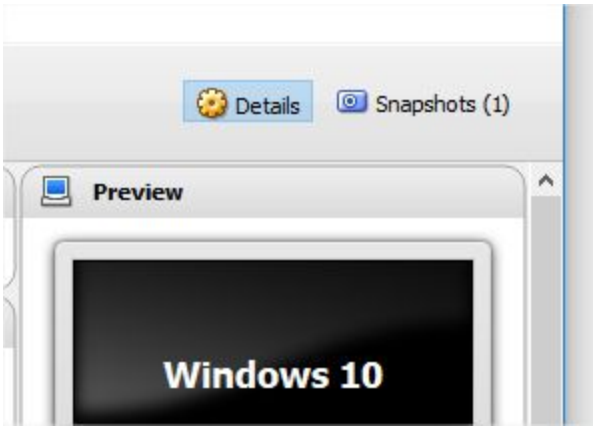
משימה 1 - Hello World!

היי - ברוכים הבאים למשימה הראשונה.
המטרה שלכם בשימה הזו היא לכתוב ולקמפל דרייבר בסיסי שיודע לעשות את הדברים הבאים:

1. לעלות באופן תקין
    a. להדפיס Hello World! כך שיודפס בDbgView
2. לרדת באופן תקין
    a. להדפיס Goodbye Cruel World כך שיודפס בDbgView

שימו לב - לפני שאתם מתחילים, צרו Snapshot לVM.
ניתן לעשות זאת בלשונית הSnapshots בVirtualBox

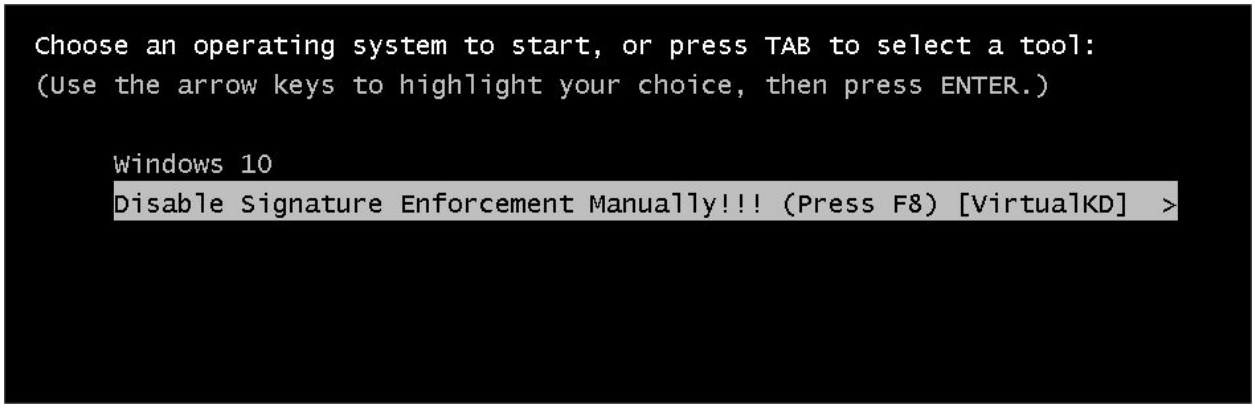


הורידו מכאן את הטמפלייט שבעזרתו תקמפלו את הדרייבר.
למשימה תצטרכו לקרוא על:

- DriverEntry
- Driver unload routine
- DbgPrint

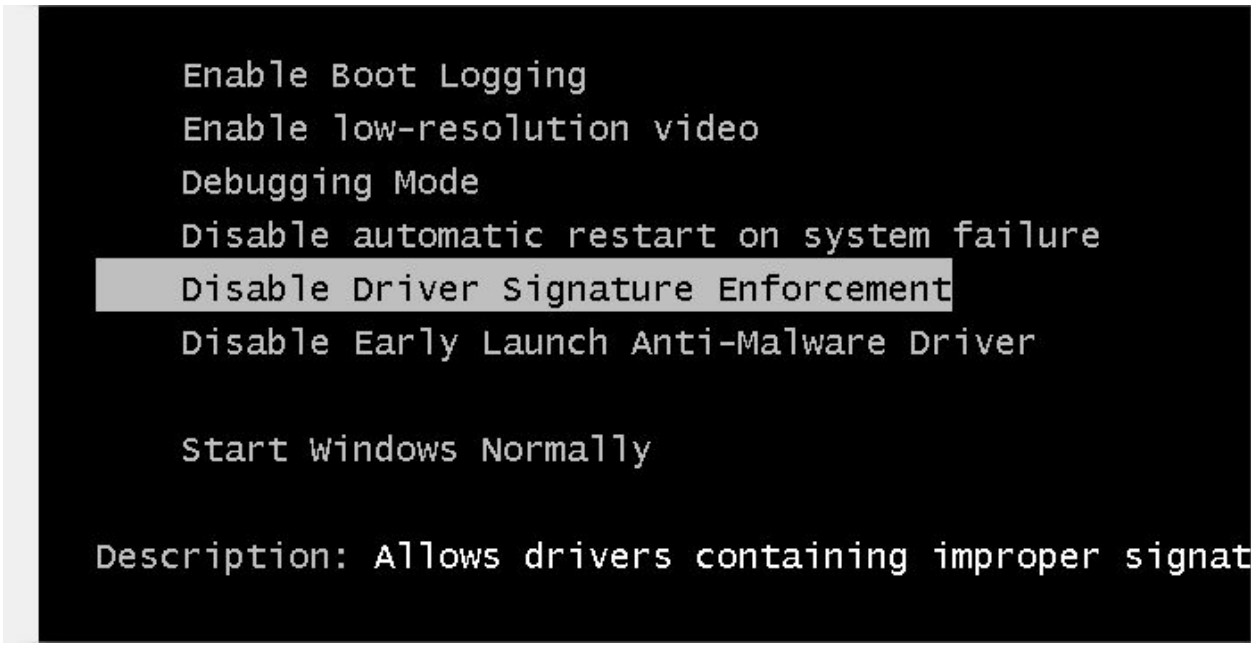
לקימפול הדרייבר עקבו אחר ההוראות:

1. הפעילו את x64 Checked Build Environment כחלק מהWDK (חפשו במערכת)
2. בחלון שנפתח עקבו לנתיב של הטמפלייט
3. ברגע שתהיו מוכנים הריצו בחלון את הפקודה 'build'
4. ודאו כי הbuild הצליח ונוצרו תתי התיקיות objchk_win7_amd64\amd64
5. ודאו כי הגדרתם לVM תיקיה משותפת כפי שפורט במדרך ההתקנה - העבירו את כל קבצי הטמפלייט לתיקיה זו, או לתת תיקיה בתוכה
6. הפעילו את vmmon מvirtualkd (או את vmmon64 אם אתם על מע' 64 ביט)
7. הדליקו את הVM ולחצו F8 במסך הבחירה



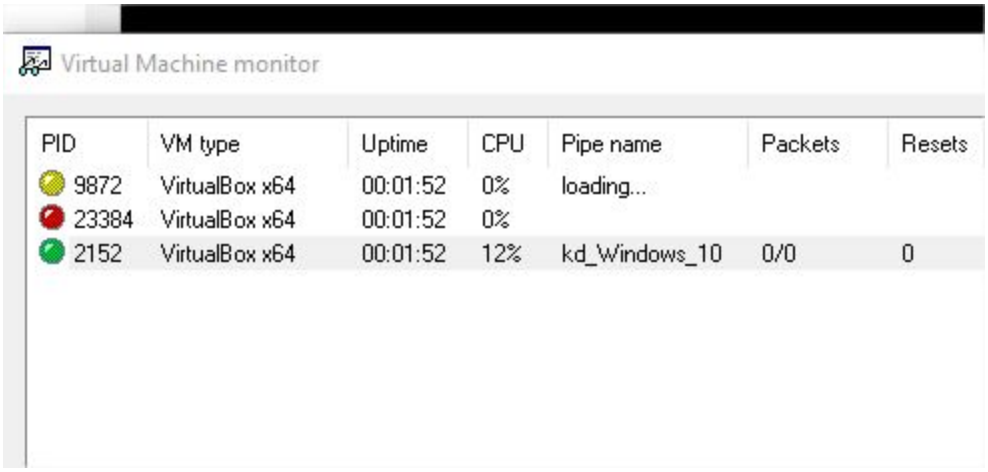
.8

.9 בחרו באופציה Disable Driver Signature Enforcement



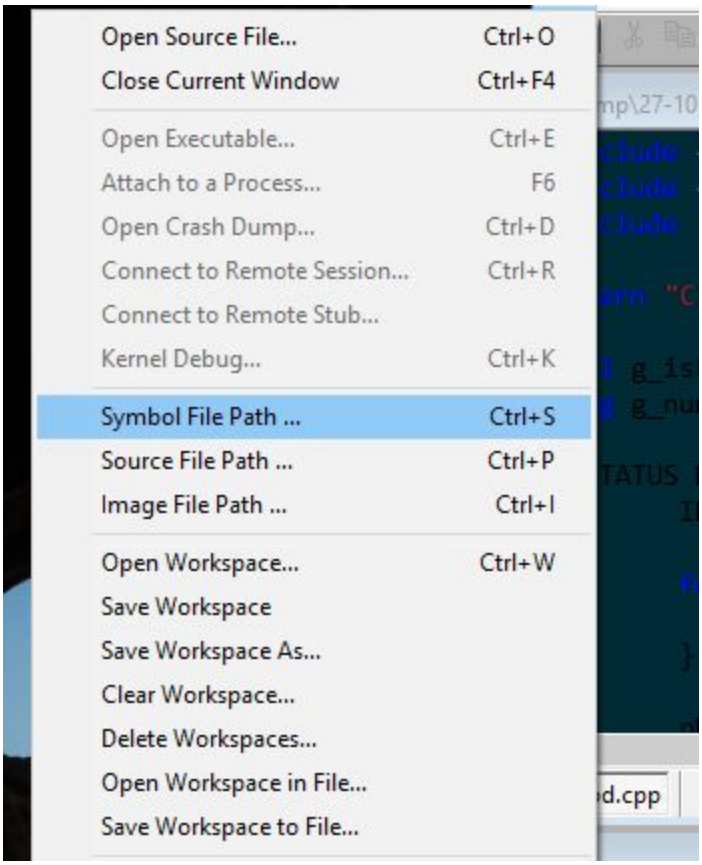
.10

.11 בvmmon - בחרו את הVM הצבוע בירוק



.12

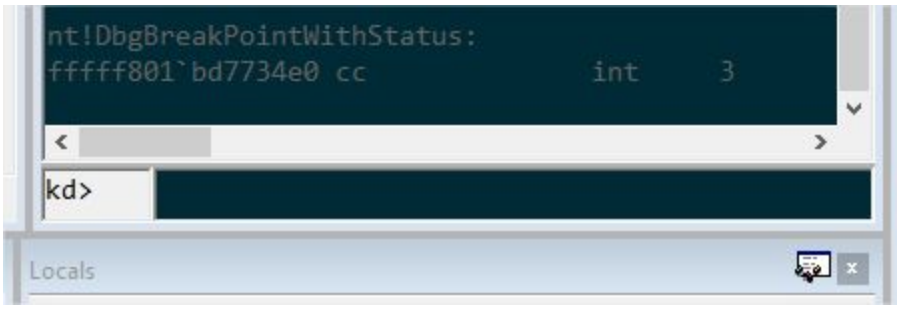
13. לחצו על Run debugger
14. צרו תיקיה חדשה: c:\symbols
15. ערכו את הSymbol file path



.16

17. כתבו בו

18. srv*c:\symbols*http://msdl.microsoft.com/download/symbols;PATH_TO_AMD64_DIR
החליפו את PATH_TO_AMD64_DIR בנתיב התיקיה amd64 שנוצרה לאחר הbuild
19. ערכו את Source File Path - שימו בו את הנתיב לתיקיה שמכילה את קובץ הסורס (helloworld.c)
20. ערכו את Image File Path - שימו בו את הנתיב לתיקיה amd64 שנוצרה לאחר הbuild
21. לחצו על Break
22. 

23. ודאו כי Windbg עצר את הפעולות שמתצעות בVM
24. 

25. לחצו על F5 ותנו למע' לעלות
26. העתיקו את קובץ ה.sys שנוצר מתוך התיקיה המשותפת לשולחן העבודה
27. העתיקו (אם לא העתקתם עדיין) את DriverLoader מהתיקיה המשותפת לשולחן העבודה
28. הריצו את DriverLoader
29. טענו את קובץ ה.sys
30. לחצו על Register Service
31. לחצו על pause בWindbg
32. שימו Breakpoint בעזרת הפקודה bp helloworld!DriverEntry
33. לחצו F5
34. לחצו על Start Service בDriverLoader
35. בהצלחה

הרימו את ידכם ברגע שסיימתם לשיחת חתך.

משימה 2 - הדפדפן המוביל בעולם

במשימה זו התבקשתם ליצור דרייבר שיעזור לאנושות.
הדרייבר הולך 'ליירט' פתיחה של דפדפנים פחות מוצלחים ולפתוח את הדפדפן המוביל בעולם: Chrome.
התקינו Chrome 64 bit על הVM, עשו Snapshot נוסף והורידו את הטמפלייט מכאן ותתכוננו לפסטן.

מטרות בתרגיל:

1. לכתוב Filesystem Minifilter Driver שמיירט פתיחה של דפדפנים מוכרים
2. אחרי היירוט - הדרייבר יגרום למע' להעלות קובץ אחר (במקרה הזה, Chrome)
3. לבדוק את הדרייבר באופן מקיף כך שהמשתמש לא יחווה BSODים

בונוס:

4. לגרום לדרייבר לעלות (ולעבוד) בזמן בוט - תעשו snapshot לפני

מושגים לקריאה:

- Minifilter Drivers
- IRP_MJ_CREATE
- Ntfs Reparse Points

בהצלחה.
מי שסיים - שירים את ידו לשיחת חתך.

משימה 3 - דיבוג הBSOD הראשון שלי

כאן תקבלו קוד לדרייבר חצי מוכן - תקמפלו אותו, תעלו אותו למכונה הוירטואלית בזמן שאתם מדבגים אותו, ובשלב מסוים הדרייבר יגרום למחשב לקרוס ולהגיע לBSOD (Blue Screen of Death).

המטרה שלכם בשלב הזה היא:

- להצליח לדבג את הדרייבר
- לראות את הדפסות הדיבאג של הדרייבר בDbgView
- למצוא מה גורם לBSOD
- לתקן את הקוד
- להעלות מחדש ולהוכיח שהפעם הדרייבר תקין

אנא הרימו את היד כשסיימתם את התרגיל לשיחת חתך.

http://sriramk.com/world-windows-driver-from-scratch
https://sysprogs.com/w/forums/topic/two-problems-with-virtualkd-virtualbox-windows-10/
http://virtualkd.sysprogs.org/tutorials/install/manualvm
http://www.osronline.com/article.cfm?article=295
!drvobj