(51) International Patent Classification:
H04L 12/26 (2006.01)  H04L 12/16 (2006.01)
H04L 12/801 (2013.01)  G06F 17/30 (2006.01)

(21) International Application Number:
PCT/SG2015/050473

(22) International Filing Date:
26 November 2015 (26.11.2015)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
2014705377  28 November 2014 (28.11.2014)  MY
10201407948Y  28 November 2014 (28.11.2014)  SG

(71) Applicant: PTE LTD, EXPERT TEAM [SG/SG]; 12 Tannery Road #02-06, HB Centre 1, Singapore 347722 (SG).

(72) Inventors: FOO, Moo Tang; 21 Jalan kesoma, Singapore 538132 (SG). FRANKIE, Chang Kok Liang; 56 Bukit Batok East Ave 5, #11-05, Singapore 659804 (SG).


(54) Title: SYSTEMS AND METHODS FOR INTERCEPTING, FILTERING AND BLOCKING CONTENT FROM INTERNET IN REAL-TIME

(57) Abstract: A system for intercepting, filtering and blocking content from the Internet in near real time which includes a filtering device mounted at the Network Service Provider (NSP) or Internet Service Provider (ISP) which obtain Internet traffic from network tap and perform searching and filtering of targeted web content, subsequently generate the output with the intended filtered content; and also includes a collection, management and visualization device for receiving the targeted filtered content for further near real-time decoding, reconstruction, classification and automatic or manual content blocking with full visibility and is manageable by the Authority.
Title of Invention:
Systems and Methods for Intercepting, Filtering and Blocking Content from Internet in Real-Time

Technical Field
Embodiments of the present invention generally relate to computer and digital processing systems for Internet content monitoring and more particularly to systems and methods for intercepting, filtering and blocking content (illegal content) from the Internet in near real-time.

Background Art
It is common for legal regulatory authorities and government organizations of various countries to monitor a big data of Internet communication activities with a view to fight against illegal or terrorist activities which has escalated in the cyber world over the past few years.

Nowadays, the Internet provides a platform for a plethora of illegal activities ranging from credit card fraud, identity phishing, to money laundry to many others. Among these illegal activities, threat posed by the illegal websites is highly detrimental and hence, blocking such illegal websites becomes of extremely high importance. Examples of such illegal websites vary from different jurisdictions depending upon local laws and regulations. For example, online gambling websites are classified as illegal in Singapore while child pornography websites are classified as illegal in UK and so on.

One possible way to block such illegal websites is to block them at the intermediary level which is at the ISPs (Internet Service Providers) or Network
Service Provider (NSP). Such blocking usually requires regulatory backing and consequently, the action varies for each jurisdiction. Moreover, the infrastructure of a large Network Service Provider (ISP) typically comprises a constantly growing network of heterogeneous routers, interconnecting millions of subscribers or customer premises devices. This network enables the subscribers to communicate and exchange data of various formats through access to rich number of applications and services.

**Technical Problem**

In recent years it has been observed we are all in the vicinity of electronic threats (eThreats) mainly from the Internet. For example, eThreats comprises a variety of attacks which can be classified into three main categories: worm-related, non-worm related (e.g., virus, Trojan), and probes (e.g., spyware, adware, identity theft, and phishing).

Furthermore, Network Service Provider (NSP) are vulnerable to eThreats propagated across networks. Generally, information pertaining to illegal websites may be collected and analyzed by obtaining multiple network packets and determining if such packets contain the information and data pertaining to illegal websites.

Subsequently, information pertaining to the illegal websites may be categorized from which corresponding packets are transmitted if the analyzed packets include harmful information, and such information can be stored in a database for further action. However, such categorization technologies are mostly based on signatures and databases, and consequently, corresponding analysis requires lot of time, which may be hours, days or may be weeks, or even longer in some cases as it required human manual process and intervention.
Therefore, such delays prevent real time monitoring, analysis and categorization of illegal websites. Bloom Filters is based on the signature-based approach and is used to build a system that scans Internet traffic. Packets enter the system and are processed by Internet Protocol (IP) wrappers. The data in the packet goes to the input buffer and then flows through the content pipeline. As the packet passes through the pipeline, multiple Bloom engines scan different window lengths for signatures of different lengths. Subsequently, data leaves the content pipeline, flows to the output buffer, streams through the wrappers, and then packets are re-injected into the network. If a Bloom engine detects a match, a hash table is queried to determine if an exact match occurred. If the queried signature is an exact match, the malicious content can be blocked and an alert message is generated within a User Datagram Protocol (UDP) packet, informing a network administrator, an end-user or an automated process that a matching signature has been detected. Even though, the bloom filters provide a solution focused on throughput performance criteria, but can only deal with certain kinds of known eThreats that can be identified by their hashing or regular expression signature.

Solution to Problem

As may be seen, the solutions described above only provide a partial solution to very small part of a particular problem. Moreover, they don't analyze, categorize and block the content online in real time. Accordingly, there exists a need in the art for systems and methods for intercepting, filtering, accurately categorize and block illegal content from the Internet in near real-time.
Summary of the Invention

According to an aspect of the present invention, a system for intercepting, filtering, reconstructing and blocking content from the Internet in near real time, includes: a filtering device mounted at a Network Service Provider for searching and filtering web content and generate the intended output with targeted filtered content. In use, the filtering device is capable of processed the targeted filtered content for decoding and reconstruction which allows visualization of the filtered content. That would eventually confirmed the accuracy of the filtered content in web content categorization. In addition, the system further includes a collection, management and visualization device to allow the Authority (such as the Law Enforcement Agencies) to visualize and enforce the blocking on illegal content.

According to another aspect of the present invention, a method for intercepting, filtering and blocking content from Internet in near real-time includes the steps of retrieving the web content including multiple network packets from a source (usually from a network tap mounted on the Network Service Provider), stripping the network packet headers and abstracting information such as MAC addresses, IP addresses and the like from the network packets by a dissector; grouping the network packets belonging to the same flow together by a flow manager; determining a protocol to be used for each group of the packets by a protocol checker; abstracting application layer (layer 7) data by a protocol decoder and grouping the application layer data into multiple of layer 7 applications; and sending the application layer data for further processing.
**Advantageous Effects of Invention**

The combination of layer 7 DPI filtering and the additional decoding and reconstruction in near real-time has allowed the system to accurately analyze and categorize the websites and allow near real-time content blocking automatically.

**Brief Description of Drawings**

In the drawings, like reference characters generally refer to the same part throughout the different views. The drawings are not necessary to scale, emphasis instead generally being placed upon illustrating the principles of the invention. In the following description, various embodiments are described with reference to the following drawings, in which:

**Fig. 1** illustrates overview deployment of a system for intercepting, filtering and blocking content from Internet in real time, according to an embodiment of the present invention;

**Fig. 2** illustrates system architecture of a system for intercepting, filtering and blocking content from internet in real time, according to another embodiment of the present invention; and

**Fig. 3** illustrates system architecture of a filter of the system for intercepting, filtering and blocking content from internet in real time, according to an embodiment of the present invention.
Detailed Description

Various embodiments of the present invention relate to systems and methods for intercepting, filtering and blocking content from the Internet in near real time. More specifically, a network tap is placed in ISP infrastructure network (usually at the Exchange Router/Gateway/Router/Border Router) before the Internet traffic leaves the National Internet Gateway. Consequently, the network tap taps and sends the traffic to the filtering device for processing in near real-time.

Fig. 1 illustrates overview deployment of a system 120 for intercepting, filtering and blocking content from internet in real time. In one embodiment, the system 120 may be employed between the Authority (such as the Law Enforcement Agency 115 and one or more internet service providers (ISPs) 1251, 1252, 1253, and the like. As may be seen, the internet 105 is accessed via a national gateway 110, which makes possible the use of lawful interception solutions as provided by various embodiments of the present invention.

Fig. 2 illustrates system architecture of a system 200 for intercepting, filtering and blocking content from internet in real time. In accordance with an embodiment of the present invention, the system 200 for intercepting, filtering and blocking content from the Internet in near real time, includes: a filtering device 205 mounted at a Network Service Provider for retrieving and filtering web content in near real-time to generate targeted filtered content. In use, the filtering device is capable of transmitting the filtered content for further decoding and reconstruction.

In accordance with an embodiment of the present invention, the system 200 further includes a collection, management and visualization device 210 for
receiving the targeted filtered content for further decoding, reconstruction, classification and content blocking.

In accordance with an embodiment of the present invention, the filtering device 205 includes a fabric switch 212 for distributing tapped Internet traffic, multiple filters 215 for receiving the Internet traffic from the fabric switch 212, filtering the Internet web content based on multiple pre-configured rules and parameters to generate the target filtered content and forwarding the filtered content to the collection, management and visualization device 210. In use, traffic of multiple 10Gbps/40Gbps/100Gbps links can be tapped and spanned to the fabric switch 212, which can then distribute the traffic by 10Gbps ports to multiple filters 215. Generally, the multiple filters 215 are configured to handle up to 160Gbps line rate traffic throughput. In addition, the multiple filters 215 are designed for layer 7 deep packet inspection (DPI) on header and payload packet content searching and filtering. In accordance with an embodiment of the present invention, the multiple rules and parameters to generate the filtered content include pre-configured combination of REGEX text string pattern, keywords, IP addresses, URLs and the like. In use, for example, multiple pre-configured keywords for online betting such as online betting, football betting, horse racing betting, football odds, betting odds, bookmarks, Asian handicaps, and the like may be pre-configured or profiled into one or more filters. Subsequently, when there is any traffic that met the pre-defined condition, the specific traffic (the entire traffic session or flow) will be filtered out and sent for further real-time decoding and reconstruction to allow further verification of the targeted traffic for accuracy with categorized visualization. Those of ordinary skill in the art will appreciate that the combination of REGEX text string pattern, keywords, IP addresses, URLs and the like can be added from time to time to improve the multiple filters 215 capability. For example, third party signatures and custom made signatures
can also be added from time to time to enhance our current filter capability for better categorization, visibility and accuracy.

In accordance with an embodiment of the present invention, the collection, management and visualization device 210 includes a classification unit 225 for decoding and classifying multiple network packets from the target filtered traffic in accordance with L7 protocols and a reconstruction unit 230 for decoding, reconstructing and retaining the filtered network packets utilizing the real-time packet reconstruction (RTPR) engine.

In accordance with an embodiment of the present invention, the collection, management and visualization device 210 further includes one or more application programming interfaces (API) 235 for allowing further action to be taken automatically or manually. In use the API includes content filtering and content blocking 245, management and visualization 240 and the like.

In accordance with an embodiment of the present invention, the system 200 further includes a mediation device 220 for passing the target filtered traffic to the collection, management and visualization device 210 in standard format that also allows reading by any third party analyzer tools.

Fig. 3 illustrates system architecture of the filter 215 of the system 200 for intercepting, filtering and blocking content from Internet in near real time, according to an embodiment of the present invention. In accordance with an embodiment of the present invention, each filter 215 includes a High Throughput Network Processor Unit (NPU) for data processing. In use, multiple 10Gbps traffic may be spanned to the input ports of each filter. Subsequently, the traffic travels through the fabric switch, which is then
distributed and sent to NPU for processing. Thereafter, the NPU performs the packet content searching and filtering according to pre-configured REGEX text string pattern, keywords and the like as explained above.

In accordance with an embodiment of the present invention, the system further includes a dissector for stripping the network packet headers and abstracting information such as MAC addresses, IP addresses and the like. In use, the whole list of the websites details like timestamp, source and destination IP addresses, source and destination MAC addresses, source and destination ports, URL links and also the full content of the websites is made viewable to the Authority. Subsequently, the Authority can also have the call to decide to manually block which URLs or IP addresses through the API integration with ISP other network security equipment, such as the web content filtering and blocking appliance, firewall and router.

In accordance with an embodiment of the present invention, the system further includes a flow manager for grouping the web content into multiple packets belonging to same flow.

In accordance with an embodiment of the present invention, the system further includes a protocol checker for determining a protocol to be used for each group of the network packets. In use, the protocol checker includes HTTP, POP3, SMTP, IMAP, FTP, VOIP, P2P and the like.

In accordance with an embodiment of the present invention, the system further includes a protocol decoder for abstracting application layer data and grouping the application layer data into multiple layer 7 applications.
In accordance with an embodiment of the present invention, the system further includes at least one database module for storing the target filtered and reconstructed traffic content.

In accordance with an embodiment of the present invention, the system further includes a graphical user interface (GUI) using web management for accessing the management and database module.

In accordance with an embodiment of the present invention, a method for intercepting, filtering and blocking content from Internet in near real time includes the steps of retrieving web content from the multiple network packets from a source, stripping headers and abstracting information such as MAC addresses, IP addresses and the like from the network packets by a dissector; grouping packets belonging to same flow together by a flow manager; determining a protocol to be used for each group of the packets by a protocol checker; abstracting application layer data by a protocol decoder and grouping the application layer data into multiple layer 7 applications; and sending the application layer data for further processing.

In accordance with an embodiment of the present invention, the method further includes the step of further decoding and reconstruction for further verification and ensure accuracy on categorization.

In accordance with an embodiment of the present invention, the method further includes the step of saving the target filtered and reconstructed data in at least one database module.
In accordance with an embodiment of the present invention, a method for intercepting, filtering and blocking content from internet in real time includes the steps of spanning the tapped traffic by multiple 10Gbps ports to the filter. If it is determined that the traffic is encrypted, the filter will send the traffic to the RTPR engine which will decode the traffic and crawl the encrypted content from the Internet and find whether it matches the pre-configured REGEX text string pattern, keywords and the like to determine whether the types and categorization of the websites.

However, if the traffic is not encrypted, the filter processes the traffic using the L7 DPI Filtering capability to filter out the traffic of interest based on REGEX text string pattern, keywords and the like, as explained above.

Therefore, as may be seen, various embodiments of the present invention provide significant advantages, such as, for example, but not limited to near real-time decoding and reconstruction for further verification and accuracy that can allow the illegitimate websites objects to be identified (displayed) and the system can block the content automatically in near real-time or allowing the Authority to manually decide to manually block the content making use of the GUI web management and API integration.
5 Claims

[Claim 1] A system for intercepting, filtering and blocking content from Internet in near real time, said system comprising:

• A filtering device mounted at a Network Service Provider for retrieving and filtering web content in near real-time to generate target filtered traffic content, said filtering device being capable of transmitting said filtered traffic content for decoding and reconstruction; and,

• A collection, management and visualization device for receiving said filtered content for further decoding, reconstruction, classification and content blocking visible and manageable by the Authority.

[Claim 2] The system as claimed in Claim 1, wherein said filtering device comprises:

• A fabric switch for distributing tapped Internet traffic; and,

• A plurality of filters for receiving said Internet traffic from said fabric switch, filtering said web content based on a plurality of rules and parameters to generate said target filtered content and forwarding said filtered content to said collection, management and visualization device.

[Claim 3] The system as claimed in Claim 2, wherein said plurality of filters are capable of layer 7 deep packet inspection (DPI) on both header and payload packet content searching and filtering.
[Claim 4] The system as claimed in Claim 2, wherein said plurality of rules and parameters comprise REGEX text string patterns, keywords, IP addresses, URLs and the like.

[Claim 5] The system as claimed in Claim 1, wherein said a collection, management and visualization device comprises:

- A classification unit for decoding and classifying multiple network packets from the target filtered traffic in accordance with L7 protocols; and
- A reconstruction unit for decoding, reconstructing and retaining the filtered network packets utilizing the real time packet reconstruction (RTPR) engine.

[Claim 6] The system as claimed in Claim 5, wherein said collection, management and visualization device further comprises at least one application programming interface (API) for allowing further action such as content blocking to be taken automatically or manually.

[Claim 7] The system as claimed in Claim 6, wherein at least one API comprises the content filtering and content blocking, management and visualization and the like.

[Claim 8] The system as claimed in Claim 2, wherein each filter of said plurality of filters comprises a High Throughput Network Processor Unit (NPU) for data processing that includes searching and filtering.
[Claim 9] The system as claimed in Claim 1, wherein said system further comprises a dissector for stripping packet headers and abstracting information such as MAC addresses, IP addresses and the like from said web content.

[Claim 10] The system as claimed in Claim 1, wherein said system further comprises a flow manager for grouping said web content into a plurality of packets belonging to same flow.

[Claim 11] The system as claimed in Claim 1, wherein said system further comprises a protocol checker for determining a protocol to be used for each group of said plurality of packets.

[Claim 12] The system as claimed in Claim 11, wherein said protocol checker comprises HTTP, POP3, SMTP, IMAP, FTP, VOIP, P2P and the like.

[Claim 13] The system as claimed in Claim 1, wherein said system further comprises a protocol decoder for abstracting application layer data and grouping said application layer data into a plurality of layer 7 applications.

[Claim 14] The system as claimed in Claim 1, wherein said system further comprises at least one database module for storing the target filtered and reconstructed traffic content.
[Claim 15] The system as claimed in Claim 1, wherein said system further comprises a web management GUI for visualization and accessing the management and database module.

[Claim 16] A method for intercepting, filtering and blocking content from Internet in near real time, said method comprising the steps of: retrieving the web content including multiple network packets from a source (usually from a network tap mounted on the Network Service Provider), stripping headers and abstracting information such as MAC addresses, IP addresses and the like from said plurality of network packets by a dissector; grouping said plurality of packets belonging to same flow together by a flow manager; determining a protocol to be used for each group of said plurality of network packets by a protocol checker; abstracting application layer data by a protocol decoder and grouping said application layer data into a plurality of layer 7 applications; and sending said application layer data for further processing.

[Claim 17] The system as claimed in Claim 16, wherein said method further comprises the step of decoding and reconstructing the filtered traffic content from the filter in near real-time.

[Claim 18] The system as claimed in Claim 16, wherein said method further comprises the step of saving and storing the data in the database module.
Claims:
We reviewed the previous 18 Claims and decided to cancel all the previous 18 Claims and replaced them with amended 4 Claims as of below.

Claim [1] A system for capturing network packets, both encrypted and non-encrypted in near line rate, inspect, decode, crawl, filter (L7 DPI Filter) and reconstruct the network packets header and payload content, categorize, classify and distribute the data for multiple applications including content blocking. The whole process is done in near real-time without delay. This would allow a newly published site such as illegal online betting site to be instantly detected and identified once anyone access the site, and also can be immediately blocked by the system as part of the content blocking application.

Claim [2] The system is capable to process both encrypted (HTTPS) and none-encrypted (HTTP) web based data content, regardless of the port numbers used (standard port for HTTP web pages is 80 and HTTPS web pages is 443) as the system identifies the web traffic base on Layer 7 (L7) instead of Layer 5 (L5) within the OSI model. For HTTPS web pages, the system is able to crawl the whole web page content which allow the L7 DPI filter to process and identify the web pages through its pattern matching mechanism.

Claim [3] The L7 DPI filter has its own pattern matching mechanism that combines the used of keywords and matchings comparison with existing or known websites. For example, a few common keywords will be identified from a betting site such as betting, casino, poker, handicap, odd and even. Couple of matching patterns can be constructed from these keywords. Whenever there is
any web page content that pass through the filter with the pattern matched, it will be classified under the same categories. Reconstruction of the web pages will further confirm that the pattern matching is accurate. All the capturing, decoding, filtering with pattern matching and reconstruction processes are done in near real-time without delay.

**Claim [4]** The system has a built in API that allows 3rd party solutions such as Application and Network Performance Management Solution, Application Monitoring Solution, Unified Threat Management (UTM) Solutions and others to interact with the System and integrate their additional features to the System.
High Throughput Network Processor Unit (NPU)
(line rate of up to 40Gbps)
Filter based on L7 DPI
Keywords Pattern: Betting - Horse Racing, Football Betting, Odds, Poker etc..., Account Names/ID, User ID, Password etc...

N x 10Gbps Traffic SPF+ Ports

Switch

DDR RAM

FLASH

Switch

DDR RAM

CPU

GPHY

N x Gigabit Ethernet Ports to 3I ATCA
## INTERNATIONAL SEARCH REPORT

### A. CLASSIFICATION OF SUBJECT MATTER

| HQ4L 12/26 (2006.01) | H04L 12/801 (2013.01) | H04L 12/16 (2006.01) | G06F 17/30 (2006.01) |

According to international Patent Classification (IPC)

### B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

| H04L 12/00, G06F 17/00 |

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

| Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) |

Databases: EPODOC, WPI, internet

Keywords: intercept, real time, service provider, filter, decode, reconstruction, classification, header, protocol, layer 7 application and related terms

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 201 0/01 991 89 A1 (BEN-AROA E. ET AL) 5 August 2010 The whole document in particular paras. [0004]-[0010], [0012]-[0013] and [0030]-[0039]; FIG. 1.</td>
<td>1-15</td>
</tr>
<tr>
<td>X</td>
<td>US 2003/022791 7 A1 (MAHER III R. D. ET AL) 11 December 2003 The whole document in particular paras. [0005]-[006], [0018]-[0032], [0038]-[0042], [0055] and [0062]; FIG. 8.</td>
<td>1-15</td>
</tr>
</tbody>
</table>

* Special categories of cited documents:

- **A** document defining the general state of the art which is not considered to be of particular relevance
- **E** earlier application or patent but published on or after the international filing date
- **L** document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- **O** document referring to an oral disclosure, use, exhibition or other means
- **P** document published prior to the international filing date but later than the priority date claimed

- **T** later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- **X** document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- **Y** document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- **&** document member of the same patent family

### Date of the actual completion of the international search

29/02/20 16 (day/month/year)

### Date of mailing of the international search report

07/03/201 6 (day/month/year)

**Name and mailing address of the ISA/SG**

**Intellectual Property Office of Singapore**

51 Bras Basah Road

#01-01 Manulife Centre

Singapore 189554

Email: pct@ipos.gov.sg

**Authorized officer**

Liu Yu (Dr)

**IPOS Customer Service Tel. No.: (+65) 6339 861 6**

---

Form PCT/ISA/210 (second sheet) (January 2015)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>Real Time Packet Reconstruction in Data Communication. 25 September 2014</td>
<td>16-1 8</td>
</tr>
<tr>
<td></td>
<td>[Retrieved on 2016-02-29 from <a href="https://www.ipi-singapore.org/technology-">https://www.ipi-singapore.org/technology-</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>offers/real-time-packet-reconstruction-data-communication]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The whole document</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 2008/0089238 A1 (FAHMY S. F.) 17 April 2008</td>
<td>16-1 8</td>
</tr>
<tr>
<td></td>
<td>The whole document in particular paras. [0005]-[0006] and [0015]-[0026]</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Real-Time Packet Reconstruction (RTPR) for Lawful Interception. 3 November</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2013</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Retrieved on 2016-02-29 from <a href="https://www.prlog.org/1235893-real-time-">https://www.prlog.org/1235893-real-time-</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet-reconstruction-rtp-for-lawful-interception.html]</td>
<td></td>
</tr>
</tbody>
</table>
**INTERNATIONAL SEARCH REPORT**

<table>
<thead>
<tr>
<th>Box No.</th>
<th>Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ii</td>
<td>This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:</td>
</tr>
<tr>
<td>1. ☐ Claims Nos.:</td>
<td>because they relate to subject matter not required to be searched by this Authority, namely:</td>
</tr>
<tr>
<td>2. ☐ Claims Nos.:</td>
<td>because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:</td>
</tr>
<tr>
<td>3. ☐ Claims Nos.:</td>
<td>because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Box No.</th>
<th>Observations where unity of invention is lacking (Continuation of item 3 of first sheet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ii</td>
<td>This international Searching Authority found multiple inventions in this international application, as follows:</td>
</tr>
<tr>
<td></td>
<td>Please refer to Supplemental Box (Continuation of Box No. III).</td>
</tr>
</tbody>
</table>

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest** ☒ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

- The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- No protest accompanied the payment of additional search fees.
This International Searching Authority found multiple inventions in this international application, as follows:

Group A: Claims 1-15 define a system comprising a filtering device mounted at network service provider for retrieving and filtering web content in real time and a collection, management and visualization device for further decoding, reconstruction, classification and content blocking visible and manageable by the Authority.

Group B: Claims 16-18 define a method comprising steps of retrieving web content, stripping headers and abstracting information, grouping packets, determining a protocol, abstracting application layer data, sending the application layer data.

Please refer to Box No. IV of Written Opinion of The international Searching Authority (Form PCT/ISA/237) for detailed explanation.
<table>
<thead>
<tr>
<th>Patent document cited isi search report</th>
<th>Publication date</th>
<th>Patent family members</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2010/0199189 A1</td>
<td>05/08/2010</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 7646728 B2</td>
<td>12/01/2010</td>
</tr>
</tbody>
</table>