DFIR

DIGITAL FORENSICS AND INCIDENT RESPONSE

NETWORK INTELLIGENCE
Global cybersecurity provider

Digital Forensics

INTRODUCTION

Digital forensics is the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence. This evidence can be extracted from many digital sources such as CD/DVDs, hard drives, flash drives, memory sticks, and magnetic tapes, etc.
Digital forensics serves as a supporting proof or corroborating evidence often made by prosecutors and defendants to refute a claim that a certain activity was done by a specific person using a piece of digital equipment. The most common use is to recover erased digital evidence to support or disprove a claim in court of law or in civil proceedings such as the eDiscovery process in courts. Forensics is also used during internal corporate investigations or intrusion investigation which includes additional activities like network and log review.

Types of Digital Forensics:
At NII, we have a full-fledged team and a well-equipped lab to carry out the following types of digital forensics:

- Computer forensics
- Mobile device forensics
- Network forensics
- Database forensics

APPROACH & METHODOLOGY

1. We follow best practice methodology and guidelines (NIST and ACPO) for acquisition and analysis of digital evidence which are admissible in court of law.

Collection: Identifying, labelling, recording and acquiring data from the possible sources, while following procedures that preserve the integrity of the data.

Process: Forensically process collected data using a combination of various automated and manual methods, and extracting data of interest, while preserving the integrity of the data.

Analysis: Analysing the results of the process phase, using legally acceptable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and process

Reporting: Reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

2. We effectively identify and investigate a breach.

Identify: Recognizing critical functions within a business and properly commanding the resources that support these functions. This enables the company to prioritize efforts effectively and craft a strategy that is consistent with existing risk management and business needs.

Respond: Quickly respond to the breach in a timely manner, appropriate actions are performed based on relevant factors such as the functional and information impact of the breach, and the likely recoverability from it.

Protect: Placing appropriate safeguards in place for mitigating and preventing cybersecurity incidents.

APPROACH & METHODOLOGY

3. Use of well-known and globally accepted forensic tools for acquisition and analysis of digital evidence.

4. Mix of enthusiastic, passionate and experienced information security professionals having skillsets in digital forensics and incident response.

SERVICES OFFERED

SERVICES OFFERED

Incident handling: Incident Response work with teams available 24/7 backed by an SLA.

Incident management training: A 2-day hands on training session for your team that is responsible for detecting, responding and managing security incidents in your organization.

Breach/Compromise assessment: Review your existing infrastructure & cloud-hosted environment to determine whether the necessary security controls have been implemented or not from the perspective of incident response.

Breach Response Assessment: Respond to a breach in a timely manner. Conduct a fact-finding exercise to determine how and why the breach had occurred. Provide solution for mitigating the threat and suggest measures for preventing the threat in future.

Malware Analysis: Proactively combat zero-day attacks and advanced threats found in email attachments, downloaded files and URLs linking to files within emails using malware analysis capabilities.

Disk forensics and analysis: Forensically acquire and analyze different storage devices like hard disks with IDE/SATA/SCSI interfaces, CD, DVD, Floppy disk, PDAs, flash cards, SIM, USB/ Fire wire disks, Magnetic Tapes, Zip drives, apple devices etc. using globally accepted tools.

Mobile forensics and analysis: Acquire and analyze hand-held devices in a forensically sound manner using globally accepted tools.

Fraud Investigation: Investigate fraud related to bribery, conflict of interest, data leakage, asset misappropriation, etc. by identifying the fraud, determining how the fraud has occurred, discover the cause or person responsible for the fraud, quantify the loss suffered due to fraud, gather relevant evidence that is admissible in court of law, suggest measures that can prevent similar frauds in future.

Forensic Readiness assessment: Pre-emptively help an organization to reduce hassle and time for responding to future breach by assessing existing logging configuration, availability, archival, and efficiency of logs etc.

ATM Forensic Audit: Audit the ATM systems of a bank. A comprehensive review encompassing of logical, physical security and forensics of the running processes and network connections.

WHY NETWORK INTELLIGENCE

NII has done extensive projects in digital forensics and has a dedicated team for carrying out these various activities. We have co-operated with law enforcement authorities in helping them getting leads in the forensics investigations and also played a vital part in internal corporate investigations for many of our clients. Our work ethics and quality deliverables have won accolades from many of our clients and their testimonials are strongest testimony to our professional and quality work deliverables. A representative list of some of the projects we have done are:

- Analysis of dozens of hard drives and correlating them with financial documents to build a water-tight case of tax evasion, FEMA violations, disproportionate assets, etc. against the accused who was arrested on other grave charges. The evidence and reports provided by us enabled regulatory agencies to pursue multiple independent cases against the accused and law enforcement was able to file a 5000-page charge-sheet
- Analysis of server logs to determine a breach in one of the country's main telecom firms done by Pakistani hackers prior to Independence day. Complete details of the steps taken by the hacker and the malware uploaded onto the servers was provided along with detailed recommendations on how to ensure such an event doesn't occur in the future
- Disk-based analysis to retrieve deleted files, email correspondence and Internet browsing history of the suspect and determine the exact nature of the financial fraud as well as determine the list of accomplices.
- Analysis of smartphones and tablets to retrieve BB Messenger, WhatsApp, and SMS communication
- Empaneled by a multi-national bank for all forensic cases in the Asia-Pacific region

ABOUT US

We are a global cybersecurity provider founded in 2001 with more than 600 team members working out of our New York, Singapore, Dubai and Mumbai offices. We offer services across 6 broad spectrums - Assessment, BCMS, GRC, Professional Services, MSSP & Trainings. We serve customers across industry verticals such as Banks and Financial Services, Technology and Media, Oil & Power, Airlines, E-commerce, Retail, etc. We believe that cybersecurity is not a destination, it is a journey and we partner with our clients to address the dynamic cybersecurity threat landscape.

TO KNOW MORE ABOUT OUR DIGITAL FORENSICS AND INCIDENT RESPONSE SERVICE: CLICK HERE

US | Singapore | India |UAE | Netherlands

info@niiconsulting.com

www.niiconsulting.com