

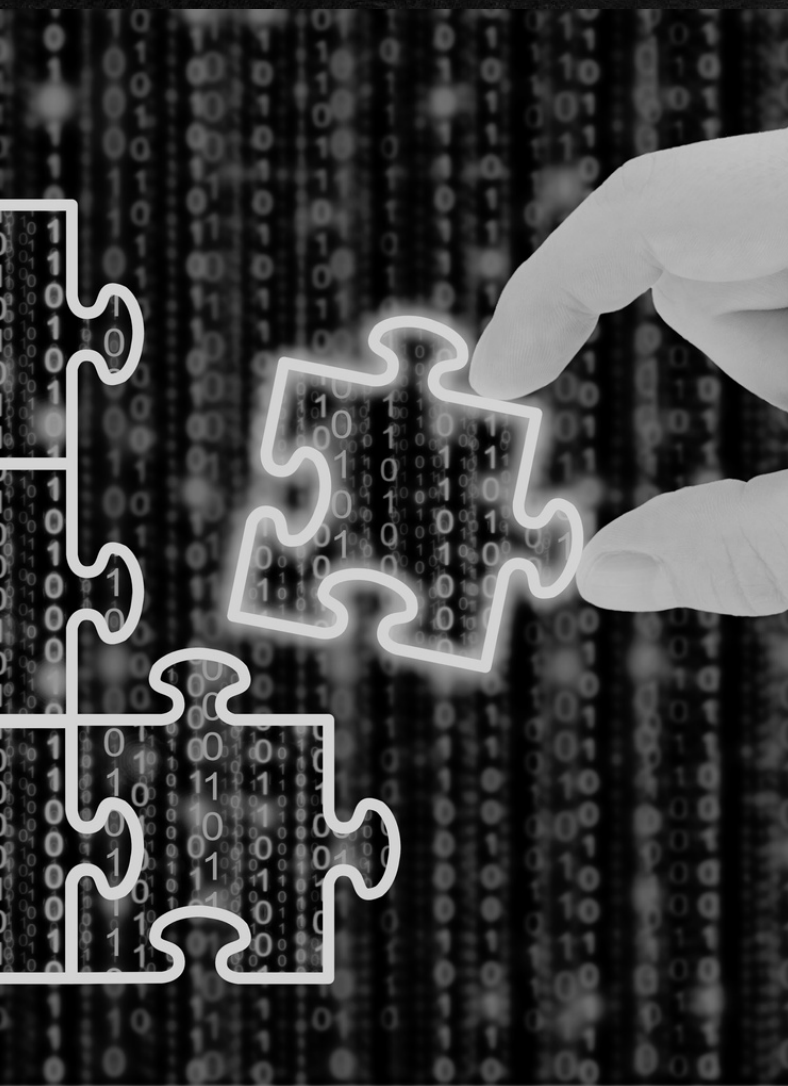
Cyber Forensics



Contact information:
www.971cybersecurity.com
info@971cybersecurity.com

Improper handling of data can result in the loss of crucial time!

During a cyber-security incident, initial assessments made by IT staff may lack the necessary forensic training, potentially compromising the integrity of digital evidence. The objective of cyber forensics is to derive knowledge from information such that a sequence of actions or events can be reconstructed. **Plus971 Cyber Security's Cyber Forensics** team has special skills required for the preservation, identification, and interpretation of digital evidence, highlighting the need for professional forensic investigations.



In today's rapidly evolving landscape, organizations increasingly rely on technology to maintain competitiveness. Customers expect a seamless online experience, prompting organizations to invest in professional websites, rapid responses to inquiries, and convenient online ordering.

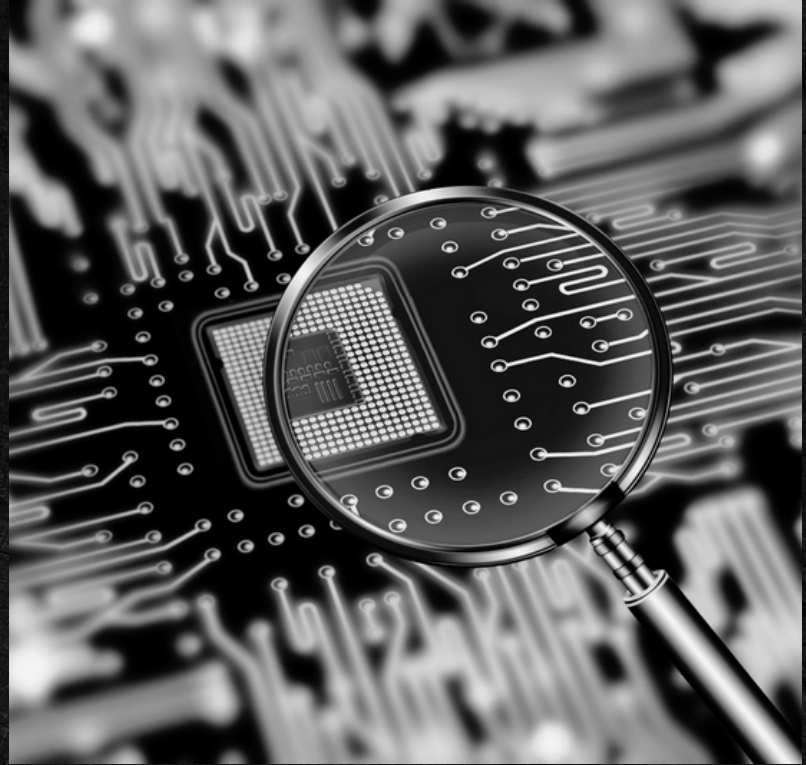
With technology integrated into daily life, individuals expect constant access to personal emails and social connections, blurring the lines between work and personal time.

Plus971 Cyber Security's Cyber Forensics constitutes a comprehensive investigative process, spanning data acquisition, analysis, documentation, knowledge extraction, and reporting, all in compliance with legal or organizational standards.

Cyber Forensics can be initiated spontaneously in response to:

- Policy breaches or misconduct.
- External legal inquiries.
- Compliance obligations.
- Risk management.
- Ensuring adherence to relevant laws.

This is where **Plus971 Cyber Security's** expert staff comes in with **exceptional forensic training**. With cyber forensics gaining traction globally, organizations must recognize its value as a proactive tool against cybercrime.



Preventing Cyberattacks

Our experts understand cybercriminal tactics and implement preventive measures to safeguard data through network scanning and access control to proactively defend against external threats.



Combating Malware

Cyber forensics plays a crucial role in mitigating malware threats by utilizing forensic analysis to trace the entry points of viruses, spyware, and other malicious software, effectively preventing them from compromising sensitive data.



Data Recovery

In the event of a data breach or identity theft, recovering deleted information is paramount for digital investigations. Our techniques and tools retrieve critical data, ensuring its integrity for legal proceedings or data recovery efforts.



Vulnerability Identification

Plus971 Cyber Security's Cyber forensics techniques uncover hidden vulnerabilities within applications, infrastructure, and websites, providing valuable insights for cybersecurity professionals.

In cyber forensics, you'll often discover vital details such as:

1. User attribution for specific actions.
2. Sequences of actions, whether authorized or user-related.
3. Log and metadata specifics including timestamps, file types, sizes, and data volumes.
4. Content details like audio, video, and text files.
5. Involved in technologies and their implications.