

# Kapitel 3

## LAN-Analyzer: Anmerkungen

Dieses kurze Kapitel soll einige der Analyser kurz beleuchten, mit denen der Verfasser in den letzten zwei Jahren seit dem ersten Erscheinen seines Buches *Networker's Guide. LAN Analysis und Windows Troubleshooting* Berührung hatte. Es haben sich nicht wenige Bewertungen verschoben.

Da der Verfasser nur mit wenigen Werkzeugen ernsthaft arbeitet (weil er den Rest für ziemlich untauglich hält), ist dieser Überblick alles andere als repräsentativ, aber sicherlich aufschlussreich, was die Bewertungskriterien im Sinne von Analyse und Troubleshooting anbetrifft.

### 3.1 Software-Analyzer

Kurz gefasst: Seitdem *EtherPeek NX* auf Gigabit-Leitungen hervorragende Ergebnisse beim Capturing erbringt, sind für den Verfasser die Hardware-Analyser für echte Fehlersuche bzw. für Troubleshooting nur noch zweite, wenn nicht gar dritte Wahl.

Entsprechend fallen hier auch die Bewertungen grundsätzlich zu Gunsten der Software-Analyser aus.

#### 3.1.1 LANdecoder32 (Triticom)

Als Erstes sei der *LANdecoder32* von Triticom ([www.triticom.com](http://www.triticom.com)) erwähnt, da fast alle Beispiele im *Networker's Guide* (Erste Auflage München 2000, Markt+Technik) mit Abbildungen dieses Analyzers illustriert worden waren – und weil der Verfasser sich fast ausnahmslos zu diesem Analyzer bekannt hatte, als dem damals besten im Sinne unbeschränkter Navigation und übersichtlicher Darstellung.

Diese Bewertung lässt sich heute in dieser Form nicht mehr aufrecht erhalten und zwar aus einigen wenigen, aber stichhaltigen Gründen:

- **Erstens** wurde das Experten-System des *LANdecoder32* durch *TraceMagic* komplett überholt und dadurch in vielen (nicht allen!) Funktionen praktisch weitgehend überflüssig. Das gilt aber auch für die Experten-Systeme aller anderen Analyser.

- **Zweitens** wurde die Protokoll-Dekodierung für NCP-über-TCP/IP nicht mehr nachgepflegt. Es kann sein, dass Triticom zu der Ansicht gelangte, dieser Markt sei inzwischen zu klein, um noch der Mühe wert zu sein; und doch fehlt dieses Decoding, wenn Messungen in einer NetWare-Umgebung anstehen.
- **Drittens** hat Triticom kein Commitment abgegeben zur Zuverlässigkeit des Capturings unter Gigabit-Bedingungen. War das so genannte AccuCapture unter Fast Ethernet noch ein unbedingter Grund, LANdecoder32 einzusetzen (da die Zuverlässigkeit bzw. die niedrige Paketverlustrate dafür sprachen), so fehlt nun die Entsprechung für Gigabit (Stand: Oktober 2002). Zwar gibt Triticom eine Liste der unterstützten Gigabit-Adapter heraus, aber gemessen am »AccuCapture« unter 100-Megabit-Bedingungen ist dies ein Rückschritt.
- **Viertens** fehlen weitere wichtige Entwicklungen wie beispielsweise die Unterstützung von WLANs (Wireless LANs).

Ansonsten aber zählt der *LANdecoder32* immer noch zu »Papas Lieblingen« (also zu den vom Autor bevorzugten Produkten), denn seine Art der Darstellung, seine Navigation über die LAN-Pakete, seine Filtermöglichkeiten sowie seine Farbgebung sind nach wie vor in der Kategorie »best of ...« anzusiedeln.

Daher sind weiterhin die Darstellungen von Paket-Dekodierungen zahlreich mit dem *LANdecoder32* erstellt worden.

Ansonsten sei hier auf einen zweiten Analyzer verwiesen, der nach Meinung des Verfassers weit aufgeschlossen hat (was Navigation, Darstellung etc. anbetrifft) und bei Gigabit-Messungen sogar die Nase vorne hat: Das ist *EtherPeek NX* von WildPackets (siehe unten).

### 3.1.2 Observer (Network Instruments)

Der *Observer* von Network Instruments ([www.networkinstruments.com](http://www.networkinstruments.com)) hat sich erstaunlich weit entwickelt. Seine statistischen Fähigkeiten sind inzwischen womöglich die besten im Kreise der kommerziellen Analyzer und die jüngsten Fortschritte bezüglich Voice over IP machen den *Observer* im Umfeld von Sprach-Daten-Netzen sogar (fast) unverzichtbar. Außerdem sind die Fähigkeiten zu verteilter Überwachung (Remote Monitoring über RMON und proprietäre Entwicklungen) in der Bedienerfreundlichkeit kaum zu schlagen.

Das kann aber nicht verdecken, dass neben der Mächtigkeit der Statistik die Qualität der Analyse nicht Schritt halten konnte.

Darstellung, Navigation, Filterfähigkeiten und Farbgebung sind noch nicht einmal durchschnittlich gut und die Möglichkeiten, sich mit *Observer* völlig unbekanntem Fehler-Szenarien zu nähern, sind aus Sicht des Verfassers mehr als bescheiden.

Andererseits gilt auch hier (wie bei allen anderen), dass dieser Mangel inzwischen aber auch nicht mehr weh tut, weil jenseits der Statistik die Fehler-Analyse sowieso über *TraceMagic* abgewickelt wird – und nicht mehr über den Analyser, der die Daten von der Leitung holte.

Da der Verfasser die Ansicht vertritt, dass kein Werkzeug alles kann und dass Statistik sowie Analyse jeweils ihre eigene Berechtigung haben, gilt im Ergebnis:

Der *Observer* gehört in jedes Netzwerk, sollte aber nicht mit Erwartungen in der Analyse überfordert werden, denen er auf Grund seiner Architektur nicht gerecht werden kann.

Schnelle Übersicht aber über (fast) alles, was sich quantifizieren bzw. in Statistiken erfassen lässt, gibt der *Observer* (fast) perfekt.

### 3.1.3 EtherPeek NX (WildPackets)

Das *EtherPeek NX* ([www.wildpackets.com](http://www.wildpackets.com)) ist der Shooting Star der Jahre 2001/2002 und das in mehrerlei Hinsicht:

Erstens sind Messungen auf Gigabit-Leitungen mit *EtherPeek NX* eine wahre Wonne (hier kann des Lobes nicht genügend ausgesprochen werden) und zweitens beginnt hier eine Software zu wachsen, die dem bislang vom Verfasser bevorzugten *LANdecoder32* wohl bald den Rang ablaufen könnte.

Navigation, Darstellung und Paket-Dekodierung sind inzwischen weitgehend gleichwertig (verglichen mit *LANdecoder32*). Wo noch Wünsche offen sind: Das Filtern ist leider noch nicht im finalen Entwicklungsstadium angekommen.

Hervorragend sind die Fähigkeiten, Paket-Dekodierungen in HTML-Format auszugeben, und schlicht überwältigend ist das Gigabit-Verhalten:

Schon Anfang 2002 hat WildPackets das Commitment (die Zusage im Sinne der Gewährleistung) abgegeben, dass bis zu ca. 60% Netzlast auf der Gigabit-Leitung bei hinreichend schnellem Prozessor des Analyzers (fast) verlustfreies Capturing möglich sei.

Der Verfasser hat mit seinem Unternehmen *Synapse:Networks* viele Gigabit-Messungen auch auf hart befahrenen Leitungen hinter sich und er kann bestätigen: Dieses Werkzeug hält, was es verspricht. Als LAN-Adapter wird zur Zeit (in 2002) eine SysConnect-GE-Karte genommen.

Manchmal wirklich atemberaubend ist die Fähigkeit, auch bei Volldampf ein schnell, zuverlässig und zugleich sanft arbeitendes Online-Experten-System arbeiten zu lassen, das über alle einfachen Fehler schnelle Auskunft gibt, entweder sortiert nach Fehlerklassen, oder sortiert nach Teilnehmeradressen oder Dialogpaaren.

Der Verfasser kann nicht verhehlen, im Sommer 2001 derlei Leistungen eines »Software-Analyzers« für glatt unmöglich gehalten zu haben – er wurde eines Besseren belehrt. Voraussetzung ist jedoch eine großzügige Hardware-Ausstat-

tung des Messrechners, der über viel Hauptspeicher, schnellen RAM-BUS und extrem schnelle Festplatte verfügen sollte (siehe hierzu: [www.staccer.de](http://www.staccer.de)).

Und wird der Preis noch in die Betrachtung einbezogen, ergibt sich das gute Gefühl, auch in Gigabit-Backbones eine sichere Technik in der Hand zu haben.

Neben *EtherPeek* (Ethernet) gibt es auch noch *TokenPeek* (Token-Ring) und neuerdings auch *AeroPeek* (Wireless LANs). Die Breite der Produktpalette überzeugt hier ebenso wie die Entwicklungsdynamik und das Preis-Leistungs-Verhältnis.

### 3.1.4 Sniffer (NAI, vormals Network General)

*Sniffer* bzw. *SnifferPro* ([www.sniffer.com](http://www.sniffer.com)) ist nach wie vor an der Spitze der Entwicklung, wenn es um die Implementation neuer Protokolle geht. Wer darauf angewiesen ist, immer möglichst aktuell mit allen neuen Protokollvarianten (um nicht zu sagen: Protokoll-Exoten) versorgt zu sein, wird auf *Sniffer* schlecht verzichten können.

Ansonsten scheiden sich beim *Sniffer* für viele Netzwerk-Admins die Geister. Verglichen mit der Leistungskraft anderer Analyzer, sogar FreeWare-Tools bzw. Open Source-Programmen, muss der Preis dem Zweifel unterworfen werden, womöglich nicht ganz angemessen zu sein.

Aus der Sicht des Verfassers ist spätestens seit *TraceMagic* bei *Sniffer* ernstlich die Frage zu stellen, ob der Hersteller sein Preis-Leistungs-Verhältnis nicht intensiv überdenken sollte.

Aber dies mögen subjektive Eindrücke eines Spezialisten sein, der die Bedürfnisse eines Gelegenheits-Analysten nicht mehr genau nachvollziehen kann. Denn es gibt durchaus *Sniffer*-Anwender, die nur ab und zu LAN-Analyse betreiben und denen nach eigenem Bekunden durchaus mit dem Experten-System des *Sniffers* geholfen werden konnte.

Der Verfasser muss also in seinem Urteil vorsichtig sein, trotzdem will er nicht verbergen, dass er die Verbreitung im Markt und das Preis-Leistungs-Verhältnis des *Sniffers* nie verstanden hat.

Zum historischen Verständnis sei der Hinweis gegeben, dass der heutige Windows-*Sniffer* weitgehend auf dem *NetXRay* von Cinco beruht (in den 90-er Jahren aufgekauft). Das Aufzeichnungsformat des heutigen *Sniffers* mit seinen .CAP-Dateien ist das alte *NetXRay*-Format.

### 3.1.5 Surveyor (Shomiti-Finisar)

Der *Surveyor* von vormals Shomiti, jetzt Finisar ([www.finisar.com](http://www.finisar.com)), gehört zu den Produkten, die sowohl als Software-Analyzer einsetzbar sind wie auch als Front-End von Hardware-Lösungen.

Die so genannte *THG-Box* (»Ten Hundred Giga«) von Shomiti-Finisar war in 2001 über einige Zeit ernstlich ein Kandidat für leistungsfähige Gigabit-Messungen und entsprechend wäre der *Surveyor* ein Werkzeug der engeren Wahl gewesen.

Ausgiebige Tests von *THG* und *Surveyor* im Herbst 2001 erbrachten jedoch Schwächen in der Hardware, die letztlich nicht hinnehmbar waren und als dann Shomiti von Finisar übernommen wurde, war leider zunächst nicht mehr klar, ob und wohin die zukünftige Entwicklung gehen würde. Aber auch unabhängig davon ist festzustellen: Es macht nicht so viel Sinn, immer nur winzige Zeitfenster von der Leitung abgreifen zu können, wenn nach 256 Megabyte der Hardware-Puffer voll ist und sodann erst derselbe ausgelesen werden muss. ...

Hier zeigt *EtherPeek NX* (WildPackets), wie man's richtig macht: ständiges Schreiben auf die Festplatte praktisch ohne nennenswerte Paketverluste.

Es mag sein, dass inzwischen die Schwächen behoben wurden, und es kann sein, dass Finisar die Entwicklung weitertreibt, aber das alles ist aus Sicht des Verfassers nicht mehr maßgeblich.

Seitdem mit *EtherPeek NX* (WildPackets) zu einem fast schon lächerlichen Preis eine extrem leistungsfähige Gigabit-Capture-Engine auf den Markt gebracht wurde, dürften die Tage der so genannten Hardware-Analyzer endgültig gezählt sein: zu teuer, zu langsam in der Produktentwicklung, zu riskant mit Blick auf das verlorene Investment, wenn sich Fehler in der Hardware bemerkbar machen.

Dies ist, wohl gemerkt, das subjektive Urteil des Verfassers. Niemand sollte darauf verzichten, ggf. durch Tests zu einem eigenen und anderen Urteil zu kommen. Der Verfasser jedoch glaubt, für diese Sicht der Dinge gute Gründe zu haben.

Ergänzend jedoch muss zu Gunsten der Finisar-Produkte festgestellt werden, dass die extrem teure Entwicklung von Gigabit-Komponenten hier ziemlich ernst genommen zu werden scheint.

Die Möglichkeiten, Hardware-Probes in Gigabit-Backbones an Stelle der zu wenig leistungsfähigen RMON-Agenten einzusetzen, sind durchaus beachtlich: Der Einsatz der *Surveyor*-Software verhilft in diesem Umfeld zu akzeptablen Ergebnissen bei *Distributed Remote Monitoring*.

Es müssen jedoch schon sehr spezielle Echtzeit-Anforderungen gestellt werden, um das erhebliche Investment in diese gehobene Technik zu rechtfertigen.

### 3.1.6 Ethereal

Mit *Ethereal* ([www.ethereal.com](http://www.ethereal.com)) ist ein Analyzer unter GPL-Lizenz auf den Markt getreten, der zum Teil über Funktionen verfügt, die extrem leistungsfähig sind und die man bei den kommerziellen Mitbewerbern vergeblich sucht.

Dass er sowohl unter Unix als auch unter Windows läuft, gibt diesem Analyzer eine universelle Note, die in der Praxis wichtig sein kann. Vor allem die Möglichkeiten des Anwenders, eigene Nutzungsformen zu konfektionieren, sind nicht gering zu schätzen.

*Ethereal* spielt für den Verfasser und sein *TraceMagic*-Konzept eine große Rolle.

*TraceMagic* unterstützt die meisten der gängigen Analyzer-Formate und somit ist es inzwischen völlig belanglos geworden, welcher Analyzer als Capture-Engine die Daten von der Leitung geholt hat und wenn das nun schon einmal egal ist, kann es eben auch ein Open-Source-Tool sein.

Im Februar 2002 stellte der Verfasser über einen seiner Kunden Kontakt zu den Programmierern von *Ethereal* her und hierdurch wurde veranlasst, dass *Ethereal* die Fähigkeit bekam, Messdaten fortlaufend in sequenziellen Trace-Dateien auf die Festplatte zu schreiben. Diese Möglichkeit war bis Anfang 2002 weder gegeben noch vorgesehen (so die Auskunft eines der Programmierer noch im Januar 2002 gegenüber dem Verfasser).

Der Umstand, dass diese Fähigkeit zum Schreiben der Messdaten in Trace-Dateien auf die Anzahl von zehn Capture-Files begrenzt wurde, lässt allerdings ahnen, dass nach der im Herbst gültigen Version 0.95 die irgendwann kommende Version 1.0 kommerziell vertrieben werden könnte. Denn wozu sollte die Zahl der Trace-Files beschränkt sein, wenn nicht zu dem Zweck, für eine Aufhebung dieser Beschränkung später Geld zu nehmen? Aber das ist Spekulation.

Sicher ist, dass mit *Ethereal* ein erheblicher Schritt nach vorne getan wurde, um den Capture-Job wenigstens auf 10/100 Megabit von teuren Markenprodukten unabhängig zu machen.

### 3.1.7 TcpDump

Diese Freeware ([www.tcpdump.org](http://www.tcpdump.org)) ist ähnlich interessant wie *Ethereal*. Beide Produkte verbindet, dass *Ethereal* erheblich angelehnt ist an *TcpDump*. *TcpDump* arbeitet in seiner Capture Engine mit dem *libcap*-Treiber, der auch in anderen Open Source-Programmen verwendet wird.

Der Verfasser hat mit folgender Konstellation gute Erfahrungen gemacht:

- Ein Unix-Server ist mit einem ATM-Adapter oder mit einem Gigabit-Ethernet-Adapter ans Netzwerk angeschlossen und Messung über Mirror-Port ist nicht möglich.
- Statt einen ATM-Tester zu bemühen (wovon der Verfasser schlicht gar nichts hält) oder die Gigabit-Ethernet-Konstruktion so weit umzubauen, dass irgendwo ein GE-Mirror-Port frei wird, wird *TcpDump* auf dem Server-Adapter gestartet.

- *TcpDump* erzeugt Aufzeichnungs-Dateien, wie es ein Analyzer auf der Leitung auch tun würde: MAC-Header, IP, TCP, alles ist korrekt vorhanden.
- Nach Beendigung der Messung werden die Trace-Dateien auf den *Trace-Magic*-Rechner kopiert.
- Sodann wertet *TraceMagic* die Aufzeichnungs-Dateien automatisch aus.

Dieses Verfahren gibt ein so immens hohes Maß an Unabhängigkeit von der Verfügbarkeit von Messpunkten im Backbone, dass es sich schon als universal einstufen lässt.

Theoretisch gibt es ähnliche Möglichkeiten auf Windows-Servern, hier aber liegen noch keine Erfahrungen des Verfassers vor (*WinPCap*-Treiber).

Auch hiermit ist ein weiterer Schritt in die Richtung getan, sich von kommerziellen Produkten unabhängig zu machen, wenn es um Capture-Engines geht.

### 3.1.8 NTOP

Als FreeWare-Capture-Engine kommt auch *NTOP* in Frage ([www.ntop.org](http://www.ntop.org)). Dieses Werkzeug verfügt auf Unix/Linux-Basis über immense Fähigkeiten in Statistik, Monitoring, Datenfluss-Kontrolle, Verkehrs-Matrix und so weiter.

Die Leistungsfähigkeit dieses Werkzeuges ist in manchen Bereichen so stark, dass man durchaus Gründe für die Überzeugung finden kann, dass kommerzielle Windows-Analyzer womöglich nur deshalb so erfolgreich sind, weil zu wenig Netzwerk-Admins mit Unix und Open Source-Software umgehen können.

Mit *NTOP* lassen sich umfangreiche Maßnahmen des Netzwerk-Monitorings durchführen.

Ein Packet-Capture ist bislang nur rudimentär möglich. Trotzdem soll hier *NTOP* erwähnt werden, weil sich eine zukünftige Entwicklung in diese Richtung abzuzeichnen beginnt.

In jedem Falle sind die Statistik-Fähigkeiten schon heute so stark, dass LAN-Analyzer für teures Geld hierfür nicht mehr zweckentfremdet werden müssen.

## 3.2 Hardware-Analyzer

Kurz vorab gesagt: Hardware-Analyzer sind aus Sicht des Verfassers für die klassische LAN-Analyse eine Technik von gestern (von wenigen Ausnahmen abgesehen, wie etwa die tragbaren Geräte von Fluke).

Diese Aussage bezieht sich nicht auf Monitoring-Systeme, wie sie beispielsweise bei Internet Providern oder Betreibern von Voice over IP laufen. Gemeint sind Systeme, die vorgeben, »LAN-Analyse« zu betreiben mit der Fähigkeit zu Fehlerdiagnose und Ursachenerkennung.

Seitdem *EtherPeek NX* (WildPackets) auf Gigabit-Leitungen hervorragende Ergebnisse mit seiner *Capture Engine* erbringt, gibt es keine ernstlichen Gründe mehr dafür, so viel Geld für die doch sehr teuren Hardware-Boliden aufzuwenden.

Tests mit Gigabit-Hardware-Analysern, die der Verfasser im Herbst 2001 sehr ausführlich angestellt hatte, offenbarten das nicht geringe Risiko, dass schon kleine Fehler in der Hardware das ganze Investment lahm legen. Rücksendung, Austausch, Warten ... das kann nicht hingenommen werden.

Die nachfolgenden Bewertungen müssen aber von jedem Leser im Zweifel durch eigene Tests nachvollzogen werden. Unter veränderten Anforderungen (die ja nicht dieselben wie die des Verfassers sein müssen) können auch andere Urteile die Folge sein.

### 3.2.1 Hardware-Hersteller begehrt TraceMagic-Code

Eine Anekdote **muss** hier vorangestellt werden, weil sie die Hilflosigkeit dieser Hersteller geradezu beispielhaft aufzeigt:

Es hat im Frühjahr 2002 Verhandlungen zwischen einem der unten aufgeführten Analyzer-Hersteller einerseits und *Synapse:Networks* andererseits gegeben (dem Unternehmen des Verfassers). Gegenstand war die Portierung von *TraceMagic*-Analyse-Funktionen in die Analyzer-Suite des besagten Herstellers (der auf eigenen Wunsch hin in den Publikationen des Verfassers anonym bleiben möchte).

Nach mehreren Wochen hat der Verfasser die Verhandlungen entnervt abgebrochen – mit dem höchst unerfreulichen Eindruck, dass die Gegenseite sowohl vertragstechnisch wie auch analysetechnisch völlig hilflos bzw. überfordert und daher im Grunde überhaupt nicht verhandlungsfähig war.

Wenn man einem angeblichen Marktführer erst noch das kleine Einmaleins der LAN-Analyse und der Client/Server-Diagnostik erklären muss, ergeben solche Gespräche irgendwann einfach keinen Sinn mehr – so jedenfalls die Wahrnehmung des Verfassers.

Als an einem Punkt der Gespräche der Analyzer-Vertreter etwas beleidigt war, weil der Verfasser die TCP/IP-Analyse-Funktionen der Gegenseite nicht recht wertschätzen wollte, und als der dortige Verhandlungsführer stolz auf sein mageres Dutzend an Schwellwerten bzw. Statistik-Zähler in diesem Bereich verwies (zehn oder elf Zähler zu IP, UDP, TCP, ICMP), konnte nicht der Hinweis unterbleiben, dass *TraceMagic* schon seit längerer Zeit mit über 200 Fehler- und Ereignis-Zählern bei der TCP/IP-Analyse arbeitet, und das sowohl im Bereich der Gesamtstatistiken (*over all hosts*) sowie für jeden einzelnen von bis zu 65.500 IP-Hosts (*per single host*).

Warum nur verhandelte dieser Hersteller mit *Synapse:Networks*, wenn er dann eingeschnappt war, dass bzw. wenn *TraceMagic* bereits in völlig anderen Dimensionen arbeitet(e)? Irgendwann muss man sich doch mal entscheiden, was man will.

Die Software besagten Herstellers zeichnete sich zudem durch dramatische Mängel aus, so beispielsweise beim Filtering. Es war wirklich kaum zu fassen. Filter auf NetBIOS-Namen erbrachten zum Teil weniger als die Hälfte der tatsächlich vorhandenen Fundstellen. Aber sagen durfte man das nicht, da war die Gegenseite gleich beleidigt.

Da fehlen einem am Ende wirklich die Worte – spätestens dann, wenn man die Preise sieht, die dieser Hersteller bis heute nimmt.

### 3.2.2 Agilent (Hewlett Packard)

*Agilent* ist eine Tochter von Hewlett-Packard, spezialisiert auf LAN-Messtechnik ([www.agilent.com](http://www.agilent.com)).

Im Herbst 2001 wurde der vormalis *Internetwork Advisor* genannte, jetzt schlicht nur *Network Analyzer* genannte Verbund von Hardware und Software getestet. Damals waren die Ergebnisse nicht überzeugend. Im Frühjahr 2002 wurde die Software erneut getestet und wieder konnte das Ergebnis nicht zufriedenstellen.

Die Zeitfenster, die das Experten-System betrachten konnte, waren einfach zu klein (zu kurz), um zuverlässig zu umfassenden Aussagen zu kommen und es waren Fehler festzustellen, die in einem so hochpreisigen Produkt einfach nicht vorkommen dürfen.

Aus Sicht des Verfassers ist auch hier die Zeit über das Konzept der Hardware-Analyzer hinweggegangen.

### 3.2.3 Acterna (Wavetech Wandel Goltermann)

*Acterna* ist die Analyse-Tochter der Firma Wavetech-Wandel-Goltermann ([www.acterna.com](http://www.acterna.com)).

Die Acterna-Software konnte in den letzten zwei Jahren nur ein einziges Mal vom Verfasser kurz betrachtet werden, ein hinreichendes Urteil liegt daher nicht vor.

### 3.2.4 Shomiti-Finisar

In 2001 wurde Shomiti von Finisar übernommen ([www.finisar.com](http://www.finisar.com)).

Was im Wesentlichen zu den LAN-Analyse-Produkten von Shomiti-Finisar zu sagen war, ist oben unter dem Stichwort *Surveyor* angeführt worden (Abschnitt »Software-Analyzer«).

Es sei noch der Hinweis erlaubt, dass Shomiti-Finisar als Hardware-Lieferant von Fluke durchaus Verdienste in der Entwicklung von leistungsfähigen Analyse-ASICs sowie passender Software erworben hat.

### 3.2.5 NetTool (Fluke)

*Fluke* ([www.flukenetworks.com](http://www.flukenetworks.com)) hat sich das Verdienst erworben, akzeptable tragbare Geräte zu entwickeln, die robust sind, mobil und die mit verhältnismäßig geringem Schulungsaufwand in den Einsatz gehen können.

Schon allein die miniaturisierten NetTool-Kästchen sind für Feldtechniker eine immense Erleichterung, weil auch Personal, das in LAN-Analyse nicht sonderlich geschult ist, in überschaubaren, einfachen Standardtests zu wichtigen Grundaussagen kommen kann.

Gemessen jedoch an ausgereiften Analyse-Lösungen müssen auch hier Zweifel am Preis-Leistungs-Verhältnis erlaubt sein.

Ansonsten jedoch läuft Fluke einigermaßen außer Konkurrenz, weil die Konzeption dieser Monitoring- und Analyse-Technik deutlich anders ist als bei klassischen LAN-Analysern.

### 3.2.6 NetVCR (NikSun)

Mit *NetVCR* ([www.niksun.com](http://www.niksun.com)) ist ein Produkt auf dem Markt, das eine Klasse für sich darstellt und hier unbedingt erwähnt werden muss. *NetVCR* ist kein üblicher Analyzer, es handelt sich vielmehr um ein Monitoring- und Archivierungs-System, dessen Grundgedanke wie folgt aussieht:

- Der gesamte LAN-Traffic wird archiviert, entweder auf Festplatten und/oder Streamer-Tapes (daher der Name »VCR«).
- Über die gesammelten, gespeicherten Daten werden in Echtzeit Tabellen, Indizes und Statistiken geführt, die per Fernzugriff via HTTP (Webbrowser) abgerufen werden können.
- Insbesondere Online-Broker, Banken und Börsenmakler können durch diese Totalarchivierung Schutz vor Beschuldigungen erlangen, ihre Online-Systeme wären zum Zeitpunkt X nicht verfügbar gewesen.
- Beliebige Zeitabschnitte aus dem Endlosarchiv können nachträglich rekonstruiert, ausgewertet und statistisch verarbeitet werden. Die LAN-Pakete beliebiger Zeitfenster lassen sich aus dem Archiv sogar in Trace-Dateien ausgeben (*Sniffer*-Format), was wiederum die nachträgliche Totalauswertung mittels *TraceMagic* ermöglicht.

Die Systeme sind nicht eben billig, aber immens leistungsfähig und gewissermaßen eine Art von Lebensversicherung:

Wenn 24 Stunden am Tag, sieben Tage die Woche, die Totalarchivierung läuft, kann bei jedem beliebigen Störfall der Datenverkehr aus dem Archiv heraus kopiert und gründlich untersucht werden.

Findet diese Untersuchung über *TraceMagic* statt (da *TraceMagic* selbstverständlich das *Sniffer*-Format unterstützt, das von *NetVCR* verwendet wird), ist praktisch kaum noch möglich, dass selbst spontan auftretende Fehler ohne Aufklärung bleiben.