UPX 사용법

DCLab 이진성

Digital Convergence Lab

A Table of Contents.

Part 1,

기본 사용법

기본 사용법

Digital Convergence Lab

UPX 다운받은 경로로 이동

```
C:₩Windows₩system32>cd C:₩Users₩Jin₩Desktop₩국과수 PJ₩upx-3.96-win64
```

upx를 입력하여 압축 해제

```
C:₩Users₩Jin₩Desktop₩국과수 PJ₩upx-3.96-win64>upx
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser    Jan 23rd 2020

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                   -9    compress better
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give more help                    -L    display software license
Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  -k     keep backup files
file..   executables to (de)compress

Type 'upx --help' for more detailed help.

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io
```

Upx 사용을 위한 환경 변수 지정

```
C:₩Users₩Jin₩Desktop>setx path "%PATH%;C:₩Users₩Jin₩Desktop₩국과수 PJ₩upx-3.96-win64"
```

기본 사용법

Digital Convergence Lab

upx filename.exe

```
C:₩>upx devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    996816 ->    478160   47.97%    win64/pe     devenv.exe

Packed 1 file.
```

upx filename.exe –o filename_upx.exe

```
C:₩>upx devenv.exe -o devenv_upx.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    996792 ->    477624   47.92%    win64/pe     devenv_upx.exe

Packed 1 file.
```

devenv_upx	2022-04-21 오전 9:44	응용 프로그램	467KB
devenv	2022-04-21 오전 9:44	응용 프로그램	974KB

기본 사용법

- testcode.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER .textbss
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - IMAGE_SECTION_HEADER .idata
  - IMAGE_SECTION_HEADER .msvcjmc
  - IMAGE_SECTION_HEADER .00cfg
  - IMAGE_SECTION_HEADER .rsrc
  - IMAGE_SECTION_HEADER .reloc
  - SECTION .text
  - SECTION .rdata
  - SECTION .data
  - SECTION .idata
  - SECTION .msvcjmc
  - SECTION .00cfg
  - SECTION .rsrc
  - SECTION .reloc

→

- testcode_upx.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER UPX0
  - IMAGE_SECTION_HEADER UPX1
  - IMAGE_SECTION_HEADER .rsrc
  - SECTION UPX0
  - SECTION UPX1
  - SECTION .rsrc

IMAGE_FILE_HEADER

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0009	Number of Sections	
000000F0	6264EE92	Time Date Stamp	2022/04/24 06:30:42 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	0102	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0100	IMAGE_FILE_32BIT_MACHINE

↓

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	6264EE92	Time Date Stamp	2022/04/24 06:30:42 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	0102	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0100	IMAGE_FILE_32BIT_MACHINE

IMAGE_OPTIONAL_HEADER

00000104	00005600	Size of Code
00000108	00004600	Size of Initialized Data
0000010C	00000000	Size of Uninitialized Data
00000110	00011023	Address of Entry Point
00000114	00001000	Base of Code
00000118	00001000	Base of Data
0000011C	00400000	Image Base
00000120	00001000	Section Alignment
00000124	00000200	File Alignment
00000128	0006	Major O/S Version
0000012A	0000	Minor O/S Version
0000012C	0000	Major Image Version
0000012E	0000	Minor Image Version
00000130	0006	Major Subsystem Version
00000132	0000	Minor Subsystem Version
00000134	00000000	Win32 Version Value
00000138	00020000	Size of Image
0000013C	00000400	Size of Headers

→

00000104	00003000	Size of Code
00000108	00001000	Size of Initialized Data
0000010C	0001E000	Size of Uninitialized Data
00000110	000215C0	Address of Entry Point
00000114	0001F000	Base of Code
00000118	00022000	Base of Data
0000011C	00400000	Image Base
00000120	00001000	Section Alignment
00000124	00000200	File Alignment
00000128	0006	Major O/S Version
0000012A	0000	Minor O/S Version
0000012C	0000	Major Image Version
0000012E	0000	Minor Image Version
00000130	0006	Major Subsystem Version
00000132	0000	Minor Subsystem Version
00000134	00000000	Win32 Version Value
00000138	00023000	Size of Image
0000013C	00001000	Size of Headers

IMAGE_SECTION_HEADER .text

00000208	2E 74 65 78	Name	.text
0000020C	74 00 00 00		
00000210	000055BF	Virtual Size	
00000214	00011000	RVA	
00000218	00005600	Size of Raw Data	
0000021C	00000400	Pointer to Raw Data	
00000220	00000000	Pointer to Relocations	
00000224	00000000	Pointer to Line Numbers	
00000228	0000	Number of Relocations	
0000022A	0000	Number of Line Numbers	
0000022C	60000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ

→

IMAGE_SECTION_HEADER UPX0

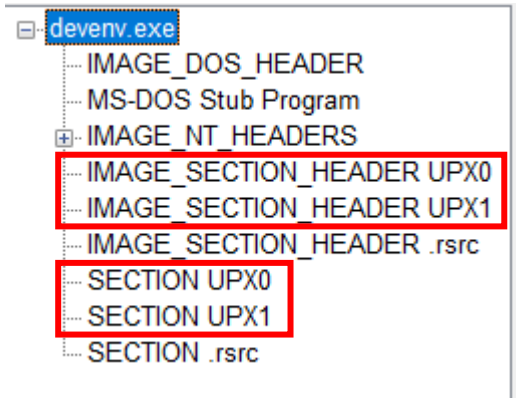
000001E0	55 50 58 30	Name	UPX0
000001E4	00 00 00 00		
000001E8	0001E000	Virtual Size	
000001EC	00001000	RVA	
000001F0	00000000	Size of Raw Data	
000001F4	00000400	Pointer to Raw Data	
000001F8	00000000	Pointer to Relocations	
000001FC	00000000	Pointer to Line Numbers	
00000200	0000	Number of Relocations	
00000202	0000	Number of Line Numbers	
00000204	E0000080	Characteristics	
		00000080	IMAGE_SCN_CNT_UNINITIALIZED_DATA
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ
		80000000	IMAGE_SCN_MEM_WRITE

기본 사용법

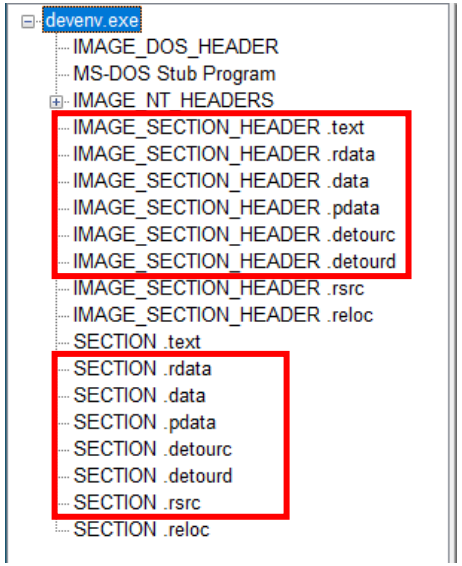
upx –d filename.exe

```
C:₩>upx -d devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser    Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     996816 <-    478160   47.97%    win64/pe     devenv.exe

Unpacked 1 file.
```

언 패킹 전

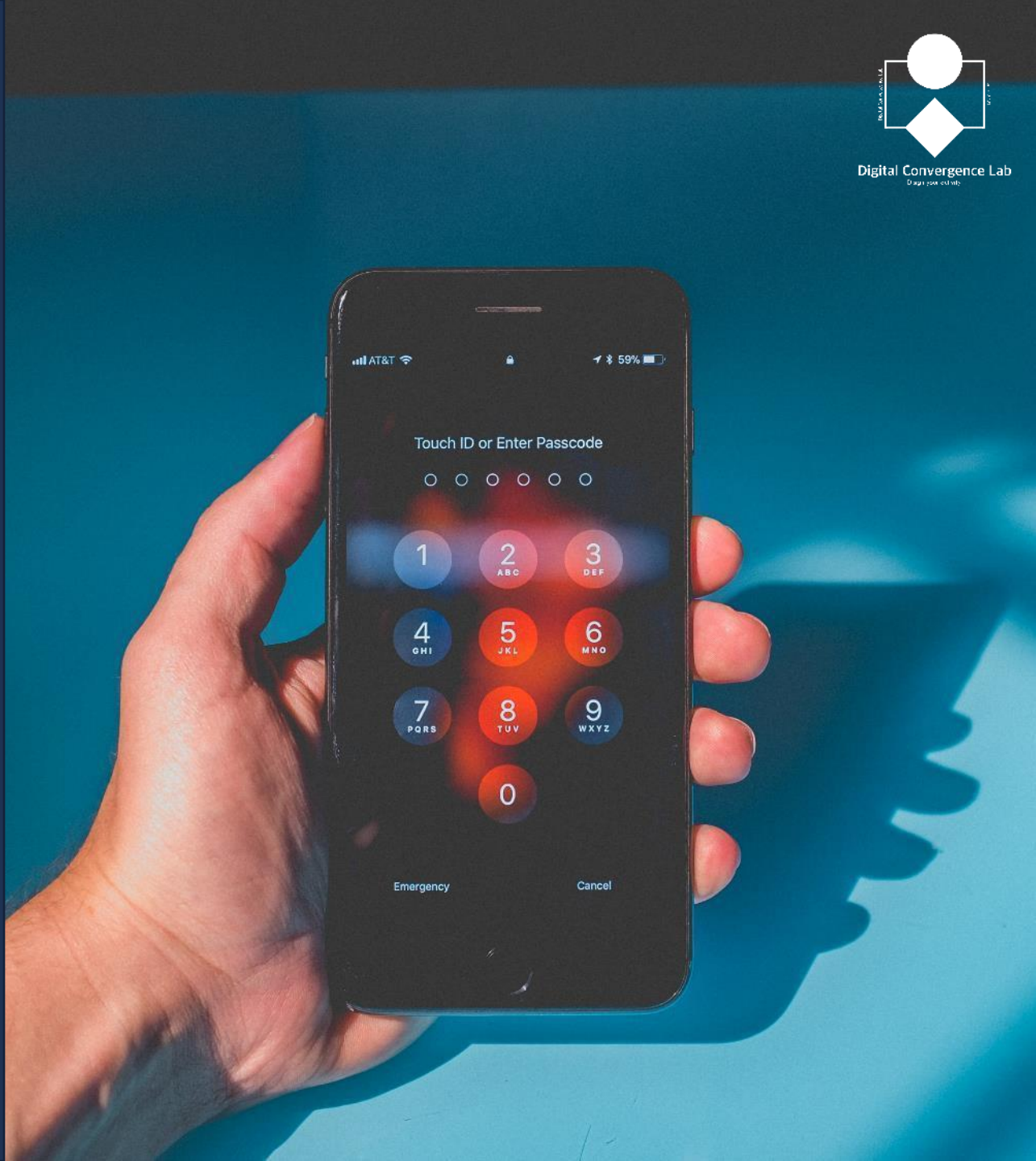


언 패킹 후



Part 2,

UPX Command



Digital Convergence Lab

UPX Command

기본 형식 ➡ upx [commend] [option] filename

Commend	Description
-1~9	1~9중 한가지를 선택하여 패킹의 수준을 선택 (숫자가 클수록 시간이 오래 걸리고 패킹 된 크기는 작아짐)
--best	최종본을 릴리즈 할 때 반드시 사용하여 패킹
-d	패킹 된 것을 언 패킹
-l	패킹 된 파일의 일부 정보를 출력
-t	패킹 된 파일의 무결성 검사
-h	도움말
-V	UPX 버전 확인
-L	UPX 라이선스 확인

Part 3,

UPX Option

UPX Option

Digital Convergence Lab

기본 옵션 (options)

Option	Description
-q	경고 무시
-q -q (-qq)	오류 무시
-q -q –q (-qqq)	출력 생성 안함
-oFILE	결과를 FLIE이름으로 생성
-f	파일 강제 압축
--no-color --mono --color --no-progress	레이아웃 설정

UPX Option

패킹 조정 옵션 (Compression tuning options)

--brute

- 사용이 가능한 모든 패킹 방법 및 필터 시도

```
C:₩>upx --brute devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
Compressing devenv.exe [win64/pe]
2/8  [*************************************************.........]   29.9%  -
```

```
C:₩>upx --brute devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    996816 ->    448464   44.99%    win64/pe     devenv.exe
Packed 1 file.
```

--ultra-brute

- --brute 보다 더 많은 패킹 변형 시도

```
C:₩>upx --ultra-brute devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
Compressing devenv.exe [win64/pe]
1/12  [*****************************************************..]   27.3%  |
```

```
C:₩>upx --ultra-brute devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    996816 ->    448464   44.99%    win64/pe     devenv.exe
Packed 1 file.
```

UPX Option

백업 옵션 (Backup options)

-k, --backup -> 백업파일 생성

```
C:₩>upx -k devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    996816 ->    478160   47.97%    win64/pe     devenv.exe

Packed 1 file.
```

devenv.ex~	2022-04-04 오전 10:55	EX~ 파일	974KB

```
C:₩>upx --backup devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    996816 ->    478160   47.97%    win64/pe     devenv.exe

Packed 1 file.
```

devenv.000	2022-04-04 오전 10:55	000 파일	974KB

--no-backup -> 백업파일 생성 안함

```
C:₩>upx --no-backup devenv.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    996816 ->    478160   47.97%    win64/pe     devenv.exe

Packed 1 file.
```

UPX Option

Digital Convergence Lab

오버레이 옵션 (Overlay options)

--overlay=copy
- 파일에 첨부된 추가 데이터 복사

--overlay=strip
- 파일에 첨부된 모든 추가 데이터 제거

--overlay=skip
- 오버레이로 파일을 압축하지 않음

win32/pe, win64/pe, rtm32/pe & arm/pe 옵션

--compress-exports=0 -> export section을 압축하지 않음

--compress-exports=1 -> export section압축 [기본값]

--compress-icons=0 -> 아이콘을 압축하지 않음

--compress-icons=1 -> 첫 번째 아이콘을 제외한 모든 것을 압축

--compress-icons=2 -> 첫번째 아이콘 디렉토리를 제외한 모든 디렉토리 압축 [기본값]

--compress-icons=3 -> 모든 아이콘 압축

--compress-resources=0 -> 리소스를 전혀 압축하지 않음

--keep-resource=list -> 목록에 지정된 리소스를 압축하지 않습니다.

--strip-relocs=0 -> 스트립을 제거하지 않음

--strip-relocs=1 -> 스트립 재배치 [기본값]

Digital Convergence Lab

“ https://upx.github.io/ ”

Q&A

Digital Convergence Lab