

Wireshark Netværks analysator

Wireshark – en kort introduktion

Af Kristen Nielsen

TheCamp.dk 2012

2012-07-25, Græsrodsgården,
Bregninge.

Wireshark start vindue

The screenshot displays the Wireshark Network Analyzer interface. The title bar reads "The Wireshark Network Analyzer [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations and analysis. Below the toolbar is a filter input field with a dropdown menu and buttons for "Expression...", "Clear", and "Apply".

The main content area is divided into three columns:

- Capture:** Features the "Interface List" (Live list of the capture interfaces (counts incoming packets)) and "Capture Options" (Start a capture with detailed options). Below this is a "Capture Help" section with links for "How to Capture" (Step by step to a successful capture setup) and "Network Media" (Specific information for capturing on: Ethernet, WLAN, ...).
- Files:** Features an "Open" section (Open a previously captured file) and an "Open Recent:" list. The list includes several files, with "T:\dumps\20120106-adecco-fr-193-203-96-2-try1.cap [not found]" highlighted. Below this is a "Sample Captures" section (A rich assortment of example capture files on the wiki).
- Online:** Features links to the "Website" (Visit the project's website), "User's Guide" (The User's Guide (local version, if installed)), and "Security" (Work with Wireshark as securely as possible).

The status bar at the bottom shows "Ready to load or capture", "No Packets", and "Profile: Default". A text box in the Online section contains the path "T:\dumps\20120106-adecco-fr-193-203-96-2-try1.cap".

Hvad er Wireshark

- Netværks analysator
 - Opsamler/læser/analyserer netværkspakker
 - Netværks teknikerens "voltmeter"
 - Open Source og modulært
 - Bedste netværks analysator til de fleste opgaver
 - Hundredevis af protokol dekodere (Dissectores)
 - Hvis du selv laver protokoller kan du skrive din egen dissector til at dekode denne.

Wireshark.org

- Stable release (juli 2012) Vers.- 1.8.1
- OS support: Windows, Mac, Linux (more distributions), *BSD, Gentoo, HP-UX, Solaris ...
- Riverbed Technology organiserer en del udvikling. Ansatte kodere mv.
- Wireshark konference: Sharkfest holdes årligt i kalifornien. Se: <http://Sharkfest.wireshark.org>
- Uddannelse: Wireshark University
- En del hardware supporterer/støtter op omkring Wireshark.

Wireshark brug

- Find data der skal analyseres:
 - Måling på netværk
 - Direkte med Wireshark + Pcap
 - Via målt fil fra andet værktøj e.g. Tcpdump,

Indsamling af måledata

- Måling direkte på host (krydset kabel)
- Brug af spanport/monitor port på switch.
 - Sender kopi af trafik til en bestemt port på switchen.
Kan f.eks. Være trafik fra f.eks. En række port, eller vlans i switchen.

Indsamling af måledata

- Måling direkte på host netport (krydset kabel)
- Brug af spanport/monitor port på switch.
 - Sender kopi af trafik til en bestemt port på switchen.
Kan f.eks. Være trafik fra f.eks. En række port, eller vlans i switchen.
- Data indhentes fra særligt oprettet målesignalsnetværk, kan f.eks. Indhente signaler fra mange switche, eller mange sites.
- Tcpdump / plink.exe (putty) kan capture data og sende disse over nettet (f.eks. Ssh kanal) til lokal wireshark.

Wireshark demo.

- Http demotrace.
-

Filter: tcp.stream eq 0 Expression... Clear Apply

VLAN	No.	Time	Source	Destination	Protocol	Info
	1	2004-05-13 12:17:07.311224	145.254.160.237	65.208.228.223	TCP	tip2 > http [SYN] Seq=0 win=8760 Len=0 MSS=1460 SACK_PERM=1
	2	2004-05-13 12:17:08.222534	65.208.228.223	145.254.160.237	TCP	http > tip2 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1380 SACK_P
	3	2004-05-13 12:17:08.222534	145.254.160.237	65.208.228.223	TCP	tip2 > http [ACK] Seq=1 Ack=1 win=9660 Len=0
	4	2004-05-13 12:17:08.222534	145.254.160.237	65.208.228.223	HTTP	GET /download.html HTTP/1.1
	5	2004-05-13 12:17:08.783340	65.208.228.223	145.254.160.237	TCP	http > tip2 [ACK] Seq=1 Ack=480 win=6432 Len=0
	6	2004-05-13 12:17:08.993643	65.208.228.223	145.254.160.237	TCP	[TCP segment of a reassembled PDU]
	7	2004-05-13 12:17:09.123830	145.254.160.237	65.208.228.223	TCP	tip2 > http [ACK] Seq=480 Ack=1381 win=9660 Len=0
	8	2004-05-13 12:17:09.123830	65.208.228.223	145.254.160.237	TCP	[TCP segment of a reassembled PDU]
	9	2004-05-13 12:17:09.324118	145.254.160.237	65.208.228.223	TCP	tip2 > http [ACK] Seq=480 Ack=2761 win=9660 Len=0
	10	2004-05-13 12:17:09.754737	65.208.228.223	145.254.160.237	TCP	[TCP segment of a reassembled PDU]
	11	2004-05-13 12:17:09.864896	65.208.228.223	145.254.160.237	TCP	[TCP segment of a reassembled PDU]
	12	2004-05-13 12:17:09.864896	145.254.160.237	65.208.228.223	TCP	tip2 > http [ACK] Seq=480 Ack=5521 win=9660 Len=0
	14	2004-05-13 12:17:09.945011	65.208.228.223	145.254.160.237	TCP	[TCP segment of a reassembled PDU]
	15	2004-05-13 12:17:10.125270	145.254.160.237	65.208.228.223	TCP	tip2 > http [ACK] Seq=480 Ack=6901 win=9660 Len=0
	16	2004-05-13 12:17:10.205385	65.208.228.223	145.254.160.237	TCP	[TCP segment of a reassembled PDU]

Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)

```

Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
  Destination: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
  Source: Xerox_00:00:00 (00:00:01:00:00:00)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
Transmission Control Protocol, Src Port: tip2 (3372), Dst Port: http (80), Seq: 1, Ack: 1, Len: 479
Hypertext Transfer Protocol
  GET /download.html HTTP/1.1\r\n
  Host: www.ethereal.com\r\n
  User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n
  Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1\r\n
  Accept-Language: en-us,en;q=0.5\r\n
  Accept-Encoding: gzip,deflate\r\n
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
  Keep-Alive: 300\r\n
  Connection: keep-alive\r\n
  Referer: http://www.ethereal.com/development.html\r\n
  \r\n
  [Full request URI: http://www.ethereal.com/download.html]

```

0000	fe ff 20 00 01 00 00 00	01 00 00 00 08 00 45 00 E.
0010	02 07 0f 45 40 00 80 06	90 10 91 fe a0 ed 41 d0	...E@... A.
0020	e4 df 0d 2c 00 50 38 af	fe 14 11 4c 61 8c 50 18 P8. La.P.
0030	25 bc a9 58 00 00 47 45	54 20 2f 64 6f 77 6e 6c	%..X..GE T /downl
0040	6f 61 64 2e 68 74 6d 6c	20 48 54 54 50 2f 31 2e	oad.html HTTP/1.
0050	31 0d 0a 48 6f 73 74 3a	20 77 77 77 2e 65 74 68	l..Host: www.eth
0060	65 72 65 61 6c 2e 63 6f	6d 0d 0a 55 73 65 72 2d	ereal.com..User-
0070	41 67 65 6e 74 3a 20 4d	6f 7a 69 6c 6c 61 2f 35	Agent: M ozilla/5
0080	2e 30 20 28 57 69 6e 64	6f 77 73 3b 20 55 3b 20	.0 (wind ows; U;
0090	57 69 6e 64 6f 77 73 20	4e 54 20 35 2e 31 3b 20	windows NT 5.1;
00a0	65 6e 2d 55 53 3b 20 72	76 3a 31 2e 36 29 20 47	en-US; r v:1.6) G
00b0	65 63 6b 6f 2f 32 30 30	34 30 31 31 33 0d 0a 41	cko/200 40113 .A

Afsluttende.

- Wireshark fungerer fint og til nesten det hele
- Let at udvide
- Mange online ressourcer, manual, erfa, sample traces etc.
- Find det hele på <http://wireshark.org>.