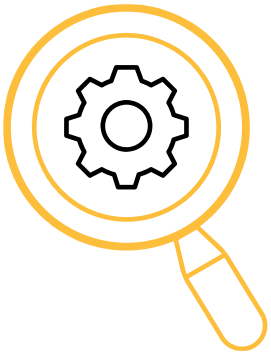
Lodestone

SERVICE BRIEF FOR

DIGITAL FORENSICS INVESTIGATION



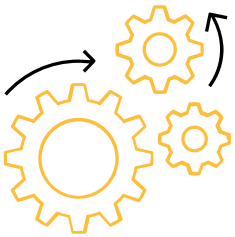
Our highly skilled digital forensic experts are equipped with state-of-the-art tools and techniques to collect, analyze, and preserve digital evidence from a wide range of electronic devices, networks, and digital media. Our expertise covers all aspects of digital forensics, including computer forensics, mobile, and email.

Our digital forensics services are tailored to meet each client's specific needs We work closely with our clients and their legal counsel to ensure that our services are delivered with the utmost professionalism, accuracy, and confidentiality.

BENEFITS

- Identification of malicious or unauthorized activity in your environment, be it from a threat actor, an insider threat, or accidental.
- Advice on impact and implications in real-world context based on the activities discovered.
- Our team of experts will provide you with the necessary information to confirm that the threat has been eliminated, and offer valuable insights on how to protect yourself from similar incidents in the future.

METHODOLOGY



Lodestone Digital Forensics Investigation involves collecting evidence in a forensically sound manner, analyzing evidence sources by experts, effectively communicating findings, and ensuring a comprehensive understanding of the incident.

The Digital Forensics Investigation is comprised of these primary phases:

Evidence Collection → **Investigation** → **Reporting** → **Way Forward Consulting**

- Evidence Collection – We work with you to collect the necessary evidence to complete the analysis and give you the answers you need. We provide several methods for this for ease and to prevent keeping your team from the important work of getting you back up and running. We use industry-standard tools and software and provide all necessary handling steps to address any legal considerations.

- Investigation
  - We analyze the evidence* collected to find all available indicators of compromise to achieve the objectives of the engagement.
  - We provide contextualization of the analysis to describe how the attack chain occurred and uncover as much information as possible about the timeline and progression of the incident.
  - We communicate with you to inform you not only of our progress, but also of any significant findings that can either help with intermediate actions or posture for future actions that may be necessary.
  - We provide the most thorough answers possible based on evidence as to how the incident was executed, what the total impact and scope of the incident were, and how to take steps to prevent future recurrence of similar attacks.

- Reporting – We provide a written final summary of the investigation with a concise description of the findings and details of the investigation for any historical preservation and reporting requirements you may have.

- Way Forward Consulting – At the end of the investigation, we provide you with industry general cybersecurity best practices to aid you in moving forward. We remain available to deliver other services to further harden your environment

*Evidence Examples

While the total list of ransomware evidence items is ever-expanding with new technologies, these are the most common examples of evidence we collect during our investigation phase:

- Physical drives from workstations or servers
- Logical forensic images of workstations or servers
- Copies of security appliance logs (e.g., firewalls, network device management suites, VPN devices, copies of server logs)
- Alert histories from antivirus and endpoint detection solutions
- Threat actors lists of any claims surrounding data exfiltration
- Other sources of evidence as applicable that provide context or support of the investigation

DURATION AND DELIVERABLES

Digital Forensics Investigation varies in duration but typically takes one to two weeks, depending on the number of systems investigated.

As part of the engagement, Lodestone will provide weekly updates from forensics experts and a comprehensive report that includes a timeline of the events surrounding the event. We will work closely with your team to give visibility and answer questions throughout the progression of the incident, which will inform business decisions and provide final findings to support internal and external reporting needs.

Connect with us:
www.lodestone.com
320 East Main Street, Lewisville, TX 75057, USA
Tel: +1-203-307-4984
info@lodestone.com

Lodestone is a global cybersecurity firm committed to helping clients prevent and investigate security incidents. It is comprised of top talent from private industry, government, intelligence, and law enforcement specializing in incident response, digital forensics, offensive security, risk management, and threat detection.