**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.

1. **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.

1. **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**.

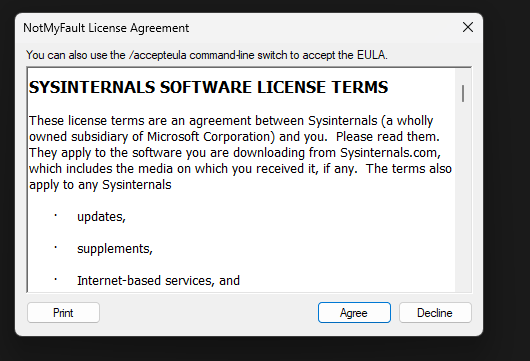
 Compatible with **Windows debugging tools** like WinDbg.

 Useful in **cybersecurity and incident response exercises**.

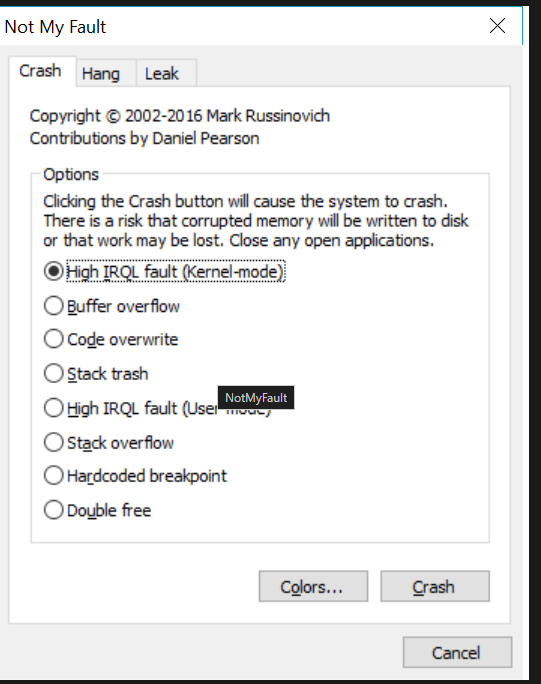
1. **Proof of Concept: Visual Walkthrough**

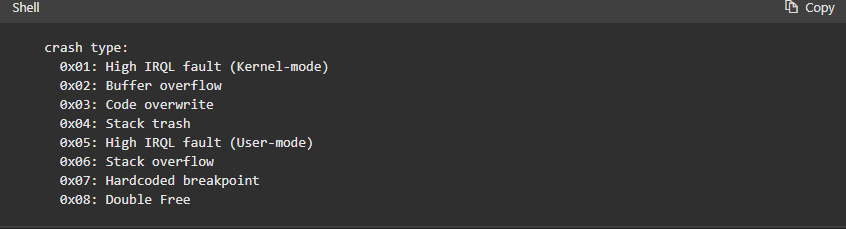
**Step-by-step usage of NotMyFault:**

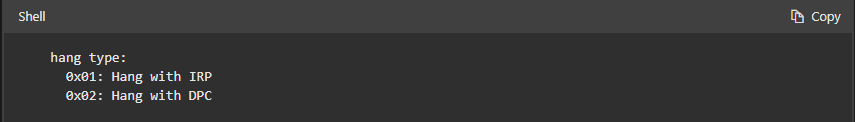
1. **Download** from Sysinternals: <https://learn.microsoft.com/en-us/sysinternals/downloads/notmyfault>



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







1. **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 |

1. **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 |

1. **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**.

1. **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.