Himanshu Chauhan

Windows Escalation/Debug Engineer - Microsoft
Kernel & User-Mode Debugging | C/C++ | Windows Internals

Bangalore, India
+91 9418575661
https://www.hichauhan.in/
hichauhan.in@gmail.com
https://www.linkedin.com/in/himanshu4186/

PROFESSIONAL SUMMARY

Windows Escalation/Debug Engineer with 5 years at Microsoft, specializing in Windows internals, kernel and user-mode debugging, C/C++ systems programming, Windows drivers, networking, and performance analysis. Experienced in diagnosing complex Windows failures through source-level code analysis, WinDbg crash and live debugging, ETW trace analysis, Time Travel Debugging, and Windows Performance Toolkit. Hands-on experience with WDM, KMDF, UMDF, IRP/IRQL, synchronization, memory management, I/O, WFP, and NDIS, with a strong foundation in TCP/IP and enterprise netowkting and security technologies. Leads high-impact technical escalations, partners with product engineering on defect qualification and fix validation, mentors engineers, and builds AI-assisted diagnostic tooling to improve engineering productivity and troubleshooting.

SKILLS / TECHNICAL PROFICIENCIES

Windows Internals & OS: Windows APIs, Processes/Threads, scheduling, thread pools, virtual memory, pool allocation, object & handles, synchronization, IRQL, I/O subsystem, IRPs, device stacks, user/kernel-mode transitions
C/C++ & Systems Programming: C, C++, multithreaded systems, data structures, thread synchronization, memory management, low-level debugging, x86/x64 assembly, registers, calling conventions
Windows Debugging & Performance: WinDbg, MEX, kernel/user-mode debugging, crash dumps, bugcheck analysis, memory corruption, heap/resource leaks, hangs/deadlocks, Time Travel Debugging, ETW, WPR, WPA, Procmon.
Windows Drivers: WDK, WDM, KMDF, UMDF, file-system minifilters, registry filter drivers, IOCTLs, IRP dispatch/completion, driver tracing and instrumentation
Windows Networking: TCP/IP, DNS, DHCP, NDIS, Windows networking stack internals (afd.sys, tcpip.sys, ndis.sys, http.sys), HTTP.sys, IPsec, VPN, TLS/Schannel, SMB/DFS, Virtualization and SDN, Packet and protocol analysis, Wireshark/Netmon/Netsh Analysis.
Security & Identity: PKI, certificates, TLS, Kerberos, NTLM, Active Directory, LDAP, 802.1X/RADIUS, security hardening, enterprise security troubleshooting
Engineering & Automation: Python, PowerShell, ETW-based diagnostics, diagnostic automation, AI-assisted engineering tooling, source-level defect analysis, technical design reviews

PROFESSIONAL EXPERIENCE

Windows Escalation Engineer - Microsoft — APRIL 2026 to Present

- Own complex Windows-platform escalations spanning kernel, drivers, user mode, memory, I/O, networking, and performance, providing code-level technical qualification between support and product engineering.
- Review Windows C/C++ source code to trace execution paths, validate defect hypotheses, analyze error handling, and identify root causes.
- Perform kernel and user-mode debugging using WinDbg/MEX, analyzing crashes, bugchecks, hangs, deadlocks, memory corruption, resource leaks, and synchronization issues.
- Use Time Travel Debugging and ETW/WPR/WPA to reconstruct intermittent failures and investigate performance, CPU, I/O, and latency regressions.
- Analyze x86/x64 assembly, registers, call stacks, and optimized code when required to correlate runtime behavior with source implementation.
- Debug Windows driver issues involving IRPs, IRQL, synchronization, and device-stack behavior, and drive qualified defects through engineering triage, fix validation, and regression verification.
- Authored and reviewed design change requests, assessing proposed changes for reliability, compatibility, servicing impact, and long-term supportability.
- Lead Severity-1 and critical incidents, collaborating with product engineering and development teams while mentoring engineers and improving escalation quality.
- Built and drove adoption of AI-assisted diagnostic tooling and engineering workflows.

Support Escalation Engineer - Windows Networking - Microsoft — JULY 2025 to MAR 2026

- Advanced to Tier 3 escalation ownership, resolving the highest-complexity Windows networking and identity failures, handling roughly two active cases per day and 300+ escalations during the role.

- Owned near-daily Severity 1 and critical-situation escalations end to end, engaging product engineering early and representing the technical position to customer engineering and leadership.
- Gained access to Windows product source code and applied C programming fundamentals to analyze production networking-stack and driver code, trace faulty code paths, and validate defect hypotheses at source level.
- Extended investigations beyond configuration and protocol analysis into code-level root cause analysis, using ETW/WPA to reconstruct failures across network, driver, and different components.
- Partnered with product engineering to file, triage, and validate defects, driving qualifying issues to resolution.
- Served as technical lead and SME for aligned engineers; conducted 200+ technical case reviews, owned Windows Networking accreditation, participated in technical interviews, and delivered mentoring, workshops, and technical training
- Trained for Windows Escalation Engineering Role focused on Windows internals, C/C++ Programming, debugging methodology, and code-level root cause analysis.
  Designed and presented an agentic AI adoption strategy to CVP-level leadership, demonstrating integration of AI agents into day-to-day engineering workflows.

Support Engineer – Networking and Active Directory - Microsoft SEPT 2021 to JUNE 2025

- Served as primary technical owner for enterprise and Premier/Unified Support customers and resolved 1,000+ enterprise Windows networking and Active Directory incidents across large-scale customer environments.
- Performed packet, protocol, and kernel-trace analysis across TCP/IP, DNS/DHCP, IPsec/VPN, TLS/Schannel, SMB/DFS, NDIS, and WFP.
- Led Severity-1 production outages end to end, coordinating customer engineering, product teams, and internal stakeholders through mitigation and root-cause analysis.
- Distinguished product defects from configuration and environmental issues, providing engineering teams with reproducible evidence, traces, and technical root-cause analysis.
- Expanded expertise into Active Directory and Identity and Authentication, Hyper-V virtual networking and SDN, while mentoring engineers and authoring technical diagnostic guidance.
- Authored public-facing and internal troubleshooting guides, diagnostic playbooks, and knowledge-base articles adopted across the support organization, reducing time to resolution.

Support Engineer Intern - Microsoft APR 2021 to JUL 2021

- Diagnosed Enterprise Windows Networking and Active Directory scenarios under senior-engineer supervision.
- Performed Windows performance triage using Event Viewer, Performance Monitor, Procmon, and Windows Performance Toolkit, documenting reproduction steps and findings for escalation to senior engineers.

AWARDS AND RECOGNITION

- India Excellence Award, Microsoft Windows Commercial (2025 and 2026)
- ACE Award, Star Achiever, Microsoft (2023)
- Pulse Award, Performance Adoption, Microsoft (2022)
- ACE Award Star Team, Microsoft (2022)

EDUCATION

MSc Data Science - Online	Manipal Academy of Higher Education	2026	9.20 - Ongoing
Bachelor of Engineering (Hons in cloud computing)	Chandigarh University	2021	8.70
Higher Secondary Education	DAV Public School	2017	9.20

CERTIFICATIONS

Microsoft AI Associate (AI 102)	**2025**
Microsoft Azure Fundamentals (AZ 900)	2025
Microsoft Data Fundamentals (DP 900)	2025
Software Defined Networking – QA Ltd	2025
Windows Internals (Pluralsight)	2026
Applied Machine Learning in Python (Coursera)	2026
Windows User Mode Debugging (UMD) – QA Ltd	2026