DoD CYBER CRIME CENTER
Cyber Forensics Laboratory (CFL)

The **Cyber Forensics Laboratory (CFL)** performs Digital and Multimedia (D/MM) forensic examinations, repairs damaged devices, expertly extracts data that would otherwise be inaccessible, and provides expert testimony in legal proceedings for DC3 customers.

CFL DATA RECOVERY CAPABILITIES

Hard Drives: Repair or bypass most complicated non-responding hard drives in a clean-room environment related to mechanical/logical failures, firmware corruption, bypass security lock, etc.

Flash Drives: Fix broken connectors, chip-off techniques, logical file system reconstruction in the absence of the controller.

Mobile Devices: Micro soldering, logic board repair, In-System Programming (ISP), Joint Test Action Group (JTAG), chip-off, flasher boxes, bootloader, Graykey, and UFED Premium services.

Servers: Any large capacity data storage system will be configured by either a software or hardware Redundant Array of Independent Disks (RAID) controller for RAID0, RAID1, RAID5, RAID6, RAID10, etc. The lab also has the capability to identify degraded drives and rebuild missing data.

Encryption: Proprietary protocols to recover encryption keys related to TPM-, BitLocker-, or WD Smartware-encrypted devices without the master or user password.

Vehicle Applications: Use non-destructive methods to chip-off and recover the data from the eMMC-NAND-NOR chips when vehicle infotainment system, telematics (OnStar), or airbag modules are not supported by commercial software.

Drone: Data extraction from embedded or removable storage device that might or might not require chip off, file system parsing, and geospatial waypoints and timeline analysis.

Thermal Camera: Identifies damaged or malfunctioning components by use of thermal imaging technology.

Milling/Polishing Machine: Remove storage and processor chips from a circuit board that are difficult to remove due to underfill and conformal coating. The machine either mills the circuit board to preserve the chip or mills the chip to preserve the circuit board.

BGA Reballer: Measure solder pads on the chip to allow precision placement of new solder balls to each pad. This process can only be accomplished with a BGA reballer; modern chips are too complex to resolder by hand.

Hot Air Rework System: Remove or attach chips to circuit board using heat profiles based on chip manufacturer specifications.

X-Rays: Capability to capture 2D and 3D projection images to identify internal damage to damaged devices or the integrated circuits.

Digital Microscope: High-resolution 3D microscope for detailed measurement and inspection for failure analysis.

Conformal Coating Remover: Removes conformal coatings containing acrylic, urethane, and silicone from devices protected with these materials.

Wire Bonder: Attach severed bond wires to the circuit board substrate and/or to the embedded crystal memory chip.

Plasma Contaminant Cleaner: Removes organic contaminants from printed circuit boards and chips and prepares surfaces for subsequent processing like BGA reballing and micro wire bonding.

Laser Decapsulation: Removes layers of epoxy conformal coating or potted material to remove the flash memory chip from the circuit board and/or removes the protective cover of flash memory chips to repair severed bond wires.
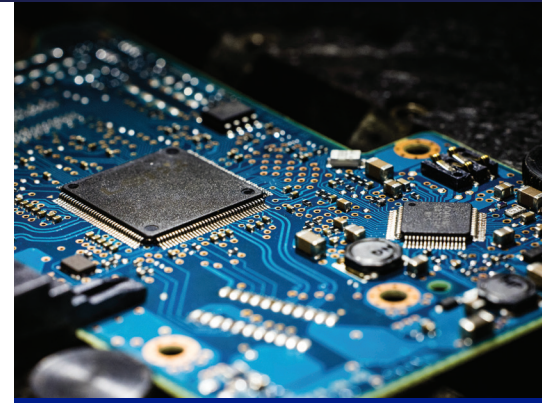
FORENSIC OPERATIONS AND SERVICES

- Counterterrorism
- Counterintelligence Matters
- Crime against Persons and Property
- Fraud
- Embedded Systems and Supply Chain Analysis
- Network Intrusions
- Malware Reverse Engineering and Analysis
- Enhancing Video and Voice Recordings
- Aircraft Mishaps
- Damaged Media and Submerged Devices
- Cell Phones, Tablets, and Other Smart Devices
- Encrypted Media
- Locked Mobile Devices
- Vehicle Infotainment/Telematics
- Internet of Things (IoT) Devices
- Other Emerging Technologies

For assistance please contact Cyber Forensics Laboratory Customer Support & Intake at **410-981-0310** or **DSN 622-2595** or email **afosi.dc3.cflintake@us.af.mil**.