Digital Forensics Techniques in Modern Fraud Investigation

Date: 2025-11-14

Introduction

The proliferation of digital technologies has fundamentally transformed the landscape of financial crime, giving rise to sophisticated methods of fraud that transcend geographical boundaries. In response, the field of digital forensics has become an indispensable component of modern fraud investigation, providing the methodologies and tools necessary to uncover, analyze, and preserve electronic evidence. Investigating digital fraud requires a multi-faceted approach, capable of tracing activities across a complex web of devices, networks, and anonymizing services. This report provides a comprehensive analysis of key digital forensics techniques employed in the investigation of fraud. It covers device and browser fingerprinting, IP address tracking, timezone analysis, phone number verification, the detection of identity masking services such as VPNs and proxies, and the specialized tools utilized by law enforcement agencies. By synthesizing evidence-based research, this document outlines the current state of these techniques, their practical applications, inherent challenges, and the best practices that guide their effective and ethical implementation.

Device and Browser Fingerprinting

Device fingerprinting is a powerful technique used to identify and track specific devices by collecting and analyzing a unique combination of hardware and software attributes. This process creates a distinct identifier, or “fingerprint,” that allows investigators to link a device to fraudulent activities, even when conventional tracking methods like cookies are disabled or IP addresses are changed. A major subset of this is **browser fingerprinting**, which focuses on attributes exposed by a web browser, such as its version, installed plugins, screen resolution, and system fonts. The aggregation of these data points can generate a highly unique hash, with research indicating that a significant percentage of browser fingerprints are unique, ranging from 83.6% to 94.2% in some studies. This makes it a resilient method for persistent identification in forensic analysis.

The evolution of these techniques has been rapid. Early methods from the 2000s focused on basic browser data, but the field advanced significantly with the introduction of more sophisticated techniques. **Canvas fingerprinting**, for example, leverages the HTML5 canvas element to render a hidden graphic. Minor variations in a device’s graphics hardware (GPU), drivers, and operating system cause the image to be rendered in a subtly unique way, which can be converted into a stable identifier. Similarly, **WebGL fingerprinting** renders 3D graphics to expose hardware differences, while **audio fingerprinting** analyzes the unique rendering of sound waves via the Web Audio API to capture anomalies specific to a device’s CPU and browser. These methods are complemented by hardware ID techniques, which gather information about physical components like CPU architecture, RAM, and battery status, providing a more stable and difficult-to-spoof layer of identification.

In the context of fraud investigation, device fingerprinting is critical for detecting and attributing malicious activities. It enables security systems to identify account takeovers, bot activity, and coordinated fraud attacks. For instance, if multiple accounts are created from a device with the same fingerprint but different user credentials, it can signal a fraud ring. In e-commerce and banking, these techniques

help flag suspicious transactions in real-time by identifying inconsistencies between a user's known device fingerprint and the one used for a transaction. For law enforcement, a device fingerprint can serve as a crucial piece of evidence linking a suspect's device to a crime scene, such as a data breach or an online scam. However, the technique is not without limitations. Fraudsters can employ spoofing methods, such as using emulators, virtual machines, or specialized tools to manipulate their device attributes and evade detection. Furthermore, the pervasive nature of fingerprinting raises significant privacy concerns, leading to regulations like GDPR and CCPA that govern its use. To mitigate these challenges, investigators often employ a multi-layered approach, combining fingerprinting with behavioral biometrics and other signals, while privacy-focused browsers like Tor and Brave implement countermeasures to resist fingerprinting by randomizing device attributes.

IP Address Tracking and Geolocation

IP address tracking and geolocation are foundational techniques in digital forensics, enabling investigators to determine the approximate physical location of an internet-connected device. An IP address serves as a unique identifier for a device on a network, and by querying this address against specialized databases, law enforcement can obtain information such as the country, city, ZIP code, and the Internet Service Provider (ISP) associated with it. This process is not a single method but a collection of technologies, including databases maintained by Regional Internet Registries, data from ISPs, and supplementary information from Wi-Fi signals or GPS data embedded in file metadata. While static IP addresses are fixed, most residential connections use dynamic IPs that change over time, adding a layer of complexity to investigations.

Law enforcement agencies utilize a variety of methods to track suspects via their IP addresses. The process often begins with analyzing IP logs from online services, social media platforms, or websites where criminal activity is suspected. Tools like Wireshark and tcpdump allow for network traffic analysis, capturing data packets to reveal the path information takes across the internet. Open Source Intelligence (OSINT) techniques further enhance tracking by correlating IP data with publicly available information. For example, EXIF data from a photograph posted online can contain precise GPS coordinates, while social media check-ins can help reconstruct a suspect's movements. Advanced geolocation APIs provide real-time location data, which can be integrated into larger investigative frameworks to enrich cyber threat intelligence by combining IP data with domain and DNS information.

The application of IP geolocation in law enforcement is extensive, particularly in combating cybercrime and fraud. It is instrumental in tracing the origins of hacking attempts, phishing campaigns, and the distribution of illegal content. In fraud detection, IP geolocation is used to flag suspicious transactions by comparing the location of the device making a purchase with the billing or shipping address on file. A significant mismatch can indicate identity theft or credit card fraud. Law enforcement can also use IP data to obtain court orders or subpoenas, compelling ISPs to release subscriber information linked to a specific IP address at a particular time. However, the accuracy of IP geolocation is a significant consideration. While it can be highly accurate at the country level, its precision at the city or street level varies widely. The use of Virtual Private Networks (VPNs), proxies, and the Tor network is a major challenge, as these tools are designed to mask a user's true IP address. Investigators must therefore use specialized tools to detect the use of such anonymizers. Furthermore, the practice of IP tracking is governed by legal and privacy considerations, requiring law enforcement to operate within strict regulatory frameworks to ensure that evidence is admissible in court and that individual privacy rights are respected.

Timezone and Timestamp Analysis

In any digital investigation, establishing an accurate timeline of events is paramount. Timezone and timestamp analysis is a meticulous forensic process focused on correctly interpreting the time information recorded by digital devices. Nearly every action on a computer or mobile device, from creating a file to sending an email, generates a timestamp. However, these timestamps can be recorded in various formats, such as Coordinated Universal Time (UTC) or the device's local time. A failure to properly account for timezone settings, Daylight Saving Time (DST), and clock inaccuracies can lead to a distorted timeline, potentially exonerating the guilty or implicating the innocent. The integrity of an investigation hinges on the examiner's ability to normalize all time-based evidence to a common standard, typically UTC, to ensure event correlation is accurate.

Identifying a device's configured timezone is a critical first step. On Windows systems, this information is stored within the system registry, specifically in the `SYSTEM\CurrentControlSet\Control\TimeZoneInformation` key. Forensic examiners analyze values such as `Bias`, `ActiveTimeBias`, and `TimeZoneKeyName` to determine the offset from UTC and whether DST was active at a given time. For mobile devices like Android, the timezone setting is often located in a file such as `/data/property/persyst.sys.timezone`. By extracting and analyzing these artifacts, an investigator can reconstruct the device's time settings and apply the correct offsets to local timestamps. This process can be complicated by outdated timezone databases on a device or user-configured incorrect settings, necessitating careful verification.

Handling timestamps requires a deep understanding of how different systems record time. Some systems store all timestamps in UTC, while others use local time, and some applications may even use "naive" timestamps without any timezone information. Forensic tools like Belkasoft X, ArtiFast Windows, and the open-source framework Plaso are designed to automate the complex process of parsing and converting timestamps from various sources. These tools can ingest data from file systems, logs, and applications, normalize all timestamps to UTC, and present them in a unified timeline. This allows an investigator to view events from multiple devices and data sources in a single, chronologically accurate sequence. Common challenges include **clock skew**, where a device's internal clock is inaccurate, and the complexities of historical DST rules, which can vary by jurisdiction and year. Best practices dictate that investigators should establish timezone settings early, use UTC as a standard for analysis, document all conversions, and, where possible, corroborate digital timestamps with external, reliable time sources to ensure the highest degree of accuracy.

Anonymity and Masking Detection

Fraudsters and other malicious actors frequently rely on services that mask their identity and location, making attribution a significant challenge for investigators. Digital forensics has developed a suite of techniques to detect and, in some cases, bypass these anonymization methods. These techniques target everything from the network level, by identifying VPNs and proxies, to the application level, by analyzing digital footprints left across the web.

VPN and Proxy Detection

VPNs and proxies are commonly used to obscure a user's true IP address by routing their internet traffic through an intermediary server. Detecting the use of these services is a critical first step in unmasking a fraudster. One of the most common methods is database-driven detection, which involves checking a user's IP address against continuously updated lists of known VPN and proxy server IPs. Threat intelligence services maintain extensive databases of IP addresses associated with commercial VPN providers, data centers, and public proxies. Another technique involves analyzing network traffic

characteristics. For example, the port numbers used for connections, the size and frequency of data packets, and inconsistencies between the IP address's geolocation and other user data (like language settings) can indicate the use of an anonymizer. Advanced systems employ machine learning and behavioral analysis to identify patterns associated with anonymized traffic, such as multiple users appearing to originate from a single IP or unusual bandwidth consumption. Research indicates that combining these methods can be highly effective, with some systems achieving high detection rates for proxies and VPNs. Unmasking the user behind the service is more difficult but can sometimes be achieved through techniques like DNS leak analysis, which may reveal the user's real IP, or by exploiting vulnerabilities in the anonymization service itself.

Identity Masking and OSINT

Beyond network-level anonymization, individuals may attempt to mask their identity by creating synthetic or fraudulent online personas. Open Source Intelligence (OSINT) provides a powerful, non-intrusive framework for detecting such deception by piecing together publicly available information. OSINT forensics involves systematically collecting and analyzing data from social media, public records, forums, data breach dumps, and the dark web to build a profile of a target. When investigating a potentially masked identity, analysts look for inconsistencies and connections. For example, a social media profile with no history, few connections, and stock photos may be a synthetic identity created for fraudulent purposes. AI-driven OSINT tools can accelerate this process by scanning vast datasets for patterns, linking disparate pieces of information, and flagging anomalies that suggest identity masking. In fraud detection, OSINT can be used to verify customer identities during onboarding or to investigate suspicious users by cross-referencing their provided information with their digital footprint. This external context can reveal if a user is part of a known fraud network or is using credentials exposed in a data breach.

Phone Number Verification and OSINT

Phone numbers are a valuable data point in investigations, often serving as a direct link to an individual. OSINT provides numerous methods for tracking and verifying phone numbers to unmask their owners. The process typically begins with a reverse phone lookup using online services like Truecaller or Whitepages, which aggregate data from public records and crowdsourced information to identify the owner's name and carrier. More advanced OSINT tools, such as Phoneinfoga, can provide further details, including the number's validity, type (mobile vs. VoIP), and associated country and city. Investigators can also search for the phone number on search engines and social media platforms, as people often link their numbers to public profiles or business listings. A key technique involves using the account recovery features of major online services (like Google or Facebook); by entering a phone number into the "forgot password" flow, an investigator can sometimes confirm if an account is registered to that number and may even see a partially redacted email address or profile picture. By cross-referencing information across multiple sources, including data breach repositories, investigators can often connect a seemingly anonymous phone number to a real identity and a broader online presence, effectively peeling back the layers of a masked identity.

Law Enforcement Tools and Methodologies

The successful investigation of digital fraud relies on a combination of a structured forensic process and a sophisticated toolkit. Law enforcement agencies and corporate investigators follow a standardized methodology to ensure that digital evidence is collected, handled, and analyzed in a manner that preserves its integrity and ensures its admissibility in legal proceedings. This process generally includes four main phases: identification of potential evidence, preservation and collection of data, analysis of the collected data, and reporting of the findings. Specialized digital forensics tools are em-

ployed at each stage to manage the complexities of extracting and interpreting data from a wide array of sources, including computers, mobile devices, servers, and cloud services.

A variety of powerful software suites are central to modern digital forensics. **EnCase Forensic** is a comprehensive platform widely used by law enforcement for its ability to perform in-depth analysis of file systems, decrypt encrypted data, and create detailed reports. It excels at creating forensic images (bit-for-bit copies) of storage media, ensuring that the original evidence remains untouched. **X-Ways Forensics** is another industry-standard tool, known for its speed and efficiency in processing large volumes of data, analyzing file systems, and recovering deleted files. For open-source solutions, **Autopsy** provides a graphical interface to The Sleuth Kit and other forensic tools, enabling investigators to perform timeline analysis, keyword searches, and data carving to recover fragments of deleted files. These tools are essential in fraud cases for examining financial records, emails, and user activity logs to reconstruct events and identify malfeasance.

In addition to these comprehensive platforms, investigators use specialized tools for specific tasks. **Magnet AXIOM** is highly regarded for its ability to extract and analyze artifacts from mobile devices and cloud sources, which is crucial for investigating fraud schemes coordinated through messaging apps or social media. For network-level investigations, tools like **Wireshark** allow for the capture and analysis of network traffic, helping to trace the source of phishing attacks or identify unauthorized data transfers. **Bulk Extractor** is a tool designed to rapidly scan a disk image for specific types of information, such as credit card numbers, email addresses, and URLs, without parsing the file system, making it highly effective for quickly identifying relevant evidence in large datasets. The selection of tools depends on the specifics of the case, but their combined use allows investigators to build a comprehensive picture of fraudulent activity, attribute actions to specific individuals, and present clear, verifiable evidence to support legal action.

Conclusion

The fight against digital fraud is a dynamic and technologically driven endeavor, requiring investigators to continuously adapt to the evolving tactics of malicious actors. The digital forensics techniques detailed in this report—from the granular analysis of a device’s hardware signature to the broad-spectrum intelligence gathering of OSINT—form the bedrock of modern fraud investigation. Device fingerprinting, IP tracking, and timestamp analysis provide the means to place a suspect behind a keyboard at a specific time, while the detection of anonymizing services and masked identities allows investigators to penetrate the layers of obfuscation that criminals use to hide. The effective application of these methods, supported by a robust toolkit of specialized software, empowers law enforcement and cybersecurity professionals to reconstruct complex fraud schemes, attribute responsibility, and produce the evidence necessary for successful prosecution. As technology continues to advance, the “cat-and-mouse” game between fraudsters and investigators will undoubtedly persist, underscoring the critical importance of ongoing research, innovation, and collaboration in the field of digital forensics.

References

Device fingerprint - Wikipedia (https://en.wikipedia.org/wiki/Device_fingerprint)
Browser Fingerprinting Techniques - Fingerprint (https://fingerprint.com/blog/browser-fingerprinting-techniques/)
What Is Device Fingerprinting? - IPQualityScore (https://www.ipqualityscore.com/device-fingerprinting)
What Is Digital Fingerprinting? - BitSight (https://www.bitsight.com/learn/cti/digital-fingerprinting)
What is device fingerprinting? - Stytch (https://stytch.com/blog/what-is-device-fingerprinting/)
What is Device Fingerprinting? - Arkose Labs (https://www.arkoselabs.com/explained/device-fingerprint-

ing/)
What is Device Fingerprinting? - DataVisor (https://www.datavisor.com/wiki/device-fingerprinting)
Device Fingerprinting: What is it and How it Works - SEON (https://seon.io/resources/device-fingerprinting/)
Device Fingerprint Spoofing: What It Is and How to Detect It - Incognia (https://www.incognia.com/blog/device-fingerprint-spoofing)
What is Browser Fingerprinting? - Focal (https://www.getfocal.ai/knowledgebase/what-is-browser-fingerprinting)
Internet geolocation - Wikipedia (https://en.wikipedia.org/wiki/Internet_geolocation)
OSINT Sources: Geolocation OSINT - Neotas (https://www.neotas.com/osint-sources-geolocation-osint/)
How to Geolocate an IP Address: A Comprehensive Guide - WhoisXML API (https://ip-geolocation.whoisxmlapi.com/blog/geolocate-ip-address)
Everything You Need to Know About IP Geolocation - Geotargetly (https://geotargetly.com/everything-you-need-to-know-about-ip-geolocation)
How Law Enforcement Tracks Hackers & Telco Scammers: Tools & Techniques - i.Lease (https://i.lease/how-law-enforcement-tracks-hackers-telco-scammers-tools-techniques/)
IP Tracer: Top Methods and Use Cases - geoPlugin (https://www.geoplugin.com/resources/ip-tracer-top-methods-and-use-cases/)
IP Geolocation: The Ultimate Guide - Abstract API (https://www.abstractapi.com/guides/ip-geolocation-the-ultimate-guide)
IP Geolocation Capabilities, Myths and Facts - IP2Location Blog (https://blog.ip2location.com/knowledge-base/ip-geolocation-capabilities-myths-and-facts/)
Can the police track you via your IP address? - Olliers Solicitors (https://www.olliers.com/news/can-the-police-track-you-via-your-ip-address/)
How Accurate is IP Geolocation? - WhatIsMyIPAddress.com (https://whatismyipaddress.com/geolocation-accuracy)
Time zone and timestamp analysis in digital forensics: A case study in an Android environment - ScienceDirect (https://www.sciencedirect.com/science/article/abs/pii/S1742287614000449)
Time Zone Information - Forensafe (https://www.forensafe.com/blogs/timezoneinformation.html)
Time Zone Identification - Digital Detective (https://www.digital-detective.net/time-zone-identification/)
Digital Forensic Timeline Analysis with Belkasoft X - Belkasoft (https://belkasoft.com/digital-forensic-timeline-analysis)
Time Zone - Forensic Focus Forums (https://www.forensicfocus.com/forums/general/time-zone/)
Time zone and timestamp analysis in digital forensics: A case study in an Android environment - ACM Digital Library (https://dl.acm.org/doi/10.1016/j.diin.2014.05.001)
Time zone question - Reddit (https://www.reddit.com/r/computerforensics/comments/4al4jt/time_zone_question/)
Identification of Time Zone Settings on Suspect Computer - Digital Detective Knowledge Base (https://kb.digital-detective.net/display/BF/Identification+of+Time+Zone+Settings+on+Suspect+Computer)
How to get timezone informaiton? - Reddit (https://www.reddit.com/r/computerforensics/comments/3yja77/how_to_get_timezone_informaiton/)
Time and date issues in forensic computing - A case study - ResearchGate (https://www.researchgate.net/publication/222531661_Time_and_date_issues_in_forensic_computing_-_A_case_study)
Find Identifying Information from a Phone Number Using OSINT Tools - Null Byte (https://null-byte.wonderhowto.com/how-to/find-identifying-information-from-phone-number-using-osint-tools-0195472/)
Telephone-OSINT - GitHub (https://github.com/The-Osint-Toolbox/Telephone-OSINT)
The Insider’s Guide to Mastering OSINT Techniques for Phone Number Tracking - Medium (https://medium.com/@efim.lerner/the-insiders-guide-to-mastering-osint-techniques-for-phone-number-tracking-

da61dd004c7c)
Phone Number Tools - AWARE Online (https://www.aware-online.com/en/osint-tools/phone-number-tools/)
In-Depth Guide to Phone Number OSINT Tools - Espy Security (https://espysys.com/blog/in-depth-guide-to-phone-number-osint-tools/)
OSINT tools for finding intel on a phone number - Reddit (https://www.reddit.com/r/OSINT/comments/cxliik/osint_tools_for_finding_intel_on_a_phone_number/)
OSINT: How to Investigate a U.S. Phone Number - Secjuice (https://www.secjuice.com/osint-how-to-investigate-us-phone-number/)
Check and locate phone number in OSINT - Medium (https://medium.com/@ibederov_en/check-and-locate-phone-number-in-osint-8beb8af50d5e)
7 Free OSINT Tools to Reverse Trace a Phone Number - Medium (https://medium.com/@samuel.i.steers/7-free-osint-tools-to-reverse-trace-a-phone-number-13b4f0e7add9)
OSINT Phone Number Investigations: A Comprehensive Guide - Lampyre (https://lampyre.io/blog/osint-phone-number-investigations-a-comprehensive-guide/)
Digital Forensics Tools - Department of Homeland Security (https://www.dhs.gov/publication/digital-forensics-tools)
A Guide to Digital Forensics Tools - ForensicsColleges.com (https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools)
Understanding The Digital Forensics Process, Techniques, and Tools - BlueVoyant (https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools)
Digital investigations and forensics - OpenText (https://www.opentext.com/products/digital-investigations-and-forensics)
What is Digital Forensics? - American Public University (https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-digital-forensics/)
Cyber Crime Investigation - Recorded Future (https://www.recordedfuture.com/threat-intelligence-101/incident-response-management/cyber-crime-investigation)
Cyber Forensics - SalvationDATA (https://www.salvationdata.com/knowledge/cyber-forensics/)
Best Digital Forensics Software - TrustRadius (https://www.trustradius.com/digital-forensics)
Forensics - Department of Homeland Security Archive (https://www.dhs.gov/archive/science-and-technology/forensics)
The Best Digital Forensic Tools For Breach Investigation And Brand Protection - Expert Insights (https://expertinsights.com/insights/the-best-digital-forensic-tools-for-breach-investigation-and-brand-protection/)
Unmasking the True Identity: Unveiling the Secrets of Virtual Private Networks and Proxies - MDPI (https://www.mdpi.com/2078-2489/16/2/126)
Novel technique can unmask up to 70% of crooks hiding behind VPNs, proxies, Tor - SC Media (https://www.scworld.com/feature/novel-technique-can-unmask-up-to-70-of-crooks-hiding-behind-vpns-proxies-tor)
Exploring Proxy Detection Methodology - ResearchGate (https://www.researchgate.net/publication/304158964_Exploring_Proxy_Detection_Methodology)
The Need for Proxy & VPN Data in Today’s Heightened Cybersecurity State - Digital Element (https://www.digitalelement.com/resources/guides/the-need-for-proxy-vpn-data-in-todays-heightened-cybersecurity-state/)
Detecting Residential Proxies - Unmasking Fraudulent IP Addresses - IPQualityScore (https://www.ipqualityscore.com/articles/view/115/detecting-residential-proxies-unmasking-fraudulent-ip-addresses)
Unmasking the True Identity: Unveiling the Secrets of Virtual Private Networks and Proxies - ResearchGate (https://www.researchgate.net/publication/388843896_Unmasking_the_True_Identity_Unveiling_the_Secrets_of_Virtual_Private_Networks_and_Proxies)

AI-Powered Proxy and VPN Detection - CrowdSec (https://www.crowdsec.net/blog/ai-powered-proxy-and-vpn-detection)
How to Detect VPNs and Proxies - Inventive (https://inventivehq.com/blog/how-to-detect-vpns-and-proxies)
Unmasking crooks hiding behind VPNs, proxies, Tor - Reddit (https://www.reddit.com/r/onions/comments/1jnjl8z/unmasking_crooks_hiding_behind_vpns_proxies_tor/)
GeoGuard - GeoComply (https://www.geocomply.com/anti-fraud-and-geolocation-solutions/geoguard/)
Forensic Investigation using Open Source Intelligence (OSINT) - FutureSkills Prime (https://www.futureskillsprime.in/blogs/forensic-investigation-using-open-source-intelligence-osint/)
OSINT Investigations: How to Avoid Being Unmasked - Traversals (https://traversals.com/blog/osint-investigations/)
OSINT & Digital Forensics - WITNESS Media Lab (https://lab.witness.org/projects/osint-digital-forensics/)
Enhancing Digital Forensics with AI-Driven OSINT: A Proactive Approach to Cybercrime Investigation - ResearchGate (https://www.researchgate.net/publication/391482255_Enhancing_Digital_Forensics_with_AI-Driven_OSINT_A_Proactive_Approach_to_Cybercrime_Investigation)
OSINT Investigation Platform - Neotas (https://www.neotas.com/osint-investigation-platform/)
How open-source intelligence can support your organization - MNP (https://www.mnp.ca/en/insights/directory/how-open-source-intelligence-support-organization)
OSINT for Cybercrime Investigations - Social Links (https://sociallinks.io/cases/osint-for-cybercrime-investigations)
What is OSINT Investigation and Why is it Important? - Corma Investigations (https://corma-investigations.com/series/osint-lookdeeper/what-is-osint-investigation-and-why-is-it-important/)
Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINTOSINT) - A timely and cohesive mix - ResearchGate (https://www.researchgate.net/publication/312049886_Digital_forensic_intelligence_Data_subsets_and_Open_Source_Intelligence_DFINTOSINT_A_timely_and_coh
Best Fraud Detection Software & Tools - ShadowDragon (https://shadowdragon.io/blog/best-fraud-detection-software-tools/)