

Open Text Inc.,

v.

AO Kaspersky Lab,

IPR2023-00124

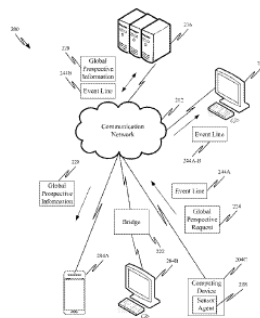
Patent Owner's Oral Argument Presentation

King & Spalding, LLP

March 14, 2024



19 Claims, 15 Drawing Sheets



2

U.S. Patent No. 9,578,045 Improves upon the Prior Art

The system filters may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in U.S. application Ser. No. 13/372,375 filed Feb. 13, 2012, “Methods and Apparatus for Dealing with Malware” (US-2012-0260340-A1), which is incorporated herein by reference in its entirety for all that it teaches and for all purposes. These filters intercept system events in a manner such that the operation of the system filter does not impact system performance, a key aspect of this solution. Events at this level tend to be very raw and generally not individually useful—on an average system, tens of millions of events take place every minute and the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. A product which impacts system performance will have considerably diminished value to an administrator and can negatively affect the results of an analysis undertaken. For example, a system

What is claimed is:

1. A method comprising:

gathering one or more events defining an action of a first object acting on a target;

generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;

assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line.

U.S. Patent No. 9,578,045 Improves upon the Prior Art

8. A system for providing forensic visibility into a system, comprising:
a device including:
a communication interface;
a processor;
data storage; and
a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
gather one or more events defining an action of a first object acting on a target;
generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;
assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and
transmit the assembled event line utilizing the communication interface.

16. A system for providing forensic visibility into a system, comprising:
a device including:
a communication interface;
a processor;
data storage; and
a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
gather one or more events defining an action of a first object acting on a target;
generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network; and
transmit the assembled event line utilizing the communication interface.

U.S. Patent No. 9,578,045 Improves upon the Prior Art

10. The system of claim 8, further comprising:
a global perspective information server; and
an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.

Petitioner's Grounds Fail

Grounds 1 fails because:

- Morris does not render obvious the “originating object” limitation (claims 1-4, 8-10, 12, and 16)
- Morris does not disclose or render obvious a “sensor agent stored on the data storage that is executable by the processor” because there is no sensor agent in Morris that requires all steps required of the sensor agent (claims 8-10, 12, and 16)
- Morris does not render obvious the claimed end recipient device or transmitting an event line thereto (claim 10)
- Van Oorschot does not render obvious an event priority using an originating object (claim 3)

Grounds 2 fails because:

- As the Board correctly found, Capalik does not disclose or render obvious the “across a network” limitation (claims 1-4, 7-10, 12, 15-18)
- Van Oorschot does not render obvious an event priority using an originating object (claim 3)

**Ground 1– “originating object”
(Claims 1-4, 8-10, 12, and 16)**

"Originating Object": *"the object that directly initiated or otherwise created the first object"*

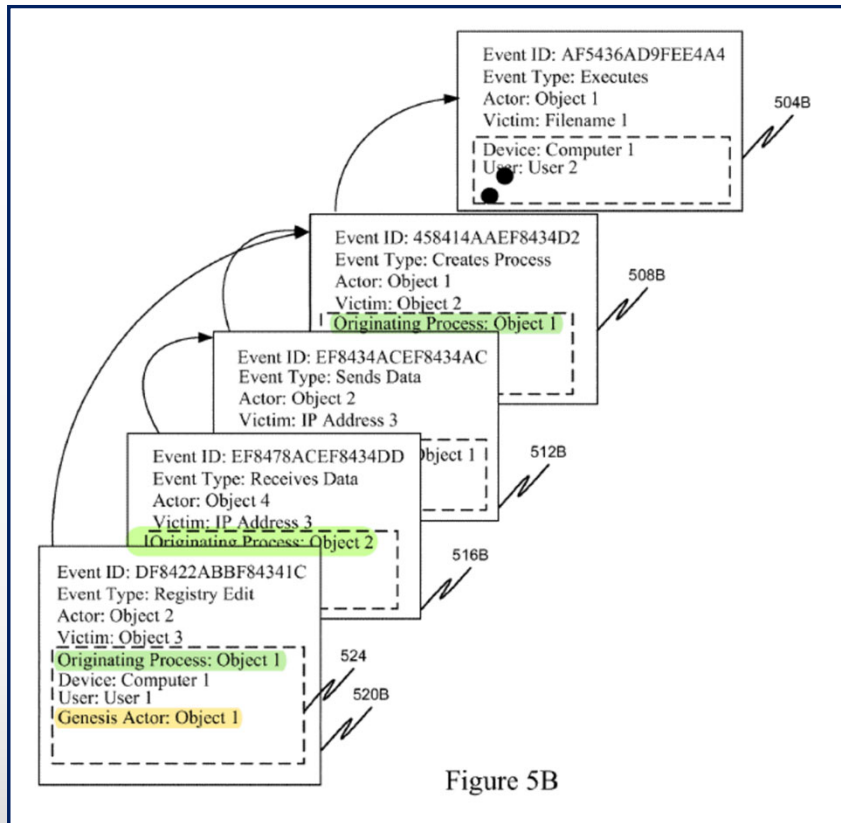
- '045 patent repeatedly distinguishes between an originating object and GenesisActor

Contextual state information may include, but is not limited to, originating processes, devices, and users. Additionally, contextual state information may include GenesisActor information and ancillary data. GenesisActor information may contain the object that is not the direct Actor of an event but which is the ultimate parent of the event being performed. For example in the case of a software installation, the GenesisActor would be the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe. Ancillary data may include

As illustrated in FIG. 5B, a contextual analysis may be applied to the captured events 504B-520B. Accordingly, a context 520B comprising an origination process, Device, User, and in some instances, a GenesisActor may further supplement or enhance the Event ID, Event Type, Actor, and Victim. Although illustrated as including an originating process, GenesisActor, device, and user, the contextual information forming the contextual state 520B may include more or less information and in varying combinations. Moreover, as illustrated in FIG. 5B, the originating process or object may be determined based on a previous event that initiated or otherwise created the current process and/or object. Additionally, as illustrated in FIG. 5B, the GenesisActor is determined based on a chain of previous events. For example, the Actor of Object 1 for system event 504B of Event Type "executes" operates on Filename 1. Object 1 subsequently creates a process Object 2 in 508B which is further utilized in both 516B and 520B. Accordingly, as the Object 1 initiated subsequent events, Object 1 may be determined to be the GenesisActor for 520B, 516B, 512B, and 508B.

"Originating Object": *"the object that directly initiated or otherwise created the first object"*

- The specification repeatedly presents the originating object and the GenesisActor as separate pieces of information



As illustrated in FIG. 5B, a contextual analysis may be applied to the captured events **504B-520B**. Accordingly, a context **520B** comprising an origination process, Device, User, and in some instances, a GenesisActor may further supplement or enhance the Event ID, Event Type, Actor, and Victim. Although illustrated as including an originating process, GenesisActor, device, and user, the contextual information forming the contextual state **520B** may include more or less information and in varying combinations. Moreover, as illustrated in FIG. 5B, the originating process or object may be determined based on a previous event that initiated or otherwise created the current process and/or object. Additionally, as illustrated in FIG. 5B, the GenesisActor is determined based on a chain of previous events. For example, the Actor of Object 1 for system event **504B** of Event Type "executes" operates on Filename 1. Object 1 subsequently creates a process Object 2 in **508B** which is further utilized in both **516B** and **520B**. Accordingly, as the Object 1 initiated subsequent events, Object 1 may be determined to be the GenesisActor for **520B**, **516B**, **512B**, and **508B**.

“Originating Object”: *“the object that directly initiated or otherwise created the first object”*

- The “originating object” is different from GenesisActor because the “originating object” supports providing a full audit trail while GenesisActor may skip steps.

The context analyzer 348 ensures that a user at the end recipient 220 is provided with the deepest view of the most important data but still has access to the full range of data if they wish to see it. Accordingly, the context analyzer 348 correlates objects within system events to additional objects known to exist. For example, the context analyzer 348 may correlate an actor, victim, and/or event type to one or more originating processes, devices, and users. Such a correlation creates an audit trail for each individual event. As will be described later, this audit trail allows an administrator, at an end recipient 220 for example, to forensically track back any event which occurs to what triggered it. Accordingly, this additional information, including the originating processes, devices, and user, allows a contextual state to be established

57. A full audit trail that allows forensic tracking back to “any event which occurs to what triggered it” requires each individual event’s immediate parent. Skipping to the ultimate parent, as Petitioner proposes through its implicit “originating object” construction, results in an incomplete event audit trail due to gaps between the immediate parent and the ultimate parent. In contrast with Petitioner’s construction, the ’045 patent uses the claimed “originating object” to create a full audit trail “to forensically track back any event which occurs to what triggered it.” (See EX-1001 12:55–63.) A full audit trail cannot be achieved with GenesisActor information because there would be gaps between the originating object (i.e., immediate parent) and the ultimate parent.

Morris does not disclose an “originating object”

- Morris’s teaching of skipping to the GenesisActor prevents the full audit trail of the ’045 patent

[0107] “Genesisactor”—the key of an object that is not the direct Actor of an event but which is the ultimate parent of the event being performed. For example in the case of a software installation, this would be the key of the object that the user or system first executed and that initiated the software installation process, e.g. Setup.exe.

**Ground 1 – “sensor agent . . .”
(Claims 8-10, 12, and 16)**

Morris does not disclose an “sensor agent” with all limitations of claims 8 and 16

- Claims 8 and 16 requires a “sensor agent” operable to do several things

8. A system for providing forensic visibility into a system, comprising:
a device including:
a communication interface;
a processor;
data storage; and
a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
gather one or more events defining an action of a first object acting on a target;
generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;
assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, and the originating object; and
transmit the assembled event line utilizing the communication interface.

16. A system for providing forensic visibility into a system, comprising:
a device including:
a communication interface;
a processor;
data storage; and
a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:
gather one or more events defining an action of a first object acting on a target;
generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network; and
transmit the assembled event line utilizing the communication interface.

Petitioner's Alleged "Sensor Agent" in Morris: Remote Computer 2

[8(e)] a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to:

Supra, [8(c)-(d)] (describing remote computer 2 configured with "local 'agent' software" for effectuating the described methods and the processor for executing the functions of the "local 'agent' software").

The remaining limitations of Claim 8 are substantively identical to method steps of Claim 1 and are rendered obvious for the same reasons detailed in Claim 1.

See Claim Appendix.

“Sensor Agent” (Remote Computer 2) Must “Gather One or More Events” (Claims 8 and 16)

gather one or more events defining an action of a first object acting on a target;

[1(a)] gathering an event defining an action of a first object acting on a target,

Morris discloses that “the base computer” gathers “events initiated by or involving the object when the object is created, configured or runs on the respective remote computers.” *Morris*, [0018].

"Sensor Agent" (Remote Computer 2) Must "Generate a Contextual State" (Claims 8 and 16)

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

- Petition does not identify any device that performs this step. Petition 14-15, 32, 35-36
 - This is fatal to Claims 8 and 16

"Sensor Agent" (Remote Computer 2) Must "Generate a Contextual State" (Claims 8 and 16)

generate a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

- Petition relies on "GenesisActor" as the "originating object." Petition 15-16, Morris ¶ 107.

As discussed above in limitation [1(b)], *Morris* discloses generating a contextual state including the "Genesisactor," which is "the ultimate parent of the event being performed." *Supra*, [1(b)]. The disclosed "Genesisactor" teaches the claimed contextual state including an indication of the originating object of the first object. }

- Reply abandons "GenesisActor" as "originating object" for this limitation. Reply 10, Morris ¶87

Morris, [0087], *see also* [0018]. In particular, paragraph [0087] of *Morris* makes clear that the "events initiated by or involving the object when the object is created, configured or runs" provide "contextual state information for the event including an originating object of the first object," as claimed.

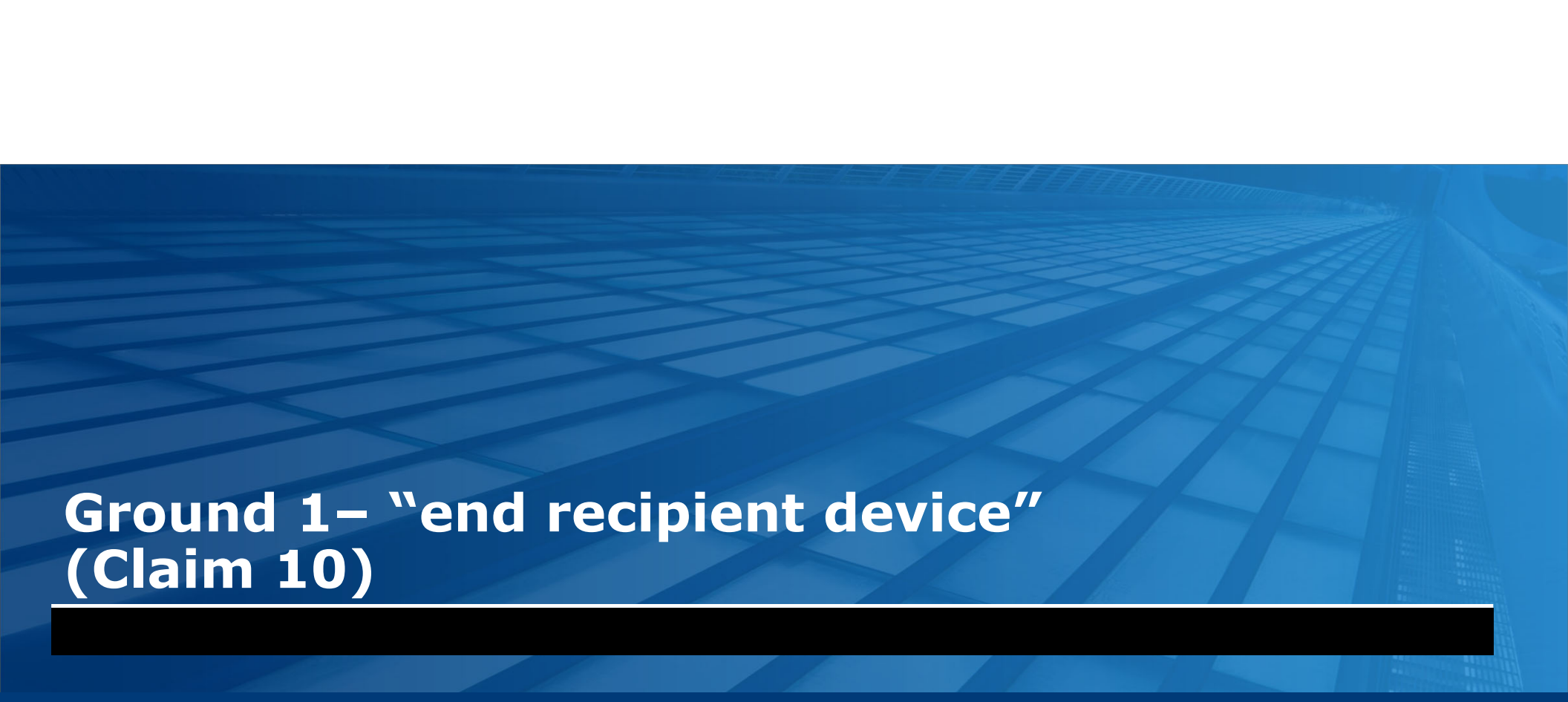
"Sensor Agent" (Remote Computer 2) Must "Obtain a Global Perspective" / Obtain "Global Perspective Information" (Claims 8 and 16)

obtain a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network;

assemble an event line including details associated with the at least one event, the details including information uniquely identifying each of the first object, the action of the first object, the target, the originating object, and global perspective information comprising information about one or more related events to the one or more events across a network; and

[0020], [0078]. Base computer 3 compares "the data about the computer object received from the plural computers" and "classif[ies] the computer object as malware on the basis of said comparison." *Id.*, [0016], [0017] ("this aspect allows

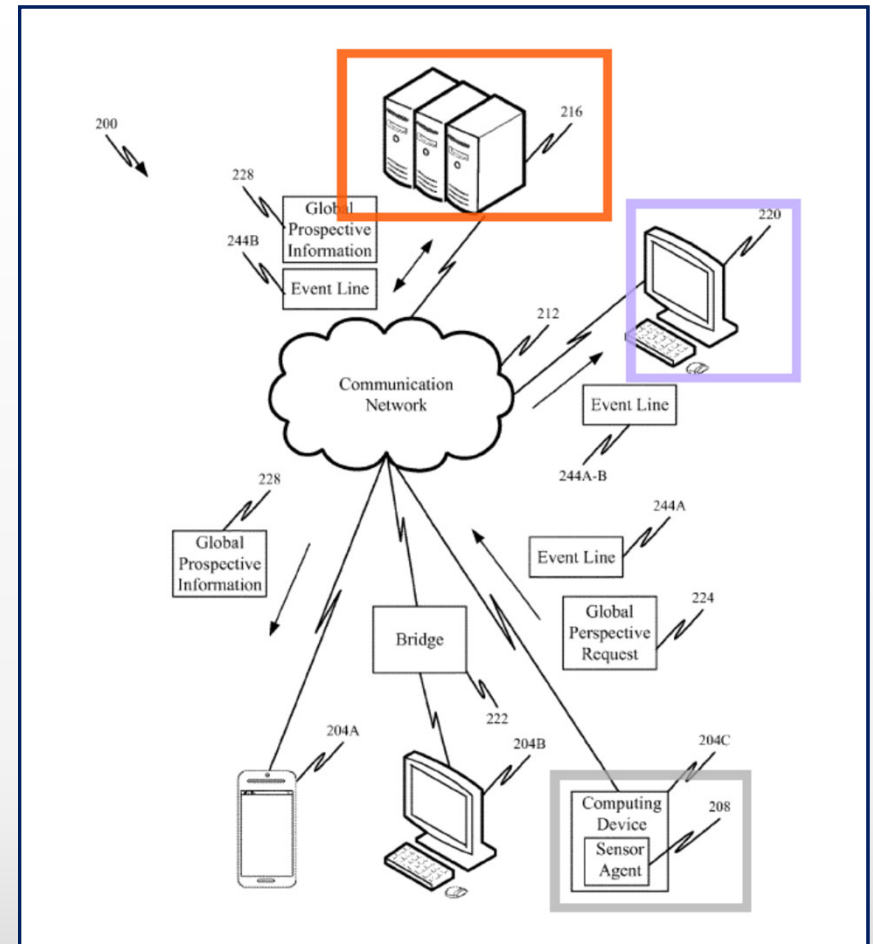
Morris therefore discloses obtaining a global perspective for the event by obtaining information concerning *a determination as to whether the first object/originating object is malware. Decl.*, ¶¶101-106.



Ground 1– “end recipient device” (Claim 10)

“End Recipient Device”: “a device that is separate from the device that includes the sensor agent and the global perspective information server”

10. The system of claim 8, further comprising:
a global perspective information server; and
an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device.



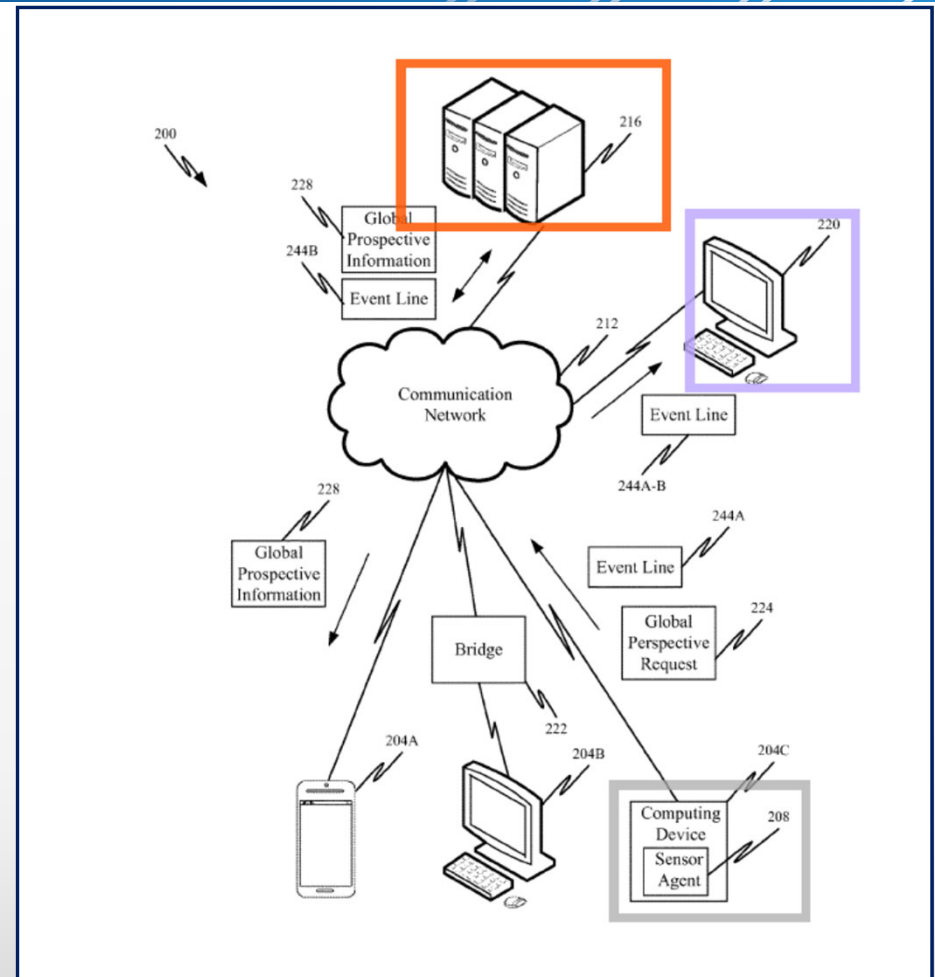
“End Recipient Device”: “a device that is separate from the device that includes the sensor agent and the global perspective information server”

- The '045 patent makes clear that the “end recipient device” must be separate from the device that includes the “sensor agent” and the “global perspective information server”

The computing device 204 includes and/or executes a sensor agent 208 in connection with the presentation of

The communication network 212 may include one or more networks capable of supporting communications between nodes of the system 200, including but not limited to a computing devices 204A-C, the global perspective information server 216 and the end recipient 220. Examples

the present disclosure. In general, the system 200 includes one or more computing device 204, each of which are interconnected to a global perspective information server 216 and end recipient 220 by one or more communication



“End Recipient Device”: “a device that is separate from the device that includes the sensor agent and the global perspective information server”

- The '045 patent makes clear that the “end recipient device” must be separate from the device that includes the “sensor agent” and the “global perspective information server”

The computing device 204 includes and/or executes a sensor agent 208 in connection with the presentation of

The communication network 212 may include one or more networks capable of supporting communications between nodes of the system 200, including but not limited to a computing devices 204A-C, the global perspective information server 216 and the end recipient 220. Examples

the present disclosure. In general, the system 200 includes one or more computing device 204, each of which are interconnected to a global perspective information server 216 and end recipient 220 by one or more communication

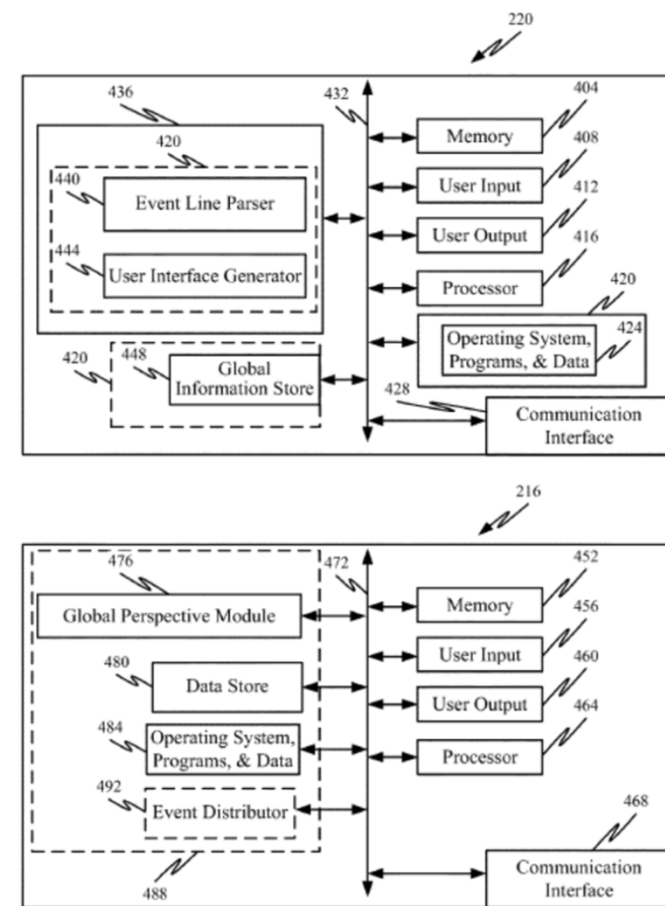


Figure 4

“End Recipient Device”: *“a device that is separate from the device that includes the sensor agent and the global perspective information server”*

- The '045 patent makes clear that the “end recipient device” must be separate from the device that includes the “sensor agent” and the “global perspective information server”

The computing device **204** includes and/or executes a sensor agent **208** in connection with the presentation of

The communication network **212** may include one or more networks capable of supporting communications between nodes of the system **200**, including but not limited to a computing devices **204A-C**, the global perspective information server **216** and the end recipient **220**. Examples

the present disclosure. In general, the system **200** includes one or more computing device **204**, each of which are interconnected to a global perspective information server **216** and end recipient **220** by one or more communication

work. Accordingly, when the event line containing event priority information is received at an end recipient **220**, the end recipient **220** may be able to more easily identify events, and/or instances of malware, that require more immediate attention.

The context analyzer **348** ensures that a user at the end recipient **220** is provided with the deepest view of the most important data but still has access to the full range of data if they wish to see it. Accordingly, the context analyzer **348**

creates an audit trail for each individual event. As will be described later, this audit trail allows an administrator, at an end recipient **220** for example, to forensically track back any event which occurs to what triggered it. Accordingly, this

Morris Does Not Disclose an “End Recipient Device” As Claimed [Claim 10]

- Petitioner points to base computer 3 as constituting the end recipient device and a global perspective information server

As described in Claim 1 above, *Morris* discloses base computer 3 connected to database 7, which together facilitate the comparison and classification of event data. *Morris*, [0014]-[0017], [0020], [0078]. A PHOSITA would have understood base computer 3 in conjunction with database 7 constitutes a *global perspective information server* and base computer 3 constitutes an *end recipient device*. Decl., ¶¶150-151. These components are depicted below in annotated Figure 1:



Grounds 1 and 2– “event priority” (Claim 3)

Van Oorschot does not render obvious an event priority using an originating object (claim 3)

- Claim 3 requires that the event priority is “based on one or more of the generated context and the global perspective for the at least one event”

3. The method of claim 1, further comprising:
obtaining an event priority based on one or more of the
generated context and the global perspective for the at
least one event, wherein the event line further includes
the event priority for the at least one event.

- Petitioner argues that van Oorschot’s “severity level” renders obvious “an event priority based on ... the **generated contextual state information**”

event.” *Van Oorschot*, 8:4-11; *Decl.*, ¶¶133-140. Indeed, *Van Oorschot* expressly contemplates displaying these event severity levels to a user to inform threat remediation tactics. *See, e.g., Van Oorschot*, Figs. 7-10. *Morris* in view of *Van Oorschot* therefore discloses obtaining an event priority based on...the generated context...wherein the event line further includes the event priority. *Decl.*, ¶¶125-140

Van Oorschot does not render obvious an event priority using an originating object (claim 3)

- The “generat[ed] contextual state” must include each of:
 - “correlating [the] event to an originating object;”
 - “an indication of the originating object of the first object;”
 - “an indication of at least one of a device on which the first object is executed and a user associated with the first object.”

generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

Van Oorschot's rules are unrelated to the "originating object"

- Petitioner argues van Oorschot's rules disclose the generated contextual state, but none relate to Claim 3's "originating object" requirements for the contextual state.

This severity level is assigned *based on the generated context* related to the event. *Van Oorschot* discloses the event data and contextual data associated with an event is divided into groups; these groups are assigned a "significance factor;" and this factor "is used as a weighting...in later assigning a severity level to an event[.]" *Id.*, 7:7-32. Policy or special attention rules are generated based on these groups,

36. These rules focus on permitted (or abnormal) activity related to certain attributes, such as "who" (e.g., "only 'system administrators' are permitted to modify files") or "where" (e.g., "types of clients at which the event can occur")—i.e., the *generated contextual state* discussed above in claim 1. *Id.*, 7:21-57. These significance factors and rules are then analyzed when assigning the severity level for an event. *See generally, id.*, 8:12-10:1; *Decl.*, ¶¶125-130.

Van Oorschot's rules are unrelated to the "originating object"

- Van Oorschot does not describe its rules/attributes as a software tool
- The user in van Oorschot is not an "originating object"

This assertion is incorrect because the attributes disclosed in Van Oorschot provide information about "the originating object." *Van Oorschot*, 7:12-27; *see also* Petition, 57-58; IPR2023-00124 Ex. 1003, ¶¶200-204, 63-67. These disclosed attributes include a contextual state of an event, including the actor, i.e., "who", which can be a user or a software tool, etc., the "action", i.e., "what", and the object/victim of the action, i.e., "on what." *Id.* As one example, when a user or software tool creates a

As a first step in configuring a security policy for the system, groups are defined in the security database. For each dimension, or attribute, in the security database, a number of groups are defined, which categorize the types of data that are to be associated with a given attribute. For example, the "when" attribute may include groups that define time elements, such as "office hours", "weekends", or "weekdays". The "who" attribute may include groups related to the various forms of users, such as "network administrators" or "general users". The "what" attribute may include groups related to the types of actions that can occur, such as "file write actions", "file read actions", "administrative actions", or "email transfer". The "on what" attribute may include, for example, groups related to the types of files being operated on. The "where", "where from", and "where to" attributes may include groups related to the types of clients at which the event can occur, the types of clients initiating the event, or the types of clients being acted upon by the event, for example "web servers", "test servers", "mail servers", "file servers", "workstations", or "database servers". In addition, each group within an attribute is assigned a significance factor, for example in the form of a number 10, 20, 30 . . . , that is used as a weighting by the event management tool in later assigning a severity level to an event, as will be described in detail below.

Van Oorschot's rules are unrelated to the "originating object"

- Petitioner's Reply conflates the "originating object" with the "first object" in an event
 - An "event" is the "action of a first object acting on a target"

1. A method comprising:
gathering one or more events defining an action of a first
object acting on a target;

This assertion is incorrect because the attributes disclosed in Van Oorschot provide information about "the originating object." *Van Oorschot*, 7:12-27; see also Petition, 57-58; IPR2023-00124 Ex. 1003, ¶¶200-204, 63-67. These disclosed attributes include a contextual state of an event, including the actor, i.e., "who", which can be a user or a software tool, etc., the "action", i.e., "what", and the object/victim of the action, i.e., "on what." *Id.* As one example, when a user or software tool creates a

As a first step in configuring a security policy for the system, groups are defined in the security database. For each dimension, or attribute, in the security database, a number of groups are defined, which categorize the types of data that are to be associated with a given attribute. For example, the "when" attribute may include groups that define time elements, such as "office hours", "weekends", or "weekdays". The "who" attribute may include groups related to the various forms of users, such as "network administrators" or "general users". The "what" attribute may include groups related to the types of actions that can occur, such as "file write actions", "file read actions", "administrative actions", or "email transfer". The "on what" attribute may include, for example, groups related to the types of files being operated on. The "where", "where from", and "where to" attributes may include groups related to the types of clients at which the event can occur, the types of clients initiating the event, or the types of clients being acted upon by the event, for example "web servers", "test servers", "mail servers", "file servers", "workstations", or "database servers". In addition, each group within an attribute is assigned a significance factor, for example in the form of a number 10, 20, 30 . . . , that is used as a weighting by the event management tool in later assigning a severity level to an event, as will be described in detail below.

**Ground 2– “global perspective”
(Claims 1-4, 7-10, 12, 15-18)**

Capalik Does Not Disclose A Global Perspective for “One or More Related Events to the at Least One Event Across a Network”

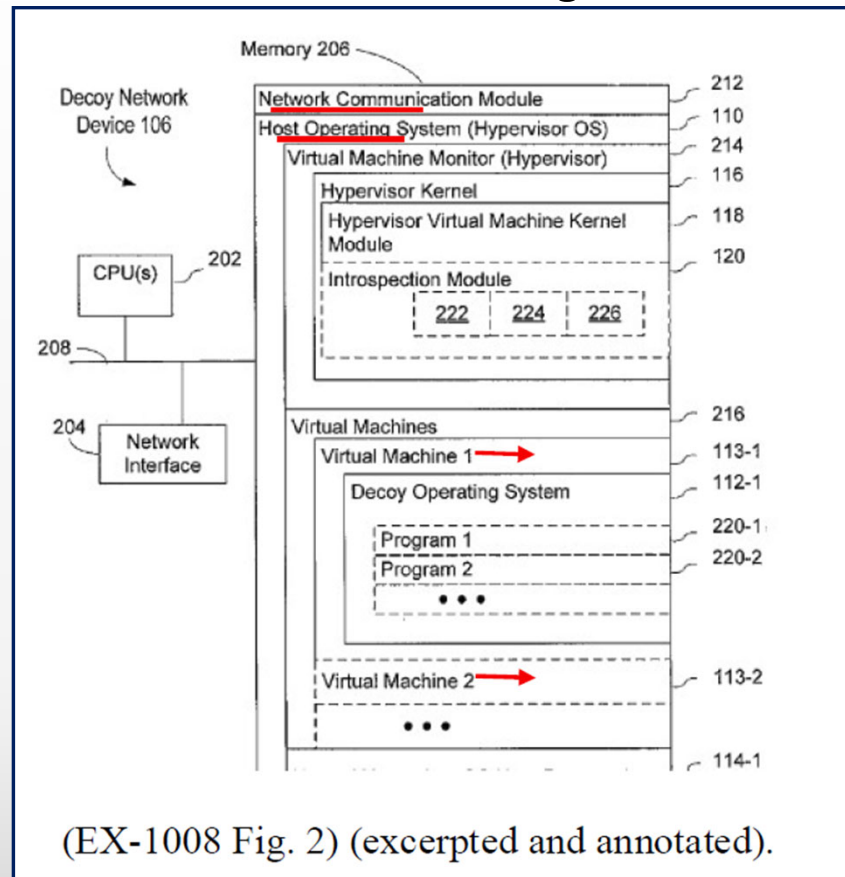
- Board correctly noted that Petitioner failed to show Capalik discloses “across a network”

With respect to Figure 4E, as Patent Owner observes, the objects and targets all exist within one virtual machine (113–1). Petitioner does not explain how that teaches or suggests obtaining a global perspective that relates to one or more other events related to the event “across a network.”

On the record before us, we are not persuaded that Petitioner has shown sufficiently for purposes of this Decision that Capalik teaches or suggests the recited “one or more related events to the at least one event across a network” of claims 1 and 8, or the similarly recited “one or more related events to the one or more events across a network” of claim 16. Nor

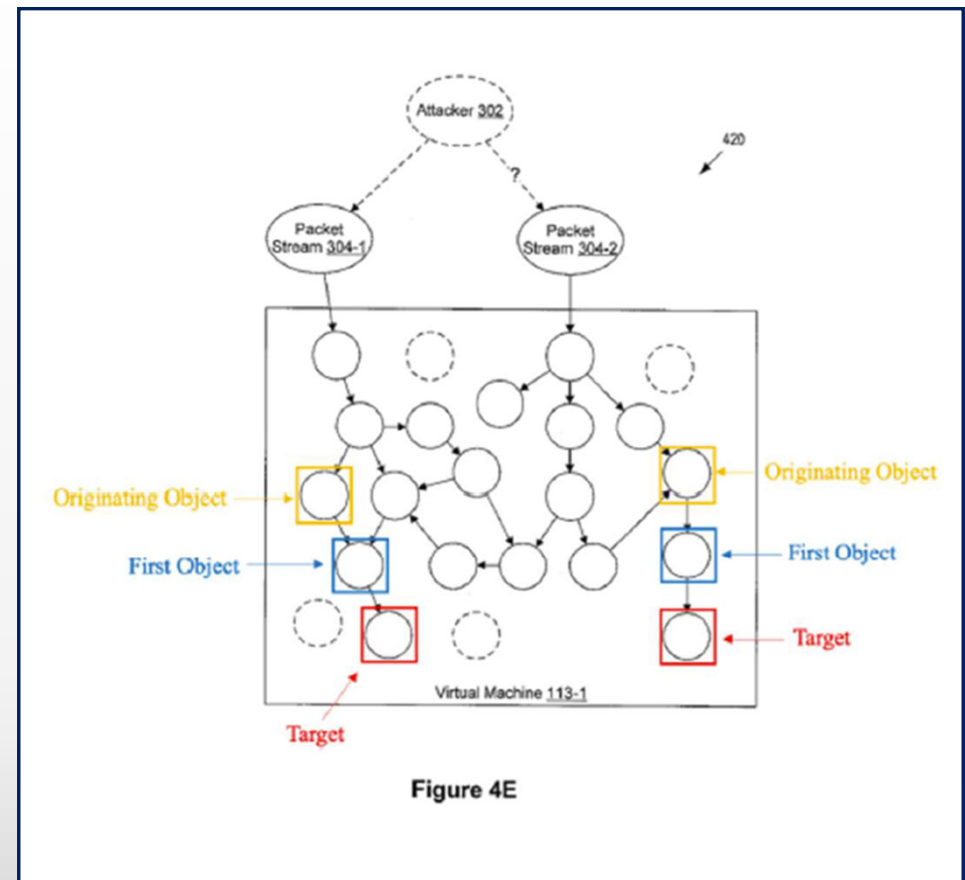
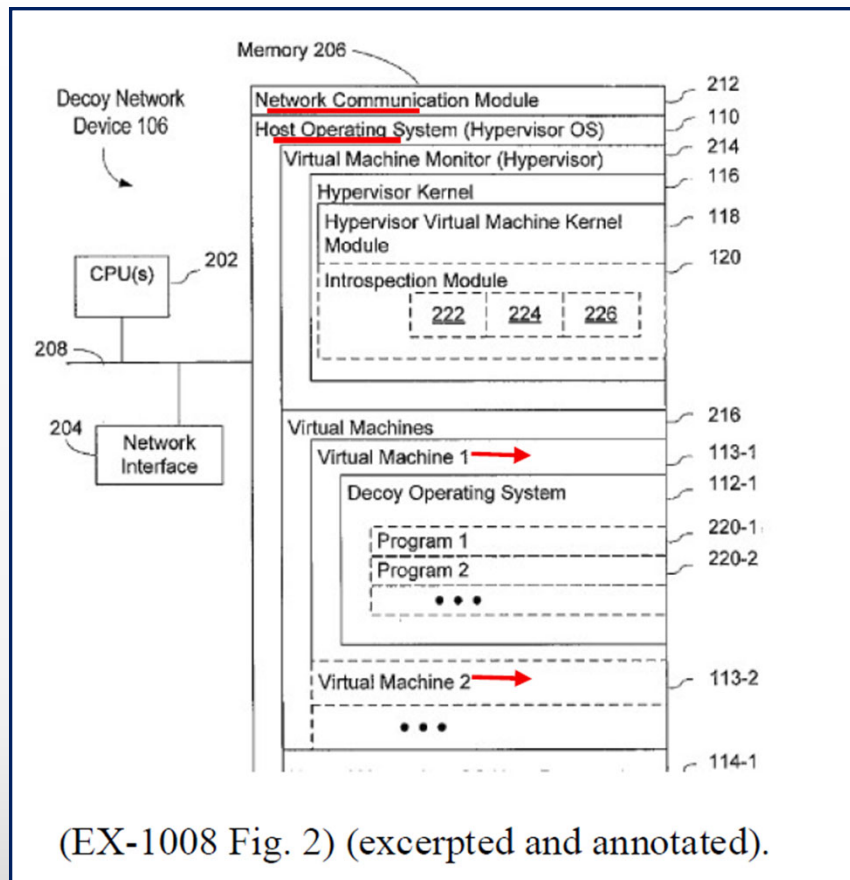
Capalik Does Not Disclose A Global Perspective for “One or More Related Events to the at Least One Event Across a Network”

- Capalik only discloses virtual machines collecting information on a single decoy device



Capalik Does Not Disclose A Global Perspective for “One or More Related Events to the at Least One Event Across a Network”

- Capalik only discloses virtual machines collecting information on a single decoy device



Capalik Does Not Disclose A Global Perspective That “Relates to One or More Other Events Across a Network”

- Capalik fails to render the claims unpatentable for the same reasons addressed during prosecution

However, as discussed above, Kumar merely teaches mapping threats to a cell within a risk correlation matrix and using the matrix to determine a state for a device within a target platform. Indeed, Kumar discloses a matrix that comprises information on a device-by-device basis and is associated with a machine or application identifier. (See Kumar, Figure 7C and paras. [0130]-[0131].) It is illogical to conclude that such a simplistic mapping of alerts to a specific device is analogous to the claimed “global perspective” that is “based on the contextual state information” and “relates to one or more other events related to the event across a network.” Rather, Kumar is focused on the integrity of a single application running on a single device. There is simply no teaching of events relating to application integrity for other devices on a network. Therefore, Kumar cannot possibly teach or suggest a “global perspective” that “relates to one or more other events related to the event across a network.” As such, Applicants respectfully request that the Examiner withdraw the rejection of claim 1 at the Examiner’s earliest convenience.

The Office Action cites to Capalik to remedy the deficiencies of Kumar. However, Capalik is similarly unavailing. Indeed, the Office Action does not allege that Capalik teaches the above claim elements but rather cites Capalik with respect to other claim elements. Capalik relates to capturing unauthorized intrusions into a computer using a hypervisor and generating a signature to identify and prevent similar attacks in the future. (See Capalik, Abstract.) However, similar to Kumar, Capalik fails to teach or suggest at least “obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and

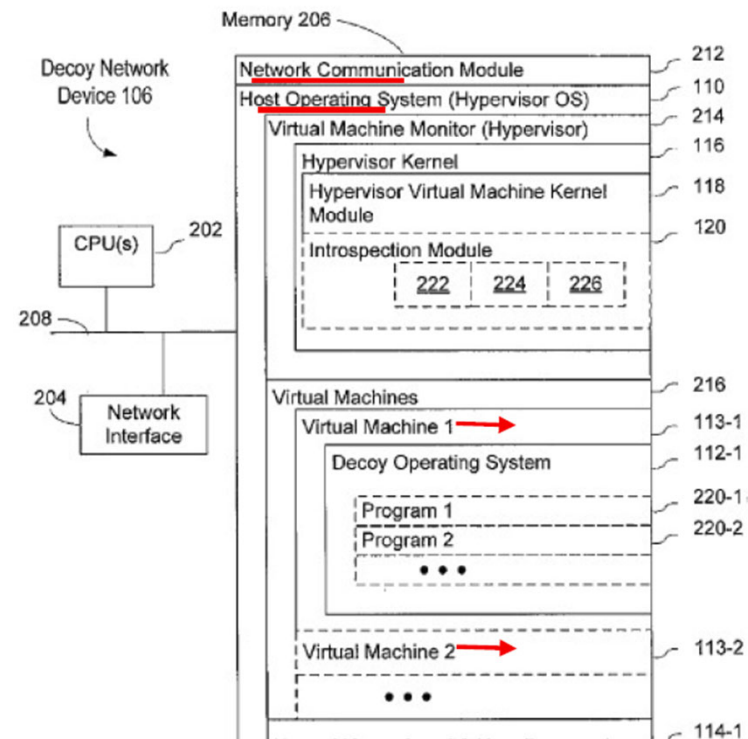
Capalik Does Not Disclose A Global Perspective for “One or More Related Events to the at Least One Event Across a Network”

'045 patent, cl. 1

obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event **across a network;**

Capalik, ¶[0130]

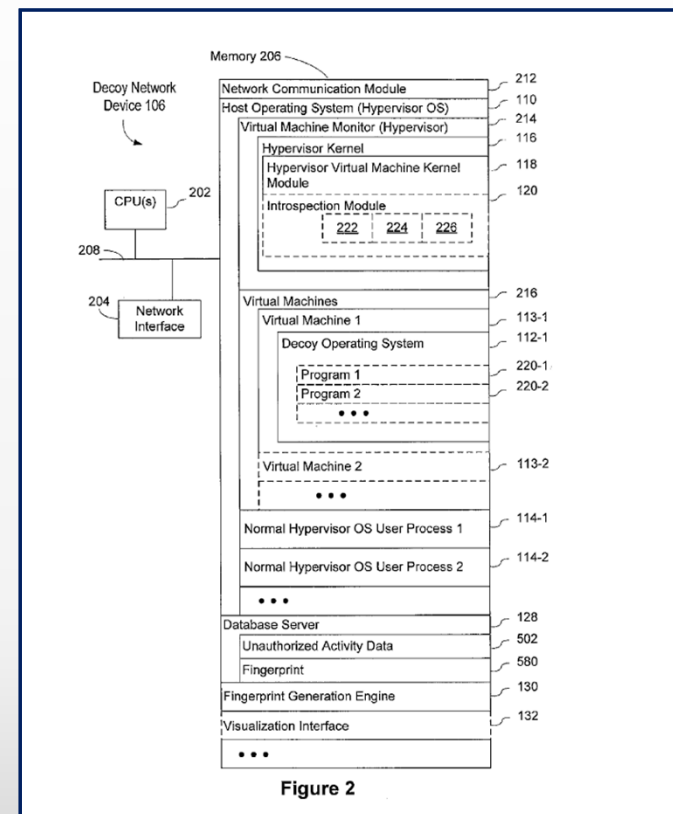
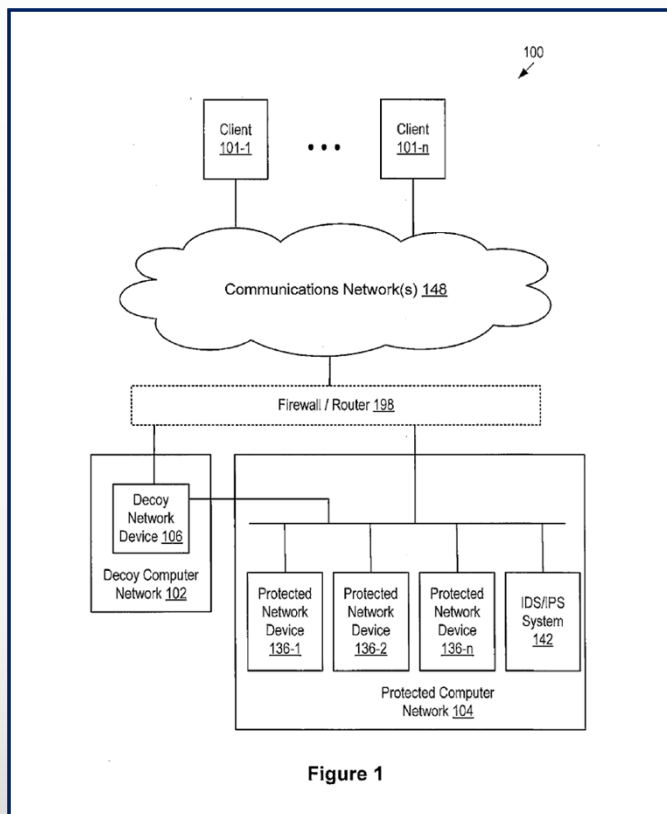
[0130] Moreover, the methods described herein need not be restricted to analysis of a single virtualized operating system but, rather, **are able to follow a chain of unauthorized activity across multiple virtualized operating systems.** This is important in identifying and thwarting advanced threats that involve multiple attackers spread across multiple systems and that evolve over long periods of time.



(EX-1008 Fig. 2) (excerpted and annotated).

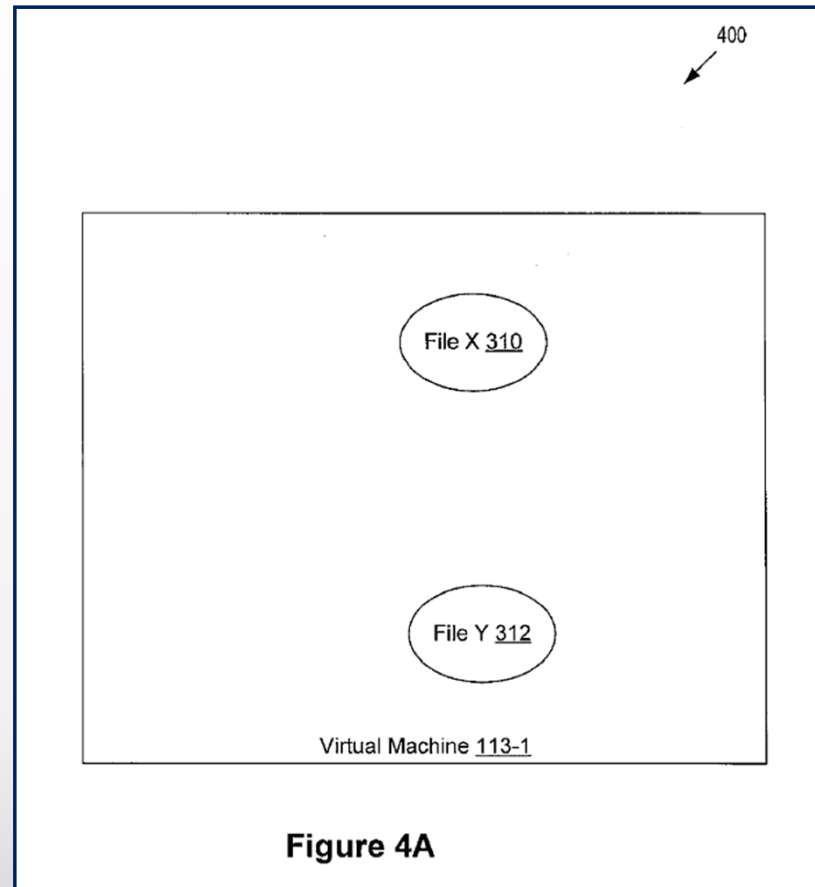
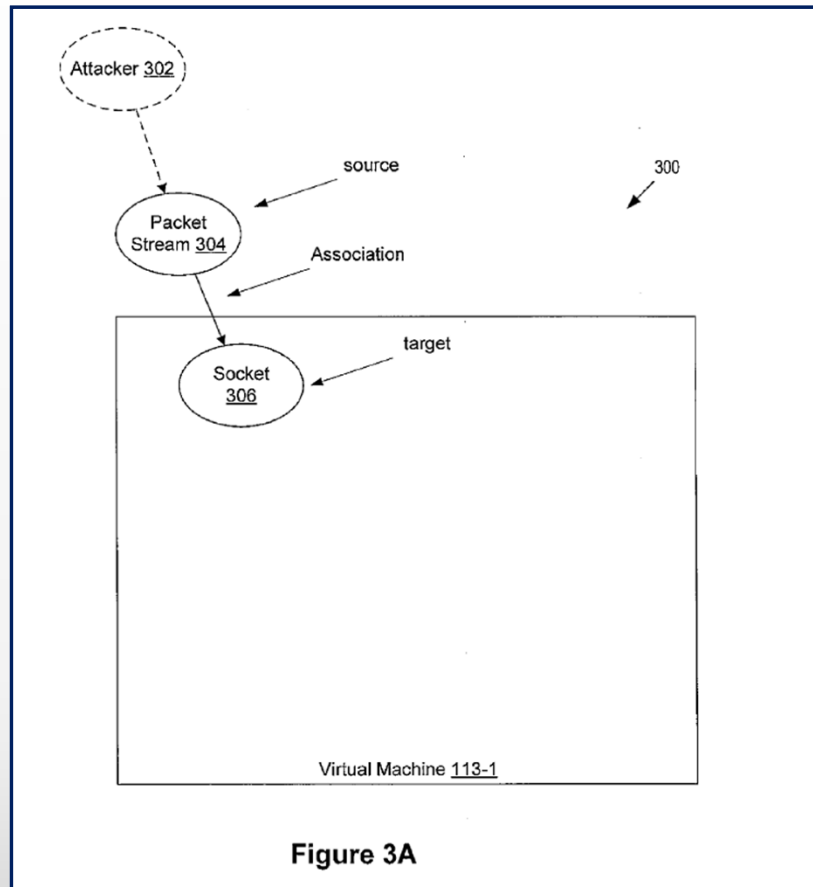
Capalik Does Not Disclose A Global Perspective for “One or More Related Events to the at Least One Event Across a Network”

- Petitioner’s new arguments do not explain how a POSITA would transform Capalik’s single decoy device to obtain/determine a global perspective of events “across a network”



Capalik Does Not Disclose A Global Perspective for “One or More Related Events to the at Least One Event Across a Network”

- Capalik repeatedly depicts activity within a single machine, not across a network



Open Text Inc.,

v.

AO Kaspersky Lab,

IPR2023-00124

Patent Owner's Oral Argument Presentation

King & Spalding, LLP

March 14, 2024