Work In Progress: Re-Documenting CIFS

Christopher R. Hertel

Storage Architect and CIFS Geek
Founder and CTO
www.ubiqx.com

ubiqx
Consulting, Inc.

SambaXP ● April, 2009

Introductions

Introductions

Who am I?

Why am I here?

How did I get myself into this mess?

Introductions

Where are we going?

...and what am I doing in this hand basket?

Introductions

Who am I?

➡ **Samba Team member**

➡ **jCIFS Team co-founder**

➡ Brain Surgeon, Playwrite, and Spiritual Healer (not really)

This geek here.

Introductions

Why am I Here?

- To tell you about the exciting new documentation...

- ...that covers CIFS circa **1996**.

Introductions

Why am I Here?

- To tell you about the exciting new documentation...

- ...that covers CIFS circa **1996**.

Yes, really.

Hang on... I'll explain why this is a good thing.

Introductions

Why am I Here?

- To tell you about the exciting new <u>Microsoft</u> documentation...

- ...that covers CIFS circa **1996**.

Part of the MCPP/WSPP documentation set.

On-line and available to the public.

Introductions

Why am I Here?

Microsoft asked a member of the *Samba Team* to document SMB/CIFS!

Introductions

Why am I Here?

Microsoft asked a member of the *Samba Team* to document SMB/CIFS !

"If you're surprised, you're not paying attention."

Introductions

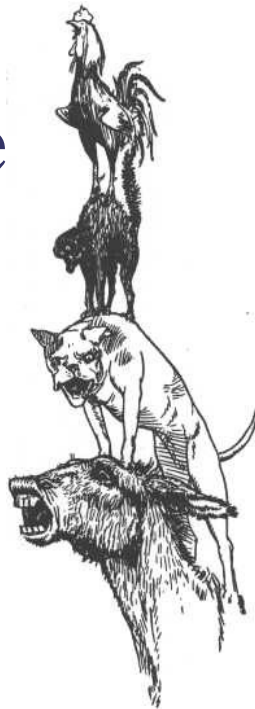How did I get myself into this mess?

In a word: **history**

Introductions

How did I get myself into this mess?

Late 1980's:

- Installed and managed branch-office LANs running DEC Pathworks
  (DEC's implementation of LAN Manager)

- Wrote a chat utility using NetBIOS Datagram Services over DECnet
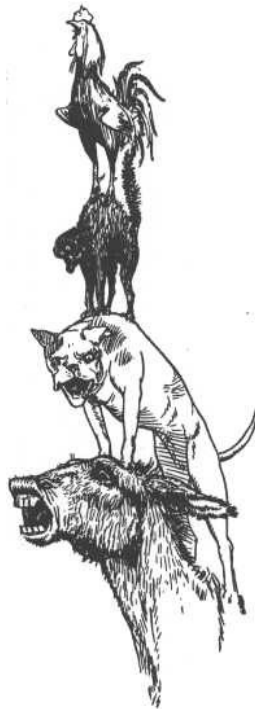
Introductions

How did I get myself into this mess?

Mid to late 1990's:

- Joined the Samba Team
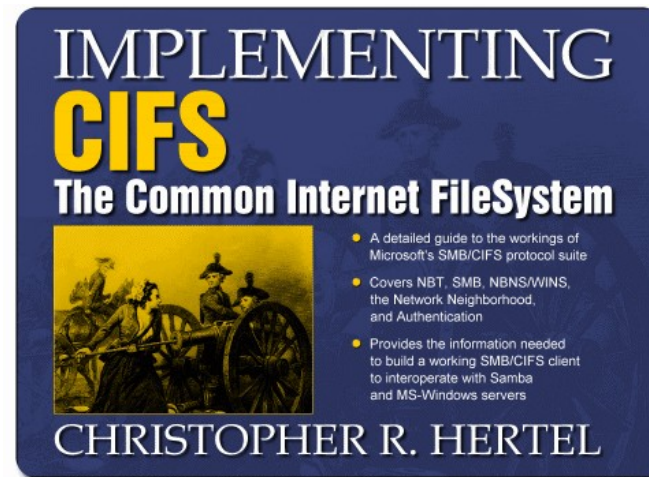
- Rewrote many parts of Samba 2.0

- Started jCIFS

Introductions

How did I get myself into this mess?

Early 2000's ► my tenuous claim to fame:

IMPLEMENTING CIFS
The Common Internet FileSystem

- A detailed guide to the workings of Microsoft's SMB/CIFS protocol suite
- Covers NBT, SMB, NBNS/WINS, the Network Neighborhood, and Authentication
- Provides the information needed to build a working SMB/CIFS client to interoperate with Samba and MS-Windows servers

CHRISTOPHER R. HERTEL

▷ I got tired of annoying Samba-folk with questions,

▷ I got tired of figuring out the same things again and again,
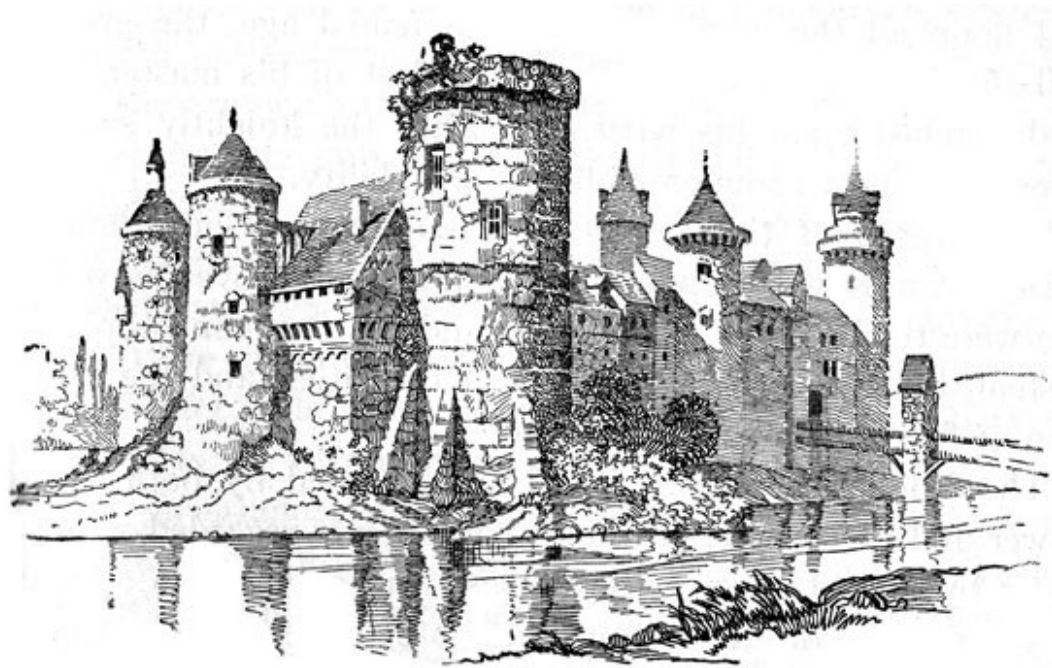
▷ I decided to keep **really good notes.**

Introductions

Where are we going?

- 🌍 History:
  Why it matters.

- 🌍 Scope:
  What is covered, & why.

- 🌍 Process:
  How we are going about it.

- 🌍 Results:
  The benefit to you.

History

History

In the early days, *SMB was documented:*

- 1984: IBM Personal Computer Seminar Proceedings, Volume 2, Number 8

- 1986: OpenNET/Microsoft Networks FILE SHARING PROTOCOL EXTENSIONS, Version 1.9, Microsoft and Intel (XENIX extensions)

- 1988: Microsoft Networks/OpenNet, Document Version 2, Microsoft and Intel (Core)

- 1988: Microsoft Networks SMB File Sharing Protocol Extensions Version 2.0, Document Version 3.3, Microsoft Corporation (LAN Manager 1.0)

- 1989: Microsoft Networks SMB File Sharing Protocol Extensions Version 3.0, Document Version 1.09, Microsoft Corporation (LAN Manager 1.2)

- 1990: Microsoft Networks SMB File Sharing Protocol Extensions Version 3.0, Document Version 1.11, Microsoft Corporation (LAN Manager 2.0)

- 1992: Microsoft Networks SMB Filesharing Protocol Extensions, Document Version 3.4, Microsoft Corporation (LAN Manager 2.1)

History

Then things started thinning out.

- 1992: X/Open CAE Specification, Protocols for X/Open PC Interworking: SMB, Version 2, X/Open Company, Ltd. (Core through LAN Manager 2.0)

- 1996: Microsoft Networks SMB File Sharing Protocol, Document Version 6.0p, Microsoft (Unfinished draft of NT LAN Manager 0.12 documentation.)

- 1997: A Common Internet File System (CIFS/1.0) Protocol, IETF INTERNET-DRAFT, Paul J. Leach, Dilip C. Naik (Unfinished draft v2 of NT LAN Manager 0.12 specification.)

- 2002: Common Internet File System (CIFS) Technical Reference, Revision: 1.0, Storage Networking Industry Association (SNIA)

- 2003: Implementing CIFS...

History

During this time...

- Windows NT
- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista

...and we knew that the documentation we already had was, in places,

- Incorrect
- Incomplete
- Incomprehensible

Never ascribe to malice that which is adequately explained by incompetence. — attributed to Napoleon Bonaparte, among others

History

This situation made people unhappy.

History

The Misinterpretation:
- "You guys want our source code!"

The Real Problem:
- No clear, documented standard for interoperability.

The Proposal:
- "Write it!"

Those who cannot learn from history are doomed to repeat it. — Santayana

History

Quick intro to the team:

CHRIS HERTEL — Ubiqx Consulting Inc — Microsoft
ROBERT RANDALL — Ubiqx Consulting Inc — Microsoft
JOSE RIVERA — Ubiqx Consulting Inc — Microsoft
MICHAEL SCHWARZ — Ubiqx Consulting Inc — Microsoft
STEVE HAND — Ubiqx Consulting Inc — Microsoft

You must be the change you want to see in the world. — Gandhi

History

Quick intro to the team:

History

Terms and Conditions

Scope
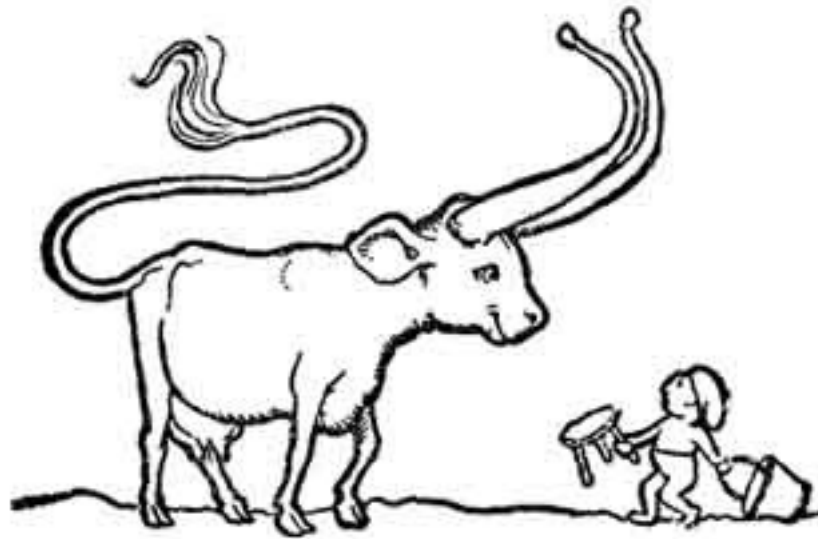
Scope

CIFS: A Common Internet File System

* What does the term "CIFS" mean this week?
  * NT LM 0.12 dialect
    * Not OS/2 LAN Manager
    * Not DOS LAN Manager
    * Certainly not the Xenix dialect
  * NT LM 0.12 dialect as of:
    * Windows NT3.51 & NT4 Server
    * Windows NT4 & 98 client

Very Limited Scope.
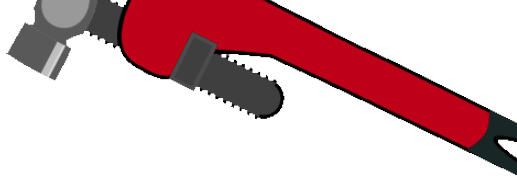
Scope
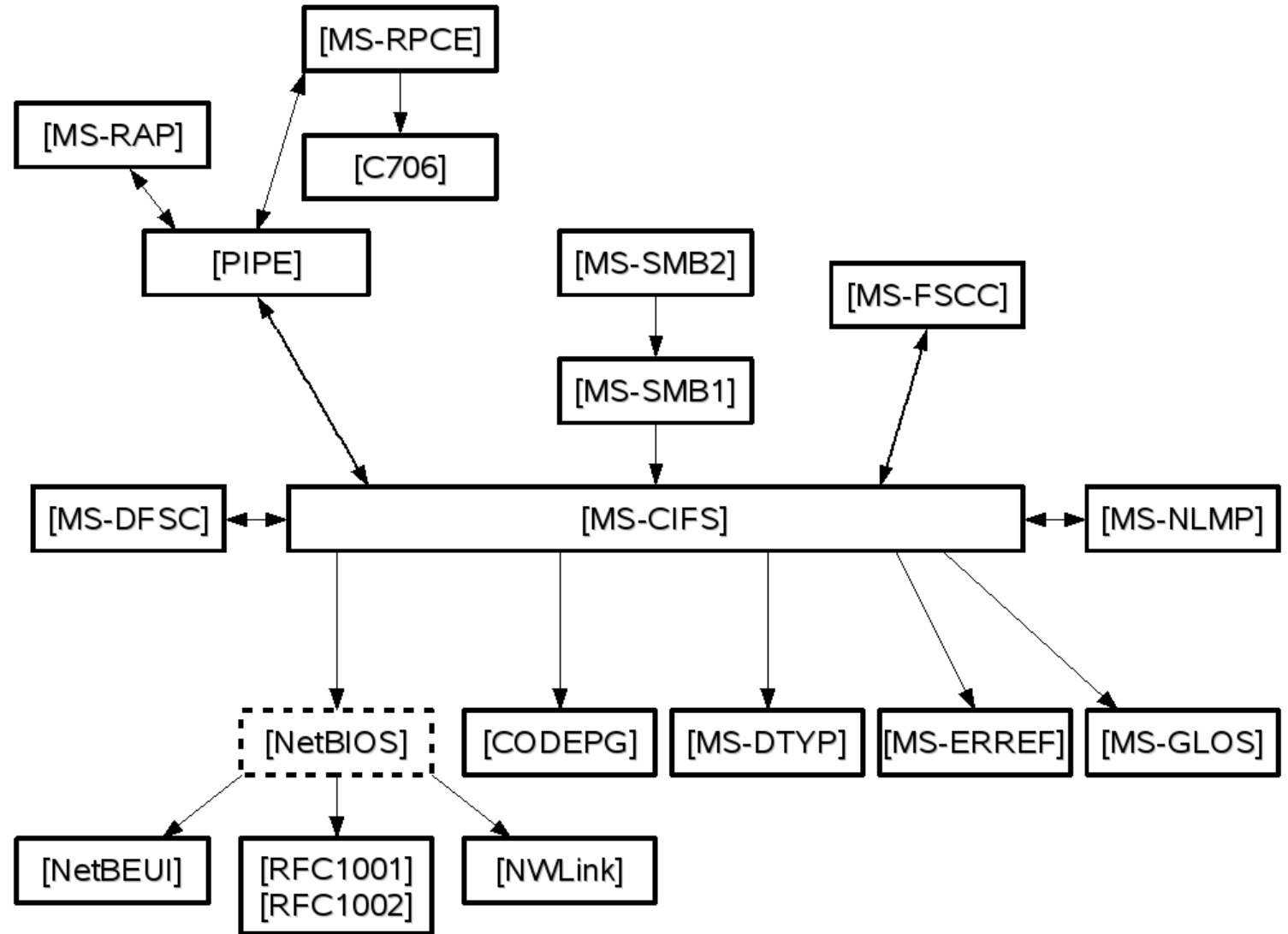
Scope

Must fit within the **TEMPLATE**

- Not a developer's dream
  - There are unusual rules
  - The format is a mix of ISO and IETF Standards styles
  - It was put together by non-techies
- We are committed to making the best of it

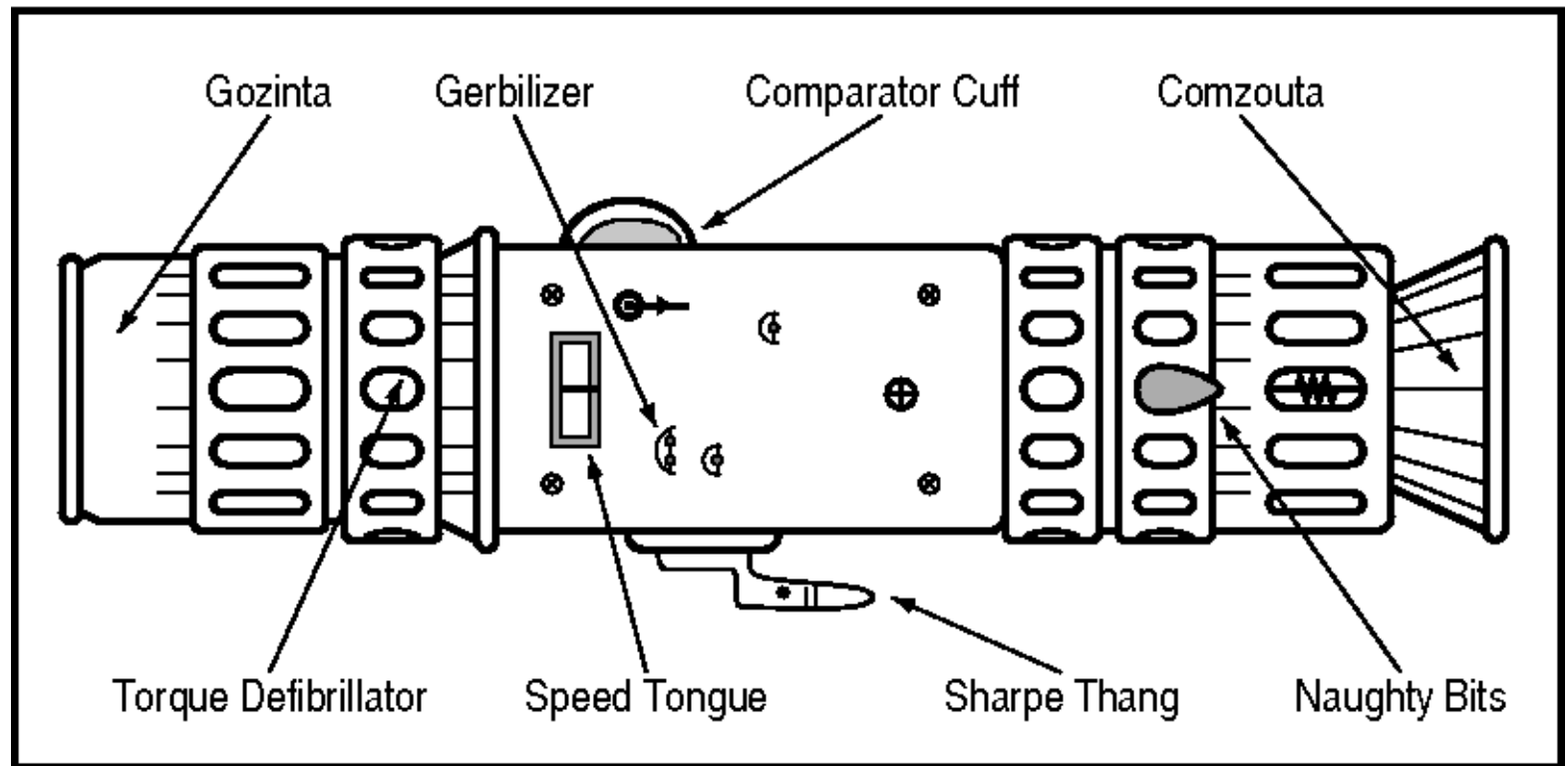(Just as Samba is committed to making the best of SMB/CIFS, eh?)

Scope

Remembering Jeremy's 2005-ish "Undocumented CIFS" presentation...

- My team has read the slides.
- We aim to make good use of Section 6: "Windows Behaviors"
- We can use constructive Feedback!
  - We'll be there at least a few more months.
  - We are submitting our own bug reports against existing docs.

Process

Gozinta · Gerbilizer · Comparator Cuff · Comzouta · Torque Defibrillator · Speed Tongue · Sharpe Thang · Naughty Bits

Process

Information Gathering

The ancient texts:

- A phenomenal source of... questions.
  - Oddities in the old IBM docs
  - Hold-overs from the Xenix docs
  - A lot to learn from the LANMAN docs
  - There are forgotten docs too
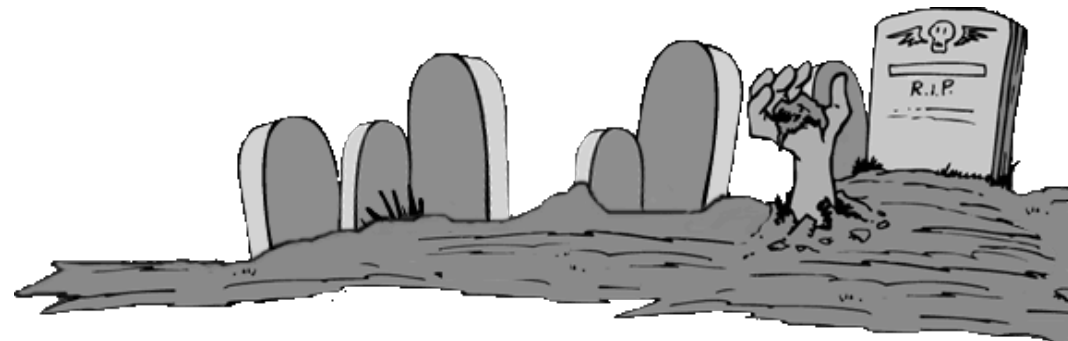 - Who here has noticed the references to a SID field in Leach/Naik?

Process

Where the bodies are buried

What I can say about the NT code is that it is
pretty much what we expected:

- Relatively thin
- Exposes Windows OS behaviors
- UNDEAD commands (Move/Copy)
- It is very old code now

Process

Writing

All writing is done to a Wiki, maintained within Microsoft.

- It's a scratch pad
- A communication medium
- Provides opportunities to review/rewrite
- Available for MS to monitor

Implementing CIFS was written in public.

- We add questions and comments to the command write-ups as we proceed.
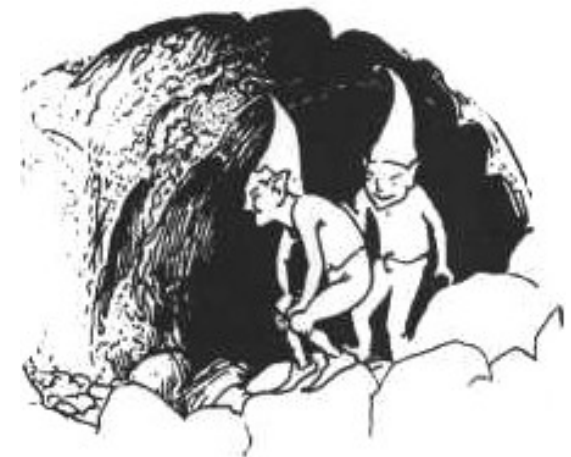
Process

Testing and Code Spelunking

Testing
- SMB Torture and jCIFS
  - Kludgey modifications to the above
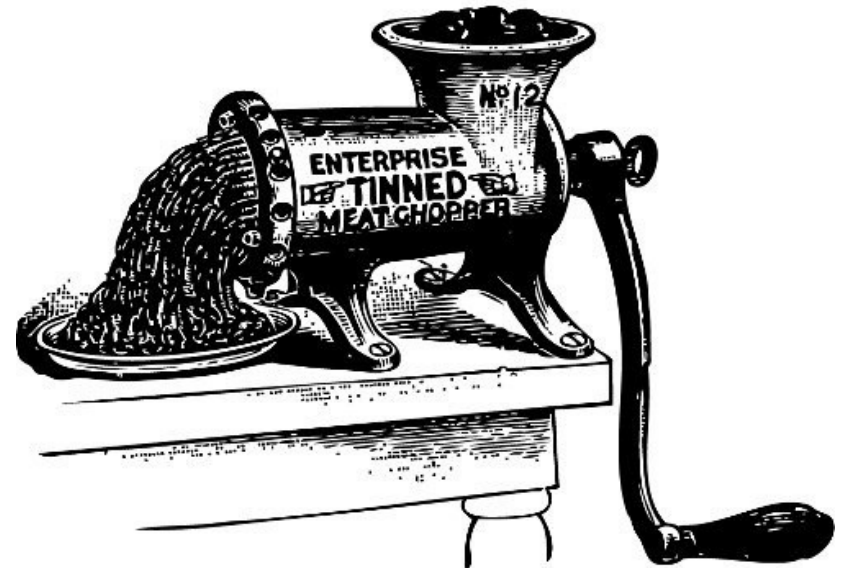- Plus a little code of our own

Code Digging
- Resolve questions
- Discover nuances
- Raise new questions

Results

Those that respect the law and love sausage should watch neither being made.
— Mark Twain

Results

Pretty much what we expected

- Studying CIFS raises as many questions as it answers
- We have to "document out" OS behaviors
- The new doc will be
  - more complete
  - more correct
  - more detailed than any previous CIFS doc
- It's still a CIFS doc

Results

Advantages this time 'round:
- Two very different perspectives
- "Are you sure that's how that works?"
- There will be a hand-off

A preview is available!
- We do want feedback

http://msdn.microsoft.com/en-us/library/dd727394.aspx
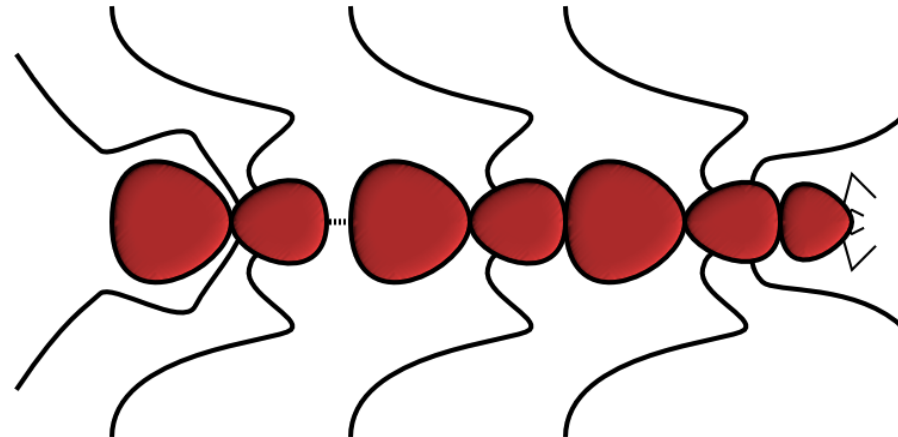
Results

What's next?

- 💡 Rewrite [MS-SMB]
- 💡 Review of related docs
  - 🔩 We have been working in these docs for months
  - 🔩 Have already started submitting bug reports

The End

Any Questions?