Microsoft Netzwerkmonitor 3.3

Mit dem Netzwerkmonitor stellt Microsoft ein Tool zur Netzwerkanalyse von Datenpaketen zur Verfügung. Mit Hilfe des Netzwerkmonitor können Datenpakete im Netzwerk gesammelt und zur Problembehandlung analysiert werden.

Der Netzwerkmonitor von Microsoft blickt auf eine lange Historie zurück. Das erste Microsoft Produkt mit einem Netzwerkmonitor war der im Systems Management Server (SMS) enthaltene Netzwerkmonitor. Die Besonderheit des Netzwerkmonitor in SMS war, dass dieser in der Lage ist, nicht nur den an den Computer, auf welchem der Netzwerkmonitor installiert war, gesendeten und versendeten Datenverkehr zu analysieren, sondern den gesamten Netzwerkverkehr.
Mit Windows Server NT war der Netzwerkmonitor das erste mal in einer beschnittenen Version enthalten. Die wohl größte Einschränkung war, dass der Netzwerkmonitor nur in der Lage ist, direkt an den Computer gesendete oder versendete Datenpakete zu analysieren. Mit Windows 2000 Server und Windows Server 2003 wurde diese Funktionalität in Form des Netmon 2 beibehalten.

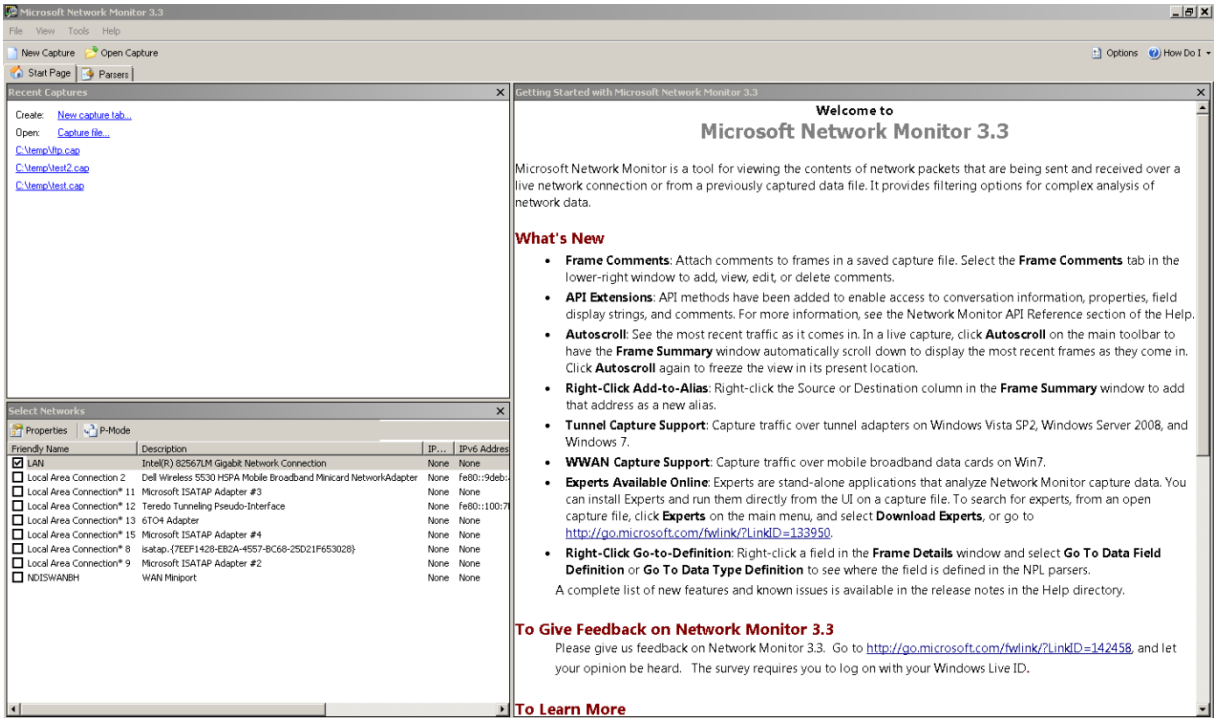
Seit Anfang 2007 bietet Microsoft den Netzwerkmonitor als Version 3 aber auch als eigenständiges Produkt zum kostenlosen Download oder als optionales Update über Windows Update an. Die aktuelle Version des Netzwerkmonitor zum Zeitpunkt der Erstellung dieses Artikels ist die Version 3.3.

Zu den Neuerungen von Netmon 3.3 zu Netmon 3.2 gehören:

- Unterstützung für WWAN (Mobile Broadband) in Windows 7
- volle Hyper-V Unterstützung
- Hinzufügen von Aliasen aus der Framezusammenfassung
- Autoscrolling
- Core Parser Set
- Unterstützung für ETL (Event Trace Log)
- Kommentierung von Rahmen
- Netzwerkmonitor Experten

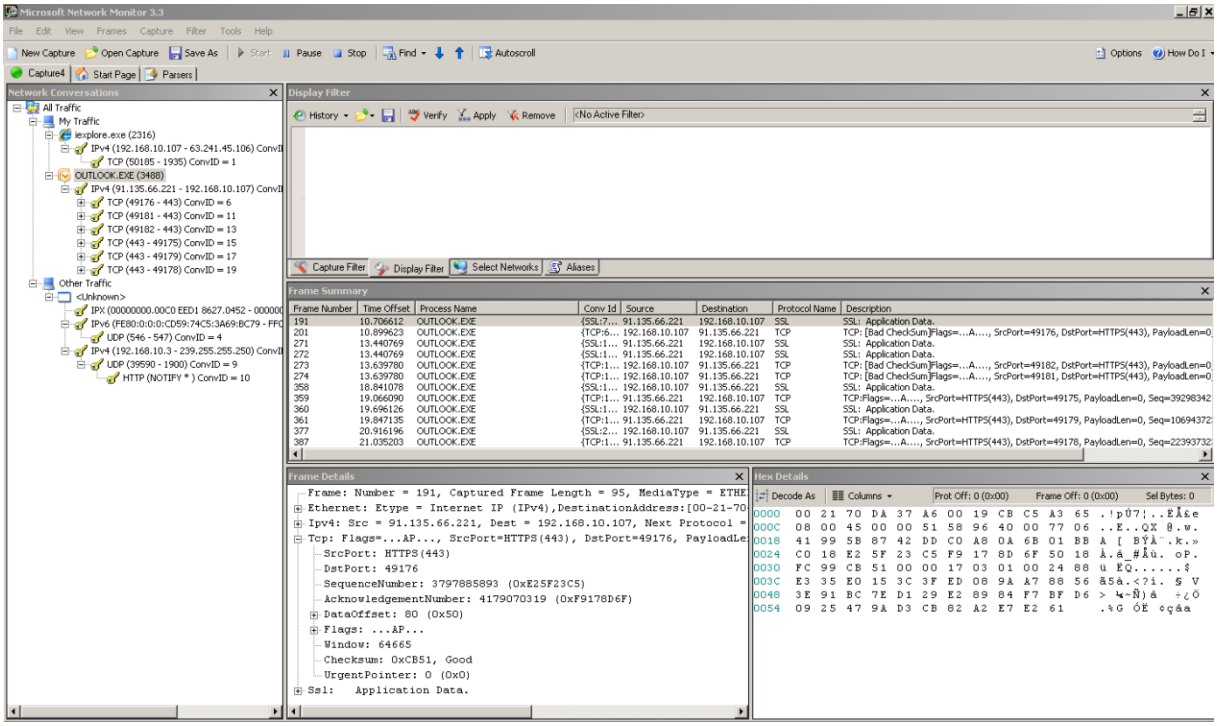
Zur Installation und Betrieb von Netmon sind folgende Voraussetzungen zu schaffen:

- Ein Betriebssystem mit Windows 7, Windows Server 2003, Windows Server 2003 Itanium, Windows Server 2008, Windows Vista, Windows Vista Business 64-Bit, Windows XP, Windows XP 64-Bit.
- Zu den Hardwarevoraussetzungen gehört ein PC mit 1 GHz Prozessor oder schneller, 1 GB RAM oder mehr und mindestens 25 MB Festplattenplatz für die Installation



Nach dem ersten Start des Netzwerkmonitors sollten Sie zuerst einige Einstellungen prüfen und gegebenenfalls anpassen. Dazu steht die Options Funktion in der Netmon GUI zur Verfügung. Auf der Registerkarte Capture können Sie Einstellungen des temporären Cache für die Capture-Dateien und den Speicherort des Cache festlegen.
Beachten Sie dabei besonders die Option Enable Conversations. Diese Funktion ermöglicht das Zuordnen von durch Netmon gesammelten Datenpaketen zu den einzelnen Prozessen auf dem Rechner. Dadurch erhalten Sie einen sehr guten Überblick über die Aktivitäten der einzelnen Prozesse, was gerade für die Fehleranalyse sehr hilfreich ist. Die Aktivierung dieser Funktion kann jedoch sehr viel Prozessorleistung verlangen, so dass es möglich ist, diese Option auszuschalten.
Bevor Sie mit der ersten Erstellung einer Sammlung beginnen, muss die Netzwerkkarte ausgewählt werden, welche mit dem Netzwerk verbunden ist, aus welchem Sie den Netzwerkverkehr analysieren möchte.
Ein weiterer essentieller Bestandteil eines Netzwerkmonitors sind Parser. Aufgabe eines Parser in Microsoft Netzwerkmonitor ist die Zerlegung und Umwandlung von gesammelten Netzwerkverkehr in für Administratoren lesbarere Informationen. Netmon wird mit einer Vielzahl von Parsern ausgeliefert; Parser können nachinstalliert werden und mit Hilfe einer Parsersprache eigene Parser erstellt werden, doch dazu mehr in einem späteren Teil dieses Artikels.

Beginnen Sie mit der Erstellung eines ersten Netzwerkcapture, indem ein neues Capture Fenster über den Befehl New Capture in der Menüleiste geöffnet wird und der Capture über den Start Button gestartet wird. Einmal erstellte Netzwerkcapture können über die Menuleiste und der Option Save as als .CAB-Datei gespeichert und für eine spätere Verwendung erneut geöffnet werden.



Wie Sie in der Abbildung sehen können, ist der Conversations-Modus in Netmon aktiv, so dass der gesammelte Netzwerkverkehr den einzelnen Prozessen auf der Maschine zugeordnet werden kann. Der Conversations-Modus hängt an jeden Frame eine Conversations-ID (ConvID) an, welche zur Zuordnung der Frames zu den Prozessen verwendet wird. Im Conversations-Fenster werden die Prozesse angezeigt und in einer Baumstruktur des Prozesses die am Datenverkehr beteiligten IP-Adressen, sowie die Source- und Destination Ports.

Auf der Registerkarte Display Filter können Sie sich einen Überblick über die einzelnen Rahmen, in der die FrameNummer, der verwendete Prozess, Source und Destination IP-Adresse, Protokoll Name und die Beschreibung des Rahmen angezeigt werden verschaffen.

Zu jedem gesammelten Rahmen vermittelt das Fenster Frame Details weitere Informationen. Zusätzlich zu den Informationen auf der Registerkarte Display Filter, werden im Fenster Frame Summary noch weitere Informationen angezeigt.
Schauen wir uns die einzelnen Rahmen, welche während des Aufbaus einer TCP/IP Verbindung erzeugt werden an:
SrcPort: 50528
Der Source Port gibt den Port an, welchen der FTP Client nutzt um mit dem FTP Server eine Verbindung herzustellen
DstPort: FTP control(21)
Der Destination Port gibt den Ziel Port auf dem FTP Server an, in diesem Fall über den FTP Control Channerl Port 21
SequenceNumber: 3128016037 (0xBA71BCA5)
Die Sequence Number wird für die forlaufende Nummerierung der Datenpakete verwendet
AcknowledgementNumber: 0 (0x0)

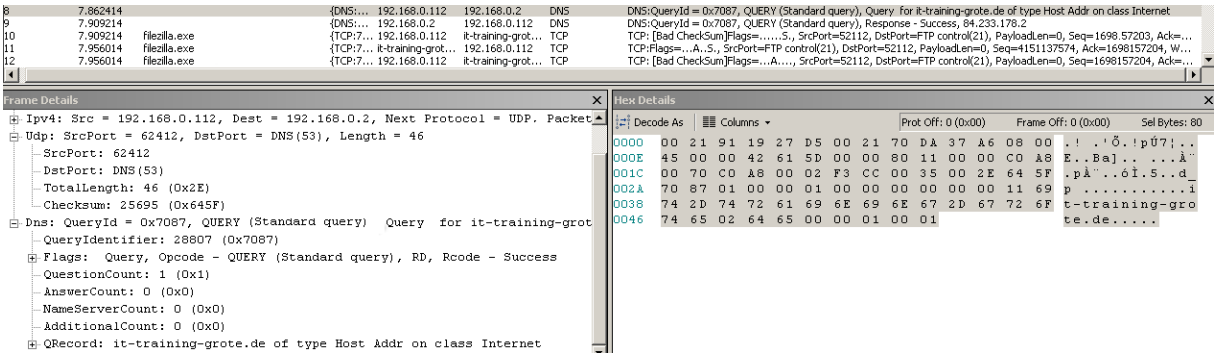
Bei der AcknowledgementNumber handelt es sich um die SequenceNumber des nächsten Datenpaketes, um sicherzustellen, dass der Empfänger alle bisherigen Pakete empfangen hat
DataOffset: 128 (0x80
Das DataOffSet Feld wird von TCP verwendet um anzuzeigen, wieviele 32-Bit Worte im TCP-Header enthalten sind, um die Startadresse der IP-Nutzlast (Payload) anzuzeigen
Window: 8192 (Negotiating scale factor 0x8) = 8192)
Checksum: 0xA2E0, Bad
Es wird eine Prüfsumme zur Erkennung von Übertragungsfehlern im TCP Protokoll verwendet
UrgentPointer: 0 (0x0)
Der Urgent Pointer gibt zusammen mit der Sequence Number die Position des ersten Byte der Nutzdaten in einem TCP Paket an.

Im Fenster Hex Details werden Ihnen alle Datenpakete im Hexadezimal Format angezeigt.
Nach erfolgter Analyse der DaDstPort: FTP control(21)tenpakete kann das Ergebnis für eine spätere Wiederverwendung gespeichert werden.

Nachdem wir uns einen Überblick über die generelle Funktionsweise des Netzwerkmonitor verschafft und einige grundlegende Begriffe geklärt haben, ist es Zeit, einen Netzwerktrace zu erstellen, um eine FTP Verbindung im Detail zu analysieren und so weitere Funktionen von Netmon kennenzulernen.

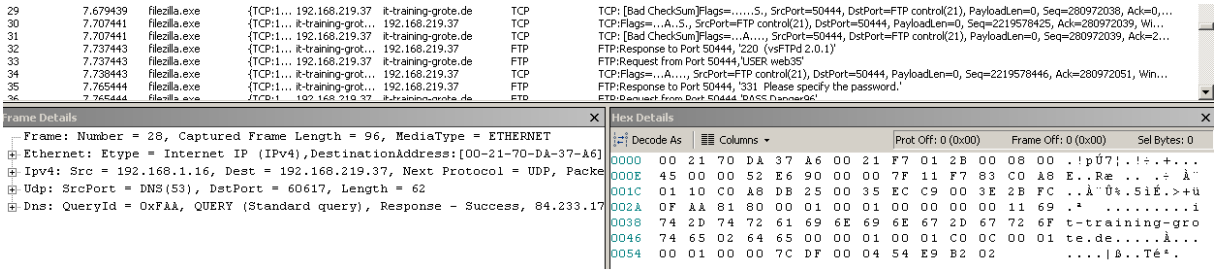
Als Praxisbeispiel für diesen Artikel wird der Verbindungsaufbau eines Windows Server 2008 zu einem FTP Server unter Verwendung des FTP Programmes Filezilla mit dem Netzwerkmonitor aufgezeichnet und die einzelnen Verbindungsschritte durchleuchtet.

Starten Sie mit Hilfe von Netmon einen Netzwerktrace und starten Sie anschließend das FTP Programm Filezilla, um eine Verbindung zu einem FTP Server aufzubauen. Damit eine Verbindung erfolgreich etabliert werden kann, ist zunächst eine Namensauflösung mit DNS durchzuführen.

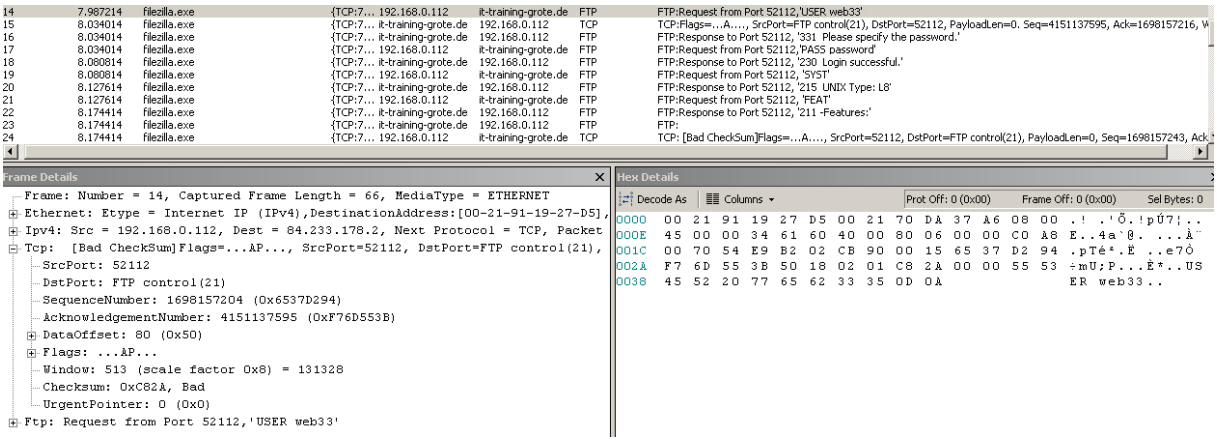


Das Ergebnis des Netzwerktrace zeigt Ihnen im Detail einen Verbindungsaufbau des Programmes Filezilla und eine DNS-Anfrage nach der Hostadresse des Ziel FTP-Servers. Die DNS Abfrage ist erfolgreich und liefert die korrekte IP Adresse des Hostnamen zurück. Im Fenster Frame Details können Sie sehen, dass eine Abfrage per UDP (User Datagram Protocol) erfolgt und als Source Port ein Random Port und

als Zielport der DNS Port 53 verwendet wird. Es erfolgt eine DNS Abfrage auf den Namen des Zielservers, welche Sie auch im Fenster Hex Details sehen können. Als nächstes startet der TCP Verbindungsaufbau mit einem Random TCP Port, gefolgt von dem Destination FTP Control Channel Port, der Angabe der Payload Länge, der Sequence Number und dem Acknowledge (ACK) Flag. In dem Frame Detail Fenster Sehen Sie wieder Detailinformationen zu dem Frame, wie die Window Size.



Als nächstes startet der Aufbau einer FTP Verbindung. Der FTP Request wird von einem Random Port für den FTP Benutzer WEB33 gestartet. Der FTP Server liefert eine Antwort auf die Anfrage an Port 52112 und fordert zur Eingabe des FTP Kennworts auf. Der Benutzer gibt das erforderliche Kennwort ein und der FTP Server antwortet bei einer erfolgreichen Anmeldung mit 230 Login successful. Als nächstes wird mit dem SYST Befehl das Betriebssystem des FTP Servers bestimmt, in diesem Fall ein UNIX System und mit dem FEAT Befehl werden alle zusätzlichen FTP Funktionen aufgelistet, welche zusätzlich zu den in RFC 959 gelisteten Funktionen zur Verfügung stehen.



Actives und Passives FTP

Zum Abschluß des FTP Verbindungsbeispiels folgt noch eine kurze Erklärung des Active und Passive FTP. Erfahrungsgemäß ist die Verwendung des korrekten FTP-Modus entscheidend für einen erfolgreichen Verbindungsaufbau je nach verwendeter Netzwerkinfrastruktur. Die FTP Spezifikation sieht zwei verschiedene Verbindungs-Modi vor: Den aktiven und den passiven FTP-Modus.

Bei der Verwendung des aktiven FTP Modus sendet der FTP Client einen zufälligen Port und seine IP-Adresse an den FTP Server mittels des PORT Befehls. Die Datenübertragung vom FTP-Server erfolgt über Port 20. Die Kommunikation erfolgt ausschließlich über den FTP Control Port.

Beispiel:

Antwort: 200 Switching to Binary mode.
Befehl: PORT 90,187,139,238,199,240
Antwort: 200 PORT command successful. Consider using PASV.
Befehl: LIST
Client initiiert die Verbindung auf Port 21 des FTP Server
FTP Server antwortet von Port 21 auf einen Port >1023 auf dem Client FTP Control Port
FTP Server initiiert die Datenverbindung von Port 20 auf einen Port >1023 über den Client Data Port
FTP Client sendet ein ACK (Acknowledge) von einem Port >1023 über den Data Port des FTP Server

Wenn Sie den passiven FTP Modus verwenden, sendet der FTP-Client ein PASV-Kommando an den FTP-Server, welcher einen Port öffnet und diesen mit seiner IP-Adresse an den FTp-Client übermittelt. Auf Client-Seite wird ein Port größer 1023 verwendet, der FTP-Server hingegen nutzt den dem Client mitgeteilten Port. Der passive FTP-Modus wird sehr häufig in Netzwerkumgebungen eingesetzt, in denen NAT verwendet wird oder eine Firewall im Einsatz ist.

Beispiel:

Antwort: 200 Switching to Binary mode.
Befehl: PASV
Antwort: 227 Entering Passive Mode (84,233,178,2,41,227)
Befehl: LIST
Client initiiert die Verbindung auf Port 21 des FTP Server
FTP Server antwortet von Port 21 auf einen Port >1023 auf dem Client FTP Control Port
FTP Client initiiert eine Verbindung zu einem Random Port >1023, welchen der FTP Server mitgeteilt hat
FTP Server sendet ein ACK (Acknowledge) und FTP-Daten auf einen Port >1023 über den Client FTP Data Port

Filterung von Netzwerktraffic

Wie Sie aus den vorangegangenen Beispielen sehen konnten, kann ein Netzwerktrace eine grosse Menge an Daten erzeugen, welche durch die Fülle an Informationen schwer zu analysieren sind. Um die Übersichtlickeit zu erhöhen und Informationen übersichtlicher darzustellen, stellt Netmon einige hilfreiche Filter zur Verfügung.
Grundsätzlich stehen zwei Filter zur Verfügung:

- Capture Filter
- Display Filter

Capture Filter

Der Capture Filter hilft Ihnen dabei, nur den gefilterten Netzwerkverkehr im Netzwerkmonitor darzustellen. Es werden eine Reihe von vordefinierten Filtern zum Filtern von Netzwerkverkehr zur Verfügung gestellt, mit deren Hilfe Netzwerkverkehr wesentlich übersichtlicher dargestellt und so Informationen wesentlich leichter gefunden werden können. Es steht Ihnen die Möglichkeit zur Erstellung eigener Filter zur Verfügung. Zur Erstellung eines Filters verwenden Sie die Registerkarte Capture Filter. In dem folgenden Eingabefeld können Sie dann eigene Capture Filter erstellen.
Das folgende Beispiel zeigt einen benutzerdefinierten Filter zur Anzeige aller Datenpakete mit Port 21 an die Ziel IP-Adresse 192.168.12.4:

TCP.Port == 21 && IPv4.DestinationAddress == 192.168.12.4

Nach Erstellung des Filters klicken Sie in der Capture Filter Menüleiste auf die Schaltfläche Verify, um den Filter auf korrekte Syntax zu prüfen, anschliessend kann der Filter durch betätigen der Schaltfläche Apply angewendet werden.
Einmal definierte Capture Filter können über die Schaltfläche History jederzeit aus dem Dropdownfeld erneut aktiviert werden. Weiterhin können Sie innerhalb eines Capture Filter verschiedene Filterabfragen mit Hilfe der Schlüsselwörter AND und OR kombinieren. Zur einfachen Protokollfilterung können Sie im Fenster Display Filter einfach das zu filternde Protokoll eingeben. Wenn SIe zum Beispiel FTP im Filter eingeben und auf Apply klicken, werden nur FTP Daten angezeigt.

Display Filter

Der Display Filter hilft Ihnen dabei, den gesammelten Netzwerkverkehr übersichtlicher zu gestalten. Es besteht zum Beispiel die Möglichkeit zur Einrichtung eines Color Filters über die Menüleiste Filter - Color Filters, mit welchem bestimmte Datenpakete farblich hinterlegt werden können. In dem Eingabefild können Sie neue Color Filter erstellen und Netzwerk Capture mit einer Vielzahl von Farben übersichtlicher hinterlegen. Die Filter Expression verwendet die gleiche Syntax wie der Capture Filter mit einem Unterschied, dass an dieser Stelle die Vorder- und Hintergrund Farbe, sowie der Text Style festgelegt werden kann. Sie können also den Capture Filter über die Zwischenablage in den Color Filter einfügen.

Aliases

Als weitere Möglichkeit zur übersichtlicheren Darstellung der Datenpakete steht Ihnen die Option zur Verwendung eines Alias zur Verfügung. Ein Alias kann im Netzwerkmonitor verwendet werden, um nicht aufgelösten IP-Adressen einen Namen zuzuweisen. Zur Erstellung eines Alias müssen Sie die Registerkarte Aliases verwenden und auf die Schaltfläche New klicken und dort einer IP-Adresse einen Alias zugeordnen. Das sollte der Hostname der Maschine sein, kann aber auch jeden beliebigen Namen erhalten. Wollen Sie Aliase dauerhaft verwenden, um diese auch für spätere Netzwerktraces zur Verfügung zu haben, können Sie die Aliase in einer Datei mit der Extension .NMA speichern, indem Sie auf das Diskettensymbol klicken.

Weitere Microsoft Netzwerkmonitor Besonderheiten

NMWIFI

Bei NMWIFI handelt es sich um ein Programm zum analysieren von Netzwerkverkehr in drahtlosen Netzwerken. Mit einer entsprechenen WLAN-Karte können somit alle Datenpakete in Wireless-Netzwerken mitgeschnitten werden. NMWIFI befindet sich im Netmon Installationsverzeichnis.

NMCAP

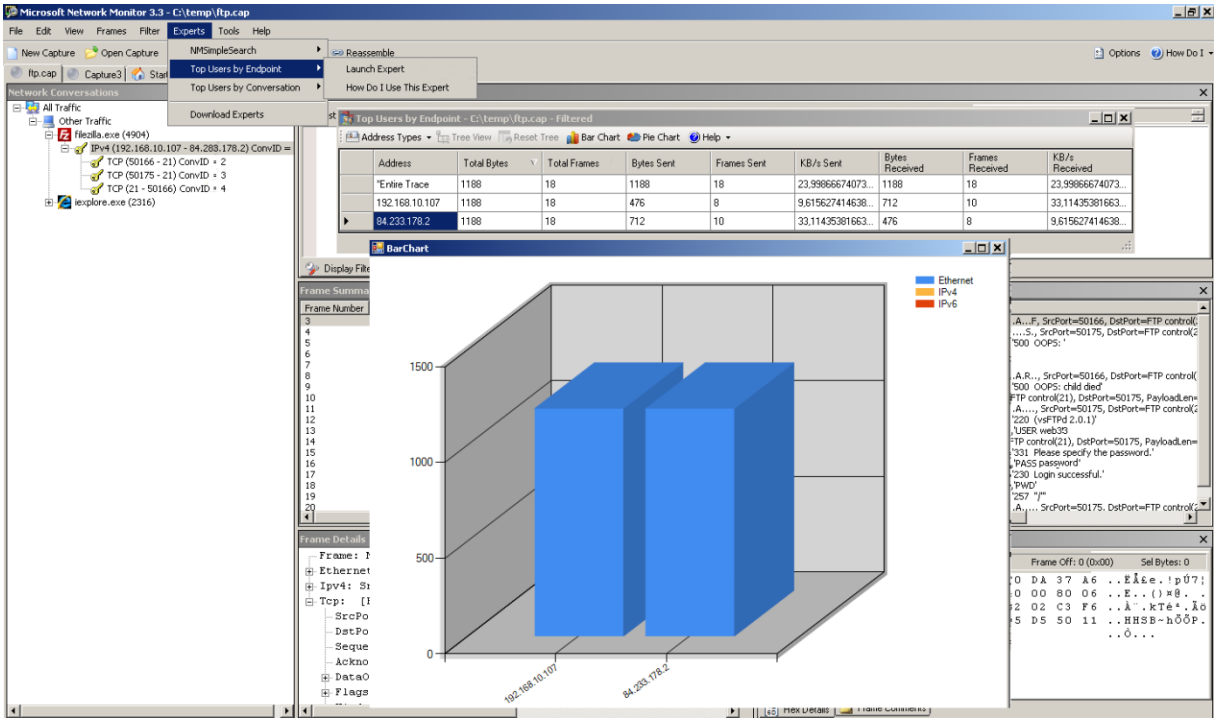
NMCAP ist das Kommandozeilen-Programm des Netzwerkmonitor, mit dessen Hilfe Netzwerkverkehr mitgeschnitten werden kann. NMCAP benötigt wesentlich weniger Speicherplatz für die Capture-Dateien als die grafische Variante des Netmon. NMCAP befindet sich wie NMWIFI im Netmon Installationsverzeichnis.

Promiscuous Mode

Der Promiscuous Mode oder auch P-Mode vom Microsoft Netzwerkmonitor genannt, erlaubt Ihnen das Sammeln von Datenpaketen, welche nicht nur für den eigenen Computer bestimmt sind. Diese Funktion können Sie jedoch nur verwenden, wenn Netmon in einen Netzwerk mit Hubs statt Switchen eingesetzt wird, oder der Netzwerkanschluß des Computers, auf welchem Netmon ausgeführt wird, an einen Monitor-Port des Switches angeschlossen ist.

Verwendung von Experten

Netzwerk Monitor Experten ermöglichen es Ihnen, mit Netmon gesammelten Datenverkehr nach bestimmten Mustern und Netzwerkverhalten auszuwerten. Experten waren bereits Bestandteil des Netmon 2, wurden mit jeder Netmon Version erweitert und erstmals mit Netmon 3.3 ist der Download von Netmon Experten über die Netmon GUI über die Menüleiste - Experts durch Anklicken von Download Experts im Untermenü möglich. Microsoft stellt auf einer eigenen Webseite verschiedene Experten zum Download zur Verfügung. Eine Installation der Netmon Experten erfolgt durch eine einfache Installationsroutine, nach dieser die Experten im Netzwerkmonitor zur Verfügung stehen. Eine der wesentlichen Neuerungen in Netmon 3.3 ist, dass installierte Experten über die Netmon GUI gestartet werden können. Ein Beispiel für einen Experten ist zum Beispiel NMTopUsers, welcher die Anzeige von Benutzern mit dem höchsten Anteil an Netzwerkverkehr in einem Netzwerktrace ermöglicht. Der Download ist über die Codeplex Webseite möglich. Nach dem Download von NMTopUsers führen Sie die Installationsroutine aus und anschließend steht der Netmon Experte NMTopUsers im Kontextmenü der Menüleiste Experts zur Verfügung. Auf der Codeplex Webseite stehen auch noch einige weitere Netmon Experten zum Download zur Verfügung. Sollten diese Experten nicht Ihren Ansprüchen genügen, so stellt Microsoft eine API (Application Programming Interface) bereit, mit der es Ihnen ermöglicht wird, Capture-Dateien zu lesen und zu filtern. Um eigene Netmon Experten zu erstellen, können Sie ein von Microsoft kostenlos zur Verfügung gestelltes SDK downloaden, welches eine Beispiel Umgebung für Experten zur Verfügung stellt und von Ihnen auf Ihre Bedürfnisse angepasst werden kann.



Network Parsing Language (NPL)

Die von Microsoft Netzwerkmonitor verwendeten Protokollparser werden mit einer spezifischen Network Parsing Language (NPL) geschrieben, welche Ihnen eine einfache Entwicklung von Parsern ermöglicht. NPL hat den Einzug mit dem Netzwerkmonitor3.0 erhalten. Die Programmsyntax erinnert etwas an C++, arbeitet aber doch anders als herkömmliche Programmiersprachen. Mit der Verwendung von NPL zur Erstellung von Parsern reduziert sich auch die Gefahr, dass schadhafter Programmcode implementiert wird, wie das zum Beispiel bei der Verwendung von DLLs der Fall sein kann.

Netmon Parser Syntax

Microsoft Netzwerkmonitor verwendet Parser, um gesammelten Datenverkehr benutzerfreundlicher darzustellen und es Ihnen somit zu ermöglichen, durch die gesammelten Datenpakete übersichtlicher navigieren zu können. Microsoft Netzwerkmonitor 3.3 wird mit einer Vielzahl von Parsern ausgeliefert. Wenn Sie zusätzliche Parser im Netzwerkmonitor integrieren wollen, steht Ihnen auf der Codeplex Webseite eine Reihe von zusätzlichen Parsern zum Download zur Verfügung. Das erstellen von eigenen Parsern ist ebenfalls möglich, jedoch gestaltet sich die Erstellung, gerade für Programmieranfänger, als ein komplexer Prozess. Nachfolgend einige Beispiele der Netmon Parser Language Syntax:

Definieren einer neuen Netmon Parser Tabelle:
Table FTPOpcodeTable
Protokolldefiniton
Protocol FTP
FTP Protokollport festlegen und FTP Definition zuordnen
case 21: FTP, ftp;

Die gezeigten Beispiele stellen nur einen kleinen Ausschnitt der Netmon Parser Language Syntax dar, eine umfangreichere Übersicht findet sich im Quellenverweis.

Quellen / Referenzen:

Microsoft Netzwerk Monitor 3 Informationen:
http://support.microsoft.com/kb/933741/en-us
Microsoft Netzwerk Monitor 3.3 Download:
http://www.microsoft.com/downloads/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f&displaylang=en
Network Monitor Open Source Parsers:
http://www.codeplex.com/NMParsers
Microsoft Netzwerkmonitor Blog
http://blogs.technet.com/netmon
Microsoft Network Monitor Experten
http://www.codeplex.com/NMExperts
Network Monitor Experts SDK
http://nmexperts.codeplex.com/Release/ProjectReleases.aspx?ReleaseId=26465