TRACE3

SECURITY BUSINESS UNIT

DIGITAL FORENSICS

Organizations are now faced with situations requiring digital forensics expertise. Unfortunately, most organizations tend to lack information, lack talent/expertise/tooling, face possible violations or pending litigations (HIPPA, PCI, SOX), and encounter abuse of technology. Organizations are unable to staff a digital forensics lab, and struggle to obtain the information they are seeking in an investigation on their own.

THE IMPORTANCE OF DIGITAL FORENSICS

The digital forensics investigation process involves the seizure, collection, analysis, and reporting of data in question. Insider threat is on the rise and poses new challenges for organizations. Mobile devices being used in the workplace is on the rise, and many workers are using personal devices to access company information. This leads to organizations needing digital forensics to identify and remediate security threats as quickly as possible. As the usage of digital devices is increasing, forensic evidence extraction is becoming an essential source of evidence.

TRACE3 DIGITAL FORENSICS INVESTIGATIONS

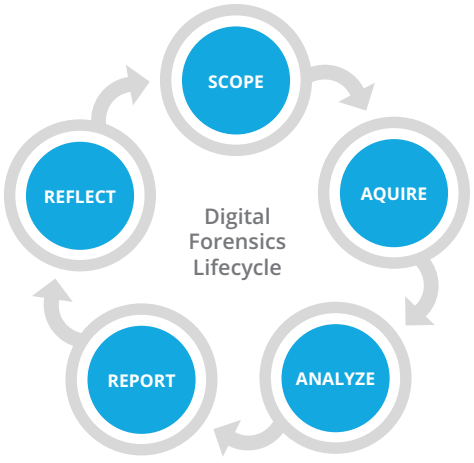
The digital forensic investigations approach is based on Trace3 providing access to the information that enables better handling and addressing risks companies are facing, from HR, security, regulatory, and loss of IP. Customers are empowered to make decisions based on the data Trace3 provides from interrogated data, systems, and devices. Trace 3 empowers organizations by offering:

Risk mitigation involving people and organizational health
Investigations help determine the presence of fraud, breach of contract, intellectual property theft, usage violations, and harassment. As part of mitigating risk, Trace3 digital forensics can acquire the necessary data, and cull what is responsive as part of subpoenas or discovery process requests.

Incident Response
Trace3 provides incident response services paired with forensics to bring a unique blend of valuable information regarding system activities, files/data that may have been accessed, how the system was penetrated, and provide additional indicators of compromise to help prevent future incidents.

Non-Standard Device Forensics and Analysis
With IoT expanding at a rapid pace, Trace3 offers the ability to perform digital forensics on a wide variety of devices. Network devices and other non-traditional items are often overlooked as evidence and not analyzed, leaving potentially critical information unexamined.

Information Risk Mitigation
Forensic wiping and wipe verification services provided by Trace3 allow organizations to securely erase data and re-issue or re-purpose devices. Forensic wiping is necessary to meet privacy standards for the data previously stored on the devices and drives.



To learn more or to engage with one of our Digital Forensics specialists, send an email to digitalforensics@trace3.com or visit www.trace3.com/security

TRACE3