

RMC ECE Computer Security Lab (CSL) – zeek logs v0.9

List of zeek log files in this reference are numbered below and alphabetical order. The log files are organized and shown by page number as indicated in the table on to the right.

| | |
|----|----------------------------|
| 1 | analyzer.log |
| 2 | app_stats.log |
| 3 | capture_loss.log |
| 4 | conn.log |
| 5 | dce_rpc.log |
| 6 | dhcp.log |
| 7 | dnp3.log |
| 8 | dns.log |
| 9 | dns_entropy.log |
| 10 | dpd.log |
| 11 | files.log |
| 12 | ftp.log |
| 13 | http.log |
| 14 | http_entropy.log |
| 15 | irc.log |
| 16 | J4ssh.log |
| 17 | kerberos.log |
| 18 | known_hosts.log |
| 19 | known_modbus.log |
| 20 | known_services.log |
| 21 | ldap.log |
| 22 | ldap_search.log |
| 23 | loaded_scripts.log |
| 24 | modbus.log |
| 25 | modbus_register_change.log |
| 26 | mysql.log |
| 27 | notice.log |
| 28 | ntlm.log |
| 29 | ntp.log |
| 30 | ocsp.log |
| 31 | packet_filter.log |
| 32 | pe.log |
| 33 | radius.log |
| 34 | rdp.log |
| 35 | reporter.log |
| 36 | sip.log |
| 37 | smb_files.log |
| 38 | smb_mapping.log |
| 39 | smtp.log |
| 40 | snmp.log |
| 41 | ssh.log |
| 42 | ssl.log |
| 43 | stat.log |
| 44 | tunnel.log |
| 45 | websocket.log |
| 46 | weird.log |
| 47 | x509.log |

| Page # | zeek logs files |
|--------|----------------------------|
| 2 | conn.log |
| | app_stats.log |
| | known_hosts.log |
| | tunnel.log |
| 3 | known_services.log |
| | analyzer.log |
| | notice.log |
| | dpd.log |
| | loaded_scripts.log |
| 4 | dhcp.log |
| | weird.log |
| 5 | ssl.log |
| | packet_filter.log |
| | ssh.log |
| | j4ssh.log |
| 6 | x509.log |
| | ocsp.log |
| | reporter.log |
| | dns.log |
| 7 | dns_entropy.log |
| | ftp.log |
| | irc.log |
| | capture_loss.log |
| 8 | http.log |
| | http_entropy.log |
| | websocket.log |
| | snmp.log |
| 9 | files.log |
| | pe.log |
| | mysql.log |
| | sip.log |
| 10 | ntp.log |
| | radius.log |
| | smtp.log |
| | dce_rpc.log |
| 11 | rdp.log |
| | ldap.log |
| | ldap_search.log |
| | ntlm.log |
| 12 | kerberos.log |
| | smb_mapping.log |
| | smb_files.log |
| | modbus.log |
| 12 | known_modbus.log |
| | modbus_register_change.log |
| 12 | dnp3.log |
| | stat.log |



conn.log

| Field | Type | Description |
|----------------|----------|--|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address (AKA ORIG) |
| id.orig_p | port | Originating endpoint's TCP/UDP port (or ICMP code) |
| id.resp_h | addr | Responding endpoint's IP address (AKA RESP) |
| id.resp_p | port | Responding endpoint's TCP/UDP port (or ICMP code) |
| proto | protocol | Transport layer protocol of connection |
| service | string | Dynamically detected application protocol, if any |
| duration | interval | Time of last packet seen – time of first packet seen |
| orig_bytes | count | Originator payload bytes; from sequence numbers if TCP |
| resp_bytes | count | Responder payload bytes; from sequence numbers if TCP |
| conn_state | string | Connection state (see conn.log:conn_state table) |
| local_orig | bool | If conn originated locally T; if remotely F |
| local_resp | bool | If Site::local_nets empty, always unset. |
| missed_bytes | count | Number of missing bytes in content gaps |
| history | string | Connection state history (see conn.log:history table) |
| orig_pkts | count | Number of ORIG packets |
| orig_ip_bytes | count | Number of ORIG IP bytes (via IP total_length header field) |
| resp_pkts | count | Number of RESP packets |
| resp_ip_bytes | count | Number of RESP IP bytes (via IP total_length header field) |
| tunnel_parents | string | If tunneled, connection UID of encapsulating parent (s) |
| orig_cc | string | ORIG GeoIP Country Code |
| resp_cc | string | RESP GeoIP Country Cod |
| community_id | string | Correlation ID with suricata alerts |
| ja4l | string | Client to server latency Measurement / Light Distance |
| ja4ls | string | Server to client latency Measurement / Light Distance |
| ja4t | string | TCP Client Fingerprinting |
| ja4ts | string | TCP Server Response Fingerprinting |

local.zeek

packages/ja4

app_stats.log

| Field | Type | Description |
|--------------|----------|---|
| ts | time | Measurement timestamp |
| ts_delta | interval | Time difference from previous measurement |
| peer | string | Name of application |
| gaps | count | Number of unique hosts that used app |
| acks | count | Number of visits to app |
| percent_lost | count | Total bytes transferred to/from app |

known_services.log

| Field | Type | Description |
|------------|--------|--|
| ts | time | The time at which the service was detected |
| host | addr | The host on which the service is running |
| port_num | port | The port number on which service is running |
| port_proto | proto | The transport-layer protocol used by the svc |
| service | string | A protocol set, matching svc's payload(s) |

conn.log: conn_state

| Field | Type |
|--------|---|
| S0 | Connection attempt seen, no reply |
| S1 | Connection established, not terminated (0 byte count) |
| SF | Normal establishment and termination (>0 byte count) |
| REJ | Connection attempt rejected |
| S2 | Established, ORIG attempts close, no RESP reply |
| S3 | Established, RESP attempts close, no ORIG reply |
| RSTO | Connection established, ORIG aborted (RST) |
| RSTR | RESP sent a RST. |
| RSTOS0 | ORIG sent SYN followed by RST, no RESP SYN-ACK |
| RSTRH | RESP sent SYN-ACK then RST; no ORIG SYN |
| SH | ORIG sent SYN then FIN, no RESP SYN-ACK (half-open) |
| SHR | RESP sent SYN-ACK then FIN; no ORIG SYN |
| OTH | No SYN seen, just midstream traffic |

conn.log: history

| Field | Type |
|-------|--|
| A | Pure ACK |
| C | Packet with a bad checksum (applies to UDP too) |
| D | Packet with payload ("data") |
| F | Packet with FIN bit set |
| G | A content gap |
| H | A SYN+ACK ("handshake") |
| I | Inconsistent packet (e.g. FIN+RST bits set) |
| Q | Multi-flag packet (SYN+FIN or SYN+RST bits set) |
| R | Packet with RST bit set |
| S | A SYN w/o the ACK bit set |
| T | Packet with retransmitted payload |
| W | Packet with a zero window advertisement |
| ^ | Connection direction was flipped by Zeek's heuristic |

known_hosts.log

| Field | Type | Description |
|-------|------|-------------------------------|
| ts | time | Time when event was generated |
| host | addr | Host IP address |

tunnel.log

| Field | Type | Description |
|-------------|--------|-------------------------------------|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| tunnel_type | string | The type of tunnel |
| action | string | The type of activity that occurred |

analyzer.log

| Field | Type | Description |
|----------------|--------|--------------------------------------|
| ts | time | Time of log entry /connection |
| cause | string | Cause of analyzer error |
| analyzer_kind | string | Type of analyzer |
| analyzer_name | string | Name of analyzer |
| uid | string | Unique identifier for the connection |
| fuid | string | Unique file identifier |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| failure_reason | string | Cause of analyzer failure |
| failure_data | string | Support info related to failure |

dpd.log

| Field | Type | Description |
|----------------|--------|--|
| ts | time | Timestamp for when protocol analysis failed |
| uid | string | Connection unique ID |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| proto | enum | Transport protocol for the violation |
| analyzer | string | The analyzer that generated the violation |
| failure_reason | string | The textual reason for the analysis failure |
| packet_segment | string | chunk of the payload that most likely resulted in the analyzer violation |

loaded_scripts.log

| Field | Type | Description |
|-------|--------|---------------------------|
| name | string | Name of the script loaded |

dhcp.log

| Field | Type | Description |
|----------------|----------------|-----------------------------------|
| ts | time | Timestamp of the event |
| uids | set[string] | Connection UID |
| client_addr | addr | Client IP |
| server_addr | addr | Server IP |
| mac | string | Client MAC Address |
| host_name | string | Name given by client |
| client_fqdn | string | FQDN given by client |
| domain | string | Domain given by sever |
| requested_addr | Addr | IP requested by client |
| assigned_addr | addr | IP issued by server |
| lease_time | interval | Leave interval |
| client_message | string | Msg with DHCP_DECLINE from client |
| server_message | string | Msg with DHCP_NAK from server |
| msg_types | vector[string] | DHCP msgs in transaction |
| duration | interval | Duration of DHCP transaction |

notice.log

| Field | Type | Description |
|------------------------------|----------|---|
| ts | time | Timestamp of the event |
| uid | string | Connection ID |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port (or ICMP code) |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port (or ICMP code) |
| fuid | string | File unique identifier |
| file_mime_type | string | Libmagic sniffed file type |
| file_desc | string | Additional context for file, if available |
| proto | proto | Transport protocol |
| note | string | The type of notice |
| msg | string | Human readable message for the notice |
| sub | string | Sub-message for the notice |
| src | addr | Source address |
| dst | addr | Destination address |
| p | port | Associated port, if any |
| n | count | Associated count or status code |
| peer_descr | string | Description for peer that raised this notice |
| actions | set | Actions applied to this notice |
| email_dest | set | The email address(es) where to send this notice |
| suppress_for | interval | Indicates the length of time that this unique notice should be suppressed |
| remote_location.country_code | string | Geo_IP info |
| remote_location.region | string | Geo_IP info |
| remote_location.city | string | Geo_IP info |
| remote_location.latitude | string | Geo_IP info |
| remote_location.longitude | string | Geo_IP info |

weird.log

| Field | Type | Description |
|-----------|--------|---|
| ts | time | Timestamp of the event |
| uid | string | Connection ID |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | Port | Responding endpoint's TCP/UDP port |
| name | string | Name of the weird that occurred |
| addl | string | Additional information accompanying the weird, if any |
| notice | bool | Indicate if this weird was also turned into a notice |
| peer | string | The peer that generated this weird |
| source | string | Analyzer that detected the weird |



| Field | Type | Description |
|---------------------------|--------|--|
| ts | time | Time when the SSL connection was first detected |
| uid | string | Unique id for the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| version | string | SSL/TSL version |
| cipher | string | SSL/TLS cipher suite that the server chose |
| curve | string | Elliptic curve the server chose when using ECDH/ECDHE |
| server_name | string | Server Name request by the client |
| resumed | bool | Flag to indicate if the session was resumed reusing the key material exchanged in an earlier connection |
| last_alert | string | Last alert that was seen during the connection |
| next_protocol | | Next protocol the server chose using the app layer next protocol extension |
| established | string | Flag to indicate if this ssl session has been established successfully, or if it was aborted during the handshake |
| ssl_history | string | SSL history showing which types of packets we received in which order |
| cert_chain_fps | | An ordered vector of all cert fingerprints for certs offered by the server |
| client_cert_chain_fps | | An ordered vector of all cert fingerprints for the certs offered by the client |
| sni_matches_cert | bool | Set to true if the hostname sent in the SNI matches the certificate, set to false if they do not match and not set if the client did not send an SNI |
| ja4l | string | Client to Server Latency Measurement / Light Distance |
| ja4ls | string | Server JA4 signature |
| validation_status | string | Result of certificate validation for this connection |
| server_version | count | Numeric version of the server in the server hello |
| client_version | count | Numeric version of the client in the client hello |
| client_ciphers | vector | Ciphers that were offered by the client for the connection (vector of count) |
| ssl_client_exts | vector | SSL Client extensions (vector of count) |
| ssl_server_exts | vector | SSL Server extensions (vector of count) |
| ticket_lifetime_hint | count | Suggested ticket lifetime sent in the session ticket handshake by the server |
| dh_param_size | count | The Diffie-Helman parameter size, when using DH |
| point_formats | vector | Supported elliptic curve point formats (vector of count) |
| client_curves | vector | The curves supported by the client (vector of count) |
| orig_alpn | vector | Application layer protocol negotiation extension sent by the client (v of string) |
| client_supported_versions | vector | TLS 1.3 supported versions (vector of count) |
| server_supported_version | vector | TLS 1.3 supported versions (vector of count) |
| psk_key_exchange_modes | vector | TLS 1.3 Pre-shared key exchange modes (vector of count) |
| client_key_share_groups | vector | Key share groups from client hello (vector of count) |
| server_key_share_group | vector | Selected key share group from server hello (vector of count) |
| client_comp_methods | vector | Client supported compression methods (vector of count) |
| sigalgs | vector | Client supported signature algorithms (vector of count) |
| hashalgs | vector | Client supported hash algorithms (vector of count) |
| ocsp_status | string | Result of OCSP validation for this connection |
| valid_ct_logs | count | Number of different Logs for which valid SCTs were seen in the connection |
| valid_ct_operators | count | Number of different Log operators related to valid SCTs in the connection |

TLS History Packet Types

| | |
|---|--|
| A | supplemental_data |
| B | heartbeat |
| C | client_hello |
| D | application_data |
| E | end_of_early_data |
| F | finished |
| G | client_key_exchange |
| H | hello_request |
| J | hello_retry_request |
| K | server_key_exchange |
| L | alert |
| M | message_hash |
| N | server_hello_done |
| O | encrypted_extensions |
| P | key_update |
| Q | unknown_content_type |
| R | certificate_request |
| S | server_hello |
| T | NewSessionTicket |
| U | certificate_status |
| V | hello_verify_request |
| W | certificate_url |
| X | certificate |
| Y | certificate_verify |
| Z | unassigned_handshake_type I change_cipher_spec |

packages/ja4

policy/protocols/ssl/validate-certs

policy/protocols/ssl/ssl-log-ext

policy/protocols/ssl/validate-ocsp

policy/protocols/ssl/validate-sct

packet_filter.log

| Field | Type | Description |
|---------|--------|---|
| ts | time | The time at which the packet filter installation attempt was made |
| node | string | This is a string representation of the node that applied this packet filter |
| filter | string | The packet filter that is being set |
| init | bool | Indicate if this is the filter set during initialization |
| success | bool | Indicate if the filter was applied successfully |

ssh.log

| Field | Type | Description |
|------------------------------|--------------|------------------------------------|
| ts | time | Time when SSH connection detected |
| uid | string | string |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| version | count | Major SSH version |
| auth_success | bool | Authentication result |
| auth_attempts | count | The number of attempts observed |
| direction | direction | Direction of the connection |
| client | string | The client's version string |
| server | string | The server's version string |
| cipher_alg | string | The encryption algorithm in use |
| mac_alg | string | The signing (MAC) algorithm in use |
| compression_alg | string | The compression algorithm in use |
| kex_alg | string | The key exchange algorithm in use |
| host_key_alg | string | The server host key's algorithm |
| host_key | string | The server's key fingerprint |
| remote_location.country_code | geo-location | Geo Data |
| remote_location.region | geo-location | Geo Data |
| remote_location.city | geo-location | Geo Data |
| remote_location.latitude | geo-location | Geo Data |
| remote_location.longitude | geo-location | Geo Data |
| hasshversion | count | Version of HASSSH |
| hassh | string | HASSSH identifier for the client |
| hasshServer | string | HASSSH identifier for the server |
| cska | string | Client host key algos |
| hasshAlgorithms | string | Client hash algos |
| sshka | string | Server host key algos |
| hasshServerAlgorithms | string | Server algos |

→ hassh plugin

j4ssh.log

| Field | Type | Description |
|-----------|--------|-----------------------------------|
| ts | time | Command timestamp |
| uid | string | Unique id of the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| ja4ssh | string | JA4 SSH signature |

reporter.log

| Field | Type | Description |
|----------|--------|--|
| ts | time | Time when event was generated |
| level | String | Severity |
| message | String | Message text |
| location | String | If avail, script location where event occurred |

x509.log

| Field | Type | Description |
|------------------------------|----------------|--|
| ts | time | Current timestamp |
| fingerprint | string | Fingerprint of the certificate - uses chosen algorithm |
| certificate.version | count | Version number |
| certificate.serial | string | Serial number |
| certificate.subject | string | Subject |
| certificate.issuer | string | Issuer |
| certificate.not_valid_before | time | Timestamp before when certificate is not valid |
| certificate.not_valid_after | time | Timestamp after when certificate is not valid |
| certificate.key_alg | string | Name of the key algorithm |
| certificate.sig_alg | string | Name of the signature algorithm |
| certificate.key_type | string | Key type, if key parseable by openssl (either rsa, dsa or ec) |
| certificate.key_length | count | Key length in bits |
| certificate.exponent | string | Exponent, if RSA-certificate |
| certificate.curve | string | Curve, if EC-certificate |
| san.dns | vector[string] | List of DNS entries in SAN |
| san.uri | vector[string] | List of URI entries in SAN |
| san.email | vector[string] | List of email entries in SAN |
| san.ip | vector[addr] | List of IP entries in SAN |
| basic_constraints.ca | bool | CA flag set? |
| basic_constraints.path_len | count | Maximum path length |
| host_cert | bool | Indicates if this certificate was a end-host certificate, or sent as part of a chain |
| client_cert | bool | Indicates if this certificate was sent from the client |

ocsp.log

| Field | Type | Description |
|----------------|--------|--|
| ts | time | Time when the OCSP reply was encountered |
| id | string | File id of the OCSP reply |
| hashAlgorithm | string | Hash algorithm used to generate issuerNameHash and issuerKeyHash |
| issuerNameHash | string | Hash of the issuer's distinguished name |
| issuerKeyHash | string | Hash of the issuer's public key |
| serialNumber | string | Serial number of the affected certificate |
| certStatus | string | Status of the affected certificate |
| revoketime | time | Time at which the certificate was revoked |
| revokereason | string | Reason for which the certificate was revoked |
| thisUpdate | time | The time at which the status being shows is known to have been correct |
| nextUpdate | time | The latest time at which new information about the status of the certificate will be available |

dns.log

| Field | Type | Description |
|-------------|----------|--|
| ts | time | The earliest time of the DNS msg |
| uid | string | Unique id of the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port (or ICMP code) |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port (or ICMP code) |
| proto | protocol | Protocol of DNS transaction |
| trans_id | count | 16 bit identifier assigned by DNS client; responses match |
| rtt | interval | Round trip time for the query and response |
| query | string | Domain name subject of the query |
| qclass | string | Value specifying the query class |
| qclass_name | string | Descriptive name of the query class |
| qtype | count | Value specifying the query type |
| qtype_name | string | Name of the query type (e.g. A, AAAA, PTR) |
| rcode | count | Response code value in the DNS response |
| rcode_name | string | Descriptive name of the response code (e.g. NOERROR, NXDOMAIN) |
| AA | bool | Authoritative Answer. T = server is authoritative for query |
| TC | bool | Truncation. T = message was truncated |
| RD | bool | Recursion Desired. T = request recursive lookup of query |
| RA | bool | Recursion Available. T = server supports recursive queries |
| Z | count | Reserved field, should be 0 in queries and responses |
| answers | vector | List of resource descriptions in answer to the query |
| TTLs | vector | Caching intervals of the answers |
| rejected | bool | Whether the DNS query was rejected by the server |

ftp.log

| Field | Type | Description |
|----------------------|--------|--|
| ts | time | Command timestamp |
| uid | string | Unique id of the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| user | string | Username for FTP session |
| password | string | Password for FTP session |
| command | string | Command issued by the client |
| arg | string | Command argument, if present |
| mime_type | string | Value specifying the query class |
| file_size | count | Libmagic file type, if transferred |
| reply_code | count | Reply code from svr in response to cmd |
| reply_msg | string | Reply msg from svr in response to cmd |
| data_channel_passive | bool | Passive or active mode |
| data_channel_orig_h | addr | Client IP address |
| data_channel_resp_h | addr | Server address for data channel |
| data_channel_resp_p | port | Server port for data channel |
| fuid | string | Unique file ID |

dns_entropy.log

| Field | Type | Description |
|---------------------|----------|--|
| ts | time | The earliest time of the DNS msg |
| uid | string | Unique id of the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| proto | protocol | Transport layer protocol of connection |
| query | string | Domain name subject of the query |
| query_entropy | count | Entropy value of the query |
| qtype | count | Value specifying the query type |
| qtype_name | string | Name of the query type (e.g. A, AAAA, PTR) |
| rcode | count | Response code value in the DNS response |
| rcode_name | string | Descriptive name of the response code (e.g. NOERROR, NXDOMAIN) |
| ans | string | List of answers to the query |
| ans_entropy | count | Entropy value of the response |
| high_answer_entropy | count | Highest entropy value in the response |

irc.log

| Field | Type | Description |
|---------------|--------|---|
| ts | time | timestamp when the command was seen |
| uid | string | Unique ID for the connection |
| id.orig_h | addr | Originating endpoint's IP |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| nick | string | Nickname given for the connection |
| user | string | Username given for the connection |
| command | string | Command given by the client |
| value | string | Value for the command given by the client |
| addl | string | Any additional data for the command |
| dcc_file_name | string | DCC filename requested |
| dcc_file_size | count | Size of the DCC transfer as indicated by the sender |
| dcc_mime_type | string | Sniffed mime type of the file |
| fuid | string | File unique ID |

6

capture_loss.log

| Field | Type | Description |
|--------------|----------|--|
| ts | Time | The time the device was discovered |
| ts_delta | interval | Time delta between this and previous measurement |
| peer | string | Distinguishes between multiple peers |
| gaps | count | Number of missed ACKs |
| acks | count | Total number of ACKs |
| percent_loss | double | Percentage of ACKs seen where the data being ACKed wasn't seen |

http_entropy.log



| Field | Type | Description |
|-------------------|----------------|---|
| ts | time | Timestamp for when the request happened |
| uid | string | Unique ID for the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| trans_depth | count | Represents the pipelined depth into the connection of this request/response transaction |
| method | string | HTTP method |
| host | string | Value of host header |
| uri | string | URI used in the request |
| uri_entropy | double | 1-gram URI entropy |
| referrer | string | Value of referrer header |
| user_agent | string | Value of the User-Agent header from the client |
| request_body_len | count | Actual uncompressed content size of the data transferred from the client |
| response_body_len | count | Actual uncompressed content size of the data transferred from the server |
| status_code | count | Status code returned by the server |
| status_msg | string | Status message returned by the server |
| info_code | count | Last seen 1xx informational reply code returned by the server |
| info_msg | string | Last seen 1xx informational reply message returned by the server |
| orig_filenames | vector[string] | An ordered vector of filenames from the client |
| resp_filenames | vector[string] | An ordered vector of filenames from the server |
| username | string | Username if basic-auth is performed for the request |
| password | string | Password if basic-auth is performed for the request |
| proxied | set[string] | All of the headers that may indicate if the request was proxied |

websocket.log

| Field | Type | Description |
|-------------------|----------------|--|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| host | string | Same as in the HTTP log |
| uri | string | Same as in the HTTP log |
| user_agent | string | |
| subprotocol | string | WebSocket subprotocol selected by svr |
| client_protocols | vector[string] | Protocols requested by the client, if any |
| server_extensions | vector[string] | Extensions selected by the server, if any |
| client_extensions | vector[string] | Extensions requested by the client, if any |
| Client_key | string | Sec_WebSocket-Key header from client |
| Server_accept | string | Sec_WebSocket-Accept header from svr |

http.log

| Field | Type | Description |
|-------------------|----------------|--|
| ts | time | Timestamp for when the request happened |
| uid | string | Unique ID for the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| trans_depth | count | Represents the pipelined depth into the connection of this request/response transaction |
| method | string | HTTP method |
| host | string | Value of host header |
| uri | string | URI used in the request |
| referrer | string | Value of referrer header |
| version | string | Value of the version portion of the reply |
| user_agent | string | Value of the User-Agent header from the client |
| origin | string | Value of the Origin header from the client |
| request_body_len | count | Actual uncompressed content size of the data transferred from the client |
| response_body_len | count | Actual uncompressed content size of the data transferred from the server |
| status_code | count | Status code returned by the server |
| status_msg | string | Status message returned by the server |
| info_code | count | Last seen 1xx informational reply code returned by the server |
| info_msg | string | Last seen 1xx informational reply message returned by the server |
| tags | set[enum] | A set of indicators of various attributes discovered and related to a particular request/response pair |
| username | string | Username if basic-auth is performed for the request |
| password | string | Password if basic-auth is performed for the request |
| proxied | set[string] | All of the headers that may indicate if the request was proxied |
| orig_fuids | vector[string] | An ordered vector of file unique IDs |
| orig_filenames | vector[string] | An ordered vector of filenames from the client |
| orig_mime_types | vector[string] | An ordered vector of mime types |
| resp_fuids | vector[string] | An ordered vector of file unique IDs |
| resp_filenames | vector[string] | An ordered vector of filenames from the server |
| resp_mime_types | vector[string] | An ordered vector of mime types |
| ja4h | string | HTTP client fingerprinting |

ja4 plugin

snmp.log

| Field | Type | Description |
|-------------------|----------|---|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| duration | interval | The amount of time between the first packet belonging to the SNMP session and the latest one seen |
| version | string | The version of SNMP being used |
| community | string | The community string of the first SNMP packet associated with the session |
| get_requests | count | The number of variable bindings in GetRequest/GetNextRequest PDUs seen for the session |
| get_bulk_requests | count | The number of variable bindings in GetBulkRequest PDUs seen for the session |
| get_responses | count | The number of variable bindings in GetResponse/Response PDUs seen for the session |
| set_requests | count | The number of variable bindings in SetRequest PDUs seen for the session |
| display_string | string | A system description of the SNMP responder endpoint |
| up_since | time | The time at which the SNMP responder endpoint claims it's been up since |

pe.log

| Field | Type | Description |
|---------------------|--------|---|
| ts | time | Timestamp |
| id | string | File id of this portable executable file |
| machine | addr | The target machine for which the file was compiled |
| compile_ts | time | File compile time |
| os | string | OS for which the file was compiled |
| subsystem | string | The subsystem that is required to run this file? |
| is_exe | bool | Is the file an executable, or just an object file? |
| is_64bit | bool | Is the file a 64-bit executable? |
| uses_aslr | bool | Does the file support Address Space Layout Randomization? |
| uses_dep | bool | Does the file support Data Execution Prevention? |
| uses_code_integrity | bool | Does the file enforce code integrity checks? |
| uses_seh | bool | Does the file use structured exception handing |
| has_import_table | bool | Does the file have an import table? |
| has_export_table | bool | Does the file have an export table? |
| has_cert_table | bool | Does the file have an attribute certificate table? |
| has_debug_data | bool | Does the file have a debug table? |
| section_names | string | The names of the sections, in order |

files.log

| Field | Type | Description |
|------------------|-------------|--|
| ts | time | Timestamp of the event |
| fuid | string | Unique file ID |
| uid | string | Unique identifier for the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| source | string | Source protocol for how the file was transferred |
| depth | count | Depth of file related to the source |
| analyzers | set[string] | Set of analysis types conducted |
| mime_type | string | Libmagic file type |
| filename | string | File name if available |
| duration | interval | Duration of the file analysis |
| local_orig | bool | If transferred via network, did data originate locally? |
| is_orig | bool | If transferred via network, was file sent by the originator? |
| seen_bytes | count | Number of bytes provided to file analysis engine |
| total_bytes | count | Total number of bytes that should comprise the file |
| missing_bytes | count | Number of bytes in the file stream missed |
| overflow_bytes | count | Number of not all-in-sequence bytes in the file stream delivered to file analyzers due to reassembly buffer overflow |
| timedout | bool | If the file analysis time out at least once per file |
| parent_fuid | string | ID associated with a container file from which this one was extracted as a part of the analysis |
| md5 | string | Hash of file |
| sha1 | string | Hash of file |
| sha256 | string | Hash of file |
| extracted | string | Local filename of extracted files, if enabled |
| extracted_cutoff | bool | Was complete file extracted? |
| extracted_size | count | Size of of extracted file |

mysql.log

| Field | Type | Description |
|-----------|--------|---|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| cmd | string | Command issued |
| arg | string | Command arguments |
| success | bool | Svr indication whether cmd was successful |
| rows | count | Number of affected rows, if any |
| response | string | Svr msg, if any |

ntp.log

| Field | Type | Description |
|------------|----------|--|
| ts | time | Timestamp of the event |
| uid | string | Connection ID |
| id.orig_h | addr | Originating endpoint's IP |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP |
| version | count | NTP version |
| mode | count | Mode identifier |
| stratum | count | Stratum identifier |
| poll | interval | Max interval between successive msgs |
| precision | interval | Precision of system clock in log2 sec |
| root_delay | interval | Total round-trip delay to the reference clock, in NTP short format |
| root_disp | interval | Total dispersion to the reference clock, in NTP short format |
| ref_id | string | 32-bit code identifying the particular server or reference clock |
| ref_time | time | Time when the system clock was last set or corrected, in NTP timestamp format |
| org_time | time | Time at the client when the request departed for the server, in NTP timestamp format |
| rec_time | time | Time at the server when the request arrived from the client, in NTP timestamp format |
| xmt_time | time | Time at the server when the response left for the client, in NTP timestamp format |
| num_exts | count | Time at the client when the reply arrived from the server, in NTP timestamp forma |

smtp.log

| Field | Type | Description |
|------------------|----------------|------------------------------------|
| ts | time | Timestamp of the event |
| uid | string | Connection ID |
| id.orig_h | addr | Originating endpoint's IP |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP |
| trans_depth | count | Transaction depth if multiple msgs |
| helo | string | Contents of HELO header |
| mailfrom | string | E-mail addresses in From header |
| rcptto | set[string] | E-mail addresses in Rcpt header |
| date | string | Contents of date header |
| from | string | Contents of from header |
| to | set[string] | Contents of To header |
| cc | set[string] | Contents of CC header |
| reply_to | string | Contents of ReplyTo header |
| msg_id | string | Contents of MsgID header |
| in_reply_to | string | Contents of In-Reply-To header |
| subject | string | Contents of Subject header |
| x_originating_ip | addr | Contents of X-Originating header |
| first_received | string | Contents of First-Received header |
| second_received | string | Contents of Second-Receved header |
| last_reply | string | Last msg svr sent to client |
| path | vector[addr] | Message tx path |
| user_agent | string | Value of User-Agent from header |
| tls | bool | Was connection switched to TLS? |
| fuids | vector[string] | Unique File IDs attached to msg |

sip.log

| Field | Type | Description |
|-------------------|----------------|---|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| trans_depth | count | Represents the pipelined depth into the connection of this request/response transaction |
| method | string | Verb used in the SIP request |
| uri | string | URI used in the request |
| date | string | Contents of the Date: header from the client |
| request_from | string | Contents of the request From: header |
| request_to | string | Contents of the To: header |
| response_from | string | Contents of the response From: header |
| response_to | string | Contents of the response To: header |
| reply_to | string | Contents of the Reply-To: header |
| call_id | string | Contents of the Call-ID: header from the client |
| seq | string | Contents of the CSeq: header from the client |
| subject | string | Contents of the Subject: header from the client |
| request_path | vector /string | The client message transmission path |
| response_path | vector /string | The server message transmission path |
| user_agent | string | Contents of the User-Agent: header from the client |
| status_code | count | Status code returned by the server |
| status_msg | string | Status message returned by the server |
| warning | string | Contents of the Warning: header |
| request_body_len | count | Contents of the Content-Length |
| response_body_len | count | Contents of the Content-Length |
| content_type | string | Contents of the Content-Type |

radius.log

| Field | Type | Description |
|---------------|----------|---|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| username | string | Username, if present |
| mac | string | MAC addr, if present |
| framed_addr | addr | Address of network access svr, if present |
| tunnel_client | string | IPv4, IPv6, or FQDN address of tunnel initiating end, if present |
| connect_info | string | Connect info, if present |
| reply_msg | string | Reply msg from svr challenge |
| result | string | Successful or filed authentication |
| ttl | interval | Duration between 1 st request and Access-Accept msg or error |

dce_rpc.log

| Field | Type | Description |
|------------|----------|--|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| rtt | interval | Round trip time from request to response |
| named_pipe | string | Remote pipe name |
| endpoint | string | Endpoint name looked up from uid |
| operation | string | Operation seen in the call |

ldap.log

| Field | Type | Description |
|--------------------|--------|-------------------------------------|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| message_id | int | Cookie value used by client machine |
| version | int | |
| opcode | string | |
| result | string | |
| diagnostic_message | string | |
| object | string | |
| argument | string | |

ldap_search.log

| Field | Type | Description |
|--------------------|----------------|-------------------------------------|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| message_id | int | Cookie value used by client machine |
| scope | string | |
| deref_aliases | string | |
| base_object | string | |
| result_count | count | |
| result | string | |
| diagnostic_message | string | |
| filter | string | |
| attributes | vector[string] | |

rdp.log

| Field | Type | Description |
|-----------------------|--------|--|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| cookie | string | Cookie value used by client machine |
| result | string | Status result for connection |
| security_protocol | string | Security protocol chosen by server |
| client_channels | vector | Channels requested by the client |
| keyboard_layout | string | Keyboard layout (language) of client machine |
| client_build | string | RDP client version used by client machine |
| client_name | string | Name of client machine |
| client_dig_product_id | string | Product ID of client machine |
| desktop_width | count | Desktop width of client machine |
| desktop_height | count | Desktop height of client machine requested |
| _color_depth | string | Color depth requested by client in high_color_depth field |
| cert_type | string | If connection is encrypted with native RDP encryption, type of cert being used |
| cert_count | count | Number of certs seen |
| cert_permanent | bool | Indicates if provided certificate or certificate chain is permanent or temporary |
| encryption_level | string | Encryption level of connection |
| encryption_method | string | Encryption method of connection |

ntlm.log

| Field | Type | Description |
|--------------------------|--------|---|
| ts | time | Timestamp of the event |
| uid | string | Connection ID |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP port |
| username | string | Username given by the client |
| hostname | string | Hostname given by the client |
| Domainname | string | Domain name given by the client |
| server_nb_computer_name | string | NetBIOS name given by the server in a CHALLENGE |
| server_dns_computer_name | string | DNS name given by the server in a CHALLENGE |
| server_tree_name | string | Tree name given by the server in a CHALLENGE |
| success | bool | Was the authentication successful? |

kerberos.log

| Field | Type | Description |
|---------------------|--------|---|
| ts | time | Timestamp |
| uid | string | Unique ID of Connection |
| id.orig_h | addr | Originating endpoint's IP address (AKA ORIG) |
| id.orig_p | port | Originating endpoint's TCP/UDP port (or ICMP code) |
| id.resp_h | addr | Responding endpoint's IP address (AKA RESP) |
| id.resp_p | port | Responding endpoint's TCP/UDP port (or ICMP code) |
| request_type | string | Request type - Authentication Service ("AS") or Ticket Granting Service ("TGS") |
| client | string | Client |
| service | string | Service |
| success | bool | Request result |
| error_msg | count | Error code |
| from | string | Error message |
| till | time | Ticket valid until |
| cipher | string | Ticket encryption type |
| forwardable | bool | Forwardable ticket requested |
| renewable | bool | Renewable ticket requested |
| client_cert_subject | string | Subject of client certificate, if any |
| client_cert_fuid | string | File unique ID of client cert, if any |
| server_cert_subject | string | Subject of server certificate, if any |
| server_cert_fuid | string | File unique ID of server cert, if any |
| auth_ticket | string | Hash of ticket used to authorize request/transaction |
| new_ticket | string | Hash of ticket returned by the KDC |

Requires following to be loaded: policy/protocols/krb/ticket-logging.zeek

known_modbus.log

| Field | Type | Description |
|-------------|------|------------------------------------|
| ts | time | The time the device was discovered |
| host | addr | The IP address of the host |
| device_type | enum | The type of device being tracked |

policy/protocols/modbus/known-masters-slaves.zeek

modbus_register_change.log

| Field | Type | Description |
|-----------|----------|---|
| ts | time | Time of the request |
| uid | string | Unique identifier for the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| register | count | The device memory offset |
| old_val | count | The old value stored in the register |
| new_val | count | The new value stored in the register |
| delta | interval | The time delta between when the old_val and new_val were seen |

policy/protocols/modbus/track-memmap.zeek



smb_mapping.log

| Field | Type | Description |
|--------------------|--------|---|
| ts | time | Timestamp of the event |
| uid | string | Connection ID |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | Port | Responding endpoint's TCP/UDP port |
| path | string | Name of tree path |
| service | string | Type of resource of tree (share, pipe, etc) |
| native_file_system | string | File system of tree |
| share_type | string | If SMB2, share type will be included |

smb_files.log

| Field | Type | Description |
|----------------|--------|--|
| ts | time | Timestamp of the event |
| uid | string | Connection ID |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| fuid | string | string File unique identifier |
| action | enum | Action this log record represents |
| path | string | Path pulled from the tree this file was transferred to or from |
| name | string | Filename if one was seen |
| size | count | Total size of the file |
| prev_name | string | If the rename action was seen, this will be the file's previous name |
| times.modified | time | File modified time |
| times.accessed | time | File accessed time |
| times.created | time | File creation time |
| times.changed | time | File changed time |

modbus.log

| Field | Type | Description |
|-----------|--------|--|
| ts | time | Time of the request |
| uid | string | Unique identifier for the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| func | string | The name of the function message that was sent |
| exception | string | The exception if the response was a failure |

| Field | Type | Description |
|-------------------|---------|---|
| ts | time | Time of the request |
| uid | string | Unique identifier for the connection |
| id.orig_h | addr | Originating endpoint's IP address |
| id.orig_p | port | Originating endpoint's TCP/UDP port |
| id.resp_h | addr | Responding endpoint's IP address |
| id.resp_p | port | Responding endpoint's TCP/UDP port |
| fc_request | string | The name of the function message in the request |
| fc_reply | string | The name of the function message in the reply |
| iin | new_val | The response's "internal indication number" |

stats.log

| Field | Type | Description |
|-----------------------------|----------|--|
| ts | time | Timestamp for the measurement |
| peer | string | Peer that generated this log. Mostly for clusters |
| mem | count | Amount of memory currently in use in MB |
| pkts_proc | count | Number of packets processed since the last stats interval |
| bytes_recv | count | Number of bytes received since the last stats interval if reading live traffic |
| pkts_dropped | count | Number of packets dropped since the last stats interval if reading live traffic |
| pkts_link | count | Number of packets seen on the link since the last stats interval if reading live traffic |
| pkt_lag | interval | Lag between the wall clock and packet timestamps if reading live traffic |
| events_proc | count | Number of events processed since the last stats interval |
| events_queued | count | Number of events that have been queued since the last stats interval |
| active_tcp_conns | count | TCP connections currently in memory |
| active_udp_conns | count | UDP connections currently in memory |
| active_icmp_conns | count | ICMP connections currently in memory |
| tcp_conns | count | TCP connections seen since last stats interval |
| udp_conns | count | UDP connections seen since last stats interval |
| icmp_conns | count | ICMP connections seen since last stats interval |
| timers | count | Number of timers scheduled since last stats interval |
| active_timers | count | Current number of scheduled timers |
| files | count | Number of files seen since last stats interval |
| active_files | count | Current number of files actively being seen |
| dns_requests | count | Number of DNS requests seen since last stats interval |
| active_dns_requests | count | Current number of DNS requests awaiting a reply |
| reassem_tcp_size | count | Current size of TCP data in reassembly |
| reassem_file_size | count | Current size of File data in reassembly |
| reassem_frag_size | count | Current size of packet fragment data in reassembly |
| reassem_unknown_size | count | Current size of unknown data in reassembly (this is only PIA buffer right now) |