Future Instruction decoding support for Dyninst & GPU Decoding and Semantics

Attendees

- Ben Woodard
- James Kupsch
- Hsuan-Heng Wu
- Barton Miller
- Matin Raayai-Ardakani
- Bolo

Future Instruction decoding support for Dyninst

- Dynisnt tried to move to capstone for x86_64 instruction decoding

- Capstone is not fixed either. Capstone is trying to move to Zydis.

    Zydis is used as a backup when DynInst fails to get the instruction

    Zydis is purely x86, Capstone has support for ARM, Power and RISC-V.

Decision: - DynInst will try inserting Zydis for a couple of months to see if it works. Capstone 6.0.0 Alpha 10 will be used for other architectures.

- How to test? Different formatting, how to standardize? objdump

- Push vendors to provide decoding libraries (registers touched/memory access patterns …)

Future Instruction decoding support for Dyninst

GPU Decoding and Semantics

- Persuade NVIDIA to provide SASS semantics without them releasing everything.
    - Give decoder, encoder, registers touched (implicit/explicit).
    - Semantics is a step higher.
    - Instruction category.
    - Number of registers.
- Make NVDisasm a library, and provide a C/C++ interface for inspecting and modifying the ELF of the cubin.

More vector instruction decoding issues #402	Aug 30, 2017
“And we will switch to use Capstone for Power and ARM in the near future. I don't think we should spent too much time to fix this piece of code” — comments in #633	Aug 28, 2019
Capstone integration for x86 and x86-64 #638	Aug 26, 2019
Use Capstone for x86 instruction decoding #1646	Dec 14, 2023
Fix capstone (follow #1646) #2334	last week

Build static libs with PIC ✓ Documentation
#2836 by hainest Contributor was merged on Jan 3 • Review requir

Update read/written registers for x86 cmpxchg instru
#2821 by hainest Contributor was merged on Dec 2, 2025 • Review

Update read/written registers for x86 system call instructions ✓ LLVM-generated-files X86
#2820 by hainest Contributor was merged on Dec 1, 2025 • Review required 2 tasks done

Update read/written registers for x86 unconditional jump instructions ✓ LLVM-generated-files X86
#2800 by hainest Contributor was merged on Oct 31, 2025 • Review required 2 tasks done

Update read/written registers for x86 loop instructions ✓ LLVM-generated-files X86
#2799 by hainest Contributor was merged on Oct 30, 2025 • Review required 2 tasks done

Update read/written registers for x86 conditional jump instructions ✓ LLVM-generated-files X86
#2798 by hainest Contributor was merged on Oct 18, 2025 • Review required 2 tasks done

Update read/written registers for x86 interrupt return instructions ✓ LLVM-generated-files X86
#2793 by hainest Contributor was merged on Oct 4, 2025 • Review required 2 tasks done

Update read/written registers for x86 string instructions ✓ LLVM-generated-files Python X86
#2790 by hainest Contributor was merged on Oct 15, 2025 • Review required 2 tasks done

Update read/written registers for x86 procedure return instructions ✓ LLVM-generated-files X86
#2789 by hainest Contributor was merged on Oct 2, 2025 • Review required 2 tasks done

Update read/written registers for x86 enter/leave instructions ✓ X86
#2788 by hainest Contributor was merged on Oct 2, 2025 • Review required 2 tasks done

Add instruction details to cstest logging ✓ Python
#2787 by hainest Contributor was merged on Oct 4, 2025 • Review required 2 tasks done

Update read/written registers for x87 comparison instructions ✓ LLVM-generated-files X86
#2784 by hainest Contributor was merged on Sep 30, 2025 • Review required 2 tasks done

Update x86 operand access information

#1604 by mxz297 Contributor was merged on Dec 2, 2021 • Review required

What is Zydis

Open-source X86 & X86-64 decoder/disassembler library created by **Zyantific**, an open-source reverse-engineering development group.

Used by x64dbg, Firefox, Webkit, and HPCToolkit (when Dynisnt fails to decode)

Capstone plans to moving to Zydis for x86_64 support

Paths forward

	Capstone 5.0.9 May 28, 2026 Missing semantics from slide 2	Capstone 6.0.0-Alpha 10 July 21, 2026	Zydis
x86_64	**Improve coverage by 40+%** Won't get until they get a new x86 backend.		✔
aarch64	✔	✔	✘
ppc64le	✔	✔	✘
riscv (rva64)	✘	✔	✘

Or do we want a mix of Capstone + Zydis?

Considerations

Red Hat SystemTap: Packaging

AMD : Extra Dependency (or dependencies)

Dyninst :

- Maintain interface for both Zydis + Capstone
- and/or between Alpha/Beta/Release versions of Capstone

GPU Decoding and Semantics

GPU Semantics

- Persuade NVIDIA to provide SASS semantics without them releasing everything.
    - Give decoder, encoder, registers touched (implicit/explicit).
    - Semantics is a step higher.
    - Instruction category.
    - Number of registers.
- Make NVDisasm a library, and provide a C/C++ interface for inspecting and modifying the ELF of the cubin.