

Forum:[Hack Forums](#)

Thread: [Getting unicode back from console commands](#)

Keat - February 21, 2019, 2:36 pm

I am trying to use `CreateProcessW()` to run `cmd.exe` and run commands. I am then trying to get unicode back so I can support all languages.

I have working code that does what I need it to. The issue I am running into is only built in command prompt commands will output unicode with the `"/u"` argument given.

```
Code WCHAR works[] = L"cmd.exe /u /c dir C:\\windows";
WCHAR dont[] = L"cmd.exe /u /c ipconfig";
```

```
BOOL fSuccess = CreateProcessW(NULL, dont, NULL, NULL, TRUE,
CREATE_NEW_CONSOLE, NULL, NULL, &si, &pi);
```

Works - will give me back unicode.

don't - will not give me unicode

I have taken a picture of the bytes it returns back to me.

This is "works". It shows that I am getting unicode back.

<https://i.imgur.com/KQepszB.png>

This is "dont". Showing it only gives me ANSI.

<https://i.imgur.com/YKpSqrU.png>

Does anyone know of a better way to go about what I am trying to accomplish. I am basically going to end up building a pseudo remote shell. I want the user to be able to send commands and get the output, but support on non English computers as well.

Full test code that is handling this:

Code `#include <Windows.h>`

```
void main() {
    HANDLE hPipeRead, hPipeWrite;

    SECURITY_ATTRIBUTES saAttr = { sizeof(SECURITY_ATTRIBUTES) };
    saAttr.bInheritHandle = TRUE;
    saAttr.lpSecurityDescriptor = NULL;

    if (!CreatePipe(&hPipeRead, &hPipeWrite, &saAttr, 0))
        return;
```

```
STARTUPINFO si = { sizeof(STARTUPINFO) };
si.dwFlags = STARTF_USESHOWWINDOW | STARTF_USESTDHANDLES;
si.hStdOutput = hPipeWrite;
si.hStdError = hPipeWrite;
si.wShowWindow = SW_HIDE;
```

```
PROCESS_INFORMATION pi = { 0 };
```

```
WCHAR works[] = L"cmd.exe /u /c dir C:\\windows";
WCHAR dont[] = L"cmd.exe /u /c ipconfig";
```

```
BOOL fSuccess = CreateProcessW(NULL, dont, NULL, NULL, TRUE,
CREATE_NEW_CONSOLE, NULL, NULL, &si, &pi);
```

```
if (!fSuccess) {
    CloseHandle(hPipeWrite);
    CloseHandle(hPipeRead);
    return;
}
```

```
BOOL bProcessEnded = FALSE;
for (; !bProcessEnded;) {
```

```
    bProcessEnded = WaitForSingleObject(pi.hProcess, 50) == WAIT_OBJECT_0;
```

```
    while (TRUE) {
        CHAR *buf = NULL;
        DWORD dwRead = 0;
        DWORD dwAvail = 0;

        if (!PeekNamedPipe(hPipeRead, NULL, 0, NULL, &dwAvail, NULL))
            break;

        if (!dwAvail)
            break;
        buf = HeapAlloc(GetProcessHeap(), 0, dwAvail);
        if (buf == NULL) {
            return;
        }

        if (!ReadFile(hPipeRead, buf, dwAvail, &dwRead, NULL) || !dwRead)
            break;
```

```
    }
}
```

```
CloseHandle(hPipeWrite);
CloseHandle(hPipeRead);
CloseHandle(pi.hProcess);
CloseHandle(pi.hThread);
return;
```

```
}
```

0xDEAD10CC - February 21, 2019, 4:46 pm

First, why are you using void main()???

Here's what the help says about the /U flag:

Code /U Causes the output of internal commands to a pipe or file to be Unicode

You're also using File I/O rather than Console I/O API's to deal with the data. This is a point of failure. Read what Python does: <https://www.python.org/dev/peps/pep-0528/>

And programs like ConEmu (which is what I use) tend to do a lot more with intercepting such calls, but they also implement this properly.

You'll see notes about ReadConsoleW/WriteConsoleW. The flag only works really on internal programs because you can tell the program to format it in such a way while you can't really do the same for external programs. There's lots of information on tricks people have used though.

Keat - February 21, 2019, 5:23 pm

(Feb 21, 2019 05:46 PM)0xDEAD10CC Wrote: [\[CITE\]](#) First, why are you using void main()???

Here's what the help says about the /U flag:

Code /U Causes the output of internal commands to a pipe or file to be Unicode

You're also using File I/O rather than Console I/O API's to deal with the data. This is a point of failure. Read what Python does: <https://www.python.org/dev/peps/pep-0528/>

And programs like ConEmu (which is what I use) tend to do a lot more with intercepting such calls, but they also implement this properly.

You'll see notes about ReadConsoleW/WriteConsoleW. The flag only works really on internal programs because you can tell the program to format it in such a way while you can't really do the same for external programs. There's lots of information on tricks people have used though.

I am using void main() because this was originally in another function but I just renamed it to main to just test. This isn't actual full code.

And I am trying to do this without ConEmu or any external stuff.

0xDEAD10CC - February 21, 2019, 7:28 pm

(Feb 21, 2019 06:23 PM)Keat Wrote: [\[CITE\]](#) I am using void main() because this was originally in another function but I just renamed it to main to just test. This isn't actual full code.

And I am trying to do this without ConEmu or any external stuff.

You didn't understand what I was saying about using ConEmu though. You could use ComEmu as a resource to understand how some of these things can be done.