SEIZURE OF EVIDENCE FROM UNIX™ COMPUTER SYSTEMS

(UNIX IS A TRADEMARK OF X/OPEN)

PRESENTED BY JOHN NAVAS
PRINCIPAL, THE NAVAS GROUP℠

SEPTEMBER 16, 1996

(THIS IS NOT LEGAL ADVICE, WHICH CAN ONLY BE PROVIDED BY AN ATTORNEY.)

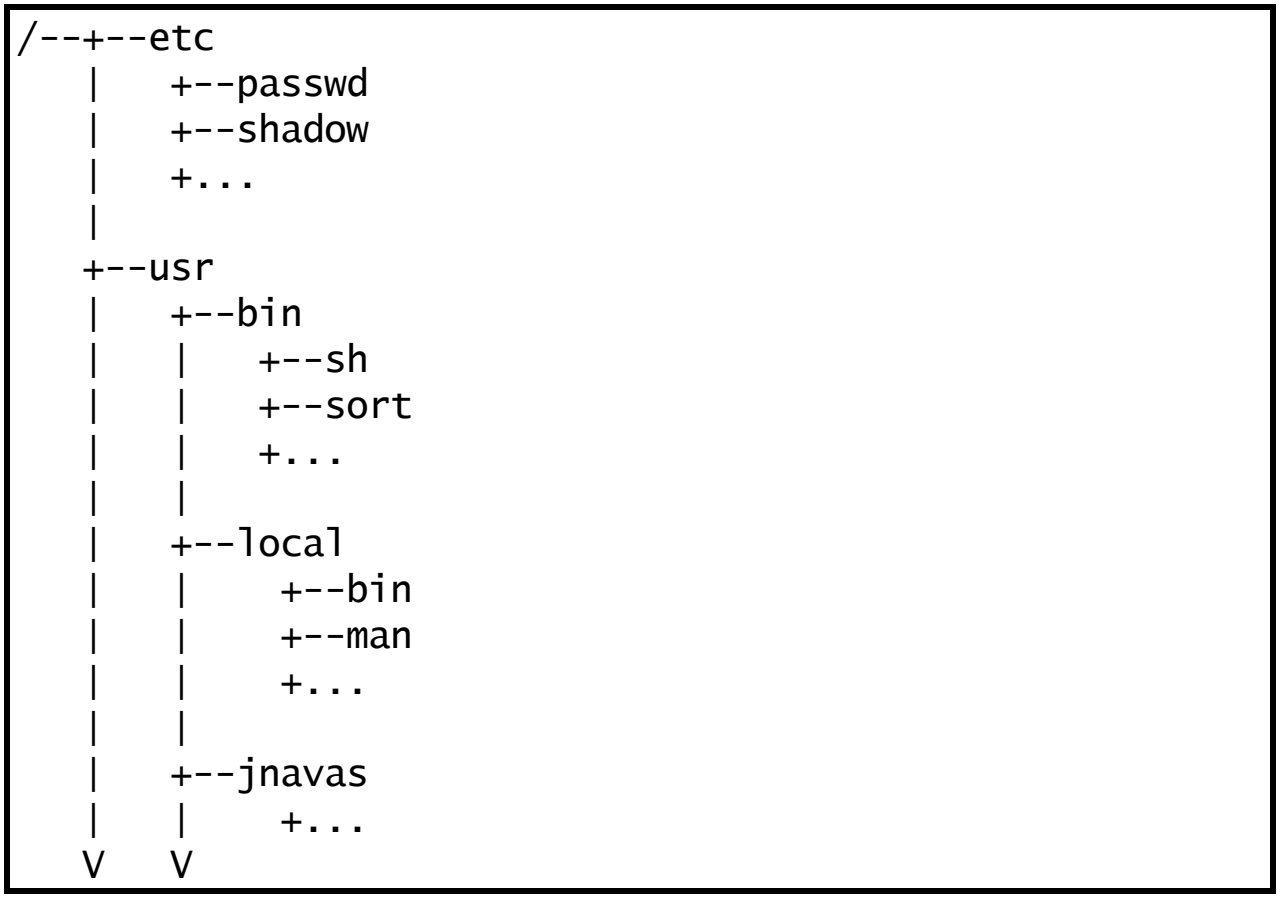
voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

I. What is UNIX

A. Brief history

B. How UNIX relates to MS-DOS

C. Typical UNIX environments



voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

II. Challenges

A. Amount of material

B. Networking

1. Servers

2. Remote file systems

C. Security

D. Variations

1. UNIX is not UNIX

2. Different command "shells"

E. Hardware interfacing

1. Physical

2. Kernel

voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

III. UNIX security overview

A. Permissions

1. User

2. Group

3. Other

B. Passwords

1. /etc/passwd

2. "Shadow" passwords /etc/shadow

3. The "root" password

C. Set User (su)

voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

IV. Technical issues

A. Common file extensions (executables; .c, .o, etc.)

B. Archives (ar, tar, and shar)

C. Compressed files compress (.Z) and gzip (.gz)

D. Encryption (DES and PGP)

E. Network File System (NFS)

F. Directories

G. Symbolic links

voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

V. Searching

A. grep

B. find

C. perl

voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

VI. Types of backup storage

A. Magnetic tape

1. QIC

2. 8mm

3. DAT

B. Hard disk

C. Cartridge disks

1. Iomega

2. SyQuest

D. CD-ROM recorders

E. Optical drives

F. Floppy diskettes

voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

VII. Strategies

A. "Drain the pond"

B. Take the source

C. Searching

D. Select "subtrees"

voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

VIII. What can go wrong

A. Shutting down the system

B. File system corruption

C. Wiping out

1. Files

2. Directories

3. File systems

IX. Summary

voice: 510/828-6764 fax: 510/828-6763 Internet: info@NavasGrp.com http://www.aimnet.com/~jnavas/

THE NAVAS GROUP

The Navas Group provides management and support services to a variety of domestic and international clients, with emphasis on high-technology marketing and product development. Expert witness services are also available. Inquiries are welcomed; extensive references are available on request.

The Navas Group
11901 West Vomac Road
Dublin, California 94568-1050
voice: 510/828-6764 fax: 510/828-6763
Internet mail: info@NavasGrp.com
World Wide Web: http://www.aimnet.com/~jnavas/

JOHN NAVAS

Principal of The Navas Group, Mr. Navas is a senior manager and expert with over 30 years of experience in general management, marketing and engineering. Industries in which he has been involved include aerospace, computers, distribution, education, food products, hotel and motel, mail order, pharmaceuticals, and telecommunications. Areas of special expertise include business planning, computer software engineering, international operations, quality improvement, and restructuring.

Over the years Mr. Navas has been qualified as an expert in marketing and engineering in several high-technology lawsuits, has advised the European Community on computer competition, and has testified extensively. Mr. Navas has been a frequent participant in computer industry groups, and has authored a number of articles and papers.

High technology lawsuits in which Mr. Navas has testified include:

United States vs. IBM
Memorex vs. IBM
Cherkas et al vs. Storage Technology Corporation et al
Olinger's Auto Parts vs. Ozie Hamerman
System Enhancement Associates vs. PKware
Ample Data vs. 3M
LaPine vs. Kyocera
Tom H. Connolly v. Hambrecht & Quist Group, et al
Treva Communications Inc. vs. The Renaissance Group, Inc.
Johnson Controls vs. State of California
Quarterdeck vs. Wollongong
Cadence Design Systems vs. Avant!