WIRESHARK / PILOT NEWSLETTER Januar 2009

Dieser Wireshark Newsletter von Leutert NetServices informiert Sie regelmässig in Kürze über wichtige Neuerungen im Zusammenhang mit dem führenden Open Source Analyser Wireshark. Durch den Erfolg des neuen, kostengünstigen Reporting Tools PILOT, werden wir ab dieser Ausgabe auch über wichtige Neuerungen zu diesem Produkt informieren. Benutzen Sie das Kontaktformular auf unserer Webseite www.wireshark.ch für eine 30-tägige, kostenlose PILOT Test-Lizenz.

Neuheiten:

- WIRESHARK Versionen 1.0.3 / 1.0.4 / 1.0.5
- PILOT Versionen 1.1 /1.2
- AirPcap Nx Dualband für 802.11a/b/g/n in USB Bauform
- Wi-Spy DBx Dualband für 2.4 GHz und 5 GHz Frequenzen

Tipps & Tricks:

- Wie wird die „VLAN Tag“ Anzeige im Ethernet Driver und Wireshark aktiviert?

Hinweise:

- SHARKFEST’09 in Kalifornien 15. – 18. Juni 2009
- Daten nächster Wireshark Kurse

Neue Features der Wireshark Versionen 1.0.3 / 1.0.4 und 1.0.5

Diese drei Versionen enthalten vorwiegend ‚Bug Fixes’, beheben einige Crash-Situationen und erweitern das Dekodieren von bestehenden Protokollen.

- **Wireshark Version 1.0.3 - Erweiterungen an bestehenden Protokollen**

AIM, Bluetooth RFCOMM, ERF, K12, NCP, PPP BCP, PPPoE, Q.933, Redback LI, RTCP, RTP, SIP, SNMP, TCP, V.120, WiMAX

- **Wireshark Version 1.0.4 - Erweiterungen an bestehenden Protokollen**

AFP, Bluetooth ACL, Bluetooth RFCOMM, DCP ETSI, DTLS, Homeplug, IEEE 802.11, IP, Modbus TCP, MP2T, NSIP, NCP, PPI, Q.931, SASL, SNMP, USB, WPS

- **Wireshark Version 1.0.5 - Erweiterungen an bestehenden Protokollen**

ANSI MAP, BSSGP, CIP, Diameter, ENIP, GIOP, H.263, H.264, HTTP, MPEG PES, PostgreSQL, PPI, PTP, Rsync, RTP, SMTP, SNMP, STANAG 5066, TACACS, TIPC, WLCCP, WSP

Neuer AirPcap Adapter für WLAN 802.11a/b/g/n in USB 2.0 Bauform

Der AirPcap Nx Adapter decodiert sämtliche WLAN Frames in den Frequenzbändern 2.4 GHz und 5 GHz, unterstützt die bekannten Standards 802.11a/b/g und als Besonderheit die neuen 802.11n Funktionen wie Channel Bonding, Multiple-In / Multiple-Out (MIMO) mit Übertragungsraten bis 300Mbps.
Mehr Informationen und Preise finden Sie auf unserer Webseite.

Durch die USB-Bauform können mehrere Adapter über einen USB-Hub kombiniert und dadurch gleichzeitige Aufzeichnungen in mehreren WLAN Kanälen durchgeführt werden. Eine ideale Funktion beim Eingrenzen von Roaming-Problemen.

Neuer Wi-Spy Adapter für WLAN 802.11a/b/g/n in USB 2.0 Bauform

Der bewährte low-cost Spectrum Analyser ist nun auch als Dual-Band Adapter für 2.4 GHz und 5GHz Frequenzbänder erhältlich.
Wi-Spy DBx hilft beim Lokalisieren von Störquellen in den WLAN Frequenzbändern und ist die ideale Ergänzung zu den AirPcap Adaptern für die Fehlersuche.

Mehr Informationen und Preise finden Sie auf unserer Webseite.

Wireshark Tipps & Tricks

Thema: Wie wird die „VLAN Tag“ Information im Wireshark aktiviert?

Virtual Local Area Networks (VLANs) werden häufig zum Segmentieren von physischen Komponenten in mehrere logische Einheiten eingesetzt. Um die Zugehörigkeit zu einem bestimmten VLAN zu kennzeichnen, versehen Switches die Frames mit einem zusätzlichen Feld, dem so genannten VLAN Tag, welches u.a. die VLAN Nummer enthält. Während früher mehrere proprietäre Verfahren verwendet wurden, ist heute IEEE 802.1q (auch ‚dot one q’ genannt) der Standard für VLAN tagging.

Frames mit VLAN Header können auf verschiedene Arten, z.B. mit Hilfe von Mirror Ports oder Network Taps aufgezeichnet werden. Die Beschreibung dieser Methoden ist jedoch nicht Thema dieser Beschreibung, detaillierte Informationen dazu finden Sie bei den entsprechenden Switch Herstellern.

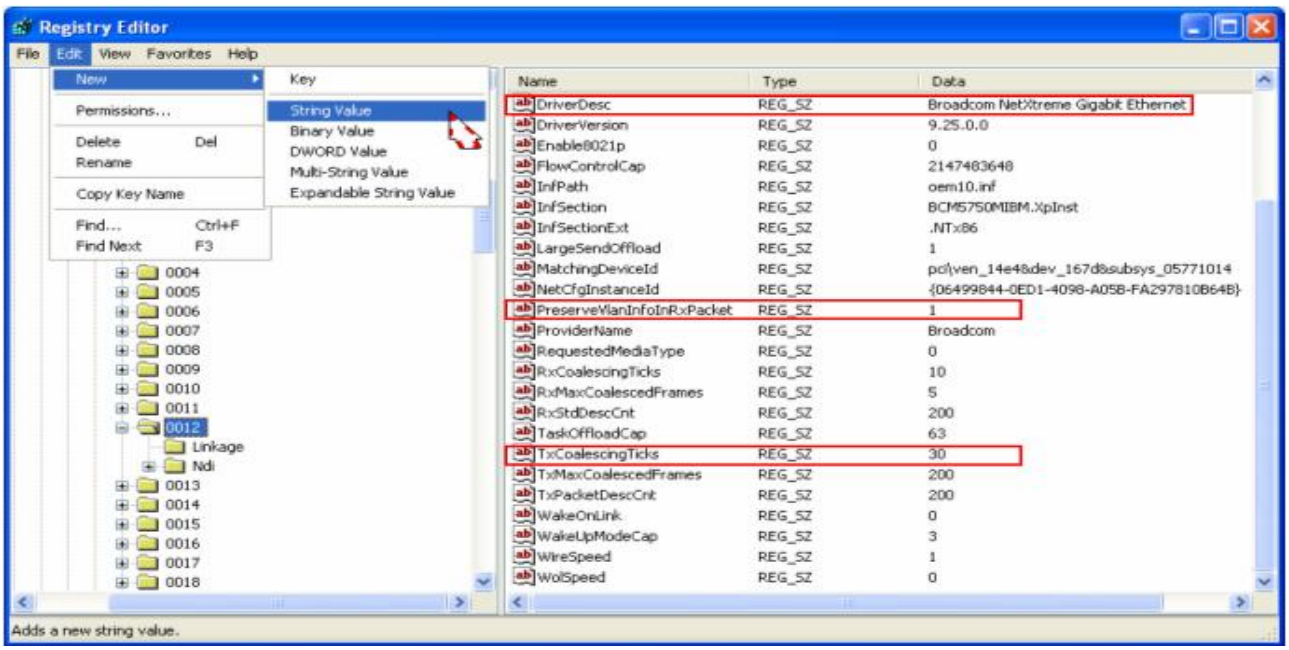
Problem: Die meisten Ethernet Adapter Driver von Notebooks unter Windows verwerfen entweder die Frames mit VLAN Header oder entfernen den VLAN Tag vor der Verarbeitung. Dadurch können diese Frames von Wireshark entweder gar nicht oder nur ohne VLAN Information dargestellt werden.

Lösung: Die grosse Mehrheit heutiger Notebooks basiert auf Ethernet Adaptern entweder von BROADCOM oder INTEL. Mit entsprechenden Änderungen in der Windows Registry können die Driver für diese Adapter so konfiguriert werden, dass sie die Frames inklusive VLAN Header an Wireshark weitergeben. Bitte beachten Sie, dass Änderungen in der Windows Registry mit grosser Sorgfalt und nur von erfahrenen Personen vorgenommen werden sollten.

Anleitung für „Broadcom NetXtreme Gigabit Ethernet“ Adapter

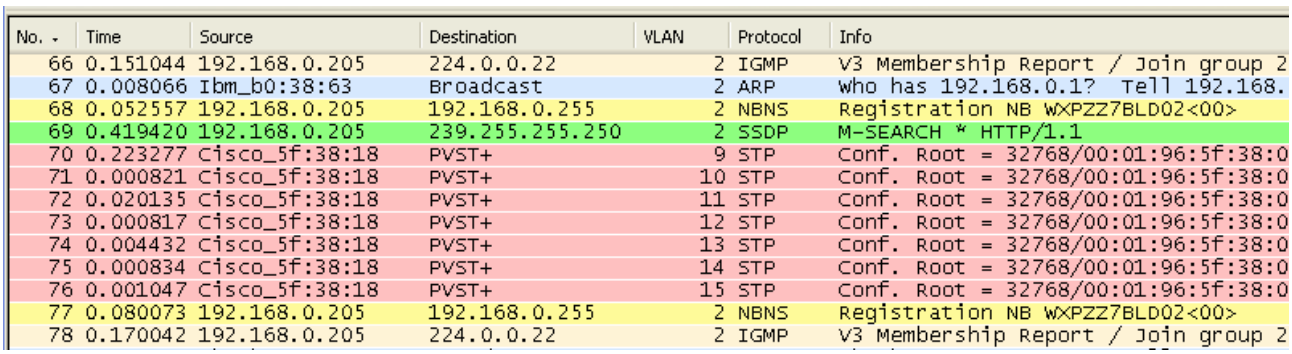
1. Suchen Sie in der Registry nach dem String „TxCoalescingTicks"
2. Verifizieren Sie durch weitersuchen, dass dieser Eintrag nur an diesem Ort (z.B. \0012) existiert.
3. Verifizieren Sie, das Sie am selben Ort (z.B. \0012) unter „DriverDesc“ den Adapter „Broadcom NetXtreme Gigabit Ethernet“ finden.
4. Suchen sie am selben Ort nach dem String „PreserveVlanInfoInRxPacket“
5. Falls der String schon existiert, fahren Sie weiter mit Schritt 7, sonst mit Schritt 6

6. Falls dieser String noch nicht existiert, eröffnen Sie ihn an dieser Stelle mit Edit > New > String Value und geben den Namen „PreserveVlanInfoInRxPacket“ ein. (Schreibweise ohne „“)
7. Klicken Sie mit der rechten Maus auf das Feld und wählen Sie „Modify“
8. Ändern Sie das Feld „Value Data“ auf den Wert 1
9. Starten Sie den Notebook neu, die VLAN Tags sind dann in Wireshark sichtbar.



Suchen Sie auf der Webseite Ihres Ethernet Adapter Herstellers nach „VLAN Support“. Die original Anleitung von Intel in Englisch finden Sie unter:
http://support.intel.com/support/network/sb/cs-005897.htm

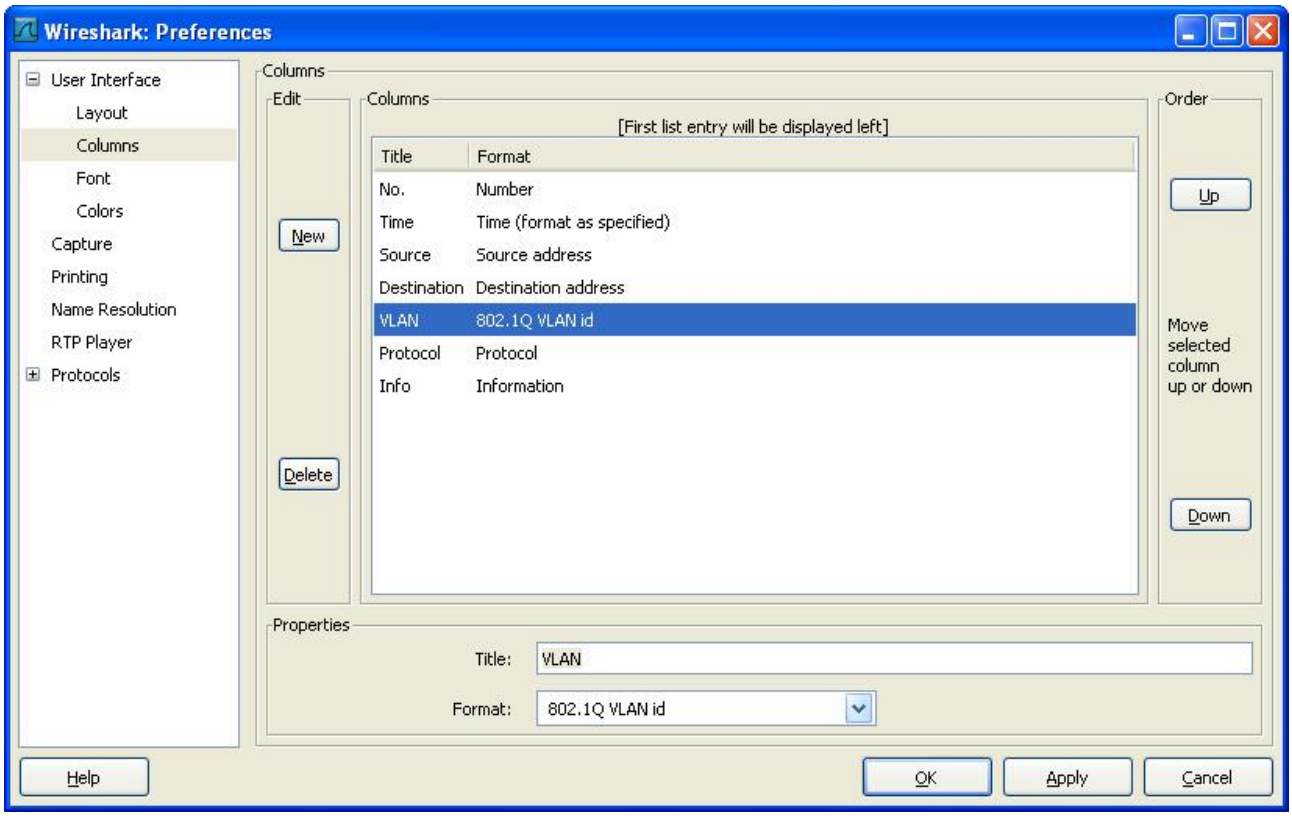
Anzeigen der VLAN Kolonne im Wireshark



No.	Time	Source	Destination	VLAN	Protocol	Info
66	0.151044	192.168.0.205	224.0.0.22	2	IGMP	V3 Membership Report / Join group 2
67	0.008066	Ibm_b0:38:63	Broadcast	2	ARP	Who has 192.168.0.1? Tell 192.168.
68	0.052557	192.168.0.205	192.168.0.255	2	NBNS	Registration NB WXPZZ7BLD02<00>
69	0.419420	192.168.0.205	239.255.255.250	2	SSDP	M-SEARCH * HTTP/1.1
70	0.223277	Cisco_5f:38:18	PVST+	9	STP	Conf. Root = 32768/00:01:96:5f:38:0
71	0.000821	Cisco_5f:38:18	PVST+	10	STP	Conf. Root = 32768/00:01:96:5f:38:0
72	0.020135	Cisco_5f:38:18	PVST+	11	STP	Conf. Root = 32768/00:01:96:5f:38:0
73	0.000817	Cisco_5f:38:18	PVST+	12	STP	Conf. Root = 32768/00:01:96:5f:38:0
74	0.004432	Cisco_5f:38:18	PVST+	13	STP	Conf. Root = 32768/00:01:96:5f:38:0
75	0.000834	Cisco_5f:38:18	PVST+	14	STP	Conf. Root = 32768/00:01:96:5f:38:0
76	0.001047	Cisco_5f:38:18	PVST+	15	STP	Conf. Root = 32768/00:01:96:5f:38:0
77	0.080073	192.168.0.205	192.168.0.255	2	NBNS	Registration NB WXPZZ7BLD02<00>
78	0.170042	192.168.0.205	224.0.0.22	2	IGMP	V3 Membership Report / Join group 2

Eröffnen Sie dazu unter ‚Edit Preferences' eine neue Kolonne mit dem Titel ‚VLAN' und wählen Sie unter ‚Format' den Wert ‚802.1Q VLAN id' (oberste Zeile in der Auswahl).

Positionieren Sie die VLAN Kolonne mit den Tasten ‚Up/Down'



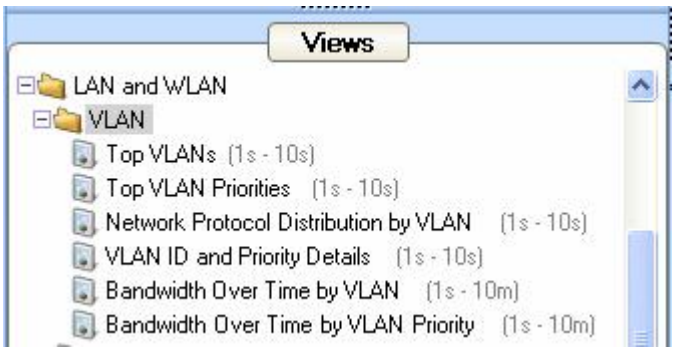
Einfügen einer Kolonne mit VLAN Nummer

PILOT
Network Analysis, Visualization and Reporting

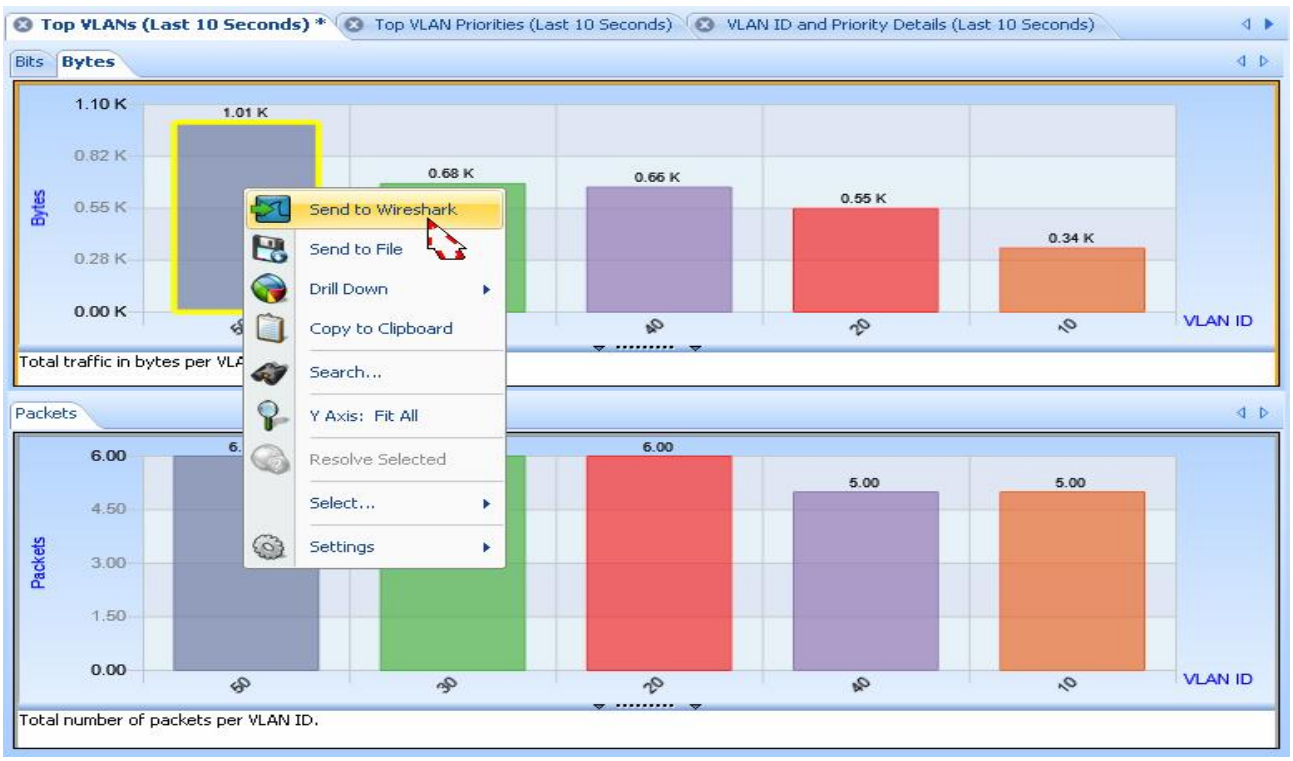
Neue Features der PILOT Versionen 1.1 und 1.2

- **Pilot Version 1.1 - Neue Views für spezielle VLAN Reports**

Views sind die vorgefertigten Reports und Statistik-Ansichten, welche durch einfaches Anklicken die entsprechende Darstellung generieren.

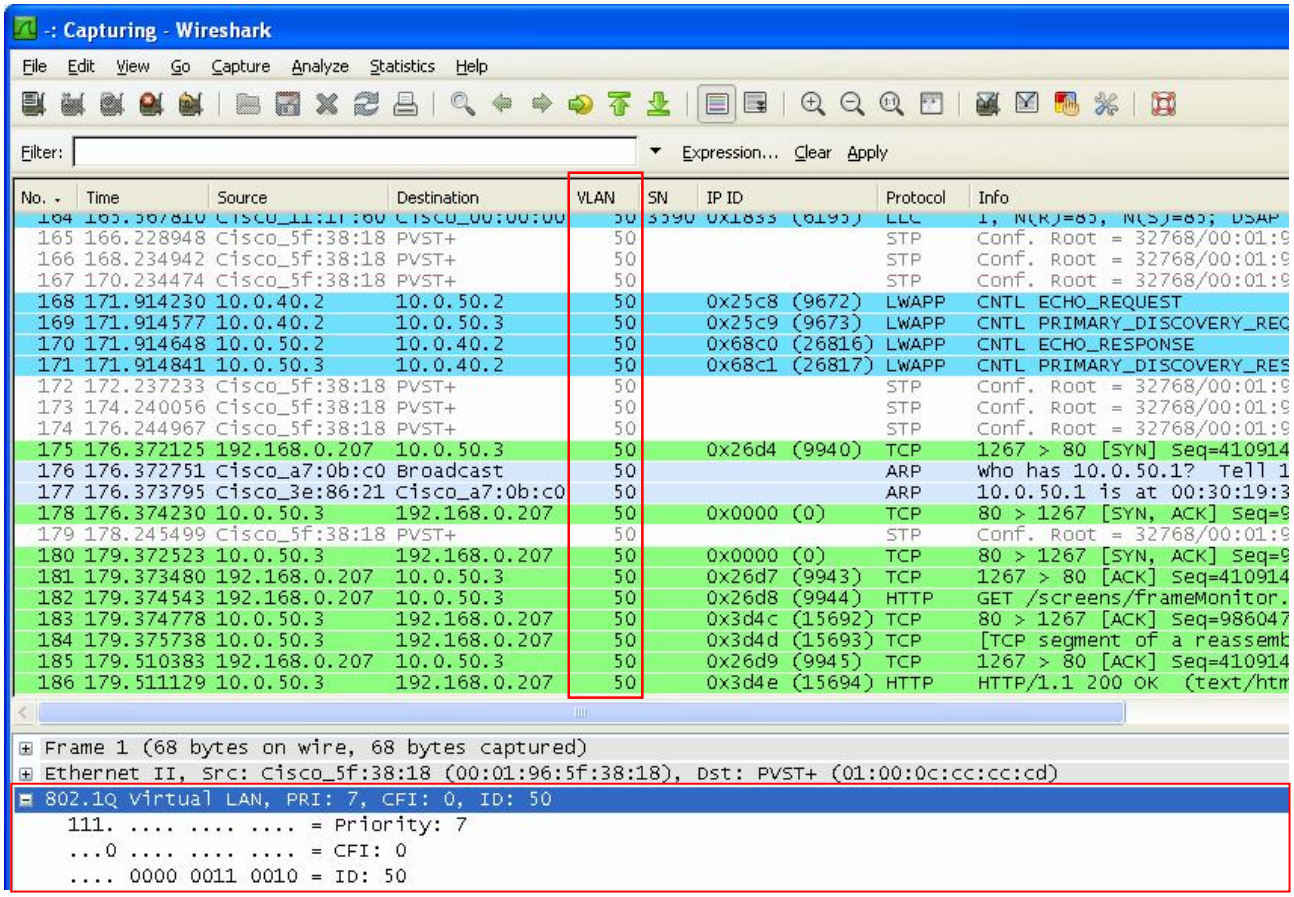


Die „Top VLANs“ View zeigt VLAN Nummern (50 – 10) geordnet nach Datenmengen:



Durch Markieren eines VLANs (z.B. 50) und wählen der Funktion „Send to Wireshark“ wird Wireshark geöffnet und alle Pakete von VLAN 50 angezeigt.

Anzeige der gefilterten Pakete von VLAN 50:



Hinweis:
Bitte lesen sie unter „Wireshark Tipps & Tricks“ wie sie die Decodierung und Anzeige der VLAN Felder im Ethernet Driver und Wireshark aktivieren.

- **Pilot Version 1.2 – Zahlreiche neue Views und Reports** (erhältlich seit 23. Januar 2009)

Mehr als zwei Duzend neue Views erweitern die Statistik- und Reporting-Möglichkeiten, u.a.:

- Application Bandwidth Over Time
- Burst Bandwidth
- Bandwidth Over Time
- Frame Size Over Time
- IP Conversations Discovery
- Top IP Talkers (based on sent + received data)
- Active Hosts Over Time
- Top 24 Subnets

Diese Version steht ab sofort zum Download in Ihrem PILOT Account zur Verfügung.

Hinweise:

- SHARKFEST'09

Nach dem Erfolg vom letzten Jahr findet auch im 2009 wieder die Wireshark Developer und User Konferenz statt. Organisator ist die Trägerfirma von Wireshark, CACE Technologies. Rolf Leutert von Leutert NetServices wird auch dieses Jahr wieder einige Session präsentieren. Die detaillierte Agenda wird in Kürze auf der Webseite publiziert. Es würde und freuen Sie dort begrüssen zu dürfen. Weitere Infos und Anmeldung unter:

http://www.cacetech.com/sharkfest.09/

- Die nächsten Wireshark Kurse:

Wireshark - VoIP Sniffer Kurs

Datum: 23.02.2009 - 24.02.2009 (2 Tage)
Ort: Hochschule Rapperswil INS, Rapperswil (CH)
Weitere Details und Anmeldung bei http://www.mylearning.ch/voice-over-ip/sniffer-workshop/

Wireshark – Wireless Training

Datum: 24.03.2009 - 26.03.2009 (3 Tage)
Ort: Schoeller network control, Wien (A)
Weitere Details und Anmeldung bei http://www.wireshark.at

Wir freuen uns über Ihren Besuch am SHARKFEST'09 oder an einem unserer Kurse

Mit freundlichen Grüssen Rolf Leutert