## CLAIMS

1. A computer-implemented method for anti-repackaging, the computer-implemented method comprising:

running a target file in an installation package;

loading a secure dynamic library in the installation package (301);

retrieving digital watermark information embedded in the target file and verification information stored in the secure dynamic library based on a code in the target file (302); and

determining, based on the digital watermark information and the verification information, whether the installation package is a repackaged installation package (303).

2. The computer-implemented method of claim 1, wherein:

the target file is a target file obtained after predetermined code is compiled; and

the digital watermark information is embedded at the end of the compiled target file.

3. The computer-implemented method of claim 2, wherein retrieving the digital watermark information comprises:

determining a start address of the digital watermark information in the target file based on an original length of the target file, wherein the original length is a length of the target file before the digital watermark information is embedded; and

retrieving the digital watermark information from the target file based on the start address.

4. The computer-implemented method of claim 1, wherein determining whether the installation package is the repackaged installation package comprises:

determining whether the digital watermark information is consistent with the verification information.

5. The computer-implemented method of claim 4, further comprising:

in response to determining that the digital watermark information is consistent with the verification information, determining that the installation package is an original installation

package.

6. The computer-implemented method of claim 4, further comprising:

in response to determining that the digital watermark information is inconsistent with the verification information, determining that the installation package is a repackaged installation package.

7. The computer-implemented method of claim 1, wherein determining, based on the digital watermark information and the verification information, whether the installation package is the repackaged installation package comprises:

when the digital watermark information is an instruction, performing an operation based on the instruction to obtain an operation result; and

determining whether the operation result is consistent with the verification information.

8. The computer-implemented method of claim 7, further comprising:

in response to determining that the operation result is consistent with the verification information, determining that the installation package is an original installation package.

9. The computer-implemented method of claim 7, further comprising:

in response to determining that the operation result is inconsistent with the verification information, determining that the installation package is a repackaged installation package.

10. The computer-implemented method of claim 1, wherein determining, based on the digital watermark information and the verification information, whether the installation package is the repackaged installation package comprises:

when the digital watermark information is an instruction, performing an operation based on the instruction to obtain an operation result; and

determining whether the operation result is consistent with an operation result in the verification information, and determining whether the instruction is consistent with an instruction in the verification information.

11. The computer-implemented method of claim 10, further comprising:

in response to determining that the operation result is consistent with the operation result in the verification information and the instruction is consistent with the instruction in the verification information, determining that the installation package is an original installation package.

12. The computer-implemented method of claim 10, further comprising:

in response to determining that the operation result is inconsistent with the verification information, determining that the installation package is the repackaged installation package.

13. The computer-implemented method of any one of claims 1 to 12, wherein the method is applied to an ANDROID operating system;

the target file is an executable file; and

the secure dynamic library is a shared object library.

14. An apparatus for anti-repackaging, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 13.