

record remaining in a communication packet and a hard disk as a main analysis target, and cannot be applied to a situation in which a live forensics technology is required.

[0031]

5 ~~The~~Embodiments of the present invention ~~is~~are made in consideration of the situation as described above. ~~That is, a main object-~~
Embodiments of the present invention ~~is to~~ provide an analysis device and the like, being capable of efficiently recording at least part of data representing a state of analysis target equipment acquired from the analysis target equipment, into a storage device with a certain capacity, in accordance with a policy.

[Solution to Problem]

[0032]

15 ~~To achieve an above-described objective, According to a first aspect, there is provided an analysis apparatus according to one aspect of the present invention includes~~ comprising: a dispatcher that is configured to be communicably connected to an analysis target device that performs operational processing by use of a processor and a memory unit, which is communicably connected to the processor, and to generate collection target data for reproducing at least part of a state of the operational processing in the analysis target device, in accordance with data being transmitted and received between the processor and the memory unit; a data mapper that is configured to assign, to one or more areas included in the collection target data, tag information for identifying the area; and a data writer that is
20 configured to save the one or more areas into a first storage device with a specific storage capacity, in accordance with a first policy defining, by use of the tag information, a procedure of saving the collection target data into the first storage.

[0032a]

According to a second aspect, there is provided an analysis apparatus comprising: a dispatcher that is configured to be communicably connected to an analysis target system including a first processing unit performing any processing and storing a state of the processing as first state information, and a second processing unit communicably connected to the first processing unit performing any processing and storing a state of the processing as second state information, to acquire data being transmitted and received between the first processing unit and the second processing unit, and, in accordance with the acquired data, to generate collection target data for reproducing a state of the analysis target system, by reproducing at least one of the first state information and the second state information; a data mapper that is configured to assign, to one or more areas included in the collection target data, tag information for identifying the area; and a data writer that is configured to save the one or more areas into a first storage device with a specific storage capacity, in accordance with a first policy defining, by use of the tag information, a procedure of saving the collection target data into the first storage device.

[0033]

~~An~~According to a third aspect, there is provided an analysis method ~~according to another aspect of the present invention includes comprising,~~ generating collection target data for reproducing at

least part of a state of operational processing in an analysis target device, in accordance with data being transmitted and received between a processor and a memory unit being communicably connected to the processor in the analysis target device that performs operational

5 processing by use of the processor and the memory unit; assigning, with respect to one or more areas included in the collection target data, tag information for identifying the area; and saving the one or more areas into a first storage device with a specific storage capacity, in accordance with a first policy defining, by use of the tag information, a procedure of saving
10 the collection target data into the first storage device .

[0034]

~~The objective is also achieved by~~ Disclosed herein is a computer program and a computer-readable storage medium in which the computer program is stored (recorded), that provide, by a computer, an analysis
15 device including the aforementioned configuration, and the corresponding analysis method.

[0034a]

According to a fourth aspect, there is provided a storage medium recording a computer program causing a computer that is configured to
20 analyze a state of operational processing in an analysis target device that performs operational processing by use of a processor and a memory unit communicably connected to the processor, to perform: processing of
generating collection target data for reproducing at least part of a state of operational processing in the analysis target device, in accordance with
25 data being transmitted and received between the processor and the memory unit in the analysis target device; processing of assigning, with respect to one or more areas included in the collection target data, tag information for identifying the area; and processing of saving the one or more areas into a first storage device with a specific storage capacity, in accordance with a

first policy defining, by use of the tag information, a procedure of saving the collection target data into the first storage device.

[Advantageous Effects of Invention]

[0035]

5 ~~The~~Embodiments of the present invention ~~is~~are able to efficiently record at least part of data representing a state of analysis target equipment acquired from the analysis target equipment, into a storage device with a specific capacity, in accordance with a policy. In other words, embodiments of the present invention ~~is~~are able to save a larger amount of

10 data, by which a state of analysis target equipment can be reproduced, by use of a storage device with a limited storage capacity.

[Brief Description of Drawings]

[0036]

[Fig. 1] Fig. 1 is a block diagram exemplifying functional

15 configurations of an analysis device and an analysis target device,

~~AMENDMENTS UNDER ARTICLE 19 OF THE PCT~~CLAIMS~~CLAIMS~~~~[Claim 1]~~

1. An analysis apparatus comprising:

5 a dispatcher that is configured to be communicably connected to an analysis target device that performs operational processing by use of a processor and a memory unit, which is communicably connected to the processor, and to generate collection target data for reproducing at least part of a state of the operational processing in the analysis target device, in accordance with data being transmitted and received between the processor and the memory unit;

a data mapper that is configured to assign, to one or more areas included in the collection target data, tag information for identifying the area; and

15 a data writer that is configured to save the one or more areas into a first storage device with a specific storage capacity, in accordance with a first policy defining, by use of the tag information, a procedure of saving the collection target data into the first storage device.

~~[Claim 2]~~

20 2. The analysis apparatus according to Claim 1, wherein

the collection target data include at least one of data representing an operating state of the processor and data stored in the memory unit, when the data being a source of the collection target data is acquired.

~~[Claim 3]~~

25 3. The analysis apparatus according to Claim 1 or 2, wherein

the data writer saves saved data that indicates a relation between the tag information, save-target data that are included in the one or more areas assigned with the tag information, and record timing information, into the first storage device, the record timing information indicating a

timing when the saved data is recorded.

~~[Claim 4]~~

4. The analysis apparatus according to Claim 3, wherein
for each of one or more pieces of the tag information, the first
5 policy includes information for specifying a storage area into which the
saved data associated with the piece of the tag information are saved in the
first storage device, and information indicating a saving method used to
saving the saved data into the storage area, and

the data writer saves the saved data into the first storage device, in
10 accordance with the first policy.

~~[Claim 5]~~

5. The analysis apparatus according to Claim 4, wherein
the saving method of the saved data is a method that is able to
specify an area into which a new piece of the saved data is saved , among
15 areas into which the saved data are saved in the first storage device.

~~[Claim 6] AMENDED UNDER ARTICLE 19 OF THE PCT~~

6. The analysis apparatus according to any one of Claims 3 to 5,
wherein

the data mapper assigns the tag information with respect to the one
20 or more areas included in the collection target data, in accordance with
mapping data indicating a relation between information for specifying the
one or more areas into which the collection target data are divided, and the
tag information for identifying the area,

~~[Claim 7]~~

25 7. The analysis apparatus according to Claim 6, wherein
the mapping data indicate a relation between memory-area
specification information that specifies one or more areas into which the
collection target data are divided, based at least part on an area in the

memory unit into which stored data which are included in the collection target data are stored, and the tag information for identifying the one or more areas into which the collection target data are divided, and

the data mapper assigns the tag information with respect to the one or more areas included in the collection target data, in accordance with the mapping data.

~~[Claim 8] AMENDED UNDER ARTICLE 19 OF THE PCT~~

8. The analysis apparatus according to Claim 7, further comprising:
a map generator that is configured to

divide stored data included in the collection target data into a plurality of areas, in accordance with information representing an architecture of the analysis target device, and

generate the mapping data indicating, for each of a plurality of the divided areas, a relation between the memory-area specification information for specifying the divided area, and the tag information for identifying an area specified by the memory-area specification information.

~~[Claim 9]~~

9. The analysis apparatus according to any one of Claims 6 to 8, further comprising a second storage device having a larger storage capacity than the first storage device, wherein

the data writer saves the saved data being saved in the first storage device into the second storage device, in accordance with a second policy defining a procedure of saving the saved data saved in the first storage device into the second storage device.

~~[Claim 10]~~

10. The analysis apparatus according to Claim 9, wherein
the second policy includes

save necessity information for specifying whether or not to

save the saved data saved in the first storage device into the second storage device, and

accumulation method information for at least specifying a trigger for saving the saved data saved in the first storage device into the second storage device, and,

when the data writer determines to save the saved data saved in the first storage device into the second storage device, in accordance with the save necessity information set to the second policy, the data writer saves at least part of the saved data saved in the first storage device into the second storage device, by detecting the trigger in accordance with the accumulation method information.

~~[Claim 11]~~

11. The analysis apparatus according to Claim 9 or 10, wherein when deleting the saved data, from the first storage device, being already saved in the first storage device,

the data writer determines whether or not to save the saved data to be deleted from the first storage device into the second storage device, in accordance with the first policy or the second policy, and saves the saved data to be deleted from the first storage device, into the second storage device in accordance with the determination.

~~[Claim 12]~~

12. The analysis apparatus according to any one of Claims 9 to 11, further comprising record management means for notifying the data writer of a request for saving the saved data saved in the first storage device into the second storage device, wherein

the data writer saves the saved data saved in the first storage device into the second storage device, in accordance with the request received from the record management means.

~~[Claim 13]~~

13. The analysis apparatus according to Claim 12, wherein
the record management means is configured to be communicably
connected to a sensor for detecting a predetermined event that can affect
operational processing in the analysis target device, and to notify the data
5 writer of the request, in accordance with detection information about the
predetermined event being notified by the sensor.

~~[Claim 14] AMENDED UNDER ARTICLE 19 OF THE PCT~~

14. The analysis apparatus according to Claims 6 to 13, further
comprising, at least a same number of the dispatchers as the analysis target
10 devices, and at least a same number of the data mappers as the dispatchers,
when a plurality of the analysis target devices exist, wherein

different dispatchers are communicably connected to a plurality of
the analysis apparatuses respectively,

different mappers assign, to one or more areas included in the
15 collection target data generated respectively in the different dispatchers,
tag information for identifying the area,

the first policy includes, for each of one or more pieces of the tag
information, information for identifying the different dispatchers ,
information for specifying a storage area into which the saved data
20 associated with the piece of the tag information are saved in the first
storage device, and information indicating a saving method of saving the
saved data into a storage area specified by the information, these pieces of
the information being associated with one another, and

the data writer saves the one or more areas included in the
25 collection target data into the first storage device as the saved data, in
accordance with the first policy.

~~[Claim 15]~~

15. The analysis apparatus according to any one of Claims 6 to 14,
further comprising:

a data reader that is configured

to extract one or more pieces of the saved data saved in the first storage device,

to extract the tag information, being set to the piece of the saved data, and the save-target data, for each of the extracted one or more pieces of the saved data, and,

to generate, by referring to the mapping data, reproduction data in which the extracted save-target data are arranged in an area associated with the extracted tag information; and

a player that is configured

to be communicably connected to a reproduction target device performing operational processing by use of a processor and a memory unit which is communicably connected to the processor, and,

in accordance with the reproduction data generated in the data reader, to load data, stored in the memory unit in the analysis target device, into a memory unit in the reproduction target device, when the reproduction data include the data stored in the memory unit in the analysis target device, and,

in accordance with the reproduction data generated in the data reader, to load data, included in the reproduction data and representing an operating state of the processor in the analysis target device, into the processor in the reproduction target device, when the reproduction data include the data representing the operating state of the processor in the analysis target device.

~~[Claim 16] AMENDED UNDER ARTICLE 19 OF THE PCT~~

16. The analysis apparatus according to Claim 15, wherein

the data reader reads, by referring to the first storage device, one or more pieces of the saved data having the the record timing information to which a same timing is set, among the saved data saved in the first storage

device.

~~[Claim 17]~~

17. The analysis apparatus according to Claim 16, wherein
when loading the reproduction data into the processor in the
5 reproduction target device or the memory unit in the reproduction target
device, the player lowers a processing speed of the processor in the
reproduction target device.

~~[Claim 18]~~

18. The analysis apparatus according to any one of Claims 15 to 17,
10 further comprising a same number of the players as a plurality of the
reproduction target devices, when a plurality of the reproduction target
devices exist, wherein
the players different from one another among a plurality of the
players are communicably connected to the respective reproduction target
15 devices among the plurality of the reproduction target devices, and,
in accordance with the reproduction data generated in the
respective data reader, each of the plurality of the players,

loads data stored in the memory unit in the analysis target
device into a memory unit in the reproduction target device connected to
20 the player, when the data stored in the memory unit in the analysis target
device are included in the reproduction data, and,

loads an operating state of the processor in the analysis
target device into a processor in the reproduction target device connected
to the player, when data representing the operating state of the processor in
25 the analysis target device are included in the reproduction data.

~~[Claim 19]~~

19. The analysis apparatus according to any one of Claims 1 to 18,
wherein
the dispatcher generates the collection target data, in accordance

with a sampling interval being set.

~~[Claim 20]~~

20. The analysis apparatus according to Claim 4, wherein
the saving method of the saved data is

5 a method that is able to determine whether or not a new
piece of the saved data can be saved into an area in which the saved data
are already saved in the first storage device.

~~[Claim 21]~~

21. An analysis apparatus comprising:

10 a dispatcher that is configured to

be communicably connected to an analysis target system
including a first processing unit performing any processing and storing a
state of the processing as first state information, and a second processing
unit communicably connected to the first processing unit performing any
15 processing and storing a state of the processing as second state
information,

to acquire data being transmitted and received between the
first processing unit and the second processing unit, and,

in accordance with the acquired data, to generate collection
20 target data for reproducing a state of the analysis target system, by
reproducing at least one of the first state information and the second state
information;

a data mapper that is configured to assign, to one or more areas
included in the collection target data, tag information for identifying the
25 area; and

a data writer that is configured to save the one or more areas into a
first storage device with a specific storage capacity, in accordance with a
first policy defining, by use of the tag information, a procedure of saving
the collection target data into the first storage device.

~~[Claim 22]~~

22. An analysis method comprising, by an information processing apparatus:

generating collection target data for reproducing at least part of a state of operational processing in an analysis target device, in accordance with data being transmitted and received between a processor and a memory unit being communicably connected to the processor in the analysis target device that performs operational processing by use of the processor and the memory unit;

assigning, with respect to one or more areas included in the collection target data, tag information for identifying the area; and

saving the one or more areas into a first storage device with a specific storage capacity, in accordance with a first policy defining, by use of the tag information, a procedure of saving the collection target data into the first storage device.

~~[Claim 23]~~

23. A storage medium recording a computer program causing a computer that is configured to analyze a state of operational processing in an analysis target device that performs operational processing by use of a processor and a memory unit communicably connected to the processor, to perform:

processing of generating collection target data for reproducing at least part of a state of operational processing in the analysis target device, in accordance with data being transmitted and received between the processor and the memory unit in the analysis target device;

processing of assigning, with respect to one or more areas included in the collection target data, tag information for identifying the area; and

processing of saving the one or more areas into a first storage device with a specific storage capacity, in accordance with a first policy

defining, by use of the tag information, a procedure of saving the collection target data into the first storage device.