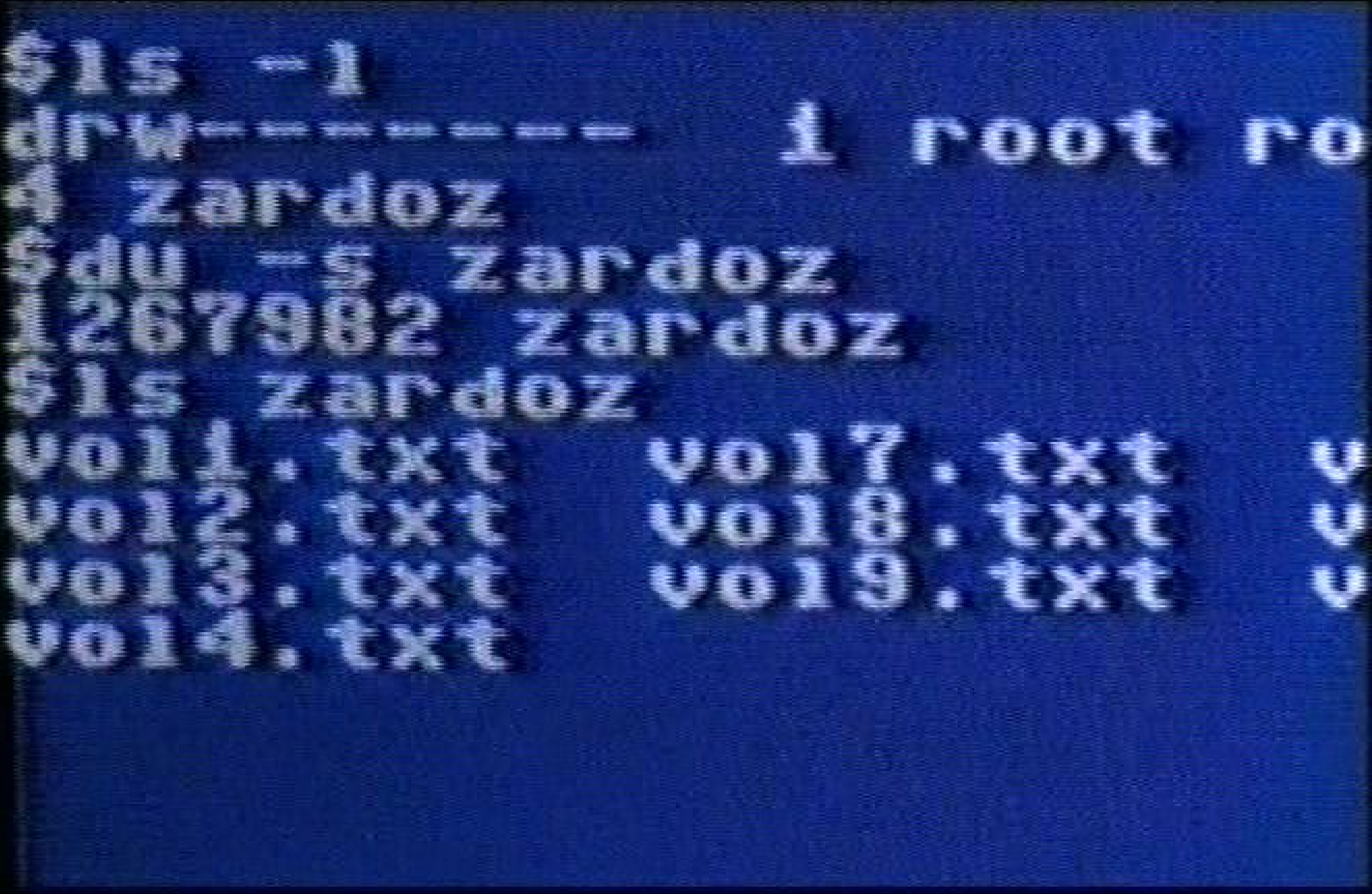
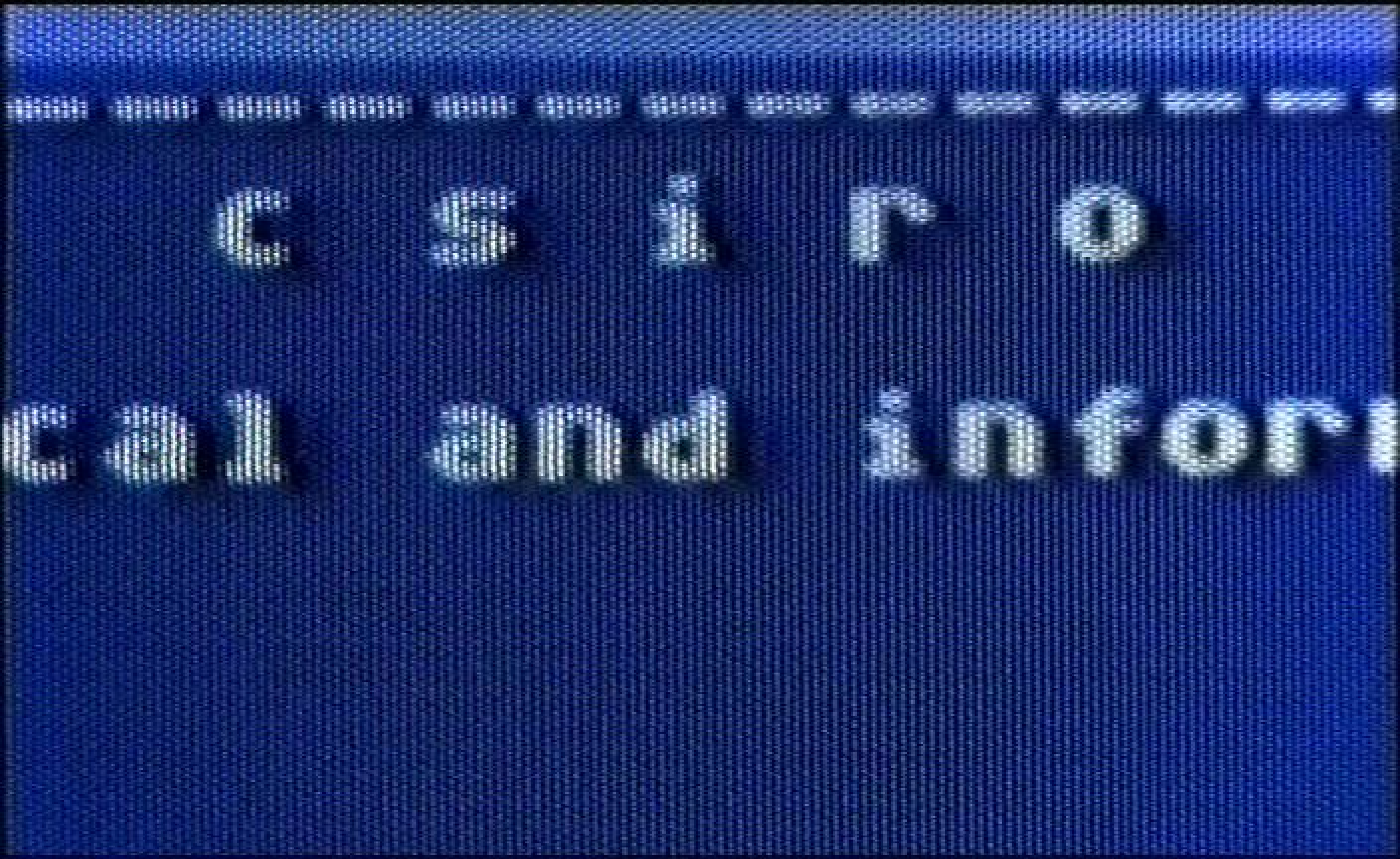
zardoz

? ? ?
HAVE
YO
EVE
HEARD
A PYGMY



```
$ls -l
drw--------    1 root ro
4 zardoz
$du -s zardoz
1267982 zardoz
$ls zardoz
vol1.txt   vol7.txt   v
vol2.txt   vol8.txt   v
vol3.txt   vol9.txt   v
vol4.txt
```

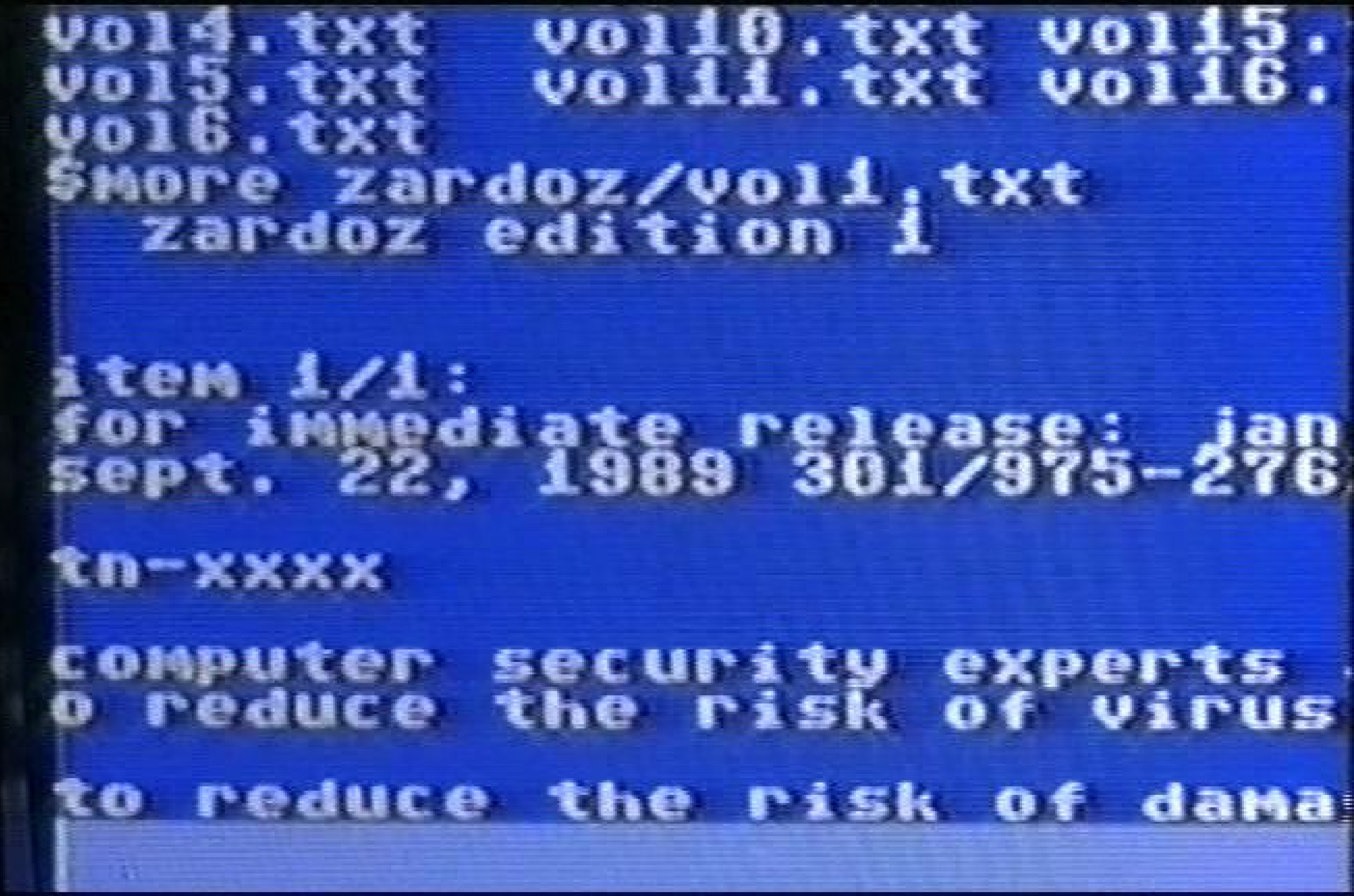
2 am



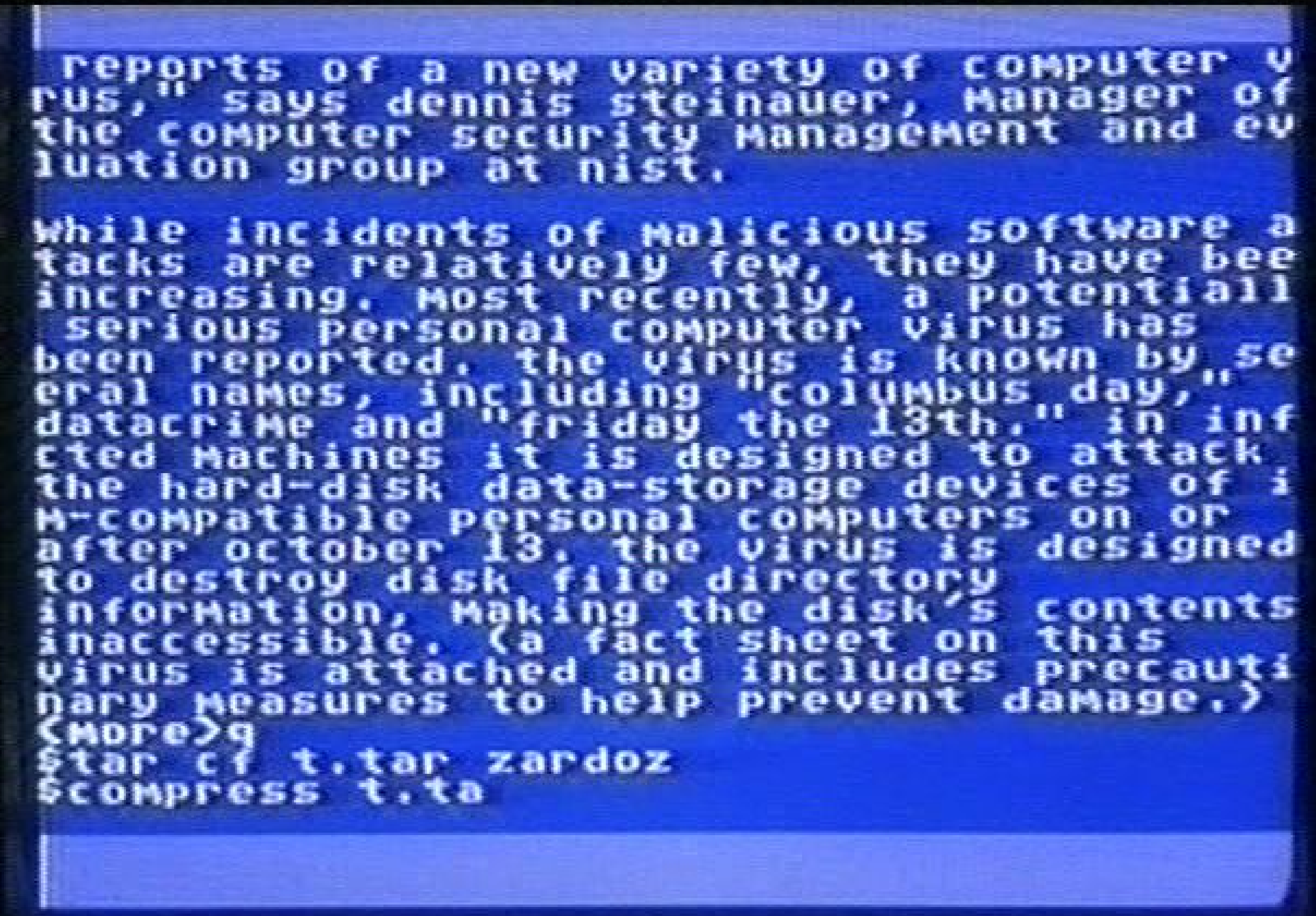
csiro

cal and infor

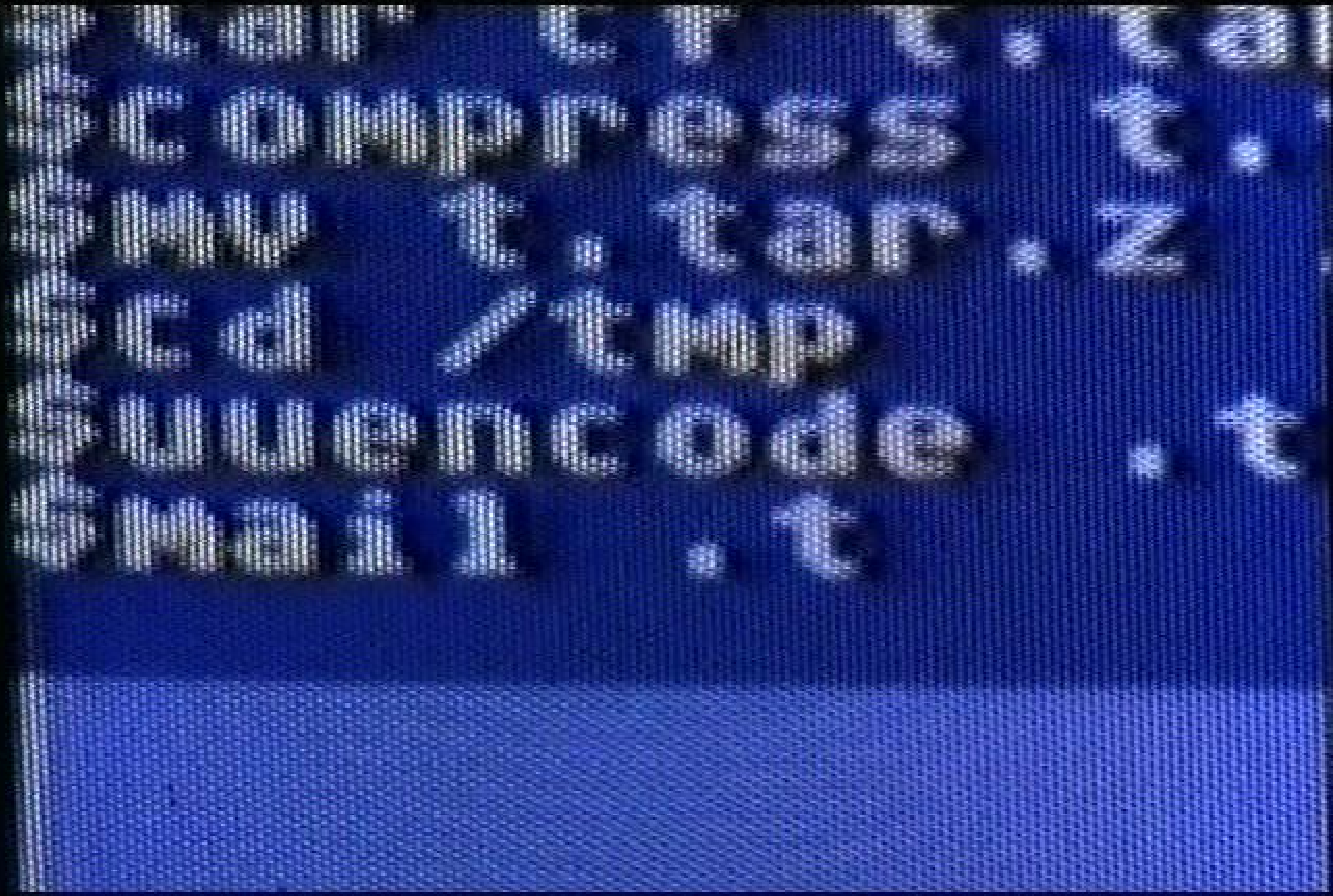
```
[illegible]
Unauthorised access not permitted.
[illegible]
[illegible]   1 root root  512 Jan 27 13:
[illegible]
```



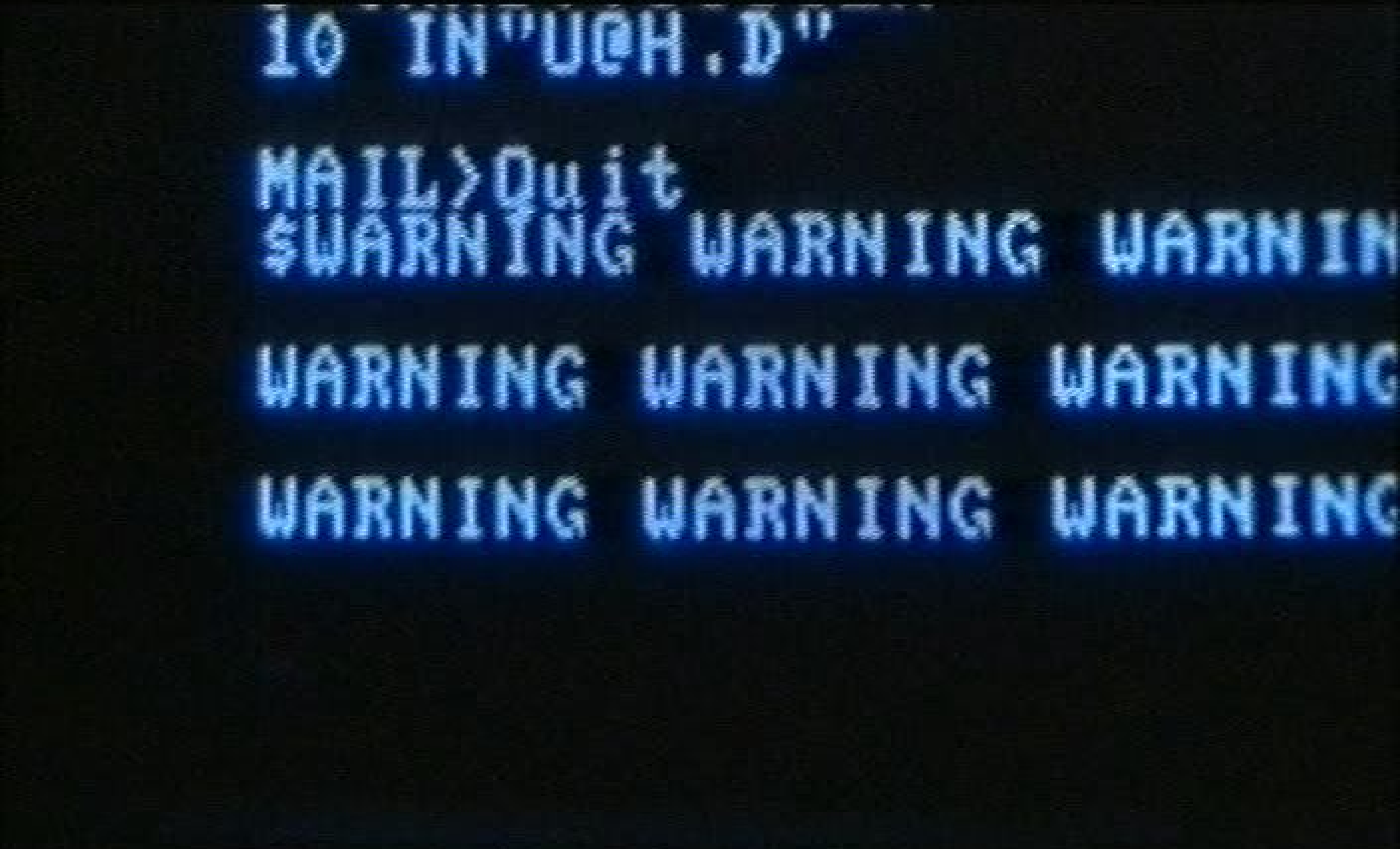
```
vol4.txt  vol10.txt vol15.
vol5.txt  vol11.txt vol16.
vol6.txt
$more zardoz/vol1.txt
  zardoz edition 1


item 1/1:
for immediate release: jan
sept. 22, 1989 301/975-276

tn-xxxx

computer security experts
o reduce the risk of virus

to reduce the risk of dama
```



```
 reports of a new variety of computer v
rus," says dennis steinauer, manager of
the computer security management and ev
luation group at nist.

while incidents of malicious software a
tacks are relatively few, they have bee
increasing. most recently, a potentiall
 serious personal computer virus has
been reported. the virus is known by se
eral names, including "columbus day,"
datacrime and "friday the 13th." in inf
cted machines it is designed to attack
the hard-disk data-storage devices of i
m-compatible personal computers on or
after october 13. the virus is designed
to destroy disk file directory
information, making the disk's contents
inaccessible. (a fact sheet on this
virus is attached and includes precauti
nary measures to help prevent damage.)
(more)q
$tar cf t.tar zardoz
$compress t.ta
```

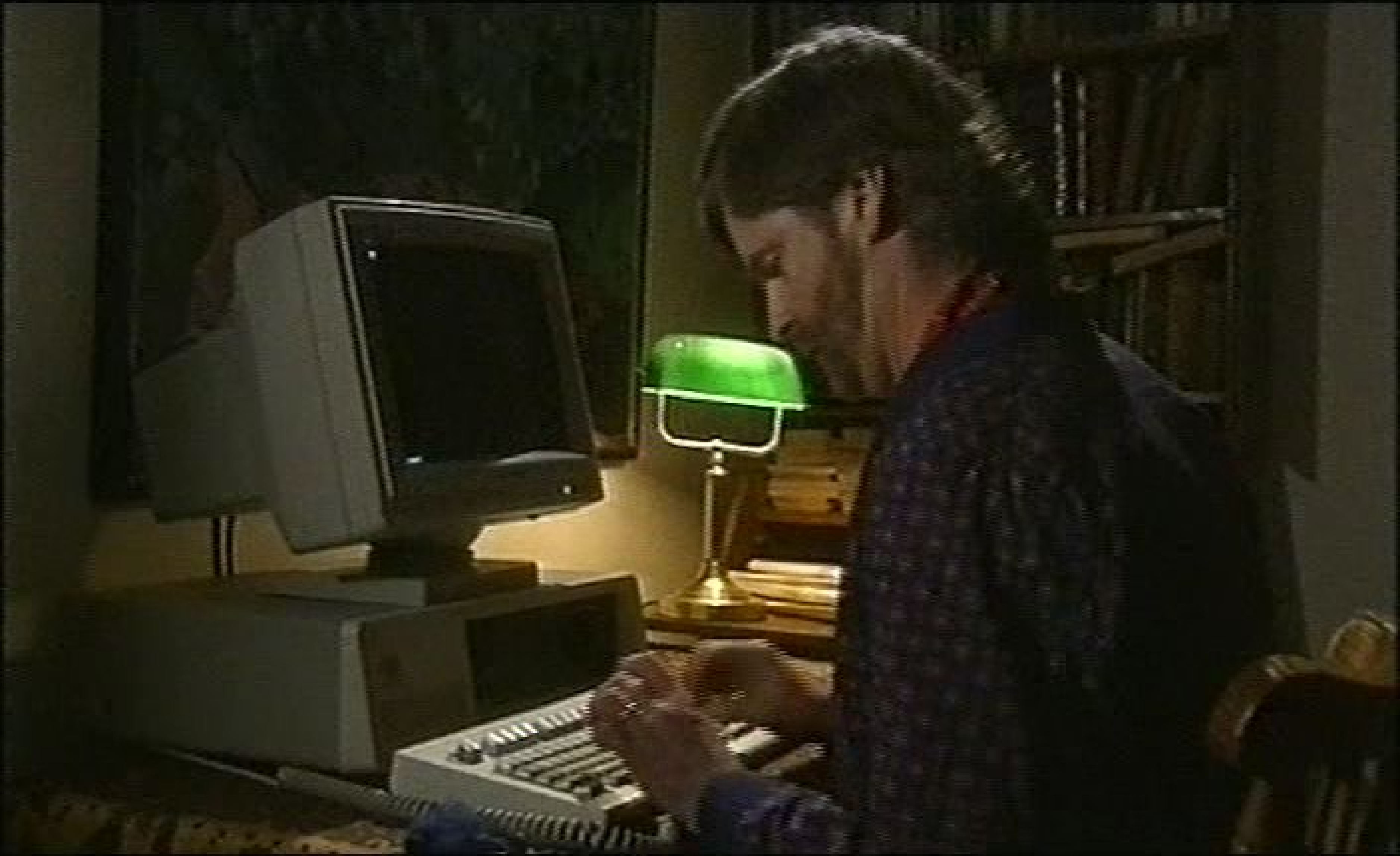


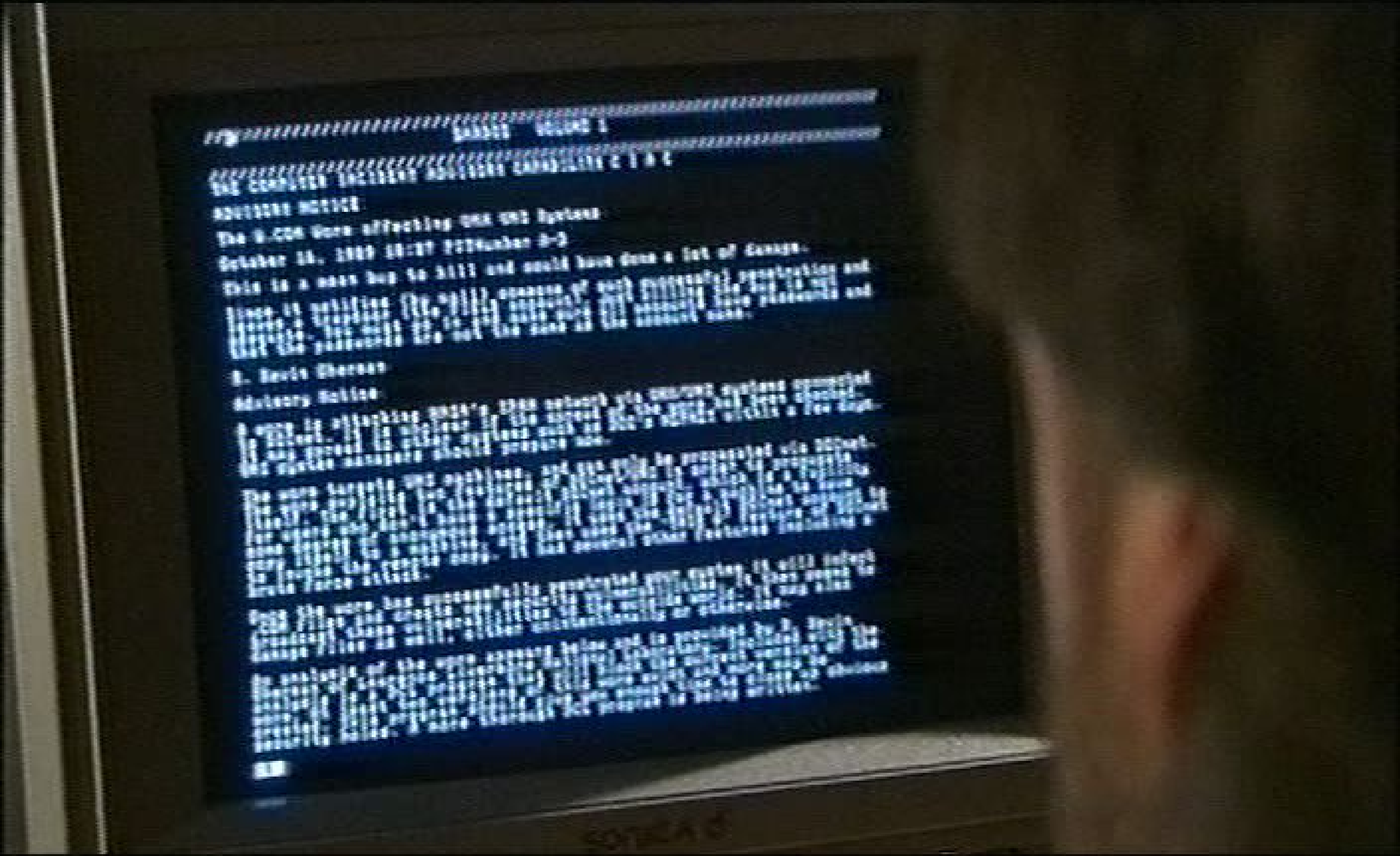
```
$tar cf t.tar
$compress t.t
$mv t.tar.Z
$cd /tmp
$uuencode .t
$mail .t
```



```
10 IN"U@H.D"

MAIL>Quit
$WARNING WARNING WARNIN

WARNING WARNING WARNING

WARNING WARNING WARNING
```

2.25 am





[illegible] VOLUME 1

THE COMPUTER INCIDENT ADVISORY CAPABILITY C I A C

ADVISORY NOTICE

The W.COM Worm affecting VAX VMS Systems

October 16, 1989 18:37 PSTNumber A-2

This is a mean bug to kill and could have done a lot of damage.

[illegible]

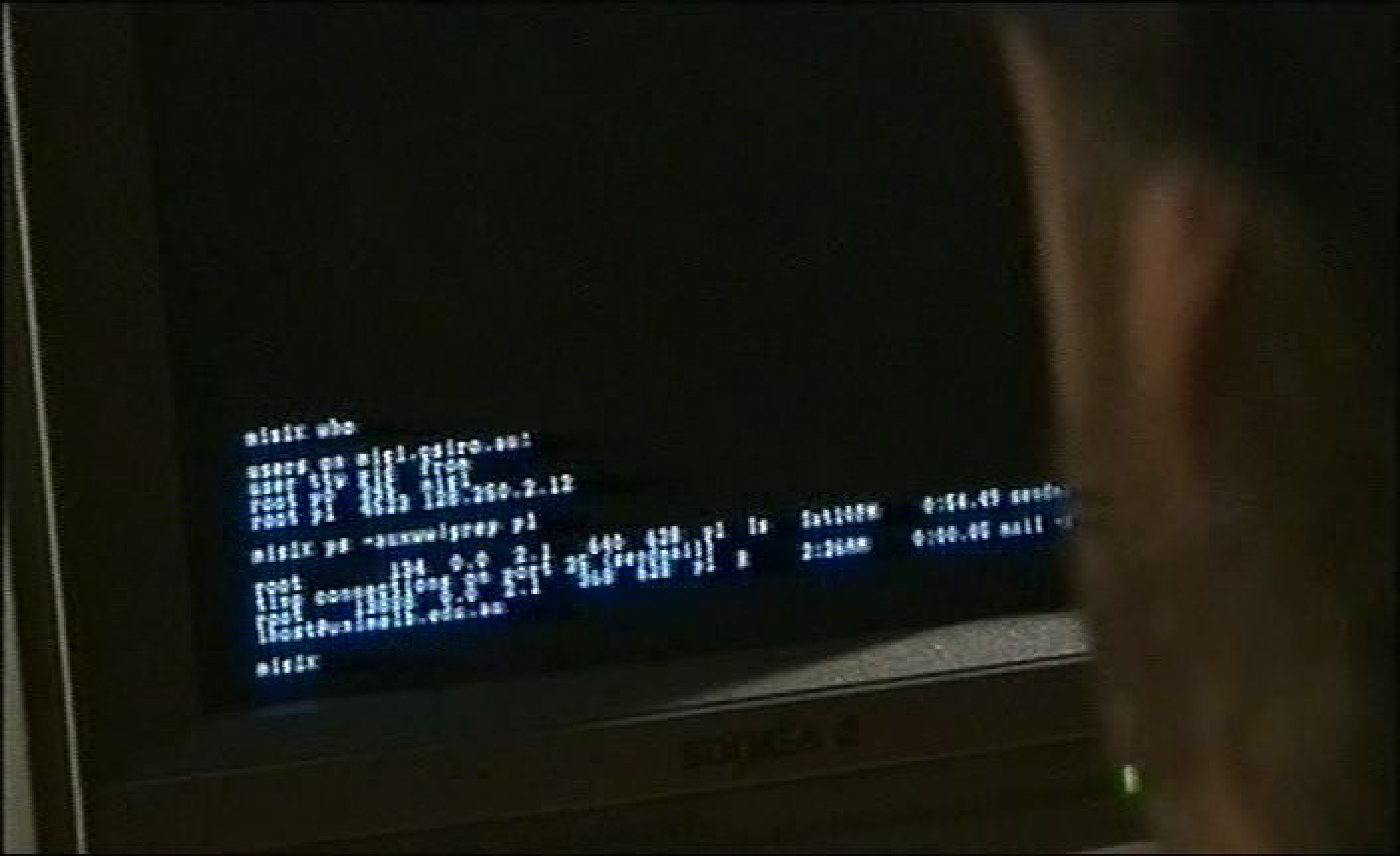
R. Kevin Oberman

Advisory Notice

A worm is attacking NASA's SPAN network via VAX/VMS systems connected [illegible]

[illegible]

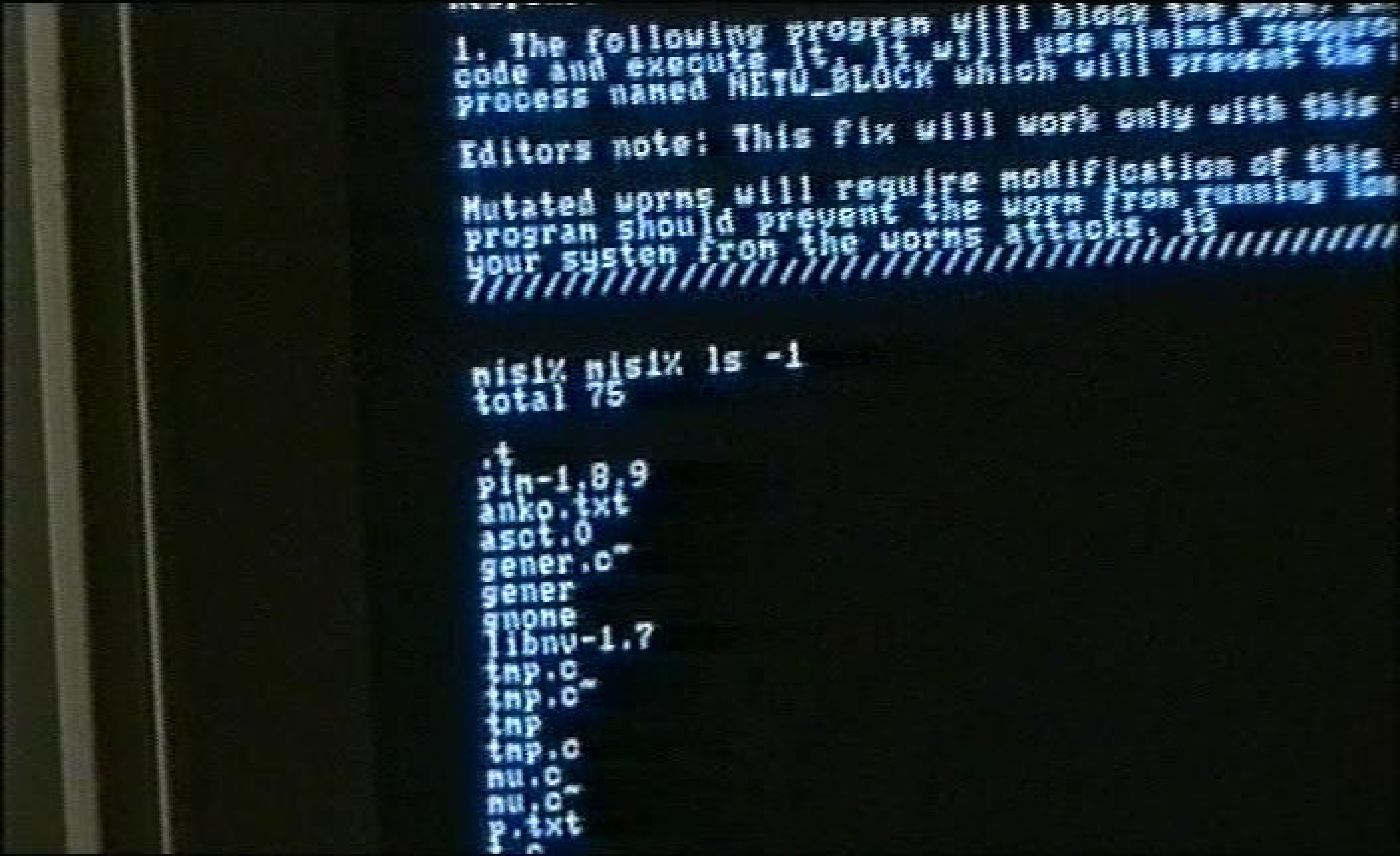
```
/////////////////////////
    ZARDOZ   VOLUME 1
/////////////////////////
ADVISORY CAPABILITY C I
```



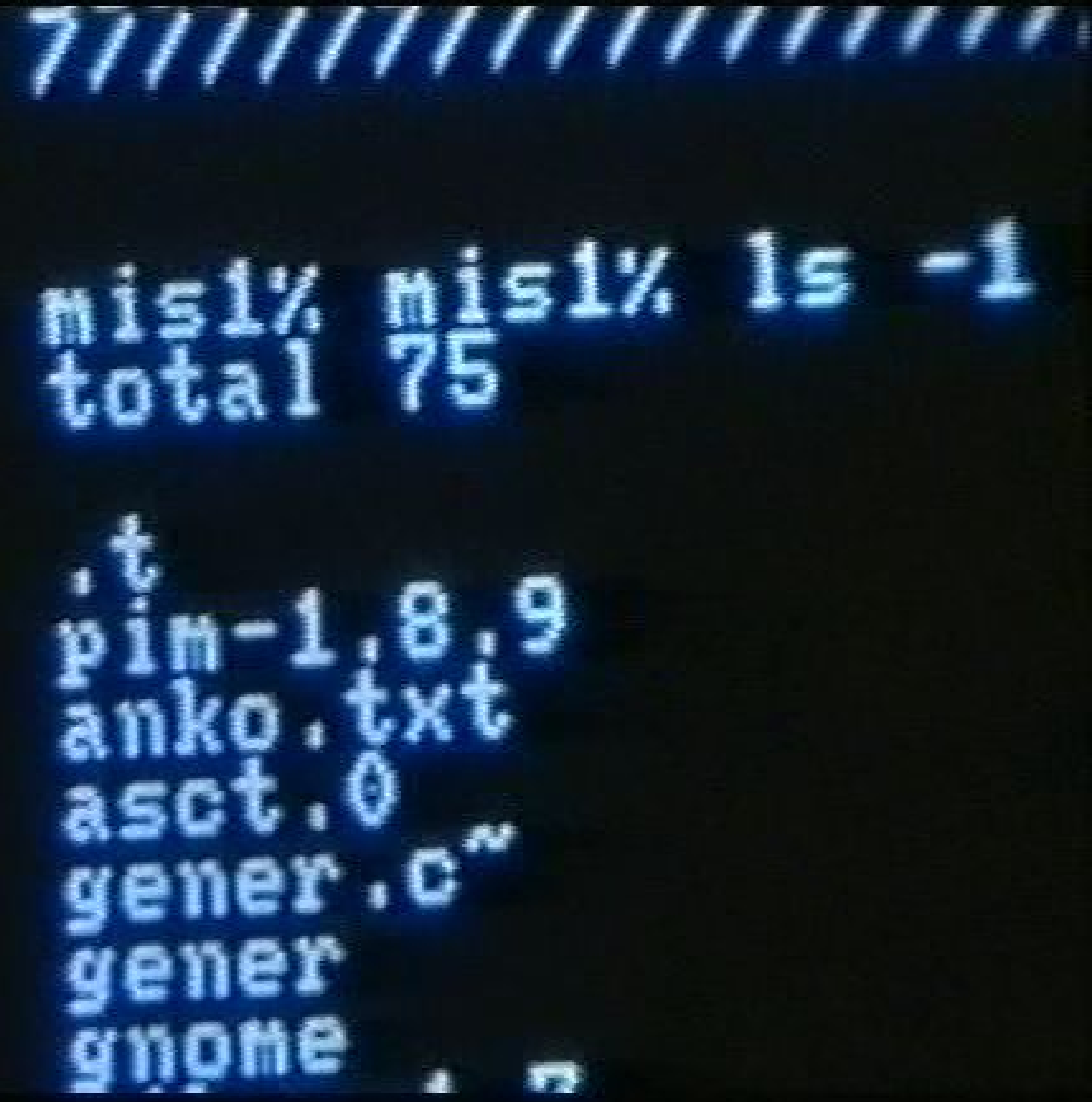
```
misix who
users on misi-cairo.eu:
user tty [illegible]  from
root p? [illegible]
root p1 [illegible] 128.260.2.12
misix ps -auxwwl|grep p1
root      134  0.0  2.1  [illegible]  640  620 p1 Is   5:11PM   0:54.45 send[illegible]
[illegible] console [illegible]                        2:26AM   0:00.05 mail -[illegible]
root [illegible]
[illegible]host@[illegible]mails.edu.eu
misix
```

ux kill -9

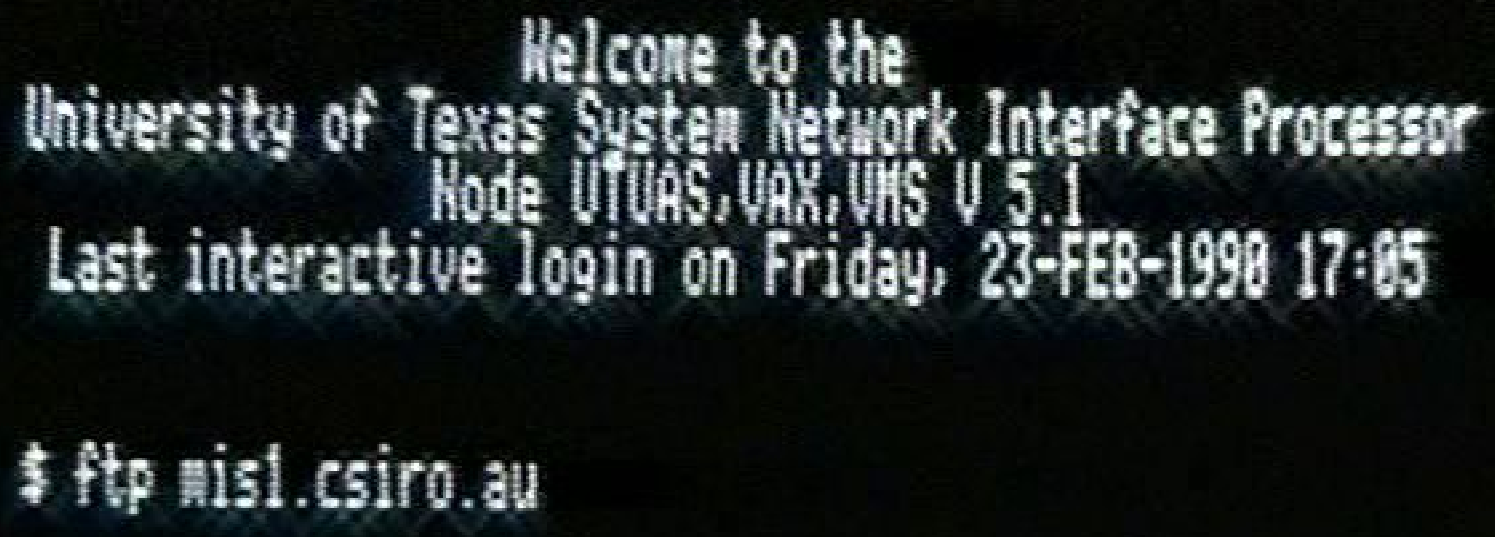
YO'
EVI
HEA
APYCH



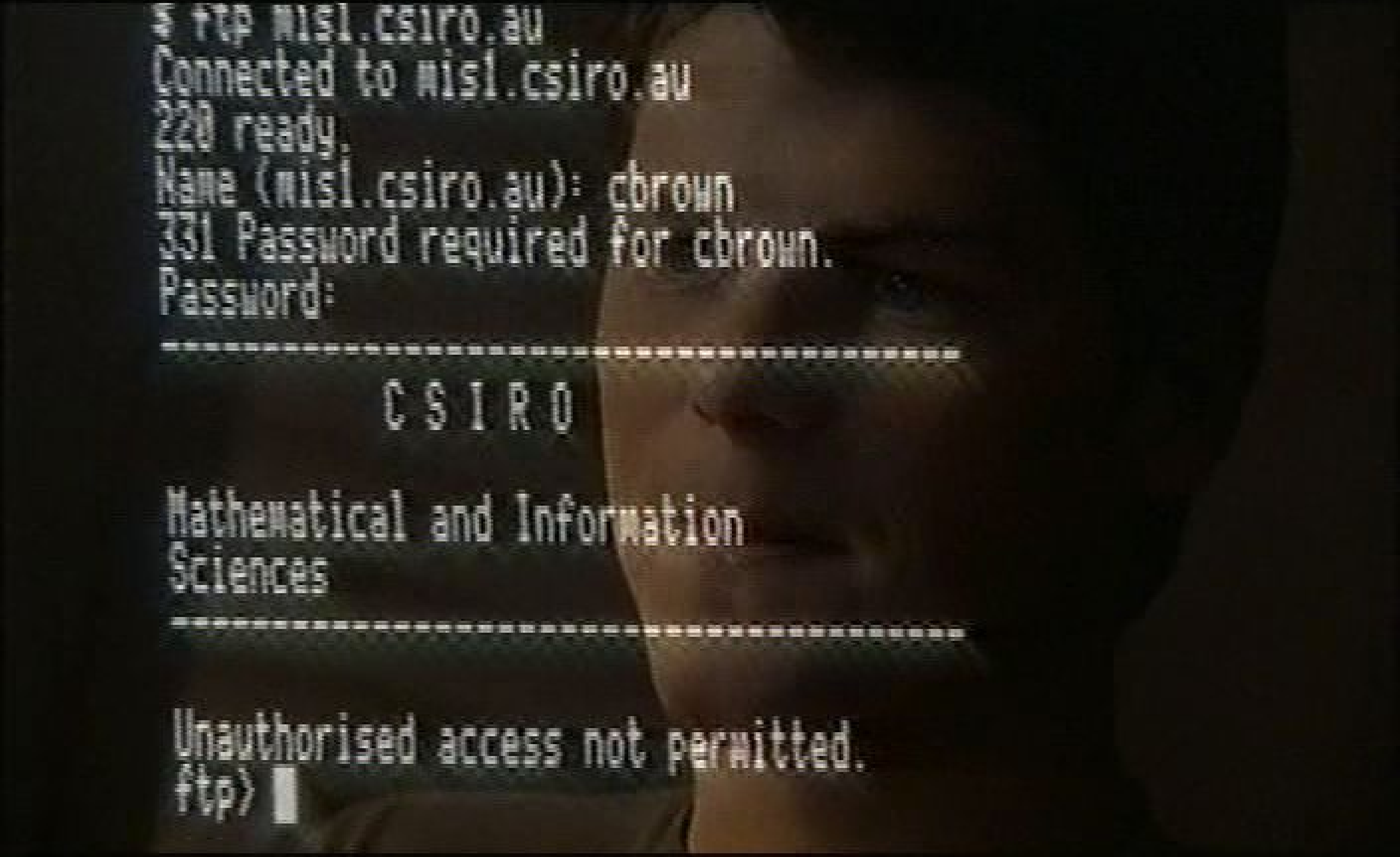
```
1. The following program will block the worm
code and execute it. It will use minimal resourc
process named NETU_BLOCK which will prevent the

Editors note: This fix will work only with this

Mutated worms will require modification of this
program should prevent the worm from running lo
your system from the worms attacks. 13
///////////////////////////////////////////////////

nisi% nisi% ls -1
total 75

 .t
 pim-1.8.9
 anko.txt
 asct.o
 gener.c~
 gener
 gnome
 libnv-1.7
 tmp.c_
 tmp.c~
 tmp
 tmp.c
 mu.c_
 mu.c~
 p.txt
```



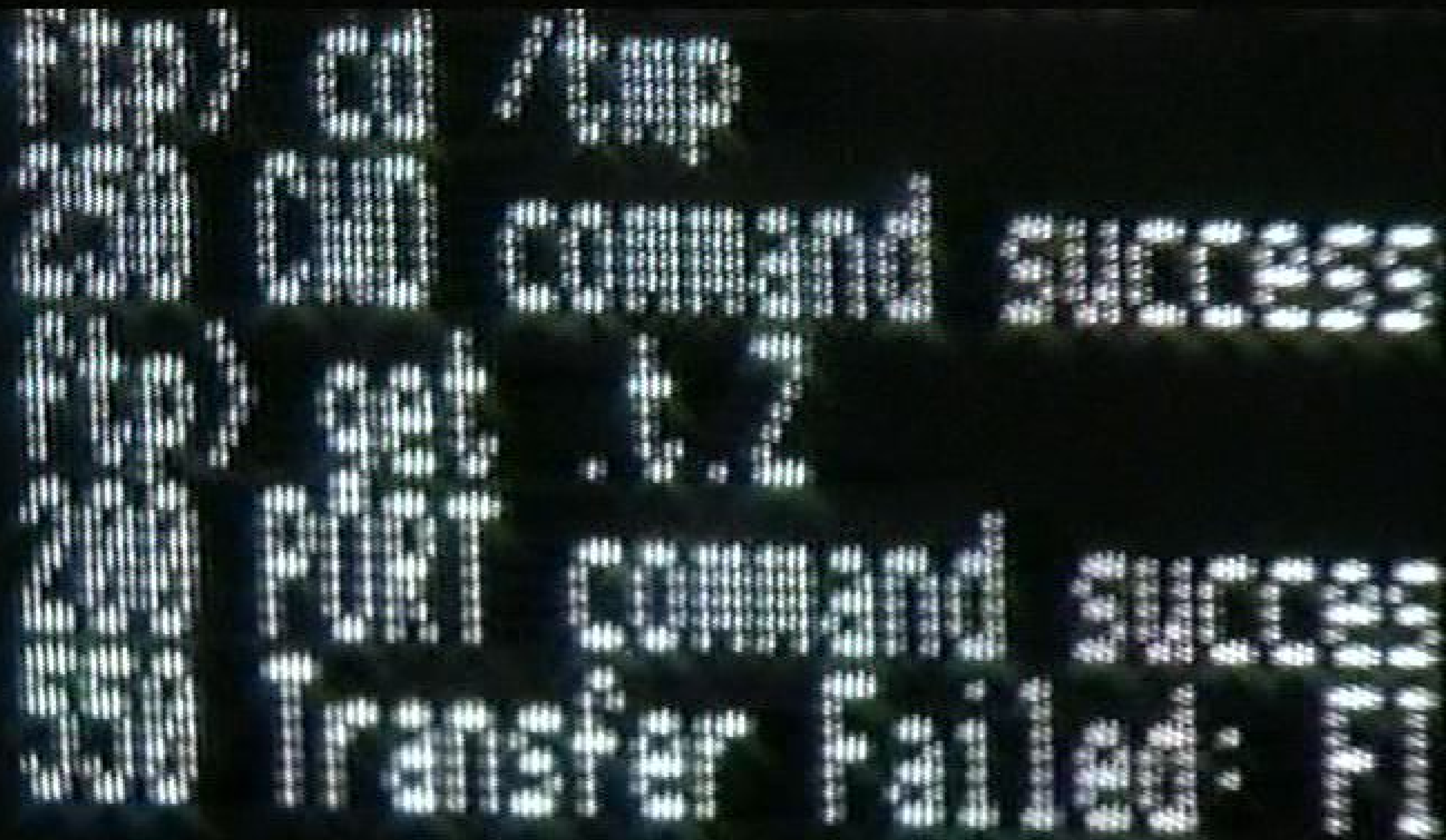
```
7//////////////////


mis1% mis1% ls -1
total 75

 .t
pim-1.8.9
anko.txt
asct.0
gener.c~
gener
gnome
```



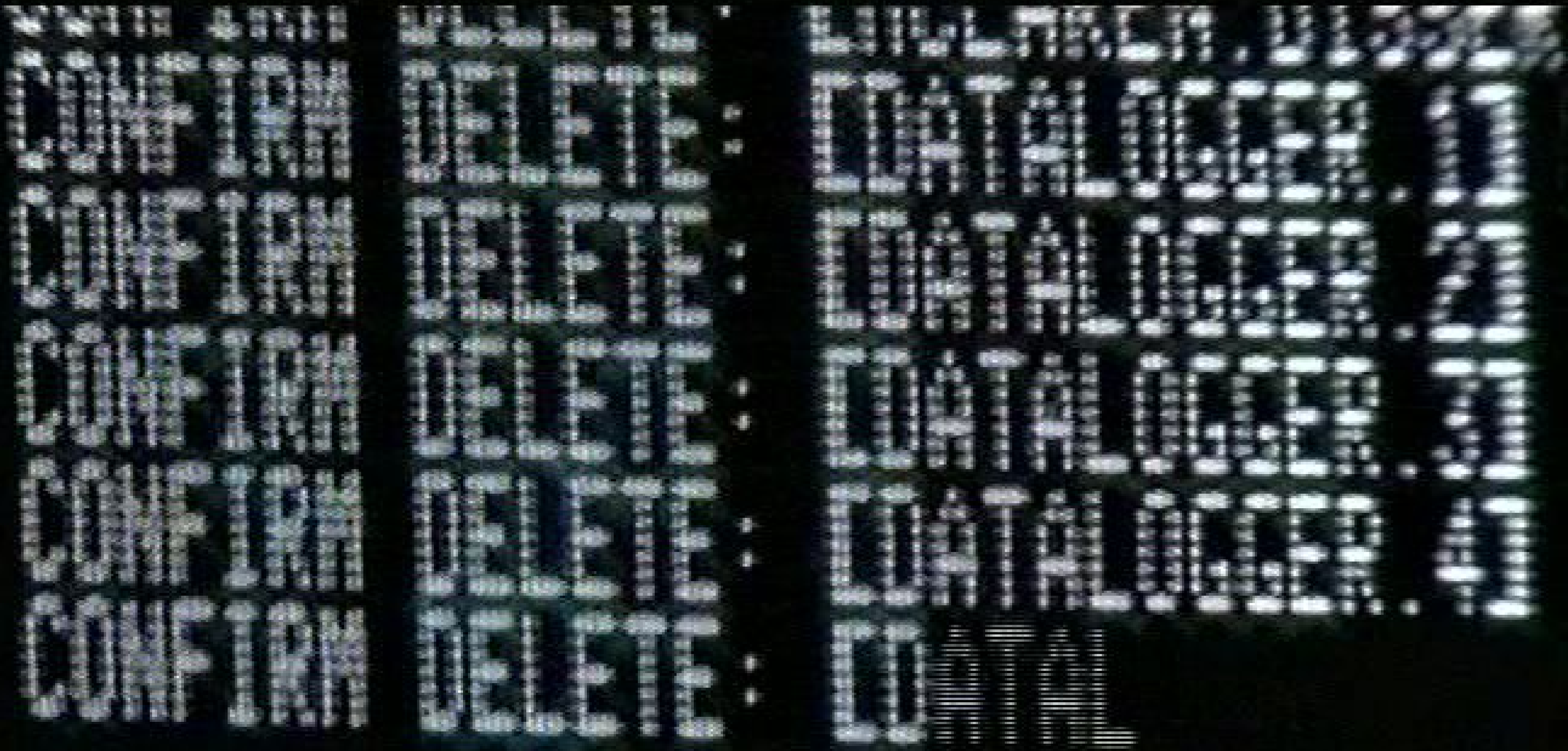
```
                  Welcome to the
University of Texas System Network Interface Processor
              Node UTVAS.VAX.VMS V 5.1
 Last interactive login on Friday, 23-FEB-1990 17:05


$ ftp mis1.csiro.au
```



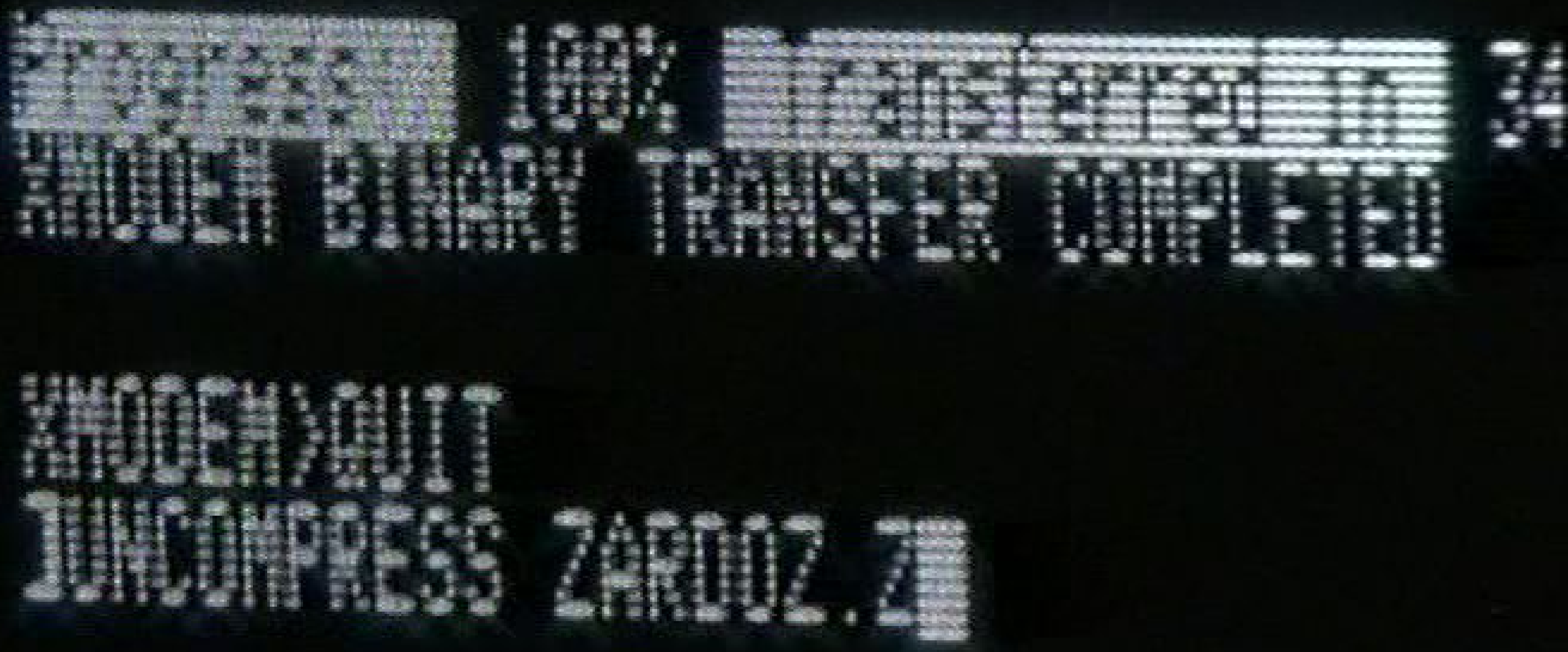
```
$ ftp mis1.csiro.au
Connected to mis1.csiro.au
220 ready.
Name (mis1.csiro.au): cbrown
331 Password required for cbrown.
Password:
-----------------------------------------------
             C S I R O

Mathematical and Information
Sciences
-----------------------------------------------


Unauthorised access not permitted.
ftp> █
```



```
ftp> cd /tmp
250 CWD command succes
ftp> get .t.z
200 PORT command succes
550 Transfer Failed: Fi
```



```
CONFIRM DELETE: [illegible]
CONFIRM DELETE: [DATALOGGER.1]
CONFIRM DELETE: [DATALOGGER.2]
CONFIRM DELETE: [DATALOGGER.3]
CONFIRM DELETE: [DATALOGGER.4]
CONFIRM DELETE: [DATAL
```



```
PROGRESS 100% [illegible] 3
XMODEM BINARY TRANSFER COMPLETED

XMODEM>QUIT
]UNCOMPRESS ZARDOZ.Z█
```

3.44 am