Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/cybersecurity-forensics-glossary/

TECHNICAL REFERENCE FOR SEARCHABLE DEFINITIONS FOR SECURITY LEADERS, EXECUTIVES AND ATTORNEYS

# Cybersecurity and Forensics Glossary of Decisive Terms

Eight categories cover the vocabulary of a breach report, a forensic examination, an AI security review and an OT assessment. Search a term, filter by category or jump to a letter, and read each definition the way an examiner would explain it across the table.

Technical terms used in incident reports, digital evidence reviews and security assessments, defined the way an examiner would explain them to a client. Search the definitions, choose a category or use the alphabet to jump to a term.

A general technical reference. Applicable duties and evidentiary standards depend on the matter and the jurisdiction, and what happened in a particular system is read from that system's own records.

## Classic Cyber Threats

The techniques and tools that continue to account for most incidents, from adware and botnets to zero day exploits, with the evidence each one tends to leave behind.

### Adware

Software that displays or delivers unsolicited advertising, typically bundled with free applications. Modern adware frequently crosses into spyware territory, tracking browsing habits, search queries, and geographic location without disclosure. In civil litigation, adware found on a device can raise questions about what other unauthorized software may have been installed and what data was collected from the user without their knowledge.

### APT (Advanced Persistent Threat)

Prolonged targeted activity intended to maintain access, obtain information or affect systems. The label describes a threat pattern, and naming a particular actor combines the technical record with threat intelligence and other corroboration. Analysis maps the access, movement and transfers supported by available records and lists each system and period those records cover, so the scope of what was touched, accessed or removed is stated against that coverage.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Back Door

A hidden mechanism, either intentionally built into software by a developer or secretly installed by an attacker, that allows unauthorized access to a system while bypassing normal authentication. Back doors can persist across reboots and survive software updates if embedded deeply enough. Forensic examiners look for back doors during post incident analysis by examining running processes, scheduled tasks, startup entries, and network connections to identify unauthorized persistent access channels.

### Black Hat

A hacker who operates outside legal or ethical boundaries, typically for personal financial gain, espionage, or malicious disruption. The term derives from old Western films where villains wore black hats. Black hat actors may work independently, as part of organized crime groups, or on behalf of state sponsors, and the line between the three is increasingly blurred in modern cybercrime.

### Bot

A compromised device running automated malware that accepts commands from a remote operator, often without any visible sign to the device's owner. Bots are the building blocks of botnets and are routinely recruited through drive by downloads, phishing, or exploitation of unpatched vulnerabilities. A single bot infection can serve as the initial foothold for lateral movement throughout an enterprise network.

### Botnet

Networks of compromised computers (bots) controlled by a threat actor through a command and control (C2) server or peer to peer protocol. Botnets are used to conduct distributed denial of service attacks, send spam at massive scale, mine cryptocurrency, steal credentials, and distribute additional malware. Modern botnets may number in the millions of devices and are leased out as a commodity on underground marketplaces. Forensic analysis of a botnet infection focuses on identifying C2 communication artifacts in network logs, browser history, and system memory.

### Brute Force Attack

A password or key guessing attack that systematically tests candidates. Speed depends on the algorithm, work factor, hardware and whether attempts occur online or against an offline hash. GPU acceleration can help with some offline workloads; rainbow tables are a separate precomputation technique and are less useful against properly salted hashes. Repeated authentication failures followed by a success warrant review, and the examiner corroborates that sequence with source addresses, session activity and account changes before calling it a successful attack.

### Buffer Overflow

A vulnerability that occurs when a program writes more data to a memory buffer than it can hold, overflowing into adjacent memory regions and potentially overwriting control data such as return addresses. Attackers craft malicious input to redirect program execution to their own code (shellcode). Buffer overflow exploits have existed for decades but remain relevant in legacy software, embedded systems, and OT/ICS environments where patching is infrequent.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Command and Control (C2)

Infrastructure and communication paths used to direct compromised systems or receive information from them. Channels may use dedicated servers or legitimate services. Available packet captures, DNS, endpoint and provider records can help test suspected communications and compromise scope. Conclusions rest on corroboration and a stated account of which sources were covered.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

### Cookies

Small data files placed on a user's device by websites to retain session state, preferences, or tracking identifiers. While cookies have legitimate uses, session cookies can be stolen by cross site scripting or man in the middle attacks to hijack authenticated sessions without needing a password. In digital forensic examinations, browser cookie files are a rich source of historical data about sites visited, login times, and user identifiers, even after browsing history has been deleted.

### Cracker

In security parlance, an individual who breaks into systems or bypasses software protections without authorization, as distinguished from a "hacker," whose original meaning referred to creative technical problem solving. The term is also used for tools that crack encrypted passwords or bypass software licensing. Forensic examiners may encounter cracking utilities on suspect devices as evidence of intentional unauthorized access attempts.

### Credential Stuffing

An automated attack that takes username and password pairs from previous data breaches and tests them against other services, exploiting the widespread habit of password reuse. Because the credentials are real and the login attempts appear legitimate, credential stuffing is best detected through behavioral analytics. In a successful credential stuffing attack the attacker simply authenticates normally using stolen data, so the examiner reads login sources, timing and volume across accounts in place of looking for an exploit.

### Cross Site Scripting (XSS)

A web application vulnerability in which an attacker injects malicious scripts into content served to other users' browsers. The victim's browser executes the script in the context of the trusted site, enabling cookie theft, session hijacking, keylogging, and redirection to phishing pages. XSS vulnerabilities frequently appear in source code reviews and are among the most commonly documented findings in web application penetration tests.

### DNS Poisoning

Also called DNS cache poisoning or DNS spoofing, this attack corrupts the cache of a DNS resolver with false records, causing users who query that server to be directed to attacker controlled IP addresses instead of legitimate ones. Victims typically see no visible warning. DNS poisoning is used to redirect banking customers to phishing sites, intercept email, and deliver malware to users who believe they are visiting trusted domains.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### DoS (Denial of Service)

An attack that makes a system, service, or network unavailable by overwhelming it with traffic or requests, or by exploiting a vulnerability that causes the target to crash. A DoS attack originates from a single source, as opposed to a DDoS attack which uses many. Network traffic logs, firewall records, and server access logs are the primary forensic artifacts used to document a DoS incident and attribute responsibility.

### DDoS (Distributed Denial of Service)

A denial of service attack launched simultaneously from thousands or millions of compromised devices (a botnet), making it far more difficult to filter and block than a single source attack. DDoS attacks are sold as a service on the dark web for as little as a few dollars per hour and are used for extortion, competitive sabotage, hacktivism, and as a distraction while attackers conduct other intrusions. Forensic documentation of a DDoS attack involves preserving packet capture data, traffic flow records, and ISP logs in a manner suitable for civil litigation or regulatory reporting.

### Drive By Download

Malware delivery that occurs automatically when a user visits a compromised or malicious web page, without any deliberate action such as clicking a download link. The attack exploits vulnerabilities in browsers, browser plugins (Flash, PDF readers, Java), or the operating system itself. Drive by downloads are a primary delivery mechanism for exploit kits and represent a significant threat to organizations whose employees browse the web on corporate machines.

### Dumpster Diving

Searching discarded documents, packaging or storage media for sensitive information. Exposed material can include account details, passwords and hardware that retains recoverable data. Secure disposal requires appropriate document destruction and media sanitization. Access rights and evidentiary use depend on the location, ownership and applicable law, so counsel confirms the lawful basis before discarded material is collected.

### Easter Egg

A hidden feature or message intentionally embedded in software by developers, activated by undocumented keystrokes or input sequences. Most Easter eggs are harmless and humorous, but they illustrate that production software can contain undisclosed functionality, which becomes relevant when examining software for unauthorized back doors or hidden capabilities. Source code review can identify Easter eggs and distinguish them from malicious hidden functions.

### Exploit Kit

A packaged toolkit, typically deployed on compromised web servers, that automatically probes visiting browsers for known vulnerabilities and delivers the appropriate exploit. Exploit kits like Blackhole (active roughly 2010 to 2013), Angler (active roughly 2013 to 2016), and RIG automated what was once a manual attack process, enabling even low skill actors to infect large numbers of victims. They are frequently the delivery mechanism for ransomware, banking trojans, and credential stealers.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Fileless Malware

Malicious activity that minimizes reliance on standalone executable files, often using memory, scripts or legitimate tools such as PowerShell and WMI. Fileless activity often leaves artifacts all the same: registry hives, event logs, script content and persistence records may remain on disk, and examiners correlate memory captures with those persistent sources. Collection priorities depend on volatility and operational risk.

### Firewall

A device or program that monitors and filters traffic under configured rules. Capabilities differ by product and deployment. Firewall records can support network analysis, and the examiner reads them against the logging settings, traffic paths, drops and retention that define their coverage, corroborating connections with endpoint and provider records.

### Gray Hat

A term used for security research that operates outside explicit authorization, sometimes followed by unsolicited disclosure or a demand for payment. The legal position depends on the conduct, jurisdiction and applicable agreements. Organizations should preserve the disclosure and involve the legal team before authorizing further access.

### Hacker

Broadly, a person with advanced technical skills who uses them to gain access to systems, networks, or data. The term originally described creative problem solvers in the computing community. Today it is used both as a neutral descriptor and as shorthand for a malicious actor; context and the white/gray/black hat distinction clarify intent. In legal proceedings, "hacker" is often used loosely, making precise technical characterization important for forensic expert witnesses.

### Indicators of Compromise (IoC)

Observable artifacts that suggest a system or network has been compromised, including malicious IP addresses, file hashes, domain names, registry keys, and behavioral patterns associated with known threat actors. Security teams share IoCs through threat intelligence platforms to help others detect the same threats quickly. In forensic analysis, documented IoCs provide the evidentiary basis for determining when and how an intrusion occurred and which systems were affected.

### Keylogger

Software or hardware that records keystrokes. A malicious keylogger may capture passwords, messages and business information; some tools also have authorized administrative uses. In corporate matters, examiners assess installation history, configuration, stored records and transmission destinations.

### Kill Chain

A model, originally developed by Lockheed Martin for military targeting, adapted to cybersecurity to describe the sequence of steps an attacker must complete to achieve an objective: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Defenders use the kill chain model to identify which stage an attacker is in and where controls can interrupt the attack. Forensic analysts reconstruct kill chains during post incident review to document exactly how an attacker moved from initial access to final impact.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Lateral Movement

The techniques an attacker uses after gaining initial access to move from system to system within a network, escalating privileges and reaching high value targets such as domain controllers, databases, or sensitive file shares. Common lateral movement methods include pass the hash, remote service exploitation, and abuse of legitimate administrative tools. Identifying lateral movement is a central task in network forensic examinations, since the most damage is often done far from the initial point of entry.

### Living Off the Land (LOTL)

An attack technique in which threat actors use legitimate, preinstalled system tools (such as PowerShell, WMI, PsExec, and certutil) to conduct malicious activities, minimizing the need to deploy custom malware. Because the tools used are trusted by the operating system and standard security products, LOTL attacks evade most signature based detection. Forensic examination of LOTL attacks requires deep analysis of event logs, PowerShell script block logging, and process creation records to distinguish malicious use from normal administrative activity.

### Logic Bomb

Malicious code deliberately inserted into software that lies dormant and fires when a specific trigger condition is met, such as a particular date, time, or the removal of an employee account from the directory. Logic bombs have been used by disgruntled insiders to destroy data or sabotage systems after termination. Source code forensics can identify logic bombs by examining version control history, comparing binaries to source, and flagging conditional constructs tied to time based or personnel based triggers.

### Malware

An umbrella term for any software designed to harm, disrupt, or gain unauthorized access to systems or data. The category includes viruses, worms, trojans, ransomware, spyware, adware, rootkits, and more. Modern malware is often modular, combining multiple capabilities such as credential theft, lateral movement, and data exfiltration into a single infection. Forensic malware analysis involves static examination of code, dynamic analysis in sandboxed environments, and behavioral correlation with network and endpoint logs.

### Man in the Middle (MitM)

An attack in which an adversary secretly positions themselves between two communicating parties, intercepting and potentially altering traffic while each party believes they are communicating directly with the other. MitM attacks are conducted through ARP spoofing, DNS poisoning, rogue Wi-Fi access points, and SSL stripping. They are particularly dangerous in financial transactions and authentication flows. TLS certificate analysis and packet captures are key forensic tools for documenting a MitM event.

### Master Program

In early botnet architecture, a master program was the central controller used by an attacker to issue commands to handler systems, which in turn relayed instructions to individual compromised hosts. The term is less common today as C2 infrastructure has grown more sophisticated, but the underlying concept of hierarchical botnet control remains relevant in analyzing legacy malware and attribution in older intrusion cases.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Payload

The component of a malware package that carries out the intended malicious action, distinct from the delivery or exploit mechanism. Payloads may encrypt files (ransomware), exfiltrate data, delete records, install a back door, or enlist the system in a botnet. Identifying the payload is a central goal of malware analysis, as it determines the actual harm caused and informs both remediation and the legal theory of damages in litigation.

### Phishing

Deceptive messages, calls or sites intended to induce actions such as revealing credentials, authorizing a payment or opening malicious content. Spear phishing targets selected recipients; whaling targets senior decision makers. Headers, links, account records and endpoint artifacts can support analysis of delivery and subsequent access, each read within its own coverage. The responsible decision maker and the legal team weigh employee reasonableness and legal consequences.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response · MITRE phishing techniques

### Phreaker

A practitioner of phone phreaking, the manipulation of telephone systems to make free calls, redirect calls, or gain unauthorized access to phone company infrastructure. Phreaking culture in the 1960s-1980s directly shaped the early hacker community. While classic phreaking techniques are largely obsolete, modern variants target VoIP systems, SS7 networks, and cellular provider infrastructure to intercept calls, redirect two factor authentication SMS codes, or conduct toll fraud.

### Polymorphic Virus

A virus that mutates its own code with each replication, changing its signature while preserving its function, specifically to evade signature based antivirus detection. Metamorphic viruses take this further by rewriting their entire logic, not just encrypting the payload. Detecting polymorphic malware requires behavioral analysis and heuristic scanning rather than static signature matching. Forensic analysis of polymorphic infections often involves unpacking the virus in a controlled environment to identify its underlying function.

### Privilege Escalation

The process by which an attacker with limited access gains higher level permissions, moving from a standard user account to local administrator, then to domain administrator or system level access. Privilege escalation exploits misconfigurations, unpatched vulnerabilities, weak service account credentials, and overly permissive Group Policy settings. Forensic examiners document privilege escalation by reviewing security event logs for unusual account activities, token manipulation events, and unexpected changes to group membership.

### Rootkit

Software designed to maintain access while hiding activity from users, administrators or security tools. Kernel mode rootkits operate within the operating system's kernel; bootkits and firmware implants act at other layers. Concealment may affect processes, files, connections or registry data. Examiners compare trusted acquisition results, memory and other independent artifacts because a compromised operating system may return misleading information.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Script Kiddie

An inexperienced attacker who uses prewritten tools, exploit scripts, and automated frameworks without understanding the underlying technical mechanisms. While script kiddies are unsophisticated, they cause real harm by deploying tools that were designed by skilled actors. Many ransomware incidents and web defacements are carried out by script kiddies using commodity exploit kits. Commodity tooling leaves fewer distinctive techniques to compare, so examiners lean on infrastructure, account and timing evidence when attribution is the question.

### Social Engineering

The manipulation of people rather than technology to obtain unauthorized access to information, systems, or facilities. Social engineering exploits human psychology, including trust, authority, urgency, and fear, more reliably than most technical attacks. Pretexting (creating a false identity), vishing (voice phishing), baiting (leaving infected USB drives), and tailgating (following authorized personnel into secured areas) are all social engineering techniques. In legal proceedings, establishing that an organization's staff were deceived rather than negligent can be critical to liability determinations.

### Spam

Unsolicited bulk electronic messages, commonly delivered through email or messaging services. Some campaigns distribute phishing, malware or fraud. Available headers can describe recorded relays, and because fields can be forged, the examiner tests each one and correlates provider, account and delivery records before attributing a campaign to a botnet, device or person.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

### Spoofing

The falsification of identifying information in a communication, such as an email sender address, IP address, caller ID, GPS coordinates, or website URL, to deceive recipients into believing the communication comes from a trusted source. Email spoofing is foundational to business email compromise (BEC) fraud. Forensic analysis of spoofed communications focuses on examining headers, authentication records (DMARC, SPF, DKIM), and network logs to distinguish the claimed source from the actual origin.

### Spyware

Software used to monitor device activity and collect information without appropriate authorization. Capabilities may include keystroke capture, screenshots, location tracking or access to microphones and cameras. In corporate espionage and unauthorized access matters, forensic analysis examines installation artifacts, permissions, captured records and possible transmission destinations. Scope and lawful access are established first, and collection follows.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### SQL Injection

A vulnerability in which untrusted input alters a database query or command. Depending on the application and permissions, exploitation can expose or change records or affect other functions. Enabled and retained application, database and web logs may show requests and execution. The examiner reads their fields, filtering, redaction and retention to set how precisely the queries and accessed data can be stated, and validates important findings against the other available sources.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response · OWASP SQL injection guidance

### Supply Chain Attack

An attack that targets a less secure element in an organization's supply chain, such as a software vendor, managed service provider, or hardware manufacturer, to gain access to the ultimate target. The SolarWinds incident, in which malicious code was injected into a software update trusted by thousands of organizations, is the defining example. Supply chain attacks are particularly difficult to detect because the malicious component arrives through a trusted update or delivery channel. Forensic analysis must trace the intrusion back to its origin in the supply chain rather than assuming the organization's own perimeter was breached directly.

### Time Bomb

A variant of a logic bomb that triggers based on a specific date or time rather than another condition. Time bombs have been used by software vendors to disable unlicensed software, but are more dangerously employed by malicious insiders to cause damage at a predetermined future date, often after the perpetrator has left the organization. Forensic examination of scheduled tasks, cron jobs, and time based conditional code is standard practice when a time bomb is suspected.

### Trojan

Malicious software presented as a legitimate application or component. A trojan spreads by delivery rather than self replication, and delivery can involve a user action, another malware component or a compromised software channel. Its payload may steal data, install a back door or provide remote access. Examiners use file metadata, hashes, execution records and controlled behavioral analysis to assess what it did.

### Virus

Malicious code that replicates by attaching to another executable object, such as a program or boot area. Replication requires execution of infected code, which may be triggered by a user or an automated process. This differs from a standalone network worm. Examiners compare file content, execution history and behavioral evidence to assess spread and impact.

### Wardriving

The practice of driving or walking through an area with a Wi-Fi enabled device to identify and map wireless networks, typically for the purpose of finding unsecured access points to exploit. Data collected during wardriving can include network names, encryption types, and GPS coordinates. The term now extends to any mobile scanning of wireless networks; warwalking and warbiking are common variants. Evidence of wardriving software on a device can be forensically significant in cases involving unauthorized network access.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Watering Hole Attack

An attack that compromises a site or service used by an intended group to create an opportunity for malicious delivery or redirection. Whether a visit led to infection depends on the exploit, device state and interaction, and the examiner tests it against available device, network and provider evidence.

NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management · MITRE drive by compromise

### White Hat

A security professional who uses hacking techniques with explicit authorization to identify and remediate vulnerabilities before malicious actors can exploit them. White hat activities include penetration testing, vulnerability assessments, and bug bounty research. Their findings are documented and disclosed to the organization rather than exploited. Engagement letters and scoping agreements are essential to establishing the legal authorization that distinguishes white hat work from criminal conduct.

### Worm

Self replicating malware that spreads across networks without requiring user interaction or a host file, exploiting vulnerabilities in network services to copy itself from machine to machine. Worms consume bandwidth and system resources as well as whatever malicious payload they carry. The WannaCry and NotPetya incidents demonstrated how a single worm can propagate across hundreds of thousands of systems in hours, causing billions of dollars in damages. Network traffic logs, firewall records, and endpoint detection data are used forensically to trace worm propagation paths.

### Zero Day Threat / Exploit

A vulnerability exploited before an effective fix or established defensive response is available, commonly before the vendor or defenders know about it. Vendor awareness, disclosure, exploitation and patch availability can occur on different dates. Analysis therefore relies on the actual timeline and observed behavior, including whatever detection coverage was in place.

### Zombie / Zombie Drone

A compromised computer that is remotely controlled by an attacker and used to carry out attacks or transmit spam without the knowledge of its owner. Zombies are the individual nodes that make up botnets. The owner of a zombie device is typically an innocent victim who unknowingly contributes to attacks against others. Forensic analysis of a suspected zombie device focuses on identifying the malware responsible, the C2 server it communicates with, and what actions were taken using the device's resources.

© 2026 Global Digital Forensics, Inc. All rights reserved.

# AI and Machine Learning Threats

The attacks that target machine learning systems and the attacks that use them, written for the leaders who are deciding how far to trust a model.

### Adversarial Machine Learning

The study of attacks on machine learning systems and the defenses against them. Attacks may target training data, model parameters, inference inputs, system integrations or private information exposed through outputs. Some input perturbations are difficult for people to notice, and others work while plainly visible. Testing should state the attacker's access, objective, capabilities and the scope of the assessment.

### AI Bias

Systematic errors in AI model outputs caused by biased training data, flawed model design, or unrepresentative sampling. AI bias can result in discriminatory outcomes in hiring, lending, law enforcement, and medical diagnosis. In litigation, AI bias has become a significant legal issue under antidiscrimination statutes. Forensic analysis of AI systems can document the training data composition, model architecture decisions, and output patterns that give rise to biased results.

### AI Governance

Policies, responsibilities and controls for managing an AI system through its lifecycle. Documentation, testing, monitoring and human oversight should match the system’s use and risk. Legal duties vary by jurisdiction, sector and use case; a voluntary risk framework organizes the program, and compliance is measured against the duties the organization's lawyers confirm for it.

### AI Hallucination

The generation by a large language model or other generative AI system of confident, plausible sounding but factually incorrect or entirely fabricated content. Hallucinations arise from the statistical nature of language model training rather than from any intent by the model to deceive. In legal and forensic contexts, AI hallucinations in submitted documents or expert analyses have led to sanctions and disciplinary actions, underscoring the need for human verification of all AI generated content used in proceedings.

### AI Supply Chain Attack

An attack targeting the development pipeline of an AI system, including training data repositories, pretrained model weights, ML libraries, or model hosting infrastructure. By compromising an upstream component, an attacker can introduce vulnerabilities or malicious behaviors into AI systems used by many downstream organizations. The attack vector is analogous to traditional software supply chain attacks but uniquely difficult to detect because the malicious behavior may only manifest under specific input conditions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### AI Model Poisoning

An attack that alters a model's learned behavior through malicious training contributions, parameter changes or a compromised training process. Data poisoning targets the training data; model poisoning can target weights or updates directly. Effects can include degraded accuracy, biased outputs or trigger dependent behavior. Review requires data provenance, model version records and evaluation of the affected training and deployment stages.

### AI Red Teaming

Authorized adversarial testing of an AI system under defined access, objectives and conditions. Findings should record the system and model versions, prompts, connected tools, attempts and observed outputs. Whether testing is legally required depends on the applicable use and jurisdiction.

### Alignment Failure

A situation in which an AI system pursues goals or produces outputs that do not reflect the values, intentions, or constraints specified by its designers or operators. Alignment failures range from minor misinterpretations of user instructions to potentially dangerous autonomous actions. In high stakes applications such as autonomous vehicles, medical diagnostics, and critical infrastructure control, alignment failures have direct safety implications. Documenting alignment failures is an emerging area of AI forensics.

### Automated Social Engineering

The use of language models, voice synthesis or automation to produce deceptive messages and impersonation attempts at scale. These tools can personalize phishing and vishing, so when AI authorship is the question, examiners weigh writing style together with message headers, account records, delivery infrastructure, audio provenance and independent evidence of the sender's actions.

### Autonomous Weapon System

A weapon system that uses artificial intelligence to select and engage targets without human intervention. Autonomous weapon systems raise profound legal and ethical questions under international humanitarian law, including questions of accountability when the system causes unlawful harm. From a cybersecurity standpoint, these systems are attack targets: compromising the AI component of an autonomous weapon could cause it to misidentify or attack unintended targets.

### Data Poisoning

The deliberate injection of corrupted, mislabeled, or manipulated data into training datasets to degrade the performance of a machine learning model or introduce specific vulnerabilities. The poisoned data corrupts the model when it is ingested during training, causing degraded accuracy or introducing hidden backdoors that an attacker can trigger later. Defenders counter data poisoning through data provenance tracking, anomaly detection during training, and outlier resistant statistical techniques that reduce the influence of outlying data points.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Deepfake

Synthetic media, typically video or audio, in which a person's likeness, voice, or words are replaced or fabricated using deep learning techniques such as generative adversarial networks. Deepfakes are used for fraud (including CEO impersonation in wire transfer scams), disinformation, nonconsensual intimate imagery, and evidence fabrication. GDF's forensic analysis of suspected deepfakes examines pixel level artifacts, facial landmark inconsistencies, audio spectral anomalies, and metadata to assess authenticity. Courts are increasingly confronted with deepfake evidence challenges.

### Evasion Attack

An adversarial attack that crafts inputs to fool a deployed machine learning model into misclassification, without modifying the model itself. Evasion attacks are inference time attacks, meaning they occur when the model is being used rather than when it is being trained. Classic examples include adding imperceptible noise to images to cause image classifiers to fail, or modifying malware code to evade ML based antivirus engines while preserving malicious functionality.

### Explainable AI (XAI)

Methods intended to help people understand an AI system’s outputs or behavior. An explanation may be approximate, so it is checked against the actual model and decision context. Accuracy, fairness and compliance are each tested separately alongside the explanation, and any legal explanation requirement depends on the applicable jurisdiction and use.

### GANs (Generative Adversarial Networks)

A class of neural network architecture consisting of two models, a generator and a discriminator, that compete against each other to produce increasingly realistic synthetic content. GANs were the dominant technology behind early deepfake systems and synthetic image generators, though diffusion models have largely supplanted them in modern synthetic media tools. They are also used legitimately in drug discovery, image enhancement, and data augmentation. From a security standpoint, GANs enable creation of synthetic faces, documents, and audio that may be used to defeat biometric authentication or fabricate evidence.

### Large Language Model Jailbreak

A technique for bypassing the safety guidelines and content filters built into a large language model (LLM) by crafting inputs that cause the model to produce content it is designed to refuse, such as instructions for creating weapons, malware, or harmful content. Jailbreaks exploit the tension between model helpfulness and safety guardrails. They are documented through AI red team exercises, and new jailbreak techniques are continuously discovered as models evolve and safety measures are updated.

### Membership Inference Attack

An attack that attempts to estimate whether a particular record was used to train a model. Results depend on model access, the method, the task and false positive or false negative risk. A positive inference is weighed against those error rates and corroborated before membership is concluded, and testing documents the attacker’s access, comparison data and validation steps; legal and privacy consequences depend on the actual facts and applicable requirements.

NIST AI 100-2 E2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Model Extraction Attack

An attack in which an adversary queries a machine learning model's API extensively to reconstruct a functional replica of the model without access to its internal parameters or training data. The extracted model can then be used to craft more effective adversarial attacks or stolen as intellectual property. Model extraction attacks raise trade secret and IP protection questions for organizations that have invested significant resources in proprietary AI model development.

### Model Inversion Attack

An attack that attempts to infer sensitive features or representative inputs from a model’s behavior or outputs. Depending on the model and access, reconstructed material may reveal patterns or approximate characteristics. Whether the output matches an actual training record or a particular individual is a separate question the evaluation tests. Evaluation should state the information available to the attacker, method, validation and uncertainty.

NIST AI 100-2 E2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations

### Neural Backdoor

A hidden vulnerability embedded in a neural network during training that causes the model to behave normally under standard inputs but produce attacker specified outputs when a particular trigger pattern is present in the input. Neural backdoors are a form of model poisoning, and because the model performs correctly on standard inputs, detection calls for trigger focused testing and provenance review beyond normal model evaluation.

### Prompt Injection

An attack against large language model based applications in which malicious instructions are embedded in user controlled input, causing the model to override its system instructions and take unintended actions. In agentic AI systems that can execute code, browse the web, or send emails, prompt injection can lead to unauthorized data exfiltration or system compromise. Prompt injection is among the most critical vulnerabilities in LLM integrated applications and is listed in the OWASP Top 10 for LLMs.

### Shadow AI

The use of AI tools by employees without the knowledge or approval of their organization's IT and security teams. Analogous to shadow IT, shadow AI creates risks including the exposure of confidential or regulated data to third party AI providers, intellectual property loss, and the use of unapproved and unvetted AI outputs in business decisions. Organizations are increasingly discovering shadow AI usage through data loss prevention tools and network traffic analysis.

### Synthetic Identity Fraud

Fraud that combines real and fabricated personal information into a fictitious identity. It may be used to open accounts, obtain credit or defeat identity checks. Generative tools can help fabricate supporting documents or media. Real people are harmed too when their identifiers are reused, and lenders may initially treat the account as genuine. Analysis correlates application records, documents, devices and transaction history.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Transfer Learning Attack

An attack on a pretrained model or its adaptation process that seeks to influence downstream behavior. A backdoor or other weakness in a base model may survive fine tuning, and whether it carries through depends on the task, training and defenses. Review should cover model provenance, integrity checks, training data, updates and deployment specific testing.

### Voice Cloning

The use of AI to generate a synthetic replica of a specific person's voice from a small sample of audio, capable of saying anything the attacker specifies. Voice clones are used in vishing attacks, CEO fraud, and the generation of fake audio evidence. Audio forensic analysis can sometimes detect voice cloning through spectral analysis, prosody examination, and comparison with known authentic recordings, though detection is increasingly challenging as synthesis quality improves.

## Dark Web and Underground

The markets, services and roles behind modern cybercrime, useful when a report traces stolen data or credentials to an underground source.

### .onion

A special use domain for Tor onion services. A version 3 onion address has a 56 character base32 label encoding a public key, checksum and version byte. Onion services conceal network locations and support both legitimate privacy sensitive publishing and criminal activity. An onion address or Tor artifact is a lead for further analysis, which the examiner corroborates with browser, account and transaction records before any conclusion about conduct.

### Access as a Service

A dark web market offering in which initial access brokers sell authenticated access to compromised corporate networks, including VPN credentials, remote desktop sessions, and webshell access. Purchasers typically use this access to deploy ransomware or conduct further intrusion. The existence of access as a service listings for a specific organization is a critical threat intelligence indicator that warrants immediate incident response action. Prices range from a few hundred dollars to tens of thousands depending on the value and privilege level of the access sold.

### Bulletproof Hosting

Web hosting services operated in jurisdictions with weak cybercrime laws or corrupt enforcement, specifically designed to ignore takedown requests from law enforcement and abuse complaints from victims. Bulletproof hosting providers knowingly host phishing pages, malware distribution servers, C2 infrastructure, and child exploitation material. They are a foundational infrastructure element for cybercriminal operations globally. Attribution of cybercrime often requires tracing C2 infrastructure back through bulletproof hosting providers to underlying operators.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Canary Trap

Distribution of distinguishable versions of information to help trace a later disclosure. A match may indicate which version reached another channel, and tying it to the person responsible means testing forwarding, shared access and other copies against the recipient records. Document version assignment, authorized recipients, access and capture history, and assess corroborating evidence within lawful scope.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

### Cryptocurrency Tumbler / Mixer

A service that pools cryptocurrency from multiple sources and redistributes it to make blockchain transaction tracing difficult, serving as a money laundering mechanism for ransomware proceeds, dark web market revenue, and other illicit crypto flows. Blockchain analytics firms and law enforcement have developed techniques to demix tumbled transactions, and several major mixing services have been seized by the FBI and Europol. Financial forensics involving cryptocurrency increasingly requires specialized blockchain analysis tools and expertise.

### Dark Web

The portion of the internet accessible only through specialized anonymizing software such as Tor or I2P, not indexed by standard search engines and not accessible through ordinary browsers. The dark web encompasses a range of activity, from privacy conscious communications to criminal marketplaces for stolen data, drugs, weapons, and cybercrime services. Organizations monitor the dark web for their own stolen credentials, data, and internal documents as part of threat intelligence programs. GDF assists attorneys and corporate clients in dark web monitoring and evidence collection for litigation.

### Dark Web Marketplace

An online market operating on the Tor network where purchasers and sellers transact in stolen data, malware, drugs, counterfeit documents, and criminal services using cryptocurrency. Notable examples have included Silk Road, AlphaBay, and Hansa, all of which were shut down by law enforcement. Dark web marketplaces operate with feedback systems, dispute resolution, and escrow services, mirroring legitimate e commerce. Evidence from dark web marketplace transactions has been used in numerous federal criminal prosecutions.

### Dead Drop

A method of communication in which parties exchange information without direct contact, traditionally using physical locations in espionage but adapted to digital contexts as a covert channel. Digital dead drops may use draft email folders shared between accounts, steganographically hidden messages in image files, or covert data embedded in cloud storage. Forensic identification of dead drop communications requires examining access logs, draft folders, and file modification timestamps across multiple accounts.

### Digital Escrow

In the context of dark web marketplaces, a system in which a trusted third party holds cryptocurrency payment until the purchaser confirms receipt of purchased goods or services, reducing fraud between criminal actors. Legitimate digital escrow exists in legal e commerce and software licensing contexts. Forensic examination of dark web escrow transaction records is used to trace the financial relationship between criminal actors and the timing of illicit transactions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Doxing

The public disclosure of an individual's private personal information, including home address, employer, family members, and financial details, without consent and typically with intent to harass, intimidate, or facilitate physical harm. Doxing is used as a harassment tool, a coercion mechanism against whistleblowers and journalists, and as precursor to "swatting" (calling in false emergency reports to a victim's address). Doxing activity leaves digital traces including forum posts, search queries, and data broker account records that are amenable to forensic analysis.

### Exit Scam

A fraud scheme common in dark web marketplaces in which the marketplace operators or vendors accumulate funds in escrow or customer deposits, then disappear with the funds without delivering purchased goods or services. Exit scams have resulted in losses of tens of millions of dollars from dark web marketplace users. They illustrate the fundamental trust problem in criminal ecosystems: the same anonymity that protects criminals from law enforcement also prevents them from reliably enforcing agreements with each other.

### I2P (Invisible Internet Project)

An anonymizing network overlay that routes traffic through a series of encrypted tunnels to provide privacy and resist traffic analysis. Unlike Tor, which is primarily used to access the public internet anonymously, I2P is optimized for internal network services (hidden services, messaging, file sharing). I2P is used by some threat actors as an alternative to Tor for C2 communications and dark web services, making it relevant in network forensic analysis of advanced threat actors.

### Initial Access Broker (IAB)

A threat actor who specializes in breaching organizations and selling the resulting network access to other criminal groups rather than exploiting it directly. IABs have become a distinct and important role in the ransomware supply chain, enabling ransomware operators to focus on deployment and extortion while outsourcing the technical work of gaining initial access. Identifying whether an IAB was involved in a breach changes the scope of the forensic examination and may affect attribution.

### Money Mule

An individual who transfers illegally obtained funds on behalf of a criminal organization, typically retaining a percentage as payment. Money mules are often recruited through work from home scams and may not initially understand they are participating in fraud. They serve a critical role in laundering proceeds from phishing, romance fraud, business email compromise, and ransomware attacks. Bank transaction records, email communications, and wire transfer logs are the primary forensic artifacts in money mule examinations.

### Paste Site

A service for sharing text, often through public or restricted links. Such services have legitimate uses and can also host stolen material, malicious code or extortion messages. A preserved post can support when material was publicly available, subject to the reliability of its timestamps and capture.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Ransomware as a Service (RaaS)

A criminal business model in which ransomware developers license their malware and supporting infrastructure to affiliates who conduct attacks and share a percentage of ransom payments with the developers. RaaS has transformed ransomware from a niche attack into an industrialized criminal enterprise, enabling even technically unsophisticated actors to deploy sophisticated ransomware. Major RaaS groups include LockBit, BlackCat/ALPHV, and Clop. Forensic examination of a RaaS attack must distinguish affiliate activity from developer activity to properly attribute the intrusion.

### Stealer Logs

Databases of credentials, cookies, browser history, and financial data harvested by information stealing malware such as Redline, Raccoon, and Vidar, and sold or distributed on dark web forums and Telegram channels. Stealer logs have become one of the primary sources of initial access for threat actors, supplying credentials for credential stuffing attacks and initial access broker listings. A corporate device appearing in publicly circulating stealer logs is a significant indicator of compromise requiring immediate forensic response.

### Tor (The Onion Router)

A privacy network that routes internet traffic through a series of volunteer operated relay nodes, wrapping the traffic in multiple layers of encryption before transmission so that each relay decrypts only one layer and learns only the previous and next hop, meaning no single node knows both the origin and destination. Tor is used by journalists, activists, law enforcement, and privacy conscious individuals for legitimate purposes, as well as by criminals to obscure their location and identity. The presence of Tor browser artifacts on a device is forensically significant and may indicate dark web activity, and the examiner reads it alongside the device's other records, accounts and timeline before any question of conduct is weighed.

### Underground Forum

An online community, typically operating on the dark web or in encrypted channels, where cybercriminals share techniques, tools, and services, buy and sell stolen data, and recruit collaborators. Major Russian language underground forums such as XSS, Exploit.in, and RaidForums (now defunct) have served as hubs for sophisticated criminal activity for decades. Law enforcement agencies monitor underground forums for threat intelligence, and posts from specific forums are frequently presented as evidence in criminal prosecutions.

### Warrant Canary

A periodically published statement about whether a provider has received a specified category of government demand. A changed or withdrawn statement can have several explanations, so a lawyer reads it alongside the provider's other notices and disclosures. Disclosure restrictions and the legal treatment of canaries vary. Counsel should assess a particular notice and its legal context.

© 2026 Global Digital Forensics, Inc. All rights reserved.

# Digital Forensics and Incident Response

The vocabulary of preservation, acquisition, analysis and reporting that attorneys and executives will hear from an examiner and from the other side's expert.

### Anti Forensics

Techniques that destroy, obscure or alter potential digital evidence, including log clearing, timestamp manipulation, secure deletion and concealment. Encryption and deletion also have legitimate uses. Examiners document the mechanism, timeline and available context and read the presence of a tool as one fact among many, while intent, spoliation or guilt are decided on the full facts under the applicable standards.

### Artifact Analysis

Examination of retained digital records such as registry entries, file system metadata, browser history and event logs to test events or explanations. Each source has its own meaning, version dependencies and retention period. Correlation can support a chronology, and the examiner keeps record coverage, source changes and alternative explanations visible in the report, so each action in the chronology is tied to the artifacts that support it.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

### Bit for Bit Copy

A copy of the readable, addressable data within a defined acquisition scope, commonly a sector level disk image. It can preserve allocated data, metadata and readable unallocated space, and the examiner records which areas were readable and how TRIM and deletion affect what remains for recovery. Examiners document source protection, read errors, acquisition scope and hash verification. A forensic image file and a directly usable disk clone are distinct outputs.

### Chain of Custody

The documented, unbroken sequence of possession, control, transfer, and analysis of evidence from the moment of collection to its presentation in a legal proceeding. Continuous, consistent custody documentation is what the examiner relies on when opposing counsel questions the admissibility or integrity of evidence. GDF maintains meticulous chain of custody documentation for every piece of evidence it handles, including signed receipts, transfer logs, storage location records, and access controls.

### Cyber Kill Chain

Lockheed Martin's adaptation of the military kill chain concept to cybersecurity, describing seven phases of a cyberattack: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. The model provides a structured framework for understanding how attacks progress and where defenders can interrupt them. Post incident forensic analysis frequently maps observed attacker activity to kill chain phases to communicate the attack narrative to executives, attorneys, and insurers.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Dead Box Forensics

Examination of a powered off device using data retained on nonvolatile storage. This avoids changes from a running operating system, and when RAM, live connections or in memory keys matter, they are captured by live acquisition beforehand. Powering off can lock encrypted volumes, so the choice between live and powered off acquisition depends on evidence priorities, safety, encryption, authority and the specific device.

### Diamond Model of Intrusion Analysis

A threat intelligence framework that models every intrusion event as having four core features: adversary, infrastructure, capability, and victim, connected at the vertices of a diamond. The model enables analysts to pivot from any known feature to discover related information about the others, facilitating threat actor attribution and pattern recognition across multiple incidents. The Diamond Model is particularly useful for structured analytic products used in intelligence sharing and litigation support.

### Digital Forensic Imaging

Creating a documented forensic copy of a defined data source. Acquisitions may be physical, logical, targeted or live, depending on the device, authority and available access. Raw images and containers such as E01 or AFF4 have different structures. Write protection is used where appropriate; unavoidable changes and read errors are recorded. Hashes and acquisition logs support integrity checks, and the court decides admissibility on the full record.

### Evidence Spoliation

The intentional or negligent destruction, alteration, concealment, or failure to preserve evidence that is known to be relevant to anticipated or ongoing litigation. Courts have broad authority to sanction spoliation, ranging from adverse inference instructions to default judgment. In digital matters, common acts of spoliation include reformatting drives, running file shredders, deleting emails after a litigation hold should have been in place, and allowing automated deletion policies to continue running after a preservation obligation arose. Forensic analysis can often detect that spoliation occurred even when the underlying data is gone.

### File Carving

A forensic technique that recovers files from unallocated disk space by identifying known file headers and footers within raw data, without relying on file system metadata. When files are deleted, the file system entry is removed, and the underlying data often stays on the disk, recoverable, up to the point it is overwritten. File carving can recover images, documents, video fragments, and database records even from formatted or partially overwritten drives. Tools such as Foremost, Scalpel, and Magnet AXIOM perform file carving as part of full forensic examinations.

### First Responder Protocol

The initial procedures for documenting a digital incident, protecting evidence and recording custody. Actions depend on safety, authority, encryption and the operating environment. A qualified responder may capture volatile information before shutdown, but doing so changes the running system and must be documented. Whether to power off, leave running or execute collection tools is decided device by device.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Forensic Timeline Analysis

The process of correlating timestamps from multiple sources, including file system metadata, event logs, registry hives, browser history, and network logs, to construct a chronological narrative of events on a system or across a network. Timeline analysis is essential for establishing when an intrusion began, when specific actions were taken, and how events relate to each other across multiple devices and accounts. In litigation, a well constructed forensic timeline is one of the most persuasive forms of digital evidence because it tells a coherent story supported by multiple independent data sources.

### Hash Value

A fixed length digest computed from data, often displayed in hexadecimal. Suitable cryptographic hashes, such as SHA-256, support integrity comparisons and known file matching; collisions are mathematically possible, so a hash works alongside custody records rather than in place of them. MD5 and SHA-1 have known cryptographic weaknesses. NIST's NSRL catalogs known software files, and specialized authorized databases serve other identification purposes.

### Incident Response Plan

A documented set of procedures that specifies how an organization will detect, contain, eradicate, recover from, and learn from security incidents. An effective incident response plan defines roles and responsibilities, communication trees, evidence preservation procedures, regulatory notification timelines, and criteria for engaging outside forensic and legal counsel. A tested plan gives the team a sequence to follow in the chaotic early hours of a breach, when evidence is most easily lost.

### Live Forensics

Evidence collection from a running system, including memory, processes, connections and accessible decrypted data. Collection changes some system state, so the method, tools and timing must be documented. A running device may expose keys or decrypted volumes that become unavailable after shutdown; recovery keys or other authorized access may also exist. Operational safety and evidence priorities determine the approach.

### Locard Exchange Principle

A principle from physical forensics that contact can produce trace evidence. Its digital analogy encourages examiners to look for related artifacts across devices and services. Examiners confirm what each source actually recorded by checking logging settings, retention and the acquired scope, and conclusions rest on the evidence actually available.

### Memory Forensics

Examination of acquired volatile memory to identify processes, connections, code and other artifacts present at acquisition. Memory may hold evidence of activity that uses few executable files, but such activity can also leave logs, registry or other persistent traces. Capture changes state and may be incomplete; findings need acquisition context and corroboration.

### MITRE ATT&CK

MITRE's knowledge base of observed adversary tactics, techniques and procedures. It provides a shared vocabulary for incident analysis and selected attack simulations. Teams select the techniques that fit the matter or test plan, in whatever order the plan calls for.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Network Forensics

The capture, recording, and analysis of network traffic and related logs to detect intrusions, reconstruct communications, identify data exfiltration, and attribute attacks. Network forensics tools include full packet capture systems, NetFlow analyzers, DNS query logs, proxy logs, and SIEM platforms. Unlike endpoint forensics, network forensics provides a record of communication between systems, including when attackers are operating on devices they have not physically touched. Network forensic evidence is particularly important in cases involving remote access, data theft, and communication between coconspirators.

### Packet Capture (PCAP)

A recording of packets observed at a capture point, commonly stored as PCAP or PCAPNG. Coverage depends on sensor placement, filters, capture length, dropped packets and retention. With encrypted traffic, the examiner works from headers and timing. Examiners document this coverage before reconstructing communications, file transfers or suspected data movement.

### Registry Analysis

Examination of Windows Registry configuration and activity artifacts, including user settings, device history and persistence mechanisms. Interpretation depends on the Windows version and artifact semantics. AppCompatCache and Amcache records, for example, are read according to the Windows version before they are cited for execution. Examiners correlate registry findings with event logs, file metadata and other independent evidence.

### Slack Space

The area between a file's logical end and the end of its allocated storage unit. It may contain padding or residual bytes, depending on the file system and write behavior. Acquisition scope and storage controller behavior shape what can be examined and recovered.

### Steganography

The practice of hiding data within other, innocuous appearing data, such as concealing a text file within the pixel data of an image, an audio file, or a video. Unlike encryption, which makes data unreadable, steganography conceals the very existence of the hidden data. Attackers use steganography to exfiltrate data covertly, embed malware instructions in benign looking files, and conduct covert C2 communications. Steganalysis, the forensic detection of steganographic content, requires specialized tools and statistical analysis of carrier files.

### Threat Hunting

A proactive security practice in which skilled analysts actively search for indicators of threat actor presence within an environment, rather than waiting for automated alerts. Threat hunters develop hypotheses based on threat intelligence and knowledge of attacker behavior, then test them by querying endpoint detection, network logs, and SIEM data. Threat hunting finds threats that evade automated detection and is particularly effective against APTs and living off the land attacks. The findings of a threat hunt often initiate formal forensic examinations and incident response actions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Threat Intelligence

Evidence based knowledge about existing or emerging threats, including attacker TTPs, indicators of compromise, targeting patterns, and actor motivations, used to inform defensive decisions. Threat intelligence is categorized as strategic (high level trends for executives), operational (specific campaigns and actors for security teams), and tactical (IoCs for security tools). In litigation, threat intelligence reports can establish whether a threat was known and whether the victim organization's defenses were appropriate relative to the known threat environment.

### Volatility Order

A collection planning principle that prioritizes evidence likely to change or disappear quickly, such as memory and running processes. NIST SP 800-86 and RFC 3227 discuss volatility alongside collection value and practical constraints. The plan must account for safety, authority, source condition and the effect of each collection step. Document why evidence was collected in a particular sequence and the preservation status of each source.

### Write Blocker

Hardware or software used to prevent host issued writes to a source medium during supported acquisitions. Compatibility and validation matter, and where a device or live acquisition calls for a method other than conventional write blocking, examiners select one suited to it. Examiners document the method, tool state and conditions of each acquisition. Write protection supports preservation, internal storage controller activity is noted where it applies, and the court decides admissibility.

## OT / ICS / SCADA Security

The terms used in industrial control and SCADA assessments, where safety and availability change what an examiner can touch and when.

### Air Gap

Separation intended to prevent direct network connectivity between environments. Removable media, maintenance devices, temporary connections and other transfer paths can weaken the separation. Identify the actual paths and operating procedures, and test the claimed separation against each of them, removable media included.

### CISA

The U.S. federal agency, established in 2018 under the Department of Homeland Security, responsible for protecting critical infrastructure from physical and cyber threats. CISA issues binding operational directives for federal agencies, publishes advisories about threats to critical infrastructure sectors, and coordinates with private sector owners of critical infrastructure on incident response and resilience. CISA's ICS-CERT (now merged into CISA) has been the primary government resource for OT/ICS vulnerability disclosures and incident response support.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Control Logic

Instructions used by PLCs, RTUs and related devices to control physical processes, including outputs, setpoints and interlocks. Languages include Ladder Diagram and Structured Text. Forensic review distinguishes application logic, firmware, configuration and operator changes, comparing each with an appropriate baseline. Collection is coordinated with plant personnel so evidence work keeps the process and the people around it safe.

### DCS (Distributed Control System)

A process control system in which control elements are distributed throughout the plant rather than centralized in a single location, connected by a high speed communications network. DCS platforms are common in chemical plants, refineries, and power generation facilities where tight, continuous process control is required. Unlike SCADA systems, which gather data from remote field sites, a DCS is typically confined to a single facility. DCS cybersecurity is a specialized discipline due to the real time constraints, proprietary protocols, and catastrophic consequences of failure in process industries.

### DNP3

Distributed Network Protocol 3 is used in utility and other control system communications. Legacy implementations and secure authentication capabilities differ. Assess the deployed version, configured controls and permitted command paths with the operator.

### HMI (Human Machine Interface)

A human machine interface displays process information and may let an operator issue commands. The exposure created by compromise depends on its configured role, permissions, connections and process safeguards. The examiner reads those settings to measure how much operator control a compromise actually reached. Examination or testing follows the operator’s safety and authorization requirements.

### Historian Database

An industrial time series source that retains selected process measurements, states and events under the deployed configuration. Recording intervals, aggregation, clock settings and retention affect coverage. Available records may help compare a process deviation, alarm or operator action with other evidence, and the examiner reads them within their recording intervals and corroborates any link between a cyber event and the deviation with network, controller and operator records.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response · NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security

### ICS (Industrial Control System)

A broad category of control systems used to monitor and control industrial processes, encompassing SCADA systems, DCS, PLCs, RTUs, and other automation technologies deployed in energy, water, manufacturing, transportation, and other critical sectors. ICS security has become a national security priority as these systems, originally designed for isolation, are increasingly networked and exposed to cyber threats. A cyberattack on ICS can cause physical damage, environmental harm, and loss of life, making ICS forensics a specialized and high stakes discipline.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Industrial Protocol

Communication protocols designed for use in industrial control environments, including Modbus, DNP3, PROFIBUS, EtherNet/IP, IEC 61850, and OPC-UA. Most traditional industrial protocols were designed for reliability and determinism rather than security, lacking authentication, encryption, or integrity verification. Network forensics in OT environments requires knowledge of these protocols to distinguish normal operational traffic from attacker generated commands, since the same protocol used by operators is used by attackers who have gained access to the OT network.

### Ladder Logic

A graphical programming language used to program PLCs, based on relay logic diagrams used in early factory automation. Ladder logic remains the most widely used PLC programming language in North American manufacturing and utility industries. Forensic analysis of ladder logic programs requires OT specific expertise: examiners compare the current PLC program against a known good baseline to identify unauthorized modifications that could alter physical process behavior, open or close valves, or disable safety interlocks.

### Modbus

An industrial communications protocol family originally developed by Modicon. Traditional Modbus serial and TCP deployments send commands in plain text and accept them from any client that can reach the device. Modbus Security adds TLS based protections, and the protection in place depends on the devices and configuration deployed. Analysts examine commands, register changes and network access controls in the process context, with operations approval before active testing.

### OT (Operational Technology)

Hardware and software that detects or causes changes in physical processes through direct monitoring and control of physical devices, processes, events, and infrastructure, as distinguished from information technology (IT) which processes and stores information. OT includes PLCs, DCS, SCADA systems, RTUs, and safety instrumented systems deployed in utilities, manufacturing, oil and gas, and transportation. The convergence of OT and IT networks has created new attack surfaces and requires security approaches that account for OT's unique real time, availability first operational requirements.

### PLC (Programmable Logic Controller)

A ruggedized industrial computer designed for real time control of machinery and processes in manufacturing, utility, and infrastructure environments. PLCs execute control logic programs continuously, reading inputs from sensors and issuing outputs to actuators based on programmed logic. Stuxnet's targeting of Siemens S7 series PLCs demonstrated that PLC firmware and programs are realistic attack targets with potentially catastrophic physical consequences. Forensic examination of PLCs requires specialized hardware connections and vendor specific software tools to read and analyze programs and execution logs.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### Purdue Model

A hierarchical reference architecture for industrial control systems, originating from the Purdue Enterprise Reference Architecture, that defines six levels of an industrial enterprise from physical processes (Level 0) through intelligent devices (Level 1), control systems (Level 2), site operations (Level 3), business logistics (Level 4), and enterprise networks (Level 5). The Purdue Model is widely used to define network segmentation requirements in ICS environments and guides the placement of security controls at boundaries between levels. Understanding the Purdue Model is essential for forensic examiners analyzing how attackers moved from IT networks into OT environments.

### RTU (Remote Terminal Unit)

A field device used in SCADA systems to collect data from sensors and instruments at remote locations and transmit it to the central SCADA master station, while also relaying control commands from the master to local actuators. RTUs are deployed at geographically distributed sites such as substations, pump stations, and wellheads. Because RTUs often operate in remote, physically unmonitored locations, physical security and secure communications protocols are both important considerations for protecting them from tampering.

### SCADA (Supervisory Control and Data Acquisition)

Supervisory systems that monitor and control distributed processes using telemetry from devices such as PLCs and RTUs. Operators use SCADA displays and commands to supervise field operations. A compromise can affect availability, process integrity or safety. Analysis correlates network traffic, operator actions, alarms and control changes and tests each observed process deviation for its own cause.

### Safety Instrumented System (SIS)

An independent system designed to bring an industrial process to a safe state when predetermined conditions are exceeded, preventing catastrophic outcomes such as explosions, toxic releases, or equipment failure. The TRITON/TRISIS malware, discovered in 2017, specifically targeted Schneider Electric Triconex safety systems at a Middle Eastern petrochemical facility, with the apparent goal of disabling safety systems to enable a catastrophic incident. Attacks against SIS are considered among the most dangerous categories of ICS cyberattack.

## Network and Infrastructure

The infrastructure and protocol terms that explain how traffic moves, how it is inspected and where the logs that reconstruct an incident live.

### CIDR (Classless Inter Domain Routing)

A method for allocating IP addresses and routing internet traffic that replaced the older class based addressing system, using a prefix notation (e.g., 192.168.1.0/24) to specify both the network address and the number of bits in the subnet mask. Understanding CIDR notation is necessary for interpreting firewall rules, access control lists, and network forensic evidence, since IP address ranges are frequently specified using CIDR in configuration files, threat intelligence feeds, and incident reports.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### DMZ (Demilitarized Zone)

A network segment that sits between an organization's internal network and the internet, hosting publicly accessible services such as web servers, email servers, and DNS resolvers while isolating them from the more sensitive internal network. If a server in the DMZ is compromised, the attacker should face additional barriers before reaching internal systems. Forensic analysis of incidents involving internet facing infrastructure frequently begins with an examination of DMZ systems, since they are the most exposed point of entry.

### DNS (Domain Name System)

The distributed system that maps domain names to records such as IP addresses and mail routing destinations. Resolver and endpoint logs can help identify malicious domains, suspicious lookups or possible DNS tunneling. The examiner accounts for caching, encrypted DNS, alternate resolvers and retention when reading which lookups a log captured.

### Egress Filtering

The application of firewall rules or network controls to outbound traffic leaving an organization's network, blocking unauthorized connections from internal systems to external destinations. Egress filtering limits the ability of malware to communicate with C2 servers and reduces data exfiltration. Organizations that rely exclusively on perimeter ingress filtering while ignoring egress controls provide attackers who gain internal access with a wide open path for data theft and C2 communication. Firewall logs showing unexpected outbound connections are often the first indicator of a compromise.

### Encryption

The process of transforming data into an unreadable format using a cryptographic algorithm and key, making it accessible only to parties who possess the correct decryption key. Encryption protects data in transit (using TLS/SSL) and at rest (using full disk encryption or file level encryption). In digital forensics, encryption presents both a challenge and an opportunity: encrypted devices may require legal process to compel decryption key disclosure, while the presence of encryption software on a suspect device may be forensically significant.

### Honeypot

A decoy resource used to observe unexpected access or study behavior. Its configuration and placement determine what an interaction means. Administrative work, monitoring, authorized tests and automated scanning must be distinguished from malicious activity. Preserve the configuration, relevant events and handling record.

NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management · NIST glossary: honeypot

### IDS / IPS (Intrusion Detection / Prevention System)

Network or host based systems that monitor traffic or system activity for signatures of known attacks or anomalous behavior. An IDS generates alerts; an IPS also blocks malicious traffic automatically. IDS/IPS logs are critical forensic artifacts: they record detection events, timestamps, source and destination IP addresses, and the specific rule or signature that fired, providing a contemporaneous record of attack activity. A quiet IDS/IPS log is confirmed against endpoint, network and account records before it is read as quiet, since sophisticated attacks are frequently designed to evade signature based detection.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### NAT (Network Address Translation)

A method in which a router maps multiple private IP addresses to a single public IP address, conserving public IP space and obscuring the internal network topology from external observers. NAT complicates forensic attribution because many devices share a single external IP address, and the examiner ties an external connection to a specific internal device and time through the internal NAT log records. Preserving NAT logs is a critical step in incident response and legal holds for network related incidents.

### Network Segmentation

The division of a network into smaller subnetworks with controlled access between them, limiting the spread of an intrusion and reducing the blast radius of a breach. Segmentation is implemented using firewalls, VLANs, and access control lists. Proper segmentation means that an attacker who compromises a workstation in accounting has to pass through a security control that can detect and block lateral movement before reaching OT systems or the finance server. Network topology documentation is essential both for security design and for forensic reconstruction of how an attacker moved through an environment.

### Packet Sniffing

The capture and analysis of network packets passing over a network, using tools such as Wireshark, tcpdump, or commercial network taps. Packet sniffing is used legitimately for network troubleshooting, performance monitoring, and forensic examination, and maliciously for credential theft, session hijacking, and reconnaissance. On switched networks, packet sniffing requires either access to a switch port mirror, a network tap, or the use of ARP poisoning to redirect traffic. With encrypted protocols, an attacker or a forensic examiner works mainly from the headers, timing and volume of the captured packets.

### PKI (Public Key Infrastructure)

A framework of policies, procedures, hardware, software, and digital certificates that enables secure electronic communications through public key cryptography. PKI is the foundation of TLS/SSL, email signing (S/MIME), code signing, and document digital signatures. Certificate authority (CA) compromise, certificate misissuance, and improper certificate validation are significant security vulnerabilities in PKI. Forensic analysis of PKI involves examining certificate chains, certificate revocation status, and CA logs to authenticate digital signatures and detect certificate based fraud.

### Proxy Server

An intermediary that forwards requests or connections and may provide caching, filtering or access controls. Forward and reverse proxies serve different positions in the communication path. Depending on configuration and protocol, retained logs may include addresses, destinations, times or volume. Analysis states the fields actually present and the requests covered, and ties a request to a person through account and endpoint records.

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response · RFC 9110: HTTP intermediaries

© 2026 Global Digital Forensics, Inc. All rights reserved.

### SIEM (Security Information and Event Management)

A platform that collects and correlates selected logs and generates alerts. It can be an important incident source, and its coverage follows the connected systems, filtering, clock accuracy, retention and export capabilities. The examiner compares its records with source system inventories and goes to the source systems themselves where they hold more detail.

### TLS / SSL

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols that provide authentication, confidentiality, and integrity for network communications. TLS is the foundation of HTTPS and secures email, VPN, and many other protocols. Weaknesses in TLS configuration (outdated protocol versions, weak cipher suites, certificate validation failures) are common penetration testing findings. In forensics, TLS interception by a network security device, where permitted by policy, can provide visibility into otherwise encrypted traffic. All TLS versions below 1.2 are considered insecure.

### VLAN (Virtual Local Area Network)

A logical subdivision of a physical network, configured at the switch level, that separates broadcast domains and controls which devices can communicate directly without passing through a router or firewall. VLANs are a primary tool for network segmentation, separating user workstations, servers, guest Wi-Fi, and OT devices from each other. VLAN hopping attacks exploit misconfigured switch ports to gain access to VLANs beyond those intended. VLAN configuration documentation is reviewed during network forensic examinations to understand what network segments an attacker could have reached.

### VPN (Virtual Private Network)

A virtual private network protects selected communications through a tunnel and may provide remote access. Stolen credentials or sessions are one possible entry route among several. Authentication and gateway records may support analysis, read within their available fields and retention and corroborated with endpoint and identity records.

### Zero Trust Architecture

An approach that grants no implicit trust solely because a user or device is inside a network or owned by the organization. NIST SP 800-207 describes resource focused access decisions based on authentication, authorization and the available security context. Access should be limited to the agreed resource and reevaluated under the organization's policy. Logging and detection are configured within the architecture, and the examiner confirms what each control recorded.

© 2026 Global Digital Forensics, Inc. All rights reserved.

## Compliance and Legal

The rules, regulations and evidentiary standards that turn a technical finding into a notification, a production or an exhibit.

### Attorney Client Privilege in Digital Evidence

A legal protection that may apply to confidential communications for obtaining or providing legal advice. Digital evidence can contain privileged material alongside ordinary business records. Whether a forensic report or communication is protected turns on its purpose and handling, which counsel assesses, and work product protection is a separate analysis. Examiners support counsel with the identification and controlled handling of privileged material.

### CCPA (California Consumer Privacy Act)

California's consumer privacy law, amended by the CPRA, gives qualifying residents rights concerning covered businesses' handling of personal information, subject to exceptions. These include access, correction, deletion and certain opt out rights. A limited private right of action concerns specified security breaches and conditions, and legal review confirms whether a given incident falls within them. Breach notification duties also arise under separate laws.

### CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act)

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 directs CISA to establish reporting requirements for covered critical infrastructure entities. The statute sets a framework for reporting covered cyber incidents within 72 hours and ransom payments within 24 hours. Applicability, definitions and implementation depend on the governing regulations and their effective dates. Counsel determines under those regulations whether a particular organization or incident must report.

### CMMC

The Department of Defense's Cybersecurity Maturity Model Certification program assesses protection of specified federal contract information and controlled unclassified information. Requirements depend on the applicable contract, assessment level and program rules. Evidence may include configurations, access controls, assessment records and operating practices.

### Daubert Standard

The federal reliability framework associated with Daubert and later decisions, applied alongside Federal Rule of Evidence 702. The court evaluates whether proposed expert testimony satisfies the applicable requirements for helpfulness, factual support and reliable methods and application. Testing, error rates, peer review and acceptance can be relevant factors, weighed case by case. The court decides admissibility.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### eDiscovery (Electronic Discovery)

The process of identifying, preserving, collecting, processing, reviewing, and producing electronically stored information (ESI) in response to litigation, regulatory inquiries, or government examinations. ESI includes email, documents, databases, social media, text messages, cloud storage, and metadata. The Federal Rules of Civil Procedure govern eDiscovery in federal litigation, including requirements for proportionality, litigation holds, and the treatment of inaccessible data. GDF provides forensic collection and processing services for eDiscovery matters requiring specialized technical expertise.

### FERPA (Family Educational Rights and Privacy Act)

A federal law protecting personally identifiable information in education records at covered educational agencies and institutions. It provides access and amendment rights and limits disclosure, with exceptions. Notice to parents after a data breach generally comes from other laws, so the school's attorneys review those alongside FERPA's disclosure rules. Examiners document access and disclosure facts while the institution and counsel determine obligations.

### FRE 902(14)

Federal Rule of Evidence 902(14) addresses authentication of data copied from an electronic device, storage medium or file through a process of digital identification, supported by a qualified person's certification. Notice and inspection requirements also apply. It differs from Rule 902(13), which concerns records generated by electronic processes or systems. Hearsay, relevance and the other admissibility issues are addressed separately from self authentication.

### GDPR

The EU General Data Protection Regulation governs personal data processing within its material and territorial scope, and that scope reaches beyond citizenship or a simple residency test. Article 33 generally requires a controller to notify the supervisory authority without undue delay and, where feasible, within 72 hours of awareness, unless the breach is unlikely to create a risk to individuals' rights and freedoms. Separate duties and exceptions apply to processors and notification of individuals. Applicability is a legal evaluation.

### HIPAA (Health Insurance Portability and Accountability Act)

U.S. health information rules applying to covered entities and business associates within their scope. The Breach Notification Rule concerns unsecured protected health information and includes exceptions and assessment requirements. Notification timing and recipients vary: individual notices generally have a 60 day outer limit, HHS reporting differs by breach size, and the media threshold concerns more than 500 residents of a state or jurisdiction. Technical findings support the legal assessment rather than determining it alone.

### NERC CIP (Critical Infrastructure Protection)

Critical Infrastructure Protection reliability standards addressing cybersecurity of covered bulk electric system assets and responsible entities. Requirements and applicability depend on the specific standard, asset categorization and jurisdiction. Evidence can include access records, configurations, change management and incident documentation. Compliance and enforcement conclusions are drawn from the applicable rules and the responsible authorities.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### NIST CSF (Cybersecurity Framework)

NIST's Cybersecurity Framework organizes cybersecurity risk management. CSF 2.0 has six functions: Govern, Identify, Protect, Detect, Respond and Recover. Profiles and tiers help organizations describe current and target practices. The framework is a voluntary reference, and an assessment identifies the version, outcomes and evidence evaluated while legal compliance remains a question for the organization's lawyers.

### PCI DSS (Payment Card Industry Data Security Standard)

The Payment Card Industry Data Security Standard covers protection of payment account data in applicable environments. Requirements address areas such as access, configuration, monitoring and vulnerability management. Following a suspected compromise, payment brands or acquiring institutions may require work by a PCI Forensic Investigator under their programs. That requirement arises case by case under those programs, and a PFI engagement is a designated role distinct from a general forensic assessment.

### SOC 2

Developed by the American Institute of CPAs (AICPA), SOC 2 is a reporting framework for service organizations that evaluates controls relevant to security, availability, processing integrity, confidentiality, and privacy of customer data. SOC 2 Type II reports, covering an actual period of operation rather than a point in time snapshot, are routinely required by enterprise customers as evidence of their vendors' security controls. In litigation involving vendor breaches, SOC 2 reports and the underlying control documentation are frequently sought in discovery to assess what security commitments were made and whether they were met.

### SOX (Sarbanes Oxley Act)

The Sarbanes Oxley Act addresses public company financial reporting and internal controls. Section 404 concerns management assessment of internal control over financial reporting, with external auditor attestation requirements and exemptions depending on issuer status. Relevant technical evidence may include access, change control and log integrity records. Counsel and accounting professionals determine the applicable obligations.

### Spoliation Sanctions

Court ordered measures addressing failures to preserve evidence under applicable law. Federal Rule of Civil Procedure 37(e) addresses electronically stored information that should have been preserved, was lost because reasonable steps were not taken, and cannot be restored or replaced. Curative measures and the more severe measures requiring intent to deprive have different conditions. Examiners document preservation and loss; the court determines consequences.

© 2026 Global Digital Forensics, Inc. All rights reserved.

## Identity and Access

The authentication and access terms behind most account compromises, from passwords and tokens to passwordless sign in and federation.

### Biometric Authentication

The use of unique biological characteristics, including fingerprints, facial geometry, iris patterns, voice, or behavioral traits, to verify a person's identity. Biometric systems are increasingly used for device unlocking, banking authentication, and border control. Unlike a password, biometric data stays with the person after a compromise, which raises the stakes of a biometric breach. The intersection of biometrics and law enforcement is significant: compelling a suspect to provide a fingerprint to unlock a device has been treated differently from compelling a password disclosure under the Fifth Amendment in some jurisdictions, though this area of law continues to evolve.

### Credential Harvesting

The collection of authentication credentials (usernames, passwords, API keys, tokens, certificates) through phishing, keylogging, memory scraping, or extraction from compromised systems. Harvested credentials are used directly for unauthorized access, sold to other threat actors, or fed into credential stuffing attacks against other services. Information stealing malware (stealers) is one of the most prolific credential harvesting mechanisms, exfiltrating browser stored passwords, session cookies, and autofill data from millions of compromised devices.

### Identity and Access Management (IAM)

The framework of policies, processes, and technologies that manages digital identities and controls what resources each identity can access. IAM encompasses user provisioning, authentication, authorization, role based access control, and audit logging. Weak IAM implementation, including excessive permissions, unmanaged service accounts, and lack of multi factor authentication, is a root cause of many significant breaches. IAM logs, including provisioning events, authentication records, and access changes, are essential forensic artifacts in insider threat and unauthorized access examinations.

### Kerberoasting

An attack in which service ticket material is obtained and subjected to offline password guessing attempts. Success depends on conditions including password strength and the available ticket encryption; the requested ticket has to be cracked offline before any plaintext password emerges. Supported authentication events and other records may help trace attempts, read within the logging coverage in place.

### Multi Factor Authentication (MFA)

Authentication using factors from different categories, such as knowledge, possession or inherence. Protection differs by method and recovery flow. Authentication logs can support analysis of prompts and sessions, and the examiner correlates them with configuration, identity and endpoint records to work out how access occurred and whether a factor was bypassed.

© 2026 Global Digital Forensics, Inc. All rights reserved.

### OAuth

A framework for delegated authorization that allows an application to receive scoped access without learning the user's password. OAuth 2.0 handles authorization, and OpenID Connect adds the identity layer used for authentication. Malicious applications may abuse consent grants or tokens to access email and files. Reviewing grants, token use, application ownership and revocation is important because revoking authorizations is a separate step from changing a password.

### Pass the Hash

An attack technique that uses a captured password hash to authenticate to remote systems without needing to know the underlying plaintext password. Windows NTLM authentication is particularly vulnerable: once an attacker dumps credential hashes from memory (using tools like Mimikatz), those hashes can be used directly to authenticate across the network. Pass the Hash attacks are a staple of lateral movement in Windows environments and leave specific event log artifacts. Forensic analysis can often correlate hash reuse patterns to trace an attacker's path through an enterprise network.

### Passwordless Authentication

Authentication without a conventional reusable password, using methods such as cryptographic authenticators or one time links. Phishing resistance varies by method. FIDO/WebAuthn passkeys are bound to a relying party and may be device bound or synchronized across devices. Assessment should cover enrollment, recovery, synchronization, device protection and fallback methods.

### SAML (Security Assertion Markup Language)

An XML based standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP), most commonly used for enterprise single sign on. When a user authenticates to the IdP, a digitally signed SAML assertion is passed to the service provider granting access. The SolarWinds supply chain attack involved forging SAML tokens (a technique sometimes called "Golden SAML"), allowing attackers to impersonate any user to cloud services without triggering standard authentication alerts.

### Single Sign On (SSO)

An arrangement allowing authentication at an identity provider to support access to connected applications. A compromised session or provider can expand access, and how far it reached depends on application policy, session state, token scope and revocation behavior, so the examiner reads identity and application records together.

### Token Theft

The theft of an authentication or session token for attempted reuse. Some valid tokens permit access with no new password or MFA prompt; replay depends on scope, expiry, revocation, binding and application controls. Microsoft’s August 2023 Midnight Blizzard report lists token theft among several initial access approaches, one possibility among others for any given incident. Examine identity, application and endpoint evidence to test suspected reuse.

© 2026 Global Digital Forensics, Inc. All rights reserved.

## Technical and Regulatory References Behind These Definitions

Use primary standards and the applicable rules when you assess a specific system or matter; a glossary entry is the starting point, and the primary sources are the authority. The forensic method vocabulary follows NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, the industrial terms follow NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, and the AI entries draw on NIST AI 100-2 E2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. Hash value and known file definitions reference the NIST National Software Reference Library.

The identity entries rely on the FIDO passkeys reference and OpenID Connect authentication documentation. The compliance and legal entries point to the Federal Rules of Evidence, the Federal Rules of Civil Procedure, HHS breach notification guidance, California consumer privacy guidance and Regulation (EU) 2016/679, the General Data Protection Regulation.

When a term in this glossary describes work you need done, the related practices are computer forensics, network forensics, AI security, OT and SCADA security and eDiscovery. Global Digital Forensics has served AmLaw 100 firms and Fortune 1000 companies since 1992 with court tested, certified examiners, and the initial consultation is free.

Which of those practices your matter needs is usually clear within a few minutes of describing it, so describe it to a senior examiner and let the engagement follow the question.

## Sources for the Logging, Identity, AI and Control System Entries

The logging, authentication, AI and industrial control definitions follow these sources: NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy; MITRE Kerberoasting technique; NIST IR 8587, Protecting Tokens and Assertions from Forgery, Theft, and Misuse; Microsoft's August 2023 Midnight Blizzard account; NIST Generative AI Profile; and NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security. These references support technical context. Applicable law comes from the governing rules, and what occurred in a specific environment is read from that environment's own records.

## Web Addresses for the Sources Cited


1. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response: https://csrc.nist.gov/pubs/sp/800/86/final
2. MITRE phishing techniques: https://attack.mitre.org/techniques/T1566/
3. OWASP SQL injection guidance: https://community.owasp.org/attacks/SQL_Injection
4. NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: https://csrc.nist.gov/pubs/sp/800/61/r3/final
5. MITRE drive by compromise: https://attack.mitre.org/techniques/T1189/
6. NIST AI 100-2 E2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf
7. NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final
8. NIST glossary: honeypot: https://csrc.nist.gov/glossary/term/honeypot
9. RFC 9110: HTTP intermediaries: https://www.rfc-editor.org/rfc/rfc9110.html#section-3.7


© 2026 Global Digital Forensics, Inc. All rights reserved.

10. NIST National Software Reference Library: https://www.nist.gov/itl/csd/secure-systems-and-applications/national-software-reference-library-nsrl
11. FIDO passkeys reference: https://fidoalliance.org/passkeys/
12. OpenID Connect authentication: https://openid.net/developers/how-connect-works/
13. Federal Rules of Evidence: https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence
14. Federal Rules of Civil Procedure: https://www.uscourts.gov/sites/default/files/document/federal-rules-of-civil-procedure.pdf
15. HHS breach notification guidance: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
16. California consumer privacy guidance: https://oag.ca.gov/privacy/ccpa
17. Regulation (EU) 2016/679, the General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
18. NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy: https://csrc.nist.gov/pubs/sp/800/41/r1/final
19. MITRE Kerberoasting technique: https://attack.mitre.org/techniques/T1558/003/
20. NIST IR 8587, Protecting Tokens and Assertions from Forgery, Theft, and Misuse: https://csrc.nist.gov/pubs/ir/8587/final
21. Microsoft's August 2023 Midnight Blizzard account: https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
22. NIST Generative AI Profile: https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

## Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

**Call (800) 868-8189**, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.