CLAIMS

1. A method for determining a virus-infected file, comprising:

at a computer system including one or more processors and memory for storing program instruction to be executed by the computer system;

loading an executable file being scanned from a storage device into the memory;

identifying a set of virus definitions for the executable file from a virus feature library, each virus definition including a virus signature and a corresponding file offset address;

without decompiling the executable file, locating data in ~~a~~ the executable file being scanned that has been loaded in the memory according to a file offset address associated with each of the set of virus definitions, wherein the data has a predefined length of a virus signature of the corresponding virus definition ~~a virus~~;

making a comparison of the virus signature with the data located in the executable file being scanned; and

determining that the executable file being scanned is a virus-infected file when the virus signature of at least one of the set of virus definitions matches the located data in the executable file being scanned.

2. The method of claim 1, wherein locating the data in the executable file being scanned that has been loaded in the memory according to the file offset address associated with each of the set of virus definitions, wherein the data has a predefined length of the virus signature of the corresponding virus definition ~~the virus~~ comprises:

locating, in the executable file being scanned and according to the file offset address associated with the virus signature of the corresponding virus definition, the data, with the file offset address as the starting point of the located data.

3. The method of ~~any of~~ claims ~~1 and 2~~, wherein making a comparison of the virus signature with the data located in the executable file being scanned comprises:

making a comparison of the virus signature with the data located in the executable file being scanned, with the file offset address as the starting point of the located data, wherein the lengths of the located data and the virus signature are the same.

4. The method of ~~any of~~ claims ~~1 and 3~~, further comprising, before locating the data in the executable file being scanned that has been located in the memory according to the file offset address associated with each of the set of ~~the~~ virus ~~signature of the virus~~definitions:

judging whether to perform the locating on the executable file being scanned according to the file offset address associated with the virus signature; and

skipping the locating when the file offset address is greater than the size of the executable file being scanned.

5. The method of ~~any of~~ claims ~~1 and 4~~, comprising, before locating the data in the executable file being scanned that has been loaded in the memory according to the file offset address associated with each of the set of ~~the~~ virus ~~signature of the virus~~ definitions:

reading the executable file being scanned from a disk, and storing the executable file being scanned in a cache.

6. The method of claim 1, further comprising:

determining that the executable file being scanned is a virus-infected file when the virus signature of each one of the set of virus definitions matches the located data in the executable file being scanned; and

determining that the executable file being scanned is a likely virus-infected file when the virus signature of at least one of the set of virus definitions does not match the located data in the executable file being scanned.

~~6.~~7. The method of claim 1, wherein the set of virus definitions include at least two virus definitions that have different virus signatures and the same file offset.

~~7.~~8. An apparatus for determining a virus-infected file, comprising:

one or more processors;

memory; and

one or more program modules stored in the memory, wherein the one or more program modules include instructions to be executed by the one or more processors, the one or more program modules including instructions for:

loading an executable file being scanned from a storage device into the memory;

identifying a set of virus definitions for the executable file from a virus feature library, each virus definition including a virus signature and a corresponding file offset address;

without decompiling the executable file, ~~a locating module for~~ locating data in ~~a~~ the executable file being scanned that has been loaded in the memory according to a file offset address associated with each of the set of ~~a~~ virus ~~signature of a virus~~definitions, wherein the data has a predefined length of a virus signature of the corresponding virus definition;

~~a comparison module for~~ making a comparison of the virus signature with the data located in the executable file being scanned; and

~~a determination module for~~ determining that the executable file being scanned is a virus-infected file when the virus signature of at least one of the set of virus definitions matches the located data in the executable file being scanned.

9. The apparatus of claim ~~6~~8, wherein the ~~locating module~~instruction for ~~is configured to~~ locat~~e~~ing the data~~,~~ in the executable file being scanned that has been loaded in the memory ~~and~~ according to the file offset address associated with each of the set of virus definitions, wherein the data has a predefined length of the virus signature of the corresponding virus definition further comprises instructions for:

locating, in the executable file being scanned and according to the file offset address associated with the virus signature of the corresponding virus definition, the data, with the file offset address as the starting point of the located data.

~~8. , the data, with the file offset address as the starting point of the located data.~~

10. The apparatus of ~~any of~~ claims ~~6~~8 ~~and 7~~, wherein the ~~comparison module is configured to~~ instruction for ~~make~~ making a comparison of the virus signature with the data located in the executable file being scanned further comprises instructions for:

making a comparison of the virus signature with the data located in the executable file being scanned, with the file offset address as the starting point of the located data, wherein the lengths of the located data and the virus signature are the same.

~~9. , with the file offset address as the starting point of the located data, wherein the lengths of the located data and the virus signature are the same.~~

~~10.~~ The apparatus of ~~any of~~ claims ~~6~~8 ~~and 8~~, wherein the one or more program modules further include instructions for:~~further comprising:~~

11. ~~a judgment module for~~ judging whether to perform the locating on the executable file being scanned according to the file offset address associated with the virus signature, wherein the locating is skipped when the file offset address is greater than the size of the file being scanned.

12. The apparatus of ~~any of~~ claims ~~6~~8 ~~and 9~~, wherein the one or more program modules further include instructions for~~further comprising~~:

~~a reading module for~~ reading the executable file being scanned from a disk, and storing the executable file being scanned in a cache.

13. The apparatus of claim 8, wherein the one or more program modules further include instructions for:

determining that the executable file being scanned is a virus-infected file when the virus signature of each one of the set of virus definitions matches the located data in the executable file being scanned; and

determining that the executable file being scanned is a likely virus-infected file when the virus signature of at least one of the set of virus definitions does not match the located data in the executable file being scanned.

~~13.~~14. The apparatus of claim 8, wherein the set of virus definitions include at least two virus definitions that have different virus signatures and the same file offset.

15. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instruction which, when executed by a device, cause the device to:

load an executable file being scanned from a storage device into the memory;

identify a set of virus definitions for the executable file from a virus feature library, each virus definition including a virus signature and a corresponding file offset address;

without decompiling the executable file,

locate data in ~~a~~ the executable file being scanned that has been loaded in the memory according to a file offset address associated with each of the set of virus definitions, wherein the data has a predefined length of a virus signature of ~~a~~ the corresponding virus definition;

make a comparison of the virus signature with the data located in the executable file being scanned; and

determine that the executable file being scanned is a virus-infected file when the virus signature of at least one of the set of virus definitions matches the located data in the executable file being scanned.

~~14.~~16. The computer readable storage medium of claim ~~11~~15, including instructions which cause the device to:

locate, in the executable file being scanned and according to the file offset address associated with the virus signature of the corresponding virus definition, the data, with the file offset address as the starting point of the located data.

~~15.~~17. The computer readable storage medium of ~~any of~~ claims ~~11~~15 ~~and 12~~, including instructions which cause the device to:

make a comparison of the virus signature with the data located in the executable file being scanned, with the file offset address as the starting point of the located data, wherein the lengths of the located data and the virus signature are the same.

~~16.~~18. The computer readable storage medium of ~~any of~~ claims ~~11~~15 ~~and 13~~, including instructions which cause the device to, before locating the data in the executable file being scanned that has been loaded in the memory according to the file offset address associated with each of the set of ~~the~~ virus definitions: ~~signature of the virus:~~

judge whether to perform the locating on the executable file being scanned according to the file offset address associated with the virus signature; and

skip the locating when the file offset address is greater than the size of the executable file being scanned.

~~17.~~19. The computer readable storage medium of ~~any of~~ claims ~~11~~15 ~~and 14~~, including instructions which cause the device to, before locating the data in the executable file being scanned that has been loaded in the memory according to the file offset address associated with each of the set of~~the~~ virus ~~signature of the virus~~definitions:

read the executable file being scanned from a disk, and store the executable file being scanned in a cache.

20. The computer readable storage medium of claim 15, wherein the set of virus definitions include at least two virus definitions that have different virus signatures and the same file offset.