200th ISSUE

DIGITAL VOICE STRESS ANALYSIS
A Modern Alternative to Polygraph Testing

MINIMIZING BIAS IN INVESTIGATIONS
Sequential Unmasking and Linear Sequential Unmasking

URBAN VS. RURAL SURVEILLANCE
A Field Guide for Seasoned Private Investigators

LESSONS FROM COLD CASE INVESTIGATIONS
Why the Smallest Clues Still Matter

DEPARTMENTS

IN EVERY ISSUE

The Unsung Heroes of Digital Forensics:
The Forensic Workstation

BY **ROBERT B. FRIED**, SENIOR VICE PRESIDENT & GLOBAL HEAD OF INVESTIGATIONS, SANDLINE GLOBAL AND
MANNY KRESSEL, CEO & FOUNDER OF BITMINDZ FORENSIC SOLUTIONS

I n our everyday lives, tools enable us to function efficiently. For example, toothpaste applies to our teeth with a toothbrush; a comb is used to untangle our hair. These tools are so seamlessly integrated into our daily routines that we rarely consider their importance. When thinking about tools in the highly specialized world of digital forensics, there's one tool that stands quietly at the center of digital forensic investigations: the forensic workstation.

Behind every skilled digital forensic practitioner stands one of these powerful systems—custom built to perform precisely, reliably, and securely.

A COMPUTER WITH PURPOSE

A forensic workstation is far from an off-the-shelf computer. It is purpose-built, and designed to ingest, process, and analyze immense volumes of digital evidence—frequently measured in terabytes. Engineers build these systems to handle the intensity and complexity of today's digital forensic investigations. For example, forensic workstations are used to mount and image storage media, run forensic software, and perform intensive processes such as the indexing of data, recovering of deleted data, cracking of passwords, and parsing of digital artifacts across a wide range of data sources.

To achieve this, forensic workstations are equipped with top-tier processors, generous memory allocations, high-throughput storage media, and advanced Input/Output (I/O) configurations. They're built with speed and stability in mind, ensuring that digital forensic practitioners can navigate massive datasets without bottlenecks or failures.

They include using enhanced data storage and transfer technology (i.e. PCIe and NVMe storage volumes, Redundant Array of Inde-

pendent Disks (RAID) configurations – leveraging multiple disks to protect data), and expertly designed, excruciatingly fast volumes optimally handling hundreds of thousands of Input/Output Operations Per Second (IOPS). It's critical that the systems can handle IOPS efficiently and not fail during the millions of read/writes that occur when processing large volumes of data.

ONE SIZE DOESN'T FIT ALL

The scope of every forensic investigation is unique. Each involves different parties, sets of data sources, and required analysis, based on the type of matter involved. That is why forensic workstations are often custom-built to expect the complexities digital forensic practitioners may encounter. For example, a lab-based system optimizes multi-threaded analysis and large-scale device imaging, while a field-based system offers portability, ruggedness, and on-site evidence triage capabilities.

Understanding these distinctions is key when designing these customized technologically advanced tools. Field-based systems often trade off raw power for mobility, but they keep essential capabilities like multiple fast volumes, an abundance of memory, and the latest high-end processors. This allows digital forensic practitioners to not only preview live digital media but also process in the field. Lab-based systems, in contrast, often run multiple forensic tools in parallel, harnessing high core counts, fast memory or storage technology. Lab-based systems often include Graphics Processing Units (GPUs) to speed up graphics and image processing, specifically speeding up digital forensics tasks such as password cracking or video evidence processing.

WHY THE NEED FOR SPEED?

The integrity of digital evidence hinges on the tools used to examine it. A mis-configured or underpowered system can lead to slow processing times, missed evidence, or even legal challenges. That's why forensic workstations are, and should be, held to a higher standard. Law enforcement agencies, the military, government entities, and private sector corporations test, validate, and certify them to meet their requirements. An exceptional forensic workstation should also preserve data integrity throughout the process, ensuring the timely presentation of results from an analysis. Today, as the footprint of devices is becoming smaller, and the data volumes exponentially larger, it is vital to leverage state-of-the-art technology to sift through the mountains of evidence that may exist across different data sources. Many investigations require swift action by investigators, and it is important to identify, preserve, collect, process, and analyze data as quickly as possible. Forensic workstations are an essential tool that enables digital forensic practitioners to defensibly and efficiently address digital evidence. They are critical instruments that uphold the credibility of digital forensic investigations.

AN INVESTMENT FOR TODAY'S DIGITAL INVESTIGATIONS

As technology continues to develop, so must the tools used to investigate it. Forensic workstations, engineered to uncover truth hidden deep within digital traces, are the quiet giants of the digital forensics field. They are an investment for today's digital investigations, and empower digital forensic practitioners, to leave no byte behind – whether deployed in the field or a forensic lab. **PI**

Robert B. Fried is an accomplished expert with decades of experience performing data collections and forensic investigations of electronic evidence. He attained a BS and MS in Forensic Science from the University of New Haven. He holds and actively maintains industry certifications and is a licensed PI in Michigan, New York, and South Carolina. Robert serves on the Board of Advisors for the Masters in Investigations program at the University of New Haven, the Global Advisory Board for EC-Council's CHFI certification, and is a Fellow at The Henry C. Lee Institute of Forensic Science at the University of New Haven. He is the author of the books: Forensic Data Collections 2.0: A Selection of Trusted Digital Forensics Content *and* Forensic Data Collections 2.0: The Guide for Defensible & Efficient Processes.

Manny Kressel is the Founder and Chief Executive Officer of BitMindz, a leading computer forensics company. With over 19 years of experience in digital forensics, 30+ years in system integration and design, and four decades in the computing field, Manny brings unparalleled expertise to his work. A former law enforcement officer in the metro Atlanta area, he was responsible for digital forensic operations within his department, including the examination of digital media, mobile device analysis, system integration, and lab infrastructure design. His extensive knowledge, hands-on experience, and specialized training uniquely position him to bridge the gap between advanced forensic hardware and the software solutions that drive digital investigations.