



Document and Media Exploitation

The National Drug Intelligence Center (NDIC) Document and Media Exploitation (DOMEX) Branch has developed a uniquely efficient approach that allows analysts to quickly organize and assimilate significant amounts of seized documentary and electronic evidence. NDIC's DOMEX methodology integrates the requesting agencies' case agents, prosecutors, and analysts into the DOMEX mission planning process, thereby ensuring that the DOMEX mission will be focused to meet the needs and priorities of the requesting agencies. In conjunction with the requestors, our experienced personnel establish the Priority Intelligence Requirements (PIRs) for each DOMEX mission, particular to each requestor's investigation, by identifying critical concerns and limiting the scope of the mission to the most important elements. The DOMEX analysts are able to quickly identify the key associations and investigative leads from the evidence. As a result, investigators, analysts, and prosecutors can more rapidly determine the scope of their evidentiary holdings, identify previously unknown relationships and assets, and better prepare for court proceedings. All DOMEX personnel are trained in proper evidence handling techniques to ensure that our services are conducted with the utmost professionalism.

DOMEX Provides:

Timely Intelligence Support Reports (ISRs) containing actionable findings, methodologies, associates, or other investigative leads, including:

- Financial information and asset identification
- Criminal history and biographical data
- Relevant organization profiles and associations
- A detailed inventory of suspect findings
- Computer-assisted analyses such as link analysis, matrix analysis, time line analysis using i2 Analyst's Notebook, and geospatial analysis using ArcView Geographic Information Systems
- Real-time results: all documents typically analyzed in a 5- to 10-day period

Equipment and Facilities

Depending on operational requirements, DOMEX will analyze evidence at NDIC facilities in Johnstown, Pennsylvania, or at our satellite location at the Joint Language Training Center in Salt Lake City, Utah, using teams of 10 to 25 analysts. NDIC has an in-house mission room that allows multiple DOMEX missions to be conducted simultaneously. DOMEX may also travel to your location and work onsite when deemed necessary. DOMEX deployable equipment consists of laptop computers and a server, which are networked onsite. Additional equipment may include printers, digital cameras, and assorted hardware and software.



Analysis

DOMEX provides new leads as they are identified throughout the mission, along with a comprehensive and fully sourced Intelligence Support Report (ISR), which is provided at the end of the mission, in both hard and soft copy. The ISR contains all actionable findings, including previously unknown links, financial information, and asset identification. DOMEX also provides an out-brief of significant findings at the conclusion of the mission.

DOMEX analysts are trained to identify assets for seizure and contribute significantly to forfeiture efforts. After each mission, DOMEX may provide further analytical services such as charts, time lines, and geographical mapping products, if needed, subsequent to the mission for court proceedings. Additional interim reports or briefings containing time-sensitive or perishable information may also be provided as needed.

DOMEX provides all completed analyses directly to the client agency to ensure compliance with dissemination policies and existing agreements. The requesting agency alone determines the degree of dissemination.

DOMEX provides its support to investigations targeting drug trafficking, money laundering, counterterrorism, and any other investigations that impact U.S. national security. DOMEX can support classified, sensitive, and foreign language investigations.

Digital Evidence Laboratory

As criminal organizations increasingly use computers and other data storage devices to further their illegal activities, there is a strong probability that electronic media will be part of your seizure. Electronic media include, but are not limited to, computer hard disk drives, removable media, mobile phones, smart phones, personal digital assistants, and gaming systems.

NDIC's Digital Evidence Laboratory (DEL) includes teams of information technology specialists who conduct electronic media exploitation using state-of-the-art equipment and technology. They perform examinations of electronic media onsite or at NDIC. Electronic data are provided in a viewable format and are integrated into a DOMEX ISR. Virtually all requests for media exploitation are incorporated into DOMEX missions. This ensures a more comprehensive and efficient analytical product.

Key NDIC Tools—RAID and HashKeeper

NDIC created the Real-time Analytical Intelligence Database (RAID) to manage large quantities of data gathered during DOMEX operations. RAID is a relational database used to record key pieces of information and to quickly identify links among people, places, businesses, financial accounts, telephone numbers, and other investigative information examined by our analysts. The software runs on any Windows operating system (Windows 2000 or higher), in any mode of operation (stand-alone or LAN). It can be used to analyze any type of information from any kind of investigation or as a case investigative/intelligence tool.



NDIC has enhanced RAID to meet the expanding support requirements of the intelligence and law enforcement communities. The improved RAID can be used for both DOMEX and investigative case intelligence support. RAID also facilitates our capability to conduct cross-case analysis. Key upgrade features include increased data storage, scalability (small database to very large, supporting a few users to hundreds), more comprehensive and efficient analytical tools, enhanced multimedia capability, an import/export wizard, dynamic additional data fields (configurable by users), data access security, easier combination/separation of cases, and the ability to apply data mining technologies across data sets.

Just as DOMEX uses RAID as its principal tool, specialists created the HashKeeper program to expedite the examination of electronic media. HashKeeper is a software application that quickly eliminates known operating system files and focuses on electronic files created by the user/subject of the investigation.

Both RAID and HashKeeper are available free of charge, and thousands of these applications have been distributed to appropriate law enforcement and intelligence agencies worldwide.

Cost to Client Agency

NDIC's DOMEX Branch provides its service at little cost to the client agency when the missions are conducted in-house at NDIC. In most instances we

ask that a case agent or prosecutor travel to NDIC at the client agency's expense to provide background on the case and address analysts' questions. The resulting analysis will be stronger with this agent/analyst interaction. If the client agency requests onsite support from DOMEX staff, the client is responsible for all travel-related costs. Additionally, if NDIC personnel are required to testify as a result of their support to an investigation, NDIC travel-related costs will be borne by the client agency.

How to Obtain DOMEX Support

Support is available to federal agencies or multi-agency law enforcement task forces and is determined on a priority basis. Any agency wishing to obtain support should submit a formal request to the Chief of the NDIC DOMEX Branch. The request should be made via the client agency's established protocol and should include the investigation summary, the priority of the investigation within the requestor's division, and an estimate of the nature and volume of the seized material to be analyzed by DOMEX. Optimally, all requests should be submitted to NDIC in advance of the projected seizure to ensure adequate case and logistical preparation. In most instances a telephonic assessment of the investigation and seized material will be conducted. For complex investigations or large quantities of seized material, it may be necessary for a DOMEX advance team to conduct an assessment at the requesting field office. A final determination of DOMEX support will be made after the assessment is completed.

**Please send all requests for
DOMEX support
as well as copies of
RAID and/or HashKeeper to:**

**National Drug Intelligence Center
Document and Media Exploitation Branch**

319 Washington Street, 5th Floor
Johnstown, PA 15901-1622

Telephone: (814) 532-4601
Fax: (814) 532-5854

E-mail: ndic.domex.request@usdoj.gov

Cover photos © Adobe Illustrator, Digital Vision Ltd. and Eyewire.

Revised 070908

Document and Media Exploitation



**U.S. Department of Justice
National Drug Intelligence Center**