Proof of Concept (PoC) Report: Hex2dec NotMyFault

Intern Name: Krushang Tanti

Internship ID: 451

Date: July 2025

1. Executive Summary

NotMyFault is a diagnostic tool developed by Sysinternals (part of Microsoft) to simulate system crashes, hangs, memory leaks, and kernel-mode crashes in Windows. It is primarily used by developers, system administrators, and cybersecurity professionals to test system stability, analyze kernel dump files, and understand how Windows handles failures. The tool provides controlled fault injection to generate BSODs (Blue Screens of Death) for educational or debugging purposes.

2. Tool Overview

- **Name:** NotMyFault
- **Developer:** Mark Russinovich / Sysinternals (Microsoft)
- **Platform:** Windows
- **Purpose:** Simulates crashes (BSOD), system hangs, memory leaks, stack overflows, etc.
- **Use Cases:** Kernel debugging, crash dump analysis, driver failure testing, system crash response testing.
- **Versions:** Available in GUI, Command-line, and mobile (Sysinternals Live) variants.

3. Benefits of Using These Tools

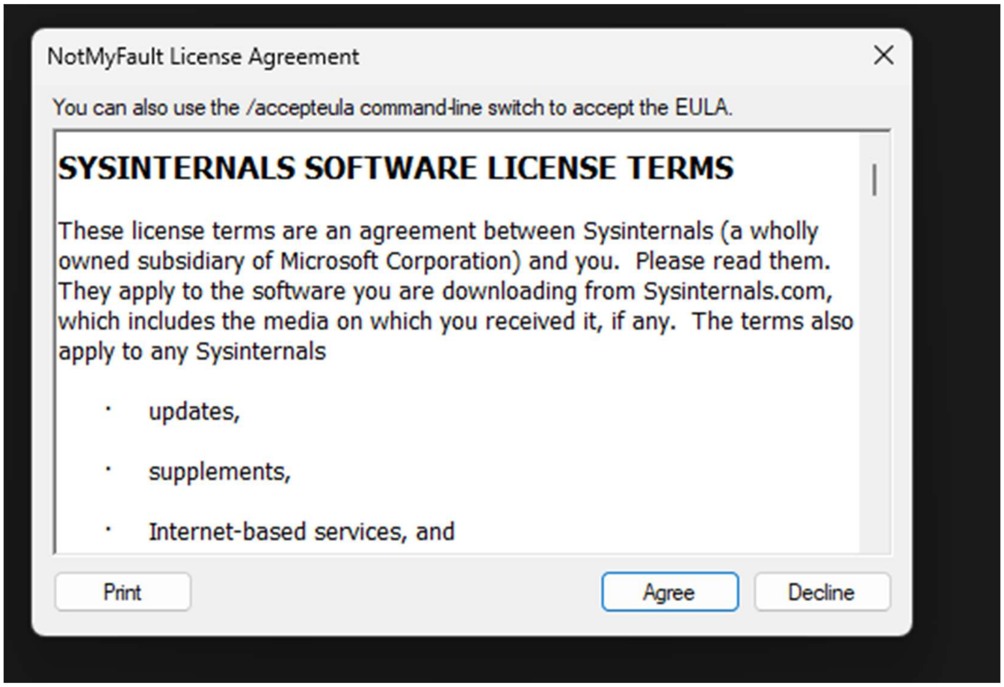
- Allows safe simulation of kernel crashes for **training or research**.
- Helps in **analyzing crash dumps (minidumps)** generated by the system.
- Useful for **developing and testing kernel-mode drivers**.

- Assists in teaching **how Windows handles system failures**.
- Compatible with **Windows debugging tools** like WinDbg.
- Useful in **cybersecurity and incident response exercises**.

4. Proof of Concept: Visual Walkthrough

Step-by-step usage of NotMyFault:

1. **Download** from Sysinternals: https://learn.microsoft.com/en-us/sysinternals/downloads/notmyfault



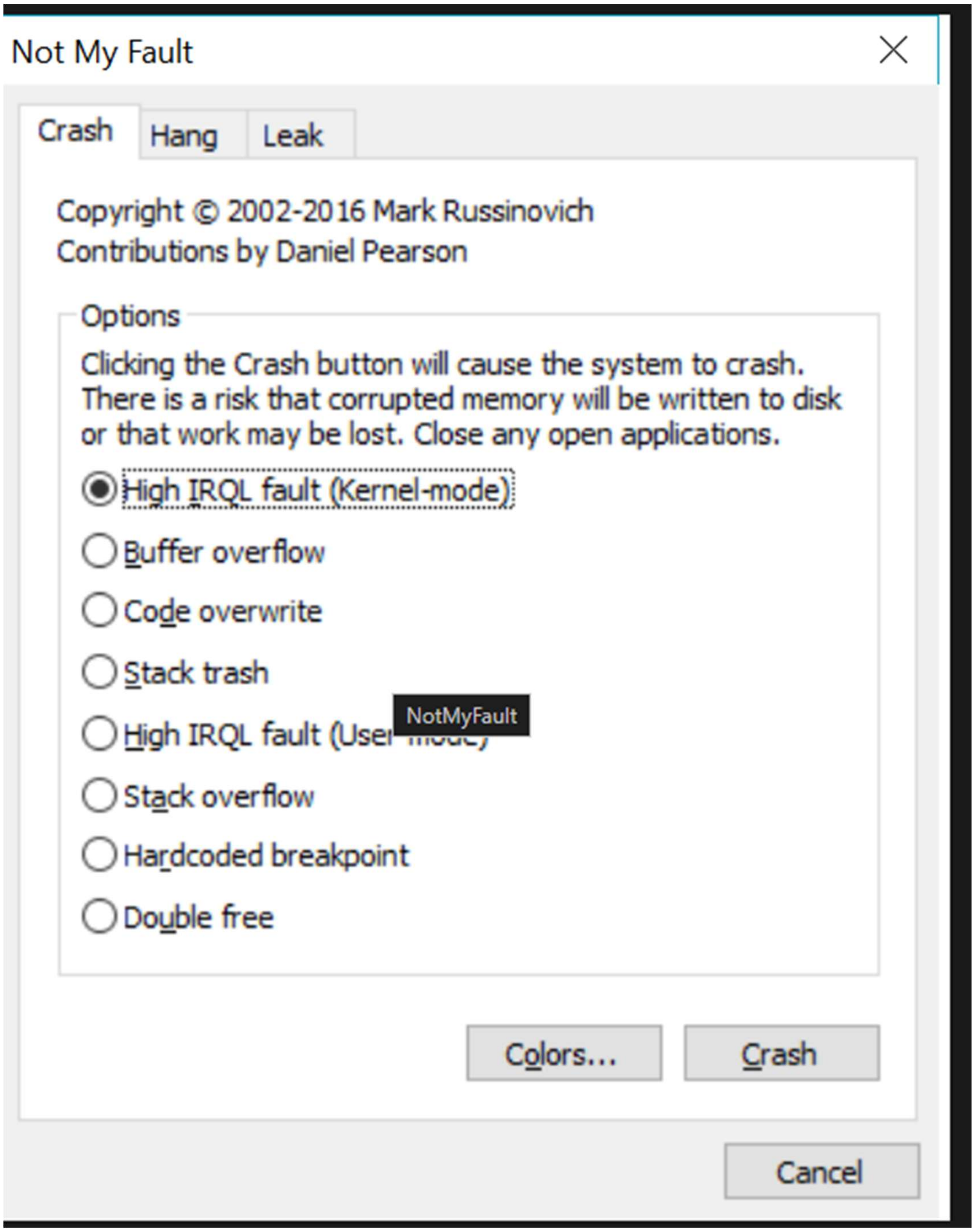
You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

2. **Run as Administrator**: Launch `NotMyFault.exe`.
3. **Choose Crash Type**:
   - Memory leak
   - Stack overflow
   - High IRQL fault
   - Buffer overrun
   - Deadlock simulation
4. **Trigger Fault**: Click "Do Bug" or “Leak Memory” depending on the test.
5. **Observe**: System will crash, freeze, or hang based on selected fault.
6. **Post-crash**: Analyze the generated `MEMORY.DMP` file using WinDbg or similar tools.

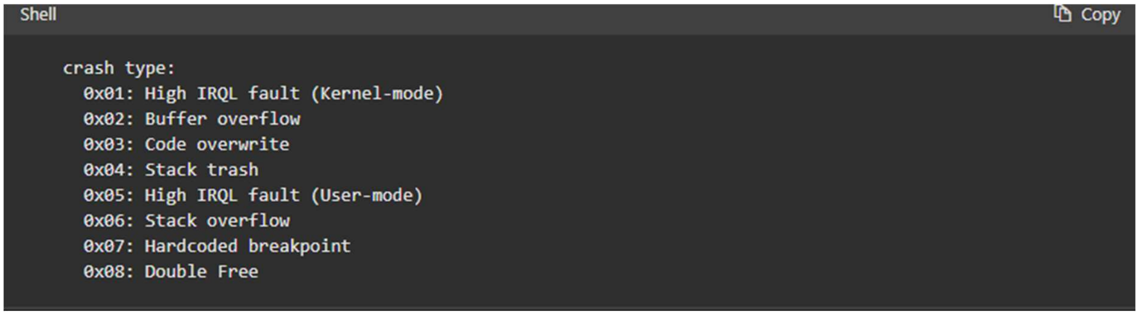


Copyright © 2002-2016 Mark Russinovich
Contributions by Daniel Pearson

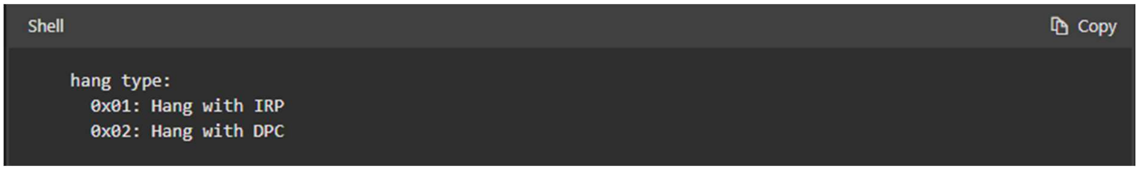
Options

Clicking the Crash button will cause the system to crash. There is a risk that corrupted memory will be written to disk or that work may be lost. Close any open applications.

● High IRQL fault (Kernel-mode)
○ Buffer overflow
○ Code overwrite
○ Stack trash
○ High IRQL fault (User-mode)
○ Stack overflow
○ Hardcoded breakpoint
○ Double free



```
crash type:
  0x01: High IRQL fault (Kernel-mode)
  0x02: Buffer overflow
  0x03: Code overwrite
  0x04: Stack trash
  0x05: High IRQL fault (User-mode)
  0x06: Stack overflow
  0x07: Hardcoded breakpoint
  0x08: Double Free
```



```
hang type:
  0x01: Hang with IRP
  0x02: Hang with DPC
```

5. Summary Table

Feature	Description
Developer	Sysinternals (Microsoft)
Tool Name	NotMyFault
Function	Simulates system crashes & hangs
Usage	Debugging, Training, Testing, Cybersecurity
Required Privileges	Administrator
Output	BSOD, memory dumps
Availability	Free
Platform	Windows only

6. Time to Use / Scenarios

Scenario	When to Use NotMyFault
Kernel Debugging Training	To generate BSODs for dump analysis practice
Crash Dump Analysis Testing	To produce dumps for forensic research
Driver Development	To simulate failures caused by buggy drivers
Incident Response Drills	For controlled crash simulations
Red Team / Blue Team Exercises	For system failure simulation in attack/defense labs
Teaching System Internals	To visually demonstrate how Windows handles crashes

7. Good About These Tools

- Lightweight and **no installation required**.
- Developed by **Microsoft**, highly trusted.
- Can **safely simulate crashes** without harming hardware.
- Provides a **realistic test environment**.
- Supports both **manual GUI** and **scripted command-line** operations.
- Generates data usable by **Windows Debugging Tools**.

8. Conclusion

NotMyFault is an essential utility for anyone working in **system-level software, driver development, or cybersecurity**. Its ability to simulate kernel crashes in a controlled environment makes it invaluable for testing system resilience, teaching operating system behavior, and preparing for real-world crash scenarios. While it should never be used on production machines, its use in labs, classrooms, and forensic settings is highly recommended.