



Analysis User Agent AUA Installation & Betrieb

Analysis User Agent (AUA)

– AUA Client / AUA Server / Installation & Betrieb –

Stand: 18. Dez. 2005



© 2005 - Synapse:Networks GmbH

[Rechte Dritter an Software und Marken sind nicht berührt – siehe Hinweise hierzu im Text.]
[Insbesondere die erwähnten Marken Ethereal und MS-Windows sind Eigentum ihrer jeweiligen Rechte-Inhaber.]



Analysis User Agent AUA Installation & Betrieb

INHALT

Zweck	3
Danksagung	4
Delivered Files	5



.....	6
Voraussetzungen für den Analysis-User-Agent (AUA)	6
Ethereal, TEthereal, WinPCap, Instsrv.exe, Svrany.exe, Scripts.....	6
Installation	6
Install-Script: AUA_(1)_Ethereal-Install.bat (INSTSRV.EXE - SVRANY.EXE – REG IMPORT)	8
Install Script: AUA_(2)_ETHERREAL.REG.txt	10
Start-Script: AUA_(3)_RUN.BAT [oder AUA_RUN.BAT].....	10
AUA-Server	17
AUA-Client.....	17



.....	18
AUA-Client: Das Anwender-Modul (AUA_Analysis_User_Agent.exe)	18
Installation	18
Bedienung durch den Anwender	21
Erster Aufruf	21
Aufruf zum Zweck der Versendung von Analyse-Aufzeichnungsdaten	22
Angaben des Anwenders zur beobachteten Störung	23
Auswahl der betroffenen Applikation(en).....	24
Angabe der Kriterien „Bedeutsamkeit“ / „Eilbedürftigkeit“	24
Eingabe beliebiger Zusatz-Angaben des Anwenders	25
Versendung der Angaben und Aufzeichnungs-Daten	25
Wenn der AUA-Server nicht erreicht wird: Fehler-Meldung	26
AUA.ServerData.TXT	27



.....	28
AUA-Server: Der Trace-File-Index / Das Index-Viewer-Modul	28
Server-Share: %AnalysisServerName% - AUAServer\$	28
Server-Modul (AUA_Server_Index_Viewer.exe).....	30



.....	32
Synapse:Networks GmbH	32



Analysis User Agent (AUA)

Zweck

LAN-Analyse der klassischen Art hat den Nachteil, dass Messungen (= Aufzeichnungen von Datenverkehr) erst nach Anwender-Hinweisen gestartet werden. Dann aber ist das vom Anwender beobachtete Verhalten längst Vergangenheit. Messungen finden dann stets mit dem Zweifel statt: Wird sich das bemängelte Verhalten je wiederholen? Und selbst, wenn: Wann würde das sein? Die Folge der nachträglich angesetzten Messungen ist (war) oft ein langes Warten. Zeit aber ist Geld.

Wenn ein Anwender Auffälligkeiten oder Fehler beobachtet, sollten die Datenverkehr-Aufzeichnungen (eng.: Traces) schon vorliegen. Sodann ist es ein Leichtes, nach Angaben des Anwenders (Uhrzeit des Geschehens und betroffene Applikation) in den Messdaten den Hergang zu finden und die Ursache festzustellen (oder wenigstens einzukreisen).

Um nun aber nicht gezwungen zu sein, für alle Anwender im Zentrum des Datennetzes sämtliche durchfließenden Daten aufzeichnen zu müssen, ist es wesentlich zweckmäßiger, auf jedem einzelnen Arbeitsplatz-PC die Kommunikations-Daten aufzuzeichnen – für jeweils einen Tag. Tritt an diesem Tag eine Störung auf, ist es die Entscheidung des Anwenders (und nur seine allein), die Aufzeichnungen auf einen zentralen Analyse-Server zu versenden, der die Messdaten sammelt und auswertet.

Die vorliegende Software zergliedert sich in:

AUA Client = `AUA_Analysis_User_Agent.EXE`

AUA Server = `AUA_Server_Index_Viewer.EXE (SIV)`

Zur Analyse der Aufzeichnungs-Daten (.DMP Trace Files) wird seitens Synapse:Networks GmbH das Analyse-Experten-System „**Trace:Magic**“ (www.tracemagic.net) empfohlen.



Danksagung

Der „Analysis User Agent“ entstand (und entsteht weiter) bei einem langjährigen Großkunden von Synapse:Networks GmbH, der **Deutschen Forschungs Gemeinschaft (DFG)** in Bonn.

Die Betreuung des dortigen Pilot-Projekts fand und findet statt unter Mithilfe zweier IT-Kollegen, die für externe Dienstleister beim Kunden vor Ort tätig sind:

Robert Cyrys
Kay Ingerfeld

MS Mikrosoftware GmbH
Döres AG

Rheinbach
Köln

R.Cyrus@mikro-software.de
Ingerfeld.Kay@doeres.com

Auf Herrn Ingerfeld geht das Script zur Installation des Windows-System-Dienstes „Ethereal“ via INSTSRV.EXE/SRVANY.EXE zurück. Er war so freundlich, das Script für diesen Zweck zur Verfügung zu stellen. Herr Ingerfeld kann auf Anfrage auch Auskunft geben über die zentrale automatische Installation mittels NetInstall.

Auf Herrn Cyrus geht die Installation des Benutzer-Programms „Analysis User Agent“ zurück (gewissemaßen dem „front end client“), die praktische Umsetzung bei den Anwendern sowie die Messdaten-Verarbeitung mittels „**Trace:Magic**“ vor Ort beim Pilot-Kunden.

Beiden sei an dieser Stelle Dank gesagt für ihre Mithilfe und ihre Anregungen.



Analysis User Agent AUA Installation & Betrieb

Gelieferte Dateien

Zur Installation werden folgende Dateien geliefert (**grün**=Hilfs-Dateien, **rot**=Installations-Dateien):

AUA_(0)_INSTALLATION_.pdf	→ Installations-Anweisungen
AUA_(1)_Ethereal-Install.bat	→ Installation des Windows-Dienstes
AUA_(2)_Ethereal.REG.txt	
AUA_(3)_RUN.BAT	→ Das vom Dienst zu startende Script
AUA_(3.1)_RUN_(Muster)_(mini)_.BAT	→ Muster-Script „mini“ = einfach
AUA_(3.1)_RUN_(Muster)_(mini)_.BAT	→ Muster-Script „midi“ = anspruchsvoll
AUA_(3.3)_RUN_(Muster)_(maxi)_.BAT	→ Muster-Script „maxi“ = manuelle Tests
AUA_(4)_Client_Files\AUA.Applications.TXT	→ AUA-Dateien im DMP-File-Verzeichnis
AUA_(4)_Client_Files\AUA.Contact.TXT	
AUA_(4)_Client_Files\AUA.Help.TXT	
AUA_(4)_Client_Files\AUA.UserData.TXT	
AUA_(4)_Client_Files\AUA_Analysis_User_Agent.exe	
AUA_(5)_Server_Files\AUA_Server_Index_Viewer.exe	→ AUA-Dateien im Server-Verzeichnis
AUA_(9)_Ethereal-Install_[STOP]_.bat	→ Script zum Entfernen des Dienstes

Die Dateien sind nummeriert, um die Reihenfolge des Abarbeitens zu kennzeichnen.

Alle Scripte und .REG-Dateien sind auf diese Namen hin abgestimmt.

Änderungen von Datei-Namen können dazu führen, dass die Installation bzw. der Betrieb fehl schlägt.



Voraussetzungen für den Analysis-User-Agent (AUA)

Es muss auf dem Arbeitsplatz-PC eine Software installiert sein, die den Datenverkehr über eine Netzwerk-Schnittstelle aufzeichnet und in Form von Dateien abspeichert.

Ethereal, TEthereal, WinPCap, Instsrv.exe, Svrany.exe, Scripts

Um hohe Kosten zu sparen, ist bis auf weiteres der Einsatz der Open-Source-Software „TEthereal“ im Blickfeld. „TEthereal“ ist ein ohne Anwendungs-Oberfläche arbeitendes Mini-Programm, das vom Analyse-Produkt „Ethereal“ abgeleitet ist und wie dieses kostenfrei aus dem Internet bezogen werden kann (GPL License). Damit „TEthereal“ die Messdaten „sehen“ und aufzeichnen kann, ist noch zuvor die Installation des Schnittstellen-Treibers „WinPCap“ Voraussetzung.

Alle Rechte am Software-Code, den Markenzeichen und sonstigen Bezeichnungen und Techniken im Umfeld von "Ethereal" liegen allein bei den Erzeugern (Ethereal (C)1998 Gerald Combs [und andere]); die Nutzung folgt den Bestimmungen von GNU/GPL ([Open Source GNU GPL](#)); siehe:

<http://www.ethereal.com/download.html>
<http://www.ethereal.com/distribution/>
<http://www.ethereal.com/distribution/win32/>

Alle Rechte am Software-Code des WinPCap-Treibers liegen allein bei den Erzeugern (NetGroup, Politecnico di Torino, Italia).

<http://winpcap.politco.it/>
<http://www.ethereal.com/distribution/win32/>

Installation

Zur Installation des WinPCap-Treibers gibt es ein kostenfreies Download:

<http://www.winpcap.org/install/default.htm>

Zur Installation der Ethereal-Software gibt es ein kostenfreies Download:

<http://www.ethereal.com/distribution/win32/>

Eine Voll-Installation der Analyse-Software Ethereal hat die Wirkung (klar gesprochen: den Nachteil), dass der Anwender über die Bediener-Oberfläche (das GUI) die Messdaten selbst einsehen kann.



Analysis User Agent AUA Installation & Betrieb

Da dies in der Regel nicht erwünscht ist, sollte mit dem kleineren Capture-Modul (Aufzeichnungs-Modul) TEthereal gearbeitet werden: Es zeichnet die Messdaten in Datei-Form auf, hat aber selbst keine Bediener-Oberfläche (da Kommandozeilen-Programm) und bietet daher den PC-Benutzern keinen Zugriff auf die Daten.

Zur Installation nur des TEthereal-Programmteils gibt es ein kostenfreies Download:

<http://www.synapse-ssc.de/index.php?id=14>

Dies ist das „**TEthereal Starter Programm**“ von Synapse:Networks GmbH.

Es enthält nur jene Programm-Dateien von Ethereal/TEthereal, die zur Aufzeichnung wirklich benötigt werden; alle weiteren Installations-Dateien sind nicht vorhanden.

Hierüber kann man sich eine volle bzw. reguläre Installation des Programms „Ethereal“ ersparen.

Es reicht vollständig, die Dateien des „**TEthereal Starter Programms**“ in ein beliebiges Verzeichnis zu kopieren.

Jedoch sollte für den Betrieb mit dem „Analysis User Agent (AUA)“ die Programm-Datei „**TEthereal_Starter.exe**“ gelöscht werden, da hierüber vom Anwender eigenständige Starts von „TEthereal“ vorgenommen werden können; diese Starts könnten jedoch die Arbeitsweise des „Analysis User Agents“ gefährden.



Analysis User Agent AUA Installation & Betrieb

Install-Script: AUA_(1)_Ethereal-Install.bat (INSTSRV.EXE - SVRANY.EXE – REG IMPORT)

Der Start der Aufzeichnung sollte bereits bei Hochfahren des Windows-Betriebssystems über ein Autostart-Script erfolgen.

Um die Messdaten-Aufzeichnung automatisch zu aktivieren, ist der sog. „Promiscuous Mode“ am Netzwerk-Treiber notwendig. Ohne diesen Betriebs-Modus würde ggf. nicht alles (oder gar nichts) aufgezeichnet. Hierzu muss Ethereal bzw. TEthereal mindestens mit Administrator-Berechtigung laufen.

Dies kann mittels der von Microsoft gelieferten Hilfs-Programme **INSTSRV.EXE** und **SRVANY.EXE** gelöst werden. Dies sind Tools von Microsoft, die Scripts, Batch-Files etc. als Dienst installiert werden. Der läuft dann unter dem System-Account des Windows-Betriebssystems.

INSTSRV.EXE / SRVANY.EXE → Quelle: Microsoft Resource Kit

Das folgende Installations-Script installiert die komplette Ethereal-Programm-Suite; hier sollte ggf. die Datei „**Ethereal.exe**“ nachträglich wieder gelöscht werden, um Anwendern keinen Zugriff auf die Messdaten zu geben.

(Das Programm „Ethereal.EXE“ arbeitet mit GUI, also mit grafischer Benutzer-Oberfläche; das Programm „TEthereal.EXE“ arbeitet als Kommandozeilen-Tool, also ohne GUI.)

Folgendes Script führt die Dienste-Installation durch (siehe unten), wobei „**INSTSRV.EXE**“ dem Windows-System bekannt gibt, dass es demnächst den Dienst „**Ethereal**“ zu geben habe, der seinerseits über „**SRVANY.EXE**“ aufzurufen sei, und über den Befehl „**REG IMPORT**“ werden die Registry-Werte geladen, die Windows beim System-Start veranlassen, die richtige Batch-Datei aufzurufen (das ist: „**AUA_(3)_RUN.BAT**“):

```

:AUA_(1)_Ethereal-Install.bat
@echo off
echo.

if "%1" == "stop" goto stop
if "%1" == "STOP" goto stop

:START
echo.
echo Einrichten des Service "Ethereal"
echo -----
echo (Anhalten und Deinstallieren mit dem Aufruf "Ethereal stop")
echo.
echo Installieren des Service...
echo.
C:\Programme\Ethereal\instsrv.exe Ethereal C:\Programme\Ethereal\Srvany.exe
REM "C:\Program Files\Ethereal\instsrv.exe" Ethereal "C:\Program Files\Ethereal\Srvany.exe"
echo.
echo --- --- ---
echo.
echo Installieren der Registry-Werte...
echo.
reg import AUA_(2)_Ethereal.reg.TXT
    
```



Analysis User Agent AUA Installation & Betrieb

```
echo.
echo --- --- ---
echo.
echo Starten des Service ...
echo.
echo (nur hier und jetzt fuer diese erste Session,
echo danach ueber den Hintergrund-Dienst) ...
echo.
net start Ethereal
echo.
echo --- --- ---
echo.

:STOP
echo Anhalten und Deinstallieren des Service "Ethereal"
echo -----
echo Stoppen des Service...
echo.
net stop Ethereal
echo.
echo --- --- ---
echo.
echo Deinstallieren des Service und der Registry-Werte...
echo.
C:\Programme\Ethereal\instsrv.exe Ethereal remove
REM "C:\Program Files\Ethereal\instsrv.exe" Ethereal remove
echo.
echo --- --- ---
echo.

:ENDE
echo.
echo *** Fertig ***
echo.
pause
```

Der Inhalt der Datei „AUA_(2)_Ethereal.REG.txt“:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ethereal\Parameters]
"Application"="C:\\Programme\\Ethereal\\AUA_(3)_RUN.BAT"
"AppDirectory"="C:\\Programme\\Ethereal"
"AppParameters"=""
```

Weiteres hierzu: Siehe nächsten Abschnitt.



Analysis User Agent AUA Installation & Betrieb

Install Script: AUA_(2)_ETHEREAL.REG.txt

Die Zeile „`reg import AUA_(2)_Ethereal.REG.txt`“ setzt die für den Dienst notwendigen Start-Parameter:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ethereal\Parameters]
"Application"="C:\\Programme\\Ethereal\\AUA_(3)_RUN.BAT"
"AppDirectory"="C:\\Programme\\Ethereal"
"AppParameters"=""
```

Hier wird lediglich die auszuführende Datei mit Pfad angegeben (`C:\\Programme\\Ethereal\\AUA_(3)_RUN.BAT`) und das Arbeitsverzeichnis.

Alle Parameter zur Konfiguration von Ethereal werden im Script „`AUA_(3)_RUN.BAT`“ gesetzt (siehe folgenden Abschnitt).

Start-Script: AUA_(3)_RUN.BAT [oder AUA_RUN.BAT]

Der eigentliche Start der Aufzeichnung erfolgt über das Batch-File „`AUA_(3)_RUN.BAT`“, das beim Windows-Boot über die oben beschriebene Dienste-Installation aufgerufen wird. (Das Script wurde ursprünglich zum manuellen Start entwickelt und kann testhalber auch weiterhin manuell betrieben werden.)

Falls auf dem Windows-PC die Namens-Konvention „8+3“ aktiviert (verlangt) sein sollte, muss die Script-Datei umbenannt werden in „`AUA_RUN.BAT`“, und in der Registry-Datei „`AUA_(2)_Ethereal.REG.txt`“ muss der Datei-Name ebenfalls entsprechend geändert (nachgetragen) werden. Möglicherweise Ausschlag gebend ist der folgende Registry-Eintrag (mit Wert 1=ON statt 0=OFF):

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
NtfsDisable8dot3NameCreation = 0x00000001
```

Es werden für die AUA-Installation folgende Dateien geliefert:

- | | |
|--|--|
| AUA_(3)_RUN.BAT | → Die "eigentliche" Script-Datei |
| AUA_(3.1)_RUN_(Muster)__(mini)_.BAT | → Muster-Script "mini" = einfach |
| AUA_(3.2)_RUN_(Muster)__(midi)_.BAT | → Muster-Script "midi" = etwas anspruchsvoll |
| AUA_(3.3)_RUN_(Muster)__(maxi)_.BAT | → Muster-Script „maxi“ = für manuelle Tests |

Das Script „`AUA_(3)_RUN.BAT`“ setzt über Umgebungs-Variablen *erstens* Pfade (in denen **T**`Ethereal.exe` liegt und in denen die .DMP Trace-Files liegen) und *zweitens* den Namen des Sammel-Servers, zu dem später die Aufzeichnungs-Daten gesendet werden (`%AnalysisServerName%`; siehe hierzu auch: `AUA.ServerDatat.TXT`).



Analysis User Agent AUA Installation & Betrieb

Es stehen zwei verschiedene Varianten in Form von Muster-Scripts zur Auswahl:

→ Zum Betrieb im Ethereal-Programm-Verzeichnis `C:\Programme\Ethereal` :

```
AUA_(3.1)_RUN_(Muster)_(mini)_.BAT
```

→ Zum Betrieb in einem beliebigen anderen Verzeichnis, etwa: `C:\Programme\Ethereal.DMP-Files` :

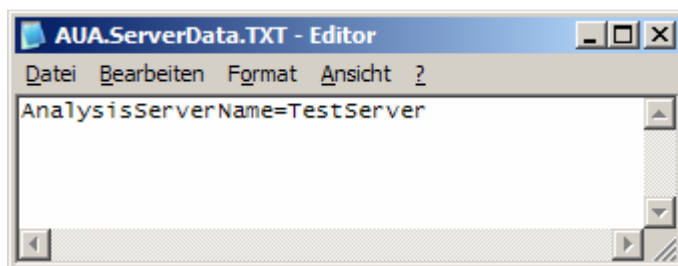
```
AUA_(3.2)_RUN_(Muster)_(midi)_.BAT
```

Gleich, welches Script verwendet wird, gelten die folgenden Maßgaben:

1. Die Zeile „set AnalysisServerName=SRVNAME“ muss editiert werden; statt „SRVNAME“ muss der echte Windows-Server-Name eingegeben werden; auf diesem Server muss das Share „AUAserver\$“ liegen.

Alternativ kann die Konfigurations-Datei „AUA.ServerData.TXT“ editiert werden mit dem Zeilen-Eintrag: „AnalysisServerName=SRVNAME“.

Es hat sich gezeigt, dass nicht immer die Umgebungs-Variable via „set“ erhalten bleibt. Die Einstellung über die Konfigurations-Datei ist daher im Zweifel sicherer.



2. Im Falle des Muster-Scripts „AUA_(3.2)_RUN_(Muster)_(midi)_.BAT“ muss der Verzeichnis-Name eingegeben werden, unter welchem die Aufzeichnungs-Daten (DMP-Files) abgespeichert werden sollen. Dies hat den einzigen Zweck, die DMP-Files nicht im „echten“ Ethereal-Programm-Verzeichnis abspeichern zu müssen (Grund: Übersichtlichkeit).
3. Ausgeführt (siehe REGISTRY-Parameter oben) wird ausschließlich das Script „AUA_(3)_RUN.BAT“. Wird eines der Muster-Scripts verwendet, muss es abgespeichert werden unter dem Namen „AUA_(3)_RUN.BAT“, und zwar in jedem Falle im Ethereal-Programm-Verzeichnis (das ist in der Regel: `C:\Programme\Ethereal`).

Folgend die zwei Muster-Scripts.

Die wirklich wichtigen Befehls-Zeilen sind **farblich hervorgehoben** worden.



Analysis User Agent AUA Installation & Betrieb

Der Aufruf von „TETHEREAL.exe“ erfolgt mit vielen Parametern.

Im Klartext kann eine von zwei Varianten genommen werden, was den Parameter „-i“ betrifft (für „Interface“, also die Netzwerk-Schnittstelle des Windows-PCs):

1. Win9x, WinME: Alte Windows-Systeme verwenden Interface-**NAMEN**.
2. Win2K, WinXP: Neue Windows-Systeme verwenden Interface-**NUMMERN**.

```
tetheréal -i CE3 -q -s 1518 -a filesize:2000 -b 100 -F libpcap -w AUA_capture_file_.dmp
tetheréal -i 1 -q -s 1518 -a filesize:2000 -b 100 -F libpcap -w AUA_capture_file_.dmp
```

Die Aufruf-Parameter insgesamt:

LAN-Interface	= -i = %PAR_i%
Quiet Operation	= -q = %PAR_q%
Frame Buffer Size	= -s = %PAR_s%
Trace File Size	= -a = %PAR_a%
Trace Files (total)	= -b = %PAR_b%
Trace File Name	= -w = %PAR_w%
Trace File Format	= -F = %PAR_F%

Die Parameter können entweder in der Befehls-Zeile **direkt** im Klartext gesetzt werden (Script „mini“) oder über Umgebungs-Variablen vor-deklariert und dann **indirekt** übergeben werden (Script „midi“), um bei manuellen Versuchen über den ECHO-Befehl darstellbar zu sein.



Analysis User Agent AUA Installation & Betrieb

Muster-Script = AUA_(3.1)_RUN_(Muster)_(mini)_.BAT :

```
:TETHEREAL_RUN.BAT
@echo off
cls

REM
REM Die Umgebungs-Variable %AnalysisServerName" wird vom Programm
REM AUA_Analysis_User_Agent.EXE abgefragt, um die DMP-Files kopieren zu koennen.
REM

set AnalysisServerName=SRVNAME

set

REM pause

If exist *.DMP del *.DMP

REM pause

tethereal -D

REM pause

:tethereal -i CE3 -q -s 1518 -a filesize:4000 -b 100 -F libpcap -w AUA_capture_file_.dmp
tethereal -i 1 -q -s 1518 -a filesize:4000 -b 100 -F libpcap -w AUA_capture_file_.dmp

REM pause

:ENDE
```



Analysis User Agent AUA Installation & Betrieb

Muster-Script = **AUA_(3.2)_RUN_(Muster)_(midi)_.BAT** :

```

:TETHEREAL_RUN.BAT
@echo on
cls

REM
REM Dieses Muster von "AUA_(3)_RUN.BAT" ist anpassungsfaehig, daher auch aufwaendiger.
REM Es ist geeignet für den Einsatz in einem *anderen* als dem Ethereal-Programm-Verzeichnis, etwa:
REM C:\Programme\Ethereal.DMP-Files
REM

REM

REM (1)
REM
REM Die Umgebungs-Variable %AnalysisServerName" wird vom Programm
REM AUA_Analysis_User_Agent.EXE abgefragt, um die DMP-Files kopieren zu koennen.
REM

set AnalysisServerName=SRVNAME

REM
REM (2)
REM
REM Die Capture-Files des Vortages löschen (sofern vorhanden):
REM

If exist *.DMP del *.DMP

REM pause

REM
REM (3)
REM
REM Die Pfade setzen ...
REM ... für das Ethereal-Programm-Verzeichnis, z.B. C:\Programme\Ethereal
REM ... für das .DMP Trace-File Verzeichnis, z.B. C:\Programme\Ethereal.DMP-Files
REM

set PATH_EXE=C:\Programme\Ethereal
set PATH_TRC=C:\Programme\Ethereal

If exist %PATH_EXE%\TETHEREAL.EXE cd %PATH_EXE%

If not exist C:\Programme\Ethereal.DMP-Files\NUL md C:\Programme\Ethereal.DMP-Files
If exist C:\Programme\Ethereal.DMP-Files\NUL set PATH_TRC=C:\Programme\Ethereal.DMP-Files

REM
REM (4)
REM
REM Bei automatischem Dienst-Aufruf ist der folgende Befehl
REM bedeutungslos.
REM

tethereal -D

```



Analysis User Agent AUA Installation & Betrieb

```
REM
REM (5)
REM
REM Die TEthereal-Parameter setzen.
REM
REM ACHTUNG zu Parameter "PAR_i" (= Interface):
REM
REM ALTE Systeme (Win9x,WinME) verwenden Interface-Namen.
REM NEUE Systeme (Win2K,WinXP) verwenden Interface-Nummern.
REM
REM

:SET
set PAR_i=-i 1
set PAR_q=-q
set PAR_s=-s 1518
set PAR_a=-a filesize:4000
set PAR_F=-F libpcap
set PAR_b=-b 100
set PAR_w=-w AUA_capture_file_.dmp

REM
REM (6)
REM
REM In das Verzeichnis der .DMP Trace-Files wechseln,
REM von dort aus dann TEthereal.exe aufrufen und das Capture starten:
REM

cd %PATH_TRC%
cd

%PATH_EXE%\tethereal %PAR_i% %PAR_q% %PAR_s% %PAR_a% %PAR_b% %PAR_F% %PAR_w% >> t_log.txt

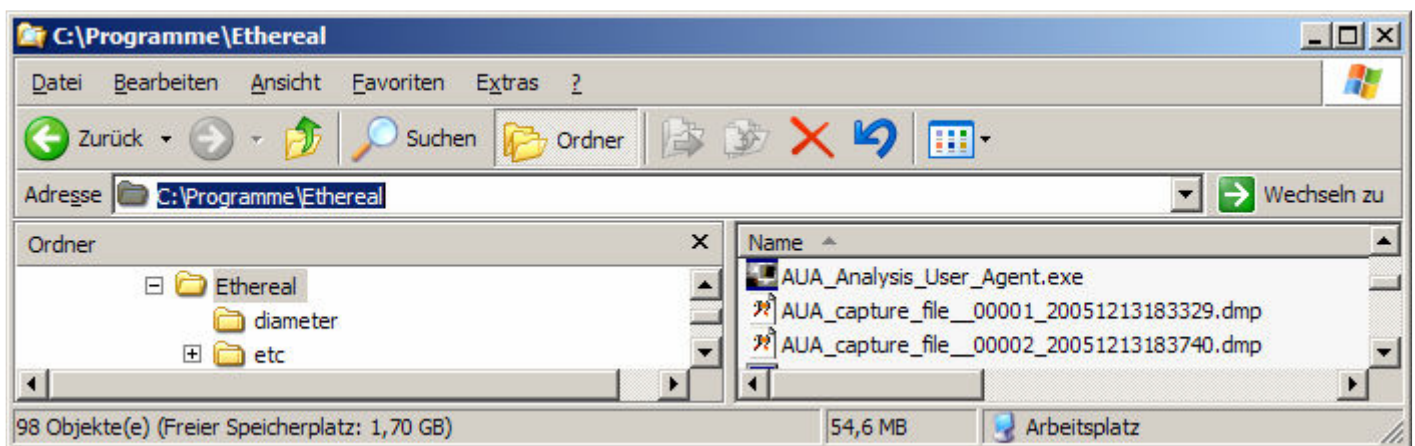
:ENDE
```



Analysis User Agent AUA Installation & Betrieb

Das Muster-Script `AUA_(3.3)_RUN_(Muster)_(maxi)_.BAT` dient lediglich ausführlichen manuellen Tests.

Das Ergebnis der TETHEREAL-Aufzeichnungen sind Dateien (engl.: *trace files*), die im Namen zusätzlich eine Datei-Nummer, das Tagesdatum und sowie die Uhrzeit führen:



Hierdurch kann später in den Messdaten schnell(er) die vom Anwender bemängelte Störung identifiziert werden, sofern der Anwender eine Uhrzeit angegeben hat.

Siehe hierzu weiter unten: „**Das Anwender-Modul (AUA_Analysis_User_Agent.exe)**“

Mit dieser Installation läuft sodann der TETHEREAL-Dienst im Hintergrund.
Sämtliche Datenkommunikation des Client-PCs wird in .DMP-Files aufgezeichnet.



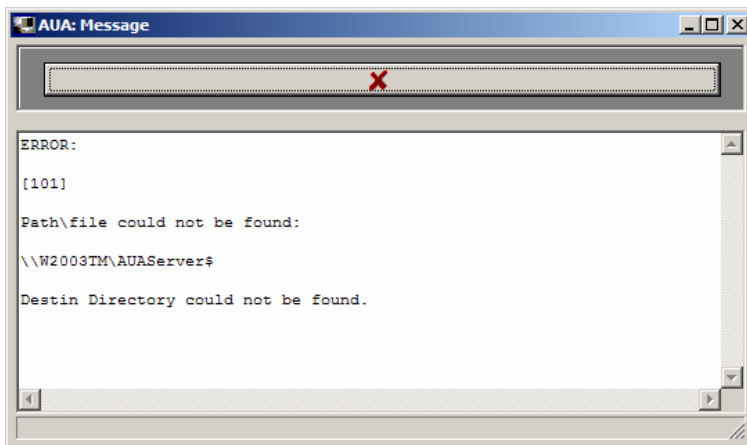
Analysis User Agent AUA Installation & Betrieb

AUA-Server

Die Daten werden an ein Windows-Share gesendet, das einen festgelegten Freigabe-Namen haben muss.
Siehe hierzu: Abschnitt „AUA-Server“ weiter unten.

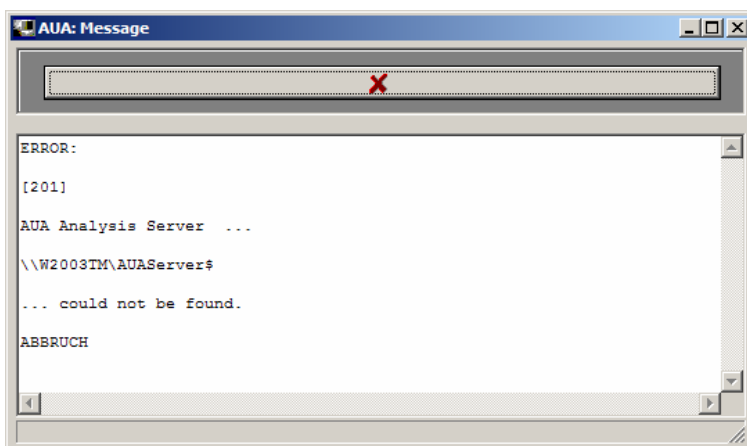
AUA-Client

Das Modul „AUA_Analysis_User_Agent.exe“ reagiert für den Fall, dass der AUA-Server nicht erreichbar sein sollte, mit einer Fehler-Meldung (mehr hierzu: siehe unten).



OBEN: Fehler-Meldung beim Aufruf des *AUA-Client-Agents*.

UNTEN: Fehler-Meldung bei START des Kopier-Vorgangs durch den *AUA-Client-Agent*.





AUA-Client: Das Anwender-Modul (AUA_Analysis_User_Agent.exe)

Dies ist das für den Anwender sichtbare Modul mit Bediener-Oberfläche, Eingabe-Möglichkeiten und [SEND]-Button.

Installation

In das Verzeichnis, in Trace-Files (.DMP) liegen, müssen die Dateien des „Analysis User Agents“ hinein kopiert werden:

AUA_Analysis_User_Agent.exe

AUA.Applications.TXT	(ist vom Kunden mit der Liste der Applikationen zu füllen)
AUA.Contact.TXT	(ist vom Kunden mit Kontakt-Daten des Help-Desks zu füllen)
AUA.Help.TXT	(gehört zur Lieferung des Herstellers)
AUA.UserData.TXT	(wird erzeugt, falls nicht vorhanden)

ACHTUNG: Je nach Variante des Scripts „**AUA_(3)_RUN.BAT**“ kann das Verzeichnis, in dem die Trace-Files (.DMP) liegen, identisch sein mit dem „Ethereal“-Programm-Verzeichnis – oder eben auch nicht, wenn für die Trace-Files ein separates Verzeichnis angegeben wurde. In jedem Falle muss „**AUA_Analysis_User_Agent.exe**“ im Trace-File-Verzeichnis liegen.

Sodann muss dafür gesorgt werden, dass der Anwender über den Windows-[START]-Button den „Analysis User Agent“ starten kann.

Eine mögliche Variante wäre, eine Link-Datei in das „StartMenü“-Verzeichnis des/der Anwender zu kopieren:



Analysis User Agent AUA Installation & Betrieb

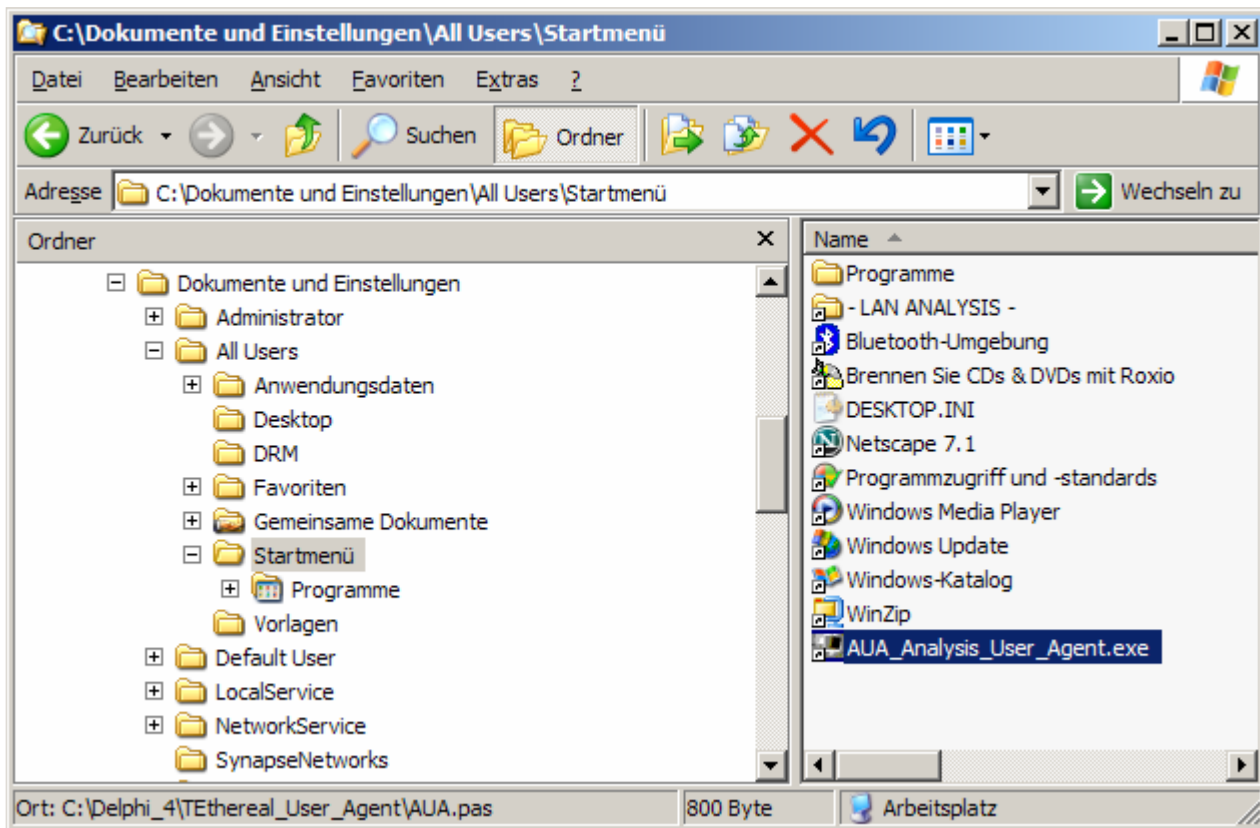


Abbildung oben:

Die LINK-Datei sollte noch umbenannt werden in „AUA Analysis User Agent“ (siehe nächste Abbildung mit START-Menü).

Abbildung unten:

Der „Analysis User Agent“ wird im START-Menü angeboten.



Analysis User Agent AUA Installation & Betrieb

The screenshot shows a Windows XP Professional desktop. The Start menu is open, displaying various options such as 'Windows-Katalog', 'WinZip', 'Analysis User Agent (AUA)', 'Programme', 'Dokumente', 'Einstellungen', 'Suchen', 'Hilfe und Support', and 'Ausführen...'. At the bottom of the Start menu, there are options to 'TraceMagic abmelden...' and 'Computer ausschalten...'. The taskbar at the bottom shows several open applications, including a Netscape browser window. The browser window is titled 'download -> Software - Netscape' and displays the website 'www.synapse-ssc.de/index.php?id=14'. The website content includes the Synapse:Networks logo, a navigation menu with 'Literatur', 'Support', 'Wir über uns', 'Kontakt', and 'Shortcuts', and a section titled 'Programm (Synapse:Networks)'. The text in the browser window describes the program's functionality, mentioning 'Ethereal' and 'Capture-Engine "tethereal.exe"'. The system clock in the bottom right corner shows the time as 12:11.



Bedienung durch den Anwender

Erster Aufruf

Beim ersten Aufruf durch den Anwender sollte dieser seine persönlichen Angaben im dafür vorgesehenen Register-Blatt vornehmen (siehe Abbildung unten).

Die eingegebenen Daten werden gespeichert in der folgenden Datei:

AUA.UserData.TXT

Für spätere Versionen des „Analysis User Agents“ ist geplant, diese Angaben in der Windows-Registry zu speichern, unter anderem zu dem Zweck, mehreren bzw. wechselnden Anwendern des PCs ihr eigenes AUA-Profil zu verschaffen.

Analysis User Agent - v0.4 (2005-12-12)

Analysis User Agent X EXIT

! | Guten Tag! | Benutzer-Angaben | Fehler-Beschreibung | Analyse-Daten übertragen | .DMP | [DEBUG]

Angaben zum PC-System:

ComputerName = LAPTOP_F3

UserName = TraceMagic

AnalysisServerName = LAPTOP_F3

Angaben zum Benutzer:

NAME, Vorname = WALTHER, Frank

Telefon-Nummer = +49.2228.9138.0

eMail-Adresse = f.walther@synapse.de

Abteilungs-Kennung = LAN Analysis

Räumlichkeit (Zimmer-Nummer) = N/A

Diese Angaben werden bei der Versendung der Analyse-Aufzeichnungen mit übertragen, um den Vorgang zuordnen zu können.

Die Angaben dienen nur der Fehler-Behandlung und werden ansonsten nicht weiter verwendet.

2005-12-12 12:13:48



Analysis User Agent AUA Installation & Betrieb

Aufruf zum Zweck der Versendung von Analyse-Aufzeichnungsdaten

Bei Auftreten einer PC-Störung sollte der Anwender wie folgt vorgehen:

1. Start von „Analysis User Agent“

Über den Link (das Icon) im START-Menü von Windows wird der „Analysis User Agent“ gestartet.

2. Überprüfung der Anwender-Angaben

Die Anwender-Angaben (Name, Telefon, etc) sollten überprüft werden.

3. Angaben zum Fehler bzw. zur beobachteten Störung

Die betroffene(n) Applikation(en) sollten angewählt und weitere Angaben eingegeben werden.

4. Versendung der Daten

Die Aufzeichnungs-Daten sowie die Benutzer-Angaben werden über den [START]-Button verschickt.



Analysis User Agent AUA Installation & Betrieb

Angaben des Anwenders zur beobachteten Störung

Die Angaben des Benutzers zur vorliegenden Störung erfolgen in drei Schritten in dem Registerblatt „Fehler-Angaben“:

Analysis User Agent - v0.4 (2005-12-12)

Analysis User Agent X EXIT

! | Guten Tag! | **Benutzer-Angaben** | Fehler-Beschreibung | Analyse-Daten übertragen | .DMP | [DEBUG]

Angaben zum Fehler-Ereignis

Betroffene Anwendungen

Bitte machen Sie hier Angaben zu den betroffenen Anwendungen und zu der Schwere des Fehlers.

- MS Windows / Betriebssystem
- MS Office (Word, Excel, PowerPoint, etc.)
- MS Project
- MS Access
- Acrobat Reader
- Internet/Mail
- Internet/Web
- Visio
- VMWare

Bedeutsamkeit --> [wenig << BEDEUTSAM >> sehr]

Eilbedürftigkeit --> [wenig << EILIG >> sehr]

--WEITERE--ANGABEN--

(Hier ist Raum für weitere Angaben.)

2005-12-12 12:21:46



Analysis User Agent AUA Installation & Betrieb

Auswahl der betroffenen Applikation(en)

Der Anwender setzt per Mausclick Kreuze in der angebotenen Liste der Applikationen.

Diese Liste wird bei jedem Programm-Start des „Analysis User Agents“ geladen aus der folgenden Datei:

`AUA.Applications.TXT`

Sollte eine Applikation nicht in dieser Liste stehen, muss sie in der Datei `AUA.Applications.TXT` nachgetragen werden.

MS Windows / Betriebssystem
 MS Office (Word, Excel, PowerPoint, etc.)
 MS Project
 MS Access
 Acrobat Reader
 Internet/Mail
 Internet/Web
 Visio
 VMWare

Angabe der Kriterien „Bedeutsamkeit“ / „Eilbedürftigkeit“

Über zwei Schieberegler erfolgt die Angabe, wie sehr der durch die Störung betroffene Vorgang als „bedeutsam“ (wichtig, unerlässlich) und die Beseitigung der Störung als „eilig (dringlich)“ eingestuft wird.

Nicht alles, was eilig ist (also nur wenig Zeit zur Reaktion lässt), ist zugleich auch wirklich bedeutsam. Nicht alles, was für ein Unternehmen wirklich bedeutsam ist, ist auch eilig (sondern hat noch Zeit).

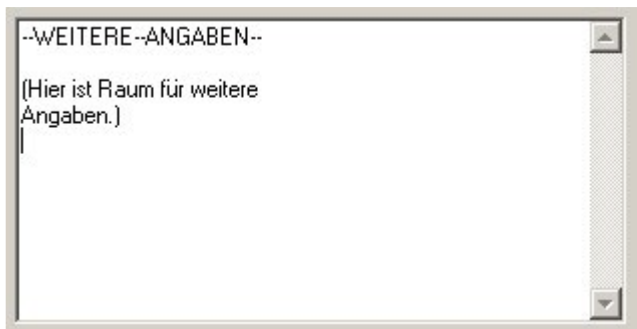
Bedeutsamkeit --> [wenig << BEDEUTSAM >> sehr]
Eilbedürftigkeit --> [wenig << EILIG >> sehr]



Analysis User Agent AUA Installation & Betrieb

Eingabe beliebiger Zusatz-Angaben des Anwenders

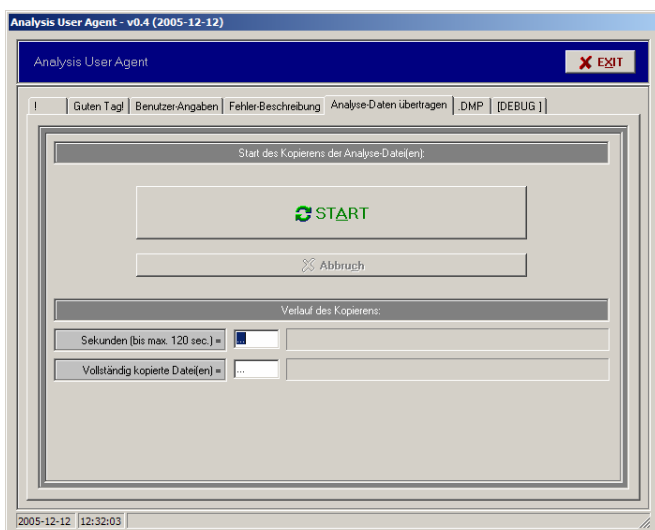
Alle weiteren Angaben macht der Anwender in dem Textfeld unten rechts. Hier sollten Uhrzeit, Hergang etc möglichst genau geschildert werden.



Versendung der Angaben und Aufzeichnungs-Daten

Sind alle Eingaben und Angaben gemacht, werden per Mausklick auf den [START]-Button die Daten versendet (entspricht einem „SEND“-Button).

Sodann hat das Programm max. 10 Minuten (= 600 Sekunden) Zeit, die Daten zu versenden. Ist diese Zeit ohne Übertragung abgelaufen, muss von einer Störung ausgegangen werden.

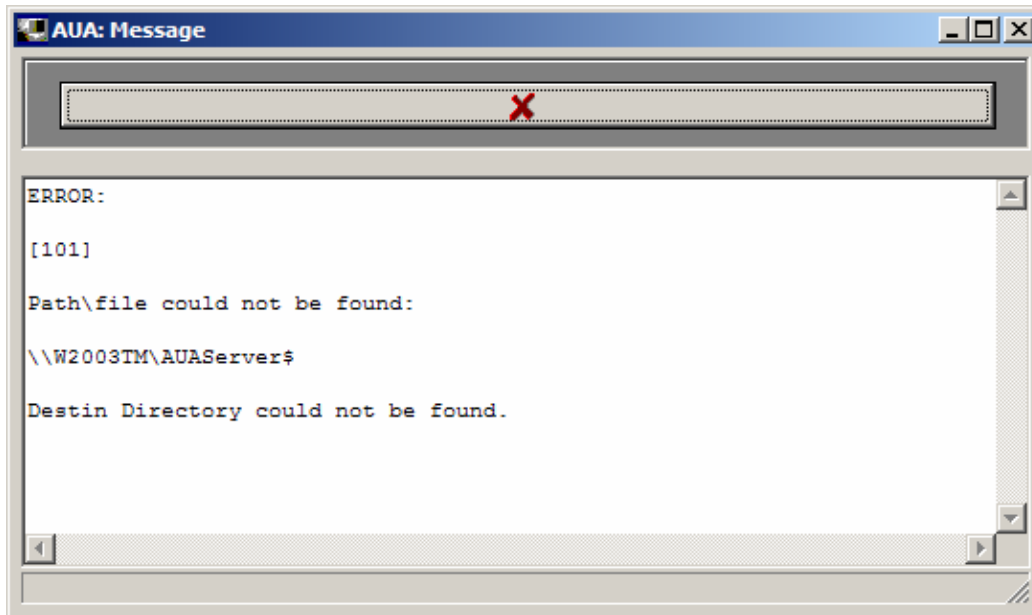


Der „Analysis User Agent“ kopiert nicht nur die Anwender-Angaben und Aufzeichnungs-Daten (.DMP), sondern erzeugt auf dem AUA-Server auch Index-Dateien, die dem Administrator erlauben, schnell Zugriff auf die Daten zu erhalten (siehe unten: „AUA-Server“).



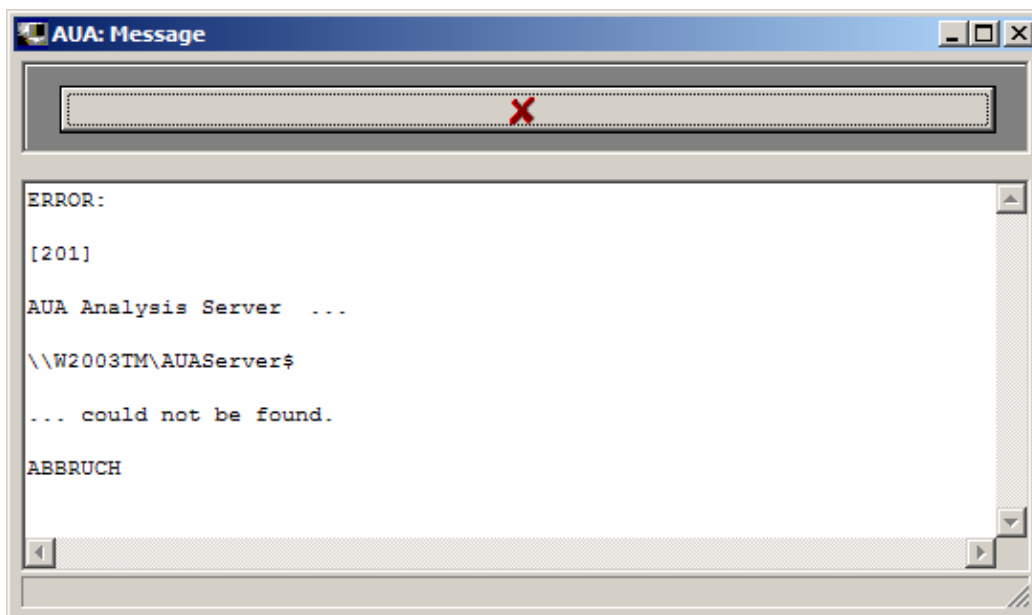
Wenn der AUA-Server nicht erreicht wird: Fehler-Meldung

Das Modul „AUA_Analysis_User_Agent.exe“ reagiert für den Fall, dass der AUA-Server nicht erreichbar sein sollte, mit einer Fehler-Meldung (mehr hierzu: siehe unten).



OBEN: Fehler-Meldung beim Aufruf des *AUA-Client-Agents*.

UNTEN: Fehler-Meldung bei START des Kopier-Vorgangs durch den *AUA-Client-Agent*.





Analysis User Agent AUA Installation & Betrieb

In diesen Fällen der Nicht-Erreichbarkeit des Servers sollten zwei mögliche Fehlerquellen ausgeschlossen werden:

- Die Umgebungs-Variable `%AnalysisServerName%` ist nicht vorhanden (obwohl sie ggf. per Batch-Script gesetzt wurde).

Und/Oder:

- Die Konfigurations-Variable „`AnalysisServerName`“ in der Datei „AUA.ServerData.TXT“ wurde nicht angegeben.

Siehe hierzu die folgenden Abschnitte.

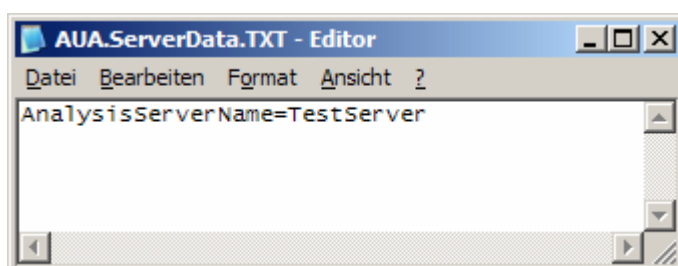
AUA.ServerData.TXT

Der Analysis User Agent ist darauf angewiesen, entweder den **NAMEN** oder die **IP-ADRESSE** des *AUA-Servers* zu kennen, um die *Capture Files* überstellen zu können.

Ein Weg, den Server-Namen oder die Server-IP-Adresse mitzuteilen, ist die Umgebungs-Variable „`AnalysisServerName`“; damit der *AUA Analysis User Agent* aber diese Umgebungs-Variable auslesen kann, muss sie über die gesamte Zeit im Windows-System gegeben sein.

Alternativ kann die Konfigurations-Datei „`AUA.ServerData.TXT`“ editiert werden mit dem Zeilen-Eintrag: „`AnalysisServerName=SRVNAME`“ (statt „`SRVNAME`“ muss der tatsächliche Name eingesetzt werden).

Es hat sich gezeigt, dass nicht immer die Umgebungs-Variable via „`set`“ erhalten bleibt. Die Einstellung über die Konfigurations-Datei ist daher im Zweifel sicherer.





AUA-Server: Der Trace-File-Index / Das Index-Viewer-Modul

Server-Share: %AnalysisServerName% - AUAServer\$

Die Daten werden an ein Windows-Share gesendet, das einen fest stehenden Freigabe-Namen haben muss:

AUAServer\$

Bis auf Weiteres steht der Name dieses Server-Shares fest und kann nicht geändert werden (ist im AUA-Programm „hart kodiert“); eine Konfigurationsfähigkeit brächte die Gefahr mit sich, dass Anwender die Messdaten-Versendung umleiten fremde bzw. illegale Rechner.

Der Name des Servers selbst wird vom „Analysis User Agent“ (Client-Modul) abgefragt aus der folgenden lokalen Umgebungs-Variablen:

%AnalysisServerName%

Es ist zwingend erforderlich, dass diese Umgebungs-Variable zuvor über ein Script (siehe oben: RUN.BAT) mit einem Wert gefüllt wird (das ist: der Name des Servers, auf welchem das Share gegeben ist):

```
set AnalysisServerName=SRVNAME
```

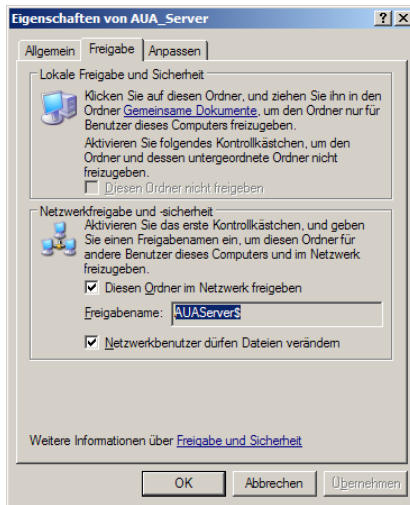
Somit ergibt sich bei Auflösung der Variablen %AnalysisServerName% in den Klartext folgender Pfad:

\\SRVNAME\AUAServer\$

Nach diesem UNC-Pfad sucht der „Analysis User Agent“ (Client-Modul), um die Messdaten abzulegen.



Analysis User Agent AUA Installation & Betrieb





Analysis User Agent AUA Installation & Betrieb

Server-Modul (AUA Server Index Viewer.exe)

Der „Analysis User Agent“ kopiert nicht nur die Anwender-Angaben und Aufzeichnungs-Daten (.DMP), sondern erzeugt auf dem AUA-Server auch Index-Dateien, die dem Administrator erlauben, schnell Zugriff auf die Daten zu erhalten.

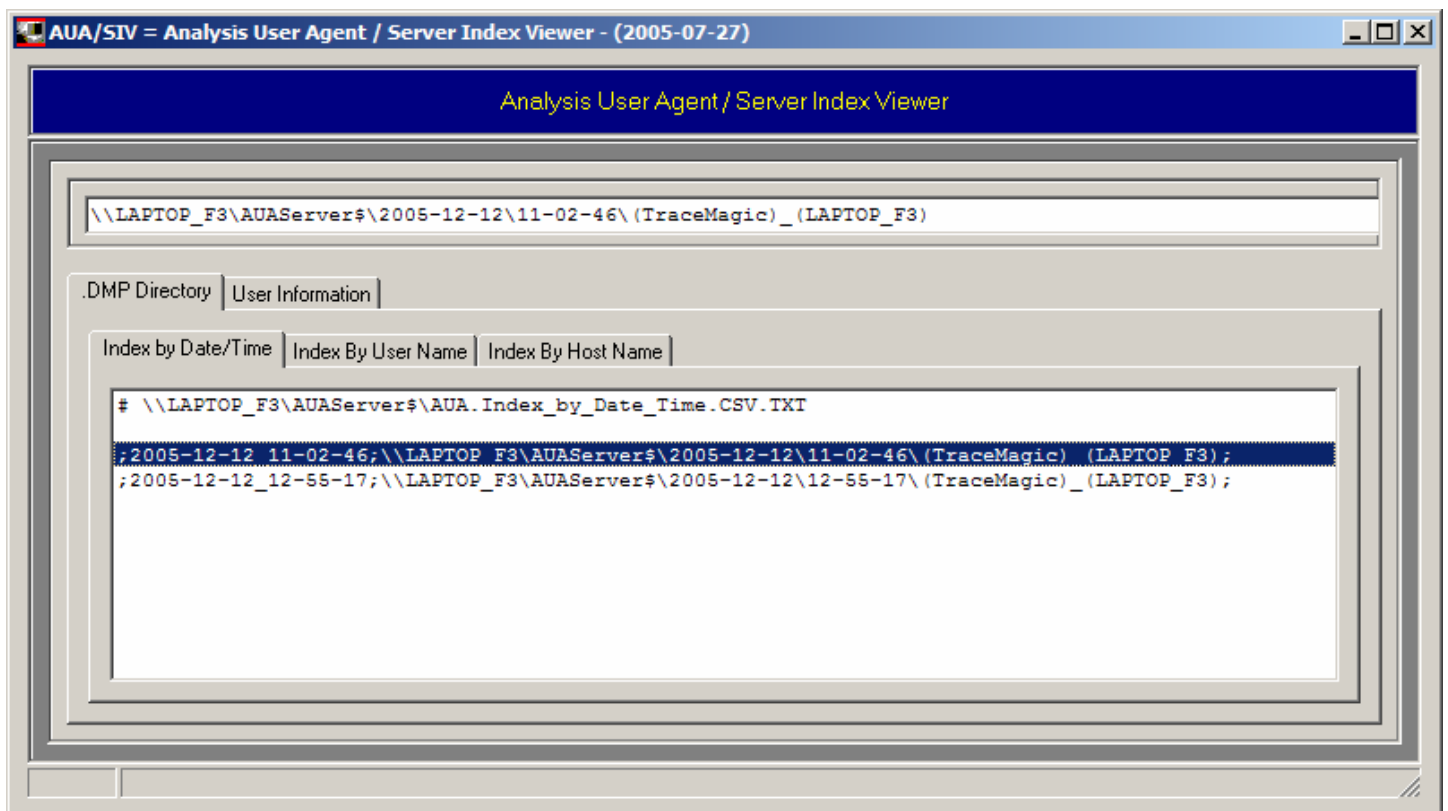
Es sind dies die folgenden Dateien:

```
AUA.Index_by_Date_Time.CSV.TXT
AUA.Index_by_Host_Name.CSV.TXT
AUA.Index_by_User_Name.CSV.TXT
```

(Sind diese drei Dateien nicht vorab vorhanden, werden sie vom AUA-Client-Modul erzeugt.)

Diese drei Index-Dateien können über das den **AUA-Server-Index-Viewer** ausgelesen werden.

Hierzu muss die Programm-Datei „**AUA_Server_Index_Viewer.exe**“ ins Haupt-Verzeichnis „**AUAServer\$**“ kopiert werden (hier liegen auch die Index-Dateien).



Mit Mausclick auf eine der CSV-Zeilen (CSV=Comma Separated Values) wird in der Pfad-Anzeige oben der Pfad im AUAServer-Verzeichnis angezeigt, unter welchem die jeweiligen Anwender-Daten zu finden sind.



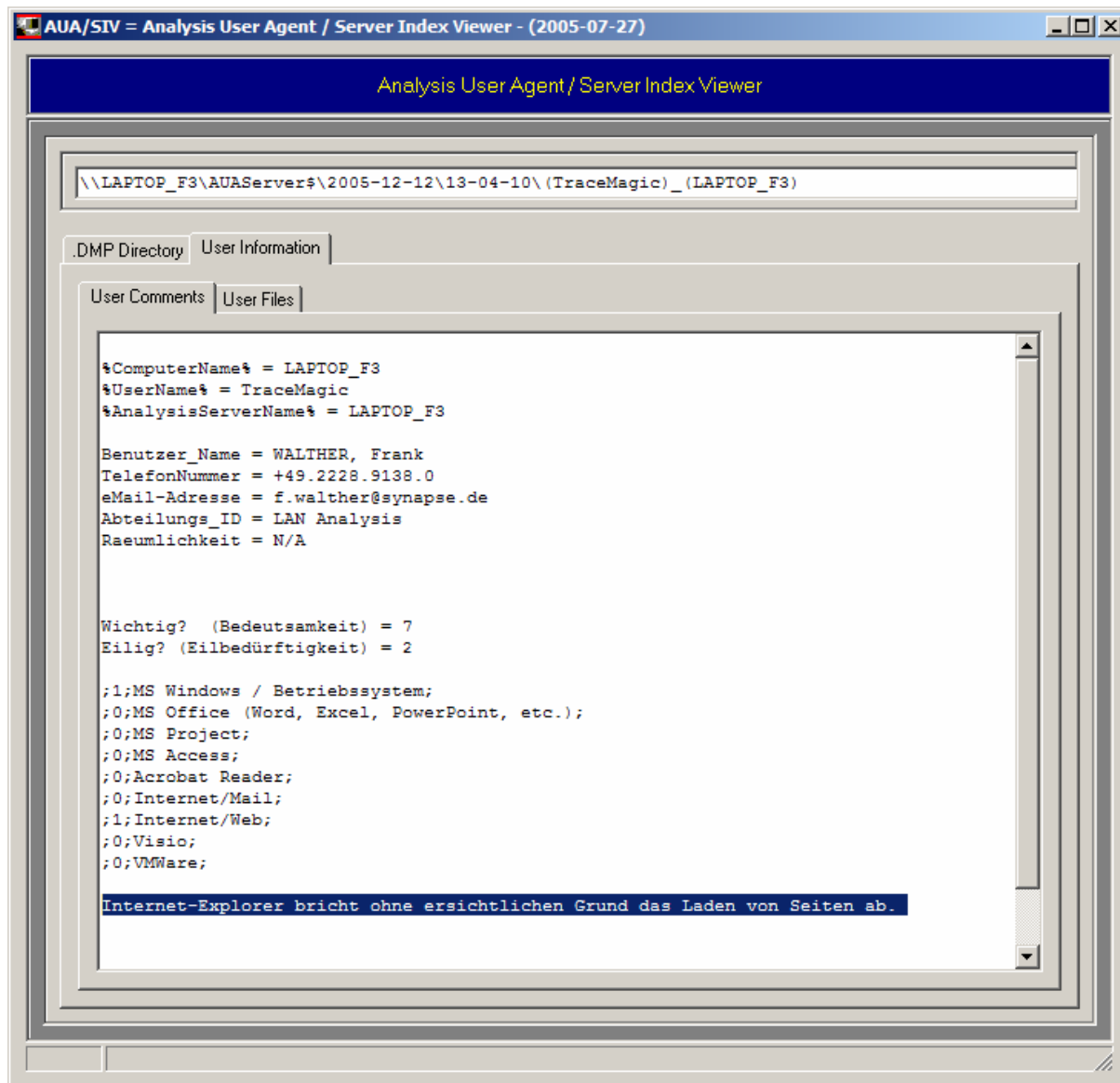
Analysis User Agent AUA Installation & Betrieb

Über die drei Register-Blätter kann sortiert werden:

- nach Datum/Uhrzeit,
- nach Anwender-Name,
- nach PC-Name.

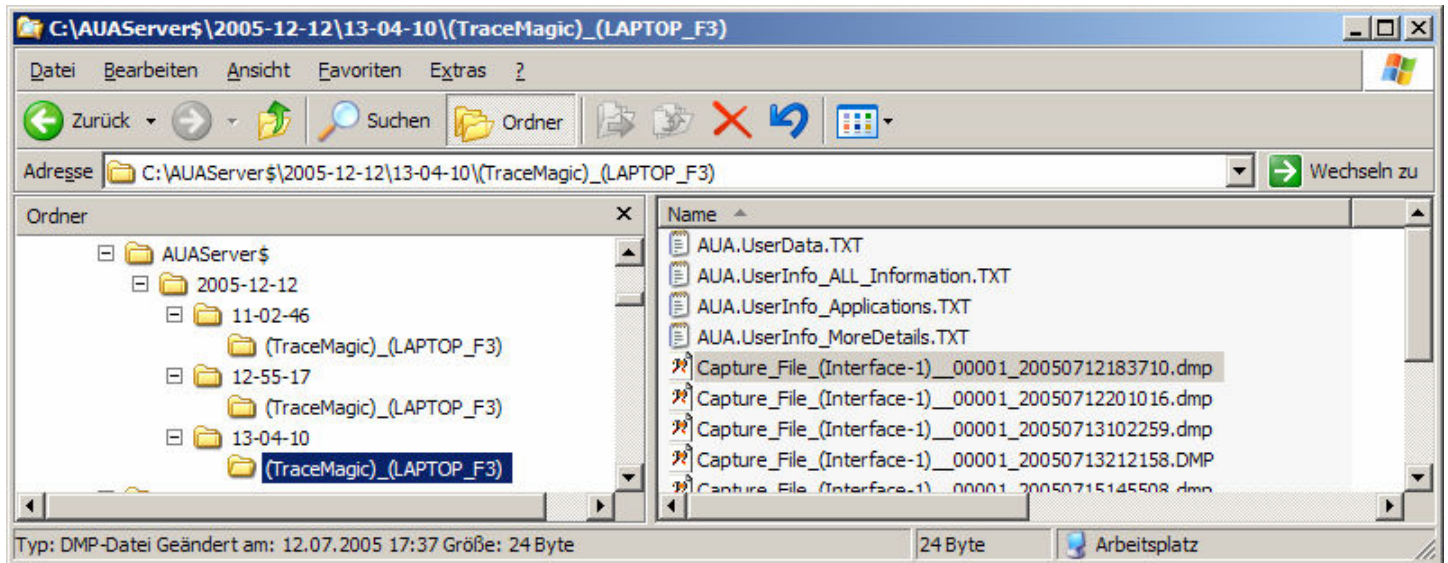
Mit einem Maus-Doppelklick auf die jeweilige CSV-Zeile öffnet sich automatisch das zweite Register-Blatt „User Information“, und es werden die vom Anwender eingegebenen Angaben dargestellt. Im Register-Blatt „User Files“ werden die übertragenen Dateien aufgelistet.

```
AUA.UserData.TXT
AUA.UserInfo_ALL_Information.TXT
AUA.UserInfo_Applications.TXT
AUA.UserInfo_MoreDetails.TXT
```





Analysis User Agent AUA Installation & Betrieb



Die im Benutzer-Verzeichnis liegenden Aufzeichnungs-Dateien (.DMP Trace-Files) sollten sodann ausgewertet werden; hierzu empfiehlt Synapse:Networks GmbH den Einsatz des Analyse-Experten-Systems „Trace:Magic“ (www.tracemagic.net).



Synapse:Networks GmbH

© 2005 Frank R. Walther / Synapse:Networks GmbH / www.synapse.de / info@synapse.de

<http://www.synapse.de/>
<http://www.tracemagic.net/>