White Paper »

Securing Evidence Delivery and Mobile Forensics

How the Southwest Missouri Cyber Crimes Task Force enabled secure, real-time data and evidence management for distributed law enforcement operating environments with ZeroTier.

In partnership with

Southwest Missouri Cyber Crimes Task Force — an ICAC unit covering 22 counties

Focus area

Secure evidence transmission, mobile forensics and data sovereignty

About ZeroTier

ZeroTier gives organizations exactly what they need: a modern solution to the overengineered chaos of legacy networking. It's secure, direct, global connectivity that actually works. Whether managing a single device or an entire enterprise fleet, ZeroTier connects everything directly through a secure network you create and control and is SOC 2 compliant. ZeroTier Quantum, which meets NIST and NSA's highest standards at CNSA 2.0, extends that simplicity as the world's first end-to-end quantum-secure networking platform. Trusted by leaders across every industry, ZeroTier received a 2026 Cybersecurity Excellence Award in the Industry Software Solution category and was named "Cybersecurity Solution of the Year 2026" by The Cyber Security Review. ZeroTier is backed by Anorak Ventures, Battery Ventures, and Bonfire Ventures. Learn more at zerotier.com.

About the Task Force

The Southwest Missouri Cyber Crimes Task Force is a dedicated Internet Crimes Against Children (ICAC) task force. The unit covers a vast 22-county jurisdiction, spanning approximately one-quarter of the state of Missouri, specializing in child exploitation investigations, digital forensics extractions, and the secure management of highly sensitive criminal evidence.

The Overview »

A secure backbone for distributed field investigations

To support daily field operations and high-stakes criminal investigations, the The Southwest Missouri Cyber Crimes Task Force (SMCCTF) tackled a complex technical challenge: securely transmitting highly sensitive digital evidence files and forensic extractions involving minors across a distributed 22-county ecosystem back to local, on-premise servers.

Traditional solutions like standard commercial clouds, public file-sharing networks, or manual physical media transfers proved insecure, legally vulnerable, or too slow to deploy. Instead, the task force designed a streamlined, software-defined network using the ZeroTier One platform, enabling secure, low-latency data transmission across a distributed field environment. Combined with the task force's in-house cryptographic services, they built a scalable, reliable, and repeatable architecture for mobile law enforcement operations.

01

The challenge »

Secure, real-time evidence management across a distributed jurisdiction

Task force investigators faced critical logistical and security hurdles daily while processing internet crimes against children:

Sovereign data privacy

The evidence handled consists of highly sensitive files, including pictures and videos of underage victims. The task force required absolute data sovereignty, ensuring evidence could never be intercepted in transit nor exposed to third-party tech platforms or mainstream cloud providers. Additionally, the rise of AI-driven exploits and quantum computing introduces serious long-term risks of "harvest now, decrypt later" (HNDL) attacks on these sensitive data transfers. While current cryptographic standards cannot fully prevent the "Harvest Now, Decrypt Later" (HNDL) or "Trust Now, Forge Later" (TNFL) attacks posed by future quantum decryption, reducing the immediate visibility and accessibility of these data streams remains a critical priority.

Inflexible field environments

Remote investigators operating on laptops in the field needed a secure way to access central servers as if they were on local office domain networks, without creating vulnerable entry points.

Forensic transfer bottlenecks

Operating two digital forensics labs, each equipped with a mobile forensic van for on-scene warrant executions (such as at schools or residences), generated massive amounts of device data. Historically, transferring these extractions required a slow, multi-step process involving physical thumb drives, delaying the chain of custody and analysis.

02

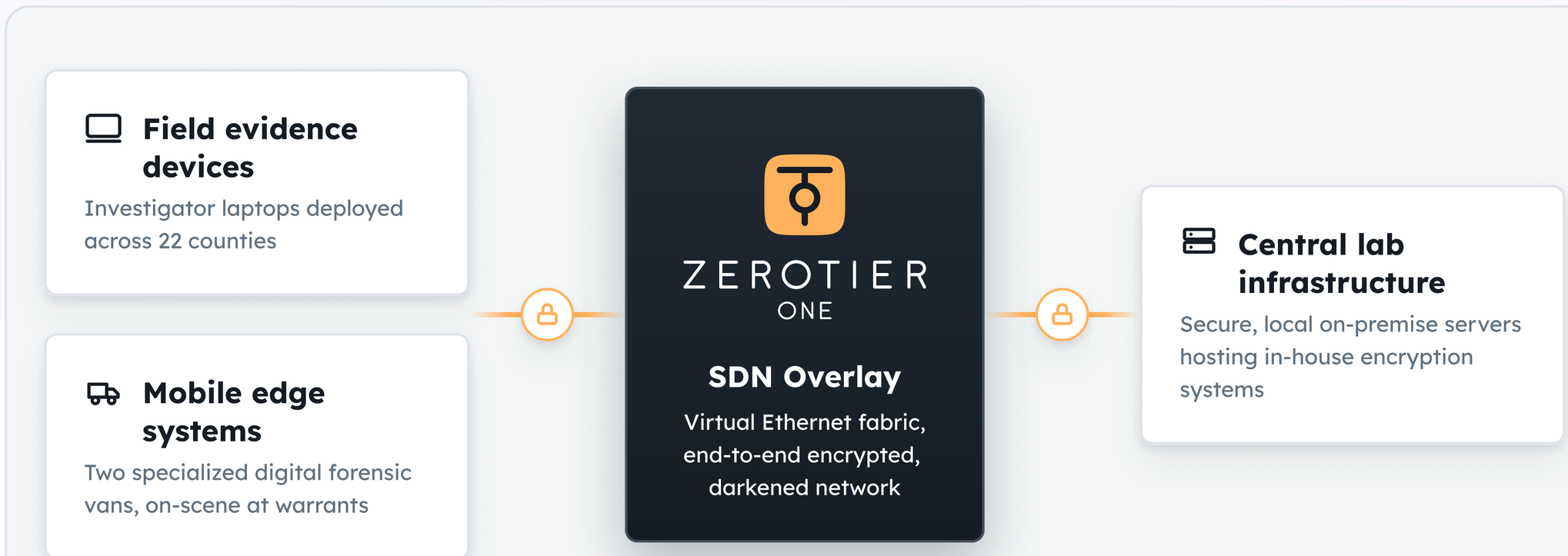
The solution »

Cryptographic evidence isolation and accelerated field forensics

1

Step 1 »

Designing a lightweight, scalable network



At the core is ZeroTier's software-defined networking (SDN) overlay, which enabled the task force to:

- **Combine VPN security with SD-WAN agility**

  Unlike traditional hub-and-spoke VPNs that hairpin traffic through a central choke point, ZeroTier operates as a peer-to-peer overlay, elegantly combining the encrypted tunneling of a VPN with the dynamic routing intelligence of an SD-WAN. This allows for direct, high-speed connections between field devices and central servers.

- **Establish peer-to-peer connections**

  ZeroTier's virtual Ethernet overlay ensured low-latency transmission directly between field laptops, forensic vans, and central servers.

- **Secure traffic end-to-end**

  Built-in encryption ensures data flows remain fully protected from outside interceptors.

- **Collapse the IP stack**

  By abstracting the network layer, ZeroTier effectively "darkens" the network, hiding connected forensic laptops and mobile devices from the public internet. This drastically reduces the task force's overall threat surface, ensuring that even advanced, AI-driven scanning tools cannot easily discover or target their network.

- **Unify disparate networks**

  Whether field units connect via cellular hot spots, public networks, or satellite, ZeroTier creates a single virtual network fabric.

- **Deploy rapidly**

  Lightweight software clients meant investigative laptops and field kits could join the secure network instantly without specialized routing hardware.

2

Step 2 »

Deploying the SDN overlay

The task force deployed the ZeroTier client across all field laptops and mobile forensic lab infrastructure. Each node is securely authorized via ZeroTier's controller with strict access controls and customized traffic rules. This tightly regulates what data moves where, safely isolating sensitive case files from the open internet.

3

Step 3 »

Unifying connectivity across WANs

ZeroTier's best-in-class multipathing allows field investigators to maintain direct peer-to-peer connectivity, whether on wired links, Wi-Fi, or even cellular networks. By automatically prioritizing the strongest link, ZeroTier ensures high-speed, direct connectivity regardless of the situation, letting forensic vans maintain uptime-critical large data extractions directly from the field.

4

Step 4 »

Strengthening security at every layer

Security is paramount when handling child exploitation material. All evidence is cryptographically saved directly to local, on-premise servers. By combining ZeroTier’s end-to-end encrypted tunnels with their own internal in-house encryption services, the SMCCTF ensures that no third-parties or IPSs can index, view, or access the data. To protect this sensitive data in transit, ZeroTier secures these direct connections using defense-grade encryption. The underlying ZeroTier One protocol relies on a robust secure handshake to establish cryptographic trust between endpoints before any data flows. Additionally, the platform is built with FIPS-capable encryption capabilities to support agencies with strict federal compliance requirements.

Zero trust isolation »

Two encryption layers

ZeroTier's end-to-end encrypted tunnels wrap the task force's own in-house cryptographic services; no third party or ISP can index, view, or access evidence in transit.

Defense-grade security »

FIPS-ready by design

ZeroTier One features a defense-grade architecture that verifies cryptographic trust before data flows. The underlying framework is fully FIPS-aligned, ensuring a one-step update to a certified network.

03

The conclusion »

Simple, resilient and secure forensic pipelines

Across daily deployments spanning 22 counties, the task force's ZeroTier-based architecture successfully connects mobile forensic vans and field laptops directly to local servers, delivering uninterrupted, high-security data transfers.

Field mobility

Field laptops behave seamlessly like domain laptops secured within the main office, keeping files shielded from interception.

No more thumb drives

The system guarantees connectivity in mission-critical scenarios and eliminates reliance on legacy physical media to transfer data.

> “ZeroTier saves us a ton of time. Even if we do extractions on scene, we can be transferring those files securely through ZeroTier while we travel. It saves a lot of time on the forensic side of things, and our investigators use it daily.”
>
> — Larry Roller, Detective, **Southwest Missouri Cyber Crimes Task Force**