

# Network Monitoring and Traffic Analysis



# Network Monitoring

---

- ❖ Agenda
  - ❖ A Quick Review of Network Monitoring
  - ❖ A Collection of Common Network Traffic Tools
    - ❖ This Will be a “Play As We Go” Lecture
    - ❖ The Tools We Will Cover:
      - ❖ FlowTools, Sniffers, Graphical, and Hacker

# Network Monitoring

---

- ❖ FlowTools
  - ❖ flow-capture, flow-cat, flow-nfilter, flow-report
- ❖ Sniffers
  - ❖ tcpdump, (snort), nload, iptraf
- ❖ Graphical Tools
  - ❖ wireshark, etherape, ntop
- ❖ Hacker Tools
  - ❖ dsniff, driftnet, ettercap

# Warning

---

- ❖ We'll Be Sniffing Traffic From Here On Out
- ❖ dsniff will be running during this lecture
- ❖ We'll Report At the End If We Caught Anything

# Monitoring Location

---

- ❖ Tends to be at the Distribution Layer (center) of Your Network
- ❖ On HP Switches, it's called the "Monitor Port"
- ❖ On Cisco Switches, it's called the "SPAN Port"
- ❖ Cisco Switches have much more powerful Capabilities for controlling the Monitoring, can control RX and TX, and even forward to another switch: RSPAN

# Monitor Location

---

- ❖ Can be Off a passive Optical Splitter (fiber)
- ❖ Need Out-of-Band Management Only (you do not want this box getting hacked... ever!)
- ❖ Requires Powerful Box: CPU/MEMORY/IO
- ❖ May need to tune NIC
- ❖ May need to tune OS
  - ❖ see: ethtool, and sysctl

# Promiscuous Mode

---

- ❖ Some of These Commands do NOT put the interface into “promiscuous mode”. To sniff all frames you need to be in promiscuous mode.
- ❖ This means your NIC will pay attention to more frames instead do just your own IP/MAC frames.
- ❖ To force promiscuous mode if necessary:
  - ❖ `sudo ifconfig eth0 promisc`
- ❖ To turn off promiscuous mode if necessary:
  - ❖ `sudo ifconfig eth0 -promisc`

# FlowTools

---

- ❖ A Cisco Router Export Flow Format: NetFlow
- ❖ A Standard for Connecting Packet Statistics
- ❖ Information tends to include additional Router Information, such as ASPATH
- ❖ You must configure the router to export flows
- ❖ Different Versions: v5, v7, etc. Make sure that you export a version that is the same as your collector



# FlowTools

---

- ❖ How it Works
  - ❖ The Router Samples Packets
  - ❖ This is a “lossy” Mechanism
  - ❖ Flows are “connection” oriented
  - ❖ The export to the collector is over UDP
  - ❖ The Traffic can be fairly High
  - ❖ A Single SYN packet will generate a “flow”

# FlowTools

---

- ❖ Installation on the Collector
  - ❖ `sudo apt-get install flow-tools`
  - ❖ `dpkg -L flow-tools`
  - ❖ Configuration in `/etc/flow-tools`
  - ❖ Startup is `/etc/init.d/flow-capture`
  - ❖ Startup config is `/etc/init.d/flow-capture.conf`
  - ❖ Example: `-w /var/flow 0/0/3002`
    - ❖ Listen on port 3002 from anywhere

# FlowTools

---

## Simple Processing Example: Report All Flows For Yesterday

```
#!/usr/bin/perl

@files=`find /flows -type f -daystart -mtime -1`;
chomp(@files);

foreach $file (@files) {
    open(INPUT,"flow-cat $file | flow-report |");
    while(<INPUT>) { print; }
}
```

# FlowTools: Output Format

---

- ❖ Defaults for flow-report command
- ❖ Configured in: `/etc/flow-tools/stat.cfg`
- ❖ Sorting can be any of: `flows,octets,packets`  
`duration,avg-pps,min-pps,max-pps, avg-bps,min-`  
`bps,max-bps`

# FlowTools: Output Format

---

```
stat-report default
type @{\TYPE:-ip-source/destination-address/
ip-protocol/ip-tos/ip-source/destination-port}
output
format ascii
sort @{\SORT:-+flows}
fields @{\FIELDS:-+}
options @{\OPTIONS:-+header,+xheader,+totals}
path |flow-rptfmt @{\RPTOPT:--f ascii}
stat-definition default
report default
```

# FlowTools: Filter Format

---

- ❖ Define Address Matches
- ❖ Filter "Primitives" plus Filter "Definitions" To Make Matches

```
filter-primitive UDPTCP
  type ip-protocol
  permit tcp
  permit udp
```

```
filter-definition udptcp
  match ip-protocol UDPTCP
```

```
filter-primitive mynetaddr
  type ip-address-mask
  permit 123.234.0.0 255.255.0.0
  default deny
```

```
filter-definition mynet
  match ip-source-address mynetaddr
  match ip-destination-address mynetaddr
```

# FlowTools: Commands

---

## Flow Tools Binaries - Chaining Commands

% flow-cat       # concatenate binary flow files and output  
% flow-nfilter   # apply filters to input flow stream  
% flow-report    # process and output flow reports

### Example:

```
flow-cat $filelist | flow-nfilter -F $filterdef | flow-report -S  
$report-format
```

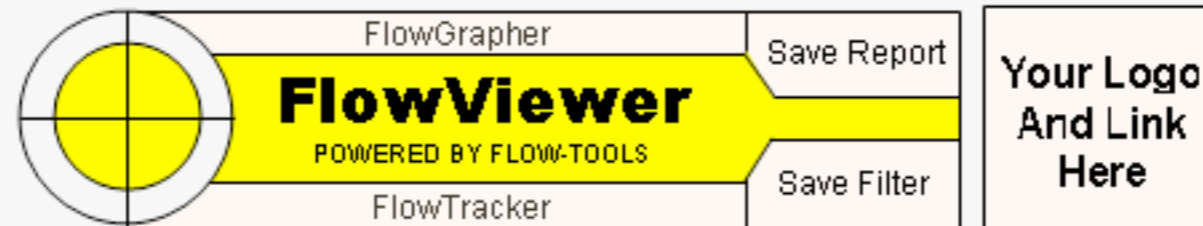
# FlowTools: Web Interface

---

- ❖ There are Three Web CGI Interface Tools
- ❖ FlowViewer, FlowGrapher, and FlowTracker
- ❖ Website: <http://ensight.eos.nasa.gov/FlowViewer/>



# FlowReport



Report: 132 Columns  
 Start Time: December 12, 2007 17:00:00 GMT  
 Device: gsfc\_6509  
 Source:

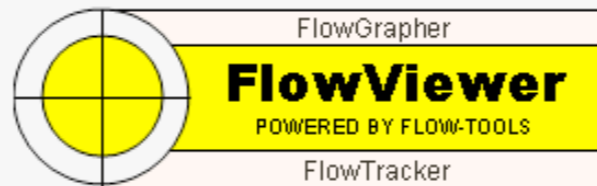
Sort Field: n/a  
 End Time: December 12, 2007 18:00:00 GMT  
 Exporter:  
 Destination: -192.168.194.0/24, -172.160.194.0/24,  
 -192.168.236.0/24, -172.160.198.0/23

Source Port:  
 Source I/F: 7, 62  
 Source AS:  
 TOS Field:  
 Include if: Any part of flow in Time Period  
 Lines Cutoff: 100

Destination Port:  
 Destination I/F: 0  
 Destination AS:  
 TCP Flag:  
 Protocols:  
 Octets Cutoff:

Start	End	Sif	SrcIPaddress	SrcP	Dif	DstIPaddress	DstP	P	Fl	Pkts	Octets
1212.16:28:15.506	1212.17:00:15.669	62	172.160.254.16	22	0	111.222.162.166	1837	6	0	66	4620
1212.16:28:17.887	1212.17:00:17.350	62	172.160.254.18	514	0	192.168.210.233	514	17	0	887	74236
1212.17:00:20.828	1212.17:00:20.828	7	172.160.195.52	3045	0	172.160.220.2	32771	6	0	1	141
1212.17:01:20.836	1212.17:01:20.836	7	172.160.195.52	3045	0	172.160.220.2	32771	6	0	1	141
1212.16:29:43.005	1212.17:01:53.025	62	172.160.254.52	22	0	111.222.162.166	1415	6	0	846	887540
1212.16:30:07.132	1212.17:02:05.378	62	172.160.254.62	514	0	192.168.210.233	514	17	0	1032	86505
1212.17:02:15.092	1212.17:02:15.092	7	172.160.195.2	53	0	172.160.220.2	32768	17	0	1	184
1212.16:30:23.118	1212.17:02:35.763	62	172.160.254.23	514	0	192.168.210.233	514	17	0	5440	476979
1212.16:30:29.323	1212.17:01:36.422	62	172.160.195.52	3045	0	198.119.135.34	50500	6	0	134	20656
1212.16:30:38.013	1212.17:02:43.919	62	172.160.254.22	514	0	192.168.210.233	514	17	0	6223	547010
1212.17:02:20.840	1212.17:02:20.840	7	172.160.195.52	3045	0	172.160.220.2	32771	6	0	1	141
1212.16:30:53.391	1212.17:02:43.363	62	172.160.254.52	514	0	192.168.210.233	514	17	0	201	17502
1212.16:31:14.747	1212.17:03:14.373	62	172.160.254.18	22	0	111.222.162.163	35690	6	0	66	5544
1212.17:03:00.620	1212.17:03:00.620	7	172.160.195.2	53	0	172.160.220.2	32768	17	0	1	176
1212.17:03:20.848	1212.17:03:20.848	7	172.160.195.52	3045	0	172.160.220.2	32771	6	0	1	141
1212.16:59:35.670	1212.17:00:00.032	62	172.160.254.27	53817	0	137.78.58.79	20	6	0	9700	13741937

# FlowViewer



Your Logo  
And Link  
Here

**Filter Criteria:**

**Device:**       **Next Hop IP:**

**Start Date:**  (mm/dd/yyyy)      **Start Time:**  (hh:mm:ss)      **TOS Field:**  (e.g., -0x0b/0x0F)

**End Date:**  (mm/dd/yyyy)      **End Time:**  (hh:mm:ss)      **TCP Flag:**       **Protocol:**

**Source IP:**       **Source Interface:**        **Source Port:**       **Source AS:**

**Dest IP:**       **Dest Interface:**        **Dest Port:**       **Dest AS:**


Notes: Multiple field entries, separated by commas, are permitted in the fields above.  
A minus sign (-) will negate an entry (e.g. -1776 for AS, would mean any AS but 1776).  
IP fields accept networks (e.g. 192.168.10.0/19), hosts, and names (e.g. www.abc.com).

## Reporting Parameters:

**Statistics:**       **Printed:**       **Include Flow if:**       **Sort Field:**

**Pie Charts:**       **Cutoff Lines:**       **Cutoff Octets:**       **Resolve Addresses:**       **Oct Conv:**       **Sampling Multip.:**

# FlowGrapher



FlowViewer  
**FlowGrapher**  
POWERED BY FLOW-TOOLS  
FlowTracker

Save Report

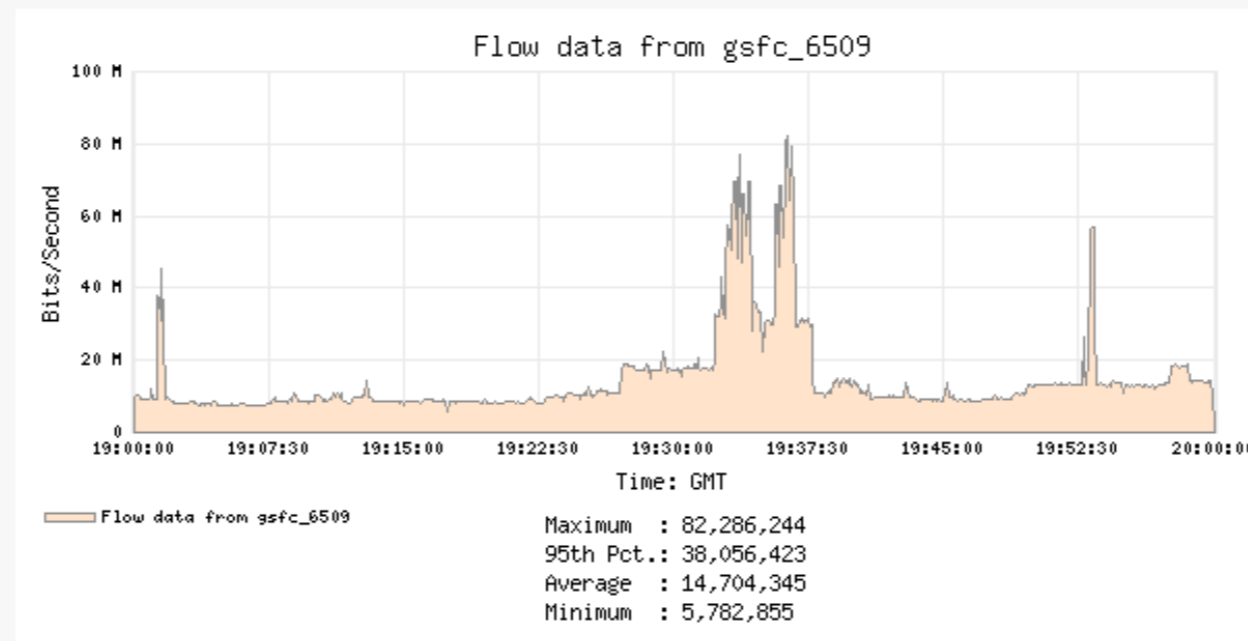
---

Save Filter

**Your Logo  
And Link  
Here**

Report: Flow Graph Bits/Second  
 Start Time: December 11, 2007 19:00:00 GMT  
 Device: vlyy\_6509  
 Source:  
 Source Port:  
 Src I/F Name: TSDIS (23)  
 Source AS:  
 TOS Field:  
 Include if: Any part of flow in Time Period  
 Detail Lines: 20

Sample Time: 5  
 End Time: December 11, 2007 20:00:00 GMT  
 Exporter:  
 Destination:  
 Destination Port:  
 Dest I/F Name:  
 Destination AS:  
 TCP Flag:  
 Protocols:  
 Graph Width: 1



Start	End	Len	Source Host	Port	Destination Host	Port	Total Bytes	Mbps
19:27:06	19:28:42	95.7	xxgre.mocsan.mirh.org	36392	samantha.cral.mirh.org	50676	101,199,734	8.457
19:28:44	19:30:28	104.5	xxgre.mocsan.mirh.org	36462	samantha.cral.mirh.org	19602	101,174,434	7.742

# SNIFFERS

---

# TCPDUMP

---

❖ Can Do Flag Matching Using TCPDUMP

❖ Summary Here: <http://www.security-forums.com/viewtopic.php?t=22770>

❖ SYN Grabbing:

❖ `'tcp[13] & 0xFF == 0x2'`

❖ SYN/ACK Grabbing:

❖ `'tcp[13] & 0xFF == 0x12'`

❖ Example Command Line:

❖ `/usr/sbin/tcpdump -n -i eth1 -s 64 -w /data/tcp/synackdata/${HOUR} 'tcp[13] & 0xFF == 0x12' < /dev/null 1>/dev/null 2>&1 &`

# TCPDUMP

---

## ❖ TRY IT!

- ❖ run tcpdump on the command-line, match SYN using the flags option: `'tcp[13] & 0xFF == 0x02'`

# NLOAD

---

- ❖ This is a quick command-line curses view of the traffic total on your interface
- ❖ `sudo apt-get install nload`
- ❖ Example: `% nload -u m -i 200`
  - ❖ megabits/second, 200msec update interval
- ❖ **TRY IT!**





# IPTRAF

---

- ❖ Curses View of Active Talkers and Interface Statistics
- ❖ Top Talkers, SRC and DEST
- ❖ Sortable by Packet Total, Byte Total ETC.

"monitor" == TCP Connections, Source/Dest

"Detailed" == Interface Only Statistics

"Statistical Breakdown" == by Protocol/Port

"Lan Station Monitor" == by MAC Address

# IPTRAF

---

- ❖ Other Options: “o”
  - ❖ “R” for DNS Lookups
  - ❖ “F” force promiscuous mode
  - ❖ “M” show packet sizes
- ❖ Filters:
  - ❖ Edit Filter, Attach Filter, Detach Filter
  - ❖ 10.1.1.1/0:65535 <-> 0.0.0.0/0:0
  - ❖ Must Specify Port Ranges
  - ❖ SRC/DST Reporting is TCP Only

# IPTRAF

---

- ❖ Can also run a Batch Mode to a File
- ❖ `% iptraf -i eth0 -B`
- ❖ `% pkill iptraf`
- ❖ `% cd /var/log/iptraf`
- ❖ **TRY IT!**

# IPTRAF

```
ait@ubuntu: ~  
File Edit View Terminal Tabs Help  
IPtraf  
TCP Connections (Source Host:Port) ————— Packets — Bytes Flags Iface  
192.168.77.128:39497 = 149442 5978121 RESET eth0  
203.159.31.69:80 = 361295 537573275 -PA- eth0  
  
TCP: 1 entries ————— Active  
  
UDP (68 bytes) from 192.168.77.128:5353 to 224.0.0.251:5353 on eth0  
UDP (49 bytes) from 127.0.0.1:50790 to 127.0.0.1:512 on lo  
UDP (49 bytes) from 127.0.0.1:50790 to 127.0.0.1:512 on lo  
ICMP dest unrch (port) (77 bytes) from 127.0.0.1 to 127.0.0.1 on lo  
ICMP dest unrch (port) (77 bytes) from 127.0.0.1 to 127.0.0.1 on lo  
Bottom ————— Elapsed time: 0:05  
Pkts captured (all interfaces): 510751 | TCP flow rate: 0.00 kbits/s  
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit
```

# GRAPHICAL TOOLS

---

# WIRESHARK

---

- ❖ <http://www.wireshark.org/>
- ❖ More than Just a Sniffer
- ❖ Protocol Decoding
- ❖ Transport Stream Reassembly
- ❖ Used to Be “Ethereal”
- ❖ Supports Filter Expression Matching
- ❖ Supports Reading/Writing Various Captures Formats
- ❖ Text-based version is: "tshark"

# WIRESHARK

---

- ❖ Standard Packet Format is "pcap", (like tcpdump)
- ❖ Filter Language is like tcpdump filters
- ❖ Output Display Format Supports Naming
  - ❖ ethernet oui, tcp/udp ports, hostnames
- ❖ Protocol and Traffic Statistics Reporting
- ❖ % sudo apt-get install wireshark
- ❖ TRY IT!

# WIRESHARK

The screenshot shows the Wireshark interface with the following components:

- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Help.
- Toolbar:** Includes icons for file operations, capture, analysis, and navigation.
- Filter Bar:** Filter: [ ] + Expression... Clear Apply
- Packets List:**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Parallel_c5:b1:15	Broadcast	ARP	Who has 10.211.55.1? Tell 10.211.55.5
2	0.005655	Parallel_00:00:02	Parallel_c5:b1:15	ARP	10.211.55.1 is at 00:1c:42:00:00:02
3	0.005792	10.211.55.5	10.211.55.1	DNS	Standard query A aitwsws.net
4	0.312514	10.211.55.1	10.211.55.5	DNS	Standard query response A 203.159.31.69
5	0.321137	10.211.55.5	203.159.31.69	TCP	36501 > http [SYN] Seq=0 Len=0 MSS=1460
6	0.324744	203.159.31.69	10.211.55.5	TCP	http > 36501 [SYN, ACK] Seq=0 Ack=1 Win=
7	0.324861	10.211.55.5	203.159.31.69	TCP	36501 > http [ACK] Seq=1 Ack=1 Win=5856
8	0.325260	10.211.55.5	203.159.31.69	HTTP	GET / HTTP/1.1
9	0.326998	203.159.31.69	10.211.55.5	TCP	http > 36501 [ACK] Seq=1 Ack=398 Win=691
10	0.327129	203.159.31.69	10.211.55.5	TCP	[TCP segment of a reassembled PDU]
11	0.327414	10.211.55.5	203.159.31.69	TCP	36501 > http [ACK] Seq=398 Ack=1449 Win=
12	0.327260	203.159.31.69	10.211.55.5	TCP	[TCP segment of a reassembled PDU]
13	0.327670	10.211.55.5	203.159.31.69	TCP	36501 > http [ACK] Seq=398 Ack=2897 Win=
- Packet Details:**
  - Frame 51 (66 bytes on wire, 66 bytes captured)
  - Ethernet II, Src: Parallel\_c5:b1:15 (00:1c:42:c5:b1:15), Dst: Parallel\_00:00:02 (00:1c:42:00:00:02)
  - Internet Protocol, Src: 10.211.55.5 (10.211.55.5), Dst: 203.159.31.69 (203.159.31.69)
  - Transmission Control Protocol, Src Port: 36501 (36501), Dst Port: http (80), Seq: 398, Ack: 34020, Len: 0
- Packet Bytes:**

```

0000  00 1c 42 00 00 02 00 1c 42 c5 b1 15 08 00 45 00  ..B.....B.....E.
0010  00 34 5c 91 40 00 40 06 b1 76 0a d3 37 05 cb 9f  .4\.@.@. .v..7...
0020  1f 45 8e 95 00 50 01 1b b7 4a be f8 5a 42 80 10  .E...P.. .J..ZB..
0030  04 ef ec f2 00 00 01 01 08 0a 00 21 e9 cf 0a b8  .....!.....
    
```
- Status Bar:** File: "/tmp/etherXXXXIH4KBL" 48 KB 00:00:46 P: 100 D: 100 M: 0 Drops: 0



# EtherApe

---

- ❖ Creates a MESH of Talking Nodes In A Window
- ❖ Lines in the MESH Get Wider as Traffic Increases
- ❖ Includes Protocol Statistics
- ❖ Some filtering expression capabilities

# NTOP

---

- ❖ Network Monitor Daemon
- ❖ <http://www.ntop.org/>
- ❖ Luca Deri, University of Pisa
- ❖ Project is now Ten Years Old!!!
- ❖ Named after "%otop", but for Networks
- ❖ Builtin Web Server Interface
- ❖ Builtin RRD Graphing

# NTOP FEATURES

---

- ❖ Traffic Characterization
- ❖ Host Characterization, History, Protocols
- ❖ Network Interface Statistics Graphs
- ❖ ASN Reporting
- ❖ sFLOW/netFlow Reporting
- ❖ Can act as Both a Receiver and Sender of NetFlow
- ❖ ThruPut Reports
- ❖ Activity Reports
- ❖ Plugins Provide Additional Feature

# NTOP Installation

---

- ❖ `% apt-get install ntop`
- ❖ `% dpkg -L ntop`
- ❖ NTOP Configuration: `/etc/ntop`
- ❖ NTOP Configuration: `/var/lib/ntop/init.cfg`
- ❖ `% sudo ntop --set-admin-password`
- ❖ `% /etc/init.d/ntop start`
- ❖ Now Point Your Browser At:
- ❖ <http://localhost:3000>
- ❖ TRY IT!

# NTOP

Network Traffic [TCP/IP]: All Hosts - Data Sent+Received

Hosts:  Data:

Host	Domain	Data	FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP
10.211.55.5		1.3 MBytes 50.0 %	0	1.3 MBytes	4.3 KBytes	0	0	0	0
sb.google.com		1.1 MBytes 40.7 %	0	1.1 MBytes	0	0	0	0	0
www.securityfocus.com		95.5 KBytes 3.6 %	0	95.5 KBytes	0	0	0	0	0
adserver.securityfocus.com		64.2 KBytes 2.4 %	0	64.2 KBytes	0	0	0	0	0
packetstorm.offensive-security.com		49.7 KBytes 1.9 %	0	49.7 KBytes	0	0	0	0	0
jlinks.industrybrains.com		10.5 KBytes 0.4 %	0	10.5 KBytes	0	0	0	0	0
m1.2mdn.net		9.6 KBytes 0.4 %	0	9.6 KBytes	0	0	0	0	0
ad.afy11.net		9.2 KBytes 0.3 %	0	9.2 KBytes	0	0	0	0	0
10.211.55.1		4.3 KBytes 0.2 %	0	0	4.3 KBytes	0	0	0	0
www.industrybrains.com		3.4 KBytes 0.1 %	0	3.4 KBytes	0	0	0	0	0

# HACKER TOOLS

---

# DRIFTNET

---

- ❖ A Sniffer for Grabbing Image Files
- ❖ <http://ex-parrot.com/~chris/driftnet/>
- ❖ Also Located on the BackTrack CD
  - ❖ % locate driftnet
- ❖ Also able to Grab MPEG Audio Files
- ❖ So the Hackers Can Grab Files Too!!!
- ❖ TRY IT!

# DRIFTNET

The screenshot shows a web browser window titled "driftnet". At the top left, there is a button labeled "Take the Survey". The main content area is a collage of various images, including a large photo of a destroyed bridge with rubble, a row of small portrait photos of people, and a row of small landscape and event photos. Below the collage is a grid of navigation buttons: "Mobile", "RSS", "Podcasts", "Email Alerts", "Desktop Alerts", "PDA", "Partner Hotels", and "How to get CNN". At the bottom, there are several logos and images, including "No Image", "world sport", "IN ASSOC WITH Nikon", "360", "CNN Traveller", "TIME.com", and "IN ASSOC WITH Kellogg".



# DSNIFF

---

- ❖ Dug Song
- ❖ <http://www.monkey.org/~dugsong/dsniff/>
- ❖ DSniff, Usenix Conference, Year 2000
- ❖ Producing Behavior Change Through Embarrassment!
- ❖ A Collection of Tools

# DSNIFF

---

- ❖ What Tools Does The DSNIFF Package Include?
  - ❖ dsniff, arpspoof, dnsspoof, macof, sshmitm, webmitm, filesnarf, webspay
- ❖ What Kind of Password Strings Does it Grab?
  - ❖ FTP, Telnet, HTTP,POP,poppass, NNTP,IMAP,SNMP, LDAP,Rlogin, RIP,OSPF,NFS, YP, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster,PostgreSQL, Meeting Maker,Citrix ICA, Symantec

# DSNIFF

---

- ❖ DSNIFF Report: Did we see any ClearText Passwords?