ONE WINDOW INTO THE EVIDENCE

Using Nuix Investigation Software and Specialist Tools to Create a Seamless Workflow

nuix

Simple. Powerful. Precise.

CONTENTS

EXECUTIVE SUMMARY

Digital forensic investigators are dealing with ever growing numbers of evidence sources with greater data volumes and in an increasing variety of formats. The traditional linear approach of imaging and analyzing each device separately and manually piecing together the results leads to cost blowouts and case backlogs. An emerging solution to this challenge is to anlayze all evidence sources within a single application.

However, no single application can handle the variety and complexity of anlaysis that some cases require. Many investigators have their preferred specialist tools to handle specific evidence types such as mobile devices, voice recordings, or large numbers of images.

This paper will explain how you can build an investigative lab around Nuix software and integrate our technology with third-party tools into an efficient workflow. Nuix software and the investigative lab methodology make it possible for you to parcel out evidence to specialist analysts or reviewers, then bring everything back together to anlayze, cross-reference, and report on.

This scalable, collaborative approach to investigation ensures you make the most efficient use of scarce resources and goes a long way toward reducing costs and backlogs.

Build an investigative lab around Nuix software and integrate our technology with third-party tools into an efficient workflow

GROWING COMPLEXITY OF DIGITAL EVIDENCE

A constant in the past decade has been the rapid growth of digital technology. Every day, new products and services are released that in some way change the shape of our daily lives. These technological changes have forced many industries to rethink, redesign, and reinvest. Digital forensics, more than many disciplines, has felt the impact of these forces. Yet it has been among the slowest to react.

An individual today could own 10 or more devices capable of generating and storing data that might be of interest to investigators

A decade ago, a typical search-and-seizure exercise would have involved a desktop computer and a mobile (dumb) phone for each suspect. Only a small number of early adopters used technologies such as smartphones, cloud email, social media, digital cameras, or MP3 players.

Today, these technologies are ubiquitous and the list continues to grow, including cloud applications and storage, smart watches and other wearable devices, smart TVs, tablet computers, drones, and portable or in-car GPS devices. An individual today could own 10 or more devices capable of generating and storing data that might be of interest to investigators.

Large-scale investigations, such as those into organized crime, multiply the degree of complexity. You need to understand and correlate data from multiple suspects, each with up to a dozen potential evidence sources. The “needle in a haystack” analogy seems inadequate to describe the difficulty of the task.

A further complicating factor is that the diversity of devices has led to a proliferation of specialist tools that work with particular types of data or evidence sources. Some focus on computer hard drives, others on mobile devices or network and cloud forensics.

Under these circumstances, how can you deal with so much data and so many evidence sources?

TRADITIONAL APPROACH LEADS TO COST AND BACKLOG PRESSURES

If you're a typical forensic technician, you might think the traditional approach is the best option. This linear methodology, outlined in Figure 1, involves taking a forensic image of each device, copying the images, analyzing their contents, and creating a report for each one. Case investigators then use the information in the reports to decide how to proceed.

This methodology is time-consuming and relies on human beings to make connections between large numbers of intelligence items across multiple evidence sources. They must manually correlate digital evidence sources with real-world people, objects, locations, and events. Introducing specialist tools adds another layer of complexity. You must copy data into these tools, perform operations using the tools' command lines or user interfaces, and then incorporate the extracted information back into the case.

On the other hand, the linear methodology has been proven over many years and validated by courts. Many investigative organizations have decided the safest approach is to find ways to make the traditional workflow as efficient as possible.

However, this approach simply cannot scale to meet the number and size of evidence sources involved in many investigations today. The process is constrained by factors including:

- The availability of forensic technicians
- The availability of computers and software licenses
- The speed of processing achievable using the hardware and software at hand
- The volume of storage required to archive forensic images until they're needed.

Investigative organizations must then juggle strict deadlines and growing backlogs of work. Low costs and quick wins become important factors in deciding which cases to pursue, rather than the importance or severity of the cases themselves.

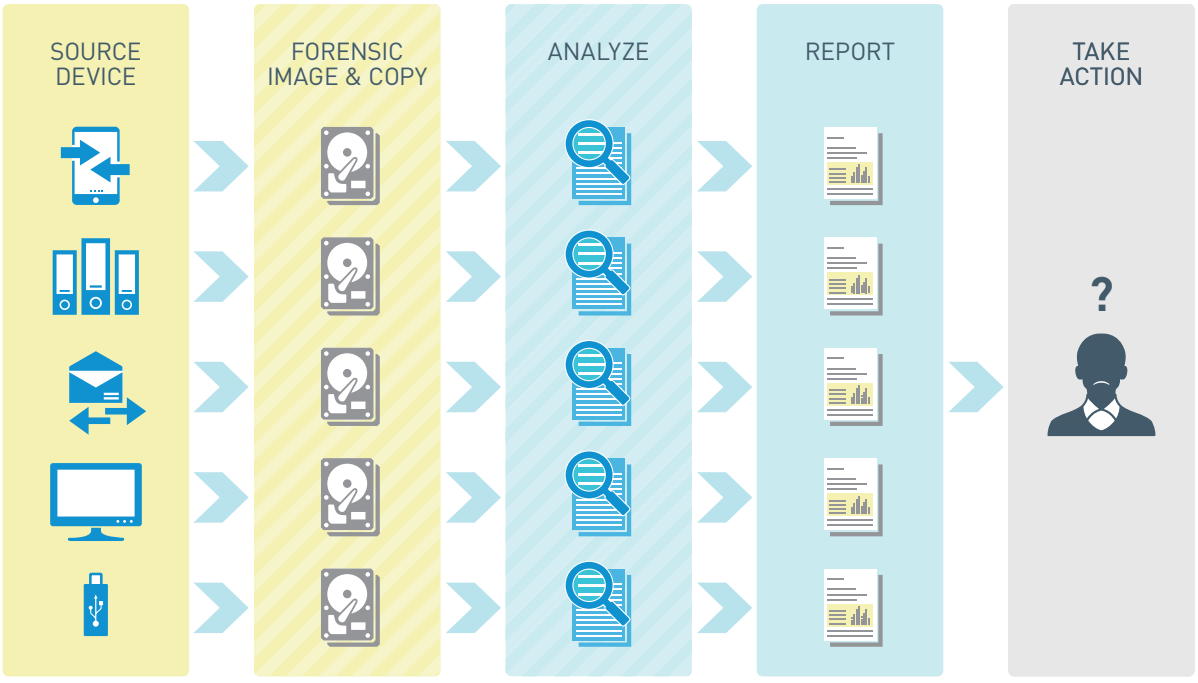

Figure 1: The traditional linear approach to digital forensic investigation.

A SINGLE WINDOW INTO THE EVIDENCE

The larger and more complex cases become, the greater the need for a more efficient investigative model. In previous white papers, we have detailed how investigators can anlayze all the evidence in one place, use the content of evidence sources to guide you to the key facts of the case, and set up an investigative lab that allows multiple investigators and subject matter experts to collaborate on digital evidence.

This method can bring together all evidence sources into a single platform for complete investigation—one window into the data

Using this methodology, as shown in Figure 2, you still follow best practice and forensically acquire each device independently. However, all analysis and reporting takes place within a single platform: Nuix. This allows you to compare and cross-reference intelligence across all evidence sources at once.

Using this method can bring together all evidence sources into a single platform for complete investigation—one window into the data. However, behind this window, you may still need the flexibility to draw on specialist solutions for different kinds of evidence.

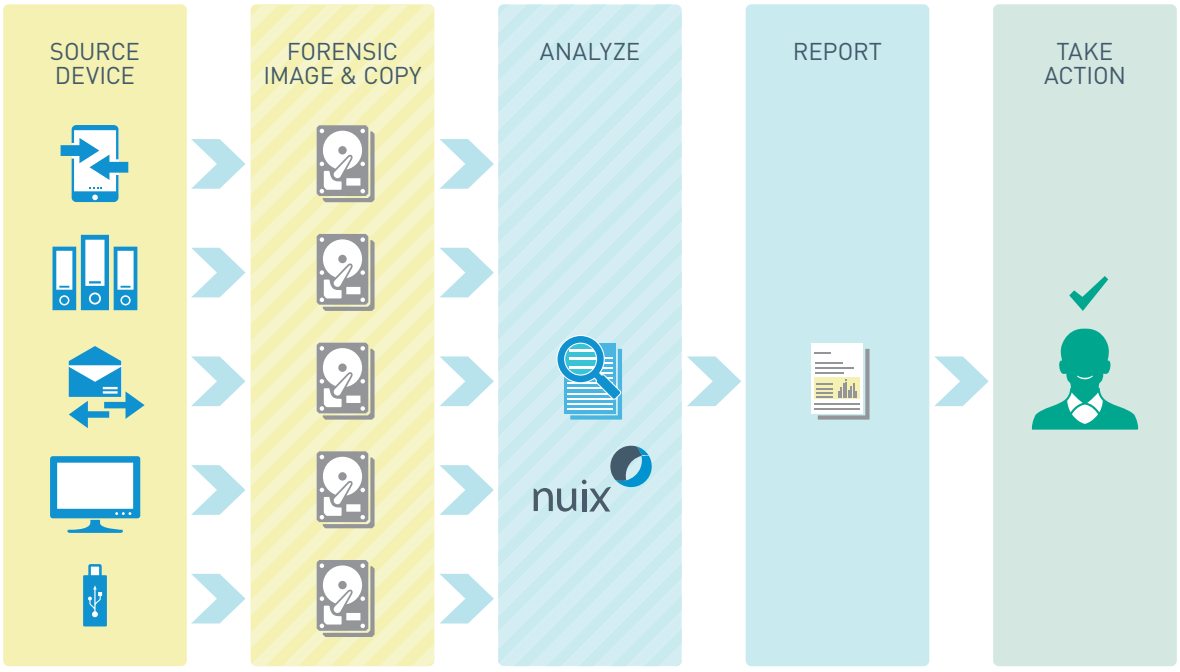

Figure 2: Analyzing digital evidence using Nuix.

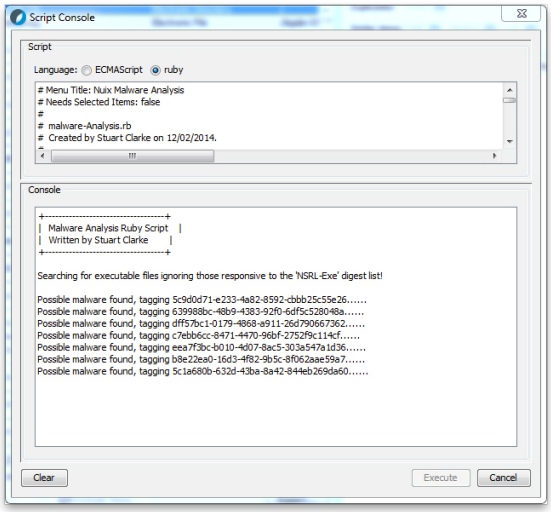

Figure 3: The Nuix scripting interface.

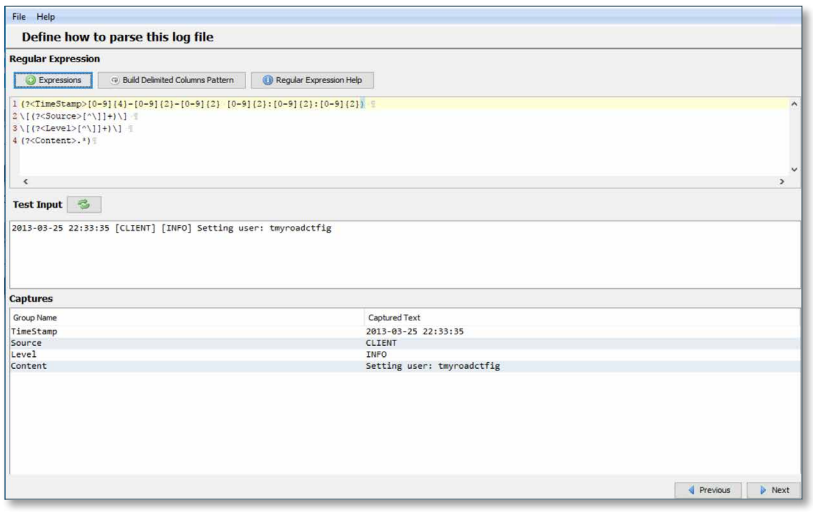

Figure 4: A script for parsing log files.

SCRIPTING, INTEGRATION AND APIs

Since 2009, Nuix has supported customers seeking to integrate its products into broader workflows with a scripting interface (see Figure 3). You can augment the functionality of Nuix Investigation & Response and Nuix Investigator Lab by running scripts to:

- Automate repetitive tasks such as creating multiple cases or subcases
- Apply processing and filtering tasks during data ingestion, for example:
  - Automatically running optical character recognition on items without text content
  - Applying keyword filters to log files to flag suspect log entries, such as those likely to contain SQL injection attacks, as soon as they're processed
- Extend the functionality of the Nuix interface, for example adding a utility that streamlines ingesting data from complex log file formats (see Figure 4)
- Send items, folders, or disk images to specialist external applications for additional processing and incorporate the results back into the Nuix case file.

Nuix provides scripts for many common tools and scenarios. You can also develop your own scripts using ECMAScript, Ruby, or Python.

Nuix works with technology partners such as ADF Solutions, Griffeye, MSAB and Voci to integrate their products at the back end.

Finally, Nuix offers application programming interfaces (APIs) to enable deeper integration between our platform and external tools:

- The **Nuix Engine API** is a collection of Nuix Engine capabilities that can be called from any Java application. It enables application developers to build robust applications directly on top of the Nuix Engine.
- The **Nuix RESTful API** exposes the essential elements of the Nuix Engine API through a simple remotely accessible interface.

You can augment the functionality of Nuix Investigation & Response and Nuix Investigator Lab by running scripts

INCORPORATING SPECIALIST TOOLS INTO THE WORKFLOW

Using Nuix's integration and scripting capabilities, you can build a seamless workflow that incorporates specialist tools as needed. This enables you to process and review masses of data with great speed and accuracy.

As well as reducing the number of irrelevant items you must search through, triaging evidence sources minimizes the volume of data your agency must retain

RAPID TRIAGE

For example, you could use ADF Solutions' Triage-G2, Triage-Examiner, or Triage-Responder applications to rapidly examine dozens or hundreds of evidence sources such as hard drives and flash memory devices (see Figure 5) and select only the most relevant exhibits. After processing this smaller, more responsive data set in Nuix, you can use the search results from the ADF tools as a starting point for deeper analysis, and quickly find the key evidence sources and facts. If the analysis in Nuix unearths additional search terms or custodians, you can rescan the previously eliminated evidence sources in ADF with this new intelligence.

As well as reducing the number of irrelevant items you must search through, triaging evidence sources minimizes the volume of data your organization must retain in archive until it is required by courts or other sources.

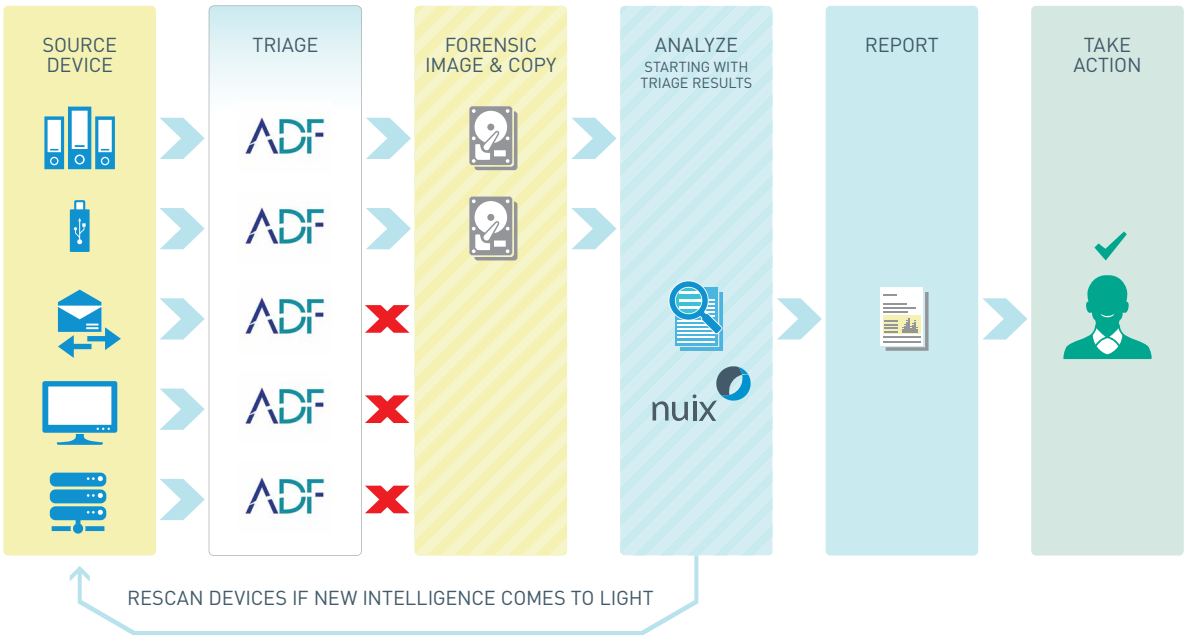

Figure 5: Using ADF Solutions to triage data sources.

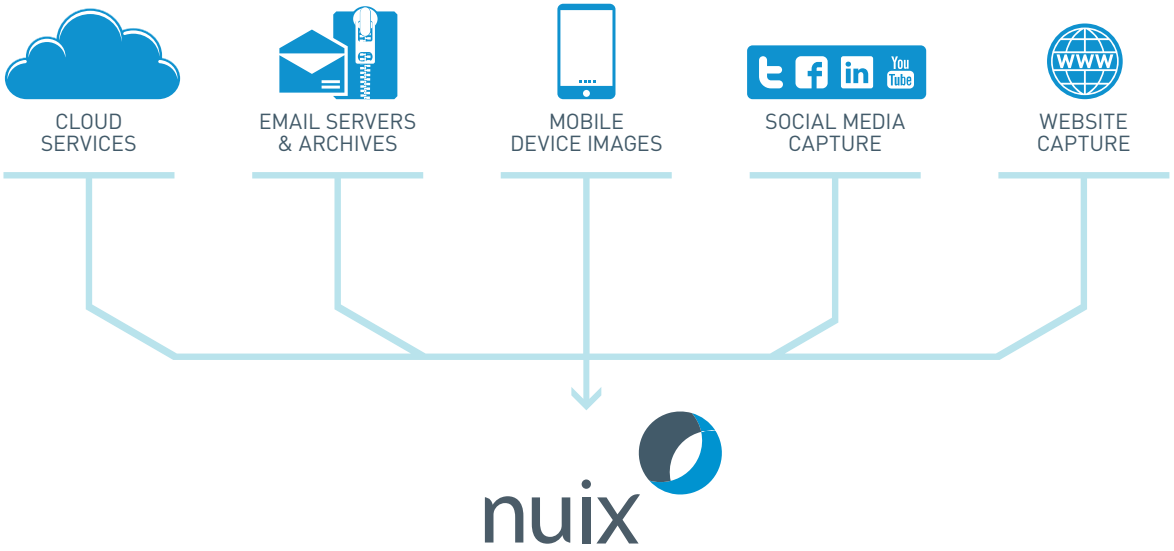

Figure 6: Using Nuix and third-party applications to process a wide variety of data sources.

INVESTIGATING MORE FILE AND DATA FORMATS

Using Nuix as the central interface for an investigation also enables you to work with many more types of data (see Figure 6).

For example, Nuix can collect data from many evidence sources that other tools can't, such as:

- Cloud storage including Amazon S3, Dropbox, Google Drive, and iCloud
- Cloud email including Gmail and Microsoft Office 365
- Microsoft Exchange Server and IBM Lotus Notes, other email servers, and all common email applications
- EMC EmailXtender and SourceOne, Veritas Enterprise Vault, and other email archives
- Enterprise content management systems including Microsoft SharePoint and EMC Documentum
- Mobile devices
- Loose files, folders, and hard drives
- All common forensic images and containers.

Using scripts, Nuix can import data from specialist tools such as website and social media capture applications (Figure 7).

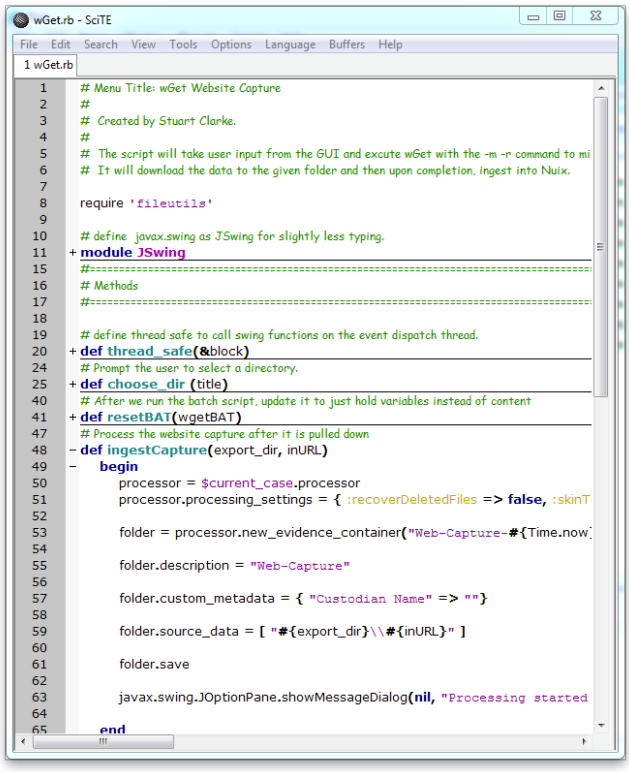

Figure 7: A website capture script.

ANALYZING MOBILE DEVICES AND COMMUNICATION PATTERNS

Mobile devices are a prime source of digital evidence—in many investigations, mobile phones and other portable devices now outnumber traditional PCs by as many as five to one.

From version 7.4 (released August 2017), Nuix can perform "logical" (non-forensic) extractions of data from popular mobile devices, as well as computer- and cloud-stored backups of these devices. For cases requiring more rigorous examination, Nuix can directly import mobile device images created by MSAB, Oxygen Forensic, and other forensic extraction tools.

This allows you to examine the contents of multiple mobile devices alongside evidence from laptops, desktops, file shares, email, archives, cloud services, and hard drive forensic images. Nuix automatically identifies and cross-references key intelligence items such as company names, sums of money, email addresses, IP addresses, locations, phone numbers, and communication activity across all evidence sources. You can recreate timelines, communication networks and maps of activity across many devices belonging to multiple suspects.

SPECIALIST APPLICATIONS

Using pre-built or custom-made scripts, you can select items or even entire disk images from within Nuix investigation software to send to external applications for deeper analysis (see Figure 8). With the results returned from these tools, scripts can:

- Add new items to a Nuix database
- Update the text or content of existing items, for example including decrypted text of encrypted items
- Tag items
- Add custom metadata to items
- Perform additional specialist analysis of specific system files
- Overlay results and intelligence from products such as ADF.

Using the investigative lab methodology detailed in a previous Nuix white paper, you can divide these tasks among specialists and subject matter experts to work concurrently, maximizing the use of available resources.

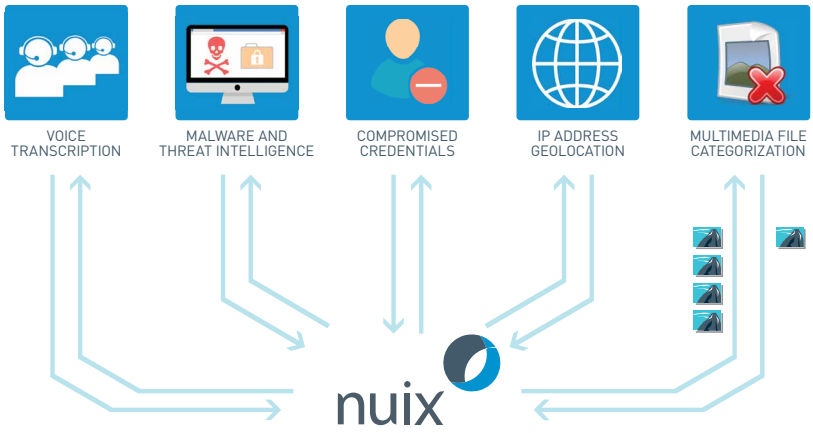

Figure 8:Sending selected data to third-party applications for deep analysis.

Using pre-built or custom-made scripts, you can select items or even entire disk images from within Nuix investigation software

Specialist application examples include:

- Converting voice recordings into transcribed text using Nuix Voice powered by Voci or other speech recognition technologies
- Analyzing suspect files using YARA signatures or sites such as VirusTotal to detect the presence of known malware
- Sending names and email addresses to data breach lists such as Have I Been Pwned? to determine if those credentials are known to have been compromised
- Converting IP addresses into geographical locations
- Sending multimedia files for analysis and comparison against lists of known child abuse images (see "Image analysis for child abuse investigations on page 11").

Figure 9: Streamlined workflow for extracting, analyzing, and categorizing multimedia files and forensically examining their sources using Nuix and Griffeye AnayzeDI.

IMAGE ANALYSIS FOR CHILD ABUSE INVESTIGATIONS

One such specialist application is Griffeye AnalyzeDI, an application designed to simplify investigations involving digital media. Nuix and Griffeye have integrated their products and developed a streamlined workflow for extracting, categorizing, and forensically examining large numbers of images in child abuse investigations. With this workflow (see Figure 9), you can:

- Extract multimedia files from seized evidence sources using Nuix tools
- Eliminate known files by comparing the extracted material to hash sets of existing digital media, such as the Project VIC and CAID databases of child abuse material
- Export unknown files into NetClean Analyze DI, then anlayze, categorize, and tag them
- Export the images back into Nuix along with their tags
- Deeply examine selected evidence sources for clues about the identity and location of victims and perpetrators
- Generate reports and present the evidence to relevant authorities.

WHAT COULD YOU DO WITH ONE WINDOW INTO THE EVIDENCE?

Investigators must deal with a large number and great variety of digital evidence sources. In the age of big data, the only approach that can address growing investigation costs and case backlogs is to provide a unified and flexible framework through which you can understand all the evidence in one place.

Nuix investigation technology delivers a single window to view, anlayze, cross-reference, and collaborate on this evidence. It can collect, process, and anlayze terabytes of data per day. It provides scripting and integration with third-party tools to give investigators the flexibility and functionality you need.

Nuix can bring together the silos of expertise within an investigative team and ensure you fully utilize all resources toward the goal of solving more cases, more efficiently.

ABOUT THE AUTHOR

STUART CLARKE

Chief Technology Officer—Cybersecurity, Nuix

Stuart is an internationally respected information security expert who is responsible for the overall security and intelligence strategy and delivery at Nuix. During his time at the company, Stuart has advised the United Nations' peak cybersecurity body ITU and provided cybersecurity training for over 60 computer emergency response teams. He led the development of Nuix Investigation & Response, an innovative investigative tool used to delve into the causes and scope of data breaches. He also currently leads the development of Nuix Insight Analytics & Intelligence, a powerful security intelligence platform.

To find out more about Nuix investigation software please visit

nuix.com/investigation

ABOUT NUIX

Nuix protects, informs, and empowers society in the knowledge age. Leading organizations around the world turn to Nuix when they need fast, accurate answers for investigation, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges.

North America
USA: +1 877 470 6849
» Email: sales@nuix.com

EMEA
UK: +44 203 786 3160
» Web: nuix.com

APAC
Australia: +61 2 9280 0699
» Twitter: @nuix

INV1707US1