CLAIM LISTING FOR ’789 PATENT

COUNT 1

1. Claim 1

   a) Limitation [1 Pre] “A method of examining packets passing through a connection point on a computer network, each packets conforming to one or more protocols, the method comprising:”

   b) Limitation [1a] “(a) receiving a packet from a packet acquisition device;”

   c) Limitation [1b] “(b) performing one or more parsing/extraction operations on the packet to create a parser record comprising a function of selected portions of the packet;”

   d) Limitation [1c] “(c) looking up a flow-entry database comprising none or more flow-entries for previously encountered conversational flows, the looking up using at least some of the selected packet portions and determining if the packet is of an existing flow;”

   e) Limitation [1d] “(d) if the packet is of an existing flow, classifying the packet as belonging to the found existing flow; and”

   f) Limitation [1e] “(e) if the packet is of a new flow, storing a new flow-entry for the new flow in the flow-entry database, including identifying information for future packets to be identified with the new flow-entry,”

   g) Limitation [1f] “wherein the parsing/extraction operations depend on one or more of the protocols to which the packet conforms.”

2. Claim 2

   a) Limitation [2] “A method according to claim 1, wherein each packet passing through the connection point is examined in real time.”

3. Claim 13

   a) Limitation [13a] “A method according to claim 1, wherein step (d) includes if the packet is of an existing flow, obtaining the last encountered state of the flow and performing any state operations specified for the state of the flow starting from the last encountered state of the flow; and”

   b) Limitation [13b] “wherein step (e) includes if the packet is of a new flow, performing any state operations required for the initial state of the new flow.”

CLAIM LISTING FOR ’789 PATENT

4. Claim 14
    - a) Limitation [14] “A method according to claim 13, wherein the state processing of each received packet of a flow furthers the identifying of the application program of the flow.”
5. Claim 15
    - a) Limitation [15] “A method according to claim 13, wherein the state operations include updating the flow-entry, including storing identifying information for future packets to be identified with the flow-entry.”
6. Claim 16
    - a) Limitation [16] “A method according to claim 15, wherein the state processing of each received packet of a flow furthers the identifying of the application program of the flow.”
7. Claim 17
    - a) Limitation [17] “A method according to claim 13, wherein the state operations include searching the parser record for the existence of one or more reference strings.”

COUNT 2

1. Claim 44
    - a) Limitation [44 Pre] “A method of examining packets passing through a connection point on a computer network, the method comprising:”
    - b) Limitation [44a] “(a) receiving a packet from a packet acquisition device;”
    - c) Limitation [44b] “(b) performing one or more parsing/extraction operations on the packet according to a database of parsing/extraction operations to create a parser record comprising a function of selected portions of the packet, the database of parsing/extraction operations including information on how to determine a set of one or more protocol dependent extraction operations from data in the packet that indicate a protocol is used in the packet;”
    - d) Limitation [44c] “(c) looking up a flow-entry database comprising none or more flow-entries for previously encountered conversational flows, the looking up using at least some of the

selected packet portions, and determining if the packet is of an existing flow;"

e) Limitation [44d] "(d) if the packet is of an existing flow, obtaining the last encountered state of the flow and performing any state operations specified for the state of the flow starting from the last encountered state of the flow; and"

f) Limitation [44e] "(e) if the packet is of a new flow, performing any analysis required for the initial state of the new flow and storing a new flow-entry for the new flow in the flow-entry database, including identifying information for future packets to be identified with the new flow-entry."

2. Claim 48

   a) Limitation [48] "A method according to claim 44, further comprising forming a signature from the selected packet portions, wherein the lookup operation uses the signature and wherein the identifying information stored in the new or updated flow-entry is a signature for identifying future packets."

3. Claim 49

   a) Limitation [49] "A method according to claim 44, wherein the state operations are according to a database of protocol dependent state operations."

COUNT 3

1. Claim 19

   a) Limitation [19 Pre] "A packet monitor for examining packets passing through a connection point on a computer network, each packets conforming to one or more protocols, the monitor comprising:"

   b) Limitation [19a] "(a) a packet acquisition device coupled to the connection point and configured to receive packets passing through the connection point;"

   c) Limitation [19b] "(b) an input buffer memory coupled to and configured to accept a packet from the packet acquisition device;"

   d) Limitation [19c] "(c) a parser subsystem coupled to the input buffer memory and including a slicer, the parsing subsystem configured to extract selected portions of the accepted packet and to output a parser record containing the selected portions;"

e) Limitation [19d] “(d) a memory for storing a database comprising one or more flow-entries for previously encountered conversational flows, each flow-entry identified by identifying information stored in the flow-entry;”

f) Limitation [19e] “(e) a lookup engine coupled to the output of the parser subsystem and to the flow-entry memory and configured to lookup whether the particular packet whose parser record is output by the parser subsystem has a matching flow-entry, the looking up using at least some of the selected packet portions and determining if the packet is of an existing flow; and”

g) Limitation [19f] “(f) a flow insertion engine coupled to the flow-entry memory and to the lookup engine and configured to create a flow-entry in the flow-entry database, the flow-entry including identifying information for future packets to be identified with the new flow-entry,”

h) Limitation [19g] “the lookup engine configured such that if the packet is of an existing flow, the monitor classifies the packet as belonging to the found existing flow; and”

i) Limitation [19h] “if the packet is of a new flow, the flow insertion engine stores a new flow-entry for the new flow in the flow-entry database, including identifying information for future packets to be identified with the new flow-entry,”

j) Limitation [19i] “wherein the operation of the parser subsystem depends on one or more of the protocols to which the packet conforms.”

2. Claim 20

a) Limitation [20] “A monitor according to claim 19, wherein each packet passing through the connection point is accepted by the packet buffer memory and examined by the monitor in real time.”

3. Claim 31

a) Limitation [31a] “A packet monitor according to claim 19, further comprising: a compiler processor coupled to the parsing/extraction operations memory, the compiler processor configured to run a compilation process that includes:”

b) Limitation [31b] “receiving commands in a high-level protocol description language that describe the protocols that may be used in packets encountered by the monitor and any children protocols thereof, and”

c) Limitation [31c] “translating the protocol description language commands into a plurality of parsing/extraction operations that are initialized into the parsing/extraction operations memory.”

4. Claim 42

a) Limitation [42] “A monitor according to claim 19, wherein the lookup engine begins processing as soon as a parser record arrives from the parser subsystem.”

Count 4

1. Claim 33

a) Limitation [33] “A packet monitor according to claim 19, further comprising: a cache subsystem coupled to and between the lookup engine and the flow-entry database memory providing for fast access of a set of likely-to-be-accessed flow-entries from the flow-entry database.”

2. Claim 34

a) Limitation [34] “A packet monitor according to claim 33, wherein the cache subsystem is an associative cache subsystem including one or more content addressable memory cells (CAMs).”