Authenticode Digitally Signed Software

Overview

Software vendors can digitally sign and timestamp the software they distribute. The code signing process ensures the end user knows the digitally signed software is legitimate, comes from a known software vendor and the code has not been tampered with since being published. All the software products published by Digital Detective have been digitally signed. This ensures that when you use our software, you can verify that it has not been tampered with and is a product developed and released by Digital Detective Group. This is extremely important when using software for forensic purposes.

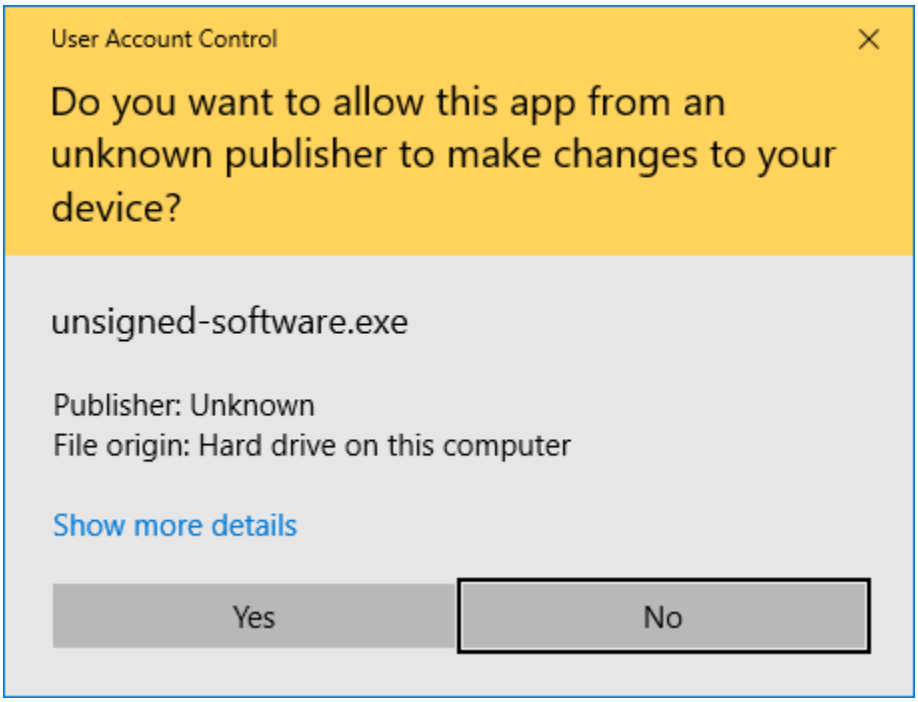
When installing software products which have not been digitally signed, you have no guarantee that they have been produced by a legitimate forensic software vendor or have not been tampered with by a third party. It would not be wise to rely upon software which has not been digitally signed for a criminal or civil case.

User Account Control

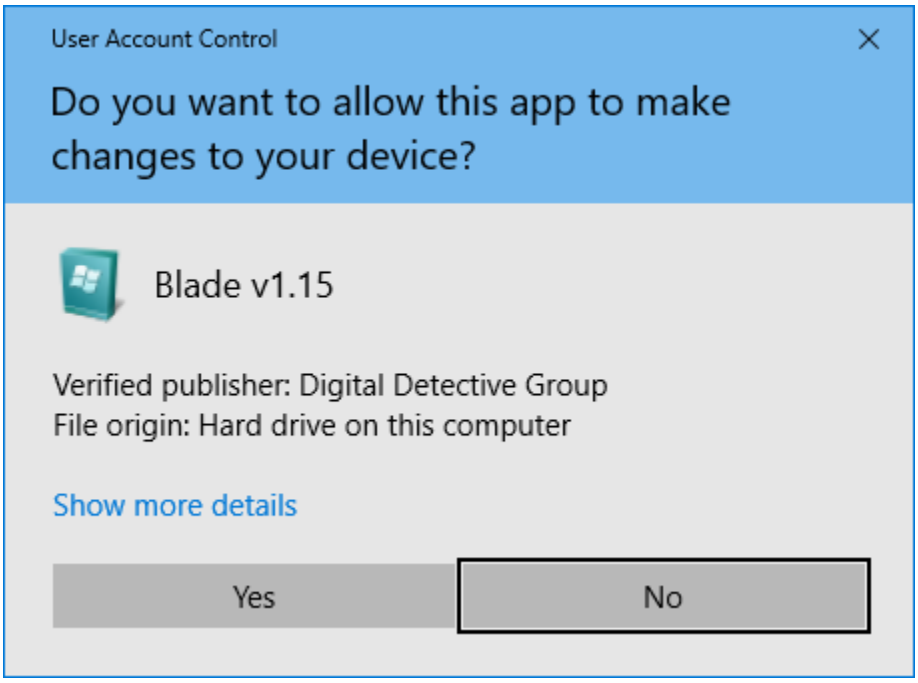
User Account Control (UAC) is a fundamental component of Microsoft's overall security vision. UAC helps mitigate the impact of malware. A fundamental principle of managing security is giving users and applications a minimal set of security permissions. This ensures that they can perform the most common operations that they need to accomplish tasks, but it greatly limits the potential damage that a malicious program can cause. For example, users rarely (if ever) need to modify operating system files directly. By preventing them from performing this action, the operating system can avoid the mistaken or malicious deletion of critical components.

Installing Digitally Signed Software

By default, even an administrator account in modern versions of Windows does not have full access to modify system settings and install programs. Thus, if you try to install a program or change critical settings, you may see your desktop fade and show only a prompt window asking if you're sure you want to do this. This is a secure desktop, designed to prevent a program from automatically approving itself. If the software you are installing has not been digitally signed, the prompt will look as follows:



When installing software that has been digitally signed, the prompt will looks as follows:

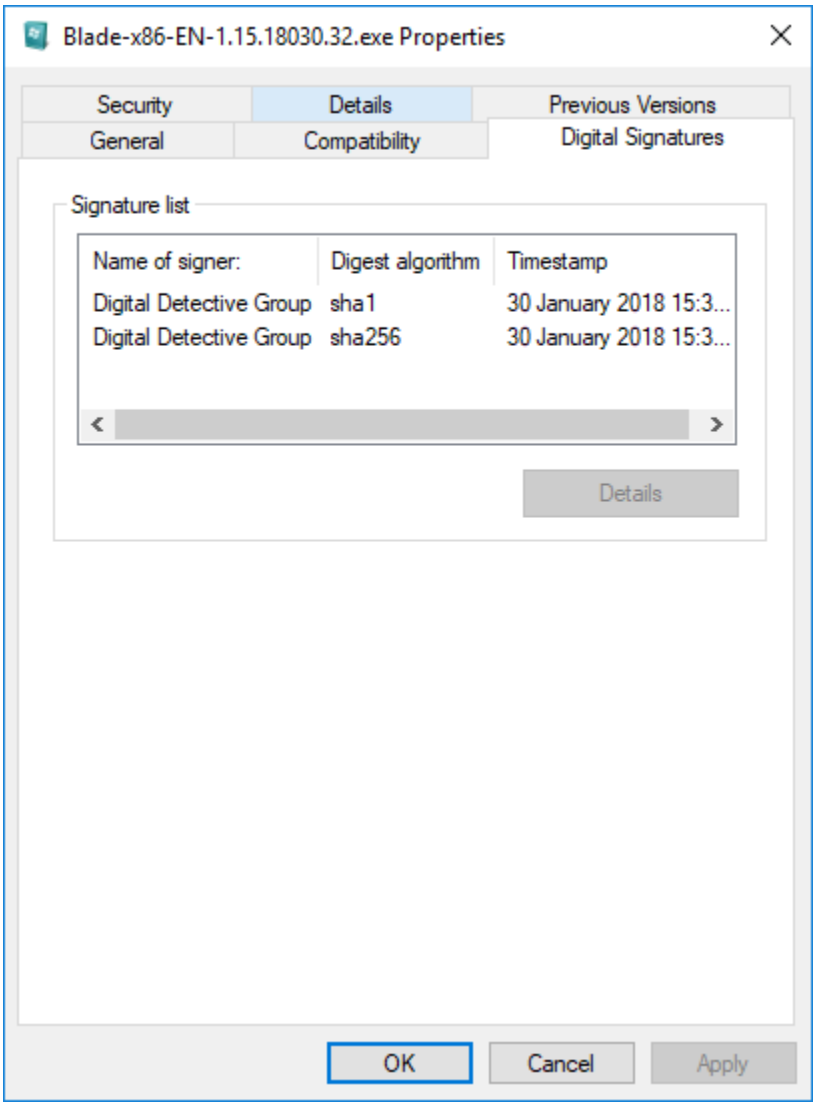


This window shows the publisher and confirms that the publisher has been verified.

Manually Verifying the Digital Signature

To verify the digital signature embedded within an individual executable or DLL, do the following:

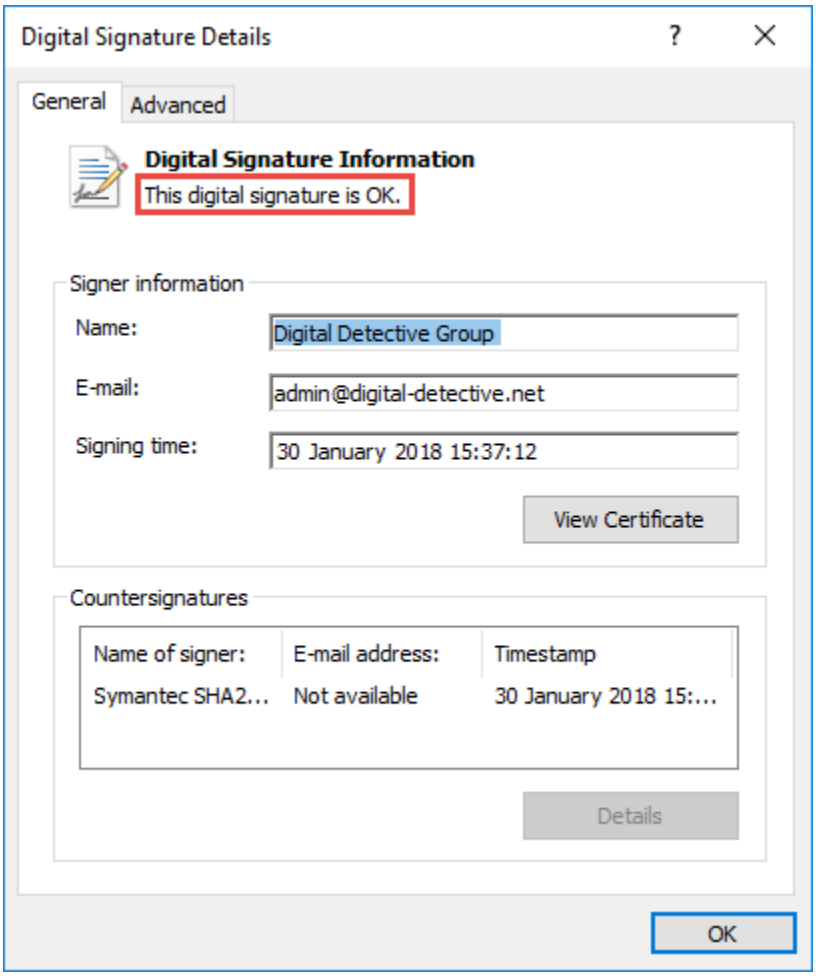
- Right click on the file and select **Properties**
- Click on the **Digital Signatures** tab



This will show you the name of the individual or company which signed the file.

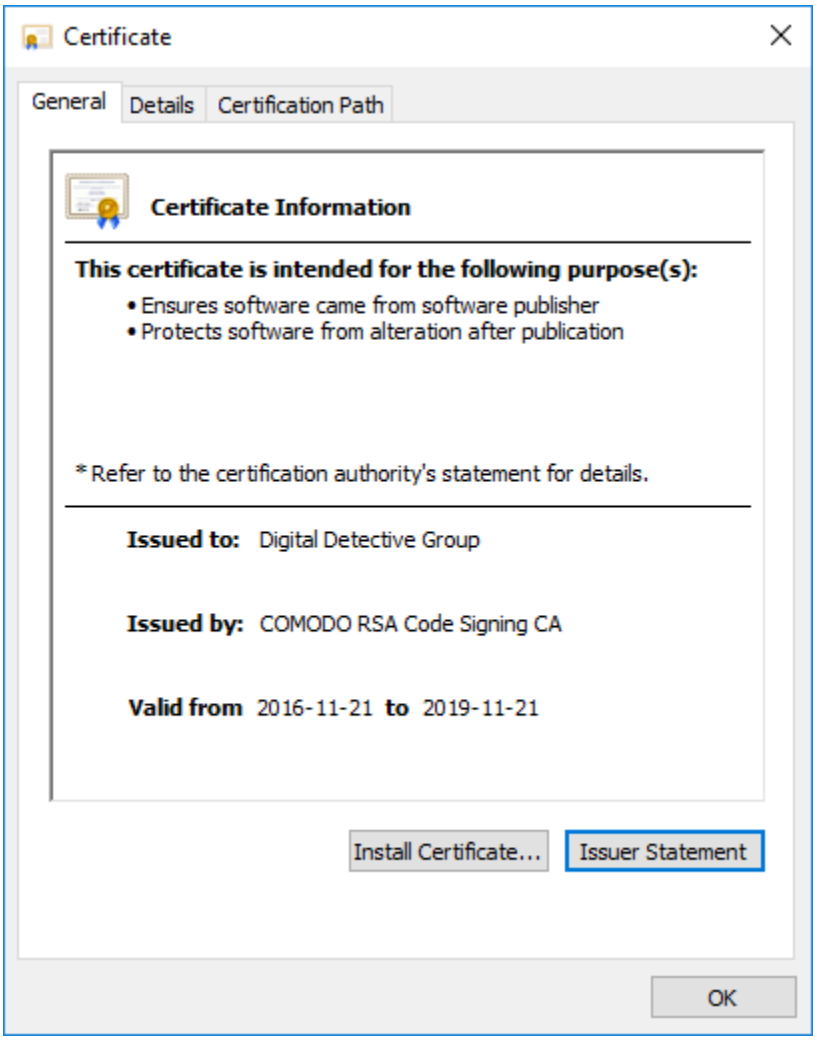
To further verify the actual digital certificate, do the following:

- Select any of the signatures in the Signature List
- Click the **Details** button



At the top of the General tab, you can see that this Digital Signature has been verified.

Clicking the **View Certificate** button will show the following:



If for any reason, the Authenticode Digital Certificate does not verify, please do not install the software.