Review - a Tool for Reviewing Tcpdump Logs

Steve Romig

romig@net.ohio-state.edu
1-614-688-3412
UTS Network Security Group
The Ohio State University
Columbus, Ohio 43210

What are packet logs?

- Not just transaction log
- Record of packet contents
- What they typed, mail they read, mail sent, URLs visited, file transferred...
- Internet equivalent of a wiretap

Why collect packet logs?

- We have crackers dialing in through our modem pool
- We want to know who they are
- More - we want to know what they do, where
- Only way to witness what they are doing
- Also aids in follow up

How do we collect packet logs?

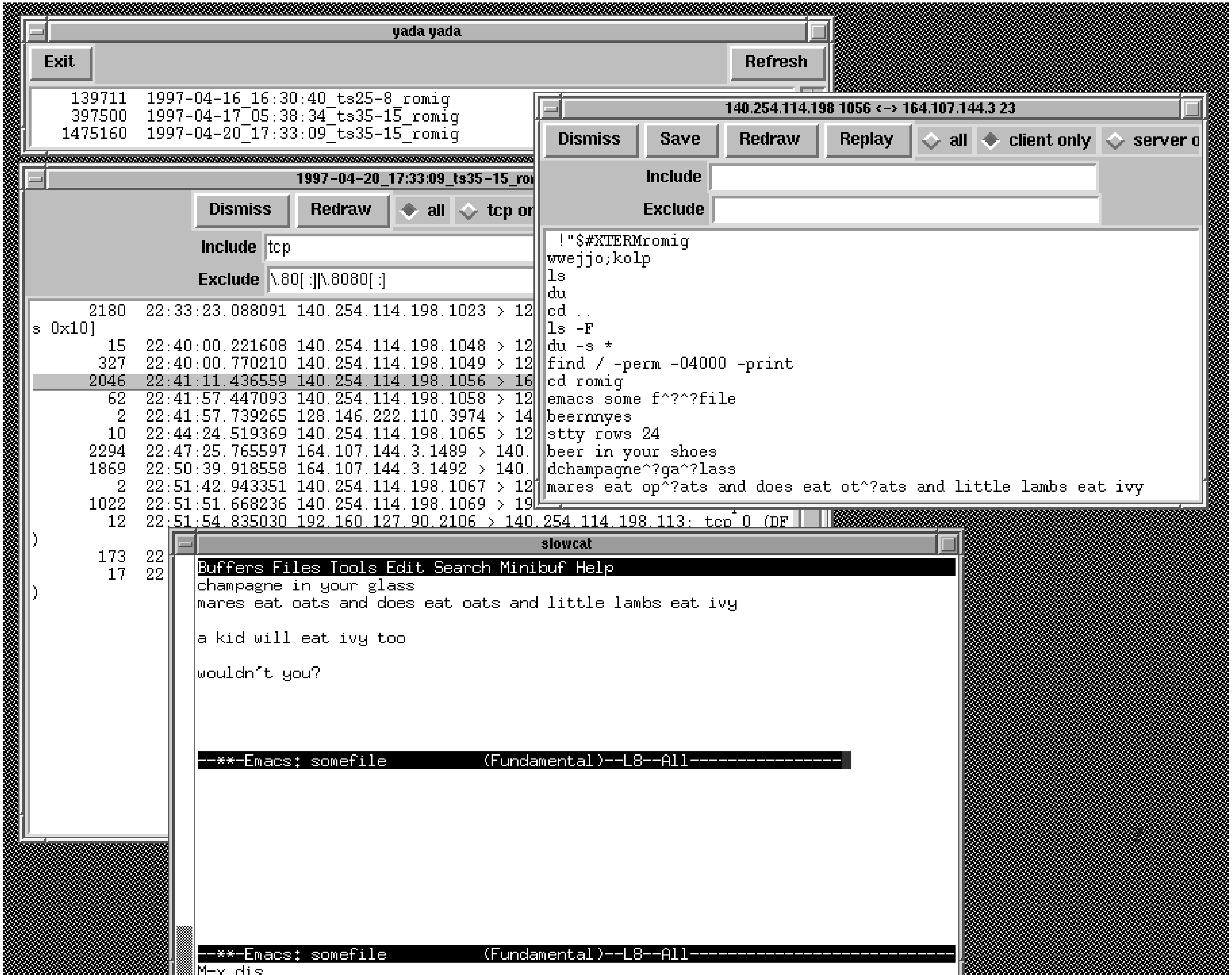
- “Automated” for most cases
- Tools watch authentication logs, detect cracker logins
- Configuration file controls actions (page, log)
- Another file tells where to log
- Tcpdump started/stopped as needed
- Generates many, many logs

The problem we faced:

- Automated collection of tcpdump logs of cracker sessions
- 1.5 gigabytes per month
- Packets are hard to read through
- Some protocols especially hard - telnet, X

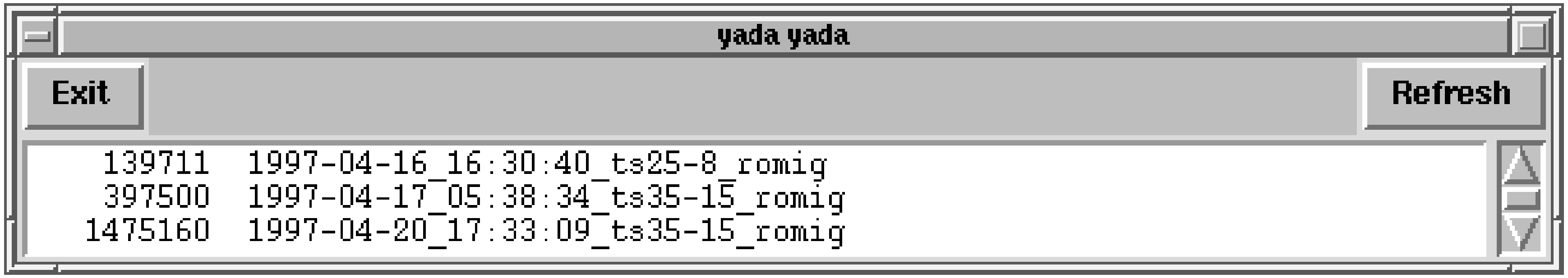
Our solution - “review”

- Perl/Tk scripts provide GUI for tcpdump
- Point-n-click to browse through logs
- Varying detail - from summary to contents
- Special replay features for telnet, X


yada yada
Exit
Refresh
139711 1997-04-16_16:30:40_ts25-8_romig
397500 1997-04-17_05:38:34_ts35-15_romig
1475160 1997-04-20_17:33:09_ts35-15_romig
1997-04-20_17:33:09_ts35-15_ro
Dismiss
Redraw
all
tcp on
Include
tcp
Exclude
\.80[:]|\.8080[:]
2180 22:33:23.088091 140.254.114.198.1023 > 12
s 0x10]
15 22:40:00.221608 140.254.114.198.1048 > 12
327 22:40:00.770210 140.254.114.198.1049 > 12
2046 22:41:11.436559 140.254.114.198.1056 > 16
62 22:41:57.447093 140.254.114.198.1058 > 12
2 22:41:57.739265 128.146.222.110.3974 > 14
10 22:44:24.519369 140.254.114.198.1065 > 12
2294 22:47:25.765597 164.107.144.3.1489 > 140.
1869 22:50:39.918558 164.107.144.3.1492 > 140.
2 22:51:42.943351 140.254.114.198.1067 > 12
1022 22:51:51.668236 140.254.114.198.1069 > 19
12 22:51:54.835030 192.160.127.90.2106 > 140.254.114.198.113: tcp 0 (DF
)
173 22
17 22
)
140.254.114.198 1056 <-> 164.107.144.3 23
Dismiss
Save
Redraw
Replay
all
client only
server o
Include
Exclude
!"$#XTERMromig
wwejjo;kolp
ls
du
cd ..
ls -F
du -s *
find / -perm -04000 -print
cd romig
emacs some f^?^?file
beernnyes
stty rows 24
beer in your shoes
dchampagne^?ga^?lass
mares eat op^?ats and does eat ot^?ats and little lambs eat ivy
slowcat
Buffers Files Tools Edit Search Minibuf Help
champagne in your glass
mares eat oats and does eat oats and little lambs eat ivy
a kid will eat ivy too
wouldn't you?
--**-Emacs: somefile (Fundamental)--L8--All----------------
--**-Emacs: somefile (Fundamental)--L8--All--------------------------
M-x dis

Main window - list of logs

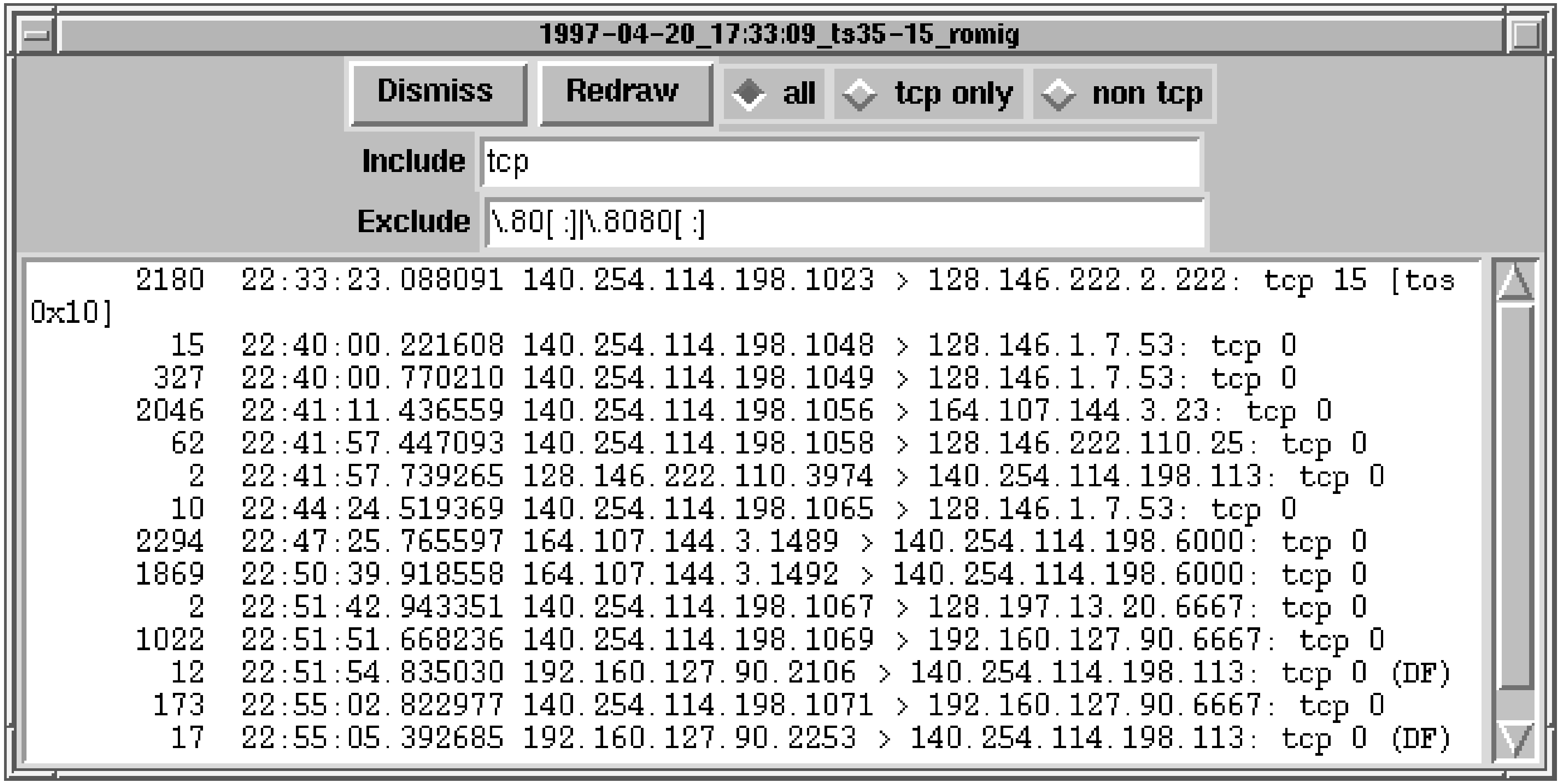
- Scroll-able list of log file names
- Names given on command line
- Log file names are arbitrary
- Log sizes in bytes indicated on left



A sample log listing window (main window)

Select a file, and get the log summary window

- Packet count, time, source, destination...
- In this example, lines matching "tcp" are included
- ...and web services are excluded



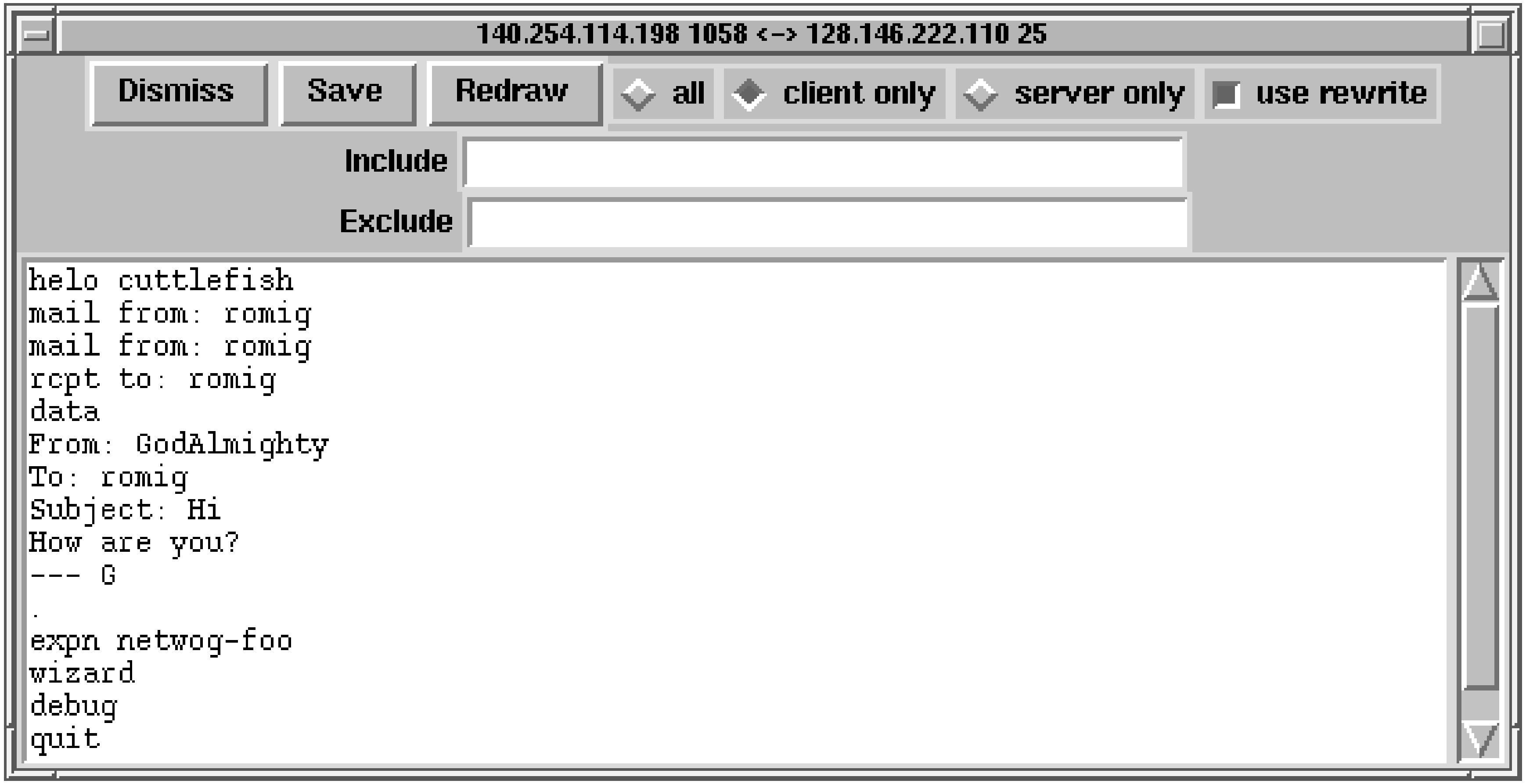
A summary window for a log

Select a session to view it. For example:

Browsing an SMTP (sending mail) session

- Client traffic selected

- Shows printable ASCII characters



Browsing an SMTP session, client traffic only

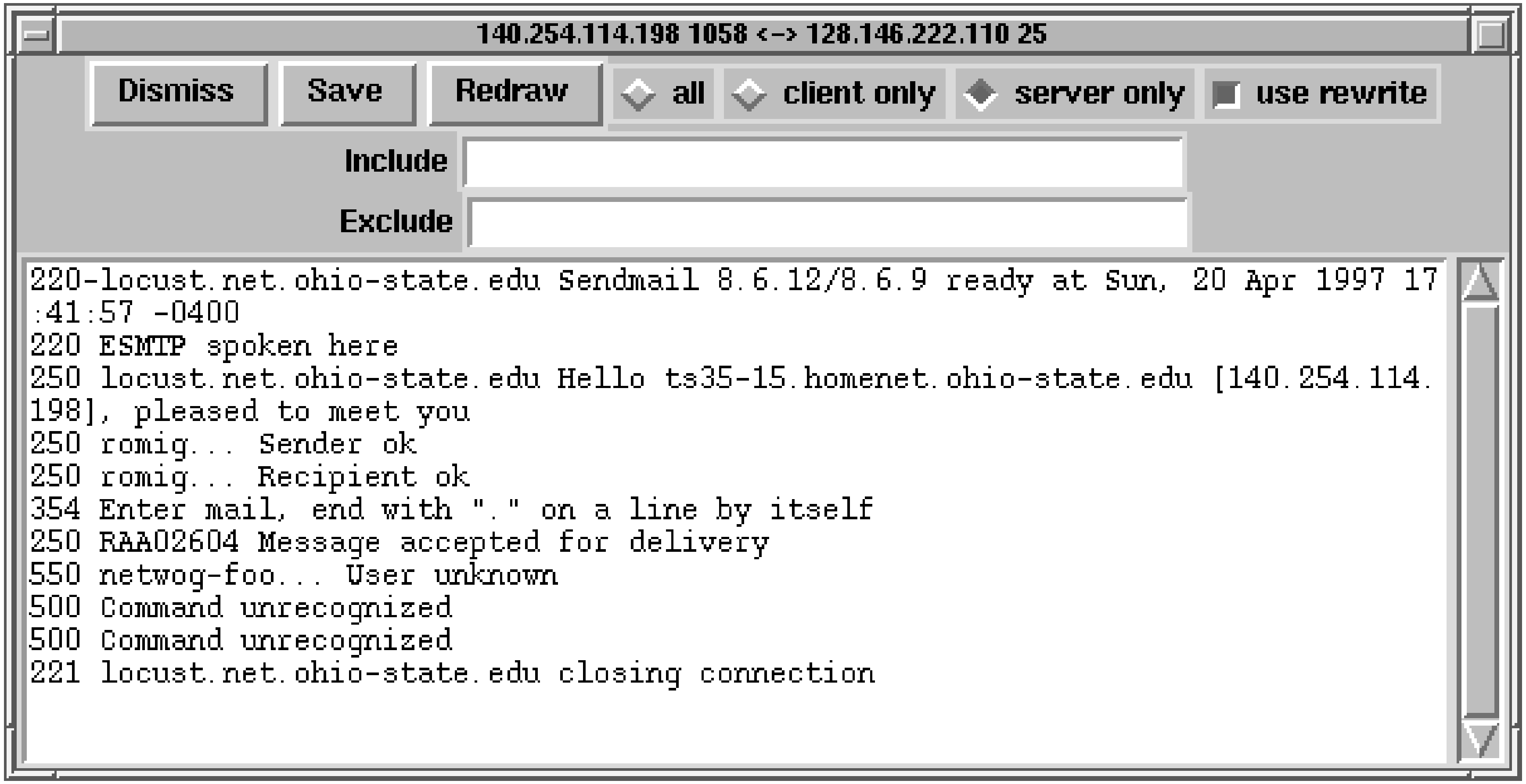
Can also:

- Show client, server or all traffic

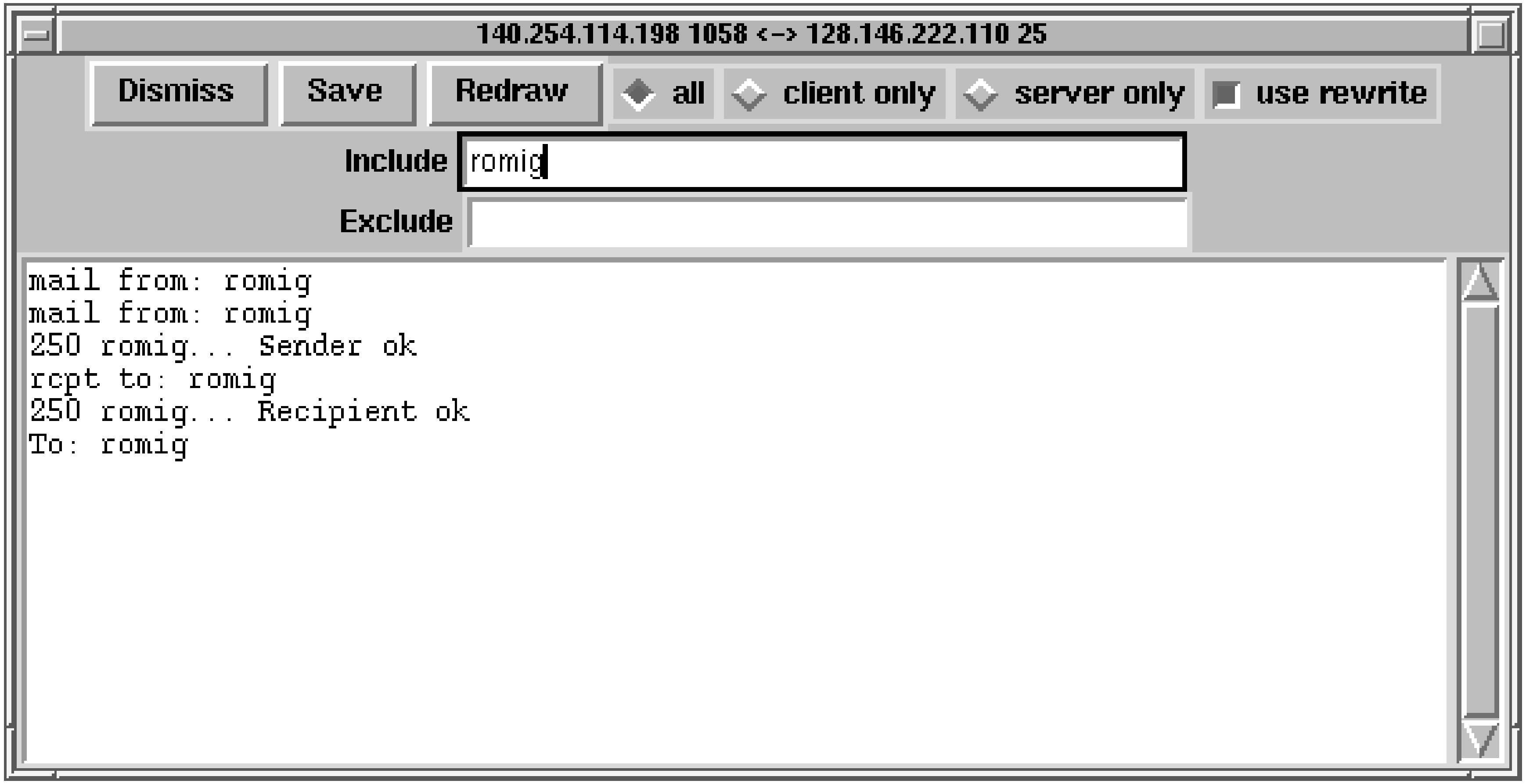
- Next slide shows server traffic

- Can filter with include/exclude

- Client/server text is NOT marked when shown together



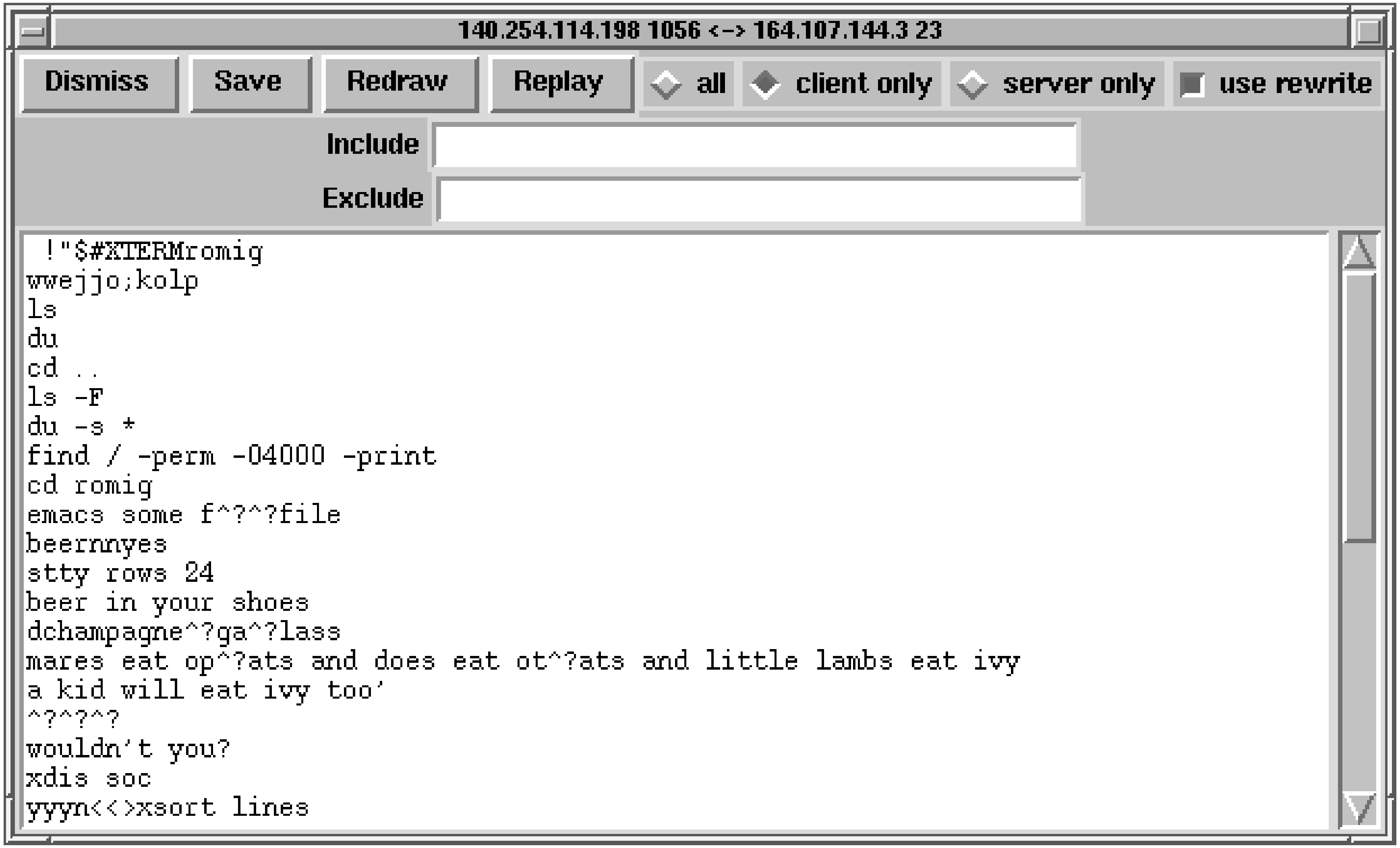
Browsing an SMTP session, server traffic



Browsing an SMTP session, all traffic, include “romig”

Another session - browsing telnet

- This example: client end only
- This is what the user typed
- Fairly easy to read
- Yes, that’s my old password at the top

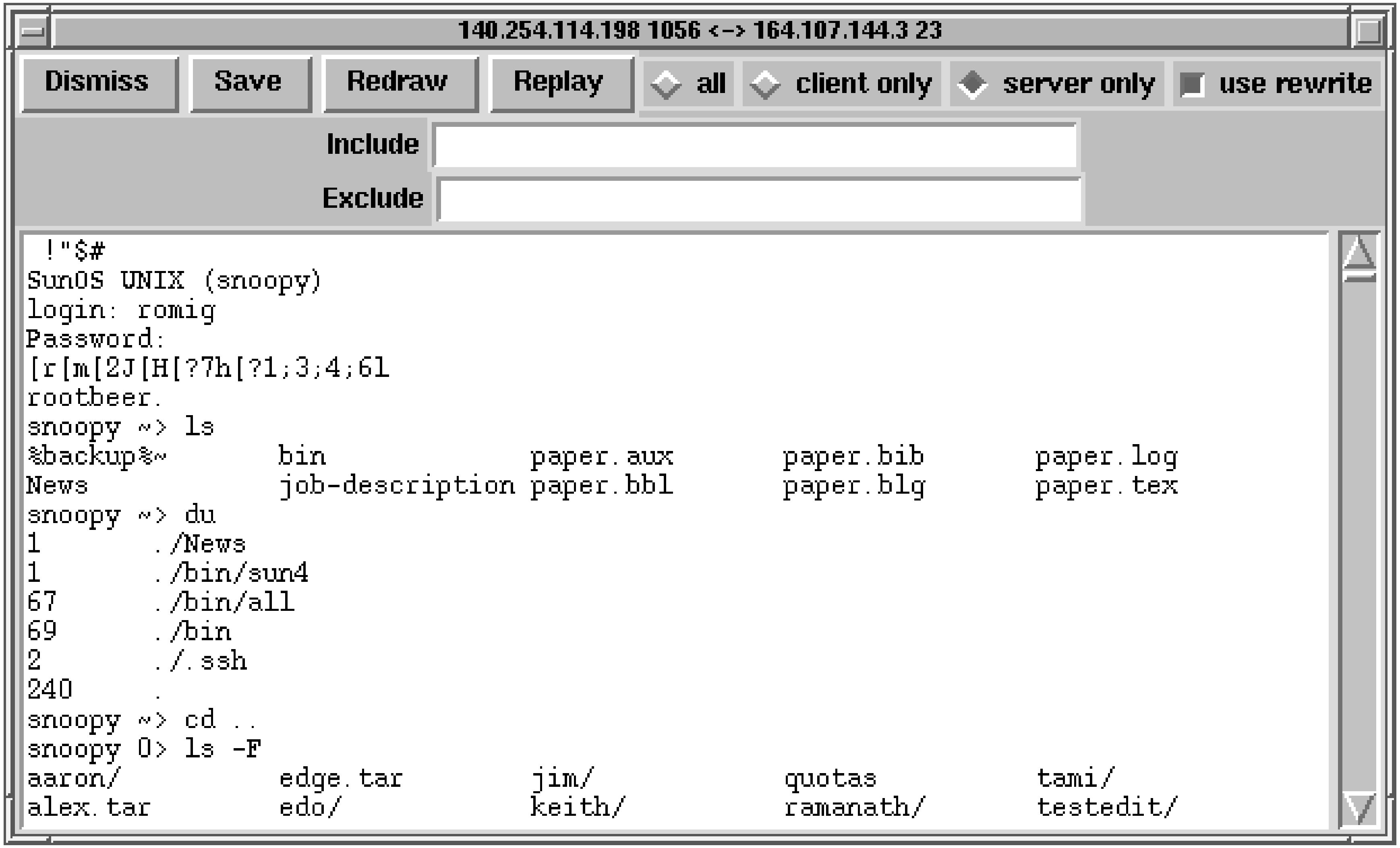


Browsing a Telnet session - what the user types

Same session, server side

- What the user sees

- This is not so bad...

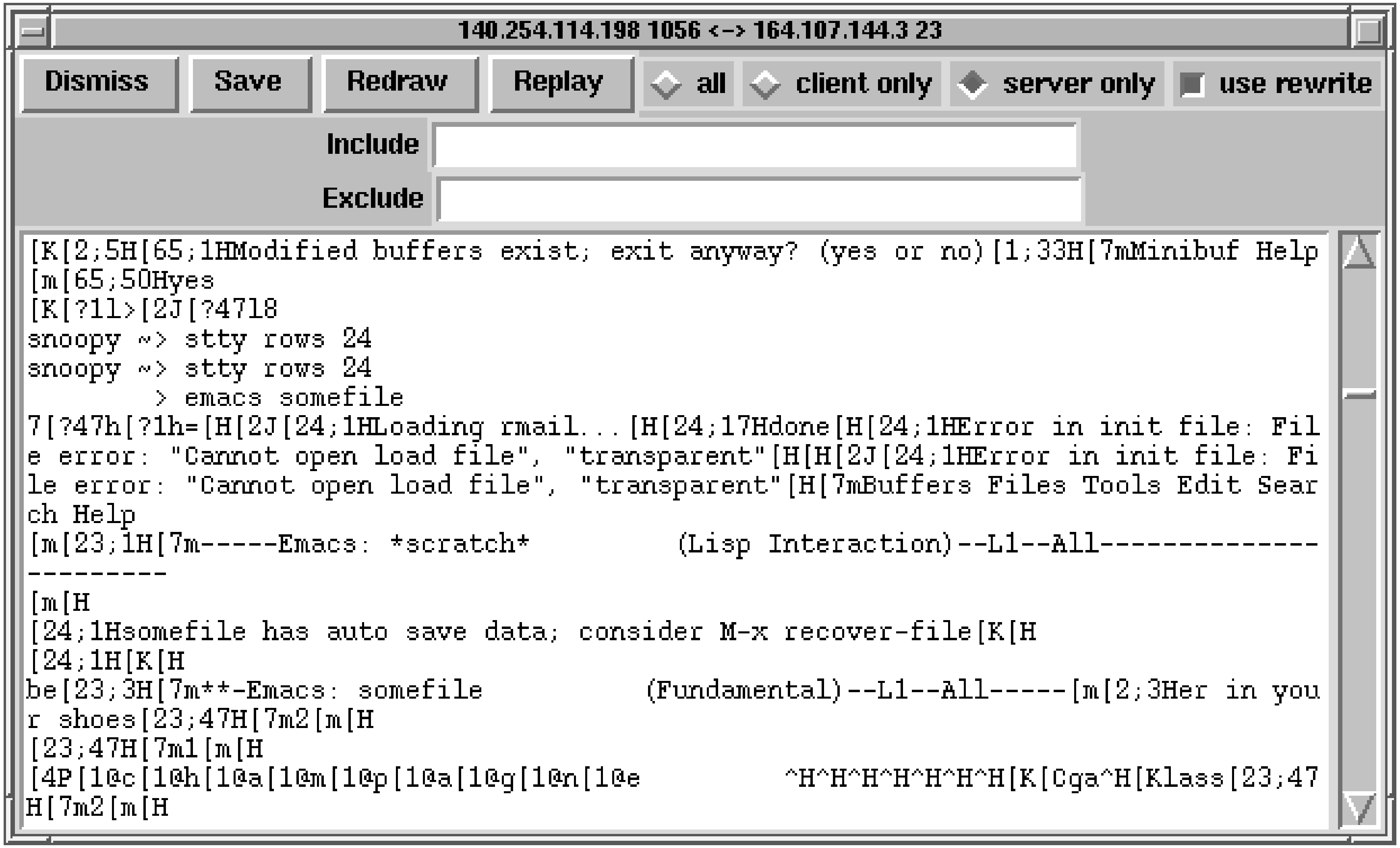


Browsing Telnet - what the user “sees”

Same session, server side

- ...but this is hard to read

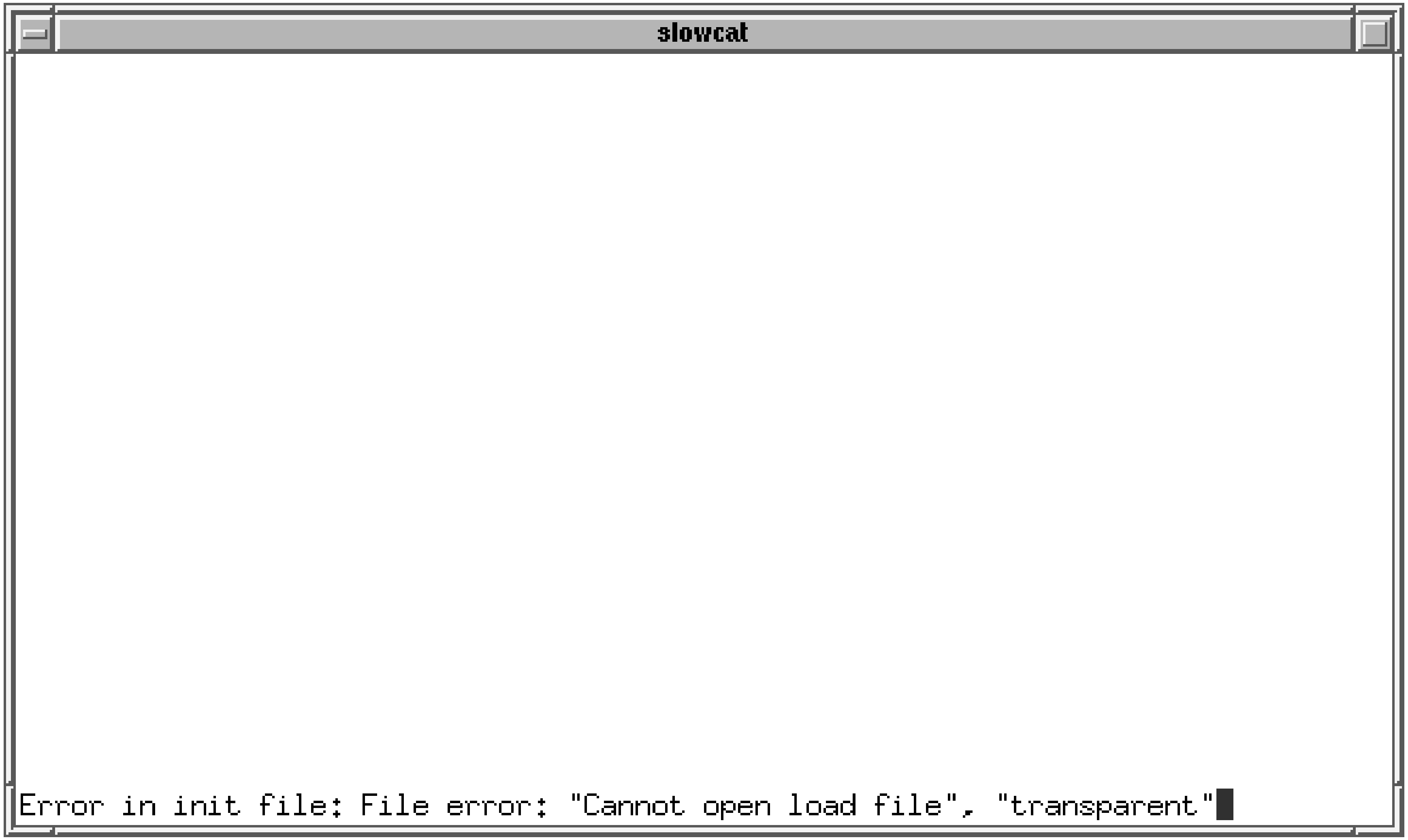
- Similar problems with output from pico, vi, pine...



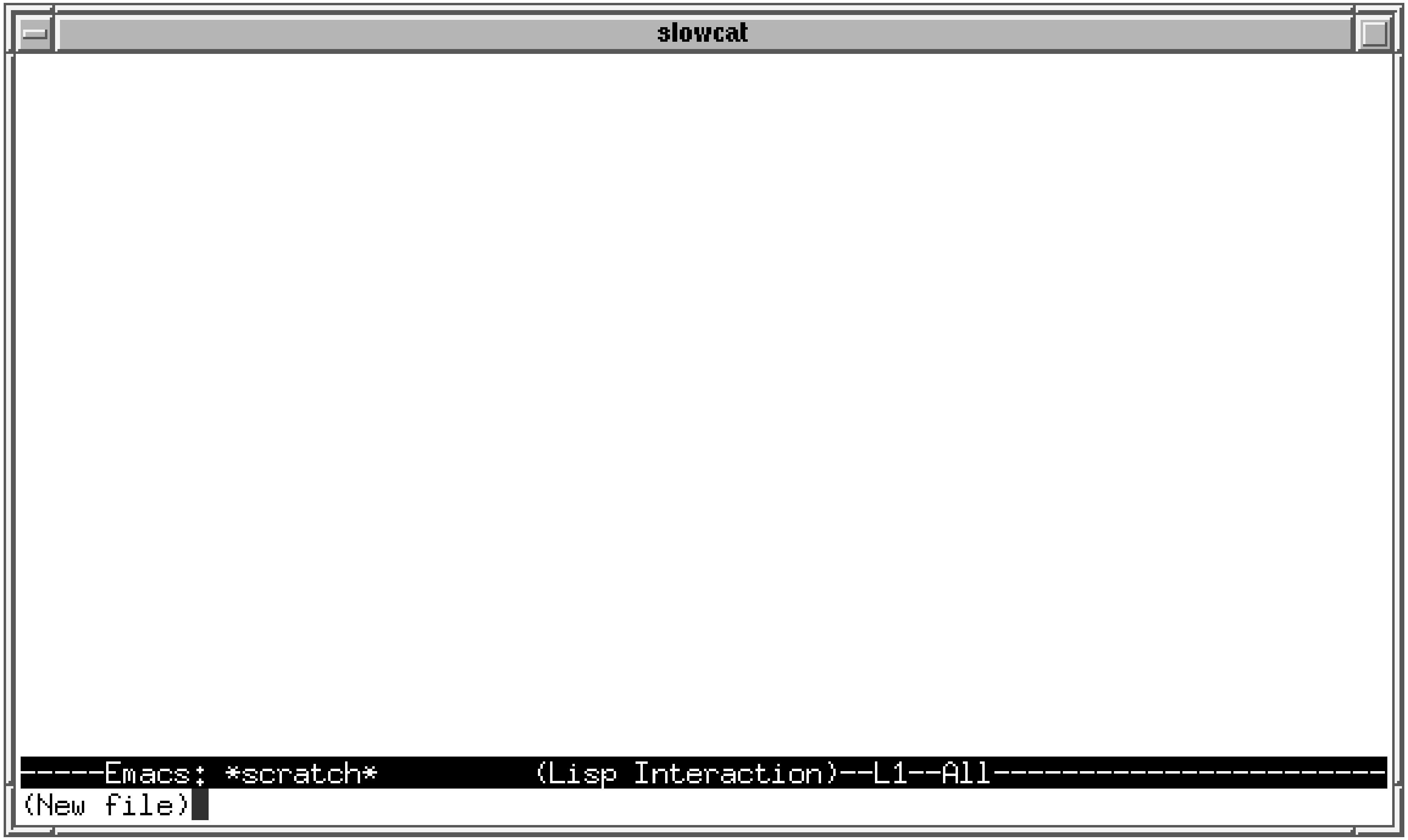
Browsing Telnet - more of what the user “sees”

Replay of a telnet session

- Easier to see what they were doing here
- Output at viewer controlled rate
- Next few slides show successive updates



Replay of telnet session



Replay of telnet session, continued

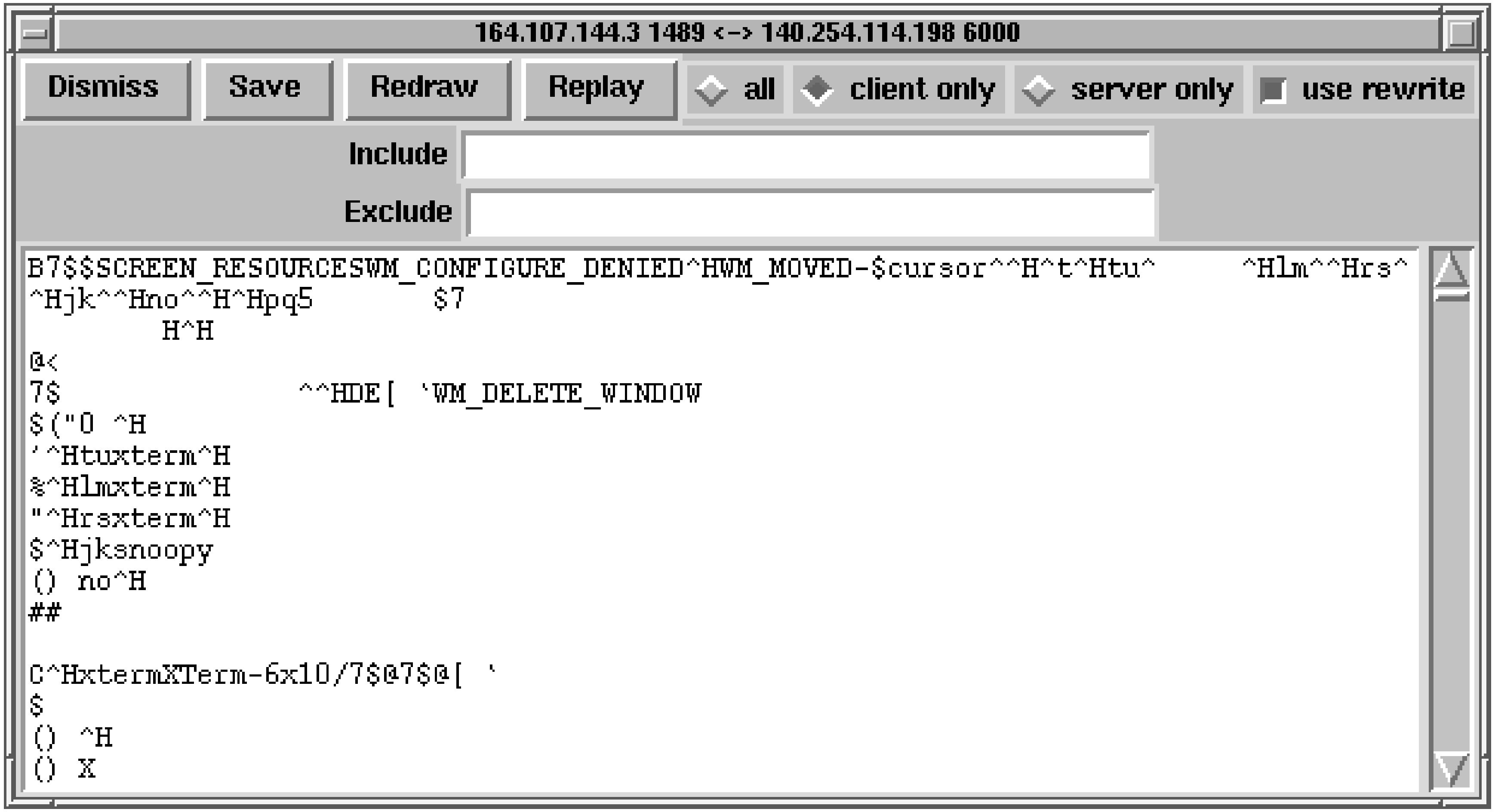
Replay of telnet session, continued

```
slowcat
wuc      ttypc   Apr 13 16:45   (ihgw1.lucent.com)
v-nguyen ttypd   Apr 20 13:09   (algw2.lucent.com)
gcao     ttype   Apr 13 14:37   (lilac:0.0)
moeller  ttypf   Apr 20 17:16   (shoes.cis.ohio-s)
romig    ttyq0   Apr 20 17:41   (ts35-15.homenet.)
saday    ttyq1   Apr  7 18:19   (chicago.cis.ohio)
msun     ttyq2   Apr 18 17:22   (kepler.enc.org:0)
jianping ttyq3   Apr  9 09:29   (death.cis.ohio-s)
zhangj   ttyq5   Apr 16 16:21   (golf.cis.ohio-st)
susskind ttyq6   Apr 10 09:28   (majel.net.ohio-s)
jiyer    ttyq7   Apr 10 11:43   (ocelot.netlab.oh)
goyal    ttyq8   Apr 10 12:14   (puma.netlab.ohio)
basak    ttyq9   Apr 14 10:37   (169.144.18.20)
dliang   ttyqb   Apr 15 10:43   (zion.cis.ohio-st)
dliang   ttyqc   Apr 15 11:11   (zion:0.0)
shih     ttyqf   Apr 18 12:31   (peacock.cis.ohio)
snoopy ~> who | less
snoopy ~> ps -axu | less
snoopy ~> netstat | less
snoopy ~> who | fgrep stego
snoopy ~> mail
No mail for romig
snoopy ~> logout
```

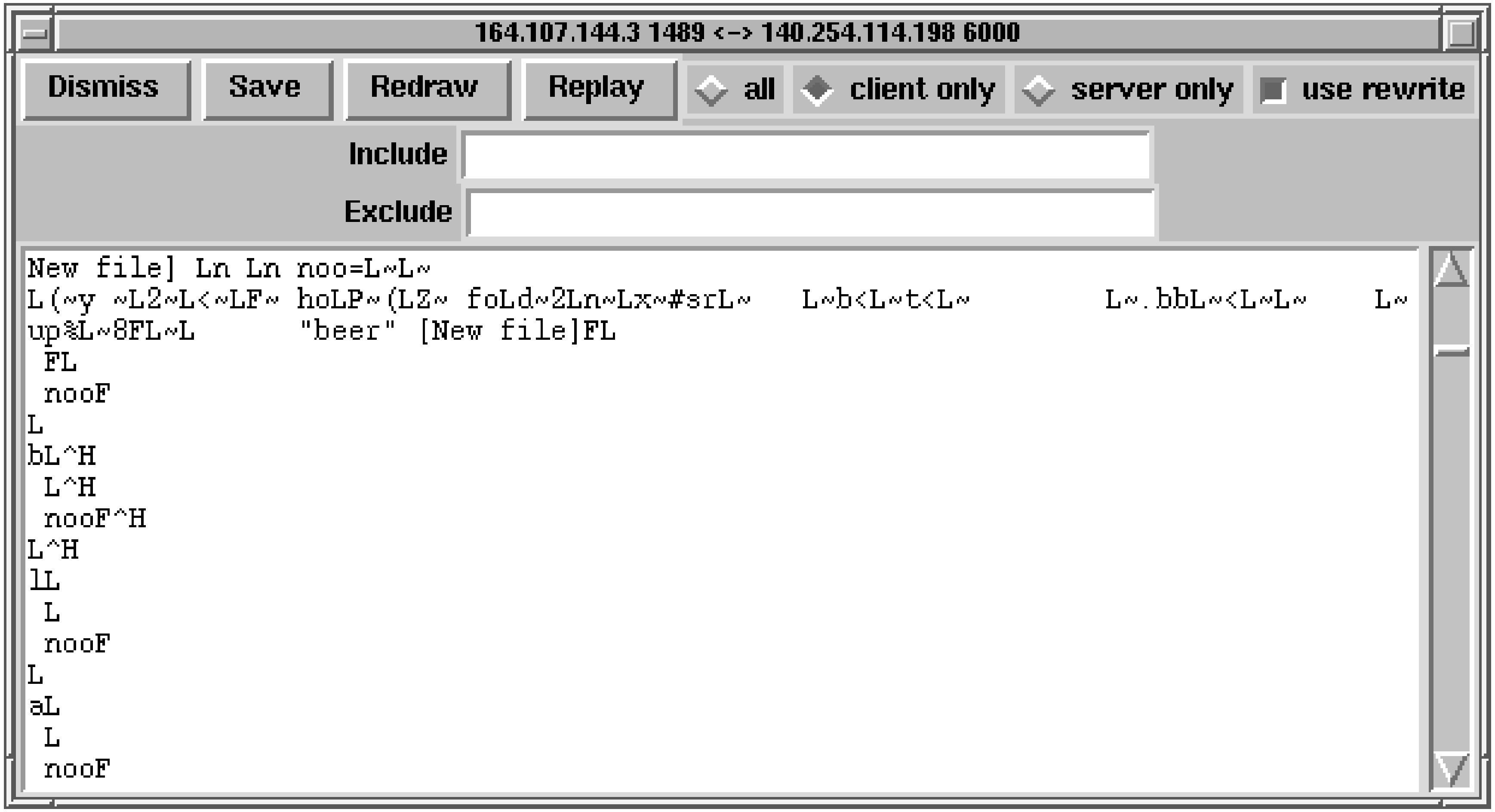
Replay of telnet session, continued

Browsing an X session

- Server side (next 2 slides)
- Key press and other events, replies, errors
- What the user typed



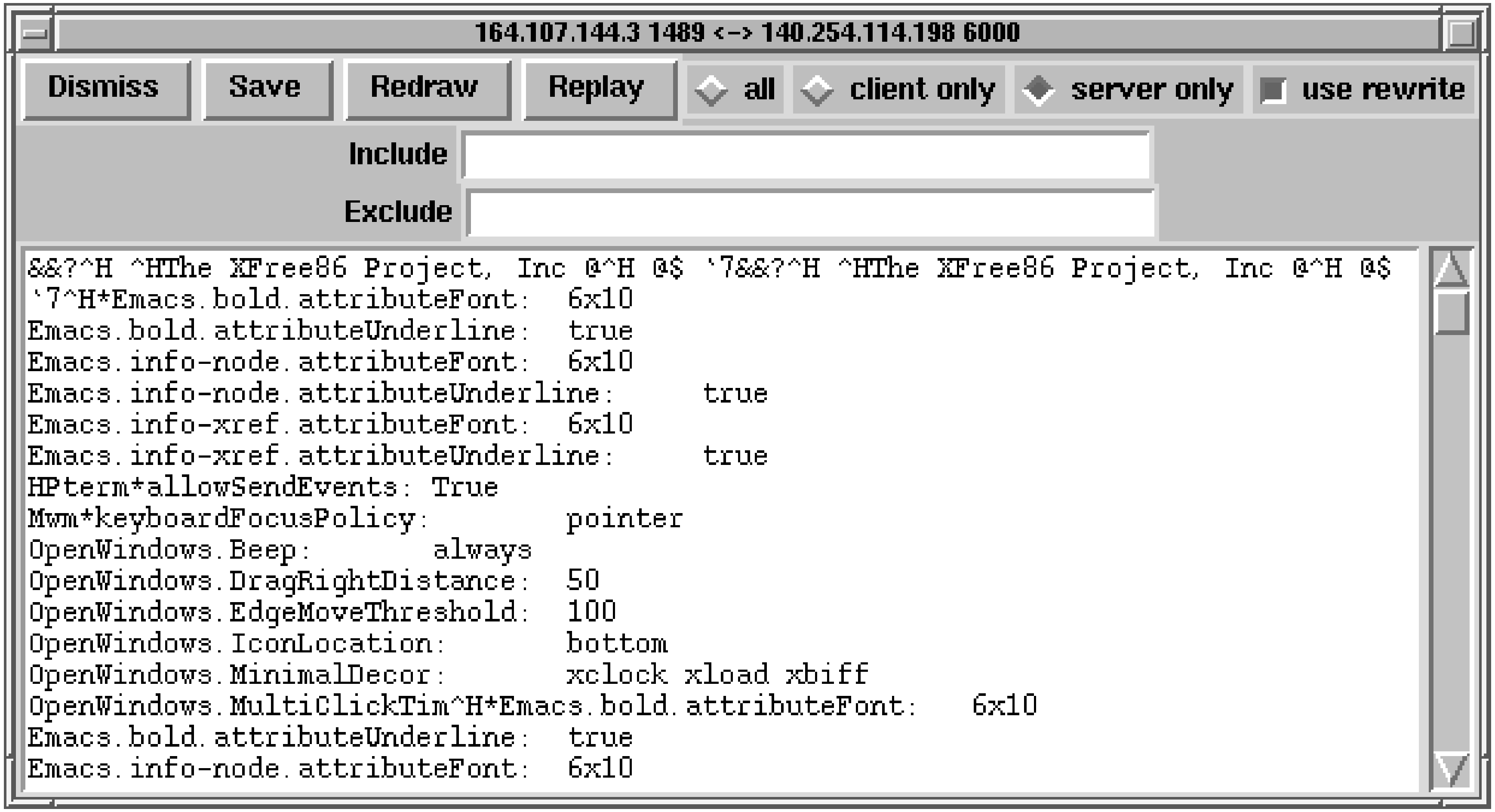
X session, server traffic (key strokes, etc)



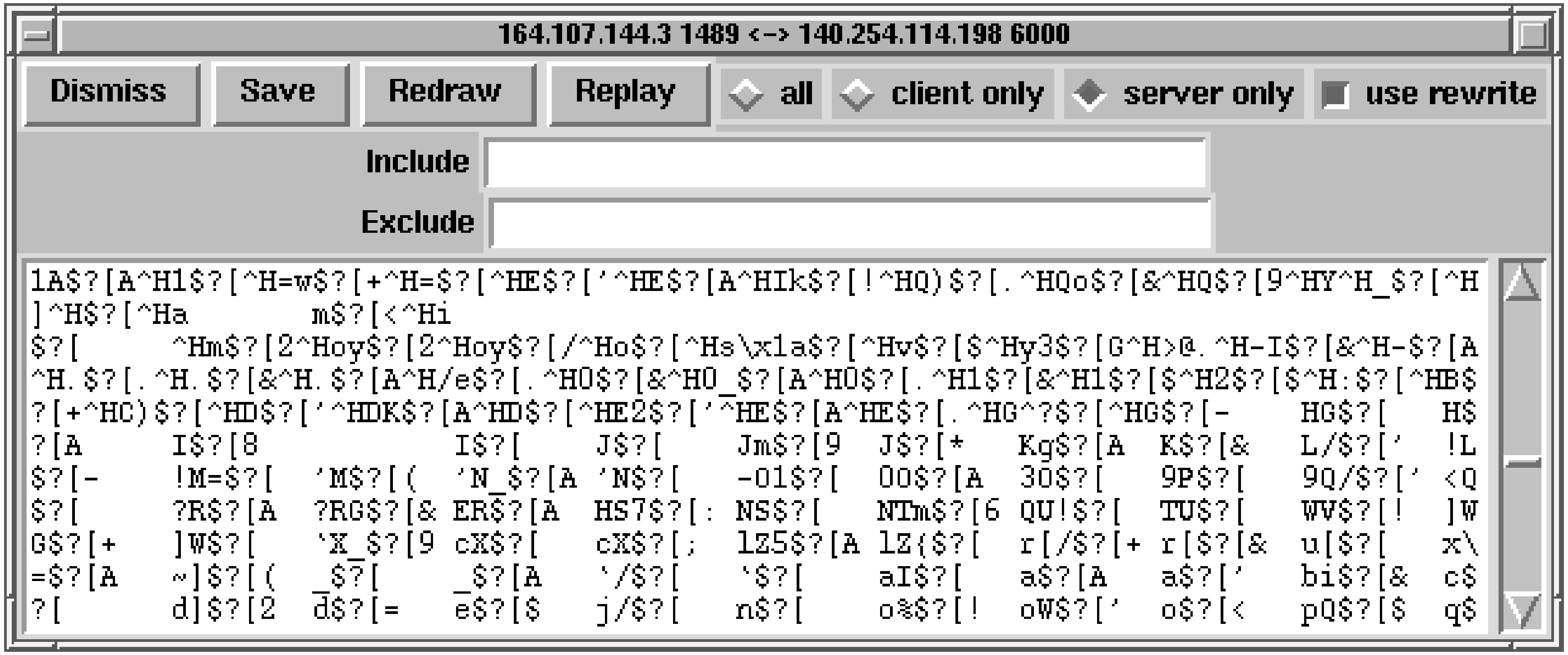
X session, server traffic, continued

Browsing an X session

- Client side traffic now (next 2 slides)
- Requests sent to the server
- “What the user sees”
- What is the user seeing now?



X session, client traffic, what the user “sees”

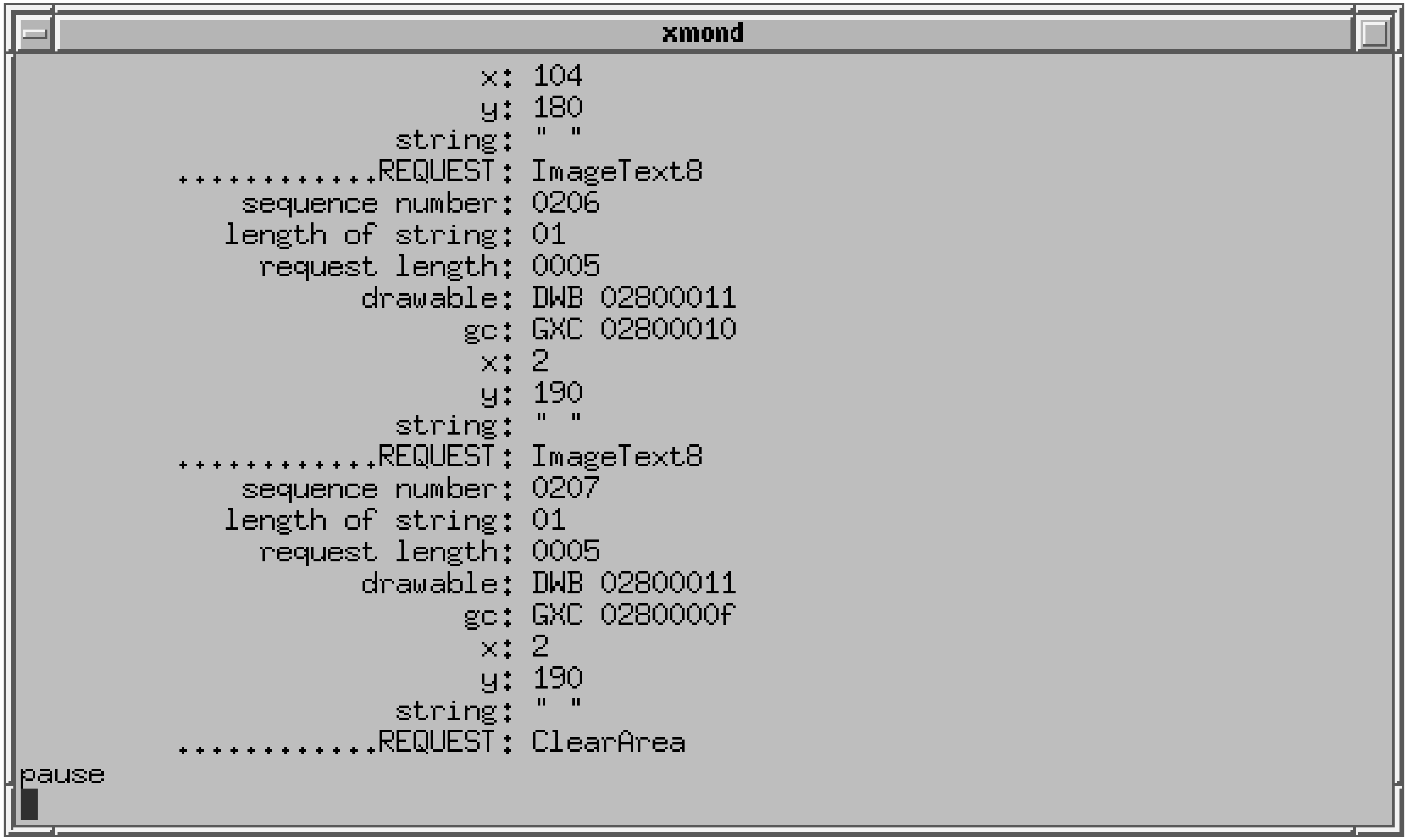


X session, client traffic continued

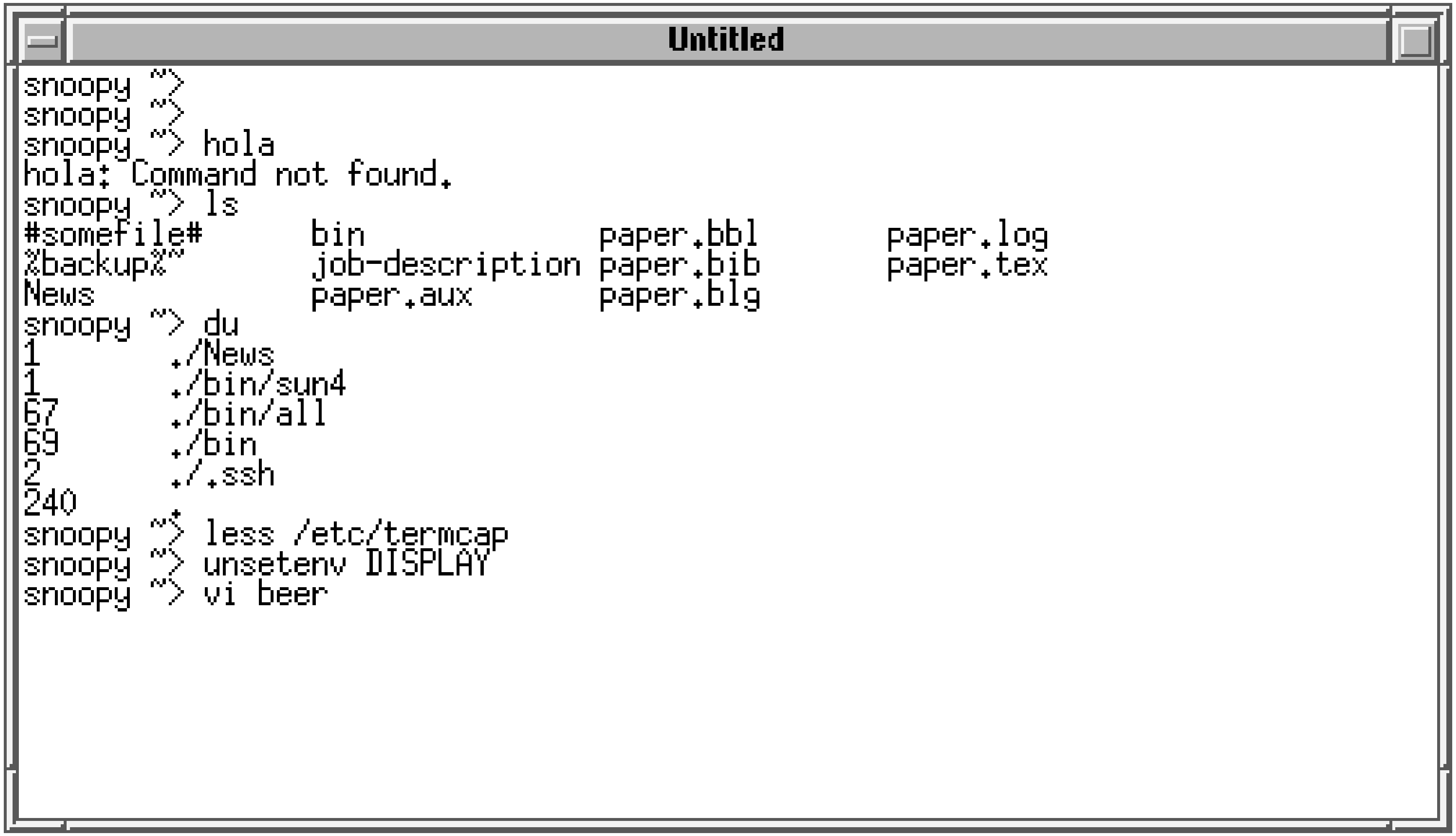
Replay of an X session

- More obvious now: the user was running vi

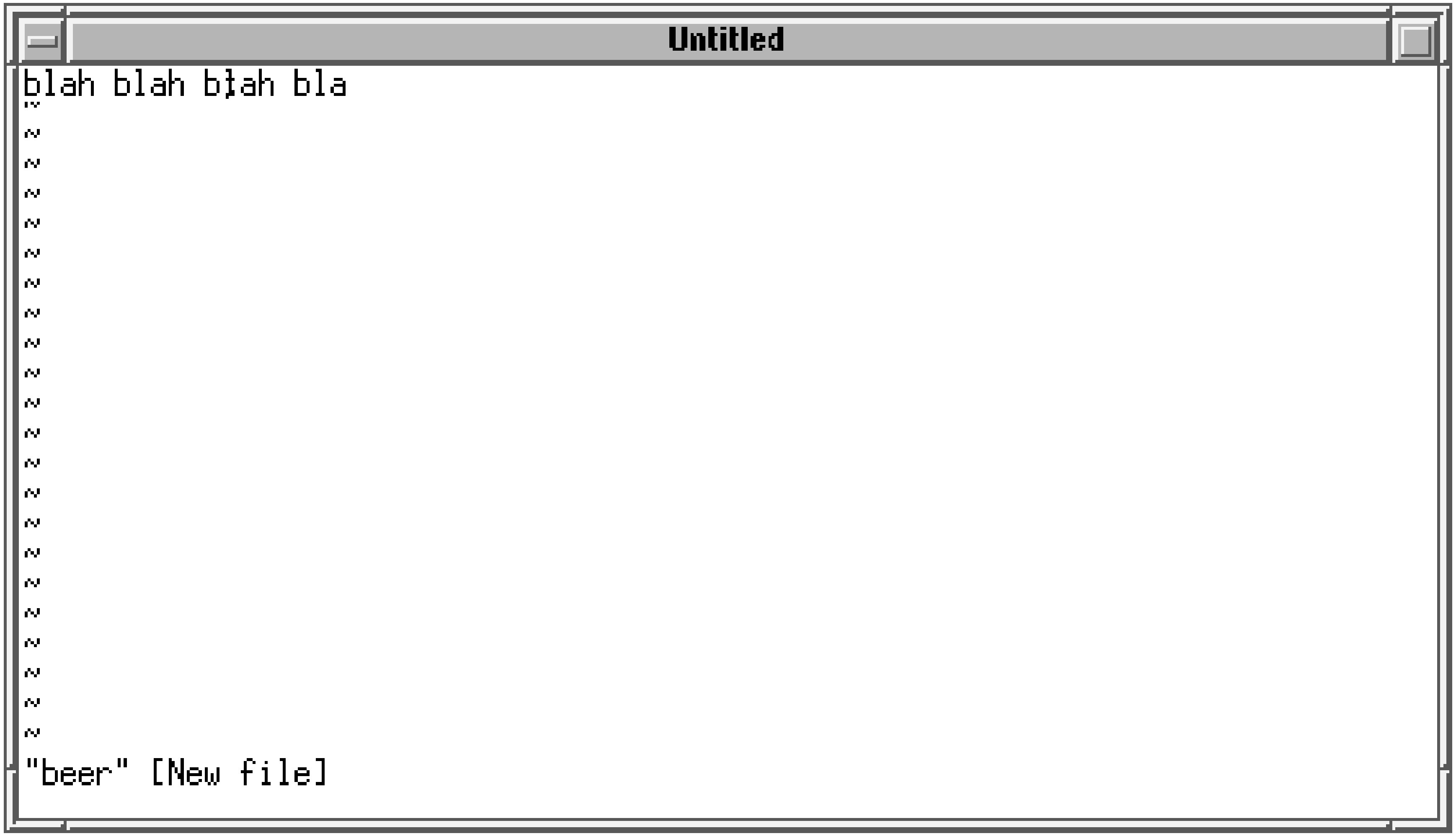
- Works for simple cases



Replay of an X session - the xmond debugging window



Replay of an X session - the xmond replay window



Replay of an X session, continued

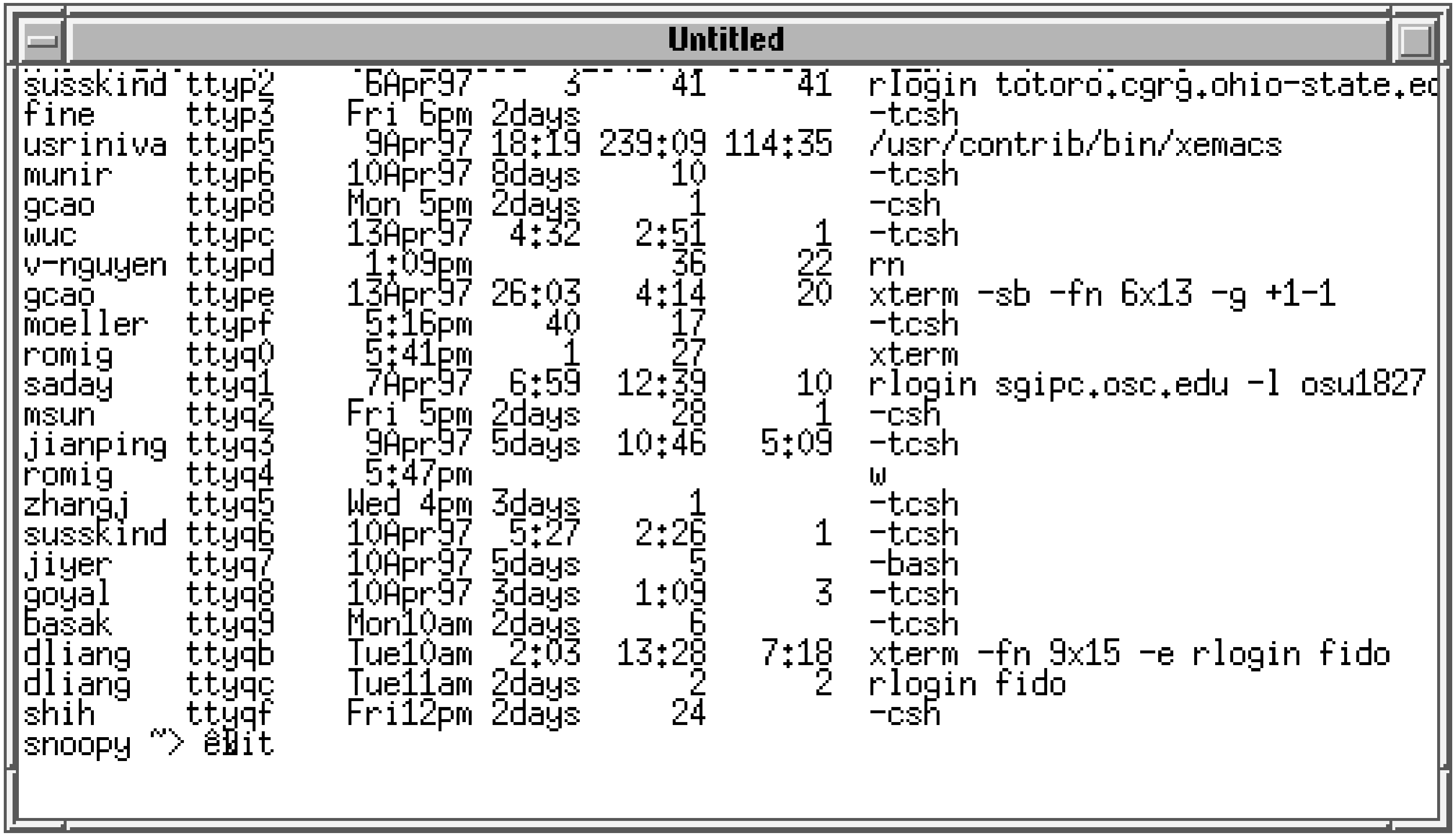
```
Untitled
blah blah blah blah blah

all that stuff about mares and oats isn't true, is it?

i mean, its rather like the old bit about woodchucks eating wood.

they
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"beer" [New file]
```

Replay of an X session, continued



Replay of an X session, continued

Future plans

- Asynchronous I/O
- Report generation
- Searching
- Integrate with other tools
- Extend X replay tools

Future plans - X Replay Improvements

- Handle more of the safe requests
- Track CreateGC and CreateWindow requests
- Map these to requests with identical features
- Then use our local GCs and Windows in future replayed requests
- Should provide more realistic replays

Legal and ethical considerations

- Consult your lawyer
- In U.S., Electronic Communications Privacy Act applies
- Policy governing when we will log contents
- Steps to reduce “friendly fire”

Availability

- Available on request
- Send email to security@net.ohio-state.edu
- Requires UNIX, perl 5.003, perl/tk module, X11R6

Review - a Tool for Reviewing Tcpdump Logs

Steve Romig

romig@net.ohio-state.edu
1-614-688-3412
UTS Network Security Group
The Ohio State University
Columbus, Ohio 43210