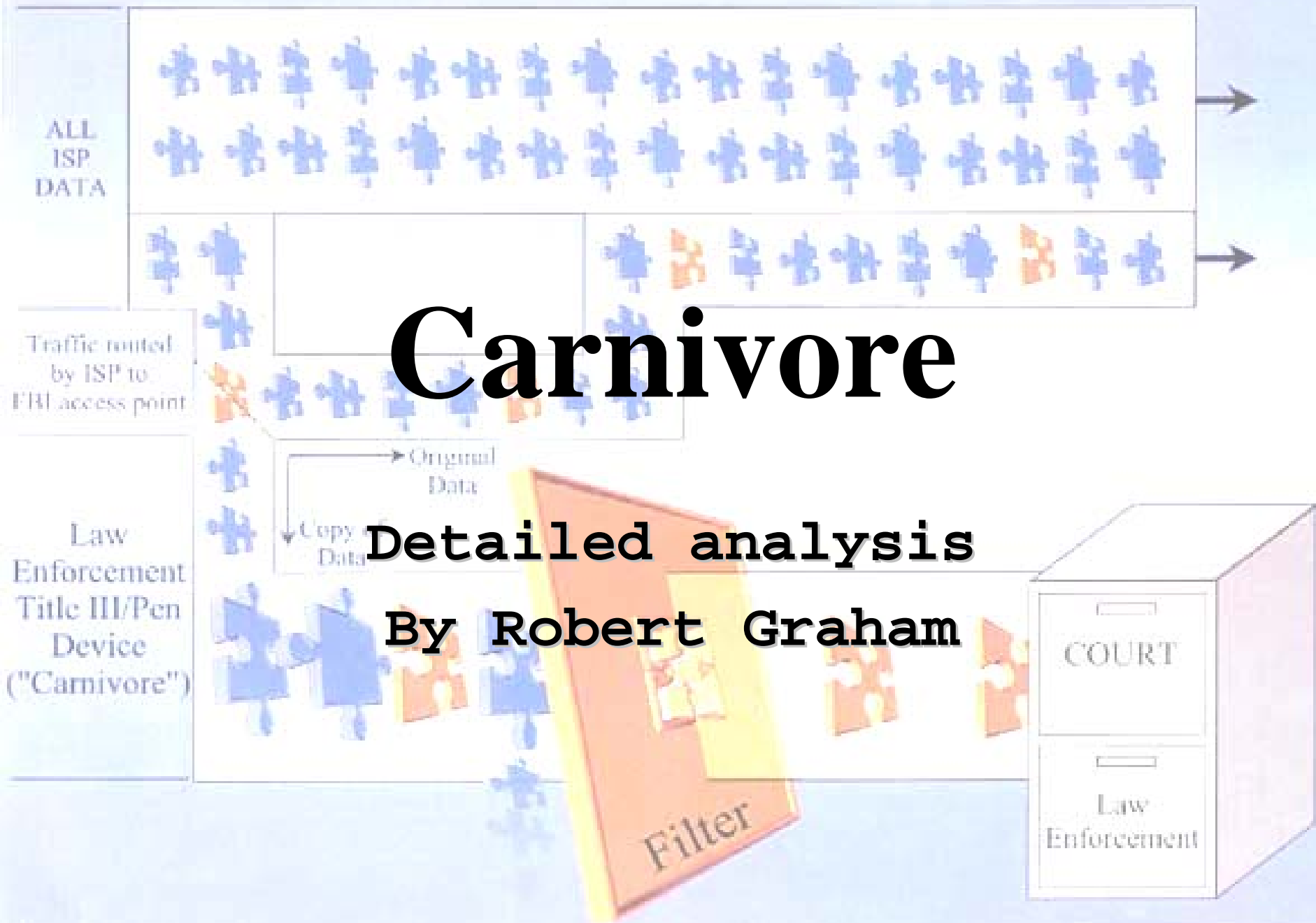


# Carnivore

**Detailed analysis**

**By Robert Graham**



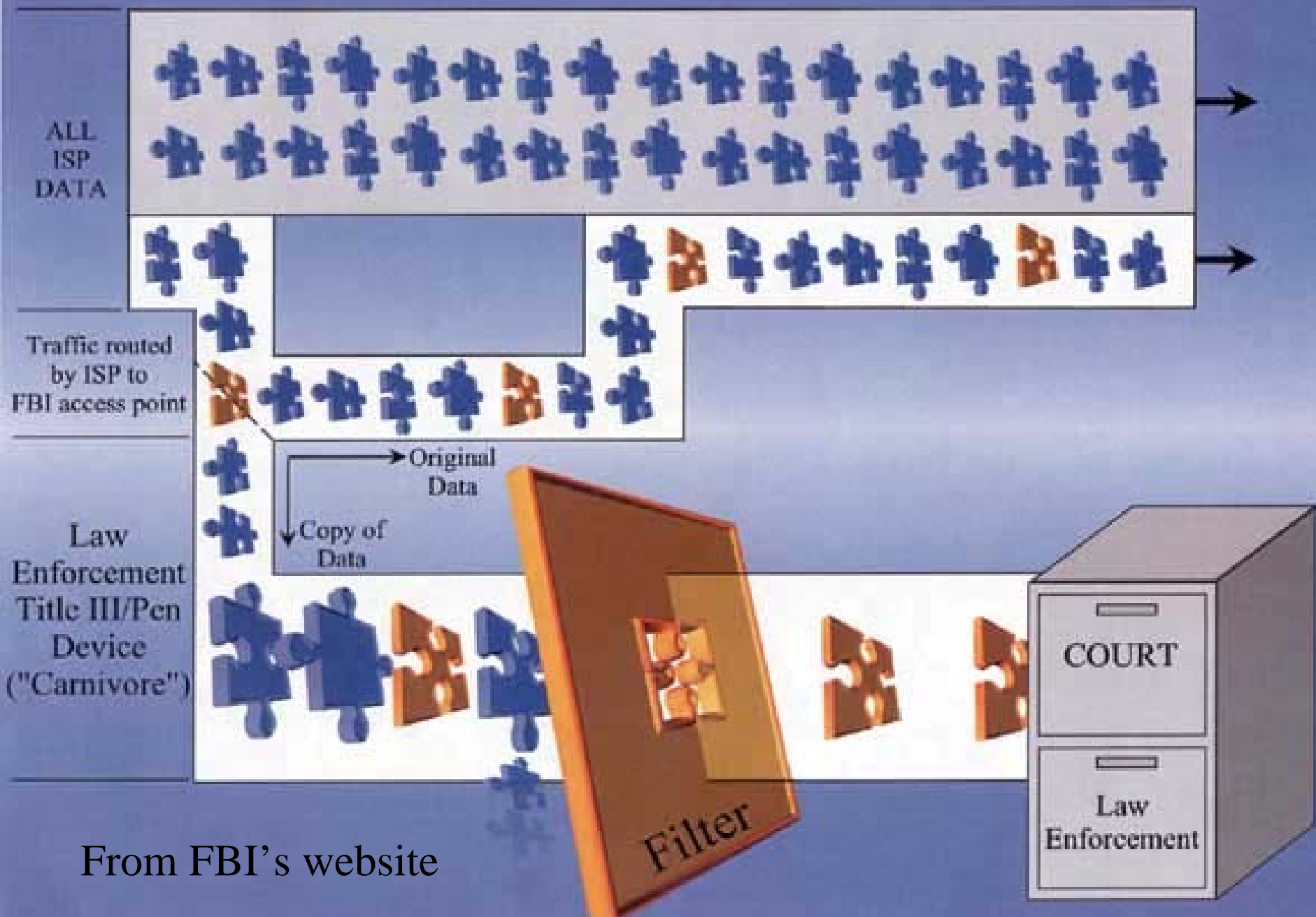
# Talk

- 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

# 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

# What isn't Carnivore

- Popular misconceptions
  - Carnivore is an Internet-wide surveillance network.
  - FBI can instantly grab any e-mail they want
  - Carnivore filters on content (e.g. plutonium)

# Proper Usage

- Proper legal authority
  - court order
- Assistance and cooperation of the ISP and sysadmin
  - court order, without which the ISP won't let the FBI in

# Protocols

- IP
  - from/to IP address
  - full content
- SMTP
  - from/to E-mail addresses
  - full content
- HTTP/FTP
  - from/to IP address

# 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 (PCAUSA packet sniffer, same as WINDUMP)
- PCanywhere dial-in

# 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

- Generally, sniffer logs would be considered hearsay
- No proof that they are accurate, reliable, and trustworthy
- Therefore, Carnivore is designed log data in a trustworthy manner that stands up in court
  - E.g. sniffs packets that carried the e-mail rather than reassembling on the fly

# 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, or dials into a number
- Carnivore:
  - Everyone who accesses a certain HTTP server
  - All to/from IP addresses
  - All to/from e-mail addresses

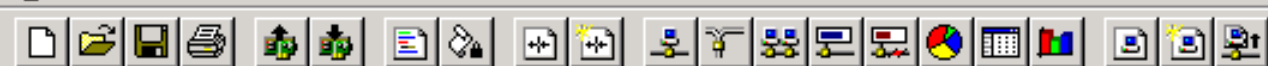
# Law: wiretap

- 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 DHCP/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)

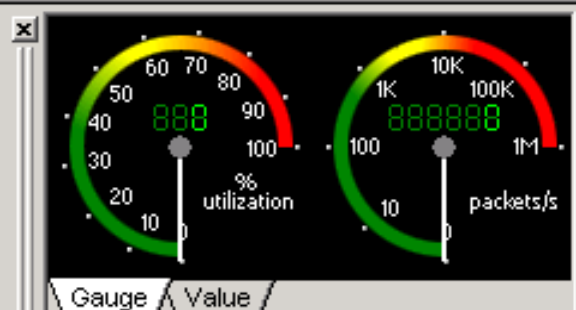


Packets received:	71
Packets filtered:	71
Packets processed:	71
Memory usage:	1%

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 robles
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



	Date	Time	Message
i	09/02/2000	10:41:39	http://207.88.53.143/us.yimg.com/i/my/detach.gif from 10.10.0.9
i	09/02/2000	10:41:39	http://207.88.53.143/us.yimg.com/images/my/arrowdown.gif from 10...
i	09/02/2000	10:41:39	http://207.88.53.143/us.yimg.com/i/we/my/69.gif from 10.10.0.9
i	09/02/2000	10:41:39	http://207.88.53.143/us.yimg.com/i/we/my/67.gif from 10.10.0.9
i	09/02/2000	10:41:39	http://207.88.53.143/us.yimg.com/i/new2.gif from 10.10.0.9
i	09/02/2000	10:42:05	New capture

# 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

# Eval RFP (Aug 24, '00)

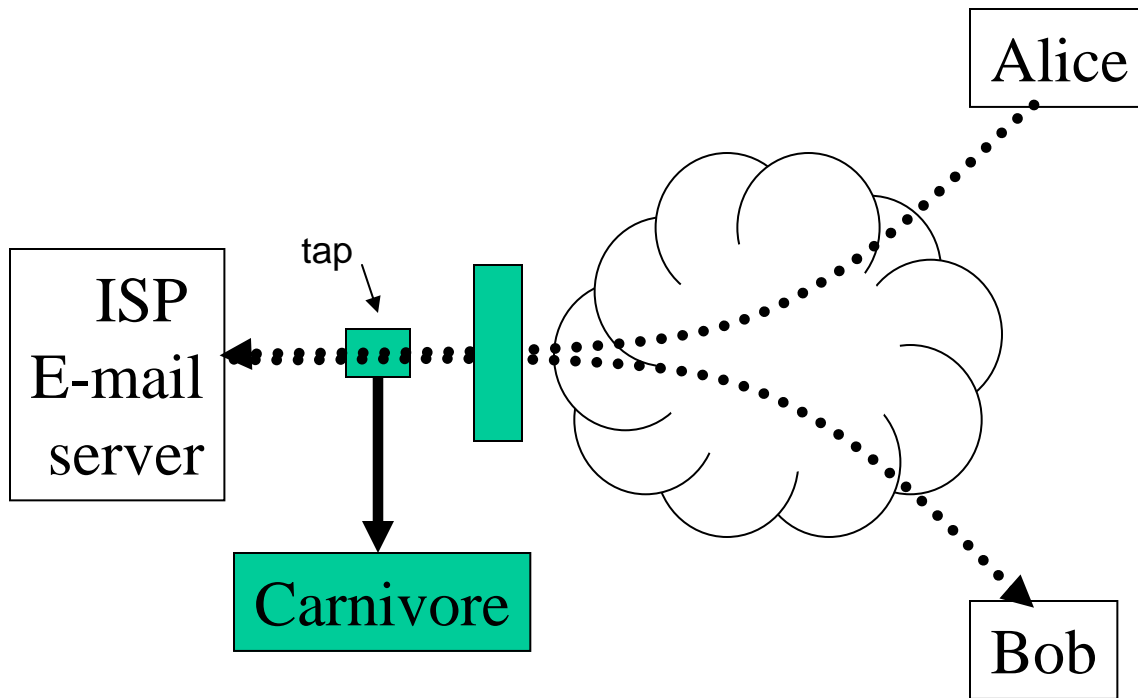
- All the info and only the info
- Introduce new risks (operational, security) to the ISP
  - Crash them? Buffer overflow?
- Risk of unauthorized monitoring (intentional, unintentional) by FBI or non-FBI personnel? (ie. Misuse by rogue FBI agents)
- Protections (audit, procedures, etc.) adequately address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

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

# Eval: All the info?

- Carnivore was found to be unable to keep up with some ISP traffic.
- Carnivore cannot handle IP and TCP fragmentation issues.
- Carnivore had bugs with application layer protocols such as SMTP pipelining and POP3.
- Carnivore may accidentally monitor other people's traffic.

# Eval: Operational risks?



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

# Eval: FBI misuse

- Carnivore has not hidden codes for misuse
- Carnivore can easily be misused by agents
  - Contains “content searching” features.
  - Can act as a packet sniffer.
- Carnivore can easily be misconfigured

# Eval: Protections adequate?

- No auditing is performed

# Eval: Conclusion

- Carnivore basically fails the test the DoJ gave it.

# 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

# 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 sophisticated?
  - No. It is extremely simple
  - 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

- 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.epic.org>
- <http://www.eff.org>

# Altivore

# libpcap

- Common API for any sniffing
- Linux
  - Usually installed on system
- Windows
  - <http://netgroup-serv.polito.it/winpcap/>
  - (winpcap is based upon the same PCAUSA library)

# How libpcap works

- Reads packets one at a time from adapter

```
devicename = pcap_lookupdev(errbuf);
hpcap = pcap_open_live(devicename, ...);
for (;;) {
    pcap_dispatch(hpcap, ..., handlePacket, ...);
}

void handlePacket(..., pcap_pkthdr *framehdr, ...)
```

# IP address filtering

- Enter in IP address
- Or enter in user logon name
  - Dynamically change IP address filter by parsing RADIUS packets
- Saves raw packets to files

# E-mail filtering

- Tracks from/to addresses
- Saves the raw packets to file