YGGDRASIL.EXE

01.01.2004

<<prev post | next post>>

Happy New Year.

I haven't updated my website in a while, and for good reason: I have not been well.

Apologies to anyone who is a fan of my work, both for the radio silence on my part, and for my lack of updates to PUCompile. I realize (thanks to your diligent commenting) that there has been a major overhaul to GCC a couple years back that is causing some major issues.

I am well aware of the new optimization flags from 3.2 completely breaking the branch prediction algorithm – and *yes*, I am also very much aware of the new .NET framework being pushed by the goons at Microsoft. Thank you again for the many, many emails I have received under this subject.

This post is not meant to announce any major update to PUCompile, and to be completely transparent: my development on the codebase has ceased as of last year. It is for that reason that I have made the codebase open source underneath GPLv2, and is now published in full on my SourceForge page.

I have no doubts that I am leaving my child in good hands with you all, and for my last parting request on this topic: Please, *treat her gently.*

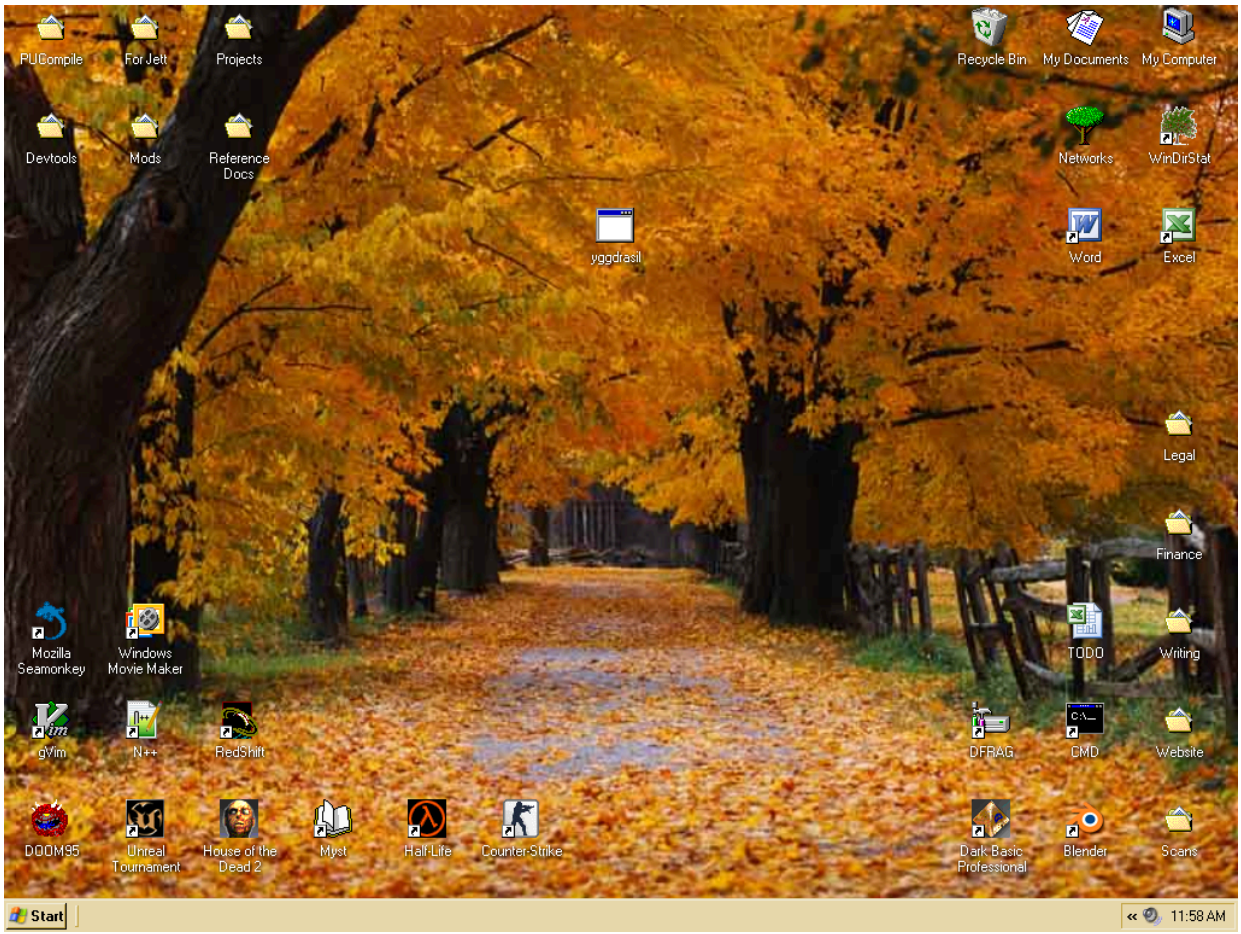
As for the intentions of this blog post: I am here before you today, two years after my last update, for two reasons.

To get this first one out of the way: I won't be around for much longer. In the interest of my privacy, all I can really tell you is that I got some bad news earlier in the year from the doctor. I ask that you please do not reach out to me or any of my friends and family regarding the nature of my condition.

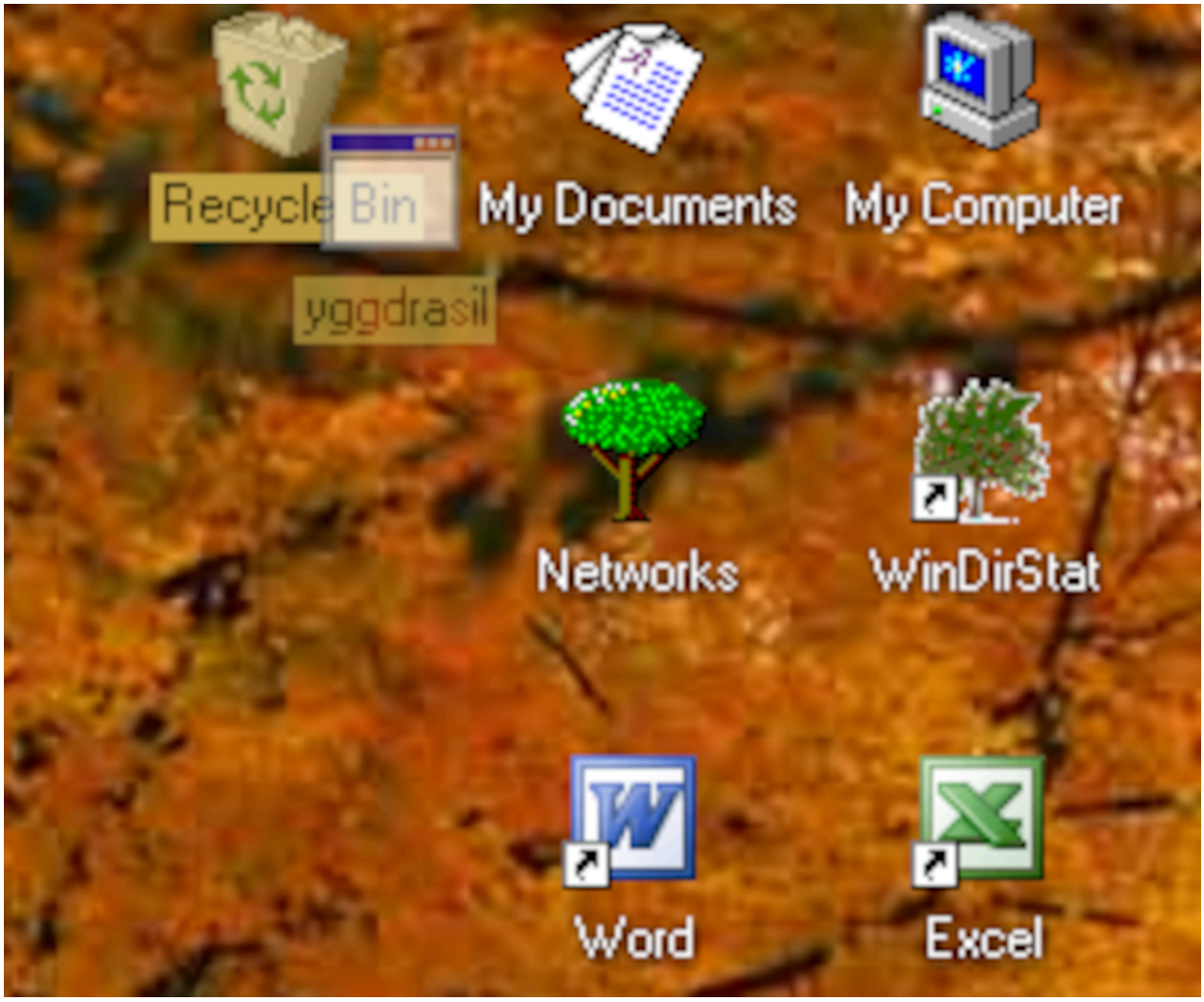
Forgive me for my bluntness in telling all of you this. I don't wish to sugarcoat the reality of my situation, and to be frank, I'm still not sure myself how to process that information. The concept of my life being finite was never alien to me, but now that I have an official expiration date, there is a countdown clock ticking down in the back of my head that is becoming more and more difficult to ignore with each passing day.

I'm not asking for your pity, nor am I asking for anything in return for this information. In fact, if there was a silver lining to all this, it's that there is a certain peace that comes with knowing. I may not have completely come to terms with what is going on, but at the very least, I've accepted it. In the words of my own late father: *it is what it is.*

I'll say nothing more on this particular matter, for there is nothing more to say on it. In actuality, if it weren't for the *other* reason I am writing this post, I wouldn't be writing here at all. I would have been perfectly content passing quietly without saying a word to anyone, and in truth, I would have much preferred it that way.

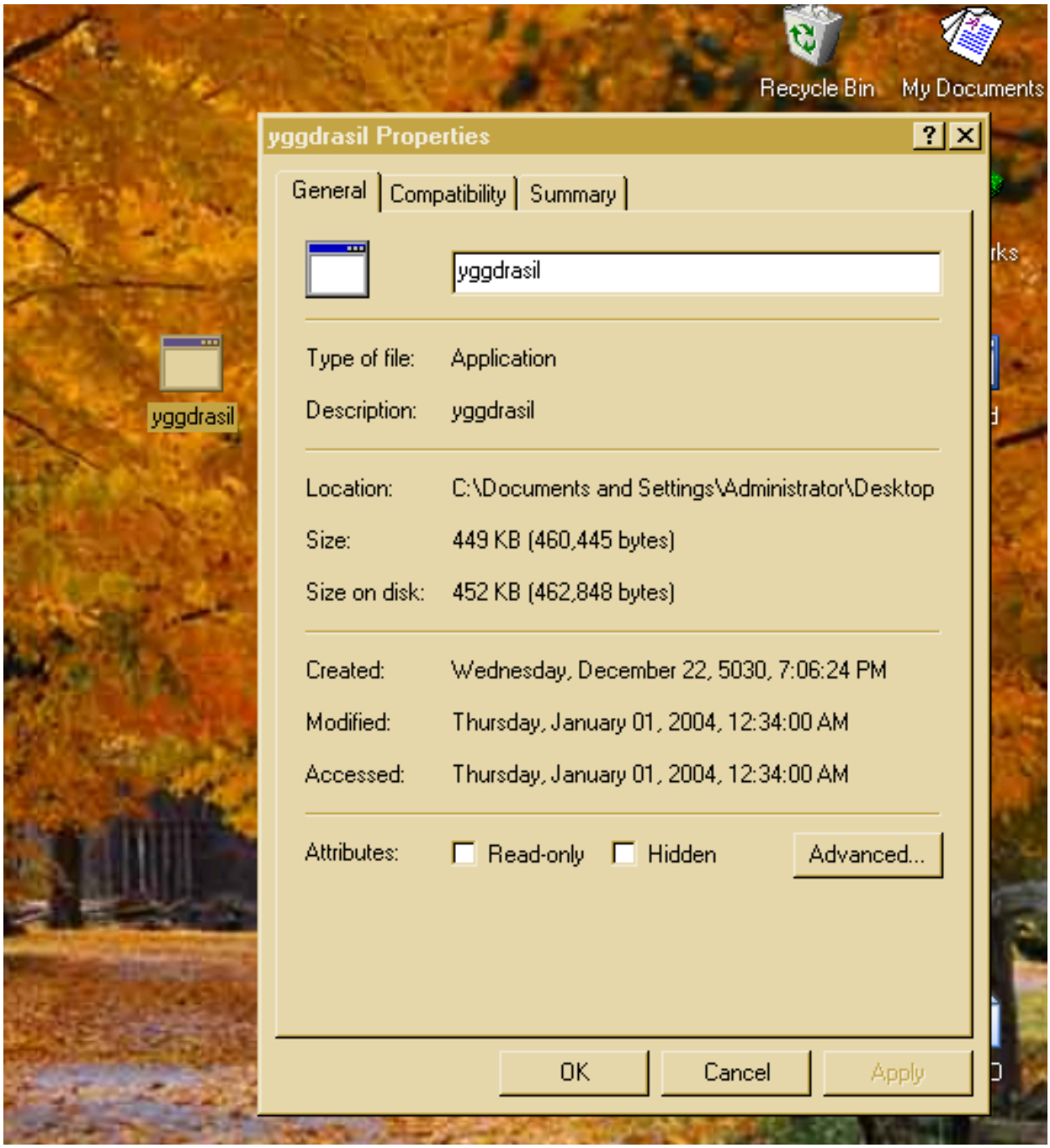


I'm not really sure *where* to begin in terms of when **YGGDRASIL.EXE** found its way into my life. If I were to be accurate to my own record, my knowledge of its existence on my PC only began as far back this last October. If it were as simple as that: a strange little program that just appeared one day, completely without fanfare, sitting there so innocently and unassuming on my desktop as if it had *always* been there, then I would have merely shrugged it off. I might have thought it to be some kind of worm, or perhaps some kind of juvenile prank on me.



Had I not paused for thought upon dragging it over the recycle bin that day, I can tell you with absolute certainty that I would not be up at five in the morning, completely awake in my hospital bed, with my ThinkPad burning my thighs red through the sheets, writing a blog post of all things.

I would instead be fast asleep, miles away in my head from any bit of troublesome 1s and 0s, spending my final moments with any kind of creature comfort I could find.



On first glance, the application was innocent enough: a tiny footprint at sub five-hundred kilobytes, not seeming to trigger any anti-virus or anti-malware software installed on my PC, legit extensions. No red flags to my own eye, but that tends to be the problem: *our eyes*. Fallible little things, easily prone to giving noisy information, degenerating in efficiency over time (severely in my case), vulnerable to the elements. We as humans are always at the whim of our accidents.

Even the best set of eyes could still be fooled. All it takes is a tiny little variance in attentiveness to miss details so innocuous. I could be forgiven then, for missing the date the application was created:

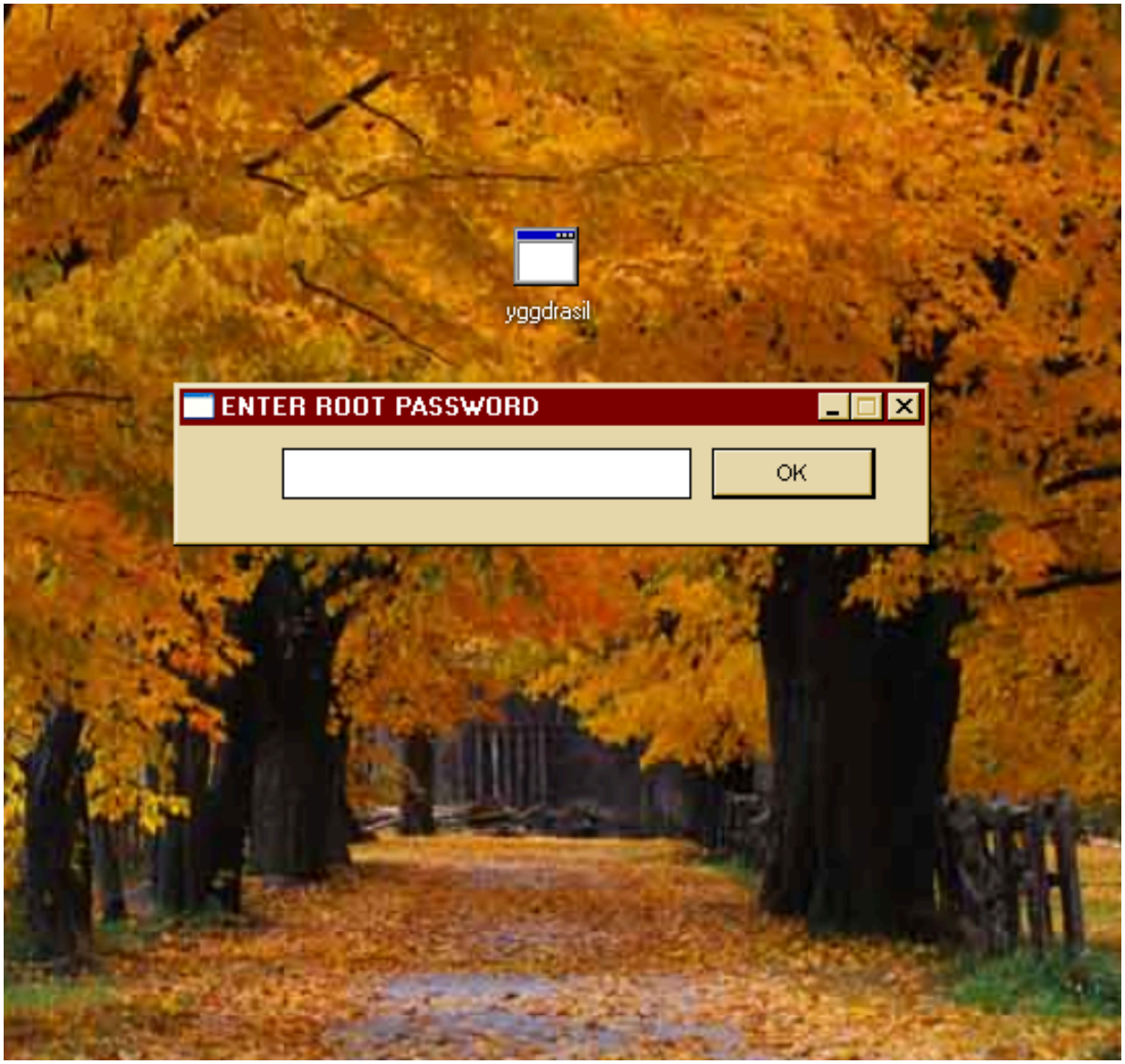
“Wednesday, December 22 5030, 7:06:24 PM”

Obviously, this was some mistake, or at best a joke told by some novice bedroom programmer. The information however did not care about my feelings toward it, instead simply *being* in response, as simple as data possibly could be: *a program from the future*, cradled right there in the middle of my desktop, resembling an apple hanging amongst the swaying autumn leaves, begging me to click into it.

Come on, Dash. You know you want to. What’s inside?

The temptation of Pandora distilled into two, little, *clicks.*

****click* *click***



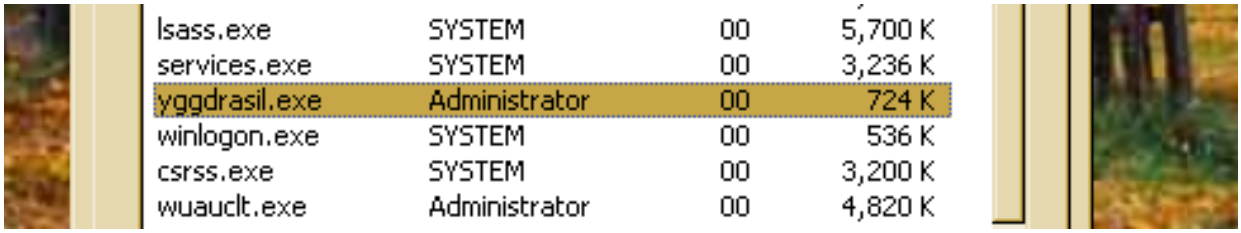
By this point, any pretension of innocence this program might have had dropped completely. Though as insignificant as a password window might be, several factors betray its facade of triviality almost immediately:

1. No trojan, worm, or otherwise would behave in this way. Malware likes to behave stealthily, lurking in the shadows of background processes, monitoring user behaviors, possibly even manipulating them. You could discard this as an obvious phishing attempt, dismissable by even the most rookie of IT specialists, and only dangerous to geezers *even older than myself* who had never touched a computer. If that were so, it would be a pitiable attempt at getting my credentials. But then, *why* would it ask me for my root password if it already had its grip on my operating system? The mere appearance of **YGGDRASIL.EXE** on my desktop without my knowledge or approval would indicate that the interloper would *already* have root access to the machine, and I'm running goddamned *Windows XP*. It's not like it would be difficult for a malicious program to get its claws into my registry files and get the information it needed without me ever even knowing.

2. My own admin login password does not work. In fact: *nothing works*. No matter what I type in, clicking 'OK' just exits the window. If this were malware with the intent to steal user information, there would be some kind of network activity being displayed on the activity monitor, but there's *nothing*. It's completely detached from the internet and runs independently from it.

Much as I tried to rationalize this program's existence, it defied my logic at almost every turn.

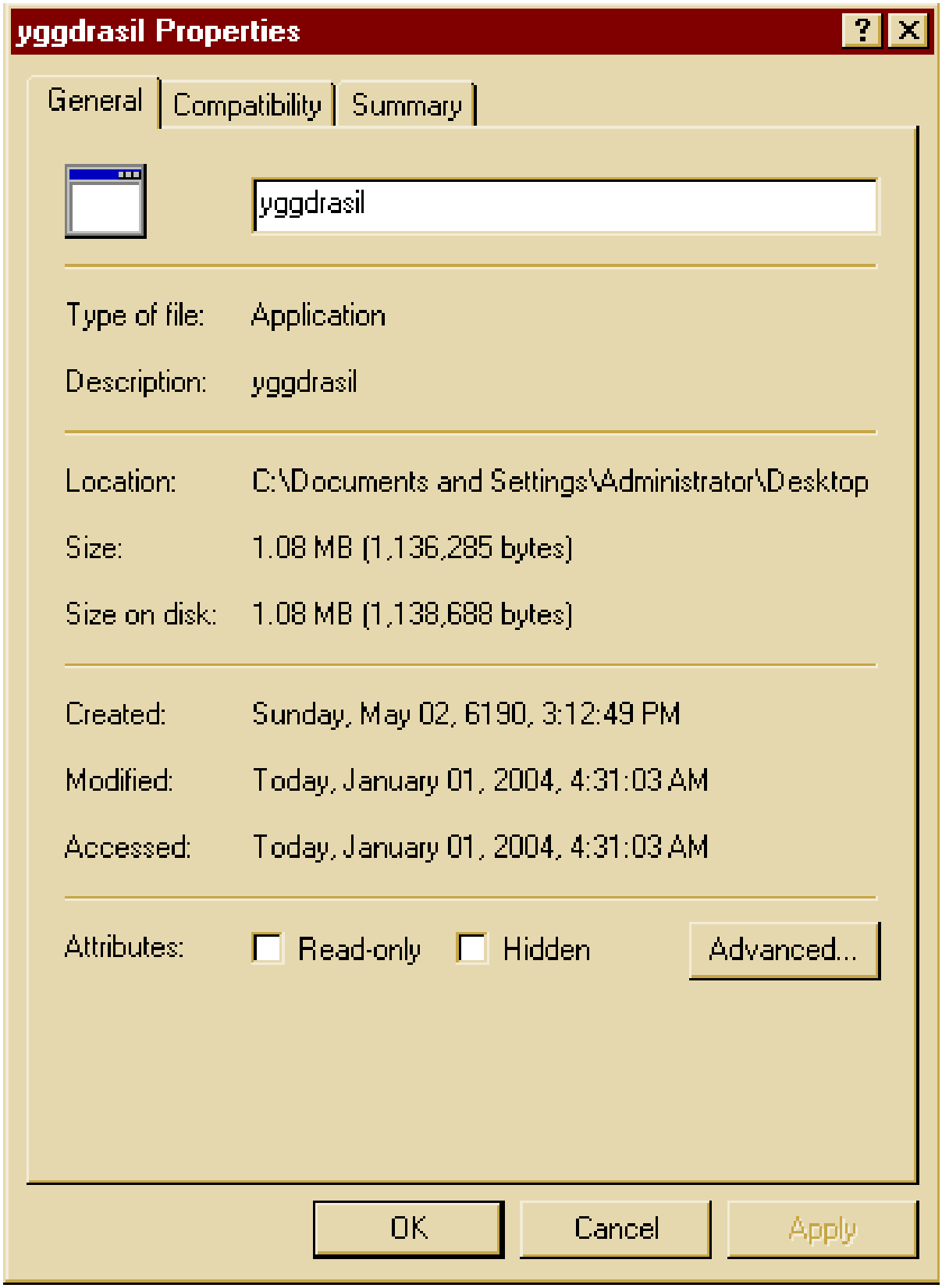
As far as I knew, this program exhibited *zero* signs of deception, and was in-fact a working program, with its mysterious features locked behind a password that I had no knowledge of.



lsass.exe	SYSTEM	00	5,700 K
services.exe	SYSTEM	00	3,236 K
yggdrasil.exe	Administrator	00	724 K
winlogon.exe	SYSTEM	00	536 K
csrss.exe	SYSTEM	00	3,200 K
wuauclt.exe	Administrator	00	4,820 K

There was, however, one key giveaway as to the nature of **YGGDRASIL.EXE**, revealed only by checking my task manager: The program continued to run in the background after running it. So there was at least *some* credence towards this application having a kind of malevolent purpose, surreptitiously running alongside all the other background processes as if it belonged there with all the others – behavior very in-line with most viral programs.

Believe it or not, this was a relief. Finally, something familiar. Something I could parse. Up until that point, I was grasping at straws as to **YGGDRASIL.EXE**'s purpose, but with this information I could at least *start* the troubleshooting process. Of course, that was *not* the beginning of the end as I had so hoped, myself at that point still somehow clinging on to some youthful naivety that all was well at its core, that *routine* could be my ticket out of this, as it always was: a comforting narrative that I told myself. One that had a defined beginning and end point. A story that made sense.

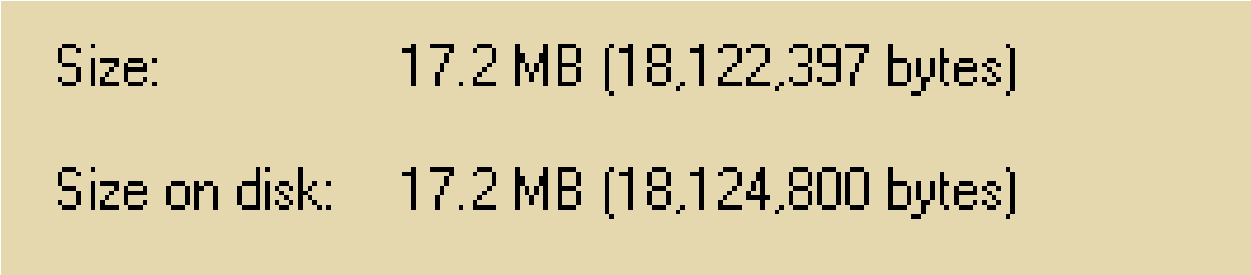

yggdrasil Properties
General
Compatibility
Summary
yggdrasil
Type of file: Application
Description: yggdrasil
Location: C:\Documents and Settings\Administrator\Desktop
Size: 1.08 MB (1,136,285 bytes)
Size on disk: 1.08 MB (1,138,688 bytes)
Created: Sunday, May 02, 6190, 3:12:49 PM
Modified: Today, January 01, 2004, 4:31:03 AM
Accessed: Today, January 01, 2004, 4:31:03 AM
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply

If only I had inspected further in that moment, not clinging to some kind of fantasy that, of all things, at least *this* was under control. I've lived a very long life, and as a result I have come across many, many different computer viruses, of all shapes and sizes. So consider it a shock to my 42-year-old soul that I had not *seen it all,* like I had so thought. That there were still new things out there, waiting to surprise me.

As my IT brain kicked into gear, I opened the properties of **YGGDRASIL.EXE** once more, and like the last time, everything *seemed* in order. That is on me for the short-sightedness, and perhaps in my old age and sickness I am losing a little bit of that *sharp edge* my brain once had. Because as surface level as right-clicking the file and clicking 'Properties' is in terms of troubleshooting, you wouldn't think that alone would give so much away, while at the same time belying nothing of its true nature. In case you are similar to me in this case and missed it, there were two major indicators that something was very, very wrong:

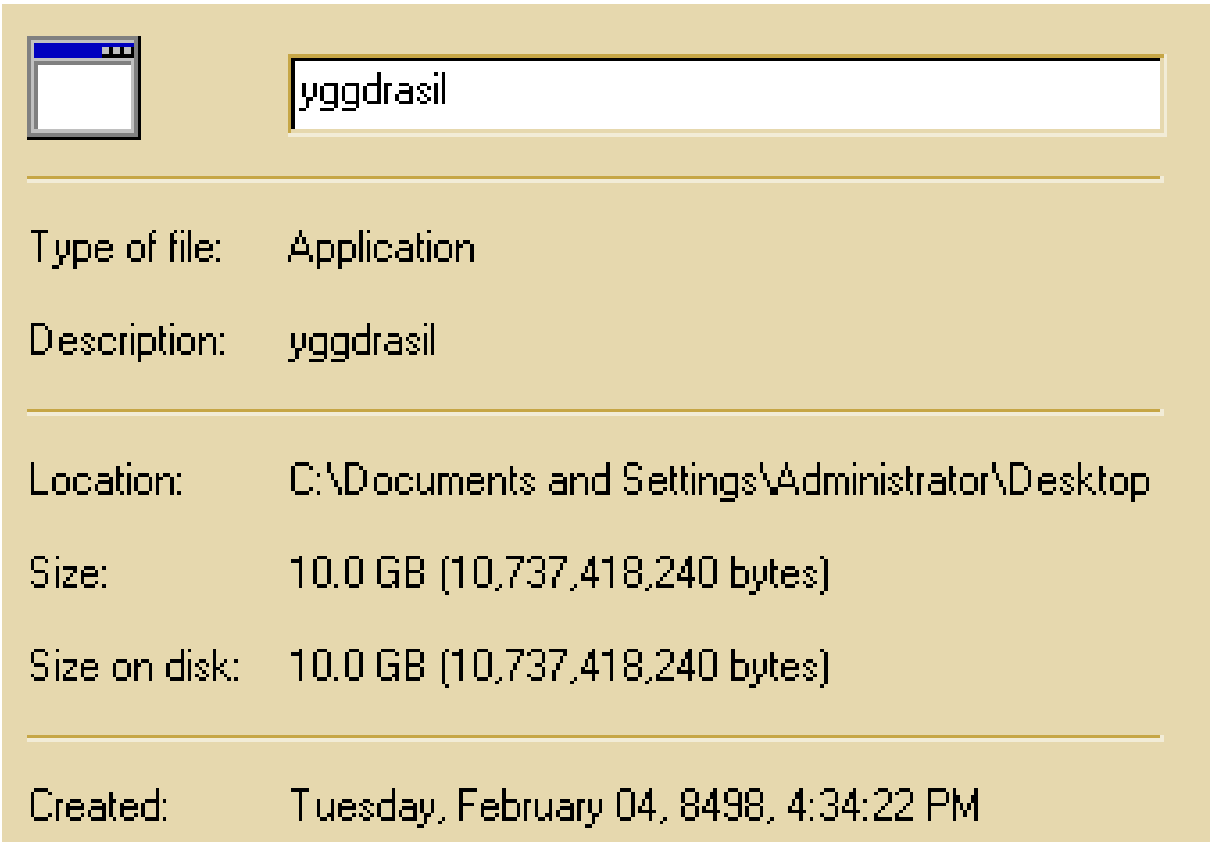
1. The 'Date Created' was no longer *December 22, 5030*, but had now jumped over 1000 years into the future year of ***6190***. Now, you could easily say that this falls in line with the 'novice programmer joke' theory posited earlier – it's not hard at all to modify the properties of any exe, and all you would need is the Windows header file to do some major damage. But if that were the case, then *why* would someone program this virus like that? I can think of no major reason to hide the 'Date Created' from the user other than to fool them, but then why the extra step? What reason would someone have to make the creation date constantly shifting around like that? It would have done a fine enough job at tricking the user if it had merely picked a date reasonable enough to cast doubt. Not only does it *not* pick a reasonable date, but it seems to be changing at random. Another check of the Properties windows confirms this, the date just randomly changes, either forward or backwards, no matter what I do with it.

2. I would have completely missed this had I not been going back and checking my screenshots, and thank heavens I did go back and check, because this detail might have completely eluded me until it were too late. A detail that, upon realization of it, didn't quite fully *register* until I had time to process it. It's a harmless enough distinction: The file was now *1.8MB* rather than *449KB*, indicating that it had more than doubled in size since I first checked it. Of course, this information hits immediately as nothing out of the ordinary. It's completely normal for file sizes to change, for a number of reasons. The fact that it was slowly growing, while certainly creepy in its own right, wasn't an indicator of any trouble on the technical side of things, though if you've made it this far in reading, you already know by now that I've become somewhat of an expert in shielding myself from the truth.



As I let **YGGDRASIL.EXE** run its mystery processes on my machine, slowly but surely, it continued to grow. I think in any other circumstance that this would have been the moment where I would normally jump into action: Doing whatever I could to quarantine this program, and submitting all of my findings on it to F-Secure, perhaps sending out a couple emails to Kaspersky and Symantec, then calling it a day.

Instead, I sat there, and I watched it grow. *And grow.*



Eventually, it came to a halt. I don't know how long I sat there watching it. It felt like hours. I remember the sunrise filtering through the blinds of my office. I might have slept there, to be honest with you I don't remember exactly. Truth be told, I've been having trouble remembering a lot as of late, so my apologies if this recollection is somewhat fragmented, but as far as I can certainly tell you: It stopped at *10GB* in size.

At a loss for what to do, I sat aside any sort of suspicions that have been developing up to that point. My analytical framework had utterly failed me. The investigative approach I had become so used to over the years was *nothing* in facing **YGGDRASIL**, and that gave me pause for thought: Had my framework *always* been a failure? Or was it merely entropic, another victim to the slow marching on of the minute-hand's orbit around the sun?

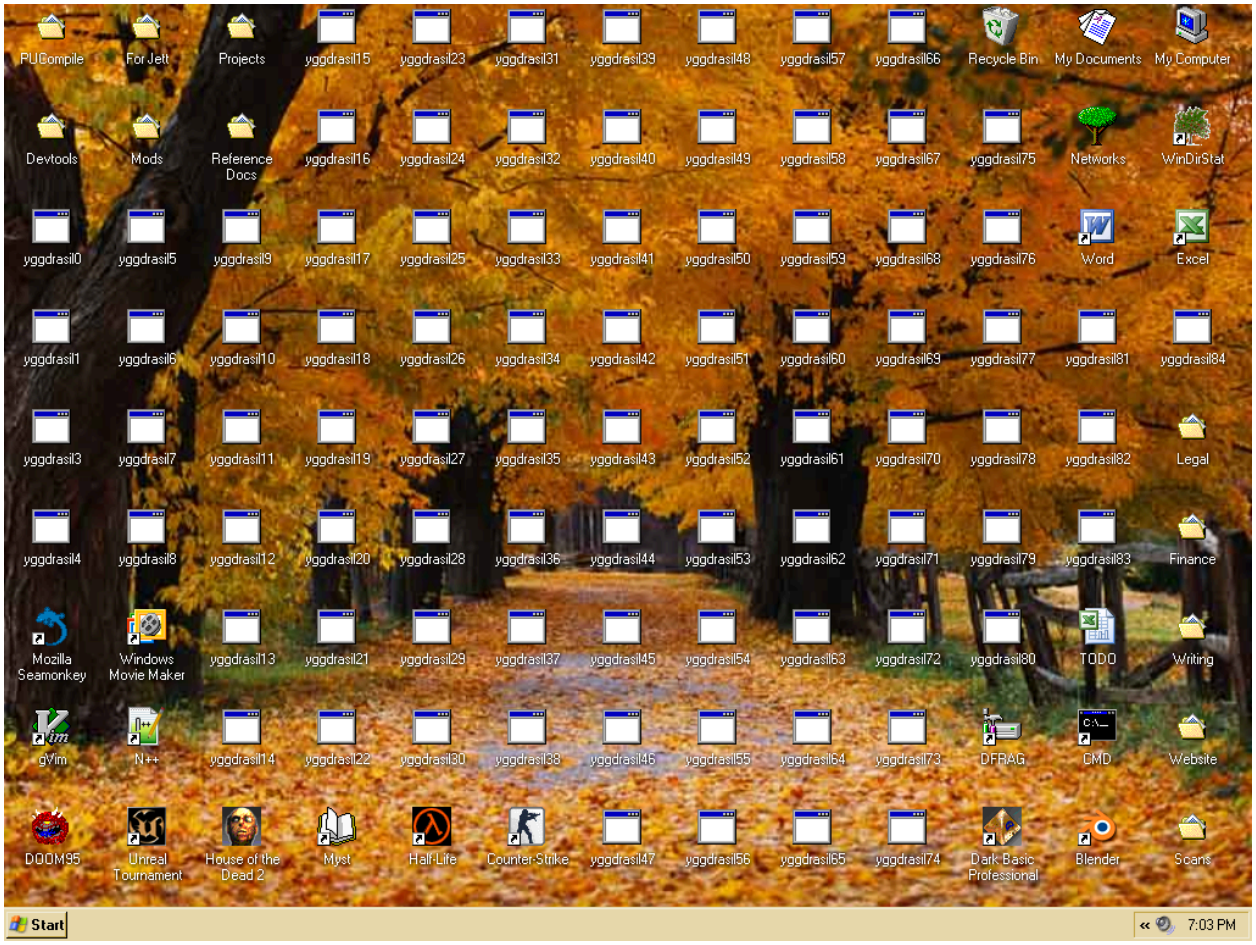
YGGDRASIL cared not either way, instead anchored onto my desktop by thousands upon thousands of bytes, as temporal winds blow its sands asunder, its origin point constantly in flux, the arced light of a quantum parabola bleeding magnet waves somewhere far, far away, and I, such a small and frail thing by comparison, was staring right into its event horizon.

I tried to sleep that night, but it never came.

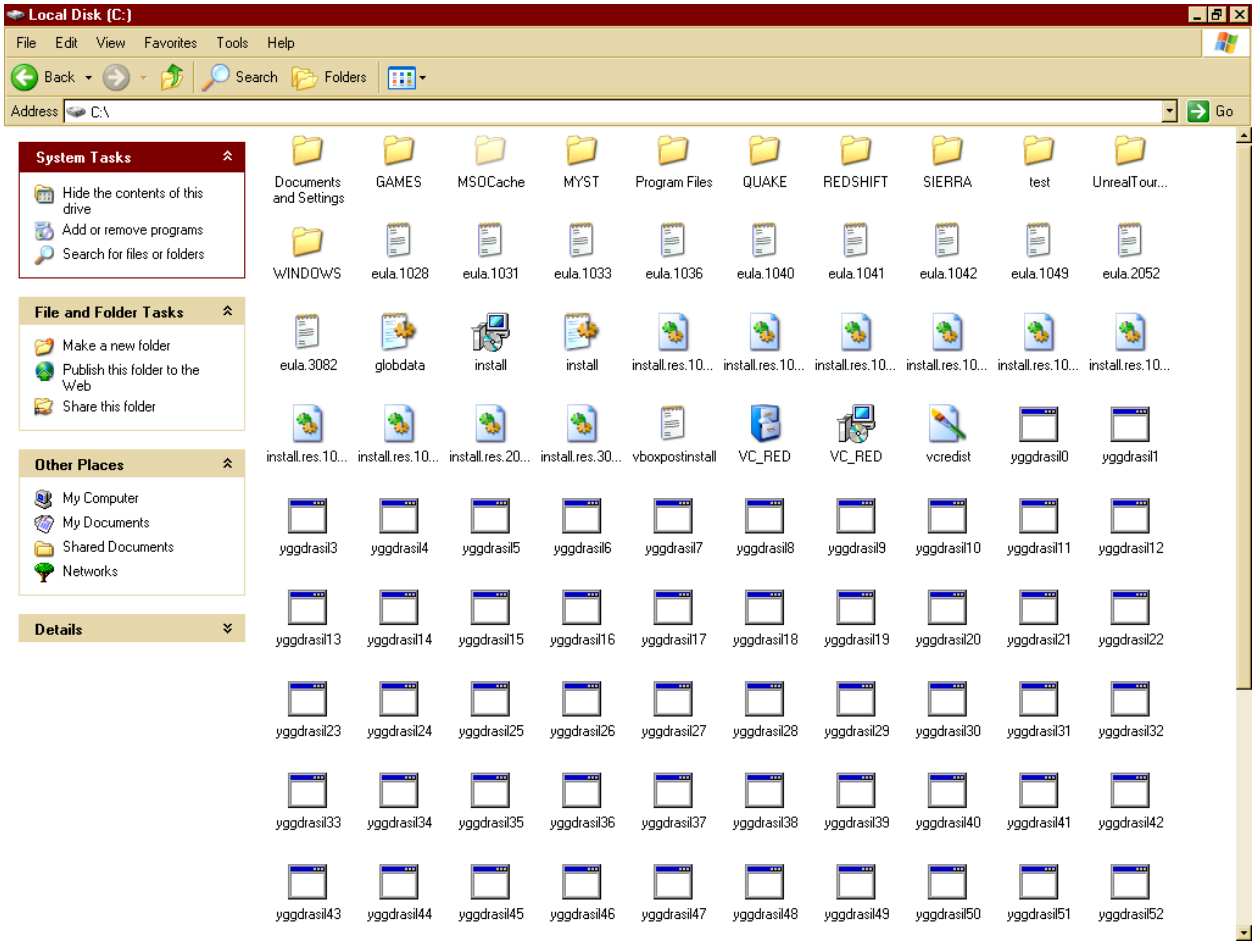
YGGDRASIL had its roots entrenched in the folds of my mind, their tentacle-like slithering pushing in and around my head where it did not belong, a parasitic network of vascular tissues burrowing and wrapping themselves deep into every crevice, trunks of wood and splinter protruding now so unnaturally into every wet crease.

At this point, I don't think I could've helped myself. What would you have done? Would it even have bothered you? You probably would have just reinstalled Windows and forgotten about it.

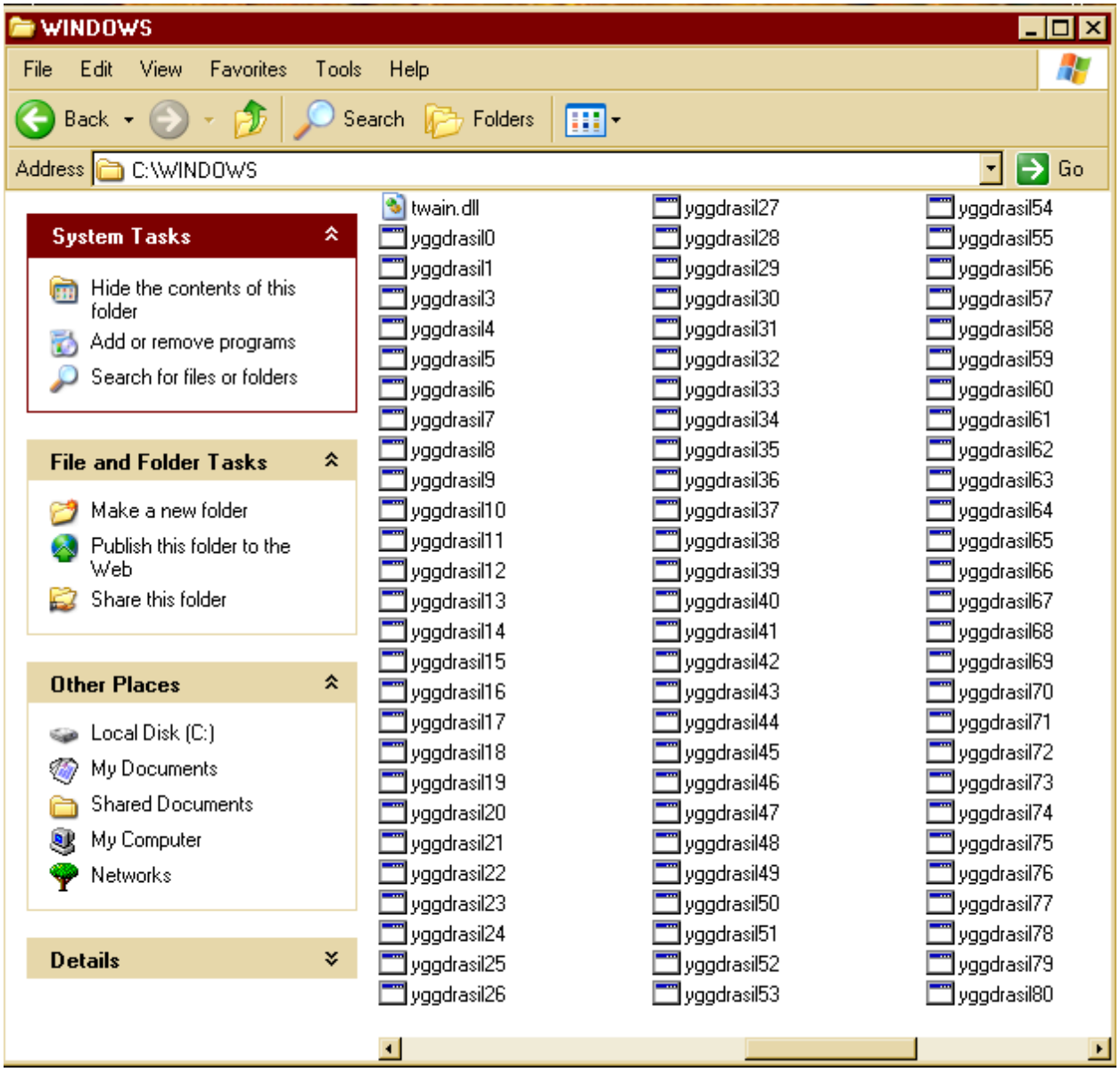
Believe me when I say that I envy you.



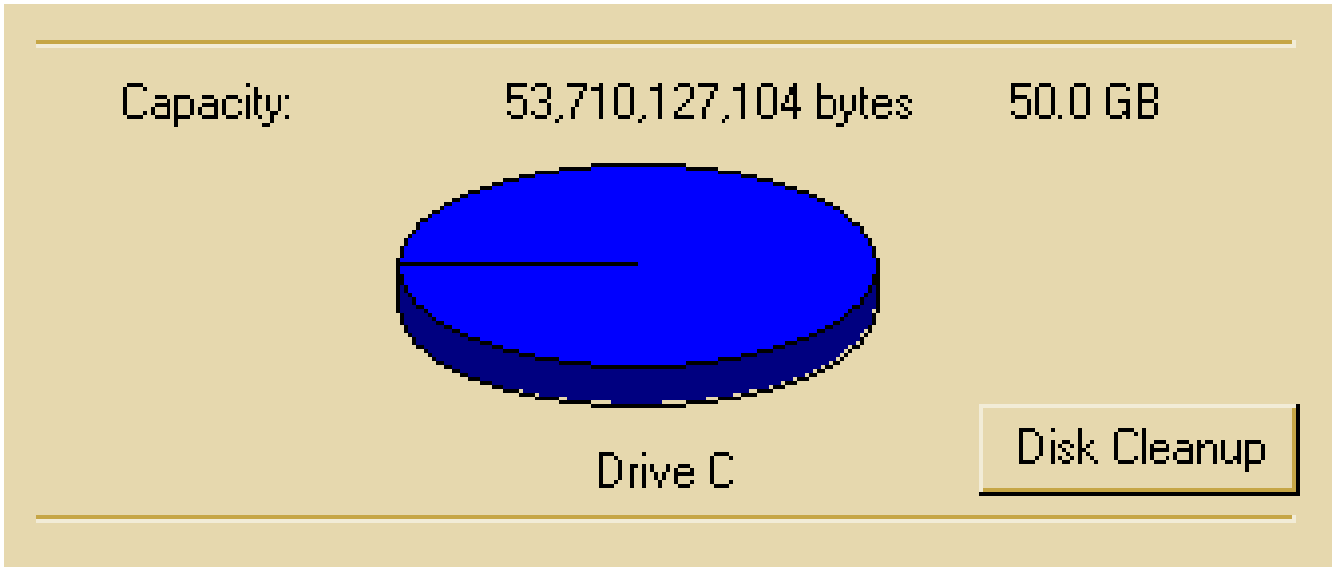
All it does, *is grow*.



And grow.


WINDOWS
File Edit View Favorites Tools Help
Back Search Folders
Address C:\WINDOWS
Go
System Tasks
Hide the contents of this folder
Add or remove programs
Search for files or folders
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Local Disk (C:)
My Documents
Shared Documents
My Computer
Networks
Details
twain.dll
yggdrasil0
yggdrasil1
yggdrasil3
yggdrasil4
yggdrasil5
yggdrasil6
yggdrasil7
yggdrasil8
yggdrasil9
yggdrasil10
yggdrasil11
yggdrasil12
yggdrasil13
yggdrasil14
yggdrasil15
yggdrasil16
yggdrasil17
yggdrasil18
yggdrasil19
yggdrasil20
yggdrasil21
yggdrasil22
yggdrasil23
yggdrasil24
yggdrasil25
yggdrasil26
yggdrasil27
yggdrasil28
yggdrasil29
yggdrasil30
yggdrasil31
yggdrasil32
yggdrasil33
yggdrasil34
yggdrasil35
yggdrasil36
yggdrasil37
yggdrasil38
yggdrasil39
yggdrasil40
yggdrasil41
yggdrasil42
yggdrasil43
yggdrasil44
yggdrasil45
yggdrasil46
yggdrasil47
yggdrasil48
yggdrasil49
yggdrasil50
yggdrasil51
yggdrasil52
yggdrasil53
yggdrasil54
yggdrasil55
yggdrasil56
yggdrasil57
yggdrasil58
yggdrasil59
yggdrasil60
yggdrasil61
yggdrasil62
yggdrasil63
yggdrasil64
yggdrasil65
yggdrasil66
yggdrasil67
yggdrasil68
yggdrasil69
yggdrasil70
yggdrasil71
yggdrasil72
yggdrasil73
yggdrasil74
yggdrasil75
yggdrasil76
yggdrasil77
yggdrasil78
yggdrasil79
yggdrasil80

…and grow.



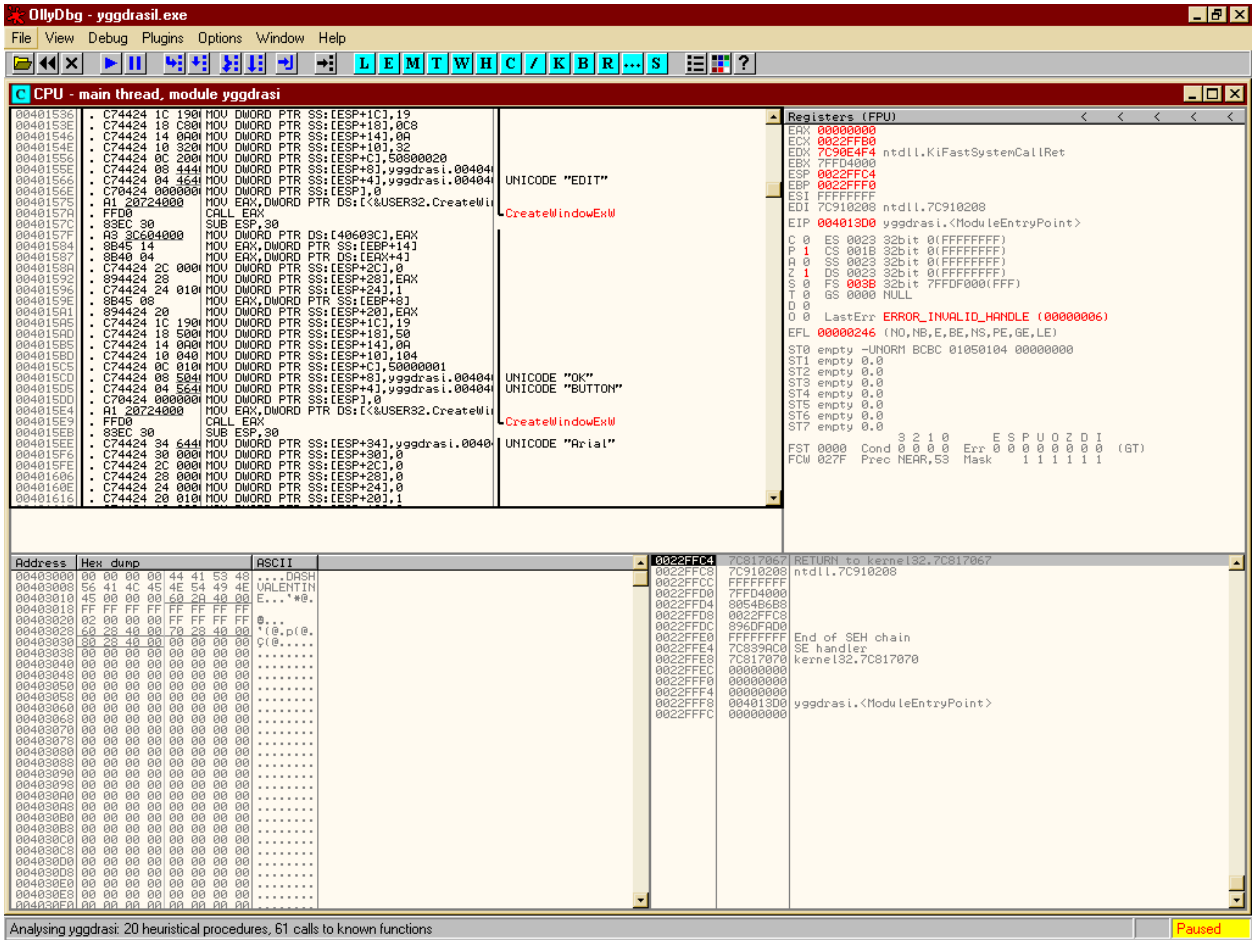
Had that been all it was, merely random bits of data on a mission to proliferate rapidly across my hard drive: I might have found it funny, endearing even. The thought that maybe this was some kind of tongue-in-cheek hoax, or perhaps an old student of mine trying to pull my leg one last time before I croak — I won't lie to you, it's a comforting thought, even now.

Heh, trying to test grandpa's operational security, *eh?* Well, you got me there, kid.

Were it that simple, then maybe I would be able to sleep in my final hours. Maybe I could spend time with people who cared for me, who loved me. I can see them now, my own family, sitting across from my hospital bed, casting worried looks in my direction, myself no doubt a sorry sight to their eyes: An old man decaying in the light of his laptop, lost between the ones and zeros.

Do you think they know? That I'm not here right now?

Of course, as you might have guessed by now: *things are never that simple*.



Address	Hex dump								ASCII
00403000	00	00	00	00	44	41	53	48	....DASH
00403008	56	41	4C	45	4E	54	49	4E	VALENTIN
00403010	45	00	00	00	60	2A	40	00	E...`*@.
00403018	FF	FF	FF	FF	FF	FF	FF	FF	
00403020	02	00	00	00	FF	FF	FF	FF	☻...
00403028	60	28	40	00	70	28	40	00	`(@.p(@.
00403030	80	28	40	00	00	00	00	00	Ç(@.....
00403038	00	00	00	00	00	00	00	00	....

Because there, *right there* in the very first few bits of **YGGDRASIL**: ***44 41 53 48 56 41 4C 45 4E 54 49 4E 45***, was my very own signature.

DASH VALENTINE

The very same signature that you will find should you pull a hex dump from PUCompile, or any software I've developed since then.

The signature that I sign every one of my programs with.

The same one I've always used since 1994, when I wrote my first program.

There it was, as evident and indisputable as information could be, the answer to my riddle, staring at me in the reflection of my screen the entire time.

There's no other explanation.

I wrote **YGGDRASIL**.

In the interest of preservation, I have uploaded **YGGDRASIL.EXE** in full to my SourceForge page.

Unfortunately, I do not have enough time left to complete my findings on the program.

This is where you come in, if you could grant an old dying soul one last wish.

I have no recollection of my development on **YGGDRASIL.EXE**, and also completely lack the source code that I *supposedly* wrote for it. While certainly a curiosity, it's not all *that* surprising that I have no memory of making it, considering my health and the medicine that they have me on. However, my program still seems to elude me.

All of my attempts to decompile the exe have been fruitless, and I just don't have the time to commit to decompilation. As much as I am driven by this compulsion to understand what I have created, even now I grow weary as my fingers type this. It's possible that I have *less* time than the doctor's might have let on, and in all honesty, that is the most likely scenario. It's hard to describe, but when you know, you know. It's a feeling. You can hear Death itself jingling around his keys, looking for the one that unlocks the door.

It's not something I feel is worth mentioning, either to my doctors or my family. What they don't know won't hurt them. Besides, *I'm tired. So very tired.* I could doze off now just closing my eyes.

My last wish from you all, is that one day a light will be shed on **YGGDRASIL.EXE**, and its true nature be revealed for all to see.

Whatever it is, whatever I did: I want it to be seen. To be understood.

I myself may never know, but it brings me some solace to think that, somewhere out there, far, far, far away, for thousands of miles, decades upon centuries from now: That there will come another mind to succeed mine, a sharper mind, another link in the chain, of a history far too great to be truly remembered, and understand something: *new.*

DASH VALENTINE

UPDATE 10/19/05

Hey yall, jett here.

Most of u probably don't know who i am. Some of u might know me for my online handle *pinecone64*. U might have played my games or seen my name under a contribution or 2 to some of dash's projects. i consider myself lucky enough to be close friends with a select few of u (U know who u are!! <3), especialy in that ive gotten to know some of yall so much better over the last couple years! dash had some really wonderful friends as it turns out :)

all that 2 say that there have been a lot of silver linings in dash's passing. i just wanted 2 say thank u to every1 who reached out to me, those of u who knew what he meant 2 me. I dont think i can ever repay yall for the goodness u have brought into my life. the hole that he left was a big one… i never thought it could b filled until yall became such a integral part of my life. please know that im glad beyond words

so for those of u who know, *thank you* :) <3 from the bottom of my heart

to those of you who dont know me or havent heard of me, dash was one of my best friends. i dont wanna speak for him as he has done SO MUCH speaking for himself already on this page!! XD and i wanna keep this update short, cuz this is not my page n all. but that being said, id like to think he would agree that we were best friends. i certainly saw him in that way. he was the closest friend i ever had. he had trouble showing it and was often very shy about his feelings, but he didnt have to be :) there would always be a certain look in his eye whenever i got him to laugh (and TRUST ME getting that asshole to laugh was NEARLY IMPOSSIBLE!!! X_X)

dash and i both care a lot for his privacy. wow, dash caring about privacy?? who would have thought an IT security guy would care about PRIVACY?? i know, major news flash there. joking aside though, my best friends privacy does matter a lot to me, so i dont want to go around kissing and telling on his behalf

all i can say is that we were *really* close :)

and yeah, i miss him.

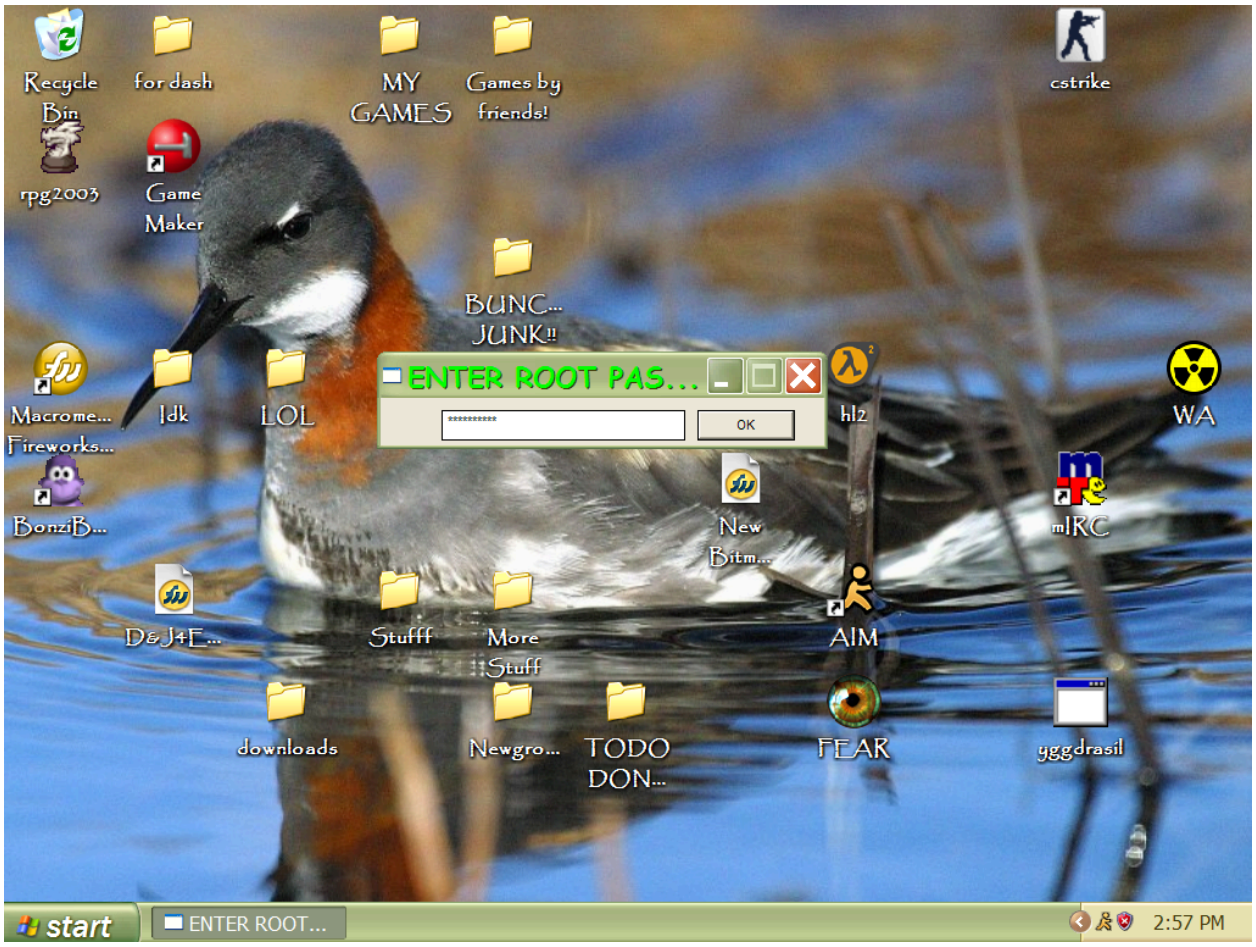
i miss him so much.

enough about my feelings though XD and let me cut to the chase! this post has kinda blown up on the SA forums and in other misc places around the web. i didnt feel like commenting in any of the discussion threads because it didnt really feel like *my* place.

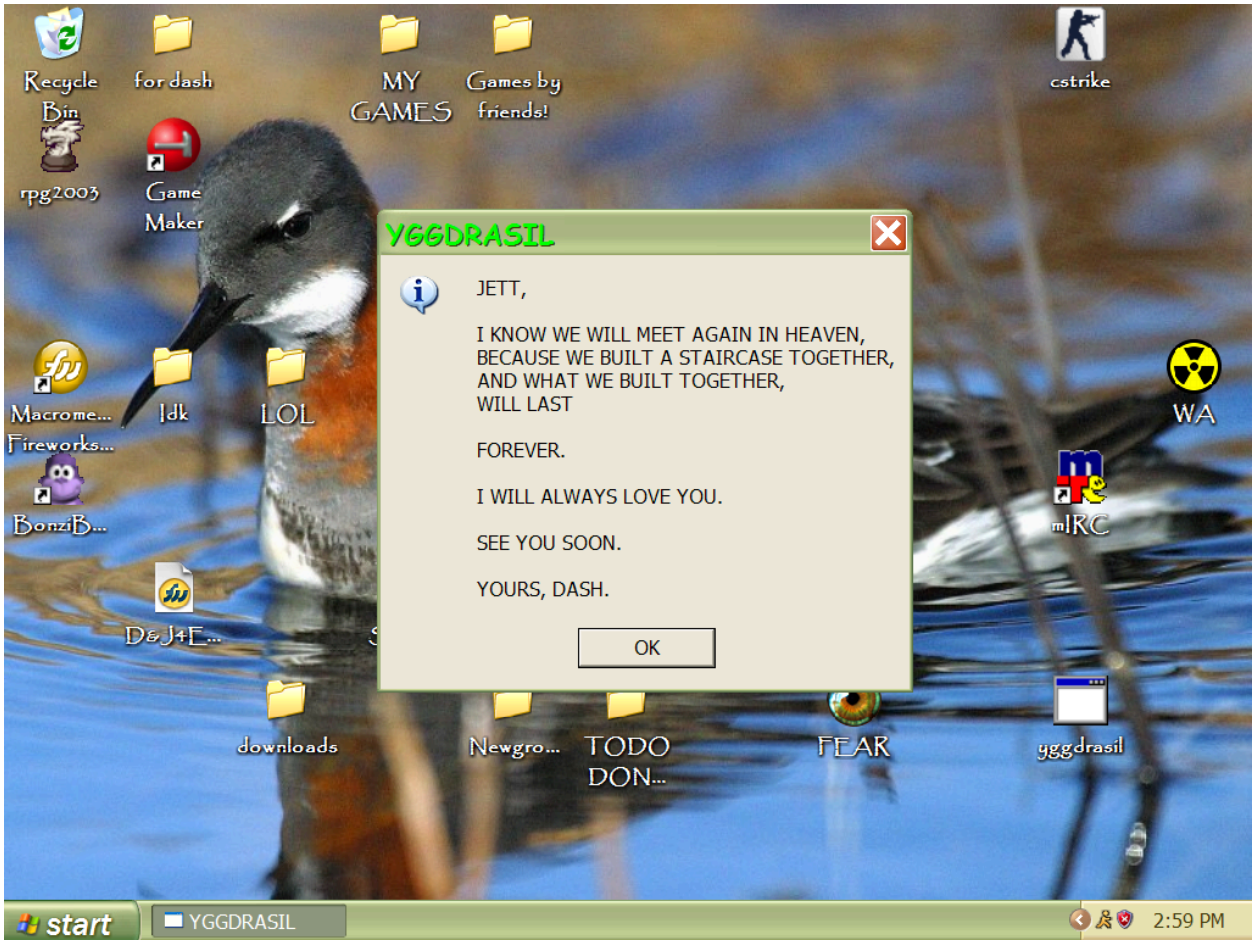
for a while i thought about posting this update. i actually went back and forth on it in my head A LOT bcuz i didnt know if it was right, or if dash would have wanted an update like this. he was a pretty private guy, and i dont think he wouldve wanted a buncha internet weirdos knowing the *real* him. the dash that *i* knew.

after what i found, i think its safe to say that he would be :)

besides, it is SO funny that he forgot *our special password*



the password we *always* used to logon to our private server



DASH ♥ JETT
4EVER