THE FORENSICS WAY

ISSUE 01 | FORENSICS AWARENESS THIS WEEK | TUESDAY, JANUARY 27, 2026

FRONT PAGE

LEGAL PRECEDENT

Federal Appeals Court Interrogates "Compelled Biometrics"

In a watershed moment for digital civil liberties, the D.C. Circuit (*United States v. Brown*) is actively debating whether the **First Amendment** shields suspects from forced biometric device unlocking. The court is examining whether a face or fingerprint acts as a "digital key" that reveals private associations—making the act of unlocking a form of compelled speech.

This ruling could fundamentally shift traffic stop protocols, requiring warrants for biometric access that was previously considered a "search incident to arrest."

TODAY'S MANDATES

Synthetic Media Transparency Laws Go Live

As of today, January 27, 2026, new state laws require all AI-generated media to contain verifiable cryptographic provenance. Forensic examiners now

Threat Bulletin

CRITICAL

CVE-2026-20944

Remote Code Execution in Microsoft Office. Exploits are bypassing standard sandboxes via malformed .docx attachments.

ACTIVE EXPLOIT

CVE-2026-20805

Windows DWM privilege escalation zero-day. Federal agencies have been ordered to patch within 48 hours.

MALWARE SPOTLIGHT

Osiris Ransomware

A new strain that specifically targets .E01 and .AFF4 forensic image files, attempting to

face a "Verification First" era, where the absence of these markers could render digital evidence inadmissible in New York and California courts.

corrupt backups during the investigative phase.

THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, JANUARY 27, 2026

CASE STUDIES: HISTORICAL GRID

THE BTK METADATA INCIDENT

The Floppy Disk Fingerprint

Dennis Rader's thirty-year run ended in 2005 through a single deleted Word file. The metadata listed "Dennis" and "Christ Lutheran Church," proving that deleted properties are never truly gone.

ROSS ULBRICHT: SILK ROAD

The Unlocked Capture

The FBI's 2013 capture of Ross Ulbricht relied on a public "snatch" of his laptop while it was still decrypted, securing 700,000 Bitcoins and his private journal of illegal operations.

STATE V. RICHARD DABATE

The Fitbit Witness

Wearable data from a Fitbit proved a victim was active over an hour after her husband claimed she had been murdered, showcasing the power of IoT evidence in court.

ENCROCHAT BREACH

Breaking the "Unbreakable"

By deploying a forensic "implant" to encrypted handsets, European agencies intercepted 100 million plain-text messages, dismantling global cartels in real-time.

PRIORITY CVE ADVISORIES

JAN 22, 2026

CVE-2026-24061 (TELNET)

GNU InetUtils Auth Bypass allowing remote root access. *Forensic Note:* Check for unusual USER env var logs.

JAN 21, 2026

CVE-2026-20045 (CISCO)

Zero-day Command Injection in Unified CM. *Forensic Note:* Look for unauthorized shell executions in call logs.

RECENT MALWARE WATCH

NEW STRAIN: JAN 2026

GOLDPICKAXE TROJAN

Sophisticated iOS/Android malware harvesting biometric face data for unauthorized bank access via deepfakes.

ALERT: JAN 2026

SECTOPRAT V.2

Remote Access Trojan using "ClickFix" lures to mimic browser updates. Highly effective at credential exfiltration.