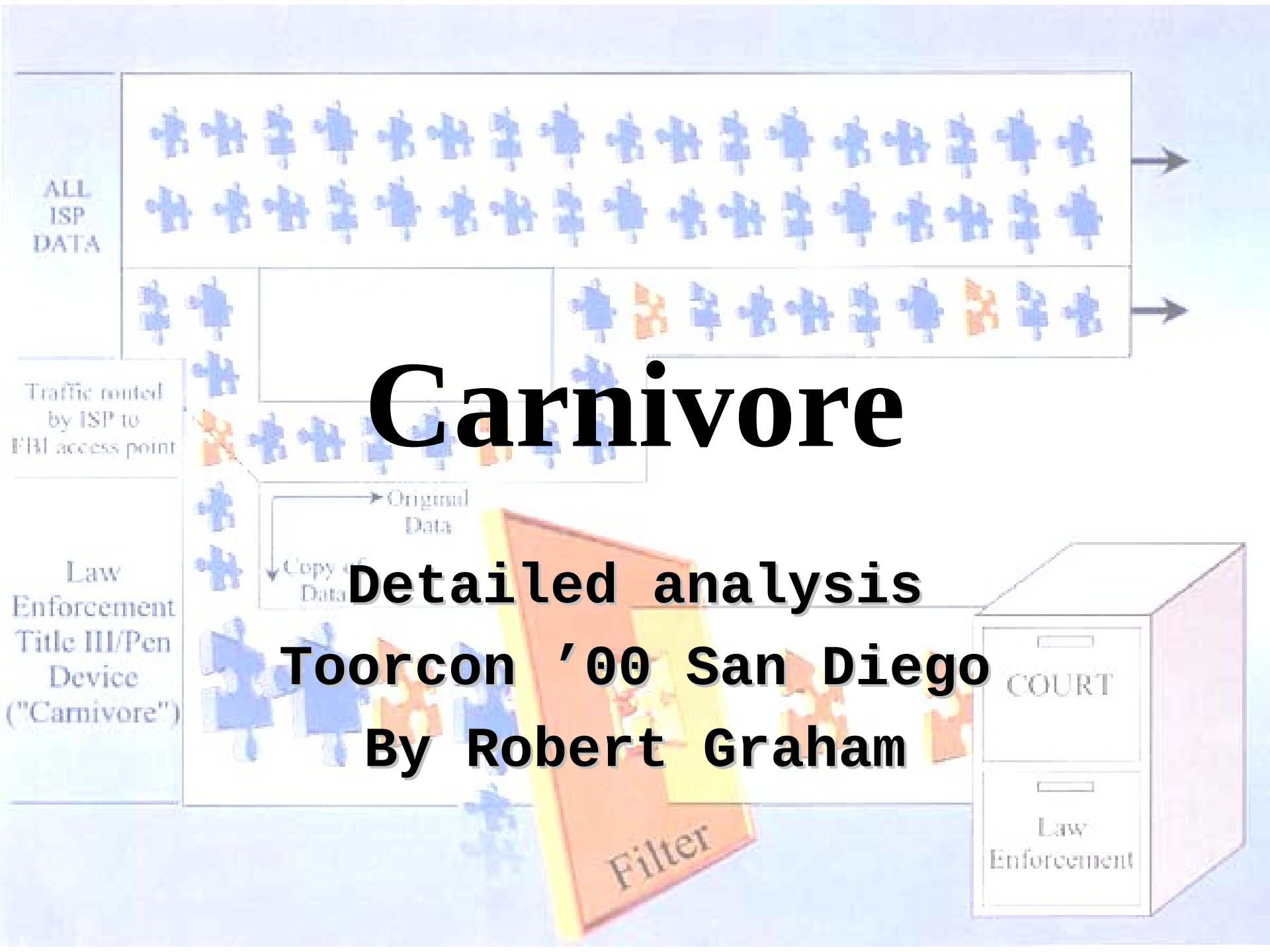


Carnivore

Detailed analysis

Toorcon ’00 San Diego

By Robert Graham

About speaker

- Robert Graham
- CTO/Network
- Writing Carnivore-like systems for 10 years

Talk

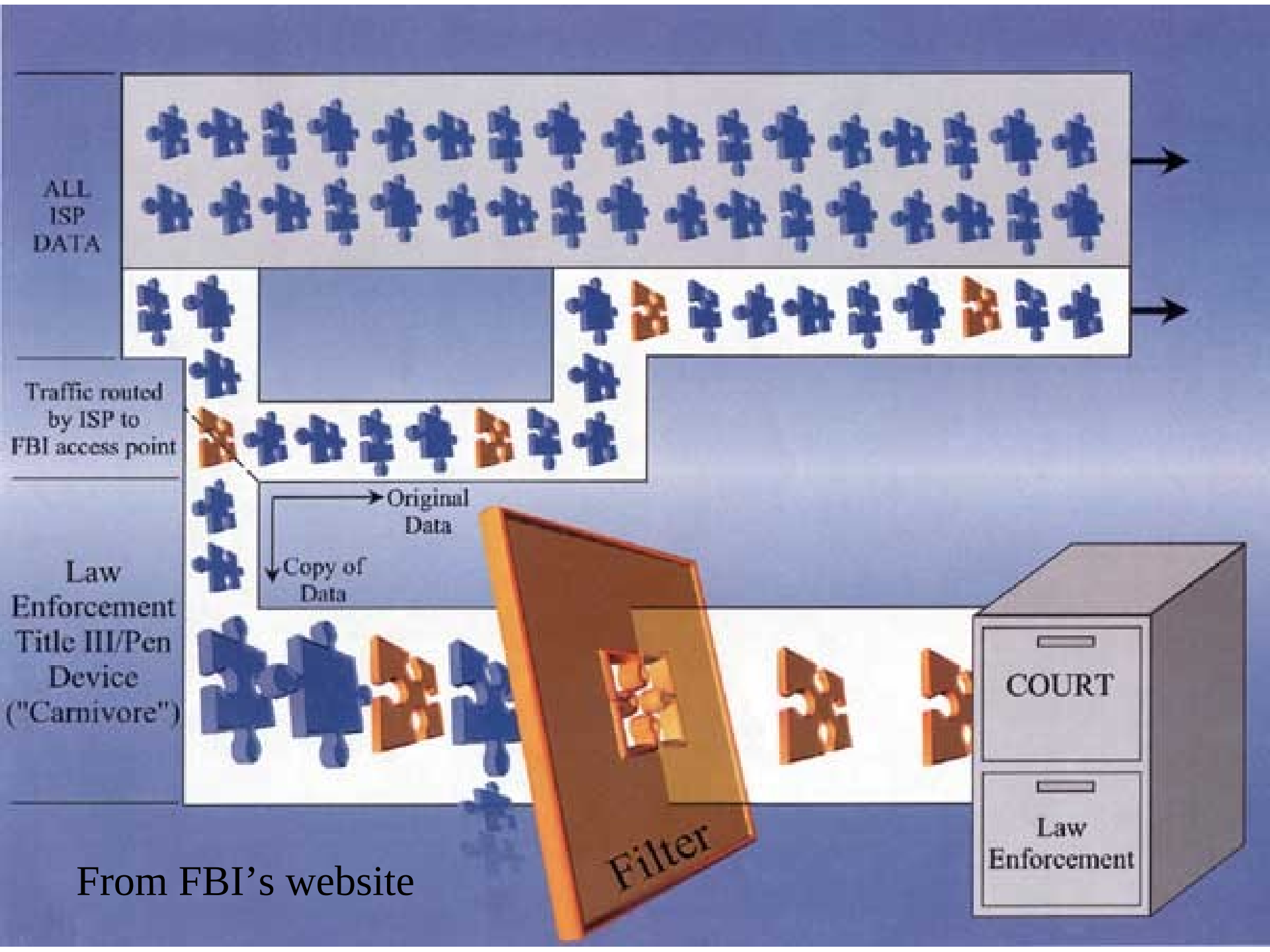
- Intro to Carnivore
- Legal details
- Technical details
- FAQ
- Reason for talk
  - Nothing you read in mainstream media is relevant to the technical details; this bugs the heck out of me

- *"They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." -- Benjamin Franklin, 1759*
- The more we ask the government to do, the more we must give up liberty
  - Example: drug laws make it hard for small businesses to get bank accounts because they must prove they aren't laundering drug money
  - Example: privacy advocates that want the government to pass laws, inviting the government to tax, regulate, and police

What is Carnivore?

A program designed to intercept Internet communication to and from people who are part of a criminal investigation.

Carnivore may *chew* all the data on the network, but it only actually *eats* the information authorized by a court order



From FBI's website

Proper Usage

- Proper legal authority
  - E.g. court order
- Assistance and cooperation of the ISP and sysadmin
- Observance of relevant statutes, practices, etc.

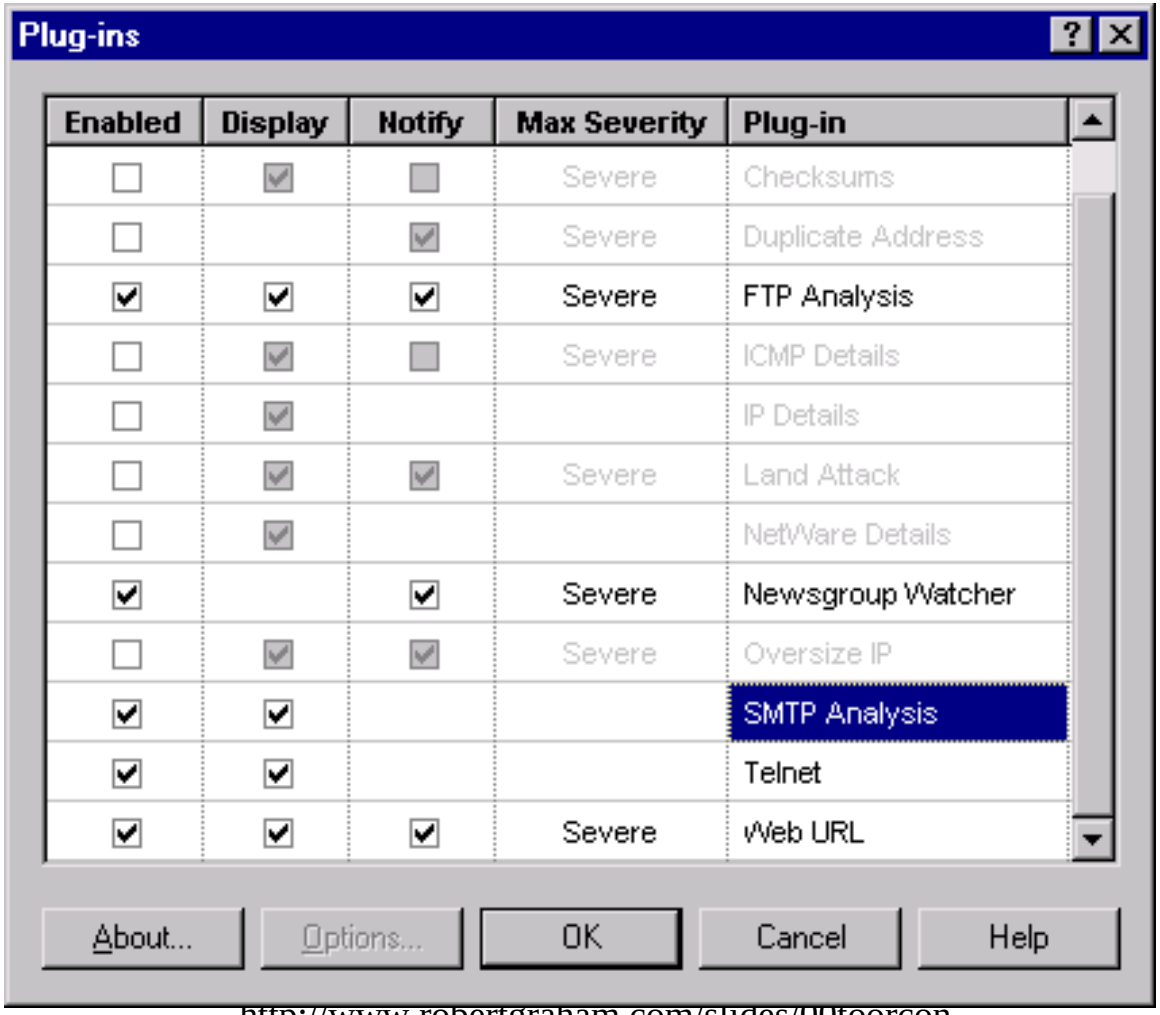
Protocols

- IP (from/to IP address)
- FTP (logs filenames transferred)
- NNTP/Usenet (logs access to newsgroups)
- SMTP (logs e-mails triggered by FROM or TO e-mail address)
- HTTP (logs URLs)
- IRC (port filter)
- Instant messaging (port filter)

Based upon

- C++, WinNT OS, COTS Pentium III, 128M RAM,, 4-18G disk, 2G Jaz drive (for evidence)
- No TCP/IP stack (!!!)
- Hardware authentication (???)
- Hardware network isolation device (Shomiti/NetOptics tap?)
- COTS communications software (Etherpeek?)
- Rumored modem dial-in?

EtherPeek plugins



http://www.robertgraham.com/slides/00toorcon

Etherpeek Descriptions

- FTP: “Detects FTP downloads and logs information on the location of the downloaded file and the address or name of the machine that initiated the download.”
- Newsgroup: “Detects access to Usenet news and logs information on the newsgroups and the address or name of the machine that initiated the action”
- SMTP: “Displays contents of and counts SMTP sessions”
- URL: “Detects accesses to WWW services over your net and logs the URL retrieved and the address or name of the machines that initiated the request”

Law: Fourth Amendment

- Wiretaps cannot cover the Internet. FBI cannot monitor all e-mail looking for the word “bomb”.
- Federal district judge must grant court order
  - Who (exactly, including e-mail)
  - Why (probable cause)
  - What (exactly which lines will be tapped, what info protocols)

Law: court order

- Two orders
  - One allowing FBI to collect the data
  - One requiring ISP to aid the FBI

Law: (cont)

- Emergency exceptions
  - Needs court order in 48-hours
  - Only Attorney General or Deputy
- Only FBI, and only certain felonies
- Hard evidence for court room
  - Not background intelligence gathering

Law: (cont)

- Minimization
  - Only the communications covered by the court order, and nothing more
  - If extra stuff leaks in, must be discarded
- Defense
  - Gets to challenge accuracy of data.
  - May move to suppress if not legally obtained

Law: enabling legislation

- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (aka. “Title III”)
- 1986 ECPA (Electronic Communications Privacy Act)
- 1994 CALEA (Digital Telephony bill)
  - Carriers must provide wiretap facilities
  - ISPs are carriers
- 1998 roving wiretap
  - Allows FBI to eavesdrop on many people as long as they only pay attention to the suspect

Law: hearsay

- Sniffer logs are considered hearsay
- No proof that they are accurate, reliable, and trustworthy

Law: hearsay

- Must satisfy certain criteria
  - Produced with normal course of business day in and day out
  - Must be “authenticated”: verified by qualified witness; Rule 901 of the Federal Rules of Evidence
  - Must be “best evidence”: if at all possible, must be the original copy.

Law: more hearsay

- Even “best evidence” not reliable
  - Can’t prove who was at the console
  - Computer can be used as a relay (e.g. Trojan Horse)
  - Computer’s IP/e-mail address can be *easily* spoofed

Law: chain of possession

- Evidence must be “sealed”
- Must document everyone who handles it and why
- Must not be altered, except in certain cases (which must be carefully documented)
- Conclusion: FBI must not put a TCP/IP stack on Carnivore box, and must lock up the disk and document everyone who handles it.

Law: trap and trace/pen register

- POTS: (partial warrant, easy to get)
  - Record everyone who dials a number
- Carnivore:
  - Everyone who FTPs a certain file
  - Everyone who accesses a certain webpage
  - Everyone who reads a certain newsgroup
  - Everyone who connects to a #chatroom

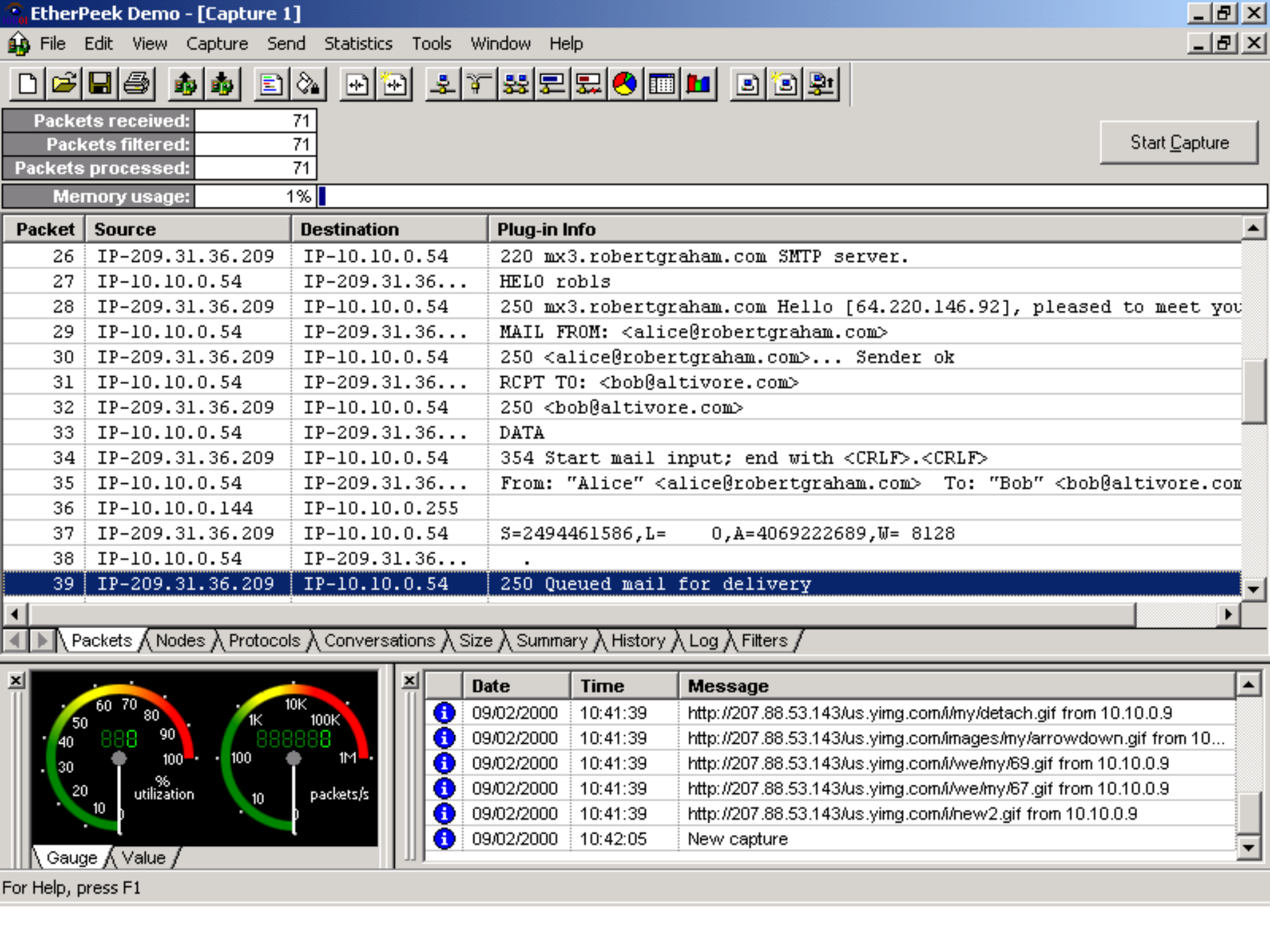
Law: wiretap

- POTS: (full warrant, hard to get)
  - Eavesdrop, van parked out on the street, somebody is actually monitoring the data.
  - Turns off the recorders if hears somebody on the line who isn't the suspect (e.g. wife, child)
- Carnivore:
  - All e-mails from/to an address
  - All traffic to/from IP address (or IP address as retrieved from TACACS/RADIUS for user account)

How SMTP works

- **HELO robls**
- **MAIL FROM:<alice@robertgraham.com>**
- **RCPT TO:<bob@altivore.com>**
- **DATA**
- **Subject: Hi\n\nBob, I've got the plutonium that you wanted.\nI'll expect payment through a money order to my Cayman Islands account. \n-Alice**
- **.**
- **QUIT**

(Each of these a separate packet)


EtherPeek Demo - [Capture 1]
File Edit View Capture Send Statistics Tools Window Help
Packets received: 71
Packets filtered: 71
Packets processed: 71
Memory usage: 1%
Start Capture
Packet Source Destination Plug-in Info
26 IP-209.31.36.209 IP-10.10.0.54 220 mx3.robertgraham.com SMTP server.
27 IP-10.10.0.54 IP-209.31.36... HELO robls
28 IP-209.31.36.209 IP-10.10.0.54 250 mx3.robertgraham.com Hello [64.220.146.92], pleased to meet you
29 IP-10.10.0.54 IP-209.31.36... MAIL FROM: <alice@robertgraham.com>
30 IP-209.31.36.209 IP-10.10.0.54 250 <alice@robertgraham.com>... Sender ok
31 IP-10.10.0.54 IP-209.31.36... RCPT TO: <bob@altivore.com>
32 IP-209.31.36.209 IP-10.10.0.54 250 <bob@altivore.com>
33 IP-10.10.0.54 IP-209.31.36... DATA
34 IP-209.31.36.209 IP-10.10.0.54 354 Start mail input; end with <CRLF>.<CRLF>
35 IP-10.10.0.54 IP-209.31.36... From: "Alice" <alice@robertgraham.com> To: "Bob" <bob@altivore.com
36 IP-10.10.0.144 IP-10.10.0.255
37 IP-209.31.36.209 IP-10.10.0.54 S=2494461586,L= 0,A=4069222689,W= 8128
38 IP-10.10.0.54 IP-209.31.36... .
39 IP-209.31.36.209 IP-10.10.0.54 250 Queued mail for delivery
Packets Nodes Protocols Conversations Size Summary History Log Filters
% utilization
packets/s
Gauge Value
Date Time Message
09/02/2000 10:41:39 http://207.88.53.143/us.yimg.com/i/my/detach.gif from 10.10.0.9
09/02/2000 10:41:39 http://207.88.53.143/us.yimg.com/images/my/arrowdown.gif from 10...
09/02/2000 10:41:39 http://207.88.53.143/us.yimg.com/i/we/my/69.gif from 10.10.0.9
09/02/2000 10:41:39 http://207.88.53.143/us.yimg.com/i/we/my/67.gif from 10.10.0.9
09/02/2000 10:41:39 http://207.88.53.143/us.yimg.com/i/new2.gif from 10.10.0.9
09/02/2000 10:42:05 New capture
For Help, press F1

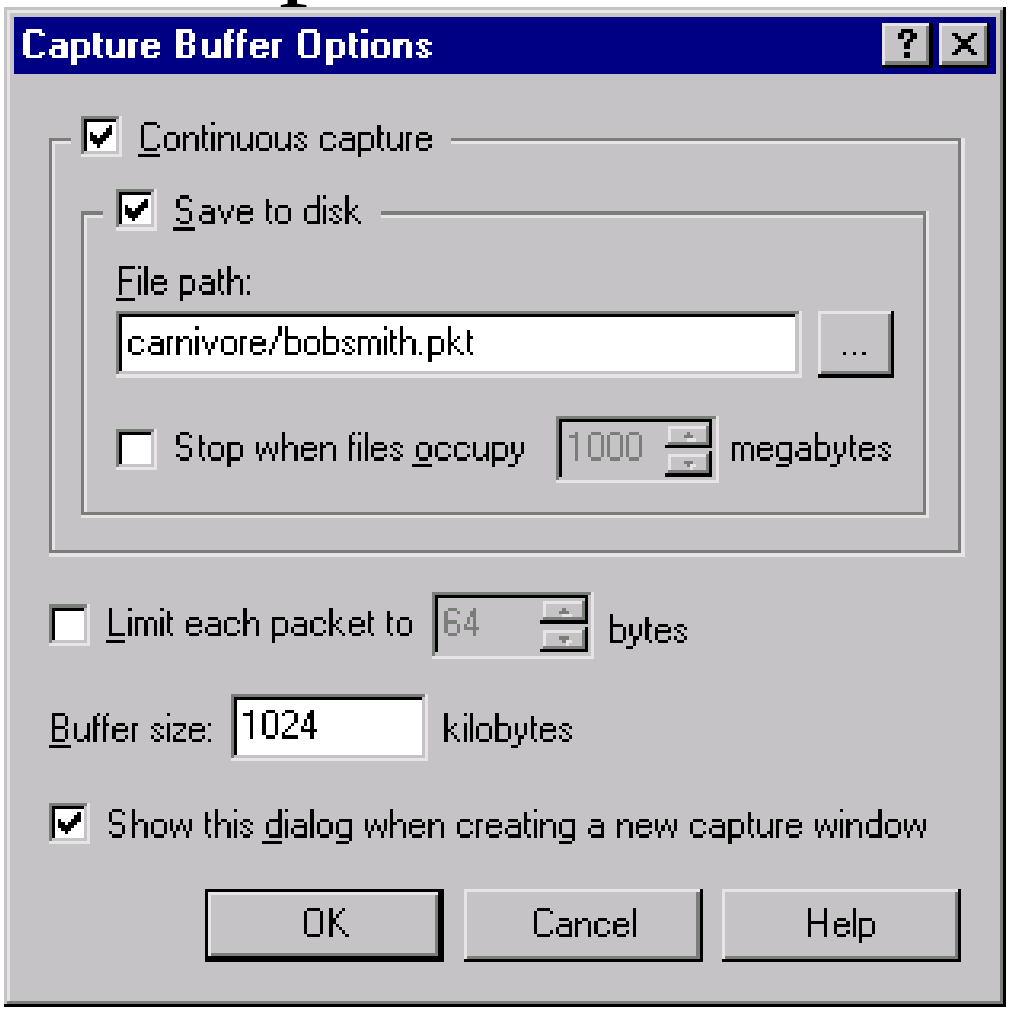
SMTP packet

```
 0  00d0 b758 92a1 0040 05a4 7932 0800 4500   ...X...@..y2..E.
10  0053 f100 4000 8006 f52d 0a0a 0009 0a00   .S..@....-......
20  0064 0e9d 0019 0414 6e84 4e27 8c8a 5018   .d......n.N'..P.
30  219d 0265 0000 4d41 494c 2046 524f 4d3a   !..e..MAIL FROM:
40  203c 526f 6265 7274 2e47 7261 6861 6d40    <Robert.Graham@
50  6e65 7477 6f72 6b69 6365 2e63 6f6d 3e0d   networkice.com>.
60  0a                                        .
```

How Carnivore works

- For all packets sent to port 25:
- If data starts with “MAIL FROM” or “RCPT TO”, compare the e-mail address against the court-authorized e-mail address.
- If the e-mail addresses match, start collecting this session (IP to/from, port to/from)
- Save the raw packets to Jaz drive

Etherpeek Omnivore



http://www.robertgraham.com/slides/00toorcon

Eval RFP (Aug 24, ‘00)

- All the info and only the info
- Introduce new risks (operational, security) to the ISP
  - Crash them? Buffer overflow?
- Risk of unauthorized monitoring (intentional, unintentional) by FBI or non-FBI personnel? (ie. Misuse by rogue FBI agents)
- Protections (audit, procedures, etc.) adequately address the risks above?

http://cryptome.org/carnivore-rfp.htm

All the info?

- Keep up with network traffic?
- Handle IP fragmentation or TCP segmentation?
- Handle SMTP state machine? (e.g. ESMTP pipelining)
- Good things:
  - By keeping the packets, you can clearly pin-point where it has failed via TCP sequence numbers.
  - Not getting all e-mail isn't a problem – you can't wiretap all communication anyway (phone, e-mail, letter's friend).

All the info?

- Can it handle fragmentation?
- **HELO robls**
- **MAIL FROM:<alice@rob**
- **ertgraham.com>**
- **RCPT TO:<bob@altivo**
- **re.com>**
- **DATA**
- **Subject: Hi\n\nBob, Le**
- **t’s get together.**
- **.**
- **QUIT**

Only the info?

- Is address matching exact or partial?
- Does it correctly parse the RSET?

```
HELO robls
MAIL FROM:<malice@robertgraham.com.au>
RCPT TO:<bob@altivore.com>
DATA
Subject: Hi\n\nBob, Let's get together.
.
RSET
MAIL FROM:<john@yahoo.com>
RCPT TO:<mary@hotmail.com>
DATA
Subject: foo\nasdfasdfasdf\n
.
QUIT
```

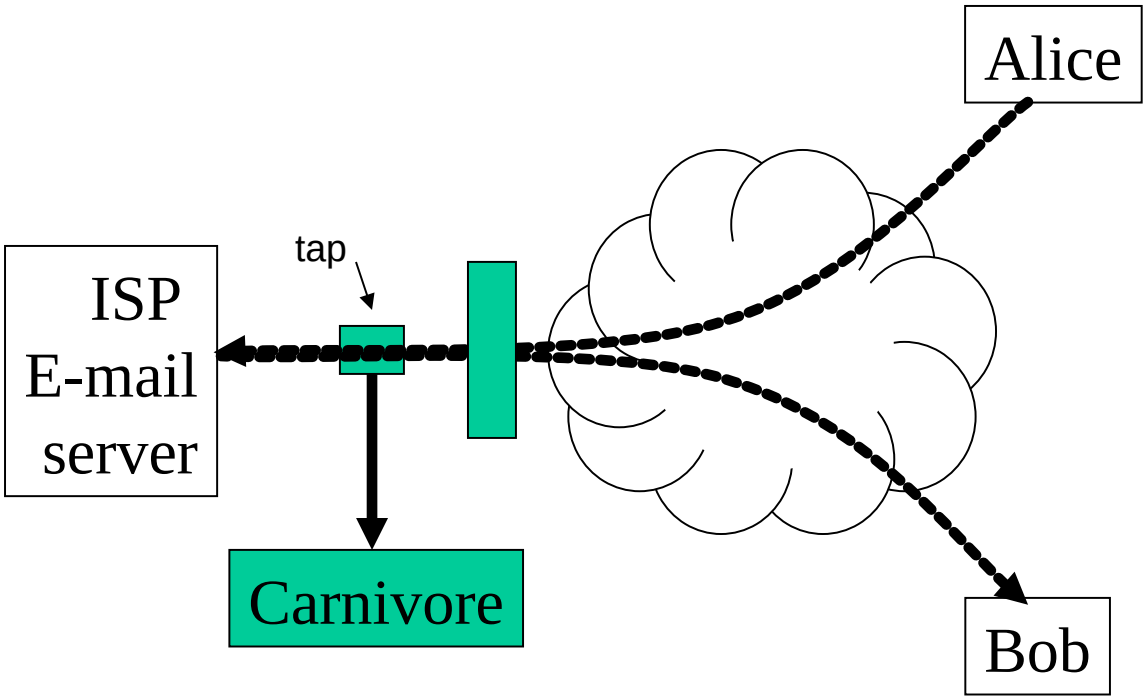
Only the info?

- Does it correctly parse the dot in face of TCP retransmits or pipelining?
- **HELO robls**
- **MAIL FROM:<m*alice@robertgraham.com*.au>**
- **RCPT TO:<bob@altivore.com>**
- **DATA**
- **Subject: Hi\n\nBob, Let's get together.\n.\n**
- **RSET**
- **MAIL FROM:<john@yahoo.com>**
- **RCPT TO:<mary@hotmail.com>**
- **DATA**
- **Subject: foo\nasdfasdfasdf\n**
- **.**
- **QUIT**

Only the info?

- People often share accounts
  - I.e. they share the identical e-mail address.
  - Remember, Carnivore has no problem with distinct e-mail accounts.
  - Traditional wiretap requires the recorders to be turned off in cases where another family member makes the call.
  - This probably isn't all that serious.

Operational risks?



Carnivore is 100% passive. Introduces no additional operational risks; though initial insertion is a small issue

Security risks?

- BUFFER-OVERFLOW!!!
  - In the underlying COTS software
  - In their plugins
  - Stats
    - Probably less than 1-kloc, easy to audit
    - But most such services have buffer overflows.
- But can't transmit
  - But Carnivore probably cannot transmit, so any compromise of the box won't result in ISP compromise

FBI misuse

- Can the FBI misuse the system?
  - Yes
  - Easy to configure to capture all traffic
  - Other plugins may be active
  - Other software may be on the box (e.g. TCPDUMP)
- However
  - Rarely connected to backbones, usually next to servers
  - FBI has just as much potential for misuse without Carnivore

Protections adequate?

- Not a technical question.
  - Real question: what % of the time will be misused?
- My guess: probably less than 1%
  - The FBI is a quagmire of bureaucratic processes.
  - They FEAR evidence that is not provided through the normal channels.

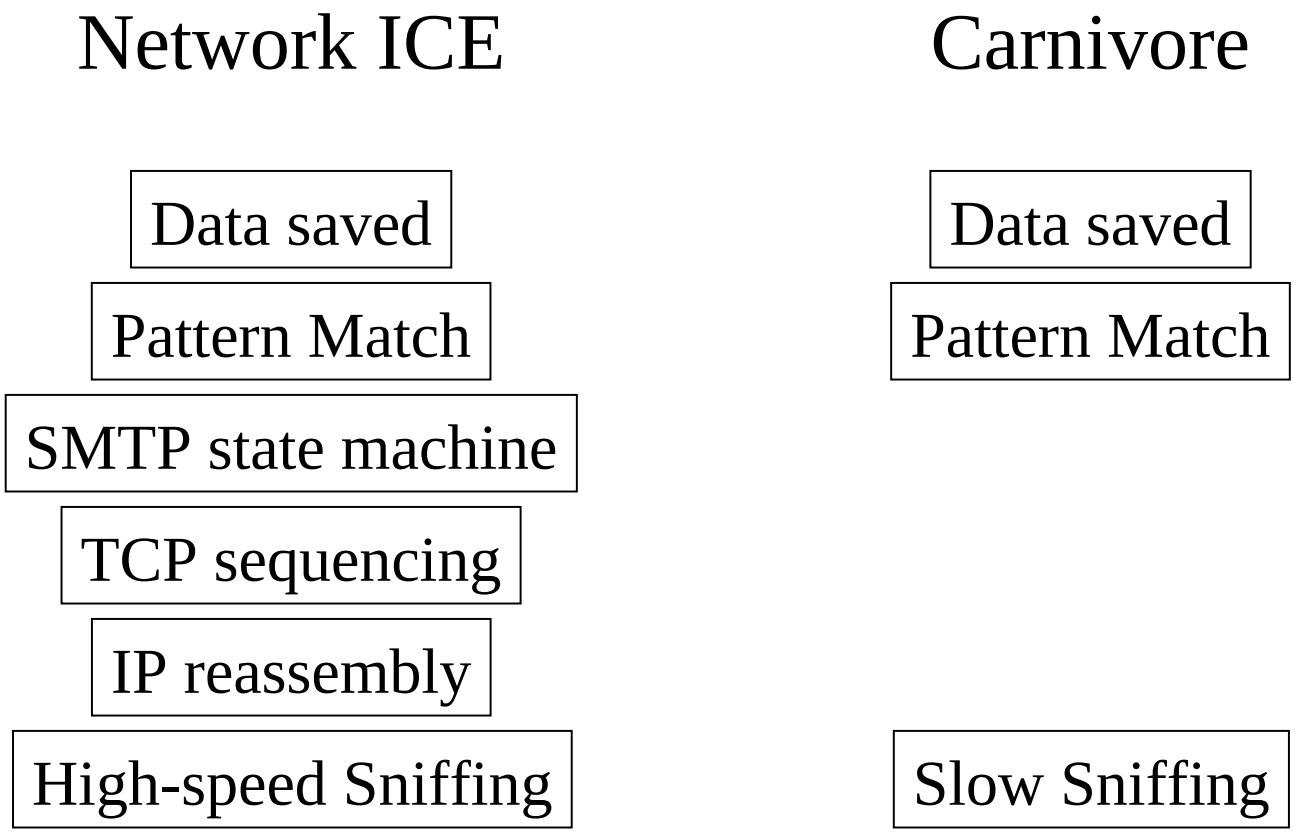
Eval RFP (reprise)

- All/only info
  - Not OK! Not enough and too much
- Operational/security risks
  - OK
- Misuse
  - Technically easy to misuse
- Protections
  - Adequate

Earthlink: case study

- Earthlink claims that Carnivore crashed their system
- FBI claims that Carnivore cannot crash networks
- They are both right
  - Carnivore normally runs as separate device, but you can also install directly on a server, which may cause numerous problems
  - Probably caused by WinNT RAS bug

Protocol stacks



http://www.robertgraham.com/slides/00toorcon

<source>

Q&A

- Can Carnivore suck up e-mail from unintended targets?
  - Yes (though FBI says “no”), though rare
- Will Carnivore corrupt e-mails, obtain fragments, or accidentally insert fragments of other e-mails?
  - No; Carnivore captures original packets, not e-mail, so all fragments clearly labeled

Q&A

- Is Carnivore superfast?
  - The FBI thinks so; my own stuff runs 10-100 times faster, so I'm a little disdainful (I think they just don't know any better).
  - Most deployments are right next to a server or mirrored on a switch, so it probably can keep up.
  - If it were placed on a major backbone, it would die a gruesome death

Q&A

- Is Carnivore sophisticated?
  - No. It is extremely simple (<500 lines of code)
  - They can't even figure out how to use libpcap (for Windows and UNIX), they must instead use a commercial-sniffer.
  - It is magic trick, like making an elephant disappear; only impressive because it looks big and you don't know what it does.

Q&A

- Does Carnivore “astonished industry specialists”
  - No.

Q&A

- How often is Carnivore used?
  - In less than 10% of court orders demanding e-mail, roughly 25 times in last 18 months.
  - Mostly terrorism cases, according to the FBI, but also mentions hackers and drug trafficking
  - Most testimony I've read from the FBI seems to stress "protecting children" (I.e. kiddy porn, chat rooms, etc.)

Q&A

- Is Carnivore an unrestrained Internet wiretap?
  - No. It is on the edges in only a couple of places, it only obtains a few people's e-mails, and each unit is removed after a few weeks, and is only authorized by high-level federal judges, and is only installed with the assistance of the ISP

Q&A

- Is it permanently located at the ISP?
  - No, judge usually requires a weekly review. Extremely difficult to get a judge to allow it for more than 45 days.
  - There is no vast network of Carnivore machines at ISPs, only a few isolated ones on the edges of the network.

Q&A

- Why doesn't the FBI release source code?
  - Because hackers will find away around it (humor: hackers would just use PGP).
  - They use commercially licensed code they cannot release (contractually).
  - Title 18 USC 2512 prohibits possession of devices designed to eavesdrop on other people's communications
  - Because they change the source depending upon the incidence (I.e. still under development)

Q&A

- Is the FBI forthcoming on basic details?
  - The FBI claims it is forthright with all basic details and not hiding anything. But as shown in this presentation, I've had to reverse engineer a lot of basic information that they've hidden.

Q&A

- Does Carnivore store/forward packets?
  - This is a false rumor widely claimed in the media. Carnivore is just a sniffer.

Q&Q

- How does this relate to Britain's Regulatory Investigative Powers (RIP) bill?
  - RIP requires every ISP to install a monitoring device that is active all the time.
  - Like Carnivore, only collects data with a court order.
  - Wants key recovery

Q&A

- How does this relate to Russia's SORM (System of Ensuring Investigative Activity)
  - SORM requires ISPs to forward all traffic to the KGB/FSB, who then gets to do anything they want with it for any reason.
  - No warrant needed.
  - Demands key recovery

Further Resources

- http://www.altivore.com
- http://www.robertgraham.com/xfer/altivore
- http://www.epic.org
- http://www.eff.org