Practical No 3

**Case Study: Unraveling a Cybersecurity Intrusion at XYZ Corporation**

**Introduction:** This Case study aims that systematically investigating and understanding the details of the cybersecurity incident. In the dynamic landscape of cybersecurity, the ability to respond swiftly to potential security breaches is critical. XYZ Corporation, a multinational company, recently discovered irregularities within its internal network. Unusual data transfers, unauthorized access attempts, and anomalies in system logs prompted immediate concerns about a potential security breach. This case study details the steps taken by XYZ Corporation's cybersecurity team to conduct a comprehensive digital forensics investigation.

**Background:** XYZ Corporation operates in multiple countries, handling sensitive information and proprietary data. The company's cybersecurity infrastructure is designed to detect and respond to potential threats proactively. However, the recent anomalies in network activities raised alarms, triggering a rapid response from the cybersecurity team. The primary objectives include identifying the source of the compromise, assessing the extent of the breach, and gathering evidence to support potential legal actions.

**Initial Response:**

1. **Incident Identification:**
   * Unusual data transfers and unauthorized access attempts were initially detected through automated monitoring tools.
   * System logs indicated anomalies and patterns inconsistent with regular network activities.
2. **Isolation of Affected Systems:**
   * To prevent further potential damage, the affected systems were immediately isolated from the network.
   * The isolation process involved disconnecting the compromised systems to contain the possible spread of the intrusion.

**Digital Forensics Investigation:**

1. **Forensic Team Activation:**
   * Upon identifying the potential breach, XYZ Corporation activated its cybersecurity incident response team, including digital forensics experts.
2. **Evidence Preservation:**
   * To ensure the integrity of potential evidence, the digital forensics team employed write blockers on the compromised systems' storage devices.
   * This step aimed to prevent unintentional modifications to the data during the acquisition process.
3. **Forensic Imaging with EnCase:**
   * EnCase, a renowned digital forensic software, was employed for acquiring forensic images of the affected systems' storage.
   * Write-protected storage devices were connected to forensic workstations running EnCase to initiate the imaging process.
4. **Verification of Write Protection:**
   * The forensics team verified the functionality of write blockers by attempting to write to the storage devices.
   * Successful prevention of changes confirmed the write blockers were operating correctly.
5. **Acquisition Settings in EnCase:**
   * Forensic experts configured EnCase with specific acquisition settings, including the type of data to be collected and the destination for the forensic images.
6. **Initiation of Forensic Imaging:**
   * The forensic imaging process was initiated, copying the data from the compromised systems' storage to secure locations, creating forensically sound images.
7. **Analysis in EnCase:**
   * With the forensic images acquired, the cybersecurity team utilized EnCase for in-depth analysis.
   * File structures, metadata, and potential artifacts were examined to identify the nature and scope of the security breach.

**Conclusion:** This case study exemplifies the meticulous digital forensics process undertaken by XYZ Corporation's cybersecurity team in response to a potential security breach. By swiftly identifying and isolating affected systems and employing industry-standard tools like EnCase and write blockers, the team aimed to not only understand the source and extent of the compromise but also to gather irrefutable evidence for potential legal actions. The ability to conduct a thorough digital forensics investigation is paramount in the modern cybersecurity landscape, allowing organizations to respond effectively to cyber threats and safeguard their digital assets.