„Handle read“

Bedienungsanleitung

Andreas Theusner 2014

H&D Services for Engineering GmbH

Inhalt

Zweck

Handle read ruft das Kommandozeilem-Programm **handle.exe** aus der Sysinternals Suite von Mark Russinovich /Microsoft ohne und mit Parametern auf.

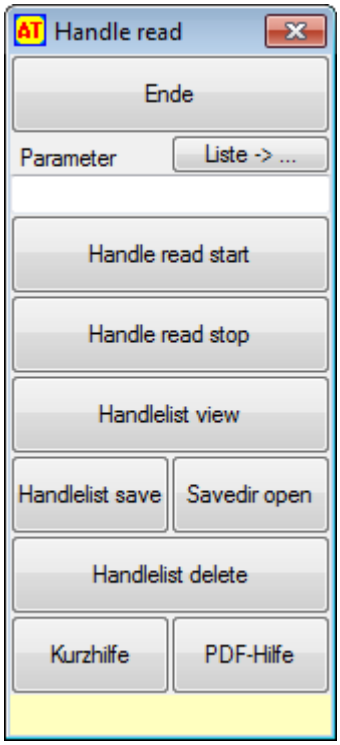
Beschreibung auf http://technet.microsoft.com/de-de/sysinternals/bb896655

Handle
Dieses praktische Befehlszeilenprogramm zeigt, welche Dateien durch welche Prozesse geöffnet wurden und vieles mehr.
Handle sucht nach Verweisen auf offene Dateien. Wenn Sie also keine Befehlszeilenparameter angeben, werden hiermit die Werte aller Handles im System aufgelistet, die auf offene Dateien verweisen, und zwar gemeinsam mit dem Namen dieser Dateien.

Handle ist Freeware und wird auf den GRICOS-DEV-Servern zur Analyse eingesetzt.
Handle benötigt Administratorrechte zum Ausführen

Handle read ruft handle.exe per Threading in einer Endlosschleife auf und schreibt die Konsolenausgabe fortlaufend in die Datei hr.txt.

Programmoberfläche



Element	Funktion	Bemerkungen
Ende	Beendet das Programm.	
Parameter	Eingabe von Parameter im Feld darunter, die an handle.exe übergeben werden.	Wenn das Feld leer ist, wird kein Parameter übergeben.
Liste -> …	Zeigt die möglichen Parameter für handle.exe an.	
Handle read start	Startet das Handle-Logging. Bei Bedarf ruft **handle.exe** eine **handle64.exe** auf.	Die Handles werden in der Datei **hr.txt** im Programmverzeichnis gespeichert. Es erfolgt jeweils ein anhängen der neuen Loggingdaten an die bisherigen Einträge. Ist diese nicht vorhanden, wird diese neu angelegt.
Handle read stop	Stoppt das Handle-Logging.	
Handlist view	Zeigt die Datei **hr.txt** an.	Dazu wird das Freeware-Programm **lister.exe** im Programmverzeichnis genutzt, welches konfigurierbar ist. Deaktiviert einige Komponenten, die anderen bleiben bedienbar. Währed des prozesses kann auch die Loggingdatei hr.txt geöffnet und schon darin gesucht werden. Neue Einträge werden dennoch reingeschrieben, weil SharedAccess unterstützt wird.
Handlist save	Speichert die Datei im Verzeichnis **save** im Programmverzeichnis.	Der Dateiname wird folgendermaßen formatiert: **Jahr-Monat-Tag_Stunden-Minuten-**

		Sekunden_hr.txt So können mehrere Logs verglichen werden. Anmerkung: Nach jedem Speichervorgang sollte die Datei **hr.txt** mit **Handlelist delete** gelöscht werden, sonst werden ale weiteren Loggings jeweils angehangen.
Savedir open	Öffnet das Verzeichnis **save** mit den gespeicherten Loggings im Windows Explorer.	
Handlelist delete	Löscht die Datei hr.txt aus dem Pogrammverzeichnis.	Beim nächsten Logging wird sie neu angelegt.
Kurzhilfe	Zeigt eine kurze Hilfe zur Orientierung an.	
PDF-Hilfe	Zeigt diese Datei an.	
gelbes Statusfeld	Zeigt den aktuellen Status bzw. die aktuell oder zuletzt durchgeführte Aktion an.	

Zugehörige Programm-Dateien:

Parameter

Handle read gibt alle angegeben Parameter oder auch keinen angegebenen Parameter 1:1 an handle.exe weiter.

Quelle: http://technet.microsoft.com/de-de/sysinternals/bb896655

Verwendung: handle [[-a] [-u] | [-c <Handle> [-y]] | [-s]] [-p <Prozessname>|<PID>> [Name]

-a

Sichert Informationen zu allen Handletypen, also nicht nur zu den Handles, die auf Dateien verweisen. Zu diesen anderen Typen gehören beispielsweise Ports, Registrierungsschlüssel, Synchronisierungsprimitive, Threads und Prozesse.

-c

Schließt das angegebene Handle (als hexadezimale Zahl interpretiert). Der Prozess muss als PID angegeben werden.

WARNUNG: Das Schließen von Handles kann zu Instabilitäten bei Anwendungen oder im gesamten System führen.

-y

Fordert nicht zum Bestätigen auf, wenn Handles geschlossen werden sollen.

-s

Gibt die Anzahl aller geöffneten Handles aus.

-u

Zeigt bei der Suche nach Handles den Benutzernamen des Besitzers an.

-p

Untersucht nicht alle Handles im System, sondern beschränkt die Suche auf die Prozesse, deren Namen mit den angegebenen Zeichen beginnt. Beispiel:

handle -p exp

sichert die geöffneten Dateien für alle Prozesse, die mit „exp“ beginnen, also auch für Explorer.

Name

Mit diesem Parameter geben Sie an, dass Handle nach Verweisen auf ein Objekt mit einem bestimmten Namen suchen soll. Wenn Sie beispielsweise erfahren möchten, ob „c:\windows\system32“ durch einen Prozess geöffnet wurde (und wenn ja, durch welchen), geben Sie Folgendes ein:

handle windows\system

Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und der angegebene Namensteil kann sich an einer beliebigen Stelle in den angegebenen Pfaden befinden.

Handle-Ausgabe

Wenn Handle nicht im Suchmodus betrieben wird (wenn Sie also keinen Namensteil als Parameter eingegeben haben), gliedert Handle die Ausgabe in Abschnitte für die einzelnen Prozesse, für den die Handleinformationen ausgegeben werden. Der Inhalt der Ausgabe wird dabei mithilfe von gestrichelten Linien strukturiert, unter denen jeweils der Prozessname und die Prozess-ID (PID) aufgeführt sind. Unterhalb des Prozessnamens werden die Handlewerte aufgeführt (in hexadezimaler Schreibweise), außerdem der Typ des Objekts, mit dem das Handle verknüpft ist, sowie der Name des Objekts (falls vorhanden).

Im **Handle**-Suchmodus werden die Namen und IDs der Prozesse auf der linken Seite ausgegeben sowie die Namen der Objekte, für die eine passende Übereinstimmung gefunden wurde, auf der rechten Seite.

Anmerkungen und Tipps

Jan Rosenneck:

…wie gerade besprochen, bietet hr.exe über die Option „-p dsq.exe“ ja die Möglichkeit direkt nach Dateien die von diesem Prozess benutzt werden zu suchen.
Man kann laut der Hilfe auch rückwärts suchen wenn man den Namen einer verdächtigen Datei kennt. In der Hilfe steht:
…
Name
Mit diesem Parameter geben Sie an, dass Handle nach Verweisen auf ein Objekt mit einem bestimmten Namen suchen soll.
Wenn Sie beispielsweise erfahren möchten, ob „c:\windows\system32“ durch einen Prozess geöffnet wurde (und wenn ja, durch welchen),
geben Sie Folgendes ein:

handle windows\system

Beim Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden, und der angegebene Namensteil kann sich an einer
beliebigen Stelle in den angegebenen Pfaden befinden.
…

Wichtig ist , dass der Dateiname offenbar der alten 8.3 Syntax entsprechen muss, also **windows\system** passt ja, da der Namensteil jeweils nicht mehr als 8 Zeichen hat
aber **dsm_cache** funktioniert nicht, entweder abkürzen z.B **dsm_** oder **dsm_ca~1**, wobei ich bisher nur **dsm_** getestet habe. Ich konnte sonst aber keine
Erklärung finden warum **dsm_cache** nicht funktioniert

Anwendungsfälle und Analyse

Dies soll hier anhand der GRI gezeigt werden.

Ein Wort zur Vorsicht

Es können natürlich auch parallele Prozesse in einem Durchlauf geloggt werden. Allerdings wird die Loggingdatei **hr.txt** dabei recht groß. Als Anhaltspunkt dient der Einsatz des Parameters GrXKernel.MSWin64.exe mit 10 parallelen Prozessen. Die Datei hr.txt kann dabei gut und gern eine Größe von 60 MB erreichen. Es empfiehlt sich daher, vor jedem größeren Lauf die Datei zu löschen bzw. vorher zu sichern.

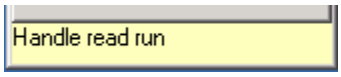
Desweiteren sollte immer nur ein angemeldeter Benutzer eine Instanz von **Handle read** und auch nur immer ein Loggingprozeß starten, auch wenn Handle read Shared-Zugriff auf die Logging-Datei beherrscht. Dieser wird beim mehrfachen Aufruf von handle.exe während des Threadings benötigt.

Parameter: GrXKernel.MSWin64.exe

Handle read

Parameter: -p GrXKernel.MSWin64.exe

Start: Klick auf Button **Handle read start**

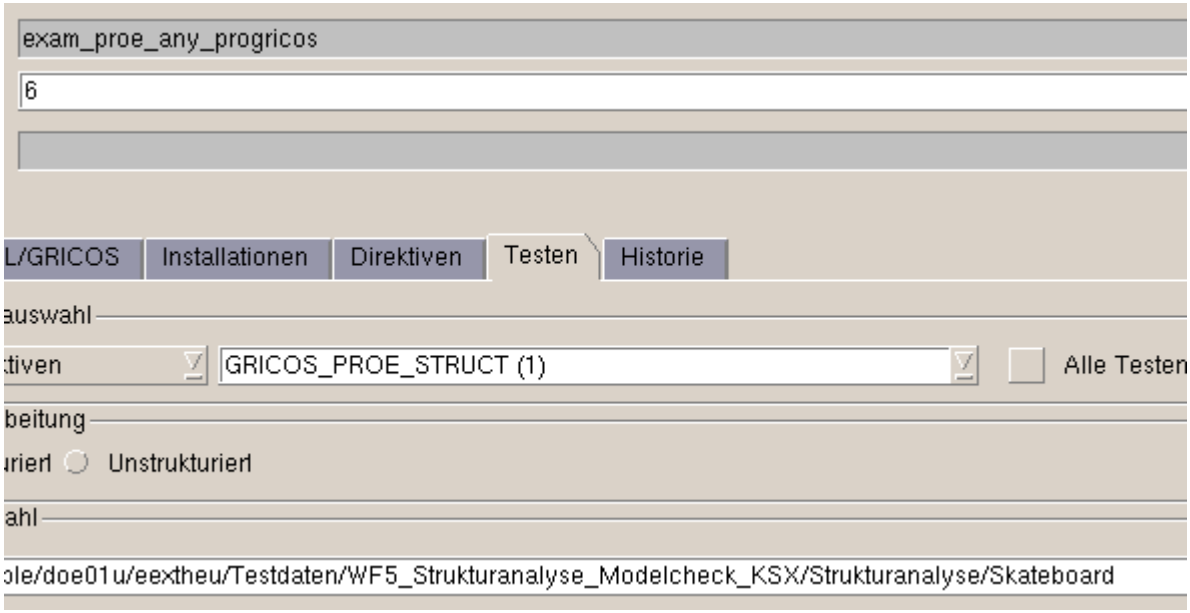


Werkbank

Start einer Konvertierung – hier GRI- KSX+Modelcheck

Modul: exam:proe_any_progricos

Direktive: GRICOS_PROE_STRUCT



Nach Ende der Konvertierung in **Handle read** auf **Handle read stop** klicken. Anschließend können mit Klick auf Handlelist view die geloggten Daten angezeigt werden.

Ist in der Werkbank ein Prozeß mit Fehler zurückgekommen obwohl andere durchliefen,

Direktive	Status	Masterfile name	App-RC	App-STATUS	Script-RC	Script-STATUS
GRICOS_PROE_STRUCT (1)	ERROR	000_000_000-skateboard.asm.1	4	RETRY	7	RETRY
GRICOS_PROE_STRUCT (1)	SUCCESS	000_000_000-skateboard.asm.1	0	OK	0	OK

dann kann hie z.B. der Name des Prozeßverzeichnisses ermittelt und in der im Logging alle dazu auftretenden Datei-/Proceßereignisse gesucht werden:

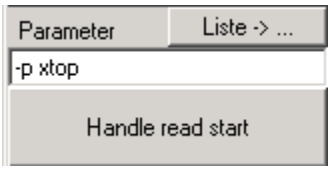
```
------------------------------------------------------------------------------
GrXKernel.MSWin64.exe pid: 9256 GRICOSWIND01\eginacv
    C: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-104020-25980\mod_1\tempdir
   1C: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\cygpid.4332
   24: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccfldf_6.0.7601.17514_none_fa396087175ac9ac
   28: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
   2C: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
   84: File  (RW-)   E:\K_DATA\pro\eginacv\GRXCache\GrXKernel.MSWin64.exe
   94: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   9C: File  (RWD)   E:\gricos\eginacv\gina_cs.stderr
   A4: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   A8: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   B4: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\S-1-5-21-3840607217-1814691404-1317497643-1000.1
   B8: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   C0: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   CC: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   D4: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   D8: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\S-1-5-21-3840607217-1814691404-1317497643-1000.1
   E0: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   E8: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   F4: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
   F8: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\S-1-5-21-3840607217-1814691404-1317497643-1000.1
  104: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
  114: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\shared.5
  118: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  11C: File  (RWD)   E:\gricos\eginacv
  124: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  128: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  12C: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  130: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  134: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  138: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  15C: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  160: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  164: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  168: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  16C: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-104020-25980\mod_1\tempdir\appl.stderr_GRICOSWIND01_6664
  170: File  (RWD)   E:\gricos\eginacv
  174: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  184: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  188: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  18C: File  (RW-)   E:\gricos\eginacv\tools\Perl_5.14.2_WINDOWS\site\lib\Jcode.pm
  194: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  198: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  19C: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  1A0: File  (R-D)   C:\Windows\System32\en-US\KernelBase.dll.mui
  1A4: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  1F0: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  1F4: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6195_none_88e41e092fab0294
  204: Section       \BaseNamedObjects\__ComCatalogCache__
  210: Section       \BaseNamedObjects\__ComCatalogCache__
  278: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-104020-25980\mod_1\tempdir\script.log
  27C: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-104020-25980\mod_1\tempdir\appl.stdout_GRICOSWIND01_6664
  280: File  (RWD)   E:\gricos\eginacv\gina_cs.stdout
  288: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-104020-25980\mod_1\tempdir\appl.stderr_GRICOSWIND01_6664
  298: Section       \RPC Control\DSEC2428
  2EC: Section       \BaseNamedObjects\cygwin1S5-d08cf07486dfbfcc\cygpid.25540
  30C: File  (RWD)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-104020-25980\mod_1\input
  338: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-104020-25980\mod_1\tempdir\script.log.dbg
------------------------------------------------------------------------------
```

Parameter: xtop.exe

Handle read

Parameter: -p xtop (für alle Prozesse, die mit dieser Zeichenfolge beginnen z.B. Mehrfachaufruf von xtop.exe)

Start: Klick auf Button **Handle read start**



Werkbank

Start einer Konvertierung – hier GRI- KSX+Modelcheck

Modul: exam:proe_any_progricos

Direktive: GRICOS_PROE_STRUCT

Handlelogging

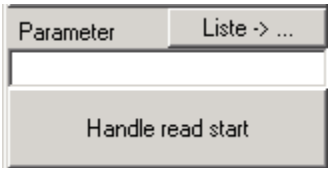
```
------------------------------------------------------------------------------
xtop.exe pid: 23688 GRICOSWIND01\eginacv
   10: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccfldf_5.82.7601.18201_none_a4d3b9377117c3df
  320: Section       \BaseNamedObjects\windows_shell_global_counters
  428: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\std.err
  458: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\trail.txt.1
  468: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\std.out
  47C: File  (RW-)   E:\K_PATH\pro\gri090000f\m090\x86e_win64\CommonFiles\text\compiled_resource\pro_default_resources.dll
  484: File  (RW-)   E:\K_PATH\pro\gri090000f\m090\x86e_win64\CommonFiles\proe\uitools\text\compiled_resource\uitools_resources.dll
  48C: File  (RW-)   C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccfldf_6.0.7601.17514_none_fa396087175ac9ac
  4CC: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\AppData\Local\Microsoft\Windo
  4D0: Section       \BaseNamedObjects\e:_gricos_eginacv_workspace_gricosdevgricoslina01_140304-135054-26552_mod_1_tempdir_AppData_Loc
  4D8: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\AppData\Roaming\Microsoft\Win
  4DC: Section       \BaseNamedObjects\e:_gricos_eginacv_workspace_gricosdevgricoslina01_140304-135054-26552_mod_1_tempdir_AppData_Roa
  4E4: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\AppData\Local\Microsoft\Windo
  4E8: Section       \BaseNamedObjects\e:_gricos_eginacv_workspace_gricosdevgricoslina01_140304-135054-26552_mod_1_tempdir_AppData_Loc
  52C: File  (RW-)   E:\K_PATH\pro\gri090000f\m090\x86e_win64\CommonFiles\proe\zbaseutils\text\compiled_resource\zbaseutils_resources.
  534: File  (RW-)   E:\K_PATH\pro\gri090000f\m090\x86e_win64\CommonFiles\proe\zbase_apps\text\compiled_resource\zbase_apps_resources.
  550: File  (RW-)   E:\K_PATH\pro\gri090000f\m090\x86e_win64\CommonFiles\libs\prowtlibs\text\compiled_resource\prowtlibs_resources.dl
  564: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir
  634: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\proe_modelcheck_log.txt
  660: File  (RW-)   E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-135054-26552\mod_1\tempdir\proe_ksx_log.txt
```

Parameter: pro_comm_msg.exe

Handle read

Parameter: leer -> Suchen im Logging nach xtop.exe

Start: Klick auf Button **Handle read start**



Werkbank

Start einer Konvertierung – hier GRI- KSX+Modelcheck

Modul: exam:proe_any_progricos

Direktive: GRICOS_PROE_STRUCT

Logging

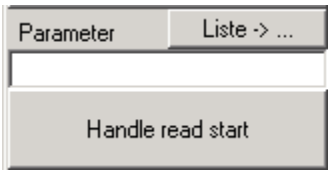
```
------------------------------------------------------------
pro_comm_msg.exe pid:  56964 GRICOSWIND01\eginacv
     C: File   (RW-)    E:\tmp\.gina_7bkE853804
```

Parameter. parametric.exe

Handle read

Parameter: leer -> Suchen im Logging nach parametric.exe

Start: Klick auf Button **Handle read start**



Werkbank

Start einer Konvertierung – hier GRI- KSX+Modelcheck

Modul: exam:proe_any_progricos

Direktive: GRICOS_PROE_STRUCT

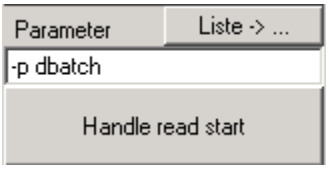
Logging

```
-------------------------------------------------------------------------------
parametric.exe pid:  57320 GRICOSWIND01\eginacv
   10: File   (RW-)    C:\Windows
   1C: File   (RW-)    E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-141054-47260\mod_1\tempdir
-------------------------------------------------------------------------------
```

Parameter: dbatch

Handle read

Parameter: -p dbactch (alle Prozesse die mit dbatch beginnen -> dbatchc.exe, dbatchs.exe etc.)
Start: Klick auf Button **Handle read start**



Werkbank

Start einer Konvertierung – hier GRI- KSX+Modelcheck
Modul: trans_proe_export_dbatch
Direktive: GRICOS

Handlelogging

```
-------------------------------------------------------------------------
dbatchc.exe pid: 37560 GRICOSWIND01\eginacv
     8: File  (R--)    E:\K_DATA\pro\eginacv\home\pro\grx\Startlog.win.GRICOSWIND01.00
     C: File  (R--)    E:\K_DATA\pro\eginacv\home\pro\grx\Startlog.win.GRICOSWIND01.00
    18: File  (RW-)    E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-142732-36468\mod_1\tempdir
    1C: File  (RW-)    C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18201_none_a4d3b9377117c3df
    64: File  (RW-)    E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-142732-36468\mod_1\tempdir\appl.stdout_GRICOSWIND01_36772
    68: File  (RW-)    E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-142732-36468\mod_1\tempdir\appl.stderr_GRICOSWIND01_36772
   24C: Section       \BaseNamedObjects\windows_shell_global_counters
-------------------------------------------------------------------------
dbatchs.exe pid: 41148 GRICOSWIND01\eginacv
     8: File  (R--)    E:\K_DATA\pro\eginacv\home\pro\grx\Startlog.win.GRICOSWIND01.00
     C: File  (R--)    E:\K_DATA\pro\eginacv\home\pro\grx\Startlog.win.GRICOSWIND01.00
    64: File  (RW-)    E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-142732-36468\mod_1\tempdir\appl.stdout_GRICOSWIND01_36772
    68: File  (RW-)    E:\gricos\eginacv\workspace\gricosdevgricoslina01\140304-142732-36468\mod_1\tempdir\appl.stderr_GRICOSWIND01_36772
   2F0: File  (RW-)    C:\ProgramData\dbs64E3.tmp
   2F8: File  (RW-)    C:\ProgramData\dbatch-41148-10.187.69.34.8001.1393939684.1
```