

## Digital Forensics

---

### Digital Evidence That Endures

Cyber exploitation and malicious activity have become increasingly sophisticated and targeted. Public and private sectors face increasing challenges in protecting their intellectual capital and critical enterprise IT assets. Many digital forensics groups have difficulty keeping up with the demands of this industry and responding to the trends in attacks.

### Why Digital Forensics From Booz Allen?

At Booz Allen Hamilton, a leading strategy and technology consulting firm, we provide services to leading corporations, government and other public agencies, emerging growth companies, and institutions. We have extensive experience conducting digital forensics investigations of varied sizes and scopes for diverse clients in the defense, civil, commercial, and intelligence sectors.

We offer professionals who are highly experienced in digital forensics. We also have more than 1,000 information assurance (IA) professionals, many of whom have high-level government clearances. In addition, we offer training in forensics best practices to improve your organization's internal forensics capability. Our staff members have experience training local, state, federal, and corporate investigators in the latest incident response and forensics analysis techniques.

### Our Digital Forensics Services and Approach

Booz Allen offers several major areas of digital forensics expertise:

- Intrusion analysis
- Host-based analysis
- Malicious code analysis
- Incident response and management
- Data theft and exposure analysis
- Vulnerability, threat, and risk management

Our Proactive Threat Identification (PTI) program is the most comprehensive digital forensics solution available. Booz Allen has developed the PTI program to go beyond the normal approach to investigations. In addition to standard forensics services, PTI focuses on identifying indicators of compromise.

#### About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for more than 90 years. Providing a broad range of services in strategy, operations, organization and change, information technology, systems engineering, and program management, Booz Allen is committed to delivering results that endure.

#### For more information contact

Ronald Ritchey  
Principal  
703/377-6704  
ritchey\_ronald@bah.com

Edwin Kanerva  
Principal  
301/543-4495  
kanerva\_ed@bah.com

[www.boozallen.com](http://www.boozallen.com)

## Digital Forensics

---

PTI uses our proprietary Automated First Responder (AFR) to identify a range of threats—from internal malfeasants to organized criminals and nation-state adversaries—using highly targeted client-side attacks such as spear-phishing to compromise fully patched systems that have up-to-date antivirus systems.

PTI is a proven, successful tool. It is a digital forensics and incident response utility designed to quickly collect specific information from a system, enabling its users to successfully identify malicious code. AFR has proven its effectiveness in situations when anti-virus, host-based intrusion detection systems or rootkit detectors have been unable to detect malicious code. We can tailor custom AFR builds to client networks and use them to push changes to hosts and remediate discovered compromises.