Wireshark 1.2 API Changes

June 16, 2009

Gerald Combs

Lead Developer | Wireshark

SHARKFEST **'09**

Stanford University

June 15-18, 2009

API Additions

…and other items of note

String Buffers

- Similar to GLib's GStrings
- Ephemeral-only
- Safe
- epan/emem.h

String Buffer Example

```
emem_strbuf_t *flags_strbuf = ep_strbuf_new_label("<None>");

for (i = 0; i < 8; i++) {
  bpos = 1 << i;
    if (tcph->th_flags & bpos) {
      if (first_flag) {
        ep_strbuf_truncate(flags_strbuf, 0);
      }
      ep_strbuf_append_printf(flags_strbuf, "%s%s",
          first_flag ? "" : ", ", fstr[i]);
    first_flag = FALSE;
  }
}
```

String Pointers: The Forbidden Dance

From this…

```
bp += MIN(512-(bp-buffer),
    g_snprintf(bp, 512-(bp-buffer),
    "DoRed"));
```

…to this:

```
ep_strbuf_append(buffer, "DoRed");
```

Proto tree

- BASE_CUSTOM
- proto_tree_add_XXX_hidden
- proto_mark_private
- Delayed field arrays

tvbuffs

- tvb_new_child_real_data
- tvb_child_uncompress
- Seasonal string fetching

String Strings

- Similar to value_strings
- match_strstr_idx
- match_strstr
- str_to_str

Lua

- Lots of activity since 1.0
- Full info @ DT-6

Columns

- check_col deprecated

packet_info

- Now officially bloated
- Maybe discuss @ RT-1?

New in checkAPIs.pl

- strdup, strndup
- bzero, bcopy, bcmp
- calloc, realloc, valloc, cfree
- g_strup, g_strdown, g_string_up, g_string_down
- tmpnam, perror
- abort, error, g_assert, g_error
- Lots more GLib & GTK+

Reorganization

- Some things moved to wsutil
  - File, String, Unicode, Type utils
  - Privileges
  - MPEG audio
- CRC code moving to epan/crc

Library Changes

- c-ares
- GeoIP

Windows

- Visual C++ Pro 2008 SP1 default
  - Welcome to “Manifest Hell”
- Support libraries still using VC++ 6
  - By force if necessary
- VC++ 6.0 support diminishing

64-bit Windows

- Officially supported in 1.2
- LLP64
- Lots of casts
- Some API types are now size_t
- No docs for cross-compile
- To cross-compile:
  1. set WIRESHARK_TARGET_PLATFORM=win64
  2. call "c:\Path\To\vcvarsall.bat" x86_amd64

Further Reading

- http://blogs.msdn.com/oldnewthing/archive/2005/01/31/363790.aspx

Bonus Material

Misc Goodies

- base64_to_tvb
- register_postdissector
- decode_bits_in_field
- proto_tree_add_bitmask_text

Future

- Python
- Web / help links