A FEDERAL CYBER CENTER

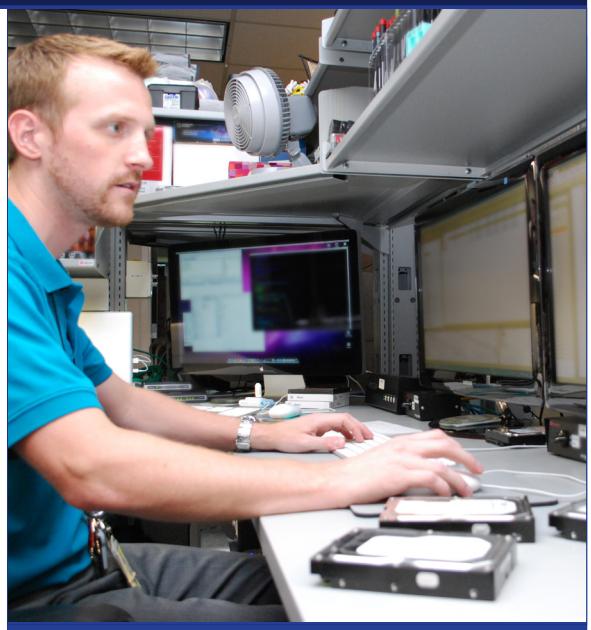
DoD CYBER CRIME CENTER (DC3)

Technical Solutions Development

TSD FACT SHEET

Technical Solutions Development (TSD) tailors innovative software and system solutions engineered to the specific requirements of digital forensic examiners and cyber intrusion analysts. TSD validates 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 addition our cooperative partnership:

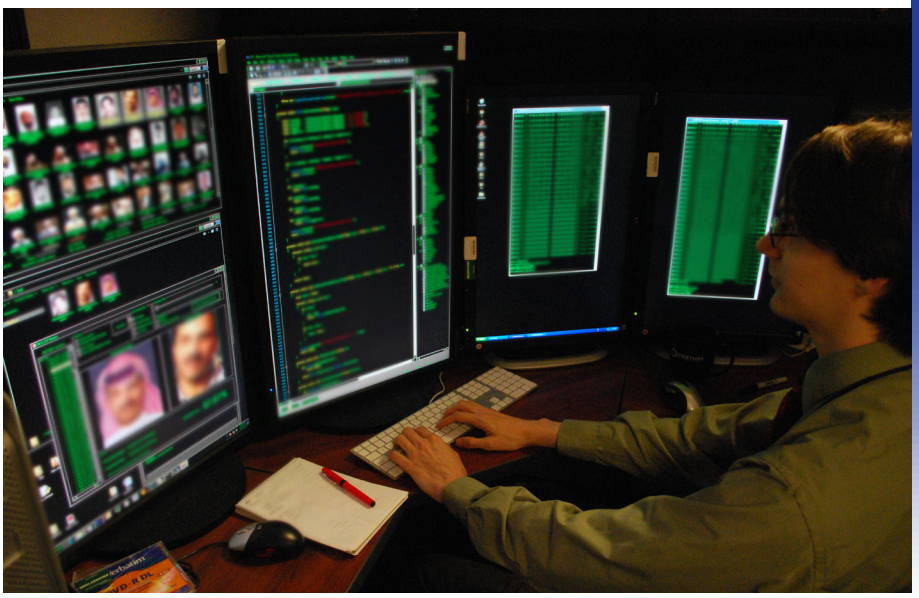
- Leads the way through proactively identifying, researching, and evaluating relevant new technologies, techniques and tools
- Actively participates in the development of industry standards including the Structured Threat Information eXpression (STIX) and Cyber-investigation Analysis Standard Expression (CASE)
- Shares in-house developed tools with federal, state and local law enforcement partners
- Maintains the Counterintelligence Tool Repository (CITR), a warehouse of classified and unclassified tools that support digital forensics and counterintelligence needs



A TSD Engineer developing new capabilities to optimize and streamline manual digital forensic processes.

" Supporting Law Enforcement, Counterintelligence, and Defense Criminal Investigative Organizations "

—TSD



DoD CYBER CRIME CENTER

TSD@dc3.mil

410-981-6610 | www.dc3.mil | info@dc3.mil

@DC3Forensics
@DC3 Cyber Crime Center

TECHNOLOGIES

Technical Solutions Development (TSD) 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 — 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 a social media database. Additionally, users can submit Requests for Information (RFIs) to DC3's Analytic Group (DC3/AG). https://analytics.dc3.smil.mil

Columbo — Columbo is a web-based application that provides a centrally managed repository to enable the collection and sharing of cyber threat data amongst analysts in DC3/AG, DC3's Defense Industrial Base Collaborative Information Sharing Environment (DCISE) and partnering cybersecurity centers. Columbo's backing repository is based on the DC3 Analytic Database (DAD). DAD merges existing analytic databases into a standardized database allowing for increased analytic capabilities, controlled access and increased sharing. DAD provides an API for current and future analytic applications allowing importing, exporting (through analytic tools) of threat data, and for execution of analytic scenario use cases.

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 human-based examination by a reverse engineer from DC3's Cyber Forensics Lab (CFL) or receiving an automated analysis report within minutes based on dozens of exploitation tools created and curated by TSD and CFL subject matter experts. https://ems.dc3on.gov

Customer Portal — Customer Portal houses a number of services of interest to DC3's external customers, including operational status updates, event coordination and product download links. The Portal provides information on DC3 Cyber Forensics Lab (CFL) case status, access to the DC3 legal document repository, and a management solution for the DCISE TechEx event, including session planning, logistical information, registration and post-conference survey. Additionally, the Customer Portal provides access to TSD developed tools and validation reports for forensics tools completed by DC3 and the U.S. Army. The tools below can be found in the Portal. https://customerportal.dc3.mil

DC3 Advanced Carver (DC3AC) — DC3AC is a state of the art file carving tool capable of extracting complete or partial files from unknown data sets including unallocated space on device images, memory dumps, page files and corrupt files. Targeted file formats include images, videos, documents, databases and executables. DC3AC contains a number of unique algorithms for identifying, reconstructing and repairing file fragments that would be unreadable on their own.

Map My Case — Map My Case is an offline geospatial visualization and analysis tool based on a portable installation of OpenStreetMap. Functionality includes plotting of GeoIP information, cell tower locations, and WiFi hotspot locations based on open source and commercial data sets. The tool can also plot image and video locations based on file metadata, and can display points and paths of interest found within GeoJSON or KML files.

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 originated with a need to support forensic examiners, in both field and lab settings, in quickly identifying "missing" pieces of evidence associated with a case. Missing Links leverages the processing power of commercial tools to scale correlation capabilities across thousands of data sources and billions of forensic artifacts.