SUMURI

ENDLESS INNOVATIONS

SUMURI.COM

SUMURI

ABOUT SUMURI

SUMURI is an award winning digital forensics company located in the state of Delaware within the United States.

SUMURI began serving the forensics community in July 2010 when it was founded by Steve Whalen, who is a Certified Forensic Computer Examiner and a retired State Trooper, and his wife Ailyn. SUMURI is known for developing innovative and forward thinking forensic software and hardware along with providing expert forensic training and services.

SUMURI's core values consist of honor, integrity, loyalty, positive attitude, dedication and most importantly, altruism; the desire to help, serve and care for others first before yourself.

We believe that our core values along with our expertise is what has driven SUMURI's success. Our team consists of experts who are known worldwide for their continued contributions to the digital forensic community.

RECON *ITR*
IMAGE TRIAGE REPORT

SUMURI

The Leading macOS Imaging, Triaging, and Reporting Solution

RECON *ITR* is a one-of-a-kind solution that acquires and processes Intel and Apple Silicon Macs like no other tool on the market. This marvel of forensic innovation is built from the ground up on macOS using Mac's full power instead of fighting against it.

RECON *ITR* requires no reverse engineering and is not ported from other operating systems, which means more data and more accurate results.

SUMURI has designed RECON *ITR* with the customer in mind, ensuring examiners have the most versatile tool available when changes occur to Apple hardware or Mac operating systems. RECON *ITR* accomplishes this and much more by including unique and revolutionary features while keeping the price significantly lower than competitors.

- Includes Three Imaging Solutions Suited for Any Case (LIVE and Bootable)
- Supports Intel and Apple Silicon M1 and M2 Processors
- Only True Triage Solution for Live Running Macs or Macs Connected in Target Disk Mode
- Contains Full Report Capabilities with Sequential Processing of Proper macOS Timestamps
- Correctly Uses Apple Extended Metadata with macOS Native Libraries
- Automatically Collects Volatile Data
- Ability to Automatically Triage Boot Camp and iOS Backups
- Includes PALADIN PRO for Windows and Linux Support

RECON ITR
IMAGE TRIAGE REPORT

THREE IMAGING SOLUTIONS FOR THE PRICE OF ONE

With the advent of new technologies like Apple Silicon that are continuously changing, some situations allow for a bootable solution, some call for targeted acquisition, and some may even require a live acquisition. RECON ITR includes both a Live and Bootable imager to ensure that you are ready for every situation.

Every purchase of RECON ITR includes two state of the art SAMSUNG drives:

- Samsung T7 SSD with Live and bootable versions RECON ITR for live triage, and reporting, along with both physical and logical imaging options

- SAMSUNG USB with PALADIN PRO with built-in CARBON (demo available) for Windows and Linux support

Support for Intel and Apple Silicon Processors

The Mac environment has undergone another massive shift in processors, moving from the long-used Intel processors to an ARM-based Silicon processor. RECON ITR now supports both Intel and Apple Silicon processors to cover almost any situation you may encounter when imaging a Mac!

The Only True macOS Triage Solution

RECON ITR is the only solution to truly have the ability to provide answers in seconds with its revolutionary triaging feature in a single tool at no extra cost. It automatically parses important information from both live systems and through Target Disk Mode within minutes. Other solutions require you to purchase more tools and take longer to get answers.

FULL REPORT CAPABILITIES

To compliment true macOS triage, RECON ITR has built-in reporting features that allow you to produce professional reports in seconds. Build comprehensive reports using the Global Search and Global Timeline to locate and bookmark only the most critical data and quickly present information in an understandable format with Sequential Processing of proper macOS timestamps.

CORRECT USE OF APPLE EXTENDED METADATA

RECON ITR was built from the ground up on macOS to ensure that RECON ITR supports proprietary metadata used in the Mac environment. Being native to macOS helps ensure that our tool can correctly identify and preserve the Apple Extended Metadata that other tools do not properly integrate.

ABILITY TO TRIAGE BOOT CAMP AND IOS BACKUPS

Like RECON LAB, RECON ITR supports more than just Mac data. RECON ITR has robust support for triaging Boot Camp partitions and iOS Backups.

INCLUDES PALADIN FOR WINDOWS AND LINUX SUPPORT

PALADIN PRO, a full forensic lab with over 150 forensic tools, is now included with all new orders of RECON ITR to image Windows, Linux, and all Intel Macs without having to erase and reinstall your software. PALADIN PRO customers can also try CARBON which is preinstalled for examiners who would like to purchase a license.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

RECON LAB
FORENSIC SUITE

SUMURI

Reputation is everything.
We help you keep it.

RECON LAB is SUMURI's flagship forensic analysis suite designed from the ground up on macOS to utilize Mac's power and give examiners access to an entirely new realm of data. RECON LAB takes traditional computer forensics and revitalizes it to be more in line with 21st century technologies through many unique and revolutionary features using native macOS libraries, sequential processing into both analysis and reporting, fully automated processing of many different operating systems, and much more.

SUMURI designed RECON LAB with every type of examiner in mind. Our three-stage approach to analysis makes sure that brand new examiners and seasoned veterans alike can get accurate results fast. Step One is automated analysis that supports the automated parsing of thousands of artifacts from macOS, Windows, iOS, Android, and Google Takeout. Step Two is semi-automated analysis using our advanced forensic viewers that assist in parsing and examining macOS Property Lists, SQLite Databases, Windows Registry and Raw Data. Step Three includes Sequential Processing and WYSIWYG reporting features through the use of StoryBoard reporting. Hundreds of revolutionary features built into RECON LAB makes manual analysis easier.

- Native to macOS
- Correctly Uses Apple Extended Attributes and Apple Timestamps with macOS Native Libraries
- Automated Analysis of macOS, Windows, iOS, Android, and Google Takeout
- Sequential Processing (Timeline Analysis)
- StoryBoard - First of its Kind WYSIWYG Forensic Reports

SUMURI.COM

RECON LAB
FORENSIC SUITE

NATIVE TO macOS

RECON LAB is developed natively on macOS and utilizes native Mac libraries to offer the most accurate representation of acquired data. These native features allow RECON LAB to display Apple Extended Attribute data with the proper macOS Timestamps missed by other forensic tools. Being designed on macOS allows RECON LAB to include a unique Hybrid Processing Engine, enabling images to be mounted and processed faster than other tools. Combining these attributes and our automated analysis functions creates one of the world's most powerful forensics suite.

CORRECT USE OF APPLE EXTENDED ATTRIBUTES

RECON LAB stands alone to integrate and support Apple Extended Attributes and proper macOS Timestamps fully. This unique and Mac-native form of metadata supports hundreds of extended attributes that can completely change a case's outcome and provide unparalleled information to examiners. Other forensic tools overlook this data, while RECON LAB makes these an essential part of the tool. RECON LAB utilizes Apple Extended Metadata, POSIX, and application-specific timestamps to give examiners as much information as possible.

AUTOMATED ANALYSIS OF macOS, WINDOWS, iOS, ANDROID, AND GOOGLE TAKEOUT

RECON LAB automates the analysis of thousands of supported artifacts, spanning macOS, Windows, iOS, Android, and Google Takeout! Simply by loading a forensic image, folder, or backup and selecting the plugin will pull all associated data and present it in an easy-to-understand format.

SEQUENTIAL PROCESSING (TIMELINE ANALYSIS)

RECON LAB features two unique ways to display information sequentially with Super Timeline and Artifact Timelines. Super Timeline generates global level timelines in a CSV or SQLite database to show all events as they transpired. Meanwhile, the Artifact Timeline visually represents events based on the timestamps collected through automated analysis. Both can provide a way to present the collected data visually to significantly reinforce case opinions.

STORYBOARD

RECON LAB's revolutionary reporting feature, StoryBoard, features many innovations to automate and enhance the reporting process. StoryBoard includes features to add bookmarked files in chronological order and include external files to help make the report more coherent. RECON LAB includes the first of its kind revolutionary WYSIWYG forensic report editor - StoryBoard. With StoryBoard's report editor, examiners can fully customize and tailor their reports to provide the most comprehensive, user-friendly, and coherent reporting experience of any tool on the market.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

PALADIN

SUMURI

The World's most Popular Linux Forensic Suite

PALADIN, SUMURI's bootable Linux distribution, was created as an opportunity to give back to the forensics community.

Offered as donationware for law enforcement, PALADIN includes over 100 pre-compiled open-source tools and our PALADIN Toolbox. The PALADIN Toolbox features imaging, hashing, image conversion, selective logical imaging, imaging of unallocated space, and automatic write blocking. PALADIN has been court-tested and is used by thousands of forensics examiners around the globe.

- PALADIN Toolbox
- Includes Over 100 Pre-Compiled Open-Source Forensic Tools
- Support for BitLocker Decryption
- Built-in Autopsy
- Imaging Across a Network
- Built-in CARBON

PALADIN

FORENSICS SIMPLIFIED

A PALADIN FOR EVERYONE

PALADIN comes in several different versions to support a variety of different hardware. PALADIN LTS (Long Term Support) is more robust, including BitLocker decryption, pre-compiled open-source forensic tools, and Autopsy built-in. PALADIN EDGE features only the PALADIN Toolbox is typically built on newer Ubuntu kernels to support newer hardware. PALADIN EDGE is available in both 64-bit and 32-bit versions.

PALADIN TOOLBOX

Every version of PALADIN features the revolutionary PALADIN Toolbox. The PALADIN Toolbox includes an imager that supports all major imaging formats such as DD, E01, Ex01, DMG, and VHD. Some of the other key features include image converter, triage, selective logical imaging, and imaging to a network share!

OPEN-SOURCE FORENSIC TOOLS

PALADIN LTS features over a hundred pre-compiled open-source forensic tools. These tools range from AFF support, hashing tools, malware analysis, password discovery, and many more.

BITLOCKER DECRYPTION

Boot, decrypt, and logically image BitLocker partitions with PALADIN Toolbox. PALADIN has full support for the decryption of partitions encrypted using the home version of Windows BitLocker.

BUILT-IN AUTOPSY

PALADIN includes SleuthKit and the Autopsy's forensic suite in PALADIN LTS, further attributing to PALADIN's nickname of the "Forensic Swiss Army Knife."

IMAGING ACROSS A NETWORK

Run out of destination drives? No problem; PALADIN can image straight to a network storage solution like a server or NAS with ease through PALADIN's Network Share feature! PALADIN utilizes SAMBA (Windows Share) or NFS Share to add network-attached storage as a destination.

BUILT-IN CARBON

PALADIN PRO now includes CARBON pre-installed for examiners who would like to buy a license! CARBON is our flagship virtualization software that is able to virtualize any Windows machine without the need for a password. CARBON also includes triage, file carving, differential analysis, and much more. Users who have made their own PALADIN will have the chance to demo CARBON free of charge.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

CARBON

SUMURI

Instant Virtualization is here!
No imaging, No disassembly!

CARBON is SUMURI's premier tool for virtualization with support for almost any Windows system or forensic image.

CARBON allows examiners to see evidence as the user, bypass passwords with the push of a button, and boot into a forensically sound virtual environment avoiding the need for disassembly. Make reports more straightforward and easy to understand by including screenshots and screen recordings form the virtualized environment. Get actionable information and generate professional reports in minutes with RECON for Windows. CARBON includes automated triaging and reporting to allow you to triage Windows machines and images with ease. Advanced data carving capabilities lets you use signature analysis to carve files in unallocated space in Windows machines and images.

- Instant Virtualization of Windows Computers and Forensic Images
- BitLocker Support
- RECON for Windows: Triage Capabilities
- Advanced File Search
- Advanced Data Carving
- Snapshot Differential Analysis
- PALADIN Toolbox - Imagers and Write-Blocking Included
- Now merged with PALADIN!

CARBON

VIRTUAL FORENSIC SUITE

INSTANT VIRTUALIZATION OF WINDOWS COMPUTERS AND FORENSIC IMAGES

CARBON has the ability to virtualize any Windows-based computer without the user's password in seconds. Boot forensics images of Windows machines to analyze them in a native environment. Virtualizing with CARBON lets the examiner see and document the computer in the exact state that the original user saw it without making any changes to the source device.

BITLOCKER SUPPORT

CARBON can virtualize Windows machines that are BitLocker encrypted with ease! Enter the recovery key upon booting the device, and within seconds, you will be logged into the user's account! Combining this with our unique ability to bypass Windows passwords allows CARBON to virtualize virtually any computer.

RECON FOR WINDOWS: TRIAGE CAPABILITIES

Examiners can instantly triage any Windows machine or forensic image using the included RECON for Windows. It also includes a reporting feature to easily generate professional reports within minutes.

ADVANCED FILE SEARCH

CARBON's Advanced File Search allows examiners to locate specific files by searching for file names, keywords, file signatures, and even custom defined file signatures.

ADVANCED DATA CARVING

Advanced File Carving allows examiners to recover hundreds of different file types in unallocated space and complete space using a built-in signature database for easy carving options as well as creating customizable signature sets.

SNAPSHOT DIFFERENTIAL ANALYSIS

SnapCompare lets examiners inspect a system for modification or tampering by comparing two Windows machine snapshots to assist with incident response and Malware investigations.

PALADIN TOOLBOX - IMAGERS AND WRITE-BLOCKING INCLUDED

PALADIN Toolbox is included for all your imaging and write-blocking needs! Images created in the PALADIN Toolbox can later be virtualized within CARBON!

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

TALINO

SUMURI

Server Solution

Forensics Workstations

eDiscovery Workstations

NUIX Workstations

Cryptanalysis

TALINO KA-L ALPHA

TALINO KA-L GAMMA

RUGGEDIZED LAPTOP

TALINO KA-L OMEGA

TALINO KA-L eDiscovery

THE POWER AND VERSATILITY OF TALINO - ACCEPT NO SUBSTITUTES

Here at SUMURI we take the greatest pride in building the very best forensic workstations anywhere. All of our TALINOs are designed by Certified Forensic Computer Examiners because we believe that the person who best understands what the modern examiner needs is someone who knows forensics! Using our unique and proprietary chassis, we accomplish three major goals:

1.) Separate the electrically sensitive components from those that produce more Electro Magnetic Interference (EMI).

2.) Since the entire chassis is made of aluminum, we can utilize its entire surface area to help spread and dissipate heat.

3.) Our proprietary chassis grid system allows for the attachment of 3D printed accessories which can be downloaded for free from our website.

All of these features ensures your TALINO runs as smoothly as possible, is extremely versatile, and long lasting.

We use only the highest quality components that have been tested and vetted here in our lab. Our Laptops are designed and optimized for forensics and come with an industry leading three-year warranty.

Every all TALINO workstations and laptops are built based on your unique requirements and to our exacting standards. No competitor offers ANYTHING close!

72h

Every TALINO workstation is burned in for 72 hours using multiple stress testing and benchmarking tools. The goal of our quality assurance team is to try and “break” the workstation before shipping it. From logical stress tests to actually physically altering the airflow in the TALINO we do everything in our power to make sure no TALINO leaves the lab until it has been put through the wringer. This is backed by our industry leading three-year warranty and lifetime access to our support line for every TALINO user. Day or night we are there when you need us.

FORENSIC LAPTOPS

TALINO KA-L ALPHA
The SUMURI TALINO KA-L Alpha is an extremely portable Forensic Workstation specifically designed to perform faster than most desktop forensic workstations. We introduced this system for several reasons as many agencies just need a really good laptop that they can depend on to process small cases, work out in the field, collect mobile phone data, or a variety of other tasks.

TALINO KA-L GAMMA
The SUMURI TALINO KA-L Gamma is a portable Forensic Workstation specifically designed to perform just as fast as other desktop forensic workstations. This system was created to meet the needs of agencies who've both come to expect the speed and power from our renowned portable TALINO Forensic Workstations, and are looking for a middle ground between our other portable offerings.

TALINO KA-L OMEGA
The SUMURI TALINO KA-L Omega is the fastest portable Forensic Workstation specifically designed to perform just as fast as most desktop forensic workstations. In fact, this powerhouse might actually be more powerful than your current forensic workstation, unless you have a full sized TALINO desktop Forensic Workstation.

TALINO KA-L eDISCOVERY
The SUMURI TALINO KA-L eDiscovery & Incident Response laptop is our high-end eDiscovery incident response laptop aimed specifically for the modern-day forensic examiner tasked with handling incident response type examinations.

RUGGEDIZED LAPTOP
The SUMURI TALINO TRL-65 is our no compromise ruggedized laptop. When you need both dust proofing and water resistance in one package along with as little sacrifice as possible when it comes to performance, the TRL-65 is your very best choice! It features a whopping six-foot drop protection, and like all TALINOs, there are tons of customization options and you will find the same awesome three year warranty you've come to know and love.

TALINO WORKSTATIONS

CRYPTANALYSIS WORKSTATION
An extremely fast and efficient decryption system featuring Intel CPUs and NVIDIA graphics cards combined with our proprietary 3mm aluminum heat dispersing chassis. All the horsepower you need to run Passware, Elcomsoft, or any other cryptanalysis solution.

FORENSIC WORKSTATION
The SUMURI TALINO KA brand of computers is built on the most reliable and stable platform designed by Certified Forensic Computer Examiners. Each custom workstation is built with expandability and a future proof mindset so that you are not replacing the computer every few years with an entirely new computer.

eDISCOVERY WORKSTATION
The SUMURI TALINO KA eDiscovery brand of computers is built on the same, CFCE designed, trusted platform as our TALINO KA workstations. Each eDiscovery workstation is built with the flexibility to handle any eDiscovery casework. From preservation to spoliation, we have you covered.

NUIX POWERED WORKSTATION
The SUMURI TALINO NUIX Forensic Workstation is our specialized high-end dual Intel CPU system. This system was designed by our certified forensic computer examiners and NUIX engineers specifically to run NUIX. The power of TALINO married to the strength of NUIX is a match made in heaven.

TALINO SERVERS

SERVER SOLUTION

The SUMURI TALINO KA Server Solution family brings everything great about TALINO KA workstations to server form factor computing in the big data arena, all designed by Certified Forensic Computer Examiners. Whether you're looking to store several hundred Terabytes for your lab or you need Petabytes for body camera footage we've got you covered. With multiple processing nodes available, our designers can build you the server that you need at a price you can't beat.

ABOUT SUMURI

SUMURI is a leading worldwide provider of solutions for digital evidence and computer forensic Training, Hardware, Software, and Services. SUMURI is also the developer of the industry standard PALADIN Forensic Suite, CARBON Virtual Forensic Suite, RECON *ITR*, RECON LAB, and TALINO Forensic Workstations.

sales@sumuri.com
+1 302.570.0015

Our Mailing Address:
P.O. Box 121 Magnolia,
DE 19962, USA

SUMURI TRAINING

When you have taken both of our MFSC courses, you are eligible to take the Certified Forensic Mac Examiner certification process at no charge.
The CFME is the only truly vendor-neutral Mac Forensic certification available and can be used to assist you in qualifying as an expert for any Mac investigation.

MFSC 101 TRAINING

Best Practices in Macintosh Forensics

Provides detailed instruction on the process of examining a Macintosh computer from the first step to last step in logical order.

MFSC 201 TRAINING

Advanced Practices in Mac Forensics

Takes the students into in-depth analysis techniques, which provides the students the ability to apply what they have learned in real world cases.

SUMURI PROFESSIONAL SERVICES

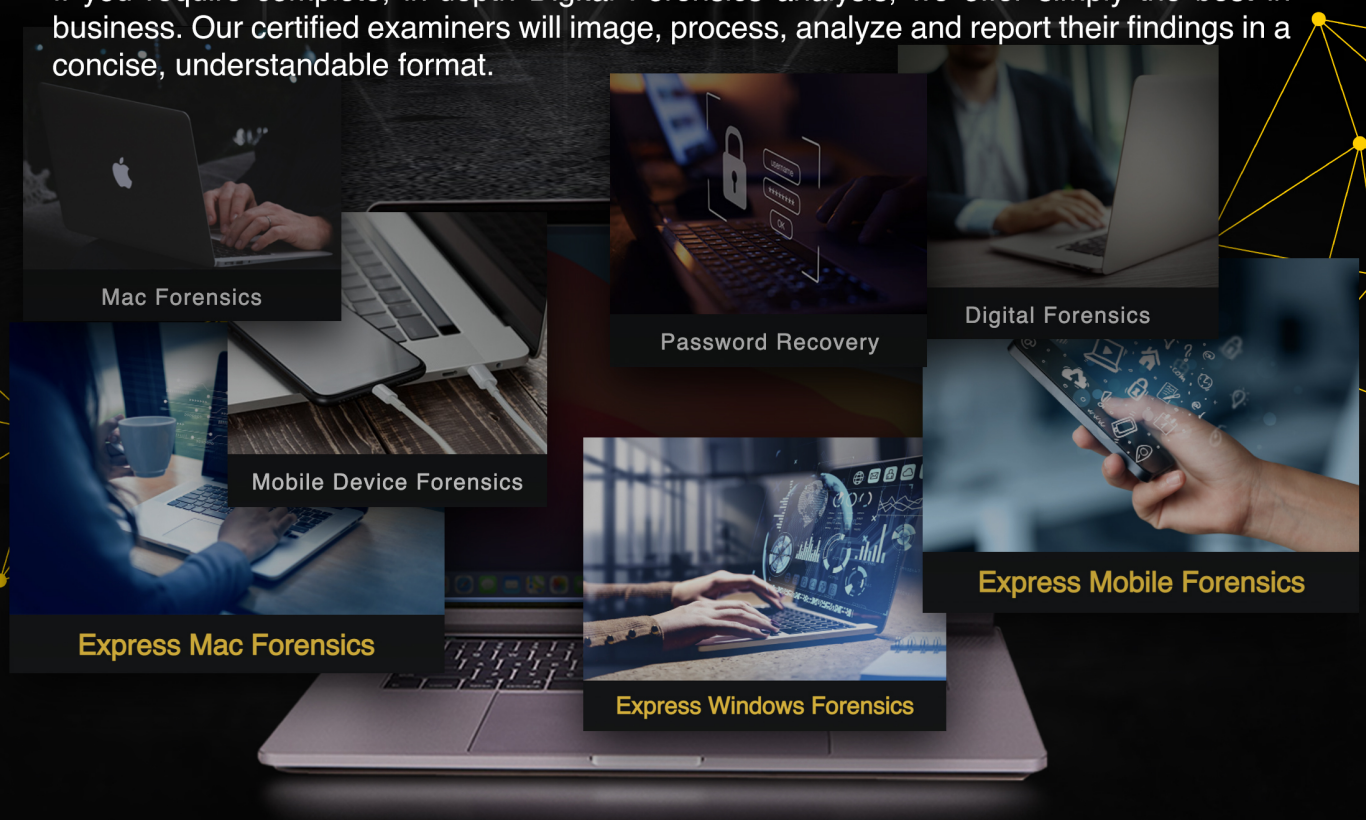
SUMURI Digital Forensic Services is known worldwide as a leader in Macintosh, Windows, and Mobile Forensics. Our DFIR team members are Certified Computer Forensic Examiners and have vast experience in imaging, analysis, and reporting.

Our DFIR consultants not only cover the United States but also Canada, Asia, Europe, the UK, and the Arabian Peninsula. We also partner with established Professional Services companies to provide even more extensive client services.

SUMURI offers two categories of Digital Forensic Services; Express, and Full.

Our Express Forensics offerings provide a cost-effective solution to your Digital Forensics needs when a complete, in-depth, and potentially expensive analysis is not required. Express Forensics is a wise choice if you need data showing device usage such as messaging, internet activity, account information, or application use. The data we can provide will assist you in your case or determine if you actually have a case.

If you require complete, in-depth Digital Forensics analysis, we offer simply the best in business. Our certified examiners will image, process, analyze and report their findings in a concise, understandable format.



SUMURI.COM

SHOP CATEGORIES

Browse through our One-Stop-Shop and make your forensic tools shopping experience more convenient. All Endless Innovation products in this catalogue and much, much more can be found at our shop online at www.sumuri.com/shop.

SUMURI.COM

SUMURI

Contact Information

 helpdesk.sumuri.com

 hello@sumuri.com

 +1 302.570.0015

 www.sumuri.com

Follow us on social media

 /company/SUMURI

 @SUMURIForensics

 @SUMURIForensics

 @SUMURIForensics

SUMURI LLC

P.O. BOX 121

MAGNOLIA, DELAWARE 19962, USA

SUMURI.COM