LAW ENFORCEMENT TOOLS AND TECHNOLOGIES

FOR

INVESTIGATING CYBER ATTACKS

GAP ANALYSIS REPORT

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES

February 2004

Technical Analysis Group
45 Lyme Road
Hanover, NH 03755
(603) 646-0700
www.ists.dartmouth.edu

LAW ENFORCEMENT TOOLS AND TECHNOLOGIES

FOR

INVESTIGATING CYBER ATTACKS

GAP ANALYSIS REPORT

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES

February 2004

Technical Analysis Group
45 Lyme Road
Hanover, NH 03755
(603) 646-0700
www.ists.dartmouth.edu

Executive Summary

The investigation of cyber attacks requires specialized tools, techniques, and training. This document provides an analysis of the gaps that exist between the needs of cyber attack investigators and the tools that are currently available in the marketplace. The second of three sequential studies, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report* provides an overview of critical areas where scientific research may be initiated to address the needs outlined in the Institute for Security Technology Studies report *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment*. The final report in this series, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Research and Development Agenda*, provides analysis of all three studies and a prioritized list of law enforcement needs that may be addressed by research and development. The three reports in this series provide law enforcement, researchers, and funding agencies with a body of current information regarding the unique challenges encountered by cyber attack investigators and priority needs requiring research.

The findings of the *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report* are as follows:

- All of the needs discovered in the *National Needs Assessment* (Appendix A) are important to the investigation of cyber attacks. Participants in the Prioritization Working Group agreed that providing solutions to any of the needs detailed in the *National Needs Assessment* would have a significant positive effect on the cyber attack investigative community.

- The needs of cyber attack investigators have not been met by the available technology solutions. Additionally, over the year since the *National Needs Assessment* was conducted, the tool development marketplace has not addressed the impediments facing cyber attack investigators.

- Most tools that we discovered are already employed in investigations in the community as a whole. Investigators and prosecutors who are using the technology solutions presented in this research (Appendix B) are using most, if not all, of the solutions that are commonly available.

- The specific needs of the cyber attack investigative community will continue to evolve as the types of cyber attacks change over time and new solutions are developed. This study, the *Gap Analysis Report,* provides a snapshot in time of investigators' needs and the technologies available for their use. The cyber attack investigative community may benefit from additional studies over time to capture their evolving needs.

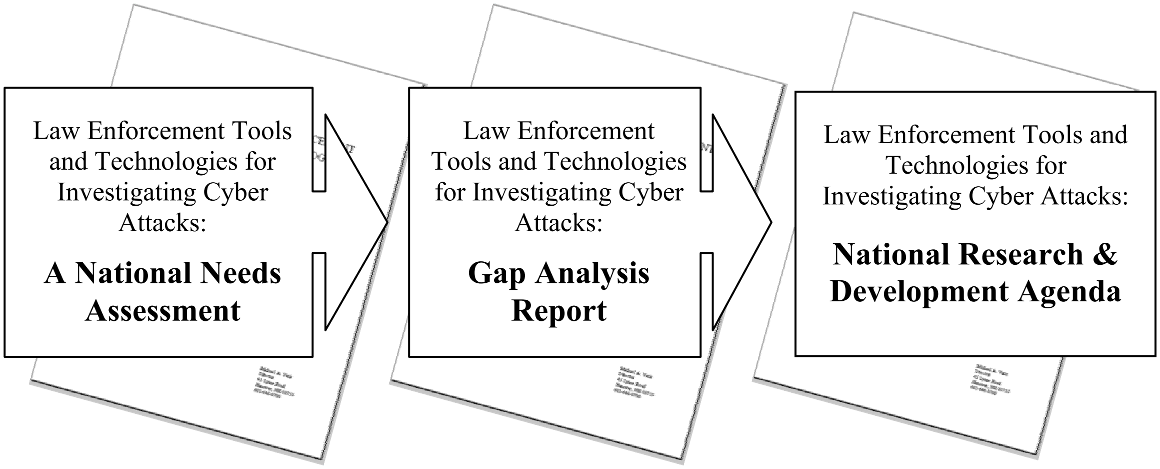
- The members of the Prioritization Working Group reached a consensus that eighteen distinct needs (Appendix D) were the most critical needs requiring additional research and development.

The *Research and Development Agenda*, to be published by ISTS in 2004, presents these critical needs, with background information, analysis and recommendations for further research and development. The challenge now lies with funding agencies, research organizations, academia and the private sector to address law enforcement's problems by contributing high-value, high-return research in this critical area.

Contents

Introduction

Filling a need for research to identify and prioritize law enforcement needs, the Institute for Security Technology Studies (ISTS) conducted three national studies concerning cyber attack investigations.[1] This paper, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report*, is the second report in this three-part, multi-year research effort. The first study, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment* is the result of a comprehensive examination of the technological impediments law enforcement encounters during cyber attack investigations.[2] The ultimate goal, realized in the third and final report *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Research and Development Agenda*, is a guidebook for developing technologies for cyber attack investigators.


Law Enforcement Tools and Technologies for Investigating Cyber Attacks:
A National Needs Assessment
Law Enforcement Tools and Technologies for Investigating Cyber Attacks:
Gap Analysis Report
Law Enforcement Tools and Technologies for Investigating Cyber Attacks:
National Research & Development Agenda

[1] This study uses the term cyber attack to refer to computer attacks that can undermine the confidentiality, integrity, or availability of a computer or information resident on it. Cyber attacks can be much more than simply website defacements. They may also be overt or covert attacks on our critical infrastructure systems. Further, cyber attacks may be perpetrated by organized crime, generally for financial gain, or possibly by hostile nations, as a form of asymmetric warfare.

[2] Available from the ISTS web site <http://www.ists.dartmouth.edu/TAG/lena.htm>.

Nature of the Problem

Ongoing cyber attacks affecting corporate, government, academic, and critical infrastructure networks are a significant law enforcement concern. Criminals routinely cross legal and ethical boundaries in the use of technology in their activities. These same criminals are often shielded from investigation or prosecution by the borderless nature of cyber attacks. Cyber attackers enjoy the ability to tap into tens of thousands of attack tools freely available on the Internet; conversely, law enforcement investigators have to prove that a particular solution did not disturb data collected for evidence. In a commercial software market flush with security products, the development of investigative solutions for law enforcement has been limited. These factors have created a situation where the tools employed by law enforcement for investigating cyber attacks are not keeping pace with the technologies employed by attackers.

Object of this Study

The *Gap Analysis Report's* authors set out to answer the following research question:

> ***What gaps exist, if any, between the needs discovered in the National Needs Assessment and tools and technologies generally available to law enforcement?***

Specifically, this document focuses on the collection, categorization, and solicitation of feedback on the available solutions to address the needs of the cyber attack investigative community.

Structure of the Report

This report begins with a brief overview of the *National Needs Assessment* and its use as a foundation for the source of the "needs" referenced throughout this report; a listing of these needs is provided for reference in Appendix A. This paper then details the research conducted to produce the *Gap Analysis Report* including; a literature review, project outreach, and cyber attack investigative tool collection efforts.

ISTS researchers developed the Gap Analysis Matrix for this study to better understand the areas where additional research and development may be required. The Gap Analysis Matrix is a graphical representation of the needs gleaned from the *National Needs Assessment* mapped against the corresponding technology solutions that purport to address those needs. The Gap Analysis Matrix is the primary deliverable of the *Gap Analysis Report* and is included as Appendix B.

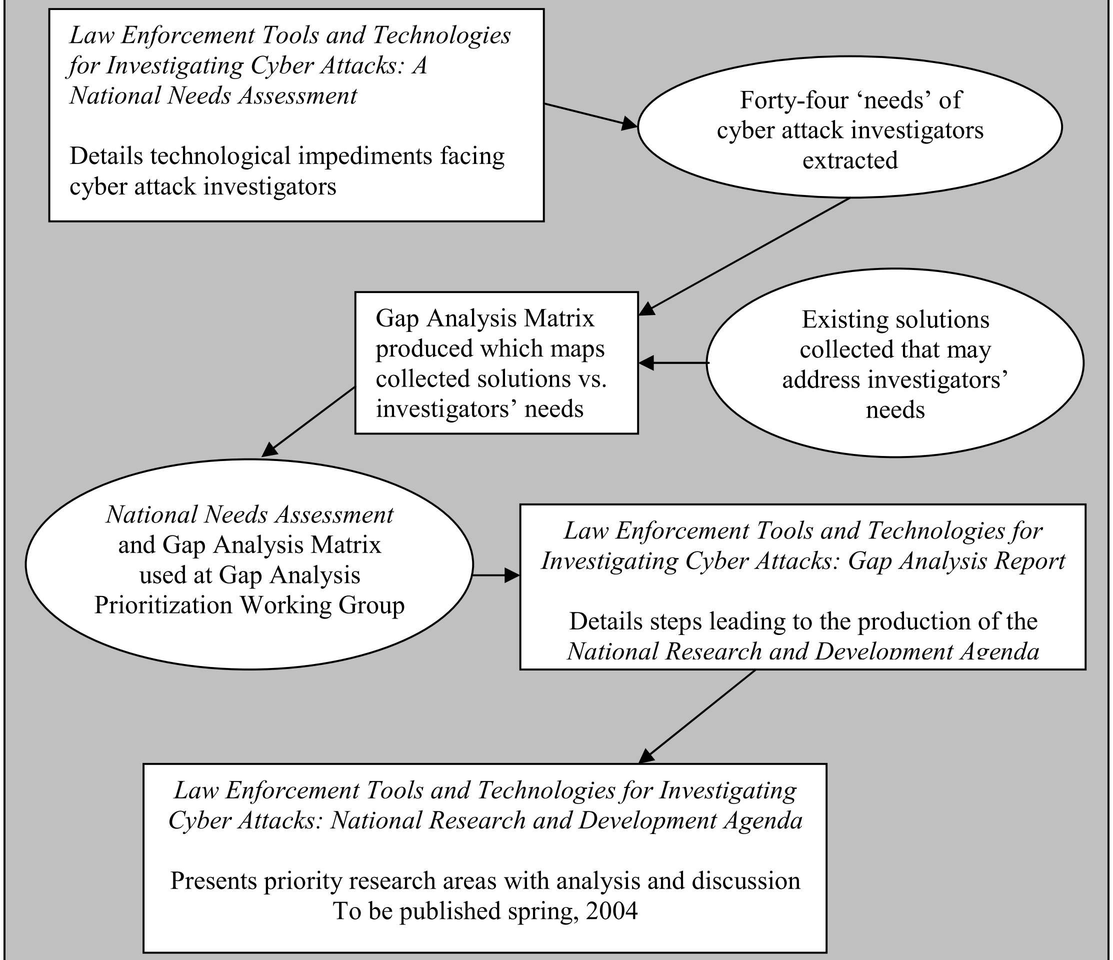
A workshop of cyber attack investigators was held near the completion of the research for the *Gap Analysis Report* to determine which needs were still research and development priorities, in light of the collected solutions. Preliminary results of validated and prioritized needs are presented in Appendix C – Gap Analysis Prioritization Working Group Data and Analysis.

An overview of the *Research and Development Agenda*, to be published in 2004, follows the summary of the *Gap Analysis Report*. The *Research and Development Agenda* contains the final recommendations for areas of priority research and development in cyber attack investigative technologies. A list of the priority research needs resulting from the Prioritization Working Group is included as Appendix D. Figure 1 shows the process to create the *Research and Development Agenda*.

Finally, this document presents conclusions derived from the *Gap Analysis Report.*

Figure 1. Description of the *Research and Development Agenda* creation process.

Documents or products are shown in squares; assessments are shown in ovals


Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment
Details technological impediments facing cyber attack investigators
Forty-four 'needs' of cyber attack investigators extracted
Gap Analysis Matrix produced which maps collected solutions vs. investigators' needs
Existing solutions collected that may address investigators' needs
National Needs Assessment and Gap Analysis Matrix used at Gap Analysis Prioritization Working Group
Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report
Details steps leading to the production of the National Research and Development Agenda
Law Enforcement Tools and Technologies for Investigating Cyber Attacks: National Research and Development Agenda
Presents priority research areas with analysis and discussion
To be published spring, 2004

National Needs Assessment Overview

The *National Needs Assessment* was generated following a comprehensive survey of cyber attack investigators at the federal, state and local levels. The *National Needs Assessment* was conducted to address the following question:

> ***What are the technological impediments facing law enforcement when investigating and responding to cyber attacks, for which research and development might provide solutions?***

The creation of the *National Needs Assessment* document followed a five stage process:

Stage 1. Literature Review and Survey Development – During the formative stage of the study, ISTS researchers conducted a literature review to identify relevant studies and reports and we found no other similar current research. ISTS staff and an independent statistician designed the survey mechanism in close consultation with experienced current and former cyber-attack investigators. The RAND Survey Research Group reviewed, edited and pilot-tested the survey with cyber attack investigators across the country

Stage 2. National Survey – Primary data was collected through a web-based survey of federal, state and local law enforcement, conducted under ISTS auspices by RAND over four months. Out of the 311 individuals validated to participate in the survey, 151 investigators completed the survey; a response rate of 48.5%. On average, respondents investigated 15 cyber-attack cases in the last three years. A majority of the population had one to four years of cyber-attack investigative experience. An additional 25% had five or more years of experience, while 23% had less than one year of experience. On average, 50% of respondents indicated they were in a supervisory role. Almost all survey participants (93%) received training for cyber-attack investigations.

Stage 3. Law Enforcement Interviews – ISTS researchers visited twelve law enforcement agencies in seven states and the District of Columbia to conduct in-depth interviews with cyber-attack investigators. One additional set of interviews was conducted via telephone. In total, ISTS staff interviewed thirty-nine investigators and prosecutors during this stage of the study.

Stage 4. Workshop – During a two-day workshop, ISTS and RAND presented the data collected from the survey to a select group of twenty-three present and former cyber-attack investigators and prosecutors for validation, and to collect further data for analysis and prioritization.

Stage 5. Final Report Production – ISTS staff created the final report by synthesizing and analyzing the data collected in Stages 2 through 4. A draft copy of the report was made available to a broad array of law enforcement and industry cyber-attack experts for review and comment. We reviewed and integrated the feedback into the final version of the study.

ISTS published the final report in June of 2002, and disseminated it widely through both hardcopy and downloadable versions. The findings resulting from the *National Needs Assessment* showed that the unique needs of law enforcement cyber attack investigators could be represented through seven categories relating to either the stage of an investigation or a special requirement:

1. Preliminary Investigation and Data Collection
2. Log Analysis
3. IP Tracing and Real-time Interception
4. Emerging Technologies
5. National Data and Information Sharing
6. Law-enforcement-specific Development Issues
7. Training

The *National Needs Assessment* showed disparities between the technology solutions used by law enforcement and their expressed requirements. Law enforcement officials surveyed clearly indicated that they do not have adequate solutions to the technological problems encountered during cyber attack cases. ISTS researchers viewed these conclusions as the perception of the study participants until an objective analysis of existing tools and technologies was conducted.

Gap Analysis Overview

Following the release of *National Needs Assessment*, ISTS staff work began on the *Gap Analysis Report*. The primary goal of this project was to identify solutions that may address the impediments discovered in the *National Needs Assessment* and produce a guide for interpreting the results. Forty-four distinct needs were distilled from the five technology-related categories[3] found in the *National Needs Assessment*. We collected over 200 existing and in-development solutions, from all sources, that could potentially address these needs after an extensive outreach effort. We then mapped these collected tools against the needs, based solely on manufacturers' claims, to determine where 'gaps' in product availability may exist. This mapping took the form of the *Gap Analysis Report's* primary deliverable, the Gap Analysis Matrix, found in Appendix B.

[3] For the *Gap Analysis Report*, only the first five Categories from the *National Needs Assessment* were used. It was determined that the information relating to Law-Enforcement-Specific Development Issues and Training was primarily focused on future tool development issues and proper training and that these focus areas were not appropriate for the *Gap Analysis Report*'s goal of examining how existing technology solutions could be used to solve investigators' existing and future needs. No attempt was made during the *Gap Analysis Report* to diverge from or expand on the foundation of the *National Needs Assessment*.

ISTS researchers then convened a working group of leaders in the field of cyber attack investigations to examine the collective data from the *National Needs Assessment* and the *Gap Analysis Report*. The group was asked to determine which needs from the *National Needs Assessment* were not satisfied by existing solutions and still required research and development. The participants then prioritized the unsatisfied needs to begin framing the *Research and Development Agenda*.

Data for the this study was collected from federal, state, and local law enforcement organizations in the United States, sponsored research entities, academia, and the private sector. The research and tool collection targeted supervisory and operational law enforcement practitioners in investigative, forensic, prosecutorial, and training capacities, and tool developers in the commercial, government, academic and open source communities.

Gap Analysis Literature Review

The Technical Analysis Group conducted a preliminary literature review for the *Gap Analysis Report* over seven weeks, from September to November of 2002, to discover if similar efforts had been conducted. Over 175 relevant documents including reports, papers, presentations, and articles were reviewed. More than 350 websites were explored, including: research institutes and centers similar to ISTS; government agencies; think tanks; information technology professional associations and journals; law enforcement agencies, associations and journals; security and incident response consultants; and computer software vendors. We examined several organizations and individuals for related research:

- Universities and institutes resembling ISTS in mission and focus including Carnegie-Mellon University, George Mason University, James Madison University, the Naval Postgraduate School, Purdue, the University of Texas at San Antonio, and the University of Tulsa.
- Federal and national agencies and offices responsible for infrastructure protection, law enforcement and standards development including; the Computer Emergency Response Team / Coordinating Center (CERT/CC), the Department of Energy's Computer Incident Advisory Capability, the Federal Bureau of Investigation (FBI) and its attendant divisions, the National Infrastructure Protection Center, the National Institute of Justice (NIJ), the Office of Justice Programs, and the National Institute of Standards and Technology (NIST).
- Think tanks and computer security consulting firms including @Stake, BoozAllen, Counterpane, Gartner, MITRE, RAND, Symantec Enterprises, and Wetstone.
- Open source news/information including LexisNexis, EBSCOhost, PR Newswire, US Newswire, University Wire, the Overseas Security Advisory Council's Cyber Library & Cyber News, WebSPIRS Criminal Justice Abstract Database, a basic "Google" web search, and several law

enforcement, computer security, and criminal justice-oriented journals and news sites, and returned no applicable results for various combinations of "law enforcement", "research", "computer or cyber crime", and "tools".

In addition to the ISTS *National Needs Assessment*, several other needs assessments have been completed, and were used as supporting information for the *Gap Analysis Report*: RAND's *Needs and Prospects for Crime-Fighting Technology*, 1999; NIJ's *Electronic Crime Needs Assessment for State and Local Law Enforcement*, 2001; and RAND's *Challenges and Choices for Crime-Fighting Technology: Federal Support of State and Local Law Enforcement*, 2001. These reports focus on the technological tools needed to fight crime, and the impediments to fighting cyber crime in particular.

Interpol's European Working Party on Information Technology Crime (EWPITC) provided law enforcement "with an in-depth overview of the tools and techniques utilized for the investigation of Information Technology Crime and to provide an extensive list of these and the value of their application," as a year 2000 project.[4] When the literature review was conducted, results were not available. Currently, the project website states that the report is complete and posted on a law enforcement only restricted website.

ISTS researchers compiled a list of thirty-nine leaders in the field of cyber attack investigations and made personal contact with twenty of these experts. The list included a cross section of those involved with cyber attack investigations and tool development from government, academia and the private sector. Collectively they expressed no knowledge of ongoing research similar to the ISTS *Gap Analysis Report*. The experts also provided suggestions regarding specific tools and technologies, additional contacts, and other sources of information on computer investigations and forensic analysis. As a result of the literature review, it was determined that no other ongoing research similar to the *Gap Analysis Report* was either completed or in progress.

Gap Analysis Outreach and Tool Collection

ISTS researchers conducted a national outreach effort to communicate the mission and scope of the project to the members of the cyber attack investigative community who may be responsible for technology solution development and/or indexing. Those contacted were asked to provide information regarding technology solution(s) at a primary collection point created on the ISTS web site.[5] This collection point allowed for developers and publishers of tools to submit their solution and define the capabilities of the tools against the needs discovered in the *National Needs Assessment.* These outreach efforts were conducted over January-February 2003 and included:

[4] Additional information available online at <http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa>.

[5] <http://www.ists.dartmouth.edu/TAG/subtool/register.htm>.

- Submission or posting to ten listservs relating to computer crime.
- Emails sent to thirty companies focused on computer forensics.
- Emails sent to forty Universities and Colleges involved with cyber attack, computer forensic or computer security programs of study.
- Emails sent to ten government-owned or sponsored research agencies.
- Emails sent to ten open-source tool producers and tool indexing sites.
- Emails sent to 1700 unique contacts in the database we generated for the *National Needs Assessment* project.

In addition to the web-based tool collection point, we worked in conjunction with the NIJ's Electronic Crime Partnership Initiative (ECPI) and NIJ sponsored Cyber Science Laboratory (CSL) in the collection of applicable solutions.[6] The ECPI's Tool and Technology Working Group compiled an index of forensic tools: The ECPI Tool Catalog. We used this catalog to supplement the tool collection efforts; it contains the manufacturers' summaries of tool functions.

The research effort collected over 200 unique tools. ISTS researchers compiled the collected solutions into a matrix, the Gap Analysis Matrix (Appendix B), that cross-references existing tools and their specific features with the forty-four needs discovered in the *National Needs Assessment*. We included, where possible, tools and technologies under development or not yet in widespread use. Many of the tools examined did not have a role in a cyber attack investigation, and therefore did not address any of the needs from the *National Needs Assessment;* these tools were not included on the Gap Analysis Matrix.

Gap Analysis Prioritization Working Group

Representatives from federal, state and local law enforcement joined with members of the academic and the government-sponsored research communities at the Law Enforcement Cyber Attack Technology Gap Analysis Prioritization Working Group in July of 2003. Twenty-two investigators from a broad spectrum of the cyber attack investigative community were present at the Prioritization Working Group, including representation from The Agora, Central Intelligence Agency, Cyber Science Laboratory, Federal Bureau of Investigation, Florida Department of Law Enforcement, NASA Office of Inspector General, National Law Enforcement and Corrections Training Center – North East, National White Collar Crime Center, New Hampshire Attorney General's Office, New York Police Department, San Diego Supercomputer Center, South Carolina Law Enforcement Division, U.S. Department of Justice, United States Secret Service, and the University of New Haven.

[6] Additional information on the ECPI can be found by contacting Cyber Science Laboratory, Fred Demma, 26 Electronic Parkway, Rome, New York 13441; 888.338.0584; <http://www.cybersciencelab.com>.

The Prioritization Working Group had three main goals:

1. To determine if the Gap Analysis Matrix presented an accurate list of currently available technology solutions to address the needs discovered in the *National Needs Assessment*.
2. To determine if the needs were adequately addressed by the currently available technology solutions represented on the Gap Analysis Matrix.
3. To prioritize the needs not adequately addressed by currently available technology solutions for the *Research and Development Agenda*.

ISTS staff used a highly structured format for the work group session. Participants reviewed copies of the *National Needs Assessment* as well as the Gap Analysis Matrix. The Gap Analysis Matrix provided participants with a picture of the available solutions for the needs being discussed. Each of the five technology-related categories, their corresponding needs from the *National Needs Assessment*, and background information and analysis were presented to the group. The comments and prioritization efforts of the participants were captured through the use of decision support software. This collaboration-enhancing software[7] allows for anonymous and non-attributable commenting, voting, ranking and prioritization work to be performed in a real-time environment.

For each of the five categories, we posed three questions regarding each of the needs to the participants to elicit their comments:

1. Are you aware of any additional solutions that meet the needs described in this category? If yes, enter the name of the solution(s).
2. What needs in this category do you feel are not met by the available solution(s)? Please add your justification for each need.

After comments were entered for the second question, we asked participants to mark those needs that should be moved forward for additional consideration. Specifically they were asked:

3. Which needs in this category require further research and development?

Each participant was allowed to mark as few or as many needs as they saw appropriate. Following the fifth and final category, all of the needs that had received at least one vote in the polling for question three were combined for final ranking and prioritization. While the participants were initially asked to evaluate the needs based on whether each required additional research and development—considering the existing tools and the quickly changing field—they now needed to consider which of the presented needs were more critical than others.

[7] GroupSystems software was used during the working group <http://www.groupsystems.com/>

The complete discussion and analysis of each of the five technology-related categories, including materials from the *National Needs Assessment*, Gap Analysis Matrix and the Prioritization Working Group is presented in Appendix C – Gap Analysis Prioritization Working Group Data and Analysis. Each section within the appendix reviews the origin of the category in the *National Needs Assessment*, explores the mapping of each category's needs versus tools in the Gap Analysis Matrix, and discusses the comments resulting from the Prioritization Working Group.

ISTS researchers asked the Prioritization Working Group participants to perform a number of ranking and resource allocation exercises, and, after viewing and discussing the results, the participants agreed on separating the needs into roughly two bands—most critical and less critical. Through this process the participants reached a consensus that eighteen of the forty-four needs are the most critical needs requiring additional research and development. The preliminary results of these prioritization efforts are presented in Appendix D - Preliminary Prioritization Findings. This band of eighteen critical needs forms the foundation of the topics discussed in the *Research and Development Agenda.*

National Research and Development Agenda Overview

The *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Research and Development Agenda*, to be published by the ISTS in 2004, will present the combined results of the *National Needs Assessment* and *Gap Analysis Report* projects. The *National Needs Assessment* uncovered and clarified the needs of the cyber attack investigative community; the *Gap Analysis Report* determined if existing solutions could potentially address the current needs. The results of both studies were examined and discussed at the Prioritization Working Group and by ISTS researchers to become the basis for the prioritization, analysis, and recommendations provided in the *Research and Development Agenda*.

Conclusion

Throughout the course of the research for the *Gap Analysis Report,* several important conclusions became apparent:

- All of the needs discovered in the *National Needs Assessment* (Appendix A) are important to the investigation of cyber attacks. Participants in the Prioritization Working Group agreed that providing solutions to any of the needs detailed in the *National Needs Assessment* would have a significant positive effect on the cyber attack investigative community.
- The needs of cyber attack investigators have not been met by the available technology solutions. Additionally, over the year since the *National Needs Assessment* was conducted, the tool development marketplace has not addressed the impediments facing cyber attack investigators.
- Most of the tools that we discovered are already employed in investigations in the community as a whole. Investigators and prosecutors who are using the technology solutions presented in this research (Appendix B) are using most, if not all of the solutions that are commonly available.
- The specific needs of the cyber attack investigative community will continue to evolve as the types of cyber attacks change over time and new solutions are developed. This study, the *Gap Analysis Report,* provides a snapshot in time of investigators' needs and the technologies available for their use. The cyber attack investigative community may benefit from additional studies over time to capture their evolving needs.
- The members of the Prioritization Working Group reached a consensus that eighteen distinct needs (Appendix D) were the most critical needs requiring additional research and development.

The *Research and Development Agenda* presents these critical needs, with background information, analysis and recommendations for further research and development. The challenge now lies with funding agencies, research organizations, academia and the private sector to address law enforcement's problems by contributing high-value, high-return research in this critical area. It is imperative that law enforcement at all levels is empowered by technology in the investigation and prosecution of cyber attacks.

Appendices

Appendix A – National Needs Assessment List of Needs

ISTS researchers examined the data and analyses from the *National Needs Assessment* in the five main technology-related categories to determine the exact, particular needs of cyber attack investigators. These user-defined needs became the points by which existing tools and technologies were be categorized. Below is a presentation of the needs, sorted by category and identifying number. The category relates to the phase of a cyber attack investigation, discussed in the *National Needs Assessment*. The identifying number serves to tie the need to the category, and reflects only the approximate order in which these items were addressed in the *National Needs Assessment,* and not their order of importance. Please refer to the *National Needs Assessment* for clarification on the concepts discussed here.

1. Preliminary Investigation and Data Collection

    1.1. Automates the collection of data from multiple operating systems to learn how a network was compromised.

    1.2. Identifies system configurations.

    1.3. Reports system configurations.

    1.4. Identifies file locations.

    1.5. Reports file locations.

    1.6. Discovers a system's role on a network.

    1.7. Reports a system's role on a network.

    1.8. Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses.

    1.9. Graphically represents network mapping results to better understand the complex relationships in the victim's network.

    1.10. Enables investigators to independently discover the topology of the network.

    1.11. Enables investigators to independently verify the topology of the network.

    1.12. Alleviates investigator's dependence on in-house staff at victim's location.

    1.13. Captures Random Access Memory (RAM) data without modification/alteration/addition.

    1.14. Captures Swap file data without modification/alteration/addition.

    1.15. Designed to process very large data sets.

2. Log Analysis

    2.1. Searches a network for logs.

    2.2. Recognizes and collects logs regardless of platform.

2.3. Recognizes and collects logs regardless of format.

2.4. Prepares logs for export to different operating system or analysis environment.

2.5. Searches for fragmentary information to reconstruct logs.

2.6. Automatically captures the individual time and date settings from compromised network computers.

2.7. Translates log files from multiple time zones to a common time frame.

2.8. Organizes data into a graphical timeline.

2.9. Provides consistent timeline and reports / graphs discrepancies in time correlations.

2.10. Creates data sets optimized for analysis, portability, and interoperability.

2.11. Contains easy-to-use search functions.

2.12. Contains analytic tools that autonomously uncover anomalies in large log files.

2.13. Presents detailed technical information in a graphical format.

2.14. Serves as a tool for prosecutors to present complex cyber attack data in the courtroom.

3. IP Tracing and Real Time Interception

3.1. Facilitates and coordinates cross-jurisdictional communications.

3.2. Provides added capability to trace and/or counter IP spoofing.

3.3. Provides added capability to detect IP spoofing.

3.4. Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception.

4. Emerging Technologies

4.1. Increases law enforcement’s ability to circumvent the obstacle of encrypted data.

4.2. Flags digital files that may contain steganographic messages.

4.3. Provides magnetic microscopy technology for law enforcement applications.

4.4. A solution(s) to securely store very large data sets that addresses data degradation and financial concerns of the law enforcement community.

5. National Data and Information Sharing

5.1. Serves as a database for collecting attack profiles in concert with a solution for performing technical exploit matching to enable law enforcement to identify attack patterns.

5.2. Serves as a database for cyber attacks that allows law enforcement agencies to quickly assess if their case is a component of larger criminal activity.

5.3. Automates analysis of logs for the presence of a virus or worm signature, specifically designed for cyber attack cases.

5.4. A resource to store and compare new virus code to existing examples.

5.5. Applies pattern recognition software to determine the origin and author of a virus or worm.

5.6. Serves as a database of Trojans, root kits, and other attack tools that is continually updated that provides investigators with relevant and timely analysis capability.

5.7. Serves as a data warehouse of legacy software and hardware for agencies responsible for cyber attack and cyber crime.

Appendix B – Gap Analysis Matrix

The Gap Analysis Matrix is the primary deliverable of the *Gap Analysis Report*. The needs of the cyber attack investigative community were distilled from the *National Needs Assessment*. The Gap Analysis Matrix maps these needs against the tools that are currently available to, and in use by, the cyber attack investigative community to show where 'gaps' in product availability may exist. A panel of cyber attack investigators used the Gap Analysis Matrix as a reference tool during the Gap Analysis Prioritization Working Group in determining if existing needs were met by existing solutions.

The Gap Analysis Matrix is spread across seven pages, broken down by the categories derived from the general stage of an investigation, detailed in the *National Needs Assessment*. Appendix B Pages 2 and 3 show the tools that address Category 1 – Preliminary Investigation and Data Collection. Category 2, Log Analysis, is spread across Appendix B Pages 4 through 7. Appendix B Pages 6 and 7 also show Categories 3 and 4, IP Tracing and Real Time Interception and Emerging Technologies Requiring Research and Development, respectively. Lastly, Appendix B Page 8 contains the tools and needs for Category 5, National Data and Information Sharing.

The Gap Analysis Matrix is organized with the needs shown across the columns and the tools that address those needs are shown in rows. If a tool that was examined had no relevance to any needs on a section of the Gap Analysis Matrix, the tool was not listed. Each distinct need distilled from the *National Needs Assessment* is shown in the column headings with its corresponding need number. The need number is consistent throughout this document and the integer refers to the category in which the need resides. For each need in a column, bold "X" marks have been placed in the rows of the tools which purport to address the particular need. The marks have been placed according to the claims of the manufacturer, per their product literature, website, or claims made on the ISTS Submit a Tool website.

To use the Gap Analysis Matrix, find the need that interests you and follow the column down to view the tools that purport to address the stated need. The Gap Analysis Matrix is color-coded as a general guide, with red indicating that very few to no tools (six or less) are mapped against a need and green indicating that there are many tools to address a need (more than twelve). Yellow is given to those needs that have a several tools mapped (between six and twelve tools).

	1. Preliminary Investigation and Data Collection														
	Operating systems							Network mapping		Digital evidence recovery			Memory resident tools		Very large data sets
Needs	Automates the collection of data from multiple operating systems to learn how a network was compromised.	Identifies system configurations.	Reports system configurations.	Identifies file locations.	Reports file locations.	Discovers a system's role on a network.	Reports a system's role on a network.	Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses.	Graphically represents network mapping results to better understand the complex relationships in the victim's network.	Enables investigators to independently discover the topology of the network.	Enables investigators to independently verify the topology of the network.	Alleviates investigator's dependence on in-house staff at victim's location.	Captures RAM data without modification/alteration/addition.	Captures Swap file data without modification/alteration/addition.	Designed to process very large data sets.
TOOL NAME	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11	1.12	1.13	1.14	1.15
NetWitness	X											X			X
ProDiscover DFT V2	X	X	X	X	X	X	X							X	X
PATHFINDER	X	X													X
SilentRunner									X			X			X
Byte Back III	X	X										X			X
Detective												X			
White Glove	X	X						X	X			X			X
Log Management Sys.															X
Shadow	X														
i2 Analysts Notebook/iBase															X
EagleCheck	X	X						X				X			
Autopsy Forensic Browser	X	X	X	X	X							X			X
CD / DVD Inspector	X	X		X	X							X			
Computer Cop Forensic Professional	X			X	X							X			X
DataLifter	X	X	X	X	X							X			
DRAC	X														
DIBS	X														
DIBS Analyzer 2	X	X	X	X	X							X		X	X
DIBS Mycroft V3				X	X										
DRIVESPY	X			X	X							X			X
Encase V4	X	X	X	X	X			X				X		X	X
SMART	X	X	X	X	X							X			X
DMZS F.I.R.E.	X	X	X	X	X							X			X
Maresware: The Suite	X	X	X	X	X							X			X

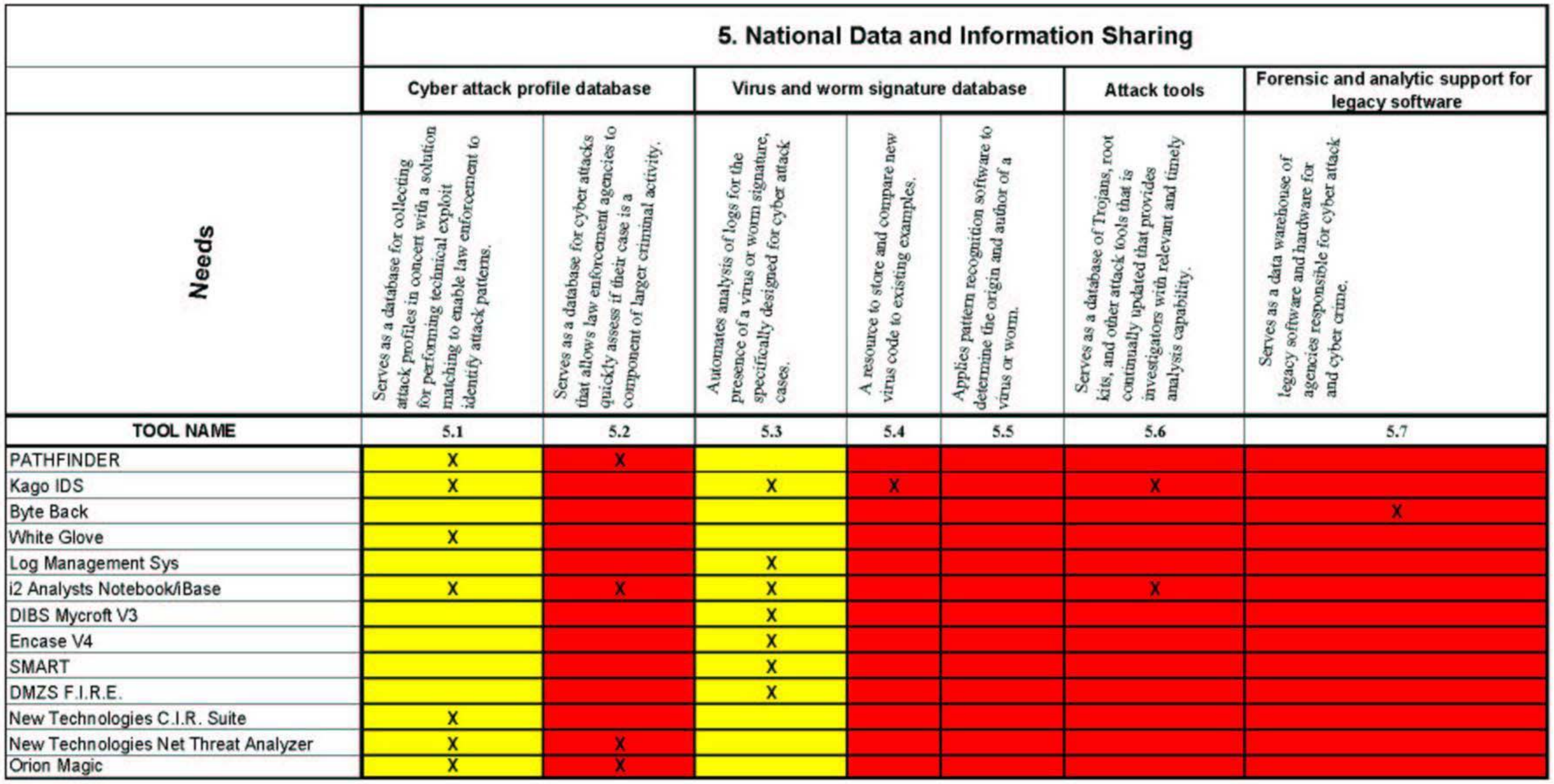
	1. Preliminary Investigation and Data Collection														
	Operating systems							Network mapping		Digital evidence recovery			Memory resident tools		Very large data sets
Needs	Automates the collection of data from multiple operating systems to learn how a network was compromised.	Identifies system configurations.	Reports system configurations.	Identifies file locations.	Reports file locations.	Discovers a system's role on a network.	Reports a system's role on a network.	Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses.	Graphically represents network mapping results to better understand the complex relationships in the victim's network.	Enables investigators to independently discover the topology of the network.	Enables investigators to independently verify the topology of the network.	Alleviates investigator's dependence on in-house staff at victim's location.	Captures RAM data without modification/alteration/addition.	Captures Swap file data without modification/alteration/addition.	Designed to process very large data sets.
TOOL NAME	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11	1.12	1.13	1.14	1.15
Norton Ghost	X														
Parben Tools	X	X	X	X	X							X			X
Win Hex	X	X	X	X	X							X			X
Evidor	X			X	X							X			X
Ilook	X	X	X	X	X							X			X
Anadisk	X			X											
Foundstone (free tools)	X	X	X	X	X							X			X
Digital Forensics, Inc. (free tools)	X	X	X	X	X							X			X
DirectorySnoop	X	X	X	X	X							X			X
LC Tech Forensic Utility Suite	X	X	X	X	X							X			X
Forensic ToolKit	X	X	X	X	X							X			X
New Technologies C.I.R. Suite	X			X	X							X		X	X
LFE				X	X										
Recover It All			X	X	X							X			
@ Stake (All Tools)	X	X	X	X	X							X			X
ACES															X
ACAT (Advanced Cataloger)				X	X										
Anasil								X	X	X	X	X			
dtSearch															X
New Technologies Net Threat Analyzer				X	X										
Orion Magic	X			X	X										X
Quick View Plus	X			X	X										
Advanced Disk Cataloger				X	X							X			
Intermapper								X	X	X	X	X			
Trinux		X	X	X	X							X			

	2. Log Analysis									
	a. Recognizes and imports logs across a network				b. Reconstructs altered or damaged logs	c. Places log data into an organized timeline				d. Organize output into a common and portable format
Needs	Searches a network for logs.	Recognizes and collects logs regardless of platform.	Recognizes and collects logs regardless of format.	Prepares logs for export to different operating system or analysis environment.	Searches for fragmentary information to reconstruct logs.	Automatically captures the individual time and date settings from compromised network computers.	Translates log files from multiple time zones to a common time frame.	Organizes data into a graphical timeline.	Provides consistent timeline and reports / graphs discrepancies in time correlations.	Creates data sets optimized for analysis, portability, and interoperability.
TOOL NAME	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10
NetWitness			X				X		X	X
The Coroners ToolKit				X	X	X		X	X	X
PATHFINDER	X	X	X			X		X		X
SilentRunner		X	X	X	X		X		X	X
Swatch	X									
Byte Back				X				X		
Detective					X		X		X	
White Glove		X		X	X		X			
Log Management Sys			X			X	X		X	X
Shadow			X						X	
i2 Analysts Notebook/iBase					X	X	X	X	X	X
Autopsy Forensic Browser		X	X	X	X	X	X	X	X	X
Computer Cop Forensic Professional					X					
DataLifter	X			X		X				X
DIBS Analyzer 2	X			X	X					X
DRIVESPY	X				X					
Encase V4	X	X	X		X	X		X		
SMART		X	X							

	2. Log Analysis									
	a. Recognizes and imports logs across a network				b. Reconstructs altered or damaged logs	c. Places log data into an organized timeline				d. Organize output into a common and portable format
Needs	Searches a network for logs.	Recognizes and collects logs regardless of platform.	Recognizes and collects logs regardless of format.	Prepares logs for export to different operating system or analysis environment.	Searches for fragmentary information to reconstruct logs.	Automatically captures the individual time and date settings from compromised network computers.	Translates log files from multiple time zones to a common time frame.	Organizes data into a graphical timeline.	Provides consistent timeline and reports / graphs discrepancies in time correlations.	Creates data sets optimized for analysis, portability, and interoperability.
TOOL NAME	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10
DMZS F.I.R.E.					X					
Maresware: The Suite					X	X				
Paraben Tools		X	X		X					
WinHex					X					
Evidor	X			X						X
Ilook		X	X	X	X					
Foundstone (free tools)										
Digital Forensics, Inc (free tools)					X					
DirectorySnoop					X					
LC Tech Forensic Utility Suite		X								
Forensic ToolKit		X	X		X					
Recover It All					X					
@ Stake (All Tools)		X	X	X	X		X	X		X
ACES					X					
Anasil										
New Technologies Net Threat Analyzer				X	X					X
Orion Magic	X							X		

	2.A. Log analysis and reporting				3. IP Tracing and Real-time Interception				4. Emerging Technologies Requiring Research and Development			
	Log file analysis		Graphical reporting		IP tracing			Real-time interception	Encryption	Stegan-ography	Magnetic microscopy	Forensic data archiving
Needs	Contains easy to use search functions.	Contains analytic tools that autonomously uncover anomalies in large log files.	Presents detailed technical information in a graphical format.	Serves as a tool for prosecutors to present complex cyber attack data in the courtroom.	Facilitates and coordinates cross-jurisdictional communications.	Provides added capability to trace and/or counter IP spoofing.	Provides added capability to detect IP spoofing.	Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception.	Increases law enforcement's ability to circumvent the obstacle of encrypted data.	Flags digital files that may contain steganographic messages.	Provides magnetic microscopy technology for law enforcement applications.	A solution(s) to securely store very large data sets that addresses data degradation and financial concerns of the law enforcement community.
TOOL NAME	2.11	2.12	2.13	2.14	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4
NetWitness	X	X	X					X		X		X
Kago IDS	X											
PATHFINDER	X		X		X			X				X
SilentRunner	X	X	X	X	X	X		X		X		
Swatch							X					
Detective	X	X										
White Glove	X	X			X	X		X				X
Log Management System	X	X										X
Shadow	X											
i2 Analysts Notebook/iBase	X		X	X	X			X				
EagleCheck					X	X		X				
Autopsy Forensic Browser	X			X								
CD / DVD Diagnostic												X
Computer Cop Forensic Professional	X											
DataLifter	X		X	X		X						
DIBS Analyzer 2			X	X								
DIBS Mycroft V3	X	X										
DRIVESPY	X											
Encase V4			X	X					X			X
SMART	X	X	X	X								
DMZS F.I.R.E.	X	X	X									
Paraben Tools	X		X	X								
WinHex	X		X	X								
Evidor	X		X	X								

	2.A. Log analysis and reporting				3. IP Tracing and Real-time Interception				4. Emerging Technologies Requiring Research and Development			
	a. Log file analysis		b. Graphical reporting		IP tracing			Real-time interception	Encryption	Stegan-ography	Magnetic microscopy	Forensic data archiving
Needs	Contains easy to use search functions.	Contains analytic tools that autonomously uncover anomalies in large log files.	Presents detailed technical information in a graphical format.	Serves as a tool for prosecutors to present complex cyber attack data in the courtroom.	Facilitates and coordinates cross-jurisdictional communications.	Provides added capability to trace and/or counter IP spoofing.	Provides added capability to detect IP spoofing.	Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception.	Increases law enforcement's ability to circumvent the obstacle of encrypted data.	Flags digital files that may contain steganographic messages.	Provides magnetic microscopy technology for law enforcement applications.	A solution(s) to securely store very large data sets that addresses data degradation and financial concerns of the law enforcement community.
TOOL NAME	2.11	2.12	2.13	2.14	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4
Ilook	X	X	X	X								
Foundstone (Free Tools)	X								X			
DirectorySnoop	X		X									
Digital Detective (free tools)	X								X			
LC Tech Forensic Utility Suite	X		X	X								
Forensic ToolKit	X		X	X								
New Technologies C.I.R. Suite	X	X	X	X								
@ Stake (All Tools)	X	X	X	X					X			
ElcomSoft Co. Ltd. (All Tools)									X			
Password Recovery Toolkit (Access Data)									X			
Pk Crack									X			
StegoWatch (Wetstone)										X		
Stegdetect										X		
ACES	X	X										
Anasil								X				
dtSearch	X											
Image Link & Suspect Presenter (Flint SW)			X	X								
MIL-CAS								X				
New Technologies Net Threat Analyzer	X	X						X				
Orion Magic	X	X	X	X								
LIMS - Plus	X	X	X	X								
NEXT Witness								X				
SNORT						X	X	X				



	5. National Data and Information Sharing						
	Cyber attack profile database		Virus and worm signature database			Attack tools	Forensic and analytic support for legacy software
Needs	Serves as a database for collecting attack profiles in concert with a solution for performing technical exploit matching to enable law enforcement to identify attack patterns.	Serves as a database for cyber attacks that allows law enforcement agencies to quickly assess if their case is a component of larger criminal activity.	Automates analysis of logs for the presence of a virus or worm signature, specifically designed for cyber attack cases.	A resource to store and compare new virus code to existing examples.	Applies pattern recognition software to determine the origin and author of a virus or worm.	Serves as a database of Trojans, root kits, and other attack tools that is continually updated that provides investigators with relevant and timely analysis capability.	Serves as a data warehouse of legacy software and hardware for agencies responsible for cyber attack and cyber crime.
TOOL NAME	5.1	5.2	5.3	5.4	5.5	5.6	5.7
PATHFINDER	X	X					
Kago IDS	X		X	X		X	
Byte Back							X
White Glove	X						
Log Management Sys			X				
i2 Analysts Notebook/iBase	X	X	X			X	
DIBS Mycroft V3			X				
Encase V4			X				
SMART			X				
DMZS F.I.R.E.			X				
New Technologies C.I.R. Suite	X						
New Technologies Net Threat Analyzer	X	X					
Orion Magic	X	X					

Addendum to Gap Analysis Matrix: Additions to the Listed Tools

A list of additional tools that were suggested by participants at the Gap Analysis Prioritization Working Group is found in Table 1 below. No attempts were made by ISTS researchers to validate the claims of the participants. The first and third columns labeled "Need #" show the number given to the need for reference throughout this study. The column marked "Tool" lists the tools that were suggested by the Prioritization Working Group participants that are not reflected on the Gap Analysis Matrix.

Two tools are presented below that were submitted after the Gap Analysis Matrix was finalized for printing for the Prioritization Working Group session. Please note that Prioritization Working Group participants were made aware of the existence of these two tools:

- The first tool, InfiniStream Security Forensics produced by Network Associates, Inc., has a number of features to address the needs numbered; 1.1, 1.6, 1.7, 1.12, 1.13, 1.15, 2.6, 2.8, 2.10, 2.13, 2.14, 3.1, 3.3, 4.4, 5.4 and 5.7.
- The second is a suite of system utilities from Sysinternal. The suite purports to address the needs numbered; 1.2, 1.3, 1.4, 1.6 and 2.4.

Table 1 – Addendum to the Gap Analysis Matrix – Tools Discussed at the Prioritization Working Group But Not Referenced on the Gap Analysis Matrix

Need #	Tool	Need #	Tool
1.1	Event Viewer by Engagement	2.5	SMART[IV]
1.1	OS commands including netstat, lsof and ps[I]	2.8	Forensic ToolKit[IV]
1.1	Kazaalite	2.9	In development tool from the Dept. of Law, School of Engineering at the University of Leeds. No other information available
1.1	AFCERT Tool (name not given by participants; believed to be the First Responder's Evidence Disk)	2.12	Silent Runner[IV]
1.2	Nmap[III]	2.12	SWATCH[IV]

1.6	Kismac[II]		2.12	Tripwire[IV]
1.6	Airopeek by Wildpacket[II]		2.12	A tool in development by New Scotland Yard was mentioned here. No additional details were given.
1.7	Snort[IV]		2.12	A tool is purported to be available at Intrusion.com
1.7	Silent Runner[IV]		2.14	NIJ is purported to have a Flash animation based presentation tool for use in the courtroom.
1.8	Nmap[III]		3.1	Various listserves and informational portals were noted here including CFID, HTCIA, IACIS, Digital DA, CyberCop and the CyberScience Lab
1.9	TNG by Computer Associates		3.3	SamSpade.org was given as a potential resource.
1.9	3Com Network Supervisor		3.4	Silent Runner[IV]
1.10	Nessus[III]		3.4	Tcpdump/windump
1.10	Nmap		3.4	Ethereal
1.10	Airopeek by Wildpacket[II]		4.2	Ongoing research at Dartmouth College in the detection of digital tampering and steganalysis
1.10	Wellenreiter[II]		4.2	DCFL and MITRE were purported to be conducting ongoing research in this area.
1.10	LanGuard		4.3	Air Force through the NLECTC-West was cited as a resource to address this need.
1.13	GNU version of dd		5.1	A number of agencies were noted that may be contacted

				as a resource to assist with this need, including FBI STAU, FBI Cyber Division, All.net, and the DHS IAIP Directorate.
1.14	DriveSpy[III]		5.2	Several agencies were suggested as resources including IACIS, DHS, IAIP, HTCIA, and IFCC
1.14	Byte Back III[IV]		5.4	Virus Consortium
1.14	Norton Ghost[IV]		5.4	TrueSecure (ICSA Labs)
1.11	Nmap[III]		5.6	CVE
1.14	Safeback (NTI) [IV]		5.6	Packetstorm
1.14	SMART[IV]		5.7	Several resources were suggested including DOD CFL, Secret Service, Postal Inspectors, FLETC, pcmuseum.com
1.14	FTK[IV]			

[I] Operating systems commands were not included in the Gap Analysis Matrix because they cover an increasingly wide and varied functional ability. Although they may be useful in an investigation, they are not intended to be used as forensic tools.

[II] The discovery and/or mapping of a wireless network was not a focus of the tool collection efforts.

[III] Many investigators mentioned tools from the hacking/cracking realm. While potentially useful in discovering network information, the use of un-vetted attack tools for evidentiary forensics is clearly problematic. In the development of the Gap Analysis Matrix, tools such as Nmap, Nessus, and other attack-focused tools were intentionally omitted.

IV Denotes tools that were included on the Gap Analysis Matrix, but were not attributed to having features that addressed the referenced need.

Appendix C – Gap Analysis Prioritization Working Group Data and Analysis

Each category discussion includes the following sections:

- Discussion of Needs and Tools
- Working Group Comments
- Preliminary Findings

The **Discussion of Needs and Tools** section examines how the collected tools map against the needs in the Gap Analysis Matrix. Further, this discussion includes a summary of the number of tools purporting to address the category's needs and mirrors the data presented to the Prioritization Working Group.

In the **Working Group Comments** section, the anonymous comments of the Prioritization Working Group participants are summarized and presented. These comments are in response to the three questions they were asked regarding each of the needs in each of the five categories. The first question asked: "Are you aware of any additional solutions that meet the needs described in this category? If yes, enter the name of the solution(s)." The second question asked: "What needs in this category do you feel are not met by the available solution(s)? Please add your justification for each need." Following the comment period, the participants were polled regarding their opinion on the following question: "What needs in this category do you feel require further research and development?" The participants were allowed to mark as many of the needs as they felt still required additional research and development.

It was possible that additional tools, not represented on the Gap Analysis Matrix, would be relevant to the participants' decisions. We provided an opportunity for participants to suggest additional solutions to ensure that the group had the best available information upon which to base their conclusions.

Conversely, many needs did not show a product availability gap and had, in fact, multiple tools marked in the Gap Analysis Matrix that purported to include applicable features. In this case, we provided Prioritization Working Group participants the opportunity to explain why they felt the need was not addressed and why it was still a research and development priority.

The **Preliminary Findings** section details the results of the polling and examines any trends or correlations that have come from the ISTS researcher's analysis of the collected data.

Category 1. Preliminary Investigation and Data Collection

Discussion of Needs and Tools

The Preliminary Investigation and Data Collection category of the *National Needs Assessment* yielded fifteen distinct needs (Table 2). Existing tools were collected and analyzed against these fifteen needs.

Table 2 – Category 1 – Preliminary Investigation and Data Collection

List of Needs

1.1.	Automates the collection of data from multiple operating systems to learn how a network was compromised.	1.9.	Graphically represents network mapping results to better understand the complex relationships in the victim's network.
1.2.	Identifies system configurations.	1.10.	Enables investigators to independently discover the topology of the network.
1.3.	Reports system configurations.	1.11.	Enables investigators to independently verify the topology of the network.
1.4.	Identifies file locations.	1.12.	Alleviates investigator's dependence on in-house staff at victim's location.
1.5.	Reports file locations.	1.13.	Captures RAM data without modification/alteration/addition.
1.6.	Discovers a system's role on a network.	1.14.	Captures Swap file data without modification/alteration/addition.
1.7.	Reports a system's role on a network.	1.15.	Designed to process very large data sets.
1.8.	Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses.		

As represented on the Gap Analysis Matrix (Appendix B) forty-eight tools and/or tool suites were plotted against the Category 1 needs. Eight of the fifteen needs presented, 1.6 – 1.11 and 1.13 – 1.14, had less then four tools purporting to address the need. This lack of tools was evident primarily in the network forensics area and included the investigator's desire to discover and report a system's role on a network; detect settings and recognize hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses; graphically represent network mapping results to better understand the complex relationships in the victim's network, and the ability for investigators to independently discover or verify the topology of the network. Two of those eight needs, 1.13 Captures RAM data without modification/ alteration/ addition and 1.14 Capture swap file data without modification/ alteration/ addition, had in fact one tool noted between them. Conversely, a majority of the listed tools purported to address numbers 1.1-1.5, 1.12 and 1.15.

Working Group Comments

1.1 Automates the collection of data from multiple operating systems to learn how a network was compromised.

Several of the participant comments centered on clarifying the use and intent of the end user license agreement for Safeback produced by NTI. A tool suggested that was not included on the Gap Analysis Matrix for this category included Event Viewer from Engagement. Participants also noted that operating system commands, such as netstat, lsof, and ps, are valuable for network forensics. These commands were not present on the Gap Analysis Matrix and may address some of the presented needs (please see the note in the Appendix B regarding OS commands). Also noted was the availability of Linux boot disks that can boot a system and mount any file systems found, read-only.

Participants discussed their need for a tool to deal with peer-2-peer networks. Kazaalite was suggested as a potential solution. One participant noted "The Air Force Computer Incident Response Team (AFCERT) has a software program that is used for identifying intrusions into their networks. According to [AFCERT], their backend can import logs from a variety of logs and vendors, and might be usable—or could be modified—to analyze logs from a variety of sources."

The participants did not appear satisfied that the existing tools adequately addressed their specific needs and concerns. Comments such as "Due to the cost of some of the tools we tend to develop our own," and "The data collection tools tend to collect everything (known file hashes aside, for the moment). This results in huge data storage needs, lengthy analysis and lots of wasted effort to find the smoking gun. There has to be a better way!" showed some level of dissatisfaction with the current state of accessible tools. The lack of tools with the ability to capture volatile information was echoed by a participant who stated "Most of the tools listed gather historical information (after system is shut down), not current state information which could disappear once the system is turned off."

1.2 Identifies system configurations.

Participants provided no relevant comments on this need.

1.3 Reports system configurations.

Only two relevant comments were generated for this particular need. The first suggested that EnCase and its "initialize case" script be used to gather system and network configuration information. EnCase was recorded in the Gap Analysis Matrix as a tool purporting to address this particular need. The second suggested the use of Nmap to gain information about the configuration of the network.

1.4 Identifies file locations.

Participants provided no relevant comments on this need.

1.5 Reports file locations.

One participant provided clarification on our claim that EnCase addresses this need, in that EnCase provides "original file paths" to the investigator during an examination.

1.6 Discovers a system's role on a network.

The only relevant discussion at the Prioritization Working Group session was not focused on discovering the role of a particular system on a network, but instead centered on the discovery of unsecured or rogue wireless networks. One participant noted that a tool for discovering wireless networks was missed in the Gap Analysis Matrix: "Kismac is great for wireless network discovery on the MAC OSX (GUI)." A second participant suggested another tool, "Airopeek NX is the best tool for wireless discovery. Unfortunately it costs."

1.7 Reports a system's role on a network.

No additions to the Gap Analysis Matrix were provided for this need; however, one participant provided a suggestion on how existing tools, not specifically designed to address this need, may present an adequate solution: "By analyzing packets coming from a particular system, tools such as snort or silent runner can give you insight as to the role of that particular system (i.e. web server, mail server...etc)."

1.8 Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses.

Two tools were brought up for discussions that were not marked on the GAM as addressing this particular need. Nmap was suggested as a solution and was described as a "good free tool." One participant asked why ILook was not marked as fulfilling this need. According to our research and two of the experts at the Prioritization Working Group, it is not believed that ILook will detect settings and recognize hardware on a network.

1.9 Graphically represents network mapping results to better understand the complex relationships in the victim's network.

One participant clarified and validated this need by stating "A tool that could do this without causing a significant impact on a victim network would be useful." Another suggested the use of TNG from Computer Associates to graphically map networks. Lastly, it was recommended to the group to look into tools that are used by system administrators; but the commenter warned that the specific requirements of investigators may differ from the needs of system administrators.

1.10 Enables investigators to independently discover the topology of the network.

This particular need generated a fair amount of comments from the participants. Several tools that purport to accomplish the task of independently discovering the topology of the network were suggested. The first tool suggested was Nessus. As one participant describes it, "Nessus is a freeware program that will probe a network and attempt to identify network devices, and for computers, attempt to identify the OS. It then displays the information graphically." It was suggested that Foundstone has some great tools that help identify the network topology and Nmap was also suggested as a potential solution; "Nmap is a free tool that will also probe the network for computers, and attempt to identify the os. There is also a windows version of this program." Discovery of the presence of, and to a limited extent, the topology of a wireless network was purported to be addressed by Airopeek NX. This tool, produced by Wildpacket, is a tool that can be used to quickly discover the topology, protocols and traffic on a wireless network. The discovery and auditing of 802.11b networks can be accomplished by a GTK/Perl Program called Wellenreiter. Additionally, a participant described a "program call called Languard. Not only will it discover what the topology is, but what services are running on the machine."

1.11 Enables investigators to independently verify the topology of the network.

Only two tools, Anasil and InterMapper, were noted in the Gap Analysis Matrix as addressing this need, and only one comment suggesting an additional tool, Nmap, was made by the participants.

1.12 Alleviates investigator's dependence on in-house staff at victim's location.

One of the participants reiterated the importance of using technology in conjunction with solid investigative techniques; "I don't think there is one tool that can alleviate an investigator's dependence on in-house staff. The human factor is always a factor in an investigation. Good up front investigating before using any 'tech' tools is crucial." Good investigative techniques will help minimize the human factor, but being able to assess the situation personally is an important aspect of the investigation. As one participant commented "There is no substitute for direct access to networks, especially when the in-house staff has no interest in cooperating with US authorities."

1.13 Captures RAM data without modification / alteration / addition.

The research and tool collection conducted as part of creating the Gap Analysis Matrix found no tools that purported to fulfill this need. However, several comments were collected that claim to have found methods by which RAM can be captured. Two of these comments included: "You can use a GNU version of dd (such as in Cygwin) to capture the RAM in Windows 2000 and XP," and "RAM can be captured from Linux and Solaris systems. Both have a device which refers to the system RAM and cat or dd can be used to copy the information." The difficulty associated with RAM capture was further corroborated by a few of the participant's comments including; "The ability to capture RAM without modification/alteration/addition is not practical since any tool used to collect the information must be run, adding itself to the RAM. However, capturing the RAM with minimal alteration can be useful."

1.14 Captures Swap file data without modification / alteration / addition.

Only three tools were noted in the Gap Analysis Matrix as addressing this need: ProDiscover DFT V2, DIBS Analyzer 2, and Encase V4. The participants noted several other tools which have the ability to capture swap file data without modification/alteration/addition. The six tools noted by participants are DriveSpy, Byte Back III, Norton Ghost, Safeback (NTI), SMART, and FTK.

1.15 Designed to process very large data sets.

The first comment by a participant of the Prioritization Working Group further validated and clarified the problem which exists when investigations include very large data sets: "I have seen forensic investigations stymied by terabytes of data…this is a prime problem with cyber terrorism." Additional comments did not provide any new tools for the Gap Analysis Matrix, but did provide insight into the ability for some of the marked tools to address this need. For example, it was noted that EnCase 4 handles large data sets well. FTK was discussed in terms of its indexing function, and whether or not this is an advantage in examining large case files. Here is a sample of the conversation over the decision support software:

> The FTK tools indexing actually helps with large case management because searches are nearly instant after the index is complete instead of a wait[ing] for the string search to be accomplished using other tools.
>
> FTK takes too long due to all the indexing up front....not efficient for large organizations with large case loads.
>
> I disagree. A lab set up properly, using FTK in a distributed system, can be quite efficient. Run your indexing off-peak (overnight, etc.), then when you sit down to work the case, everything is instantly available.
>
> That is fine and dandy if you have a small case load. In our organization, indexing up front on large storage devices (with a large case loads) can take too long, no matter how you have your lab set up.

Obviously, the participants disagreed on the value of up-front indexing on large cases, however, it should be noted that the ability for the tool to perform as advertised was not questioned in this particular dialogue.

Preliminary Findings

As noted in the Gap Analysis Prioritization Working Group section on page 8, the participants were asked to mark the needs that they felt were still a research and development priority. The results from the poll for Category 1, Preliminary Investigation and Data Collection, are presented in Table 3 below. All of the fifteen needs presented in this category received at least three votes from the twenty-two participants. This indicates that at least a minority of the group felt that all of the needs in this category required additional research and development.

Two needs received more than 50% of the participants votes: "1.8 Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses" and "1.10 Enables investigators to independently discover the topology of the network." On the Gap Analysis Matrix, need numbered 1.8 showed four software solutions that purported to have applicable features.

These software packages are White Glove, EagleCheck, Encase V4, and Anasil. Additionally, Prioritization Working Group participants noted that ILook and Nmap may also function in this capacity.

Need numbered 1.10 generated several comments during the Prioritization Working Group, including a number of comments to suggest additional relevant software. The Gap Analysis Matrix listed Anasil as the only tool to contain features that address this need. The participants added Nessus, Nmap, Airopeek, Wildpacket, Wellenreiter, Languard and a suite of tools produced by Foundstone to the list of applicable solutions. The addition of these tools to the discussion appeared to prove inconsequential as twelve of the participants felt that enabling investigators to independently discover the topology of the network was still a research and development priority. No justification was given by the participants as to why the existing solutions were not sufficient to address the needs numbered 1.8 and 1.10.

Table 3 – Results of polling: What needs in Category 1 do you feel require further research and development?

Need		Number of Votes
1.8	Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses.	12
1.10	Enables investigators to independently discover the topology of the network.	12
1.1	Automates the collection of data from multiple operating systems to learn how a network was compromised.	10
1.6	Discovers a system's role on a network.	10
1.11	Enables investigators to independently verify the topology of the network.	10
1.13	Captures RAM data without modification/alteration/addition.	10
1.7	Reports a system's role on a network.	9
1.9	Graphically represents network mapping results to better understand the complex relationships in the victim's network.	8
1.12	Alleviates investigator's dependence on in-house staff at victim's location.	8

1.15	Designed to process very large data sets.	8
1.2	Identifies system configurations.	6
1.3	Reports system configurations.	6
1.14	Captures Swap file data without modification/alteration/ addition.	5
1.4	Identifies file locations.	4
1.5	Reports file locations.	3

Category 2. Log Analysis

Discussion of Needs and Tools

The Gap Analysis Matrix maps thirty-five tools against the fourteen Category 2 needs. The needs appeared to be fairly well addressed by the collected tools as each of the needs had at least eight tools marked as having applicable features. Needs "2.5 Searches for fragmentary information to reconstruct logs" and "2.10 Creates data sets optimized for analysis, portability, and interoperability" were well represented, with twenty-two and twelve tools, respectively, purporting to address those particular needs. Need "2.11 Contains easy-to-use search functions" appeared to be a feature inherent to most of the solutions listed in this category as thirty-two solutions claimed to address this need.

Table 4 – Category 2 – Log Analysis

List of Needs

2.1.	Searches a network for logs.	2.8.	Organizes data into a graphical timeline.
2.2.	Recognizes and collects logs regardless of platform.	2.9.	Provides consistent timeline and reports / graphs discrepancies in time correlations.
2.3.	Recognizes and collects logs regardless of format.	2.10.	Creates data sets optimized for analysis, portability, and interoperability.
2.4.	Prepares logs for export to different operating system or analysis environment.	2.11.	Contains easy-to-use search functions.
2.5.	Searches for fragmentary	2.12.	Contains analytic tools that

	information to reconstruct logs.		autonomously uncover anomalies in large log files.
2.6.	Automatically captures the individual time and date settings from compromised network computers.	2.13.	Presents detailed technical information in a graphical format.
2.7.	Translates log files from multiple time zones to a common time frame.	2.14.	Serves as a tool for prosecutors to present complex cyber attack data in the courtroom.

Working Group Comments

2.1 Searches a network for logs.

Participants commented that several of the tools marked within the Gap Analysis Matrix did not contain features that addressed this need. One participant noted that they are “not aware of any tool that will look across multi-server networks (Domains) for the various types of log files.” Another participant summarized the group’s comments when they remarked that they “have doubts that any of this software can do this without the cooperation of the system that maintains the logs.” Participants saw promise in the progress that has been made in the web-stats area.

2.2 Recognizes and collects logs regardless of platform.

The majority of participants’ comments further validated and clarified the intent of this need. One participant recognized that a “tool is needed to conduct log file correlation, and present [one set of] data based on multiple types of logs.” Another commenter summarized the other thoughts on the topic; “Tools that could check the system configuration and determine where log files exist and automatically collect them…would be good.”

Silent Runner was noted on the Gap Analysis Matrix, and one participant provided clarification on its features in this area; “Silent Runner recognizes different logs, however, it needs tweaking for certain types of logs before it can be used.”

2.3 Recognizes and collects logs regardless of format.

Additional validation of this need was provided by one participant who commented that “logs are tough to find... we’ve once found an obsolete marketing tool run by a little guy hiding in a small department that actually had valuable information for us.” The true breadth of the problem facing investigators was summarized by a participant who wrote: “Another problem is not just the various logs generated by the OS, but also application logs." Another offered a suggestion to software and OS developers to "agree on a standard record layout for all logs. It would then be easy to develop a tool that could recognize, collect and analyze them."

2.4 Prepares logs for export to different operating system or analysis environment.

The comments of the participants focused on a discussion of the portability of Syslog data. Where one participant noted that Syslog data is in a pretty basic format and usually doesn't require exporting for use in another environment, another noted that Syslog does need parsing if you want to do any kind of network correlation and that none of the listed tools accomplish this task for Syslog data.

2.5 Searches for fragmentary information to reconstruct logs.

The Prioritization Working Group participants correctly noted that SMART has features that address this need, but the tool was not marked on the Gap Analysis Matrix for this need.

2.6 Automatically captures the individual time and date settings from compromised network computers.

Clarification and validation of this need was provided by one participant who wrote: "Synchronizing time in logs is a real pain. What is really needed here is a tool for getting independent verification of time." Embedding time-stamps into HTML on webpages was discussed; however, the ease in which time-stamps may be spoofed was brought up as a possible flaw in the proposed idea. No new tools were discussed for this need.

2.7 Translates log files from multiple time zones to a common time frame.

The participants saw this need as being integrally linked to, and equally important as, capturing a time and date settings discussed in above in need numbered 2.6; "Time zone is very important....especially on an e-mail case and proving a network intrusion." If the time stamps are valid, but no corrections are made for the time zone difference, then the logs will not correlate correctly. As one participant noted, "This is critical functionality since defense attorneys will definitely use non-matching times as a major attack on the examiners' conclusions." No additional tools to address this need were suggested.

2.8 Organizes data into a graphical timeline.

The participants validated that the entry on the Gap Analysis Matrix under this need for EnCase was in fact valid; "EnCase does this on a file access basis...good for determining log access." The participants also added Forensic Tool Kit (FTK, Access Data) which was not marked for this need on the Gap Analysis Matrix. Also discussed was the need for analyzing the timeline of events that occur on IRC and other peer-2-peer networks.

2.9 Provides consistent timeline and reports / graphs discrepancies in time correlations.

A solution that is currently under development was volunteered by a participant; the Department of Law in the School of Engineering at the University of Leeds is working on a prototype to accomplish this need. No other information about the prototype was available.

2.10 Creates data sets optimized for analysis, portability, and interoperability.

This need was further clarified by a member of the group. They had written that "on numerous occasions, IP's send log files that are not compatible or viewable on the investigator's computer. A universal tool that extracts, reads and views log files would be nice." No additional tools were noted.

2.11 Contains easy-to-use search functions.

Although this need appeared to be a function available in almost every tool listed on the Gap Analysis Matrix, the complexity of this issue was brought to light by a participant who noted that each network operating system seems to have its own proprietary tool for examining a variety of log files. However, the need for a system like this was reiterated by a commenter who wrote: "Flexibility in searching data sets and log files is critical to detecting illegal activities and complex correlations. Large data sets can often conceal much useful information."

2.12 Contains analytic tools that autonomously uncover anomalies in large log files.

The discussion regarding this need included suggestions of several additional tools that may have some capacity to address this need. Traditional forensic tools discussed included Silent Runner and Swatch, while IDS systems such as Snort/Snarf, and Tripwire. Solutions under development from New Scotland Yard and Intrusion.com were also suggested as potential solutions. A few of the participants believed that addressing this need as a whole was a difficult task, and suggested making short-term achievable goals a priority. These goals included a "web site with info on relevant log files would be great…. Knowing what logs to look for with various applications could help even in writing search warrants," and "state-aware analysis tools that can detect spoofed IPs and other nefarious activities based on illogical traffic patterns."

2.13 Presents detailed technical information in a graphical format.

The mark for Silent Runner under this need was validated by a participant who wrote "Silent Runner has a great play back feature and graphics tool." Validation for the need came in the form of a comment which read; "A tool like this would be great for the 'non-technical' grand juries and judges."

2.14 Serves as a tool for prosecutors to present complex cyber attack data in the courtroom.

This need was one of the most commented-upon topics and discussions focused on the particular features of tools listed on the Gap Analysis Matrix, specifically ILook, EnCase, i2 Analysts Notebook, and an under-development solution from the NIJ. ILook received excellent reviews of its presentation abilities: "ILook does a good job (from a prosecutor's perspective) with producing e-mail search results in a courtroom friendly format." Silent Runner also received positive comments mainly touting Silent Runner's visual network attack features. Negative feedback was collected regarding Silent Runner being cost prohibitive for many law enforcement agencies. The discussion surrounding i2 was positive as well: "i2 is a useful tool for showing visual relationships in data and does accept import of data in standard file formats," and "i2 is very good at presentation combining telephone records with timeline of occurrences." Lastly, NIJ was rumored to have recently developed flash animation presentation tools for use in the courtroom with participation from DOJ-CCIPS.

Preliminary Findings

The results from the polling of participants regarding which needs they felt were still a research and development priority is found in Table 5. Three of the needs received more than 50% of the participants votes: "2.13 Presents detailed technical information in a graphical format," "2.14 Serves as a tool for prosecutors to present complex cyber attack data in the courtroom," and "2.2 Recognizes and collects logs regardless of platform." The top two needs both address representing the complex data recovered during an investigation either to the investigator or to non-technical persons, such as those that would be present in a courtroom. The third, fourth and fifth needs are related to recovering logs from a network. All of the needs received votes from at least seven participants, or approximately 32% of the group.

The needs that received more than 50% of participants' votes were fairly represented by solutions in the Gap Analysis Matrix. Needs numbered 2.13, 2.14, and 2.15 all had more than eleven tools that claimed to address their particular need.

Table 5 – Results of polling: What Needs in Category 2 do you feel require further research and development?		Number of Votes
2.13	Presents detailed technical information in a graphical format.	13
2.14	Serves as a tool for prosecutors to present complex cyber attack data in the courtroom.	13
2.2	Recognizes and collects logs regardless of platform.	12
2.3	Recognizes and collects logs regardless of format.	11
2.1	Searches a network for logs.	10
2.10	Creates data sets optimized for analysis, portability, and interoperability.	10
2.4	Prepares logs for export to different operating system or analysis environment.	9
2.8	Organizes data into a graphical timeline.	9
2.9	Provides consistent timeline and reports / graphs discrepancies in time correlations.	9
2.5	Searches for fragmentary information to reconstruct logs.	8
2.6	Automatically captures the individual time and date settings from compromised network computers.	8
2.11	Contains easy-to-use search functions.	8
2.13	Presents detailed technical information in a graphical format.	8
2.7	Translates log files from multiple time zones to a common time frame.	7

Category 3. IP Tracing and Real Time Interception

Discussion of Needs and Tools

Four needs were extracted from the *National Needs Assessment* that capture the fundamental problems facing law enforcement investigators in this area. The Gap Analysis Matrix, found in Appendix B, shows the solutions that were collected and mapped against the needs in this category. The four needs are presented below in Table 6.

Table 6 – Category 3 – IP Tracing and Real-time Interception

List of Needs

3.1.	Facilitates and coordinates cross-jurisdictional communications.
3.2.	Provides added capability to trace and/or counter IP spoofing.
3.3.	Provides added capability to detect IP spoofing.
3.4.	Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception.

There were only a small number of solutions that claimed to address these needs. The need numbered "3.4 Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception" had eleven solutions purporting to address this need; the most in this category. Needs numbered 3.1 and 3.2 each had five solutions mapped, while need 3.3 had only two solutions that claimed to address the need.

Working Group Comments

3.1 Facilitates and coordinates cross-jurisdictional communications.

Participants volunteered a multitude of organizational systems that assist in cross-jurisdictional communications. These included the US DOJ 24x7 Network, FBI Legal Attaché Network, NLECTC system, Joint Cyber Task Force, DOD JTF/CNO Law Enforcement/Counter Intelligence Center, American Prosecutor's Research Institute, CCIPS, Regional JTTFs, National White Collar Crime Center and their Internet Fraud Complaint Center (IFCC), and ICANN. A heavy reliance on personal contacts was also noted.

Technology solutions to contact associates such as telephones, pagers, and email are often used by investigators. Listserves such as CFID, HTCIA, IACIS, and Digital-DA were reported to "do amazing things now" and are "very useful for communicating with folks in other jurisdictions who can help you." Secure law enforcement-only web portals, such as CyberCop and the newly revamped Cyberscience Lab website were also suggested as great solutions for reaching across jurisdictional lines.

3.2 Provides added capability to trace and/or counter IP spoofing.

The participants did not provide additional technology solutions for this need. Instead the comments focused on the development of systems for geo-locating IP addresses. “There are efforts in the intelligence and homeland security world to identify where activity ‘should’ come from based on IP address registrations. Better tools are needed to monitor the national gateways to detect suspicious activity,” and “At least one company has been researching methods to ‘map’ cyberspace. If they can match all IPs addresses to their physical location (of registration) it is then easier to identify who is operating from away from home or being spoofed.” The latter suggestion was tempered by its author who wrote, “This is a mammoth project though, but if you could sit at every major node and watch the traffic you could eventually figure who is where.”

3.3 Provides added capability to detect IP spoofing.

Very few comments were generated for this need. One participant suggested that using Sam Spade to take a “quick look at email headers is sometimes helpful.” A second participant noted to use Sam Spade with caution, because the “hacker [may be] using a web proxy, or an anonymizer” which would make gaining useful information from the header difficult.

3.4 Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception.

Law enforcement investigators are often faced with copious amounts of data as a result of a legally authorized electronic surveillance. The parsing, isolation of relevant material, and analysis of this data can be a very time consuming task. Several tools to assist in capturing data were suggested, including tcpdump, Silent Runner, windump and Ethereal.

One participant commented on working with the business sector in this type of surveillance: “All major telecommunications switch vendors provide law enforcement monitoring features which can identify, isolate, copy, and record transmissions from target addresses in real-time.” However, this was noted by several participants as being cost prohibitive in some cases.

Capturing and viewing only the data that is relevant to the search warrant is a definite concern to law enforcement as discussed in the *National Needs Assessment* and further validated by one participant who wrote “There is definitely a need for easy-to-use tools that will capture and parse huge amounts of information and are proven to be able to capture ONLY the data authorized to capture.”

Preliminary Findings

All of these needs in this category were believed to require additional research and development by more than 50% of the participants. In fact, two-thirds of the participants felt that the needs numbered 3.3 and 3.4 required additional research and development as seen in Table 7. As noted above in Discussion of Needs and Tools, this category was under-represented by solutions, with at most eleven solutions purporting to have features to address these particular needs and at the least, two solutions.

Table 7 – Results of polling: What Needs in Category 3 do you feel require further research and development?		**Number of Votes**
3.3	Provides added capability to detect IP spoofing.	14
3.4	Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception.	14
3.1	Facilitates and coordinates cross-jurisdictional communications.	12
3.2	Provides added capability to trace and/or counter IP spoofing.	11

Category 4. Emerging Technologies

Discussion of Needs and Tools

The *National Needs Assessment* produced four needs in the Emerging Technologies category as seen in Table 8. The Gap Analysis Matrix shows that this category is under-represented by the collected tools.

Table 8 – Category 4 – Emerging Technologies

List of Needs

4.1.	Increases law enforcement's ability to circumvent the obstacle of encrypted data.
4.2.	Flags digital files that may contain steganographic messages.
4.3.	Provides magnetic microscopy technology for law enforcement applications.
4.4.	A solution(s) to securely store very large data sets that addresses data degradation and financial concerns of the law enforcement community.

All of the needs in this category had less than seven tools purporting to address their requirements. One particular need, "4.3. Provides magnetic microscopy technology for law enforcement applications," had no tools mapped against it.

Working Group Comments

4.1 Increases law enforcement's ability to circumvent the obstacle of encrypted data.

Participants offered no additional tools to address this need. A participant summarized the problem facing law enforcement when they wrote, "The bottom line is that strong encryption works well and is a [real problem] for law enforcement." One suggestion was put forward to use ILook to build a dictionary from a seized hard-drive to use as the foundation of a dictionary attack on the encrypted material. Key loggers, installed under proper authority, were discussed as a manner to defeat encryption by capturing usernames and passwords. Regardless of the technology solutions available, this problem seemed to be grounded in "overcoming the perception of whether law enforcement is achieving this objective consistent with Constitutional guarantees."

Another participant suggested that there may be a "legislative solution, at least with domestic products. For example, a requirement that any encryption program provided in the U.S. must have a registered back-door key, held in escrow and available to LE with the right paper?" Other participants noted that this concept was discussed in the past and it was not a viable option for a number of reasons, including imposing unfair restrictions on products made in the US.

4.2 Flags digital files that may contain steganographic messages.

Participants highlighted some ongoing research from the DCFL and MITRE, and validated the work being conducted by Wetstone Technologies. There is research under development at Dartmouth College in the area of digital tampering and steganographic detection. However, as one participant stated, "Many great tools exist, but not one does the trick. You need multiple tools, and still that is not enough."

4.3 Provides magnetic microscopy technology for law enforcement applications.

Magnetic microscopy is generally regarded as the cutting edge in the retrieval of multiple-wipe deleted data and data recovery from damaged media. In the *National Needs Assessment*, investigators saw a need for this technology to be made more available, particularly for state and local agencies. The participants commented that there are very few agencies or research facilities that have the capability to conduct this type of work, however it was noted that their assistance is usually only available in extreme situations. It was suggested that a measure of these services is provided by the Air Force through the NLECTC-W system.

4.4 A solution(s) to securely store very large data sets that addresses data degradation and financial concerns of the law enforcement community.

Investigators are commonly faced with storing a growing library of case-related digital data. Storing this data securely and in a way in which media and/or data degradation is minimized adds to the cost. One of the participants commented on the situation facing law enforcement investigators, "This is more a [funding] problem, than a technology problem. Chasing the technology, for LE, is just expensive." This type of problem is not uncommon in this field, where the criminals have a monetary or personal incentive to invest in technology; while investigators usually do not have an unlimited budget to dedicate to keeping pace with the offenders.

Preliminary Findings

The participants were asked which of the needs were still research and development priorities in light of the solutions presented on the Gap Analysis Matrix and in the workshop discussions. An overwhelming 77% of the participants included a vote for need "4.1 Increases law enforcement's ability to circumvent the obstacle of encrypted data" (Table 9). Although need 4.1 received the most participant votes, it had the most tools noted on the matrix among the other needs in this category. This need appears to be a continuing need of the investigative community and appears to be as controversial as it is critical, based on the participant's comments. A second need, "4.2 Flags digital files that may contain steganographic messages," received 50% of the participants' votes and had a corresponding four tools mapped on the Gap Analysis Matrix. Steganalysis software will continue to grow and evolve in response to new steganographic algorithms and it does not appear as if the greater problem will be solved in the immediate future.

Table 9 – Results of polling: What Needs in Category 4 do you feel require further research and development?		**Number of Votes**
4.1.	Increases law enforcement's ability to circumvent the obstacle of encrypted data.	17
4.2.	Flags digital files that may contain steganographic messages.	11
4.4.	A solution(s) to securely store very large data sets that addresses data degradation and financial concerns of the law enforcement community.	7
4.3.	Provides magnetic microscopy technology for law enforcement applications.	6

Category 5. National Data and Information Sharing

Discussion of Needs and Tools

Analysis of the *National Needs Assessment* and related material produced seven needs in the Data and Information Sharing category. A listing of the Category 5 needs is found in Table 10. The Gap Analysis Matrix lists thirteen tools which have some capability to address at least one of the needs in this category.

Five of the needs numbered 5.2 and 5.4-5.7, had less than four technology solutions mapped on the Gap Analysis Matrix. One of these needs, "5.5 Applies pattern recognition software to determine the origin and author of a virus or worm," did not have a single available technology solution mapped on the Gap Analysis Matrix. Needs numbered 5.1 and 5.3 were both addressed by seven listed tools on the Gap Analysis Matrix

Table 10 – Category 5 – National Data and Information Sharing

List of Needs

5.1.	Serves as a database for collecting attack profiles in concert with a solution for performing technical exploit matching to enable law enforcement to identify attack patterns.
5.2.	Serves as a database for cyber attacks that allows law enforcement agencies to quickly assess if their case is a component of larger criminal activity.
5.3.	Automates analysis of logs for the presence of a virus or worm signature, specifically designed for cyber attack cases.
5.4.	A resource to store and compare new virus code to existing examples.
5.5.	Applies pattern recognition software to determine the origin and author of a virus or worm.
5.6.	Serves as a database of Trojans, root kits, and other attack tools that is continually updated that provide investigators with relevant and timely analysis capability.
5.7.	Serves as a data warehouse of legacy software and hardware for agencies responsible for cyber attack and cyber crime.

Working Group Comments

5.1 Serves as a database for collecting attack profiles in concert with a solution for performing technical exploit matching to enable law enforcement to identify attack patterns.

Participants suggested a number of agencies and organizations that have some capacity to address this need. FBI HQ Special Technologies Applications Section, The FBI's Cyber Division, Fred Cohen's All.net, and CERT were all suggested as potential starting points for additional information in this area. The overall issue was summarized by one participant who wrote:

> We need to identify one specific agency, location, etc. and give them the responsibility for this. There is too much competition among the federal agencies who lobby for jurisdiction, budgets, etc., and spend more time and effort on arguing with other agencies, watching what other agencies are doing and telling on them for doing it than completing the actual mission for which they are charged. In a nutshell, someone needs to make a decision. There is too much redundancy.

It was noted by participants that the newly organized Department of Homeland Security Information Analysis Infrastructure Protection Directorate has this need noted in their mission; however, it is not expected for this particular area to be functional in the immediate future.

5.2 Serves as a database for cyber attacks that allows law enforcement agencies to quickly assess if their case is a component of larger criminal activity.

Participants suggested a number of organizations that may serve in a capacity to address this need. These agencies include IACIS, DHS IAIP, CFID, HTCIA, and IFCC. None of these agencies are equipped to handle real-time, secure information sharing regarding active cyber attack cases. No technology-specific solutions were suggested.

5.3 Automates analysis of logs for the presence of a virus or worm signature, specifically designed for cyber attack cases.

Participants provided no relevant comments on this need.

5.4 A resource to store and compare new virus code to existing examples.

Participants suggested that The Virus Consortium, consisting of members of the law enforcement and anti-virus vendor communities, is a starting point to examine this type of data. Other participants noted that their organizations use third-party entities, such as the Truesecure Corporation (ICSA Labs), to collect and provide them with relevant data and analyses.

5.5 Applies pattern recognition software to determine the origin and author of a virus or worm.

Participants provided no relevant comments on this need.

5.6 Serves as a database of Trojans, root kits, and other attack tools that is continually updated that provides investigators with relevant and timely analysis capability.

Participants suggested integrating more closely with the anti-virus vendors to use the data they collect in the course of investigations. CVE and Packetstorm were also noted as sites on the Internet that should be consulted when looking for information on attack tools.

5.7 Serves as a data warehouse of legacy software and hardware for agencies responsible for cyber attack and cyber crime.

Participants suggested additional research be conducted about the services provided by the DoD in this area: “The DoD Computer Forensics lab keeps a large variety of legacy and new hardware. I don’t know if there is any technological way of checking what they have, other than a phone call.” Another participant noted that the “Secret Service and Postal Inspections used to have libraries of software and lots of old legacy hardware that they would loan out. A searchable database (web-based) that LE could access, for this stuff, would be very useful. I see requests on listservs all the time for tape drives, old backup software programs, etc.” Several other suggestions were given, including FLETC and pcmuseum.com, maintained by the Menz brothers.

Preliminary Findings

All of the needs received at least six participant votes for the need for additional research and development. Four of the seven needs received 50% or better support from the participants that additional work is needed (Table 11). Three of these needs are closely related and fall under the need for additional databases and informational resources related to the investigation of cyber attacks. The Gap Analysis Matrix showed that there are at least seven tools that purport to address at least parts of the top-voted need; “5.1 Serves as a database for collecting attack profiles in concert with a solution for performing technical exploit matching to enable law enforcement to identify attack patterns.” The needs that fell into the second and fourth spots had very few solutions marked in the Gap Analysis Matrix; four mapped solutions for need numbered 5.2 and two for need numbered 5.6. The third highest ranked need had seven tools marked for it on the Gap Analysis Matrix, similar to the top ranked need.

Table 11 – Results of polling: What Needs in Category 5 do you feel require further research and development?		**Number of Votes**
5.1	Serves as a database for collecting attack profiles in concert with a solution for performing technical exploit matching to enable law enforcement to identify attack patterns.	14
5.2	Serves as a database for cyber attacks that allows law enforcement agencies to quickly assess if their case is a component of larger criminal activity.	13
5.3	Automates analysis of logs for the presence of a virus or worm signature, specifically designed for cyber attack cases.	12
5.6	Serves as a database of Trojans, root kits, and other attack tools that is continually updated that provides investigators with relevant and timely analysis capability.	11
5.5	Applies pattern recognition software to determine the origin and author of a virus or worm.	10
5.4	A resource to store and compare new virus code to existing examples.	7
5.7	Serves as a data warehouse of legacy software and hardware for agencies responsible for cyber attack and cyber crime.	6

Appendix D – Preliminary Prioritization Findings

The prioritization exercises at the Prioritization Working Group were an opportunity to take the needs that had received at least one participant's vote in the five earlier category discussions and attempt to determine which of the needs were a more critical research and development priority. In this particular case at the Prioritization Working Group, all of the needs received at least one vote for requiring additional research and development from the participants. Therefore, all forty-four needs from the five categories were moved forward for consideration in the prioritization exercises.

A series of resource allocation and rank order exercises were conducted to determine which needs were most critical and, just as importantly, least critical to the investigators at the Prioritization Working Group. After a number of these exercises were conducted, the group reached a consensus that eighteen of the forty-four needs under consideration were the most critical needs requiring research and development.

Table 12 below lists the eighteen most critical needs in their approximate final order of criticality as determined by the Prioritization Working Group participants.

Table 12 – List of Most Critical Needs Requiring Additional Research and Development as Determined by the Prioritization Working Group

Need #	Need	Final Order
4.1.	Increases law enforcement's ability to circumvent the obstacle of encrypted data.	1
3.2.	Provides added capability to trace and/or counter IP spoofing.	2
2.13.	Presents detailed technical information in a graphical format.	3
2.14.	Serves as a tool for prosecutors to present complex cyber attack data in the courtroom.	4
3.3.	Provides added capability to detect IP spoofing.	4
1.13.	Captures RAM data without modification/alteration/ addition.	6
2.2.	Recognizes and collects logs regardless of platform.	7

2.1.	Searches a network for logs.	8
3.4.	Parses, isolates relevant material, and analyzes data captured in the course of legally authorized data interception.	8
1.8.	Detects settings and recognizes hardware on a network, including information on the presence and type of firewall(s), router(s), and network addresses.	10
3.1.	Facilitates and coordinates cross-jurisdictional communications.	10
2.3.	Recognizes and collects logs regardless of format.	10
1.1.	Automates the collection of data from multiple	13
5.2.	Serves as a database for cyber attacks that allows law enforcement agencies to quickly assess if their case is a component of larger criminal activity.	14
1.15.	Designed to process very large data sets.	15
1.9.	Graphically represents network mapping results to better understand the complex relationships in the victim's network.	16
4.2.	Flags digital files that may contain steganographic messages.	17
5.1.	Serves as a database for collecting attack profiles in concert with a solution for performing technical exploit matching to enable law enforcement to identify attack patterns.	18

Appendix E – Report Information

List of Tables

Acknowledgments

The Institute for Security Technology Studies extends it sincere appreciation to the many individuals and organizations from government, industry, and academia that participated in the Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report.

@Stake
Agora
Air Force Research Laboratory
Bank of America
BOS-NET
Bell Labs
Central Intelligence Agency
Carnegie Mellon / Software Engineering Institute
CERT CC
Computer and Technology Crime High-Tech Response Team (CATCH)
Counterpane
County of Los Angeles Sheriff's Department
CyberCop Portal
Cyber Science Laboratory
Decision Strategies
Delaware State Police
Earthlink
Federal Bureau of Investigation
Florida Department of Law Enforcement
Future Focus
Georgetown University - Georgetown Institute for Information Assurance
Hewlett-Packard
HTCIA
Joint Task Force - Computer Network Operations
Knowledge Solutions
Los Alamos National Lab
Mitre
NASA Office of Inspector General
National Institute of Justice
National Law Enforcement and Corrections Training Center – North East
National Law Enforcement and Corrections Training Center – West
National White Collar Crime Center
New Hampshire Attorney General's Office
New Jersey State Police
NYECTF
New York Police Department CITU
Philadelphia Police Department
Purdue University
SANS
San Diego Supercomputer Center
SEARCH
South Carolina Law Enforcement Division
State of Connecticut Department of Public Safety
State Street
Stroz Associates
Tenable Security
United States Department of Justice
United States Environmental Protection Agency
University of New Haven
United States Secret Service
University of Tulsa - Center for Information Security
Utica College of Syracuse University - Computer Forensic R&D Center
Vermont State Police
Wetstone Tech

Contact Information

Please address comments and questions to:

Law Enforcement Tools and Technologies for Investigating
Cyber Attacks: Gap Analysis Report
Technical Analysis Group
The Institute for Security Technology Studies
45 Lyme Rd.
Hanover, NH 03755
Telephone: (603) 646-0700
Fax: (603) 646-0660

Project e-mail: <tag@ists.dartmouth.edu>

The ISTS website is available at <http://www.ists.dartmouth.edu>

The ISTS Technical Analysis Group web site is available at
<http://www.ists.dartmouth.edu/TAG/>

Director:

Martin Wybourne

Research Staff for the Report:

Bill Brosius
Kathleen Cassedy
Robert Hillery
Stacy Kollias
Andrew Macpherson
Kevin O’Shea

The following individuals directly contributed to the creation of this study:

Leo Arsenault
Henry “Chip” Cobb
Nicole Hall-Hewett
Colleen Hurd

David Kotz
Dennis McGrath
Brett Tofel
Steve Snyder

The following outside organization directly contributed to the creation of this study:

GroupSystems / Ventana East Corporation

Publication Notice

LAW ENFORCEMENT TOOLS AND TECHNOLOGIES

FOR

INVESTIGATING CYBER ATTACKS

Gap Analysis Report

First Printing:

This project was supported under Award No. 2000-DT-CX-K001 from the Office for Domestic Preparedness, U.S. Department of Homeland Security. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security.