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. This methodology—HashKeeper and the Real-time Analytical Intelligence Database (RAID) software—allows associations and investigative leads to be quickly identified. As a result, investigators, analysts, and prosecutors can more rapidly determine the scope of their evidentiary holdings and previously unknown relationships and assets and are better equipped to prepare for court proceedings.

DOMEX Provides:

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

- Financial information/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, and timeline analysis using i2 Analyst Notebook, and geospatial analysis using ArcView Geographic Information Systems.
- Real-time results: all documents typically analyzed in a 5-10 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 week, along with a comprehensive ISR and an out-brief of significant findings at the conclusion of the mission.

After the initial mission, analysts can provide further analytical services to the requestor for a limited time. DOMEX may provide interim reports or briefings containing time-sensitive or perishable information 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.

Please note that this service is currently limited to significant counternarcotics, counterterrorism, or national security 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, and personal digital assistants.

NDIC's Digital Evidence Laboratory (DEL) includes teams of information technology specialists who conduct electronic media exploitation with state-of-the-art equipment and technology. They perform real-time computer examinations onsite or at NDIC. Electronic data are provided in a viewable format as well as being 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 Pieces of Software—RAID and HashKeeper

NDIC created 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 management 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.

REAL-TIME ANALYTICAL INTELLIGENCE DATABASE

RAID

Just as DOMEX uses RAID as its principal tool, specialists created the HashKeeper program to expedite the analysis 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 these instances, however, we ask that an agent/investigator 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 on-site 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 multiagency law enforcement task forces with a federal component 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 as far as possible in advance of the projected seizure to ensure adequate case and logistical preparation. A DOMEX advance team consisting of a Team Leader and a Lead Analyst may travel to the requesting federal field office to conduct an assessment of the seized material and to begin coordination for the future Doc Ex mission. A final determination of DOMEX support will be made after the advance team returns to NDIC.

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

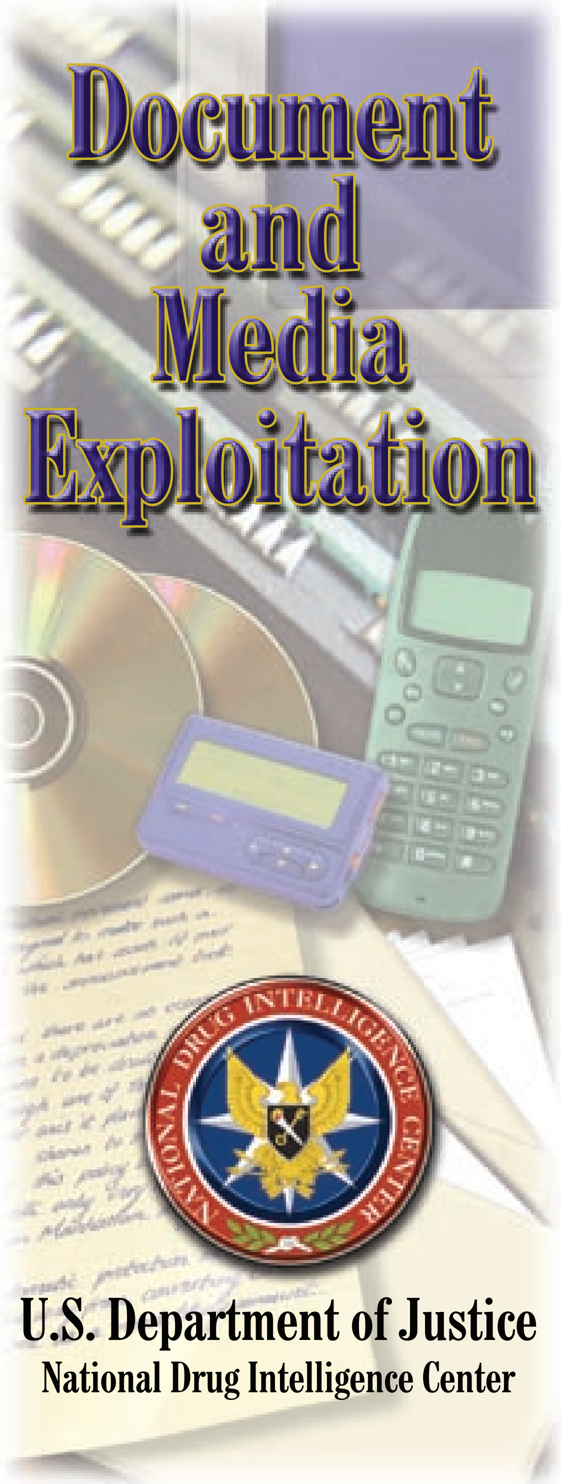
319 Washington Street, 5th Floor
Johnstown, PA 15901-1622

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 052008



Document and Media Exploitation

NATIONAL DRUG INTELLIGENCE CENTER

U.S. Department of Justice
National Drug Intelligence Center