Advanced Certificate in War Crimes and Justice

Evidence Collection in Conflict Zones

Evidence collection in conflict zones is a multidisciplinary practice that brings together legal, forensic, humanitarian, and security expertise. The purpose of this glossary is to equip learners with precise definitions of the terminology that underpins the process, to illustrate how each term is applied in real-world settings, and to highlight the practical challenges that arise when gathering proof of war crimes amid active hostilities. The entries are organized alphabetically, but each definition is followed by a brief example or a note on implementation to foster a learner-friendly experience.

Admissibility – The legal standard that determines whether a piece of evidence may be presented before a court or tribunal. An item is admissible if it is relevant, reliable, and obtained in accordance with applicable procedural rules. For instance, a photograph of a destroyed village may be admissible in a war-crimes trial only if the chain of custody can be demonstrated and the image has not been altered.

Authentication – The process of establishing that a document, object, or digital file is what it purports to be. Authentication often involves linking the evidence to a credible source, such as a satellite provider, a forensic analyst, or an eyewitness. A forensic examiner might authenticate a piece of shrapnel by matching its metallurgical composition to the type of ammunition known to have been used by a particular armed group.

Ballistics – The scientific study of the behavior, flight, and impact of projectiles. In the context of war-crimes investigations, ballistics analysis can link a bullet recovered from a victim's body to a specific weapon system, thereby implicating the responsible force. An example is the use of microscopic striation comparison to match a rifle bullet to a seized rifle discovered in a rebel arsenal.

Chain of custody – The documented, chronological trail that records the possession, transfer, analysis, and storage of evidence from the moment of collection until its presentation in court. Maintaining an unbroken chain of custody is essential to prevent allegations of tampering. A field investigator who discovers a mass-grave must immediately log the location, time, and condition of each set of remains, assign a unique identifier, and sign each transfer form as the evidence moves to a forensic laboratory.

Chain of evidence – A broader concept that includes the chain of custody but also encompasses the logical connections that link individual pieces of evidence to the alleged crime. It demonstrates how each item supports the overall narrative of the case. For example, satellite imagery showing the movement of armored vehicles, combined with eyewitness testimony describing a shelling event, together form a chain of evidence that can substantiate an allegation of unlawful attack on civilians.

Civilian protection – The set of actions taken to safeguard non-combatants from the effects of armed conflict. While not strictly a term of evidence collection, understanding civilian protection measures helps investigators identify violations and collect relevant data. An illustration is the documentation of a school that was deliberately targeted despite being marked with the internationally recognized red cross symbol.

Confidentiality – The obligation to keep sensitive information, such as witness identities or classified intelligence, from unauthorized disclosure. In conflict zones, breaches of confidentiality can endanger sources and compromise investigations. An investigator might store witness statements on encrypted devices and limit access to a small, vetted team.

Contextual analysis – The interpretive work that situates raw evidence within the broader operational, geographic, and temporal framework of the conflict. Contextual analysis helps differentiate between lawful and unlawful acts. For example, a drone strike image must be examined alongside military orders, target selection procedures, and the presence of civilians at the time of the attack.

Digital evidence – Information stored or transmitted in electronic form, including photographs, video recordings, metadata, communications logs, and geolocation data. Digital evidence is increasingly vital in modern conflicts where combatants rely on smartphones and social media. A practical application is the extraction of GPS coordinates from a video file to verify the location of an alleged massacre.

Documentary evidence – Any written, printed, or electronic record that can substantiate facts. This includes official reports, orders, maps, medical records, and incident logs. An example is a cease-fire agreement that was signed but later violated; the original document serves as documentary evidence of the parties' obligations.

Forensic anthropology – The scientific discipline that applies skeletal analysis to identify victims, determine cause of death, and reconstruct events. In conflict zones, forensic anthropologists may examine mass-burial sites to establish the age, sex, and trauma patterns of the deceased. A case study involves the exhumation of a mass grave, where forensic anthropologists identified bullet wounds consistent with small-caliber firearms.

Forensic analysis – The systematic examination of physical or digital evidence using scientific methods. Forensic analysis can include DNA testing, chemical assays, microscopy, and ballistic matching. For instance, forensic analysts may test soil samples collected from a weapon cache to determine whether the soil's composition matches the terrain of a specific battlefield.

Geolocation data – Information that specifies the geographic coordinates of a device or object at a given time. Geolocation data is extracted from satellite imagery, GPS devices, or metadata embedded in photos and videos. A practical use is to corroborate a victim's testimony that a particular attack occurred at a specific coordinate, by matching the geotagged video to that location.

Humanitarian law – Also known as international humanitarian law (IHL), the body of rules that seeks to limit the effects of armed conflict on civilians and combatants. Understanding humanitarian law is essential for recognizing when an act constitutes a war crime. For example, the deliberate targeting of a hospital violates IHL and creates a category of evidence that must be documented.

Human rights documentation – The systematic collection of information about violations of civil, political, economic, social, and cultural rights. While distinct from war-crimes evidence, human-rights documentation often overlaps with conflict-zone investigations. An NGO may compile testimonies of forced displacement, which can later be used as evidence in a war-crimes tribunal.

Identification tag – A unique label assigned to each piece of evidence to ensure traceability. Tags often include a code, date, collector's initials, and a brief description. For example, a piece of shrapnel might be labeled "SH-2024-07-15-A1" and entered into an evidence register.

Incident report – A written account of an event that records the date, time, location, participants, and observed actions. Incident reports are foundational documents that guide subsequent evidence collection. A field officer may file an incident report describing an artillery strike that resulted in civilian casualties, which then triggers a forensic team's deployment.

Intelligence sources – Information obtained from classified or open-source channels that can illuminate the planning, execution, or command structure of alleged crimes. Intelligence must be handled carefully to protect sources and to verify accuracy. A tribunal may admit satellite imagery from a commercial provider as intelligence evidence, provided the source's reliability is demonstrated.

Judicial admissibility – The criteria set by a court to determine whether evidence can be considered during a trial. Judicial admissibility encompasses relevance, authenticity, chain of custody, and compliance with procedural rules. Evidence that fails any of these thresholds may be excluded, regardless of its probative value.

Legal standard – The level of proof required to establish a fact in court. In war-crimes proceedings, the standard is typically "beyond a reasonable doubt," meaning that the evidence must leave no logical explanation other than the defendant's guilt. Understanding the legal standard helps investigators prioritize the collection of the most compelling evidence.

Mass-grave investigation – A specialized forensic operation that involves the systematic excavation, documentation, and analysis of multiple human remains buried together. Mass-grave investigations require careful mapping, photographic documentation, and the preservation of contextual information. An example is the excavation of a mass grave in a rural village, where each set of remains is recorded with its exact depth and orientation.

Metadata – Data that provides information about other data, such as creation date, device identifier, and file size. Metadata is crucial for verifying the authenticity of digital evidence. For instance, the metadata of a video file may reveal that it was recorded on a specific date and time, supporting the claim that the footage depicts a particular incident.

Medical documentation – Records that detail injuries, treatments, and diagnoses, often produced by hospitals, clinics, or field medics. Medical documentation can serve as evidence of the nature and severity of injuries sustained during an attack. A doctor's report describing shrapnel wounds to a civilian provides medical documentation that can corroborate witness testimony.

Open-source intelligence (OSINT) – Information gathered from publicly available sources, such as news reports, social media posts, and satellite imagery. OSINT is a valuable complement to on-the-ground evidence collection, especially when access to a site is restricted. An investigator might use OSINT to locate a damaged infrastructure that was not reported in official channels.

Photographic evidence – Still images captured to document a scene, object, or event. Photographic evidence must be taken with proper techniques to ensure clarity, scale, and context. A field photographer may include a calibrated ruler or a known object (e.G., A vehicle) in the frame to provide scale for damage assessment.

Probative value – The ability of evidence to prove something pertinent to the case. Evidence with high probative value directly supports an element of the alleged crime. For example, a recovered weapon that matches the caliber of ammunition found in victims' bodies has high probative value for establishing weapon use.

Protective custody – The safeguarding of witnesses or victims who are at risk of retaliation. Protective custody may involve relocation, anonymity, or secure communication channels. In conflict zones, protective custody is often coordinated with local authorities, NGOs, or international bodies to ensure the safety of vulnerable individuals.

Remote sensing – The acquisition of information about an area from a distance, typically using satellites, drones, or aircraft. Remote sensing can detect changes in terrain, the presence of weapon systems, and patterns of destruction. An example is the use of high-resolution satellite imagery to identify the location of a temporary detention facility that is later corroborated by survivor testimony.

Security clearance – An authorization that permits individuals to access classified or sensitive information. Security clearance is required for investigators handling intelligence that may reveal operational details of military forces. A forensic analyst with the appropriate clearance may be allowed to review intercepted communications that provide context for an alleged attack.

Sexual violence evidence – Documentation related to crimes of sexual violence, including survivor statements, medical examinations, forensic samples, and photographs of injuries. Collecting this evidence requires trauma-informed approaches and strict confidentiality. An example is the collection of DNA swabs from a survivor's clothing, which can later be matched to a perpetrator's DNA profile.

Site preservation – The act of protecting a location from alteration, contamination, or destruction after an alleged crime has been identified. Site preservation is critical for maintaining the integrity of evidence. Investigators may erect barriers, issue temporary cease-fire orders, or coordinate with military units to prevent further damage to a bomb-site.

Standard operating procedure (SOP) – A set of written instructions that prescribe the steps to be followed in a specific situation. SOPs guide investigators on how to safely collect, handle, and transport evidence. A typical SOP for collecting shell fragments may outline the use of gloves, the labeling process, and the packaging method for transport to a laboratory.

Statutory limitation – The time period within which legal action must be initiated after an alleged crime. While many war-crimes statutes have no limitation period, some national laws impose deadlines. Understanding statutory limitations helps investigators prioritize cases where evidence may become time-barred.

Survivor testimony – An oral account given by an individual who experienced or witnessed an alleged war crime. Survivor testimony is a cornerstone of many prosecutions, but it must be recorded accurately, with attention to language, cultural context, and potential trauma. An investigator might use a trained interpreter to ensure that a survivor's description of an attack is captured verbatim.

Technical forensic – The branch of forensic science that deals with the analysis of non-biological materials, such as explosives residues, fire patterns, and building collapse. Technical forensic evidence can link a particular type of munition to a specific manufacturer. For example, the detection of a unique explosive compound can indicate the use of a certain class of artillery shells.

Victim identification – The process of establishing the identity of individuals who have suffered harm, often through forensic methods like DNA profiling, dental record comparison, or facial reconstruction. Victim identification is essential for both accountability and humanitarian purposes. In a conflict scenario, DNA samples from a mass-grave may be matched to living relatives to provide closure.

Witness statement – A written or recorded account from a person who observed an event but was not directly harmed. Witness statements can corroborate survivor testimony or provide independent verification of facts. A field officer may obtain a witness statement from a local shopkeeper who saw a convoy pass through a town moments before an alleged attack.

Chain of evidence form – A standardized document used to record the movement of evidence, including details of each custodian, date and time of transfer, and condition of the item. The form is signed by each person who handles the evidence, creating a transparent audit trail. Failure to complete the chain of evidence form can lead to challenges regarding the evidence's reliability.

Chain of custody log – A digital or paper log that tracks the chronological custody of each piece of evidence. The log includes timestamps, signatures, and notes on any observed changes. In conflict-zone investigations, a chain of custody log may be maintained on encrypted tablets to reduce the risk of loss.

Chain of command – The hierarchical structure within a military or armed group that defines authority and responsibility. Understanding the chain of command helps investigators identify who ordered or approved an alleged illegal act. For example, linking a shelling order to a senior commander establishes command responsibility.

Compliance audit – A systematic review of an organization's procedures to ensure they meet legal, ethical, and operational standards. In evidence collection, a compliance audit may assess whether SOPs align with international guidelines for war-crimes investigations. Audits can reveal gaps, such as insufficient training in handling biological samples.

Criminal liability – The legal responsibility for committing a crime, which can be individual (direct perpetrator) or collective (command responsibility). Evidence must demonstrate the elements of criminal liability, including actus reus (the prohibited act) and mens rea (the intent). A forensic report showing that a weapon was used deliberately against civilians contributes to establishing criminal liability.

Critical incident – An event that has a high potential for causing significant loss of life, injuries, or property

damage. Critical incidents often trigger immediate evidence-collection protocols. A missile strike that destroys a refugee camp would be classified as a critical incident, prompting rapid deployment of forensic teams.

Documentation protocol – The set of guidelines that dictate how evidence, observations, and interviews are recorded. Documentation protocols ensure consistency and reliability across different investigators and locations. A protocol may require that every photograph be accompanied by a written caption describing the scene, time, and camera settings.

Evidence bag – A sealed container used to store physical evidence, designed to prevent contamination and preserve the item's condition. Evidence bags are often made of tamper-evident material and labeled with the identification tag. A forensic technician might place a recovered grenade fragment in a nylon evidence bag, sealing it with a zip lock and stamping the date.

Evidence collection kit – A pre-assembled set of tools and supplies needed to gather and preserve various types of evidence. Kits may include gloves, tweezers, evidence bags, cameras, and forms. Deploying a standardized evidence collection kit helps ensure that investigators have the necessary resources, even in remote or hostile environments.

Evidence preservation – The suite of actions taken to maintain the original condition of evidence from the moment of collection until it is examined. Preservation includes controlling temperature, humidity, and exposure to light. For example, biological samples must be kept frozen to prevent degradation, while explosive residues should be stored in airtight containers.

Evidence relevance – The relationship between a piece of evidence and a fact that is at issue in the case. Evidence that does not directly support or refute a material fact is considered irrelevant and may be excluded. A photograph of a distant mountain range is irrelevant to an allegation of unlawful shelling unless it can be shown to be the actual location of the attack.

Evidence tampering – The intentional alteration, destruction, or substitution of evidence to influence the outcome of an investigation or trial. Detecting tampering involves forensic techniques such as fingerprint analysis, DNA testing, and digital forensics. A broken seal on an evidence bag may indicate possible tampering, prompting a thorough examination.

Forensic chain of custody – The specific segment of the chain of custody that pertains to the forensic analysis phase, documenting each transfer to and from laboratories, the analysts involved, and any procedural steps taken. Maintaining a forensic chain of custody is essential for the admissibility of scientific results. A forensic chemist must sign a chain of custody form when receiving a soil sample for explosive residue testing.

Forensic photography – The practice of taking photographs that accurately record the condition and details of a crime scene or evidence item. Forensic photography follows strict standards for lighting, scale, and angle. An investigator may capture a series of overlapping photographs of a destroyed building to create a comprehensive visual record.

Geospatial analysis – The examination of spatial data to identify patterns, relationships, and trends. In conflict-zone investigations, geospatial analysis can map the distribution of attacks, the movement of forces, and the location of civilian populations. A geospatial analyst might overlay satellite imagery with population density maps to assess the impact of an airstrike on civilian areas.

Humanitarian access – The right of neutral actors, such as NGOs and UN agencies, to reach populations in need and gather information without interference. Humanitarian access is often negotiated with combatants and is crucial for evidence collection. When humanitarian access is granted, investigators can safely enter a town to document alleged violations.

International criminal law – The body of law that defines and prosecutes crimes such as genocide, crimes against humanity, and war crimes. International criminal law provides the legal framework that guides the collection, preservation, and presentation of evidence. Understanding its principles helps investigators align their methods with the expectations of tribunals like the International Criminal Court.

Legal provenance – The documented origin and history of a piece of evidence, demonstrating that it has been obtained lawfully and ethically. Legal provenance is especially important when evidence originates from sources that may have been compromised, such as seized documents from a hostile party. A legal provenance statement may accompany a set of intercepted communications to confirm that the acquisition complied with international standards.

Medical forensic – The application of medical knowledge to legal investigations, including the examination of injuries, disease, and cause of death. Medical forensic experts may produce reports that detail the nature of wounds, timing, and potential weapons used. For example, a medical forensic examiner might determine that a burn injury resulted from a napalm attack based on the pattern of tissue damage.

Mitigation evidence – Information that demonstrates steps taken to reduce the impact of an alleged violation, such as evacuation notices, humanitarian aid distribution, or protective measures. While mitigation does not excuse the crime, it may affect sentencing. Collecting mitigation evidence requires coordination with local authorities and humanitarian actors.

Multimedia evidence – Any combination of audio, video, photographs, and text that together provide a richer depiction of an event. Multimedia evidence can be more persuasive than a single format because it offers multiple perspectives. An investigator might compile a video of an artillery strike, audio recordings of explosions, and photographs of the aftermath to create a comprehensive multimedia dossier.

Open-source verification – The process of confirming the authenticity and accuracy of information obtained from publicly available sources. Verification may involve cross-checking multiple independent sources, analyzing metadata, and using geolocation techniques. An analyst verifying a viral video of a massacre would compare the background landmarks with satellite imagery to confirm the location.

Operational security (OPSEC) – The set of measures taken to protect sensitive information about investigative activities from adversaries. OPSEC is essential to prevent interference, intimidation, or retaliation. For instance, investigators may use coded language in field notes to conceal the identity of a protected witness.

Photogrammetry – The science of making measurements from photographs, often used to reconstruct three-dimensional models of a crime scene. Photogrammetry can be employed to document the layout of a destroyed building or the trajectory of a projectile. A forensic team may generate a 3-D model of a bomb crater to analyze blast patterns.

Physical evidence – Tangible items that can be examined directly, such as weapons, clothing, debris, and biological samples. Physical evidence is often the most compelling form of proof because it can be subjected to scientific testing. A piece of shrapnel recovered from a victim's body is a piece of physical evidence that can be linked to a specific type of artillery shell.

Probative threshold – The minimum level of relevance and reliability that evidence must meet to be considered by a tribunal. The probative threshold ensures that only evidence that meaningfully contributes to establishing a fact is admitted. Evidence that merely repeats known information without adding new insight may fall below the threshold.

Protective equipment – Gear such as helmets, ballistic vests, and chemical-protective suits that safeguard investigators from hazards present in conflict zones. Wearing appropriate protective equipment reduces the risk of injury while collecting evidence. For example, investigators entering a site contaminated with chemical agents must wear respirators and protective suits.

Remote verification – The validation of evidence using methods that do not require physical presence at the site, such as satellite imagery analysis or drone surveillance. Remote verification is useful when access is blocked or too dangerous. An analyst may remotely verify the destruction of a bridge by comparing pre- and post-strike images.

Satellite imagery – High-resolution pictures taken from orbiting satellites, used to monitor changes on the ground. Satellite imagery can reveal the presence of mass graves, the movement of troops, and the extent of infrastructure damage. A war-crimes investigator may use satellite imagery to pinpoint the location of a temporary detention camp.

Security protocol – The set of procedures designed to protect investigators, evidence, and witnesses from threats. Security protocols may include risk assessments, convoy planning, and emergency evacuation plans. Implementing a robust security protocol is essential when working in hostile environments.

Sexual violence forensic kit – A specialized collection kit that includes swabs, preservative solutions, documentation forms, and PPE for collecting evidence of sexual assault. Proper use of the kit ensures that biological evidence is preserved for DNA analysis while respecting the survivor's dignity. The kit may also contain a rape-kit container with a tamper-evident seal.

Site assessment – The initial evaluation of a location to determine the scope of evidence, safety hazards, and logistical needs. Site assessment informs the deployment of resources and the selection of appropriate collection methods. An investigator conducting a site assessment of a bombed school would note structural collapse, potential unexploded ordnance, and the presence of civilian remains.

Standard of proof – The degree of certainty required to establish a fact in a legal proceeding. In war-crimes

trials, the standard of proof is typically “beyond a reasonable doubt.” Understanding the standard of proof guides investigators in gathering sufficient and compelling evidence.

Technical chain of custody – The portion of the chain of custody that deals specifically with the handling of technical or digital evidence, such as hard drives, encrypted files, and communication logs. Maintaining a technical chain of custody involves hash verification, secure storage, and controlled access. A forensic analyst may calculate a SHA-256 hash of a seized laptop before transferring it to a secure lab.

Temporal analysis – The examination of time-related data to establish the sequence of events. Temporal analysis can involve timestamps from video recordings, logs from communication devices, and the order of physical damage. For example, correlating the timestamp of a drone video with the time reported by survivors helps verify the chronology of an attack.

Threat assessment – The systematic evaluation of potential dangers to investigators, evidence, and witnesses. Threat assessments consider factors such as active combat, presence of armed groups, and local political dynamics. Conducting a threat assessment before entering a contested area helps mitigate risks.

Trace evidence – Small, often microscopic material that can link a suspect to a crime scene, such as soil particles, fibers, or residues. In conflict zones, trace evidence may include fragments of explosive compounds or metal shavings from weaponry. An analyst might compare trace metal particles found on a victim’s clothing with those collected from a suspected weapon cache.

Victim-centred approach – An investigative methodology that places the needs, rights, and dignity of victims at the forefront of evidence collection. This approach emphasizes informed consent, confidentiality, and psychological support. Applying a victim-centred approach ensures that evidence gathering does not re-traumatize survivors.

Witness protection program – A set of measures designed to safeguard individuals who provide testimony against perpetrators. Protection may involve relocation, anonymity, and legal safeguards. In war-crimes contexts, witness protection programs are often coordinated with international bodies to guarantee safety across borders.

Weapon provenance – The documented origin and supply chain of a weapon, including manufacturing details, serial numbers, and distribution routes. Establishing weapon provenance can help attribute responsibility to a specific state or non-state actor. A forensic report that traces a missile fragment to a factory in a particular country provides weapon provenance.

Weapon residue analysis – Laboratory testing that detects and characterizes chemical residues left by explosives or propellants. Residue analysis can confirm the type of munition used and sometimes its origin. For example, detecting a unique peroxide-based explosive residue on a bomb fragment can link it to a specific weapons manufacturer.

Witness statement form – A standardized document used to capture the account of a witness, including sections for personal details, description of events, and signatures. The form ensures consistency and completeness across multiple interviews. A witness statement form may also include a section for the

interviewer's observations about the witness's demeanor.

Witness reliability – An assessment of the credibility of a witness based on factors such as consistency, corroboration, and potential bias. Reliability is evaluated during both the collection phase and the judicial phase. A witness who provides a coherent, detailed account that aligns with physical evidence is generally considered reliable.

Witness testimony admissibility – The legal criteria that determine whether a witness's oral account can be presented in court. Admissibility depends on relevance, competence, and the absence of undue prejudice. A tribunal may exclude testimony if the witness was coerced or if the testimony is deemed hearsay.

Zero-tolerance policy – A strict stance that prohibits any form of misconduct, such as evidence tampering or breach of confidentiality, within an investigative team. Implementing a zero-tolerance policy reinforces the integrity of the evidence-collection process. Violations are typically met with immediate disciplinary action.

The terms above form the core lexicon that students of the Advanced Certificate in War Crimes and Justice must master. Mastery of each concept enables practitioners to navigate the complex terrain of conflict-zone investigations, to produce evidence that meets the exacting standards of international tribunals, and to uphold the rights of victims and survivors. By internalizing these definitions, learners are better prepared to confront the logistical, legal, and ethical challenges that accompany the pursuit of accountability in the most hostile environments.