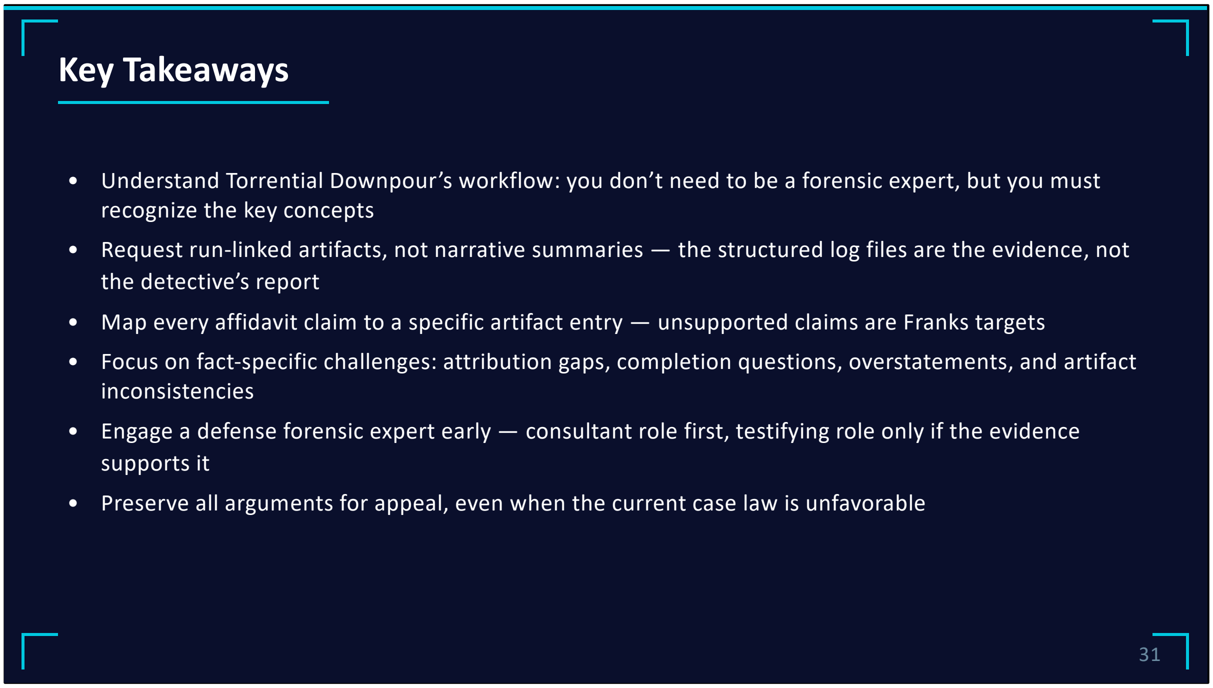
- Fact-specific affidavit challenges (Franks)
- Attribution gaps (IP ≠ person)
- Artifact inconsistencies and overstatements
- CGNAT and emerging network complexities

Key Cases: United States v. Hoeffener • United States v. Ewing • United States v. Youngman • United States v. Carme

https://torrentialdownpour.net/blog/torrential-downpour-case-law-2015-2025/

Ten years of case law reveals clear patterns:

- broad suppression theories face the public exposure doctrine and rarely succeed, but fact-specific challenges consistently create defense opportunities.
- Largely settled areas: the Fourth Amendment search argument against swarm monitoring, probable cause based on controlled downloads with hash verification, source code discovery denial, and the making-available debate being mooted by actual downloads.
- Areas where defense continues to prevail: Franks challenges based on concrete affidavit overstatements, attribution gaps at every level of the IP-to-person chain, artifact inconsistencies undermining government claims, and emerging network complexities like CGNAT.



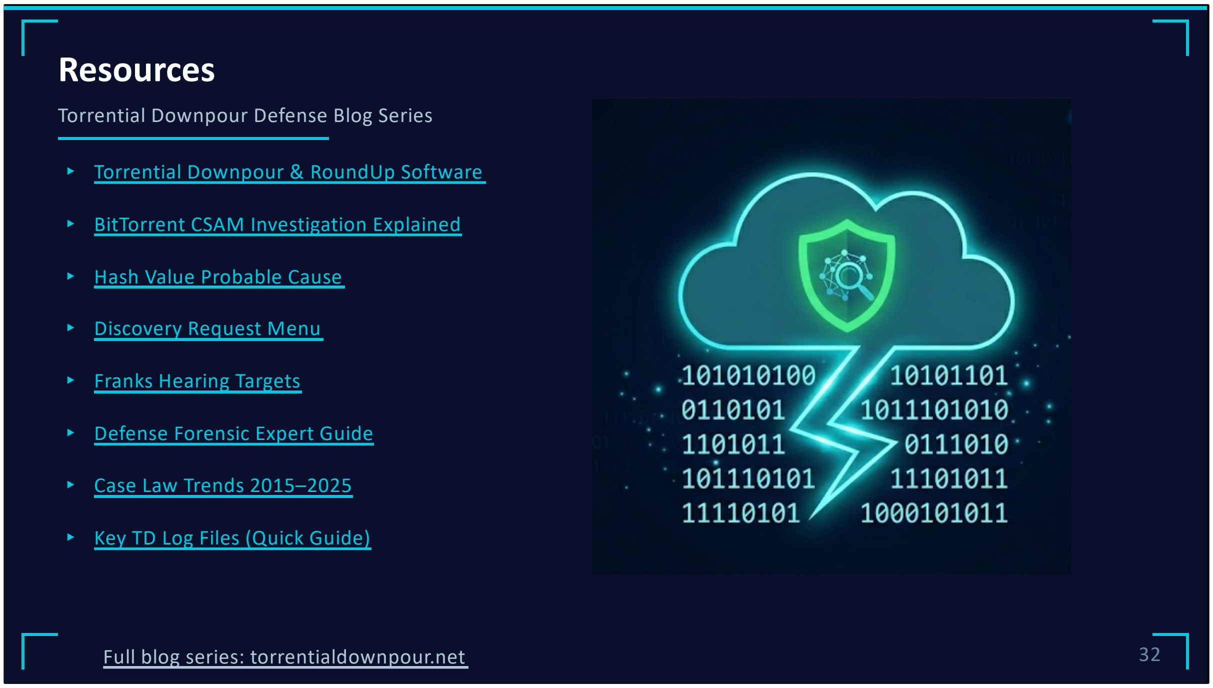
Key Takeaways

- Understand Torrential Downpour’s workflow: you don’t need to be a forensic expert, but you must recognize the key concepts
- Request run-linked artifacts, not narrative summaries — the structured log files are the evidence, not the detective’s report
- Map every affidavit claim to a specific artifact entry — unsupported claims are Franks targets
- Focus on fact-specific challenges: attribution gaps, completion questions, overstatements, and artifact inconsistencies
- Engage a defense forensic expert early — consultant role first, testifying role only if the evidence supports it
- Preserve all arguments for appeal, even when the current case law is unfavorable

31

Six key takeaways from this presentation:

- Defense attorneys do not need to become forensic experts to effectively handle BitTorrent CSAM cases.
- The essential requirements are recognizing key technical concepts, requesting the right artifacts, and working with experts who can translate technical evidence into legal arguments.
- The most effective defense work is fact-specific — map the affidavit claims to the actual artifacts, identify where the government has overstated or assumed facts not in evidence, and focus challenges on those concrete discrepancies.
- Engaging a forensic expert early in a consulting capacity helps guide discovery, triage, and strategy before committing to a trial theory.



Resources

Torrential Downpour Defense Blog Series

- Torrential Downpour & RoundUp Software
- BitTorrent CSAM Investigation Explained
- Hash Value Probable Cause
- Discovery Request Menu
- Franks Hearing Targets
- Defense Forensic Expert Guide
- Case Law Trends 2015–2025
- Key TD Log Files (Quick Guide)

101010100
10101101
0110101
1011101010
1101011
0111010
101110101
11101011
11110101
1000101011

Full blog series: torrentialdownpour.net

The full blog series at torrentialdownpour.net covers each topic from this presentation in depth, with practical guidance, sample discovery language, and case law references. The blog is designed as a companion resource for attorneys handling BitTorrent CSAM cases and is regularly updated as new case law develops.

LUCID TRUTH TECHNOLOGIES®

Questions?

Kenneth G. Hartman

Lucid Truth Technologies

ken@lucid-truth.com

torrentialdownpour.net

LucidTruthTechnologies.com