A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER

Information Technology (XT)

The **Directorate of Information Technology (XT)** unifies IT operations end-to-end and provides the organization with a singular area of focus for IT-related issues, including application development, knowledge management, records management, service desk, network, and software and hardware management.

XT provides technical solutions and network and systems expertise for the DC3 mission spaces as well as external stakeholders providing tools and services to DoD Intelligence and Law Enforcement communities. XT also functions as the DoD repository for cyber counterintelligence tools. The expertise of the staff involves help desk, technical, and project support as well as creating innovative solutions, enterprise architecture, records management and knowledge management. Primary mission focal points include:

- Management of 12 multiple classification networks both on-premise and in the Cloud—some standard DoD, others non-DoD—in support of Defense Criminal Investigations.
- Tailoring innovative software and system solutions engineered to the specific requirements of digital forensic examiners and cyber intrusion analysts.
- Validating digital forensic tools from the Commercial off-the-shelf, Government off-the-shelf and open source domains to ensure relevancy and reproducibility as to expected use in coordination with our cooperative partnerships.
- Leads the way through proactively identifying, researching, and evaluating relevant new technologies, techniques and tools.
- Actively participates in the development of industry standards including the Structured Threat Information eXpression (STIX) and Cyber-investigation Analysis Standard Expression (CASE).
- Maintains the Counterintelligence Tool Repository (CITR), a warehouse of classified and unclassified tools that support digital forensics and counterintelligence needs.

TECHNOLOGIES

Information Technology (XT) maintains, develops, and supports a large variety of tools and enterprise solutions for DC3 mission areas, DC3 customers, and other partnering agencies. Several notable efforts are highlighted below:

Analytic Customer Portal–The Analytic Customer Portal is a system that hosts a number of datasets for analysts both internal and external to DC3. The system provides users the ability to search DNS-monitored data, GeoIP data, and additional data sources. Additionally, users can submit Requests for Information (RFIs) to the Analytic Group within DC3 at: https://analytics.dc3.smil.mil

Customer Portal–The Customer Portal houses a number of products and services of interest to external customers of DC3, including operational status updates, event coordination, and product download links. The Portal provides information on DC3 Cyber Forensics Laboratory case status and regulates access to the DC3 legal document repository. Finally, the Portal serves as a management solution for DC3 TechEx events, with tools to assist in planning sessions and logistics, registering participants, and conducting post-conference surveys. The Customer Portal also provides access to DC3-developed tools as well as validation reports for forensics tools completed by DC3 and the U.S. Army. The toolbox that can be found in the Portal at https://customerportal.dc3.mil includes the following:

- **DC3 Advanced Carver (DC3AC)–**DC3AC is a state-of-the-art, patented file-carving capability to extract complete or partial files from unknown data sets, which can include those found within unallocated space on device images, memory dumps, page files, and corrupt files. Targeted file formats can encompass images, videos, documents, databases, and executables. DC3AC contains a number of unique algorithms for identifying, reconstructing, and repairing file fragments that would otherwise be unreadable.
- **DC3 SQLite Dissect–**DC3 SQLite Dissect is a SQLite file parser offering capabilities to recover and retrieve deleted information. Data is recovered through analysis of the contents of the SQLite files and generation of signatures for the data. Those signatures are then used to dissect unallocated space within the files. DC3 SQLite Dissect supports both SQLite databases and Journaling files. The tool uses a write-ahead log (WAL) to determine the timeline of events in order to reveal transactional history, which can be used to generate reports on user activity (e.g., the addition and deletion of data over time). DC3 SQLite Dissect includes an Application Programming Interface (API), and can export recovered results in multiple formats, such as CSV (Comma Separated Values), XLSX (Excel), and SQLite.
- **Electronic Malware Submission (EMS)–**EMS allows both DC3 analysts and external customers to safely and securely submit malware for examination. Submitters have the option of requesting a thorough examination to be conducted by a reverse engineer from the Cyber Forensics Laboratory within DC3, or requesting an automated analysis report (results of which can be available within minutes) generated by a combination of the dozens of exploitation tools created and curated by DC3 subject matter experts. Submissions may be made at: https://ems.dc3on.gov/
- **GeoSuite–**GeoSuite is a set of capabilities centered around geospatial visualization and analysis. Currently, it consists of an offline geospatial mapping capability which supports plotting of files based on geo metadata and GeoIP, cell tower locations, along with Wi-Fi hotspots based on open source and commercial datasets. The second offering in the GeoSuite serves as a parsing tool to output data in a format which can be visualized in the mapping capability. Currently, the parser supports a number of commercial small Unmanned Aircraft Systems (sUAS), fitness trackers, and dash cams. Finally, in concert with the offline mapping capability, the third tool provides a visualizer for sUAS flight paths with associated telemetry data overlays.
- **Missing Links–**Missing Links is a forensic analysis tool suite comprised of two software components: the Missing Links Explorer and the Missing Links Extractor. The concept sprang from the need to support forensic examiners, in both field and lab settings, to be able to quickly identify the "missing links"–apparent gaps in the evidence associated with a particular case. The resulting suite of tools leverages the processing power of commercial tools to scale correlation capabilities across thousands of data sources and billions of forensic artifacts.