Claims

1. A system for intercepting, filtering and blocking content from internet in real time, said system comprising:

a filtering device mounted at a network service provider for retrieving and filtering web content in real-time to generate filtered content, said filtering device being capable of transmitting said filtered content for decoding and reconstruction, said filtering device comprising, a fabric switch for retrieving and distributing said web content, and, a plurality of filters for receiving said web content from said fabric switch, filtering said web content based on a plurality of parameters to generate said filtered content and forwarding said filtered content to said collection device; and,

a collection device mounted at a law enforcement agency for receiving said filtered content for further classification, decoding and reconstruction.

~~2. The system as claimed in Claim 1, wherein said filtering device comprises:~~

~~a fabric switch for retrieving and distributing said web content; and,~~

~~a plurality of filters for receiving said web content from said fabric switch, filtering said web content based on a plurality of parameters to generate said filtered content and forwarding said filtered content to said collection device.~~

~~3~~ 2. The system as claimed in Claim 1 ~~2~~, wherein said plurality of filters are capable of layer 7 header deep packet inspection (DPI) and payload content filtering.

~~4~~ 3. The system as claimed in Claim 1 ~~2~~, wherein said plurality of parameters comprise keywords, REGEX patterns, IP addresses, URLs` ~~and the like~~.

~~5~~ 4. The system as claimed in Claim 1, wherein said collection device comprises:

a classification unit for decoding and classifying a first plurality of packets contained in said filtered content in accordance with L7 protocols; and

a reconstruction unit for reconstructing and retaining said first plurality of packets by employing real time packet reconstruction (RTPR).

~~6~~ 5. The system as claimed in Claim ~~5~~ 4, wherein said collection device further comprises at least one application programming interface (API) for using said first plurality of packets obtained after RTPR for further action.

~~7~~ 6. The system as claimed in Claim 5 ~~6~~, wherein at least one API comprises content filtering, content blocking, and warrant management ~~and the like~~.

~~8~~ 7. The system as claimed in Claim 1 ~~2~~, wherein each filter of said plurality of filters comprises a High Throughput Network Processor Unit (NPU) for data processing.

~~9~~ 8. The system as claimed in Claim 1, wherein said system further comprises a dissector for stripping headers and abstracting information such as MAC addresses, IP addresses and the like from said web content.

~~10~~ 9. The system as claimed in Claim 1, wherein said system further comprises a flow manager for grouping said web content into a second plurality of packets belonging to same flow.

~~11~~10. 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 first and second plurality of packets.

~~12~~11. The system as claimed in Claim 10 ~~11~~, wherein said protocol checker comprises HTTP, POP3, SMTP, and the like.

~~13~~12. 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.

~~14~~13. The system as claimed in Claim 1, wherein said system further comprises at least one database module for storing said filtered content.

~~15~~14. The system as claimed in Claim ~~1~~ 13, wherein said system further comprises a web management GUI for accessing said at least one database module.

~~16~~15. A method for intercepting, filtering and blocking content from internet in real time, said method comprising the steps of:

retrieving web content from a source, said web content comprising a plurality of packets;

stripping headers and abstracting information such as MAC addresses, IP addresses and the like from said plurality of 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 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.

~~17~~16. The system as claimed in Claim 15 ~~16~~, wherein said method further comprises the step of determining if further decoding is needed.

~~18~~17. The system as claimed in Claim 15 ~~16~~, wherein said method further comprises the step of sending data to application data recorder if further decoding is needed.

~~19~~18. The system as claimed in Claim 15 ~~16~~, wherein said method further comprises the step of saving data in at least one database module.