13 Netzwerkanalyse

Christian Zahler

Sniffer erstellen Kopien von Frames (Pakete auf OSI-Schicht 2), um deren Header bzw. Inhalt analysieren zu können.

Marktübersicht

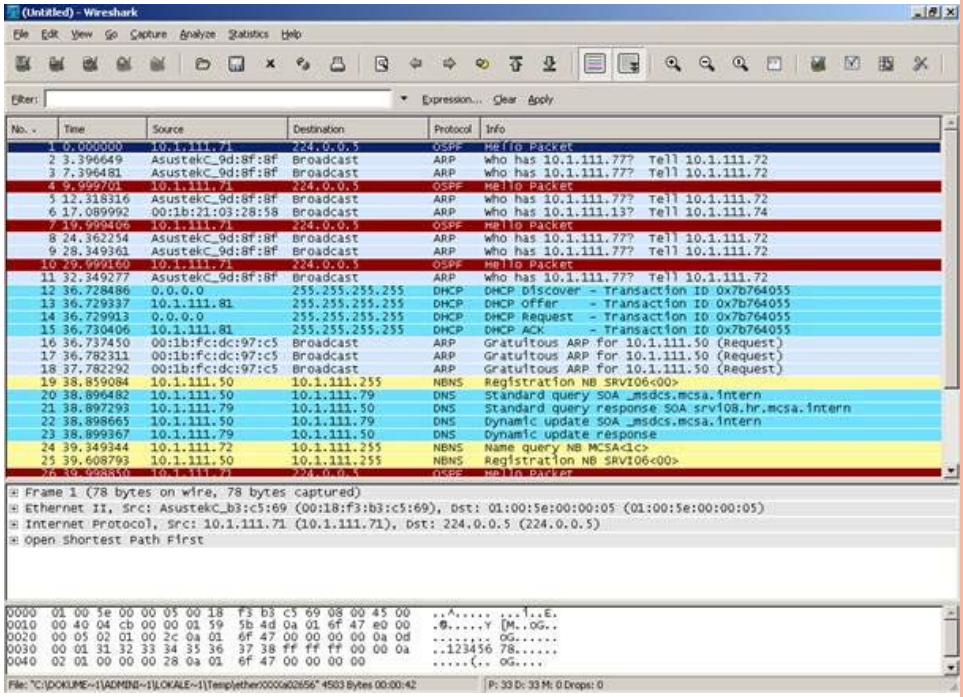
Freie Produkte

- Wireshark (ehemals: ethereal; oft mit Treiber WinPCap kombiniert)
- Ettercap
- NETCORtools (TCP Trace basierend)
- Tcpdump

Proprietäre Produkte

- Microsoft Network Monitor(Bestandteil von Microsoft Windows Server)
- Clearsight Analyzer (Clearsight Networks)
- EtherPeek, OmniPeek, GigaPeek (WildPackets)
- LANdecoder32 (Triticom)
- NetSpector (INAT)
- NetVCR (Niksun)
- NetworkActiv PIAFCTM
- Observer (Network Instruments)
- OptiView (Fluke Networks)
- Sniffer (Network General)
- TraceCommander (Synapse Networks)
- webSensor und webProbe (Moniforce)

Sehr gerne wird Wireshark eingesetzt.



⇨12.8 Bindung von Netzwerkprotokollen an die Netzwerkkarte unter Windows

Damit Netzwerkkartentreiber und Netzwerkprotokoll ordnungsgemäß zusammenarbeiten, müssen die Protokolltreiber (zum Beispiel für TCP/IP) an den Netzwerkkartentreiber **gebunden** werden. Diese Bindung kann folgendermaßen angezeigt und geändert werden:

Öffnen Sie das Systemsteuerungs-Objekt „Netzwerkverbindungen“ und wählen Sie den Menüpunkt **Erweitert** – **Erweiterte Einstellungen** (gegebenenfalls drücken Sie bei Vista die ALT-Taste, um die Pulldown-Menüs anzuzeigen).