WIRE**SHARK** Newsletter März 2010

Dieser Wireshark Newsletter von Leutert NetServices informiert Sie regelmässig in Kürze über wichtige Neuerungen im Zusammenhang mit dem führenden Open Source Analyser Wireshark und dem Monitoring & Reporting Tool CACE PILOT.

Schlagzeilen:

- WIRESHARK Versionen 1.2.2 / 1.2.3 / 1.2.4/ 1.2.5/ 1.2.6
- Neu: Shark Appliance, verteilte Gigabit Analyse mit Wireshark und Pilot
- Tipps, Tricks & Talks: Wireshark Expert
  Wie nutze ich das Wireshark Expert System für die Fehlersuche?
- Hinweise: Daten nächster Wireshark Kurse und Präsentationen

Neue Features der Wireshark Versionen 1.2.2 bis 1.2.6

Die fünf Wireshark Versionen 1.2.2 bis 1.2.6 enthalten vorwiegend ‚Bug Fixes' und zahlreiche Erweiterungen von bereits decodierten Protokollen, hier die Liste in alphabetischer Reihenfolge:

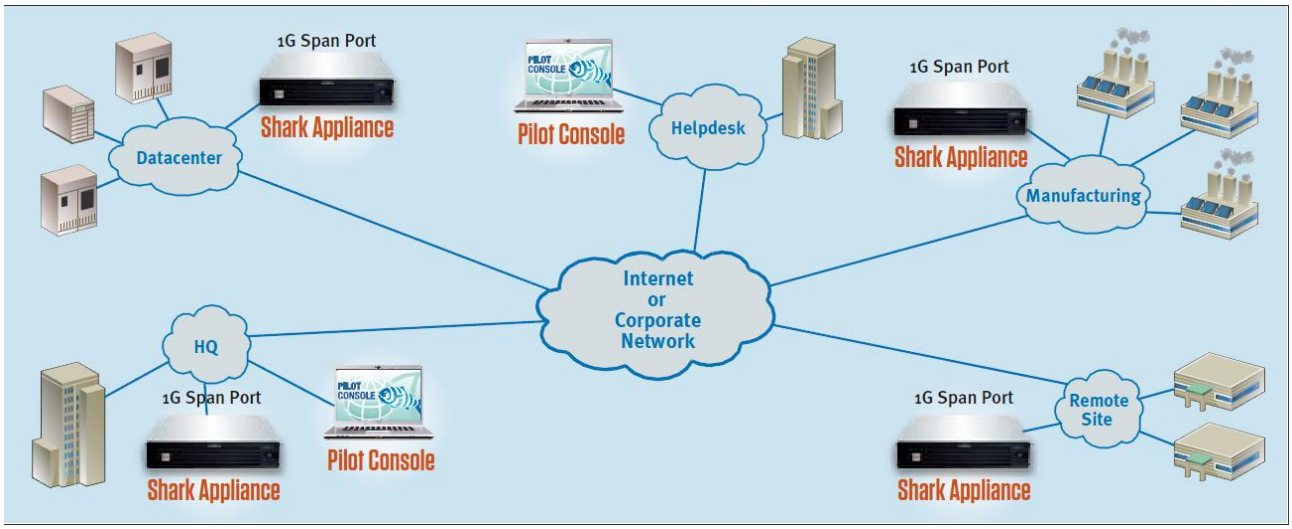
BJNP, BOOTP/DHCP, DAP, DCERPC, DCERPC NT, DHCP, DHCPv6, Diameter, DNS, E.212, eDonkey, FIP, FIP, GPRS LLC, GSM A RR, GTP, GTPv2, H.248, IEEE 802.11, IP, IPFIX/Netflow, IPMI, IPsec, ISAKMP/IKE, ISUP, Kerberos, Kingfisher, LDAP, MGCP, MIP, NAS EPS, NCP, OPCUA, Paltalk, RADIUS, RANAP, RSL, RTCP, SBus, SCTP, SIP, SMB, SMB2, SNMP, SSL, TCP, Teamspeak2, TIPC, TTE, VNC, WBXML, WPS, X.509sat, ZRTP

Neu: Wireshark Analyse mit verteilten Shark Appliances

Wie bereits am SharkFest'09 angekündigt, stellt die Trägerfirma von Wireshark, CACE Technologies (ausgesprochen wie Case) unter dem Namen ‚Shark Distributed Monitoring System' (SDMS) eine kostengünstige Produktelinie für die verteilte Aufzeichnung und Analyse vor. Damit eröffnen sich neue Möglichkeiten für die permanente Fern-Überwachung von wichtigen Punkten in Ihrem Netzwerk unter Weiterverwendung des professionellen Open-Source Analysetools Wireshark.

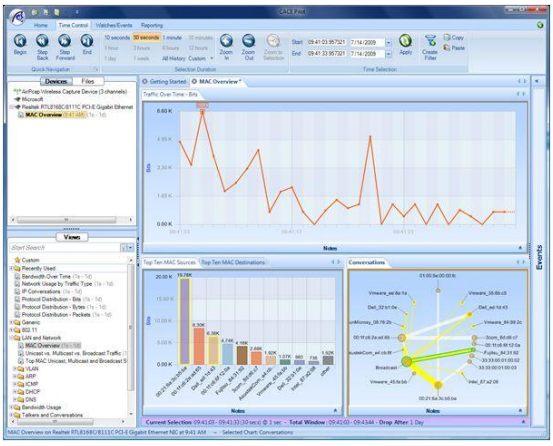
LEUTERT NetServices
Phone +41 79 430 55 23
leutert@wireshark.ch
www.wireshark.ch
Steigstrasse 28
CH-8307 Effretikon

Ein Shark Distributed Monitoring System besteht aus verteilt platzierten, fertig konfigurierten Hardware Einheiten, sogenannten Shark Appliances, der zentralen Überwachungs-, Reporting- und Alarmierungssoftware Pilot Console und Wireshark für die detallierte Paketanalyse.



Verteilt platzierte Shark Appliances überwacht durch eine oder mehrere Pilot Consolen

Die Pilot Console basiert auf der bereits seit Anfang 2009 als standalone Version verfügbaren Cace Pilot Software, beide sind von der Bedienung her identisch.
Bei der Verarbeitung von sehr grossen Files stösst man mit Wireshark an Grenzen, Pilot ermöglicht auf einfache Art mit grafischen Filtern diese Rohdaten (bis TB) zu reduzieren, bevor diese mit einem Mausclick an Wireshark für die detaillierte Paketanalyse übergeben werden.
Bereits erworbene Cace Pilot Lizenzen können auf die Pilot Console aufgerüstet werden.



Shark Appliance SA-104

Shark Appliance SA-208

Die Shark Appliance wird zurzeit in zwei Ausführungen angeboten und unterstützt Datenaufzeichnung mit Wirespeed von Full-Duplex Gigabit Links und ist bestückt mit einer (SA-104) oder zwei (SA-208) Dual-Port-TurboCap Ethernet Adapter von CACE Technologies.
Auf einem optimierten Linux basiert der Shark Packet Redorder, welcher die Daten auf RAID arrangierten Hardisks von 4 TB (SA-104) oder 8 TB (SA-208) speichert. Auch grössere Speichervolumen sind auf Anfrage möglich.

Als Variante zu den fertig konfigurierten Shark Appliances, bietet Cace Technologies die Möglichkeit, mit Hilfe des Shark Appliance Kits eine eigene Einheit zusammenzustellen.
Der Kit besteht aus der notwendigen Software und wahlweise aus einem (SAK-100), oder zwei (SAK-200) Dual-Port-TurboCap Gigabit Ethernet Adapter. Dazu benötigen Sie für die Überwachung / Steuerung noch mindestens eine Pilot Console Lizenz.

Mehr Informationen und Preise finden Sie auf unserer Webseite unter www.wireshark.ch.
Leutert NetServices unterstützt Sie als exklusiver Reseller von CACE Technologies für die Schweiz gerne in der Auswahl der optimalen Konfiguration. Kontaktieren Sie uns für eine Demonstration in Ihrer Firma oder für eine Testinstallation in Ihrem Netzwerk.

Tipps, Tricks & Talks

Wie nutze ich das Wireshark Expert System für die Fehlersuche?

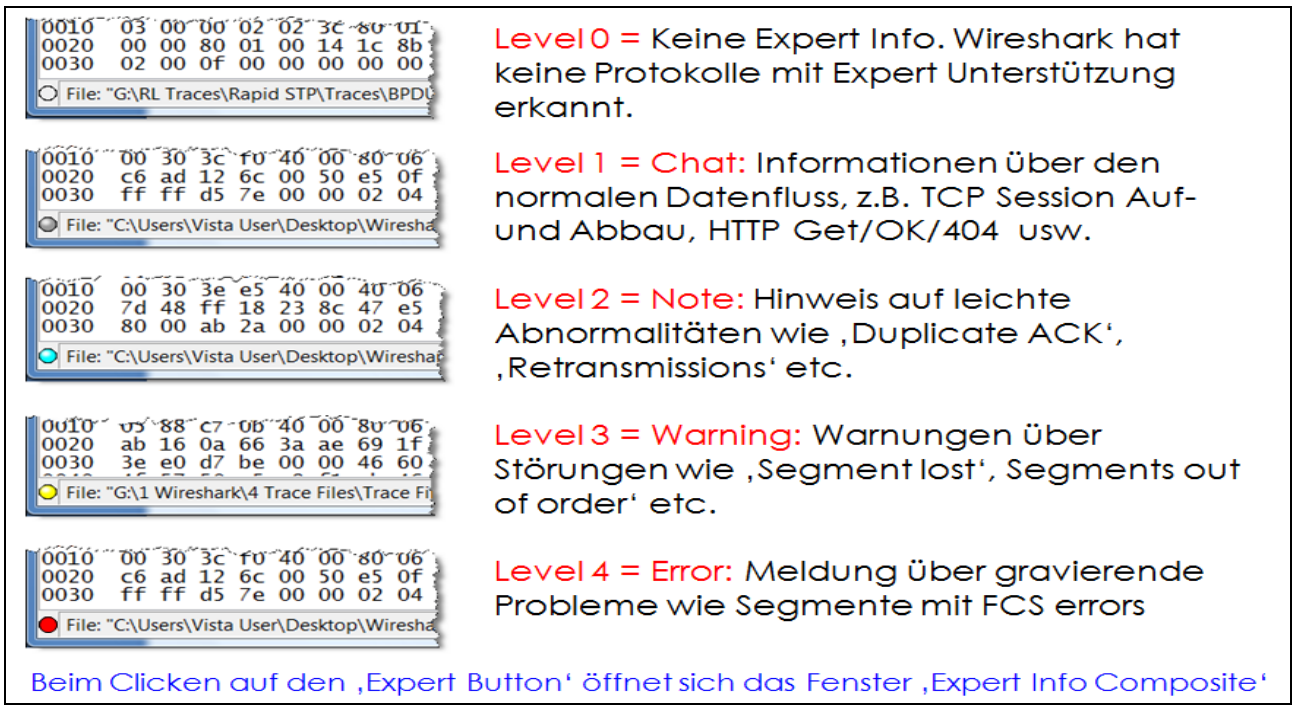
Zuerst klären wir die Frage:
Was ist der Unterschied zwischen einem Protokoll Analyser mit und ohne Expert System?

Ein Analyser wie Wireshark decodiert möglichst viele verschiedene Protokolle (beim Wireshark sind es inzwischen gegen 1'000) in hohem Detaillierungsgrad, zeigt möglichst alle Header und Felder und versieht diese mit kurzen Erklärungen oder Kommentaren. Diese Funktion ist zwar sehr aufwändig und wertvoll für die Fehlersuche, stellt jedoch noch kein Expert System dar, da jedes Paket und Protokoll nach fixen Regeln zerlegt und dargestellt wird.

Ein Expert System versucht in einem ganz spezifischen Gebiet (in unserem Fall Netzwerkprotokolle) Probleme zu erkennen und dazu Kommentare und Entscheidungshilfen anzubieten.

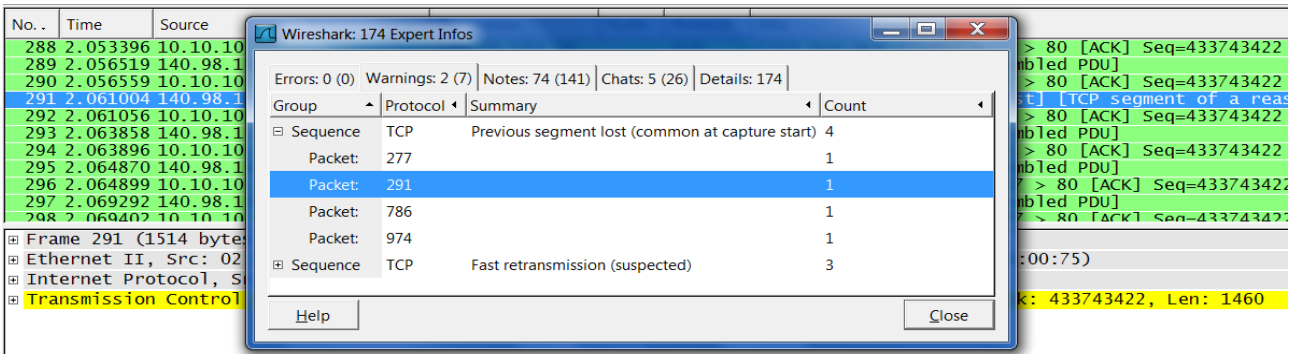
Diese Funktion ist nur möglich, wenn die Pakete nicht als einzelne Einheiten behandelt werden, sondern in ihrem Zusammenhang und zeitlichen Ablauf interpretiert werden. Das heisst, ein Expert Analyse System kennt die wichtigsten Abläufe z.B. einer TCP Session und ist in der Lage, in den verschiedenen Phasen Abnormalitäten zu erkennen und zu gewichten.
Eine weitere Bedingung ist, dass ein Protokoll überhaupt vordefinierte Abläufe kennt, dieses wird dann als ‚stateful' bezeichnet (z.B. TCP); bei einem ‚stateless' Protokoll wie z.B. UDP kann ein Expert System keine Unterstützung bieten.
Wireshark bietet Expert System Unterstützung für das TCP Protokoll, analysiert sämtliche TCP Sessions und meldet mit Hinweisen und Warnungen allfällige Abnormalitäten. Diese werden nach ihren möglichen Schweregrad (Severity) in Gruppen geordnet.

Der Wireshark Expert zeigt den höchsten vorkommenden Störungslevel mit entsprechendem Farbcode im ‚Expert Button' links unten.



Quelle: Kurs ‚TCP/IP Analyse mit Wireshark' von Leutert NetServices

Das Fenster ‚Expert Info Composite' zeigt die erkannten Symptome, geordnet nach den verschiedenen Fehlerlevel und versehen mit den entsprechenden Paketnummern. Beim Anclicken einer Fehlermeldung, springt Wireshark im Hintergrund auf die entsprechende Paketnummer.



Das Wireshark Expert System kann bei der Analyse von Aufzeichnungen mit vielen TCP Sessions wertvolle Unterstützung leisten, jedoch detaillierte Protokoll-Kenntnisse nicht ersetzen.
Das TCP Protokoll ist sehr robust und kann viele Fehlersituationen selbstätig korrigieren, so dass sich eine Fehlersituation nicht zwangsläufig negativ auswirken muss.

Verwenden Sie deshalb die Meldungen des Expert Systems als Hinweise, welche Sie in die Beurteilung der Situation zusammen mit anderen Fakten mit einbeziehen.

Hinweise

Die nächsten öffentlichen Wireshark Kurse und Präsentationen:

IPv6 Netzwerkanalyse mit Wireshark

Datum:	31.05.2010 - 01.06.2010 (2 Tage)
Ort:	Comicro-Netsys, Wangen
Kurs-Details und Anmeldung bei	Comicro-Netsys

Wireshark - VoIP Sniffer Kurs

Datum:	07.06.2010 - 08.06.2010 (2 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

WLAN Netzwerkanalyse mit Wireshark und AirPcap

Datum:	12.07.2010 - 14.07.2010 (3 Tage)
Ort:	Comicro-Netsys, Wangen
Kurs-Details und Anmeldung bei	Comicro-Netsys

TCP/IP Netzwerkanalyse mit Wireshark

Datum:	01.11.2010 - 03.11.2010 (3 Tage)
Ort:	Comicro-Netsys, Wangen
Kurs-Details und Anmeldung bei	Comicro-Netsys

Leutert NetServices präsentiert am Heise IPv6 Kongress vom 20. und 21. Mai 2010 in Frankfurt ein technisches Tutorial zum Thema "IPv6 entdecken mit Wireshark".

Leutert NetServices präsentiert am SHARKFEST '10 vom 14. bis 17. Juni 2010 in Palo Alto, Kalifornien bereits zum dritten Mal Sessions über die praktische Anwendung von Wireshark für Protokollanalyse und Troubleshooting.

Besten Dank für Ihr Interesse
Mit freundlichen Grüssen Rolf Leutert