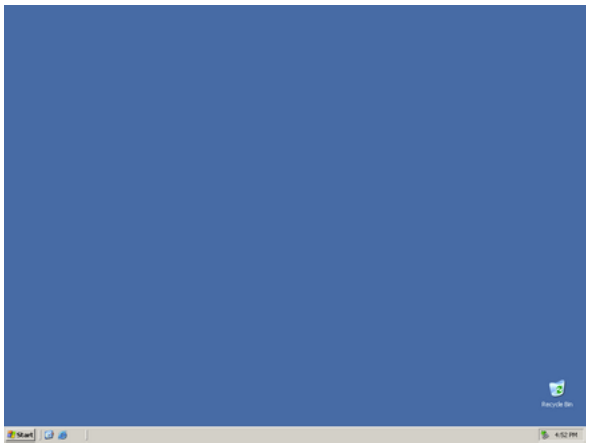
Windows Research Kernel

5.2.3800.1807.WRKP1.2(daveprobert)

Build of Windows Server 2003



OS family	Windows NT
Version number	5.2
Build number	3800
Build revision	1807
Architecture	x86, AMD64
Build lab	WRKP1.2(daveprobert)
Compiled on	2006-06-22

About dialog

The **Windows Research Kernel** (*WRK, Microsoft Windows Academic Operating System*) is a portion of the source code of Windows Server 2003 Service Pack 1 kernel, which was released publicly in 2009. It was used primarily in universities, academies and scientific centers for investigating and researching the Windows NT kernel structure and working principles.

WRK contains near-full realization of the Service Pack 1 kernel (and, probably, future updates of existing functions), with partially missing pieces of source code (which can be recovered using the Windows Server 2003 RTM kernel and included libraries). Excluded sources are primarily in the areas of plug-and-play, power management, the device verifier, kernel debugger interface, and virtual DOS machine (VDM).

Internal preliminary definitions and grammar mistakes have been fixed, removed original credentials of

Contents

Description

Besides kernel source code, WRK includes following:

- Hardware Abstraction Layers (HAL) of Windows Server 2003 SP1 for x86 systems, and their PDB debugging files, such as:
  - ACPI compatible EISA/ISA (`halacpi.dll`),
  - ACPI 1.0 - APIC platform (`halmacpi.dll`),
  - MPS 1.4 (`halmps.dll`),
- VGA boot driver (`bootvid.dll`), along with its pre-compiled library,
- Application Compatibility database interface module, with its pre-compiled library (SDBAPI),
- Resource file for `ntoskrnl.exe` (`ntoskrnl.res`), containing build number, development lab and date of compilation,
- WRK specific libraries: `ntoswrk.lib` and `ntosarch.lib`, containing all missing implementations,
- Documentation for working with WRK, e.g. compilation and modification, among with Windows Kernel internals,
- Batch script (*`.bat`*) to copy WRK into a specific destination (by default, into root of **C:** disk).

The `ntoswrk.lib` is the largest library in Research Kernel, as it contains all implementations of functionality, which is not included as source code, such as HAL implementations and other corresponding functions of kernel, largely used by WRK and defined into header files. Over 10 unincluded and new files have been identified from this library (i386 version), in comparison with Windows Server 2003 RTM kernel structure, among with 184 files which exist in RTM source code, but likely have been changed or excluded. However, these implementations do not fully comply with the original Windows Server 2003 SP1 kernel, as most of them bypass critical calls involving the Processor Control Region (PCR), the Processor Control Block (PRCB), and other kernel-internal components.

The resulting image has a build number of 3800.1807, while the included HAL images contain the likely canonical build number - 3790.1807. This version is hardcoded inside initialization code located at `ntoswrk.lib`, and it requires manual patching or modification of RTM kernel. It also bears a specific build lab — `WRKP1.2(daveprobert)`, assuming that the WRK is a private compile, published by Microsoft employee Dave Probert, who was working at Microsoft's NT kernel subdivision as of compilation[1].

To compile WRK, you must initiate it's environment primarily at `C:\WRK-v1.2`, by copying or extracting that folder in root of `C:\` or another disk you prefer. Next, open Command Prompt (cmd.exe) and navigate to WRK folder, after which run command initializing environment:

```
C:\WRK-v1.2>wrkenv.bat [x86 or amd64]
```

If you won't specify any architecture, by default WRK environment will initialize itself for x86 machines, but you can append **`amd64`** at the end of command and run it for AMD64 systems. After that, build WRK by running this command:

```
C:\WRK-v1.2>build.bat
```

This command will build kernel by using pure NMake ruleset and pre-compiled libraries. Resulted output will be stored on `base\ntos\BUILD\EXE` folder.

Booting

To run the kernel, a Windows XP Professional x64 Edition or Windows Server 2003 SP1 machine is required, because of the boot loader and session manager incremental changes, which resemble only SP1 versions and newer. Additional patches are need to run it on Windows XP SP1 and Windows Server 2003 RTM. Windows Server 2003 SP2 and later versions are not supported by WRK.

To boot the target system with WRK, the compiled kernel file must be copied (`wrkx86.exe` for x86, or `wrkamd64.exe` for AMD64). For x86 systems, it is also needed to copy `halacpim.dll` or other HAL files included in the WRK (such as `halmacpi.dll` and `halmps.dll`) into `C:\Windows\System32`.

Then, a new boot record in `boot.ini` should be created.

`boot.ini` boot record [Expand]

After adding the boot record, restart the virtual machine and choose the WRK boot entry.

References

1. From August 1996 to March 2011, Dave Probert worked on core kernel architecture of NT Kernel, including heterogeneous parallel and energy efficient computing, threading/processes, notifications, services, programming models and more. https://www.linkedin.com/in/daprobert/details/experience/