~ Technical Note ~

Reading the Onion: Tor, the Dark Web, and the Forensic Investigator

What the network hides, and what the host cannot

Author: Christopher L. T. Brown, Technology Consulting in Digital Forensics, AI & InfoSec, October 2026

Introduction

Ask most people what Tor does and the answer comes back simple: it makes you anonymous online. The real answer is narrower, and a good deal more useful. Tor conceals *who is talking to whom* on the wire. It does not make a machine forget what took place on it. For a forensic investigator, that distinction is the entire case.

Dark web investigations work rarely turns on breaking Tor's cryptography. It turns on the same discipline that carries surface-web investigations: recovering what the browser left behind on the host, and following the operational slip that exposes the people who run the service. What follows is how Tor actually works, where its protection genuinely stops, and how investigators convert those limits into admissible evidence.

The "dark web" is only the corner of the network most people mean. The surface web is what search engines index. The deep web is everything reachable but not indexed, from email inboxes to paywalled databases. The dark web is the narrow slice whose services that are sometimes only available for a short time and move from server to server. Accessing these “dark web” locations are most normally accessed through Tor or a similar anonymity network and live behind those 56-character onion addresses. When an investigator calls a case "dark web," it’s a concept, not a specific place you go to and that last band address is almost always where the work happens.

How Tor works, one circuit at a time

Tor routes traffic through a circuit of three volunteer relays: a guard (entry) node, a middle node, and an exit node. The client negotiates a distinct symmetric key with each relay and wraps every packet, called a cell, in three layers of encryption, hence the onion. Each node strips one layer, learns only its immediate neighbor, and passes the rest along. The guard knows who is connecting but not where they are going; the exit knows the destination but not the sender; the middle knows neither.

The design is elegant and the limits are honest. Tor defeats a passive observer on any single hop, but it was never meant to withstand an adversary who can watch both ends of the connection

and correlate timing and volume. It also cannot help a user who sends unencrypted HTTP through the exit node, where the final leg runs in plaintext. Both limits matter in dark web cases, where the useful evidence usually sits at one end of the circuit rather than in the middle.

The browser and the hidden service

Tor Browser is Firefox's extended-support release, hardened and locked to private browsing, with NoScript enabled by default. Its job is to keep the browser from leaking identity through cookies, canvas fingerprinting, or unusual browser behavior.

Sites on the Tor network run as onion services. An onion address is 56 characters ending in ".onion", and it is self-authenticating: the address derives from the service's public key, so the browser confirms it reached the intended site without any certificate authority. The server's location stays hidden from visitors, and traffic between user and service is encrypted end to end, which is why onion services do not depend on HTTPS the way clearnet sites do.

None of this hides what the user's own computer records about the visit.

Where anonymity actually ends: the host

The gap between what Tor promises on the wire and what it can deliver on the device is where forensic value concentrates. Private browsing stops the browser from deliberately writing history. It cannot stop the operating system from doing it.

A peer-reviewed audit by Muir, Leimich, and Buchanan at Edinburgh Napier University demonstrated this precisely. Default bookmarks shipped with Tor Browser persist on disk and in memory, uniquely identify the browser, and survive uninstallation and logout. On Windows 10, the titles of pages visited in Tor are written into the registry, so an examiner can reconstruct what a suspect was reading. Live memory, even after the browser is closed and the software removed, still returned the full path to the Tor executable and the username that ran it.

The trail can be broad. Windows records program execution in UserAssist and MuiCache keys. Prefetch files note that the browser ran. The pagefile carries fragments of closed sessions, and SQLite databases in the browser's profile keep bookmarks and site data. RAM is the richest source of all, provided the machine is acquired while still running. A write-blocked image of a seized machine can answer three questions a defense would rather an examiner never pose: was Tor installed, was it used, and what was viewed. Layered encryption undoes none of that, because the adversary Tor fails against here is the one standing at the keyboard.

None of this requires exotic tools. Autopsy carves disk images, the Volatility framework parses memory captures, and a write blocker paired with an Imager, preserves the original media while the examiner works from a copy.

Reaching the operator, not the cipher

History shows investigators reach dark web targets through infrastructure and operational error, not through breaking Tor. In 2017 the FBI and DEA, alongside Dutch police and Europol, took down AlphaBay and Hansa in a single coordinated stroke. Dutch authorities located Hansa's servers in the Netherlands, seized them, and then ran the marketplace under judicial authorization for a month, watching vendors and buyers before closing it. AlphaBay's administrator was identified and arrested in Thailand, and servers were seized in Canada and the Netherlands.

Two years earlier, the Silk Road 2.0 seizure redirected more than 400 ".onion" addresses with the cooperation of roughly 16 nations. The pattern repeats in every major operation, because the cryptography was never the weak point. A seized server, a misconfiguration, a captured administrator's laptop, or a careless cryptocurrency trail did the work that strong encryption could not be bothered to resist.

And that trail is rarely guesswork. Blockchain analysis now threads through most major dark web cases, following cryptocurrency from a seized wallet to an exchange that keeps know-your-customer records, the point where a pseudonymous username becomes a name on a subpoena.

The method that makes it admissible

Evidence recovered this way only wins in court if the process can be defended. NIST Special Publication 800-86 lays out the four phases: collection, examination, analysis, and reporting. Collection means acquiring data so its integrity holds, which for volatile memory means a live capture before shutdown. Examination and analysis extract and interpret. Reporting records what was done, by whom, and why.

For hidden-network cases the discipline tightens further. Hash every artifact at the moment of capture. Write-block physical media. Log circuit fingerprints, session metadata, and investigator attribution with timestamps, so chain of custody can be rebuilt from seizure to testimony. Tor defeats weak adversaries. It does not defeat careful documentation.

Key takeaways

- Tor protects traffic in transit, not the fingerprints a browser leaves on its own machine.
- The richest forensic sources are local: registry keys, SQLite databases, the pagefile, Prefetch, and especially live memory.
- Dark web takedowns succeed through infrastructure seizure and operator error, not through breaking encryption.
- Admissibility rests on NIST SP 800-86 discipline: collection, examination, analysis, and reporting, with hashing and chain of custody throughout.

Sources & Further Reading

1. A short introduction to Tor — The Tor Project

2. Onion services — The Tor Project, Tor Browser support
3. A Forensic Audit of the Tor Browser Bundle — Muir, Leimich & Buchanan, Edinburgh Napier University
4. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response — Kent, Chevalier, Grance & Dang (2006)
5. Massive blow to criminal Dark Web activities after globally coordinated operation — Europol (2017)
6. Dozens of Online Dark Markets Seized — Silk Road 2.0 — FBI (2014)