

```

.uuu
  z@#"%c
  @!!!R. #c
dT!!!!!!>
  '!!!!!!N "i u*" #s : "
@?!!!!!!R
  t!!!!!!#u "i .@ ^$
:R!!!!!!X
  '!!!!!!#c "i:# ?>
R!!!!!!X
  '!!!!!!N @
4W!!!!!!>
  '!!!!!!Ru" ?!!!!!!X
  'X!!!!!!9~ . . 'X!!!!!!6
R!!!!!!tF z$#` h &!!UR!!!!F
?!!!!$X!!!$ .@ X $WTR!!!!X
M!!!!i#U!E . @F ! FdR!!!!f
  'X!!!!#c'?u@#"*$N. :$ F'9!!!!@
9!!!!!!?NM ^*c dF ' @!!!!!!X>
R!!!!!!& "e d K<!!!!!!XF
  'X!!!!!!M> ^N f < E!!!!!!X"
  t!!!!!!# ^N : " .e$"^ Fn!!!!XP
  #X!!!!!!ML *c z" .e$$$$$ M'!!!!W*
  "UX!!X@t ^%u. ""*#).zd$$$$$ <\*@**"
  'N 4$$$$@$$$)$ $$$$k4$$$$$$$E :$
  ?> "$$$$$$":$$$W$$$ "$$$$$$$$ %
  : " ? ^#*" S "$$$$$$ ?
F L d$L X
& t$i @$$$ f
* $$$$$$$$$$\& @
  '*. W'$$$$$$$$$FM h u#
  ^*muz* % $$$$$$": ` "
  # ^**" d
  "****"

```

```

=====
Auto-Forensic-USB V2 (version 2)
=====

```

~Education/Personnel USE Only~ © Deano (copyright 2016)

About the Coder:

Dean is a cyber security specialist, with multiple qualifications in networking and security, some being Comptia network+, EC Council Certified Ethical Hacker, Cisco CCNA and EC Council Certified Computer Hacking Forensic Investigator. with multiple years of experience in the Cyber Security industry and most recent years dealing with forensics on Windows systems and mobile platforms, Dean has honed his skills to be able to bring you this program, which he wrote and modified to be able to serve his purpose of speedy system forensics such as password recovery and Internet Activity.

Features:

- * Writes a key-logger to System32 and will log all keys and you can sync the logs when the USB is plugged back in

- * Puts all used browser passwords stored in the internet browsers to a text file on the USB
- * Puts all Internet history to a text file on the USB
- * Puts all search history to a text file on the USB
- * Remove passwords
- * Get System Info to USB
- * Simple Pranks

Some Features May not be available in 32bit Systems but these are not essential.

USB Use:

1: Before use please make sure to disable the System Anti-Virus as it may recognise programs in this tool as dangerous, do not worry as this is a false positive, If you do not disable the antivirus it can damage the tool and cause some features not to function properly. To see how to disable your antivirus see attached page.

2: Click and Run the Forensic .bat file in the main directory, and follow the on screen instruction make sure to read the instructions or the program will exit.

3: Once the program has runs, the extra features will be available from the new CMD window.

4: All recovered data will be saved in the folder named recovery, under the time and date of the program being run

5. if a program opens just click X on the top right corner as the program on the windows system may not have been updated to most recent. this is not an issue and the information will still be recovered

Legal:

I am not responsible for anything you do with this program, only use this program for educational display or for personnel use, do not use this program on systems that you do not have permissions to use it on. you do not have permission to recreate, rewrite, resell, reproduce, clone or copy this tool and its code, doing so is subject to legal action by the code writer.

Note: I would like to Take a moment to say thank you for purchasing my software and helping fund my future endeavours.

=====

Auto-Forensic-USB V2 (version 2)


=====

~Education/Personnel USE Only~ © Deano (copyright 2016)

How to Disable Antivirus

How to Temporarily Disable your Anti-virus


AVAST

Right-click on the avast! icon in system tray (looks like this:  but orange in color starting with v5). Select avast! shields control and there will be options to disable avast for 10 minutes, 1 hour, until the computer is restarted or permanently.

AVG

Right-click the AVG icon in the system tray next to the clock.
Click Temporarily disable AVG protection.
Choose how long you want the protection to be disabled and whether to disable the Firewall as well, and then click OK.
You can disable AVG also from the Advanced settings:
Open the AVG Program.
On the Options menu, click Advanced settings.
Select Temporarily disable AVG protection in the menu on the left side.
Click the Temporarily disable AVG protection button.
Choose how long you want the protection to be disabled and whether to disable the Firewall as well, and then click OK.

AVIRA ANTIVIR

Please navigate to the system tray on the bottom right hand corner and look for an open white umbrella on red background.
* right click it-> untick the option AntiVir Guard enable.
* You should now see a closed, white umbrella on a red background (looks to this: )

BIT DEFENDER

* Double click on the system icon for Bit Defender.
* When the Bit Defender window appears, move mouse arrow to the left side and click >> Virus Shield.
* Move mouse arrow to the black check by Virus Shield is enabled and click.
* The black works will change to red, >> Virus Shield is disabled.
* Move mouse arrow to the top right corner and click the down arrows.
* Bit Defender is now inactive.
* To enable Bit Defender, do the same steps except click to enable.

BKAV Internet Security Professional

* Double click the tray icon to bring up the GUI.
* Choose Options/Tùy chọn (2nd tab at the left, depending on what language you are using).
* Uncheck Real-time Protection.
* You can also right click on the tray icon and choose Exit/Thoát

CA Internet Security Suite 2010

- * To turn off the Firewall, right-click on the CA Shield icon in the system tray, click My Internet, then click Disable Firewall.
- * To turn it back on, right click system tray icon, click My Internet, then click Enable Firewall.
- * To temporarily disable the Antivirus, right-click the CA Shield icon in the system tray, click My Computer, then click Enable Snooze.
- * Enter the snooze time in minutes (up to 999, approx 16 2/3 hours) in the box and click Snooze.
- * To end snooze, follow the same procedure and click Wake Now on the page for entering snooze time.
- * To disable Antivirus on a longer basis, double-click the CA Shield icon in the system tray.
- * When Security Center comes up, click Update Settings in the My Computer tab.
- * Then click the red X next to Auto Scan.
- * To re-enable, follow the same procedure and click the green checkmark.

Comodo Internet Security

- * Right click the icon on the system tray.
- * Hover over Antivirus, then Firewall and Defence+ to disable them.
- * To reactivate real-time protection, repeat step 2 but set each to Enabled.

ESET NOD32 ANTIVIRUS V4

- * Double click on the system tray icon: on the bottom right hand corner.
- * Select Disable real-time file system protection.
- * A popup will ask "Are you sure you want to disable...protection?"
- * Click "Yes" to disable the Antivirus guard.

Emsisoft Anti-Malware & Internet Security

- * Right-click on the Emsisoft shield icon in the system tray (green with white outline).
- * Choose Pause protection, then Disable until computer restart.
- * The shield icon will turn red with a white cross in the middle, and the GUI will be in red instead of green.
- * Note: Do NOT exit EAM/EIS instead of disabling real-time protection, as File Guard will remain active even when the program itself is not running.

ESET SMART SECURITY

- * Double click on the system tray icon: to open the main application window.
- * Or via Start >> All Programs >> ESET >> ESET Smart Security.
- * Click on Setup >> Antivirus and antispyware >> Temporarily disable Antivirus and antispyware protection.
- * When prompted to confirm temporarily disable select Yes.
- * Note: Protection will be automatically started after a system reboot.

F-SECURE ANTIVIRUS

- Please navigate to the system tray on the bottom right hand corner and look for a blue sign.
- * right click it-> select Unload.
 - * The F-Secure sign should now be surrounded by a red striked through circle (looking like this:)

KASPERSKY ANTIVIRUS

- Please navigate to the system tray on the bottom right hand corner and look for a sign.

- * right click it-> select Pause Protection.
- * click on -> By User Request
- * a popup will claim that protection is now disabled and a sign like this: will now be shown.

G-Data Internet Security

- * Go to Settings > AntiVirus > Real-time protection.
- * Under Virus monitor, Behavior monitor and Exploit Protection, uncheck Enabled (recommended).
- * To reactivate real-time protection, repeat step 1 and re-check all Enabled (recommended) checkboxes.

MCAFEE ANTIVIRUS

Please navigate to the system tray on the bottom right hand corner and look for a sign.

- * Right-click it -> chose "Exit."
- * A popup will warn that protection will now be disabled. Click on "Yes" to disable the Antivirus guard.

MCAFEE SECURITY CENTER 7.1

Please navigate to the system tray and double-click the taskbar icon to open Security Center.

- * Click Advanced Menu (bottom mid-left).
 - * Click Configure (left).
 - * Click Computer & Files (top left).
 - * VirusScan can be disabled in the right-hand module and set when it should resume or you can do that manually later on.
 - * Do the same via Internet & Network for Firewall Plus.
- Instructions to disable McAfee Security

MICROSOFT SECURITY ESSENTIALS

- * Right-click on the MSE icon in the system tray and choose Open.
- * Click the Settings tab, then click Real Time Protection.
- * Uncheck the box next to "Turn on real time protection".
- * Click the "Save changes" button.
- * Exit MSE when done.

NORTON ANTIVIRUS (by Symantec)

Please navigate to the system tray on the bottom right hand corner and look for a sign.

- * right-click it -> chose "Disable Auto-Protect."
- * select a duration of 5 hours (this assures no interference with the cleanup of your pc)
- * click "Ok."
- * a popup will warn that protection will now be disabled and the sign will now look like this:

NORTON

- * Right-click the Norton 360 Premier Edition icon in the system tray and select Disable Antivirus Automatic-Protect.
- * You will get a new dialog box with five options: 15 minutes, 1 hour, 5 hours, Until system restart, Permanently.
- * Choose 5 hours.

PC TOOLS THREATFIRE

Right-click on ThreatFire's icon near the clock (it's an orange flame) and select Suspend.

When you see that the icon has turned from an orange flame to a blue icon with an orange strip in the middle, ThreatFire has been temporarily disabled.

Qihoo 360 Total Security

Right click on the tray icon to bring up the menu.

Drag the slider at the corner in Protection: On to the left.

To reactivate real-time protection, open the menu and drag the slider to the right.

SYMANTEC ENDPOINT PROTECTION

Right click on the icon in the taskbar notification area & select "Disable Symantec EndPoint Protection".

Windows Defender on Windows 7/8/10

Right-click on the MSE icon in the system tray and choose Open.

Click the Settings tab, then click Real Time Protection.

Uncheck the box next to "Turn on real time protection".

Click the "Save changes" button.