NAME

auparse_interpret_field, auparse_interpret_realpath,auparse_interpret_sock_family,auparse_interpret_sock_port,auparse_interp

SYNOPSIS

#include <auparse.h>

const char *auparse_interpret_field(const auparse_state_t *_au_);
const char *auparse_interpret_realpath(const auparse_state_t *_au_);
const char *auparse_interpret_sock_family(auparse_state_t *_au_);
const char *auparse_interpret_sock_port(auparse_state_t *_au_);
const char *auparse_interpret_sock_address(const auparse_state_t *_au_);

DESCRIPTION

auparse_interpret_field allows access to the interpreted value in the current field of the current record in the current event. The returned string is escaped using the chosen method. The returned value will be destroyed if you call this function again. If you need to interpret another field and keep this value, you will have to copy it for later use.

Examples of things that could be interpreted are: uid, gid, syscall numbers, exit codes, file paths, socket addresses, permissions, modes, and capabilities. There are likely to be more in the future. If a value cannot be interpreted, its original value is returned.

auparse_interpret_realpath is like auparse_interpret_field except that it will call realpath on the results of gluing the cwd and file together. This also implies that it only valid to be called for the file name given in a PATH record.

auparse_interpret_sock_family will only return the socket family portion of a socket address.

auparse_interpret_sock_port will only return the port portion of a socket address. Not all socket families have a port. If that is the case, you will get a NULL value in which case your best option is to use the normal interpretation function.

auparse_interpret_sock_address will only return the address portion of a socket address. Not all socket families have an ip address. If that is the case, you will get a NULL value in which case your best option is to use the normal interpretation function.

RETURN VALUE

Returns NULL if there is an error otherwise a pointer to the interpreted value.

SEE ALSO

auparse_get_field_int(3), **auparse_get_field_str**(3), **auparse_set_escape_mode**(3).

AUTHOR

Steve Grubb