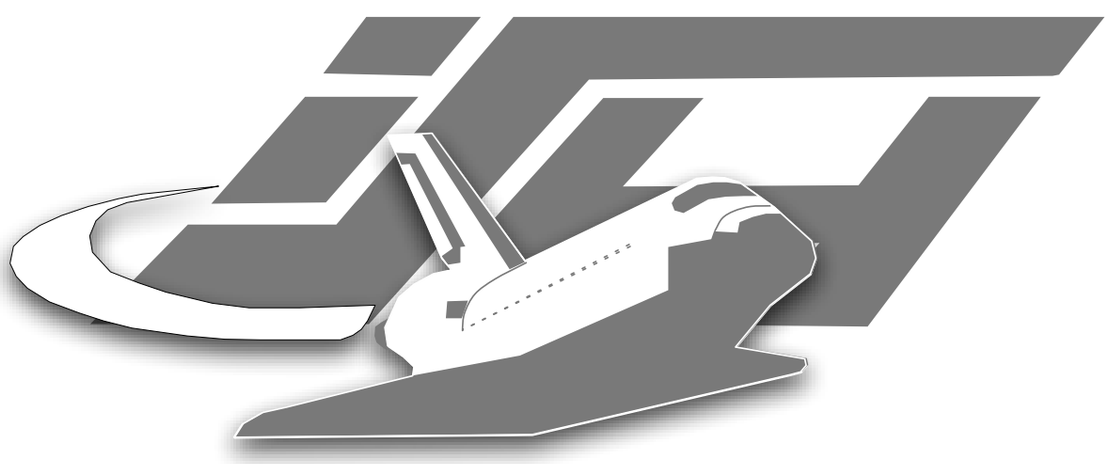
0wned by an iPod

Maximillian Dornseif

PacSec 2004



Laboratory for Dependable Distributed Systems

RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

RWTH

UNIVERSITY
OF TECHNOLOGY
AACHEN

Agenda

- Who we are and what we do
- Introduction to Firewire
- Demo
- Technical Details of hacking by FireWire
- Forensics by FireWire
- What to do about it

Who are we?

- RWTH Aachen University, Germany
- Laboratory for Dependable Distributed Systems
- Michael Becher, Maximillian Dornseif, Halvar Flake, Christian Klein

Introduction into Firewire

What is Firewire?

- Developed by Apple Computers since 1985
- IEEE 1394 (1995), IEEE 1394a (2000), IEEE 1394b (2002).
- Marketed by Apple as Firewire or FireWire
- Marketed by Sony as iLink

FireWire

- Serial bus, similar but more sophisticated than USB
  - Faster
  - Peer-to-Peer, needs no computer
  - More Power

Marketplace

- Apple - pushing FireWire hard:

  - Since January 1999 in Desktops

  - Since January 2000 in Notebooks
  - September 2000 where the last non-FireWire machines shipped
  - October 2001: iPod as FireWire killer-app

- Sony - we'll come to that
- Others: most upper class systems come with FireWire

FireWire by Sony

Other FireWire

- Audio
- Printers
- Scanners
- Cameras
- GPS
- Lab Equipment
- Industrial Control

Things to come

FireWire in the automobile market

http://66.102.11.104/search?q=cache:YPQ9lS7fqaAJ:www.

Google

Electronic Engineering Times

all on a single, TI FireWire® ch

Texas Instruments — Real World Signal Processing™

Aug.28, 2004

Home | Design Corner | Test Lab | Production Line | Times People

Quick Search

GO

Advanced Search

Membership

Login
Register Now
Update Profile
Change Alert Preferences

Services

eeResearch
eeEvents
Vendor Events
Useful Links
Marketing Services
Advertiser Services

get simple, cost-effective

NEWS & TRENDS

Print Version | E-mail this to a colleague | Send

FireWire in the automobile market

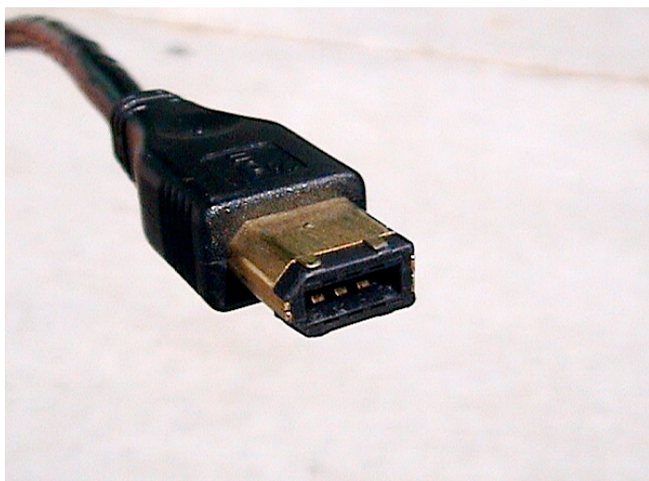
Posted : 16 Jul 2004

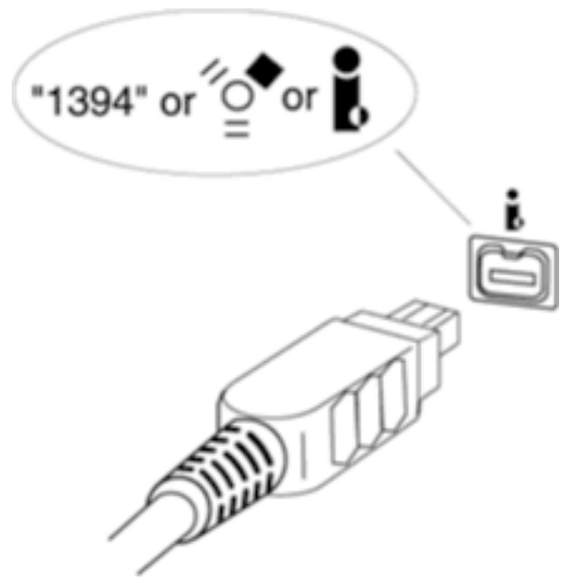
Although the controller area network dominates the current automobile market, other bus systems are being increasingly used in this market to respond to data transmission requirements, reliability and customers' needs.

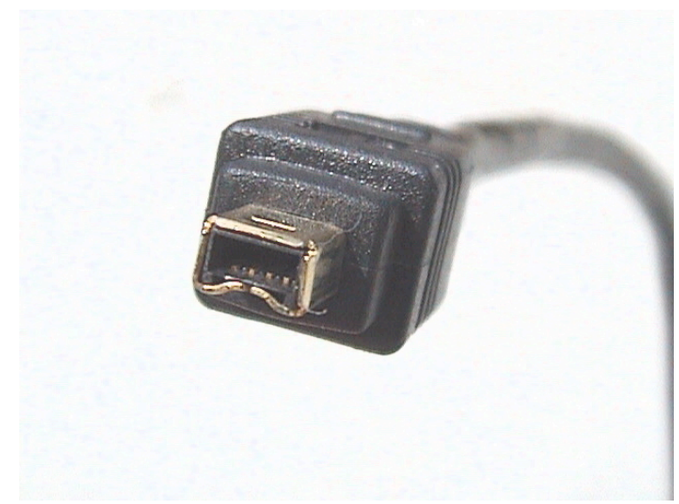
The first cars that support "real-time multimedia" applications according to the FireWire Standard are expected to enter the market in 2005. Families on their Sunday outings will then no longer have to endure the eternal question "Are we nearly there yet?" from their children. Thanks to the simple, economical use of video games and audio signals which the family is accustomed to at home, the question is more likely to be: "Oh, are we there already?"

get simpl
cost-effect
A/V data
connectivi

Confusion

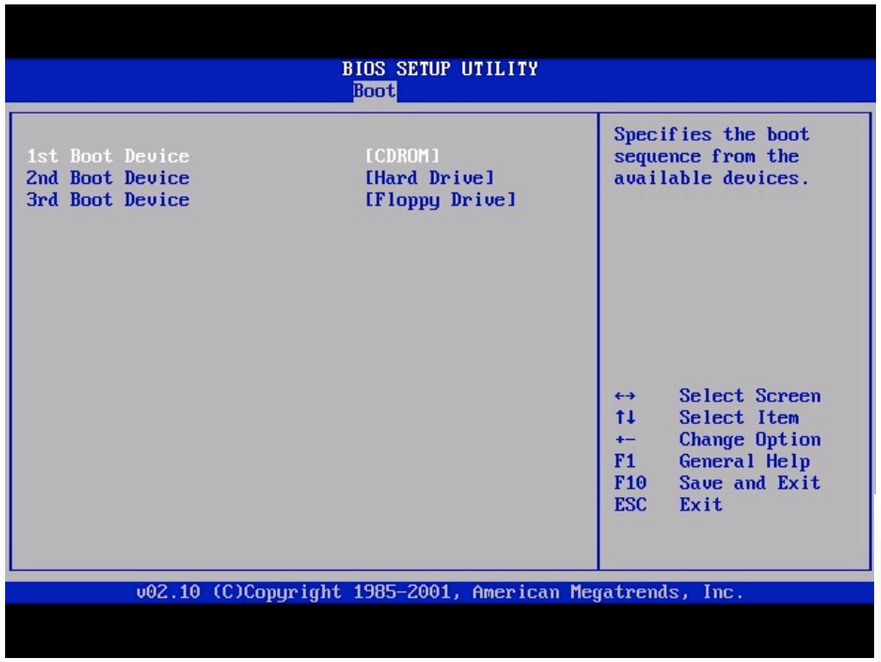


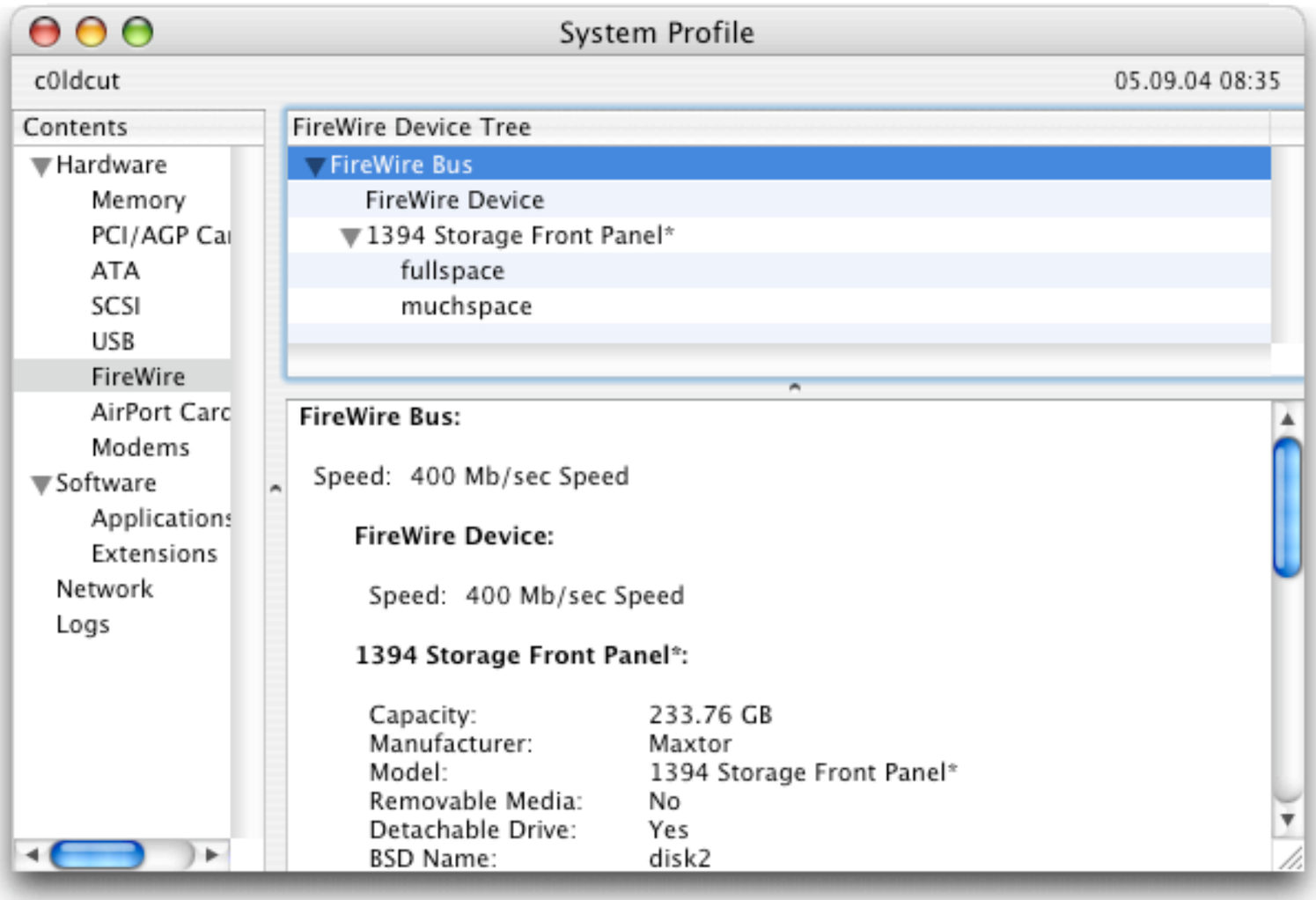




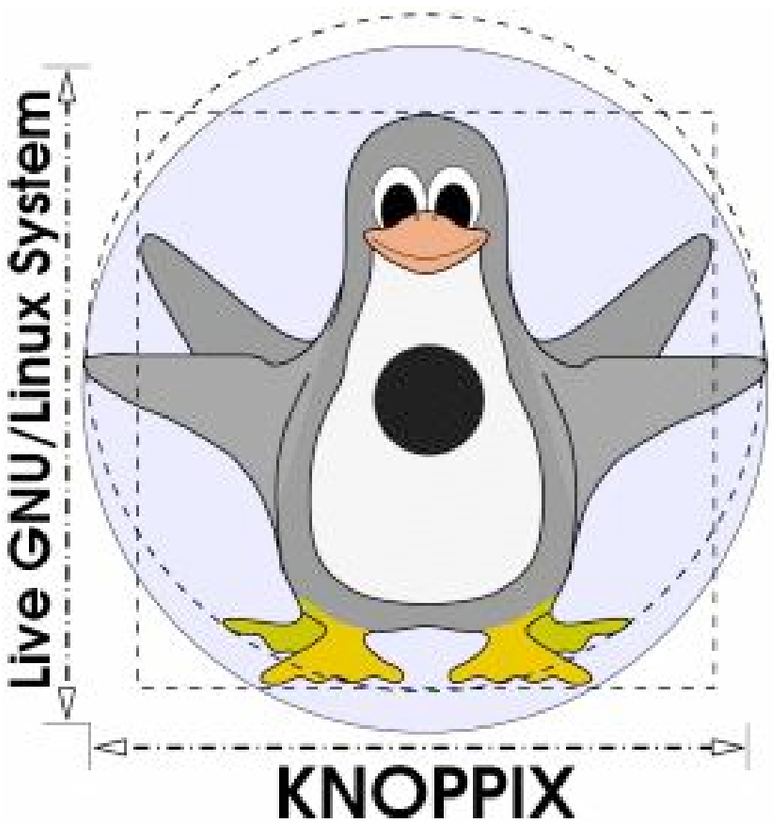
Demos

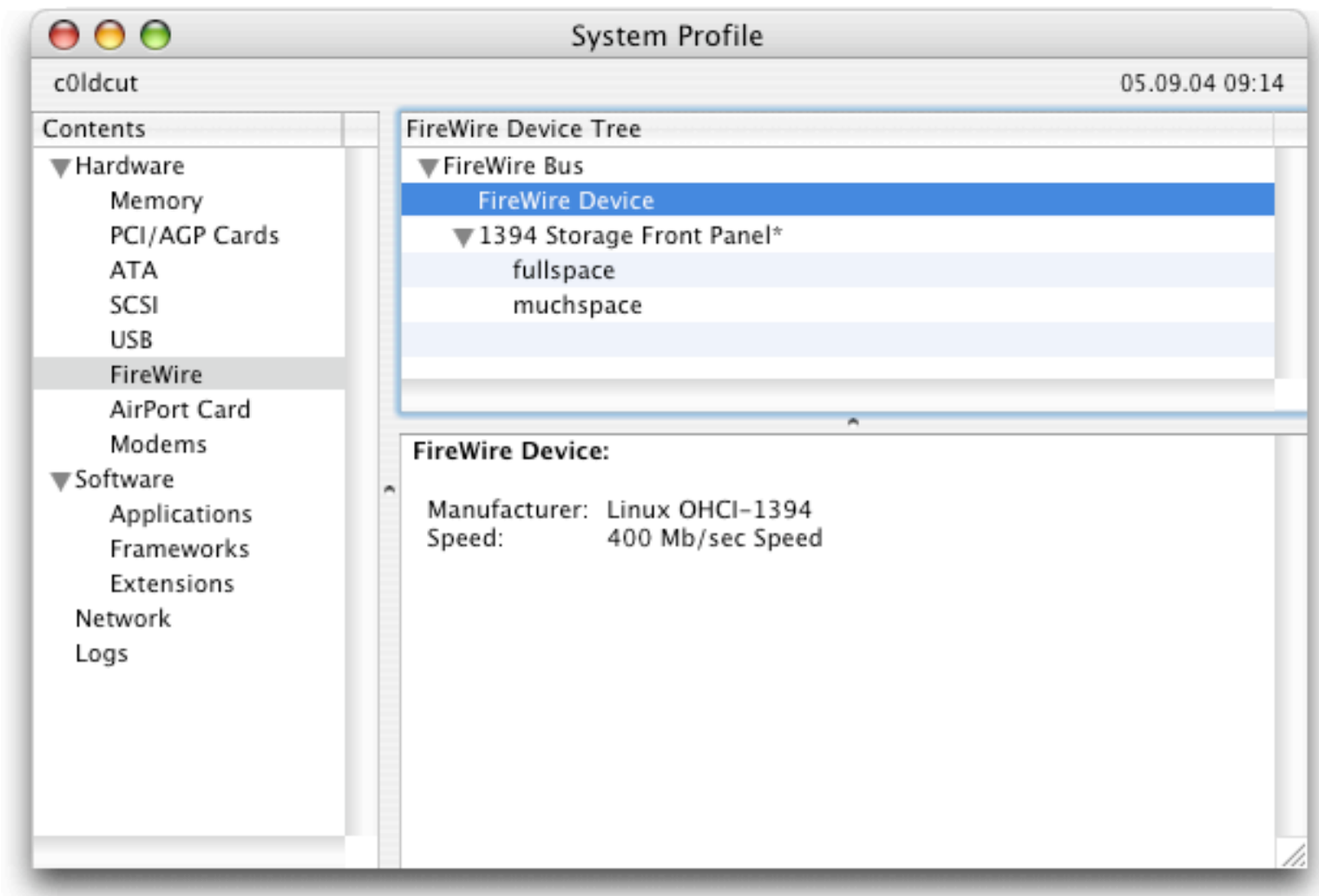
Connecting different Systems


BIOS SETUP UTILITY
Boot
1st Boot Device [CDROM]
2nd Boot Device [Hard Drive]
3rd Boot Device [Floppy Drive]
Specifies the boot sequence from the available devices.
↔ Select Screen
↑↓ Select Item
+- Change Option
F1 General Help
F10 Save and Exit
ESC Exit
v02.10 (C)Copyright 1985-2001, American Megatrends, Inc.

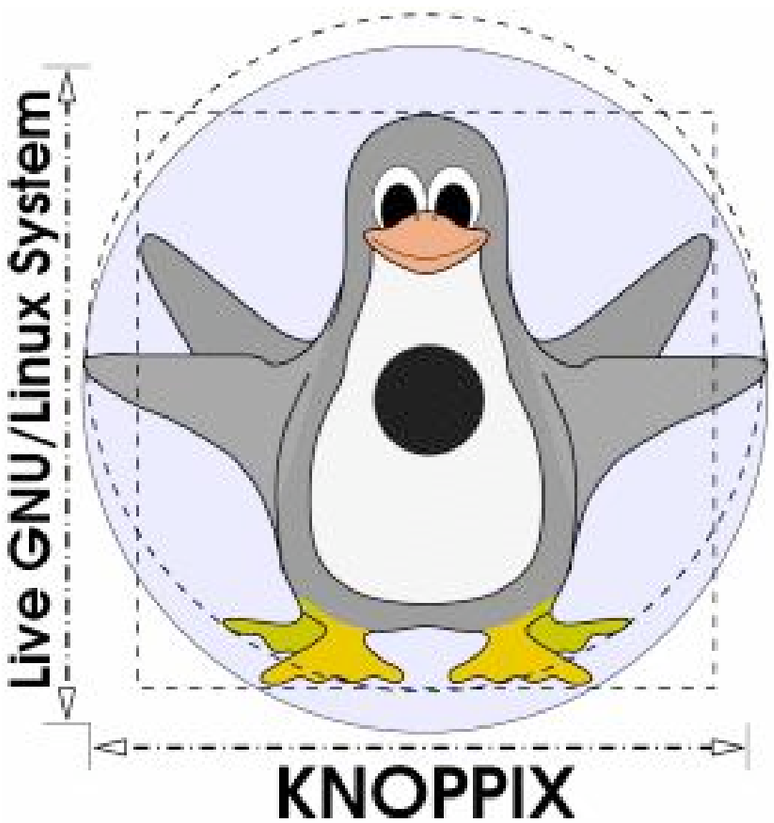

System Profile
c0ldcut
05.09.04 08:35
Contents
Hardware
Memory
PCI/AGP Ca
ATA
SCSI
USB
FireWire
AirPort Card
Modems
Software
Applications
Extensions
Network
Logs
FireWire Device Tree
FireWire Bus
FireWire Device
1394 Storage Front Panel*
fullspace
muchspace
FireWire Bus:
Speed: 400 Mb/sec Speed
FireWire Device:
Speed: 400 Mb/sec Speed
1394 Storage Front Panel*:
Capacity: 233.76 GB
Manufacturer: Maxtor
Model: 1394 Storage Front Panel*
Removable Media: No
Detachable Drive: Yes
BSD Name: disk2

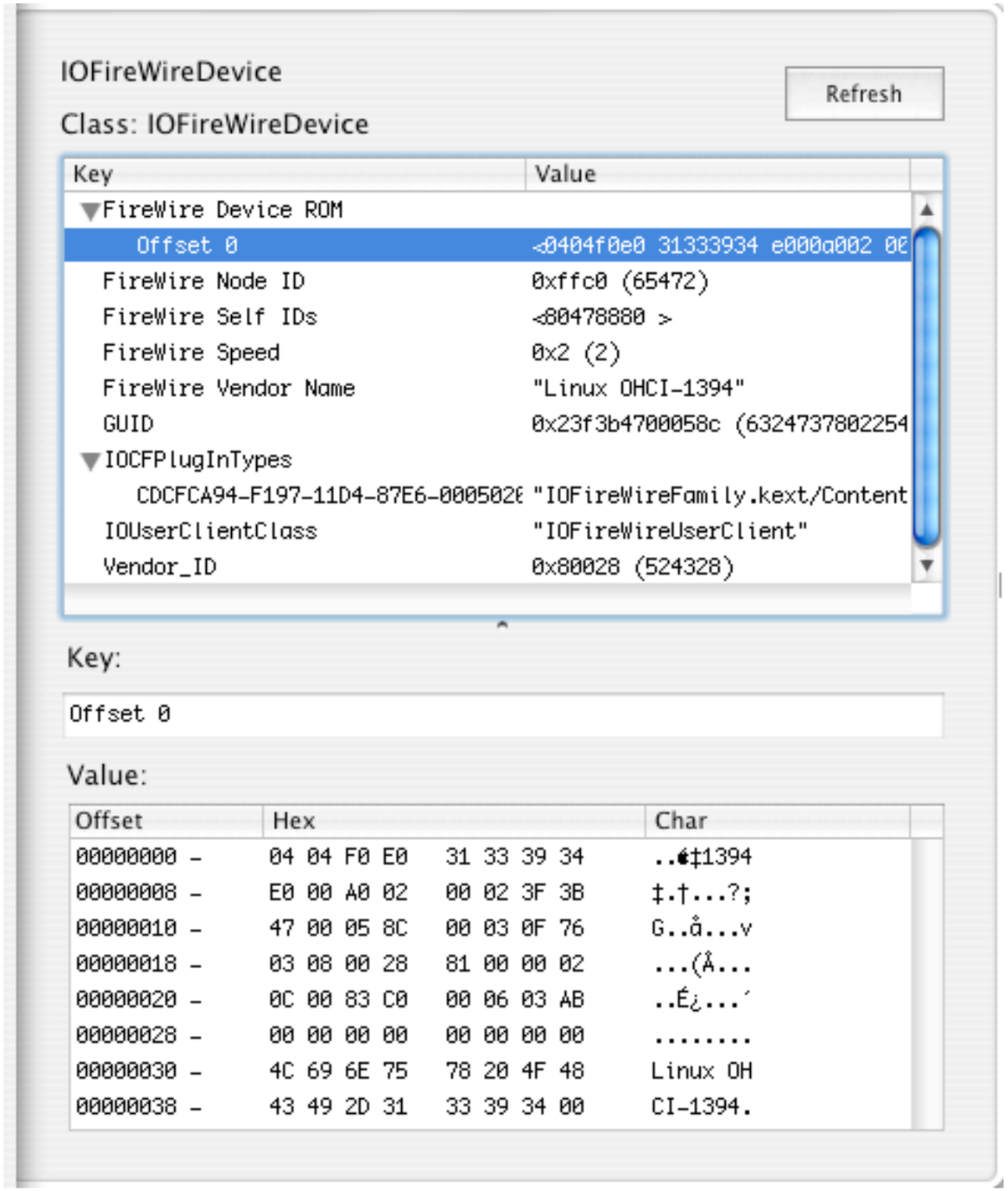

KNOPPIX
VERSION 3.3


Live GNU/Linux System
KNOPPIX

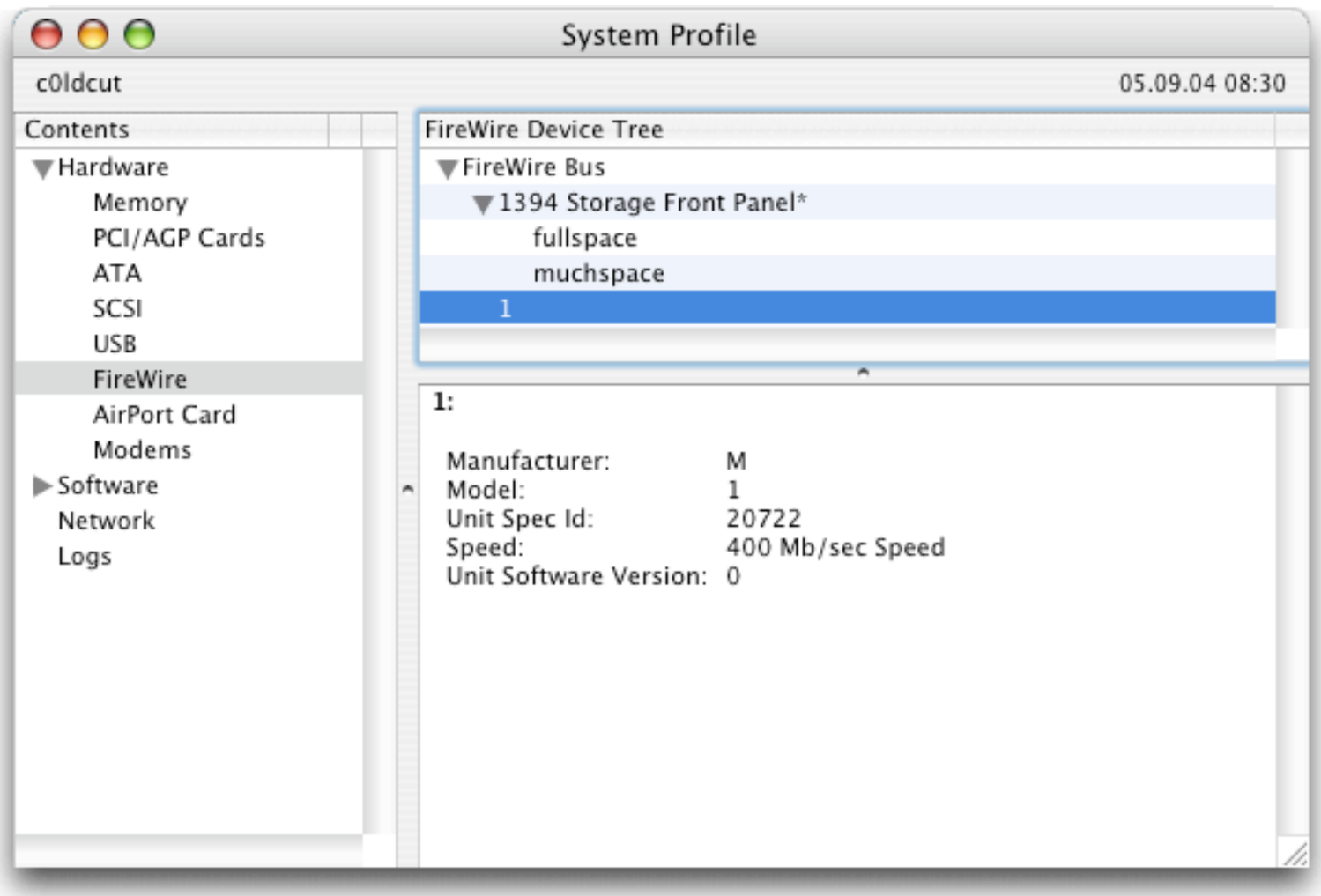

System Profile
c0ldcut
05.09.04 09:14
Contents
Hardware
Memory
PCI/AGP Cards
ATA
SCSI
USB
FireWire
AirPort Card
Modems
Software
Applications
Frameworks
Extensions
Network
Logs
FireWire Device Tree
FireWire Bus
FireWire Device
1394 Storage Front Panel*
fullspace
muchspace
FireWire Device:
Manufacturer: Linux OHCI-1394
Speed: 400 Mb/sec Speed


KNOPPIX
VERSION 3.3


Live GNU/Linux System
KNOPPIX


IOFireWireDevice
Refresh
Class: IOFireWireDevice
Key
Value
FireWire Device ROM
Offset 0
<0404f0e0 31333934 e000a002 0
FireWire Node ID
0xffc0 (65472)
FireWire Self IDs
<80478880 >
FireWire Speed
0x2 (2)
FireWire Vendor Name
"Linux OHCI-1394"
GUID
0x23f3b4700058c (6324737802254
IOCFPlugInTypes
CDCFCA94-F197-11D4-87E6-000502
"IOFireWireFamily.kext/Content
IOUserClientClass
"IOFireWireUserClient"
Vendor_ID
0x80028 (524328)
Key:
Offset 0
Value:
Offset
Hex
Char
00000000 – 04 04 F0 E0 31 33 39 34 ..¢‡1394
00000008 – E0 00 A0 02 00 02 3F 3B ‡.†...?;
00000010 – 47 00 05 8C 00 03 0F 76 G..å...v
00000018 – 03 08 00 28 81 00 00 02 ...(Å...
00000020 – 0C 00 83 C0 00 06 03 AB ..É¿...´
00000028 – 00 00 00 00 00 00 00 00 .....
00000030 – 4C 69 6E 75 78 20 4F 48 Linux OH
00000038 – 43 49 2D 31 33 39 34 00 CI-1394.


Microsoft
Windows xp
Klicken Sie auf Ihren Benutzernamen, um sich anzumelden.
Bill Gates
Chemiker
Computer ausschalten
Nach der Anmeldung können Konten hinzugefügt oder geändert werden.
Klicken Sie in der Systemsteuerung auf "Benutzerkonten".


System Profile
c0ldcut
05.09.04 08:30
Contents
Hardware
Memory
PCI/AGP Cards
ATA
SCSI
USB
FireWire
AirPort Card
Modems
Software
Network
Logs
FireWire Device Tree
FireWire Bus
1394 Storage Front Panel*
fullspace
muchspace
1
1:
Manufacturer: M
Model: 1
Unit Spec Id: 20722
Speed: 400 Mb/sec Speed
Unit Software Version: 0

Technical Details

Unified Memoryspace

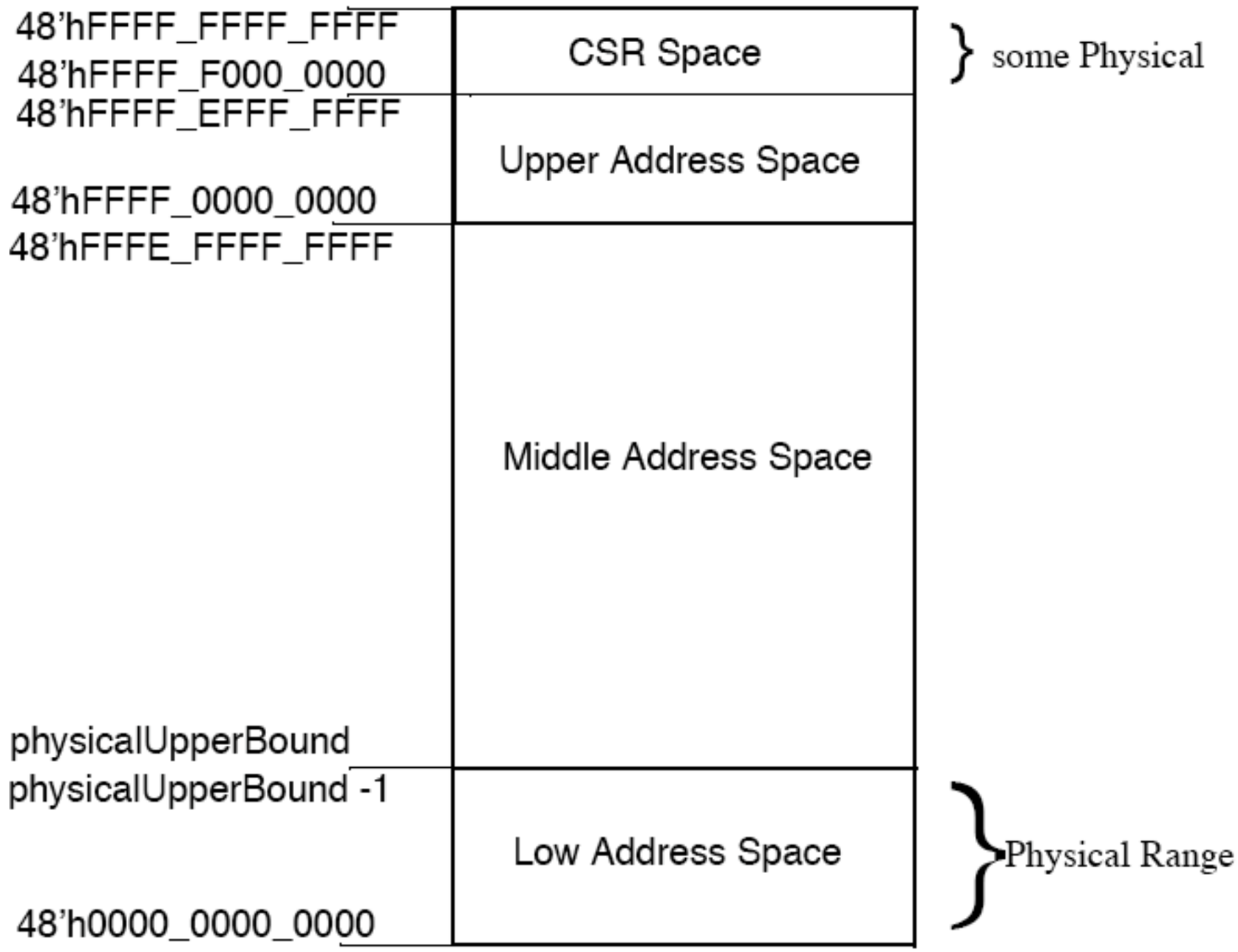


Figure 1-2 — Node Offset Map

OHCI

- Asynchronous functions
  - Can be used to access on-board RAM and RAM on extension cards (PCI)

physical requests - physical requests, including physical read, physical write and lock requests to some CSR registers (section 5.5), are handled directly by the Host Controller without assistance by system software." (OHCI Standard)

OHCI Filters

- "Asynchronous Request Filters"
  "The 1394 Open HCI allows for selective access to host memory and the Asynchronous Receive Request context so that software can maintain host memory integrity. The selective access is provided by two sets of 64-bit registers: PhysRequestFilter and AsynchRequestFilter. These registers allow access to physical memory and the AR Request context on a nodeID basis." (OHCI Standard)

- PhysicalRequestFilter Registers (set and clear)
  "If an asynchronous request is received, passes the AsynchronousRequestFilter, and the offset is below PhysicalUpper-Bound (section 5.15), the sourceID of the request is used as an index into the PhysicalRequestFilter. If the corresponding bit in the PhysicalRequestFilter is set to 0, then the request shall be forwarded to the Asynchronous Receive Request DMA context. If however, the bit is set to 1, then the request shall be sent to the physical response unit." (OHCI Standard)

Exploiting Reads

- We can read arbitrary memory locations. So we can:
  - Grab the Screen contents
  - Just search the memory for strings
  - Scan for possible key material
  - Parse the whole physical memory to understand logical memory layout.

Exploiting Writes

- We can write arbitrary data to arbitrary memory location. So we can:
  - Mess up
  - Change screen content
  - Change UID/GID of a certain process
  - Inject code into a process
  - Inject an additional Process

Forensics by Firewire

The forensics schism

- Unplug, do post-mortem disk-analysis
  - Misses Processes, open connections, etc.
- Gather information on the live system, afterwards do a clean shutdown and do afterwards disk-analysis
  - Contaminates evidence during the information gathering

Live Memory Dumps

- Being able to dump the whole memory without software support would solve the schism
- Tribble is a specialized pice of hardware being able to dump physical memory via DMA transfers over the PCI bus
- If you can do the same via Firewire, you get away with a software only solution

Forensics Challenges

- There is little experience in reconstructing logical/virtual memory from physical memory dumps
- To find open network connections etc. we have to parse a bunch of kernel structures

Conclusions

Shields-Up!

- Ensure that only fully trusted devices are connected to your FireWire ports
- Press you driver/OS vendors about FireWire filtering

Be Prepared for Forensics

- You might want to keep FireWire ports on incident prone systems at hand
  - Keep them physically secured
- Have some software ready to do memory dumps via FireWire