

RECONSTRUCTING A DATASET AFTER DETECTION OF A NETWORK SECURITY THREAT IN A NETWORK

ABSTRACT

The present disclosure concerns a computer-implemented method for reconstructing a dataset after detection of a network security threat in a network. The method comprises: determining a maximum flow for returning data associated with the network security threat to a source dataset via each of a plurality of paths through which the data has passed from the source dataset to the destination dataset; starting from the destination dataset, determining the data to be transferred to each dataset in the plurality of paths between the destination dataset and the one or more source datasets such that the data can be returned to the one or more source datasets, the data transferred in each path not exceeding the determined maximum flow for the path; adding the details of the determined amount of data to be transferred to a forensic report; and outputting the forensic report.

[Figure 13]