

Оглавление:

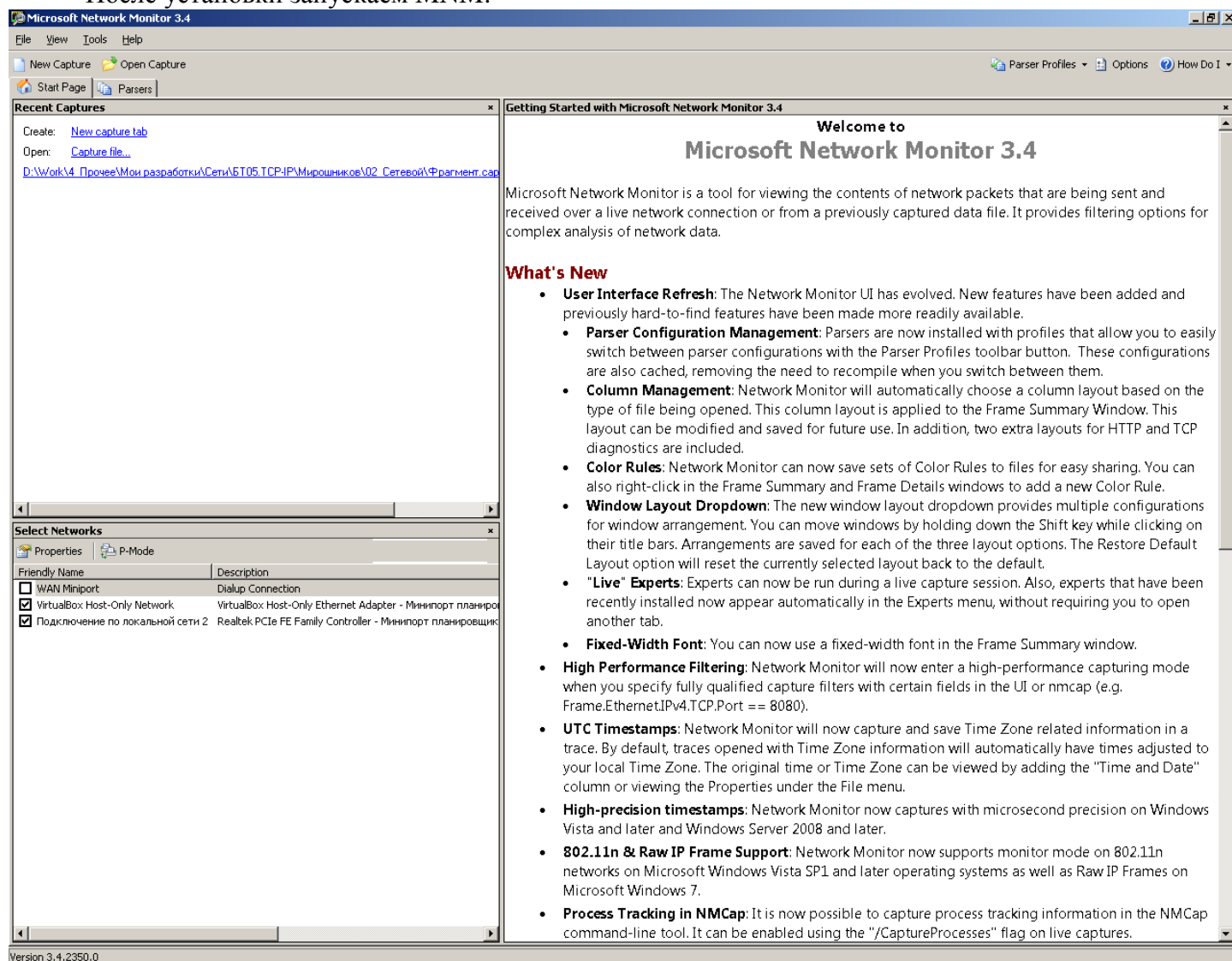
	Введение.	1
1.	Запуск, останов MNM и сохранение захваченных данных.	3
1.1.	Запуск захвата данных.	3
1.2.	Останов захвата данных.	3
1.3.	Сохранение результатов захвата данных.	4
2.	Настройка MNM.	4
2.1.	Настройка вида представления.	4
2.1.1.	Окно «Network Conversations»(сетевой трафик).	5
2.1.2.	Окно «Frame Summary»(обзор кадров).	6
2.1.3.	Окно «Frame Details»(детали по кадрам).	8
2.1.4.	Окно «Hex Details»(Hex-Dump кадра).	9
2.1.5.	Окно «Display Filter»(экранный фильтр).	10
2.2.	Настройка параметров работы MNM.	10
3.	Анализ захваченных данных.	13
3.1.	Отображение трафика, сгруппированного по приложениям и IP-адресам – окно «Network Conversations»(сетевой трафик).	13
3.2.	Отображение трафика, отфильтрованного в соответствии с заданным условием – окно «Display Filter»(экранный фильтр).	14
3.3.	Визуальное выделение трафика цветом, сформированным в соответствии с «Color Rules»(цветовые правила).	20
	Формирование «Color Rules»(цветовые правила) через контекстное меню.	20
	Формирование «Color Rules»(цветовые правила) через пиктограмму «Color Rules» на панели инструментов окна «Frame Summary»(обзор кадров).	21
3.4.	Замена MAC- и IP-адресов осмысленными псевдонимами - «Aliases»(псевдоним).	21
	Формирование «Aliases»(псевдонимы) через контекстное меню.	22
	Формирование псевдонима через пиктограмму «Aliases» на панели инструментов окна «Frame Summary»(обзор кадров).	22
3.5.	Поиск данных в захваченном трафике в соответствии с заданным условием.	23

Введение:

Данная статья предназначена для обучения использования сетевого анализатора Microsoft Network Monitor v.3.4. (далее по тексту «MNM»).

Дистрибутив скачиваем с официального сайта Microsoft: <http://www.microsoft.com/en-us/download/details.aspx?id=4865>.

После установки запускаем MNM:



Рабочее пространство MNM состоит из 4-х зон:


1. Панель меню: **File View Tools Help** - «File»(операции с файлами), «View»(управление отображением окон), «Tools»(управление настройками), «Help»(помощь).
2. Панель инструментов («New Capture», «Open Capture», «Parser Profiles», «Options», «How Do I»):



На панели, в зависимости от выбранного пункта меню, отображаются пиктограммы инструментов или действий. При загрузке на панели представлены «New Capture»(новый захват), «Open Capture»(открыть ранее сохраненный файл захвата), «Parser Profiles»(профиль анализатора), «Options»(опции, настройки), «How Do I»(как это сделать).

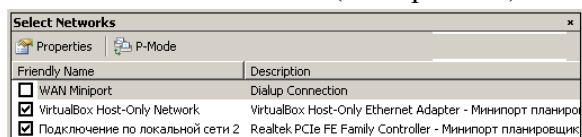
3. Панель вкладок: **Start Page Parsers**. При первой загрузке отображаются вкладки «Start Page»(стартовая страница) и «Parsers»(анализаторы).
4. Строка статуса: **Version 3.4.2350.0**

Наибольший интерес представляет собой зона панели с вкладками. Вкладка «Start Page»(стартовая страница) состоит из следующих трех окон:

- Окно «Recent Capture»(предшествующий захват):

 . В окне содержатся два обязательных элемента: «Create: New Capture»(создать новый захват), «Open: Capture file...»(открыть ранее сохраненный файл захвата). Оба пункта выполняют аналогичные действия, что и при нажатии на пиктограммы «New Capture» и «Open

Capture» на панели инструментов. Если ранее сохранялись файлы захвата, то они будут представлены в этом окне ниже.

- Окно «Select Networks»(выбор сетей):



В данном окне представлены сетевые интерфейсы ПК, с которых возможно осуществление захвата трафика. Пиктограмма «Properties»(свойства) отображает конфигурацию сетевого интерфейса ПК, на котором установлен фокус(подсвечен). Пиктограмма «P-Mode» управляет режимом «Promiscuous Mode»(всеядный или неразборчивый режим) выбранного сетевого интерфейса. Режим «P-Mode» позволяет сетевому интерфейсу захватывать пакеты, адресованные другим сетевым интерфейсам - в нормальном режиме такие пакеты отбрасываются. Использование режима «P-Mode» имеет смысл только в сетях с общей средой передачи - топология «Шина»(коаксиал, hub, wi-fi).

- Окно «Getting Started with Microsoft Network Monitor 3.4»(начальные данные по использованию):



В данном окне представлены краткие возможности MNM.

1. Запуск, останов MNM и сохранение захваченных данных.

Для начала работы с MNM необходимо в окне «Select Networks»(Выбор сетей) выбрать сетевой интерфейс или несколько интерфейсов, с которых будет осуществляться захват IP-пакетов, при необходимости включить режим «P-Mode». На представленном выше рисунке их три:

- «WAN Miniport»(модемное соединение);
- «VirtualBox Host-Only Network»(виртуальный сетевой адаптер виртуальной машины Oracle VirtualBox, работающий в режиме «Host-Only Network»);
- «Подключение по локальной сети 2» – реальный сетевой Ethernet-адаптер.

Отмечаем необходимые сетевые интерфейсы.

1.1. Запуск захвата данных

- Нажимаем пиктограмму «New Capture»(новый захват) на панели инструментов, панель инструментов принимает следующий вид (добавлены четыре активные пиктограммы «Save As»(сохранить как), «Capture Settings»(установки захвата), «Start»(пуск) и «Layout»(планировка, расположение окон), а также две не активные – «Pause»(приостанов захвата) и «Stop»(останов захвата)):



Панель меню принимает следующий вид:

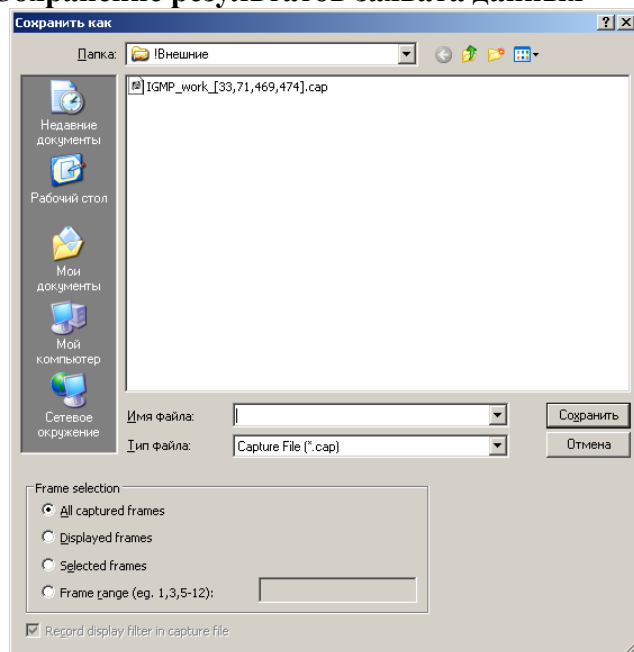


- добавлены пункты меню: «Edit»(управление внутренним буфером – вырезать, копировать и вставить), «Frames»(операции с Ethernet-кадрами), «Capture»(управление захватом – пуск, приостанов и останов), «Filter»(управление экраным фильтром) и «Experts»(загрузка сетевых экспертов).
- Нажимаем пиктограмму «Start» на панели инструментов или клавишу «F5».

1.2. Останов захвата данных

Нажимаем пиктограмму «Stop» на панели инструментов или клавишу «F7».

1.3. Сохранение результатов захвата данных



Нажимаем пиктограмму «Save As» на панели инструментов или клавиши «Ctrl+S» и указываем месторасположение, имя файла с сохраняемыми данными захвата, а также диапазон сохраняемых кадров, указанных в секции «Frame selection»(выбор кадров для сохранения):

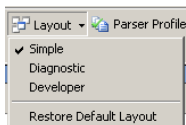
- «All captured frames»(все захваченные кадры);
- «Displayed frames»(отображаемые кадры). В данной опции можно также управлять записью экранного фильтра в сохраняемый файл захвата («Record display filter in capture file»), в остальных опциях запись экранного фильтра в сохраняемый файл производится автоматически;
- «Selected frames»(выделенные кадры);
- «Frame range»(указанные кадры).

После чего нажать кнопку «Сохранить».

2. Настройка MNM.

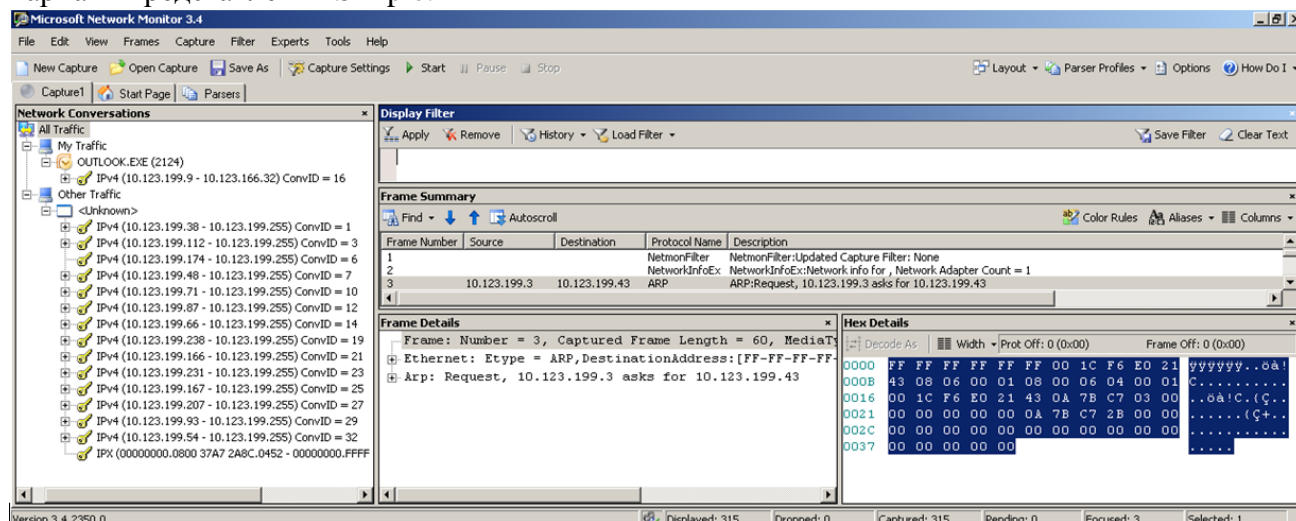
2.1. Настройка вида представления:

Настройка вида представления MNM производится нажатием на пиктограмму «Layout»(планировка, расположение окон) на панели инструментов. В меню можно выбрать один из следующих вариантов:

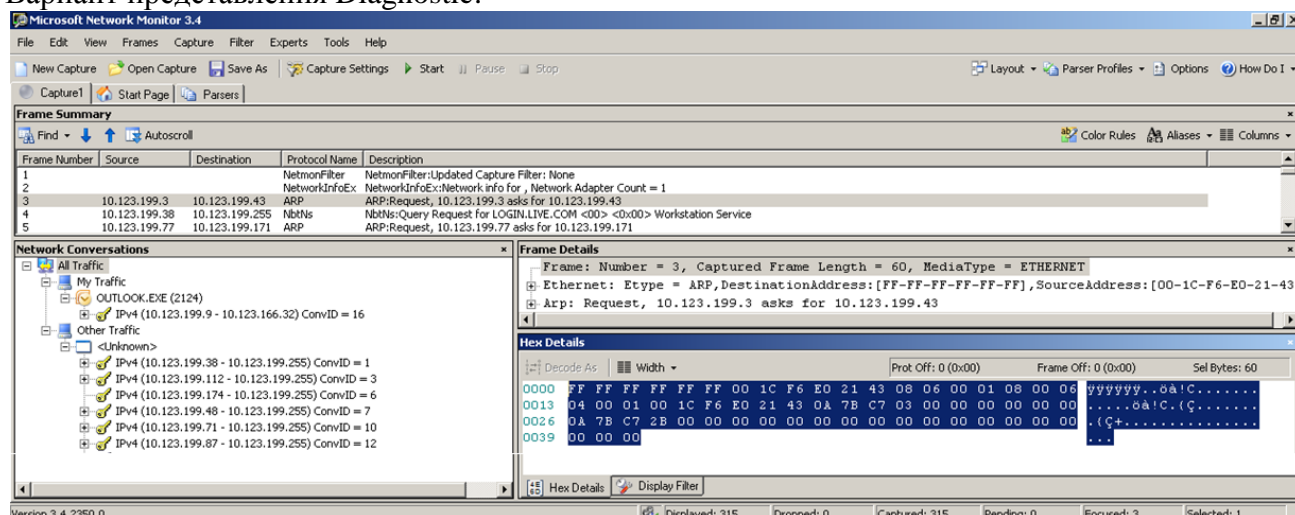


- | | |
|------------------------|--------------------------------------|
| Simple | - Простой |
| Diagnostic | - Диагностический |
| Developer | - Разработчик |
| Restore Default Layout | - Восстановление к виду по умолчанию |

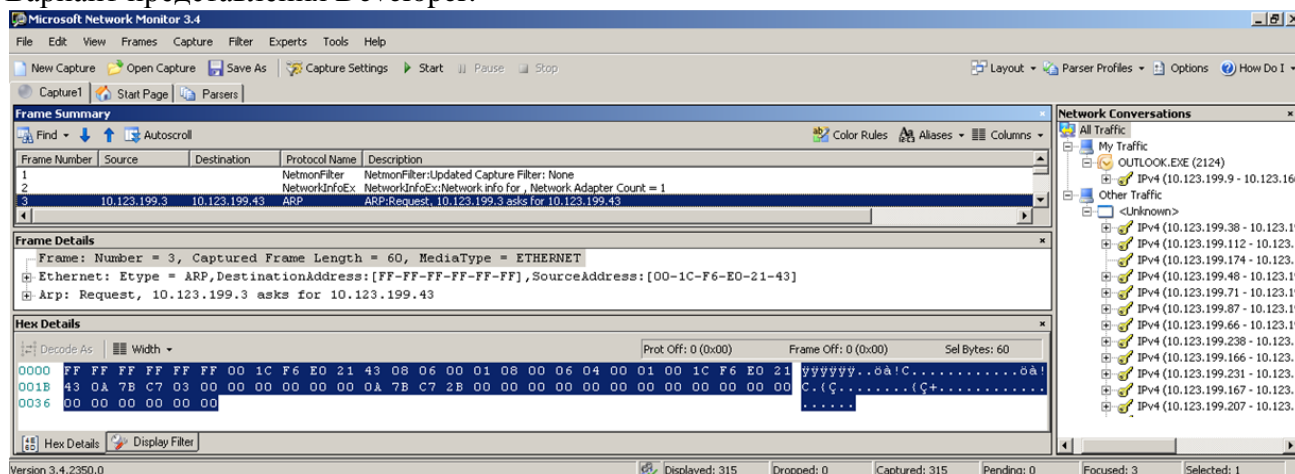
➤ Вариант представления Simple:



➤ Вариант представления Diagnostic:



➤ Вариант представления Developer:

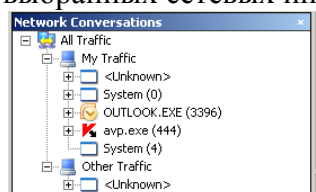


В каждом из трех перечисленных вариантов представления имеется пять окон:

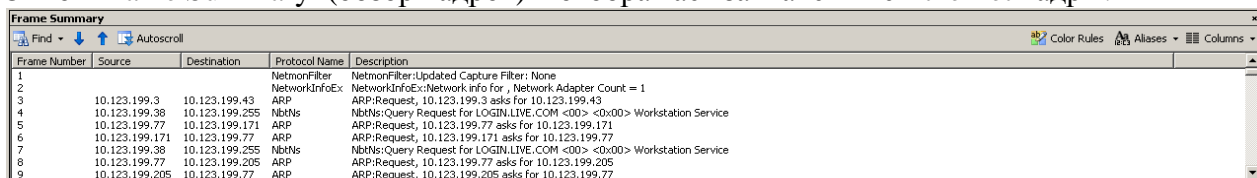
- 2.1.1. Network Conversations (сетевые разговоры, сетевой трафик);
- 2.1.2. Frame Summary (обзор кадров);
- 2.1.3. Frame Details (детальная информация по кадрам, детали по кадрам);
- 2.1.4. Display Filter (Фильтр отображения, экранный фильтр);
- 2.1.5. Hex Details (Детальная информация в шестнадцатитеричном(Hex) виде, Hex-Dump кадра).

Внимание: Каждое окно можно закрыть путем нажатия левой кнопки мыши (ЛКМ) на «крестик» в правом верхнем углу окна. Для возвращения окна в рабочую область необходимо в меню «View» выбрать пункт меню соответствующего окна.

- 2.1.1. Окно «Network Conversations»(сетевой трафик) - отображает сетевой трафик, захваченный с выбранных сетевых интерфейсов и сгруппированный по приложениям и IP-адресам.



2.1.2. Окно «Frame Summary»(обзор кадров) – отображает захваченные Ethernet кадры.



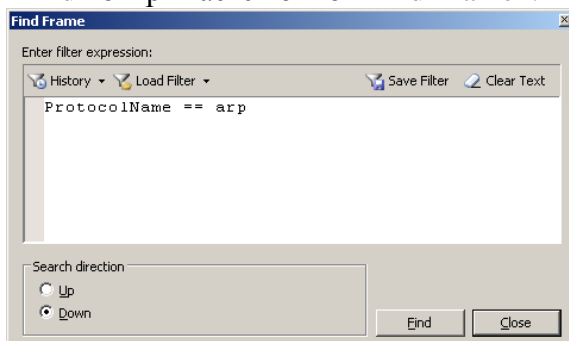
Frame Number	Source	Destination	Protocol Name	Description
1			NetmonFilter	NetmonFilter:Updated Capture Filter: None
2			NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 1
3	10.123.199.3	10.123.199.43	ARP	ARP:Request, 10.123.199.3 asks for 10.123.199.43
4	10.123.199.38	10.123.199.255	NbNls	NbNls:Query Request for LOGIN.LIVE.COM <00> <0x00> Workstation Service
5	10.123.199.77	10.123.199.171	ARP	ARP:Request, 10.123.199.77 asks for 10.123.199.171
6	10.123.199.171	10.123.199.77	ARP	ARP:Request, 10.123.199.171 asks for 10.123.199.77
7	10.123.199.38	10.123.199.255	NbNls	NbNls:Query Request for LOGIN.LIVE.COM <00> <0x00> Workstation Service
8	10.123.199.77	10.123.199.205	ARP	ARP:Request, 10.123.199.77 asks for 10.123.199.205
9	10.123.199.205	10.123.199.77	ARP	ARP:Request, 10.123.199.205 asks for 10.123.199.77

Данное окно состоит из трех частей:

- Заголовка окна;
- Панели инструментов окна («Find», «Autoscroll», «Color Rules», «Aliases», «Columns»);
- Таблицы вывода («Frame Number», «Source», «Destination», «Protocol Name», «Description»);

Панель инструментов окна «Frame Summary»(обзор кадров) позволяет управлять отображением и навигацией:

2.1.2.1. «Find»(найти) - позволяет осуществлять поиск информации по заданным критериям. В меню можно выбрать: «Find... Ctrl+F»(найти), «Find Next F3»(найти следующее совпадение), «Find Previous Shift+F3»(найти предыдущее совпадение), «Go To... Ctrl+G»(перейти к кадру с указанным номером). При выборе подменю «Find» открывается окно «Find Frame»:

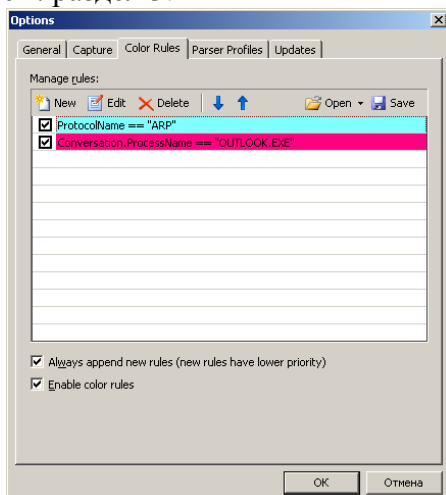


В данном окне необходимо ввести «filter expression»(выражение фильтрации). Подробнее по использованию см. раздел 3 ниже.

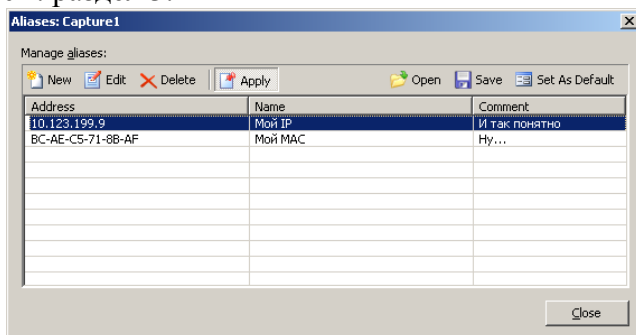
2.1.2.2. «Autoscroll»(автопрокрутка) - позволяет автоматический переход на последний принятый кадр. Если кнопка утоплена, то «Autoscroll» включен. При выключении «Autoscroll» курсор будет оставаться на выбранном кадре.

2.1.2.3. Кнопки «↕» служат для перехода на следующую или предыдущую строку таблицы.

2.1.2.4. «Color Rules»(цветовые правила) - позволяет проводить цветовое выделение кадров в окне «Frame Summary»(обзор кадров) по определенным критериям. Подробнее см. раздел 3.



- 2.1.2.5. «Aliases»(псевдоним) – позволяет назначать псевдонимы(альтернативные имена) IP- и MAC-адресам отображаемых в таблице окна «Frame Summary». Подробнее см. раздел 3.



- 2.1.2.6. «Columns»(Столбцы) – позволяет управлять столбцами: отображать наборы столбцов, выбирать и удалять столбцы и менять их месторасположение в таблице окна «Frame Summary».

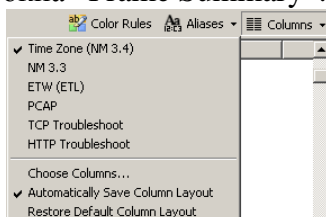
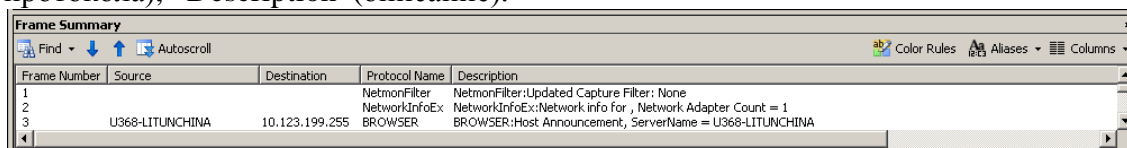
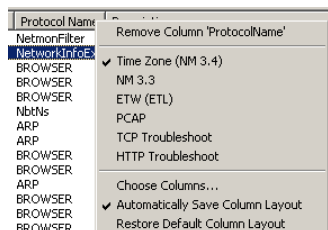


Таблица окна «Frame Summary»(обзор кадров) представлена по умолчанию пятью столбцами: «Frame Number»(номер кадра), «Source»(IP-адрес или имя NetBIOS источника), «Destination» (IP-адрес или имя NetBIOS назначения), «Protocol Name»(наименование протокола), «Description»(описание).



Внимание: Сама таблица структурно состоит из столбцов(columns), которые по горизонтали образует строки – все управление таблицей строится управлением столбцами, а не строками! Каждый столбец состоит из двух элементов: заголовка и собственно поля столбца таблицы. Для каждого элемента столбца таблицы имеется свой набор действий, вызываемый нажатием правой кнопкой мыши (ПКМ):

- ПКМ на заголовке столбца таблицы:



Позволяет выбирать вид отображения таблицы (по умолчанию это Time Zone (NM 3.4)), удалять столбцы заголовков (Remove Column `xxx`), а также переопределять(добавлять, удалять) состав столбцов таблицы и определять их порядок вывода (Choose Columns...).

Внимание: Мышью можно перетаскивать столбец на новое место, нажав и удерживая ЛКМ на заголовке столбца таблицы, а также изменять размеры столбца. Также можно изменять размер шрифта в каждом окне – для этого надо ЛКМ установить курсор(фокус) в любое окно, затем, зажав клавишу «Ctrl» прокрутить колесико мыши. Особое внимание необходимо обратить на пункт «Choose Columns...»(выбор столбцов), который позволяет вручную выбрать необходимые поля в таблице, позволяя тем самым формировать соответствующие регулярные выражения в фильтрах с помощью контекстного меню, вызываемого нажатием ПКМ на соответствующем поле столбца таблицы – см. следующий пункт;

- ПКМ на поле столбца таблицы:

Frame Number	Source	Destination	Protocol Name	Description
10	U316-POLOZKOVAE			
11	10.123.199.205	Copy		Ctrl+C
12	U561-GANTIMUREA	Copy 'Source'		
13	U464-PESTRETSOV	Add 'Source' to Display Filter		
14	U354-MARKOVAM			
15	U361-CHURAKOVAT	Add 'Source' as Color Rule		
16	U337-KURSUPOVAA	Disable This Color Rule		
17	U359-JANX			
18	U276-NAUMOVAYE	Create Alias for 'Source' Address		
19	U272-LVOWWG			
20	U562-PODOPRIG	Find Conversations		
21	U342-SHKEDOVATA	Select All		Ctrl+A
22	U340-VANEEVAV			
23	U348-BEZDENEZH			
24	ND-DOO	Parse Frame as XML		
25	U562-BANCISHIKTL	View Selected Frame(s) in a New Window		
26	U564A-TOKAREVAE	Add Selected Frame(s) To		
27	10.123.199.3			
28	U344-KUDRYAVTSE	Experts		
29	10.123.199.3			

Позволяет осуществлять следующие операции:

- [Copy Ctrl+C] – копирует в буфер обмена всю строку таблицы;
- [Copy `xxx`] – копирует в буфер обмена содержимое поля, в котором установлен указатель мыши.
- [Add `xxx` to Display Filter] – копирование в окно «Display Filter» содержимого поля, в котором установлен указатель мыши, в качестве аргумента в регулярном выражении. См. раздел 3;
- [Add `xxx` as Color Rule] – добавление в качестве аргумента в регулярное выражение цветовых правил значения поля, в котором установлен указатель мыши, что вызывает выделение цветом подходящих под условие регулярного выражения кадров;
- [Create Alias for `Source` или `Destination` Address] – Создание псевдонимов только для полей «Source» или «Destination»;
- [Find Conversations] – поиск трафика между «Source» и «Destination» по выбранным протоколам (IPv4, TCP, UDP, SMB, MSRPC и т.п.).

Внимание: Работа с контекстным меню полей столбцов таблицы является мощным средством автоматизации создания «Display Filter»(фильтров отображения) и «Color Rule»(цветовых правил), позволяющих эффективно фильтровать и выделять цветом кадры захватываемого трафика. Подробнее см. раздел 3.

Внимание: При работе в окне «Frame Summary»(обзор кадров) меняет свое представление

строка статуса: Displayed: 1115 Dropped: 0 Captured: 1115 Pending: 0 Focused: 328 Selected: 1, где:

- «Displayed» – показывает количество отображаемых кадров. Если не установлены фильтры, то значения «Displayed» и «Captured» будут равны;
- «Dropped» - показывает количество отброшенных кадров. Если монитор работает в режиме «P-mode»(неразборчивый режим – см. выше) или сетевой интерфейс подключен к порту коммутатора, то данное поле всегда будет равно «0». Если режим «P-mode» выключен и сетевой интерфейс подключен к порту Hub, то кадры, не предназначенные для данного сетевого интерфейса, будут отбрасываться(dropped);
- «Captured» - показывает количество захваченных кадров;
- «Pending» - показывает количество нераспознанных кадров;
- «Focused» - показывает номер кадра в текущей сессии(Capture), значение поля «Focused» равно значению поля «Frame Number»(номер уадра) в таблице окна «Frame Summary»(обзор кадров);
- «Selected» - показывает количество выделенных кадров;

2.1.3. Окно «Frame Details»(детали по кадрам) - отображает детальную информацию по каждому кадру с вложенными в него структурами протоколов верхнего уровня модели DOD:

Frame Details
Frame: Number = 316, Captured Frame Length = 54, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-00-0C-07-AC-09], SourceAddress: [BC-AE-C5-71-8B-AF]
IPv4: Src = 10.123.199.9, Dest = 10.123.166.32, Next Protocol = TCP, Packet ID = 1169, Total IP Length = 40
Tcp: Flags=...&...., SrcPort=1155, DstPort=11374, PayloadLen=0, Seq=1787724927, Ack=2342139299, Win=65535 (scale factor 0x0) = 65535

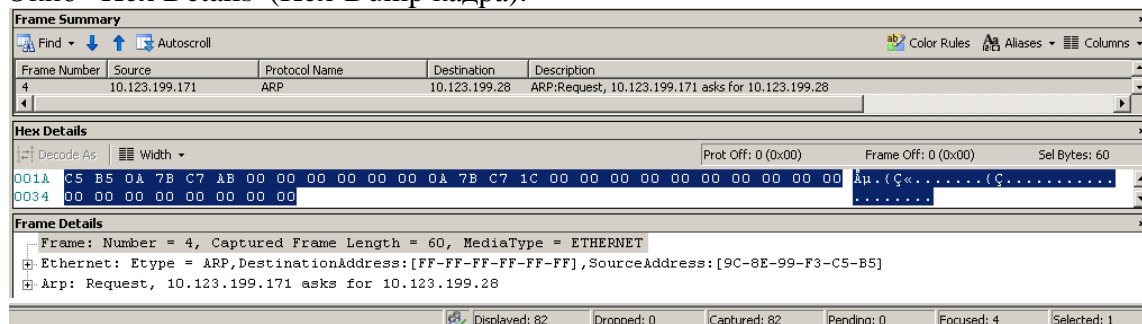
В первой строке указывается общая информация о кадре. Данная информация вычисляется и обобщается MNM из реальных полей кадра:

Frame: Number = 316, Captured Frame Length = 54, MediaType = ETHERNET, что означает:

Кадр: Номер = 316, Размер кадра в байтах = 54, Тип среды передачи/Тип кадра = ETHERNET.

Далее следует несколько, в зависимости от «вложенных» в кадр структур протоколов верхнего уровня модели DOD, пунктов. Каждый пункт начинается со знака «+», нажав на который ЛКМ, будет развернута структура соответствующего протокола.

2.1.4. Окно «Hex Details»(Hex-Dump кадра):

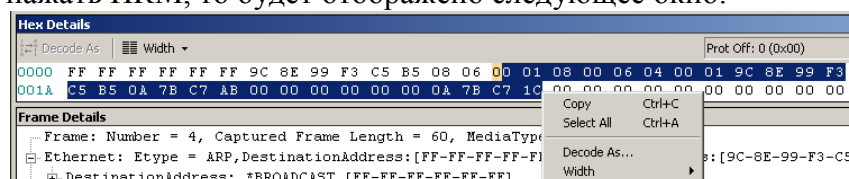


На вышеприведенном рисунке в окне «Frame Summary»(обзор кадров) показан кадр №4, содержащий протокол ARP.

В окне «Hex Details»(Hex-dump кадра) указан шестнадцатеричный(Hex) дамп кадра, позволяющий видеть все значения полей кадра в Hex и ASCII видах. Окно «Hex Details» состоит из трех частей:

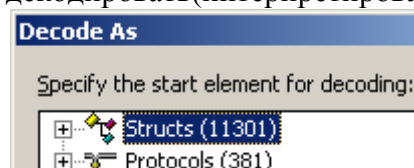
- Заголовка, в котором отображается заголовок окна;
- Панели инструментов, в которой отображаются две пиктограммы: «Decode As»(декодировать как) – неактивна и «Width» - управление шириной Hex-таблицы, а также статусной строки, в которой отображается три параметра:
 - «Prot Off:» - смещение от начала структуры протокола;
 - «Frame Off» - смещение от начала кадра;
 - «Sel Bytes:» - число выделенных байт.
- Собственно таблицы, которая состоит из трех столбцов:
 - Значение смещения в таблице;
 - Данные в шестнадцатеричном(Hex) виде;
 - Данные в текстовом(ASCII) виде.

Внимание: Если в таблице в зоне Hex или ASCII выделить некоторое количество байтов и нажать ПКМ, то будет отображено следующее окно:



- Copy Ctrl+C - Копировать выделенный фрагмент в буфер обмена.
- Select All Ctrl+A - Выделить все.
- Decode As... - Декодировать как.
- Width - Открывает меню с настройкой ширины таблицы.

Наибольший интерес представляет собой пункт меню «Decode As...», который позволяет декодировать(интерпретировать) выделенный фрагмент как структуру или протокол:



МNM позволяет распознать и интерпретировать 11 301 структуру или 381 протокол.

2.1.5. Окно «Display Filter»(экранный фильтр) – предназначено для ввода регулярных выражений, позволяющих управлять отображением информации в окне «Frame Summary»(обзор кадров)в соответствии с критериями отбора, заданными в регулярном выражении.

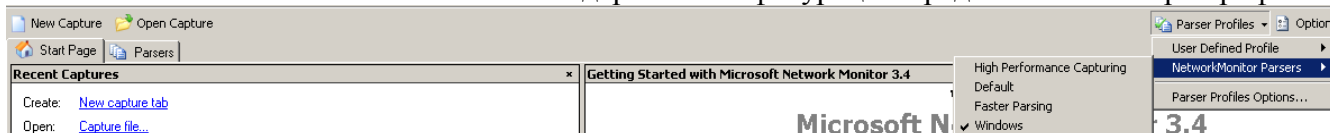


Окно «Display Filter» состоит из трех частей:

- Заголовка, в котором отображается заголовок окна;
- Панели инструментов, в которой отображаются шесть пиктограмм: «Apply»(применить фильтр), «Remove»(снять фильтр), «History»(история - обеспечивает доступ к ранее введенным выражениям), «Load Filter»(загрузить фильтр - обеспечивает доступ к стандартным(шаблонным) фильтрам и сохраненным пользовательским фильтрам), «Save Filter»(сохранить фильтр – обеспечивает сохранение фильтра в файле .NMF), «Clear Text»(Очистка окна с регулярными выражениями).
- Окно редактора, в котором записываются регулярные выражения фильтрации – подробнее см. раздел 3.

2.2. Настройка параметров работы MNM

Основной настройкой, влияющей на скорость работы анализатора и на полноту распознавания захваченного трафика является выбор «Parsers Profiles»(профиля анализатора). Для выбора профиля в панели инструментов анализатора нажимаем ЛКМ пиктограмму «Parsers Profiles»-«NetworkMonitor Parsers». В стандартной конфигурации представлено четыре профиля:



- High Performance Capturing - Обеспечивает наивысшую скорость анализа трафика при фильтрации, улавливая протоколы канального сетевого и транспортного уровня модели DOD.
- Default - Подходит для большинства потребностей в анализе сетевого трафика.
- Faster Parsing - Обеспечивает минимальный анализ захваченного трафика при максимальной скорости записи.
- Windows - Обеспечивает полный анализ протоколов для Microsoft Windows в соответствии с библиотекой MSDN.

Внимание: Самым «знающим» профилем анализатора и соответственно самым медленным является профиль «Windows». Если при захвате трафика не обнаруживается требуемый трафик, например, IGMP, то необходимо выбрать профиль «Windows».

Внимание: В зависимости от выбранного профиля анализатора в окне «Frame Summary»(обзор кадров) по разному будут отображаться значения столбцов «Source» и «Destination». Так для «High Performance Capturing» в указанных столбцах будут указаны соответствующие IP-адреса, во всех остальных профилях в данных столбцах будут указаны псевдонимы IP-адресов, соответствующие именам ПК.

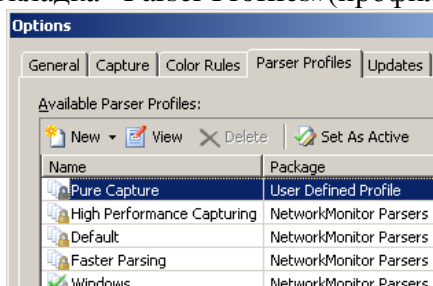
Доступ к основным настройкам MNM можно получить двумя способами:

- На панели инструментов нажать ЛКМ на пиктограмме «Options»;
- На панели инструментов нажать ЛКМ на пиктограмме «Parsers Profiles»-«Parsers Profiles Options...»

В обоих случаях будет выведено окно «Options» имеющее пять вкладок: «General»(общие настройки), «Capture»(настройки захвата), «Color Rules»(правила выделения цветом), «Parser Profiles»(профили анализатора), «Updates»(обновления MNM). По умолчанию отображается вкладка «Parser Profiles»(профили анализатора).

Рассмотри подробнее настройки MNM:

- Вкладка «Parser Profiles»(профили анализатора).



Профили анализаторы рассматривались выше в данном разделе, кроме «Pure Capture», который позволяет проводить захват и анализ только Ethernet-кадров. Для более эффективного захвата с использованием профиля «Pure Capture» рекомендуется запускать MNM из командной строки:

```
nmcap /capture /file samplecapture.cap
```

Рассмотрим подробнее использование профиля «Pure Capture» с использованием консольной программы «nmcap». Команда имеет несколько параметров. Полный список команд можно получить «nmcap /?»:

Nmcap [network] [capture protocol] [capture filename], где

[network] – обязательный параметр обозначающий имя сетевого интерфейса с которого необходимо начать захват данных.

Данный параметр может принимать следующие параметры:

(*) - все сетевые интерфейсы;

(x,y,z) – указанные сетевые интерфейсы. Для просмотра номеров сетевых интерфейсов нужно воспользоваться командой «nmcap /DisplayNetwork»

[capture protocol] – необязательный параметр обозначающий протокол(SMB, LDAP, DNS, DHCP), который необходимо захватывать.

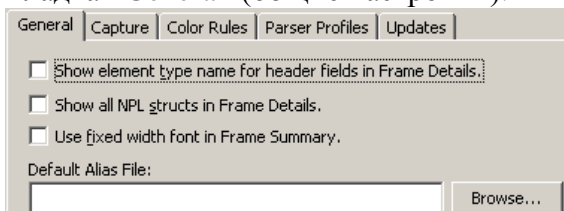
[capture filename] – обязательный параметр обозначающий имя захвата.

Пример: nmcap /network 1 /capture DNS /file MyCaptureFile.cap

В дополнение к сказанному с помощью пиктограмм на данной вкладке можно:

- Устанавливать используемый профиль по умолчанию при загрузке MNM – «Set As Active»;
- Удалять профиль – «Delete» - неактивно для приведенных профилей;
- Просматривать параметры профиля – «View»;
- Создавать новые профили – «New».

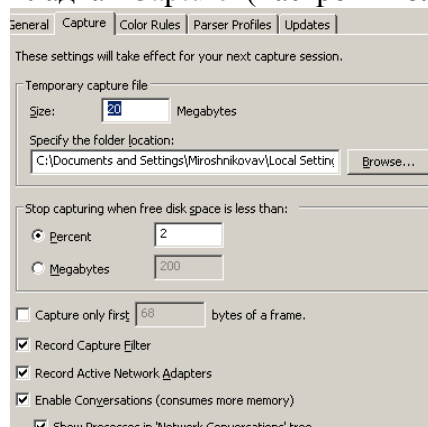
- Вкладка «General»(общие настройки).



- Show element type name for header fields in Frame Details – Показывать в окне «Frame Details»(детальная информация по кадрам) имя типа элемента для полей заголовка, например, «< UINT16 HardwareType: Ethernet>» и «< HardwareType: Ethernet> (UINT16: U – Unsigned(беззнаковое), INT – INTeger(целое), 16 - кол-во битов);

- Show all NPL structs in Frame Details – Показывать все NPL(Network Monitor Parsing Language) структуры в окне «Frame Details»(детальная информация по кадрам);
- Use fixed width font in Frame Summary – Использовать шрифт фиксированной ширины в окне «Frame Summary»(обзор кадров);
- Default Alias File: - Установить по умолчанию псевдонимы для IP- и MAC-адресов, сохраненные в файле «.nma».

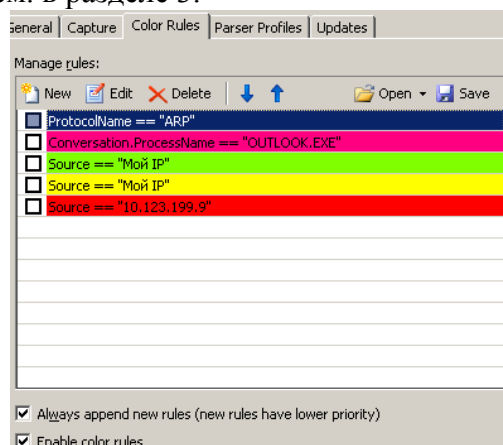
• Вкладка «Capture»(настройки захвата).



- Раздел «Temporary capture file»(временный файл захвата).
 - ✓ Параметр «Size»(размер) определяет размер временного файла захвата в мегабайтах;
 - ✓ Параметр «Specify the folder location:» определяет месторасположение временного файла захвата.
- Раздел «Stop capturing when free disk space is less than:»(Остановить захват, когда свободное место на диске меньше).
- Параметр «Capture only first bytes a frame.»(Захватывать первые XX байтов кадра).

- Параметр «Record Capture Filter»(запись фильтра захвата) – позволяет записать в файл захвата «.cap» фильтр захвата.
- Параметр «Record Active Network Adapters»(запись активных сетевых адаптеров) – позволяет записать в файл захвата «.cap» трафик с активных сетевых адаптеров.
- Параметр «Enable Conversations (consumes more memory)»включить разделение сетевого трафика по приложениям, протоколам и адресам (потребляет больше памяти)).
- Параметр «Show Processes in «Network Conversations» tree»(показывать процессы в дереве «Network Conversations»).

• Вкладка «Color Rules»(правила выделения цветом). Подробнее создание цветового правила см. в разделе 3.



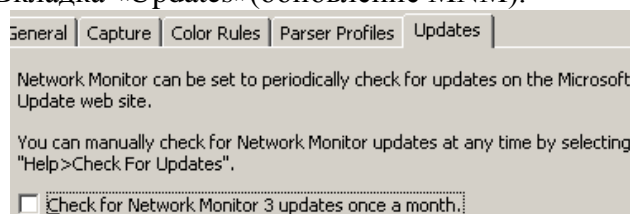
Панель инструментов позволяет

- Создавать новые правила – «New»;
- Редактировать текущие правила – «Edit»;
- Удалять текущие правила – «Delete»;
- Сохранять текущие правила – «Save»;
- Загружать сохраненные правила – «Open».

Always append new rules (new rules have lower priority)
- Всегда добавлять новые правила (новые правила имеют более низкий приоритет).

Enable color rules – Включить цветовые правила.

• Вкладка «Updates»(обновление MNM).



Check for Network Monitor 3 updates once a month – Проверка обновления Network Monitor один раз в 3 месяца.

3. Анализ захваченных данных

Для удобства анализа захваченных данных NMN предлагает следующие средства группировки, выделения и поиска информации:

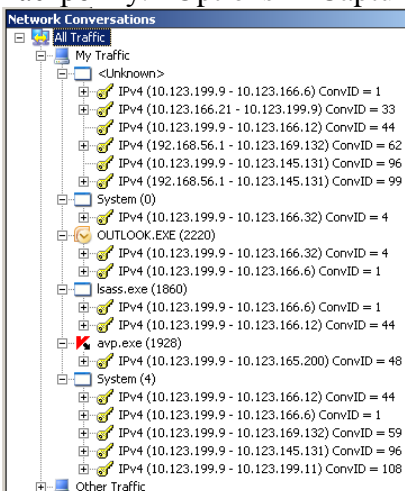
- Отображение трафика, сгруппированного по приложениям и IP-адресам – окно «Network Conversations»(сетевой трафик);
- Отображение трафика, отфильтрованного в соответствии с заданным условием – окно «Display Filter»(экранный фильтр);
- Визуальное выделение трафика цветом, сформированным в соответствии с «Color Rules»(цветовые правила);
- Замена MAC- и IP-адресов осмысленными псевдонимами - «Aliases»(псевдоним);
- Поиск данных в захваченном трафике в соответствии с заданным условием.

3.1. Отображение трафика, сгруппированного по приложениям и IP-адресам – окно «Network Conversations»(сетевой трафик). Прежде чем кидаться с головой в море отловленного трафика и не захлебнуться в нем, необходимо воспользоваться средством «Network Conversations». Для вызова соответствующего окна необходимо нажать ЛКМ на пункт меню «View»-«Network Conversations». В открывшемся окне будут три элемента:



- «All Traffic»;
- «My Traffic»;
- «Other Traffic».

Внимание: Если окно «Network Conversations» не открывается – необходимо проверить настройку: «Options»-«Capture»-«Enable Conversations (consumes more memory)».



В элементе «My Traffic»(мой трафик) отображается входящий и исходящий сетевой трафик с выбранного при запуске MNM собственного сетевого интерфейса и сгруппированного по процессам(System(0,4), OUTLOOK.EXE(2220), lsass.exe(1860), avr.exe(1928) – в скобках указан идентификатор процесса, PID – см. параметр «Show Processes in «Network Conversations» tree» в «Options»-«Capture»). В группе «Unknown»(неизвестно) собран трафик, который не принадлежит какому-либо процессу.

В элементе «Other Traffic»(другой трафик) отображается, как правило, широкополосный или мультикастовый трафик.

Внимание: При выборе любой строки в любой секции окна «Network Conversations» заголовок окна «Frame Summary»(обзор кадров) изменит свой вид: в нем появится «Conversation Filter»: Frame Summary - [Conversation Filter], указывающий на то, что в окне «Frame Summary»(обзор кадров) отображены лишь кадры соответствующие условиям, заданным в окне «Network Conversations». Кроме этого, в статусной строке параметр «Displayed» укажет количество кадров, соответствующим значениям фильтра. Для снятия фильтра необходимо в окне «Network Conversations» установить курсор мыши (ЛКМ) на элементе «All Traffic».

Внимание: Управлять поиском необходимого трафика между определенными IP-адресами можно не только в окне «Network Conversations», но и с помощью контекстного меню в окне «Frame Summary». Например, для поиска DNS-трафика между двумя unicast-адресами необходимо воспользоваться пунктом контекстного меню «Find Conversation»(найти трафик) в окне «Frame Summary»(обзор кадров), для этого необходимо:

- Сделать видимым окно «Network Conversations»(сетевой трафик) - иначе не работает;
- В окне «Frame Summary»(обзор кадров) установить курсор мыши на любое поле столбца таблицы, которое в поле «Protocol Name» указан протокол «DNS»(такую строку можно найти

просмотром данного поля в таблице, или с помощью экранного фильтра – об этом ниже или с помощью функции поиска – об этом ниже) нажать ПКМ и в контекстном меню выбрать «Find Conversation»(найти трафик);

- В появившемся меню выбрать протокол «DNS»

Результатом будет следующее:

- Заголовок окна «Frame Summary»(обзор кадров) изменит вид на «Frame Summary – [Conversation Filter]»;
- В окне «Frame Summary»(обзор кадров) будут отображены кадры, содержащих в себе структуру «DNS», и у которых входящие или исходящие IP-адреса соответствуют IP-адресам, указанные в полях «Source» и «Destination» той строки таблицы окна «Frame Summary», на которую был установлен фокус;
- В окне «Network Conversations» будет раскрыта ветвь дерева, содержащая выбранный трафик;
- В статусной строке будет указана соответствующая информация по количеству отображенных(Displayed) кадров.

Соответственно, для поиска определенного трафика для определенных IP-адресов лучше всего воспользоваться экранным фильтром или функцией поиска – см. ниже.

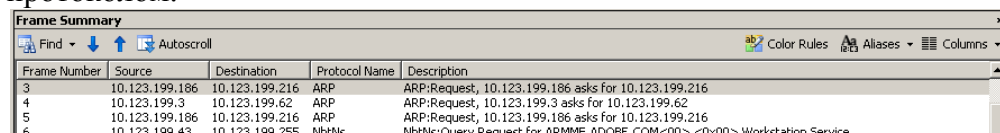
3.2. Отображение трафика, отфильтрованного в соответствии с заданным условием – окно «Display Filter»(экранный фильтр).

В окне «Display Filter» условия отбора кадров необходимо задавать вручную с использованием, так называемых, регулярных выражений. Несмотря на кажущуюся сложность именно «Display Filter» является самым мощным и гибким средством фильтрации трафика.

3.2.1. Рассмотрим сначала формирование экранных фильтров с помощью, так называемого способа «Right-Click Filtering». Данный способ работает в окнах «Frame Details»(детали по кадрам) и «Frame Summary»(обзор кадров). Использование «Right-Click Filtering» удобно в том случае, когда необходимые данные уже видны в окне «Frame Summary» и нуждаются в фильтрации(отделения плевел от зёрен).

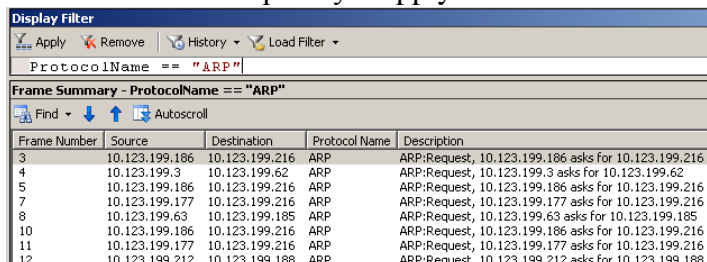
- **Задача 1: Найти с помощью экранного фильтра все кадры с протоколом ARP.**

Предположим, что в окне «Frame Summary»(обзор кадров) мы нашли кадр №3 с ARP протоколом и хотим отобразить в окне «Frame Summary» только кадры с этим протоколом.



Frame Number	Source	Destination	Protocol Name	Description
3	10.123.199.186	10.123.199.216	ARP	ARP:Request, 10.123.199.186 asks for 10.123.199.216
4	10.123.199.3	10.123.199.62	ARP	ARP:Request, 10.123.199.3 asks for 10.123.199.62
5	10.123.199.186	10.123.199.216	ARP	ARP:Request, 10.123.199.186 asks for 10.123.199.216
6	10.123.199.43	10.123.199.255	NbtNs	NbtNs:Query Request for ARMMF.ADOBE.COM<00> <0x00> Workstation Service

Для этого нужно нажать ПКМ на поле «Protocol Name» строки №3 и в контекстном меню выбрать «Add "Protocol Name" to Display Filter». В результате этого в окне «Display Filter»(экранный фильтр) появится строка «ProtocolName == "ARP"» и при нажатии на пиктограмму «Apply» окно «Frame Summary» отобразит следующие кадры:



Display Filter

Apply Remove History Load Filter

ProtocolName == "ARP"

Frame Summary - ProtocolName == "ARP"

Frame Number	Source	Destination	Protocol Name	Description
3	10.123.199.186	10.123.199.216	ARP	ARP:Request, 10.123.199.186 asks for 10.123.199.216
4	10.123.199.3	10.123.199.62	ARP	ARP:Request, 10.123.199.3 asks for 10.123.199.62
5	10.123.199.186	10.123.199.216	ARP	ARP:Request, 10.123.199.186 asks for 10.123.199.216
7	10.123.199.177	10.123.199.216	ARP	ARP:Request, 10.123.199.177 asks for 10.123.199.216
9	10.123.199.63	10.123.199.185	ARP	ARP:Request, 10.123.199.63 asks for 10.123.199.185
10	10.123.199.186	10.123.199.216	ARP	ARP:Request, 10.123.199.186 asks for 10.123.199.216
11	10.123.199.177	10.123.199.216	ARP	ARP:Request, 10.123.199.177 asks for 10.123.199.216
12	10.123.199.212	10.123.199.188	ARP	ARP:Request, 10.123.199.212 asks for 10.123.199.188

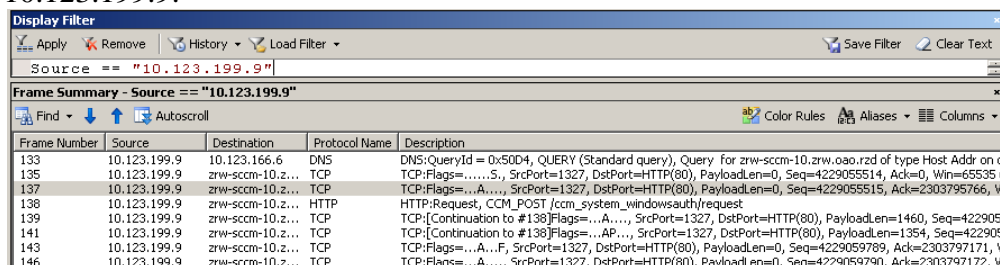
Необходимо обратить внимание на то, как изменился заголовок окна «Frame Summary» - в нем указан действующий фильтр: ProtocolName == "ARP".

- **Задача 2: Найти с помощью экранного фильтра все кадры, содержащие IP-датаграммы с определенным IP-адресом источника.**

Для этого нужно нажать ПКМ на поле «Source» интересующего нас IP-адреса и в контекстном меню выбрать «Add "Source" to Display Filter». **Внимание:** Нужно

обратить внимание на состояние окна «Frame Summary», если в его заголовке присутствует название фильтра, то его необходимо снять нажатием ЛКМ на пиктограмме «Remove» окна «Display Filter». В принципе новый фильтр накладывается корректно на все данные, но лучше не рисковать (MNM может содержать ошибки в коде).

Итак, очищаем старый фильтр нажатием ЛКМ на пиктограмме «Remove» окна «Display Filter» и формируем новый фильтр - в качестве источника выбран адрес 10.123.199.9:



- **Задача 3: Найти с помощью экранного фильтра все кадры, содержащие IP-датаграммы с IP-адресом источника 10.123.199.9 и содержащие в себе структуру DNS.**

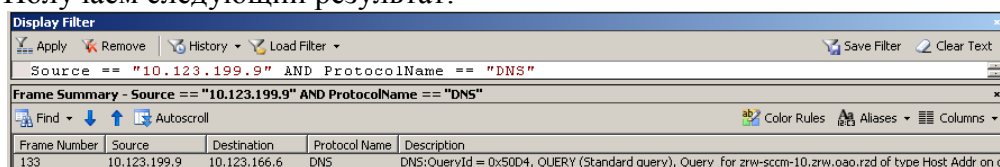
Здесь речь идет о двойном фильтре, который реализуется следующим образом:

- В окне «Display Filter» снимаем ранее наложенный экранный фильтр – нажать пиктограмму «Remove»;
- В окне «Display Filter» очищаем содержимое окна редактора - нажать пиктограмму «Clear Text»;
- В окне «Frame Summary» нажать ПКМ на поле «Source» с IP-адресом 10.123.199.6 и в контекстном меню выбрать «Add "Source" to Display Filter»;
- В окне «Display Filter» активируем фильтр - нажать пиктограмму «Apply»;
- В окне «Frame Summary» нажать ПКМ на поле «Protocol Name» с протоколом DNS и в контекстном меню выбрать «Add "Protocol Name" to Display Filter» - в окне «Display Filter» в окне редактора будет отображена следующая команда:

«Source == "10.123.199.9" OR ProtocolName == "DNS"»

Необходимо заменить логический оператор «OR»(ИЛИ) на логический оператор «AND»(И);

- В окне «Display Filter» активируем фильтр - нажать пиктограмму «Apply»;
- Получаем следующий результат:



Для формирования экранных фильтров, содержащих два и более условий, применяются следующие логические операторы:

- «OR», «||» - логическое «ИЛИ»;
- «AND», «&&» - логическое «И»;
- «NOT», «!» - логическое «НЕТ» - отрицание.

Пример:

- «ARP or NbtNs» - отобразит в окне «Frame Summary» кадры, содержащие в себе ARP- и NbtNs-сообщения.
- «ARP and Source == "10.123.199.3"» - отобразит в окне «Frame Summary» кадры с ARP-сообщениями у которых в поле «Source» указан IP-адрес 10.123.199.3. **Внимание:**

кадры с ARP-сообщениями не содержат IP-датаграмм, поэтому, в данном примере указанный IP-адрес находится в структуре ARP, соответственно если ввести такой фильтр «ARP and IPv4.address == 10.123.199.3», то в окне «Frame Summary» не будет отображено ни одной записи!!!

- «not ARP» или «!ARP» - отобразит в окне «Frame Summary» все кадры не имеющем в своем составе ARP-сообщений.

Для формирования экранных фильтров также применяются следующие операторы присвоения и сравнения:

- «==» - равно;
- «!=» - не равно;
- «<» - меньше чем;
- «>» - больше чем.

Пример:

- «Source == "10.123.199.3"» - отобразит в окне «Frame Summary» кадры, у которых в поле таблицы «Source» хранится указанный IP-адрес;
- «Ethernet.DestinationAddress != BROADCAST» - отобразит в окне «Frame Summary» кадры, у которых в поле кадра «Ethernet.DestinationAddress» хранится любой MAC-адрес кроме широковещательного;

Приоритет выполнения операций в экранном фильтре регулируется круглыми скобками: «()».

Пример: «!(Destination == "10.123.199.1" AND Source == "10.123.199.203")»

3.2.2. Рассмотрим вариант ручного создания экранных фильтров в окне редактора окна «Display Filter». Данный способ фильтрации трафика применяется в случае, когда в окне «Frame Summary» нет возможности выбора необходимых параметров – они еще не видны.

В самом начале необходимо сказать, что в MNM уже встроено много стандартных фильтров, которые можно вызвать, нажав в окне «Display Filter» ЛКМ на пиктограмме «Load Filter»-«Standards Filters».

При работе в редакторе окна «Display Filter» есть несколько особенностей:

- Комментарии начинаются с символов «//»;
- При наборе текста фильтра, если после слова фильтра указать «.», то возникает меню с предполагаемыми вариантами. Если меню не возникло, значит вариантов нет. Использование символа «.» позволяет сформировать более точный фильтр;
- В фильтрах возможно применение логических операторов «И», «ИЛИ», «НЕТ», а также группирование круглыми скобками;
- Широковещательный адрес может обозначаться как: «BROADCAST» или «0xFFFFFFFF» или «FF-FF-FF-FF-FF-FF».

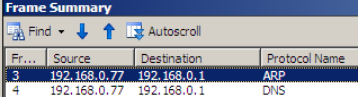
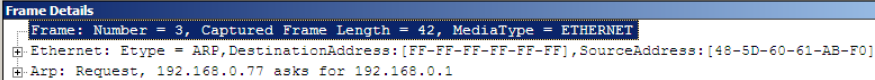
В нижерасположенной таблице приведены примеры формирования фильтров с разделением их по уровням модели DOD. Необходимо обратить внимание на то, что одного и того же результата можно добиться несколькими видами команд фильтров. По все видимости каждому профилю анализатора (Parser Profile) соответствует свой набор команд. В документации на MNM сказано, что команды фильтров, начинающиеся со слова «FRAME» относятся к формату «High Performance Capture filtering»:

№	Содержимое фильтра
Канальный уровень модели DOD	
1.	ARP или ProtocolName == "ARP" (отображает все кадры содержащие структуру ARP)
	ARP.SendersIp4Address == 192.168.0.77 (отображает все кадры с ARP-запросами от ПК с IP-адресом 192.168.0.77)
	Protocol.ARP (отображает все кадры содержащие структуру ARP)
	Protocol.ARP.TargetMacAddress != 0x0 (отображает все кадры с ARP-ответами)
	Ethernet.ARP (отображает все кадры содержащие структуру ARP)
2.	Ethernet.ARP.TargetMacAddress != 00-00-00-00-00-00 AND Ethernet.ARP.SendersIp4Address == 192.168.0.77 (отображает кадры с ARP-ответами от ПК с IP-адресом 192.168.0.77)
	Ethernet.Address == 01-02-03-04-05-06 (отображает кадры, в которых MAC-адрес отправителя или получателя равен указанного в выражении)
	FRAME.Ethernet.ARP (отображает все кадры содержащие структуру ARP)
	FRAME.Ethernet.ARP.OpCode == 0x1 (отображает все кадры с ARP-запросами)
	Кроме протокола ARP еще на канальном уровне можно отфильтровать все кадры рассылаемые широковещательно: protocol.Ethernet.DestinationAddress == 0xffffffffffff Ethernet.DestinationAddress == FF-FF-FF-FF-FF-FF FRAME.Ethernet.DestinationAddress == BROADCAST А также: Frame.WiFi.Address == 0x00508DD111A1 Protocol.PPPoE
Сетевой уровень модели DOD	
2.	IPv4 или ProtocolName == "IPv4" (отображает все кадры содержащие структуру IPv4)
	IPv4.Address == 192.168.0.1 (отображает все кадры, содержащие IP-датаграммы с адресом источника или назначения равного «192.168.0.1»)
	IPv4.Address == IpConfig.LocalIpv4Address (отображает все кадры, содержащие IP-датаграммы с адресом источника или назначения равного текущему IP-адресу)
	IPv4.Address == 10.0.0.1 and IPv4.Address == 10.0.0.222 (отображает трафик между двумя IP-хостами)
	Protocol.IPv4 (отображает все кадры содержащие структуру IPv4)
	Protocol.IPv4.ICMP (отображает все кадры, содержащие IP-датаграммы с протоколом ICMP)
	Ethernet.IPv4 (отображает все кадры содержащие структуру IPv4)
	Ethernet.IPv4.TotalLength > 1479 (отображает все кадры, содержащие IP-датаграммы размером от 1480 до 1500 байт)

	FRAME.Ethernet.IPv4 (отображает все кадры содержащие структуру IPv4) FRAME.Ethernet.IPv4.DestinationAddress == 192.168.0.77 (отображает все кадры, содержащие IP-датаграммы с адресом назначения «192.168.0.77»)
На сетевом уровне, т.е. используя префикс «IPv4», можно фильтровать кадры с ICMP(IPv4.ICMP) и IGMP(IPv4.IGMP), так как структуры этих протоколов инкапсулируются в IP-датаграммы.	
Транспортный уровень модели DOD	
3.	UDP или ProtocolName == "UDP" (отображает все кадры содержащие структуру UDP) Udp.Port == 389 (отображает все кадры с LDAP протоколом) TCP или ProtocolName == "TCP" (отображает все кадры содержащие структуру TCP) TCP.Port == 389 (отображает все кадры с LDAP протоколом)
	Protocol.UDP (отображает все кадры содержащие структуру UDP) Protocol.UDP.Port == 339 (отображает все кадры с LDAP протоколом) Protocol.TCP (отображает все кадры содержащие структуру TCP) Protocol.TCP.Port == 339 (отображает все кадры с LDAP протоколом)
	Ethernet.IPv4.Udp (отображает все кадры содержащие структуру UDP) Ethernet.IPv4.Udp.Port == 339 (отображает все кадры с LDAP протоколом) Ethernet.IPv4.Tcp (отображает все кадры содержащие структуру TCP) Ethernet.IPv4.Tcp.Port == 80 (отображает все кадры HTTP протокола)
	Frame.Ethernet.Ipv4.UDP (отображает все кадры содержащие структуру UDP) Frame.Ethernet.Ipv4.UDP.Port == 80 (отображает все кадры HTTP протокола) Frame.Ethernet.IPv4.TCP (отображает все кадры содержащие структуру TCP) Frame.Ethernet.IPv4.TCP.Port == 80 (отображает все кадры HTTP протокола)
Прикладной уровень модели DOD	
4.	DNS или ProtocolName == "DNS" (отображает все кадры содержащие структуру DNS)
	Protocol.DNS (отображает все кадры содержащие структуру DNS)
	Ethernet.Ipv4.Udp.Port == 53

	(отображает все кадры содержащие структуру DNS)
	Frame.Ethernet.IPv4.UDP.Port == 53
	(отображает все кадры содержащие структуру DNS)

Внимание: при наборе команд фильтрации необходимо обратить внимание на следующие моменты:

<ul style="list-style-type: none">  <p>В окне «Frame Summary»(обзор кадров) в кадре №3 в столбце «Source» указан IP-адрес 192.168.0.77. При наложении следующего фильтра: «IPv4.address == 192.168.0.77» кадр с №3 отсутствует в окне «Frame Summary». Данная ситуация происходит потому, что кадр №3 не содержит структуру «IPv4», но содержит структуру протокола ARP, в которой в поле «SendersIp4Address» и содержится IP-адрес 192.168.0.77 (см. окно «Frame Details»), который и подставляется в столбец «Source» окна «Frame Summary»:</p>  <p>Для того чтобы отфильтровать все кадры, у которых в столбце «Source» указан IP-адрес 192.168.0.77 необходимо задать следующий фильтр: «Source == "192.168.0.77"»</p> 	<p>Следующие фильтры будут отображать кадры, в соответствующих полях которых, имеется указанная строка (это удобно, чтобы не рыться в соответствующих структурах кадров):</p> <p>Property.Source.contains("moses.drweb.com") (отображает кадры, у которых в столбце «Source» содержится строка «moses.drweb.com»)</p> <p>Property.Destination.contains("sitecheck2.opera.com") (отображает кадры, у которых в столбце «Destination» содержится строка «sitecheck2.opera.com»)</p> <p>Property.Description.contains("Continuation to #292") (отображает кадры, у которых в столбце «Description» содержится строка «Continuation to #292»)</p> <p>Property.ProtocolName.contains("HTTP") (отображает кадры, у которых в столбце «ProtocolName» содержится строка «HTTP»)</p>
<ul style="list-style-type: none"> <p>Следующий фильтр будет отображать кадры, у которых в определенных позициях кадра содержится определенная информация (это удобно когда структура протокола верхнего уровня, инкапсулированного в кадр, неизвестна MNM):</p> <p>UINT16(FrameData, 12)==0x0806 (отображает кадры, у которых по смещению(см.«Frame Off:») 12_{Dec} имеется 16-ти битное поле равное «0806_{Hex}»)</p> 	<p>Следующие фильтры являются составными(используются логические операторы):</p> <p>TCP.Port == 80 AND Source == "192.168.0.77" (отображает HTTP-трафик от ПК с IP-адресом 192.168.0.77 – в левой части используется информация из структуры TCP, а в правом содержимое поля столбца «Source»)</p> <p>ARP or BROWSER (отображает все кадры, содержащие структуры ARP и BROWSER)</p> <p>!ARP and !ICMP and !IPX (отображает все кадры, кроме содержащих структуры ARP, ICMP и IPX)</p> <p>IPv4.address == 192.168.0.77 AND (HTTP or SMB) (отображает все кадры, в которых в качестве IP-адреса источника или назначения выступает 192.168.0.77 и в которых имеются структуры HTTP или SMB)</p> <p>!(Tcp.port == 3389) and !(Tcp.port == 1494) and !(Tcp.port == 1503)</p>

(отображает все кадры, кроме кадров со структурами Terminal Service и Citrix)

Conversation.ProcessName == "OUTLOOK.EXE"

(отображает все кадры порожденные процессом «OUTLOOK.EXE»)

3.3. Визуальное выделение трафика цветом, сформированным в соответствии с «Color Rules»(цветовые правила).

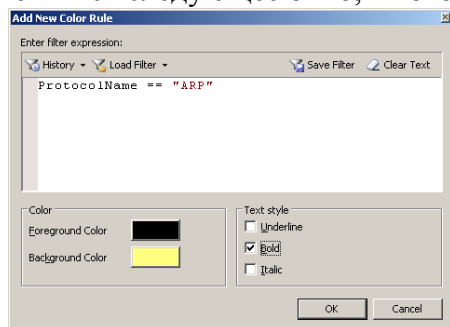
Визуальное выделение трафика цветом является очень удобным средством в обработке захваченного трафика. Воспользоваться «Color Rules»(цветовые правила) можно двумя способами:

- Через контекстное меню, вызываемое нажатием ПКМ на полях столбцов в окне «Frame Summary»(обзор кадров) и в окне «Frame Details»(детали по кадрам);
- Через пиктограмму «Color Rules» на панели инструментов окна «Frame Summary»(обзор кадров).

Формирование «Color Rules»(цветовые правила) через контекстное меню

Данный способ формирования цветовых правил является наиболее удобным. Например, необходимо выделить цветом все кадры, содержащие структуру ARP. Для этого:

- В окне «Frame Summary»(обзор кадров) находим любой кадр, где в поле столбца «Protocol Name» указан «ARP»;
- Установить курсор в поле «Protocol Name»;
- Нажать ПКМ и в контекстном меню выбрать «Add `Protocol Name` as Color Rule»;
- Появится следующее окно, в котором:



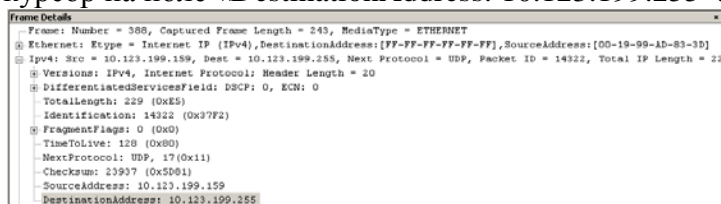
- ✓ В секции «Color» можно установить цвета переднего(Foreground) и заднего(Background) фона для строк таблицы, которые соответствуют заданному выражению фильтрации (filter expression);
- ✓ В секции «Text style» можно установить параметры шрифта текста строк таблицы, которые соответствуют заданному выражению фильтрации (filter expression) – «Underline»(подчеркнутый), «Bold»(жирный), «Italic»(курсив);

Далее нажать кнопку «OK». Результат будет выглядеть следующим образом:

Frame Number	Source	Destination	Protocol Name	Description
1			NetmonFilter	NetmonFilter:Updated Capture Filter: None
2			NetworkInfoEx	NetworkInfoEx:Network info for , Network Adapter Count = 1
3	U359-MIRO...	10.123.199.241	ARP	ARP:Request, 10.123.199.9 asks for 10.123.199.241
4	10.123.199.241	U359-MIRO...	ARP	ARP:Response, 10.123.199.241 at 00-00-AA-B7-6C-E7
5	U359-MIROSH...	10.123.199.241	UDP	UDP:SrcPort = 1132, DstPort = 1124, Length = 41
6	10.123.199.241	U359-MIROSH...	MSRPC	MSRPC:dg Request: Seq=0x7475732D Opnum=0x7363 Frag=0x6275 Serial=0x79 ActId={73790200-0100-2...

Пример 2. Необходимо выделить цветом все широковещательные IP-датаграммы с адресом назначения 10.123.199.255. Для этого:

- В окне «Frame Summary»(обзор кадров) находим любой кадр, где в поле столбца «Destination» указан IP-адрес 10.123.199.255 и устанавливаем на него курсор;
- В окне «Frame Details»(детали по кадрам) раскрываем структуру «IPv4», устанавливаем курсор на поле «DestinationAddress: 10.123.199.255»:



- Нажать ПКМ и в контекстном меню выбрать «Add Selected Value as Color Rule». Появится следующее окно:



Нужно обратить внимание на то, что IP-адрес 10.123.199.255 в выражении фильтрации (filter expression) представлен в Hex виде: 0xa7bc7ff ;

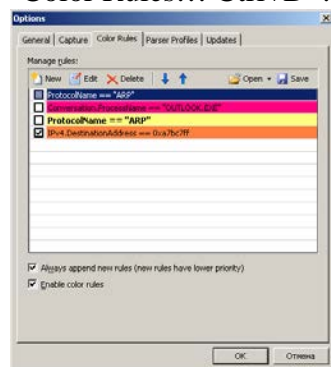
- Далее нажать кнопку «ОК». Результат будет выглядеть следующим образом:

Frame Number	Source	Destination	Protocol Name	Description
384	U562-AKSENOVAYS	10.123.199.138	ARP	ARP:Request, 10.123.199.139 asks for 10.123.199.138
385	10.123.199.161	10.123.199.255	NbtNs	NbtNs:Query Request for WWW.GSTATIC.COM<00> <0x00> Workstation Service
386	U562-AKSENOVAYS	10.123.199.138	ARP	ARP:Request, 10.123.199.139 asks for 10.123.199.138
387	STOL-NIKORYAK	10.123.199.255	BROWSER	BROWSER:Request Announcement, ResponseName = STOL-NIKORYAK
388	U266A-MATOVNIK <00>	10.123.199.255	BROWSER	BROWSER:Local Master Announcement, ServerName = U266A-MATOVNIK
389	U266A-MATOVNIK <00>	10.123.199.255	IPv4	IPv4:Src = 10.123.199.159, Dest = 10.123.199.255, Next Protocol = 0xf1, Packet ID = 14322, Total I
390	10.123.199.161	10.123.199.255	NbtNs	NbtNs:Query Request for WWW.GSTATIC.COM<00> <0x00> Workstation Service
391	INET-PC	10.123.199.255	BROWSER	BROWSER:Host Announcement, ServerName = INET-PC
392	10.123.199.3	10.123.199.46	ARP	ARP:Request, 10.123.199.3 asks for 10.123.199.46

Внимание: Пример №2 приведен для демонстрации использования цветовых правил в окне «Frame Details»(детали по кадрам). Быстрее такой фильтр можно было сделать через окно «Frame Summary»(обзор кадров).

Формирование «Color Rules»(цветовые правила) через пиктограмму «Color Rules» на панели инструментов окна «Frame Summary»(обзор кадров)

При нажатии пиктограммы «Color Rules» на панели инструментов окна «Frame Summary»(обзор кадров) возникает следующее окно, которое можно также вызвать через меню MNM «Frames»-«Color Rules... Ctrl+D»:



В данном окне цветовые правила можно создавать(New), редактировать(Edit), удалять>Delete), сохранять в файле (Save), загружать из ранее сохраненного файла (Open).

Для того чтобы цветовые правила работали, необходимо установить «галку» на «Enable color rules» и хотя бы на одном созданном правиле, после чего нажать кнопку «ОК».

Для создания нового правила из данного окна нужно нажать пиктограмму «New» и в открывшемся окне «Add New Color Rule» ввести выражение фильтрации(filter expression).

Данный способ создания цветовых правил является довольно трудоемким по сравнению со способом формирования цветовых правил через контекстное меню, однако, данный способ позволяет формировать гибкие условия фильтрации трафика. **Внимание:** При создании цветовых правил действуют те же самые выражения и приемы(подсказки при нажатии символа «.»), что и при составлении правил фильтрации в окне «Display Filter», описанных в п.3.2.2. Т.е. одинаково будут работать следующие четыре вида формата фильтров:

- **IPv4** или **ProtocolName == "IPv4"**
- **Protocol.IPv4**
- **Ethernet.IPv4**
- **FRAME.Ethernet.IPv4**

Все форматы приведенных фильтров выделяют одни и те же кадры со структурами «IPv4».

3.4. Замена MAC- и IP-адресов осмысленными псевдонимами - «Aliases»(псевдоним).

Использование «Aliases»(псевдонимы) позволяют улучшить восприятие IP- и MAC-адресов сетевых интерфейсов при анализе сетевого трафика путем замены соответствующего адреса на семантически понятный аналог, например, в столбцах «Source»(источник) и

«Destination»(назначение) таблицы окна «Frame Summary»(обзор кадров) удобнее будет, если вместо «10.123.199.9» будет указано «Мой IP_10.123.199.9».

Внимание: Профили анализатора (Parser Profiles) «Default», «Faster Parsing» и «Windows» в столбцах «Source»(источник) и «Destination»(назначение) таблицы окна «Frame Summary»(обзор кадров), назначают псевдоним IP-адресу локального сетевого интерфейса, соответствующего NetBIOS имени ПК.

Воспользоваться «Aliases» – назначить псевдонимы можно двумя способами:

- Через контекстное меню, вызываемое нажатием ПКМ на полях столбцов «Source»(источник) и «Destination»(назначение) таблицы в окне «Frame Summary»(обзор кадров);
- Через пиктограмму «Aliases»(псевдонимы) на панели инструментов окна «Frame Summary»(обзор кадров).

Формирование «Aliases»(псевдонимы) через контекстное меню

В окне «Frame Summary»(обзор кадров) ЛКМ устанавливаем курсор на поле в столбцах «Source»(источник) или «Destination»(назначение), нажимаем ПКМ и в контекстном меню выбираем «Create Alias for `xxx` Address». Возникает следующее окно:

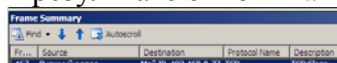
В поле «Address:» автоматически подставляется выбранный в таблице адрес.

В поле «Name:» указывается текст, который будет отображаться в выбранном в таблице поле вместо адреса.

В поле «Comment:» вводится комментарий, поясняющий назначение псевдонима.

Поля «Address:» и «Name:» помечены знаком «*», что означает, что данные поля обязательны для заполнения.

В результате окно «Frame Summary»(обзор кадров) будет иметь следующий вид:



Внимание: При использовании профилей анализатора (Parser Profiles) «Default», «Faster Parsing» и «Windows» назначить псевдоним адресам сетевых интерфейсов текущего ПК таким образом не удастся. В этом случае необходимо воспользоваться пиктограммой «Aliases» на панели инструментов окна «Frame Summary»(обзор кадров).

Формирование псевдонима через пиктограмму «Aliases» на панели инструментов окна «Frame Summary»(обзор кадров)

При нажатии ЛКМ пиктограммы «Aliases»(псевдоним) на панели инструментов окна «Frame Summary»(обзор кадров) возникает следующее меню:



Пункт «Apply» отмечен «галочкой», что означает, что режим использования псевдонимов используется.

Нажатие ЛКМ на пункте «Manage Aliases» вызывает следующее окно:

В данном окне псевдонимы можно создавать(New), редактировать(Edit), удалять(Delete), сохранять в файле (Save), загружать из ранее сохраненного файла (Open), а также устанавливать по умолчанию (Set As Default).

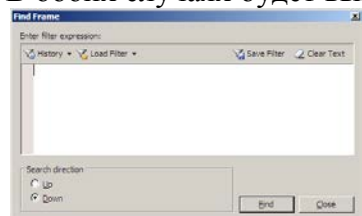
Пиктограмма «Apply»(применить) выглядит нажатой, что означает, что режим использования псевдонимов используется.

3.5. Поиск данных в захваченном трафике в соответствии с заданным условием.

Наряду с фильтрацией трафика функция поиска является наиболее важной при анализе захваченного трафика. Вызов функции поиска можно совершить двумя способами:

- Через главное меню MNM: «Frames»-«Find»-«Find... Ctrl+F»;
- В окне «Frame Summary»(обзор кадров) на панели инструментов нажать ЛКМ на пиктограмме «Find».

В обоих случаях будет выведено следующее окно «Find Frame»(поиск кадров):



Окно «Find Frame» представлено:

- Заголовком;
- Окном редактора выражения фильтрации, состоящем из области ввода и четырех пиктограмм: «History»(история ввода), «Load Filter»(загрузить фильтр), «Save Filter»(сохранить фильтр), «Clear Text»(очистить текст);
- Панелью «Search direction»(направление поиска), позволяющая осуществлять поиск вверх(Up) или вниз(Down) от строки, на которой установлен фокус(курсор). Управлять поиском можно следующими клавишами: «F3» - «Find Next»(найти следующее совпадение) и «Shift+F3» - «Find Previous»(найти предыдущее совпадение);
- Кнопок управления поиском: «Find»(поиск) и «Close»(закреть окно поиска).

Внимание: Необходимо обратить на строку подсказки сверху окна редактора - «Enter filter expression:»(введите выражение фильтра), говорящая о том, что для поиска информации можно использовать те же самые выражения и приемы(подсказки при нажатии символа «.»), что и при составлении правил фильтрации в окне «Display Filter», описанных в п.3.2.2. Т.е. одинаково будут работать следующие четыре вида формата фильтров(поиск кадров со структурами «IPv4»):

- **IPv4** или **ProtocolName == "IPv4"**
- **Protocol.IPv4**
- **Ethernet.IPv4**
- **FRAME.Ethernet.IPv4**

Внимание: При наложении фильтра поиск будет осуществляться только в соответствующих значению фильтра кадрах – ограничение зоны поиска!