**Guide to Setting Up LockDown Browser Project**

1. **Install Git**

<https://git-scm.com/downloads>

**1. Install Visual Studio**

* Download and install **Visual Studio** (any version will work, but the latest 2022 is recommended).
* During installation, ensure the following components are checked:
  + **.NET Desktop Development**
  + **Desktop Development with C++**
* Complete the installation process.

A screenshot of a computer

Description automatically generated

**2. Create a Project Directory**

* Create a folder for your project. For example:

For example,

“C:\Users\abcd2\OneDrive\Documents\temp\LockdownBrowserProject”

* This directory will host all scripts, builds, and related files.

**3. Clone the Repository**

* Clone the necessary repository into the project folder.
* Of just copy and paste it in you really only need a couple of files.

**4. Update Configuration Files**

**BuildDetours.ps1**

* Open the BuildDetours.ps1 file and change the following line to match your project directory

$projectDir = "C:\Users\abcd2\OneDrive\Documents\temp\LockdownBrowserProject"

To your directory.

**Host.wsb**

* In the Host.wsb file, update:

<HostFolder>C:\Users\abcd2\OneDrive\Documents\temp\LockdownBrowserProject</HostFolder>

* To match

**5. Open Developer Command VS 2022**

* Search for **Developer Command Prompt for Vs** and open it. A close up of a text

  Description automatically generated
* Navigate to your project directory by typing:

cd "C:\Users\abcd2\OneDrive\Documents\temp\LockdownBrowserProject"

**6. Disable Windows Defender**

* Make sure **Windows Defender** is turned off, as it may detect withdll.exe as a potential threat.

**7. Run the Build Script**

* Execute the BuildDetours.ps1 script by entering the following command:

powershell Set-ExecutionPolicy Unrestricted -Scope Process; .\BuildDetours.ps1

* When prompted, type R to proceed.
* Wait for the process to complete. You should see a confirmation that the build was successful.

A black background with white text

Description automatically generated

**8. Open Windows Sandbox**

* Open the project directory in **Windows Sandbox** by clicking on the option.



* In Windows Sandbox, you'll notice a new folder created for your project.

A yellow folder with white text

Description automatically generated

**9. Run the Cleanup Script in Sandbox**

* Open **PowerShell** within Windows Sandbox.
* Navigate to the project directory:

cd .\Desktop\LockdownBrowserProject\

Run the cleanup command:

Set-ExecutionPolicy Bypass -Scope Process; .\remover.ps1

* When prompted, press Y to confirm.
* Wait for the process to finish. You should see \*\* Done! indicating completion.

**10. Remove SystemBiosVersion**

* To remove the SystemBiosVersion, execute the following commands in PowerShell:

Remove-ItemProperty -Path "HKLM:\HARDWARE\DESCRIPTION\System" -Name "SystemBiosVersion"

Get-ItemProperty -Path "HKLM:\HARDWARE\DESCRIPTION\System" -Name "SystemBiosVersion"

* If you see an error, it has been successfully removed.

**11. Final Registry Check**

* Use the following command to verify all related properties:

$registryPath = "HKLM:\HARDWARE\DESCRIPTION\System"

Get-ItemProperty -Path $registryPath | Select-Object `

SystemBiosVersion, `

SystemBiosDate, `

VideoBiosVersion, `

ProcessorNameString, `

MachineType, `

SystemModel, `

BaseBoardProduct, `

BaseBoardManufacturer | Format-List \*

If you see something like this has been removed.

A screen shot of a computer

Description automatically generated

**12. Verify Deleted Files**

* To check if files have been deleted, run:

Set-ExecutionPolicy Bypass -Scope Process; .\CheckDeletions.ps1

* Again, press Y when prompted.

**Next**

**13. Download LockDown Browser**

Download the LockDown Browser from: LockDown Browser Download

<https://download.respondus.com/lockdown/download-finished.php?id=>

You'll need an ID to download. You can find or brute-force a valid ID, typically consisting of 9 digits (e.g., 872615552). This should already been provided by your institution.

A screenshot of a computer

Description automatically generated

**14. Execute Setup Script**

* Once downloaded, run the following command:

.\SetupLockdown.ps1

* Navigate back to,

A blue and white box with red text

Description automatically generated

* Click on the javascript button
* If you see no message indicating something then you just bypassed MOTHER FUCKEN LOCKDOWN BROWSER BITCH!!!

A screenshot of a computer

Description automatically generated

**15. Verification**

* Perform a system check via the Help Center. You should not see any processes listed, confirming successful patching.

A white background with black and red lines

Description automatically generated with medium confidence

**16. Check Logs**

* Check the **local disk** for logs that indicate whether the injection was successful and other interactions with the LockDown Browser.

A screenshot of a computer

Description automatically generated

* You’ll see a log that tells you whether injection Is successful and other calls that LockDown Browser is calling.
* Now you're ready to take your exam. When it’s time for your exam the professor will have a link in the browser to launch LockDown Browser. Once click to launch the injection will start automatically. A screenshot of a computer

  Description automatically generated

Please note: After closing Windows Sandbox, all data and changes are erased, leaving no trace behind. Each time you start Windows Sandbox, it opens with a clean slate. Therefore, you will need to reinstall and execute the necessary commands each time you use it wont take longer than 5 mins to set up.