CLAIMS

1. A method ~~comprising employing at least one hardware processor of~~performed by a computer system, ~~to:~~

the method comprising intercepting a domain name service (DNS) reply message ~~received at the computer system, the DNS reply message~~[28] comprising a target internet protocol (IP) address indicating a network location of a remote resource, the method characterized by the DNS reply message further comprising a service activation flag~~;~~ [27],

and by having the computer system carry out the steps of:

determin~~e~~ing according to a value of the service activation flag [27] whether a forensic data collection service is active;

in response, if the service activation flag [27] indicates that the forensic data collection service is active, modifying the DNS reply message [28] by replacing the target IP address with a dummy IP address;

intercepting an electronic communication directed towards a destination IP address;

determin~~e~~ing whether the destination IP address matches the dummy IP address; and

in response to determining whether the destination IP address matches the dummy IP address, if the destination IP address matches the dummy IP address, performing a forensic data collection procedure for characterizing emerging malware, the forensic data collection procedure comprising ~~transmitting~~determining a set of ~~metadata~~forensic data [30] characterizing the electronic communication and transmitting the set of forensic data [30] to a remote security server [16].

2. The method of claim 1, wherein performing the forensic data collection procedure further comprises ~~employing the at least one hardware processor~~having the computer system ~~to~~ re-route the electronic communication via a tunnel connecting the computer system to the remote security server [16].

3. The method of claim 1, further characterized by having the computer system, in response to determining whether the destination IP address matches the dummy IP

address, if the destination IP address matches the dummy IP address, forward the electronic communication to the target IP address.

~~3~~4. The method of claim 1, wherein the set of ~~metadata~~forensic data [30] includes the target IP address and a timestamp of the electronic communication.

4~~5~~. The method of claim ~~3~~4, wherein the set of ~~metadata~~forensic data [30] further comprises an indicator of a size of a payload of the electronic communication.

~~5~~6. A computer system ~~comprising at least one hardware processor~~ configured to ~~execute~~intercept a domain name service (DNS) ~~proxy and a communication manager, wherein:~~

~~the DNS proxy is configured to:~~

~~intercept a DNS~~ reply message ~~received at the computer system, the DNS reply message~~[28] comprising a target internet protocol (IP) address indicating a network location of a remote resource, the computer system characterized by the DNS reply message [28] further comprising a service activation flag [27], the computer system further characterized by executing a DNS proxy [56] and a communication manager [58], wherein:

the DNS proxy [56] is configured to:

in response to intercepting the DNS reply message [28],

determine according to a value of the service activation flag [27] whether a forensic data collection service is active, and

in response, if the service activation flag [27] indicates that the forensic data collection service is active, modify the DNS reply message [28] by replacing the target IP address with a dummy IP address; and

the communication manager [58] is configured to:

intercept an electronic communication directed towards a destination IP address,

determine whether the destination IP address matches the dummy IP address, and

in response to determining whether the destination IP address matches the dummy IP address, if the destination IP address matches the dummy IP address, perform a forensic data collection procedure for characterizing emerging malware, the forensic data collection procedure comprising ~~transmitting~~determining a set of ~~metadata~~forensic data [30] characterizing the electronic communication and transmitting the set of forensic data [30] to a remote security server [16].

~~6~~7. The ~~method~~computer system of claim ~~1~~6, wherein performing the forensic data collection procedure further comprises ~~employing the at least one hardware processor to~~ re-route~~e~~ing the electronic communication via a tunnel connecting the computer system to the remote security server [16].

8. The computer system of claim 6, wherein the communication manager is further configured, in response to determining whether the destination IP address matches the dummy IP address, if the destination IP address matches the dummy IP address, to forward the electronic communication to the target IP address.

~~7~~9. The computer system of claim ~~5~~6, wherein the set of ~~metadata~~forensic data [30] includes the target IP address and a timestamp of the electronic communication.

~~8~~10. The computer system of claim ~~7~~9, wherein the set of ~~metadata~~forensic data [30] further comprises an indicator of a size of a payload of the electronic communication.

~~9~~11. A non-transitory computer-readable medium storing instructions which, when executed by ~~at least one hardware processor of~~ a computer system, cause the computer system to ~~form a domain name service (DNS) proxy and a communication manager, wherein:~~

~~the DNS proxy is configured to:~~

intercept a domain name service (DNS) reply message [28]~~received at the computer system, the DNS reply message~~ comprising a target internet protocol (IP) address

indicating a network location of a remote resource, the computer-readable medium characterized by the DNS reply message [28] further comprising a service activation flag [27], the computer-readable medium further characterized by causing the computer system to form a DNS proxy [56] and a communication manager [58], wherein:
the DNS proxy [56] is configured to:

in response to intercepting the DNS reply message [28], determine according to a value of the service activation flag [27] whether a forensic data collection service is active, and

in response, if the service activation flag [27] indicates that the forensic data collection service is active, modify the DNS reply message [28] by replacing the target IP address with a dummy IP address; and

the communication manager [58] is configured to:

intercept an electronic communication directed towards a destination IP address,

determine whether the destination IP address matches the dummy IP address, and

in response to determining whether the destination IP address matches the dummy IP address, if the destination IP address matches the dummy IP address, perform a forensic data collection procedure for characterizing emerging malware, the forensic data collection procedure comprising ~~transmitting~~determining a set of ~~metadata~~forensic data [30] characterizing the electronic communication and transmitting the set of forensic data [30] to a remote security server [16].

10~~2~~. A server computer system [14] ~~comprising at least one hardware processor~~ configured to engage in domain name service (DNS) transactions with a plurality of client systems [10a-f], ~~and~~the server computer system [14] characterized by being further configured to:

in response to a determination that an Internet domain is suspected of malice, determine a target device profile according to the Internet domain, the target device profile collectively representing electronic devices characterized by being located within a selected geographic area and executing a selected operating system;

in response to receiving a DNS query message [26] comprising a domain name of the Internet domain, identify according to the DNS query message [26] a client system [10] where the DNS query message [26] originated;

in response to identifying the client system [10], determine whether the client system [10] matches the target device profile;

in response to determining whether the client system [10] matches the target device profile, when the client system [10] matches the target device profile, transmit a DNS reply message [28] to the client system, the DNS reply message [28] comprising a target Internet Protocol (IP) address associated with the domain name, the DNS reply message [28] further configured to include a service activation flag [27] for activating a forensic data collection procedure on the client system [10]; and

in response to determining whether the client system [10] matches the target device profile, when the client system [10] does not match the target device profile, transmit another DNS reply message to the client system, the other DNS reply message comprising the target IP address and further configured to not include the service activation flag [27];

~~wherein the client system is configured to interpret receiving the service activation flag as a trigger for performing a forensic data collection procedure according to an electronic communication directed to or incoming from the target IP address~~.

1~~1~~3. The server computer system of claim 1~~0~~2, ~~wherein the at least one hardware processor is~~ further characterized by being configured to:

in response to determining whether the client system [10] matches the target device profile, when the client system [10] matches the target device profile, determine whether the client system [10] is eligible for forensic data collection according

to a count of DNS query messages previously received from the client system [10]; and

in response, transmit the DNS reply message [28] including the service activation flag [27] only when the client system [10] is eligible for forensic data collection.

124. The server computer system of claim 102, ~~wherein the at least one hardware processor is~~ further characterized by being configured to:

in response to determining whether the client system [10] matches the target device profile, when the client system [10] matches the target device profile, determine whether the client system [10] is eligible for forensic data collection according to a count of DNS query messages including the domain name previously received at the server computer system [14]; and

in response, transmit the DNS reply message [28] including the service activation flag [27] only when the client system [10] is eligible for forensic data collection.

135. The server computer system of claim 102, ~~wherein the at least one hardware processor is~~ further characterized by being configured to:

in response to determining whether the client system [10] matches the target device profile, when the client system [10] matches the target device profile, determine whether the client system [10] is eligible for forensic data collection according to a count of distinct client systems [10a-f] having transmitted DNS query messages to the server computer system [14] within a selected time interval; and

in response, transmit the DNS reply message [28] including the service activation flag [27] only when the client system [10] is eligible for forensic data collection.

146. The server computer system of claim 102, ~~wherein the at least one hardware processor is~~ further characterized by being configured to:

in response to determining whether the client system [10] matches the target device profile, when the client system [10] matches the target device profile, lookup a

client profile database [19] to determine whether a selected software application is installed for execution on the client system [10]; and

in response, transmit the DNS reply message [28] including the service activation flag [27] only when the selected software application is installed for execution on the client system [10].

15~~7~~. The server computer system of claim 10~~2~~, ~~wherein the at least one hardware processor is~~ further characterized by being configured to:

in response to determining whether the client system [10] matches the target device profile, when the client system [10] matches the target device profile, randomly select the client system [10] for forensic data collection; and

in response, transmit the DNS reply message [28] including the service activation flag [27] only when the client system [10] is selected for forensic data collection.

16~~8~~. The server computer system of claim 10~~2~~, wherein the target device profile represents electronic devices further characterized by being of a selected appliance type.

17~~9~~. The server computer system of claim 10~~2~~, ~~wherein the at least one hardware processor is~~ further characterized by being configured to identify the client system [10] according to a client ID [25] included in the DNS query message [26], the client ID [25] uniquely identifying the client system [10] among the plurality of client systems [10a-f].

~~18~~20. The server computer system of claim 17~~9~~, wherein the client ID [25] comprises a hash value.

~~19. The method of claim 1, wherein the forensic data collection procedure further comprises transmitting an indicator of a current state of a client system selected from the plurality of client systems according to whether the electronic communication originated at the client system.~~

~~20. The computer system of claim 5, wherein the forensic data collection procedure further comprises transmitting an indicator of a current state of a client system selected from the plurality of client systems according to whether the electronic communication originated at the client system.~~