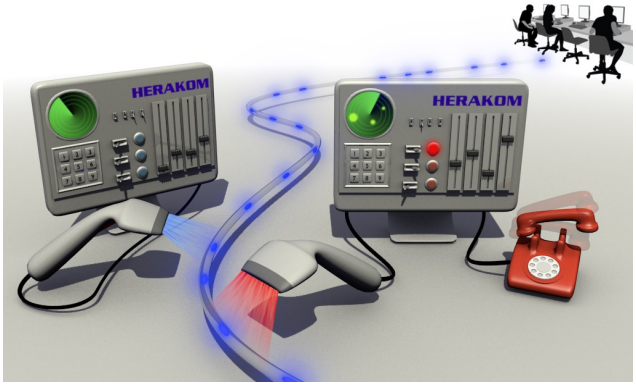
Modulares Messsystem Blackbox



Das Modulare **MessSystem-** Individualkonfiguration Blackbox der HERAKOM GmbH übernimmt vielfältige Aufgaben bei der Erfassung, Analyse von Störungen und Auswertung in WAN/ LAN Netzwerken durch effiziente Messtechnik.
Eine Lösung für alle Module: **- Funktion Qualität Schutz & Sicherheit**
Es können permanent ausführliche Verbindungsübersichten erstellt werden, beispielsweise über die Dauer von Medienverbindungen z.B. ISDN, TCP/IP, SIP, DNS- Verbindungen, Faxübertragungen usw. Natürlich ist auch die dauerhafte Protokoll- Analyse der Datenkommunikation an unterschiedlichen Schnittstellen machbar. Insgesamt stehen bis zu **8 x S_0 und bis zu je 2 x S_{2M}, V.24 und V.11 zur Auswahl und die LAN Schnittstelle** zur Verfügung. Das MessSystem kann modular mit den verschiedensten Schnittstellen individuell zusammengestellt werden. Bei Bedarf aber auch **nur für die LAN- Analyse**. Es können bei Kombinationen von **WAN/ LAN Verbindung die Schnittstellen** parallel aufgezeichnet werden. Die Analyse von Paketen auf 10/100/1000 Base-T-Leitungen ist über die fest eingebaute Ethernet-Schnittstelle oder einen optionalen Ethernet-TAP möglich. Als Analysepunkte kommen Link-Ports oder Spiegel-Ports (SPAN-Ports) an Switches in Frage, oder der Ausgang eines TAP (Hardwarezeitstempel) zum passiven Abgriff der Daten eines Links. Die Protokollerkennung erfolgt automatisch.

Der Paket-Treiber versetzt die eingebaute Ethernet-Schnittstelle/Karte(n) in den *Promiscuous Mode*, in dem alle Pakete an die EasyTrace-Applikation geleitet werden. Die Pakete erhalten Zeitstempel und werden in Dateien auf der Festplatte gespeichert. Gleichzeitig erfolgt die Anzeige der Daten in der EasyTrace-Protokolle-Ansicht. Somit ist die Analyse eines Netzwerksegments online oder offline möglich.

Zentrale Steuerkomponente ist die Blackbox (Embedded PC), der als EasyTrace Server automatisch vorkonfiguriert und über eine IP- Adresse für eine Daueraufzeichnung aktiviert werden kann. Ein EasyTrace client kann das MessSystem somit jederzeit aktivieren/ deaktivieren. Die erfassten Daten können dann wahlweise Online oder sinnvollerweise bei einer Daueraufzeichnung zur weiteren Offline-Verarbeitung zu einer anderen Arbeitsstation im LAN kopiert werden.

Umfangreiche Auswertungsmöglichkeiten stehen in EasyTrace LAN zur Verfügung:
- Listen von TCP-Sitzungen, PPP-Verbindungen und IP-Paketen
- Analyse des Datendurchsatzes, des Paketflusses (grafisch), Protokollstatistiken und Protokollfehler
- RTP-Analyse:Jittermessung SIP, H.323 inkl.Filterung* aller TCP Pakete, bei denen die RTT größer als 200ms ist
- Import und Export von Daten in verschiedenen Formaten
- Alarmierung bei Verhaltensmustern* usw.

Es können mit einem oder mit mehreren PCs Messungen an mehreren Analysepunkten gleichzeitig vorgenommen werden. Im Falle von mehreren MessSystemen lassen sich synchrone Zeitstempel erzielen, da sich *EasyTrace für Windows* bei der Ermittlung der Zeitstempel mit der Uhr des PC synchronisiert und die PC-Uhren untereinander durch Abgleich z. Bsp. mit einem NTP-Server synchronisiert werden können.

Mögliche Ausstattung des Modularen Messsystem- Individualkonfiguration (Industrie-PC)
- Core i5, 2,7GHz, 4 oder 8GB DDR3,
- 500GB Harddisk, Betriebssystem Windows 7 oder 8
- Schnittstellen: 2x GigaLAN, 5xRS232/422/485,
- 4xUSB 3.0, 2x USB2.0, CFAST
- wahlweise PCMCIA-Slot Typ I/II
- wahlweise DVI/VGA/2xDisplayport
- Metallgehäuse, Abmessungen: 114x 215 x 272mm^3 (Hx Bx T)Optional: Akku-Pack (ca. 2Stunden) zum nutzen eines geordneten Herunterfahren des Systems bei Stromausfall

HERAKOM GmbH
Wolfsbachweg 62, 45133 Essen, Tel. 0201 / 46694223, Fax: 0201 / 46694232, E-Mail: Heikeh@Herakom.de, http://www.herakom.de
HRB Essen 11 694, Steuernummer: 112/5960/0479, Ust.-Id-Nr.: DE 811945307, Geschäftsführerin: Heike Hüttemann
Bankverbindung: Sparkasse Essen Haarzopf, BLZ 360 501 05, Kto. Nr. 3 303 393

Die Technik in Stichworten

Lieferumfang:
Modulares Messsystem Hardware mit der gewünschten Schnittstellenausstattung und zusätzlicher Hardware-Option, CD-ROM mit Applikationssoftware und NDIS-Treiber für LAN-Trace über die integrierte Netzwerkkarte, unterstützt wird der Spiegelport (automatische Duplikatserkennung), Deutsche Dokumentationen. **Optional:** TAP USB 2.0/ 3.0 inkl. Treiber; WAN-Box mit den gewünschten Schnittstellen.

Unterstützte Protokolle:
LAN: 802.2, 802.3, 802.1Q, 802.1p, PPPoE/PPPoA (T-DSL), X.25, X.75 over Ethernet, IPX, Cisco-HDLC, MLP (PPP) Multilink, PPP (alle Control-Protokolle), PAP, CHAP, BAP, LCP, SNAP, ARP, RARP, OSPF, IPv4, IPv6, ICMP, RSVP, IGMP, DHCP, BOOTP, TCP, UDP, RTCP, RTP, H.323**, NetBIOS, DNS, SNMP*, SIP**, Compression Protokolle: LZS Stack (PPP), MPPC Microsoft(PPP), Kerberos, FoIP T.38/ T.30/ T.4, Diameter Radius** u.v.m.
WAN: E-DSS1, Q.931, QSIG(ECMA), X.25,X.75, X.31, MONOSYNC /BISYNC / BSC, V.110**, Frame Relay**, IPX, Cornet T/S, CSTA**, SNA, SS7*, H.323*, V5.1, V5.2, TCP/IP, PPP(auch Multilink), Cisco HDLC, raw IP u.v.m.

Optinale Hardware Module WAN-Box
Modulare Adaption von unterschiedlichen Schnittstellen
- **ISDN S_0** im B-/D-Kanal, max. 8x **S_0**
- **V.24** (max. 2x) synch/asynch.(je120-200kbit)
- **V.11/ X.21** (max. 2x), je max. 2Mbit (vollduplex)
- **S_{2M}** (max. 2x) im D- u. B-Kanal (E1)

Dekodieren und Aufzeichnen:
- Automatische Protokollerkennung und Dekodierung der enthaltenen Protokolle
- Online Defragmentierung v. Protokollen (selektiv abschaltbar
- Monitoring mit mehreren Schnittstellen mit Scroll-Synchronisation bei mehreren Aufzeichnungsfenstern
- Konfigurierbare Duplikatserkennung für Traces am Spiegelport (Mirrorport)
- Umfang der Anzeige konfigurierbar

Speichern, Laden und Drucken:
- Speichern, Laden und Drucken von aufgezeichneten Daten automatisch im Hintergrund oder manuell.
- Ablage gesplitteter Dateien täglich, wöchentlich oder in Intervallen zu frei wählbaren Zeitpunkten inkl. automatischer Erstellung verschiedener Auswertungen und Übersichten.
- Speicherung von Dateien mit benutzerdefinierten Datei-Informationen.
- Automatische Erstellung von Projektdateien mit Zusammenfassung aller Dateien einer Arbeitssitzung.
- Auswertung und Grafiken als PDF, PNG, BMP usw. oder über die Zwischenablage möglich.

Filtern der Daten:
- Filter für Ethernet, IP, PPP, TCP, UDP, HEX-Bytes, Paketlänge.
- Filterung nach Protokollen, Adressen, Rahmentypen, IP-Optionen, Port-Nummern, Fragmente, Richtungen
- Filter wirken wahlweise als Aufzeichnungs- oder Anzeigefilter
- Alle Filter in einer Liste als Filterprofil speicherbar (Liste kann auf andere PCs übertragen werden).
- Logische Verknüpfungen einzelner Filterkriterien.
- Anzeige der aktiven ausgewählten Filterprofile in einer Baumstruktur
- Wechsel zwischen den gefilterten Ansichten innerhalb des Filterbaums
- Verhaltensfilter*

Weitere Eigenschaften der Filter
Alle Filter in einer Liste als Filterprofil speicherbar, Anwendung als Aufzeichnungs oder Anzeigefilter, Logische Verknüpfungen einzelner Filterkriterien. Anzeige der aktiven ausgewählten Filterprofile

Flexible Suchfunktion nach Zeit oder Frame und Textsuche in den dekodierten Daten; Zustandsanzeige aktiv/inaktiv pro Kanal (Fenster)

Protokollschichten 1 / 2 / 3 nach folgenden Kriterien ausblendbar:
- Schicht 1 Daten filtern
- Schicht 2 Daten ausblenden oder/ und Filtern
- Schicht 3 Daten ausblenden oder/ und Filtern

Übersichten:
IP-Pakete: Zeitstempel, Quell- u. Ziel-IP-Adresse, Packet-ID, TTL, Protokoll
TCP-Sitzungen:
Zeitstempel, Quell- und Ziel-IP-Adresse inkl. Portnummern, Dauer, gesendete und empfangene Datenmenge, Wiederholungen
PPP-Verbindungen:
Zeitstempel, Richtung, Versuche, Endpunkt-ID, Login, Transport, Komprimierung, Blockgröße, gesendete Datenmenge, Protokolle
DNS-Auflösungen
Medienverbindungen (ISDN, SIP, H.323 usw.)
Faxübertragungen (Foip T.38/T.30/T.4)

Auswertungen/Statistikfunktionen
Datendurchsatz:
Grafische und numerische Anzeige der Datenrate, getrennt für Rx-/Tx-Richtung. Darstellung absolut oder prozentual, Werte dezimal oder mit binärer Basis, Auflösung von 1 Sekunde bis 1 Stunde pro Messintervall
Grafische Paketflussanalyse:
Die Auslastung der o. g. Funktionen wird in Grafik- und Tabellenanzeigen dargestellt.
Protokollstatistik:
Es wird eine tabellarische und Grafische Übersicht über Summenzähler in Paketen, Bruttovolumen, Nutzlastvolumen und Fehlern für jede dargestellte Strukturschicht angezeigt.
Eine schichtenorientierte Farbgebung der Tabelle wird unterstützt. Grafiken sind speicher- und druckbar.
Protokollfehler:
Grafische Auswertung aller erkannten Protokollfehler, Fehler im TCP-Protokoll.
RTP-Analyse:
Jittermessung für VoIP (SIP**, H.323**)
Top Talker Statistik:
In Tabellen und/oder Grafischer Darstellung wählbar fallend/ steigend. Umfangreiche Filtermöglichkeiten. Grafiken sind speicher- und druckbar u.v.m.
Aktivitätsanalyse von Kommunikationsverbindungen: Paketflüsse lassen sich als Volumendiagramm über der Zeit darstellen.
Sitzungs- Aktivitätsanzeige: Bietet die Möglichkeit Ressourcennutzung einzelner Stationen in Bezug auf unterschiedlichen Kennzahlen und in unterschiedlichen Aggregationen zu analysieren.

Unterstützte Formate:
Sniffer, Acterna Examine, Ethereal (LibPcap), Wireshark Pcapng, transparentes Binärformat.

Dateien können im csv Format gespeichert werden

Optionale Hardware-Ausstattung:
TAP** zur nichtinvasiven Überwachung eines Links.
- Anschluss an dem Messsystem über USB 2.0 und/oder USB 3.0
- Verfügbar bis Gigabit- Ethernet (10/100/1000MBit/s in Kürze 10Gigabit*) (8ns Hardwarezeitstempel)
- Optinale Stromversorgung über USB (1x 5V DC)

Automatische Steuerung über Kommandozeilen-Befehle (Command Line Interface, CLI)**

TLS- Entschlüsselung**
Verschlüsselte Rufe (SRTP) können entschlüsselt werden (sofern Schlüssel und Passwort bekannt sind).

In Vorbereitung:
Alarmierung bei Verhaltensmustern*+**
„EasyTrace Script- Sprache- Modul. Das Modul bietet z.B. die Möglichkeit bei einer Daueraufzeichnung des Netzverkehr´s viele Bedingungen zu hinterlegen um Alarme auszulösen. Folgende Themen können mit dem Erweiterungmodul abgesichert werden: Ereignisse, Manipulationen, Angriffe usw.

Web-Interface**: - aktuelle Snapshots ausgewählter Ansichten (Statistiken) können über eine Webschnittstelle, mit erweiterten Funktionsumfang auch per Smartphone, für definierbare Anwender zugänglich gemacht werden.(Auf Grund von Limitierungen des Übertragungsnetzes kann hier grundsätzlich keine Live-Funktion angeboten werden.

*= in kürze verfügbar **= Optional erhältlich

HERAKOM GmbH
Wolfsbachweg 62, 45133 Essen, Tel. 0201 / 46694223, Fax: 0201 / 46694232, E-Mail: Heikeh@Herakom.de, http://www.herakom.de
HRB Essen 11 694, Steuernummer: 112/5960/0479, Ust.-Id-Nr.: DE 811945307, Geschäftsführerin: Heike Hüttemann
Bankverbindung: Sparkasse Essen Haarzopf, BLZ 360 501 05, Kto. Nr. 3 303 393