



# מעבדה 8



CSRP

DFIR

## מבוא ל-DFIR

יצירת סביבת מעבדה של Windows

- עמוד 1 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

## נושאי המעבדה



הבן מכונת Windows 10 שתשמש לאורך הקורס.

## זמן מוערך



10 דקות.

## סביבת המעבדה



Windows 10 ISO •

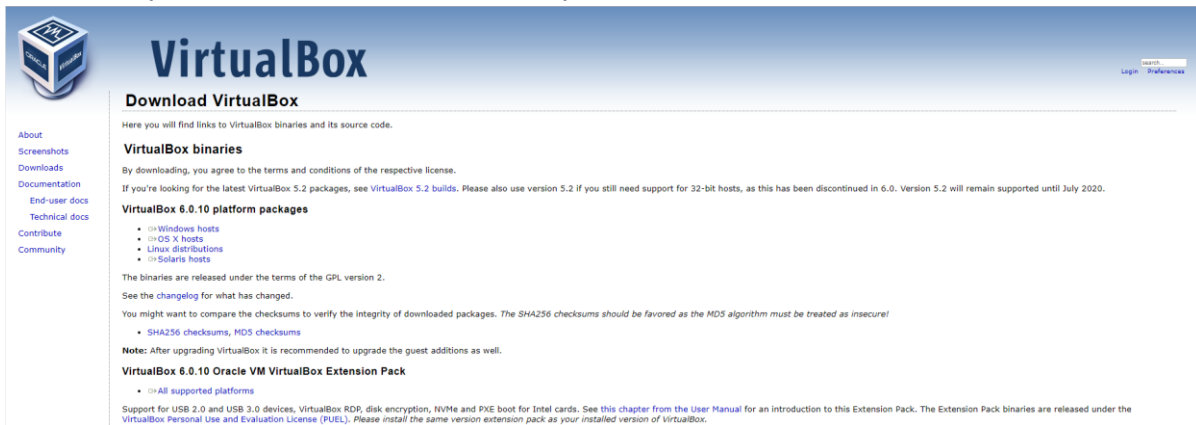
## משימת מעבדה:

צרו התקנת VM של Windows 10 והתקינו את Flare-VM באמצעות סקריפט ההתקנה שלה.

1 אם עדיין לא הותקן, הורידו VirtualBox למערכת ההפעלה שאתם משתמשים בה. התקינו אותו עם הגדרות ברירות המחדל, והתקינו Windows 10 ISO.

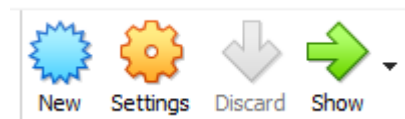
**פתרון:**

VirtualBox מתאימה לכל מערכות ההפעלה. הקפידו להוריד אותה מהאתר המקורי.

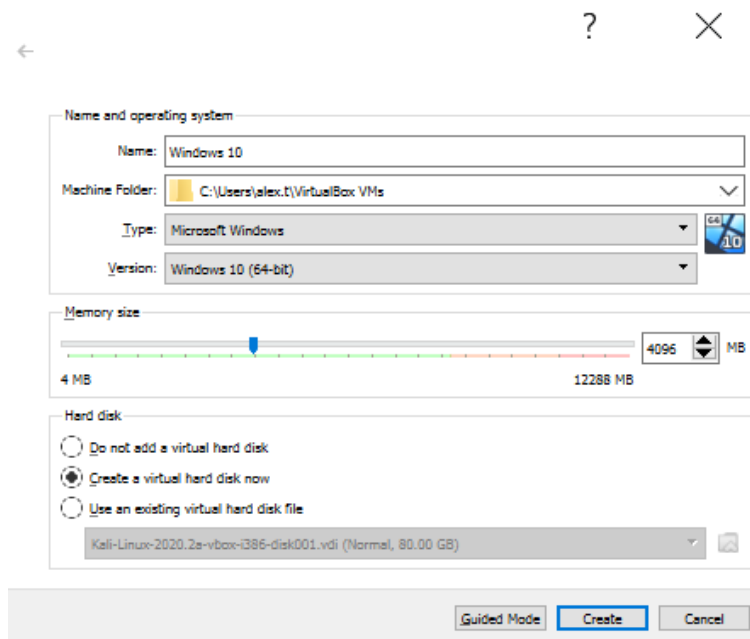


The screenshot shows the VirtualBox website's 'Download VirtualBox' page. It includes a navigation menu on the left with links like 'About', 'Screenshots', 'Downloads', 'Documentation', 'End-user docs', 'Technical docs', 'Contribute', and 'Community'. The main content area is titled 'Download VirtualBox' and contains information about binaries, platform packages for Windows, OS X, Linux, and Solaris, and the Oracle VM VirtualBox Extension Pack. It also includes a changelog and checksum information.

לחצו New כדי ליצור סביבה חדשה.



הזינו את השם "Windows 10" (יש לשנות את הסוג והגרסה בהתאמה אחרי שאתה מזין את השם), וציינו מיקום לשמירת הקבצים (גודל הקבצים יגדל ככל שהכמות תגדל).



The screenshot shows the 'Name and operating system' dialog box in VirtualBox. The 'Name' field is set to 'Windows 10'. The 'Machine Folder' is 'C:\Users\alex.t\VirtualBox VMs'. The 'Type' is 'Microsoft Windows' and the 'Version' is 'Windows 10 (64-bit)'. Below this, the 'Memory size' is set to 4096 MB on a scale from 4 MB to 12288 MB. Under 'Hard disk', the option 'Create a virtual hard disk now' is selected. A file path is shown: 'Kali-Linux-2020.2a-vbox-1386-disk001.vdi (Normal, 80.00 GB)'. At the bottom, there are buttons for 'Guided Mode', 'Create', and 'Cancel'.

לחצו Next, הגדירו את גודל ה-RAM ל-4096, ולחצו Next עוד פעם.

- עמוד 3 -

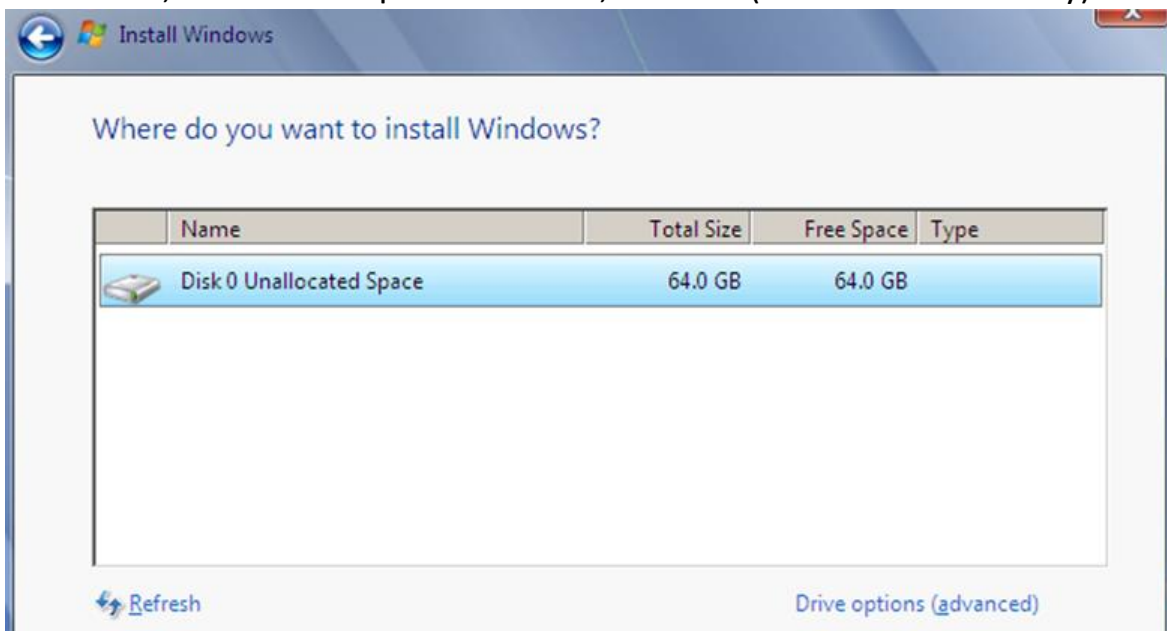
כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

בחרו Create a virtual hard disk now -> Create -> VDI -> Next -> Dynamically allocated  
ציינו שטח אחסון בגודל של עד 64 GB (זה לא אומר שכל השטח הזה ישמש, אבל בגלל  
שהגדרנו אותו כדינמי, הוא יגדל עד שכל 64 GB יהיו בשימוש, אז הוא יתריע שנגמר לך  
שטח האחסון, והוא לא ימשיך).  
הפעילו את המכונה ובחלו הקופץ הראשון, לחץ Folder, נווטו אל הקובץ Windows 10  
ISO, ולחץ Start.

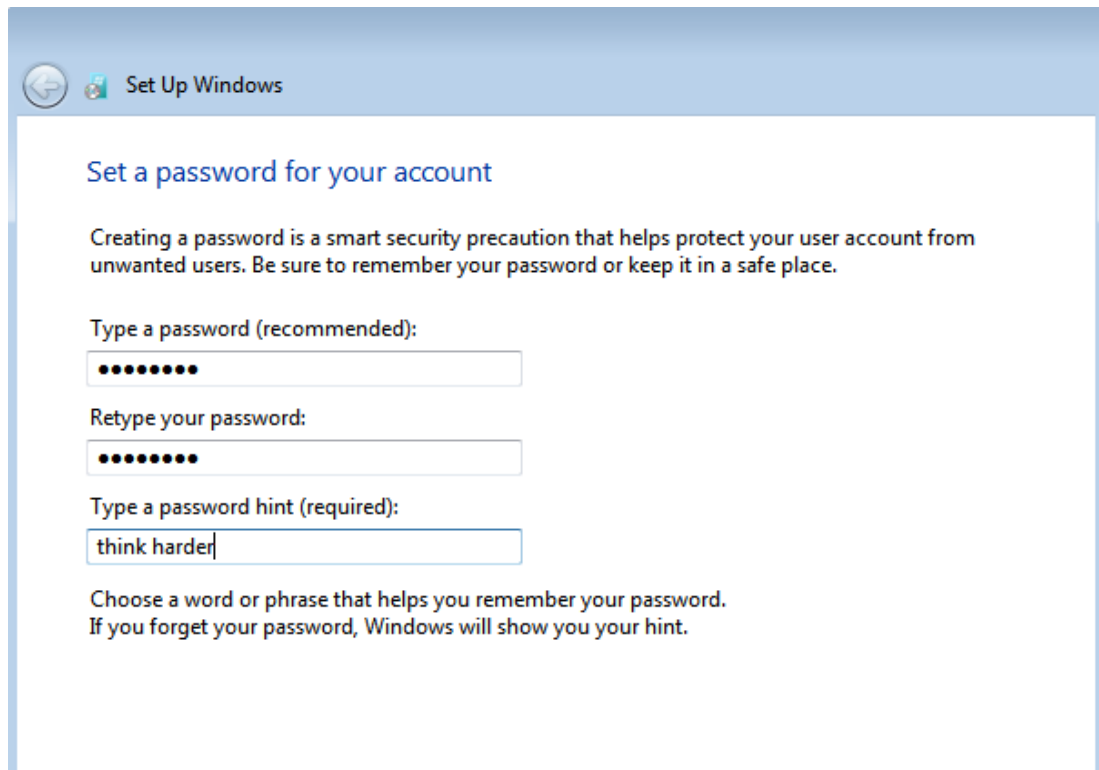
2 התקינו Windows 10 על VirtualBox.  
הכניסו את שם המשתמש "admin" והסיסמה "Pa\$\$w0rd".

### פתרון:

באשף ההתקנה הראשון של Windows, קבעו את שפת ברירת המחדל (English), לחצו  
Next, ואז לחץ Install Now. קבלו את תנאי הרישיון ע"י לחיצה על הקופסה ואז Next.  
בחרו "Custom (Install Windows Only)", בחרו את הדיסק היחיד ברשימה, ולחצו Next.



המתינו עד שההתקנה תסתיים ואל תאתחלו את המחשב. כאשר ההתקנה מגיעה ל-  
100%, המכונה תאתחל עצמה מחדש. קבעו את שם המשתמש ל-admin, ואת הסיסמה  
ל-Pa\$\$w0rd.



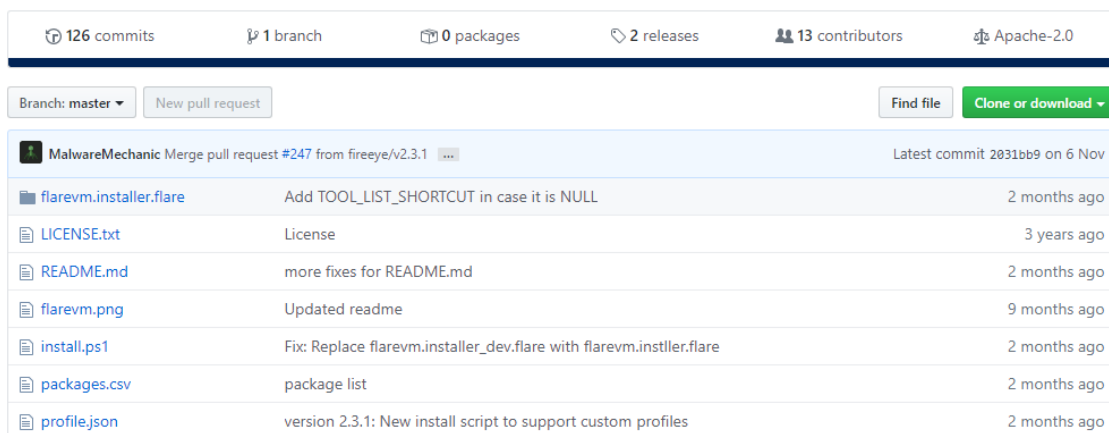
השתמשו בהגדרות המומלצות וקבעו את התאריך והשעה.

3 נווטו אל דף ה-GitHub של Flare-VM והורידו את סקריפט ההתקנה.

**פתרון:**

דף ה-GitHub של Flare-VM:

<https://github.com/fireeye/flare-vm>



ביוון ש-GitHub לא מותקן כברירת מחדל ב-Windows, לחצו Clone & Download וחלצו את התוכן אל תיקיית ההורדות.

4 הריצו את סקריפט ההתקנה של Flare-VM.

- עמוד 5 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

שימו לב: במהלך התקנת הסקריפט על המכונה/מחשב יתבצע הפעלה מחדש ובנוסף, תתבקשו להכניס סיסמא.

### פתרון:

פתחו PowerShell כ-administrator ונווטו אל התיקייה בה סקריפט ההתקנה **install.ps1** ממוקם.

הריצו את הפקודה: **Set-ExecutionPolicy Unrestricted** ואז הכניסו Y כדי לתת לסקריפט הרשאות הרצה.

ולאחר מכן את הפקודה: **.\install.ps1**. ואז הכניסו R כדי להתחיל את הרצת הסקריפט.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd "C:\Users\John Doe\Downloads\flare-vn-master\flare-vn-master"
PS C:\Users\John Doe\Downloads\flare-vn-master\flare-vn-master> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\Users\John Doe\Downloads\flare-vn-master\flare-vn-master> .\install.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\Users\John Doe\Downloads\flare-vn-master\flare-vn-master\install.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
[+] No custom profile is provided...
[+] Checking if script is running as administrator..
[+] Getting user credentials ...

Windows PowerShell credential request
Enter your credentials.
Password for user John Doe: *****

[+] Installing Boxstarter
Chocolatey is going to be downloaded and installed on your machine. If you do not have the .NET Framework Version 4 or greater, that will also be downloaded and installed.
```

אתם תתבקשו להזין את אישורי המשתמש המקומי (כדאי להשתמש בחשבון ה-admin המקומי במהלך ההתקנה).