rdp.log | Remote Desktop Protocol (RDP)

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when the event happened
uid	string	Unique ID for the connection
id	conn_id	The connection's 4-tuple of endpoint addresses/ports
cookie	string	Cookie value used by client machine (username)
result	string	Status result for the connection. It's a mix between RDP negotiation failure messages and GCC server create response messages.
security_protocol	string	Security protocol chosen by server
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	The color depth requested by the client
cert_type	string	If the connection is being encrypted with native RDP encryption, this is the type of cert being used
cert_count	count	The number of certs seen: X.509 can transfer an entire certificate chain
cert_permanent	bool	Indicates if the provided certificate or certificate chain is permanent or temporary
encryption_level	string	Encryption level of the connection
encryption_method	string	Encryption method of the connection
ssl[1]	bool	Flag the connection if it was seen over SSL

[1] *Present if policy/protocols/rdp/indicate_ssl.bro is loaded*