FileSystem.GetDigitalSignature

Method	**GetDigitalSignature**
Module	FileSystem
Library	Core
Action	Returns all certificates used in an authenticode signature that are not used for timestamping.
Parameters	`FilePath` (string): The full path of the file.
Return values	`CertificateIndex` (string): An index for each certificate chain returned. For example, if you had only one signature on the file, there may be multiple rows returned (as the certificate chain may be long), but all rows returned would have a `CertificateIndex` of 0. This can be used to isolate a particular certificate chain. This is a zero indexed number.
	`CertificateType` (string): The type of the certificate. Possible values: "Signing", "Intermediate", "Root" and "Self-signed". ⓘ The CertificateType return value is inferred from the depth of the certificate in the chain built by the device. A depth 0 certificate can be marked as 'Self-signed' if no other certs in its trust chain can be found.
	`Depth` (string): The depth of a certificate in a certificate chain. This starts from the certificate used to sign the file, which is 0. The next certificate in the chain is 1, and so on. I.e. a zero-indexed number. The Depth return value builds a certificate trust chain. ⓘ If a certificate chain cannot be built on a device, for example if certificates are missing from the certificate store, the chain returned may be incorrect and will reflect this. This will also affect the `CertificateType` return value.
	`EffectiveDate` (string): The date at which the certificate becomes valid ('`NotBefore`').
	`ExpiryDate` (string): The date at which the certificate is no longer valid ('`NotAfter`').
	`FileName` (string): The full path of the file.
	`HashAlgorithm` (string): The algorithm of the hash used to create the digital signature. If the hashing algorithm used is SHA-1, SHA-256, SHA-384 or SHA-512, the return values will be "SHA1", "SHA256", "SHA384" and "SHA512" respectively. Other hashing algorithms will return an OID, such as "1.2.840.113549.1.1.9". These OIDs are searchable online, on sites such as oidref.com.
	`Issuer` (string): The Issuer field of the certificate.
	`SerialNumber` (string): The serial number of the certificate. This is supposed to be (according to RFC5280) a positive integer assigned by the issuing CA that is unique. It is a nice way to identify a certificate if you are dealing with a single CA. ⚠ If you are dealing with multiple CAs, this is not a good way to specify a cert as this field can be zero.
	`SignatureStatus` (string): "`Signed`" if the certificate is signed otherwise "`Unsigned`".
	`Subject` (string): The Subject field of the certificate, containing the Common Name of the certificate.
	`Thumbprint` (string): The SHA1 hash of the certificate content and the certificate serial number.
Example	`FileSystem.GetDigitalSignature(FilePath:"c:\\tmp\\SomeProgram.exe");`
Platforms	• Windows
Notes	Does not return the timestamping certificates.