리버스 엔지니어링 기드라 실전 가이드_URL 모음

위치	페이지	각주 번호	URL
앞부속	4		https://github.com/tkmru
			https://tkmru.dev/
	5		https://www.linkedin.com/in/crattack/
			https://www.linkedin.com/in/jeayong-lim-91b639203/
	11		https://www.hanbit.co.kr/src/10507
	16	1	https://www.vmware.com/jp/products/workstation-player.html
		2	https://www.virtualbox.org/
		3	https://github.com/fireeye/flare-vm
1장	38	1	https://software.intel.com/content/www/us/en/develop/articles/intel-sdm.html#combined
	57		https://github.com/corkami/pics/blob/master/binary/pe101/pe101.pdf
			http://www.openrce.org/reference_library/files/reference/PE%20Format.pdf
		3	https://uclibc.org/docs/psABI-x86_64.pdf
2장	66	1	https://www.hex-rays.com/products/ida/
		2	https://github.com/radareorg/radare2
		3	https://www.rsaconference.com/industry-topics/presentation/come-get-your-free-nsa-reverse-engineering-tool
		4	https://ghidra-sre.org/
		5	https://github.com/NationalSecurityAgency/ghidra
		6	https://www.blackhat.com/us-19/briefings/schedule/#ghidra---journey-from-classified-nsa-tool-to-open-source-16309
	67	※1	https://wikileaks.org/ciav7p1/
	69		https://adoptopenjdk.net/releases.html?variant=openjdk11&jvmVariant=hotspot
			https://docs.aws.amazon.com/corretto/latest/corretto-11-ug/downloads-list.html
	120	※1	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13625
		※3	https://www.mbsd.jp/blog/20171130.html
		※4	https://github.com/NationalSecurityAgency/ghidra/issues/71
3장	130	2	https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123(v=vs.85)
	134	3	https://docs.microsoft.com/en-us/windows/win32/api/shlwapi/nf-shlwapi-pathfileexistsa
	153	4	https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessw
4장	166		https://github.com/AllsafeCyberSecurity/ghidra_scripts
	170	5	https://docs.oracle.com/javase/jp/8/docs/technotes/tools/windows/javadoc.html
	172		https://www.eclipse.org/downloads/packages/installer
	184		https://jython.readthedocs.io/en/latest/
	245	※1	https://docs.microsoft.com/ja-jp/archive/msdn-magazine/2017/december/c-visual-c-support-for-stack-
5장	248		https://crackmes.one/
			https://overthewire.org/wargames/

			https://pwnable.kr/
			https://pwnable.xyz/
			https://challenges.re/
			http://reversing.kr/
			https://www.root-me.org/en/Challenges/Cracking/
			https://0x00sec.org/c/reverse-engineering/challenges
		1	http://ctf.codeblue.jp/
		2	https://www.seccon.jp/
		3	https://ctf.westerns.tokyo/ja/
		4	https://www.defcon.org/html/links/dc-ctf.html
		5	https://hitcon.org/
		6	http://codegate.org/en/hacking/general
	251	7	https://www.tutorialspoint.com/c_standard_library/c_function_fgets.htm
	254	9	https://gchq.github.io/CyberChef/
	257	※1	https://nvd.nist.gov/vuln/detail/CVE-2019-13623
		※2	https://github.com/NationalSecurityAgency/ghidra/issues/789
	258	10	https://www.tutorialspoint.com/c_standard_library/c_function_strncmp.htm
	273	※1	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16941
		※2	https://github.com/NationalSecurityAgency/ghidra/issues/1090
	283	11	https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/
		12	https://blog.malwarebytes.com/threat-analysis/2019/01/analyzing-new-stealer-written-golang/
		13	https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
		14	https://www.lac.co.jp/lacwatch/pdf/20180614_cecreport_vol3.pdf
		15	https://github.com/jgamblin/Mirai-Source-Code
	285	16	https://github.com/spyoungtech/grequests
	288	17	https://github.com/felberj/gotools
		18	https://github.com/felberj/gotools/releases
	295		https://play.golang.org/
6장	301		https://github.com/AllsafeCyberSecurity/Ghidra_Data_Type
	303		https://github.com/AllsafeCyberSecurity/Ghidra_FIDB
	306	2	https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-messageboxw
	308	3	https://docs.microsoft.com/en-us/windows/win32/api/synchapi/nf-synchapi-createmutexw
		4	https://docs.microsoft.com/en-us/windows/win32/debug/system-error-codes
	310	5	https://docs.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regopenkeyexw
	311	6	https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-key-security-and-access-rights
	312		https://github.com/a0rtega/pafish
			https://github.com/LordNoteworthy/al-khaser
			https://github.com/hfiref0x/VMDE
			https://evasions.checkpoint.com/
	314	7	https://docs.microsoft.com/ko-kr/cpp/c-runtime-library/reference/memcpy-wmemcpy?view=msvc-160

	316	8	https://docs.microsoft.com/ko-kr/windows/win32/api/heapapi/nf-heapapi-heapalloc
	333	9	https://docs.microsoft.com/en-us/windows/win32/api/winhttp/nf-winhttp-winhttpconnect
	334	10	https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-getcomputernamea
		11	https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-getusernamea
	335		https://github.com/AllsafeCyberSecurity/py-findcrypt-ghidra
		12	https://github.com/Yara-Rules/rules/blob/master/crypto/crypto_signatures.yar
	341	13	https://docs.microsoft.com/en-us/windows/win32/api/winhttp/nf-winhttp-winhttpopenrequest
	344	14	https://docs.microsoft.com/en-us/windows/win32/api/winhttp/nf-winhttp-winhttpaddrequestheaders
		15	https://docs.microsoft.com/en-us/windows/win32/api/winhttp/nf-winhttp-winhttpsendrequest
	362	16	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getdrivetypew
	363	17	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getdiskfreespaceexw
	368	18	https://docs.microsoft.com/en-us/windows/win32/api/winsock/nf-winsock-gethostname
		19	https://docs.microsoft.com/en-us/windows/win32/api/ws2tcpip/nf-ws2tcpip-getaddrinfo
		20	https://docs.microsoft.com/en-us/windows/win32/api/ws2def/ns-ws2def-addrinfoa
	369	21	https://docs.microsoft.com/en-us/windows/win32/api/winsock2/nf-winsock2-wsaaddresstostringw
	370	22	https://docs.microsoft.com/en-us/windows/win32/api/heapapi/nf-heapapi-heaprealloc
	374	23	https://docs.microsoft.com/en-us/windows/win32/winmsg/windows
	376	24	https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-getwindowthreadprocessid
		25	https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-getwindowtextw
	380	26	https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-postmessagew
	383	27	https://docs.microsoft.com/en-us/windows/win32/api/tlhelp32/nf-tlhelp32-createtoolhelp32snapshot
	384	28	https://docs.microsoft.com/en-us/windows/win32/api/tlhelp32/nf-tlhelp32-process32firstw
		29	https://docs.microsoft.com/en-us/windows/win32/api/tlhelp32/ns-tlhelp32-processentry32
	385	30	https://docs.microsoft.com/en-us/windows/win32/api/psapi/nf-psapi-enumprocessmodules
		31	https://docs.microsoft.com/en-us/windows/win32/api/psapi/nf-psapi-getmodulefilenameexw
	386	32	https://docs.microsoft.com/en-us/windows/win32/api/psapi/nf-psapi-getmoduleinformation
		33	https://docs.microsoft.com/en-us/windows/win32/api/psapi/ns-psapi-moduleinfo
	391	34	https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-lookupprivilegevaluew
	392	35	https://docs.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-adjusttokenprivileges
		36	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-token_privileges
	395	37	https://docs.microsoft.com/en-us/windows/win32/api/shellapi/nf-shellapi-shellexecuteexw
		38	https://docs.microsoft.com/en-us/windows/win32/api/shellapi/ns-shellapi-shellexecuteinfow
	401	39	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-findfirstfilew
		40	https://docs.microsoft.com/en-us/windows/win32/api/minwinbase/ns-minwinbase-win32_find_dataw
	405	41	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-deletefilea
	406	42	https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-movefilew
	408	43	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-createfilew
	409	44	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-writefile
	412	45	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getfilesize
	413	46	https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-readfile
	419	47	https://docs.microsoft.com/en-us/windows/win32/api/namedpipeapi/nf-namedpipeapi-createpipe

		48	https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-createprocessw
	420	49	https://docs.microsoft.com/en-us/windows/win32/api/sysinfoapi/nf-sysinfoapi-getsystemdirectoryw
		50	https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/ns-processthreadsapi-startupinfow
	421	51	https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/ns-processthreadsapi-process_information
	424	52	https://docs.microsoft.com/en-us/windows/win32/api/namedpipeapi/nf-namedpipeapi-peeknamedpipe
7장	437	※1	https://vmpsoft.com/
	439	3	https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-globalalloc
	443	4	https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-localalloc
		5	https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtualalloc
	449	6	https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtualprotect
		7	https://docs.microsoft.com/en-us/windows/win32/memory/memory-protection-constants
	452	8	https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-enumwindows
	460	10	https://docs.microsoft.com/en-us/windows/win32/api/libloaderapi/nf-libloaderapi-loadlibrarya
	461	11	https://docs.microsoft.com/en-us/windows/win32/api/libloaderapi/nf-libloaderapi-getprocaddress
	463	12	https://docs.microsoft.com/en-us/windows/win32/api/errhandlingapi/nf-errhandlingapi-getlasterror
		13	https://docs.microsoft.com/ja-jp/windows/win32/api/sysinfoapi/nf-sysinfoapi-gettickcount
		14	https://docs.microsoft.com/en-us/windows/win32/api/synchapi/nf-synchapi-sleep
	474	15	https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-teb
	475	16	https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb
	476	17	https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb_ldr_data
		18	https://www.winehq.org
		19	https://github.com/wine-mirror/wine/blob/master/include/winternl.h
	477	20	https://docs.microsoft.com/en-us/windows/win32/api/ntdef/ns-ntdef-list_entry
	482	21	https://docs.microsoft.com/ja-jp/windows/win32/api/subauth/ns-subauth-unicode_string
	484	22	https://github.com/wine-mirror/wine/blob/master/include/winnt.h
	485	23	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_nt_headers32
	486	24	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_optional_header32
	487	25	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_data_directory
	514	26	https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtualalloc
	546	27	https://docs.microsoft.com/en-us/cpp/c-runtime-library/reference/stricmp-wcsicmp-mbsicmp-stricmp-l-wcsicmp-l-mbsicmp-l?view=msvc-160
		28	https://docs.microsoft.com/en-us/cpp/c-runtime-library/reference/tolower-tolower-towlower-tolower-l-towlower-l?view=msvc-160
	551	29	https://docs.microsoft.com/en-us/cpp/c-runtime-library/reference/strcmp-wcscmp-mbscmp
	556	30	https://docs.microsoft.com/en-us/windows/win32/api/debugapi/nf-debugapi-isdebuggerpresent
	557	31	https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-exitprocess
	560	32	https://docs.microsoft.com/en-us/windows/win32/api/errhandlingapi/nf-errhandlingapi-seterrormode
	564	33	https://docs.microsoft.com/en-us/cpp/c-runtime-library/reference/memcpy-wmemcpy?view=msvc-160&viewFallbackFrom=vs-2019
	576	34	https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-messageboxa
	578	35	https://docs.microsoft.com/en-us/cpp/c-runtime-library/reference/memset-wmemset?view=msvc-160&viewFallbackFrom=vs-2019
	583	36	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-osversioninfoexa#remarks
	587	37	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_nt_headers32

	589	38	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_file_header
	590	39	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_section_header
	594	40	https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtualfree
	597	41	https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_enclave_import
8장	616	그림 8-1	https://www.netscout.com/blog/asert/innaput-actors-utilize-remote-access-trojan-2016-presumably
	617		https://www.malware-traffic-analysis.net/2017/02/06/index3.html
		2	https://twitter.com/malware_traffic
	620		https://github.com/hasherezade/hollows_hunter/wiki
	623		https://github.com/AllsafeCyberSecurity/ghidra_scripts
	629	※1	https://github.com/fireeye/flare-floss
	634	4	https://docs.microsoft.com/ko-kr/windows-hardware/drivers/ddi/wdm/ns-wdm-_file_full_ea_information
	641	5	https://docs.microsoft.com/ko-kr/windows/win32/api/combaseapi/nf-combaseapi-cocreateinstance
	662	7	https://docs.microsoft.com/ko-kr/windows/win32/api/winnt/ns-winnt-image_nt_headers32
		8	https://docs.microsoft.com/ko-kr/windows/win32/api/winnt/ns-winnt-image_file_header
	665	10	https://docs.microsoft.com/ko-kr/windows/win32/api/winnt/ns-winnt-image_section_header
		11	https://stackoverflow.com/questions/17436668/how-are-pe-base-relocations-build-up
9장	670		https://developer.android.com/training/basics/firstapp?hl=ja
		1	https://developer.android.com/studio/command-line/adb?hl=ja
	672	2	https://github.com/testwhat/SmaliEx
		3	https://developer.android.com/studio/build/multidex?hl=ja
	683	4	https://documentation-service.arm.com/static/5ed66080ca06a95ce53f932d
	685	5	https://docs.oracle.com/javase/jp/1.4/guide/jni/spec/functions.doc.html
		5(영어)	https://docs.oracle.com/javase/7/docs/technotes/guides/jni/spec/functions.html
	686		https://docs.oracle.com/javase/jp/8/docs/technotes/guides/jni/spec/functions.html
		6(영어)	https://docs.oracle.com/en/java/javase/16/docs/specs/jni/functions.html
	687	7	https://docs.oracle.com/javase/jp/8/docs/technotes/guides/jni/spec/functions.html#Call_type_Method__
		7(영어)	https://docs.oracle.com/en/java/javase/16/docs/specs/jni/functions.html#calltypemethod-routines-calltypemethoda-routines-calltypemethodv-routines
	688	8	https://docs.oracle.com/javase/jp/8/docs/technotes/guides/jni/spec/functions.html#Get_type_Field_
		8(영어)	https://docs.oracle.com/en/java/javase/16/docs/specs/jni/functions.html#gettypefield-routines
	690	9	https://bitbucket.org/JesusFreke/smali/downloads/
	697	12	https://developer.android.com/studio/run/emulator
		13	https://ghidra-sre.org
	698	14	https://www.7-zip.org/download.html
	699		https://bitbucket.org/iBotPeaches/apktool/downloads/
		16	https://ibotpeaches.github.io/Apktool/install/
	711		https://github.com/Ayrx/JNIAnalyzer/blob/master/JNIAnalyzer/data/jni_all.gdt
		18	https://www.ayrx.me/
	712	19	https://docs.oracle.com/javase/jp/8/docs/technotes/guides/jni/spec/invocation.html#JNJI_OnLoad
		19(영어)	https://docs.oracle.com/en/java/javase/16/docs/specs/jni/invocation.html#jni_onload

		20	https://docs.oracle.com/javase/8/docs/technotes/guides/jni/spec/invocation.html
	714	21	https://docs.oracle.com/javase/jp/6/technotes/guides/jni/spec/invocation.html
		21(영어)	https://docs.oracle.com/en/java/javase/16/docs/specs/jni/invocation.html
		22	https://docs.oracle.com/javase/jp/9/docs/specs/jni/functions.html
		22(영어)	https://docs.oracle.com/en/java/javase/16/docs/specs/jni/functions.html#gettypefield-routines
	718	23	https://docs.oracle.com/javase/7/docs/technotes/guides/jni/spec/functions.html#wp5833
	720		https://github.com/AllsafeCyberSecurity/py-findcrypt-ghidra
	738	24	https://developer.android.com/ndk/guides/cpu-arm-neon?hl=ja
		24(영어)	https://developer.android.com/ndk/guides/cpu-arm-neon
	740	25	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
	752	26	https://developer.android.com/reference/android/content/Context#getFilesDir()
	755	27	https://developer.android.com/ndk/reference/group/asset
	758	29	https://github.com/NationalSecurityAgency/ghidra/issues/556
	773	33	https://developer.android.com/reference/dalvik/system/DexFile
		34	https://android.googlesource.com/platform/libcore-snapshot/+/refs/heads/ics-mr1/dalvik/src/main/java/dalvik/system/DexFile.java
	774	35	https://developer.android.com/reference/dalvik/system/InMemoryDexClassLoader
	776	38	https://android.googlesource.com/platform/frameworks/base/+/master/core/java/android/app/ActivityThread.java#1005
	777	39	https://android.googlesource.com/platform/frameworks/base/+/master/core/java/android/app/ActivityThread.java#1869
		40	https://android.googlesource.com/platform/frameworks/base/+/master/core/java/android/app/ActivityThread.java#6162
	778	41	https://android.googlesource.com/platform/frameworks/base/+/master/core/java/android/app/LoadedApk.java#1170
	779	42	https://android.googlesource.com/platform/frameworks/base/+/master/core/java/android/app/Instrumentation.java#1151
	783	43	https://android.googlesource.com/platform/dalvik/+/0dcf6bb/vm/native/dalvik_system_DexFile.cpp
	784	44	https://android.googlesource.com/platform/dalvik/+/0dcf6bb/vm/native/dalvik_system_DexFile.cpp#249
	786	45	https://developer.android.com/reference/java/lang/ClassLoader
		46	https://android.googlesource.com/platform/libcore/+/master/dalvik/src/main/java/dalvik/system/BaseDexClassLoader.java#54
	787	47	https://android.googlesource.com/platform/libcore/+/master/dalvik/src/main/java/dalvik/system/DexPathList.java#71
		48	https://android.googlesource.com/platform/libcore/+/master/dalvik/src/main/java/dalvik/system/DexPathList.java#654
		49	https://android.googlesource.com/platform/libcore/+/master/dalvik/src/main/java/dalvik/system/DexPathList.java#703
	798	50	https://developer.android.com/reference/android/content/SharedPreferences
	802	53	https://developer.android.com/reference/javax/crypto/spec/SecretKeySpec
	803	54	https://developer.android.com/reference/javax/crypto/Cipher
	806	55	https://developer.android.com/reference/android/webkit/WebView
	807	56	https://developer.android.com/training/monitoring-device-state/doze-standby.html
	811	57	https://developer.android.com/reference/org/json/JSONObject
	815	58	https://developer.android.com/reference/java/net/HttpURLConnection
	817	59	https://developer.android.com/reference/android/telephony/SmsManager#getDefault()
		60	https://developer.android.com/reference/android/telephony/SmsManager#divideMessage(java.lang.String)
	819	61	https://developer.android.com/reference/java/lang/Runnable
	822	63	https://developer.android.com/reference/android/app/AlarmManager
	828	65	https://source.android.google.cn/devices/tech/dalvik/dalvik-bytecode
	829	※1	https://github.com/NationalSecurityAgency/ghidra/issues/1255

부록 A	868	6	https://www.sans.org/blog/a-few-ghidra-tips-for-ida-users-part-1-the-decompiler-unreachable-code/
	870	7	https://out7.hex-rays.com/demo
		7	https://www.hex-rays.com/products/idahome/
	872		https://github.com/JeremyBlackthorne/Ghidra-Keybindings
부록 B	875	8	http://virustotal.github.io/yara/
	876	9	https://github.com/ghidraninja/ghidra_scripts
	877	10	https://github.com/ReFirmLabs/binwalk/wiki/Using-the-Binwalk-IDA-Plugin
		11	https://github.com/you0708/ida/tree/master/idapython_tools/findcrypt
	879	12	https://github.com/daenerys-sre/source
	880	13	https://github.com/0xb0bb/pwndra
	882	14	https://github.com/L4ys/LazyIDA
		15	https://github.com/AllsafeCyberSecurity/LazyGhidra
	884	16	https://github.com/AllsafeCyberSecurity/ghidra_scripts
		17	https://github.com/fireeye/flare-ida
	886	※2	https://github.com/Cisco-Talos/GhIDA
		※3	https://github.com/Cisco-Talos/Ghidraaas
		※4	https://github.com/radareorg/r2ghidra-dec