minispy.c
DriverEntry
Vista
MiniSpyData.PFltSetTransactionContext = (PFLT_SET_TRANSACTION_CONTEXT) FltGetRoutineAddress("FltSetTransactionContext");
MiniSpyData.PFltGetTransactionContext = (PFLT_GET_TRANSACTION_CONTEXT) FltGetRoutineAddress("FltGetTransactionContext");
MiniSpyData.PFltEnlistInTransaction = (PFLT_ENLIST_IN_TRANSACTION) FltGetRoutineAddress("FltEnlistInTransaction");
FltRegisterFilter
&FilterRegistration
Callbacks
②SpyPreOperationCallback
SpyNewRecord
recordList = SpyNewRecord();
FltGetFileNameInformation
FltParseFileNameInformation
FltReleaseFileNameInformation
FltGetFileNameInformation
SpySetRecordName
FltReleaseFileNameInformation
SpyLogPreOperationData
RecordListに登録する
SpyPostOperationCallback
SpyEnlistInTransaction
SpyLog(recordList);
SpyLogTransactionNotify
②SpyPostOperationCallback
SpyLogPostOperationData
SpyLog(recordList);
Contexts
SpyDeleteTxfContext
SpyFilterUnload
SpyQueryTeardown
マニュアルでVolumeをdetachした場合
Vista
SpyKtmNotificationCallback
SpyLog(recordList);
&MiniSpyData.Filter
FltBuildDefaultSecurityDescriptor
FltCreateCommunicationPort
SpyConnect
SpyDisconnect
FltCloseClientPort
SpyMessage
Switch
GetMiniSpyLog
④SpyGetLog
while (!IsListEmpty(&MiniSpyData.OutputBufferList) && (OutputBufferLength > 0)) {
pList = RemoveHeadList(&MiniSpyData.OutputBufferList);
InsertHeadList
SpyFreeRecord(pRecordList);
GetMiniSpyVersion
FltFreeSecurityDescriptor
FltStartFiltering
mspyUser.c
main
FilterConnectCommunicationPort
CreateThread
mspyLog.C!RetrieveLogRecords
③FilterSendMessage(GetMiniSpyLog,buffer)
ScreenDump
FileDump
while (inputChar = (CHAR)getchar()) {
InterpretCommand
switch (parm[1]) {
case 'a':
case 'A':
①FilterAttach(MINISPY_NAME,(PWSTR)buffer)
case 'd':
case 'D':
FilterDetach(MINISPY_NAME,(PWSTR)buffer,instanceString);
case 'l':
case 'L':
ListDevices();
FilterVolumeFindFirst
case 's':
case 'S':
Context->NextLogToScreen = !Context->NextLogToScreen;
case 'f':
case 'F':
Context->OutputFile = fopen(parm, "w");