LAN Analyzer / Capture Engines

Diskussion: Aufzeichnung von Messdaten mit Blick auf Kompatibilität zu TraceMagic

Wird die automatische Verarbeitung von Aufzeichnungen eines LAN-Datenverkehrs mittels **Trace:Magic** angestrebt, sollte gründlich betrachtet werden, wie die MessDaten bzw. deren Aufzeichnungen zu Stande kommen bzw. welche Produkte dafür in Frage kommen.

Die folgende Diskussion betrachtet Verfahrensweisen und Produkte.

Die Wertungen und Empfehlungen ergeben sich aus der Sicht einer bestmöglichen Datenverarbeitung bzw. Analyse mittels **Trace:Magic**.

Einsätze außerhalb dieses Zwecks könn(t)en im Einzelfall zu anderen Wertungen führen und wären insofern dann subjektiv.

Allgemein gilt seit Sommer/Herbst 2006, dass für den Zweck späterer Auswertung mittels **Trace:Magic** die Daten-Aufzeichnung mit dem LAN-Analyzer **Trace:Commander** von Synapse:Networks betrieben werden sollte.

Trace Commander → .DMP → TRACE:MAGIC

Der Schritt, nach einem Experten-System zur Messdaten-Auswertung ein Experten-Tool zur Messdaten-Aufzeichnung zu entwickeln, war nur folgerichtig und setzt Anwendern bzw. Kunden nunmehr ohne Kosten in die Lage, beliebige Messpunkte abzugreifen und die LAN-Daten aufzuzeichnen.

Trace:Commander arbeitet im Hintergrund mit der *Capture-Engine* der *Wireshark*-Suite (siehe unten) und nutzt folglich das TcpDump/Wireshark-Format, steuert aber den *Capture*-Prozess mit eigener Logik und bietet Funktionen, die insbesondere für Dauer-Aufzeichnungen extrem wichtig sind und anderswo am Markt nicht (oder nur bedingt) aufzufinden sind.

Heidesheim/Rolandseck, Januar 2007

Frank R. Walther

Synapse:Networks GmbH
Frank R. Walther
Geschäftsführer

INHALT

Welche Capture Engines (Aufzeichnungs-Systeme) passen zu Trace:Magic – und warum ?

Trace:Magic ist eine Software zur automatischen Auswertung von MessDaten, genauer: von aufgezeichneten Datenübertragungen eines lokalen Netzwerks (LAN).

Trace:Magic zeichnet den Datenverkehr eines LANs nicht selber auf, sondern wertet nur die Aufzeichnungen anderer Systeme aus.

Diese Aufzeichnungs-Systeme wurden (und werden) noch als „LAN Analyzer" bezeichnet; inzwischen setzt sich der eher neutrale Begriff der „Capture Engine" durch (was nicht wörtlich, aber sinngemäß etwa mit „Aufzeichnungs-System" übersetzt werden könnte).

Zwecks größtmöglicher Aussicht auf verwertbare Ergebnisse ist sicher zu stellen, dass die Daten-Aufzeichnungen mit Rücksicht auf die spätere Verarbeitung durch **Trace:Magic** erfolgen.

Daher stellt sich die Frage: Welche *Capture Engine* ist tauglich mit Blick auf **Trace:Magic**?

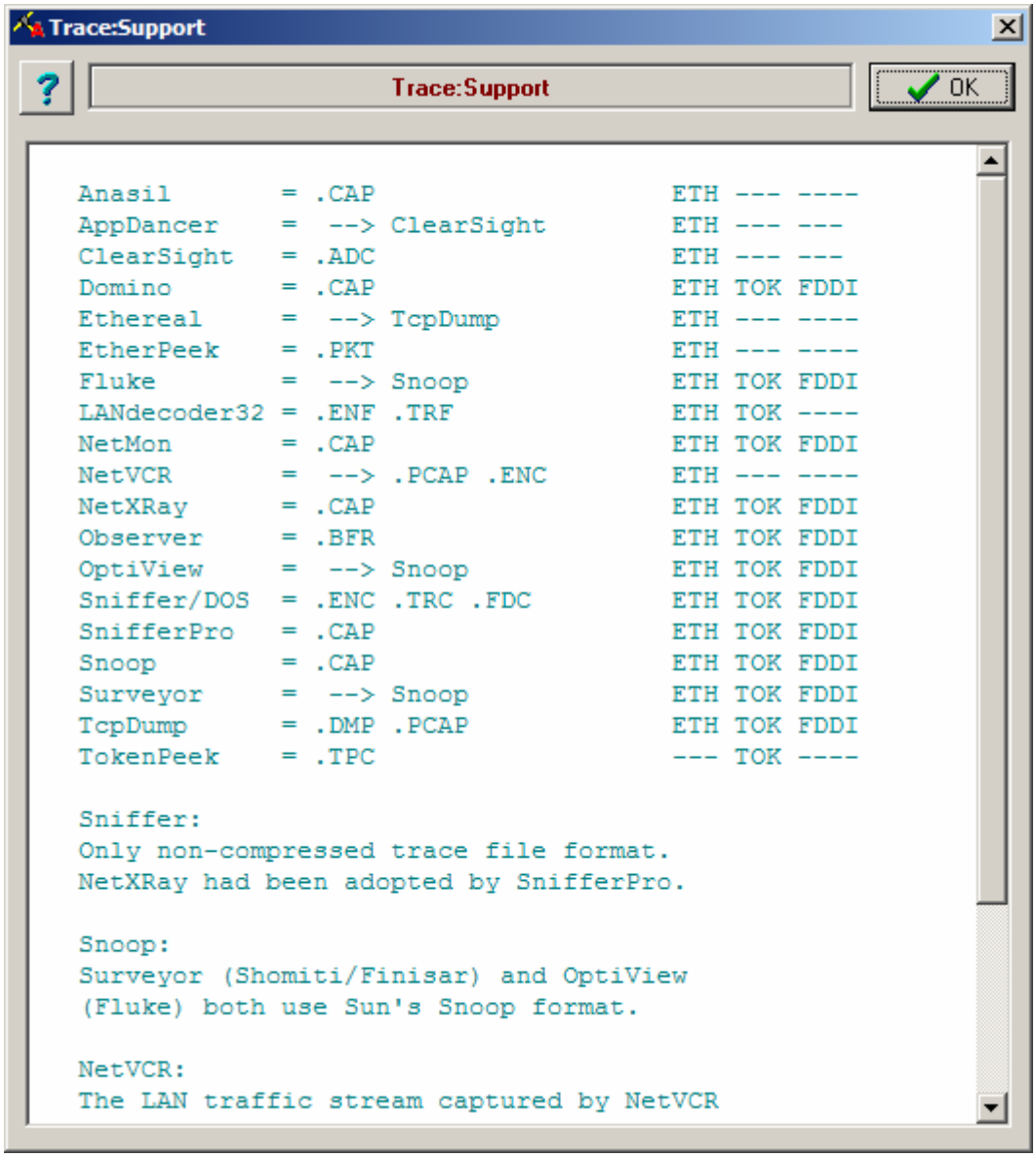
Unterstützte Aufzeichnungs-Formate

Folgende Aufzeichnungs-Formate werden unterstützt (Produkt, Datei-Endung, LAN):

```
Anasil       = .CAP                  ETH --- ----
AppDancer    =  --> ClearSight       ETH --- ---
ClearSight   = .ADC                  ETH --- ---
Domino       = .CAP                  ETH TOK FDDI
Ethereal     =  --> TcpDump          ETH --- ----
EtherPeek    = .PKT                  ETH --- ----
Fluke        =  --> Snoop            ETH TOK FDDI
LANdecoder32 = .ENF .TRF             ETH TOK ----
NetMon       = .CAP                  ETH TOK FDDI
NetVCR       =  --> .PCAP .ENC       ETH --- ----
NetXRay      = .CAP                  ETH TOK FDDI
Observer     = .BFR                  ETH TOK FDDI
OptiView     =  --> Snoop            ETH TOK FDDI
Sniffer/DOS  = .ENC .TRC .FDC        ETH TOK FDDI
SnifferPro   = .CAP                  ETH TOK FDDI
Snoop        = .CAP                  ETH TOK FDDI
Surveyor     =  --> Snoop            ETH TOK FDDI
TcpDump      = .DMP .PCAP            ETH TOK FDDI
TokenPeek    = .TPC                  --- TOK ----

Sniffer:
Only non-compressed trace file format.
NetXRay had been adopted by SnifferPro.

Snoop:
Surveyor (Shomiti/Finisar) and OptiView
(Fluke) both use Sun's Snoop format.
```


Trace:Support
Trace:Support
OK
Anasil = .CAP ETH --- ----
AppDancer = --> ClearSight ETH --- ---
ClearSight = .ADC ETH --- ---
Domino = .CAP ETH TOK FDDI
Ethereal = --> TcpDump ETH --- ----
EtherPeek = .PKT ETH --- ----
Fluke = --> Snoop ETH TOK FDDI
LANdecoder32 = .ENF .TRF ETH TOK ----
NetMon = .CAP ETH TOK FDDI
NetVCR = --> .PCAP .ENC ETH --- ----
NetXRay = .CAP ETH TOK FDDI
Observer = .BFR ETH TOK FDDI
OptiView = --> Snoop ETH TOK FDDI
Sniffer/DOS = .ENC .TRC .FDC ETH TOK FDDI
SnifferPro = .CAP ETH TOK FDDI
Snoop = .CAP ETH TOK FDDI
Surveyor = --> Snoop ETH TOK FDDI
TcpDump = .DMP .PCAP ETH TOK FDDI
TokenPeek = .TPC --- TOK ----
Sniffer:
Only non-compressed trace file format.
NetXRay had been adopted by SnifferPro.
Snoop:
Surveyor (Shomiti/Finisar) and OptiView
(Fluke) both use Sun's Snoop format.
NetVCR:
The LAN traffic stream captured by NetVCR

Einordnung / Kritik

Es folgt eine Kritik der unterstützten Analyzer bzw. ihrer Aufzeichnungs-Formate.

Diese Kritik erfolgt immer aus Sicht einer möglichen Verarbeitung der aufgezeichneten LAN-Daten mittels **Trace:Magic** .

Anasil (.CAP) (ETH)

Anasil ist ein kaum verbreitetes Produkt eines kaum bekannten Herstellers.

Für den Einsatz im Sinne von **Trace:Magic** spielt es keine Rolle.

AppDancer/ClearSight (.ADC) (ETH)

Der „ClearSight"-Analyzer (vormals: AppDancer) ist für Echtzeit-Betrachtungen einiger Applikations-Vorgänge interessant, etwa zur Nachvollziehen einzelner Aktionen eines Anwendungs-PCs.

Für den Einsatz im Sinne von **Trace:Magic** spielt er keine Rolle.

Domino (.CAP) (ETH,TOK,FDDI)

Der "Domino"-Analyzer von Acterna (Wavetek-Wandel-Goltermann) hatte eine Zeit lang Beachtung im Markt gefunden, spielt aber heute keine wesentliche Rolle mehr. Die Hardware ist im Gigabit-Umfeld noch u.U. interessant; die Möglichkeiten der Software sind bei diesen Preisen jedoch zu begrenzt.

Das Aufzeichnungs-Format wird in **Trace:Magic** nicht weiter gepflegt; im Falle von Veränderungen gegenüber dem z.Zt. implementierten Format kann eine Unterstützung nicht als sicher angesehen werden.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt keine Rolle.

Ethereal (.DMP,.PCAP) (ETH,TOK,FDDI)

Seit 2006 ist Ethereal abgelöst durch Wireshark. Siehe unten: Wireshark.

EtherPeek, GigaPeek (.PKT) (ETH)

WildPackets ist der Hersteller der Wahl, wenn es um *Capture Engine*s geht, die MessDaten liefern für die Verarbeitung mit **Trace:Magic**.

EtherPeek NX (WildPackets)

EtherPeek_NX ist bestens geeignet für Messungen=Aufzeichnungen am Switch-Mirror-Port. Paket-Verluste treten nur sehr selten auf; die Erfahrung zeigt, dass mindestens bis 60% Last pro Sekunde die Aufzeichnungen verlustfrei sind (oder doch sehr weitgehend verlustfrei sind), teilweise treten signifikante Verluste erst bei der Marke von etwa 80% Netzlast auf.

Das Experten-System von EtherPeek_NX ist sehr gut geeignet, Zeit-Abläufe sichtbar zu machen. Da **Trace:Magic** sich bis Version 5 (TMv5) nicht mit Details der Zeitstempel befasst, ist EtherPeek_NX das empfohlene Komplementär zu TMv5. Die ab TMv6 einsetzende Betrachtung von Zeit-Abläufen wiederum beruht auf dem Aufzeichnungs-Format von EtherPeek_NX ab Version 3 (und nicht anderen Analyzer-Formaten).

Daher ist EtherPeek_NX das eindeutig empfohlene Analyzer-Produkt für den Einsatz mit **Trace:Magic**.

Packet Grabber (WildPackets)

Der „Packet Grabber" ist die reine *Capture Engine* aus EtherPeek, ohne Darstellung der Daten, ohne Analyse-Funktionen. Vorteil: Sehr preisgünstig und effizient im Sinne der Prozessor-Auslastung.

Für **Trace:Magic** hervorragend geeignet (siehe „EtherPeek_NX").

GigaPeek (WildPackets)

GigaPeek ist für Full-Duplex-Messungen ausgelegt (EtherPeek_NX nur für Half-Duplex-Messungen am Mirror-Port); hierfür bietet WildPackets eine zusätzliche Hardware an namens Tetra2.

Das Aufzeichnungs-Format von GigaPeek wird seitens **Trace:Magic** ab TMv5 unterstützt. (Dies gilt jedenfalls für Mirror-Port-Messungen; bei Tap-Messungen könnte es ggf. noch Ergänzungs-Bedarf geben.)

LANdecoder32(.ENF,.TRF) (ETH,TOK)

LANdecoder32 (Triticom) war bis Anfang der 2000er Jahre die erste Wahl am Markt. Inzwischen ist diese Vorrang-Stellung an den Hersteller WildPackets verloren gegangen.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt keine Rolle mehr.

NetMon (.CAP) (ETH,TOK,FDDI)

Der "Networks Monitor" von Microsoft (Bestandteil von SMS, Systems Management Server) ist interessant, weil er für SMS-Anwender kostenfrei mitgeliefert wird und stichprobenartige Messungen per Fernzugriff ermöglicht.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt keine Rolle.

NetVCR (.PCAP,.ENC) (ETH)

Insofern NetVCR (Niksun) in der Lage ist, seine LAN-Aufzeichnungen nachträglich im Format von Sniffer (.ENC) oder Ethereal (.PCAP) auszukoppeln, können sie auch von **Trace:Magic** verarbeitet werden.

Jedoch sind hier Beschränkungen gegeben, die höchst unerfreulich sind: Die NetVCR-Daten können immer nur in eine einzige (dann schnell zu große) Trace-Datei ausgekoppelt werden, und nicht in viele kleine Dateien (sequenziell).

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt keine erhebliche Rolle.

NetXRay (.CAP) (ETH,TOK,FDDI)

NetXRay (Cinco) wurde in den 1990er-Jahren von Sniffer (Network General) aufgekauft und ging in SnifferPro auf.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses inzwischen untergegangene Produkt keine Rolle mehr.

Observer (.BFR) (ETH,TOK,FDDI)

Observer (Network Instruments) ist in der Darstellung einfacher Verkehrs-Statistiken stark sowie in der Behandlung von VoIP (Voice over IP).

Seine Schwächen sind: Paket-Verluste bei der Aufzeichnung; fehlende Analyse-Funktionen schon auf rudimentärer Basis; völlig ungenügende Bedienerführung bei Darstellung der Datenpakete.

Der bis 2005 maßgebliche Observer-Distributor hat sich aus dem Geschäft mit Wirkung zum 31.3.2005 zurück gezogen; daher muss damit gerechnet werden, dass dieser Analyzer seinen Markt in Deutschland nach und nach verlieren wird. Dies entspräche Vorhersagen, die seitens Synapse:Networks GmbH schon lange zuvor gemacht wurden.

Observer wird gut unterstützt, aber nicht als erste Wahl betrachtet.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt keine vorrangige Rolle.

OptiView (.CAP) (ETH,TOK,FDDI)

OptiView (Fluke) zeichnet im Snoop-Format (Sun Microsystems) auf und verwendet für die Darstellung den Surveyor (Shomiti/Finisar), der per OEM-Lizenz geliefert wird.

Da OptiView nicht für Dauer-Messungen mit fortlaufender MessDaten-Aufzeichnung über Stunden oder Tage ausgelegt ist, kommt er für Langzeit-Messungen nicht in Betracht.

Außerdem scheint die OEM-Lizenz auszulaufen; auch wird der Surveyor seitens des Lizenz-Gebers allem Anschein nach nicht mehr sonderlich gepflegt zu werden.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt daher nur eine untergeordnete Rolle.

Sniffer (.ENC,.TRC,.FDC,.CAP) (ETH,TOK,FDDI)

Sniffer (Network General, vormals NAI) gehört für Synapse:Networks GmbH zu den am meisten überschätzten Analyse-Produkten überhaupt.

SnifferPro auf Windows-PCs zeichnet sich aus durch erhebliche Paket-Verluste in der Aufzeichnung; durch eine völlig ungenügende Bedienerführung bei der Paket-Darstellung; mit erstaunlich unzureichenden Analyse-Funktionen und sogar Fehlern.

Nach mehreren Jahren in Folge, in denen Sniffer seinem Eigentümer NAI (McAfee) Verluste brachte, wurde die Sniffer-Division verkauft an Privat-Investoren, die das Projekt nun wieder unter dem alten Hersteller-Namen „Network General" fortführen.

Erhebliche Personal-Entlassungen, unübersehbare Rücknahmen von Produkten und Strategien, allenthalben greifbare Abwanderungen von Kunden zu anderen Herstellern (WildPackets) bzw. Produkten (TcpDump, Ethereal) lassen bezweifeln, dass Sniffer noch eine erhebliche Rolle im Markt spielen wird.

Das vermutlich unumkehrbare Sterben dieses Produktes bzw. Herstellers entspricht langjährigen Voraussagen seitens Synapse:Networks GmbH und wird ohne jedes Bedauern zur Kenntnis genommen.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt keine Rolle mehr.

Surveyor (.CAP) (ETH,TOK,FDDI)

Der Surveyor (Shomiti/Finisar) hat in Deutschland kaum Verbreitung gefunden; nur seine indirekte Verbreitung als OEM-Version bei Fluke (siehe: OptiView) hat zu beschränkter Bekanntheit geführt.

Es spricht einiges dafür, dass dieser Analyzer nicht mehr sonderlich gepflegt wird; die OEM-Lizenz gegenüber Fluke (OptiView) wird dem Anschein nach auch nicht mehr verlängert.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt keine Rolle.

TcpDump (.DMP) (ETH,TOK,FDDI)

Siehe: Ethereal.

TokenPeek (.TPC) (TOK)

TokenPeek (WildPackets) gehört zu den wenigen noch am Markt verfügbaren Produkten zur Token-Ring-Analyse.

Es wird von **Trace:Magic** unterstützt; aber Token-Ring ist inzwischen weltweit fast überall durch Ethernet abgelöst worden.

Für den Einsatz im Sinne von **Trace:Magic** spielt dieses Produkt daher keine Rolle mehr.

TraceCommander (.DMP) (ETH)

Trace:Commander ist ein LAN-Analyzer, der eigens von Synapse:Networks entwickelt wurde, um bestmöglich Messdaten zu erzeugen, die optimal im Format für **Trace:Magic** aufgezeichnet sind.

Selbst Anwender, die über einen oder mehrere der oben genannten LAN-Analyzer verfügen, sollten mit Blick auf **Trace:Magic** die Aufzeichnung von LAN-Messdaten mit **Trace:Commander** bewerkstelligen.

Mit den Modulen **PingNotes** (Modul zum Senden von Störmeldungen durch Anwender), **CaptureWizard** (Aufzeichnung der Messdaten samt Nachtschaltung und Datenverwaltung) und **MiniMagic** (Auswertung der Messdaten in Fast-Echtzeit) bietet **Trace:Commander** eine Suite an Funktionen, die optimal insbesondere für Dauer-Aufzeichnungen, aber auch für Notfall-Troubleshooting geeignet sind.

Das Modul zur Messdaten-Aufzeichnung (CaptureWizard) ist kostenfrei.
Das Modul zur Messdaten-Auswertung (MiniMagic) ist kostenpflichtig zu lizensieren.

Trace:Commander wurde nicht nur entwickelt, um Messdaten für **Trace:Magic** zu liefern. Die Entwicklung wurde auch veranlasst, um Kunden eine leicht bedienbare und kostenfreie Alternative zu kommerziellen Analyzern zu bieten, da in segmentierten Netzwerken die erforderliche Zahl kommerzieller Lizenzen kaum mehr bezahlbar ist. Aber auch der kostenfreie Open-Source-Analyzer *Wireshark* bietet für Langzeit-Aufzeichnungen und Notfall-Analysen nicht die Funktionen, die aus Sicht von Synapse:Networks erforderlich sind, um in geeigneter Weise handlungsfähig zu sein.

Info+Download: www.tracecommander.net

Wireshark, TcpDump (.DMP,.PCAP) (ETH,TOK,FDDI)

Die Open-Source-Produkte "TcpDump" (Linux) und "Wireshark" (vormals: Ethereal) (Windows, Linux) werden immer wichtiger, seitdem die LANs in immer mehr Teil-Segmente getrennt wurden/werden (*switched networks*).

Switched Networks erhöhen den Zwang zum Einsatz immer mehr *Capture-Engines*; die Zahl der MessPunkte erhöht sich mit der Zahl der Netzwerk-Segmente.

Aus finanzieller Sicht wird es immer schwieriger, für alle MessPunkte kommerzielle Produkte zur Daten-Erfassung und –Aufzeichnung einzusetzen.

Technisch gesehen gelten folgende Faustformeln:

TcpDump (Linux)

Hier scheinen sich Entwicklungen anzudeuten, dass zuverlässige und (weitgehend) verlustfreie Aufzeichnung des Datenverkehrs möglich werden könnte. Hier muss die Entwicklung noch beobachtet und die verfügbare Technik getestet werden.

TcpDump ist eine reine *Capture Engine*; Darstellung und Analyse der aufgezeichneten Daten sind nicht möglich; hierzu bedarf es zusätzlicher Produkte (wie *Wireshark* oder *TraceMagic*).

Trace:Magic kann TcpDump-Daten problemfrei auswerten, sofern nicht etwaige Paket-Verluste dem entgegen stehen und sofern bestimmte Format-Vorgaben eingehalten wurden.

Wireshark (vormals: Ethereal) (Linux, Windows)

Die Erfahrung zeigt, dass **Wireshark** einen zu langsamen Programm-Code besitzt, um bei hohen Datenraten verlustfrei aufzeichnen zu können.

Wireshark ist geeignet für Aufzeichnungen auf Arbeitsplatz- oder Workgroup-Ebene, und auch das ohne Gewähr der verlustfreien Erfassung.

Trace:Magic kann Wireshark-Daten problemfrei auswerten, sofern die Paket-Verluste dem nicht im Wege stehen und sofern bestimmte Format-Vorgaben eingehalten wurden.

Das passende Aufzeichnungs-Format kann problemlos sicher gestellt werden durch den Einsatz des Kommandozeilen-Tools „**TShark**" – hierbei handelt es sich um eine DOS-Box-Variante, die über kein GUI verfügt.

Der von Synapse:Networks entwickelte LAN-Analyzer **Trace:Commander** nutzt im Hintergrund das TShark-Modul zur Messdaten-Aufzeichnung – und sorgt dafür, dass die MessDaten-Aufzeichnung genau im **Trace:Magic**-kompatiblen Format abläuft. Siehe oben: **Trace:Commander**.

Zusammenfassung / Ergebnis / Empfehlung

Für die nächste Zukunft werden absehbar (aus Sicht von Synapse:Networks) nur noch zwei Gruppen von *Capture Engine*s von Belang sein:

1. Commercial Analyzer = WildPackets (EtherPeek, GigaPeek, OmniPeek)
2. Open Source Analyzer = Wireshark (Windows) / TcpDump (Linux)

Die Messdaten-Aufzeichnung kann und soll in 80-98% aller Fälle über **Trace:Commander** stattfinden (und somit über die *Capture Engine* von Wireshark). In extremen Gigabit-Umgebungen kann und soll ggf. weiterhin mit WildPackets-Produkten gearbeitet werden.

Im Einzelnen bedeutet dies:

Messungen in Core-Backbones via Mirror-Port (Half-Duplex-Mode am Analyzer-Interface):

Es wird **Trace:Commander** empfohlen.

Messungen in Core-Backbones via Media-Splitter/Taps (Full-Duplex-Mode am Analyzer-Interface):

Sofern nicht mit Aggregation-Taps gearbeitet wird (dann wäre **Trace:Commander** möglich), kann **GigaPeek / OmniPeek** von WildPackets empfohlen werden.

Messungen an der Peripherie (Workgoup Switches, WAN Routers):

Es wird **Trace:Commander** empfohlen.

Messungen des Zeitverhaltens, …

in denen Antwortzeiten durch Auswertung der *Packet Time Stamps* analysiert werden soll, ist aus Sicht von **Trace:Magic** (ab TMv6) vorläufig (noch) zwingend das EtherPeek-Format erforderlich, da zur Zeit bei Delta-Zeit-Analysen nur dieses TimeStamp-Format unterstützt wird.