Introduction to Incident Response Cheat Sheet

3 Key Concepts of Information Security:

- **Confidentiality:** Protecting information from unauthorized access.
- **Integrity:** Ensuring the accuracy and completeness of information.
- **Availability:** Guaranteeing timely and reliable access to information and services.

Cyber Incident Statistics (High-Level - Need Specific Data for Details):

- Frequency of attacks is [mention a general trend, e.g., increasing].
- Common attack vectors include [list a few, e.g., phishing, malware, ransomware].
- Average cost of a data breach is [mention a general range or impact].

Computer Security Incident:

- An event that actually or potentially jeopardizes the confidentiality, integrity, or availability of information or information systems.

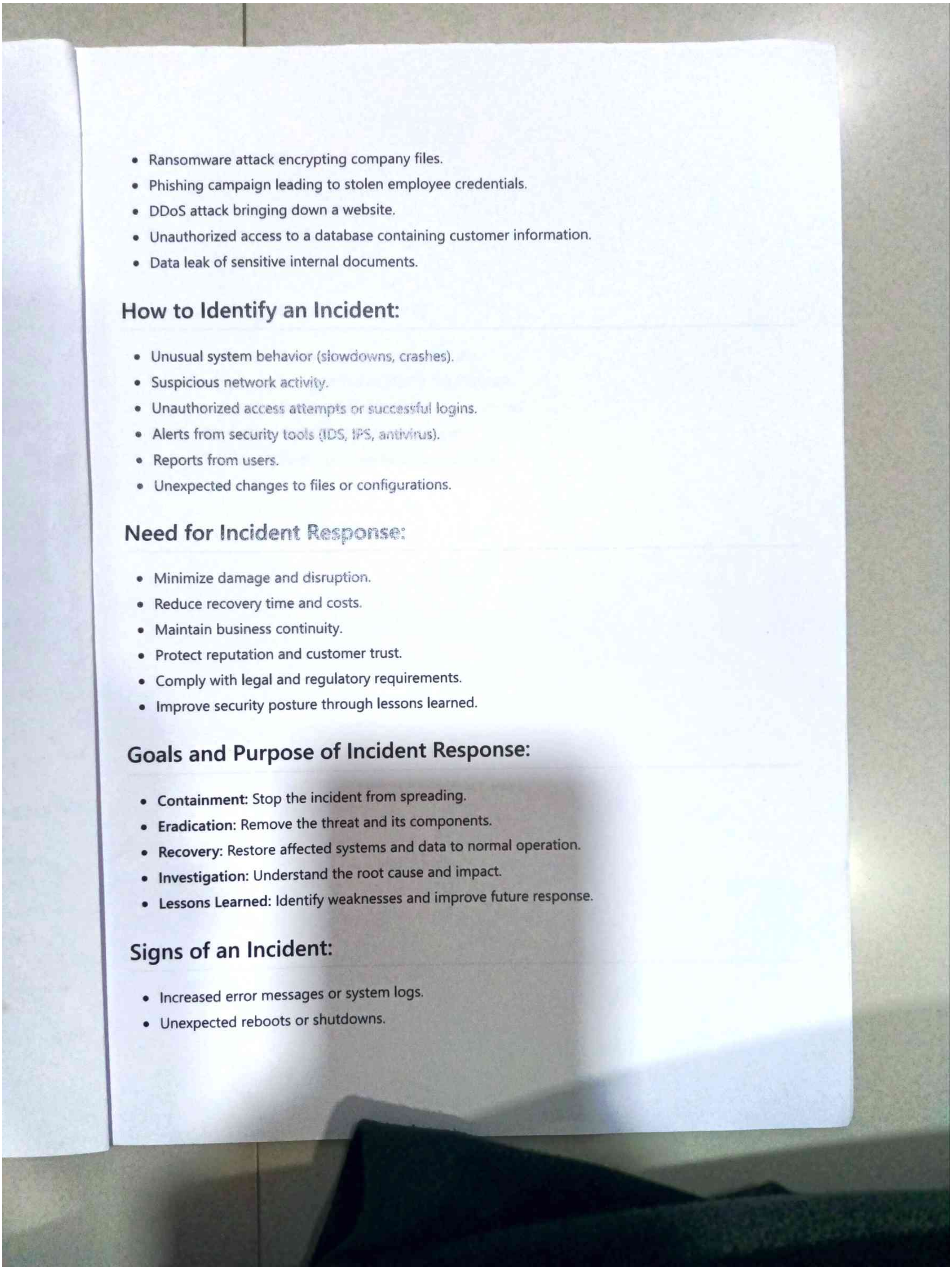
Information Warfare:

- Conflict in cyberspace involving nation-states or state-sponsored groups, targeting critical infrastructure, espionage, or disruption.

Types of Computer Security Incidents:

- **Malware:** Viruses, worms, ransomware, spyware.
- **Phishing:** Deceptive emails or messages to steal credentials.
- **Denial of Service (DoS/DDoS):** Overwhelming systems to disrupt services.
- **Unauthorized Access:** Gaining entry without permission.
- **Data Breach:** Sensitive information is exposed or stolen.
- **Insider Threats:** Malicious or unintentional actions by employees.

Examples of Computer Security Incidents:



- Ransomware attack encrypting company files.
- Phishing campaign leading to stolen employee credentials.
- DDoS attack bringing down a website.
- Unauthorized access to a database containing customer information.
- Data leak of sensitive internal documents.

How to Identify an Incident:

- Unusual system behavior (slowdowns, crashes).
- Suspicious network activity.
- Unauthorized access attempts or successful logins.
- Alerts from security tools (IDS, IPS, antivirus).
- Reports from users.
- Unexpected changes to files or configurations.

Need for Incident Response:

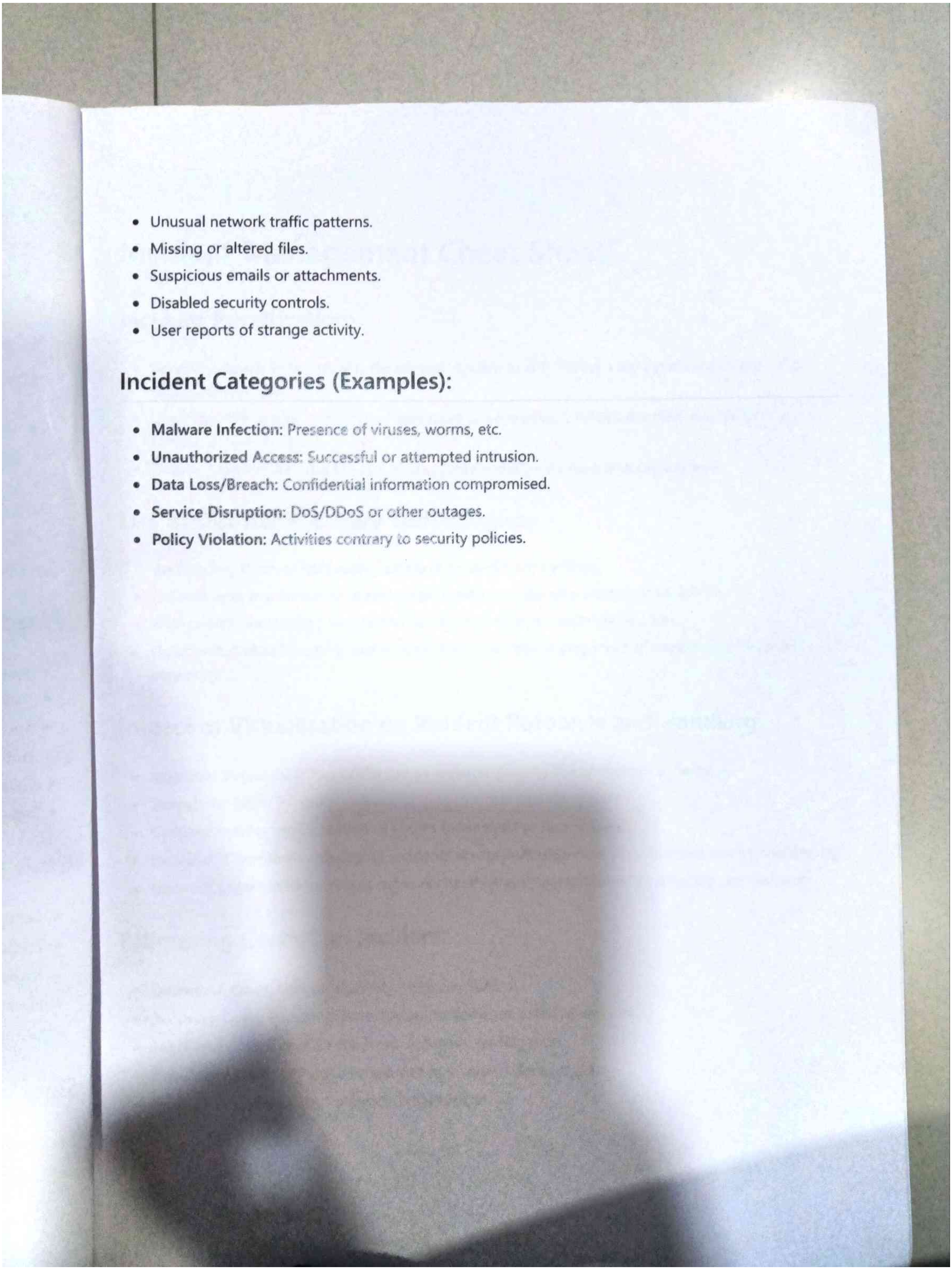
- Minimize damage and disruption.
- Reduce recovery time and costs.
- Maintain business continuity.
- Protect reputation and customer trust.
- Comply with legal and regulatory requirements.
- Improve security posture through lessons learned.

Goals and Purpose of Incident Response:

- **Containment:** Stop the incident from spreading.
- **Eradication:** Remove the threat and its components.
- **Recovery:** Restore affected systems and data to normal operation.
- **Investigation:** Understand the root cause and impact.
- **Lessons Learned:** Identify weaknesses and improve future response.

Signs of an Incident:

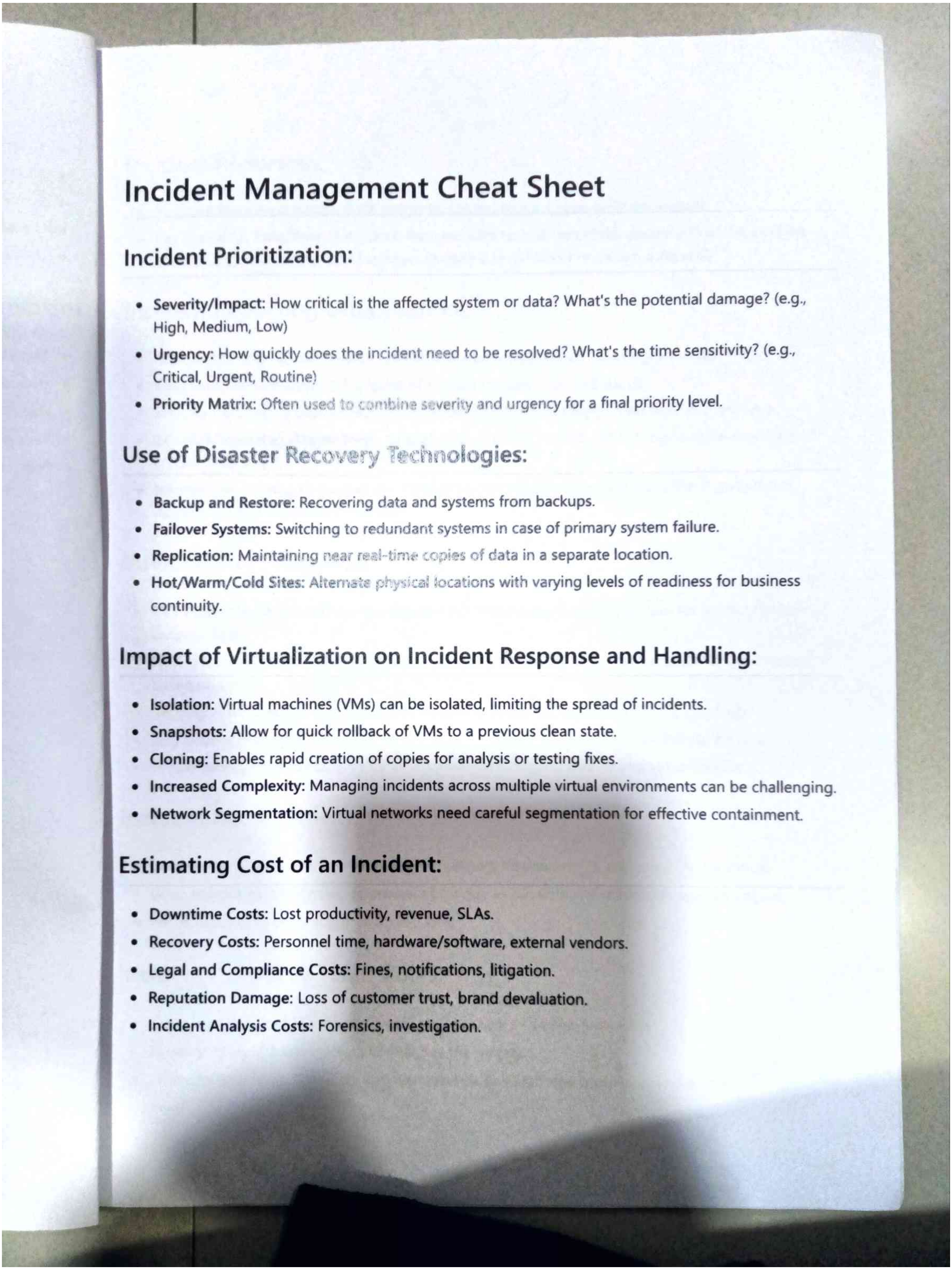
- Increased error messages or system logs.
- Unexpected reboots or shutdowns.



- Unusual network traffic patterns.
- Missing or altered files.
- Suspicious emails or attachments.
- Disabled security controls.
- User reports of strange activity.

Incident Categories (Examples):

- **Malware Infection:** Presence of viruses, worms, etc.
- **Unauthorized Access:** Successful or attempted intrusion.
- **Data Loss/Breach:** Confidential information compromised.
- **Service Disruption:** DoS/DDoS or other outages.
- **Policy Violation:** Activities contrary to security policies.



Incident Management Cheat Sheet

Incident Prioritization:

- **Severity/Impact:** How critical is the affected system or data? What's the potential damage? (e.g., High, Medium, Low)
- **Urgency:** How quickly does the incident need to be resolved? What's the time sensitivity? (e.g., Critical, Urgent, Routine)
- **Priority Matrix:** Often used to combine severity and urgency for a final priority level.

Use of Disaster Recovery Technologies:

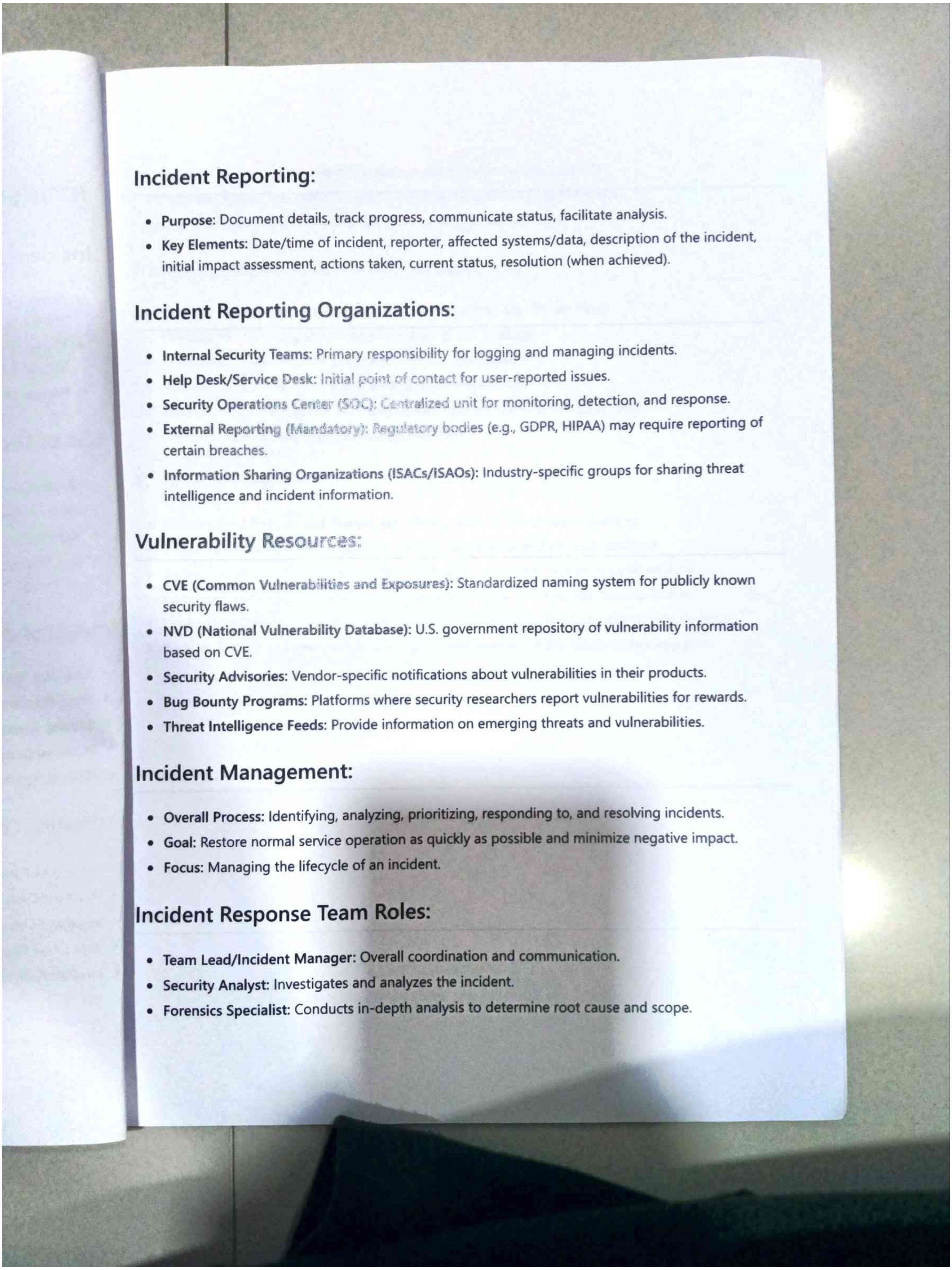
- **Backup and Restore:** Recovering data and systems from backups.
- **Failover Systems:** Switching to redundant systems in case of primary system failure.
- **Replication:** Maintaining near real-time copies of data in a separate location.
- **Hot/Warm/Cold Sites:** Alternate physical locations with varying levels of readiness for business continuity.

Impact of Virtualization on Incident Response and Handling:

- **Isolation:** Virtual machines (VMs) can be isolated, limiting the spread of incidents.
- **Snapshots:** Allow for quick rollback of VMs to a previous clean state.
- **Cloning:** Enables rapid creation of copies for analysis or testing fixes.
- **Increased Complexity:** Managing incidents across multiple virtual environments can be challenging.
- **Network Segmentation:** Virtual networks need careful segmentation for effective containment.

Estimating Cost of an Incident:

- **Downtime Costs:** Lost productivity, revenue, SLAs.
- **Recovery Costs:** Personnel time, hardware/software, external vendors.
- **Legal and Compliance Costs:** Fines, notifications, litigation.
- **Reputation Damage:** Loss of customer trust, brand devaluation.
- **Incident Analysis Costs:** Forensics, investigation.



Incident Reporting:

- **Purpose:** Document details, track progress, communicate status, facilitate analysis.
- **Key Elements:** Date/time of incident, reporter, affected systems/data, description of the incident, initial impact assessment, actions taken, current status, resolution (when achieved).

Incident Reporting Organizations:

- **Internal Security Teams:** Primary responsibility for logging and managing incidents.
- **Help Desk/Service Desk:** Initial point of contact for user-reported issues.
- **Security Operations Center (SOC):** Centralized unit for monitoring, detection, and response.
- **External Reporting (Mandatory):** Regulatory bodies (e.g., GDPR, HIPAA) may require reporting of certain breaches.
- **Information Sharing Organizations (ISACs/ISAOs):** Industry-specific groups for sharing threat intelligence and incident information.

Vulnerability Resources:

- **CVE (Common Vulnerabilities and Exposures):** Standardized naming system for publicly known security flaws.
- **NVD (National Vulnerability Database):** U.S. government repository of vulnerability information based on CVE.
- **Security Advisories:** Vendor-specific notifications about vulnerabilities in their products.
- **Bug Bounty Programs:** Platforms where security researchers report vulnerabilities for rewards.
- **Threat Intelligence Feeds:** Provide information on emerging threats and vulnerabilities.

Incident Management:

- **Overall Process:** Identifying, analyzing, prioritizing, responding to, and resolving incidents.
- **Goal:** Restore normal service operation as quickly as possible and minimize negative impact.
- **Focus:** Managing the lifecycle of an incident.

Incident Response Team Roles:

- **Team Lead/Incident Manager:** Overall coordination and communication.
- **Security Analyst:** Investigates and analyzes the incident.
- **Forensics Specialist:** Conducts in-depth analysis to determine root cause and scope.

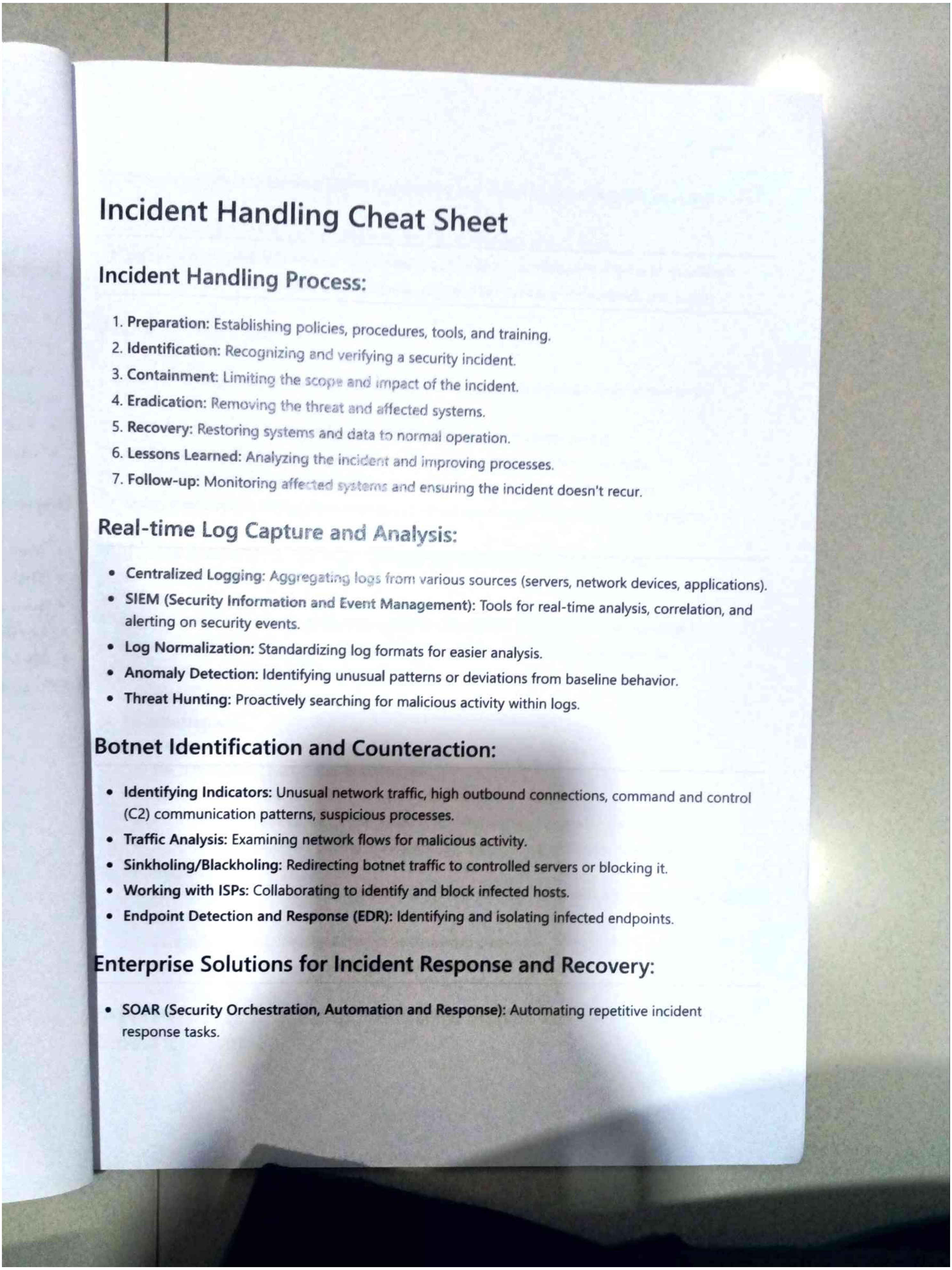
- **Communication Liaison:** Handles internal and external communications.
- **Technical Specialists:** Provide expertise on specific systems or applications.
- **Legal/Compliance:** Advises on legal and regulatory requirements.

Incident Response Team Responsibilities:

- **Detection and Analysis:** Identifying and understanding security incidents.
- **Containment:** Limiting the scope and impact of the incident.
- **Eradication:** Removing the threat and affected components.
- **Recovery:** Restoring systems and data to normal operation.
- **Post-Incident Analysis:** Documenting lessons learned and improving processes.
- **Communication:** Keeping stakeholders informed.

Dependencies:

- **Well-Defined Policies and Procedures:** Clear guidelines for incident handling.
- **Trained Personnel:** Staff equipped to identify, respond to, and manage incidents.
- **Security Tools and Technologies:** Infrastructure for detection, prevention, and analysis.
- **Communication Channels:** Reliable methods for internal and external communication.
- **Up-to-Date Documentation:** System configurations, network diagrams, contact information.
- **Regular Testing and Exercises:** Validating the effectiveness of the incident response plan.



Incident Handling Cheat Sheet

Incident Handling Process:

1. **Preparation:** Establishing policies, procedures, tools, and training.
2. **Identification:** Recognizing and verifying a security incident.
3. **Containment:** Limiting the scope and impact of the incident.
4. **Eradication:** Removing the threat and affected systems.
5. **Recovery:** Restoring systems and data to normal operation.
6. **Lessons Learned:** Analyzing the incident and improving processes.
7. **Follow-up:** Monitoring affected systems and ensuring the incident doesn't recur.

Real-time Log Capture and Analysis:

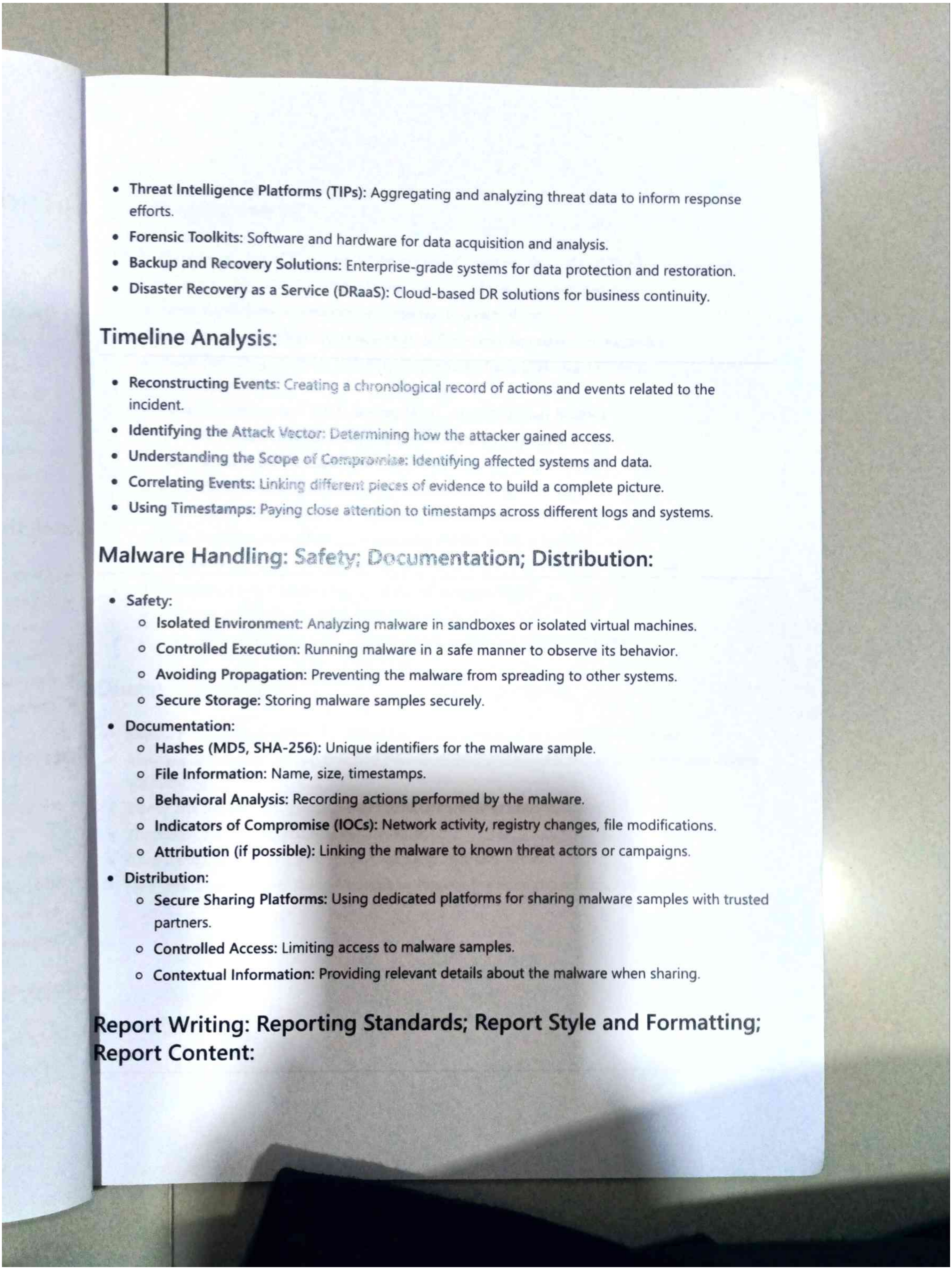
- **Centralized Logging:** Aggregating logs from various sources (servers, network devices, applications).
- **SIEM (Security Information and Event Management):** Tools for real-time analysis, correlation, and alerting on security events.
- **Log Normalization:** Standardizing log formats for easier analysis.
- **Anomaly Detection:** Identifying unusual patterns or deviations from baseline behavior.
- **Threat Hunting:** Proactively searching for malicious activity within logs.

Botnet Identification and Counteraction:

- **Identifying Indicators:** Unusual network traffic, high outbound connections, command and control (C2) communication patterns, suspicious processes.
- **Traffic Analysis:** Examining network flows for malicious activity.
- **Sinkholing/Blackholing:** Redirecting botnet traffic to controlled servers or blocking it.
- **Working with ISPs:** Collaborating to identify and block infected hosts.
- **Endpoint Detection and Response (EDR):** Identifying and isolating infected endpoints.

Enterprise Solutions for Incident Response and Recovery:

- **SOAR (Security Orchestration, Automation and Response):** Automating repetitive incident response tasks.



- **Threat Intelligence Platforms (TIPs):** Aggregating and analyzing threat data to inform response efforts.
- **Forensic Toolkits:** Software and hardware for data acquisition and analysis.
- **Backup and Recovery Solutions:** Enterprise-grade systems for data protection and restoration.
- **Disaster Recovery as a Service (DRaaS):** Cloud-based DR solutions for business continuity.

Timeline Analysis:

- **Reconstructing Events:** Creating a chronological record of actions and events related to the incident.
- **Identifying the Attack Vector:** Determining how the attacker gained access.
- **Understanding the Scope of Compromise:** Identifying affected systems and data.
- **Correlating Events:** Linking different pieces of evidence to build a complete picture.
- **Using Timestamps:** Paying close attention to timestamps across different logs and systems.

Malware Handling: Safety; Documentation; Distribution:

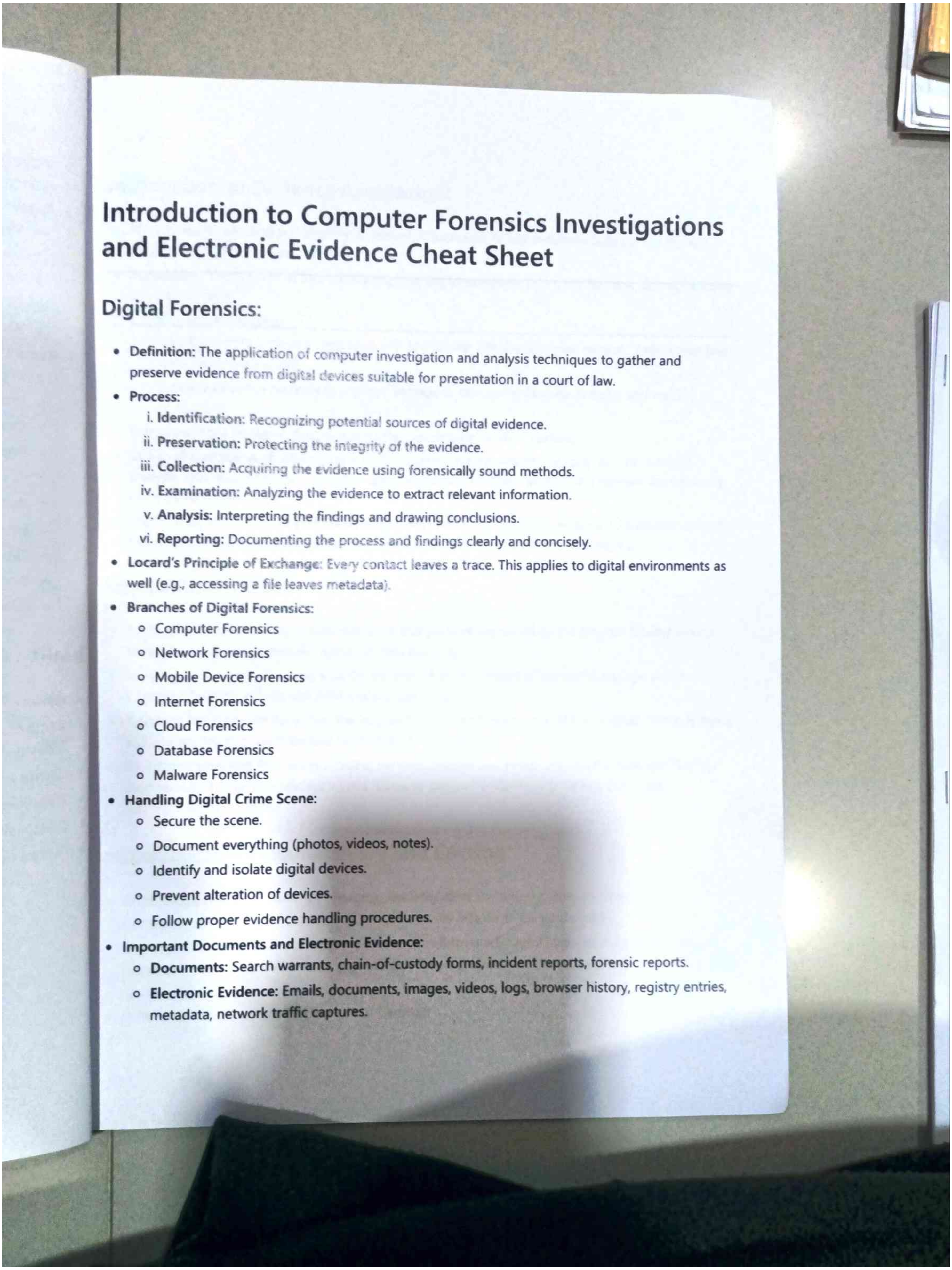
- Safety:
  - **Isolated Environment:** Analyzing malware in sandboxes or isolated virtual machines.
  - **Controlled Execution:** Running malware in a safe manner to observe its behavior.
  - **Avoiding Propagation:** Preventing the malware from spreading to other systems.
  - **Secure Storage:** Storing malware samples securely.
- **Documentation:**
  - **Hashes (MD5, SHA-256):** Unique identifiers for the malware sample.
  - **File Information:** Name, size, timestamps.
  - **Behavioral Analysis:** Recording actions performed by the malware.
  - **Indicators of Compromise (IOCs):** Network activity, registry changes, file modifications.
  - **Attribution (if possible):** Linking the malware to known threat actors or campaigns.
- **Distribution:**
  - **Secure Sharing Platforms:** Using dedicated platforms for sharing malware samples with trusted partners.
  - **Controlled Access:** Limiting access to malware samples.
  - **Contextual Information:** Providing relevant details about the malware when sharing.

Report Writing: Reporting Standards; Report Style and Formatting; Report Content:

- **Reporting Standards:** Following established organizational or industry guidelines for incident reports (e.g., NIST 800-61).
- **Report Style and Formatting:**
  - **Clear and Concise Language:** Avoiding jargon where possible or explaining technical terms.
  - **Logical Structure:** Organizing information in a clear and sequential manner.
  - **Professional Tone:** Maintaining an objective and factual style.
  - **Consistent Formatting:** Using headings, bullet points, and tables for readability.
  - **Visual Aids (if applicable):** Including diagrams or charts to illustrate findings.
- **Report Content:**
  - **Executive Summary:** A brief overview of the incident and key findings.
  - **Incident Details:** Date, time, reporting source, affected systems.
  - **Description of the Incident:** What happened? How was it discovered?
  - **Impact Assessment:** Business disruption, data loss, financial implications.
  - **Containment, Eradication, and Recovery Actions:** Steps taken to address the incident.
  - **Root Cause Analysis (if determined):** Why did the incident occur?
  - **Lessons Learned:** Recommendations for preventing similar incidents in the future.
  - **Timeline of Events:** A chronological record of key actions.
  - **Evidence and Artifacts:** Supporting data and findings.
  - **Contact Information:** Details of the incident responders and report authors.

Quality Assurance:

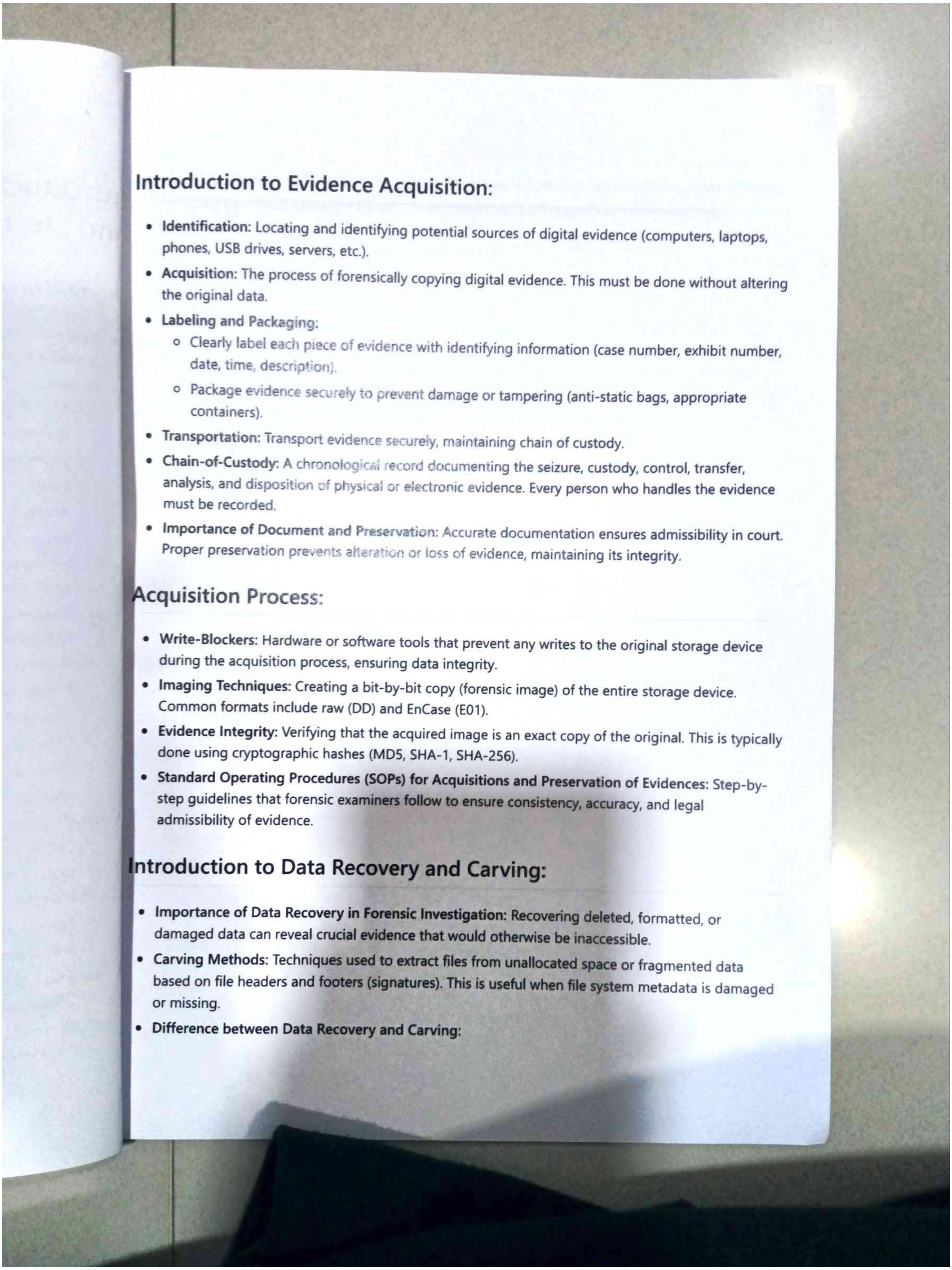
- **Review Process:** Having reports reviewed by senior personnel or other team members.
- **Accuracy and Completeness:** Ensuring the information presented is factual and all relevant details are included.
- **Clarity and Readability:** Verifying that the report is easy to understand.
- **Timeliness:** Issuing reports in a timely manner.
- **Consistency:** Maintaining a consistent reporting style and format.
- **Feedback Incorporation:** Using feedback to improve the reporting process and quality.



Introduction to Computer Forensics Investigations and Electronic Evidence Cheat Sheet

Digital Forensics:

- **Definition:** The application of computer investigation and analysis techniques to gather and preserve evidence from digital devices suitable for presentation in a court of law.
- **Process:**
  i. **Identification:** Recognizing potential sources of digital evidence.
  ii. **Preservation:** Protecting the integrity of the evidence.
  iii. **Collection:** Acquiring the evidence using forensically sound methods.
  iv. **Examination:** Analyzing the evidence to extract relevant information.
  v. **Analysis:** Interpreting the findings and drawing conclusions.
  vi. **Reporting:** Documenting the process and findings clearly and concisely.
- **Locard's Principle of Exchange:** Every contact leaves a trace. This applies to digital environments as well (e.g., accessing a file leaves metadata).
- **Branches of Digital Forensics:**
  - Computer Forensics
  - Network Forensics
  - Mobile Device Forensics
  - Internet Forensics
  - Cloud Forensics
  - Database Forensics
  - Malware Forensics
- **Handling Digital Crime Scene:**
  - Secure the scene.
  - Document everything (photos, videos, notes).
  - Identify and isolate digital devices.
  - Prevent alteration of devices.
  - Follow proper evidence handling procedures.
- **Important Documents and Electronic Evidence:**
  - **Documents:** Search warrants, chain-of-custody forms, incident reports, forensic reports.
  - **Electronic Evidence:** Emails, documents, images, videos, logs, browser history, registry entries, metadata, network traffic captures.



Introduction to Evidence Acquisition:

- **Identification:** Locating and identifying potential sources of digital evidence (computers, laptops, phones, USB drives, servers, etc.).
- **Acquisition:** The process of forensically copying digital evidence. This must be done without altering the original data.
- **Labeling and Packaging:**
  - Clearly label each piece of evidence with identifying information (case number, exhibit number, date, time, description).
  - Package evidence securely to prevent damage or tampering (anti-static bags, appropriate containers).
- **Transportation:** Transport evidence securely, maintaining chain of custody.
- **Chain-of-Custody:** A chronological record documenting the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. Every person who handles the evidence must be recorded.
- **Importance of Document and Preservation:** Accurate documentation ensures admissibility in court. Proper preservation prevents alteration or loss of evidence, maintaining its integrity.

Acquisition Process:

- **Write-Blockers:** Hardware or software tools that prevent any writes to the original storage device during the acquisition process, ensuring data integrity.
- **Imaging Techniques:** Creating a bit-by-bit copy (forensic image) of the entire storage device. Common formats include raw (DD) and EnCase (E01).
- **Evidence Integrity:** Verifying that the acquired image is an exact copy of the original. This is typically done using cryptographic hashes (MD5, SHA-1, SHA-256).
- **Standard Operating Procedures (SOPs) for Acquisitions and Preservation of Evidences:** Step-by-step guidelines that forensic examiners follow to ensure consistency, accuracy, and legal admissibility of evidence.

Introduction to Data Recovery and Carving:

- **Importance of Data Recovery in Forensic Investigation:** Recovering deleted, formatted, or damaged data can reveal crucial evidence that would otherwise be inaccessible.
- **Carving Methods:** Techniques used to extract files from unallocated space or fragmented data based on file headers and footers (signatures). This is useful when file system metadata is damaged or missing.
- **Difference between Data Recovery and Carving:**

- **Data Recovery:** Attempts to reconstruct the file system and recover files based on its structure.
- **Data Carving:** Ignores the file system and searches for file signatures within raw data.

- **Data Recovery:** Attempts to reconstruct the file system and recover files based on its structure.
- **Data Carving:** Ignores the file system and searches for file signatures within raw data.

Forensic Analysis Cheat Sheet

Windows OS Architecture:

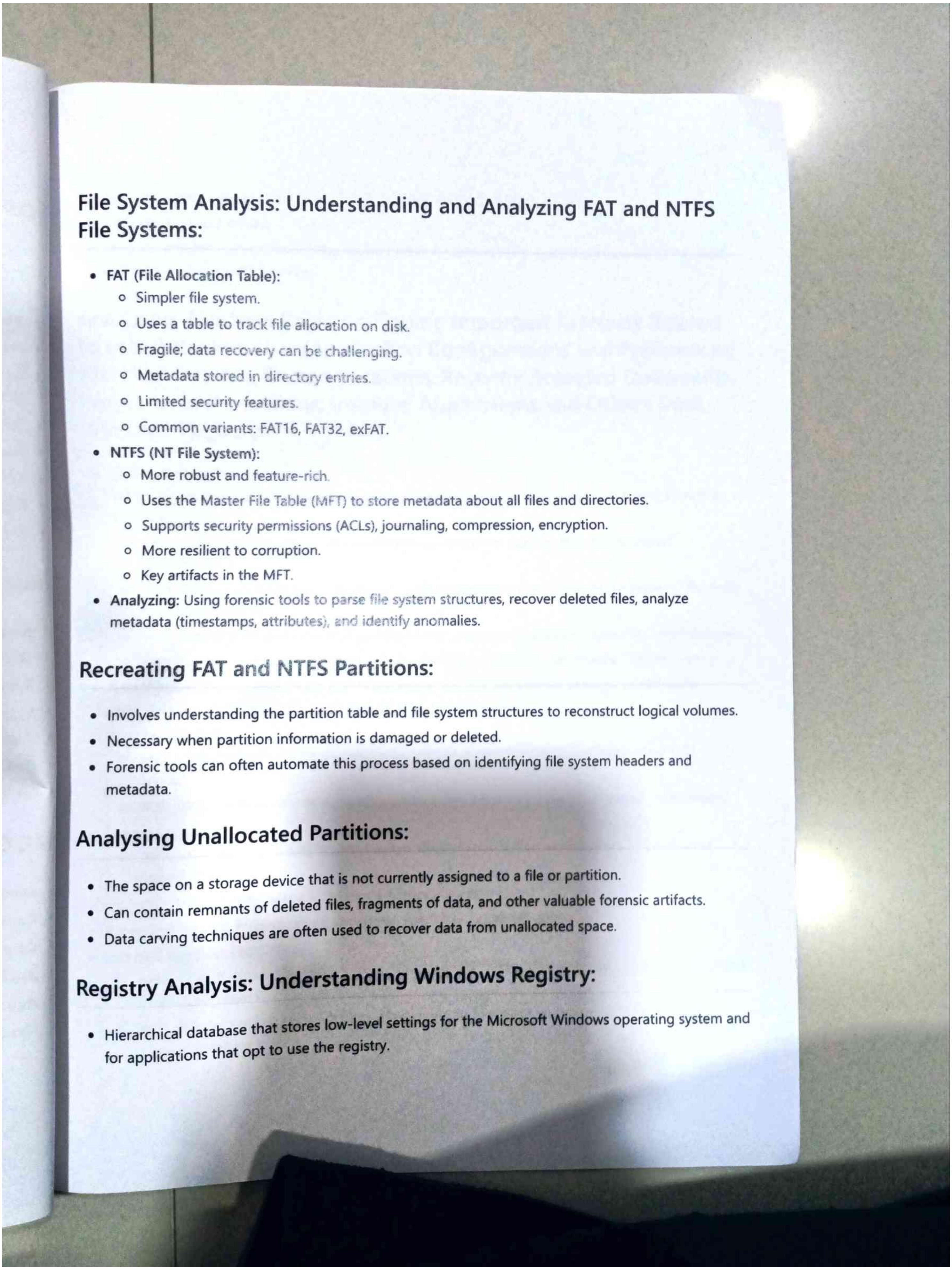
- **Kernel:** Core of the OS, manages hardware and provides services to other components. (NT Kernel)
- **Hardware Abstraction Layer (HAL):** Isolates the kernel from hardware specifics.
- **Executive Services:** Provides core system services (e.g., memory management, process management, I/O).
- **Subsystems:** Provide different operating environments (e.g., Win32, NT Subsystem).
- **User Mode:** Where applications run.
- **Kernel Mode:** Where core OS components run with direct hardware access.
- **Registry:** Hierarchical database storing configuration settings.
- **File System:** Organizes and manages files (NTFS is primary).

Linux OS Architecture:

- **Kernel:** Core of the OS, manages hardware and provides services. (Linux Kernel)
- **Shell:** Command-line interpreter for user interaction. (e.g., Bash, Zsh)
- **System Libraries:** Provide functions for applications to interact with the kernel.
- **System Utilities:** Tools for managing the system (e.g., commands like `ls` , `grep`).
- **X Window System/Wayland:** Graphical display server.
- **Desktop Environment:** Provides a GUI (e.g., GNOME, KDE).
- **File System:** Hierarchical structure starting with `/` (root). Common file systems include ext4, XFS.

MAC OS Architecture:

- **Kernel (XNU):** Hybrid kernel combining Mach microkernel and BSD components.
- **Darwin:** Open-source foundation of macOS.
- **Core Services:** Essential system-level frameworks.
- **Application Frameworks:** Libraries and tools for developers (e.g., Cocoa).
- **Aqua:** Graphical user interface.
- **File System:** HFS+ (older), APFS (current).



File System Analysis: Understanding and Analyzing FAT and NTFS File Systems:

- **FAT (File Allocation Table):**
  - Simpler file system.
  - Uses a table to track file allocation on disk.
  - Fragile; data recovery can be challenging.
  - Metadata stored in directory entries.
  - Limited security features.
  - Common variants: FAT16, FAT32, exFAT.
- **NTFS (NT File System):**
  - More robust and feature-rich.
  - Uses the Master File Table (MFT) to store metadata about all files and directories.
  - Supports security permissions (ACLs), journaling, compression, encryption.
  - More resilient to corruption.
  - Key artifacts in the MFT.
- **Analyzing:** Using forensic tools to parse file system structures, recover deleted files, analyze metadata (timestamps, attributes), and identify anomalies.

Recreating FAT and NTFS Partitions:

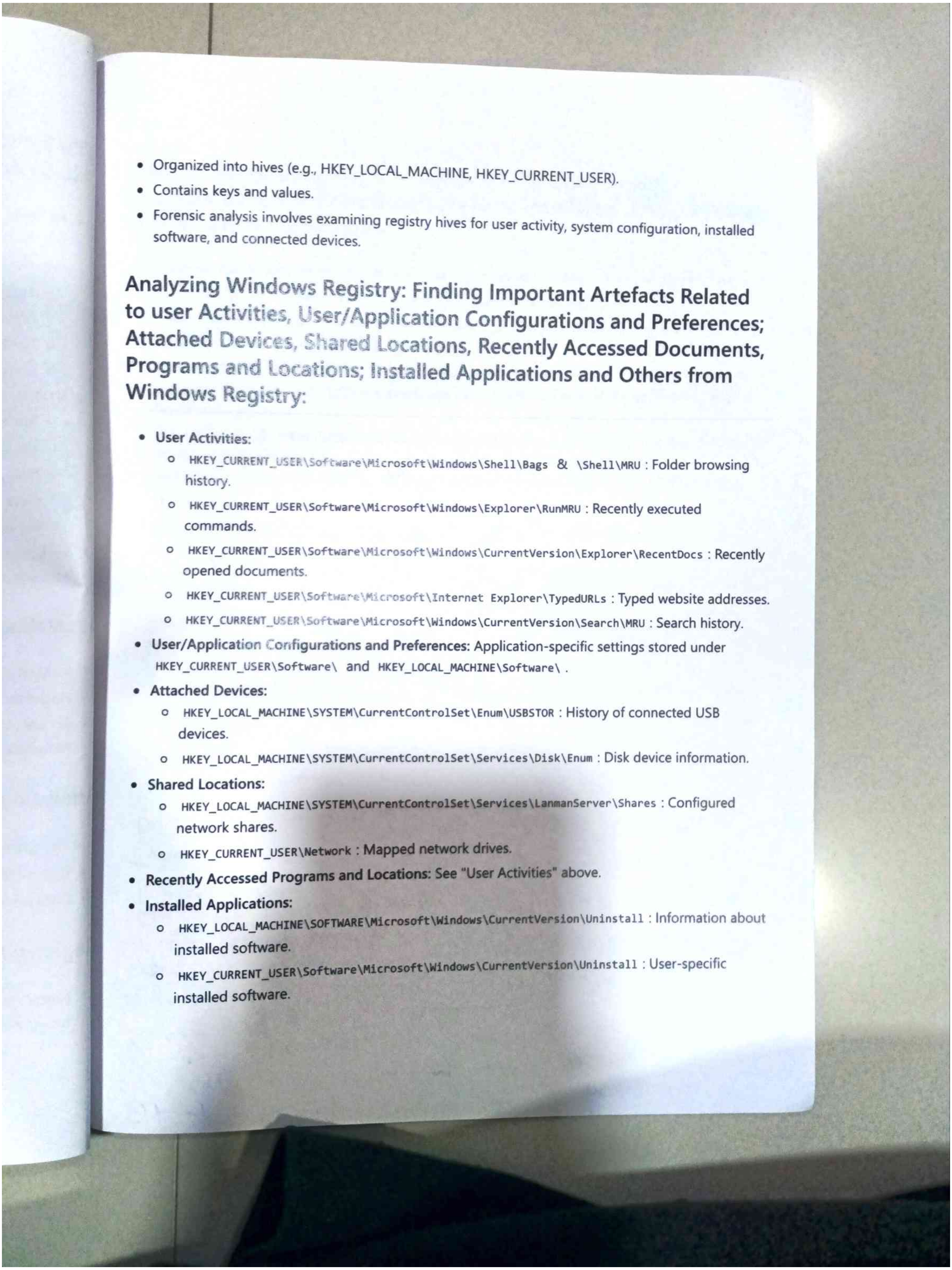
- Involves understanding the partition table and file system structures to reconstruct logical volumes.
- Necessary when partition information is damaged or deleted.
- Forensic tools can often automate this process based on identifying file system headers and metadata.

Analysing Unallocated Partitions:

- The space on a storage device that is not currently assigned to a file or partition.
- Can contain remnants of deleted files, fragments of data, and other valuable forensic artifacts.
- Data carving techniques are often used to recover data from unallocated space.

Registry Analysis: Understanding Windows Registry:

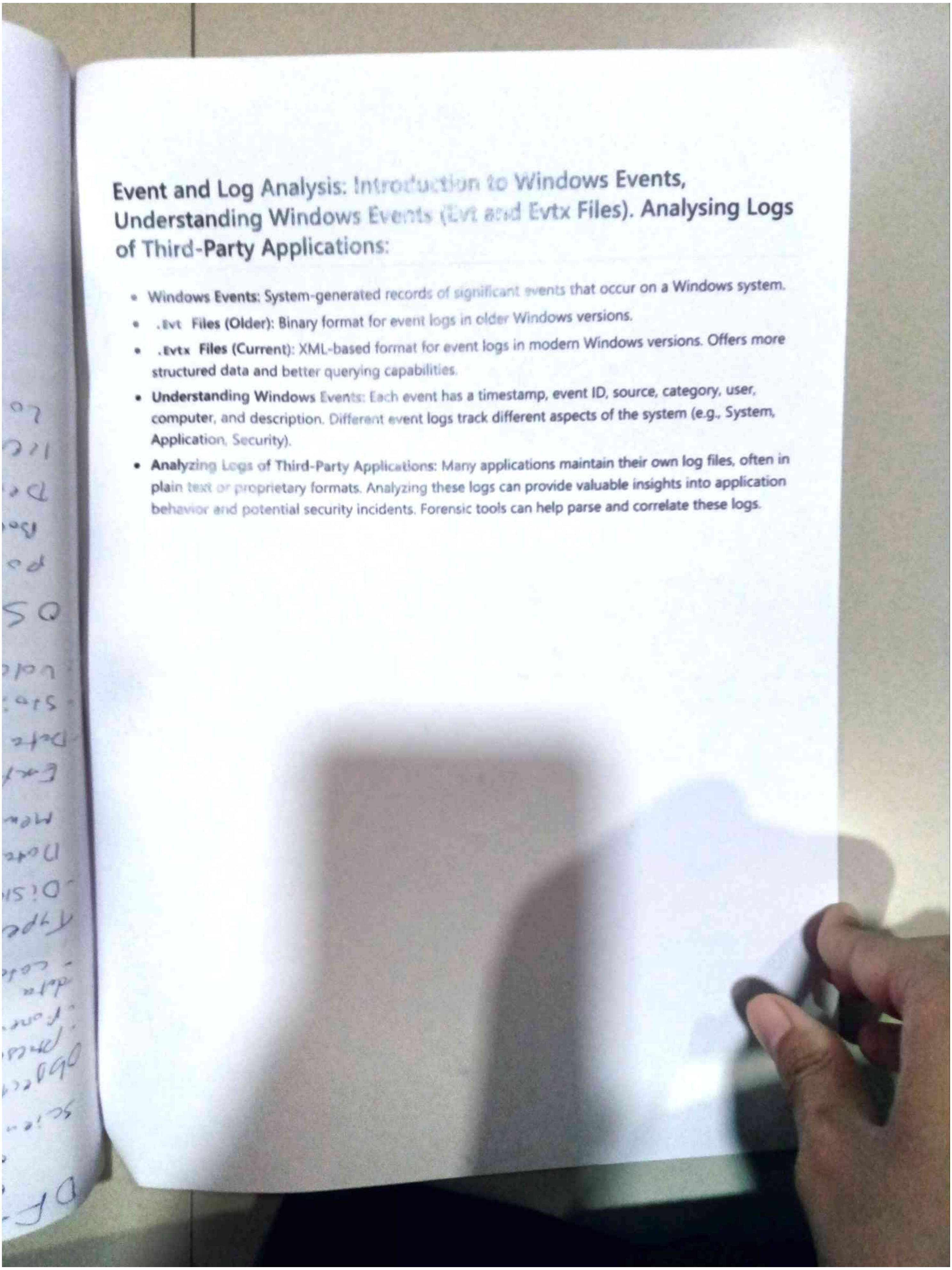
- Hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry.



- Organized into hives (e.g., HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER).
- Contains keys and values.
- Forensic analysis involves examining registry hives for user activity, system configuration, installed software, and connected devices.

Analyzing Windows Registry: Finding Important Artefacts Related to user Activities, User/Application Configurations and Preferences; Attached Devices, Shared Locations, Recently Accessed Documents, Programs and Locations; Installed Applications and Others from Windows Registry:

- **User Activities:**
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Bags` & `\Shell\MRU` : Folder browsing history.
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\Explorer\RunMRU` : Recently executed commands.
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs` : Recently opened documents.
  - `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs` : Typed website addresses.
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Search\MRU` : Search history.
- **User/Application Configurations and Preferences:** Application-specific settings stored under `HKEY_CURRENT_USER\Software\` and `HKEY_LOCAL_MACHINE\Software\` .
- **Attached Devices:**
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR` : History of connected USB devices.
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk\Enum` : Disk device information.
- **Shared Locations:**
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares` : Configured network shares.
  - `HKEY_CURRENT_USER\Network` : Mapped network drives.
- **Recently Accessed Programs and Locations:** See "User Activities" above.
- **Installed Applications:**
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` : Information about installed software.
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall` : User-specific installed software.



Event and Log Analysis: Introduction to Windows Events, Understanding Windows Events (Evt and Evtx Files). Analysing Logs of Third-Party Applications:

- **Windows Events:** System-generated records of significant events that occur on a Windows system.
- **`.Evt` Files (Older):** Binary format for event logs in older Windows versions.
- **`.Evtx` Files (Current):** XML-based format for event logs in modern Windows versions. Offers more structured data and better querying capabilities.
- **Understanding Windows Events:** Each event has a timestamp, event ID, source, category, user, computer, and description. Different event logs track different aspects of the system (e.g., System, Application, Security).
- **Analyzing Logs of Third-Party Applications:** Many applications maintain their own log files, often in plain text or proprietary formats. Analyzing these logs can provide valuable insights into application behavior and potential security incidents. Forensic tools can help parse and correlate these logs.