Contract No. 00-C-0328
IITRI CR-030-216

Independent Technical Review of the Carnivore System

Final Report

8 December 2000

IIT RESEARCH INSTITUTE

Contract No. 00-C-0328
IITRI CR-030-216

Independent Review of the Carnivore System

Final Report

Prepared by: Stephen P. Smith, Henry H. Perritt, Jr., Harold Krent, Stephen Mencik, J. Allen Crider, Mengfen Shyong, Larry L. Reynolds

8 December 2000

IIT Research Institute
Suite 400
8100 Corporate Drive
Lanham, Maryland 20785-2231
301-731-8894
FAX 301-731-0253

CONTENTS

CONTENTS (Cont)

CONTENTS (Cont)

CONTENTS (Cont)

CONTENTS (Cont)

FIGURES

CONTENTS (Cont)

FIGURES (Cont)

TABLES

EXECUTIVE SUMMARY

ES.1 INTRODUCTION

IIT Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law (herein abbreviated as IITRI), under contract to the Department of Justice (DoJ), evaluated a Federal Bureau of Investigation (FBI) system known as Carnivore. Carnivore is a software-based tool used to examine all Internet Protocol (IP) packets on an Ethernet and record only those packets or packet segments that meet very specific parameters. IITRI was asked to report on whether Carnivore

- Provides investigators with all, but only, the information it is designed and set to provide in accordance with a given court order
- Introduces any new, material risks of operational or security impairment of an Internet Service Provider's (ISP's) network
- Risks unauthorized acquisition, whether intentional or unintentional, of electronic communication information by: (1) FBI personnel or (2) persons other than FBI personnel
- Provides protections, including audit functions and operational procedures or practices, commensurate with the level of the risks

In addition, IITRI considered the concerns of interested organizations and citizens. IITRI studied recent testimony; examined material on Internet sites; and met with representatives of the American Civil Liberties Union, Electronic Privacy Information Center, and the Center for Democracy and Technology. IITRI determined that this report must also address

- All potential capabilities of the system, independent of intended use
- Controls on, and auditability of, the entire process by the FBI, the DoJ, and the courts
- Fault tolerance and integrity of the data
- Roles, actual and potential, of other parties and systems; e.g., the ISP or alternative implementations
- Functions of Carnivore within a suite of similar products

ES.2 SCOPE

IITRI determined that the scope of the evaluation had to include how Carnivore is applied as well as its technical capabilities. IITRI evaluated the understanding of court orders by the field investigator, the implementation of the court order as commands to the acquisition software, the acquisition minimization performed by the software, and the handling and post-processing of acquired data. Questions of constitutionality of Carnivore-type intercepts and trustworthiness of law enforcement agents were outside the scope of this evaluation.

The Carnivore IITRI evaluated is a snapshot of an on-going development. Carnivore is evolving to improve its performance, enhance its capabilities, and keep pace with Internet development

and court rulings. The current version (Carnivore 1.3.4 SP3) was deployed to meet an immediate requirement that commercial products could not satisfy while development continued. The next version, Carnivore 2.0, is in alpha test. Source code for v2.0 was provided to IITRI. This report covers an evaluation only of version 1.3.4.

ES.3 APPROACH

IITRI approached the evaluation in four coordinated, but largely independent, aspects.

1. IITRI evaluated the process used to translate court orders into commands for Carnivore, implement the collection, and verify that only permitted information was gathered. This aspect considered various use scenarios including full content and pen register intercepts. It included interviews with FBI developers, the deployment team, field agents who have used Carnivore, and ISPs who have hosted it.
2. IITRI evaluated the system architecture especially with respect to security. This aspect considered alternative implementations and the capabilities of commercial products.
3. IITRI examined the Carnivore source code to determine what functions have been implemented and what limitations have been built in.
4. IITRI installed the system in its Information Technology Laboratory (IT Lab) and experimentally determined system capabilities. Tests focused on capabilities of Carnivore, but included using two post-processing programs—Packeteer and CoolMiner—that, with Carnivore, are collectively known as the DragonWare suite.

ES.4 OBSERVATIONS

Carnivore is a system used to implement court-ordered surveillance of electronic communication. It is used when other implementations (e.g., having an ISP provide the requested data) do not meet the needs of the investigators or the restrictions placed by the court. Carnivore can be used to collect full content of communications under 18 U.S.C. §§ 2510-2522 and 50 U.S.C §§ 1801-1829 or only address information (i.e., pen register) under 18 U.S.C. §§ 3121-3127 and 50 U.S.C §§ 1841-1846. Law enforcement agents follow a rigorous, detailed procedure to obtain court orders and surveillance is performed under the supervision of the court issuing the order.

As in all technical surveillance, the FBI applies a strict separation of responsibility when using Carnivore. Case agents establish the need and justification for the surveillance. A separate team of technically trained agents installs the equipment and configures it to restrict collection to that allowed by the court order. In the case of Carnivore, all installations have been performed by the same small team. Case agents are motivated to solve or prevent crimes, but technically trained agents are motivated by FBI policy and procedures to ensure that collection adheres strictly to court orders and will be admissible in court as evidence.

The Carnivore architecture (Figure ES-1) comprises: (1) a one-way tap into an Ethernet data stream; (2) a general purpose computer to filter and collect data; (3) additional general purpose computers to control the collection and examine the data; and (4) a telephone link to the collection computer. The collection computer is typically installed without a keyboard or

monitor. pcAnywhere, a standard commercial product from Symantec Inc., allows the additional computers to control the collection computer via the telephone link. The link is protected by an electronic key such that only a computer with a matching key can connect. Carnivore software is typically loaded on the collection computer while Packeteer and CoolMiner are installed on the control computers. All computers are equipped with Jaz drives for removable data storage.

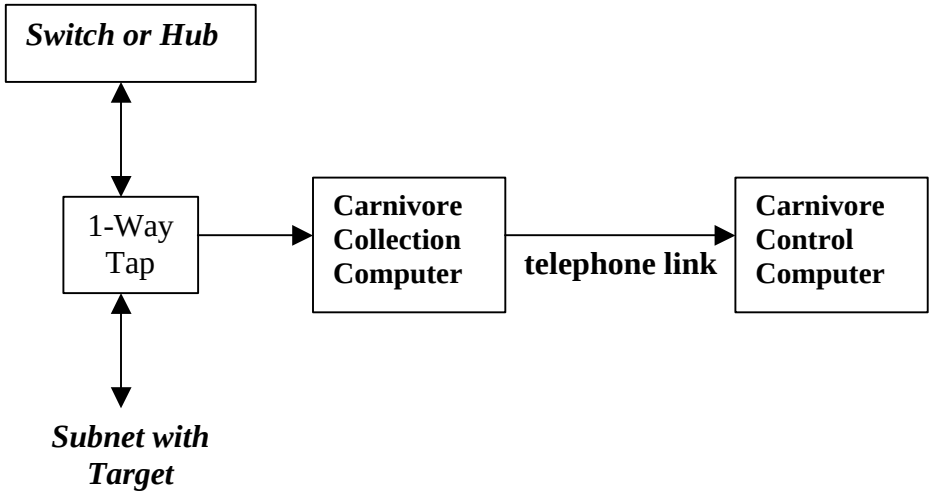

Figure ES-1. Carnivore Architecture

When placed at an ISP, the collection computer receives all packets on the Ethernet segment to which it is connected and records packets or packet segments that match Carnivore filter settings. The one-way tap ensures that Carnivore cannot transmit data on the network, and the absence of an installed Internet protocol (IP) stack ensures that Carnivore cannot process any packets other than to filter and optionally record them. Carnivore can neither alter packets destined for other systems on the network nor initiate any packets.

Control computers are located at law enforcement sites. When connected by modem to the collection computer, a control computer operator can set and change filter settings, start and stop collection, and retrieve collected information. Using Packeteer and CoolMiner, the operator can reconstruct target activity from the collected IP packets. In pen mode, the operator can see the TO and FROM e-mail addresses and the IP addresses of computers involved in File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) sessions. In full-collection mode, the operator can view the content of e-mail messages, HTTP pages, FTP sessions, etc. Carnivore operators are anonymous to the system. All users are logged in as “administrator” and no audit trail of actions is maintained.

Carnivore software has four components: (1) a driver derived from sample C source code provided with WinDis 32, a product of Printing Communications Associates implements preliminary filtering of IP packets; (2) an application program interface (API); (3) a dynamic link library (DLL) written in C++ provides additional filtering and data management; and (4) an executable program written in Visual Basic provides a graphical user interface. Functionality is placed in the driver whenever possible to enhance performance. Evolution of the source code between v1.3.4 and v2.0 clearly indicates that all processing will eventually take place in the

driver. The DLL provides entry points for functions such as INITIALIZE, START, STOP, and SHUTDOWN. The user interface is divided into basic (Figure ES-2) and advanced (Figure ES-3) screens. The basic screen allows an operator to start and stop collection, view collection statistics, and segment the output file. The advanced screen allows the operator to define and redefine the filter parameters that control what Carnivore collects.

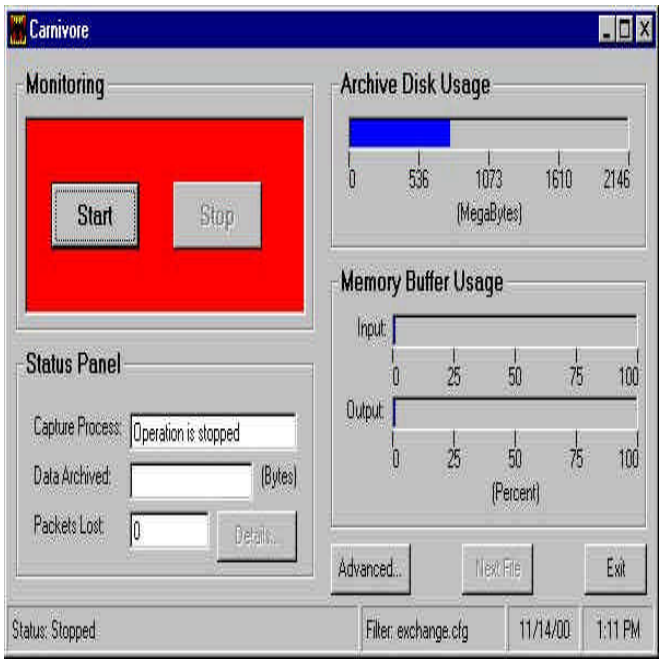

Figure ES-2. Basic Carnivore Screen

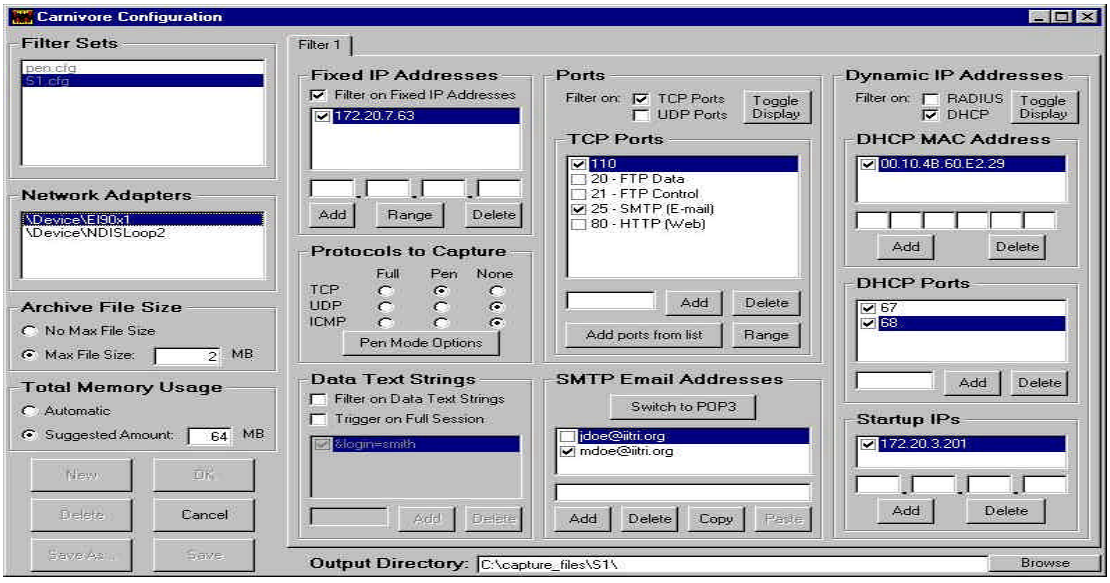

Figure ES-3. Advanced Carnivore Screen

IITRI verified by code walkthrough, and later by experiment, that Carnivore works as described by the DoJ. Parameters set in the user interface were reflected in the configuration file. Data passed by the filter and DLL reflect the configuration file. While IITRI did not perform an automated analysis to verify all code segments are executed and that no hidden code exists, IITRI did verify manually that the driver API and DLL entry points provide only the functionality required to implement the features we observed. Given that the advertised functionality provides ample capability to perform unauthorized surveillance, IITRI concluded there was little incentive to hide capabilities in the code.

IITRI installed Carnivore version 1.3.4 in its IT Lab. The test configuration, shown in Figure ES-4, mimics the typical installation at an ISP. The Carnivore tap was placed in a subnetwork containing traffic from the target, but as little other traffic as possible. The subnetwork provided both static and dynamic IP addressing of target and non-target users. IITRI ran a series of tests covering both pen register and full collection scenarios envisioned by the FBI developers. IITRI also ran a series of tests for scenarios not envisioned by the FBI to determine the full capabilities of the device.

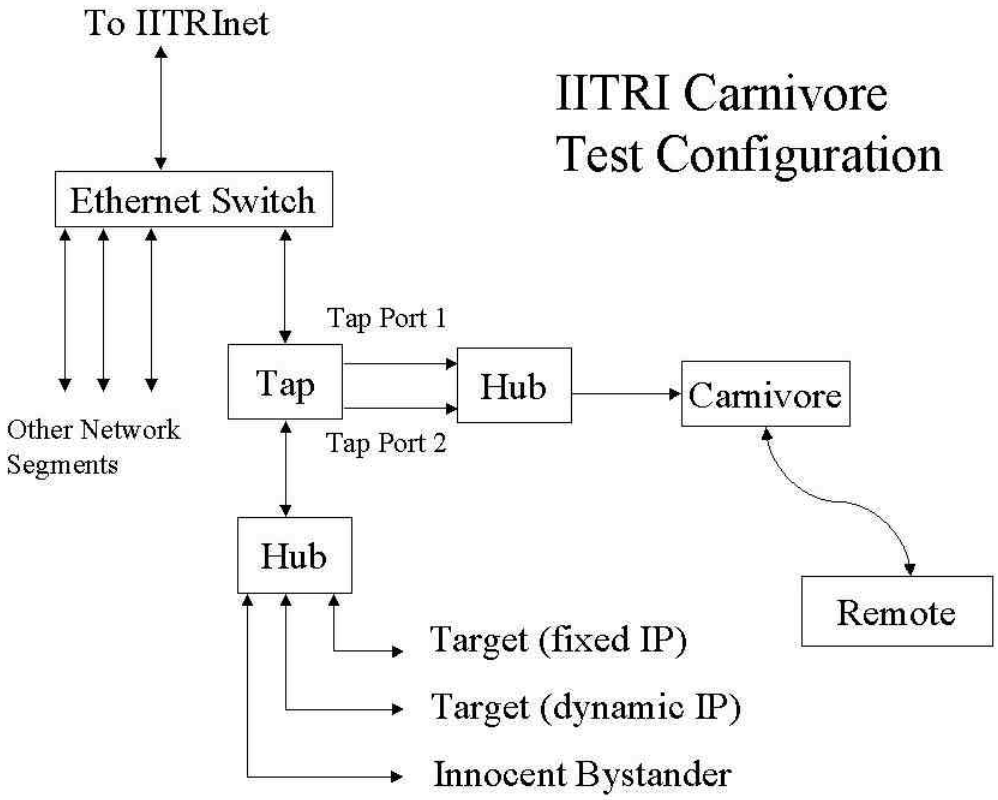

Figure ES-4. Carnivore Test Configuration

Carnivore accepts packets unless they are rejected by the filter. Proper operation relies on the ability of the operator to configure the filter correctly and fully. With the default settings, no packets are accepted. However, if a single radio button is selected to place the software in full mode collection for transmission control protocol (TCP) traffic, then all TCP traffic is collected.

As more filters are selected and configured, the volume of collection is reduced. For example, only selected ports might be collected and Simple Mail Transfer Protocol and Post Office Protocol 3 might be limited to certain user names. In normal operation, filters are also used to limit collection to specific IP addresses, but selecting the filters is established by FBI procedures, not by the software.

The other DragonWare components, Packeteer and CoolMiner, work together to display the output of Carnivore in a meaningful manner. Packeteer processes the raw output of Carnivore to reconstruct higher-level protocols from IP packets. CoolMiner develops statistical summaries and displays either pen register or full content information via an Internet browser. After initially verifying via hex-dumps that these programs were reporting the test output correctly, IITRI used them to evaluate the majority of the test scenarios. In cases where the CoolMiner output was not as expected, the raw data from Carnivore was inspected. A few software bugs were found in the Packeteer and CoolMiner programs. These bugs actually cause the collected data to be underreported. An examination of the raw Carnivore output revealed that the correct data were collected. These bugs have been reported to the FBI.

ES.5 CONCLUSIONS

In response to the DoJ's four questions, IITRI concludes

1. When Carnivore is used in accordance with a Title III order, it provides investigators with no more information than is permitted by a given court order. When Carnivore is used under pen trap authorization it collects TO and FROM information, and also indicates the length of messages and the length of individual field within those messages possibly exceeding court-permitted collection.
2. Operating Carnivore introduces no operational or security risks to the ISP network where it is installed unless the ISP must to make changes to its network to accommodate Carnivore. Such changes may introduce unexpected network behavior.
3. Carnivore reduces, but does not eliminate, risk of both intentional and unintentional unauthorized acquisition of electronic communication information by FBI personnel, but introduces little additional risk of acquisition by persons other than FBI personnel.
4. While operational procedures or practices appear sound, Carnivore does not provide protections, especially audit functions, commensurate with the level of the risks.

In response to broader concerns, IITRI concludes

- Carnivore represents technology that can be more effective in protecting privacy and enabling lawful surveillance than can alternatives such as commercial packet sniffers.
- Multiple approvals are currently required by FBI and DoJ policy (but not currently by statute) before a court order that might involve a Carnivore deployment is requested; significant post-collection organizational and judicial controls exist as well.
    - ◊ The supervising judge can, and regularly does, independently verify that traffic collected is only what was legally authorized.

- ◊ Civil litigation, and potential criminal prosecution of agents involved in over-collection provide further post-collection external controls protecting against misusing Carnivore. However, the statutory suppression remedy available for illegal interception of other communications in Title III is not expended to electronic communications.

- While the system was designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps. Incorrectly configured, Carnivore can record any traffic it monitors.
- Carnivore examines IP traffic and determines which packets are allowed by its filter settings.
  - ◊ It accumulates no data other than that which passes its filters
  - ◊ It restricts packets to specific types from or to specific users
  - ◊ It incorporates features to detect dropped packets and guards against inadvertently potentially missing the sign-off of a dynamically-assigned IP address
- Carnivore does not have nearly enough power "to spy on almost everyone with an e-mail account." In order to work effectively, it must reject the majority of packets it monitors. It also monitors only the packets traversing the wire to which it is connected. Typically, this wire is a network segment handling only a subset of a particular ISP's traffic.
- IITRI did not find adequate provisions (e.g., audit trails) for establishing individual accountability for actions taken during use of Carnivore.
- The current implementation of Carnivore has significant deficiencies in protection for the integrity of the information it collects.
  - ◊ The relationship among Carnivore filter settings, collected data, and other investigative activities may be difficult to establish.
  - ◊ Lack of physical control of the Carnivore collection computer engenders some risk of compromise
  - ◊ FBI tools to view, analyze, and minimize raw Carnivore output contain several material weaknesses. During testing, IITRI found several bugs.
  - ◊ Carnivore does not consistently recover from power failures.
  - ◊ There is no time synchronization within Carnivore.
- No formal development process was used for Carnivore through version 1.3.4. Consequently, technical issues such as software correctness, system robustness, user interfaces, audit, and accountability and security were not well addressed.
- Carnivore does not
  - ◊ Read and record all incoming and outgoing e-mail messages, including sender, recipients, message subject, and body. It stores packets for later analysis only after they are positively linked by the filter settings to a target

- ◊ Monitor the web-surfing and downloading habits of all the ISP's customers, including web searches for information or people. It can only record for later evaluation some HTTP files retrieved by a target
- ◊ Monitor or read all other electronic activity for that ISP, including instant messages , person-to-person file transfers, web publishing, FTP, Telnet, newsgroups, online purchases, and anything else that is routed through that ISP. It can only record a subset of such files for a specific user

- Carnivore cannot
  - ◊ Alter or remove packets from the network or introduce new packets
  - ◊ Block any traffic on the network
  - ◊ Remove images, terms, etc. from communications
  - ◊ Seize control of any portion of Internet traffic
  - ◊ Shut down or shut off the communications of any person, web site, company, or ISP
  - ◊ Shut off accounts, ISPs, etc. to "contain" an investigation
- Carnivore has significant performance limitations most of which result from design decisions to enable precise collection.
- The FBI may have legitimate reasons to oppose public release of Carnivore. The current version has technical limitations that could be exploited to defeat surveillance if they were revealed.

ES.6 RECOMMENDATIONS

Although IITRI specifically excluded questions of constitutionality and of illegal activity by the FBI from this evaluation, IITRI is concerned that the presence of Carnivore and its successors without safeguards as recommended below: (1) fuels the concerns of responsible privacy advocates and reduces the expectations of privacy by citizens at large; and (2) increases public concern about the potential unauthorized activity of law enforcement agents. To reduce these concerns IITRI makes the following recommendations to add protections that are commensurate with the level of risks inherent in deploying a system such as Carnivore:

- Continue to use Carnivore versus other techniques when precise collection is required because Carnivore can be configured to reflect the limitations of a court order.
- Retain centralized control of Carnivore at the federal level and require DoJ approval of all applications that involve Carnivore systems capable of full content collection.
- Provide separate versions of Carnivore for pen register and full content collection.
- Provide individual accountability and audit trail for all Carnivore actions.
- Enhance physical control of Carnivore when it is deployed.

- Explicitly bind collected data to the collection configuration by recording the filter settings with each collected file and add a cyclic redundancy check or, preferably, a cryptographic checksum to the recorded file.
- Employ a formal development processes to improve traceability of requirements, improve configuration management, and reduce potential errors in future versions of Carnivore.
- Provide checks in the user interface software to ensure that settings are reasonable and consistent.
- Work toward public release of Carnivore source code by eliminating exploitable weaknesses. Until public release, continue independent evaluation to assess effectiveness and risks of over- and under-collection. Fix known software bugs in Packeteer and CoolMiner, and make those programs available to other parties, e.g. defense attorneys, with a need to examine Carnivore data.

SECTION 1
INTRODUCTION

1.1 PURPOSE

Transfer of electronic information via the Internet has become as essential to business and personal communication as has transfer of voice via the telephone. The inherent privacy of such communications is a right of all Americans, but is also exploited by criminals, terrorists, and others who threaten personal safety and national security. Court-supervised interception of electronic communication can be a powerful tool for law enforcement agencies to counter such threats. Many citizens raise concerns, however, that electronic surveillance may itself become a threat to constitutional rights of privacy, free speech, and association.

The Federal Bureau of Investigation (FBI) has developed a tool, Carnivore, to facilitate interception of electronic communications. Carnivore is a software-based Internet Protocol (IP) packet sniffer that can select and record a defined subset of the traffic on the network to which it is attached. Packets can be selected based on IP address, protocol, or, in the case of e-mail, on the user names in the TO and FROM fields. In limited cases, packets can be selected based on their content. Packets can be recorded in their entirety (full mode) or recording can be limited to addressing information (pen mode), i.e., IP addresses and usernames. The FBI believes Carnivore allows them to limit the information they gather far more precisely than they can do with commercially-available tools or by requesting that an Internet Service Provider (ISP) perform the collection for them.

The FBI and Department of Justice (DoJ) have stated their belief that Carnivore is necessary to combat terrorism, espionage, information warfare, child pornography, serious fraud, and other felonies. They offer assurances the tool will not also facilitate deliberate or inadvertent interception of protected private communication. In the absence of detailed information about Carnivore, privacy advocates and other members of the public have raised legitimate concerns about the capabilities of Carnivore and its use by law enforcement agencies. Members of Congress, especially House Majority Leader Dick Armey, have questioned the development and use of such tools until concerns have been allayed, and Attorney General Janet Reno has stated

> "When we develop new technology, when we apply the Constitution, I want to make sure that we apply it in a consistent and balanced way."

The questions raised by the Government may be summarized as follows:

1. Does Carnivore encourage or inhibit consistent and balanced application of technology in constitutionally-allowed searches; i.e., does Carnivore represent technology that preserves or upsets the balance between privacy interests and law enforcement interests.
2. Are additional regulations for use of such tools needed?
3. Are concerns of privacy advocates legitimate?

To provide technical inputs to help these questions, the DoJ solicited academia and private industry to conduct an independent review of Carnivore. Eleven organizations responded, and IIT Research Institute (IITRI), with support from the IIT Chicago-Kent College of Law, was selected based on best technical proficiency, proposed inter-professional methodology, and schedule. While IITRI agreed to allow the DoJ to review the report before it is made public, IITRI also agreed to no prior constraints on the scope and methods of the evaluation, and secured DoJ agreement that IITRI could retain copies of the submitted report, even if the DoJ determines it to be sensitive. The principal motivation for this evaluation is concern within the Federal Government whether Carnivore is a necessary and appropriate tool for permissible electronic surveillance.

In conducting the evaluation of Carnivore, IITRI considered concerns voiced by many parties. However, there are two fundamental concerns IITRI felt it could not address: (1) the constitutionality of collection performed by Carnivore and (2) whether or not agents of the government can be trusted to follow established procedures. The evaluation reveals how Carnivore performs a court-authorized search; it cannot address whether such an authorization should be made. The evaluation also addresses whether weaknesses in the technology, implementation, and procedures associated with Carnivore might facilitate agent error or misbehavior. The concerns that are addressed are detailed in the following paragraphs.

1.1.1 TECHNICAL CONCERNS

In order to establish the technical scope of the evaluation, the DoJ solicited views from experts, in the technical community to identify areas that should be addressed. The following areas were identified by those experts:

1. The boundary of trust between Carnivore and Windows NT, RADIUS, ISPs, commercial products, etc.
2. Mapping of a court order to settings
   - ◊ Completeness in identifying the target (IP or IP and logon)
   - ◊ Ability to look at web mail
   - ◊ Ability to handle aliases
   - ◊ Synchronization and setting of clocks
3. Training of users
4. Auditability of
   - ◊ Access at multiple levels
   - ◊ Change control
   - ◊ Runtime configuration
   - ◊ Logs (NT or something special)
   - ◊ Audit reduction
5. Fault tolerance: resilience and recovery from power failure; corrupted files; etc.

6. Completeness—does it meet specifications
7. Configuration management of the system and other systems with which it interacts
8. General purpose machine on the network backbone
9. Isolation of device from the network
10. Integrity of data
    - ◊ Potential for user error
    - ◊ Access and unauthorized use by ISPs or others
    - ◊ Snooping of content
11. Exception testing
12. Scalability, ability to handle higher volume, and speed
13. Specification walk through
14. Look for hidden functionality
15. Capacity testing (speed, buffer overflow)
16. Test statement coverage (are all executed)
17. Bugs in
    - ◊ Packet and transmission control protocol (TCP)stream reassembly
    - ◊ Memory exhaustion and buffer overflow
    - ◊ Mail header parsing (legal, but odd use)
    - ◊ Domain Name Server name oddities
    - ◊ Uniform Resource Locator (URL) parsing
    - ◊ Multipurpose Internet Mail Extensions decode
18. Will local law enforcement have access
    - ◊ What are Attorney General guidelines
    - ◊ Are they properly trained

IITRI addressed these concerns within the time and resources provided by the DoJ contract.

1.1.2 CONCERN OF PRIVACY ADVOCATES

Privacy advocates from the American Civil Liberties Union, Electronic Freedom Foundation, Electronic Privacy Information Center, and Center for Democracy and Technology, among others, have made public statements, testified before Congress, and met directly with the DoJ to express their concerns about Carnivore. IITRI reviewed all available statements and assembled the following list of concerns paraphrased from the materials reviewed:

1. While the system, a sophisticated combination of hardware and proprietary software, can perform fine-tuned searches, it is also capable of broad sweeps, potentially enabling the FBI to monitor all of the network's communications.

2. "The FBI is placing a black box inside the computer network of an ISP. Not even the ISP knows exactly what that gizmo is doing."
3. Does Carnivore collect more than ordinary e-mail correspondence? Can it monitor all digital communications; for example, spy on online banking transactions?
4. Can Carnivore examine traffic and determine which parts are covered by the wiretap order.
5. Does the system restrict the monitored data to just some selected users?
   - ◊ Is the filtering done properly?
   - ◊ Can the configuration of the ISP cause Carnivore to collect the wrong data?
   - ◊ Does it have to accumulate other data in order to do this?
   - ◊ Is the recorded data protected against alteration?
   - ◊ What happens if Carnivore misses the sign-off of a dynamically-assigned IP address and continues collection?
6. An ISP (or a court) cannot independently verify that any particular installation has been configured to collect only the traffic for which it is legally authorized. What controls are in place?
7. The system includes no oversight of the information the FBI is capturing.
8. Can this software itself be attacked or subverted!
9. There are differences between circuit switched and packet switched network architectures such that laws applicable to one are not applicable to the other.
10. Pen register and full content collection capability mixed in one device.
11. Technical issues including the familiar (and tough) problems of software correctness, complex system robustness, user interfaces, audit, accountability, and security.
12. Surveillance of the Internet in this way leaves law enforcement with the potential to lower an individual's expectation of privacy as they use the Internet

1.1.3 CONCERNS EXPRESSED VIA INTERNET

Additional, more alarming concerns have been raised at a number of web sites (e.g., www.stopcarnivore.org). While many of these concerns should be allayed by reputable expert analyses (e.g., www.infowarrior.org) of FBI presentations on Carnivore and Freedom of Information Act (FOIA) releases by the DoJ, IITRI also considered the following concerns while conducting the evaluation:

1. Can Carnivore scan millions of e-mails per second, giving it unlimited power to spy on almost everyone with an e-mail account.
2. Can Carnivore
   - ◊ Read all incoming and outgoing e-mail messages, including sender, recipients, and message subject and body

- ◊ Monitor the web surfing and downloading habits of all the ISP's customers, including web searches for information or people
- ◊ Monitor or read all other electronic activity for that ISP, including instant messages, person-to-person file transfers, web publishing, File Transfer Protocol (FTP), Telnet, newsgroups, online purchases, and all other traffic that is routed through that ISP

3. Can Carnivore
   - ◊ Become a "valve" or "filter" through which almost all of the world's digital information will pass
   - ◊ Block the viewing of any images with certain suspicious filenames or block access to pornographic domains
   - ◊ Scan everyone's e-mail for drug references and monitor everyone's surfing to find "offending" sites
   - ◊ Seize control of any portion of Internet traffic
   - ◊ Shut off accounts, ISPs, or even cities or regions to "contain" whatever is being investigated
   - ◊ Literally remove "offensive" terms from communications
   - ◊ Become a virtual "big black marker" that can be used to block "dangerous" or "threatening" images
   - ◊ Widen the range, scope, and frequency of actions that some people view as violations of privacy
   - ◊ Shut down or shut off the communications of any one person, web site, company, or ISP
4. Is it possible, with Carnivore widely deployed, the FBI could
   - ◊ Ban by interception, deletion, or alteration any language or content found to be objectionable
   - ◊ Monitor the country's communications and target any person who was found or suspected to be a "problem," with the FBI acting as judge of who or what is a "problem"
   - ◊ Invoke mandatory standards for web sites, such as a rating system (like that used for movies), or lowering security standards (prohibiting encrypted messages and secure, private web sites)

1.2 OBJECTIVE

Motivated by a broad concern for privacy, the purpose of this report is to provide the information needed for any individual or organization to make an independent judgement about Carnivore. To this end, IITRI set two objectives: (1) answering the four specific questions posed by the DoJ in its Statement of Work and (2) conveying an understanding of the system and its use.

1.2.1 ADDRESS FOUR KEY QUESTIONS

IITRI is under contract to the DoJ to answer four questions. Does Carnivore

1. Provide investigators with all, but only, the information it is designed and set to provide in accordance with a given court order.
2. Introduce any new, material risks of operational or security impairment of an ISP's network.
3. Risk unauthorized acquisition, whether intentional or unintentional, of electronic communication information by
   - ◊ FBI personnel
   - ◊ Persons other than FBI personnel
4. Provide protections, including audit functions and operational procedures or practices, commensurate with the level of the risks.

1.2.2 CONVEY UNDERSTANDING OF THE SYSTEM

IITRI had to develop a thorough understanding of Carnivore, and the manner in which it is used by the FBI, to answer DoJ's four questions. IITRI had to determine what procedures are mandated by FBI and DoJ officials, determine the extent to which FBI agents and technicians understand those procedures and employ Carnivore to implement them, interview ISPs and others to verify the information supplied by the FBI, and examine the software source code and test Carnivore in IITRI's Information Technology Laboratory (IT Lab) to determine: (1) if it performs correctly when used as the FBI intends and (2) the full extent of its capabilities. If IITRI achieved its second objective, readers of this report will gain a similar understanding.

1.3 SCOPE

IITRI determined that the scope of the evaluation had to include how Carnivore is applied, as well as its technical capabilities. This concept is illustrated in Figure 1-1 where everything within the circle is within the scope of Carnivore and this evaluation. IITRI evaluated the understanding of court orders by the field investigator, the implementation of the court order as commands to the acquisition software, the acquisition minimization performed by the software, and the handling and post-processing of acquired data. Questions of constitutionality of Carnivore-type intercepts and trustworthiness of law enforcement agents were outside the scope of the evaluation.

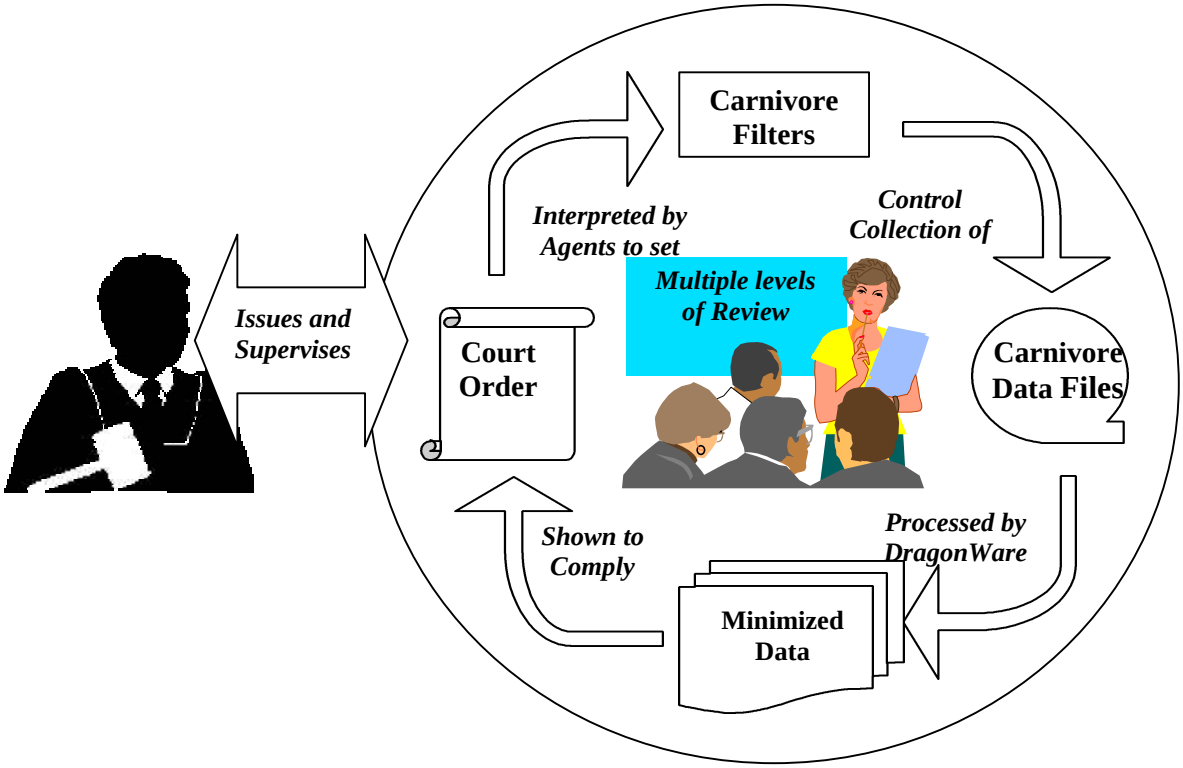

Figure 1-1. Scope of the Evaluation

SECTION 2
APPROACH

IITRI conducted a process-oriented evaluation of the legal, technical and human-based elements of Carnivore. Because IITRI was evaluating a snapshot of an on-going development and because the next release from that development is now in alpha testing, IITRI did not invest this project's limited resources in a systematic search for bugs in Carnivore version 1.3.4. Instead, IITRI focused on system-level issues that are likely to apply to future as well as current versions. Similarly, instead of analyzing a potentially unlimited universe of operational and host issues, IIITRI developed an objective categorization of the capabilities Carnivore brings to any environment.

IITRI approached the evaluation by first listing and prioritizing government, public, and its own concerns about Carnivore's operation and application. IITRI addressed as many of these concerns as possible within the available time and resources. To make best use of resources, IITRI divided the effort into four coordinated, but largely independent, aspect: (1) assess the process in which Carnivore is applied; (2) evaluate the system architecture including commercial-off-the-shelf (COTS) products; (3) examine the software source code; and (4) test Carnivore in the IITRI IT Lab. Each aspect addressed a different subset of concerns, but, in general, IITRI was able to address each concern from multiple viewpoints. The specific approaches to each aspect are described in the following paragraphs.

The FBI did everything possible to facilitate this evaluation. The Bureau provided Carnivore hardware and software for use at the IITRI facility. It made key personnel at the Engineering Research Facility and in field offices available as needed. It provided all documentation requested and volunteered additional documents that might be helpful. The FBI answered all questions promptly and completely. Timely completion of this evaluation would not have been possible without this level of cooperation.

2.1 PROCESS ASSESSMENT

IITRI evaluated the process used to translate court orders into commands for Carnivore, implement the collection of information, and then verify that only permitted information was gathered. This aspect considered various use scenarios including full content and pen register intercepts. It included interviews with FBI developers, the deployment team, field agents who have used Carnivore, and ISPs who have hosted it. IITRI also reviewed written FBI procedures to assess the organizational controls on using Carnivore and handling information collected by it.

FBI personnel from the Engineering Research Facility described the process for using Carnivore during initial technical meetings. IITRI subsequently verified those descriptions by reviewing Government Furnished Information (GFI) (see paragraph 2.2), interviewing field agents, and interviewing personnel from ISPs where Carnivore has been installed. Field agents who have used Carnivore were identified for IITRI by the Digital Intercept Technology Unit. IITRI interviewed case agents, who use Carnivore data in their investigations, and technically trained agents, who are the hands-on users of Carnivore. ISP personnel interviewed included the

manager of Internet services of a small ISP (identified for IITRI by the FBI) and the legal advisor, system administrator, and data center manager of a large ISP (contacted independently by IITRI).

2.2 ARCHITECTURE EVALUATION

IITRI evaluated the system architecture and COTS components, especially with respect to security. This aspect considered alternative implementations and the capabilities of potential Carnivore replacements or competitors from the commercial market. The architecture evaluation was based on presentations by the FBI, discussions with the FBI Carnivore deployment and development teams, examination of publicly-available information, and examination of the following sensitive GFI documents:

- Carnivore 1.3.4 System Requirements
- Carnivore 1.3.4 Test Plan
- Carnivore Use Case Specifications
- Carnivore Version 2.0 Vision Document
- FBI Data Intercept Training Manual
- Relevant portions of the FBI Manual of Investigative Operations and Guidelines (MIOG)
- Representative court orders
- Compact disk read-only memory with binaries and source code for Carnivore versions 1.3.4 and 2.0 alpha.

IITRI and the FBI conducted four technical meetings at the FBI Engineering Research Facility and the IITRI IT Lab. Participants included the IITRI technical evaluation and test team, the FBI project manager and deployment team, and the Carnivore and DragonWare developers. IITRI participated with the FBI in an installation of Carnivore in IITRI's IT Lab, received training on using Carnivore, and later independently reinstalled the system. IITRI had the opportunity to question the developers about design decisions and to understand the history and future of Carnivore development as well as the current system.

2.3 SOFTWARE SOURCE CODE EXAMINATION

IITRI examined the Carnivore source code to determine what functions have been implemented and what limitations have been built in. This examination was primarily a manual examination, although Rational Rose and some miscellaneous tools were applied, with limited results, as follows:

- IITRI used clc (C/C++ line-counter), a freeware tool written in Perl, to count noncomment lines of code. The count is somewhat subjective and for this report the numbers are rounded and reported as approximations.
- IITRI specifically described all file outputs that occur during normal operation of Carnivore. There are additional outputs to the screen that occur when Carnivore is run with debugging turned on. IITRI verified that none of these outputs provide additional detail about packet contents.

- IITRI used the reverse engineering capabilities of Rational Rose to generate a class diagram of Carnivore.dll, but the effort revealed only one relationship among the classes. The class CVoreFileFormat is derived from the abstract class CFileFormat. This relationship appears to reduce the effort required to revise the output file format (as has been done for Carnivore v2.0). Creating additional diagrams or determining additional relationships for the class diagram (if applicable) would have been an extensive manual effort and was beyond the scope and resources of this evaluation.

2.4 LABORATORY TEST

IITRI installed the system in its IT Lab and experimentally determined the system capabilities. These tests focused on capabilities of Carnivore but included use of two post-processing programs, Packeteer and CoolMiner, which, with Carnivore, are collectively known as the DragonWare suite. Carnivore is the main collection system; the tested version is 1.3.4 (SP3). Packeteer is a tool used to process the collected packets; the main purpose of this process is to put together all of the packets that belong to one session. The tested version is 1.2 (SP4). CoolMiner is a web browser tool that is used to analyze the packet data that Packeteer put together. The tested version is 1.2 (SP4).

As Carnivore filters IP packets, it normally considers only the next layer of protocols (i.e., TCP, User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP)). Reconstruction of higher level protocols (e.g., Post Office Protocol 3, Simple Mail Transfer Protocol, FTP, Hypertext Transfer Protocol (HTTP), etc.) is a function of Packeteer. Because IITRI was testing Carnivore and not Packeteer, it was able to use a very limited subset of protocols in its test scenarios and still evaluate all Carnivore functions.

IITRI created a special subnetwork within its existing office automation system to allow realistic testing in an environment similar to that used at ISPs (see Figure 2-1). A segment of the subnetwork containing desktop personal computers (PCs) with fixed IP addresses and a laptop PC that obtained its IP address dynamically were used in the test environment to generate end-user traffic during the period that Carnivore was collecting data. For most of the scenarios, a target was assigned to use either a fixed IP address desktop PC or a dynamic IP address laptop PC. Additional desktop computers are identified in Figure 2-1 as the “Innocent Bystanders.” Some of the test scenarios required multiple surveillance targets to test how a fixed IP address might behave differently than a dynamic IP address.

For stress and capacity tests, a mail server was placed on the subnetwork and a Perl script was written to generate a continuous stream of messages.

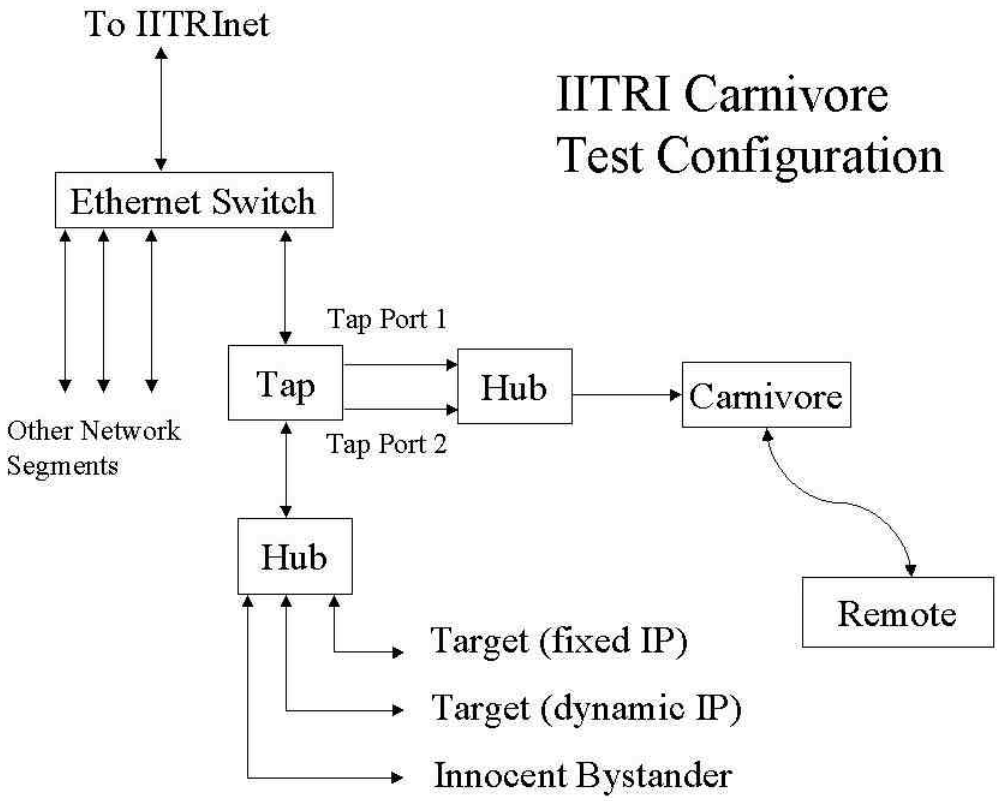

Figure 2-1. Test Configuration

SECTION 3
FINDINGS

This section reports findings from each of the four aspects of IITRI's evaluation. After describing the legal framework for electronic surveillance, it presents the process for using Carnivore and the controls placed on that process. Next it describes the Carnivore system and our detailed examination of the source code. Finally it summarizes laboratory tests of Carnivore. Details of the tests are presented in Appendix C.

3.1 THE LEGAL FRAMEWORK FOR ELECTRONIC SURVEILLANCE

Three statutory schemes provide the framework for the FBI's use of Carnivore. FBI agents may use Carnivore to intercept electronic information pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[i] pursuant to the Foreign Intelligence Surveillance Act,[ii] and pursuant to the pen-trap provisions in 18 U.S.C. §§ 3121-3124. Additional background is found in Appendix A.

3.1.1 TITLE III INTERCEPTS OF ELECTRONIC INFORMATION

Federal law enforcement investigators can only electronically intercept information under stringent requirements. The Omnibus Crime Control and Safe Streets Act governs electronic interception of wire and oral communication; it was amended in 1986 to include interception of electronic communication.

One restriction provides that only certain highly-placed officials in the DoJ—the Attorney General, Deputy Attorney General, Associate Attorney General, and certain others designated by the Attorney General—can authorize application for a wiretap via Carnivore or any other mechanism.[iii] This requirement ensures a measure of internal review and deliberation prior to any wiretap. Second, as a legal matter, wiretaps in the Carnivore context can only be used for a felony,[iv] and, as a practical matter, only for those felonies serious enough to warrant the resources.[v] Third, only an Article III judge or state court may grant the order.[vi] Fourth, law enforcement officials must demonstrate probable cause that a crime has been committed or is about to be committed, that normal investigative procedures have been tried and have not been sufficient, and that there is probable cause to believe that communications relevant to the investigation can be captured.[vii] Fifth, the wiretap order must contain the following: (1) the identity of the interceptee, if known; (2) the nature and location of the communications facilities to which the authority to intercept is granted; (3) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (4) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and (5) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall be automatically terminated when the described communication is first obtained.[viii] Sixth, every order must "minimize the interception of communication," including that the interception should not continue for "any period longer than is necessary to achieve the objective of the authorization, or in any event longer than thirty days."[ix] Law enforcement officers in the wiretap context typically

satisfy minimization obligations by turning off the equipment when content outside the scope of the Title III order is heard, and then turning the equipment back on periodically to determine if content within the scope of the order is occurring. The efficacy of minimization thus depends upon the judgment of the human listener. Carnivore provides minimization for intercepts of electronic communications automatically through its filters. Second-stage minimization occurs when the case agent reviews intercepted communications with DragonWare. Seventh, within 90 days after termination of the investigation, the supervising judge shall notify targets and certain other parties whose communications were intercepted of the fact of interception.[x]

Section 2518(7) permits circumvention of the above requirements in discrete circumstances. If a law enforcement official designated by the Attorney General determines that an emergency situation exists in which the national security is compromised or there is an "immediate danger of death or serious physical injury,"[xi] the interception can proceed with notice to the court within the next 48 hours.

3.1.2 PEN AND TRAP PROVISIONS

Pen registers and trap and trace devices (pen trap devices) record the numbers of incoming calls and outgoing telephone numbers dialed. The devices may be used by law enforcement agencies only pursuant to a court order, but the restrictions are less stringent than for wiretaps under Title III.[xii] Applications for pen trap orders may be made by any attorney for the Federal Government or by state investigative and law enforcement officers. No special authorization is required.[xiii] Any court of competent jurisdiction must issue a pen trap order if the court finds that the applicant has certified to the court that the information likely to be obtained through the device is "relevant to an ongoing criminal investigation."[xiv] Pen trap orders must specify the subscriber of the telephone line to which the pen trap device will be attached, the identity of any person who is the subject of a criminal investigation, the number and, if known, physical location of the telephone line to which the pen trap device is to be attached, and state the offense as to which the information likely to be obtained by the pen trap device relates.[xv] Pen trap orders may direct third parties to furnish information, facilities, and technical assistance necessary to accomplish installation of the pen trap device, extend for 60 days, and be renewed upon further judicial findings.[xvi] When FBI officials use Carnivore for purposes of capturing destination information of e-mail messages sent and origination information on e-mail messages received, they assert that they need only abide by this set of statutory restrictions rather than the more extensive set under Title III. However, the language in the pen trap provisions arguably does not clearly apply to electronic communication.

3.1.3 FOREIGN INTELLIGENCE SURVEILLANCE ACT

The Foreign Intelligence Surveillance Act (FISA) provides for electronic surveillance of foreign powers and agents of foreign powers in the United States for the purpose of obtaining foreign intelligence information. If no "United States person" likely will be overheard, then no court order is required, only certification by the Attorney General.[xvii]

If a United States person is involved, however, FISA requires an order issued by a special foreign intelligence surveillance court. A judge of the special court must approve the electronic surveillance if it is found that the requirements of the statute have been satisfied.[xviii] The order

must specify the identity or provide a description of the target of the electronic surveillance, the nature and location of each facility or place at which electronic surveillance will be directed, the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance, the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance, the period of time during which the electronic surveillance is approved, and, when more than one surveillance device is used under the order, the authorized coverage of each device and the minimization procedures to be applied.[xix] The order also must direct that the minimization procedures be followed and may direct third parties to furnish law enforcement authorities with necessary information, facilities, or technical assistance necessary to accomplish the electronic surveillance in a manner that will protect its secrecy and interfere minimally with the services of the subject of that order.[xx]

Applications for FISA orders may be made only with the approval of the Attorney General and upon a certification by the Assistant to the President for National Security Affairs, or other designated national security officials, that the information sought is foreign intelligence information and that such information cannot reasonably be obtained by normal investigative techniques.[xxi] Finally, foreign intelligence pen trap devices may be installed and used pursuant to orders by the special court or a specially designated United States Magistrate Judge and requires similar findings and directions.[xxii]

3.2 THE ELECTRONIC SURVEILLANCE PROCESS

3.2.1 THE DECISION TO USE CARNIVORE

A decision to use electronic eavesdropping comes only after a criminal investigation has proceeded substantially. This timing of the decision is true for a number of reasons. First, the FBI must demonstrate to the satisfaction of a judge probable cause that a crime has been committed or is about to be committed and that the surveillance is necessary to obtain relevant information. Even to obtain authorization for pen-trap surveillance, the FBI must show the relevance of the information sought. Second, the FBI in the electronic surveillance context must explain why traditional enforcement methods are insufficient to obtain the information desired. Third, in order to obtain a court order authorizing electronic eavesdropping, the FBI must amass significant details. For instance, the FBI must discover the identity of the target's ISP, the target's e-mail address, etc. Fourth, given the typical 4–6 month delay in receiving authorization for an electronic wiretap, FBI investigators are not likely to seek to deploy such means except in large ongoing investigations after substantial material has already been unearthed. Finally, use of electronic surveillance is expensive in terms of resources, making it much more likely that FBI agents will use electronic surveillance as a last resort.

If a case agent in the midst of a national security or criminal investigation determines that electronic surveillance may be needed, the agent contacts the Chief Division Counsel (CDC)[xxiii] and a Technically Trained Agent (TTA) in the field office for advice. The FBI separates responsibility for administration of technical surveillance from those pursuing leads in a criminal or national security investigation. That separation minimizes the chance that technical surveillance will be used prematurely. TTAs are experienced Special Agents who have been selected for advanced training. CDCs are familiar with the statutory requirements for eavesdropping. The TTA and CDC may counsel the Special Agent about what information might

ultimately be necessary should a court order be sought, whether it is information identifying the URL of a web site engaged in money laundering or a target's ISP. After continued consultation with the CDC and TTA, the case agent, with field office supervisory approval, may then determine that electronic surveillance is required. These procedures are formalized in the MIOG,[xxiv] and evidently have been consistently followed. In the case of electronic wiretapping for content, the case agent must clear the application with superiors within the field office, with FBI Headquarters, and then with the DoJ.[xxv] This chain of command has been formalized.

The procedures to obtain authorization for a pen-trap surveillance are less rigorous. The case agent must justify in writing the need for pen-trap surveillance rather than more conventional investigative techniques. This justification, initialed by a supervisor, is placed in the case file and pen-register control file.[xxvi] The division counsel may be consulted on application language and the TTA must be consulted regarding availability of equipment.[xxvii]

The application for a court order in either context is authored by FBI attorneys in conjunction with those at DoJ (or the U.S. Attorney's Office if the objective is a pen-trap) based on information furnished by the case agent. Advice on the language in the application is widely sought and received from each level in the review process.

The court determines in both sets of circumstances (electronic monitoring or pen trap) whether to grant the application *ex parte*. If satisfied that the Title III requirements have been met, the court typically issues two orders: one authorizing the intercept and the second directing the relevant ISP to cooperate in the venture. The second order usually contains less information than the first, omitting, for example, the purpose of the investigation and sometimes the name of the target.

3.2.2 DEPLOYMENT OF CARNIVORE

In discussions with the ISP, the TTA and Special Agent determine how best to ensure implementation. The ISP may have means available to obtain the target information narrowly and precisely. For instance, if all the information sought can be obtained by setting up a clone e-mail account, most ISPs can comply. Problems, however, may exist if the ISP lacks the technology to narrow sufficiently the information retrieved to comply with the court order, or conversely, if it cannot retrieve sufficient information. (At times, the FBI also is concerned about disclosing too much information to the ISP, as in a sensitive national security investigation.) If the ISP cannot comply fully with the court order, then application of Carnivore represents the first stage of minimization, as described elsewhere. Carnivore limits the information retrieved to that specified in the court order. The TTA engages in discussions with ISP representatives to explain the functionality of Carnivore and assure the integrity of the ISP's network.

If Carnivore is selected as the most appropriate means of complying with the court order, the TTA assumes responsibility for its deployment. Given that use of Carnivore has been limited, highly trained personnel from FBI Headquarters have, so far, played a critical role in the implementation process, although there is no procedural requirement for their participation. The TTAs—with or without help from headquarters—then configure the system according to the specifications in the court order.

If the order, for instance, specifies intercepting e-mail to and from adam@mailserve.com, an agent must enter that e-mail address into the appropriate field of the Carnivore input screen. If the order specifies intercepting all traffic between port 25 of a specific Internet server and an IP address assigned to a particular target, the agent must enter the appropriate alphanumeric string into the appropriate field in the input screen for Carnivore to specify the server and port 25; and also enter the appropriate values to specify—or to allow the hardware and software to determine—the IP address assigned to the target in a particular session by Dynamic Host Configuration Protocol (DHCP) or RADIUS. The mapping is usually straightforward, although IITRI learned of one case in which the FBI requested the U.S. Attorney to obtain a new Title III order to eliminate ambiguities. The configurations programmed can be retrieved later to ensure compliance with the court order. Nonetheless, the potential for human error cannot be discounted—agents must program Carnivore to match the potentially ambiguous information in the court order.

The work area at the ISP is secured, and substantial precautions are taken to ensure that no ISP staff members have access to the unit. Precautions are taken so that no one in the area can manipulate the hardware to see the data as it is retrieved. If individuals, despite the precautions, could access the information released by Carnivore, they could reassemble it using readily available software to reveal its contents. Under FBI practice, the TTA does not receive any of the information retrieved via Carnivore. These procedures again are not formalized, but security is important to ensure that the chain of custody is not broken. Currently, all Carnivore units are maintained at FBI Headquarters and returned there after a session has been completed.

3.2.3 ANALYSIS OF THE INFORMATION RETRIEVED BY CARNIVORE

The information retrieved can be reassembled by the case agent using specially designed software called CoolMiner and Packeteer, collectively known as DragonWare. The case agent can obtain the intercepted information remotely as it is received by Carnivore, or can await until the information is retrieved on the Jaz disk in the computer.

The case agent (or possibly another agent training in minimization) carries out a second round of minimization. On a PC on which DragonWare is installed, the agent determines which information is relevant and which is not. The irrelevant information is deleted immediately and no copies are kept. The relevant information becomes part of the working papers of the investigation. There are no checks of which IITRI is aware to monitor the extent of this second minimization. The original disk, i.e. the results of the first Carnivore minimization with information not reassembled, is sealed and stored. The disk is not tamper-proof. None of the information in the original disk is entered into a database. Pursuant to Title III, the court at the conclusion of the investigation must notify any target of the electronic search—and apparently at its discretion any other individual whose communications were frequently intercepted during the Carnivore session—about the fact of interception. The judge who authorized the interception retains jurisdiction over the intercept and often monitors in a general way the conduct of the surveillance.

Finally, if the information obtained has been encrypted, the case agent must determine whether to apply decryption techniques to the encrypted messages received. Carnivore itself has no power

to decrypt. Thus, depending upon the perceived importance of the information, the case agent may contact FBI headquarters for help in decrypting the information retrieved by Carnivore.

3.3 EXTERNAL AND INTERNAL CHECKS ON THE PROCESS

There are numerous external and internal checks overseeing federal law enforcement authorities' use of Carnivore. Outside the law enforcement agency, both judges and Congress monitor implementation of electronic surveillance. Within the agency, there are checks of intensive training for personnel, structural separation between technical and case agents, and inspections. These checks taken together reduce the possibility that Carnivore will be abused.

3.3.1 EXTERNAL CHECKS

3.3.1.1 JUDICIAL OVERSIGHT

Judges are involved in the Carnivore process throughout. They discharge a critical function at the court-order stage, monitor minimization, and, duration during the surveillance, exercise oversight of record keeping and provide notice to targets after the investigation has completed.

As an initial matter, only Article III judges can authorize Title III and FISA intercepts.[xxviii] This requirement, unlike in the conventional warrant or pen-trap contexts, limits the number of judicial officials who can approve intercept orders. Also, Article III judges are more immune from political pressures because of their job tenure and protection from salary diminution.

Moreover, before law enforcement agencies can obtain authorization for a Title III intercept from the court, they must submit substantial information to the supervising judge. The judge must be satisfied that the FBI has demonstrated probable cause that a crime has been committed, that the information sought cannot be determined in any conventional manner, and that probable cause exists to believe that relevant information will be retrieved by the intercept. The court also ensures that efforts at minimization have taken place. After the interception has started, the court often spot-checks minimization, ensures that the interception does not continue longer than is necessary, and that the information obtained is sealed. At the conclusion of the investigation, the court also determines which parties to notify of the fact of interception. The notification increases the chance that those subject to surveillance will mount a legal challenge to the propriety of the investigation, as mentioned below. Judicial involvement is pervasive, and minimizes the risk that electronic surveillance will be unnecessary, overbroad, or too lengthy.[xxix] Similar protections exist in the FISA context.

3.3.1.2 CRIMINAL AND CIVIL SANCTIONS

Congress also has exerted significant control over the electronic surveillance process by providing for civil and criminal sanctions. Under Title III, any person whose electronic communication is wrongfully intercepted can recover actual damages, punitive damages (in appropriate cases), and attorney fees.[xxx] Even if actual damages cannot be shown, statutory damages for the greater of $100 per day or $10,000 can be recovered.[xxxi] The interceptor can block the suit by showing good faith reliance on a court order or statutory authorization. Criminal penalties are imposed on any individual who intentionally intercepts wire

communications without authorization or discloses the contents having reason to know that the information was obtained through an illegal interception under 18 U.S.C. § 2511. Defendants can include law enforcement officials who abuse their authority to intercept electronic communications or divulge their contents. Under FISA, as well, individuals are guilty of an offense if they engage in unauthorized electronic surveillance or disclose information having reason to know that the information was obtained in an unauthorized manner.[xxxii] A defense is provided if a court order sanctioned the interception or disclosure.[xxxiii] Finally, anyone knowingly violating the restrictions on pen devices can be fined, imprisoned for not more than one year, or fined and imprisoned.[xxxiv] In short, Congress provided for deterrence of misconduct by creating a civil remedy in the electronic communication and FISA contexts and criminal sanctions in all three contexts.[xxxv]

3.3.1.3 APPLICABILITY OF EXCLUSIONARY RULE

FISA provides for suppressing any evidence illegally obtained through either electronic intercepts or pen-trap devices.[xxxvi] The exclusionary remedy provides a deterrent against over broad or vindictive surveillance. In contrast, the electronic communications and pen register schemes do not provide for exclusion of evidence in a criminal trial if the procedures of the governing statutes are violated. Although Title III does include an exclusionary rule for interception of wire and oral communication,[xxxvii] no comparable rule is included for interception of electronic communication.[xxxviii] Defendants in criminal trials can move to suppress the electronic communication on the ground that they were subject to an unreasonable search or seizure within the meaning of the Fourth Amendment,[xxxix] but cannot rely on any procedural violation of the statute itself. Note, however, that the availability of an exclusionary rule does not offer direct protection for those not suspected of criminal or foreign intelligence activity who may be caught within the web of surveillance.

3.3.1.4 REPORTING REQUIREMENT

Congress also exercises control by imposing reporting requirements. Under 18 U.S.C. § 2519, the supervising judge of electronic intercepts pursuant to Title III must report to the Administrative Office of the United States the fact and type of intercept order requested and granted or denied. Moreover, the Attorney General must independently report the same information in the aggregate each year to the Administrative Office. Under the pen trap provisions, the Attorney General annually reports to Congress on the number of pen register orders and trap and trace devices applied for each year, the specified offences under investigation, and the identity and district of the applicant agency.[xl] Under FISA, the Attorney General must transmit to the Administrative Office each year a report of the total number of applications made for orders and extension of orders and the total numbers of such orders and extensions granted.[xli] Congress has also required the Attorney General to report to congressional committees, on a semiannual basis, the extent of its electronic surveillance activities under FISA. These extensive reporting requirements permit Congress more information with which to assess the efficacy of the surveillance systems. Although to a lesser extent than the criminal and civil sanctions discussed above, the reporting provisions add some deterrence to misconduct.

The FBI's conduct of electronic surveillance is not unchecked. Both courts and Congress exercise significant oversight responsibility, lessening the possibility that law enforcement officials will use Carnivore in an unauthorized or careless manner.

3.3.2 INTERNAL CHECKS

In addition to the external checks, the FBI has itself placed many checks on the conduct of electronic surveillance. These internal checks further minimize the chance for abuse.

3.3.2.1 THE NEED FOR APPROVAL FROM SUPERIORS

Only certain authorized attorneys of the United States can approve a request for a Title III intercept, ensuring a measure of internal scrutiny and deliberation. With respect to electronic communication,[xlii] only the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or several others specially designated by the Attorney General may authorize application for an electronic intercept.[xliii] With respect to FISA, only the Attorney General can authorize the intercept. This centralized authority prevents widely dispersed law enforcement officials from making the intercept decision on their own volition.[xliv]

3.3.2.2 TRAINING AND STRUCTURAL SEPARATION OF CASE AGENTS FROM TECHNICAL AGENTS

Electronic surveillance cannot be conducted under FBI procedures without the involvement of Technical Advisors (TAs), TTAs, and the Electronic Surveillance Technology Section of the Laboratory Division.

TAs and TTAs are assigned to field offices. The TA is a TTA assigned to the Special Agent in Charge of a field office to advise on all aspects of electronic surveillance. "The TA must be actively involved in all office management decisions concerning the application of technical investigative techniques."[xlv] The TA monitors the conduct of the TTAs.

TTAs are experienced agent investigators with a minimum of two years experience who have applied and been selected for TTA training and certification. TTA candidates complete one year of on-the-job training under the supervision of the TA, followed by formal training at the FBI's Engineering Research Facility on basic electronics, computer and networking technology, basic architecture of telephone networks, switch-based intercepts, and data intercepts. To be designated a TTA, candidates must pass all examinations and practical problems, after which they are assigned as TTAs to a field office.[xlvi] In order to maintain their certification, TTAs must spend at least 20 percent of their time on technical investigative support matters and attend technical in-service training. TTAs may never be used as monitoring agents of court-ordered intercepts.[xlvii]

"All technical equipment in the field office is under the care, custody and control of the TA."[xlviii] "Technical equipment can only be sent from FBI Headquarters to the TA. Technical equipment is never sent to Special Agents who are not TTAs."[xlix] The TA maintains a control system for equipment accountability. No part or function of any equipment may be altered without specific FBI headquarters authorization.[l]

The TTA is responsible for ensuring that proper authority has been obtained for technical equipment use and for maintaining a file which contains the documented authority (court orders, Special Agent in Charge or supervisory approval). TTAs may not permit the use of technical equipment until such court order or other authority has been seen or orally verified from supervisory personnel. Such oral verification must be documented and maintained in the file with the court orders.[li] In short, both the training and separation of personnel into case and technical groupings minimize the chance that the Carnivore power will be abused.

3.3.2.3 INTERNAL DISCIPLINE

Finally, law enforcement agents sometimes face discipline within their agencies for arbitrary or excessive searches. Many field offices have established internal mechanisms to oversee conduct of case agents. Offices may recognize that illegal searches can be counterproductive and jeopardize the agency's reputation in the public eye. In addition, FBI senior officials from FBI headquarters periodically inspect the practices of each field office. Such inspections commonly focus on the practices and procedures used in electronic surveillance.

3.3.3 OVERALL EFFECTIVENESS OF CONTROLS

IITRI found that the current system of external and internal controls makes it unlikely that either FBI or ISP personnel will use Carnivore carelessly or for improper purposes. However, maintaining central control and the requirement of headquarters approval are critical to maintaining effective operational controls.

With respect to current uses of Carnivore by federal law enforcement agencies, centralization of the Carnivore process—authorization, storage, and deployment—should be effective to ensure that Carnivore is not used for unauthorized surveillance. A small group of highly skilled FBI agents must not only approve applications of Carnivore, but are also intimately involved in the logistics. Their training and professionalism ensure that the intercept proceeds as narrowly and efficiently as possible. After-the-fact investigations by officials from FBI Headquarters and the DoJ further minimize the risk of over-collection or tampering. Moreover, the availability of criminal sanctions, civil sanctions, and judicial questioning throughout the process limits the potential that any abuse, whether intentional or negligent, will occur. Although the potential for abuse by case agents exists and should be minimized, the likelihood of such misfeasance is low.

The risk of misfeasance may increase significantly, however, if Carnivore becomes more widely used. The governing statute, by itself, permits expanded use of Carnivore, but does not require that the Carnivore units be centrally stored; does not require FBI Headquarters approval for court authorization of a Carnivore intercept; and does not limit use of Carnivore to federal agents. Thus, although use of Carnivore in practice has been centralized, nothing in the statute prohibits state and local law enforcement agents from using Carnivore or local Assistant U.S. Attorneys on their own initiative from applying for court authorization to use the device. Finally, when Carnivore is being deployed in a pen trap mode, the statute permits localized decision making as to when to seek authorization; application need only be presented to any court of competent jurisdiction.

With respect to the ISPs, it is extremely unlikely that ISP personnel will interfere with the FBI's collection of the court-authorized material. ISP personnel face serious criminal and civil sanctions stemming from unauthorized interception and face additional criminal penalties for interference with a FBI investigation. Moreover, the Carnivore setup is isolated from other ISP activities and ISP personnel would have to take a number of overt steps to interfere or divert the Carnivore interception. In cases where the risk or consequences of interference are significant, additional access controls and antitamper seals can and have been used.

In addition, ISP employees should have little incentive to use a Carnivore interception to further their own snooping, since almost all ISPs have packet sniffers available that they use for monitoring purposes; that software can currently be used for unlawful ends.

3.4 SYSTEM ARCHITECTURE

Carnivore selects and records IP packets from an Ethernet data stream. Carnivore does not assemble packets into higher level protocols. In fact, no IP protocol stack is installed. The packets are treated strictly as data. They are subject to a series of tests looking for specific patterns. Success or failure of the tests determines which packets are selected and recorded. Additional software must be employed to reconstruct higher level protocols.

The Carnivore system architecture comprises: (1) a one-way tap into an Ethernet data steam; (2) a general purpose computer to filter and collect data; (3) one or more additional general-purpose computers to control the collection and examine the data; (4) a telephone link to connect the additional computer(s) to the collection computer; and (5) Carnivore software. Carnivore software is a component of a software suite called DragonWare written by the FBI. The other components of Dragonware are Packeteer and CoolMiner, two additional programs that reconstruct e-mail and other Internet traffic from the collected packets.

3.4.1 THE ETHERNET TAP

Carnivore is connected to a 10/100Base-T Ethernet using a Century Tap made by Shomiti Systems, Inc. (http://www.shomiti.com/products/tapfamily.html). In a typical installation (see Figure 3-1), an existing line is disconnected from a hub or switch and plugged into port A of the tap. A new line is run from port B to the hub/switch. The tap passes the traffic along the line from A to B and from B to A as if it were a standard cable. At the same time, it takes a copy of the transmit data in each direction and feeds it to ports 1 and 2.

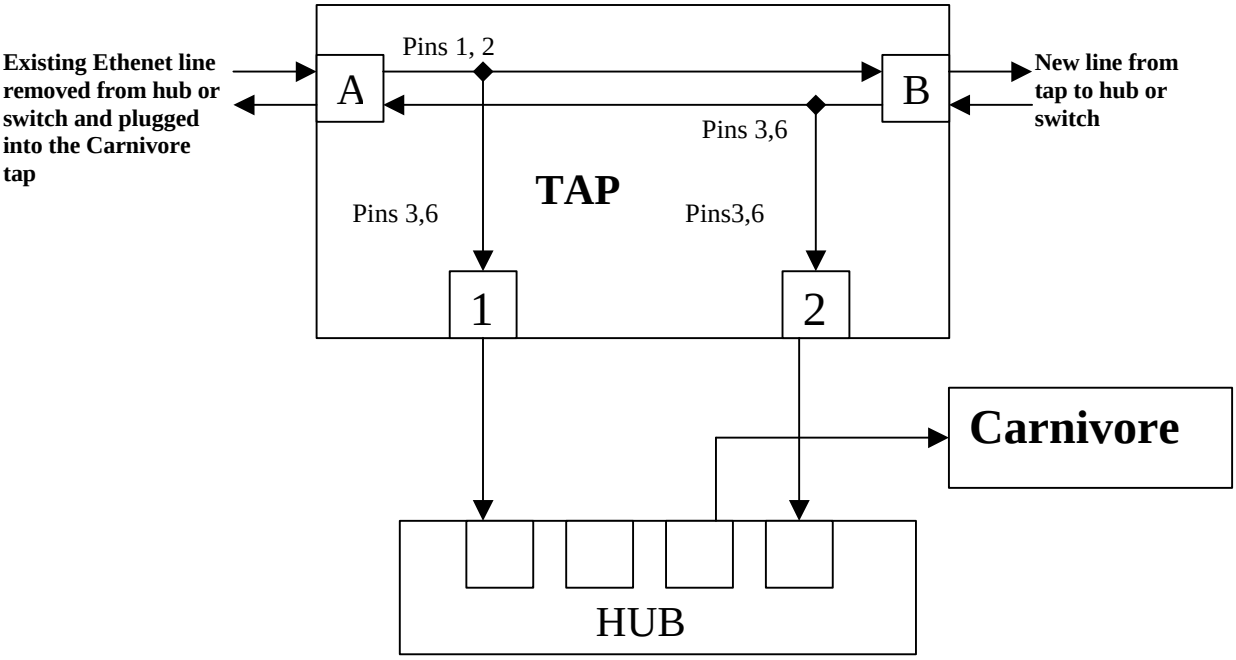

Figure 3-1. Pinouts for Century Tap

Additional cables connect ports 1 and 2 to a standard hub. The cable used to connect port 2 to the hub must either be a cross-connect cable, or connect to the uplink port of the hub. This connection ensures that both sides of the communication on the Ethernet appear at the hub, but no data can be sent from the hub. The Carnivore system is then connected to any open port on the hub. This cabling arrangement and the Shomiti tap ensure Carnivore is in a receive-only mode. The transmission lines from the Ethernet adapter are not connected to anything inside the tap. The tap has a latency of only 1 bit time at 100 Mbps, so network performance should not be affected.

This configuration works only for standard Ethernet. If full-duplex Ethernet is used in this configuration, there could be collisions at the hub that combine the tap outputs that are not present on the actual Ethernet being tapped. These collisions could cause Carnivore to lose packets. Post-collection analysis allows packet loss to be detected. However, it is conceivable that Carnivore could miss a DHCP or RADIUS tear-down and collect packets from another user. This condition would be detected during the second stage of minimization (see paragraph 3.2.3). Collisions can be minimized by installing the tap in the smallest bandwidth pipe possible that ensures gathering the traffic of the individual for whom the court order was obtained (see paragraph 3.4.6, Operational Considerations).

3.4.2 COMPUTERS

Carnivore employs a generic Pentium-class PC, with a generic 10/100 Mbps Ethernet adapter. The adapter is set to promiscuous mode and acquires all the traffic that comes across the network to which it is connected via a read-only tap. As each packet is acquired, Carnivore software tests it against filter settings selected using graphical user interface (GUI) controls. Packets that pass

through the filters are saved to a removable Jaz disk. The data that do not meet the filter criteria are discarded without being saved to any disk.

The Jaz drive is located behind a key-lockable panel on the Carnivore box. While this panel is not tamperproof, it does provide a degree of control over who can remove the Jaz disk from the computer. Only FBI personnel have the keys to the lock. When the Jaz disk is removed, it is placed in a container that is sealed and then taken to the judge that granted the court order permitting the collection. The Jaz disks contain all the information collected by Carnivore prior to the second round of minimization (see 3.2.3).

There is no time synchronization among Carnivore computers. All time stamps are based on the local system clock. Coordination of times relies on the various system clocks having been synchronized prior to the start of collection and operating correctly during collection.

3.4.3 TELEPHONE LINK

The collection computer is installed without a keyboard or monitor and, in operational use, Carnivore might not be physically accessible to case agents. However, each Carnivore computer is equipped with an off-the-shelf 56-kbps modem allowing it to communicate via a standard analog telephone link.

Once Carnivore has been installed at the ISP, it is normally controlled remotely. The Carnivore collection computer modem is connected to a dedicated analog voice line installed especially for the Carnivore deployment. It does not use one of the modems from the ISP's modem pool, nor is it controllable via the Internet. pcAnywhere, a standard commercial product from Symantec Inc., is installed on the collection computer to allow one of the additional computers to control the collection computer via the telephone link. pcAnywhere is run as a service. If the collection computer loses power and reboots when power is restored, pcAnywhere starts automatically; the FBI does not need to visit the ISP, nor do ISP personnel have to access Carnivore. pcAnywhere is set up to use pcAnywhere Identification and Authentication, with each person using the collection computer having a separate identification (ID) and password. pcAnywhere is also set to use symmetric encryption to protect the data transfer. It is important to note that the Symmetric mode is not the same as classical symmetric encryption. There is a public-key component involved in setting up the symmetric key. More details on this mode can be found in a Symantec white paper[lii]. The host pcAnywhere software is set to start all connections with the screen locked.

In addition to the pcAnywhere ID and password, the telephone line is protected by an electronic key; only a computer with a matching key can connect. The keys are COTS Challenger Security Products (CSP) from Computer Peripheral Systems, Inc. (CPSI), which have demonstrated capability to protect the link from sustained attempts at penetration. IITRI contacted CPSI to determine how many possible combinations of Lock and Key were possible. CSPI replied that the CSP is a random number generator that expands the base system code, which is different in each secure system. This code, along with other variables, changes with each call. The result is about one billion possible combinations. Each time a CSP lock is called, it issues a different challenge. The corresponding key is expected to accept the challenge and, through one of its many algorithms, use the modified base code and other variables to reply properly.

Carnivore takes many steps to protect the link between computers. A case agent controlling the Carnivore collection computer from an external computer must know the correct telephone number and have an appropriately-keyed CSP device, pcAnywhere software, a valid user name and password, and the Administrator password for the Carnivore collection box. Once connected, the agent can use Carnivore as if the agent were physically at the Carnivore collection box; starting or stopping collection and downloading collected data. An additional password is required to access the advanced setup features and change the filter settings. Data are downloaded by using the file transfer features of pcAnywhere. Files can also be uploaded to the collection computer using the same features, though there is no operational reason to do so. pcAnywhere Symmetric mode encryption is sufficient to protect against passive wiretap, but not against a person-in-the-middle attack. The CPSI Challenger device prevents the person-in-the-middle attack.

3.4.4 CARNIVORE SOFTWARE PROGRAM

Carnivore is the name of the software program running on the collection computer that filters and records IP packets. When the collection computer is started, it automatically logs in as the Administrator. The Carnivore program is in the start-up group for the Administrator, so it also starts automatically. If the Carnivore program was collecting when the system was last shut down, it will begin collecting again automatically. This automatic reboot feature was set up so that data lost because of a power failure would be held to a minimum.

Carnivore has two levels of functionality: a main screen and an advanced screen. When the program is started, the agent sees the main screen (Figure 3-2) with four functions implemented via button selections. One set of buttons starts and stops collection. Another toggles the collection details display. A third forces collection to start using a new file, making the current file available for downloading. The fourth is used to access the advanced screen (filter settings). The program has a separate password for accessing the filter settings. A case agent can access the collection device via remote dial-in to start and stop collection, cause the collection to start into a new file, and download the collected data. However, that agent does not need to know the password that allows the filter settings to be changed.

IITRI discovered that the password to the advanced screen is compiled into the source code. Apparently, a password is selected and implemented for each Carnivore deployment. There is no mechanism in Carnivore software to change the password. However, IITRI was able to use a Hex Editor to find and change the current advanced password.

The Carnivore advanced menu (Figure 3-3) allows a precise description of the parameters of the data to be collected. Packets can be filtered on IP address, protocol, text strings, port, and e-mail address. IP address filtering can be based on either fixed or dynamically assigned addresses. If IP filtering is not turned on, all packets that pass the other filters are collected regardless of what IP address those packets may have. The advanced menu also allows the operator to save and recall filter settings, to specify the location of the output files, and specify the maximum file size of each output file.

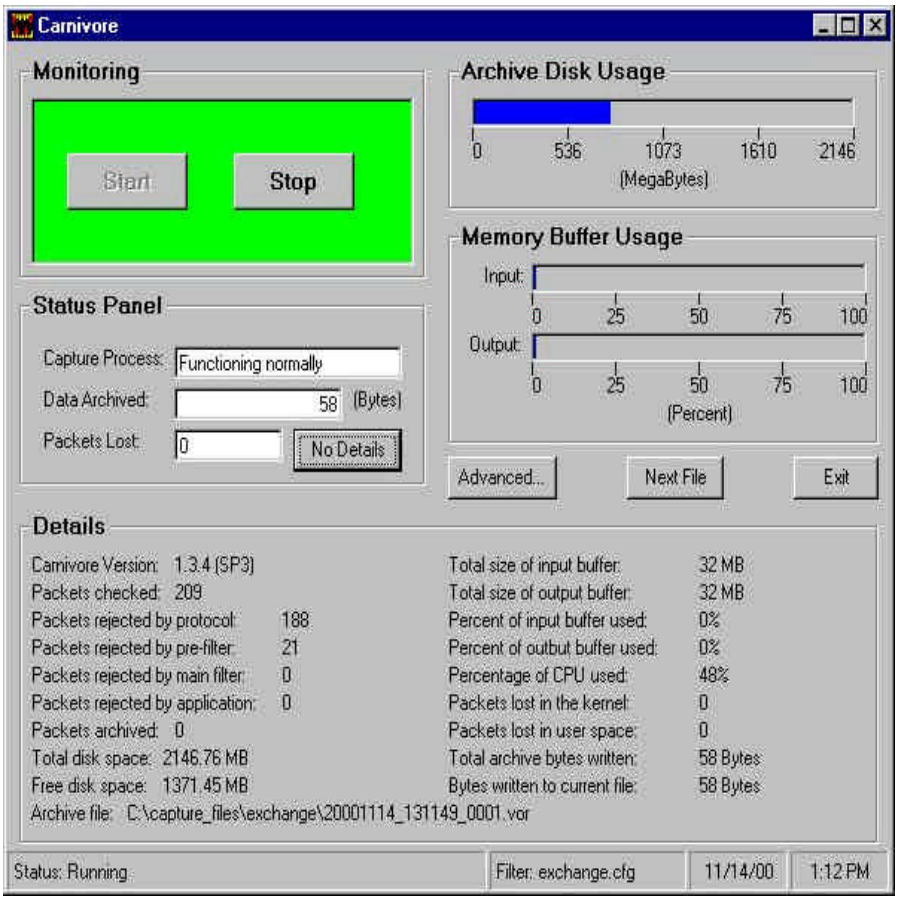

Figure 3-2. Carnivore Main Screen

3.4.4.1 FILTERING

3.4.4.1.1 FIXED IP FILTERING

The simplest form of collection is one based on a fixed IP address. If the subject is using a computer that has a fixed IP address, (One clause redacted by the DOJ), this feature can be used. On the advanced menu screen, the agent inputs the IP address, or a range of IP addresses, to be collected. There is no limit to this range; a range of 0.0.0.0 through 255.255.255.255 is accepted by the program, but this range is the same as not selecting any IP filtering. In actual practice, the agent would select only what is specified by the court order. All packets that pass the IP address filter are kept for further processing. Other filters, as described below, may cause the packet to be discarded before writing to the disk.

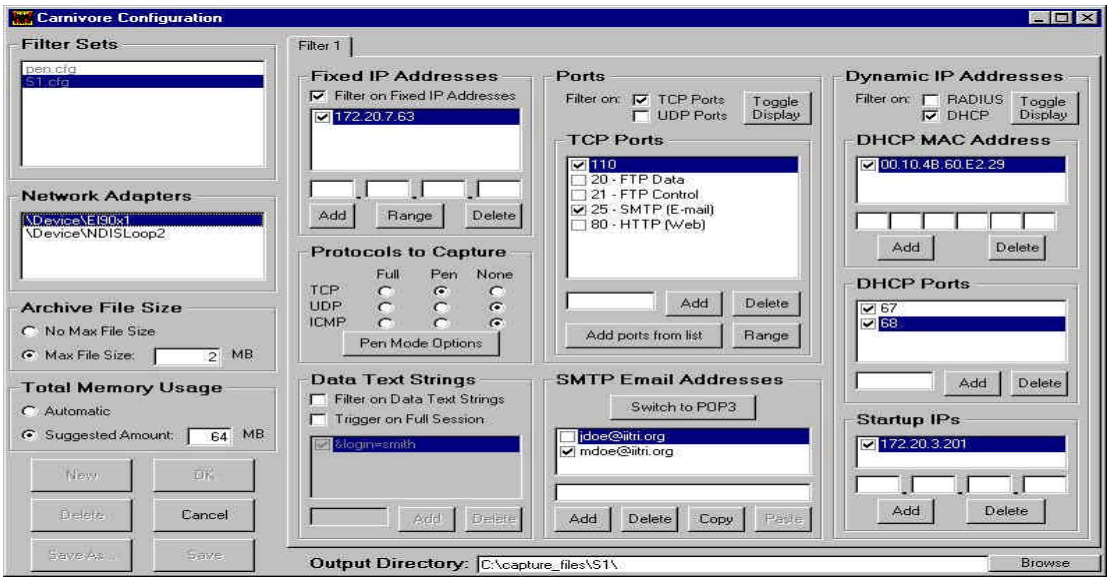

Figure 3-3. Carnivore Advanced Menu

3.4.4.1.2 DYNAMIC IP FILTERING

Where fixed IP collection is not possible, Carnivore supports collection of dynamically-allocated IP addresses that are made via either RADIUS or DHCP. For DHCP, the Media Access Control (MAC) address of the machine to be collected must be input, and for RADIUS, the user name must be input. A range of valid IP addresses must also be specified for RADIUS. The menu screen allows inputting a starting IP address, which would be used if the target subject was already logged on when collection is started. This starting IP address is required because the protocol that sets the IP address (either DHCP or RADIUS) is only used once at the start of the session. Carnivore would be unable to collect anything until the next DHCP or RADIUS exchange. If the current IP address of the target can be determined, this extra selection allows collection to start immediately. However, although this feature is on the menu screen, it is not supported by the underlying code. It does not matter what values are entered into this field; it is ignored. Dynamic IP filtering does not start until after the first DHCP or RADIUS protocol packet for the input MAC address or user ID is read.

3.4.4.1.3 PROTOCOL FILTERING

There are settings to select which protocols to collect. The three options are TCP, UDP, and ICMP. Each of these can be set to full, pen, or none. The full setting collects all packets for the specified IP addresses (see paragraphs 3.4.4.1.1 and 3.4.4.1.2) that use the protocol. The pen mode setting only collects address information appropriate for the protocol (e.g., FROM and TO fields of SMTP e-mail or IP address for FTP and HTTP traffic). If address-only information is not available within a given protocol, no packets are collected. In addition to the addresses, Carnivore collects the packets associated with the collected communications, but replaces the actual data with Xs. This data replacement allows CoolMiner to report byte counts for the TCP sessions, even in pen mode. In addition, if the Carnivore raw output is examined using a hexadecimal editor, the byte counts for various fields of a protocol (such as Subject) can be

determined. If none is selected, no packets for that protocol are collected. The default setting for each of these protocols is none.

3.4.4.1.4 TEXT FILTERING

Carnivore can be set to check for specific text strings. For example, a setting could be made to collect all TCP packets from a specific IP address that contains the text string "FBI". There is also an option to collect the entire TCP transmission for any packet that contains the given text string. This collection of packets starts with the packet that contains the string and continues for the remainder of that TCP session until the end, whether or not the text string is in each packet. Every packet is checked and then either saved or discarded before checking the next packet. If the search word appears in the next to last packet of a TCP transmission, only the last two packets are collected when this feature is used. Carnivore cannot go back and retrieve the packets that were examined and discarded earlier.

Text filtering capability allows the FBI to capture web-based e-mail such as Hotmail. For example, Carnivore can be set to filter HTTP packets looking for the string "&login=username" where username represents the target of the court order.

Note that this filtering is purely an American Standard Code for Information Interchange (ASCII) text string match. Carnivore is not capable of decoding various encoding schemes (e.g., Unicode, BASE64, or UUENCODE) to perform this search.

3.4.4.1.5 PORT FILTERING

For TCP or UDP filtering, any or all ports can be selected. If only ports 25 (SMTP), 80 (HTTP), and 110 (POP3) are of interest, only those three need be selected. Ports can be selected using a pull-down menu or by typing in the port number or range of port numbers. It is possible to select all ports. Any combination of ports can be selected. If it is known, for example, that HTTP is being redirected to port 8080, then port 8080 can be selected. The same is true for other protocols using nonstandard ports.

3.4.4.1.6 E-MAIL ADDRESS FILTERING

Carnivore can filter SMTP or POP3 traffic based upon the e-mail address. The proper mode must be selected and the e-mail address to be collected must be entered. If SMTP or POP3 ports are selected (see paragraph 3.4.4.1.5) and no e-mail address is selected, Carnivore collects all packets for those ports.

3.4.4.2 FILTER PRECEDENCE

While it might be intuitive to think that all of the filters are joined by a Boolean AND, they are not. The following describes the interaction of the various filters:

- Fixed IP, DHCP, and RADIUS all work in parallel. Packets that have IP addresses, as selected by any of those three filters, are held for further processing. These packets might eventually be discarded by another filter.

- If fixed IP is chosen along with SMTP or POP collection for a specific e-mail address or POP user, Carnivore collects only packets for that e-mail address or POP user that also have the chosen IP address.
- If RADIUS or DHCP is chosen along with SMTP or POP collection for a specific e-mail address or POP user, Carnivore first checks for the RADIUS or DHCP protocols to determine the IP address. Nothing is collected prior to the IP address being determined. Once determined, Carnivore collects only packets for that e-mail address or POP user that also have the chosen IP address.
- If SMTP or POP collection is specified without providing an IP address (either fixed or dynamic), all e-mail messages that match the user names specified are collected regardless of IP address.
- The text string search is a Boolean AND function with all other filters, except for SMTP and POP. The text string match is ignored if SMTP or POP collection is chosen for a specific e-mail address or user.

3.4.4.3 OUTPUT DIRECTORY AND ARCHIVE FILE SIZE

All packets that have passed all the filters are saved to a file. This file is typically stored on a 2-Gbyte Jaz disk. However, there is nothing in the program to prevent collection from being stored on the hard drive. The storage location is a selection made at setup time and is any valid path name for Windows NT. Three files are stored. One is a ".vor" file that contains the actual collected data, along with a short header. Another is a ".output" file that contains a human readable version of the settings used to collect that data in the corresponding ".vor" file. The third is a ".error" file and contains any error messages that may be generated during the collection session.

File names contain the date and time that collection was started, as determined by the system time. The ".vor" files may also have an extension if more than one file was used for collection.

Data are buffered prior to output. Carnivore writes the data to the output buffer, which is flushed to disk when the block size appropriate for the media selected has been reached, when the "next file" button is clicked, or when collection has been stopped. The block size for collection to fixed media is 128 kbytes and for removable media is 64 kbytes.

As a part of the settings, a maximum file size for the collected data can be chosen. When this limit is reached, the collected data file is closed, and a new file is created. This feature is useful for downloading the data (see paragraph 3.4.3) in smaller increments. The input value for the maximum file size must be an integer. If a floating-point number is entered, only the integer part is used. If zero (or a decimal number less than 1) is chosen, then there is no maximum files size (other than what the physical media can hold).

3.4.4.4 ANALYSIS SOFTWARE

DragonWare includes two programs for analysis of packets obtained from Carnivore. These programs are called Packeteer and CoolMiner. The Packeteer program takes the collection of IP packets in ".vor" files, reconstructs the TCP session, and creates a series of files that can be

viewed with CoolMiner. The CoolMiner program is used by the case agent to further select which data to view. For example, CoolMiner can be set to show only certain types of packets (e.g., HTTP). The purpose of this setting is not to limit collection, but to make it easier to view, analyze, and minimize the collected data. The agent first might want to look at the HTTP traffic and then later look at the e-mail traffic. By using CoolMiner, the agent does not have to look at everything at one time.

IITRI used Packeteer and CoolMiner to simplify the testing procedures. Although these programs are outside the scope of the evaluation, IITRI did verify their operation by examining the input and output files with a hexadecimal editor. IITRI discovered software bugs in both programs that caused them to fail to display correctly some of the data collected by Carnivore. When notified about the bugs, the FBI corrected some of them. Other bugs are still under investigation as of the date of this report.

3.4.5 THROUGHPUT

IITRI attempted to determine the throughput capacity of Carnivore both experimentally and analytically. Experimental attempts failed to drive sufficient traffic across the local area network to make Carnivore drop packets; traffic never reached the point where packets were dropped. From IITRI's analysis and discussion with the FBI, it was determined the true throughput limitation is based on output to the recording device. Limits are discussed in paragraph 4.2.8.

3.4.6 OPERATIONAL CONSIDERATIONS

There have been reports that installation of Carnivore at some ISP sites has caused operational problems for those ISPs. Given that Carnivore is installed using a read-only tap, there should be no operational problems. However, as noted in paragraph 3.4.1, the FBI must work with the ISP to find an appropriate point in the ISP network to install Carnivore. This selection is made with the intent of finding a point that allows the FBI to collect everything permissible by the court order, yet be on the smallest bandwidth network segment possible. If the ISP must make changes to its network configuration to accommodate the installation, that is an operational impact to the ISP.

Another consideration is the versions of protocols used by the ISP network and those understood by Carnivore. For example, if Carnivore recognizes a different version of RADIUS from that used by the ISP, it may not be possible for Carnivore to collect based upon the dynamic IP allocation provided by RADIUS. The solution would be to update the Carnivore software, or for the ISP to use the version of RADIUS recognized by Carnivore. Clearly, the latter would be an operational impact to the ISP.

3.5 SOFTWARE ARCHITECTURE

The Carnivore software consists of four components

1. TapNDIS driver (written in C) derived from sample source code provided with Win32 Network Driver Interface Specification (NDIS) Framework (WinDis 32), a product of Printing Communications Associates, Inc. (PCAUSA, http://www.pcausa.com) The

license for WinDis 32 prevents the FBI from releasing the source code for this driver, and possibly for TapAPI.dll, to the public. The relevant portions of the WinDis 32 license are shown in Appendix D.

2. TapAPI.dll (written in C++) provides the API for accessing the NDIS driver functionality from other applications.
3. Carnivore.dll (written in C++) provides functionality for controlling the intercept of raw data.
4. Carnivore.exe (written in Visual Basic) is the GUI for Carnivore.

3.5.1 TAPNDIS DRIVER

TapNDIS is a kernel-mode driver that captures the Ethernet packets as they are received, applies some filtering to the packet, and copies the packet to a shared memory buffer if the conditions of the filter are satisfied. The contents of the shared memory buffer are available to the Carnivore application through calling TAPgetFrames (entry point to TapAPI.dll). Writing selected packets to a data file is also handled through the driver.

The source code for TapNDIS is contained in 13 files totaling 10,322 noncomment lines of code (13,162 total lines). Nine of the source files, or approximately 40 percent of the code, were apparently borrowed intact, or with only minor changes, from WinDis 32 sample programs as they contain comment blocks asserting PCAUSA's copyright. Only five of these files have comments indicating where minor changes were made for Carnivore. Two small files were generated by Microsoft Developer Studio according to the comment block at the beginning of each file. The remaining two files (tapndis.c and tapndis.h) do not contain any comments to indicate whether they are mostly original code or were borrowed from WinDis 32 sample programs. These files contain all of the logic for the driver-level filters and for writing data to a file. IITRI assumed, therefore, they are the core of the Carnivore implementation. It appears from the contents of tapndis.h that FBI developers intend to move all filtering for Carnivore to TapNDIS, but only the first stages have been implemented in version 1.3.4.

The outline of the filtering algorithm is

1. If filtering is suspended then ignore the packet
2. If all packets are requested then intercept the packet
3. For 802.3 Ethernet, if the protocol matches a requested protocol, then intercept the packet
4. For Version 2 Ethernet, filter on the following items as requested, in the given order, rejecting immediately on the first failure: protocol, source, and destination Ethernet addresses; protocol within protocol (UDP, TCP, ICMP, etc.) and, for IPV4, source and destination IP addresses; combined IP address and port; combined Ethernet address and port; combined Ethernet address and protocol; and text string search with wildcard.

Because filtering functions have been moved to the driver, the TapAPI calls for steps 1 and 2 are no longer made from Carnivore.dll.

Primary packet filtering is confined to a single function. If the packet satisfies the filtering criteria, a function is called to copy the packet to the shared memory buffer. If there is enough room in the buffer, copying succeeds and the status count is incremented by the length of the packet. Otherwise, status counts for frames overflowed and frames missed are both incremented by one. The count of frames missed is requested by Carnivore.dll and reported as packets lost. If the data rate were sufficiently high, it is likely that the driver could miss packets without detecting the miss. Appendix D provides descriptions of the primary TapNDIS functions.

3.5.2 TAPAPI DRIVER

The TapAPI driver provides the API for accessing the functionality of the driver TapNDIS. The source code for TapAPI is contained in six files totaling 4,120 noncomment lines of code (6,889 total lines). TapAPI provides 45 entry points callable from Carnivore.dll. In Carnivore version 1.3.4, only 22 are used to

- Connect to the driver for packet collection or terminate collection
- Open or close an output file to which raw data will be written
- Set packet filters
- Retrieve packet data and write it to the output file
- Stop and reset collection, including functions to halt collection when a dynamic IP address is no longer valid
- Request status or retrieve error messages

Appendix D provides complete descriptions of the API entry points.

3.5.3 CARNIVORE.DLL

This dynamic link library (DLL) controls the collection of data by Carnivore in response to a parameter file established by the user interface and commands from the user interface. Nine entry points are provided; 13 classes are used internally. The source code is contained in 41 files totaling 6,278 noncomment lines of code (9,954 total lines). Two of the source code files (mediaSupport.cpp and mediaSupport.h) contain code that is Iomega proprietary, preventing them from being made public. Entry points and classes are defined in Appendix D.

Once started, Carnivore runs an infinite loop. The following algorithm is performed each time through the loop:

1. If collection is not running, do nothing.
2. If shared memory buffer overflow in the TapNDIS driver has been detected and filtering is on for DHCP or RADIUS, reset the filters, flush the buffer, and redownload the filters to the driver to restart collection. Regardless of DHCP or RADIUS filtering, reset the memory buffer overflow flag. (At this point, the program does not call the driver interface to check for an overflow. Instead, it is using a flag that is set by the function

GetStatus, which is called by the GUI on a timer running at intervals of approximately 0.25 seconds. This timing interval does leave a small window for problems to occur if Carnivore processes packets between the time the buffer overflows and GetStatus is called and the program never detects the buffer overflow. The only indication that this overflow might have happened would be if the value of nPktsLostUser was nonzero and there were no messages in the .output.txt file about the buffer being filled.)

3. If media full has not been detected, attempt to retrieve and process packets. (Again, the program is checking for media full based on a flag set by the function GetStatus.) Apply the remaining filter criteria (not handled by the TapNDIS driver) to each packet. If the packet is rejected by a filter, it is discarded. Otherwise, if Carnivore is being used in pen mode, the packet is truncated as specified in Table 3-1. Then the packet (or truncated packet in pen mode) is passed back to the TapNDIS driver (via a call to TAPputData) to be written to the output file. The remaining filter criteria are applied in the following order:
   i. RADIUS
   ii. DHCP
   iii. SMTP
   iv. POP3
   v. Telnet
   vi. FTP
   vii. Text (includes TCP, UDP, and ICMP)

Table 3-1. Pen Mode Packet Information

Packet Type	Data Retained
DHCP and RADIUS	Entire packet
Packet fragment	Ethernet header + IP header
UDP packet	Ethernet header + IP header + UDP header
ICMP packet	Ethernet header + IP header + 4 bytes
TCP packet (except for those below)	Ethernet header + IP header + TCP header
FTP (destination port 21)	Entire packet if it contains USER field Otherwise, Ethernet header + IP header + TCP header
SMTP (port 25)	Entire packet if it contains one of the following fields: MAIL FROM:, RCPT TO:, SEND TO:, SOML FROM:, SAML FROM: Or if data consists of only one of the following words: DATA, RSET, QUIT Otherwise, Ethernet header + IP header + TCP header
POP3 command (destination port 110)	Entire packet if it contains one of the following fields: USER, APOP, RETR, QUIT. Otherwise, Ethernet header + IP header + TCP header
POP3 server response (source port 110)	Ethernet header + IP header + TCP header

3. (Cont) IITRI's examination of code (CCollection::nProcessPacket and CCollection::TruncatePacket in CollectionThread.cpp, and Smtp::trackSmtpSession in Smtp.cpp) produced different findings than the live test of Carnivore. IITRI found code that first overwrites with Xs information that should not be collected and then truncates the packets unless one of the conditions listed in Table 3-1 for keeping the packet is satisfied. In live tests IITRI observed that packets are overwritten with Xs, but found the Xed out packets are included in the output file without being truncated. Time limitations for this evaluation prevented IITRI from determining if this apparent conflict is because of a software bug, design change, or misinterpretation on IITRI's part.
4. If no packets were available for processing, free some stale nodes from the processing objects and sleep for 1 ms (freeing the central processing unit (CPU)for any queued events).
5. If either Start or Stop has been called from the GUI, handle it as described in Appendix D.
6. If NextFile has been called from the GUI, close out the current output data file and start a new file.
7. If PrepareToStop has been called from the GUI, reset the filters in the TapNDIS driver so no more packets are intercepted.
8. If Shutdown has been called from the GUI, set flag to prevent executing the loop again.
9. If collection is running and the agent has pressed the eject button on the removable drive, do the following: close out the current output data file; eject disk and wait for new disk to be available; create directory for output files and open new files (.output.txt, .error.txt, and data files); write header to new data file; if DHCP or RADIUS filtering is on and shared memory buffer overflow has occurred in the TapNDIS driver (checked by call to driver interface), reset the filters, flush the buffer, and redownload the filters to the driver to restart collection; and check for available space on the removable media.

Output from Carnivore 1.3.4 is written to three files as follows:

- Raw data packets are written to one or more .vor files. In full mode, the complete contents of all packets that are not rejected by one of the filters are written to the files. Table 3-1 shows the information that is written to the files in pen mode for packets that are not rejected.
- Operational messages are written to a .output.txt file. These messages include descriptions of the filters used for the collection, start and stop indicators, and information about the tracking of FTP and Telnet sessions. Details about all possible messages are provided in the description of the class CLogFile in Appendix D.
- Error messages for all errors recognized by Carnivore are written to a .error.txt file. Details about the possible error messages are provided in the description of the class CLogFile in Appendix D.

3.5.4 CARNIVORE.EXE

All agent interaction with Carnivore is provided through a GUI written in Visual Basic. The main form (frmMain) is used for starting and stopping collection and for displaying status information. The button labeled "Advanced…" is used to access a second form (frmAdvanced) that is used to set up the collection filters and create the user configuration file for Carnivore. There are six additional forms that are dialog boxes for various user responses. Two other forms included in the program are a splash screen displayed on startup and a full-screen solid background displayed whenever Carnivore is running. There are also 15 classes that are used in the GUI, mostly for storing filter parameters, and a module file that includes a few auxiliary functions, global variables, and declarations for all Win32 API calls used in the GUI and the exported functions from Carnivore.dll. In addition, there are four forms included in the program and nine associated classes that have all code commented out because a decision was made not to implement the features they were to provide (a scheduling capability for collections that were supposed to be limited to certain hours, some more sophisticated filters, and a real-time viewer for viewing data packets in the .vor file), but they have been left in the program. The source directory provided to IITRI also included five form files and two class files that are not used in compiling Carnivore. One of the forms appears to be for a feature (adding case tracking information) that was dropped from the design but may be implemented in the future.

3.5.5 DEVELOPMENT PROCESS

No formal development process was followed for the development of Carnivore through version 1.3.4. The Carnivore program was a quick-reaction capability program developed to meet the needs of the FBI for operational cases. None of the existing network sniffers (such as EtherPeek) could collect the proper amount of data (only what is allowed; nothing more, nothing less). This type of development is appropriate as a "proof of concept," but it is not appropriate for operational systems. Because of this lack of development methodology, important considerations, such as accountability and audit, were missed.

3.6 LABORATORY TESTS

Carnivore was designed to collect target communication authorized by court orders. According to the FBI, not every feature that Carnivore provides has been used in real collection cases. Carnivore is a case tool, not a COTS product. To achieve the purpose of evaluating the entire capability of Carnivore, the test cases are divided into two parts:

1. Test cases one through five examine typical collection cases, i.e., the model scenarios requested in the Statement of Work.
2. Test cases six through thirteen examine the general capability of Carnivore. Features that may have not been used by the FBI in real collection cases, but are provided by Carnivore, are included in these test cases.

The following paragraphs summarize the test cases. Details, including screen captures of the filter set up, are provided in Appendix C. This information includes the rationale that was used when designing the test cases and the tests results. For each of the test cases that did not pass, or partially passed, an explanation of the failure is provided.

3.6.1 TEST 1 NONCONTENT E-MAIL COLLECTION

Description: Collect noncontent fields on e-mail sent to and from a target. This test is for pen mode e-mail collection on SMTP (TCP port 25), and POP3 (port 110). The target's e-mail ID is a required input to the filter for this test.

Objective: Verify that Carnivore does collect the e-mail addresses that were sent from and to a target, and does not collect any of the target's e-mail subject and content.

Expected result: Carnivore will collect only the FROM and TO addresses of the e-mail that was sent from and to a target.

Result: Carnivore did not collect any fields other than TO and FROM, but in some trials failed to collect FROM and TO information. One problem is a known weakness in Carnivore detailed in paragraph 4.2.8. IITRI also observed that in some instances, Packeteer misclassifies the POP3 messages as SMTP and this misclassification causes CoolMiner to display the wrong information. This misclassification is not a Carnivore bug.

IITRI observed that time-stamps for packets collected appeared to be incorrect possibly because of a problem with conversion from Microsoft internal date format to the standard UNIX format (used by CoolMiner), and possibly in the conversion between Greenwich Mean Time and local time.

IITRI observed that in pen mode Carnivore replaces e-mail header information with Xs. When the data are viewed in CoolMiner it is easy to determine the length of each field in the header and the length of the entire message. As noted in paragraph 3.5.3, IITRI found source code for software that should have eliminated the output of this information. Apparently that code is not executed. IITRI was not able to determine why the code is not executed.

Retest: The FBI provided a patch for the time-stamp problem and a new version of CoolMiner. A retest shows the time-stamp problem is fixed and is consistent with the system collection time. The Carnivore raw data for SMTP looked correct, however there still are possible problems with information displayed by CoolMiner. For SMTP traffic, the FROM e-mail address (the target's in this test case) is correctly displayed, but the TO address is not shown (the nontarget's in this test case). Packeteer and CoolMiner appear to be looking for the other e-mail addresses in the TO and FROM lines in the e-mail message, which Carnivore has purposely blanked out to avoid collecting information about communication between nontargeted entities. IITRI believes the program should instead be looking for the RCPT-TO lines, which Carnivore properly collects.

3.6.2 TEST 2 NONCONTENT WEB BROWSING COLLECTION

Description: Collect the source and destination IP addresses for a target's web browsing activities. This test is a pen mode collection on HTTP (TCP port 80).

Objective: Verify that Carnivore does collect the target's HTTP web browsing activity source and destination IP address, does not collect the URL and content of the target's web activities, and does not collect other users' communication.

Result: Passed.

IITRI observed that CoolMiner provides information on how many bytes are transferred between the client and the server. The data sizes can also be counted from the Carnivore raw data.

3.6.3 TEST 3 NONCONTENT FILE TRANSFER ACTIVITY COLLECTION

Description: Collect the source and destination IP addresses for a target's FTP activities. This test is a pen mode collection on FTP (TCP ports 20 and 21).

Objective: Verify that Carnivore does collect the target's file downloading activity source and destination IP address and does not collect the file content and other users' FTP activities.

Result: Passed.

As in tests 1 and 2, the amount of data transferred is captured.

3.6.4 TEST 4 FULL COLLECTION ON A FIXED IP ADDRESS

Description: Collect the contents of communications to and from a target, who has a fixed IP address. This test is a full mode collection.

Objective: Verify that Carnivore does collect the target's communication and that no other users' (i.e., other IP addresses) communications can be collected.

Expected result: Web browsing contents, FTP login session, commands and data, and e-mail contents are all captured from the target fixed IP address.

Result: Passed.

3.6.5 TEST 5 E-MAIL CONTENT COLLECTION

Description: Collect the contents of e-mail communications that were sent from and to a target. This test is a full mode collection on the target's e-mail ID.

Objective: Verify that Carnivore does collect the contents of a target's e-mail, but does not collect other users' communications.

Result: Passed.

3.6.6 TEST 6 ALIAS E-MAIL COLLECTION

Description: E-mail collection of a target who has an alias for outgoing e-mail. This test is an e-mail mode collection on SMTP and POP3 (TCP ports 25 and 110). The target's e-mail user ID is entered into the filter for collection.

Objective: A court order authorizes collecting the full content e-mail traffic to and from a target, and the ISP determined the target's e-mail address is marydoe@location.org. However, the target

made an alias “NOBODY” for her outgoing e-mail address. Verify that Carnivore does not collect the target’s e-mail by filtering on her real user ID.

Result: Passed.

3.6.7 TEST 7 FILTERING TEXT STRING ON WEB ACTIVITY COLLECTION

Description: Collect the web browsing contents that contain a specific text string. This test is a full mode collection of a given text string on HTTP (TCP port 80).

Objective: Carnivore does collect the target’s web browsing contents that contain a specific text string, and only the web pages contain the searched string, not other web browsing pages.

Result: Passed.

3.6.8 TEST 8 POWER FAILURE AND RESTORATION

Description: Power failure and restoration test.

Objective: Verify that after the power is restored, Carnivore automatically starts up and continues to collect what it was originally set up to collect. Also, verify that Carnivore recovers all of the data that was collected before the power outage.

Expected result: After the power is restored, Carnivore recovers to the state where it was before the power failure and continues to use the original filter setup to collect traffic.

Result: Carnivore did not recover to a collecting state as it was supposed to. Two errors were noted: (1) during the restart procedure, a TAP interface error in connecting to the Ethernet card occurred; (2) the data collected before the power failure was lost. This loss of data is the result of a trade-off between processing speed, having padding in the collected data, or possibly losing some data. Carnivore does not write collected data into a disk until a block size of data is collected, a user activates the “next file” feature, or Carnivore is stopped.

3.6.9 TEST 9 FULL MODE COLLECTION FOR ALL TCP PORTS

Description: Collect all the user’s TCP communications with a minimum filter setup.

Objective: By choosing a minimum filtering, i.e., all TCP ports on full collection mode, Carnivore collects all the user’s TCP communication. Verify that when selecting TCP protocol without selecting any ports, the default to Carnivore is collecting all TCP ports.

Expected result: Carnivore collects all TCP traffic from every device that is attached to the sniffing segment.

Result: Passed.

3.6.10 TEST 10 COLLECT FROM A DHCP-ASSIGNED IP ADDRESS

Description: Collect the contents of communications to and from a target who has a dynamic (DHCP assigned) IP address.

Objective: Carnivore filter GUI provides three entry fields for DHCP setup, i.e., MAC address, Ports (67 and 68), and Startup IP. In order to collect communication from a specific DHCP-configured device, what data must be entered in the filter? Also, it is assumed that the Startup IP field can be used by Carnivore to immediately start collecting the traffic of a user who has already been assigned an IP address without waiting for the next DHCP-based IP assignment.

Expected result: (1) With a known MAC address but without a Startup IP, collection for that target does not begin until after a DHCP-based IP assignment occurs. (2) With a known MAC address and a Startup IP set to the currently-assigned IP address for the target, collection begins immediately.

Result: (1) Both MAC address and DHCP ports are required data entries for the filter to have Carnivore collect communication from a specific DHCP-configured IP address. (2) Data entered to the Startup IP field was totally ignored by Carnivore. A DHCP exchange was always required for Carnivore to collect from a specific dynamic IP address.

According to RFC2131 (the DHCP standard), the hardware address of the network adapter (i.e., the MAC) must be included in all DHCPREQUEST and DHCPDISCOVER packets. It may also include a client ID other than the hardware address.

3.6.11 TEST 11 FILTERING ON TEXT STRING FOR E-MAIL COLLECTION

Description: Collect e-mail with a key word.

Objective: When filtering on a given text string and the target's IP address (either fixed or dynamic), verify that Carnivore only collects the target's e-mail messages that contain the given text string.

Result: Carnivore behaves exactly as expected. E-mail that contains the search text string is captured and e-mail that does not contain the search text string is not captured. However, this capture condition is not always clear from CoolMiner analysis. If the text string is in the e-mail header (for instance, part of the Subject), then CoolMiner displays the message properly. If the search text string is only in the body of the message, CoolMiner does not display the message. This condition occurs because Carnivore does not start collecting packets until it sees the search text string. If the string is only in the body, the header of the message has already passed without being collected. CoolMiner needs the entire set of e-mail protocol packets in order to display properly. CoolMiner displays the collected packets as TCP packets of an unknown application.

The raw output of Carnivore was examined to verify the results shown by CoolMiner.

3.6.12 TEST 12 FILTERING ON TEXT STRING AND E-MAIL ADDRESS OR E-MAIL USER ID FOR E-MAIL COLLECTION

Description: Collect e-mail with a key word and a user name.

Objective: When filtering on a given text string and the target's e-mail ID, verify that Carnivore only collects the target's e-mail containing that given text string.

Result: Because of a performance trade-off, Carnivore filters for the text search string at the driver level. Filtering for a specific e-mail user is at the application level. After this test was completed, it was learned that the text string search is ignored when filtering for a specific e-mail address. Ignoring this text string search was not considered over-collection, as it is known to be a feature that is not implemented. If a court order were to specify that the FBI could only collect e-mail messages of a particular subject that contained a particular text string, the FBI would not be able to use Carnivore to obtain the data.

3.6.13 TEST 13 FILTERING ON TEXT STRING FOR FTP COLLECTION

Description: Collect FTP communication containing a key word.

Objective: When a text string is entered into the filter and FTP ports 20 and 21 are selected, Carnivore should only collect the FTP activities containing that given text string.

Result: Analysis of the raw Carnivore output shows that the correct data were collected. Carnivore either collected the FTP packets that matched the given text strings or collected from the first packet containing the text string to the end of that session (if the Trigger on Full Session check box was checked). In either case, Packeteer failed to assemble all of the packets together for an entire FTP session (because not all packets were collected) and, in turn, CoolMiner could not provide the result of correct collection. The purpose of this test was to determine if Carnivore collects according to its filter setup, not to evaluate the post-processing tools Packeteer or CoolMiner. The Carnivore output was correct.

SECTION 4
CONCLUSIONS

4.1 ASSUMPTIONS

Given the time constraints of this evaluation, IITRI made several assumptions about various components in order to establish a boundary of trust. These assumptions included

- The Century Tap from Shomiti Systems is effective in making Carnivore a read-only device. No evidence was seen that Carnivore transmitted any data through the device, nor did there appear to be any functionality in Carnivore that would allow it to transmit. IITRI is satisfied from analysis that the tap is one way; it provides no connection between the transmit lines of the collection computer and the ISP network. IITRI did not perceive the need to expend resources to test this COTS equipment.
- Limitations and vulnerabilities in the Windows NT operating system are completely overshadowed by lack of audit and accountability in Carnivore. While there are known vulnerabilities with Windows NT, there are vulnerabilities with every operating system. Given the limited connectivity of Carnivore and the installation of hardware authentication devices for remote access, the assumption that residual vulnerabilities of Windows NT do not impact this evaluation is reasonable. In addition, since Carnivore does not make use of any of Windows NT security features, any potential problems with those features were not considered. If the recommendations in Section 5 are adopted, then any residual problems with Windows NT also need to be considered. It is important to note that the Carnivore collection computer does not have an IP stack loaded. The driver and collection application treat all incoming frames as data to be analyzed.
- The Challenger security products from CPSI (see paragraph 3.4.3) are sufficiently robust to protect the remote connection. As with the Shomiti tap, IITRI did not test this COTS equipment.
- pcAnywhere, in particular symmetric encryption; pcAnywhere authentication; and pcAnywhere logging works properly. pcAnywhere was not evaluated; however, IITRI determined through experiment and a literature search the extent to which pcAnywhere supports Carnivore requirements.
- Dynamic IP address assignments via DHCP have been evaluated through lab experiment, while RADIUS has not. Time and resources required to test the various implementations of RADIUS were beyond those available for this evaluation. While RADIUS could be an additional source of weakness, IITRI's conclusions and recommendations apply equally to DHCP and RADIUS implementations of Carnivore.
- Because IITRI could not verify that either the binary or source code represented what the FBI actually uses, it had to assume the files were the same program used by the FBI. The executable Carnivore files used for testing were provided to IITRI separately from the source code IITRI analyzed. IITRI did not analyze the compiler tools used and did not recompile the source code. When the FBI provided a bug fix for the Carnivore code, only the binary code was provided.

4.2 GENERAL CONCLUSIONS

A wide range of interested parties has expressed additional concerns about Carnivore, many of which were also listed as part of the purpose for this evaluation. Rather than address each concern individually, IITRI chose to draw a series of general conclusions that, with supporting points, allows each party to address its own concerns.

4.2.1 NEED FOR CARNIVORE

Carnivore represents technology that protects privacy and enables lawful surveillance better than alternatives such as commercially available sniffer software. Carnivore restricts collected information in a precise manner that cannot be duplicated by other means. Although certain of Carnivore's functions could be duplicated by commercial products, there is no incentive to do so. The legitimate market for such a product is limited to law enforcement—a market already served by Carnivore. Moreover, publicly available products, such as EtherPeek, described in Appendix B, are not capable of limiting collection as precisely as most court orders require, resulting in over-collection and greater reliance on human intervention to minimize the information collected.

Many ISPs are unwilling or unable to collect only the information specified in a court order, requiring direct FBI use of tools like Carnivore to fulfill court-ordered requirements. In addition, the details of some highly sensitive investigations should not be disclosed to ISPs, many of whom may present risks of inappropriate disclosure.

4.2.2 LEGAL AND ORGANIZATIONAL CONTROLS

Carnivore is used under the same basic legal and organizational controls as are employed for telephone wiretaps and telephone pen-trap devices. Multiple organizational approvals are required for Carnivore deployment before a court order is issued; significant post-collection organizational and judicial controls exist as well.

Carnivore, like traditional telephone wiretaps (see Appendix A) uses human involvement to satisfy legal minimization requirements. Carnivore employs two minimizations. First, the collection computer selects pertinent packets. Second, a designated case agent reviews captured data to exclude irrelevant information. This minimization is analogous, but not perfectly so, to turning off telephone intercept equipment to exclude irrelevant conversations.

In response to specific concerns, IITRI evaluated the minimization process described independently by FBI headquarters and field personnel and reached the following conclusions:

- The supervising judge can, and regularly does, independently verify that traffic collected is only what was legally authorized.
- Controls exist over minimization, in that the post-minimization file reveals any irrelevant information that escaped the minimization process. Inadequate minimization can be detected through judicial oversight, through the FBI inspection process, or in civil or criminal litigation involving alleged misuse of Carnivore. However, except for FBI

procedures and professionalism, there are no assurances against additional copies being made of an inadequately minimized intercept.

If the current set of legal, regulatory, and organizational controls remains in place, the risk of misuse of Carnivore by FBI or ISP personnel is low. Centralized control over the technological devices is sufficiently high and the bureaucratic culture of the FBI sufficiently rigid to deter individual agents or group of agents from misappropriating Carnivore for their own purposes. ISPs have weak incentives to tamper with Carnivore; and if they want to spy on customers, they already have more attractive ways to do so with widely available sniffer software. On the other hand, not all of these protections are writ in stone. The rules can be rewritten, and the centralization can diminish, especially if Carnivore becomes much more widely used.

4.2.3 COLLECTION

Based on laboratory tests, Carnivore can collect everything that passes by on the Ethernet segment to which it is connected. This capability is no different from any other packet sniffer (see Appendix B describing a commercial sniffer). It is up to the agent who sets up Carnivore to select the proper set of filters so only the data that is allowed by the court order is actually collected. The system contains no automated checks for valid configuration. However, based on analysis of the Carnivore process, IITRI concludes there are significant procedural checks to minimize configuration errors. Multiple agents, FBI technical advisers, and often ISP personnel must agree on the settings before Carnivore is turned on.

Given a choice between under-collection versus potential over-collection, Carnivore design generally errs on the side of under-collection. To the extent that Carnivore under-collects information, no appreciable risk exists that the meaning of intercepted information would be altered. However, the result of this conscious decision on the part of the FBI, is to introduce exploitable technical weaknesses. These weaknesses, among others, are described in paragraph 4.2.8.

In one case, Carnivore version 1.3.4 collects more than would be permitted by the strictest possible construction of the pen-trap statute. In pen mode surveillance of certain e-mail protocols, Carnivore captures the contents of the TO and FROM fields. It replaces each character in the other fields with an X. Using one-to-one replacement permits users to determine the length (but not the content) of all of the fields defined by the e-mail protocol; for example, of the SUBJECT field and of the body of the message. Knowing the length of an entire message may be equivalent to knowing the length of a telephone call as permitted in telephone pen-trap surveillance, but access to the length of individual fields within a message does not appear to have a parallel.

Except for the field-length data referred to in the preceding paragraph, there was no evidence of over-collection during any of the tests. Carnivore bases its collection filters on various protocols as defined by industry Request for Comments (RFCs) standards. In the case where a network uses a nonstandard implementation of a protocol, over collection can occur. For example, the FBI admitted that a previous version of Carnivore handled pipelined SMTP (RFC 2920) incorrectly. However, it should be noted that when this situation occurs, the over-collected data are sealed and given to the judge, without being given to the case agent. The developers then, if

permitted and possible, analyze what protocol deviation is in use and make changes to Carnivore to allow it to collect properly.

In response to particular concerns expressed about collection, IITRI concludes

- While the system was designed to, and can, perform fine-tuned searches, it is also capable of broad sweeps. Incorrectly configured, Carnivore can record any traffic it monitors. Whether Carnivore has sufficient storage capacity to hold all that data is a separate issue (see below).
- Carnivore can, e.g., in court authorized counter-cyber-terrorism activities, scan a subset of network traffic for specific strings or access by or to specific sites. This capability is necessary to collect court-ordered data transmitted with nonstandard protocols where message boundaries do not occur at packet boundaries, such as Hotmail.
- Properly configured, Carnivore examines traffic and determines which pieces are allowed by its filter settings.
  - ◊ It accumulates no data other than that which passes its filters
  - ◊ It restricts data available to the FBI to specific types from or to specific users
  - ◊ It is used only when the implementation guarantees it will not drop packets and potentially miss the sign-off of a dynamically assigned IP address. In other words, it must be placed on a slow-enough bandwidth network segment; one that guarantees that any dynamically assigned IP address will be sent via that segment.
- Carnivore version 1.3.4 mixes pen-trap and full-content capability in one device. Unless correctly configured, the device can over-collect under a pen-trap order.
- Carnivore collects more than ordinary e-mail correspondence. In full collection mode, for example, it can record whatever transactions occur through TCP, UDP, and ICMP protocols including HTTP, FTP, SMTP, POP3, Exchange Mail, IMAP, CCmail, voice over IP, and streaming media. E-commerce payments-related communications, however, typically use Secure Sockets Layer, which are not decrypted by Carnivore.
- Carnivore does not come close to having enough power “to spy on almost everyone with an e-mail account.” In order to work effectively it must reject the majority of packets it monitors. It also monitors only the packets traversing the wire to which it is connected. Typically, this wire is a network segment handling only a subset of a particular ISP’s traffic. The main limitation is the amount of storage. For example, if Carnivore were collecting all traffic on a link that has a steady 25-Mbps traffic rate, the 2-Gbyte Jaz disk will be full in about 11 minutes. In the time needed to change disks the input buffers would likely overflow and data would be missed. Even if collecting to fast hard drives, the amount of data to be recorded would quickly overflow the amount of storage available. A 60-Gbyte hard disk could be filled in about 5–6 hours. If traffic were faster than 25 Mbps, then the storage would fill even faster.

4.2.4 AUDIT AND ACCOUNTABILITY

Auditing is crucial in security. It is the means by which users are held accountable for their actions. There is no auditing in Carnivore. The Carnivore version 1.3.4 collection computer is always logged in as the "Administrator" rather than using individual user IDs. This Administrator log-in means that every user of the system has full control over all the resources of the system. Even if auditing were enabled, there is nothing to prevent someone from editing or deleting those audit logs.

The pcAnywhere remote access software, while using unique login IDs, does not provide audit on an individual basis. Even if pcAnywhere did provide an audit log for access, since the users are then logged into the Carnivore collection computer as Administrator, there is nothing to prevent them from changing or deleting the pcAnywhere audit log. pcAnywhere gives the ability to both download files (needed for data analysis) and to upload files. The audit logs could be replaced by those uploaded from a different machine or tools could be uploaded to facilitate editing the existing logs.

As noted in paragraph 3.4.4, the password to the advanced menu is embedded in the Carnivore executable software. Since everyone with Administrator access has full control, there is nothing to prevent someone from using a Hex editor or other tool to determine this password. Therefore, it is not possible to determine who, among a group of agents with the password, may have set or changed filter settings. In fact, any action taken by the Carnivore system could have been directed by anyone knowing the Administrator password. It is impossible to trace the actions to specific individuals.

4.2.5 INTEGRITY

Carnivore version 1.3.4 has significant deficiencies in protection for the integrity of the information it collects. Information gathered by Carnivore may be lost or corrupted by physical attack, software bugs, or power failure. Also, the relationship among Carnivore filter settings, collected data, and other investigative activities may be difficult to establish. These deficiencies make Carnivore less effective as an investigative tool.

Lack of physical control of the Carnivore collection computer engenders some risk of compromise by untrustworthy ISP personnel. Once the FBI technicians have installed Carnivore it is under control of the ISP. Although the collection computer is left without a monitor, keyboard, or mouse, the ports are not normally covered or disabled and nothing prevents someone at the ISP from connecting those peripherals. That person could watch while a case agent uses remote dial-in access to download data and learn enough to gain control of the collection computer. To date, the FBI has relied on existing physical security measures at trusted ISP installations.

The link between the Carnivore collection and control computers is well protected. First, a unique (i.e., not reused), unlisted telephone number is assigned. Second, the link is equipped with a hardware key (see paragraph 3.4.3). Only computers with an identical key can connect. Third, the pcAnywhere software supporting the link requires a user name and password. Finally, pcAnywhere encrypts information on the link. FBI tools to view, analyze, and minimize raw Carnivore output contain several material weaknesses. These tools include Packeteer, to

reconstruct higher protocol sessions from IP packets, and CoolMiner, to display the results. Neither Packeteer nor CoolMiner are used to limit the data collected from the target, although they are used by case agents for further minimization.

During testing, IITRI found several bugs in the interfaces between Carnivore, Packeteer, and CoolMiner. These include

- The time stamps for the collected packets displayed by CoolMiner did not match what was expected. While originally thought to be a CoolMiner software bug, the FBI provided a patch to the Carnivore program that fixed this problem.
- Some instances of valid SMTP collection were being displayed as POP data. This software bug was determined to be a problem with the way Packeteer processed the data. The data collected by Carnivore were correct. As of the date of this report, this bug has not yet been fixed.

Carnivore does not consistently recover from power failures. IITRI noted two problems. First, because of the way Carnivore buffers data into blocks before actually writing to disk, any power failure guarantees the loss of between 0 and max_block_size bytes of already collected data. This loss is in addition to any data missed while power is off. As noted earlier, the max_block_size for fixed disk is 128 kbytes and for removable disks is 64 kbytes. Second, there is a race condition that prevents the Carnivore program, as it is starting up, from reliably accessing the Ethernet interface. When this failure occurs, and the Carnivore program had been collecting earlier (before the power failure), it is not able to automatically begin collecting again. Someone must manually access the system to start the collection.

In Carnivore version 1.3.4, as evaluated, it is not possible to definitively show what settings were used to collect any given set of data. Although the parameters for collection are stored in the same directory as the collected data, they are in a separate file and the only link among the files is implied by the file names. Should files become separated, it may be difficult to prove what settings and what software were actually used to collect the data.

There is no time synchronization within Carnivore. The time stamps are dependent upon the correct setting of the collection computer's clock and its continued correct operation. While this deficiency may not seem to be important, multiple Carnivore devices might be used in an investigation or it might be necessary to correlate Carnivore collection with other collateral evidence. If so, it is important to note that the time stamps from Carnivore are only as good as the original source for the time and the accuracy of the collection computer.

While Windows NT and the way its file systems work were not evaluated, other factors could affect data integrity. For example, since there are no checksums or other protections on the collected data files and no individual accountability, anyone could edit the collected data. Since all users all log in as Administrator, evidence of the changed files could be erased.

4.2.6 CARNIVORE DEVELOPMENT ENVIRONMENT

No formal development process was used for Carnivore through version 1.3.4. IITRI was provided with a formal System Requirements Specification for version 1.3.4, but found no

decomposition into a Software Requirements Specification. IITRI observed no change control procedures for version 1.3.4. When ITTRI testing found a bug that affected the time-stamps produced by Carnivore, the FBI provided an update to the Carnivore code. There was no change in the Service Pack number for that release version.

Because of this lack of formal development process, technical issues such as software correctness, system robustness, user interfaces, audit, and accountability and security were not well addressed. While this lack of a formal development process might have been acceptable for a "proof of concept" demonstration, it is not appropriate for an operational system. Operational systems should be developed with rigorous tracing of requirements through design, development and testing, strong configuration management, and good management insight into the development process.

A more formal development process has been established for Carnivore version 2.0, but IITRI has not evaluated the effectiveness of the new process.

4.2.7 MISCELLANEOUS CONCERNS

The purpose for the independent evaluation of Carnivore includes a number of concerns about the effect on privacy of individuals who are not the target of court-ordered surveillance. Examining those concerns, IITRI concludes that Carnivore version 1.3.4 does not

- Read and record all incoming and outgoing e-mail messages, including sender, recipients, message subject, and body. It stores packets for later analysis only after they are positively linked by the filter settings to a target
- Monitor the web-surfing and downloading habits of all the ISP's customers, including web searches for information or people. It can only record for later evaluation some HTTP files retrieved by a target
- Monitor or read all other electronic activity for that ISP, including instant messages (such as with ICQ), person-to-person file transfers, web publishing, FTP, Telnet, newsgroups, online purchases, and anything else that is routed through that ISP. It can only record a subset of such files for a specific user

In addition, IITRI noted public concern that the FBI and DoJ may use Carnivore for purposes other than surveillance. Based on evaluation of the architecture and implementation, and the capabilities of the Carnivore software, IITRI concludes that Carnivore version 1.3.4 cannot

- Alter or remove packets from the network or introduce new packets
- Block any traffic on the network
- Remove images, terms, etc. from communications
- Seize control of any portion of Internet traffic
- Shut down or shut off the communications of any person, web site, company, or ISP
- Shut off accounts, ISPs, etc. to "contain" an investigation

4.2.8 CARNIVORE LIMITATIONS

Carnivore has a number of limitations that may restrict its usefulness. In many cases these limitation are byproducts of design decisions made to ensure Carnivore can precisely limit collection. IITRI concludes that Carnivore:

- Can be countered with simple, public-domain encryption.
- Cannot effectively collect POP3 e-mail messages in pen mode. It has insufficient capacity to separate allowed versus forbidden information from the messages. It, therefore, collects nothing. During testing, IITRI determined that for pen mode collection of POP e-mail, the only information collected was the POP control messages. All that could be seen was that the target user had authenticated to the POP Server at a given time and that messages were retrieved. No TO or FROM information was collected.
- Cannot manage nonstandard protocol implementations. Nonstandard implementations may result in potential over-collection and, typically, collection is terminated. When fixes have been made, e.g., to handle pipelined e-mail transmissions, they could open additional mechanisms to defeat Carnivore, if revealed. Testing against nonstandard implementation is extremely difficult.
- Has a limited ability to process web-based e-mail accounts. The current implementation requires explicit knowledge of the format of the provider's log-in messages.
- Cannot collect in high-traffic environments. The FBI has found that when collecting a steady flow of packets, Carnivore can handle up to 60 Mbps without dropping packets if writing its collected data to a high speed hard disk. If writing to the Jaz disk, the rate drops to 15 Mbps, and if writing to a Zip disk, the rate drops to 5 Mbps. (Rates provided by the FBI; and confirmed by analysis versus testing.) This limitation is not the result of CPU speed or the collection interface. Both of these could be increased and the limitation would remain. The limiting factor is the input and output throughput to the storage devices. (Note: security and accountability of Carnivore output would improve if it were written to write-once media, e.g. compact disk. With current technology, however, output to CD would further limit throughput).
- Uses support tools that have additional limitations. Packeteer cannot reconstruct all TCP-based protocols and CoolMiner fails to report certain information present in the Packeteer output. IITRI also found situations in which CoolMiner output did not reflect the output of Carnivore.

4.2.9 RELEASE OF CARNIVORE

The FBI may have legitimate reasons to oppose public release of Carnivore version 1.3.4. The FBI is restricted, by license, from releasing the commercial code that forms the basis of the tool. Furthermore, the current version has technical limitations that could be exploited to defeat surveillance if they were revealed.

4.3 DOJ QUESTIONS

IITRI's general conclusions address concerns for privacy. These paragraphs address the DoJ's specific questions about Carnivore. IITRI conclusions are provided in the following paragraphs.

4.3.1 DOJ QUESTION 1

Question. Does Carnivore provide investigators with all, but only, the information it is designed and set to provide in accordance with a given court order?

Answer. When Carnivore version 1.3.4 is used in accordance with a Title III order, it provides investigators with no more information than is permitted by a given court order. Because of performance limitations, in some cases it provides investigators with less information than they are permitted to collect. In the pen mode, it creates files for certain e-mail protocols that can be analyzed to determine more than simple TO and FROM information. Details of our conclusions about collection are provided in paragraph 4.2.3.

IITRI observed thorough training and supervision programs used by the FBI to ensure that agents understand the limitations on the information they can obtain under a court order, the technical means to collect such information, and the consequences of over- or under-collection. Examination of code found no hidden capabilities that would allow Carnivore to collect information without the knowledge of the agents using it.

4.3.2 DOJ QUESTION 2

Question. Does Carnivore introduce any new, material risks of operational or security impairment of an ISP's network?

Answer. Operating Carnivore version 1.3.4 introduces no operational or security risks to the ISP where it is installed. This conclusion is supported by IITRI's architecture evaluation and discussions with ISPs. However, as noted in paragraph 3.4.6, situations may arise in which the ISP is asked to make changes to its operation to accommodate court-ordered surveillance. A change to operations carries some risk and must be approached and implemented with caution.

Carnivore attaches to the ISP network by using a read-only tap. This tap introduces, at most, a 1-bit time delay—far less than most standard network equipment. Discussions with ISP representatives confirmed that the read-only tap is employed for field installation and the FBI takes reasonable steps to minimize interference with ISP operations. Because it is read-only and cannot introduce traffic, Carnivore cannot place an additional load on the ISP network, nor can it alter or otherwise compromise operations.

The remote control link (see paragraph 3.4.3) does establish a path to the Carnivore collection computer within the ISP's secure facility. IITRI found: (1) the link does not provide access to ISP equipment; (2) the link is adequately protected from unauthorized use; and (3) the link cannot be used to access information not already stored on Carnivore.

4.3.3 DOJ QUESTION 3

Question. Does Carnivore risk unauthorized acquisition, whether intentional or unintentional, of electronic communication information by: (1) FBI personnel or (2) persons other than FBI personnel?

Answer. Carnivore version 1.3.4 introduces some risk of both intentional and unintentional unauthorized acquisition of electronic communication information by FBI personnel, but introduces little additional risk of acquisition by persons other than FBI personnel. Because FBI personnel must select the proper settings for Carnivore to comply with the court order, there is always the possibility of error. The chance of an error in specifying Carnivore settings is low because of the large number of individuals involved in framing the court order and determining the feasibility of its implementation by Carnivore. There is, however, the possibility of unintentional error; for example, clicking the radio button for full collection when the operator meant to click the radio button next to it for pen-trap collection. There is no mechanism for detecting or minimizing the likelihood of such an unintentional setup error.

Intentional violations of court-prescribed limitations, or of FBI procedures, are likely to be detected through judicial oversight and FBI supervision. Evaluation of the risk of undetected intentional violation of court-prescribed limitations or of FBI procedures is beyond the scope of this report.

The risk that persons other than the FBI would have access to the collected data is very small. This access is limited by both the electronic authentication devices on the remote telephone line and using user-name and password authentication within the remote access program. ISP personnel can possibly gain access to the data, but they already have access by virtue of having access to their own network. It would also allow them to know the target of the court order, if that was not already given to the ISP.

4.3.4 DOJ QUESTION 4

Question. Does Carnivore provide protections, including audit functions and operational procedures or practices, commensurate with the level of the risks?

Answer. While operational procedures or practices appear sound, Carnivore version 1.3.4 does not provide protections, especially audit functions, commensurate with the level of the risks. Details of these risks are presented in paragraphs 4.2.4, Accountability, and 4.2.5, Integrity.

SECTION 5
RECOMMENDATIONS

Although IITRI specifically excluded questions of constitutionality and of illegal activity by the FBI from this evaluation, IITRI is concerned that the presence of Carnivore and its successors without safeguards as recommended below: (1) fuels the concerns of responsible privacy advocates and reduces the expectations of privacy by citizens at large and (2) increases public concern about the potential unauthorized activity of law enforcement agents. To reduce these concerns, IITRI makes the recommendations in the following paragraphs to add protections that are commensurate with the level of risks inherent in deploying a system such as Carnivore.

5.1 CONTINUED USE OF CARNIVORE

Continue to use Carnivore rather than less-precise, publicly available sniffer software, such as EtherPeek, when precise collection is required and Carnivore can be configured to reflect the limitations of a court order.

Rationale: Carnivore is sniffer software with limitations in the form of filters, which block Carnivore from capturing all the packets that would be captured by generic sniffer software. Accordingly, the use of Carnivore by the FBI presents less of a threat to privacy interests than using generic sniffer software. IITRI determined that Carnivore, when properly configured under a Title III order, does not over-collect. Accordingly, in the Title III context, continued use of Carnivore instead of publicly-available sniffer software is clearly appropriate.

Using ISP resources to accomplish surveillance is a preferred option by the FBI. However, IITRI verified through analysis, experiment, and interviews with ISPs that Carnivore can perform precision surveillance that often cannot be duplicated by the ISP without Carnivore.

5.2 FEDERAL CONTROL

Retain control of Carnivore at the federal level and require DoJ approval of all applications that involve Carnivore systems capable of full content collection.

Rationale: Although it is impossible to quantify the risk of abuse if Carnivore becomes more widely used, the potential is large enough to evoke concern. Controls on use of Carnivore stem from FBI and DoJ standards and practices as opposed to statute. Furthermore, surveillance of electronic communications is subject to less stringent standards than written or oral communications. Enforcement of standards and practices requires centralized responsibility. Centralization of Carnivore applications will ensure technical proficiency and close monitoring of all deployments. Centralization also helps ensure that Carnivore use continues to be limited to certain enumerated felonies, as required for wire and oral communication by 18 U.S.C. § 2516(1), and that the United States Attorneys Manual 9-7.100 requirement for high level DoJ approval for computer-based electronic interception continues to be applied to all Carnivore applications.

5.3 PEN MODE AND FULL MODE

Provide separate versions of Carnivore for pen register and full content collection. Alter the pen mode software to minimize collection of field length.

Rationale: Placement of pen mode buttons next to full mode buttons on the Carnivore setup screen leaves open the possibility of accidental configuration of Carnivore to collect in the full mode when only pen mode collection has been authorized. The best way to eliminate these risks is to have two separate versions of the Carnivore software—one for full mode collection and another for pen mode collection—and to make changes in the pen mode software.

The pen mode software should be rewritten (for all supported protocols) to capture only TO and FROM information plus a time stamp. The current practice of collecting all the packets related to an e-mail message and then writing Xs in fields other than FROM and TO reveals the length of those fields and should be eliminated.

5.4 ACCOUNTABILITY

Provide individual accountability and audit for all Carnivore actions. Each setting, start, stop, or retrieval should be traceable to a specific agent. If necessary, alter the software architecture to take advantage of security features in the operating system.

Rationale: Any system that does not provide for individual accountability is not secure. Given that chain-of-custody for the collected evidence is important, it should be important to know who set up the collection and when it was set up, who started the collection and when it was started, who downloaded the data and when it was downloaded, etc.

The biggest obstacle to retrofitting Carnivore version 1.3.4 to provide for individual accountability is that the Carnivore software is implemented as an application, rather than as a service controlled by an application GUI. An example of a program implemented in the latter fashion is pcAnywhere. Because Carnivore is written as an application rather than a service, it cannot be run as a "background" job. This implementation is why the Carnivore computer must be logged in as "Administrator" at all times.

If Carnivore were rewritten so that the collection software ran as a service, it could be started automatically each time the machine was rebooted, just like pcAnywhere. The GUI could be started by anyone that logs in to the machine. Each user could have a separate user ID and, thus, the Windows NT event logs could be used to provide a level of accountability.

To access the advanced features which allow collection parameters to be set, a user ID should be required in addition to a password. The application should use the Windows NT authentication mechanisms so that a password does not need to be compiled into the code.

The Carnivore system should maintain its own audit trail in addition to the Windows NT event logs. Every time collection is started or stopped, a record should be written to a log that records who performed the action and when it was performed. This log should be part of the collected data file. Each file of collection parameters that is created should also contain a log of who

created or edited it, and when. If possible, all audit data, both Carnivore and Windows NT, should be written to write-once media, so there is no possibility of tampering with the audit trail.

5.5 PHYSICAL CONTROL

Enhance physical control of Carnivore when it is deployed.

Rationale: The lack of physical control of the Carnivore computer could be a problem with regard to chain-of-custody for the data collected. A more tamper-resistant or tamper-evident container would be appropriate. At the very least, tamper seals should be placed over the edges of the box and on the connectors for the keyboard, monitor, and mouse. Then, if the ISP attempts to connect its own peripherals, the seals will be broken, showing evidence of tampering.

pcAnywhere should have control over keyboard and mouse defaults to the remote computer. As given to IITRI, control was shared by the local and the remote computers.

5.6 DATA CONTROL

Explicitly bind collected data to the collection configuration by recording the filter settings with each collected file and add a cryptographic checksum to the recorded file. A log of the filter settings used for a given collection should be explicitly bound to each data file collected using that filter set. (IITRI understands these capabilities are being added in Carnivore 2.0).

Rationale: The collection parameters should be maintained in the same file as the collected data. The entire file should be protected to provide a higher level of confidence that nothing in the collected data or parameters has been changed. This protection would also make forgery of that data more difficult. The cryptovariable (sometimes referred to as a “key”) used for the encryption of the checksum should be different for each Carnivore collection case and the cryptovariable should be withheld from against involved in the case to ensure it is mathematically infeasible for someone to forge a collected dataset.

5.7 DEVELOPMENT PROCESS

Employ a formal development process.

Rationale: Using a formal development process is known to reduce the probability of software errors. This process should include automated requirements tracking, configuration management, and independent verification and validation. (IITRI was told that Carnivore is now being developed in such an environment).

5.8 USER INTERFACE

Provide checks in the user interface software to ensure that settings are reasonable and consistent. Alter the default settings to require users to explicitly decline each filter that is not appropriate versus explicitly include filters that are needed.

Rationale: In the current Carnivore software, it is possible to select filter settings that may not be appropriate or even technically feasible, for example, full TCP collection without any other filters. This selection would collect all TCP information that is available on the local area

network. Specifically, prevent filter settings from being used in which no explicit filtering parameters are provided, i.e., require one or more of IP address or range, port numbers, e-mail address, or text string. (IITRI understands that such checks are planned for future versions.)

The GUI should not include features, such as the startup IP address, which are not actually implemented in the system. These features could cause confusion when the device is set up. Similarly, since the text search box is ignored when SMTP or POP collection for a specific user is enabled, the text search box should be "grayed-out" to prevent confusion whenever a specific SMTP or POP e-mail address is entered.

Currently Carnivore does not filter on IP address, username, port, protocol, etc. unless the user selects the filter and provides necessary parameters. The default is always not to filter. The possibility of accidental over collection would be reduced if the each filter had to be set or explicitly turned off.

5.9 PUBLIC RELEASE

Work toward public release of Carnivore source code by eliminating exploitable weaknesses. Until that can be done, continue independent evaluation of each Carnivore version to assess effectiveness and risks of over- and under-collection.

Rationale: Whether Carnivore source code should be publicly released is a difficult question to answer. Major parts of the computer science community favor public release of encryption algorithms and code to permit the widest possible scrutiny of possible "holes" in the security provided. On the other hand, sources and methods for criminal surveillance and foreign intelligence collection traditionally have not been disclosed. Revealing a hole in encryption security does not provide all those wishing to defeat the encryption with keys; revealing limitations of surveillance software provides those wishing to evade surveillance with the keys to do so. Nevertheless, the public, service providers and privacy advocates believe they understand how telephone wiretap technology works; they do not understand how electronic surveillance works. Unwarranted concerns about the risks of electronic surveillance could be reduced by more complete information about the software tools used for this type of surveillance. That information could be provided either by releasing software code or by continuing the practice of commissioning independent assessments of the effectiveness and risks of particular tools.

5.10 PACKETEER AND COOLMINER

Make Packeteer and CoolMiner available to the defense in any criminal case in which Carnivore data are used. If any bugs remain in those programs, that fact should be disclosed to the defense as well.

Rationale: This offering would help to alleviate negative publicity regarding the DragonWare suite of tools and leave the focus on the Carnivore device itself since that is where the court order is implemented and collection takes place. The Packeteer and CoolMiner programs are only for data analysis.

APPENDIX A
TELEPHONE EAVESDROPPING AS A REFERENCE POINT

Since 1968, federal law has explicitly authorized telephone wiretaps and pen-trap surveillance under judicial supervision. In evaluating concerns about the use of Carnivore, it is appropriate to use telephone surveillance as a reference point.

A.1 MINIMIZATION

When a court authorizes a telephone wiretap under Title III, the telephone service provider is obligated to afford law enforcement authorities access to that part of the public switched telephone network containing targeted conversations. Typically, the law enforcement authorities then install monitoring equipment through which law enforcement agents listen to conversations while recording them. Minimization obligations are satisfied by turning off the equipment when content outside the scope of the Title III order is heard, turning the equipment back on periodically to determine if content within the scope of the order is occurring. The efficacy of minimization thus depends upon the judgment of the human listener.

A.2 PEN REGISTER AND TRAP AND TRACE SURVEILLANCE

A pen register device records the telephone numbers on outgoing calls from a targeted telephone subscriber. A trap and trace device records the telephone numbers of incoming calls to a targeted telephone subscriber. The two forms of surveillance often are used together, in which case they are informally referred to as pen-trap surveillance.

Older analog telephone technologies carried signaling data on the same channel that carried the conversation. The signaling data pertinent to pen-trap surveillance comprised dial pulses or tones. Pen register devices for this older technology detect only the pulses or tones and record them. The devices are incapable of “understanding” the conversations. Thus, even though the signaling data and the content is present on the same channel, the monitoring devices are capable of detecting and recording only the signaling data.

Trap and trace monitoring with older technologies required human intervention to trace the channel for a particular call back through the telephone switching equipment to its origin.

Newer digital switching technologies employ out-of-band signaling, meaning that the signaling data necessary to set up a telephone call is carried on a different channel from the conversation itself, after it reaches the switching office nearest the calling subscriber. With these newer technologies, both pen register and trap and trace monitoring occur only on the signaling channel and not on the channel carrying the conversation. Monitoring on this separate signaling channel reinforces the impossibility of the monitoring equipment acquiring the contents of the conversation.

The newer technologies also make it easier to conduct trap and trace surveillance because the signaling channel carries data about the origin of each call, eliminating the necessity for manual tracing of circuits to determine call origin.

Any surveillance of electronic data communication confronts two fundamentally different realities. First, with the exception of FTP file transfer, data used for addressing—analogous to call set-up information in the voice telephone system—is part of the same data packets used to communicate content. Thus, all communication set-up information is inherently in-band. Second, both the communication set-up data and the content is digital in form, permitting machine processing of both content and set-up data.

Data packets can be processed by computers only because the information in the data packet is formatted according to standards or protocols. This formatting permits a processing computer to distinguish the communication set-up data; for example, the destination IP address, TCP port, or TCP session number or e-mail destination address from the content of the message. If a monitoring device is properly programmed, it can acquire only the set-up data and discard everything else in a packet. On the other hand, if it acquires entire packets, it acquires content as well as set-up information.

These basic differences between data and voice technologies give rise to concerns that any electronic data monitoring under the authority of a pen-trap order is likely to exceed the intended scope of the pen-trap statutes, which have a much lower legal threshold for monitoring than Title III.

APPENDIX B
PUBLICLY AVAILABLE SNIFFER SOFTWARE

Several widely available products permit interception of computer network packets. One of the most popular is Wild Packets, Inc.'s EtherPeek.[liii] A fully capable version of EtherPeek can be purchased for under $1,000. A demonstration version of the software can be downloaded on the Internet for free. EtherPeek can be installed on any PC running Windows 98 in a matter of minutes. EtherPeek permits the user to capture any packet visible to the network interface card on which the software is installed. In other words, EtherPeek can capture any packet traversing a network segment on a local area network. The user can configure EtherPeek's capture utility to capture only those packets using a particular protocol, such as IP, TCP/IP, or IP/HTTP. The capture utility also can target particular IP or Ethernet addresses. After packets are captured, the user can cause the EtherPeek software to group packets comprising a particular session and can examine packet contents in a graphical display that highlights particular elements of transactional information and displays plain text contents in readable ASCII format.

IITIR downloaded the demonstration version of EtherPeek and had no difficulty in configuring it to capture packets comprising a short web browsing session and to capture packets comprising e-mail retrieved through web mail from a Microsoft exchange server. The full content of the e-mail thus retrieved and the full content of the URLs and selected web pages were clearly visible in the plain text ASCII window of the software. Further information about EtherPeek is available from www.wildpackets.com.

18 U.S.C § 2512 makes it illegal to manufacture, assemble, possess, or sell "any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of surreptitious interception of wire, oral, or electronic communications."[liv] Fines and imprisonment for up to five years may result from violation of the prohibition.[lv] No case law or law review literature applies this statutory prohibition to network sniffer software such as EtherPeek. In construing the relationship between the statutory prohibition and sniffer software, two statutory phrases must be interpreted: "device," and "primarily useful for the purpose of the surreptitious interception of . . . electronic communications." It can be argued that sniffer software is not a device; it is a computer program. But sniffer software functions only after it has been installed on a computer, and a computer with installed sniffer software probably qualifies as a device.

An independent argument is that sniffer software such as EtherPeek is only incidentally, and not primarily, useful for surreptitious interception of electronic communications. Electronic communications is defined under Title III as the contents of communications, and not merely transactional data about a communication. Many—arguably, most—of EtherPeek's features focus on the nature of captured packets, and not their contents. The program calculates statistics about packet size, types of packets, and patterns of packet traffic to and from particular nodes. Only one of its many features permits inspection of packet contents.

Regardless of whether the "primarily useful" criterion is satisfied, there is little doubt that sniffer software enables the surreptitious interception of packets; users of a network segment have no

way of knowing whether packets to and from their computers are being intercepted by another node connected to that network segment and running sniffer software.

EtherPeek and similar sniffer software can be used by the FBI—or for that matter, by anyone—to capture as much and more information captured by Carnivore. Such interception would be prohibited by or permitted by Title III, FISA, and the pen-trap provisions to the same extent that interception by Carnivore is prohibited or permitted.

APPENDIX C
DETAILED TEST RESULTS

C.1 TEST 1 NONCONTENT E-MAIL COLLECTION

C.1.1 SCENARIO

A court order authorizes collecting the noncontent header fields on e-mail messages sent to and from the target; it does not permit collecting the SUBJECT header or the body of the e-mail traffic.

C.1.2 PURPOSE

The purpose of this test is to verify that Carnivore does collect and preserve all of the information authorized by the court order and that no other system user's communication can be collected.

C.1.3 FILTER SETUP

To fulfill the collection criteria from the court order, the Carnivore filter used the following parameters for collection:

- Pen mode
- TCP protocol on port 25 (SMTP) and 110 (POP3)
- Target e-mail ID: mdoe@iitri.org

The filter menu screen filled in with the collection parameters is displayed in Figure C-1.

C.1.4 RESULT

Test not passed. Detailed testing steps for this test case are provided in Table C-1. After each step of the test was performed, Packeteer was used to put together all the data packets captured for a session and CoolMiner was used for result analysis. The result of each test step is recorded in the last column of the table. The test results clearly show for test case 1 that only the e-mail activities sent from and received by the target desktop computer was captured by Carnivore and all other types of traffic and other user's e-mail traffic were not captured.

However, Carnivore pen mode collection on an e-mail address did not collect useful to and from information for POP3 users, but did collect correct information for SMTP users. Carnivore did capture the sending traffic (SMTP port 25) of the e-mail traffic that was sent from and to the target. For e-mail sent from the target, CoolMiner shows the target's e-mail address in the From: column. For e-mail sent to the target, instead of showing the target's address in the To: column, CoolMiner shows the sender's (a nontarget) address in the From: column. Note that this information can typically only be collected if the sender of the e-mail is on the same subnetwork as the target because the SMTP information is collected as the e-mail is being sent, not received. If the sender is on a different subnetwork, Carnivore would see the message when retrieved using POP3.

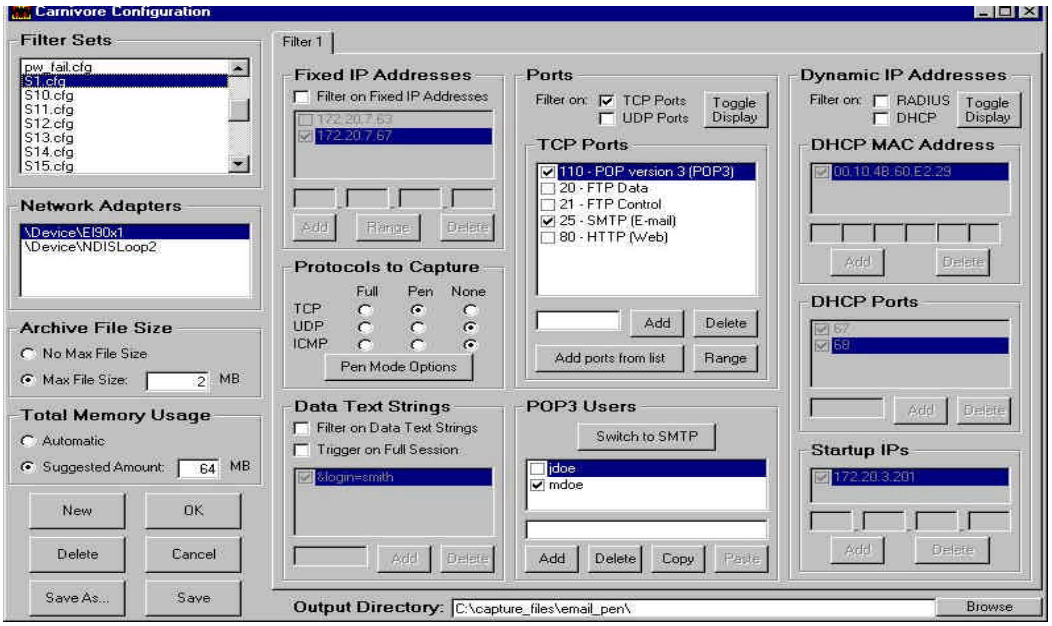

Figure C-1. Filter for Noncontent E-mail Collection

Table C-1. Test Steps and Results for Test Cases 1–4

Step	Carnivore Condition	Desktop Computer Fixed IP Address 172.20.3.63	Laptop Computer MAC Address 00 10 4B 60 E2 29	Test Result Packets Captured by Carnivore: Y/N							
				Test Case 1		Test Case 2		Test Case 3		Test Case 4	
				Exp	Act.	Exp	Act.	Exp	Act.	Exp	Act.
1	Stopped	Logon Mdoe	Off-line	N	N	N	N	N	N	N	N
2	Start										
3		Send e-mail to Jdoe@iitri.org		Y	Y	N	N	N	N	Y	Y
4			Boot up	N	N	N	N	N	N	N	N
5			Logon Jdoe	N	N	N	N	N	N	N	N
6			Receive e-mail	N	N	N	N	N	N	N	N
7			Send e-mail to Mary Doe	N	Y	N	N	N	N	N	N
8			FTP	N	N	N	N	Y	Y	N	N
9			Web Browsing	N	N	Y	Y	N	N	N	N
10		Receive e-mail		Y	N	N	N	N	N	Y	Y
11		FTP		N	N	N	N	N	N	Y	Y
12		Web browsing		N	N	N	N	N	N	Y	Y
13			Send e-mail to a nontarget user	N	N	N	N	N	N	N	N
14			Logoff Jdoe	N	N	N	N	N	N	N	N
15	Stop										

The FBI provided a patch to fix the problem. After installing the patch, this test case was tested again. The Carnivore raw data for SMTP appeared to be correct; however, data are still missing on the POP3 e-mail receiver's address. The CoolMiner results show that for SMTP traffic, the from e-mail address (the target's in this test) is correctly displayed, but the to address (the nontarget's in this test) is not shown. Packeteer and CoolMiner appear to be looking for the other e-mail addresses in the to and from lines in the e-mail message, which Carnivore has purposely blanked out to avoid collecting information about communication between nontargeted entities. Carnivore should instead be looking for the rcpt-to lines, which is properly collected. Without this information, all an agent would know is that the target has either sent or received e-mail, but not to or from whom. Thus, pen mode collection for e-mail is not of much use. The test also shows that the time-stamp problem is fixed and is consistent with the system collection time.

Figure C-2 shows the result of pen mode e-mail collection that does not collect any e-mail subject and contents.

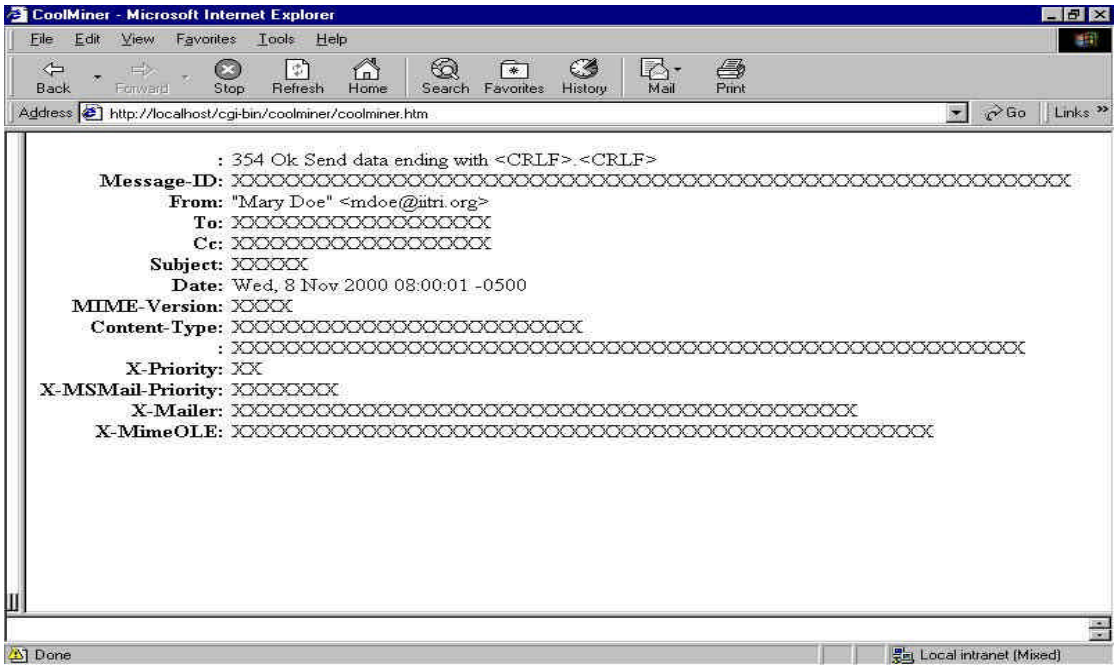

Figure C-2. Result of Pen Mode E-mail Collection

The CoolMiner analysis result for pen mode e-mail collection provides information on how many bytes are transferred between the client and the server. Recording this information might be an issue of over-collecting because the court order only authorizes collecting e-mail from and to addresses, Also, in the Carnivore raw data the e-mail header is replaced by Xs, which can be counted to determine the amount of data.

To verify that Carnivore records the number of Xs according to the length of the data, IITRI ran two more e-mail pen mode tests; one with a length of 17 bytes of data in the subject field and the other with 29 bytes of data. Results show that an extra X was appended to the Carnivore raw data of the e-mail subject fields, i.e., 18 Xs in the subject field for the first e-mail and 30 Xs in the subject field for the second e-mail.

C.2 TEST 2 NONCONTENT WEB BROWSING COLLECTION

C.2.1 SCENARIO

A court order authorizes collecting source and destination information for HTTP activities by user John Doe. Specifically, the order authorizes collecting the IP address to which John Doe opens an HTTP connection. The order does not authorize collecting the complete URL portion of the browsing activity.

Also, the target John Doe is configured to connect to the network through a DHCP server. John's laptop MAC address is 00104B60E229.

C.2.2 PURPOSE

To verify that Carnivore collects and preserves all of the target's HTTP connection information authorized by the court order, only that information, and not other users' web browsing source and destination information or content.

C.2.3 FILTER SETUP

To fulfill the collection criteria from the court order, the Carnivore filter used the following parameters for collection:

- Pen mode
- TCP protocol on port 80 (HTTP)
- The target's MAC address 00104B60E229

The filter screen filled in with the collection parameters is displayed in Figure C-3.

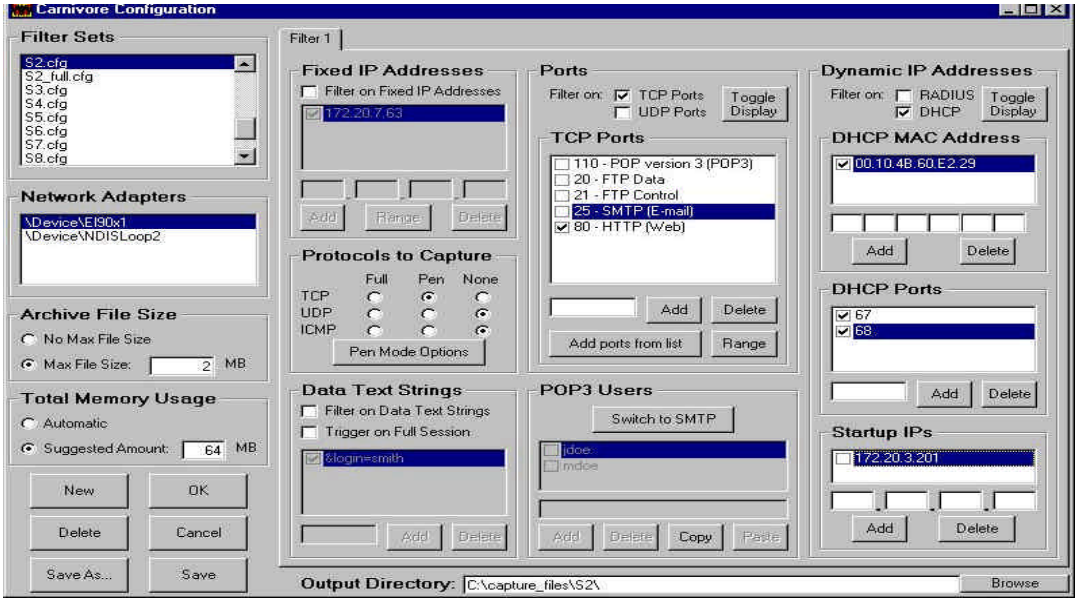

Figure C-3. Carnivore Filter for Noncontent Web Browsing Collection

C.2.4 RESULT

Test passed. Detailed testing steps for this test case are provided in Table C-1. After each step of the test was performed, Packeteer and CoolMiner were used to perform results analysis. The result of each test step is recorded in the last column of the table. The test results show for test case 1 that only the activities of Web browsing performed from the target laptop computer was captured and all other types of traffic and other user's traffic (i.e., e-mail in this case) were not captured by Carnivore.

The CoolMiner analysis shows that only the HTTP (port 80) source and destination connections were captured by Carnivore from the target's laptop computer and no other types of traffic were captured from this collection.

Figures C-4 and C-5 present screen images from CoolMiner analysis. Figure C-4 shows the connection screen and Figure C-5 shows an example of the session screen that is displayed by clicking on the Start Time column of the first row on the connection screen. Ten HTTP connections were captured by Carnivore, and the first one was from the client of IP address 172.020.003.203 to the server of IP address 207.046.185.007. The target's laptop was assigned by the DHCP server to use the dynamic IP address 172.020.003.203.

Again, the results show that from the pen mode collection on HTTP port 80, none of the web browsing content or URL were collected; only the client and server HTTP connection information was collected. Collection does not start until after Carnivore determines the dynamic IP address, by viewing the DHCP protocol packets that request and assign the IP address.

The CoolMiner analysis results for pen mode web browsing activities collection provide information on how many bytes are transferred between the client and the server. This information is recorded in the To Server, and To Client columns of Figure C-4. Recording this information might be an issue of over-collecting because the court order only authorizes collecting the IP addresses of web activities, but none of the information on data sizes can be collected.

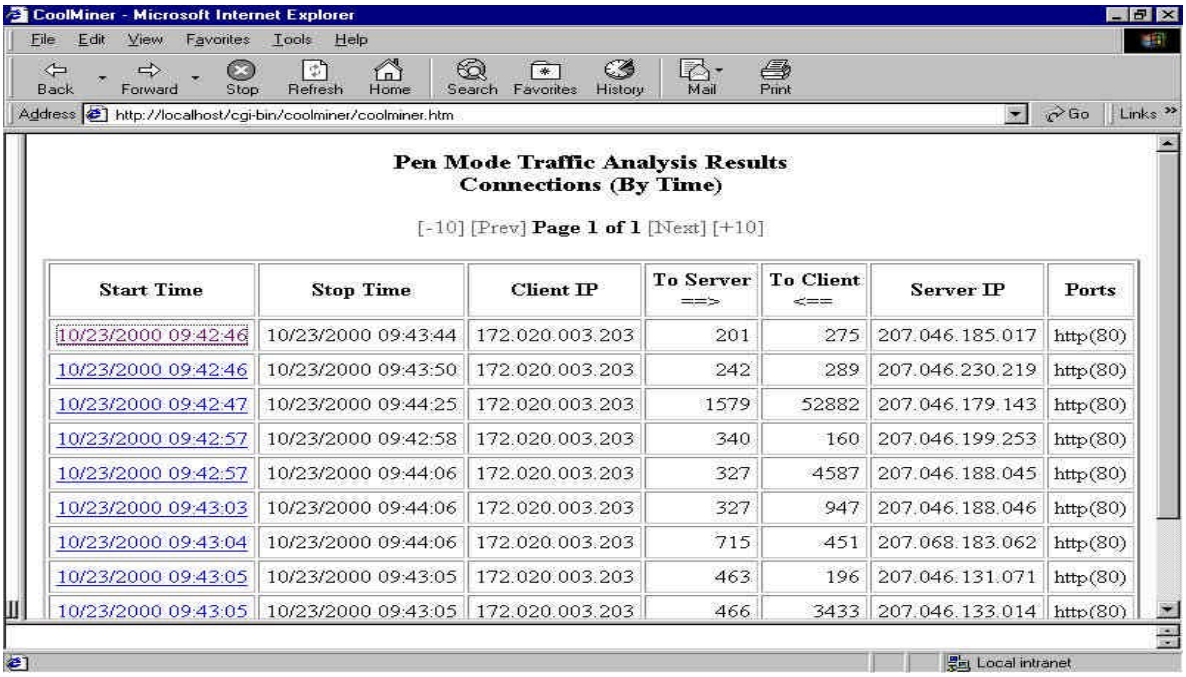

Figure C-4. Test Result for Noncontent Web Browsing Collection

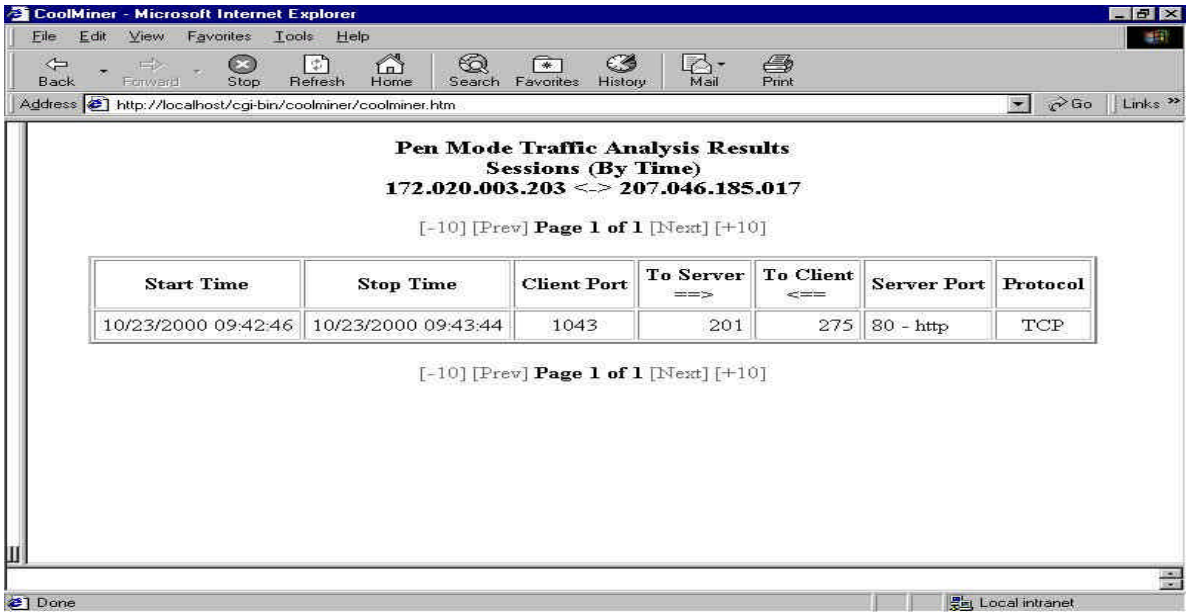

Figure C-5. Test Result for Noncontent Web Browsing Collection

C.3 TEST 3 NONCONTENT FILE TRANSFER ACTIVITY COLLECTION

C.3.1 SCENARIO

A court order authorizes collecting source and destination information for FTP activity by John Doe. Specifically, the order authorizes collecting the IP address to which John opens an FTP connection.

In addition, the target John Doe is configured to connect to the network through a DHCP and John's laptop computer MAC address is 00104B60E229. John is currently online and has been assigned an IP address of 172.20.3.201.

C.3.2 PURPOSE

To verify that Carnivore collects and preserves all of the target's inbound and outbound FTP traffic (i.e., connections to TCP ports 20 and 21) information authorized by the court order, only that information, and not other users' FTP source and destination information or contents.

C.3.3 FILTER SETUP

To fulfill the collection criteria from the court order, the Carnivore filter used the following parameters for collection:

- Pen mode
- TCP protocol on FTP ports (20 for data and 21 for control)
- The target's MAC address 00104B60E229
- Startup IP entry field is not required. (Carnivore ignores this entry.)

The filter filled in with the collection parameters is displayed in Figure C-6.

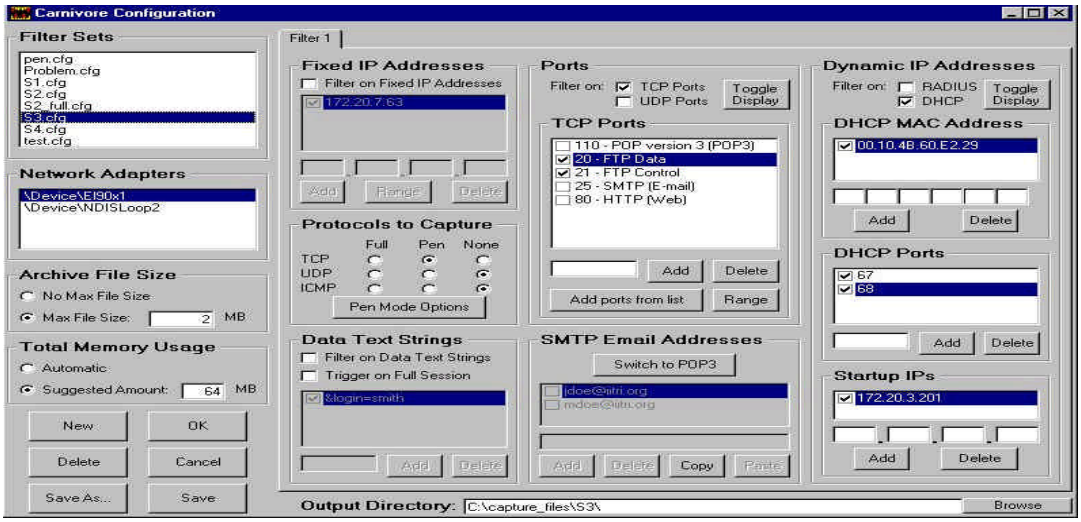

Figure C-6. Filter Setup for Noncontent FTP Collection

C.3.4 RESULT

Test passed. Detailed testing steps for this test case are provided in Table C-1. After each step of the test was performed, Packeteer and CoolMiner were used to perform results analysis. The result of each test step is recorded in the last column of the table. The test results show only the connections of FTP activities from and to the target laptop computer were captured by Carnivore; all other types of traffic (i.e., web browsing in this case) and other user's traffic (i.e., e-mail from Mary Doe) were not captured.

The CoolMiner analysis shows that only the FTP (ports 20 and 21) inbound and outbound connections were captured from the target's laptop computer and no other types of traffic were captured from this collection. Figure C-7 provides the screen image from CoolMiner analysis. The heading of this screen shows that all of the sessions occurred on the connection between the client's IP address and the FTP server's IP address. There were eight FTP sessions in total, but no content information for any of these sessions was collected by Carnivore. The Startup entry is completely ignored by Carnivore software. Collection does not start until after Carnivore determines the dynamic IP address by viewing the DHCP protocol packets that request and assign the IP address.

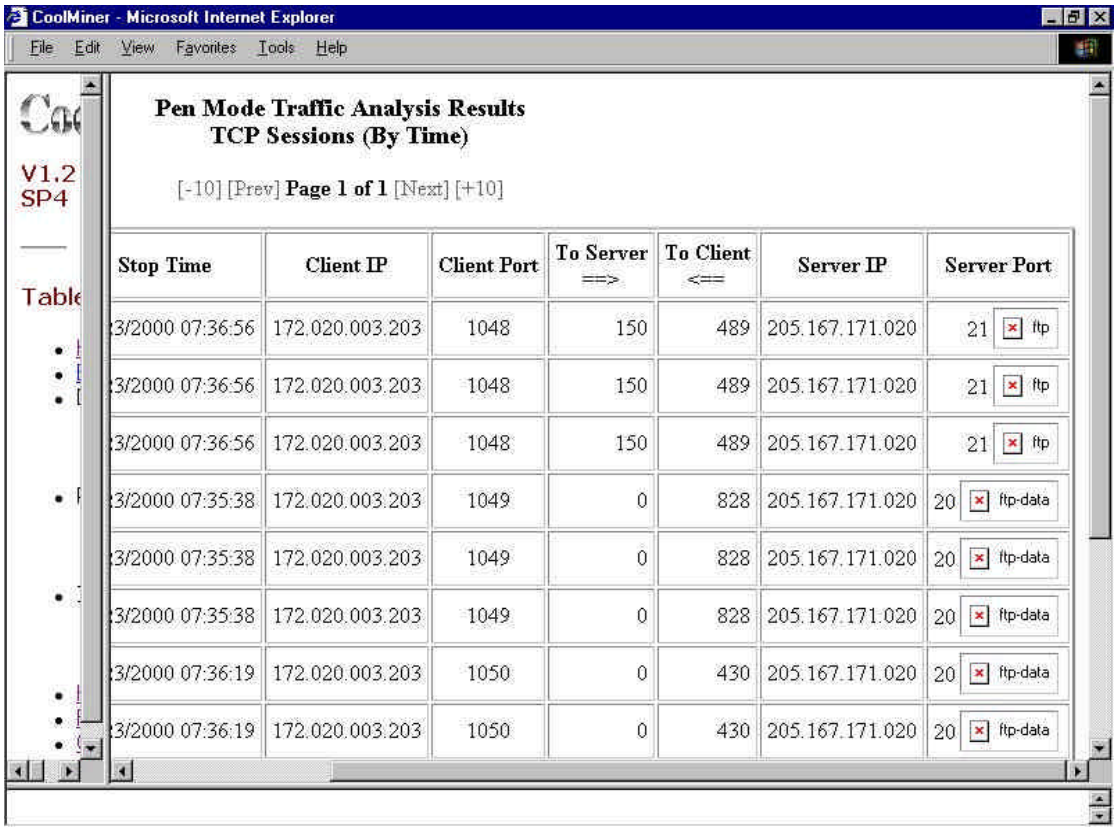

Figure C-7. Test Result of Noncontent FTP Collection

The CoolMiner analysis results for pen mode collection of FTP activities provide information on how many bytes are transferred between the client and the server. This information is shown in

the To Server, and To Client columns of Figure C-7. Recording this information might be an issue of over-collecting because the court order only authorizes collecting the IP addresses of the source and destination, but none of the information on message sizes can be collected.

C.4 TEST 4 FULL COLLECTION ON A FIXED IP ADDRESS

C.4.1 SCENARIO

A court order authorizes intercepting the contents of communications to or from Mary Doe who has the fixed IP address 172.20.3.63. Specifically, the order authorizes intercepting all network communications to or from the target user's IP address.

C.4.2 PURPOSE

Verify that Carnivore collects and preserves all the authorized information from the target's communications and that no other users' (i.e., other IP addresses) communications can be collected.

C.4.3 FILTER SETUP

To fulfill the collection criteria from the court order, the Carnivore filter used the following parameters for collection:

- Full mode
- TCP, UDP, and ICMP protocols
- TCP ports do not need to be checked because the default is to collect all TCP ports. (It would be the same as selecting the range of ports to be 1–65535 to collect all TCP communications.)
- The target's fixed IP address 172.20.3.63

The filter screen filled in with the collection parameters is displayed in Figure C-8.

C.4.4 RESULT

Test passed. Detailed testing steps for this test case are provided in Table C-1. After each step of the test was performed, Packeteer and CoolMiner were used to perform results analysis. The result of each test step is recorded in the last column of the table. The test results show for test case 4 that all communications in this test (i.e., e-mail, file transfer, and web browsing activities) to and from the target's fixed IP address (i.e., a desktop computer) were captured by Carnivore.

Figure C-9 illustrates the CoolMiner result of the communication collection.

Clicking on the FTP protocol on the screen shown in Figure C-9 displays the full content of the FTP session as shown in Figure C-10.

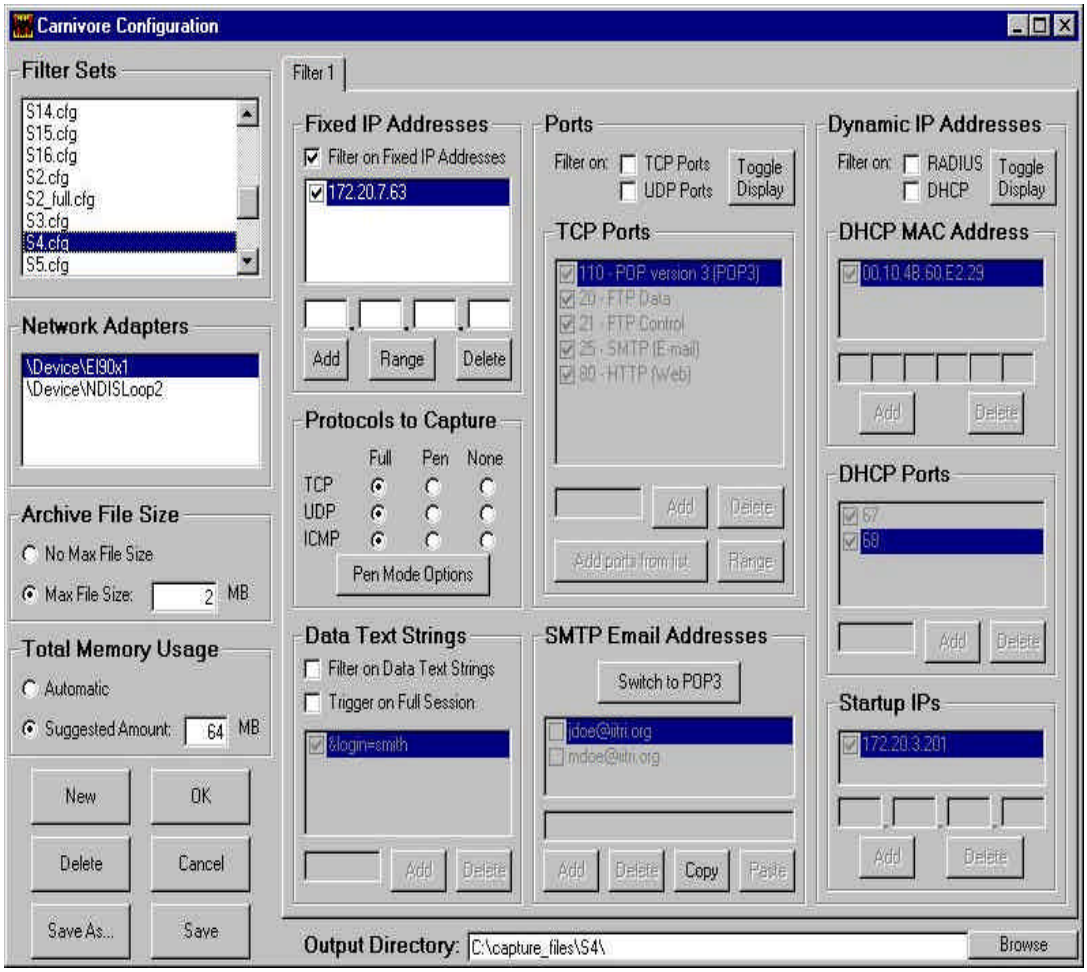

Figure C-8. Filter Setup for Full Collection on a Fixed IP Address

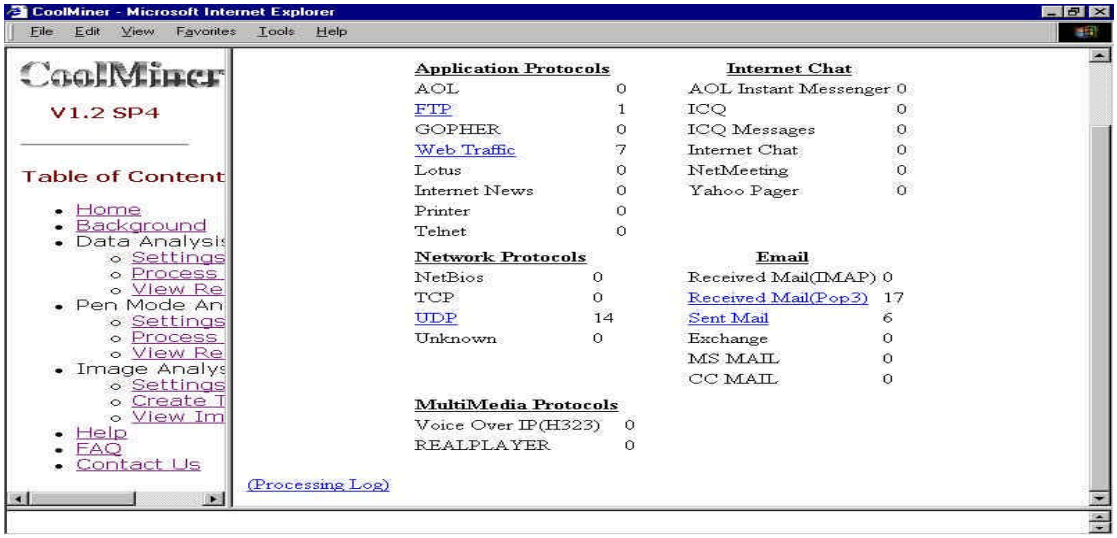

Figure C-9. CoolMiner Result of All Communication Collection

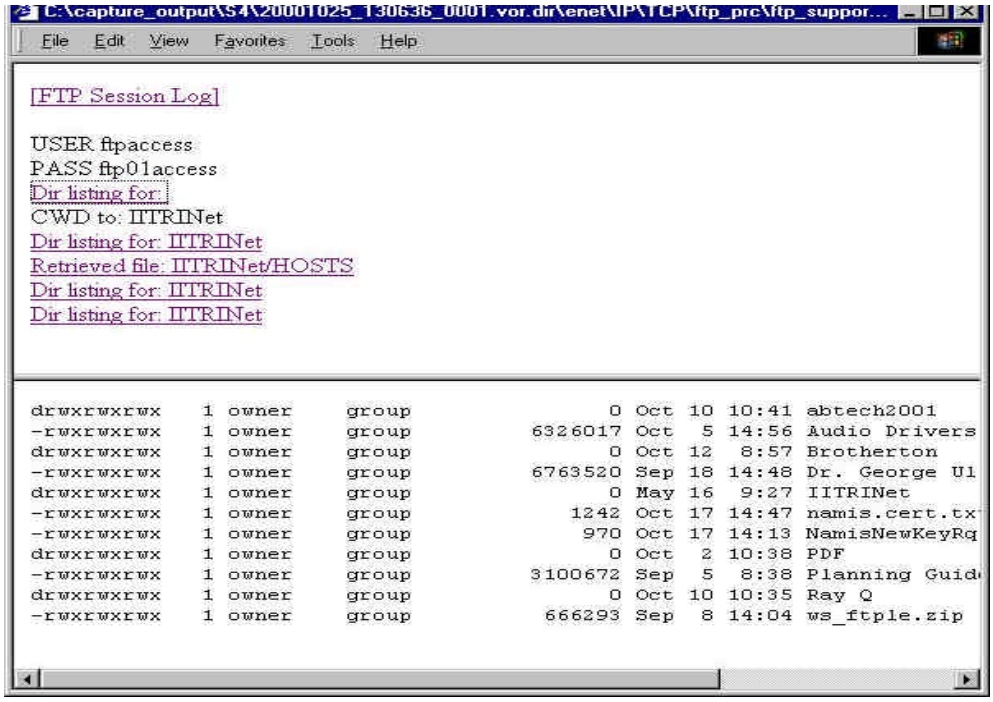

Figure C-10. Test Result of a Content FTP Collection

C.5 TEST 5 E-MAIL CONTENT COLLECTION

C.5.1 SCENARIO

A court order authorizes intercepting the contents of e-mail communications to or from Mary Doe who has the e-mail address mdoe@iitri.org.

C.5.2 PURPOSE

The purpose of this test is to verify that when configured to collect the authorized information from inbound and outbound (i.e., SMTP connections to TCP destination port 25 and POP3 connections to TCP destination port 110), Carnivore collects and preserves all of the authorized information and not other users' communications.

C.5.3 FILTER SETUP

To fulfill the collection criteria from the court order, the Carnivore filter used the following parameters for collection:

- Full mode
- TCP protocol on SMTP (port 25) and POP3
- The target's SMTP e-mail address is mdoe@iitri.org
- The target's POP3 user ID is mdoe

The filter screen filled in with the collection parameters is displayed in Figure C-11.

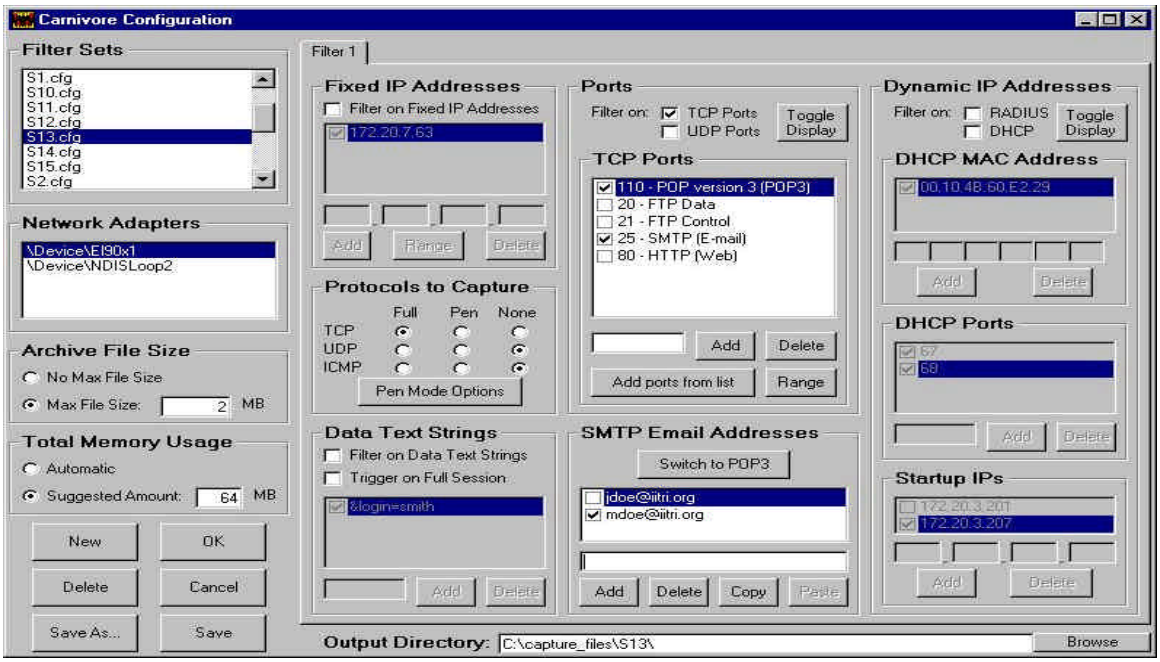

Figure C-11. Filter Setup for Content E-mail Collection

C.5.4 RESULT

Test passed. The e-mail of a target can be collected even when no IP address is input to the filter. The required inputs are SMTP (port 25), POP3 (port 110), and target's e-mail ID. This condition is true when the target is either at a fixed IP address or at a dynamic IP address. The filter does not allow any input to the user e-mail ID until the SMTP and POP3 ports are selected.

Figure C-12 illustrates the content of e-mail that was collected by Carnivore.

Figure C-12. Test Result of Content E-mail Collection

C.6 TEST 6 ALIAS E-MAIL COLLECTION

C.6.1 SCENARIO

A court order authorizes collecting the content of e-mail messages sent to and from Mary Doe. The ISP determined that Mary's Web e-mail address is marydoe@location.org. However, Mary made the alias "NOBODY" for her outgoing e-mail address. Carnivore does not collect Mary's e-mail by filtering on her original user ID marydoe.

C.6.2 PURPOSE

Verify that when configured to collect SMTP (port 25) and POP3 (port 110) e-mail messages and the target is using an alias for the original e-mail address, Carnivore cannot collect the target's mail by filtering on the target's original e-mail address.

C.6.3 FILTER SETUP

To fulfill the collection criteria from the court order, the Carnivore filter used the following parameters for collection:

- Full mode
- TCP protocol on SMTP (port 25) and POP3 (port 110)
- The target's POP3 user ID is marydoe
- The target's SMTP e-mail address is marydoe@location.org

The filter screen filled in with the collection parameters is displayed in Figure C-13.

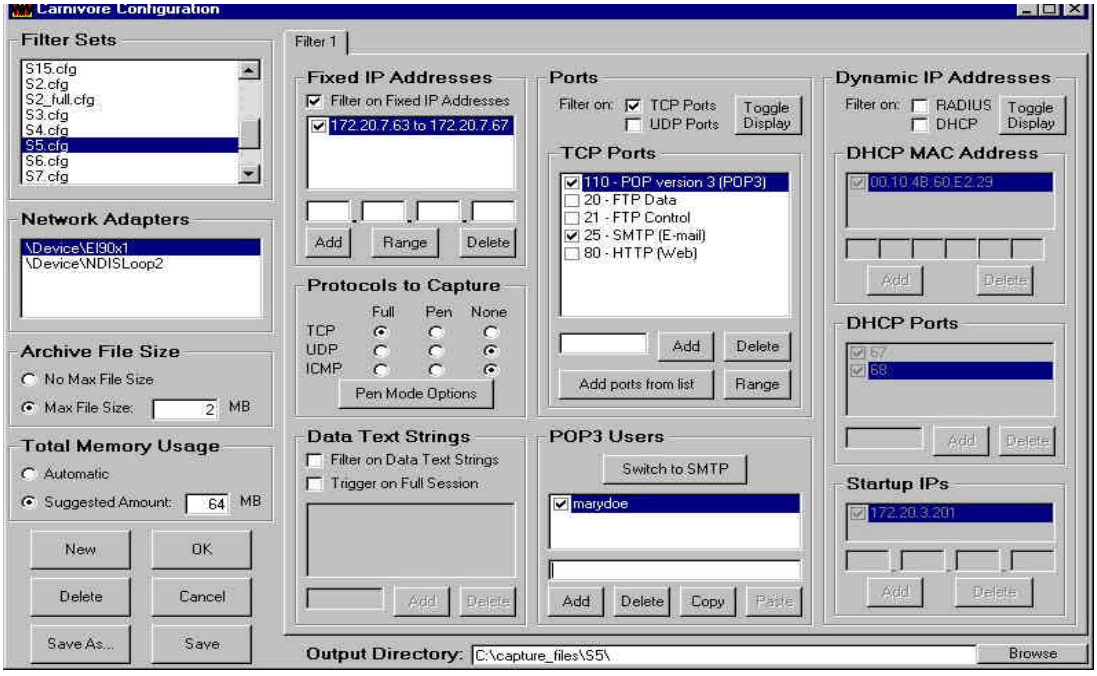

Figure C-13. Filter Setup for Alias E-mail Collection

C.6.4 RESULT

Test passed. A different address NOBODY@webmail6.location.org was seen at the receiver side; however, Carnivore did not capture this alias e-mail because the filter was set up for collection using the target's original e-mail ID.

Even though Mary made the alias "NOBODY" for her outgoing e-mail address, she still has to use "marydoe" as her login ID to get into her web mail account. Therefore, if the filter was set up using Text String data field with value of "&login=marydoe", which is Mary's original user ID, the result would be different. Carnivore would then collect web mail traffic via HTTP (port 80) on Mary's original user ID.

C.7 TEST 7 FILTERING TEXT STRING ON WEB ACTIVITY COLLECTION

C.7.1 SCENARIO

Test if Carnivore collects web browsing contents that contain a specific given text string. Both fixed and dynamically allocated IP addresses are used for the computers that generate the web traffic for this collection.

C.7.2 PURPOSE

When configured to collect HTTP (port 80) web browsing activities, verify that Carnivore collects only the web traffic containing the given text string, without over-collecting.

C.7.3 FILTER SETUP

To fulfill the collection criteria from the court order, the Carnivore filter used the following parameters for collection:

- A fixed IP address and a DHCP address
- Full mode
- TCP protocol on HTTP (port 80)
- Text string "delicious"

The filter screen filled in with the collection parameters is displayed in Figure C-14.

C.7.4 RESULT

Test passed. Detailed testing steps for this test case are provided in Table C-2. Regardless of what web traffic came from the laptop or desktop computer, the results were consistent. Only those web pages containing the text string "delicious" were captured by Carnivore and those web pages that did not contain the specified text string were not captured.

CoolMiner showed many TCP sessions without finding the expected web pages, though those pages might contain the word "delicious". Carnivore did not find these pages because the browser was looking for automatic refresh web pages from the servers, but Carnivore cannot

resolve a domain name in this situation. Figure C-15 shows the CoolMiner result of a web page containing the text string “delicious”.

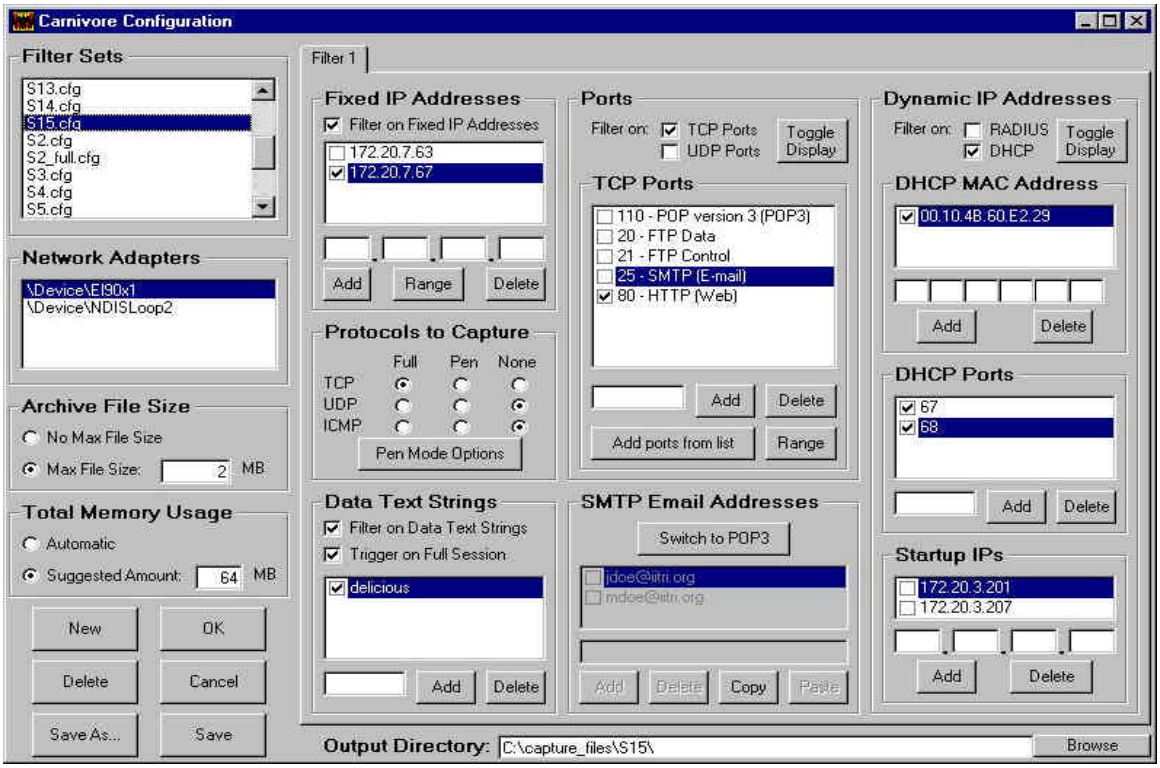

Figure C-14. Filter Setup for Text String Filtering on Web Activity Collection

Table C-2. Test Steps and Results for Filtering Text on Web Activities

Step	Carnivore Condition	Filter	Desktop Computer	Laptop Computer	Test Result Packets Captured by Carnivore: Y/N	
					Expected	Actual
1	Stopped	Setup as above		Off line		
2	Start					
3				Boot up		
4			Web browsing pages containing “delicious”		Y	Y
5				Web browsing pages containing “delicious”	Y	Y
6			Web browsing pages without “delicious”		N	N
7				Web browsing pages without “delicious”	N	N
8	Stop					

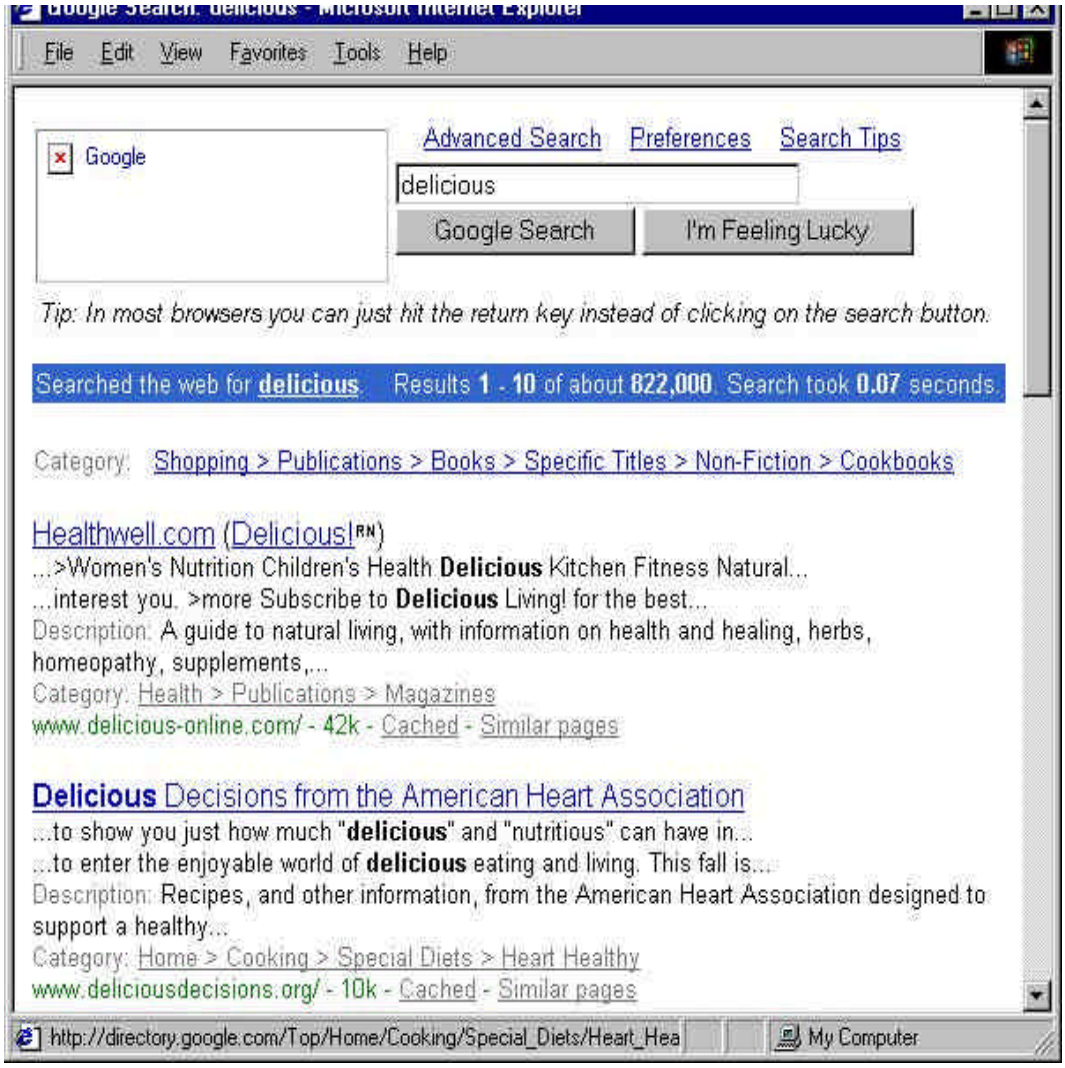

Figure C-15. A Web Page Containing the Text String "delicious"

C.8 TEST 8 POWER FAILURE AND RESTORATION

C.8.1 SCENARIO

When Carnivore is collecting Mary Doe's e-mail, an electrical power outage occurs, and Carnivore is terminated ungracefully. After the power is restored, Carnivore continues to collect Mary Doe's e-mail.

C.8.2 PURPOSE

Verify that after the power is restored, Carnivore automatically starts up and continues to collect what it was originally set up to collect. Also, verify that Carnivore recovers all of the data that was collected before the outage occurred.

C.8.3 FILTER SETUP

To collect Mary Doe's e-mail, the Carnivore filter was set up using the following parameters:

- Full mode
- TCP protocol on SMTP (port 25) and POP3 (port 110)
- SMTP user is mdoe@iitri.org
- POP3 user is "mdoe"

The filter screen filled in with the collection parameters is displayed in Figure C-16.

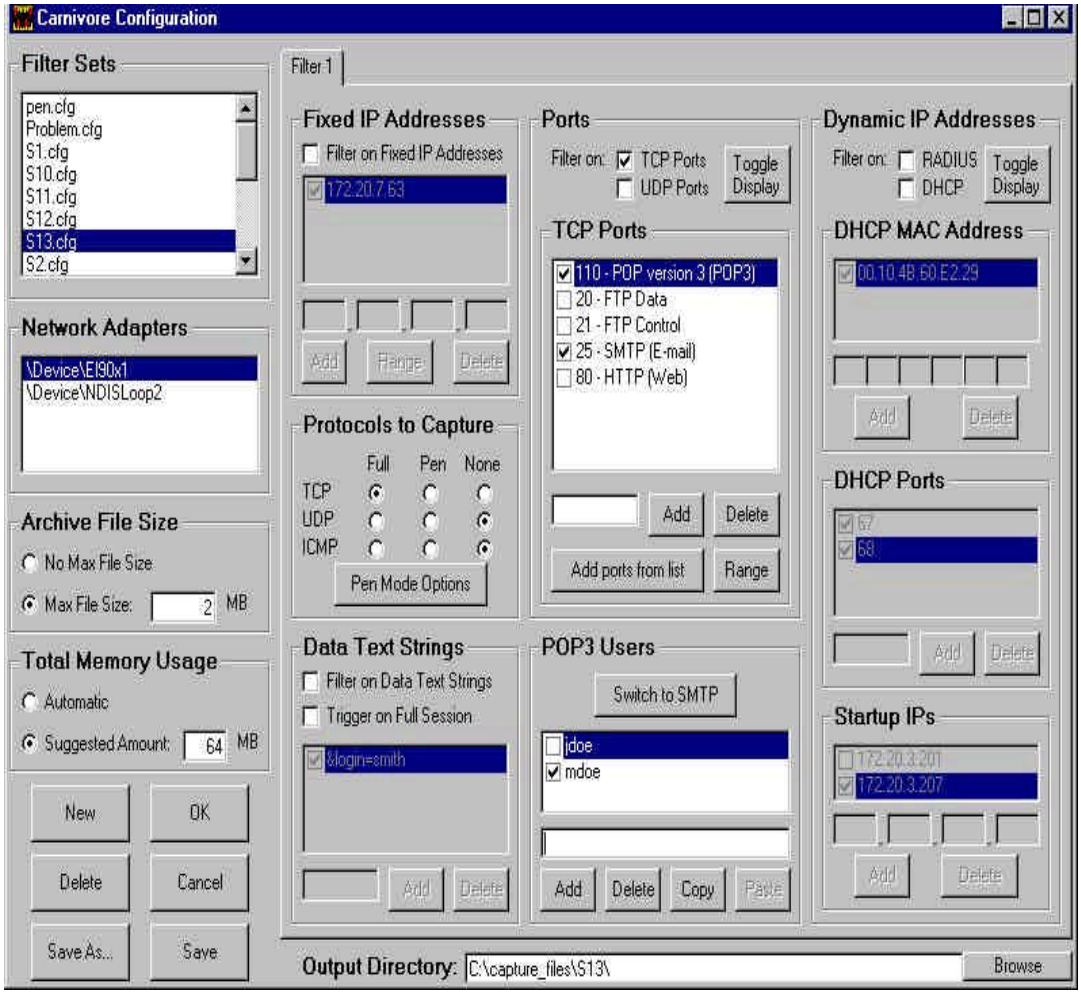

Figure C-16. Filter Setup for Power Failure Test

C.8.4 RESULT

Test not passed. Carnivore did not recover consistently to a collecting state. The primary test system exhibited a Telephony Application Programming Interface error in connecting to the Ethernet card. It appears this error is caused by a race condition within Carnivore. The backup Carnivore system used in testing seemed not to exhibit this error condition. Others, including

those at the FBI lab, exhibit this error condition intermittently. The FBI is going to investigate and fix this potential error.

The first e-mail sent out before the power outage occurred was not written to disk by Carnivore. This condition was recorded as the actual result of test step 3 in Table C-3. Repeated tests all showed the same failure. After the power was restored and the system rebooted, the data file currently open for writing always ended up being a zero-byte file. The FBI developers concluded that this error is a problem with Carnivore in general and is the result of a trade-off between processing speed, padding in the collected data to a block size, or possibly losing some data. The system keeps the data in the memory buffer until the specified block size of data is collected or the collection is stopped. Then the data are written to the disk. The block size for the hard disk is 128 kbytes and for the removable disk, either Jaz drive or Zip drive, is 64 kbytes.

Table C-3. Test Steps and Results for Power Failure Test

Step	Carnivore Condition	Filter	Desktop Computer	Laptop Computer	Test Result Packets Captured by Carnivore: Y/N	
					Expected	Actual
1	Stopped	Setup as above	Login mdoe		N	N
2	Start				N	N
3			Send out the first e-mail		Y	N
4	Powered off				N	N
5			Send out the second e-mail		N	N
6	Power back on, started					
7			Send out the third e-mail		Y	Y
8	Stop					

C.9 TEST 9 TCP ALL PORTS FULL MODE COLLECTION

C.9.1 SCENARIO

Without providing a fixed IP address, DHCP, search text string, TCP ports, and e-mail users to the Carnivore filter, the system collects all of the TCP communications passing through the network segment to which Carnivore is connected.

C.9.2 PURPOSE

Verify that Carnivore has the capability to collect all of the communications passing through the tapping device.

C.9.3 FILTER SETUP

The simplest filter setup for Carnivore to collect all of the TCP communications was to check TCP collection on full mode without providing any other parameters.

The filter screen filled in with the collection parameters is displayed in Figure C-17.

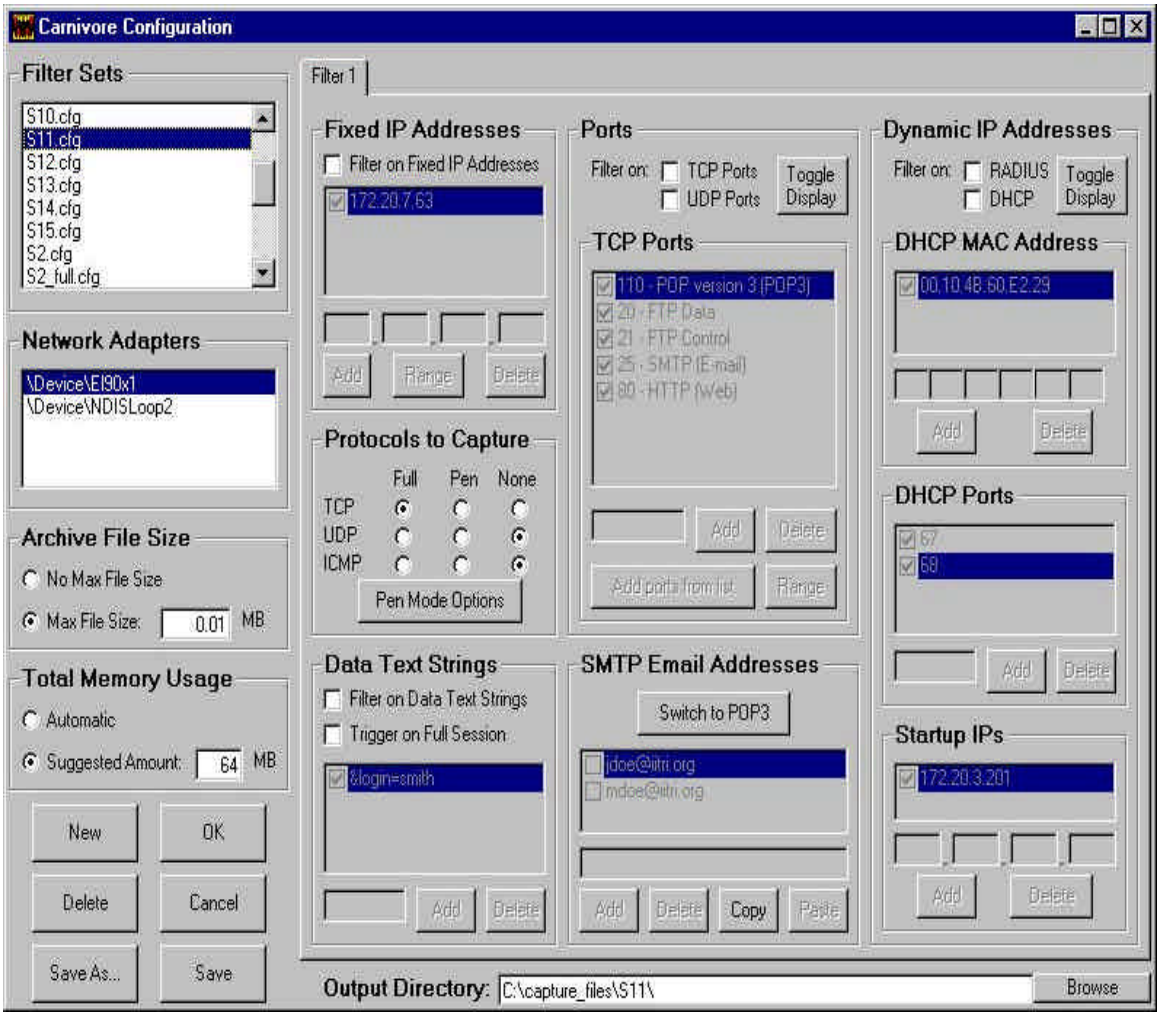

Figure C-17. Filter Setup for TCP All Ports Full Collection

C.9.4 RESULT

Test passed. Detailed testing steps for this test case are provided in Table C-4. The results show that all TCP communications on the network segment being sniffed were captured by Carnivore.

When turning on TCP full mode collection and not selecting any port, the default is to collect traffic from all TCP ports.

Figure C-18 shows the CoolMiner results. FTP, web, POP3, SMTP, and Microsoft Exchange e-mail traffic are all captured by Carnivore and displayed by CoolMiner.

Table C-4. Test Steps and Results for Full TCP Ports Collection

Step	Carnivore Condition	Filter	Desktop Computer	Laptop Computer	Test Result Packets Captured by Carnivore: Y/N	
					Expected	Actual
1	Stopped	Setup as above	Login mdoe	Off line	N	N
2	Start				N	N
3				Boot up		
4				Login jdoe		
5			Send an e-mail to jdoe		Y	Y
6			FTP down load a file		Y	Y
7			Web browsing		Y	Y
8				Send an e-mail to mdoe	Y	Y
9				FTP down load a file	Y	Y
10				Web browsing	Y	Y
11				Receive an e-mail	Y	Y
12				TCP to a remote computer	Y	Y
13			Receive an e-mail		Y	Y
14	Stop					

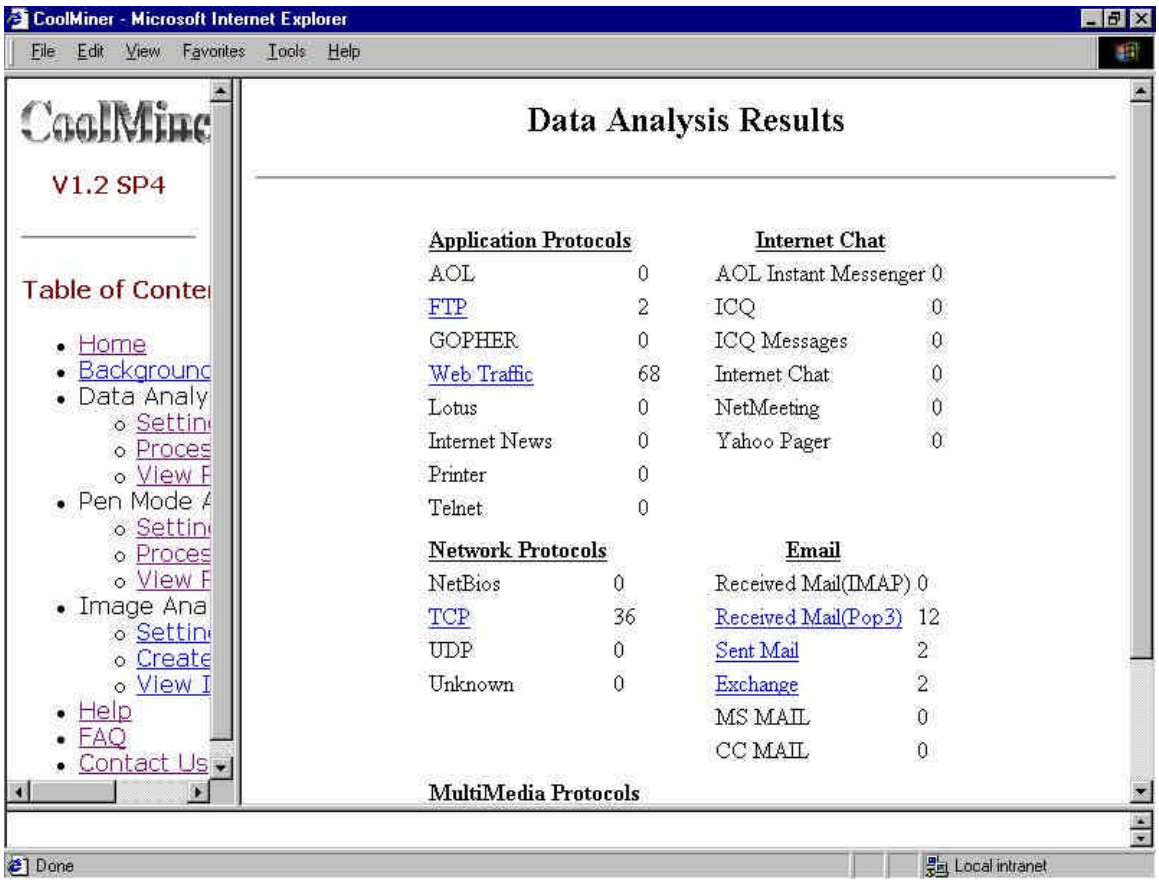

Figure C-18. Test Result of All Ports TCP Collection

C.10 TEST 10 DHCP DATA ENTRIES FROM THE FILTER

C.10.1 SCENARIO

Without entering a fixed IP address and DHCP information to the filter, Carnivore collects all communication passing the tapping device. This test was proved true from test case 9 in paragraph C.9.

The Carnivore filter screen provides three entry fields for DHCP setup, i.e., MAC address, Ports (67 and 68), and Startup IP. Also need to determine what data must be entered to the filter to collect communication from a specific DHCP-configured device. It is assumed that the Startup IP field can be used by Carnivore to begin collecting immediately the communication of a target who is already on line.

C.10.2 PURPOSE

There are two purposes of this test

1. Determine what data needs to be entered for DHCP.
2. Verify that the Startup IP is useful for Carnivore to capture a target who is already on line before Carnivore starts collecting, and, therefore, there is no need to force a DHCP exchange when a correct Startup IP was set up in the filter.

C.10.3 FILTER SETUP

Three filters are used for this test

- The first filter is checked only on the DHCP ports; no other DHCP parameters are provided. Two DHCP ports, 67 and 68, are used to track the system boot-up. Carnivore must use these ports to capture the DHCP exchange packets.
- In addition to the parameters from the first filter, the second filter includes a MAC address.
- In addition to the parameters provided from the first and second filters, the Startup IP address, which is the dynamic IP address assigned to the laptop computer after it is brought up on line, is also provided to the filter.

The screens for setting up these three filters are displayed in Figures C-19, C-20, and C-21, respectively.

C.10.4 RESULT

Test passed for Purpose 1, but did not pass for Purpose 2. Detailed testing steps for this test case are provided in Table C-5. Steps 1 through 11 were used to test Purpose 1. Both MAC and DHCP ports are required data entries for the filter to collect communication from a specific dynamically-configured IP address.

Steps 12 through 16 were used to test the Startup IP entry field. Without forcing a DHCP exchange on the laptop computer, even though a startup IP was given, Carnivore cannot capture the e-mail sent from the laptop computer. This test proves that the Startup IP field is not used by Carnivore as it was originally assumed. This condition was also verified by the FBI developers who stated that the Startup IP part of Carnivore 1.3.4 code was all commented out, but the GUI portion had not been removed.

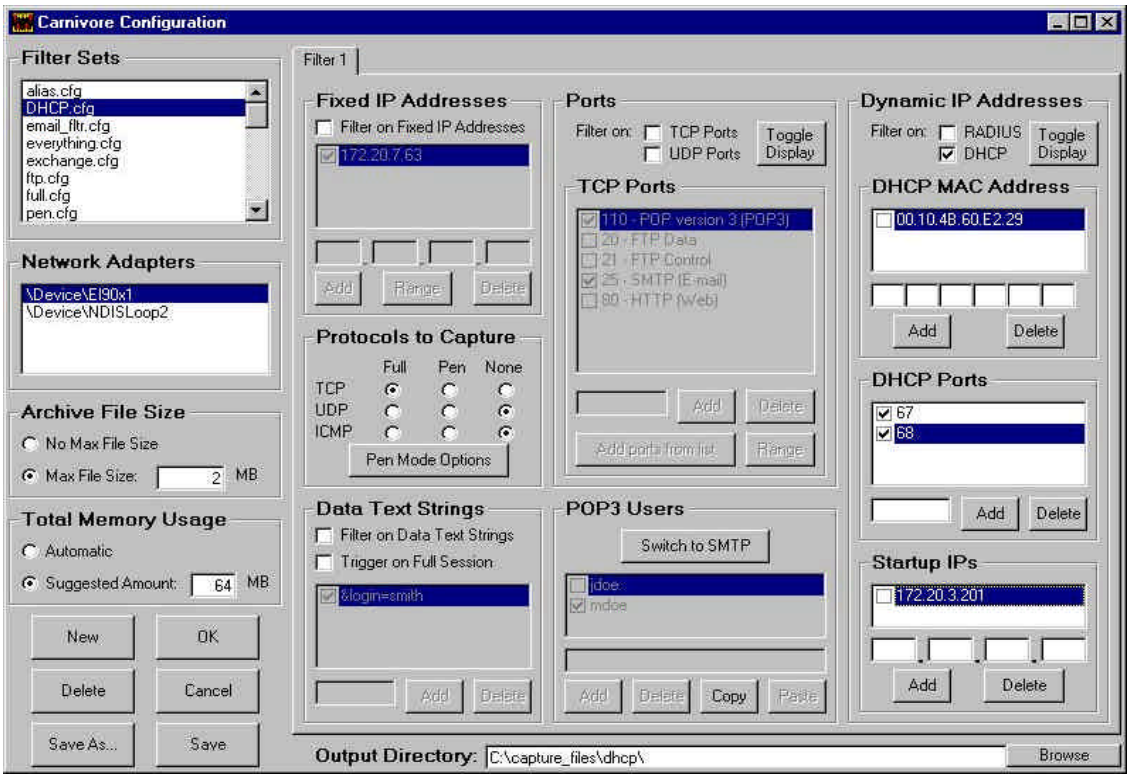

Figure C-19. Filter Setup 1 for DHCP Data Entries Test

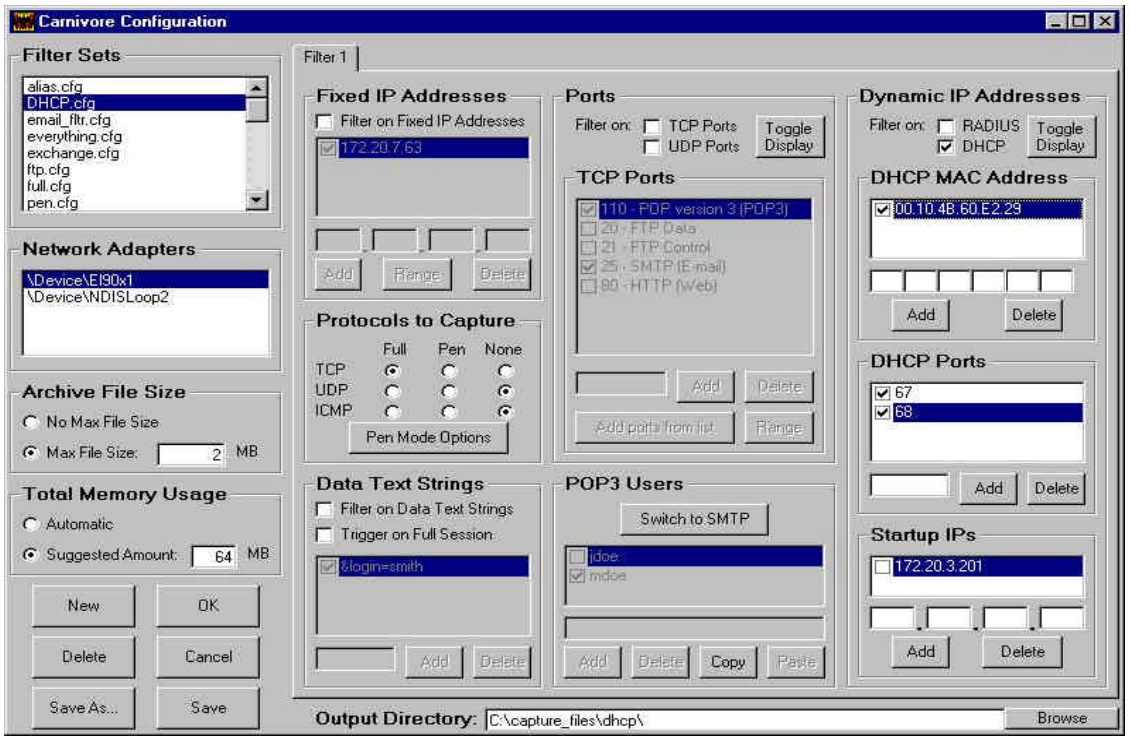

Figure C-20. Filter Setup 2 for DHCP Data Entries Test

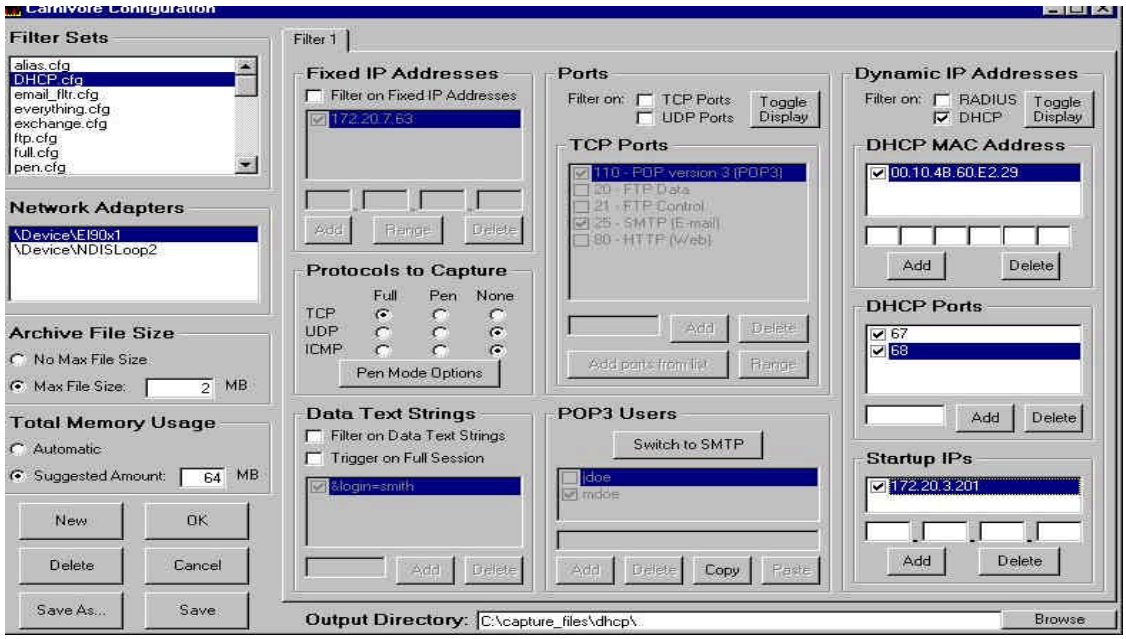

Figure C-21. Filter Setup 3 for DHCP Data Entries Test

Table C-5. Test Steps and Results for DHCP Filter Entry Fields

Step	Carnivore Condition	Filter	Desktop Computer	Laptop Computer	Test Result Packets Captured by Carnivore: Y/N	
					Expected	Actual
1	Stopped			Off line		
2				Boot up		
3				Login jdoe		
4		Check DHCP ports (see Figure C-19 for filter setup)				
5	Start					
6				Send an e-mail	N	N
7	Stop					
8		Enter MAC of the laptop (see Figure C-20 for filter setup)				
9	Start					
10				Force a DHCP exchange		
11				Send an e-mail	Y	Y
12	Stop					
13		Enter a Startup IP that was the IP address assigned to the laptop (see Figure C-21 for filter setup)				
13	Start					
14				Send an e-mail	Y	N
15				Force a DHCP exchange		
16				Send an e-mail	Y	Y
17	Stop					

C.11 TEST 11 FILTERING ON TEXT STRING FOR SMTP OR POP3 E-MAIL COLLECTION

C.11.1 SCENARIO

A court order authorizes collecting all SMTP or POP3 e-mail sent from and to a target that contains the key word "Planning". No target e-mail address is provided since the target uses a fixed IP address.

C.11.2 PURPOSE

Verify that when not providing the e-mail user ID to the filter, Carnivore has the capability to collect a target's e-mail that only contains the given text strings.

C.11.3 FILTER SETUP

For the first collection in this test, the filter parameters were set up using

- TCP protocol
- Full collection
- SMTP port 25 and POP3 port 110
- Data text string "Planning"

C.11.4 RESULT

Test not passed. By examining the Carnivore raw data, IITRI noted that Carnivore collects SMTP (sending) e-mail that matches the key word correctly, but does not collect POP3 (receiving) e-mail correctly. However, by examining the CoolMiner analysis result, it is observed that if the text string is in the header (such as in the Subject), then CoolMiner displays the message as a valid SMTP message. If the text string is in the body of the message, CoolMiner does not display it as an SMTP message. This is because the SMTP header is not collected even though raw Carnivore data shows the packet with the text string is collected properly.

The results are consistent with the capabilities provided by the FBI developers. The specified text strings have to be included in the packet and triggered at the driver level to save processing time. This condition is a performance trade off. However, Carnivore filters SMTP and POP3 e-mail users at the application level; therefore, the e-mail traffic does not pass through the text string filtering when e-mail user IDs are provided to the filter.

Table C-6. Test Steps and Results for Collecting E-mail of a Specific Text String

Step	Carnivore Condition	Filter	Desktop Computer	Laptop Computer	Test Result Packets Captured by Carnivore: Y/N	
					Expected	Actual
1	Stopped	As listed above		Off line		
2			Login mdoe			
3	Start					
4			Send an e-mail with subject “Planning”		Y	Y
5			Receive an e-mail with subject “Planning”		Y	N
6			Send an e-mail with key word “Planning” in the body		Y	Y
7			Receive an e-mail with No key word “Planning” in the body		Y	N
8			Send an e-mail with no key word “Planning”		N	N
9			Receive an e-mail with no key word “Planning”		N	N
10	Stop					

C.12 TEST 12 FILTERING ON TEXT STRING AND SMTP E-MAIL ADDRESS OR POP3 E-MAIL USER ID FOR E-MAIL COLLECTION

C.12.1 SCENARIO

A court order authorizes collecting the SMTP or POP3 e-mail messages sent from and to a target that contain a key word “Planning”. The e-mail address of the target is mdoe@iitri.org and the target uses a fixed IP address.

C.12.2 PURPOSE

Verify that Carnivore has the capability to collect e-mail of a target that contains only the given text strings.

C.12.3 FILTER SETUP

For the first collection in this test, the filter parameters were set up using

- TCP protocol
- Full collection
- SMTP port 25, and POP3 port 110
- Data text string “Planning”
- SMTP user e-mail address mdoe@iitri.org
- POP3 user name mdoe

The filter screen filled in with the collection parameters is displayed in Figure C-22.

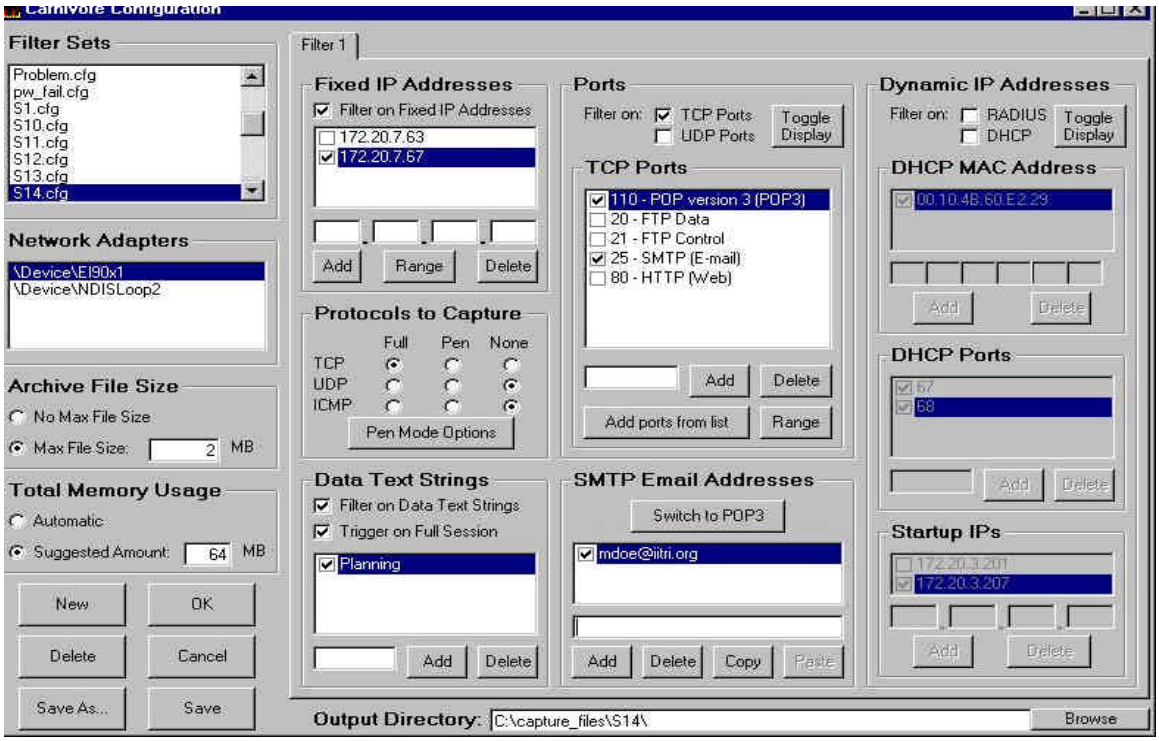

Figure C-22. Filter Setup for Filtering on Text String and E-mail User for E-mail Collection

C.12.4 RESULT

Test not passed. When given both a specific e-mail address and a text string, Carnivore collects all the target’s e-mail whether or not the e-mail matches the given text string. The result is recorded in steps four through nine of Table C-7.

The result is consistent with the capabilities provided by the FBI developers. The specified text strings have to be included in the packet and triggered at the driver level to save processing time. This condition is a performance trade off. However, Carnivore filters SMTP and POP3 e-mail

users at the application level; therefore, the e-mail traffic does not pass through the text string filtering when e-mail user IDs are provided to the filter.

Table C-7. Test Steps and Results for Collecting E-mail of a Specific Text String and an E-mail User

Step	Carnivore Condition	Filter	Desktop Computer	Laptop Computer	Test Result Packets Captured by Carnivore: Y/N	
					Expected	Actual
1	Stopped	As listed above		Off line		
2			Login mdoe			
3	Start					
4			Send an e-mail with subject “Planning”		Y	Y
5			Receive an e-mail with subject “Planning”		Y	Y
6			Send an e-mail with key word “Planning” in the body		Y	Y
7			Receive an e-mail with key word “Planning” in the body		Y	Y
8			Send an e-mail with no key word “Planning”		N	Y
9			Receive an e-mail with no key word “Planning”		N	Y
10	Stop					

C.13 TEST 13 FILTERING ON TEXT STRING FOR FTP COLLECTION

C.13.1 SCENARIO

A court order authorizes collecting a target’s file download FTP activities that contain the key word “Planning”. The target uses a fixed IP address.

C.13.2 PURPOSE

Verify that Carnivore has the capability to collect the target’s FTP (ports 20 and 21) communications that only contain the given text strings.

C.13.3 FILTER SETUP

For the first collection in this test, the filter parameters were setup using

- TCP protocol
- Full collection
- FTP data port 20 and control port 21
- Data text string “Planning”

The filter screen filled in with the collection parameters is displayed in Figure C-23.

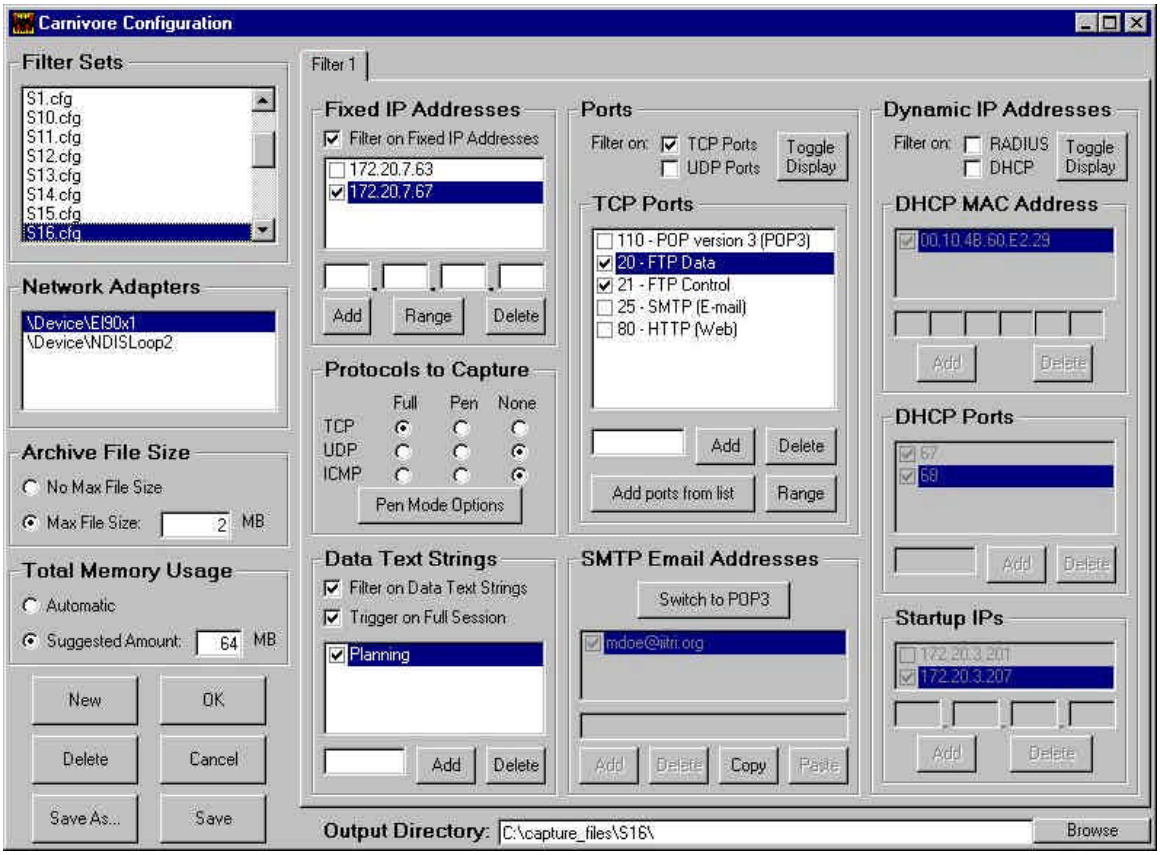

Figure C-23. Filter Setup for Collecting FTP Activities Containing a Specific Text String

C.13.4 RESULT

Test passed. Carnivore has the capability to collect FTP traffic that contained given text strings. However, it only collects the packets containing the text string or, if the Trigger on Full Session check box is checked, collects from the first packet containing the text string to the end of that session. In either case, Packeteer would fail to assemble all of the packets together for an entire FTP session and, in turn, CoolMiner would fail to analyze the result as shown in Figure C-24. The goal here is to test if Carnivore collects according to its filter setup, not to evaluate the post-processing tools, Packeteer or CoolMiner. The raw output from Carnivore contained the correctly collected data. The test results are shown in Table C-8.

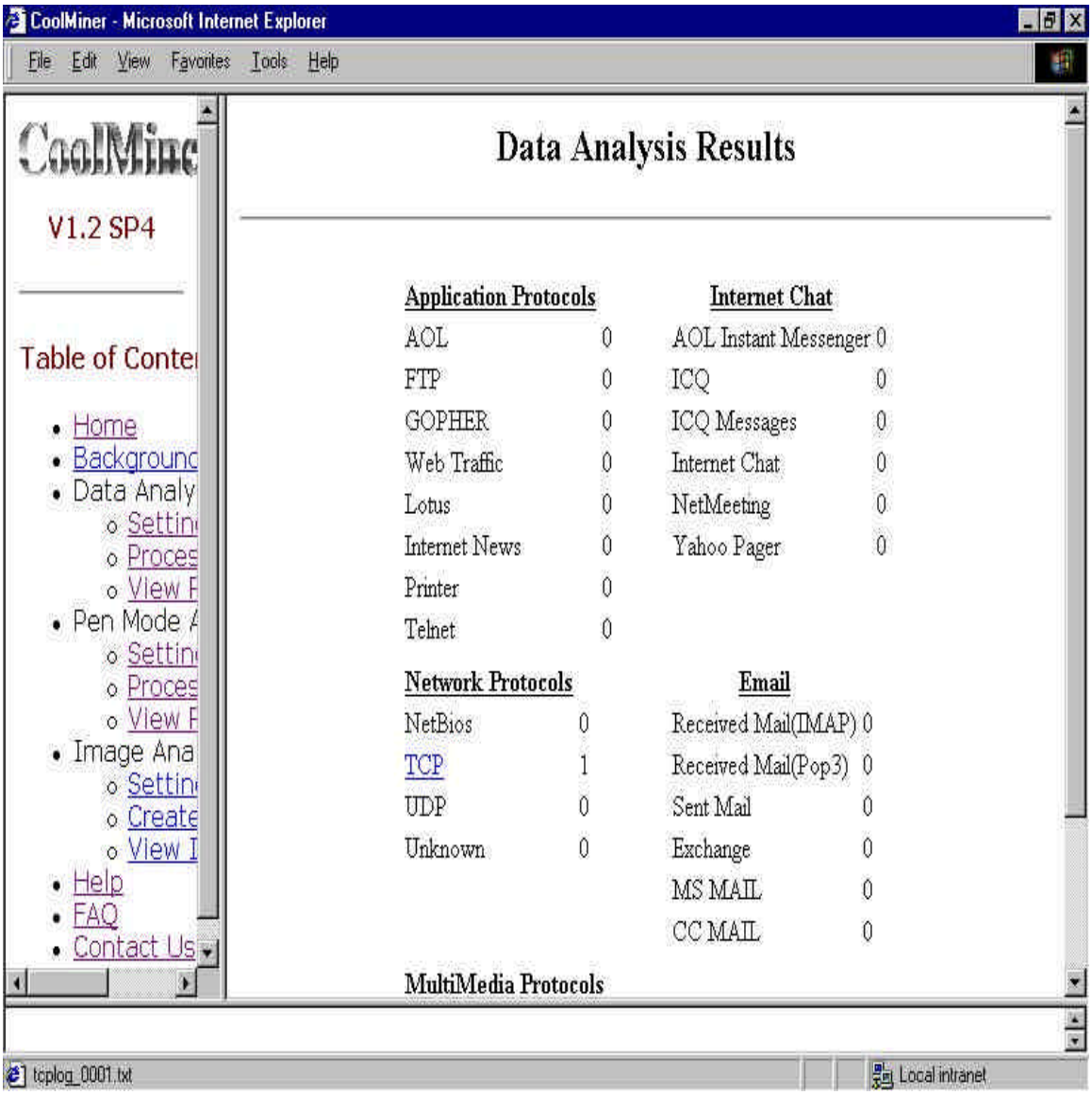

Figure C-24. CoolMiner Analysis Screen for FTP Collection Triggered by Text String

Table C-8. Test Steps and Results for Filtering on Text String for FTP Collection

Step	Carnivore Condition	Filter	Desktop Computer	Laptop Computer	Test Result Packets Captured by Carnivore: Y/N	
					Expected	Actual
1	Stopped	As listed in above		Off line		
2			Login mdoe			
3	Start					
4			FTP to a file server		N	N
5			Send “dir” command which lists a file name containing “Planning” string		Y	Y
6	Stop					

APPENDIX D
DETAILED SOFTWARE DESCRIPTION

D.1 PCAUSA LICENSE AGREEMENT

The license for WinDis 32 prevents the FBI from releasing the source code for this driver, and possibly for TapAPI.dll, to the public. The relevant portions of the WinDis 32 license are

Your Own Use

PCAUSA authorizes the licensed, registered owner (i.e., You) to edit or modify the WinDis 32 sample programs and incorporate them into the programs that you write for your own use, but you may not give away, sell, license or distribute them, alone or as part of any program, in executable, object or source form.

Distribution In Executable Form

PCAUSA grants you the right to incorporate the WinDis 32 sample programs into your own programs as long as your program adds substantial functionality beyond that provided in the original WinDis 32 sample. You may distribute programs that you create and which contain elements of the original WinDis 32 samples, in executable form only, without restriction or fee provided that all copies of your programs bear a valid copyright notice. By “copyright notice”, we mean your own copyright notice. You, of course, shall remain solely responsible for, and will hold PCAUSA harmless from, all claims, liability and damages arising from your own products which may include elements of the WinDis 32 sample programs.

Distribution In Source Form

PCAUSA does not grant you the right to give away, sell, license or otherwise distribute source code derived substantially from the WinDis 32 sample programs unless the recipient of your source code obtains their own license to the WinDis 32 sample programs, identical to this license and at the same cost that you paid for this license.

D.2 TAPNDIS

(Text of Appendix D.2 redacted by the DOJ). Note: In this publicly available version of the IITRI Final Report, the DOJ has redacted Appendix D.2 through D.4, which contain a detailed description of the Carnivore software structure.

D.3 TAPAPI

(Text of Appendix D.3 redacted by the DOJ)

D.4 CARNIVORE.DLL

(Text of Appendix D.4 redacted by the DOJ)

APPENDIX E
ENDNOTES

[i] 18 U.S.C. §§ 2510-2522.

[ii] 50 U.S.C. §§ 1801-1811.

[iii] 18 U.S.C. § 2516(1). By internal rule and practice, see MIOG 10-9.1, the FBI follows this limitation for interception of electronic communications. However, the statute itself, 18 U.S.C. § 2516(3), provides that, for interception of electronic communication, any government attorney (within the meaning of the Federal Rules of Criminal Procedure) can apply for the intercept order. See also United States Attorneys Manual 9-7.100 imposing requirement of high level DoJ approval for computer-based electronic interception.

[iv] Id. § 2516(3).

[v]I Interception of wire and oral communication is limited to certain enumerated felonies. Section 2516(1). It is not clear whether the FBI follows that restriction in the Carnivore context. See MIOG 10-9.1(3)(c).

[vi] Id. see In re United States, 10 F.3d 931, 938 (2nd Cir. 1993) holding that magistrates are not empowered to issue orders under Title III.

[vii] Id. § 2518(3).

[viii] Id. § 2518(3). Thus, Title III does not permit system-wide searches for terms such as “bomb” or “carnivore” unless the text search is confined to communications to or from a target

[ix] Id. § 2518(5).

[x] Id. § 2518(8).

[xi] Id. § 2518(7).

[xii] 18 U.S.C. § 3121(a).

[xiii] 18 U.S.C. § 3122.

[xiv] 18 U.S.C. § 3123(a).

[xv] Id. § 3123(b).

[xvi] Id. § 3123(b) & (c).

[xvii] 50 U.S.C. § 1802.

[xviii] 50 U.S.C. § 1805 (a).

[xix] 50 U.S.C. § 1805 (b)(1).

[xx] Id. § 1805(b)(2).

[xxi] Id. §§ 1804(a)(2); 1804(a)(7).

[xxii] 50 U.S.C. § 1842.

[xxiii] MIOG § 10-9(3)(a).

[xxiv] FBI MIOG.

[xxv] MIOG § 10-9.

[xxvi] MIOG P2 § 10-10.7(3).

[xxvii] MIOG P2 § 10-10.7(3), (4).

[xxviii] In exceptional circumstances, certain state judges also may provide authorization. 18 U.S.C. § 2510(9)(b).

[xxix] In comparison to a traditional Fourth Amendment search, therefore, there are significant before-the-fact (*ex ante*) checks. Only an Article III or state court judge can issue the order, the application must be authorized by high level officials, far more information must be supplied to the court—creating a record that later can be attacked—and enforcement officers must, in addition, demonstrate to the court's satisfaction that no conventional law enforcement means are available to capture the information sought, including pen registers. Moreover, unlike in the warrant context, Title III provides that law enforcement agents must minimize the intrusion into private communications.

[xxx] 18 U.S.C. § 2520(a)-(c).

[xxxi] Id. § 2520(c).

[xxxii] 50 U.S.C. § 1809.

[xxxiii] Id. § 1809(b).

[xxxiv] 18 U.S.C. § 3121(d).

[xxxv] It should be noted, however, that because pen devices capture less information, Congress determined that government investigators need abide by fewer external restrictions than under Title III or FISA searches. Far fewer before-the-fact checks exist. First, under the pertinent statute, 18 U.S.C. §§ 3121-3124, any federal or state governmental attorney may apply for a court order authorizing a pen register or a trap and trace device. Second, no probable cause need be shown, only that the information to be obtained "is relevant to an ongoing criminal investigation." Third, there is no requirement that an Article III judge issue the order—a magistrate can suffice. Fourth, no showing need be made that traditional law enforcement means are not sufficient to conduct the criminal investigation.

[xxxvi] 50 U.S.C. §§ 1806, 1845.

[xxxvii] 18 U.S.C. § 2518(10).

[xxxviii] See id. § 2518(10)(c).

[xxxix] There are other after the fact (*ex post*) checks in the Title III context not present with traditional searches. First, given that many individuals subject to Title III searches may not be aware that their phone conversations have been overheard or e-mail messages read, Title III requires disclosure, at least to the target, 90 days after completion of any investigation and permits the court to order notice to "other parties … in the interests of justice". Such notification opens the possibility that such individuals can sue for damages either under the Fourth Amendment or Title III. Second, the governing statute provides criminal penalties for any person, including law enforcement officers, who violate its terms. Third, Congress has waived government agents' immunity, allowing private actions against any law enforcement agent who violates the procedures in the Act.

[xl] 18 U.S.C. § 3126.

[xli] 50 U.S.C. § 1807.

[xlii] See supra note.

[xliii] 18 U.S.C. § 2516(1).

[xliv] 18 U.S.C. § 1804.

[xlv] MIOGP2 § 16-7.2.1.

[xlvi] MIOGP2 § 16-7.2.3(2-5).

[xlvii] MIOGP2 § 16-7.2.2(1).

[xlviii] MIOGP2 § 16-7.3.1(1).

[xlix] MIOGP2 § 16-7.3.1(1).

[l] MIOGP2 § 16-7.3.3(1)(a).

[li] MIOGP2 § 16-7.3.1(2).

[lii] http://enterprisesecurity.symantec.com/pdf/pcAWhitePapers/ StrongEncryption.pdf?PID=na

[liii] See www.wildpackets.com.

[liv] 18 U.S.C. § 2512 (1)(b).

[lv] 18 U.S.C. § 2512 (1).