

DISCOVERING EVIDENCE IN MOBILE INFORMATION

Make mobile part of your investigative process

There are now more active mobile devices on the planet than people. Nearly two-thirds of the world's population owns at least one mobile phone.

Smartphones and related IoT gadgets—smart watches, tablets, drones, GPS devices, cars, refrigerators, etc.—are increasing the amount and variety of data that investigators and legal professionals must consider as evidence.

More data sources for litigation, investigation, and regulatory matters means you need to spend more time indexing, extracting, and reviewing the information. You're also less likely to find the vital evidence in a single device.

For more information, visit www.nuix.com or call:

NORTH AMERICA

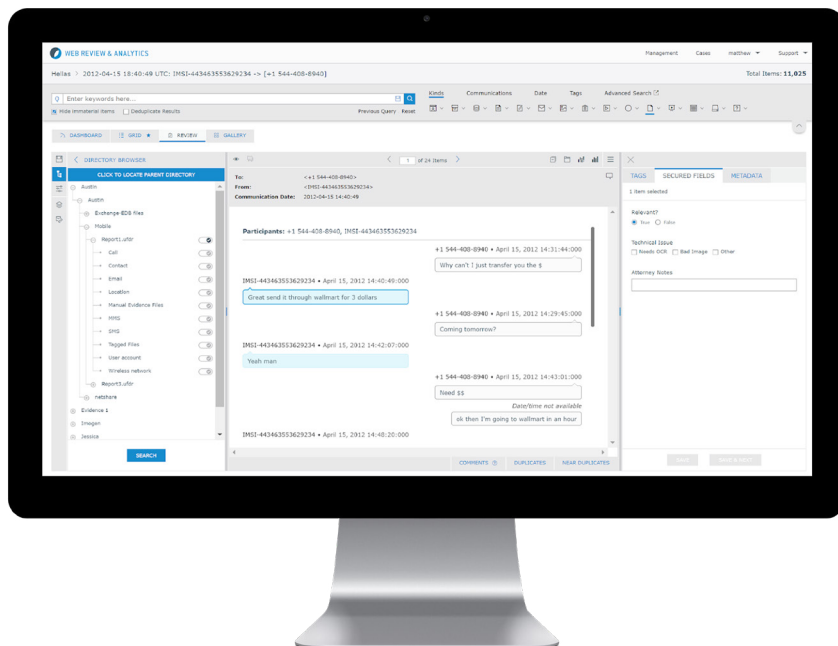
USA: +1 877 470 6849

EMEA

UK: +44 203 934 1600

APAC

Australia: +61 2 9280 0699



Simplified review display, intuitive data structure targeted data management

MANY DEVICES, ONE INVESTIGATIVE WINDOW

Luckily, Nuix simplifies your ability to find connections between multiple evidence sources and custodians. We give you a single window into call histories, email, messaging, and communication patterns across multiple mobile devices and other digital artifacts.

Our software captures data directly from mobile devices and their local or cloud backups. We turn raw data—text, images, video, audio, and metadata—into contextualized information for over 1,000 formats and source types.

Nuix' processing power and intuitive user interface allow you to review the data that supports your investigation. You can index, search, and analyze all the material at once, and tag and track items for review by other team members or external experts.



MAKE CONNECTIONS ACROSS MULTIPLE CUSTODIANS

Nuix makes evidence available to investigators, analysts, lawyers, risk managers, subject matter experts, and anyone else who needs it.

COLLABORATIVE INVESTIGATION

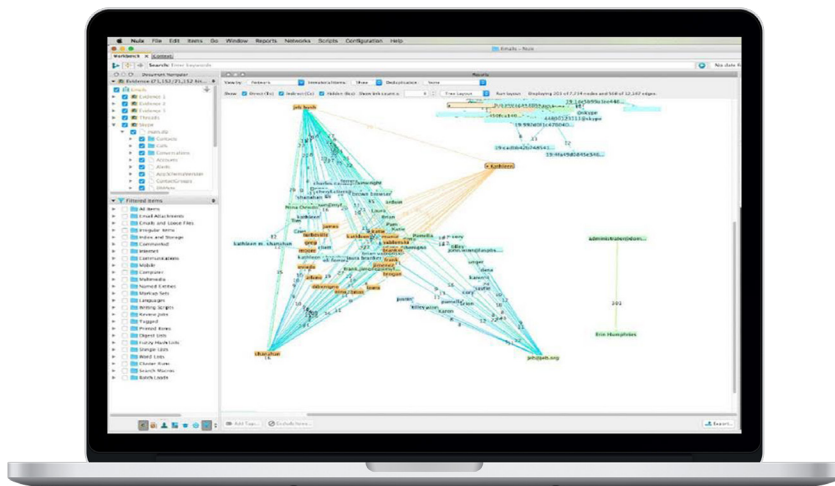
Using a web browser, team members can securely and conveniently collaborate throughout the investigation process, from early case assessment through intelligent analysis to review and production.

Configurable dashboards, search filters, metadata profiles, and review windows provide investigative insights.

ANALYTICS AND VISUALIZATION

With Nuix, you can visualize patterns within and across data sources, using powerful analytics to quickly identify key facts and uncover connections between people, objects, locations, and events.

Nuix provides powerful tools that map locations from photos, call records, fitness devices, GPS devices, and geolocation data extracted from IP addresses.



Analyze communication patterns across mobile devices, email, Skype, and more.

ABOUT NUIX

Nuix understands the DNA of data at enormous scale. Our software pinpoints the critical information organizations need to anticipate, detect, and act on cybersecurity, risk, and compliance threats. Our intuitive platform identifies hidden connections between people, objects, locations, and events – providing real-time clarity, control, and efficiency to uncover the key facts and their context. www.nuix.com.

NORTH AMERICA

USA: +1 877 470 6849

EMEA

UK: +44 203 934 1600

APAC

Australia: +61 2 9280 0699

EVERY 60 SECONDS:

448,800+ tweets

29 million WhatsApp messages

3.3 million Facebook posts

500+ hours of YouTube video

156+ million emails sent

65,000+ Instagram Photos

3.8 million Google searches

152.8 TB of data created

Sources: *What Happens Online in 60 Seconds, Things That Happen on Internet Every 60 Seconds, 10 Key Marketing Trends for 2017*

COLLECT MOBILE DATA

Nuix offers three ways to collect data from mobile devices:

- Creating logical images from live iOS and Android mobile devices
- Parsing mobile device backups stored on computer hard drives or in the cloud
- Importing mobile device forensic images from vendors including Cellebrite, MSAB, and Oxygen.

All three methods retrieve large volumes of relevant and responsive data. Having a variety of methods is especially critical as manufacturers respond to consumers' privacy concerns with encrypted and locked-down devices.