Forensics for Commanders

Introduction

Commanders at all levels should be aware of how forensic science supports the warfighter across the full range of military operations. This pamphlet provides information about the DoD Forensics Program, forensic functions and capabilities, mission areas, and operational processes that will enable commanders to fully leverage forensics in support of their operations.

Point of Contact: Office of the Provost Marshall General (OPMG)
Strategic Initiatives

Email: opmg.portalmaster@us.army.mil
(include "Forensics" in the subject line)

Figure 1

What is DoD Forensics?

The Global War on Terrorism (GWOT) has produced emerging needs and capabilities for forensics across the spectrum of combatant operations. The **goal of DoD Forensics** is to individualize, identify, associate, and link people, places, things, intentions, activities, organizations, and events to each other. DoD Forensics supports the full spectrum of ever-changing, emerging military operations and homeland defense by providing key enablers to meet traditional, irregular, disruptive, and catastrophic challenges.

Multidisciplinary forensic sciences contribute to examining sites; identifying, tracking and targeting the enemy; locating and identifying individuals; identifying the origin of arms, ammunition, and explosives; determining the cause and manner of death and prosecuting offenders in court systems. Intelligence operations benefit from the rapid forensic exploitation of sites, items, and information, enabling U.S. and coalition forces to eliminate threats and to kill, capture, or prosecute enemies.

Recently, operations in the Iraqi Theater of Operation (ITO) have **validated the importance of forensics** in providing intelligence and battlefield awareness for military decision-making and operations at all levels. DoD is rapidly pushing forensic capabilities forward into the ITO to help the Warfighter: (1) identify insurgents, terrorists, and/or enemy combatants; (2) link them directly to equipment, documents, or devices and (3) provide the documented basis for action (Figure 1).

- Nuclear DNA
- Drug Chemistry
- Digital Evidence
- Latent Prints
- Forensic Pathology
- Trace Evidence
- Forensic Documents
- Forensic Odontology
- Forensic Toxicology
- Firearms and Toolmarks
- Forensic Anthropology
- Mito-DNA
- Forensic Databases

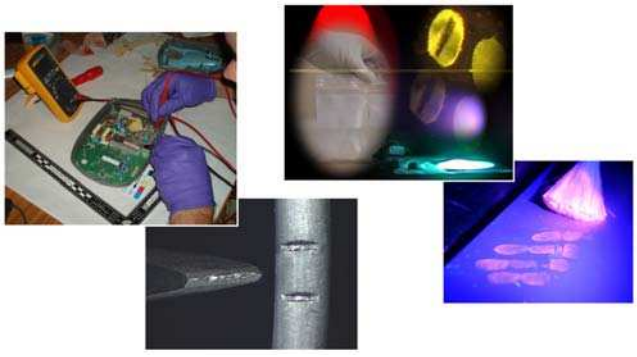

Figure 2

DOD Forensic Toolkit

Although the DoD possesses considerable forensics capabilities (see Figure 2), the focus has been traditionally on investigative, judicial, and medical functions. However, **emerging forensic capabilities also significantly aid the U.S. and coalition forces' intelligence operations** resulting in the identification of friendly and enemy forces and the elimination of enemy threats through disruption, targeting, detention, and subsequent prosecution.

Analysis of forensic materials acts as a force multiplier by enabling operating forces to identify enemies and **add depth and scope to the intelligence picture.** Items such as fingerprints and DNA enable Warfighters to identify specifically who handled an item, such as an improvised explosive device (IED), and to connect a particular person with a certain place or events. **The resulting information often provides the usable intelligence, moral, and legal justification needed to target, apprehend, and prosecute terrorists or enemy combatants.**

Capabilities to collect, analyze, and exploit latent prints, DNA, firearms signatures, tool marks, trace evidence, and document and media exploitation have all been employed in the ITO with great success. DoD is transcending traditional uses of forensic science by becoming surge-capable and focused on providing holistic and sustainable service to a multi-use customer, based world-wide.

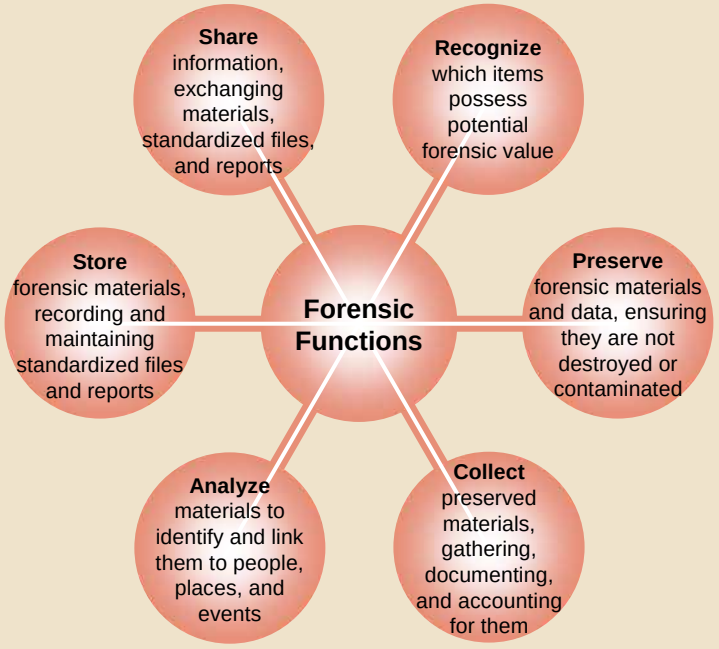

Figure 3

Six Forensic Functions

DoD recognizes six forensics functions listed below. These functions do not always occur sequentially and they often occur in parallel order (see Figure 3).

Recognize: This involves locating and distinguishing materials that have potential forensic value. It may entail special methods to detect items.

Preserve: This involves protecting materials and data from the moment those items are recognized as holding potential forensic value. Materials must be protected and preserved by available, reasonable measures (marking, packaging, and tracking) to prevent contamination, loss, or alteration.

Collect: This describes recovery of materials from a site. The site is documented and contextual information is recorded, within the parameters allowed by the situation, and the materials accounted for. This often includes limited processing of specific items or areas in an effort to detect additional forensically-relevant information. Presumptive testing of materials may also be involved.

Analyze: Forensic analysis may occur from the recognition of materials and contextual information at the site, to in-depth examination at mobile or traditional (i.e., institutional) labs. Presumptive testing of materials may be involved. A variety of factors (the submitting unit's request, expected use of the results, time priorities, available lab resources, etc.) dictate the type of analyses and examinations that a lab will perform

Store: Materials and associated information must be maintained until an issue is fully adjudicated or resolved. Policies and procedures should dictate proper disposition. Balancing information assurance with necessary retrieval capabilities is critical when storing data.

Share: Once forensic analyses are completed, results are catalogued and shared in accordance with policies and procedures. Interoperability is key to developing databases and retrieving information. Sharing information with the relevant stakeholders, to include the submitting unit, is vital.

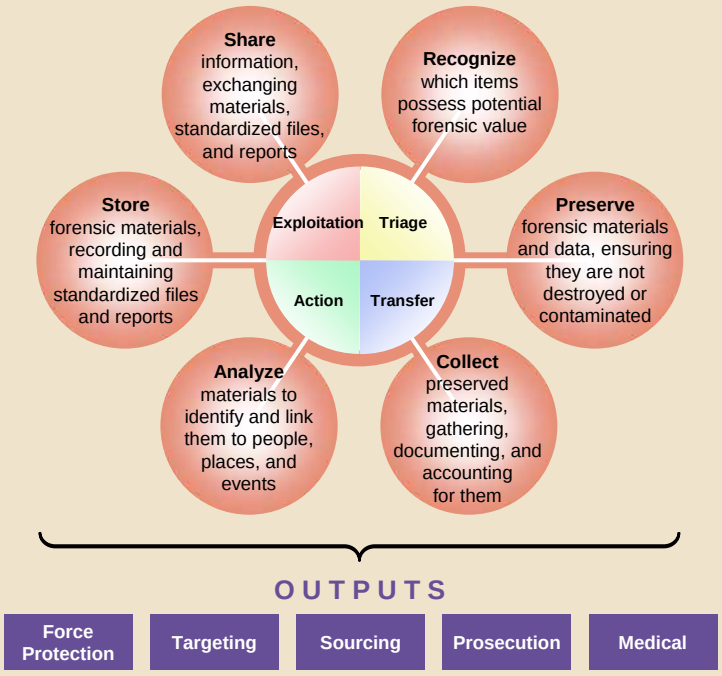

Figure 4

Operational Process

The specific activities performed to carry out the six forensic functions comprise an operational process that is separate from but related to the forensic functions. This process, as depicted in figure 4, includes the activities of **triage, transfer, exploitation and action,** each of which may occur in any or all of the forensic functions.

Triage: Forensic materials are prioritized or triaged at nearly every step of the operational process. This begins at the site by deciding which materials might hold forensic value. Triage continues each time an individual handles or examines the materials. The appropriate facility for analysis (e.g., lab) must be confirmed—and whether the materials can indeed be analyzed.

Triage also involves prioritizing which lab section(s) should receive which materials, as well as how long the materials should be stored. Even the reporting and sharing of information is prioritized.

Transfer: Transfer consists of physically transporting materials or transmitting electronic information. Once forensic materials are in the hands of those collecting them, the materials and information are usually transferred to an appropriate location that allows for a more complete analysis (see Transfer Process in Figure 8).

Exploitation: Exploitation is taking full advantage of any information for tactical, operational, or strategic purposes. After the information, personnel, and materials collected during operations are forensically analyzed, the resulting actionable intelligence is fed back into the operations process—in a word, exploited—to produce an advantage for follow-on actions. Exploitation uses the results of forensic analysis, to produce an action.

Action: Exploiting the results of forensic analysis may lead to such actions as targeting, apprehension and prosecution of suspects, or helping medical personnel resolve their issues. Once the appropriate action has been taken to exploit the results of the scientific analyses, the operational process has been completed.

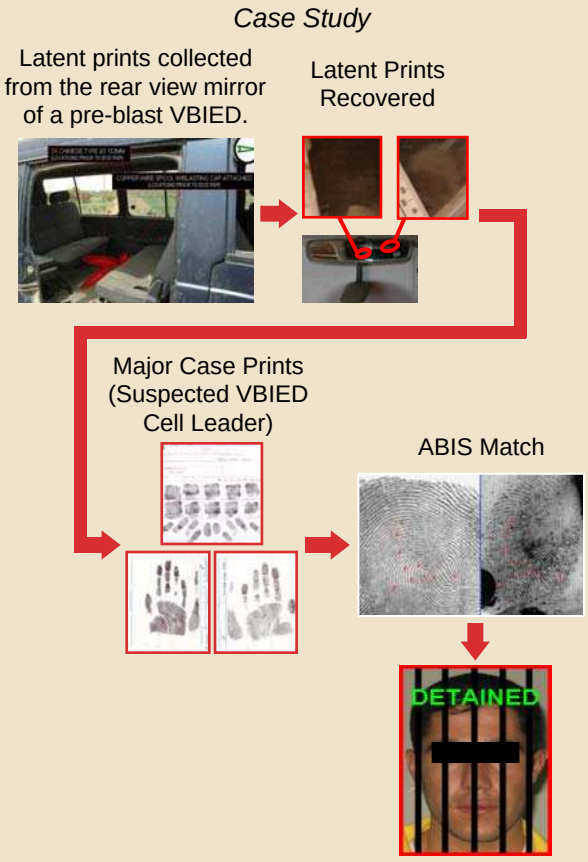

Figure 5

Mission Areas Defined

Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF) have validated the importance of forensic science to the military decision-making process across all echelons of warfare, from near real-time actionable intelligence for tactical commanders to products relevant to combatant commanders, Services, DoD, and national intelligence activities.

Force protection: Preventive measures taken to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information.

Targeting: The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.

Sourcing: Linking the exploited forensic material in conjunction with other information obtained through law enforcement or intelligence channels, both deployed forward and in CONUS, to provide an overarching picture of movement and origin of components, regional groups involved, and transnational sponsorship.

Support to prosecution: Matching individuals to particular locations, events, or devices, through the collection, analysis, and exploitation of forensic material. Utilizing latent prints (LPs), tool marks, trace evidence, DNA, and analysis from other forensic disciplines. Forensics assists with "hold and release" decisions at the site (see case study in Figure 5). Results can be compiled for a criminal prosecutorial package, which will be used in conjunction with testimony of experts in order to further detain or charge an individual suspected or proven to have been involved in acts against coalition forces or Iraqi Security Forces.

Medical: Identification of individuals and determination of the cause and manner of death.

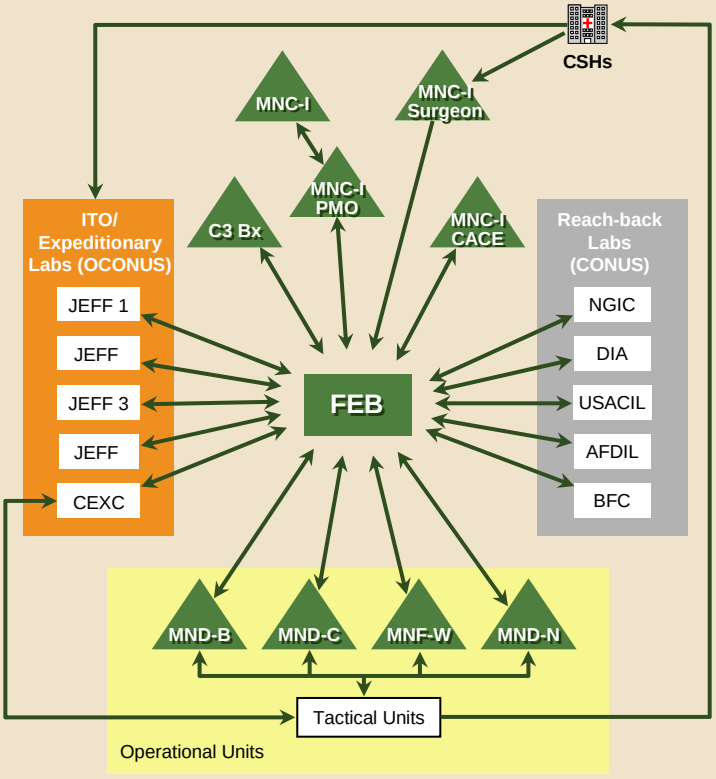

Figure 6

The Forensic Landscape

Within MNC-I, a Forensic Exploitation Battalion (FEB) (see Figure 6) is responsible for forensic operations. The FEB provides C2 for four geographically dispersed Joint Expeditionary Forensic Facilities (JEFF) (one per MND/F). The FEB provides MNC-I and subordinate commands with responsive, time-sensitive forensic analysis and exploitation. The FEB helps to integrate and synchronize the elements of the forensic functions and process shown in figures 3 and 4.

JEFFs are relocatable laboratories (trailers, shelters, and/or buildings) that provide the capability to perform processing, analyses, and exploitation of non-IED forensic material, disseminate and share information, and support reach-back functions among laboratories, deployed elements, and/or at a site.

The Combined Explosives Exploitation Cell (CEXC) was initially established in 2004 to provide in-theater analysis, TECHINT, advice to explosive ordnance disposal (EOD) personnel on IED construction and techniques in order to indentify trends, identify IED bomb makers and enable both offensive and defensive counter-IED operations by Coalition Forces. All IED material is transferred to CEXC for initial analysis.

For additional capabilities, quality assurance, and surge capacity, organizations in CONUS are utilized. These organizations may include the National Ground Intelligence Center, Defense Intelligence Agency, U.S. Army Criminal Investigation Laboratory, Armed Forces DNA Laboratory, and the Biometric Fusion Center.

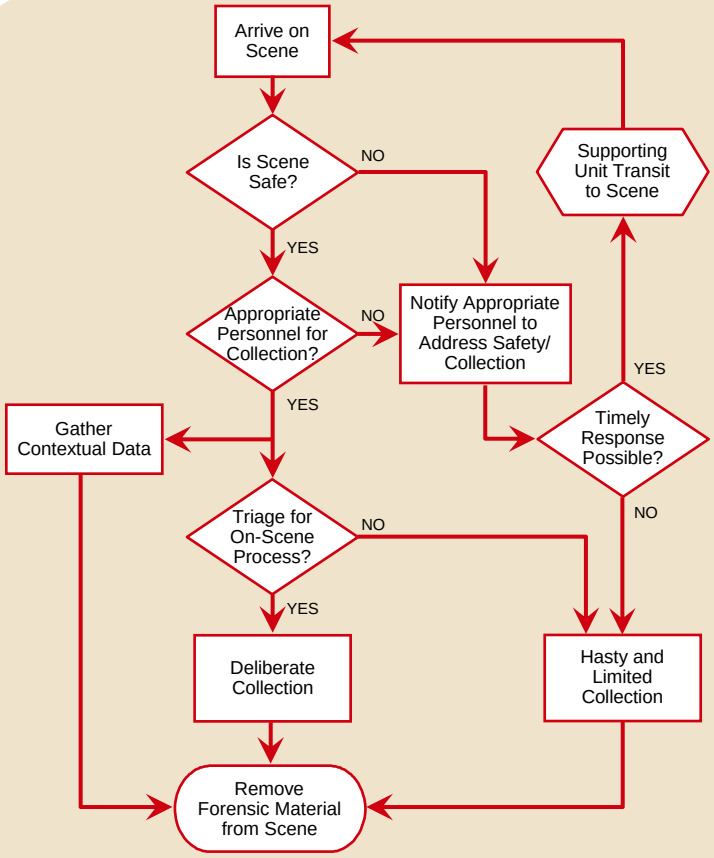

Figure 7

The Collection Process

Site collection (Figure 7) may cover a wide-ranging variety of physical evidence—blood and other biological materials, computer materials, explosives, drugs, firearms, and more. At a minimum, the collector must photograph and/or sketch the evidence in its original position; properly collect and package the evidence and properly mark the evidence to ensure that it is legally sufficient for potential later prosecutions. Collection involves carefully packaging detected items so that their physical integrity is maintained (in containers providing appropriate levels of protection), cross-contamination with other items is prevented, and a chain of custody is initiated.

The collection of forensic materials for eventual submission to a laboratory should be completed systematically to preserve the intelligence and/or evidentiary value of the items, and the process needs to capture all of the relevant contextual data (the five Ws—who, what, where, when, and why) that time allows. Collecting and submitting any amount of forensic material (physical evidence) without providing the context in which it was obtained severely limits its usefulness for any subsequent forensic analyses.

While recognizing and dealing with the safety and security of each location, collectors and their leaders must learn to identify, search for, locate (detect), collect, and preserve items. This may also entail the limited "processing" of items, such as developing latent prints from fixed items (large and/or immobile structures or objects such as doorways and desktops) when the need is present and security allows for it.

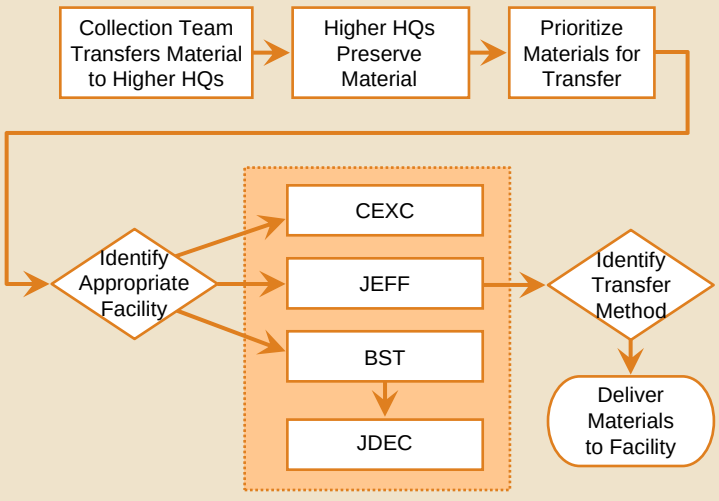

Figure 8

The Transfer Process

Transfer consists of physically transporting materials or transmitting electronic information. Once forensic materials are in the hands of those collecting them, the materials and information are usually transferred to an appropriate location that allows for a more complete analysis. Factors such as the type of forensic material (e.g., IED, non-IED), perishability, the purpose of the follow-on forensic examination (identification, targeting, detention, prosecution, or sourcing), the distance to the lab, the mode of transportation available (ground, air, or mail), conditions (a secure or non-secure area), and weather all play a role in determining when, how, and where the collected material will be transported (Figure 8).

Material related to explosives or a weapon of concern, including explosive charges, suspected HME, electronic components, containers, timers, anti-material rifles, and improvised or modified weapon systems or delivery methods—should be transported to CEXC for exploitation.

Material not related to explosives—such as firearms, human remains, and latent prints—may be transported to one of the JEFFs for exploitation.

Documentation or media-related material, including such things as hard drives and manuals, should be transported to the BST at the BCT level for exploitation and translation.

Chain of custody, contextual information, and preservation of forensic material are paramount throughout the transfer process.

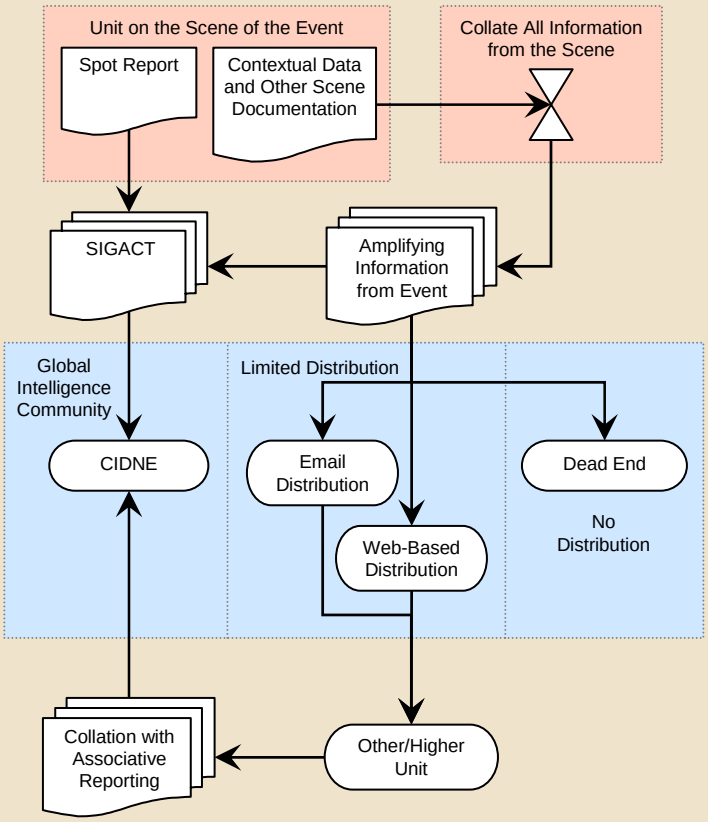

Figure 9

Contextual Information Data Flow

Figure 9 represents the unit's flow of information resulting from the collection of forensic material and the supporting contextual data.

Spot report—produced by the unit responding to the scene. While on the scene of the event, the unit produces a SITREP, SALUTE, or spot report (in general) for higher headquarters and/or BDOC/JOC. It may request further support or indicate the level of activity and provide feedback for completion of efforts at the scene of the event.

SIGACT—the higher headquarters and or BDOC/JOC of the unit responding to the scene of an event normally will normally produce a SIGACT or significant activity report. The collection of forensic material should always have a SIGACT associated with it to preserve the most contextual data possible and tie it to other important information and distribute it to a global information pool.

Amplifying data—upon returning from the site, the responding unit should consolidate all contextual data associated with the event. This should include all relevant reporting generated in relation to the scene, detainee data, photographic records, and storyboard-type information. Ideally, this amplifying information should be linked directly with the SIGACTs in order to distribute it widely to the global intelligence community. The amplifying data should be collated by the unit's S-2 or S-3 and distributed to a larger audience through the direct association of the information via Combined Information Data Network Exchange (CIDNE), the CENTCOM-directed reporting tool for Iraq, Afghanistan, and the horn of Africa for SIGACTS, IED, and HUMINT reporting.

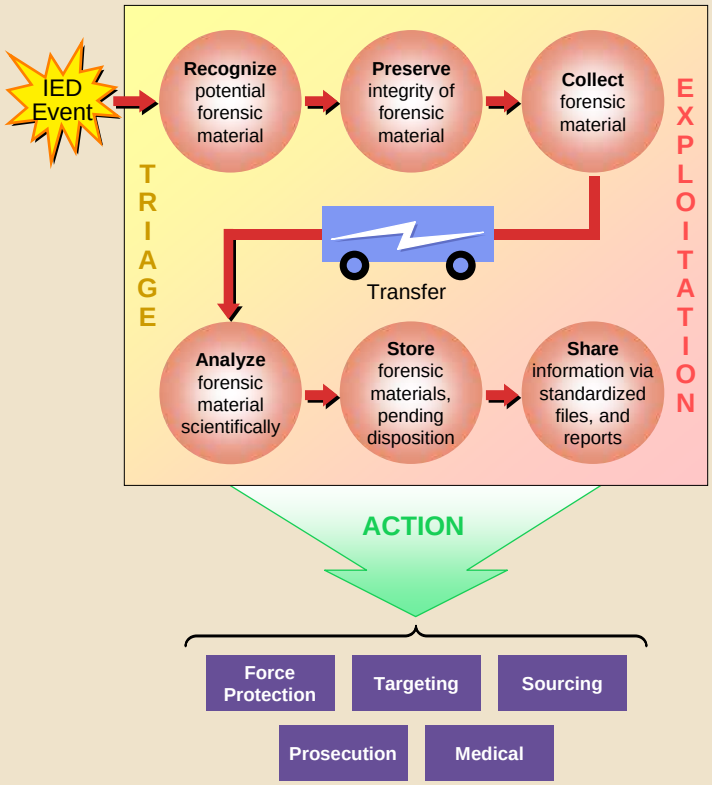

Figure 10

IED Explosion: A Vignette Illustrating the Six Forensic Functions and Operational Process

The event of an Improvised Explosive Device (IED) explosion serves to illustrate the forensic functions. A military convoy inadvertently explodes an IED. Personnel trained to **recognize** the potential items that can be further examined for information must process the site. The search for IED parts begins at the crater created by the explosion and works outward, within the security limitations of the scene, until all possibilities are exhausted. The forensic items are then **preserved** in such a way as to ensure their integrity, after which they are **collected** (recovered) and transported to the appropriate forensic facility. Upon arrival, the items are subjected to scientific **analyses**. The physical materials are **stored** until their proper disposition is determined. Reports are written and **shared** with the submitting unit, higher commands, and other decision makers. Commanders and supporting staff members can then use the reports to make decisions and take action (see Figure 10).