Literarisches Code-Quartett 2004

Andreas Bogk
Felix von Leitner
FX of Phenoelit
Michael Natterer

Literarisches Code-Quartett 2004

Build Process

```
/*
*       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
*       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
*       !!!!!!!IF YOU CHANGE TABS TO SPACES, YOU WILL BE KILLED!!!!!!!
*       !!!!!!!!!!!!!!DOING SO FUCKS THE BUILD PROCESS!!!!!!!!!!!!!!!!
*       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
*       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
*/
```

Literarisches Code-Quartett 2004

Eingabefokus

```
win2k/private/shell/browseui/menuband.cpp

    case WM_CONTEXTMENU:
        // HACKHACK (lamadio): Since the start button has the keyboard focus,
        // the start button will handle this. We need to forward this off to the
        // currently tracked item at the bottom of the chain
        LRESULT lres;
        IWinEventHandler* pweh;

        if (_fMenuMode &&
            SUCCEEDED(QueryService(SID_SMenuBandBottomSelected,
            IID_IWinEventHandler, (LPVOID *)&pweh)))
        {
            // BUGBUG (lamadio): This will only work because only one of the two
            // possible toolbars handles this
```

Literarisches Code-Quartett 2004

Alpha Compiler

`win2k/private/shell/shell32/util.cpp`

```
  // BUGBUG (reinerf)
  // the fucking alpha cpp compiler seems to fuck up the goddam
  // type "LPITEMIDLIST", so to work around the fucking peice of
  // shit compiler we pass the last param as an void *instead of
  // a LPITEMIDLIST
```

Literarisches Code-Quartett 2004

Word HTML

```
///////////////////////////////////////////////////////////
//
// !!HACKHACKHACKHACKHACKHACKHACKHACKHACKHACKHACKHACKHACK
//
// Again, because of the nasty break on empty bits in
// ui-generated elements, we must ignore simulated text
// when certain elements are nested. For example,
// <blockquote> and <div>.
//

if (_textInScope == TIS_FAKE &&
    (bsTop.pNodeBlock->Tag() == ETAG_BLOCKQUOTE ||
     bsTop.pNodeBlock->Tag() == ETAG_DIV))
{
    fBreak = NO_BREAK;
}

//
// !!HACKHACKHACKHACKHACKHACKHACKHACKHACKHACKHACKHACKHACK
//
///////////////////////////////////////////////////////////
```

Literarisches Code-Quartett 2004

Eudora

```
//
//  Eudora is a pile of crap.
//
//  When they get a NM_DBLCLK notification from a treeview, they say,
//  "Oh, I know that treeview allocates its NMHDR from the stack, and
//  there's this local variable on Treeview's stack I'm really interested
//  in, so I'm going to hard-code an offset from the pnmhdr and read the
//  DWORD at that location so I can get at the local variable.  I will then
//  stop working if this value is zero."
//
//  The conversion to UNICODE changed our stack layout enough that they
//  end up always getting zero -- it's the NULL parameter which is the
//  final argument to CCSendNotify.  Since all this stack layout stuff is
//  sensitive to how the compiler's optimizer feels today, we create a
//  special notify structure Just For Eudora which mimics the stack layout
//  they expected to see in Win95.
//
typedef struct NMEUDORA {
    NMHDR   nmhdr;
    BYTE    Padding[48];
    DWORD   MustBeNonzero;      // Eudora fails to install if this is zero
} NMEUDORA;
```

Literarisches Code-Quartett 2004

Fensterverwaltung

```
win2k/private/shell/shlwapi/mlui.cpp

      // Grab the title of the parent
      GetWindowTextWrapW(hWnd, szBuffer, ARRAYSIZE(szBuffer));

      // HACKHACK YUCK!!!!
      // Is the window the Desktop window?
      if (!StrCmpW(szBuffer, L"Program Manager"))
      {
          // Yes, so we now have two problems,
          // 1. The title should be "Desktop" and not "Program Manager", and
          // 2. Only the desktop thread can call this or it will hang the desktop
          //    window.

          // Is the window Prop valid?
          if (GetWindowThreadProcessId(hWnd, 0) == GetCurrentThreadId())
```

Literarisches Code-Quartett 2004

Fehlercodes

```
win2k/private/inet/wininet/urlcache/instcon.cxx

      // CD not in drive.
      case ERROR_INVALID_DRIVE:
      case ERROR_NOT_READY:
      case ERROR_WRONG_DISK:

          dwError = ERROR_INTERNET_INSERT_CDROM;
          break;
```

Literarisches Code-Quartett 2004

Cryptic Phone I

```c
x = 3;
p = (unsigned char *)(prot->txcryptcnt);
for (i=0; i<16; i++)
{
  y = *p;
  *p += x;
  if (*p++ >= y)
    break;
  x = 1;
}
```

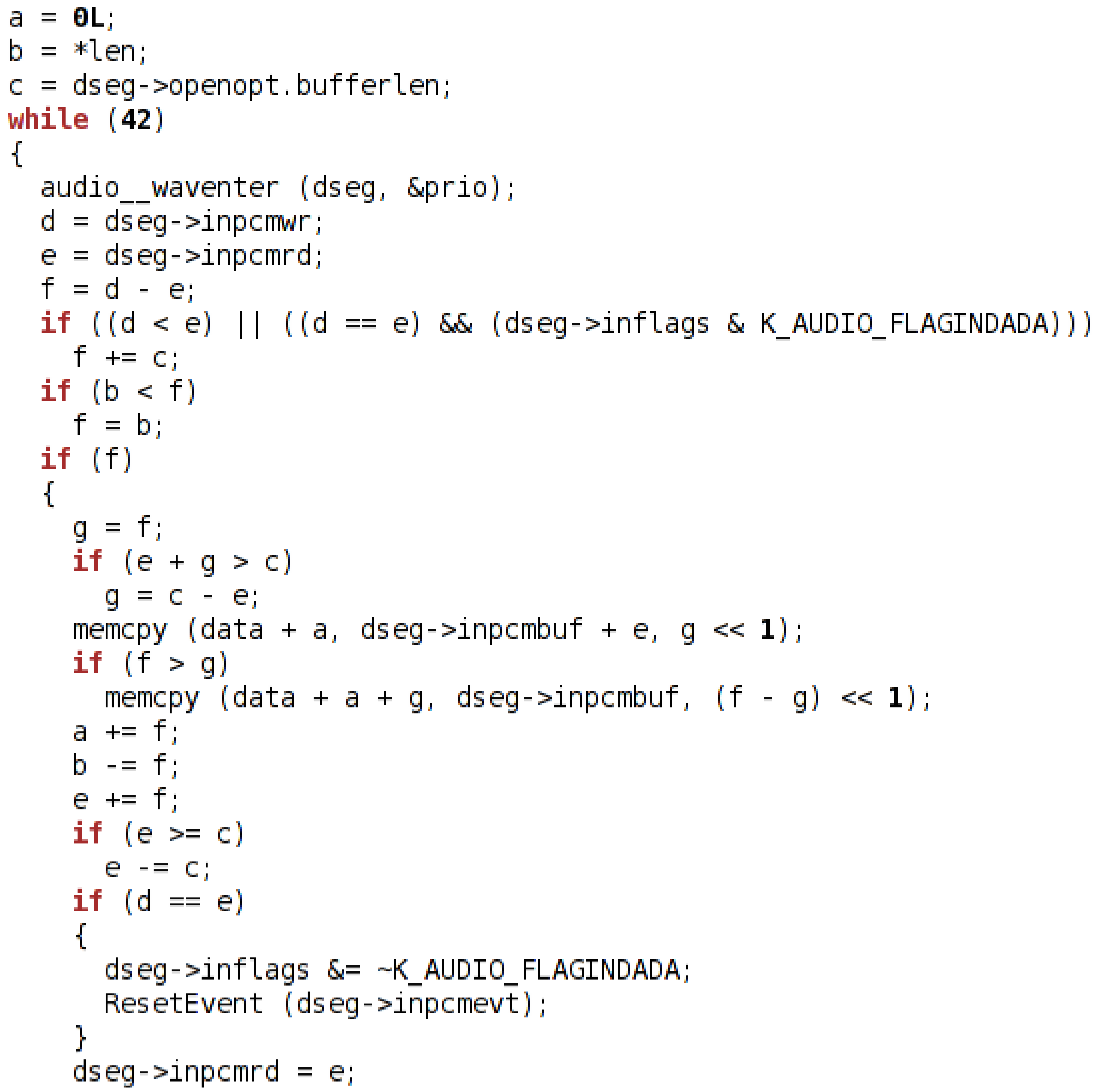
Literarisches Code-Quartett 2004

Cryptic Phone II

```c
/* Add sync-info */
p = (unsigned char *)(prot->rxcryptcnt);
x = data & 0x0F;
*p = (*p & 0xC0) | (x << 2);
if ((x & 0x01) == 0)
  y = 6;
else
  y = 8 + (x << 1);
x = data >> 4;
for (i=0; i<2; i++)
{
  p[y>>3] = (p[y>>3] & ~(0x03 << (y & 0x06))) | ((x & 0x03) << (y & 0x06));
  x >>= 2;
  y += 2;
}
```

Literarisches Code-Quartett 2004

Cryptic Phone III



```c
a = 0L;
b = *len;
c = dseg->openopt.bufferlen;
while (42)
{
  audio__waventer (dseg, &prio);
  d = dseg->inpcmwr;
  e = dseg->inpcmrd;
  f = d - e;
  if ((d < e) || ((d == e) && (dseg->inflags & K_AUDIO_FLAGINDADA)))
    f += c;
  if (b < f)
    f = b;
  if (f)
  {
    g = f;
    if (e + g > c)
      g = c - e;
    memcpy (data + a, dseg->inpcmbuf + e, g << 1);
    if (f > g)
      memcpy (data + a + g, dseg->inpcmbuf, (f - g) << 1);
    a += f;
    b -= f;
    e += f;
    if (e >= c)
      e -= c;
    if (d == e)
    {
      dseg->inflags &= ~K_AUDIO_FLAGINDADA;
      ResetEvent (dseg->inpcmevt);
    }
    dseg->inpcmrd = e;
```

Literarisches Code-Quartett 2004

Memory Corruption

```
IOS-11.2-8/sys/os/sched.c:409:

  /*
  * Duplicates of certain scheduler variables.  Some process keeps
  * trashing memory and causing the scheduler to trip up.  These variables
  * are used to validate key data structures.
  *
  * DO NOT MOVE THESE VARIABLES.  They are purposefully some distance away
  * from their original declarations.
  *
  * DO NOT MODIFY THESE DECLARATIONS.  They are set up to force some
  * variables into the DATA segment and some into the BSS.  This further
  * separates the variables in memory and prevents accidental corruption
  * of both variables.
  */
  sprocess *forkx_2 = NULL;     /* current process (data copy) */
  sprocess *forkx_3;            /* current process (bss copy) */
```

Literarisches Code-Quartett 2004

Error Handling

```
MySql 4.1.7, ndb/src/common/util/strdup.c

  #ifndef HAVE_STRDUP
  char *
  strdup(const char *s){
    void *p2;
    p2 = malloc(strlen(s)+1);
    strcpy(p2, s);
    return p2;
  }
  #endif
```

Literarisches Code-Quartett 2004

man strcpy
man strcat
man memset

```
MySQL 4.1.7, innobase/log/log0recv.c:2988:

      log_dir_len = strlen(log_dir);
      /* reserve space for log_dir, "ib_logfile" and a number */
      name = memcpy(mem_alloc(log_dir_len + ((sizeof logfilename) + 11)),
              log_dir, log_dir_len);
      memcpy(name + log_dir_len, logfilename, sizeof logfilename);


      buf = ut_malloc(LOG_FILE_HDR_SIZE + OS_FILE_LOG_BLOCK_SIZE);
      memset(buf, LOG_FILE_HDR_SIZE + OS_FILE_LOG_BLOCK_SIZE, '\0');
```

Literarisches Code-Quartett 2004

Giftnullbyte

```
MySQL 4.1.7, libmysqld/log.cc:2322:

  void print_buffer_to_nt_eventlog(enum loglevel level, char *buff,
                                   uint length, int buffLen)
  {
    HANDLE event;
    char   *buffptr;
    LPCSTR *buffmsgptr;
    DBUG_ENTER("print_buffer_to_nt_eventlog");

    buffptr= buff;
    if (length > (uint)(buffLen-4))
    {
      char *newBuff= new char[length + 4];
      strcpy(newBuff, buff);
      buffptr= newBuff;
    }
    strmov(buffptr+length, "\r\n\r\n");       /* think strcpy */
```

Literarisches Code-Quartett 2004

Stack-Buffer

```
mysql-4.1.8/libmysql/libmysql.c:660:

  my_bool     STDCALL mysql_change_user(MYSQL *mysql, const char *user,
                                    const char *passwd, const char *db)
  {
    char buff[512],*end=buff;
    int rc;
    DBUG_ENTER("mysql_change_user");

    if (!user)
      user="";
    if (!passwd)
      passwd="";

    /* Store user into the buffer */
    end=strmov(end,user)+1;
```

Literarisches Code-Quartett 2004

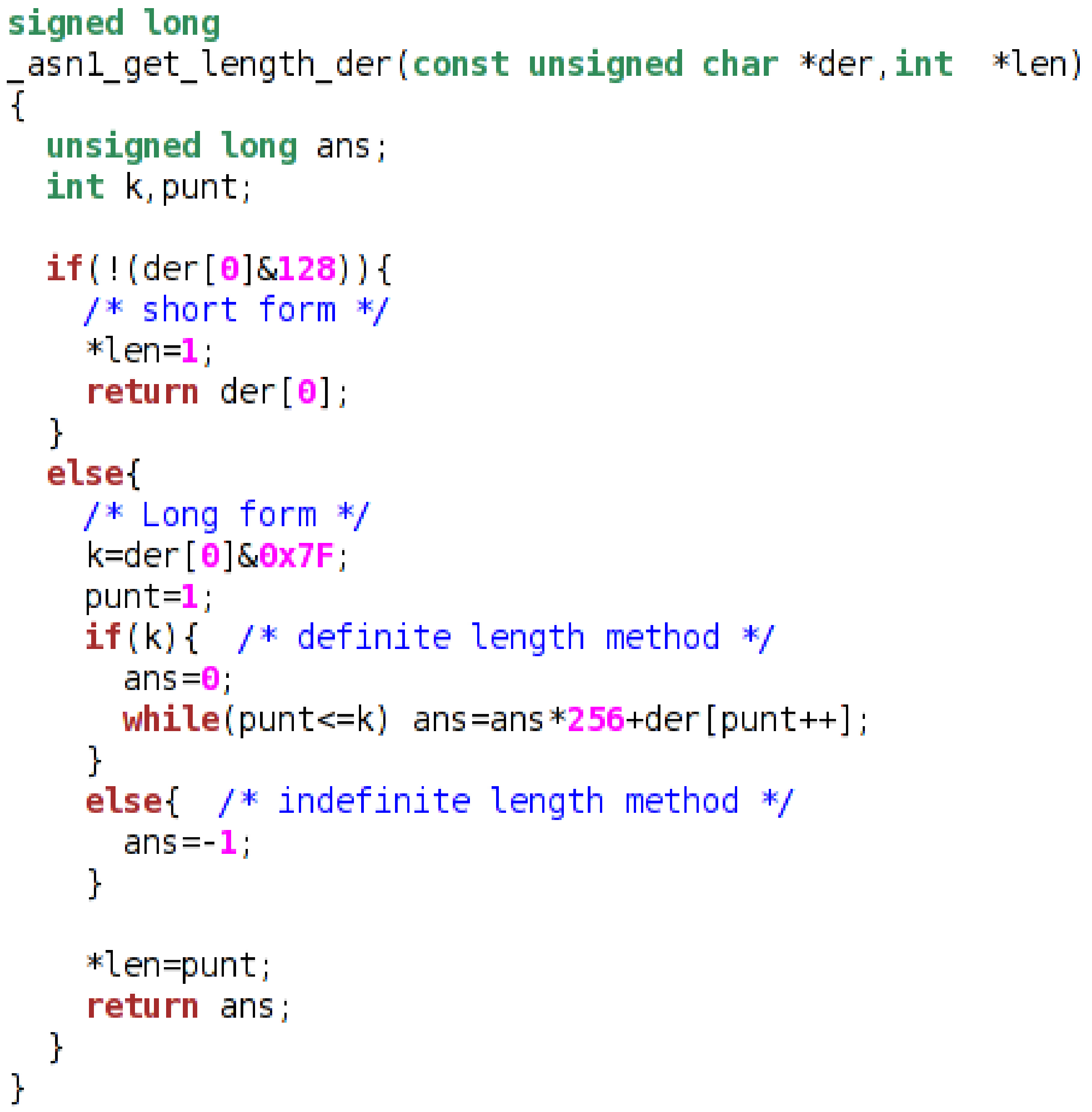
Stack-Buffer

mysql-**4.1.8**/sql-common/client.c:**1514**:

```
MYSQL * STDCALL
CLI_MYSQL_REAL_CONNECT(MYSQL *mysql,const char *host, const char *user,
                      const char *passwd, const char *db,
                      uint port, const char *unix_socket,ulong client_flag)
{
  char                buff[NAME_LEN+USERNAME_LENGTH+100];
  // [...]
  if (!net->vio &&
      (!mysql->options.protocol ||
      mysql->options.protocol == MYSQL_PROTOCOL_TCP))
  {
    unix_socket=0;                          /* This is not used */
    if (!port)
      port=mysql_port;
    if (!host)
      host=LOCAL_HOST;
    sprintf(host_info=buff,ER(CR_TCP_CONNECTION),host);
```

Literarisches Code-Quartett 2004

GNUTLS ASN.1



```
signed long
_asn1_get_length_der(const unsigned char *der,int  *len)
{
  unsigned long ans;
  int k,punt;

  if(!(der[0]&128)){
    /* short form */
    *len=1;
    return der[0];
  }
  else{
    /* Long form */
    k=der[0]&0x7F;
    punt=1;
    if(k){  /* definite length method */
      ans=0;
      while(punt<=k) ans=ans*256+der[punt++];
    }
    else{  /* indefinite length method */
      ans=-1;
    }

    *len=punt;
    return ans;
  }
}
```

Literarisches Code-Quartett 2004

GNUTLS ASN.1

gnutls-**1.1.22**/lib/minitasn1/decoding.c:**2071**:

```c
int
_asn1_get_octet_der(const unsigned char *der,int *der_len,
                    unsigned char *str,int str_size, int *str_len)
{
  int len_len;

  /* if(str==NULL) return ASN1_SUCCESS; */
  *str_len=_asn1_get_length_der(der,&len_len);

  *der_len=*str_len+len_len;
  if ( str_size >= *str_len)
          memcpy(str,der+len_len,*str_len);
  else {
        return ASN1_MEM_ERROR;
  }

  return ASN1_SUCCESS;
}
```

Literarisches Code-Quartett 2004

C String Handling

wget 1.9.1 shows us why C string handling sucks:

```
  /* Allocate the memory for the request.  */
  request = (char *)alloca (strlen (command)
                            + strlen (full_path)
                            + strlen (useragent)
                            + strlen (u->host)
                            + (port_maybe ? strlen (port_maybe) : 0)
                            + strlen (HTTP_ACCEPT)
                            + (request_keep_alive
                               ? strlen (request_keep_alive) : 0)
                            + (referer ? strlen (referer) : 0)
                            + (cookies ? strlen (cookies) : 0)
                            + (wwwauth ? strlen (wwwauth) : 0)
                            + (proxyauth ? strlen (proxyauth) : 0)
                            + (range ? strlen (range) : 0)
                            + strlen (pragma_h)
                            + (post_content_type
                               ? strlen (post_content_type) : 0)
                            + (post_content_length
                               ? strlen (post_content_length) : 0)
                            + (opt.user_header ? strlen (opt.user_header) : 0)
                            + 64);
```

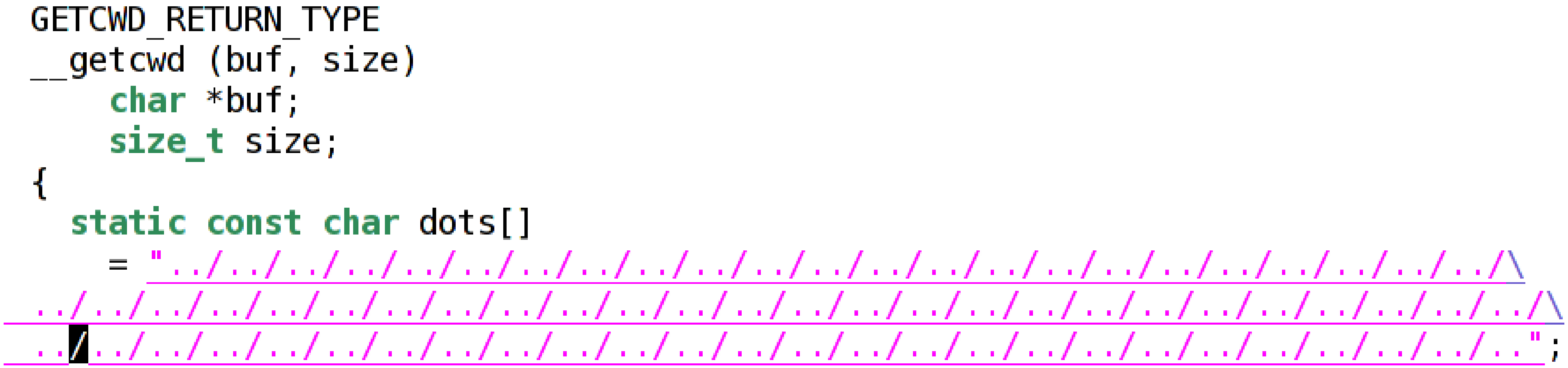
Literarisches Code-Quartett 2004

C String Handling

```c
  /* Construct the request.  */
  sprintf (request, "\
%s %s HTTP/1.0\r\n\
User-Agent: %s\r\n\
Host: %s%s%s%s\r\n\
Accept: %s\r\n\
%s%s%s%s%s%s%s%s%s%s\r\n",
           command, full_path,
           useragent,
           squares_around_host ? "[" : "", u->host, squares_around_host ? "]" : "",
           port_maybe ? port_maybe : "",
           HTTP_ACCEPT,
           request_keep_alive ? request_keep_alive : "",
           referer ? referer : "",
           cookies ? cookies : "",
           wwwauth ? wwwauth : "",
           proxyauth ? proxyauth : "",
           range ? range : "",
           pragma_h,
           post_content_type ? post_content_type : "",
           post_content_length ? post_content_length : "",
           opt.user_header ? opt.user_header : "");
```

Literarisches Code-Quartett 2004

Elegance and Grace



```
GETCWD_RETURN_TYPE
__getcwd (buf, size)
    char *buf;
    size_t size;
{
  static const char dots[]
    = "../../../../../../../../../../../../../../../../../../../../../../../\
../../../../../../../../../../../../../../../../../../../../../../../../../../\
../../../../../../../../../../../../../../../../../../../../../../../../../..";
```

Literarisches Code-Quartett 2004

Honorable Mentions

glibc ld.so gdb interface

glibc shared library mprotect