NTREPID

The Mobile Advantage

Authentic Operations in a Mobile-First World

One of the biggest global developments in the 21st century has been the transition from desktop devices to mobile devices as the primary method for accessing the internet. In 2025, mobile devices account for roughly 62% of all web traffic while desktops make up roughly 36%. This has helped with the democratization of knowledge and information, but it has also created challenges for intelligence, defense, and enterprise operations. Criminals and online adversaries move fluidly between devices, making it difficult to trace and track their activities. Online investigators and auditors need solutions that allow them to adapt and keep pace with their adversaries while presenting as mobile-first users. In this paper, we will explore how the shift towards mobile has reshaped cyber operations and digital investigations, and how Ntrepid provides the solutions and capabilities needed to keep pace.

The Global Shift to Mobile

7.21 billion people worldwide use smartphones daily. Mobile devices factor into every part of life, from personal and relationship matters, to business dealings and government activities. The shift to a mobile-first world has been driven by how people and organizations interact with the digital world. Social media platforms, messaging apps, and location-based services are optimized for mobile usage. The expansion of mobile applications, mobile-optimized content, and app-specific communication channels has created new data sources and investigative opportunities, but also new challenges around attribution, compliance, and security. Investigators who rely solely on desktop solutions risk appearing inauthentic, losing access to critical platforms, or raising suspicion in their target environments.

One of the impacts of increased mobile adoption, is that maintaining an authentic online presence has become increasingly difficult. Today, the majority of internet users access platforms through smartphones, often during evenings, weekends, and irregular hours. In contrast, operating exclusively from desktop environments between 9–5, Monday through Friday, creates a detectable and unrealistic pattern of life that platforms and adversaries can easily flag as inauthentic.

The Mobile Majority

Fast Facts

62% of all web traffic now comes from mobile devices

7.21 billion smartphone users worldwide access the internet daily

Mobile-first platforms dominate digital interactions

Modern smartphones are also deeply integrated into a broader digital ecosystem, connected to cloud services, identity management systems, and smart devices. Using an unsecured mobile device to appear as an authentic mobile user online presents opportunity and risks as users can enjoy seamless access to mobile-first applications and data collection environments, but the number of digital traces that can be analyzed for inconsistencies increases as well.

As mobile connectivity continues to expand on a global scale, the expectation of an authentic mobile signature is critical for online operations. Investigators and analysts require solutions that allow them to securely access the internet with an authentic mobile signature that aren't susceptible to the various avenues of exposure that regular mobile phones are. Even when appearing online as authentic mobile users, these operators also require automated workflows that can carry out authentic online behavior even when the operators themselves are offline or away from their devices.

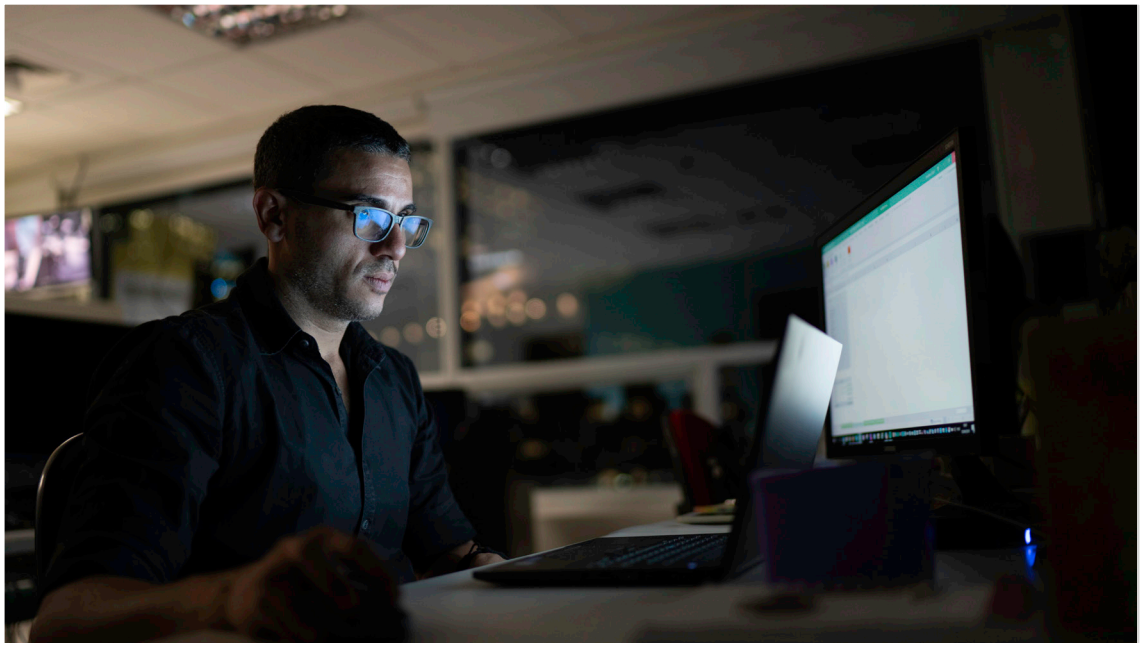
Implications for Digital Investigations

The landscape for digital investigations is more complex to navigate than ever. With mobile phones as the leading method for accessing the internet, having an inauthentic mobile signature for your digital presence could lead to the exposure of your entire operation. Analysts need to appear authentically in online spaces to avoid detection from platforms' algorithms and other online users.

> **"Maintaining authenticity, persistence, and operational security is critical to today's online missions"**

The offensive capabilities of adversaries have grown with advancements in mobile technology. These operators can deploy spyware and surveillance tools to monitor communications, track movements, and pilfer sensitive data. Investigators need to have a solid understanding of adversarial tradecraft across mobile devices, and they must ensure that their mobile operations are indistinguishable from legitimate users.

When it comes to intelligence, defense, and enterprise missions, being mobile-first is a necessity to deal with the wide number of adversaries who use mobile platforms as their primary mode of operations. It is not enough to give the appearance of being a mobile user in digital spaces. Investigators require authentic mobile access that can persist across apps, geolocations, and devices without detection. While there are new challenges presented by mobile-first adversaries, there are solutions that can help investigators keep pace with the targets they're pursuing.



> **In a mobile-first world where technology is constantly evolving, Ntrepid enables mission success through authenticity and precision.**

Meeting the Needs of Investigators

In a mobile-first landscape, investigators require defensive and forensic solutions that match the sophistication of the environments they operate in. The Ntrepid Platform delivers this capability by providing authentic mobile access through physical smartphones, managed attribution, and cover-consistent device signatures. These capabilities ensure investigators can safely operate across mobile-only platforms, collect open-source intelligence, and defend against adversaries who increasingly exploit mobile operating system vulnerabilities and deploy spyware. With integrated forensic oversight and auditing, investigators gain not only secure access but also verifiable evidence handling that stands up to regulations and scrutiny.

Equally critical is the ability to scale and evolve at the pace of adversary innovation. Ntrepid equips investigators with a scalable, enterprise-ready platform that supports hundreds of devices, on-demand networks, and integrated workspaces, allowing teams to expand operations without sacrificing oversight or authenticity. Our AI-powered Attribution Intelligence keeps investigators ahead of automated detection systems, replicating authentic human behavior patterns while reducing cognitive load. This combination of scalable infrastructure, mobile-first access, and AI-driven automation ensures investigators remain mission-ready, capable of operating securely and effectively in a mobile-first environment increasingly defined by speed, scale, and technological sophistication.

Conclusion

The rise of mobile-first activity has permanently reshaped the digital landscape, creating both opportunity and complexity for investigators. As adversaries adapt their tactics across mobile ecosystems, maintaining authenticity, persistence, and operational security is critical. Ntrepid delivers these capabilities through a unified platform that combines authentic mobile access, mission-level managed attribution, and AI-driven automation. By providing investigators with real devices, scalable infrastructure, and integrated oversight, Ntrepid ensures secure, compliant, and credible operations in any online environment. In a mobile-first world where technology is constantly evolving, Ntrepid enables mission success through authenticity and precision.

Contact us to learn more about the full spectrum of Ntrepid solutions.

www.ntrepidcorp.com
1.800.921.2414
solutions@ntrepidcorp.com

NTREPID