NetWitness Platform Unified Data Model Available Concepts

Meta Class	Meta Concept	Log Parser Key	Log Parser Key Flag	Meta Key	Meta Type	Meta Index	Notes
Reserved	Time	time	Transient	time	TimeT	IndexValues	This is the time at which a session hits a NetWitness Decoder. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness.
Reserved	Decoder Source	did	Transient	did	Text	IndexValues	This is the unique identifier used to identify a NetWitness Decoder. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Collector ID	lc.cid	None	lc.cid	Text	IndexValues	This is a unique Identifier of a Log Collector. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
	Source ID			source.id	UInt32		
Reserved	Medium	medium	Transient	medium	UInt8	IndexValues	This key is used to identify if it’s a log/packet session or Layer 2 Encapsulation Type. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness. 32 = log, 33 = correlation session, < 32 is packet session
	Exporter IPv4 Address			exporter.ipv4	IPv4		
	Exporter IPv6 Address			exporter.ipv6	IPv6		
Network	Service Type			service	UInt32	IndexValues	This is used to capture layer 7 protocols
Reserved	Device Type	device.type	None	device.type	Text	IndexValues	This is the name of the log parser which parsed a given session. This key should never be used to parse Meta data from a

							session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Miscellaneous	Process	child_process process	None	process	Text	IndexValues	This key is used to capture the Process Name, in case of parent child relationship, this can be used for child process name context.
Network	Traffic Flow Direction	direction	None	direction	Text	IndexValues	This Key should never be used in a parser, this is a reserved key used by the product to calculate the direction.
Physical	Country	country	Transient	country	Text	IndexValues	This is used to capture Country
Physical	Source Country	location_src	None	country.src	Text	IndexValues	This is used to capture Source Country
Physical	Destination Country	location_dst	None	country.dst	Text	IndexValues	This is used to capture Destination Country
Physical	ISP			isp	Text		This is used to capture service provider.
Physical	ISP			isp.src	Text		This is used to capture source service provider.
Physical	ISP			isp.dst	Text		This is used to capture destination service provider.
Physical	Source Organization	org.src	None	org.src	Text	IndexValues	This is used to capture the source organization based on the GEOPIP Maxmind database.
Physical	Destination Organization	org_dst org.dst	None	org.dst	Text	IndexValues	This is used to capture the destination organization based on the GEOPIP Maxmind database.
Investigations	ATT&CK Tactic	attack.tactic	None	attack.tactic	Text	IndexValues	MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. This key is used to capture the associated tactics.
Investigations	ATT&CK Technique	attack.technique	None	attack.technique	Text	IndexValues	MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. This key is used to capture the associated techniques.
Investigations	ATT&CK Technique ID	attack.tid	None	attack.tid	Text	IndexValues	MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. This key is used to capture the associated techniques.

Investigations	Behaviors of Compromise	boc	None	boc	Text	IndexValues	This is used to capture behaviour of compromise
Investigations	Indicators of Compromise	ioc	None	ioc	Text	IndexValues	This is key capture indicator of compromise degree of danger
Investigations	IOC Score	ioc.score	None	ioc.score	UInt16	IndexValues	This is key capture indicator of compromise degree of risk
Investigations	Enablers of Compromise	eoc	None	eoc	Text	IndexValues	This is used to capture Enablers of Compromise
Investigations	Investigation Category	inv.category	None	inv.category	Text	IndexValues	This used to capture investigation category
Investigations	Investigation Context	inv.context	None	inv.context	Text	IndexValues	This used to capture investigation context
Miscellaneous	UEBA Schema	ueba.schema	None	ueba.schema	Text	IndexValues	Capture values related to UEBA criteria
Miscellaneous	Action Event	web_method action	None	action	Text	IndexValues	This key is used to capture the primary action in a session
Miscellaneous	Errors	error	Transient	error	Text	IndexValues	This key captures All non successful Error codes or responses
Reserved	Parse Error	parse.error	None	parse.error	Text	IndexValues	This is a special key that stores any Meta key validation error found while parsing a log session. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Cryptography	Certificate Error String	cert_error	Transient	cert.error	Text		This key captures the Certificate Error String
Miscellaneous	Result	result	None	result	Text	IndexValues	This key is used to capture the outcome/result string value of an action in a session.
Miscellaneous	Result Code	resultcode	None	result.code	Text	IndexValues	This key is used to capture the outcome/result numeric value of an action in a session
Investigations	Event Activity	ec_activity	None	ec.activity	Text	IndexValues	This key captures the particular event activity(Ex:Logoff)

Investigations	Event Outcome	ec_outcome	None	ec.outcome	Text	IndexValues	This key captures the outcome of a particular Event(Ex:Success)
Investigations	Event Subject	ec_subject	None	ec.subject	Text	IndexValues	This key captures the Subject of a particular Event(Ex:User)
Investigations	Event Theme	ec_theme	None	ec.theme	Text	IndexValues	This key captures the Theme of a particular Event(Ex:Authentication)
Miscellaneous	Category	category	None	category	Text	IndexValues	This key is used to capture the category of an event given by the vendor in the session
	User Account	administrator logon_id owner service_account uid	None	username	Text	IndexValues	Deprecated, use user
Identity	Source User Account	c_username	None	user.src	Text	IndexValues	This key should only be used to capture the Source User in the event
Identity	Destination User Account	username	None	user.dst	Text	IndexValues	This key should only be used to capture the Destination User in the event
Network	Hostname Aliases	hostname devicehostname hostid r_hostid workstation web_host web_ref_host alias.host	None	alias.host	Text	IndexValues	This key should be used when the source or destination context of a hostname is not clear.Also it captures the Device Hostname. Any Hostname that isnt ad.computer.
Network	Source Hostname	shost	None	host.src	Text	IndexValues	This key should only be used when it’s a Source Hostname.
Network	Destination Hostname	dhost	None	host.dst	Text	IndexValues	This key should only be used when it’s a Destination Hostname
Miscellaneous	Client Application	agent	None	client	Text	IndexValues	This key is used to capture only the name of the client application requesting resources of the server. See the user.agent meta key for capture of the

							specific user agent identifier or browser identification string.
Miscellaneous	User Agent	user_agent	None	user.agent	Text	IndexValues	This key captures the user agent identifier or the browser identification string. See the client meta key for the client application making the request.
Network	Source IP Address	saddr	None	ip.src	IPv4	IndexValues	This key should only be used when it’s a Source IP Address.
Network	Destination IP address	daddr	None	ip.dst	IPv4	IndexValues	This key should only be used when it’s a Destination IP Address.
Network	Domain	domainname domain	None	domain	Text	IndexValues	This key should only be used to capture a Network Domain when the directionality is not clear. Use web.domain/tld/cctld/sld for Web based Domains
Email	E-mail Address	user_address cc bcc email	None	email	Text	IndexValues	This key is used to capture a generic email address where the source or destination context is not clear
File	Filename	filename	File	filename	Text	IndexValues	This key is used to capture the complete filename/Webpage with extension where the directionality is not clear. This should not include the directory/path
File	Directory	directory	None	directory	Text	IndexValues	This key is used to capture the file directory or path only
Miscellaneous	Parameter	param	None	param	Text	IndexValues	This key is the parameters passed as part of a command or application, etc.
Miscellaneous	Context	context info	None	context	Text	IndexValues	This key captures Information which adds additional context to the event.
Counters	Device class Counter 1	dclass_counter1	Transient	dclass.c1	Int32		This is a generic counter key that should be used with the label dclass.c1.str only
Counters	Device class Counter 1 Description	dclass_counter1_string	Transient	dclass.c1.str	Text		This is a generic counter string key that should be used with the label dclass.c1 only
Counters	Device class Counter 2	dclass_counter2	Transient	dclass.c2	Int32		This is a generic counter key that should be used with the label dclass.c2.str only

Counters	Device class Counter 2 Description	dclass_counter2_string	Transient	dclass.c2.str	Text		This is a generic counter string key that should be used with the label dclass.c2 only
Counters	Device class Counter 3	dclass_counter3	Transient	dclass.c3	Int32		This is a generic counter key that should be used with the label dclass.c3.str only
Counters	Device class Counter 3 Description	dclass_counter3_string	Transient	dclass.c3.str	Text		This is a generic counter string key that should be used with the label dclass.c3 only
Counters	Device class Ratio 1	dclass_ratio1	Transient	dclass.r1	Text		This is a generic ratio key that should be used with the label dclass.r1.str only
Counters	Device class Ratio 1 Description	dclass_ratio1_string	Transient	dclass.r1.str	Text		This is a generic ratio string key that should be used with the label dclass.r1 only
Counters	Device class Ratio 2	dclass_ratio2	Transient	dclass.r2	Text		This is a generic ratio key that should be used with the label dclass.r2.str only
Counters	Device class Ratio 2 Description	dclass_ratio2_string	Transient	dclass.r2.str	Text		This is a generic ratio string key that should be used with the label dclass.r2 only
Counters	Device class Ratio 3	dclass_ratio3	Transient	dclass.r3	Text		This is a generic ratio key that should be used with the label dclass.r3.str only
Counters	Device class Ratio 3 Description	dclass_ratio3_string	Transient	dclass.r3.str	Text		This is a generic ratio string key that should be used with the label dclass.r3 only
Counters	Event Counter	event_counter	Transient	event.counter	Int32		This is used to capture the number of times an event repeated
Cryptography	Certificate Thumbprint	cert.thumbprint	None	cert.thumbprint	Text	IndexValues	This key is used to capture the certificate thumbprint only
Cryptography	Certificate Common Name	cert_common	None	cert.common	Text	IndexValues	This key is used to capture the Certificate common name only
Cryptography	Certificate Common Name Source	cert_common_src	None	cert.common.src	Text	IndexValues	This key is used to capture the Certificate common name source only
Cryptography	Certificate Common Name	cert_common_dst	None	cert.common.dst	Text	IndexValues	This key is used to capture the Certificate common name source only
Cryptography	Certificate host category	cert_hostname_cat	Transient	cert.host.cat	Text		This key is used for the hostname category value of a certificate

Cryptography	Certificate Subject	cert_subject	None	cert.subject	Text	IndexValues	This key is used to capture the Certificate organization only
Cryptography	Certificate serial number	cert.serial	Transient	cert.serial	Text		This key is used to capture the Certificate serial number only
Cryptography	Certificate Authority	cert_ca	None	cert.ca	Text	IndexValues	This key is used to capture the Certificate signing authority only
Cryptography	Certificate status	cert_status	Transient	cert.status	Text		This key captures Certificate validation status
Cryptography	Cipher Name	encryption_type	Transient	crypto	Text	IndexValues	This key is used to capture the Encryption Type or Encryption Key only
Cryptography	Destination (Server) Cipher	d_cipher	Transient	cipher.dst	Text		This key is for Destination (Server) Cipher
Cryptography	Destination (Server) Cipher size	d_ciphersize	Transient	cipher.size.dst	Int32		This key captures Destination (Server) Cipher Size
Cryptography	Encryption peer identity	peer_id	Transient	peer.id	Text		This key is for Encryption peer’s identity
Cryptography	Encryption peer IP Address	peer	Transient	peer	Text		This key is for Encryption peer's IP Address
Cryptography	Encryption scheme used	scheme	Transient	scheme	Text		This key captures the Encryption scheme used
Cryptography	Encryption scheme used	sigtype	Transient	sig.type	Text		This key captures the Signature Type
Cryptography	IkE Cookie 1	ike_cookie1	Transient	ike.cookie1	Text		ID of the negotiation — sent for ISAKMP Phase One
Cryptography	IKE Cookie 2	ike_cookie2	Transient	ike.cookie2	Text		ID of the negotiation — sent for ISAKMP Phase Two
Cryptography	IKE Negotiation Phase	ike	Transient	ike	Text		IKE negotiation phase.
Cryptography	Source (Server) Cipher	s_cipher	Transient	cipher.src	Text		This key is for Source (Client) Cipher
Cryptography	Source (Server) Cipher size	s_ciphersize	Transient	cipher.size.src	Int32		This key captures Source (Client) Cipher Size

Database	Database ID	db_id	Transient	db.id	Text		This key is used to capture the unique identifier for a database
Database	Database instance name	instance	Transient	instance	Text		This key is used to capture the database server instance name
Database	Database Name	db_name	Transient	database	Text	IndexValues	This key is used to capture the name of a database or an instance as seen in a session
Database	Database server Process ID	db_pid	Transient	db.pid	Int32		This key captures the process id of a connection with database server
Miscellaneous	Function	function	None	function	Text	IndexValues	This key is used to capture the function name.
Database	Index ID	index	Transient	index	Text		This key captures IndexID of the index.
Database	Logical Reads	lread	Transient	lread	Int32		This key is used for the number of logical reads
Database	Logical Writes	lwrite	Transient	lwrite	Int32		This key is used for the number of logical writes
Database	Permissions	permissions	Transient	permissions	Text		This key captures permission or privilege level assigned to a resource.
Database	Physical Reads	pread	Transient	pread	Int32		This key is used for the number of physical writes
Database	SQL Transaction ID	trans_id	Transient	transact.id	Text		This key captures the SQL transantion ID of the current session
Database	Table Name	tbl_name	Transient	table.name	Text		This key is used to capture the table name
Email	Source E-mail Address	from	None	email.src	Text	IndexValues	This key is used to capture the source email address only, when the source context is not clear use email
Email	Destination E-mail Address	to	None	email.dst	Text	IndexValues	This key is used to capture the Destination email address only, when the destination context is not clear use email
Email	Subject	subject	None	subject	Text	IndexKeys	This key is used to capture the subject string from an Email only.
Endpoint	Machine State	host.state	None	host.state	Text	IndexValues	This key is used to capture the current state of the machine, such as blacklisted, infected,

							firewall disabled and so on
Endpoint	Registry Key	registry.key	None	registry.key	Text	IndexValues	This key captures the path to the registry key
Endpoint	Registry Value	registry.value	None	registry.value	Text	IndexValues	This key captures values or decorators used within a registry entry
File	Attachment	attachment	None	attachment	Text	IndexValues	This key captures the attachment file name
File	File Entropy	file_entropy	None	file.entropy	Float32	IndexValues	This is used to capture entropy vale of a file
File	Extension	web_extension extension	None	extension	Text	IndexValues	This key is used to capture the extension portion of a filename / extension of the page that was requested
File	File Type	filetype	Transient	filetype	Text	IndexValues	This key is used to capture the type of file only
File	File Category	file.cat	None	file.cat	Text	IndexValues	This key captures the type of file such as 'office application' or 'scripting engine'
File	File Category Source	file.cat.src	None	file.cat.src	Text	IndexValues	This key captures the type of file such as 'office application' or 'scripting engine'. This value is populated when there is a concept of source within the session
File	File Category Destination	file.cat.dst	None	file.cat.dst	Text	IndexValues	This key captures the type of file such as 'office application' or 'scripting engine'. This value is populated when there is a concept of destination within the session
File	Filename Source	filename_src	None	filename.src	Text	IndexValues	This is used to capture name of the parent filename, the file which performed the action
File	Filename Destination	filename_dst	None	filename.dst	Text	IndexValues	This is used to capture name of the file targeted by the action
File	Filename	filename.int	File	filename.int	Text	IndexValues	This key is used to capture the internal name of a file internal, such as the original or internal name in the PE structure of a windows executable.
File	File Size	filename_size	None	filename.size	Int32	IndexKeys	This key is used to capture the size of the file only
File	Source File Directory	directory.src	None	directory.src	Text	IndexValues	This key is used to capture the directory of the source process or file

File	Target File Directory	directory.dst	None	directory.dst	Text	IndexValues	This key is used to capture the directory of the target process or file
Miscellaneous	Source Checksum	checksum.src	None	checksum.src	Text	IndexValues	This key is used to capture the checksum or hash of the source entity such as a file or process.
Miscellaneous	Target Checksum	checksum.dst	None	checksum.dst	Text	IndexValues	This key is used to capture the checksum or hash of the the target entity such as a process or file.
File	Task Name	task_name	None	task.name	Text	IndexValues	This is used to capture name of the task
File	File Vendor	file_vendor	None	file.vendor	Text	IndexValues	This is used to capture Company name of file located in version_info
Healthcare	Patient Identifier	patient_id	Transient	patient.id	Text		This key captures the unique ID for a patient
Healthcare	Patient's First Name	patient_fname	Transient	patient.fname	Text		This key is for First Names only, this is used for Healthcare predominantly to capture Patients information
Healthcare	Patient's Last Name	patient_lname	Transient	patient.lname	Text		This key is for Last Names only, this is used for Healthcare predominantly to capture Patients information
Healthcare	Patient's Middle Name	patient_mname	Transient	patient.mname	Text		This key is for Middle Names only, this is used for Healthcare predominantly to capture Patients information
Identity	Accesses	accesses	None	accesses	Text	IndexValues	This key is used to capture actual priviliges used in accessing an object
Identity	Authentication Method	authmethod	Transient	auth.method	Text		This key is used to capture authentication methods used only
Identity	Domain OU	dn	None	dn	Text	IndexValues	X.500 (LDAP) Distinguished Name
Identity	Distinguished Name Source	src_dn	Transient	dn.src	Text		An X.500 (LDAP) Distinguished name that is used in a context that indicates a Source dn
Identity	Distinguished Name Destination	dst_dn	Transient	dn.dst	Text		An X.500 (LDAP) Distinguished name that used in a context that indicates a Destination dn

Identity	Domain ID	domain_id	Transient	domain.id	Text		This key captures Pre Windows 2000 (NetBIOS) name of the domain ONLY
Identity	Federated Identity Provider	federated_idp	Transient	federated.idp	Text		This key is the federated Identity Provider. This is the server providing the authentication.
Identity	Federated Service Provider	federated_sp	Transient	federated.sp	Text		This key is the Federated Service Provider. This is the application requesting authentication.
Identity	First name of a Person	user_fname	Transient	firstname	Text		This key is for First Names only, this is used for Healthcare predominantly to capture Patients information
Identity	Full Name	patient_fullname user_fullname	Transient	fullname	Text		This key is for Full Names only, this is used for Healthcare predominantly to capture Patients information, and for email senders and recipient names.
Identity	Full Name Source	user_fullname_src	None	fullname.src	Text		This key is for Full Names only, this is used for email sender name
Identity	Full Name Dest	user_fullname_dst	None	fullname.dst	Text		This key is for Full Names only, this is used for email recipient name
Identity	Host Role	host_role	None	host.role	Text	IndexValues	This key should only be used to capture the role of a Host Machine
Identity	Last name of a Person	user_lname	Transient	lastname	Text		This key is for Last Names only, this is used for Healthcare predominantly to capture Patients information
Identity	Ldap Generic	ldap	Transient	ldap	Text		This key is for Uninterpreted LDAP values. Ldap Values that don’t have a clear query or response context
Identity	Ldap Responses	ldap.response	Transient	ldap.response	Text		This key is to capture Results from an LDAP search
Identity	Ldap search criteria	ldap.query	Transient	ldap.query	Text		This key is the Search criteria from an LDAP search
Identity	Middle name of a Person	user_mname	Transient	middlename	Text		This key is for Middle Names only, this is used for Healthcare predominantly to capture Patients information
Identity	Owner	original_owner	None	owner	Text	IndexValues	This is used to capture username the process or service is running as, the author of the task

Identity	Password	password	Transient	password	Text	IndexKeys	This key is for Passwords seen in any session, plain text or encrypted
Identity	Realm	realm	Transient	realm	Text		Radius realm or similar grouping of accounts
Identity	User Account	user	None	user	Text	IndexValues	This key should be used when the source/destination/initiated/target of a username is not clear
Identity	User Role	user_role	Transient	user.role	Text		This key is used to capture the Role of a user only
Identity	User Unique ID/Logon ID	user.id	None	user.id	Text	IndexValues	This key is used to capture Unique identifier for an account.
Identity	Source User Session ID	c_sid	Transient	user.sid.src	Text		This key captures Source User Session ID
Identity	Destination User Session ID	sid	Transient	user.sid.dst	Text		This key captures Destination User Session ID
Identity	User's Department	user_dept	Transient	user.dept	Text		User's Department Names only
Identity	Organization	user_org	Transient	org	Text	IndexValues	This key captures the User organization
Identity	Service Account	service.account	None	service.account	Text		This key is a windows specific key, used for capturing name of the account a service (referenced in the event) is running under. Legacy Usage
Identity	Logon Type	logon_type	None	logon.type	Text	IndexValues	This key is used to capture the type of logon method used.
Identity	Description of Logon Type	logon_type_desc	None	logon.type.desc	Text	IndexValues	This key is used to capture the textual description of an integer logon type as stored in the meta key 'logon.type'.
Identity	User Profile	profile	Transient	profile	Text		This key is used to capture the user profile
Investigations	Event Categorization ID	event_cat event.cat	Transient	event.cat	UInt32		This key captures the Event category number
Investigations	Event Category Name	event_cat_name event.cat.name	None	event.cat.name	Text	IndexValues	This key captures the event category name corresponding to the event cat code
Investigations	File Analysis	analysis.file	None	analysis.file	Text	IndexValues	This is used to capture all indicators used in a File Analysis. This key should be used to capture an analysis of a file

Investigations	Process Analysis	analysis.process	None	analysis.process	Text	IndexValues	This is used to capture all indicators used in analysis of processes such as Endpoint.
Investigations	Service Analysis	analysis.service	None	analysis.service	Text	IndexValues	This is used to capture all indicators used in a Service Analysis. This key should be used to capture an analysis of a service
Investigations	Session Analysis	analysis.session	None	analysis.session	Text	IndexValues	This is used to capture all indicators used for a Session Analysis. This key should be used to capture an analysis of a session
Investigations	Vendor supplied Event Category	vendor_event_cat	Transient	event.vcat	Text		This is a vendor supplied category. This should be used in situations where the vendor has adopted their own event_category taxonomy.
Miscellaneous	Phone	calling_from calling_to phone_number	Transient	phone	Text		This is used to capture the Phone Number or a Calling station ID
Miscellaneous	Autorun Type	autorun_type	None	autorun.type	Text	IndexValues	This is used to capture Auto Run type
Miscellaneous	Change Attribute	change_attribute	Transient	change.attrib	Text		This key is used to capture the name of the attribute that’s changing in a session
Miscellaneous	Change New	change_new	Transient	change.new	Text		This key is used to capture the new values of the attribute that’s changing in a session
Miscellaneous	Change Old	change_old	Transient	change.old	Text		This key is used to capture the old value of the attribute that’s changing in a session
Miscellaneous	Checksum	checksum	None	checksum	Text	IndexValues	This key is used to capture the checksum or hash of the entity such as a file or process. Checksum should be used over checksum.src or checksum.dst when it is unclear whether the entity is a source or target of an action.
Miscellaneous	Checksum Algorithm	checksum.alg	None	checksum.algo	Text	IndexValues	This key is used to provide algorithm context for checksum meta.
Miscellaneous	Comments	comments	Transient	comments	Text		Comment information provided in the log message
Miscellaneous	Connection ID	connectionid	Transient	connection.id	Text		This key captures the Connection ID

Miscellaneous	Content Type	content	Transient	content	Text	IndexValues	This key captures the content type from protocol headers
Miscellaneous	Content Type	content_type	Transient	content.type	Text		This key is used to capture Content Type only.
Miscellaneous	Content Version	content_version	Transient	content.version	Text		This key captures Version level of a signature or database content.
Miscellaneous	Context Subject	s_context	Transient	context.subject	Text		This key is to be used in an audit context where the subject is the object being identified
Miscellaneous	Context Destination	context.dst	None	context.dst	Text	IndexValues	This key is to be used in an audit context where the target is the object being identified
Miscellaneous	Context Source	context.src	None	context.src	Text	IndexValues	This key is to be used in an audit context where the source is the object being identified
Miscellaneous	CPU Time	cpu	Transient	cpu	UInt32		This key is the CPU time used in the execution of the event being recorded.
Miscellaneous	Credit Card Number	cc.number	Transient	cc.number	Text		Valid Credit Card Numbers only
Miscellaneous	CVE	cve	Transient	cve	Text		This key captures CVE (Common Vulnerabilities and Exposures) - an identifier for known information security vulnerabilities.
Miscellaneous	Destination SPI Index	dst_spi	Transient	spi.dst	Text		Destination SPI Index
Miscellaneous	Device Name	device	None	device.name	Text	IndexValues	This is used to capture name of the Device associated with the node Like: a physical disk, printer, etc
Miscellaneous	Disposition	disposition	None	disposition	Text	IndexNone	This key captures the The end state of an action.
Miscellaneous	DNS Query Type	dns_querytype	Transient	dns.querytype	Text		This key is used to capture the DNS Query type only
Miscellaneous	Document/File number	doc_number	Transient	doc.number	Int32		This key captures File Identification number
Miscellaneous	Employer identification number	ein.number	Transient	ein.number	Text		Employee Identification Numbers only
Miscellaneous	Event Description	detail event_description	None	event.desc	Text	IndexValues	This key is used to capture a description of an event available directly or inferred

Miscellaneous	Event Hostname	event_computer	None	event.computer	Text	IndexValues	This key is a windows only concept, where this key is used to capture fully qualified domain name in a windows log.
Miscellaneous	Reference ID	id	None	reference.id	Text	IndexValues	This key is used to capture an event id from the session directly
Miscellaneous	Event Log Name	event_log	Transient	event.log	Text		This key captures the Name of the event log
Miscellaneous	Event Session ID	sessionid session_id	Transient	log.session.id	Text		This key is used to capture a sessionid from the session directly
Miscellaneous	Linked (Related) Session ID	sessionid1	Transient	log.session.id1	Text		This key is used to capture a Linked (Related) Session ID from the session directly
Miscellaneous	Event Source	event_source	None	event.source	Text	IndexValues	This key captures Source of the event that’s not a hostname
Miscellaneous	Event State	event_state	None	event.state	Text	IndexValues	This key captures the current state of the object/item referenced within the event. Describing an on-going event.
Miscellaneous	Event Type	event_type	None	event.type	Text	IndexValues	This key captures the event category type as specified by the event source.
Miscellaneous	Event User	event_user	None	event.user	Text		This key is a windows only concept, where this key is used to capture combination of domain name and username in a windows log.
Miscellaneous	Expected Value	expected_val	Transient	expected.val	Text		This key captures the Value expected (from the perspective of the device generating the log).
Miscellaneous	Filter Category Number	fcatnum	Transient	fcatnum	Text		This key captures Filter Category Number. Legacy Usage
Miscellaneous	Filter	filter	None	filter	Text	IndexValues	This key captures Filter used to reduce result set
Miscellaneous	Filter Result	fresult	Transient	fresult	Int32		This key captures the Filter Result
Miscellaneous	Found Search	found	Transient	found	Text	IndexValues	This is used to capture the results of regex match
Miscellaneous	Group ID	groupid	Transient	group.id	Text		This key captures Group ID Number (related to the group name)

Miscellaneous	Group Name	group	None	group	Text		This key captures the Group Name value
Miscellaneous	Group Object	group_object	Transient	group.object	Text		This key captures a collection/grouping of entities. Specific usage
Miscellaneous	Hardware/Serial ID	hardware_id	Transient	hardware.id	Text		This key is used to capture unique identifier for a device or system (NOT a Mac address)
Miscellaneous	Incident Name	incident	Transient	incident	Text		Name of an incident such as a group of alerts, audit logs, or remdiation logs.
Miscellaneous	Incident Name	incident.id	Transient	incident.id	Text		Unique identifier of an incident such as a group of alerts, audit logs, or remdiation logs.
Miscellaneous	Job Number	jobnum	Transient	job.num	Text		This key captures the Job Number
Miscellaneous	Languages	language	Transient	language	Text	IndexValues	This is used to capture list of languages the client support and what it prefers
Miscellaneous	LifeTime	lifetime	Transient	lifetime	UInt16		This key is used to capture the session lifetime in seconds.
Miscellaneous	Link to Data	link	Transient	link	Text	IndexKeys	This key is used to link the sessions together. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Miscellaneous	Linked Signature ID	sigid1	Transient	sig.id1	Int32		This key captures IDS/IPS Int Signature ID. This must be linked to the sig.id
Miscellaneous	Message	message	Transient	message	Text		This key captures the contents of instant messages
Miscellaneous	Message Body	message_body	Transient	message.body	Text		This key captures the The contents of the message body.
Miscellaneous	Name of the Terminal	terminal	Transient	terminal	Text		This key captures the Terminal Names only
Miscellaneous	Node	node	Transient	node	Text		Common use case is the node name within a cluster. The cluster name is reflected by the host name.
Miscellaneous	Object Name	obj_name	None	obj.name	Text	IndexValues	This is used to capture name of object
Miscellaneous	Object Type	obj_type	None	obj.type	Text	IndexValues	This is used to capture type of object

Miscellaneous	Observed Value	observed_val	Transient	observed.val	Text		This key captures the Value observed (from the perspective of the device generating the log).
Miscellaneous	Operation Number	operation_id	Transient	operation.id	Text		An alert number or operation number. The values should be unique and non-repeating.
Miscellaneous	Operating System	os	None	OS	Text	IndexValues	This key captures the Name of the Operating System
Miscellaneous	Packets Total	packets	None	packets	UInt32		This key is the total number of packets sent/received in a session. Also, in cases where the Sent or Received context is not clear, this can be used.
Miscellaneous	Parent Node Name	parent_node	Transient	parent.node	Text		This key captures the Parent Node Name. Must be related to node variable.
Miscellaneous	Policy Contents	policy_value	Transient	policy.value	Text		This key captures the contents of the policy. This contains details about the policy
Miscellaneous	Policy ID	policy_id	Transient	policy.id	Text		This key is used to capture the Policy ID only.
Miscellaneous	Policy Name	policyname signame	None	policy.name	Text	IndexValues	This key is used to capture the Policy Name only.
Miscellaneous	Pool ID	pool_id	Transient	pool.id	Text		This key captures the identifier (typically numeric field) of a resource pool
Miscellaneous	Pool Name	pool_name	Transient	pool.name	Text		This key captures the name of a resource pool
Miscellaneous	Port(Physical/Logical)	portname	Transient	port.name	Text		This key is used for Physical or logical port connection but does NOT include a network port. (Example: Printer port name).
Miscellaneous	Source Process Name	parent_process process_src	Transient	process.src	Text		This key is used to capture the Source Proccess Name, in case of parent child relationship, this can be used for parent process name context
Miscellaneous	Process ID	process_id	Transient	process.id	Int64		This key is used to capture the Process ID, in case of parent child relationship, this can be used for child process id context.
Miscellaneous	Source Process ID	process_id_src	Transient	process.id.src	Int64		This key is used to capture the Source Proccess ID, in case of parent child relationship, this can be used for parent process id context

Miscellaneous	Process ID Value	process_id_val	Transient	process.id.val	Text		This key is a failure key for Process ID when it is not an integer value
Miscellaneous	Source Parameter	param.src	None	param.src	Text	IndexValues	This key captures source parameter
Miscellaneous	Target Parameter	param.dst	None	param.dst	Text	IndexValues	This key captures the command line/launch argument of the target process or file
Miscellaneous	Product Name	product	Transient	product	Text		This key is used to capture the name of the product.
Miscellaneous	Reference Id1	id1	None	reference.id1	Text	IndexNone	This key is for Linked ID to be used as an addition to "reference.id"
Miscellaneous	Reference Id2	id2	None	reference.id2	Text	IndexNone	This key is for the 2nd Linked ID. Can be either linked to "reference.id" or "reference.id1" value but should not be used unless the other two variables are in play.
Miscellaneous	Match Search Item	match	Transient	match	Text	IndexKeys	This key is for regex match name from search.ini
Miscellaneous	Risk	risk	None	risk	Text	IndexValues	This key captures the non-numeric risk value
Miscellaneous	Risk Number	risk_num	None	risk.num	Float64	IndexValues	This key captures a Numeric Risk value
Miscellaneous	Risk Number Community	risk_num_comm	None	risk.num.comm	Float32		This key captures Risk Number Community
Miscellaneous	Risk Number NextGen	risk_num_next	None	risk.num.next	Float32		This key captures Risk Number NextGen
Miscellaneous	Risk Number SandBox	risk_num_sand	None	risk.num.sand	Float32		This key captures Risk Number SandBox
Miscellaneous	Risk Number Static	risk_num_static	None	risk.num.static	Float32		This key captures Risk Number Static
Miscellaneous	Rule Group	rule_group	Transient	rule.group	Text		This key captures the Rule group name
Miscellaneous	Rule Name	rulename	None	rule.name	Text		This key captures the Rule Name
Miscellaneous	Rule Number	rule	Transient	rule	Text		This key captures the Rule number
Miscellaneous	Rule Template	rule_template	Transient	rule.template	Text		A default set of parameters which are overlayed onto a rule (or rulename) which efffectively constitutes a template

Miscellaneous	Rule Unique ID	rule_uid	Transient	rule.uid	Text		This key is the Unique Identifier for a rule.
Miscellaneous	Search Engine Queries	search.text	Transient	search.text	Text	IndexKeys	This key captures the Search Text used
Miscellaneous	Sensor Name	sensor	Transient	sensor	Text		This key captures Name of the sensor. Typically used in IDS/IPS based devices
Miscellaneous	Serial Number	serial_number	None	serial.number	Text		This key is the Serial number associated with a physical asset.
Miscellaneous	Server Application	application	Transient	server	Text	IndexValues	This key is used to capture the name of the server application only
Miscellaneous	Server ID	server.id	Transient	server.id	Text	IndexValues	This key is used to capture the UUID of the server application only
Miscellaneous	Application Identification	appid	Transient	appid	Text	IndexValues	Application identification from OpenAppID
Miscellaneous	Severity	severity	Transient	severity	Text		This key is used to capture the severity given the session
Miscellaneous	Signature ID	sigid	None	sig.id	Int32	IndexValues	This key captures IDS/IPS Int Signature ID
Miscellaneous	Signature String	sigid_string	Transient	sig.id.str	Text		This key captures a string object of the sigid variable.
Miscellaneous	Signature Name	sig.name	None	sig.name	Text	IndexValues	This key is used to capture the Signature Name only.
Miscellaneous	SNMP OID	snmp.oid	Transient	snmp.oid	Text		SNMP Object Identifier
Miscellaneous	SNMP Value	snmp.value	Transient	snmp.value	Text		SNMP set request value
Miscellaneous	Source SPI Index	src_spi	Transient	spi.src	Text		Source SPI Index
Miscellaneous	SQL Query	sql	Transient	sql	Text	IndexKeys	This key captures the SQL query
Miscellaneous	Stream Info	streams	Transient	streams	UInt8	IndexValues	This key captures number of streams in session
	Client stream scanned bytes			scanned.client	UInt64		
	Server stream scanned bytes			scanned.server	UInt64		

Miscellaneous	Sub component Version	component_version	Transient	comp.version	Text		This key captures the Version level of a sub-component of a product.
Miscellaneous	Library	library	Transient	library	Text		This key is used to capture library information in mainframe devices
Miscellaneous	Listnum	listnum	Transient	listnum	Text		This key is used to capture listname or listnumber, primarily for collecting access-list
Miscellaneous	TCP Flags	tcp_flags	None	tcp.flags	UInt8		This key is captures the TCP flags set in any packet of session
Miscellaneous	TCP Flags Description	tcp.flags.desc	None	tcp.flags.desc	Text	IndexValues	This key is captures the textual representation, such as SYN or ACK, of TCP flags set in any packet of session.
Miscellaneous	Trigger Description	trigger_desc	Transient	trigger.desc	Text		This key captures the Description of the trigger or threshold condition.
Miscellaneous	Trigger Value	trigger_val	Transient	trigger.val	Text		This key captures the Value of the trigger or threshold condition.
Miscellaneous	Type Of Service	tos	Transient	tos	Int32		This key describes the type of service
Miscellaneous	Agent Id	agent.id	None	agent.id	Text	IndexValues	This key is used to capture agent id
Miscellaneous	Versions	version	None	version	Text	IndexValues	This key captures Version of the application or OS which is generating the event.
Miscellaneous	Vendor Name	vendor	None	vendor	Text	IndexValues	This key captures vendor name, such as SASE vendor.
Miscellaneous	Virtual system name	vsys	Transient	vsys	Text		This key captures Virtual System Name
Miscellaneous	Virus Name	virusname	None	virusname	Text	IndexValues	This key captures the name of the virus
Miscellaneous	VMWARE Target	vm_target	Transient	vm.target	Text		VMWare Target **VMWARE** only varaible.
Miscellaneous	Vulnerability Reference	vuln_ref	Transient	vuln.ref	Text		This key captures the Vulnerability Reference details
Miscellaneous	Workspace Description	workspace_desc	Transient	workspace	Text		This key captures Workspace Description
Miscellaneous	Payload Source	src_payload	Transient	payload.src	Text		Deprecated, use payload.req. This key is used to capture source payload

Miscellaneous	Payload Destination	dst_payload	Transient	payload.dst	Text		Deprecated, use payload.res. This key is used to capture destination payload
Miscellaneous	Mailbox ID/Name	mail_id	Transient	mail.id	Text		This key is used to capture the mailbox id/name
Network	Bytes Received	rbytes	Transient	rbytes	UInt64	IndexKeys	This key should only be used to capture the size of Bytes Received
Network	Bytes Sent	sbytes	None	bytes.src	UInt64	IndexKeys	This key should only be used to capture the size of Bytes Sent
Network	Bytes Total	bytes	None	bytes	UInt64		This key is the total number of Bytes sent/received in a session. Also, in cases where the Sent or Received context is not clear, this can be used.
Network	Source Domain	domain.src	None	domain.src	Text	IndexValues	This key should only be used to capture Source Domain Only.
Network	Destination Domain	domain.dst	None	domain.dst	Text	IndexValues	This key should only be used to capture Destination Domain Only.
Network	Ethernet Protocol	eth_type	None	eth.type	UInt16	IndexValues	This key is used to capture Ethernet Type, Used for Layer 3 Protocols Only
Network	Gateway	gateway	Transient	gateway	Text		This key is used to capture the IP Address of the gateway
Network	Hostname Originating	host.orig	None	host.orig	Text	IndexValues	This is used to capture the original hostname in case of a Forwarding Agent or a Proxy in between.
Network	ICMP Code	icmpcode	Transient	icmp.code	UInt32		This key is used to capture the ICMP code only
Network	ICMP Type	icmptype	Transient	icmp.type	UInt32		This key is used to capture the ICMP type only
Network	Capture Interface	capture.port	Transient	capture.port	Text	IndexValues	The interface from which a session was captured (eg, en0)
Network	Source Interface	sinterface	Transient	sinterface	Text	IndexValues	This key should only be used when it’s a Source Interface
Network	Interface Destination	dinterface	Transient	dinterface	Text		This key should only be used when it’s a Destination Interface
Network	Interface Generic	interface	Transient	interface	Text		This key should be used when the source or destination context of an interface is not clear

Network	IP Aliases	devicehostip alias.ip	None	alias.ip	IPv4	IndexValues	This key should be used when the source/destination/local/remote context of an IPv4 address is not clear
Network	IP Address v4 Translated Source	ip.trans.src	None	ip.trans.src	IPv4		This key should only be used when it’s a Source Translated IP Address
Network	IP Address v4 Translated Destination	ip.trans.dst	None	ip.trans.dst	IPv4		This key should only be used when it’s a Destination Translated IP Address
Network	IP Address Originating	ip.orig	None	ip.orig	IPv4	IndexValues	This is used to capture the original systems IPv4 address in case of a Forwarding Agent or a Proxy in between.
Network	Tunnel IP v4 Source			tunnel.ip.src	IPv4		Tunnel endpoint source IPv4 address.
Network	Tunnel IP v4 Destination			tunnel.ip.dst	IPv4		Tunnel endpoint destination IPv4 address.
Network	Source IPv6 Address	saddr_v6	None	ipv6.src	IPv6	IndexValues	This key should only be used when it’s a Source IP v6 Address
Network	Destination IPv6 address	daddr_v6	None	ipv6.dst	IPv6	IndexValues	This key should only be used when it’s a Destination IP v6 Address.
Network	IPv6 Aliases	alias.ipv6	None	alias.ipv6	IPv6	IndexValues	This key should be used when the source or destination context of an IPv6 address is not clear
Network	IP Address v6 Originating	ipv6.orig	None	ipv6.orig	IPv6	IndexValues	This is used to capture the original systems IPv6 address in case of a Forwarding Agent or a Proxy in between.
Network	Tunnel IP v6 Source			tunnel.ipv6.src	IPv6		Tunnel endpoint source IPv6 address.
Network	Tunnel IP v6 Destination			tunnel.ipv6.dst	IPv6		Tunnel endpoint destination IPv6 address.
Network	Ethernet Source	smacaddr	None	eth.src	MAC	IndexValues	This key should only be used when it’s a Source Mac Address.
Network	Ethernet Destination	dmacaddr	None	eth.dst	MAC	IndexValues	This key should only be used when it’s a Destination Mac Address

Network	MAC Address Generic	devicehostmac alias.mac	None	alias.mac	MAC		This key should be used when the source or destination context of a Mac Address is not clear
Network	Network mask Source	smask	Transient	smask	Text		This key is used for capturing source Network Mask
Network	Network mask Destination	dmask	Transient	dmask	Text		This key is used for Destionation Device network mask
Network	Network mask Generic	mask	Transient	mask	Text		This key is used to capture the device network IPmask.
Network	Network Name	netname	Transient	netname	Text	IndexValues	This key is used to capture the network name associated with an IP range. This is configured by the end user.
Network	Session Retransmits	rpackets	Transient	rpackets	UInt32		This key is used to capture the total number of retransmitted packets.
Network	Payload bytes in retransmitted packets	rpayload	Transient	rpayload	UInt32		This key is used to capture the total number of payload bytes seen in the retransmitted packets.
Network	Non-Protocol Specific Source Port	port.src	None	port.src	UInt16	IndexValues	This key should only be used when it’s a Source Port.
Network	Non-Protocol Specific Destination Port	port.dst	None	port.dst	UInt16	IndexValues	This key should only be used when it’s a Destination Port.
Network	Port Generic	port	None	port	UInt16	IndexValues	This key should only be used to capture a Network Port when the directionality is not clear
Network	Port Translated Source	port.trans.src	None	port.trans.src	UInt16	IndexValues	This key should only be used when it’s a Source Translated Port Number
Network	Port Translated Destination	port.trans.dst	None	port.trans.dst	UInt16	IndexValues	This key should only be used when it’s a Destination Translated Port Number
Network	IP Protocol	ip_proto	None	ip.proto	UInt8	IndexValues	This key should be used to capture the Protocol number, all the protocol nubers are converted into string in UI
Network	Protocol	protocol	Transient	protocol	Text		This key should be used to capture the protocol name
Network	Protocol Detail	protocol_detail	Transient	protocol.detail	Text		This key should be used to capture additional protocol information

Network	Service Name	service service.name	None	service.name	Text	IndexValues	This is used to capture descriptive service name, typically seen in Windows
Network	Network Service Name	network_service	Transient	network.service	Text		This is used to capture layer 7 protocols/service names
Network	TCP Source Port	tcp.srcport	Transient	tcp.srcport	UInt16	IndexValues	Deprecated, use port.src. This key capture source port for tcp protocol
Network	TCP Destination Port	tcp.dstport	Transient	tcp.dstport	UInt16	IndexValues	Deprecated, use port.dst. This key capture destination port for tcp protocol
Network	UDP Source Port	udp.srcport	Transient	udp.srcport	UInt16	IndexValues	Deprecated, use port.src. This key capture source port for udp protocol
Network	UDP Target Port	udp.dstport	Transient	udp.dstport	UInt16	IndexValues	Deprecated, use port.dst. This key capture destination port for udp protocol
Network	Tunnel Protocol	tunnel.proto	Transient	tunnel.proto	Text		Tunnel or virtual network protocol
Network	Virtual Network ID	vni	Transient	vni	UInt32		This key should only be used to capture the ID of a virtual network such as VLAN, VxLAN, Geneve, etc.
Network	Vlan Name	vlan.name	Transient	vlan.name	Text		This key should only be used to capture the name of the Virtual LAN
Network	Vlan Number	vlan	Transient	vlan	UInt16		Deprecated, use vni and tunnel.proto "vlan"
Network	VxLAN ID			vxlan	UInt32		Deprecated, use vni and tunnel.proto "vxlan"
Network	Zone Source	src_zone	Transient	zone.src	Text		This key should only be used when it’s a Source Zone.
Network	Zone Destination	dst_zone	Transient	zone.dst	Text		This key should only be used when it’s a Destination Zone.
Network	Zone Generic	zone	Transient	zone	Text		This key should be used when the source or destination context of a Zone is not clear
Physical	City	city	Transient	city	Text	IndexValues	This is used to capture the City location based on the GEOPIP Maxmind database.
Physical	Source City	city.src	Transient	city.src	Text	IndexValues	This is used to capture the source City location based on the GEOPIP Maxmind database.

Physical	Destination City	city.dst	Transient	city.dst	Text	IndexValues	This is used to capture the destination City location based on the GEOPIP Maxmind database.
Physical	Decimal Latitude			latdec	Float32	IndexNone	This is used to capture the Latitude based on the GEOPIP Maxmind database.
Physical	Source Latitude	latdec_src	None	latdec.src	Float32	IndexNone	This is used to capture the source Latitude based on the GEOPIP Maxmind database.
Physical	Destination Latitude	latdec_dst	None	latdec.dst	Float32	IndexNone	This is used to capture the destination Latitude based on the GEOPIP Maxmind database.
Physical	Decimal Longitude			longdec	Float32	IndexNone	This is used to capture the Longitude based on the GEOPIP Maxmind database.
Physical	Source Longitude	longdec_src	None	longdec.src	Float32	IndexNone	This is used to capture the source Longitude based on the GEOPIP Maxmind database.
Physical	Destination Longitude	longdec_dst	None	longdec.dst	Float32	IndexNone	This is used to capture the destination Longitude based on the GEOPIP Maxmind database.
Physical	Location	location_desc	Transient	loc.desc	Text	IndexValues	This is used to capture either the complete address or a description about a location being referenced in a session
Physical	State or province name	location_state	Transient	loc.state	Text		This is used to capture the State Name as seen in a session.
Reserved	Concentrator Source	cid	Transient	cid	Text	IndexValues	This is the unique identifier used to identify a NetWitness Concentrator. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Entropy Request	entropy.req	Transient	entropy.req	UInt16		This key is only used by the Entropy Parser, the Meta Type can be either UInt16 or Float32 based on the configuration
Reserved	Entropy Response	entropy.res	Transient	entropy.res	UInt16		This key is only used by the Entropy Parser, the Meta Type can be either UInt16 or Float32 based on the configuration
Reserved	Event Source Group	device.group	None	device.group	Text	IndexValues	This key should never be used to parse Meta data from a session (Logs/Packets)

							Directly, this is a Reserved key in NetWitness
Reserved	Device Class	device.class	None	device.class	Text	IndexValues	This is the Classification of the Log Event Source under a predefined fixed set of Event Source Classifications. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Device Discovery Score			device.disc	UInt8		
Reserved	Device Discovery Type			device.disc.type	Text		
Reserved	Device Host	device.host	None	device.host	Text	IndexValues	This is the Hostname of the log Event Source sending the logs to NetWitness. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Device IP	device.ip	None	device.ip	IPv4	IndexValues	This is the IPv4 address of the Log Event Source sending the logs to NetWitness. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Device IPv6	device.ipv6	None	device.ipv6	IPv6	IndexValues	This is the IPv6 address of the Log Event Source sending the logs to NetWitness. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Feed Category	feed.category	Transient	feed.category	Text	IndexKeys	This is used to capture the category of the feed. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Feed Description	feed_desc	None	feed.desc	Text	IndexKeys	This is used to capture the description of the feed. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness

Reserved	Feed Name	feed_name	None	feed.name	Text	IndexKeys	This is used to capture the name of the feed. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Header ID	header.id	None	header.id	Text		This is the Header ID value that identifies the exact log parser header definition that parses a particular log session. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Event Relay IPv4 Address	forward.ip	None	forward.ip	IPv4	IndexValues	This key should be used to capture the IPV4 address of a relay system which forwarded the events from the original system to NetWitness.
Reserved	Event Relay IPv6 Address	forward.ipv6	None	forward.ipv6	IPv6	IndexValues	This key is used to capture the IPV6 address of a relay system which forwarded the events from the original system to NetWitness. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Log Collector Time	lc.ctime	None	lc.ctime	TimeT		This is the time at which a log is collected in a NetWitness Log Collector. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Message ID1	vid	Transient	msg.vid	Text		This is the Message ID2 value that identifies the exact log parser definition which parses a particular log session. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Message ID	msg_id	None	msg.id	Text	IndexValues	This is the Message ID1 value that identifies the exact log parser definition which parses a particular log session. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness

Reserved	Most Common Byte Count Request	mcbc.req	Transient	mcbc.req	UInt32		This key is only used by the Entropy Parser, the most common byte count is the number of times the most common byte (above) was seen in the session streams
Reserved	Most Common Byte Count Response	mcbc.res	Transient	mcbc.res	UInt32		This key is only used by the Entropy Parser, the most common byte count is the number of times the most common byte (above) was seen in the session streams
Reserved	Most Common Byte Request	mcb.req	Transient	mcb.req	UInt8		This key is only used by the Entropy Parser, the most common byte request is simply which byte for each side (0 thru 255) was seen the most
Reserved	Most Common Byte Response	mcb.res	Transient	mcb.res	UInt8		This key is only used by the Entropy Parser, the most common byte response is simply which byte for each side (0 thru 255) was seen the most
Reserved	NWE Callback Id	nwe.callback_id	None	nwe.callback_id	Text	IndexKeys	This key denotes that event is endpoint related
Reserved	Payload Request	payload.req	Transient	payload.req	UInt32		Number of payload bytes in the request (client) stream.
Reserved	Payload Response	payload.res	Transient	payload.res	UInt32		Number of payload bytes in the response (server) stream.
Reserved	Payload Size	payload	Transient	payload	UInt32		This is the size of a payload in a Packet Session. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Message	msg	Transient	msg	Text	IndexNone	This key is used to capture the raw message that comes into the Log Decoder
Reserved	Remote Session ID	rid	Transient	rid	UInt64	IndexKeys	This is a special ID of the Remote Session created by NetWitness Decoder. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Session ID			sessionid	UInt64		This is a special ID of the session created by NetWitness Decoder. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Session Size	size	Transient	size	UInt32		This is the size of the session as seen by the NetWitness Decoder. This key should

							never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Source Filename	sourcefile	Transient	sourcefile	Text	IndexValues	This is the name of the log file or PCAPs that can be imported into NetWitness. This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Split Sessions	session.split	Transient	session.split	UInt16	IndexValues	This key should never be used to parse Meta data from a session (Logs/Packets) Directly, this is a Reserved key in NetWitness
Reserved	Unique Byte Count Request	ubc.req	Transient	ubc.req	UInt32		This key is only used by the Entropy Parser, Unique byte count is the number of unique bytes seen in each stream. 256 would mean all byte values of 0 thru 255 were seen at least once
Reserved	Unique Byte Count Response	ubc.res	Transient	ubc.res	UInt32		This key is only used by the Entropy Parser, Unique byte count is the number of unique bytes seen in each stream. 256 would mean all byte values of 0 thru 255 were seen at least once
Reserved	Endpoint Source Process ID	process.vid.src	None	process.vid.src	Text	IndexValues	Endpoint generates and uses a unique virtual ID to identify any similar group of process. This ID represents the source process.
Reserved	Endpoint Target Process ID	process.vid.dst	None	process.vid.dst	Text	IndexValues	Endpoint generates and uses a unique virtual ID to identify any similar group of process. This ID represents the target process.
Reserved	Text Token	word	Transient	word	Text	IndexValues	This is used by Concentrator to create a full-text index on any logs set that are processed by the log tokenizer parser on the Log Decoder. Archivers use a simple prefix-only index.
Storage	Disk Volume	disk_volume	Transient	disk.volume	Text		A unique name assigned to logical units (volumes) within a physical disk
Storage	Logical Unit Number	lun	Transient	lun	Text		Logical Unit Number.This key is a very useful concept in Storage.

Storage	Port World Wide Name	pwwn	Transient	pwwn	Text		This uniquely identifies a port on a HBA.
Threat	Alerts	alert	Transient	alert	Text	IndexValues	This key is used to capture name of the alert
Threat	Threat Category	threat_name	None	threat.category	Text	IndexValues	This key captures Threat Name/Threat Category/Categorization of alert
Threat	Threat Description	threat_val	None	threat.desc	Text	IndexValues	This key is used to capture the threat description from the session directly or inferred
Threat	Threat Source	threat_source	None	threat.source	Text	IndexValues	This key is used to capture source of the threat
Time	Event Time	event_time	None	event.time	TimeT	IndexValues	This key is used to capture the time mentioned in a raw session that represents the actual time an event occured in a standard normalized form
Time	Event Time String	event_time_string	Transient	event.time.str	Text		This key is used to capture the incomplete time mentioned in a session as a string
Time	Duration	duration_string	Transient	duration.str	Text		A text string version of the duration
Time	Duration in seconds	duration	None	duration.time	Float64		This key is used to capture the normalized duration/lifetime in seconds.
Time	Event Effective time	effective_time	Transient	effective.time	TimeT		This key is the effective time referenced by an individual event in a Standard Timestamp format
Time	Event End time	endtime	Transient	endtime	TimeT		This key is used to capture the End time mentioned in a session in a standard form
Time	Event Queing Time	event_queue_time	Transient	event.queue.time	TimeT		This key is the Time that the event was queued.
Time	Expiration time	expiration_time	Transient	expire.time	TimeT		This key is the timestamp that explicitly refers to an expiration.
Time	Expiration time string	expiration_time_string	Transient	expire.time.str	Text		This key is used to capture incomplete timestamp that explicitly refers to an expiration.
Time	Recorded time	recorded_time	Transient	recorded.time	TimeT		The event time as recorded by the system the event is collected from. The usage scenario is a multi-tier application where the management layer of the system records it's own timestamp at the time of

							collection from its child nodes. Must be in timestamp format.
Time	Time Start	starttime	None	starttime	TimeT	IndexValues	This key is used to capture the Start time mentioned in a session in a standard form
Time	Time Zone	timezone	None	timezone	Text	IndexValues	This key is used to capture the timezone of the Event Time
Web	Country Code Top level domain	cctld	Transient	cctld	Text		This key captures Country Top Level Domain extracted from a URL
Web	DNS Response Text	dns.resptext	Transient	dns.resptext	Text		This key is used to capture the DNS response text only
Web	DNS Response Type	dns.responsetype	Transient	dns.response type	Text		This key is used to capture the DNS Response type only
Web	FQDN	fqdn	None	fqdn	Text	IndexValues	Fully Qualified Domain Names
Web	Referer	web_referer referer	None	referer	Text	IndexKeys	This is used to capture the Web Referrer URL address specifically.
Web	Reputation Number	reputation_num	Transient	reputation.num	Float64		Reputation Number of an entity. Typically used for Web Domains
Web	Root URLPath	web_root	Transient	web.root	Text		This key captures the root URL path
Web	Second Level Domain	sld	Transient	sld	Text	IndexValues	Second Level Domains extracted from a URL
Web	Top Level Domains	tld	Transient	tld	Text	IndexValues	Top Level Domains extracted from a URL
Web	URL	url	Transient	url	Text		This key is used for capturing complete url
Web	Querystring	query web_query	None	query	Text	IndexKeys	This key is used to capture the Query portion of the URL.
Web	Web Cookie	web_cookie	Transient	web.cookie	Text		This key is used to capture the Web cookies specifically.
Web	Web page	webpage	Transient	web.page	Text		The captures the web page information
Web	Web referer Domain	web_ref_domain	Transient	web.ref.domain	Text		Web referer's domain
Web	Web referer query	web_ref_query	Transient	web.ref.query	Text		This key captures Web referer's query portion of the URL

Web	Web referer Root URLPath	web_ref_root	Transient	web.ref.root	Text		Web referer's root URL path
Web	Web Referrer page	web_ref_page	Transient	web.ref.page	Text		This key captures Web referer's page information
Web	Web request Domain	web_domain	Transient	web.domain	Text		This key captures Domain name in the Web Request
Wireless	Access Point	access_point	None	access.point	Text	IndexValues	This key is used to capture the access point name.
Wireless	WLAN Service Set Identifier	ssid bssid	Transient	wlan.ssid	Text	IndexKeys	This key is used to capture the ssid of a Wireless Session
Wireless	WLAN frequency channel	wifi_channel	Transient	wlan.channel	UInt16	IndexKeys	This is used to capture the channel names
Wireless	WLAN name/number	wlan	Transient	wlan.name	Text		This key captures either WLAN number/name
Miscellaneous	JA3 Fingerprint	ja3	Transient	ja3	Text	IndexValues	JA3 MD5 hash representing a client application's hello request during TLS negotiation.
Miscellaneous	JA3S Fingerprint	ja3s	Transient	ja3s	Text	IndexValues	JA3S MD5 hash representing a server response to a client application during TLS negotiation.
Miscellaneous	JA4 Fingerprint	ja4	Transient	ja4	Text	IndexValues	JA4 hash representing a fingerprint of a TLS client.
Miscellaneous	TLS Extensions Length	tls.extensionlen	Transient	tls.extensionlen	UInt16	IndexValues	Number of TLS extensions presented during negotiation.
Miscellaneous	TLS Premaster			tls.premaster	binary		TLS Premaster
Miscellaneous	Client Handshake Secret			tls.client.hdshk	binary		TLS 1.3 Client Handshake Secret
Miscellaneous	Server Handshake Secret			tls.server.hdshk	binary		TLS 1.3 Server Handshake Secret
Miscellaneous	Client Application Secret			tls.client.app	binary		TLS 1.3 Client Application Secret
Miscellaneous	Server Application Secret			tls.server.app	binary		TLS 1.3 Server Application Secret
Miscellaneous	Client Early Traffic Secret			tls.client.early	binary		TLS 1.3 Client Early Traffic Secret

Miscellaneous	ESM Callback			esm.callback	Text		Internal value for ESM feed.
	Active Directory Workstation Destination	ad_computer_dst	None	ad.computer.dst	Text	IndexValues	Deprecated, use host.dst
	Active Directory Workstation Source			ad.computer.src	Text	IndexValues	Deprecated, use host.src
	Active Directory Domain Destination			ad.domain.dst	Text	IndexValues	Deprecated, use domain.dst
	Active Directory Domain Source			ad.domain.src	Text	IndexValues	Deprecated, use domain.src
	Active Directory Username Destination			ad.username.dst	Text	IndexValues	Deprecated, use user.dst
	Active Directory Username Source			ad.username.src	Text	IndexValues	Deprecated, use user.src
	Alert ID	alert_id	None	alert.id	Text	IndexValues	Deprecated, New Hunting Model (inv.*, ioc, boc, eoc, analysis.*)
	Child Pid	child_pid	Transient	child.pid	Int32		Deprecated, use process.id
	Child Pid Value	child_pid_val	Transient	child.pid.val	Text		Deprecated, use process.id.val
	Destination Domain	ddomain	Transient	ddomain	Text		Deprecated, use domain.dst
	Translated Destination Address	dtransaddr	Transient	dtransaddr	Text		Deprecated, use ip.trans.dst
	Translated Destination Port	dtransport	Transient	dtransport	UInt16	IndexValues	Deprecated, use port.trans.dst. NOTE: There is a type discrepancy as currently used, TM: Text, INDEX: UInt16
	Ethernet Host Address	macaddr	None	eth.host	MAC		Deprecated, use alias.mac
	Event Classification			event.class	Text	IndexValues	Deprecated

	IP Address	hostip	None	ip.addr	IPv4	IndexValues	Deprecated, use alias.ip
	Destination Port	dport	None	ip.dstport	UInt16	IndexValues	Deprecated, use port.dst
	IP Source Port	sport	Transient	ip.srcport	UInt16	IndexValues	Deprecated, use port.src
	IPv6 Address	hostip_v6	Transient	ipv6.addr	IPv6		Deprecated, use alias.ipv6
	IP V6 Protocol			ipv6.proto	UInt8	IndexValues	Deprecated, use ip.proto
	Network Port	network_port	None	network.port	UInt64	IndexValues	Deprecated, use port. NOTE: There is a type discrepancy as currently used, TM: Int32, INDEX: UInt64 (why neither chose the correct UInt16?!)
	Originating IP Address	orig_ip	None	orig_ip	Text	IndexValues	Deprecated, use ip.orig, ipv6.orig or host.orig based on value type
	Device Address	paddr	None	paddr	IPv4	IndexValues	Deprecated
	Parent Pid	parent_pid	Transient	parent.pid	Int32		Deprecated, use process.id.src
	Privilege	privilege	Transient	privilege	Text		Deprecated, use permissions
	Process Time	processing_time	Transient	process.time	Text		Deprecated, use duration.time
	Risk: Informational	risk_info	None	risk.info	Text	IndexValues	Deprecated, use New Hunting Model (inv.*, ioc, boc, eoc, analysis.*)
	Risk: Suspicious	risk_suspicious	None	risk.suspicious	Text	IndexValues	Deprecated, use New Hunting Model (inv.*, ioc, boc, eoc, analysis.*)
	Risk: Warning	risk_warning	None	risk.warning	Text	IndexValues	Deprecated, use New Hunting Model (inv.*, ioc, boc, eoc, analysis.*)
	Source Domain	c_domain sdomain	Transient	sdomain	Text		Deprecated, use domain.src
	Site Category			site.cat	Text	IndexValues	Deprecated, use category
	SSL CA			ssl.ca	Text	IndexKeys	Deprecated, use cert.ca
	SSL Checksum			ssl.checksum	Text		Deprecated, use checksum

	SSL Common Name			ssl.common	Text		Deprecated, use cert.common
	SSL Subject			ssl.subject	Text	IndexKeys	Deprecated, use cert.subject
	SSL Destination Version	d_sslver	Transient	ssl.ver.dst	Text		Deprecated, use version
	SSL Source Version	s_sslver	Transient	ssl.ver.src	Text		Deprecated, use version
	Translated Source Address	stransaddr	Transient	stransaddr	Text		Deprecated, use ip.trans.src
	Translated Source Port	stransport	Transient	stransport	UInt16	IndexValues	Deprecated, use port.trans.src. NOTE: There is a type discrepancy as currently used, TM: Text, INDEX: UInt16
Physical	Country name	location_country	Transient	loc.country	Text		Deprecated, use country
Physical	City name	location_city	Transient	loc.city	Text		Deprecated, use city
		audit_class	Transient	audit.class	Text		Deprecated key defined only in table map.
		binary	Transient	binary	Text		Deprecated key defined only in table map.
		cert_hostname	Transient	cert.host.name	Text		Deprecated key defined only in table map.
		data	Transient	data	Text		Deprecated key defined only in table map.
		dead	Transient	dead	Int32		Deprecated key defined only in table map.
		device.type.id	Transient	device.type.id	Int32		Deprecated key defined only in table map.
		entry	Transient	entry	Text		Deprecated key defined only in table map.
		event_name	None	event.name	Text		Deprecated key defined only in table map.
		h_code	Transient	hcode	Text		Deprecated key defined only in table map.
		inode	Transient	inode	Int64		Deprecated key defined only in table map.
		level	None	level	Int32		Deprecated key defined only in table map.
		nodename	Transient	node.name	Text		Deprecated key defined only in table map.

		obj_id	Transient	obj.id	Text		Deprecated key defined only in table map.
		obj_server	Transient	obj.server	Text		Deprecated key defined only in table map.
		obj_value	Transient	obj.val	Text		Deprecated key defined only in table map.
		parent_pid_val	Transient	parent.pid.val	Text		Deprecated key defined only in table map.
		resource	Transient	resource	Text		Deprecated key defined only in table map.
		resource_class	Transient	resource.class	Text		Deprecated key defined only in table map.
		site	Transient	site	Text		Deprecated key defined only in table map.
		stamp	Transient	stamp	TimeT		Deprecated key defined only in table map.
		statement	Transient	statement	Text		Deprecated key defined only in table map.
		trans_from	Transient	trans.from	Text		Deprecated key defined only in table map.
		trans_to	Transient	trans.to	Text		Deprecated key defined only in table map.
		url_raw	Transient	url.raw	Text		Deprecated key defined only in table map.
File	Directory Path	dir.path	None	dir.path	Text	IndexValues	This key contains context for the directory path such as whether it is a user directory or a Windows program directory. This will be populated if there is no concept of source or destination path within the session. Otherwise, see the meta keys for Directory Path Source or Directory Path Destination.
File	Directory Path Source	dir.path.src	None	dir.path.src	Text	IndexValues	This key contains context for the directory path such as whether it is a user directory or a Windows program directory. This will be populated if there is a concept of source path within the session. Otherwise, see the meta keys for Directory Path or Directory Path Destination.
File	Directory Path Destination	dir.path.dst	None	dir.path.dst	Text	IndexValues	This key contains context for the directory path such as whether it is a user directory or a Windows program directory. This will

							be populated if there is a concept of destination path within the session. Otherwise, see the meta keys for Directory Path or Directory Path Source.
Identity	Community ID	community.id	Transient	community.id	Text	IndexNone	Community ID is a string identifier representing a given network flow and may be used to reduce the pivots between disparate event sources to a simple string comparison. Click here for the specification.