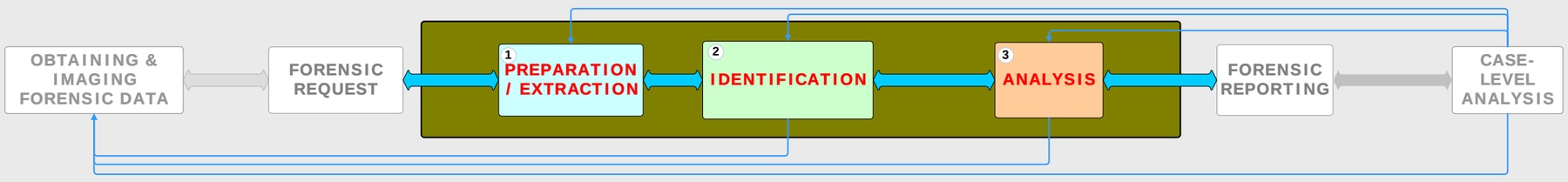
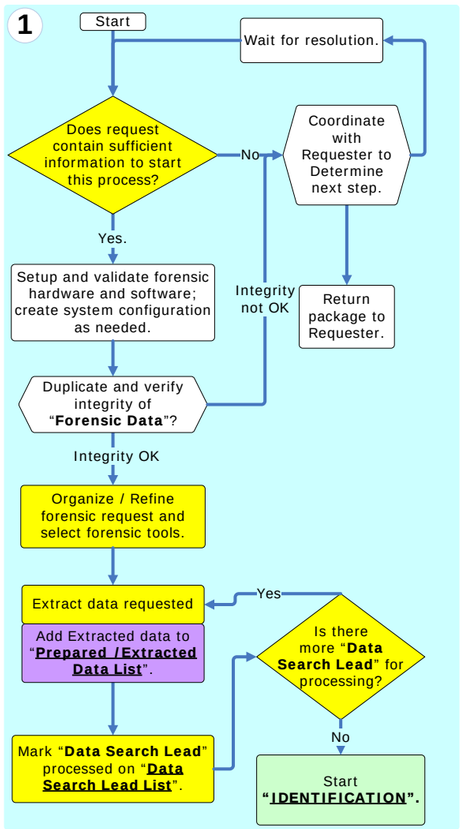
DIGITAL FORENSIC ANALYSIS METHODOLOGY

Last Updated: August 22, 2007

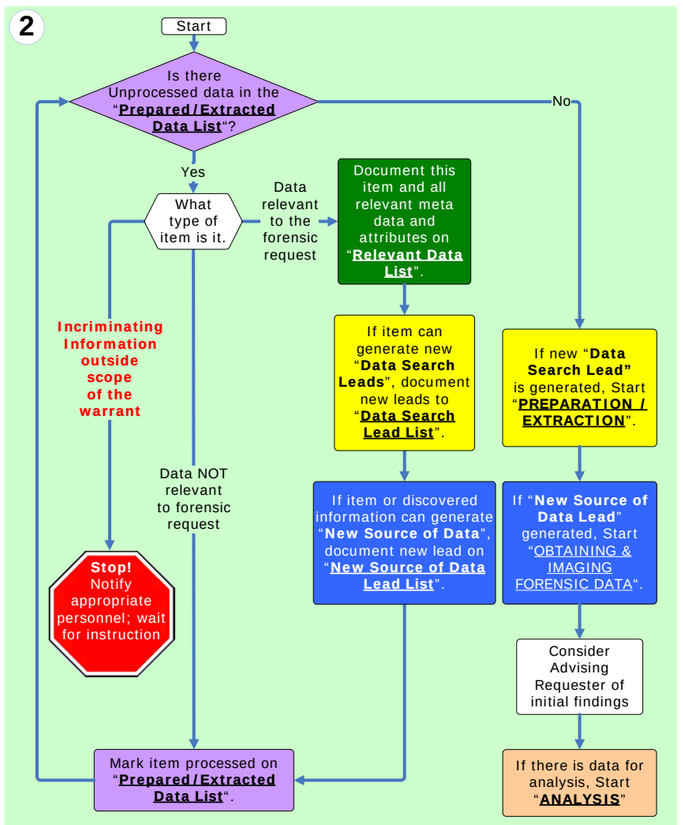
PROCESS OVERVIEW



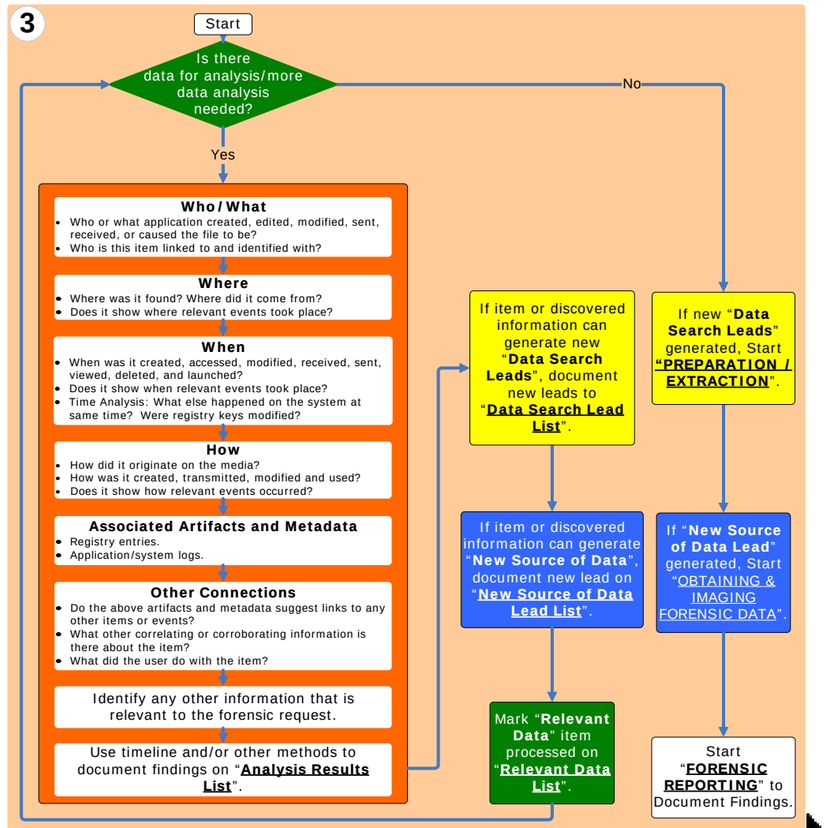
PREPARATION / EXTRACTION



IDENTIFICATION



ANALYSIS



Return On Investment (Determine when to stop this process. Typically, after enough evidence is obtained for prosecution, the value of additional forensic analysis diminishes.)

LISTS

Search Leads

Data Search Leads	Comments/Notes/Messages
Generally this involves opening a case file in the tool of choice and importing forensic image file. This could also include recreating a network environment or database to mimic the original environment. Sample Data Search Leads: • Identify and extract all email and deleted items. • Search media for evidence of child pornography. • Configure and load seized database for data mining. • Recover all deleted files and index drive for review by case agent/forensic examiner.	Use this section as needed. Sample Note: • Please notify case agent when forensic data preparation is completed.

Extracted Data

Prepared / Extracted Data	Comments/Notes/Messages
Prepared / Extracted Data List is a list of items that are prepared or extracted to allow identification of Data pertaining to the forensic request. Sample Prepared / Extracted Data items: • Processed hard drive image using Encase or FTK to allow a case agent to triage the contents. • Exported registry files and installed registry viewer to allow a forensic examiner to examine registry entries. • A seized database files is loaded on a database server ready for data mining. •	Use this section as needed. Sample Message: • Numerous files located in c:\movies directory have .avi extensions but are actually Excel spreadsheets.

Relevant Data

Relevant Data	Comments/Notes/Messages
Relevant Data List is a list of data that is relevant to the forensic request. For example: • If the forensic request is finding information relating credit card fraud, any credit card number, image of credit card, emails discussing making credit card, web cache that shows the date, time and search term used to find credit card number program, Etc are Relevant Data as evidence. In addition, Victim information retrieved is also Relevant Data for purpose of victim notification.	Use this section as needed. Sample Note: • Attachment in Outlook.pst>message05 has a virus in it. Make sure an anti-virus software is installed before exporting and opening it. • Identified and recovered 12 emails detailing plan to commit crime.

New Data Source Leads

New Source of Data Leads	Comments/Notes/Messages
New Source of Data Lead List is a list of data that should be obtained to corroborate or further investigative efforts. Sample New Source of Data Leads: • Email address: Jdoe@email.com. • Server logs from FTP server. • Subscriber information for an IP address. • Transaction logs from server.	This is self explanatory. Use this section as needed. Sample Notes: During forensic analysis of subject John Doe's hard drive image on credit card fraud, a email message revealed that Jane Doe asks John Doe for payment on credit card printing machine.

Analysis Results

Analysis Results	Comments/Notes/Messages
Analysis Result List is a list of meaningful data that answers the who, what, when, where and how questions in satisfying the forensic request. Sample Analysis Results: 1. \Windows\$NtUninstallKB887472$\10.dat \data\sentbox.dbx\message5.eml \Special Tools\stegano.exe Modified and emailed img to ... 1/4/03 → 1/5/03	Use this section as needed Sample Notes: 1. 10.dat, message5.eml and stegano.exe show that John Doe used steganography tool to hides a ten dollar image in 10.dat at 11:03 PM 01/05/03 and emailed it to Jane Doe at 11:10 PM 01/05/03.

Department of Justice (DOJ)
Computer Crime and intellectual Property Section (CCIPS)
Cybercrime Lab
http://www.cybercrime.gov
(202) 514-1026