



DCFL

Defense Computer Forensics Laboratory
DC3 Superior Digital Forensics

INTRUSIONS LABORATORY REQUEST

	INVESTIGATOR	ALTERNATE
Name		
Agency Name		
Physical Mailing Address		
Email Address		
Commercial Number		
DSN Number		
Mobile Number		
Fax Number		

Requesting Agency's Case Number or Case ID:

Classification level of case:

Name of **SUBJECT** (LAST, FIRST):

Name and Location of **PARTNER**:

Date Information Rec'd by **DCISE**:

Is this an initial request or a follow on request?

Initial request

Follow-on request.

If this is a Follow-on Request, please provide the DCFL case number:

Describe the situation and background surrounding the investigation, including seizure of the evidence/media:



DCFL

Defense Computer Forensics Laboratory
DC3 Superior Digital Forensics

DEFENSE CYBER CRIME CENTER

INTRUSIONS LABORATORY REQUEST

MALWARE

RAPTOR – Rapid, limited exam performed on a single piece of malware, looking for actionable indicators. Malware must be noted in the media table below. Electronic communication required. This is a best effort product within a 5 hour analysis window (estimate only).

Indicator Based Examination – This exam leverages automated processes to determine malware indicators including a manual technical review and verification by an examiner. If necessary the examiner will supplement the analysis however it will NOT include manual observations to explain the relevance of the indicators.

Operational Leads Examination – This exam includes indicators paired with a “best-effort” manual analysis that may identify additional indicators, characteristics, artifacts, and attributes of the submitted malware and any significant correlation to previous examinations. This product is for customers who prefer to rely on the expertise of the examiners to determine the relevant scope, breadth, and focus of the examination.

Focused Analysis Examination – This exam will focus on answering a discrete set of limited questions defined by the requestor about specific files. Unless otherwise specified, this product will only provide answers to these specific questions and will assume that the customer already has the basic indicators. Time estimates will rely on the difficulty and number of the submitted files and the scope of the request.

Comments- Please describe additional processes to be conducted or any other pertinent information below:



DCFL

Defense Computer Forensics Laboratory
DC3 Superior Digital Forensics

DEFENSE CYBER CRIME CENTER

INTRUSIONS LABORATORY REQUEST

REQUESTED PROCESSES

SYSTEMS

RAPTOR – Rapid, limited exam performed on a single system, looking for actionable items. System must be noted in the media table below. Electronic communication required. (24 Business hours, estimate only)

Standard Exam – All standard examination processes will be performed.

Focused Exam – Examination will only include specific processes requested below:

Comments- Please describe additional processes to be conducted or any other pertinent information below:



DCFL

Defense Computer Forensics Laboratory
DC3 Superior Digital Forensics

INTRUSIONS LABORATORY REQUEST

NETWORK BASED ARTIFACTS

RAPTOR – Rapid, limited exam performed on a single artifact, looking for actionable items. Artifact must be noted in the media table below. Electronic communication required. (24 Business hours, estimate only)

Full Network Capture Analysis – Examination of network capture looking for relevant artifacts.

Text Based Log Analysis – Examination of text logs looking for relevant artifacts.

Comments- Please describe additional processes to be conducted or any other pertinent information below:

MEDIA SUBMITTED FOR EXAMINATION/ANALYSIS

Description	Quantity	Security Classification	RAPTOR

Signature

Printed Name:	Date:	Signature:



DCFL

Defense Computer Forensics Laboratory
DC3 Superior Digital Forensics

DEFENSE CYBER CRIME CENTER

ACCEPTANCE OF TERMS
EFFECTIVE 9 JUL 12

1. ACCEPTANCE OF TERMS

The Defense Computer Forensic Laboratory (DCFL) provides its services (defined below) to you (“the Customer”) subject to the following Terms of Service (TOS), which may be updated by us, from time to time without notice to you. The most current version of the TOS will be attached to the DCFL Form 1 – Laboratory Submission Form. By filling out and signing this form you accept and agree to be bound by the terms and provision of the TOS. In addition, materials and information you submit to DCFL (such as evidence or victim information) are subject to DCFL policy guidelines and procedures applicable to such items. Policy guidelines and procedures are hereby incorporated into the TOS.

2. DESCRIPTION OF DCFL SERVICES

The DCFL works to ensure standardized, efficient case processing and examination to ensure customers receive the maximum benefit from examination results and other DCFL products and services. This effort is conducted using a rich collection of resources including, without limitation or minimum, various forensic and support tools, procedures, protocols, and methods that conform to accepted and standard practices in the forensic community.

The DCFL will conduct a full or limited examination of provided evidence submitted to DCFL, bounded by the terms outlined by customer on the DCFL Form 1 and in accordance to DCFL standard operating procedures and instructions, and to the extent of the DCFL’s capabilities.

Where a case submission requires equipment to be ordered for processing, any remainder of work on the case will be processed separately. Should the required equipment be unavailable, this fact will be communicated with the customer and the media unable to be processed will be returned to the customer unexamined.

Case submissions with special devices (e.g. cell phone, PDA, Xbox) will be processed in a manner to prevent unnecessary holdups in the completion of the case examination, and provide the customer with key case information most expediently.

Evidence sent to the DCFL requiring a damaged media recovery (DMR) procedure to be performed will not be processed until all necessary equipment is in place. This can, at times, mean a lengthy period of time may elapse before evidence is processed.

3. GENERAL PRACTICES REGARDING CASE PROCESSING

From time to time DCFL may deviate from its standard processes in order to use the most efficient and practicable solution to serve the customer.

4. YOUR SUBMISSION OBLIGATIONS

When requesting a case to be processed by the DCFL, the Customer must complete a Form 1 in order to outline the services requested, media submitted, and key background information relevant to the investigation. This will assist DCFL analysts in pinpointing useful data, depth of examination requested, and other pertinent information regarding the request. Customers will also ensure classification markings of individual items and overall collections are quickly and readily identifiable.



DCFL

Defense Computer Forensics Laboratory
DC3 Superior Digital Forensics

DEFENSE CYBER CRIME CENTER

**ACCEPTANCE OF TERMS
EFFECTIVE 9 JUL 12**

The following items must be included with submitted evidence for DCFL to perform an examination:

- Completed and signed DCFL Form 1 – Laboratory Submission Form
- Search authority documentation
- Evidence listing
- Chain of custody document(s)
- Customer reference numbers for evidence, as required by customer regulations
- Notes on Form 1 regarding media that has been damaged prior to shipment to DCFL; also, which person in a case each piece of evidence is associated with, if known (e.g. subject's thumb drive, victim's laptop, etc.)
- All electrical charge cords, download cords, passwords to files/devices (e.g. from a Post-It note of passwords located near the device at a crime scene, or ones given up by subjects during interviews), devices on which a piece of media was created (e.g. a video camera to go with a home video tape), and any other related equipment or information that would increase probability of full access to case-relevant data
- The following must be provided if they exist:
 - Witness statements and/or discussions
 - Subject statements
 - Copy of charge sheet(s)
 - Notes detailing any prior analysis conducted by someone outside DCFL (if applicable)

5. FORENSIC DATA EXTRACTION SUBMISSIONS

Case submissions for the post FDE processing require additional documentation. Customers submitting this type of examination must provide the following additional documentation:

- Documentation noting that a pediatrician has viewed the selected objects
- Documentation noting the case has undergone legal review
- Documentation noting the case has been sent to the National Center for Missing and Exploited Children (NCMEC)
- The following must be provided if they exist:
 - Witness statements and/or discussions
 - Subject statements
 - Copy of charge sheet(s)

6. MISSING OR ADDITIONAL INFORMATION

You agree that DCFL may contact you at any time to request missing or additional information in order to perform an examination on a case. You agree that if this information is not provided, or if after a reasonable period of three business days such requests for information are not met, DCFL has the right to return materials submitted to DCFL unexamined.



DCFL

Defense Computer Forensics Laboratory
DC3 Superior Digital Forensics

DEFENSE CYBER CRIME CENTER

ACCEPTANCE OF TERMS
EFFECTIVE 9 JUL 12

7. GENERAL PRACTICES REGARDING EVIDENCE AND CASE INFORMATION

Strict safeguards are in place for the protection of information and confidentiality of customer information, regardless of how obtained or media in which the information is conveyed (e.g., printed, electronic files, email, or verbal conversation). Information will not be disseminated by DCFL without prior approval from the customer.

Strict evidence handling and storage procedures will be conducted by the laboratory at all times.

DCFL takes exacting care in ensuring its processes do not damage or destroy evidence. However, should this event occur, the customer will be notified as soon as the alteration is recognized.

Discrepancies in evidence will be double checked according to DCFL procedures, and once the discrepancy is verified, the customer will be contacted for resolution. The actions taken in the resolution of evidence discrepancies will be documented and recorded in the case file.

8. COMMUNICATION

The DCFL shall be willing to cooperate with the customer or its representatives in clarifying the customer's request and in monitoring DCFL's performance in relation to the work performed, while ensuring confidentiality for the customer and all other customers.

As soon as practical after receiving a case, DCFL shall complete and send a DCFL Case Receipt Acknowledgement e-mail. A DCFL section chief, the deputy laboratory director, and the case agent's Computer Crime Operations Chief shall be copied on the acknowledgement e-mail.

Further case correspondence, whether by e-mail, fax, mail, or notes/voice recordings of telephone conversations, shall be noted and recorded to be included for record in the case file.

9. NOTICE

You agree that DCFL's use of the ASCLD/LAB name and symbol are trademarks and the property of ASCLD/LAB. Without ASCLD/LAB's explicit prior permission, you agree not to display or use in any manner the ASCLD/LAB name or symbol.