CERIAS

the center for education and research in information assurance and security

A Multi-phased Approach to Steganography Detection

Prof. James Goldman, William Eyre, Asawaree Kulkarni

PHASE I
SIGNATURE DETECTION

PHASE II
ARTIFACT DETECTION

Phase I Process : Web Survey and Search for Steganography

❑ An attempt to determine the prevalence of the use of steganography in the wild.

❑ Conducted in conjunction with the Indiana State Police and National White Collar Crime Center.

❑ The research used signature-based detection tools to detect the possible embedding of steganography by as many as 16 information hiding tools on 1.2 million URLs.

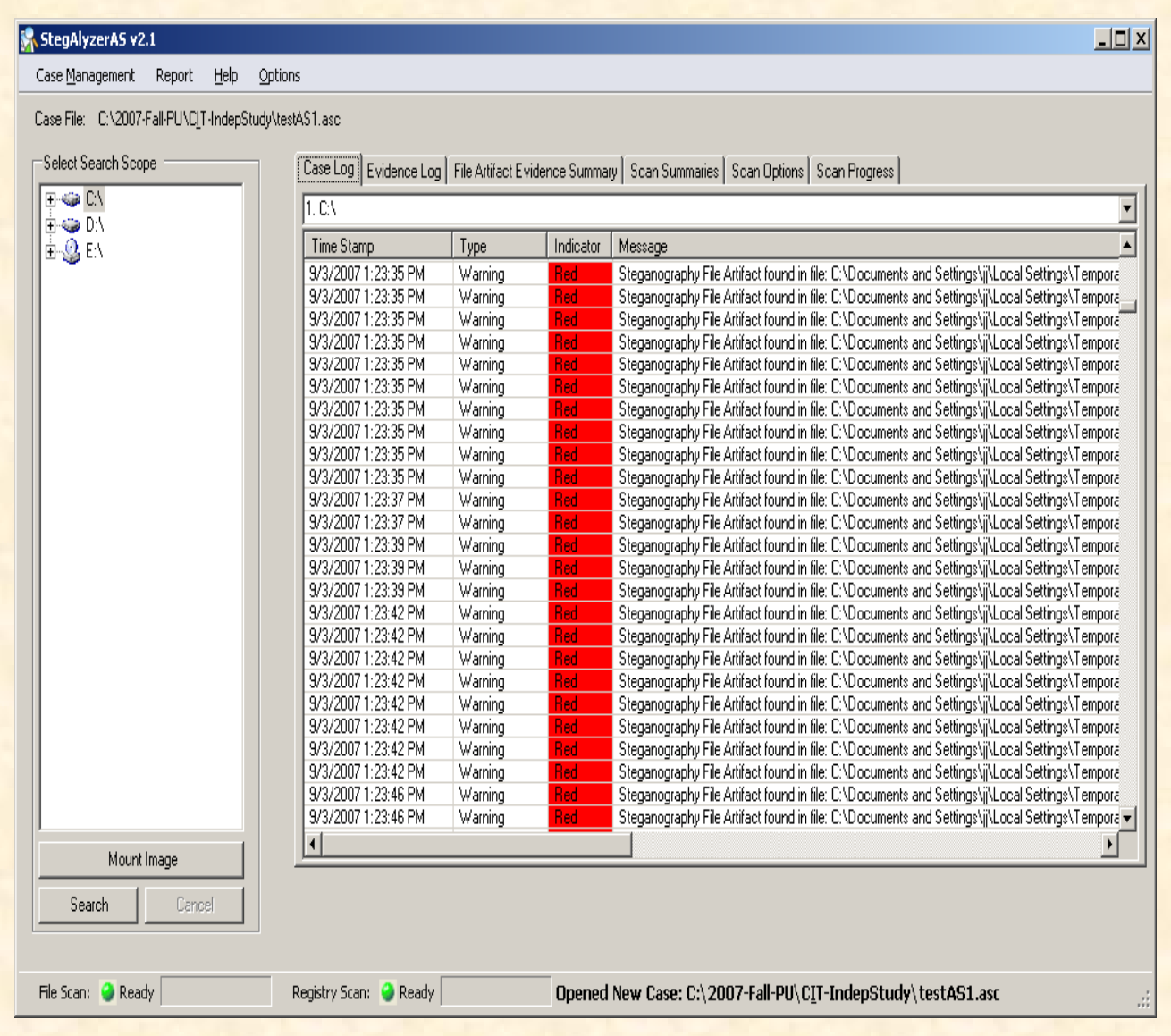
❑ Analysis of over 75,000 images looking for steganography.

Stegalyzer Tool

❑ The detection software selected for the survey was StegAlyzerSS version 1.1, named StegScan 1.1.

❑ It is signature-based.

❑ It performed well with append analysis as well as LSB analysis.



Case File: C:\2007-Fall-PU\CIT-IndepStudy\testAS1.asc

1. C:\

Time Stamp	Type	Indicator	Message
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:35 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:37 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:37 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:39 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:39 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:39 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:42 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:46 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora
9/3/2007 1:23:46 PM	Warning	Red	Steganography File Artifact found in file: C:\Documents and Settings\jj\Local Settings\Tempora

File Scan: Ready

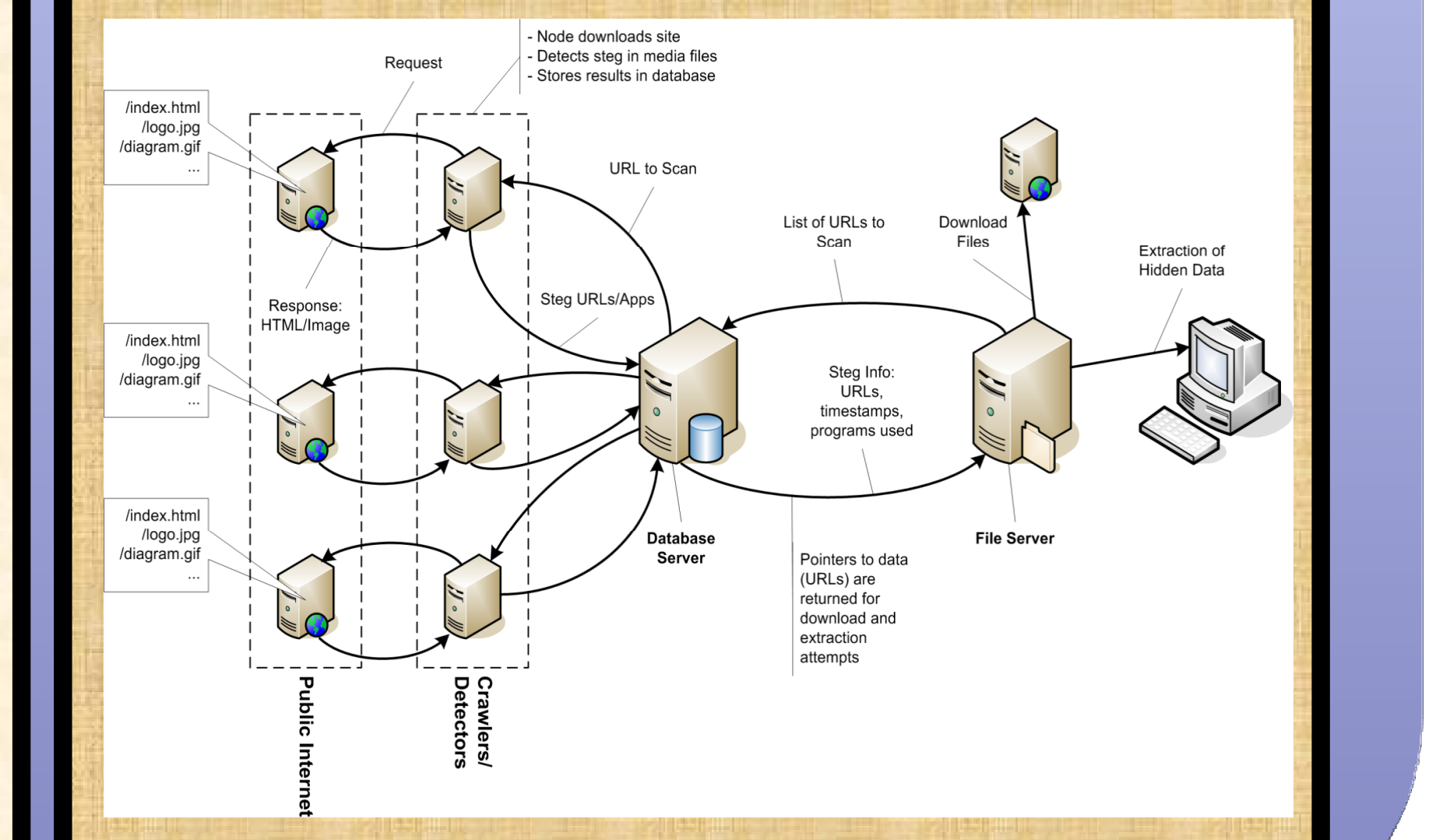
Registry Scan: Ready

Opened New Case: C:\2007-Fall-PU\CIT-IndepStudy\testAS1.asc

Web Crawler System Architecture

❑ The survey was conducted by crawling selected base URLs recursively until there were no more links in the domain of the base URL to visit.

❑ One database server was always on line. This data base server was the supervisor and passed each next URL to the crawling nodes.



Phase I Results

The phase I survey did not find any evidence that steganography is being used on the Web. There are several possible reasons for this:

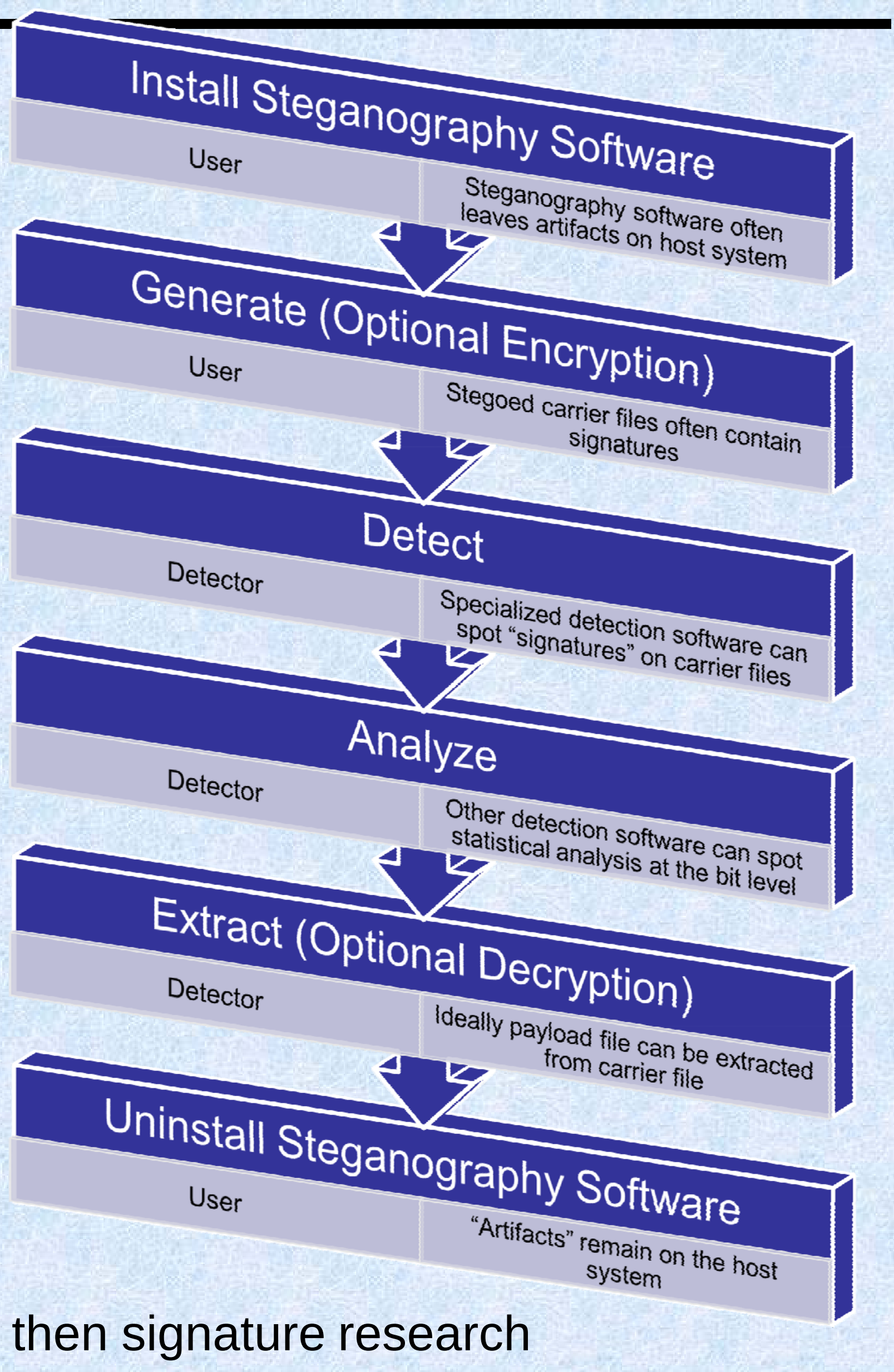
❑ There is no steganography in images on the Web.
❑ The sample size was too small .
❑ There was steganography; however it was not hidden in the file formats that the detection software was able to detect against.
❑ There was steganography in the surveyed images; however it was not hidden using the algorithms that the detection software knew the signatures of.

The Stego Method

❑ The failure to detect steganography in the wild led to the development of the model of The Stego Method and a change in focus for future directions in the steganographic research.

❑ The next step is to concentrate on the detection of host system artifacts (artifacts left by the installation and use of the steganography applications) on the machines of criminals and terrorists. Over 100 suspect machines have been scanned to date.

❑ When it has been determined what applications are popular among those detected, then signature research can be concentrated on the most commonly used applications' signatures.


Install Steganography Software
User
Steganography software often leaves artifacts on host system

Generate (Optional Encryption)
User
Stegoed carrier files often contain signatures

Detect
Detector
Specialized detection software can spot "signatures" on carrier files

Analyze
Detector
Other detection software can spot statistical analysis at the bit level

Extract (Optional Decryption)
Detector
Ideally payload file can be extracted from carrier file

Uninstall Steganography Software
User
"Artifacts" remain on the host system

PURDUE UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center