WIRE**SHARK** Newsletter Juli 2009

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:

Bericht zum SHARKFEST'09 in Kalifornien 15. – 18. Juni 2009

Zum zweiten Mal fand am 15. – 18. Juni 2009 in lockerem, aber sehr lehrreichem Ambiente die Wireshark User & Developer Konferenz statt. Diesmal im Campus der renommierten Stanford University, im Silicon Valley. Mit dem Event verbindet CACE Technologies, die Trägerfirma von Wireshark, verschiedene Ziele: Durch den Einsatz von Wireshark will sie vertieftes Protokoll-Know-how vermitteln, mit dem Analyser verwandte Produkte vorstellen und gemeinsam mit Entwicklern wie Usern neue Funktionen und künftige Weiterentwicklungen definieren.


Stanford University, California

Themen im Bereich Netzwerk-Monitoring und -Analyse wurden in verschiedenen Learning Tracks für Entwickler, Einsteiger und Fortgeschrittene diskutiert. Die dort vorgestellten Neuentwicklungen konzentrieren sich auf die Bereiche WLAN, VoIP, Security und Highspeedanalyse bis 10 GBit/s.

Alle Präsentationen können unter http://www.cacetech.com/sharkfest.09/ heruntergeladen werden. Ich präsentierte die Session: „BU-5 (Leutert) Analyzing WLANs with Wireshark & AirPcap"

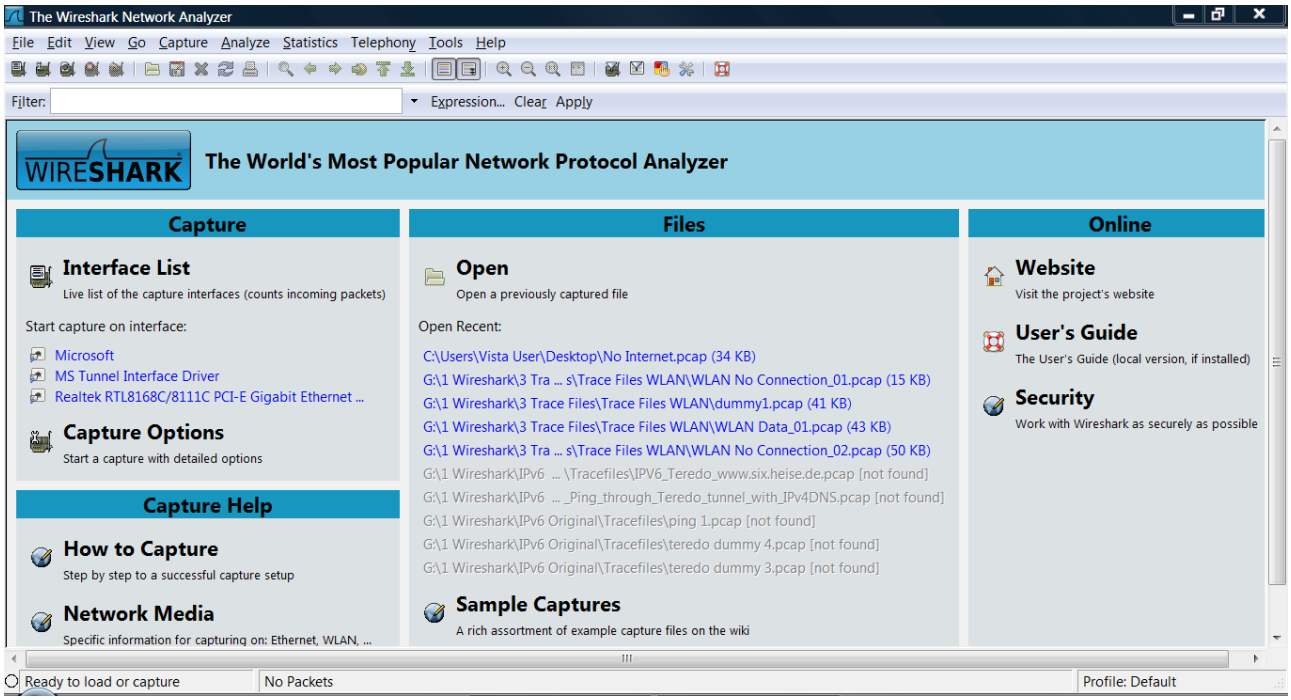
← Benutzer, Entwickler und Core Designer in einer Runde; ganz rechts, **Gerald Combs**, Urentwickler von Ethereal/ Wireshark.

Im Gegensatz zu anderen Firmen, welche ihre Core Entwickler möglichst abschirmen, finden hier Diskussionen über Anregungen, Wünsche und Verbesserungsvorschläge in zwanglosem Rahmen statt. Solche Sessions und der direkte Kontakt zu den Benutzern tragen dazu bei, die Position von Wireshark als das erfolgreichste Analysetool weiter zu festigen.

Neue Features der Wireshark Versionen 1.0.6 / 1.0.7 / 1.0.8 und 1.2.1

Die drei Versionen 1.0.6 / 1.0.7 / 1.0.8 enthalten vorwiegend ‚Bug Fixes', beheben einige Crash-Situationen und erweitern das Dekodieren von bestehenden Protokollen. Die Version 1.2.0 respektive **1.2.1** enthält zahlreiche neue Funktionen, die wichtigsten werden hier vorgestellt:

Neue Wireshark Startup Seite

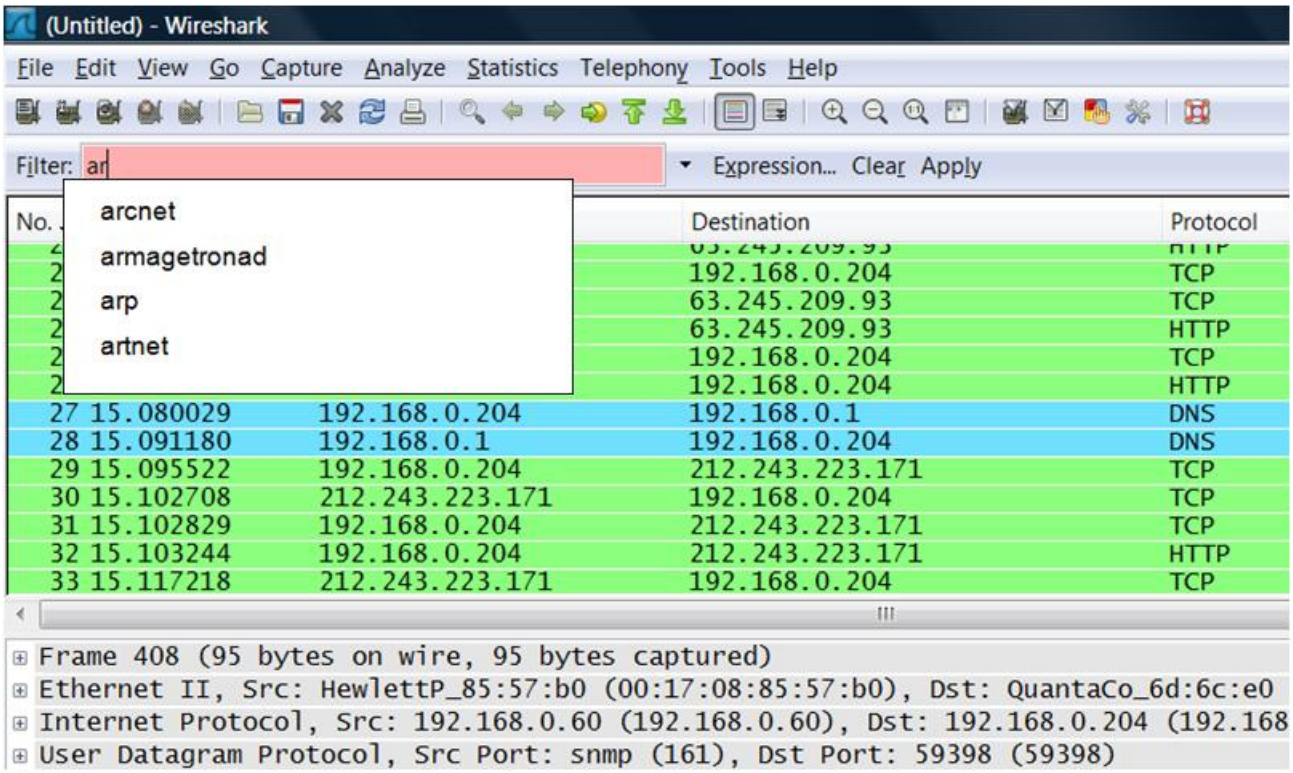


Ein wenig gewöhnungsbedürftig, aber nach kurzer Zeit sehr praktisch präsentiert sich die neue Einstiegseite von Wireshark. Rechnung getragen wurde hier vor allem den zahlreichen Gelegenheitsbenutzern von Wireshark; sind doch die wichtigsten Funktionen wie ‚Interface List', ‚List of previously captured files' und einige Links zu Help direkt von dieser Seite wählbar.
Der Capture Vorgang kann direkt durch Anklicken eines der ‚Capture Interfaces' gestartet werden.

Für alle welche Wireshark nach wie vor über die Icons oder Pull-Down-Menüs bedienen wollen hat sich jedoch nichts geändert.

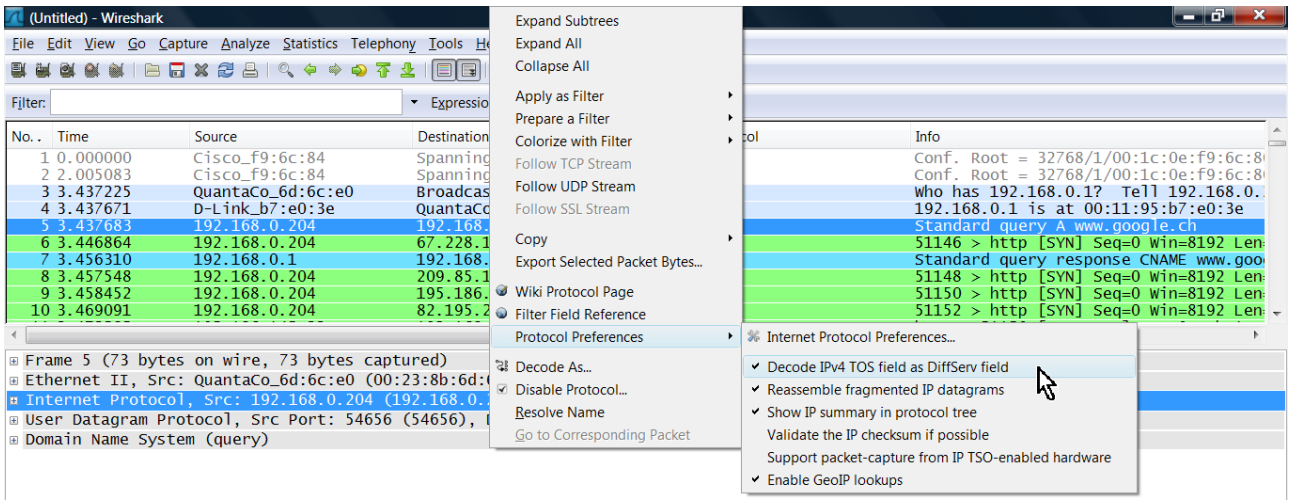
Neu wird Wireshark mit dem zuletzt verwendeten ‚Configuration Profile' und den zuletzt eingestellten Kolonnen-Breiten aufgestartet. Einige Probleme (Crashes) habe ich jedoch unter Windows Vista beim Verwenden von verschiedenen Profilen festgestellt. Falls nicht bereits ein entsprechenden Bug Report existiert, werde ich einen eröffnen.

Display Filter autocomplete



Diese Funktion erleichtert die Eingabe von Display-Filtern durch Anbieten aller Eingabemöglichkeiten, welche mit den bereits eingegebenen Buchstaben oder Zahlen (im Beispiel ar) noch zur Verfügung stehen (bekannt z.B. von Google). Durch Doppelklick auf eine der angebotenen Möglichkeiten wird diese als Filter-String übernommen und mit ‚Apply' aktiviert.

Erweiterte Konfigurationsmöglichkeiten mit rechtem Mausklick

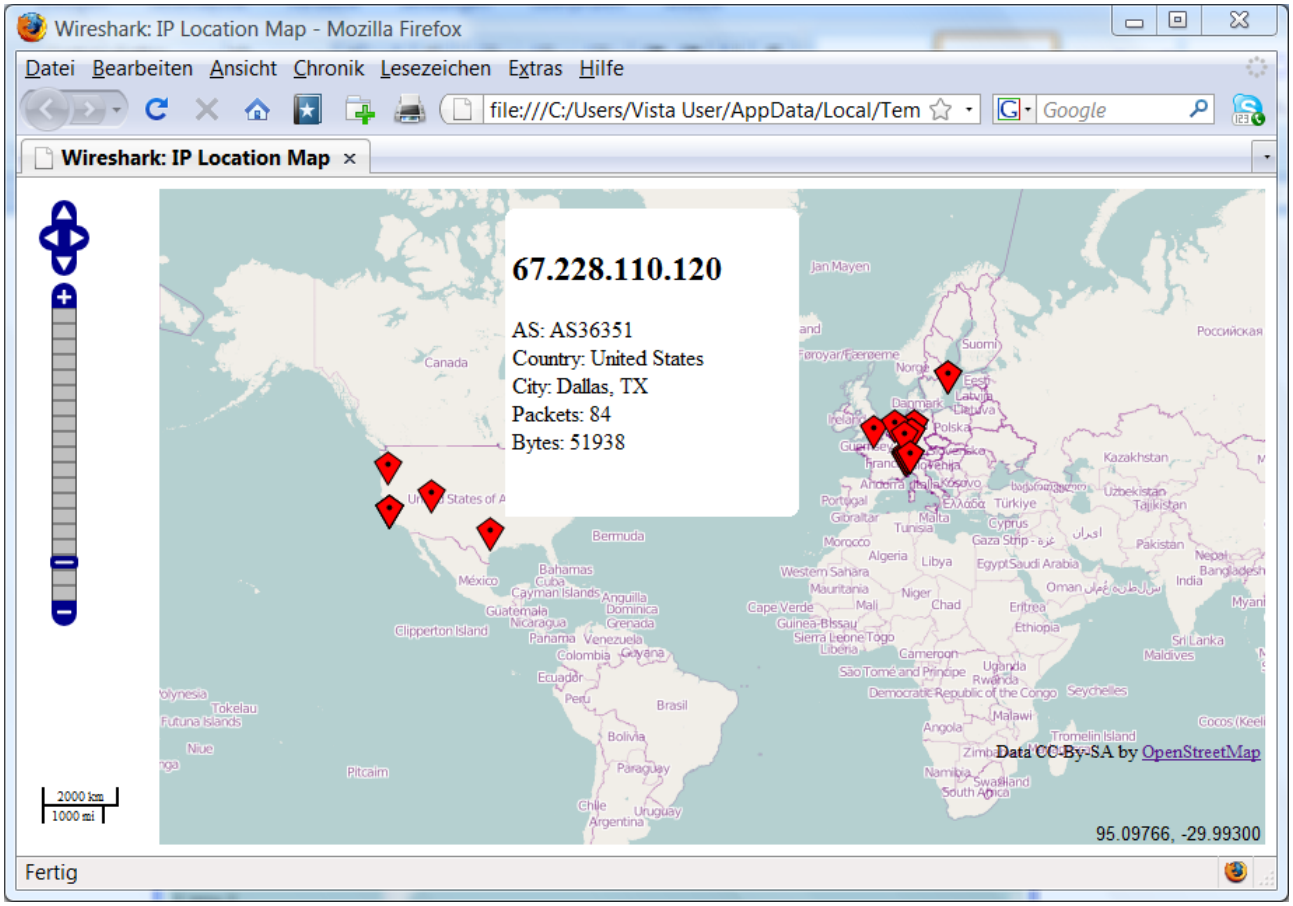


Durch Anwählen z.B. des IP Headers mit der rechten Maustaste im ‚Packet Detail', können unter der Position ‚Protocol Preferences' in einem neuen Fenster direkt Einstellungen vorgenommen werden.

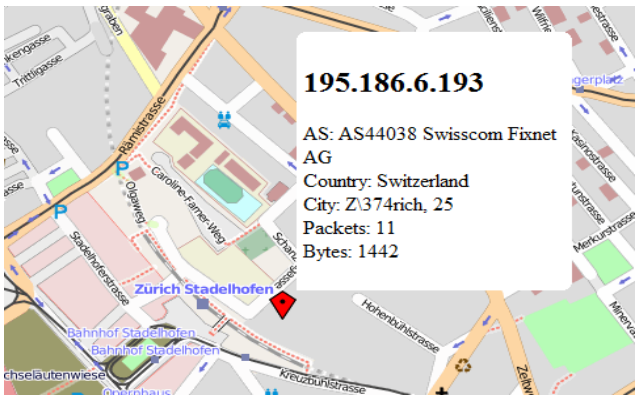
Zum Beispiel kann auf diese Weise schnell und einfach die Interpretation des ‚TOS' Feldes in die ‚DiffServ'-Darstellung umgeschaltet werden.

Geographische Darstellung von IP-Adressen

Die spektakulärste Zusatzfunktion ist sicher die neue Möglichkeit, IP-Adressen direkt aus einem Wireshark Capture File heraus im Browser geographisch darzustellen.



Durch Anklicken einer Markierung werden neben der IP-Adresse zusätzliche Informationen wie Autonomous System Numbers (AS), Land und Stadt eingeblendet.



Als Basis dienen die öffentlich zugänglichen Informationen über IP-Adressen-Einträge und als Hintergrund der Darstellung wird die kostenlose Karte OpenStreetMap verwendet.

← Durch Einzoomen in die Karte lässt sich eine IP Adresse im Stadtplan lokalisieren, nur mit den Umlauten klappt es noch nicht perfekt.

Genutzt werden kann diese Möglichkeit zum Orten von Web-Serverstandorten in der ganzen Welt, oder wenn die Wireshark-Aufzeichnung bei einem Webserver erfolgt, kann damit die Herkunft der verschiedenen Webzugriffe aufgezeigt werden.

Installation und Bedienung

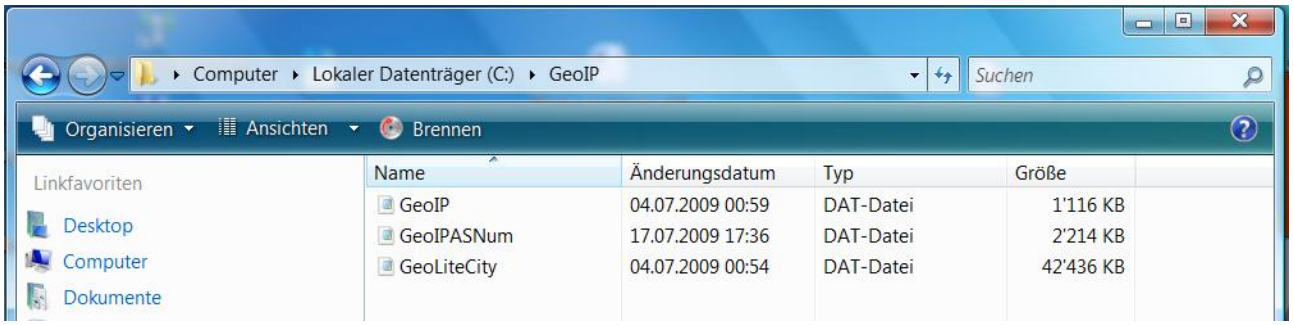
Basis für die Zuordnung der IP-Adressen bildet die kostenlose Datenbank GeoIP von MaxMind, welche lokal auf dem PC installiert wird (ca. 45 MB). Sie liefert den registrierten IP-Besitzer und dessen Koordinaten. Für die geographische Darstellung wird jedoch Internet-Zugriff auf den Kartenlieferanten OpenStreetMap benötigt, und der Browser muss JavaScripts unterstützen.

Die folgenden Schritte zeigen die Installation und die Bedienung

1. Installation der GeoIP Datenbank

Laden Sie die folgenden drei komprimierten Files herunter, dekomprimieren Sie die Files (z.B. mit WinZip) und speichern Sie diese an einem Ort Ihrer Wahl (z.B. unter C:\GeoIP).

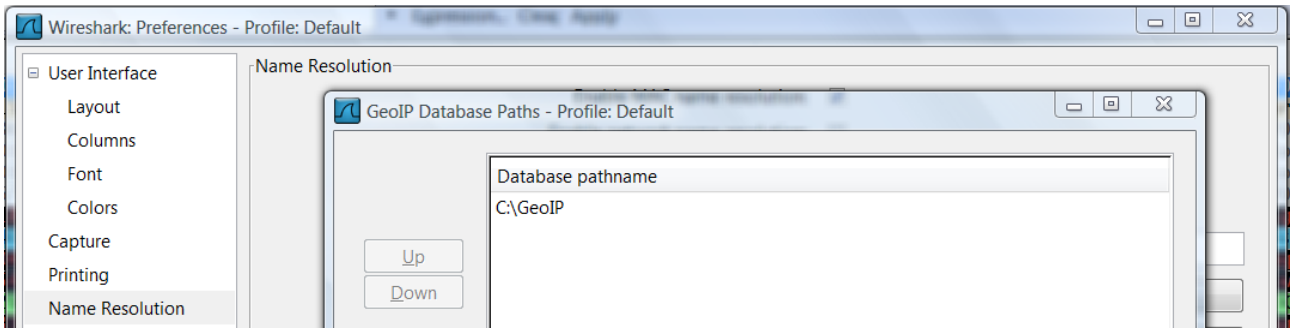
http://geolite.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz
http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
http://geolite.maxmind.com/download/geoip/database/asnum/GeoIPASNum.dat.gz



Die drei GeoIP Dateien im Ordner C:\GeoIP

2. Konfigurieren von Wireshark

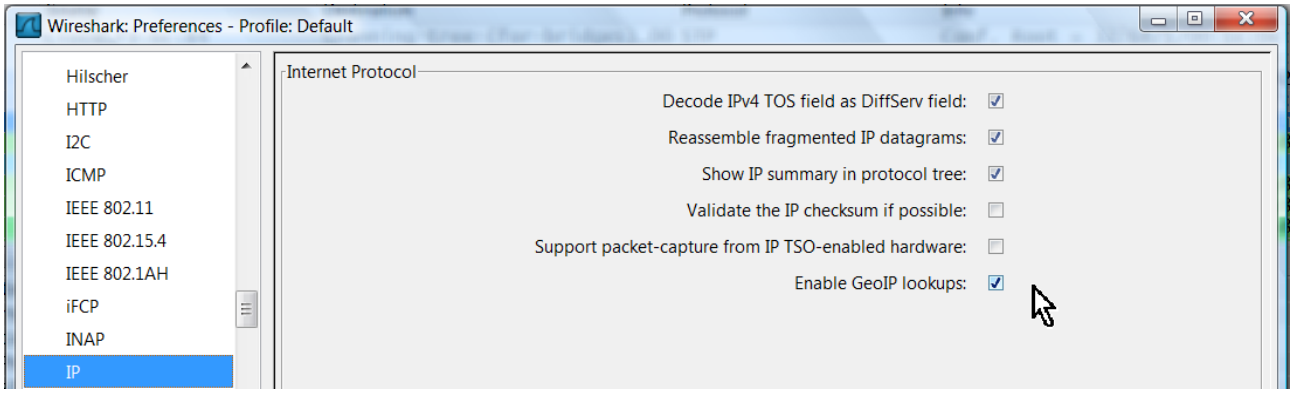
Geben Sie den Pfad der GeoIP Dateien im Wireshark unter → Preferences → Name Resolution → GeoIP database directories ein:



3. Aktivieren von GeoIP Lookups

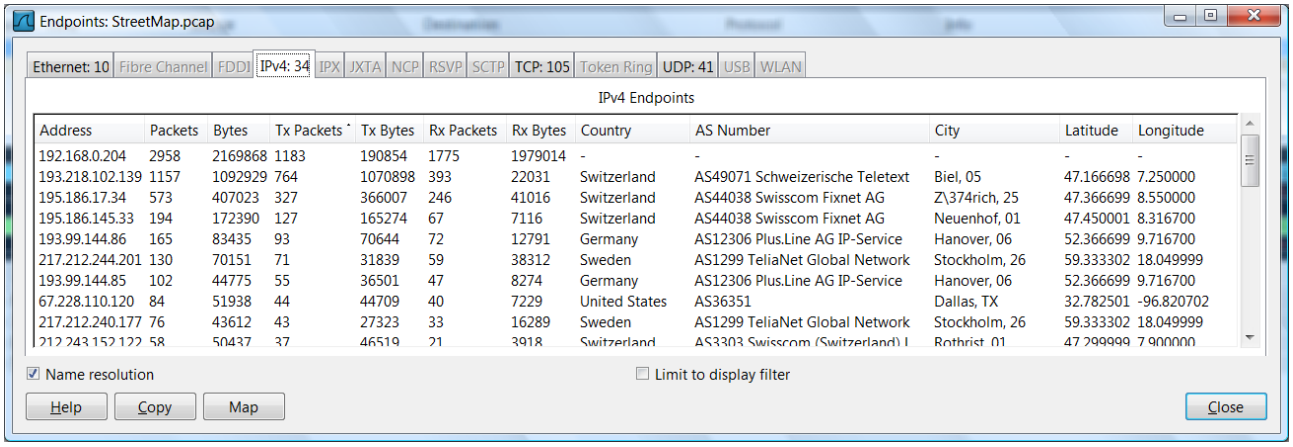
Schliessen Sie Wireshark und starten Sie Wireshark neu!

Schalten Sie unter → Preferences → Protocols → IP → Enable GeoIP lookups die Funktion ein



4. Bedienung von GeoIP Lookups

Starten Sie ‚Capture' mit Wireshark, öffnen Sie Ihren Browser und greifen auf einige Webseiten zu. Stoppen Sie den Aufzeichnungsvorgang und wählen Sie → Statistics → Endpoints → IPv4



Neben den üblichen Feldern werden Country, AS Number, City und die Koordinaten sichtbar.

Betätigen Sie die Taste ‚Map', ein Browser Fenster wird geöffnet und zeigt die Lokationen.

5. Anmerkungen

Natürlich funktioniert dies nur mit öffentlichen IP-Adressen und nicht mit privaten Adressen wie 10.x.x.x, 172.16.x.x bis 172.31.x.x und 192.168.x.x, da diese überall verwendet werden können und weder einem Besitzer noch einer geographischen Lokation zugeordnet sind.
Aus diesem Grund können auch Aufzeichnungen, welche z.B. in einem Firmennetz, hinter einem Proxy Server gemacht wurden, mit GeoIP nicht lokalisiert werden.

>No rocket science, but a good example how public available data could be usefully combined!<

A complete, affordable wireless network analysis and troubleshooting solution, integrated with Wireshark.

Markante Neuerung wurden am Sharkfest'09 auch für das Monitoring und Reporting Tool PILOT angekündigt. Einige sind bereits verfügbar, andere werden in Kürze erhältlich sein.

WiFi PILOT v1.2

Der neue WiFi PILOT ist ein Subset der CACE PILOT Software, bereits bekannt als kostengünstiges Monitoring und Reporting Tool. Die einfache Bedienung mit Hilfe von ‚Views', welche auf ein Wireshark Tracefile gezogen werden, wurde beibehalten. Die Einschränkung besteht darin, dass mit WiFi Pilot nur WLAN-Aufzeichnungen analysiert und graphisch dargestellt werden können.
Neu ist auch die Zusammenarbeit zwischen Cace Technologies (AirPcap Hersteller) und Metageek (Wi-Spy Hersteller). Diese Kombination macht Sinn, da sich die beiden Produkte optimal ergänzen. Während Pilot in Kombination mit Wireshark und dem AirPcap die Aufzeichnung und Analyse von WLAN Frames ermöglicht, zeigt der Spektrum Analyser Wi-Spy allfällige Störquellen im Wireless-Bereich auf.

Die WiFi PILOT Software wird in einem Bundle zusammen mit einem AirPcap und einem Wi-Spy USB-Adapter angeboten und kostet bei uns in der Grundkonfiguration CHF 732.00. Mehr Informationen zu diesem Produkt erhalten Sie auf der Webseite von Cace Technologies und in unserem nächsten Newsletter.

Powerful and Affordable Network Analysis, Visualization and Reporting. Integrated with Wireshark

PILOT für Server/Client

Die Vollversion von CACE PILOT wird in Kürze wesentliche neue Funktionen erhalten. Angekündigt wurde am Sharkfest'09 eine Server/Client-fähige Version, wie sie von einigen Kunden schon angefragt worden ist. Dies wird den Einsatz von Pilot als zentrale Überwachungstelle von verteilt platzierten Clients und damit eine kostengünstige Fernüberwachung an kritischen Netzwerkpunkten ermöglichen.
Einige Details sind schon bekannt, so wurde bei der Entwicklung besonders auf die effiziente Nutzung der Bandbreite zwischen Server und Client geachtet, übertragen werden nur Metadaten der Aufzeichnung. Die Pilot Bedieneroberfläche wird dann dazu dienen, bestimmte kritische Bereiche auszuwählen, von welchen dann die detaillierten Frames für die Analyse mit Wireshark an den zentralen Server übertragen werden.

Mehr Informationen dazu in unserem nächsten Newsletter.

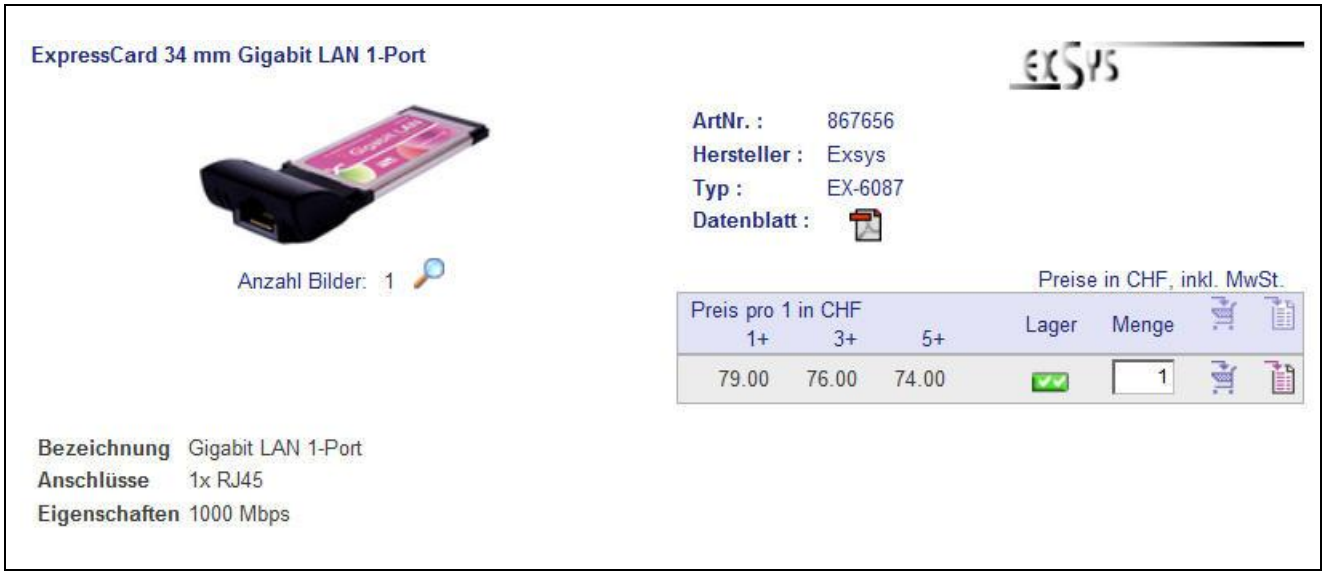
Tipps, Tricks & Talks

Nachtrag zum Thema: Wie wird die „VLAN Tag" Information im Wireshark aktiviert?

Der Beitrag im letzten Newsletter zu diesem Thema ist auf reges Interesse gestossen, und das Bedürfnis, VLAN Tags zu decodieren, scheint gross zu sein.

Gemäss Feedback von verschieden Seiten, scheint es bei gewissen Herstellern von eingebauten Gigabit Ethernet Adaptern unter Windows nicht möglich zu sein, die VLAN Tags sichtbar zu machen. Dies trotz Eingriffen in die Registry und Durchspielen aller Varianten in den Konfigurationsmenüs.

Falls dies bei Ihnen auch der Fall sein sollte, bietet sich nur noch eine Möglichkeit: die eines externen Ethernet Adapters. Auch hier besteht jedoch keine Garantie, dass der Driver die notwendigen Informationen liefert. Ein Modell, welches ich getestet habe und das einwandfrei funktioniert ist der Typ EX-6087 von der Firma EXSYS, im neuen ExpressCard Format und erhältlich z.B. bei der Firma Disdata.



Quelle: Disdata online Katalog, alle Angaben ohne Gewähr

Hinweise:

Die nächsten öffentlichen Wireshark Kurse und Präsentationen:

Swiss Open Systems User Group

8.-10.9.09 Workshop-Tage

WS 12: IPv6 entdecken mit Wireshark, eine technische Einführung

Datum:	10.9.2009 13.30 - ca. 17.00 Uhr
Ort:	ETH Zürich
Referent:	Rolf Leutert

TCP / IP Netzwerkanalyse mit Wireshark

Datum:	07.09.2009 - 09.09.2009 (3 Tage)
Ort:	Comicro-Netsys, Wangen
Kurs-Details und Anmeldung bei	Comicro-Netsys

WLAN Netzwerkanalyse mit Wireshark und AirPcap

Datum:	21.09.2009 - 23.09.2009 (3 Tage)
Ort:	Comicro-Netsys, Wangen
Kurs-Details und Anmeldung bei	Comicro-Netsys

Wireshark - VoIP Sniffer Kurs

Datum:	7.12.2009 bis 8.12.2009 (2 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

Besten Dank für Ihr Interesse

Mit freundlichen Grüssen Rolf Leutert