

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 Embodiments of the present invention are made in consideration of the situation as described above. Embodiments of the present invention 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
10 device with a certain capacity, in accordance with a policy.

[Solution to Problem]

[0032]

 According to a first aspect, there is provided an analysis apparatus comprising: a dispatcher that is configured to be communicably connected
15 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
20 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 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
25 procedure of saving the collection target data into the first storage 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,

the data mapper assigns the tag information with respect to the one 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 which are included in the collection target data, and the tag information for identifying the area, and the data writer saves the saved data being saved in the first storage device into a 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.

[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 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,

the data mapper assigns the tag information with respect to the one 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 which are included in the collection target data, and the tag information for identifying the area, and the data writer saves the saved data being saved in the first storage device

9c

into a 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.

[0033]

5 According to a third aspect, there is provided an analysis method 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 wherein a 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
15 data is recorded,

a data mapper assigns the tag information with respect to the one 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 which are included in the collection target data, and the
20 tag information for identifying the area, and
the data writer saves the saved data being saved in the first storage device
into a 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.

25 [0034]

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 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 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 wherein a 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,

a data mapper assigns the tag information with respect to the one 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 which are included in the collection target data, and the tag information for identifying the area, and the data writer saves the saved data being saved in the first storage device into a 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.

[Advantageous Effects of Invention]

[0035]

Embodiments of the present invention are able to efficiently record at least part of data representing a state of analysis target equipment
5 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 are able to save a larger amount of data, by which a state of analysis target equipment can be reproduced, by use of a storage device with a limited storage capacity.

10 [Brief Description of Drawings]

[0036]

[Fig. 1] Fig. 1 is a block diagram exemplifying functional configurations of an analysis device and an analysis target device,

CLAIMS

1. An analysis apparatus 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 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, 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,

the data mapper assigns the tag information with respect to the one 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 which are included in the collection target data, and the tag information for identifying the area, and

the data writer saves the saved data being saved in the first storage device into a 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.

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,
5 when the data being a source of the collection target data is acquired.

3. The analysis apparatus according to Claim 1, wherein
for each of one or more pieces of the tag information, the first
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
5 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
accordance with the first policy.
4. The analysis apparatus according to Claim 3, wherein
10 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
areas into which the saved data are saved in the first storage device.
5. The analysis apparatus according to Claim 4, wherein
15 the mapping data indicate a relation between memory-area
specification information that specifies one or more areas which are
included in the collection target data, 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 which are included in the collection target data, and

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

6. The analysis apparatus according to Claim 5, further comprising:
a map generator that is configured to

divide stored data included in the collection target data into
10 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
15 identifying an area specified by the memory-area specification
information.

7. The analysis apparatus according to Claim 1, wherein
the second policy includes
20 accumulation 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
5 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 accumulation necessity information set to the second policy, the data
10 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.

8. The analysis apparatus according to Claim 7, wherein
when deleting the saved data, from the first storage device, being
15 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
20 device in accordance with the determination.

9. The analysis apparatus according to Claim 7 or 8, 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

25 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.

10. The analysis apparatus according to Claim 9, 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 writer of the request, in accordance with detection information about the predetermined event being notified by the sensor.

11. The analysis apparatus according to any one of Claims 5 to 10, further comprising, at least a same number of the dispatchers as the analysis target 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 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 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, and

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

12. The analysis apparatus according to any one of Claims 5 to 11, 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
5 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

10 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
15 data reader, to load data, stored in the memory unit in the analysis target
device, into the 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
20 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.

25 13. The analysis apparatus according to Claim 12, 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.

14. The analysis apparatus according to Claim 13, wherein
when loading the reproduction data into the processor in the
reproduction target device or the memory unit in the reproduction target
5 device, the player lowers a processing speed of the processor in the
reproduction target device.

15. The analysis apparatus according to any one of Claims 12 to 14,
further comprising a same number of the players as a plurality of the
reproduction target devices, when a plurality of the reproduction target
10 devices exist, wherein

the players different from one another among a plurality of the
players are communicably connected to the respective reproduction target
devices among the plurality of the reproduction target devices, and,

in accordance with the reproduction data generated in the
15 respective data reader, each of the plurality of the players,

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

20 loads data representing 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 the analysis target device are included in the reproduction
data.

25 16. The analysis apparatus according to any one of Claims 1 to 15,
wherein

the dispatcher generates the collection target data, in accordance

with a sampling interval being set.

17. The analysis apparatus according to Claim 3, 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.

18. An analysis apparatus comprising:
a dispatcher that is configured to

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

15 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
20 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
25 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, 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,

5 the data mapper assigns the tag information with respect to the one 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 which are included in the collection target data, and the tag information for identifying the area, and

10 the data writer saves the saved data being saved in the first storage device into a 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.

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

- 5 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;
- 10 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
- 15 the first storage device, wherein a 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,
- 20 a data mapper assigns the tag information with respect to the one 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 which are included in the collection target data, and the tag information for identifying the area, and
- 25 the data writer saves the saved data being saved in the first storage device into a 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.

20. 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
5 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;

10 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 wherein a 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
5 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,

a data mapper assigns the tag information with respect to the one or more areas included in the collection target data, in accordance with
10 mapping data indicating a relation between information for specifying the one or more areas which are included in the collection target data, and the tag information for identifying the area, and
the data writer saves the saved data being saved in the first storage device into a second storage device, in accordance with a second policy defining a
15 procedure of saving the saved data saved in the first storage device into the second storage device.