

# Cykor 2주차 과제 탐구 보고서

# 목차

가. 사용된 헤더파일 .....	3
나. cd 함수 .....	4
다. pwd 함수 .....	4
라. 파이프라인 .....	5~6
마. 공백 제거 함수 .....	6
바. 다중 연산자 .....	7~9
사. 백그라운드 .....	9
아. 문장 분리 함수 .....	10
자. 단일 명령어 실행 함수 .....	11~12
차. main .....	13
카. 보안 위협을 고려한 요소들 .....	14~15
타. 한계점 .....	15~16

## 가. 사용된 헤더파일(1~7)

작성 코드	<pre> 1  √ #include &lt;stdio.h&gt; 2    #include &lt;stdlib.h&gt; 3    #include &lt;string.h&gt; 4    #include &lt;unistd.h&gt; 5    #include &lt;sys/wait.h&gt; 6    #include &lt;signal.h&gt; 7    #include &lt;errno.h&gt; </pre>
설명	<p>1. #include &lt;stdio.h&gt; : 표준 입출력 함수들, 예: printf, scanf, fgets 등</p> <p>2. #include &lt;stdlib.h&gt; : 메모리 할당, 프로그램 종료, 문자열 변환 함수들 ex) malloc, free 등</p> <p>3. #include &lt;string.h&gt; : 문자열 처리 함수들, 예: strcpy, strlen, strcmp, strtok 등</p> <p>4. #include &lt;unistd.h&gt; : 유닉스/리눅스 시스템 호출 함수들, 예: fork, exec, chdir 등</p> <p>5. #include &lt;sys/wait.h&gt; : 자식 프로세스 관련 처리 함수들, 예: wait, waitpid 등</p> <p>6. #include &lt;signal.h&gt; : 시그널 처리 관련 함수 및 상수 백그라운드를 위해서 사용, 예: signal 등</p> <p>7. #include &lt;errno.h&gt; : 에러 번호를 정의한 헤더, 예: errno 전역 변수 같은 에러 코드</p>

## 나. cd 함수(19~27)

작성 코드	<pre> 19 int cd(char* path) { 20     path += 3; 21     path = remove_whitespace(path); 22     if (chdir(path) != 0) { 23         perror("cd 오류"); 24         return 1; 25     } 26     return 0; 27 }</pre>
설명	<p>20~21: path에 저장된 문자열에서 "cd " 부분을 뛰어넘기 위해서 +3을 해주고 오류가 생기지 않기 위해서 remove_whitespace를 이용해서 양끝의 공백을 제거하여 이동하기 위한 주소만 남겨둔다.</p> <p>22~26: chdir(path)를 통해 현재 작업 디렉토리를 path로 변경한다. chdir()이 성공하면 0, 실패하면 -1을 반환하기 때문에 실패했을 때 perror를 통해 오류를 출력하고 1을 반환하고, 성공하면 0을 반환한다.</p>

## 다. pwd 함수(29~38)

작성 코드	<pre> 29 int pwd() { 30     char cwd[100]; 31     if (getcwd(cwd, sizeof(cwd))) { 32         printf("%s\n", cwd); 33         return 0; 34     } else { 35         perror("pwd 오류"); 36         return 1; 37     } 38 }</pre>
설명	<p>31~37: getcwd()를 통해서 cwd에 현재 작업중인 디렉토리 주소를 불러온다. 저장에 성공하면 printf를 통해 주소를 출력하고, 실패하면 null을 반환하여 else문안에 있는 perror를 출력한다. 또한 각각 호출한곳에 성공유무를 알려주기 위해 성공하면 0, 실패하면 1을 반환한다.</p>

## 라. 파이프라인(41~93)

작성  
코드

```
41 void multi_pipe(char *command) {
42     char *cmds[10];
43     int num = 0;
44
45     char *token = strtok(command, "|");
46     while (token != NULL && num < 10) {
47         token = remove_whitespace(token);
48         if (strlen(token) > 0) {
49             cmds[num++] = token;
50         }
51         token = strtok(NULL, "|");
52     }
53
54     int prev_fd = -1;
55
56     for (int i = 0; i < num; i++) {
57         char *args[100];
58         split_args(cmds[i], args);
59
60         int pipe_fd[2];
61         if (i < num - 1 && pipe(pipe_fd) < 0) {
62             perror("pipe 실패");
63             exit(1);
64         }
65     }
```

```
66     pid_t pid = fork();
67     if (pid == 0) {
68         if (prev_fd != -1) {
69             dup2(prev_fd, 0);
70             close(prev_fd);
71         }
72         if (i < num - 1) {
73             close(pipe_fd[0]);
74             dup2(pipe_fd[1], 1);
75             close(pipe_fd[1]);
76         }
77
78         execvp(args[0], args);
79         perror("명령 실행 실패");
80         exit(1);
81     }
82     else {
83         if (prev_fd != -1) {
84             close(prev_fd);
85         }
86         if (i < num - 1) {
87             close(pipe_fd[1]);
88             prev_fd = pipe_fd[0];
89         }
90         waitpid(pid, NULL, 0);
91     }
92 }
93 }
```

<p><b>설명</b></p>	<p>45~52: " "을 기준으로 명령어들을 쪼개고 remove_whitespace를 이용해서 양쪽 공백을 제거한다. 그 다음 각각을 순서대로 cmd 배열에 저장한다.</p> <p>54: 이전 명령어의 읽기 파이프 끝을 저장하기 위한 변수.</p> <p>56: 파이프에 있는 명령어들을 실행하기 위한 반복문.</p> <p>57~58: cmds에서 명령어를 불러와 split_args()를 통해서 실행가능한 형태로 만든다.</p> <p>60~64: 마지막 명령어가 아니라면, 새로운 파이프를 생성하여 읽기/쓰기 파일 디스크립터 생성. 만약 실패 시 perror 출력 후 종료.</p> <p>66~81: 만약 자식 프로세스라면, 이전 명령어의 출력이 현재 명령어의 입력으로 들어오도록 dup2(prev_fd, 0), 다음 명령어가 존재한다면, 현재 명령어의 출력을 파이프로 보내기 위해 dup2(pipe_fd[1], 1)을 사용한다. 마지막으로 execvp()로 명령어를 실행하고, 실패 시 perror 출력 후 종료.</p> <p>82~91: 만약 부모 프로세스라면 자식프로세스가 끝날때까지 waitpid()기다린다. 종료후에는 필요한 읽기 파이프만 유지한다.</p>
------------------	---

## 마. 공백 제거 함수(95~107)

<p><b>작성 코드</b></p>	<pre> 95 char *remove_whitespace(char *str) { 96     while (*str == ' '    *str == '\t'    *str == '\n') { 97         str++; 98     } 99 100     char *end = str + strlen(str) - 1; 101 102     while (end &gt; str &amp;&amp; (*end == ' '    *end == '\t'    *end == '\n')) { 103         *end = '\0'; 104         end--; 105     } 106     return str; 107 } </pre>
<p><b>설명</b></p>	<p>96~98: while문을 통해 받은 명령어의 문자열 앞부분의 공백을 제거.</p> <p>100: 문자열의 마지막 주소를 변수에 저장.</p> <p>102~105: while문을 통해 받은 명령어의 문자열 뒷부분의 공백을 제거.</p>

## 바. 다중 연산자(109~164)

작성  
코드

```
109 void logical_command(char *logic) {
110     char *now = logic;
111     int last = 0;
112     int run_next = 1;
113
114     while (*now != '\0') {
115         char *next_and = strstr(now, "&&");
116         char *next_or = strstr(now, "||");
117         char *next_semi = strchr(now, ';');
118
119         char *next = NULL;
120         int type = 0;
121
122         if (next_and && (!next || next_and < next)) {
123             next = next_and;
124             type = 1;
125         }
126
127         if (next_or && (!next || next_or < next)) {
128             next = next_or;
129             type = 2;
130         }
131
132         if (next_semi && (!next || next_semi < next)) {
133             next = next_semi;
134             type = 3;
135         }
136
137         char *segment = now;
138         if (next != NULL) {
139             *next = '\0';
140         }
141
142         segment = remove_whitespace(segment);
143
144         if (run_next && strlen(segment) > 0) {
145             last = single_command(segment);
146         }
147
148         if (next != NULL) {
149             if (type == 1) {
150                 run_next = (last == 0);
151             }
152             else if (type == 2) {
153                 run_next = (last != 0);
154             }
155             else {
156                 run_next = 1;
157             }
158             now = next + (type == 3 ? 1 : 2);
159         }
160         else {
161             break;
162         }
163     }
164 }
```

## 설명

110: 현재 처리 중인 명령어의 위치를 저장하는 포인터 변수.

111: 명령어의 실행 결과를 저장하는 변수. 논리 연산자에 따라 다음 명령어의 실행 여부를 결정하는 데 사용한다.

112: run\_next는 다음 명령어를 실행할지 말지를 결정하는 변수. 초기값은 1로 설정되어 있고, 기본적으로 첫 번째 명령어는 실행된다.

114: now의 위치가 명령어의 끝까지 갈 때 동안 반복문을 실행한다.

115~117: strstr(curr, "&&"), strstr(curr, "||"), strchr(curr, ';')를 이용해 각각 &&, ||, ;가 현재 위치 이후에 있는지 찾는다. 그 후 찾은 위치를 next\_and, next\_or, next\_semi에 저장한다.

119: 가장 먼저 나오는 논리 연산자 위치를 변수에 저장한다.

120: 발견된 연산자의 종류를 &&는 1, ||는 2, ;는 3으로 type 변수를 설정한다.

122~135: next\_and가 존재하고 next가 아직 설정되지 않았거나, next\_and가 next보다 더 앞에 있으면 next를 next\_and로 설정하고, type을 1로 설정한다. next\_or와 next\_semi도 마찬가지로 작동한다.

137~140: 현재 명령어를 segment 변수에 저장한다. next가 존재하면, next 위치에 'w0'을 넣어 segment가 논리 연산자 앞까지의 명령어만 포함하게 만든다.

142: remove\_whitespace를 통해 명령어 앞뒤의 공백을 제거한다.

144~146: run\_next가 1일 경우, 즉 이전 명령어가 실행되어야 한다면 single\_command(segment)를 통해 명령어를 실행하고, 그 결과를 last에 저장한다.

148~161: next가 존재하면, 해당 논리 연산자에 맞춰 run\_next 값을 설정한다.

- type == 1 (&&): last == 0이면 다음 명령어를 실행하도록 run\_next를 1로 설정.

- type == 2 (||): last != 0이면 다음 명령어를 실행하도록 run\_next를 1로 설정.

- type == 3 (세미콜론): 항상 run\_next = 1로 설정하여 무조건 다음



	<p>명령어가 실행되도록 한다.</p> <p>now를 다음 명령어로 이동하고 type == 3일 경우 next + 1로 이동하여 ; 다음부터 시작하고, 그렇지 않으면 next + 2로 이동하여 논리 연산자 다음부터 시작한다. 만약 next가 NULL이면 반복문을 종료시킨다.</p>
--	---

## 사. 백그라운드(166~177)

작성 코드	<pre> 166  void background(void) { 167      int saved_errno = errno; 168      pid_t pid; 169      int status; 170 171      while ((pid = waitpid(-1, &amp;status, WNOHANG)) &gt; 0) { 172          printf("[백그라운드 종료] pid: %d\n", pid); 173          fflush(stdout); 174      } 175 176      errno = saved_errno; 177  }</pre>
설명	<p>167: errno 값을 백업해둔다. waitpid 실행 중 오류가 발생해도 기존의 오류 상태를 보존하기 위해서이다.</p> <p>168: 자식 프로세스의 pid를 저장할 변수 pid 선언.</p> <p>169: 자식 프로세스 종료 상태를 저장할 변수 status 선언.</p> <p>171~174: waitpid(-1, &amp;status, WNOHANG)을 사용하여 좀비 프로세스를 회수한다. WNOHANG은 종료된 자식이 없으면 기다리지 않고 바로 반환하게 한다. 자식 프로세스가 종료되었다면 해당 pid를 출력한다. 출력 후 fflush(stdout)으로 출력 버퍼를 비워 즉시 출력되도록 한다.</p> <p>176: 함수 시작 시 백업해둔 errno 값을 복원하여, 이 함수에서의 waitpid 호출이 외부 오류 상태에 영향을 주지 않도록 한다.</p>

## 아. 문장 분리 함수(179~188)

작성 코드	<pre> 179 void split_args(char *input, char **args) { 180     int i = 0; 181     char *token = strtok(input, " "); 182 183     while (token != NULL &amp;&amp; i &lt; 99) { 184         args[i++] = remove_whitespace(token); 185         token = strtok(NULL, " "); 186     } 187     args[i] = NULL; 188 }</pre>
설명	<p>180~181: 입력 문자열을 strtok 함수를 사용하여 공백 기준으로 나누어 첫 번째 토큰을 추출한다.</p> <p>183~186: token이 NULL이 아니고 개수가 99 미만일 때까지 반복하여 토큰을 하나씩 remove_whitespace를 사용하여 각 토큰의 앞뒤 공백을 제거한 후 저장하고, 이후 strtok으로 다음 토큰을 얻는다.</p> <p>187: 마지막에 args[i]를 NULL로 설정하여 명령어 함수들이 이 배열의 끝을 인식할 수 있도록 한다.</p>

## 자. 단일 명령어 실행 함수(190~235)

<p>작성 코드</p>	<pre> 190 int single_command(char *command) { 191     command = remove_whitespace(command); 192 193     int background = 0; 194     size_t len = strlen(command); 195     if (len &gt; 0 &amp;&amp; command[len - 1] == '&amp;') { 196         background = 1; 197         command[len - 1] = '\0'; 198         command = remove_whitespace(command); 199     } 200 201     if (strcmp(command, "exit") == 0) { 202         exit(0); 203     } 204     if (strncmp(command, "cd ", 3) == 0) { 205         return cd(command); 206     } 207     if (strcmp(command, "pwd") == 0) { 208         return pwd(); 209     } 210     if (strchr(command, ' ')) { 211         multi_pipe(command); 212         return 0; 213     } 214 215     char *args[100]; 216     split_args(command, args); 217 218     pid_t pid = fork(); 219     if (pid == 0) { 220         execvp(args[0], args); 221         perror("실행 실패"); 222         exit(1); 223     } 224     else { 225         if (!background) { 226             int status; 227             waitpid(pid, &amp;status, 0); 228             return WEXITSTATUS(status); 229         } 230         else { 231             printf("[백그라운드 실행] pid: %d\n", pid); 232             return 0; 233         } 234     } 235 } </pre>
<p>설명</p>	<p>191: 받은 문자열의 앞뒤 공백을 제거하여 명령어를 만든다.</p> <p>193~199: 명령어 끝이 &amp;이면 백그라운드 실행임을 의미한다. 그러므로 background를 1로 설정하고, &amp;를 제거한 후 다시 공백을 제거해 명령어를 정리한다.</p> <p>201~203: strcmp를 이용해 명령어의 가장 앞단어가 "exit"이라면 프로그램을 종료시킨다.</p>

	<p>204~206: strcmp를 이용해 명령어의 가장 앞부분 3개가 "cd"라면 cd 함수를 호출한다. cd 함수가 성공하면 0을 반환하고 실패하면 1을 반환한다.</p> <p>207~209: strcmp를 이용해 명령어의 가장 앞단어가 "pwd"라면 pwd 함수를 호출한다. pwd 함수가 성공하면 0을 반환하고 실패하면 1을 반환한다.</p> <p>210~213: strchr를 이용해 명령어에   문자가 포함되어 있는지 판단하고, 포함되어 있다면 multi_pipe() 함수를 호출한다.</p> <p>215~216: 명령어를 split_args를 통해 실행할 수 있는 형태로 쪼갬다.</p> <p>218: 자식 프로세스를 생성한다.</p> <p>219~223: 만약 자식 프로세스라면 execvp()를 이용해서 cd,pwd를 제외한 나머지 명령어를 실행한다.</p> <p>224~234: 만약 부모 프로세스라면 백그라운드 실행중이 아니라면 waitpid로 자식 프로세스의 종료를 기다리고 종료 상태를 반환한다. 백그라운드가 실행중이면 메시지만 출력하고 기다리지 않는다.</p>
--	---

## 차. main(237~258)

<p><b>작성 코드</b></p>	<pre> 237 int main() { 238     signal(SIGCHLD, background); 239 240     char command[100]; 241 242     while (1) { 243         char cwd[100]; 244         getcwd(cwd, sizeof(cwd)); 245         printf("%s\$ ", cwd); 246         fflush(stdout); 247 248         if (!fgets(command, sizeof(command), stdin)) { 249             break; 250         } 251 252         command[strcspn(command, "\n")] = 0; 253 254         logical_command(command); 255     } 256 257     return 0; 258 }</pre>
<p><b>설명</b></p>	<p>238: 자식 프로세스가 종료될 때, SIGCHLD 시그널 발생하면 background 함수를 호출한다.</p> <p>244~246: getcwd()를 통해 현재 디렉토리의 경로를 문자열로 cwd에 저장하고 출력한다. 현재 디렉토리 경로를 출력하고 \$를 붙여 입력을 유도한다. fflush(stdout)를 이용해 출력 버퍼를 비워 즉시 화면에 출력되도록 보장한다.</p> <p>248~250: 사용자로부터 한 줄 입력을 받아 command에 저장한다. fgets()가 NULL을 반환하면 입력 오류이므로 루프를 종료한다.</p> <p>252: 입력된 명령어의 끝에 있는 '\n'를 '\0'로 바꿔 문자열을 끝을 프로그램이 인식할 수 있도록 지정한다.</p> <p>254: command를 logical_command 함수로 전달하여 명령어들을 실행시킨다.</p>

## **카. 보안 위협을 고려한 요소들**

### **1. 좀비 프로세스 제거**

#### **가) 좀비 프로세스란?**

: 실행은 끝났지만, 부모가 수거하지 않아 시스템에 남아 있는 자식 프로세스의 껍데기.

#### **나) 좀비 프로세스의 문제점**

: 좀비가 쌓이면 PID를 점점 잡아먹고, 스택 오버플로우와 같이 시스템에서 더 이상 프로세스를 만들 수 없는 상황도 생긴다. 또한, 좀비 프로세스를 일부러 쌓아서 시스템을 느려지게 만드는 간단한 DoS 공격 수단이 되기도 한다.

#### **다) 적용한 해결 방법**

: `signal(SIGCHLD, handler)`를 사용해, 자식 종료 시 자동으로 `waitpid(-1, ..., WNOHANG)`를 통해 좀비 프로세스 수거.

### **2. 파일 디스크립터(FD) 및 리소스 누수**

#### **가) 파일 디스크립터란?**

: 열어놓은 파일 디스크립터를 제대로 닫지 않아서, 사용하지도 않으면서 시스템 자원을 점점 차지하는 현상.

#### **나) 파일 디스크립터(FD)의 문제점**

: `pipe()`나 `dup2()`로 생성된 FD를 닫지 않으면 리눅스의 FD 제한을 초과해, 입출력 오류나 프로세스 고장 발생 가능성이 있다.

#### **다) 적용한 해결 방법**

: 파이프 사용 후 불필요한 FD는 항상 `close()`로 정리, `dup2()` 이후에도 원본 FD를 닫아 리소스 누수를 방지하였다.

### **3. 개행 파싱 오류**

#### **가) 파싱의 중요성**

: 파싱을 통해 명령어 조작 공격을 예방하고 입력 오류로 인한 오동작을 차단, 내부/외부 명령의 안전한 구분 실행 가능하다.

## 나) 적용한 해결 방법

: remove\_whitespace()와 split\_args() 함수를 만들어 모든 명령어와 인자에서 정확하게 분리하고 앞뒤 공백 제거함으로써 파싱 안정성과 명령 실행의 정확도 향상.

## 타. 한계점

### 1. 백그라운드의 출력

```
/home/minjun_9/myshell$ sleep 3 &  
[백그라운드 실행] pid: 2334  
/home/minjun_9/myshell$ [백그라운드 종료] pid: 2334
```

<백그라운드의 출력 문제 사진>

: 기존 bash 셸에서는 백그라운드가 다음 명령어를 실행할 때 함께 출력되어야 하는데 그것까지는 구현하지 못함. 구현하려고 노력하였으나 코드가 꼬여 프로그램 자체가 작동하지 않는 문제점 발생. 끝내 포기함

### 2. 백그라운드 이후 동작이 이루어지지 않음

```
minjun_9@BOOK-4ULMSOMPT6:~/myshell/Cykor_Assignment_week2$ sleep 3 & pwd  
[1] 3364  
/home/minjun_9/myshell/Cykor_Assignment_week2  
minjun_9@BOOK-4ULMSOMPT6:~/myshell/Cykor_Assignment_week2$ make run  
./myshell  
/home/minjun_9/myshell/Cykor_Assignment_week2$ sleep 3 & pwd  
sleep: invalid time interval '&'  
sleep: invalid time interval 'pwd'  
Try 'sleep --help' for more information.  
/home/minjun_9/myshell/Cykor_Assignment_week2$ sleep 3 && pwd  
[백그라운드 실행] pid: 3554  
/home/minjun_9/myshell/Cykor_Assignment_week2  
/home/minjun_9/myshell/Cykor_Assignment_week2$ [백그라운드 종료] pid: 3554
```

< 백그라운드 이후 동작이 이루어지지 않는 사진>

: 사진과 같이 기존 bash 셸에서는 백그라운드가 이후 뒤에 명령어가 작동해야 하지만 명령어가 바로 작동하지 않고 오류가 나는 것을 확인할 수 있다. 하지만 뒤에 다중 연산자가 오면 잘 작동한다. 다중 연산자 &&과 충돌이 일어나 안되는 줄 알고 연산자들의 우선순위를 주거나 다른 방법들을 시도 해봤지만 위와 같이 오류가 나거나 &&과 &을 구별하지 못하여 &을 &&으로 작동하는 오류가 계속 반복돼서 포기함.

### 3. 파이프 함수내에 단일 명령어 호출

: 파이프를 이용해서 명령어들을 쪼갠 다음 명령어들을 원래는 단일 명령어 함수를 호출하여 처리해야 하는데, 단일 명령어 안에 파이프를 확인하는 구문이 있어서 오류가 발생한다. 따로 분리해서 만들어보고 다른 방법을 시도 해봤지만 `execvp()` 사용이 가장 효율적이어서 어쩔 수 없이 파이프를 사용할 때는 `cd`와 `pwd`가 직접 만든 함수에서 작동하지 않고 `execvp()`를 통해서 작동한다.