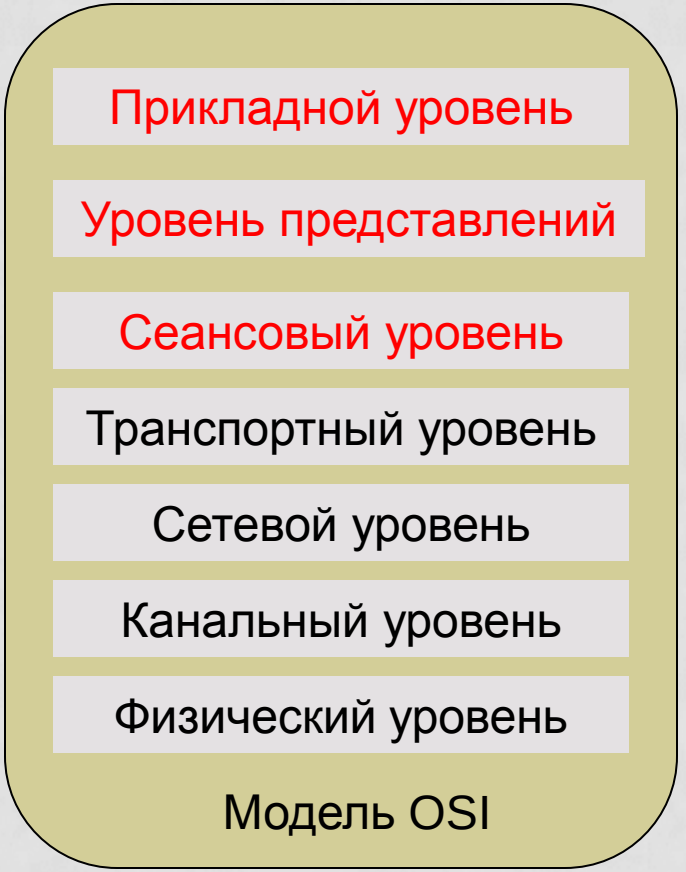
ИНФОРМАЦИОННЫЕ СЕТИ

СЕМИНАР 2.
ПРОТОКОЛЫ ВЕБ-СЛУЖБ
HTTP, FTP

ПРОТОКОЛЫ ПРИКЛАДНОГО УРОВНЯ

- **Прикладной уровень** – набор протоколов, с помощью которых пользователи и приложения получают доступ к разделяемым ресурсам в сети – принтерам, файлам, гипертекстовым страницам.
- Единица данных, с которыми оперирует прикладной уровень, называется **сообщением**.



ПРОТОКОЛ HTTP

- HTTP – протокол прикладного уровня, используемый для соединения и передачи данных между клиентскими компьютерами и HTTP-серверами.
- Запросы клиентов часто передаются от браузера к HTTP-серверам типа Appache или IIS.
- В настоящее время, большинство серверов и браузеров поддерживает версию HTTP/1.1.

ОСНОВНЫЕ ПОНЯТИЯ ПРОТОКОЛА HTTP

- **Сообщение** – основная единица обмена данными между клиентом и сервером. Сообщения обычно посылаются как часть процесса TCP-соединения. В качестве стандартного порта используется 80 порт.
- **Ресурс** – объект или служба, доступные на веб-сервере. Обычно html или xml-страница.
- **Запрос –** сообщение от клиента к серверу, которое запрашивает ресурс. В большинстве случает сообщение представляет GET-запрос.
- **Ответ –** сообщение от сервера к клиенту, которое возвращает информацию, указанную в сообщении запроса.

ОСНОВНЫЕ ПОНЯТИЯ ПРОТОКОЛА HTTP

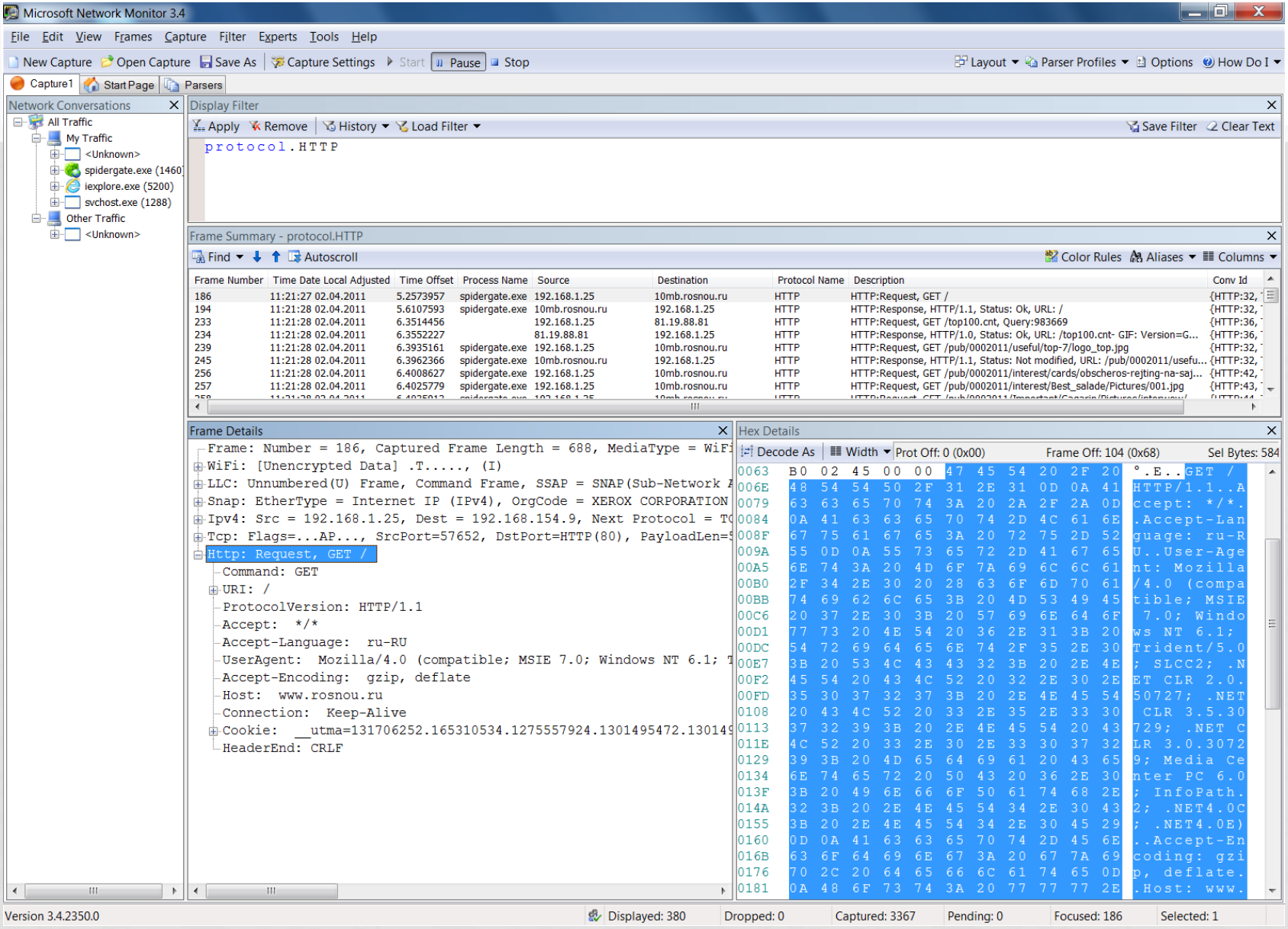
- **Метод –** действие, которое следует выполнять на запрашиваемом ресурсе.
- **Клиент** – любая программа, устанавливающее соединение с http-сервером для выдачи запроса.
- **Сервер** – процесс, принимающий http-запросы по соединениям от клиентских программ и предоставляющий ответные данные.
- **Кэш –** хранилище ответных сообщений прокси-клиента или сервера, используемые для сохранения кэшируемых ресурсов.

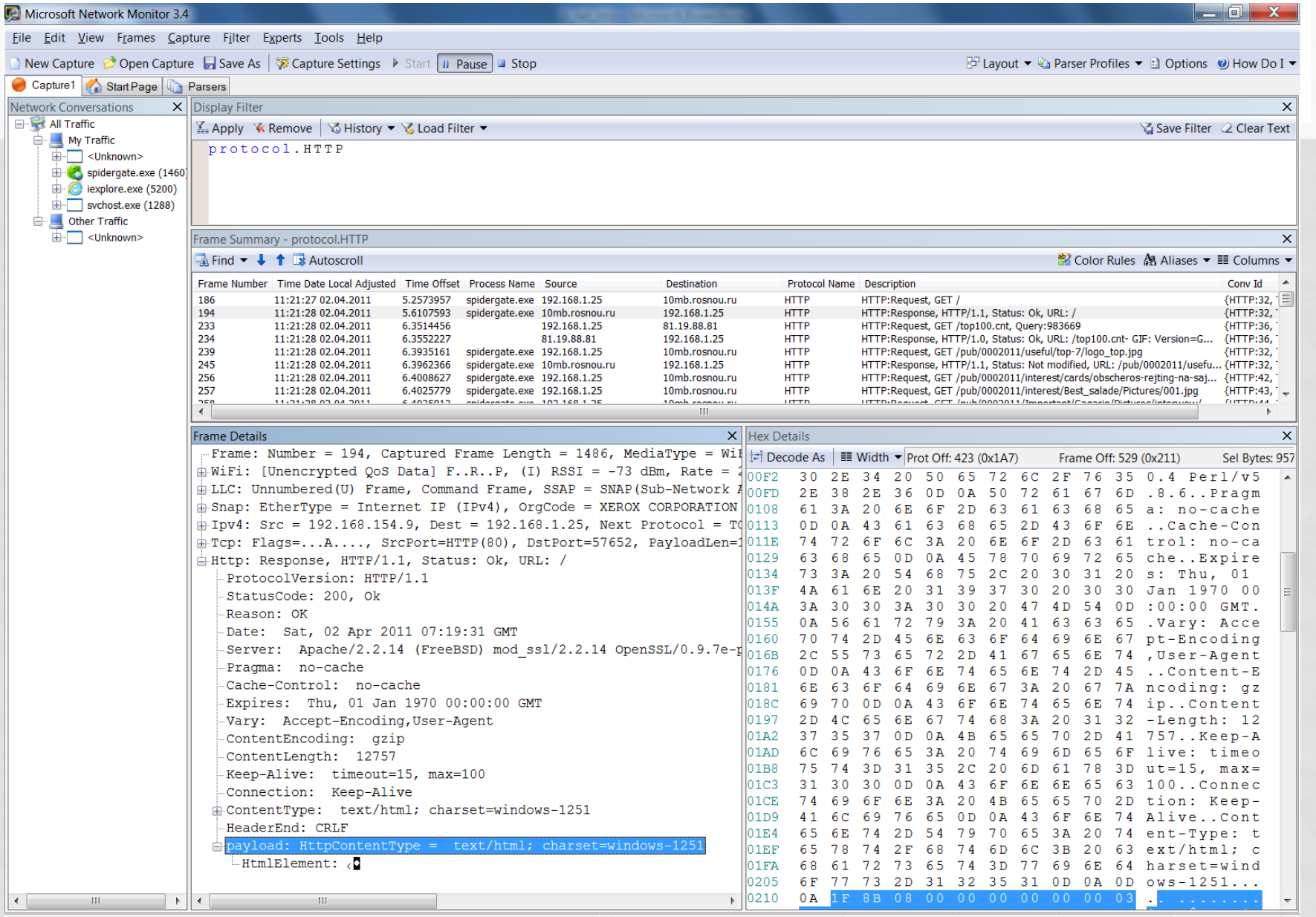
ОСНОВНЫЕ ПОНЯТИЯ ПРОТОКОЛА HTTP

- **Туннель** – посредник транспортного уровня между программами клиента и сервера, который не принимает участия в процессе запроса/ответа, за исключением передачи данных.
- **Шлюз –** http-сервер, получающий запросы от имени другого сервера, часто отображается клиенту в виде запрашиваемого сервера.
- **Прокси** – программа, которая действует как клиент, и как сервер по http-соединению, получая сообщения от программы клиента, переоформляя запросы, как если бы прокси был клиентом, и возвращая ответы исходному заказчику.
- **URL –** унифицированный локатор ресурсов – стандартный способ обозначения ресурсов в интернет. *Протокол://имя_хоста:порт/месторазмещение/имя_ресурса.*
- **Диапазон –** http-сообщения предоставляются в виде байтовых последовательностей (диапазонов). Если клиент запрашивает ресурс у http-сервера, ему необходимо знать общее число байт, поскольку объем ресурса может быть слишком велик для передачи за одну транзакцию.

РАБОТА HTTP

- http – протокол клиент-серверных соединений (запросов/ответов).
- Клиент выдает сообщение запроса, содержащий метод запроса, URI, идентификатор версии протокола и информацию относящуюся к ресурсу.


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
<Unknown>
spidergate.exe (1460)
iexplore.exe (5200)
svchost.exe (1288)
Other Traffic
<Unknown>
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
protocol.HTTP
Frame Summary - protocol.HTTP
Find Autoscroll
Color Rules Aliases Columns
Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source | Destination | Protocol Name | Description | Conv Id
186 | 11:21:27 02.04.2011 | 5.2573957 | spidergate.exe | 192.168.1.25 | 10mb.rosnou.ru | HTTP | HTTP:Request, GET / | {HTTP:32,
194 | 11:21:28 02.04.2011 | 5.6107593 | spidergate.exe | 10mb.rosnou.ru | 192.168.1.25 | HTTP | HTTP:Response, HTTP/1.1, Status: Ok, URL: / | {HTTP:32,
233 | 11:21:28 02.04.2011 | 6.3514456 | | 192.168.1.25 | 81.19.88.81 | HTTP | HTTP:Request, GET /top100.cnt, Query:983669 | {HTTP:36,
234 | 11:21:28 02.04.2011 | 6.3552227 | | 81.19.88.81 | 192.168.1.25 | HTTP | HTTP:Response, HTTP/1.0, Status: Ok, URL: /top100.cnt- GIF: Version=G... | {HTTP:36,
239 | 11:21:28 02.04.2011 | 6.3935161 | spidergate.exe | 192.168.1.25 | 10mb.rosnou.ru | HTTP | HTTP:Request, GET /pub/0002011/useful/top-7/logo_top.jpg | {HTTP:32,
245 | 11:21:28 02.04.2011 | 6.3962366 | spidergate.exe | 10mb.rosnou.ru | 192.168.1.25 | HTTP | HTTP:Response, HTTP/1.1, Status: Not modified, URL: /pub/0002011/usefu... | {HTTP:32,
256 | 11:21:28 02.04.2011 | 6.4008627 | spidergate.exe | 192.168.1.25 | 10mb.rosnou.ru | HTTP | HTTP:Request, GET /pub/0002011/interest/cards/obscheros-rejting-na-saj... | {HTTP:42,
257 | 11:21:28 02.04.2011 | 6.4025779 | spidergate.exe | 192.168.1.25 | 10mb.rosnou.ru | HTTP | HTTP:Request, GET /pub/0002011/interest/Best_salade/Pictures/001.jpg | {HTTP:43,
Frame Details
Frame: Number = 186, Captured Frame Length = 688, MediaType = WiFi
WiFi: [Unencrypted Data] .T....., (I)
LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Network A
Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION
Ipv4: Src = 192.168.1.25, Dest = 192.168.154.9, Next Protocol = TC
Tcp: Flags=...AP..., SrcPort=57652, DstPort=HTTP(80), PayloadLen=5
Http: Request, GET /
Command: GET
URI: /
ProtocolVersion: HTTP/1.1
Accept: */*
Accept-Language: ru-RU
UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; T
Accept-Encoding: gzip, deflate
Host: www.rosnou.ru
Connection: Keep-Alive
Cookie: __utma=131706252.165310534.1275557924.1301495472.130149
HeaderEnd: CRLF
Hex Details
Decode As Width Prot Off: 0 (0x00) Frame Off: 104 (0x68) Sel Bytes: 584
0063 B0 02 45 00 00 47 45 54 20 2F 20 °.E..GET /
006E 48 54 54 50 2F 31 2E 31 0D 0A 41 HTTP/1.1..A
0079 63 63 65 70 74 3A 20 2A 2F 2A 0D ccept: */*.
0084 0A 41 63 63 65 70 74 2D 4C 61 6E .Accept-Lan
008F 67 75 61 67 65 3A 20 72 75 2D 52 guage: ru-R
009A 55 0D 0A 55 73 65 72 2D 41 67 65 U..User-Age
00A5 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 nt: Mozilla
00B0 2F 34 2E 30 20 28 63 6F 6D 70 61 /4.0 (compa
00BB 74 69 62 6C 65 3B 20 4D 53 49 45 tible; MSIE
00C6 20 37 2E 30 3B 20 57 69 6E 64 6F 7.0; Windo
00D1 77 73 20 4E 54 20 36 2E 31 3B 20 ws NT 6.1;
00DC 54 72 69 64 65 6E 74 2F 35 2E 30 Trident/5.0
00E7 3B 20 53 4C 43 43 32 3B 20 2E 4E ; SLCC2; .N
00F2 45 54 20 43 4C 52 20 32 2E 30 2E ET CLR 2.0.
00FD 35 30 37 32 37 3B 20 2E 4E 45 54 50727; .NET
0108 20 43 4C 52 20 33 2E 35 2E 33 30 CLR 3.5.30
0113 37 32 39 3B 20 2E 4E 45 54 20 43 729; .NET C
011E 4C 52 20 33 2E 30 2E 33 30 37 32 LR 3.0.3072
0129 39 3B 20 4D 65 64 69 61 20 43 65 9; Media Ce
0134 6E 74 65 72 20 50 43 20 36 2E 30 nter PC 6.0
013F 3B 20 49 6E 66 6F 50 61 74 68 2E ; InfoPath.
014A 32 3B 20 2E 4E 45 54 34 2E 30 43 2; .NET4.0C
0155 3B 20 2E 4E 45 54 34 2E 30 45 29 ; .NET4.0E)
0160 0D 0A 41 63 63 65 70 74 2D 45 6E ..Accept-En
016B 63 6F 64 69 6E 67 3A 20 67 7A 69 coding: gzi
0176 70 2C 20 64 65 66 6C 61 74 65 0D p, deflate.
0181 0A 48 6F 73 74 3A 20 77 77 77 2E .Host: www.
Version 3.4.2350.0
Displayed: 380
Dropped: 0
Captured: 3367
Pending: 0
Focused: 186
Selected: 1


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
<Unknown>
spidergate.exe (1460)
iexplore.exe (5200)
svchost.exe (1288)
Other Traffic
<Unknown>
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
protocol.HTTP
Frame Summary - protocol.HTTP
Find Autoscroll
Color Rules Aliases Columns
Frame Number Time Date Local Adjusted Time Offset Process Name Source Destination Protocol Name Description Conv Id
186 11:21:27 02.04.2011 5.2573957 spidergate.exe 192.168.1.25 10mb.rosnou.ru HTTP HTTP:Request, GET / {HTTP:32,
194 11:21:28 02.04.2011 5.6107593 spidergate.exe 10mb.rosnou.ru 192.168.1.25 HTTP HTTP:Response, HTTP/1.1, Status: Ok, URL: / {HTTP:32,
233 11:21:28 02.04.2011 6.3514456 192.168.1.25 81.19.88.81 HTTP HTTP:Request, GET /top100.cnt, Query:983669 {HTTP:36,
234 11:21:28 02.04.2011 6.3552227 81.19.88.81 192.168.1.25 HTTP HTTP:Response, HTTP/1.0, Status: Ok, URL: /top100.cnt- GIF: Version=G... {HTTP:36,
239 11:21:28 02.04.2011 6.3935161 spidergate.exe 192.168.1.25 10mb.rosnou.ru HTTP HTTP:Request, GET /pub/0002011/useful/top-7/logo_top.jpg {HTTP:32,
245 11:21:28 02.04.2011 6.3962366 spidergate.exe 10mb.rosnou.ru 192.168.1.25 HTTP HTTP:Response, HTTP/1.1, Status: Not modified, URL: /pub/0002011/usefu... {HTTP:32,
256 11:21:28 02.04.2011 6.4008627 spidergate.exe 192.168.1.25 10mb.rosnou.ru HTTP HTTP:Request, GET /pub/0002011/interest/cards/obscheros-rejting-na-saj... {HTTP:42,
257 11:21:28 02.04.2011 6.4025779 spidergate.exe 192.168.1.25 10mb.rosnou.ru HTTP HTTP:Request, GET /pub/0002011/interest/Best_salade/Pictures/001.jpg {HTTP:43,
Frame Details
Frame: Number = 194, Captured Frame Length = 1486, MediaType = WiF
WiFi: [Unencrypted QoS Data] F..R..P, (I) RSSI = -73 dBm, Rate = 2
LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Network A
Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION
Ipv4: Src = 192.168.154.9, Dest = 192.168.1.25, Next Protocol = TC
Tcp: Flags=...A...., SrcPort=HTTP(80), DstPort=57652, PayloadLen=1
Http: Response, HTTP/1.1, Status: Ok, URL: /
ProtocolVersion: HTTP/1.1
StatusCode: 200, Ok
Reason: OK
Date: Sat, 02 Apr 2011 07:19:31 GMT
Server: Apache/2.2.14 (FreeBSD) mod_ssl/2.2.14 OpenSSL/0.9.7e-p
Pragma: no-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Vary: Accept-Encoding,User-Agent
ContentEncoding: gzip
ContentLength: 12757
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
ContentType: text/html; charset=windows-1251
HeaderEnd: CRLF
payload: HttpContentType = text/html; charset=windows-1251
HtmlElement:
Hex Details
Decode As Width Prot Off: 423 (0x1A7) Frame Off: 529 (0x211) Sel Bytes: 957
00F2 30 2E 34 20 50 65 72 6C 2F 76 35 0.4 Perl/v5
00FD 2E 38 2E 36 0D 0A 50 72 61 67 6D .8.6..Pragm
0108 61 3A 20 6E 6F 2D 63 61 63 68 65 a: no-cache
0113 0D 0A 43 61 63 68 65 2D 43 6F 6E ..Cache-Con
011E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 trol: no-ca
0129 63 68 65 0D 0A 45 78 70 69 72 65 che..Expire
0134 73 3A 20 54 68 75 2C 20 30 31 20 s: Thu, 01
013F 4A 61 6E 20 31 39 37 30 20 30 30 Jan 1970 00
014A 3A 30 30 3A 30 30 20 47 4D 54 0D :00:00 GMT.
0155 0A 56 61 72 79 3A 20 41 63 63 65 .Vary: Acce
0160 70 74 2D 45 6E 63 6F 64 69 6E 67 pt-Encoding
016B 2C 55 73 65 72 2D 41 67 65 6E 74 ,User-Agent
0176 0D 0A 43 6F 6E 74 65 6E 74 2D 45 ..Content-E
0181 6E 63 6F 64 69 6E 67 3A 20 67 7A ncoding: gz
018C 69 70 0D 0A 43 6F 6E 74 65 6E 74 ip..Content
0197 2D 4C 65 6E 67 74 68 3A 20 31 32 -Length: 12
01A2 37 35 37 0D 0A 4B 65 65 70 2D 41 757..Keep-A
01AD 6C 69 76 65 3A 20 74 69 6D 65 6F live: timeo
01B8 75 74 3D 31 35 2C 20 6D 61 78 3D ut=15, max=
01C3 31 30 30 0D 0A 43 6F 6E 6E 65 63 100..Connec
01CE 74 69 6F 6E 3A 20 4B 65 65 70 2D tion: Keep-
01D9 41 6C 69 76 65 0D 0A 43 6F 6E 74 Alive..Cont
01E4 65 6E 74 2D 54 79 70 65 3A 20 74 ent-Type: t
01EF 65 78 74 2F 68 74 6D 6C 3B 20 63 ext/html; c
01FA 68 61 72 73 65 74 3D 77 69 6E 64 harset=wind
0205 6F 77 73 2D 31 32 35 31 0D 0A 0D ows-1251...
0210 0A 1F 8B 08 00 00 00 00 00 00 03 .. ..
Version 3.4.2350.0
Displayed: 380
Dropped: 0
Captured: 3367
Pending: 0
Focused: 194
Selected: 1

HTTP-ЗАПРОС

- http-запрос выдается серверу, агенту туннелирования, прокси, шлюза и каждому участнику транзакции, которые одновременно обрабатывают несколько http-соединений.
  - http-запросы обычно выделяются через **80 TCP**-порт, хотя приложения могут определять другие порты.
- В протоколе http/1.1 по одному соединению обрабатывается несколько транзакций, называемых keep-alive, которые улучшают производительность протокола.
  - http не обеспечивает механизмов для гарантированной доставки сообщений, гарантированность обеспечивается транспортным протоколом TCP.

URI-ИДЕНТИФИКАТОРЫ

- URI – стандарт формата для определения извлекаемого ресурса.
- URL является подмножеством URI.
- URI имеет следующий вид:
  - <алгоритм>://<имя_хоста>:<порт>/<полный_путь>?<запрос>
- Для запросов к веб-узлу обычно в качестве алгоритма указывается http – по имени протокола.

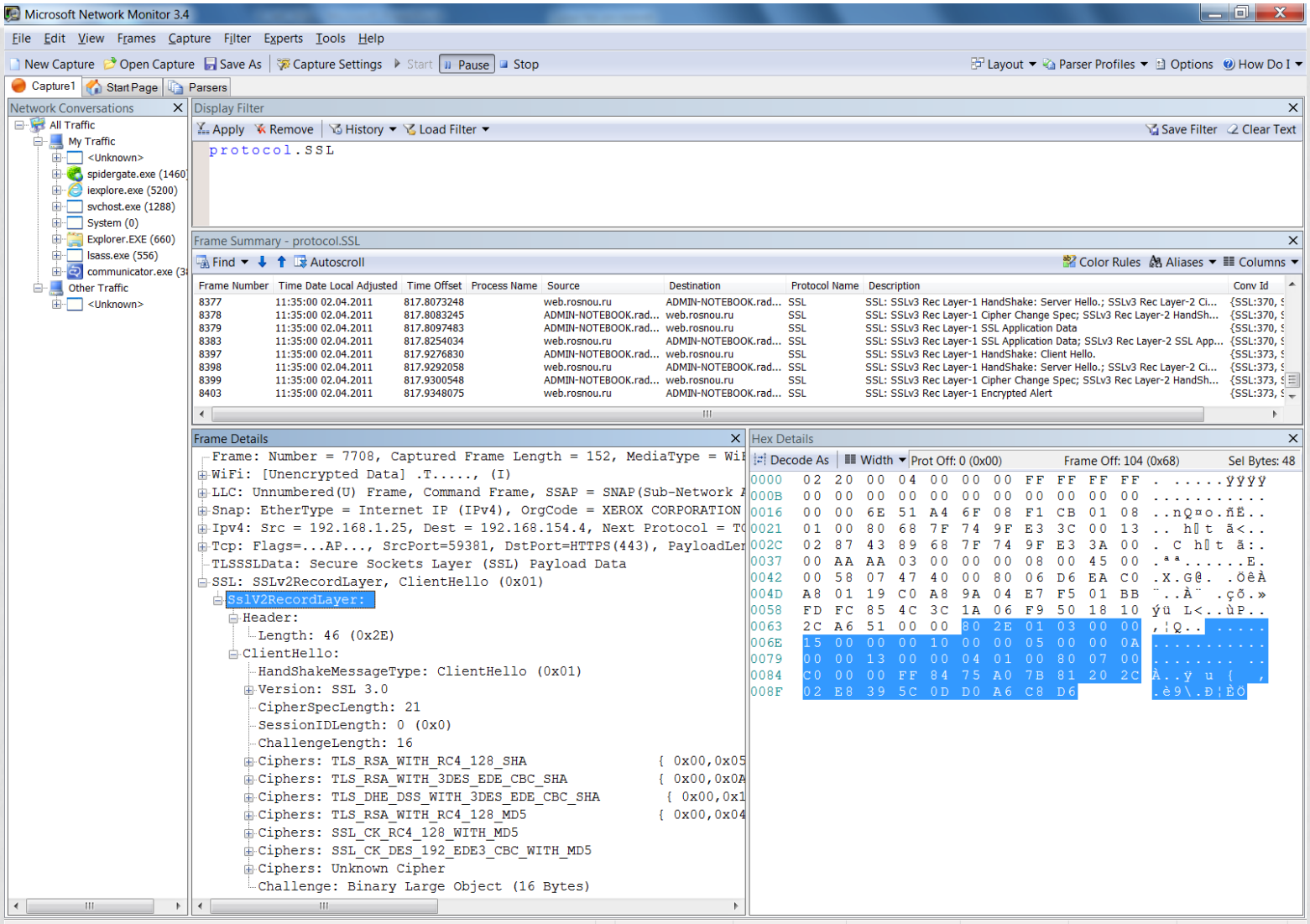
МЕТОДЫ СООБЩЕНИЙ ЗАПРОСА

- Методы – действия, запрашиваемые в сообщении запроса для выполнения на сервере или применения к объекту ресурса. Основные методы:
  - Options – запрашивает информацию, относящуюся к возможностям сервера и к действиям, выполняемым над ресурсом. Результаты не кэшируются.
  - Get – запрашивает у сервера объект, методы бывают условными или частичными.
  - Head – аналогичен get, за исключением того, что сервер возвращает не ресурс а информацию о нем.
  - Post – клиент использует данное сообщение для отправки серверу больших блоков данных.
  - Put – для создания объекта под запрашиваемым URI, используется как простой механизм выгрузки файлов.
  - Delete – запрос на удаление конкретного ресурса на сервере
  - Trace – для запроса тестового возвращаемого сообщения запроса.
  - Connect – используется для прокси, которые могут динамически становится туннелями, как того требует туннелирование на уровне SSL.

КОДИРОВКА HTTP

- HTTP использует кодировку содержимого для определения механизмов модификации данных (например, компрессию), применяемых к объекту.
- Кодировка содержимого регистрируется IANA и включает следующее:
  - GNU's Not UNIX Zip – формат компрессии, определенной в RFC 1952
  - Compress – UNIX-формат компресии-шифрования
  - Defate – сочетание zlib- и deflate-механизмом компрессии и шифрования, определенных в RFC 1950, 1951
  - Identity – стандартный механизм шифрования, указывающий что к объекту шифрование не применено.

SSL-СОЕДИНЕНИЯ



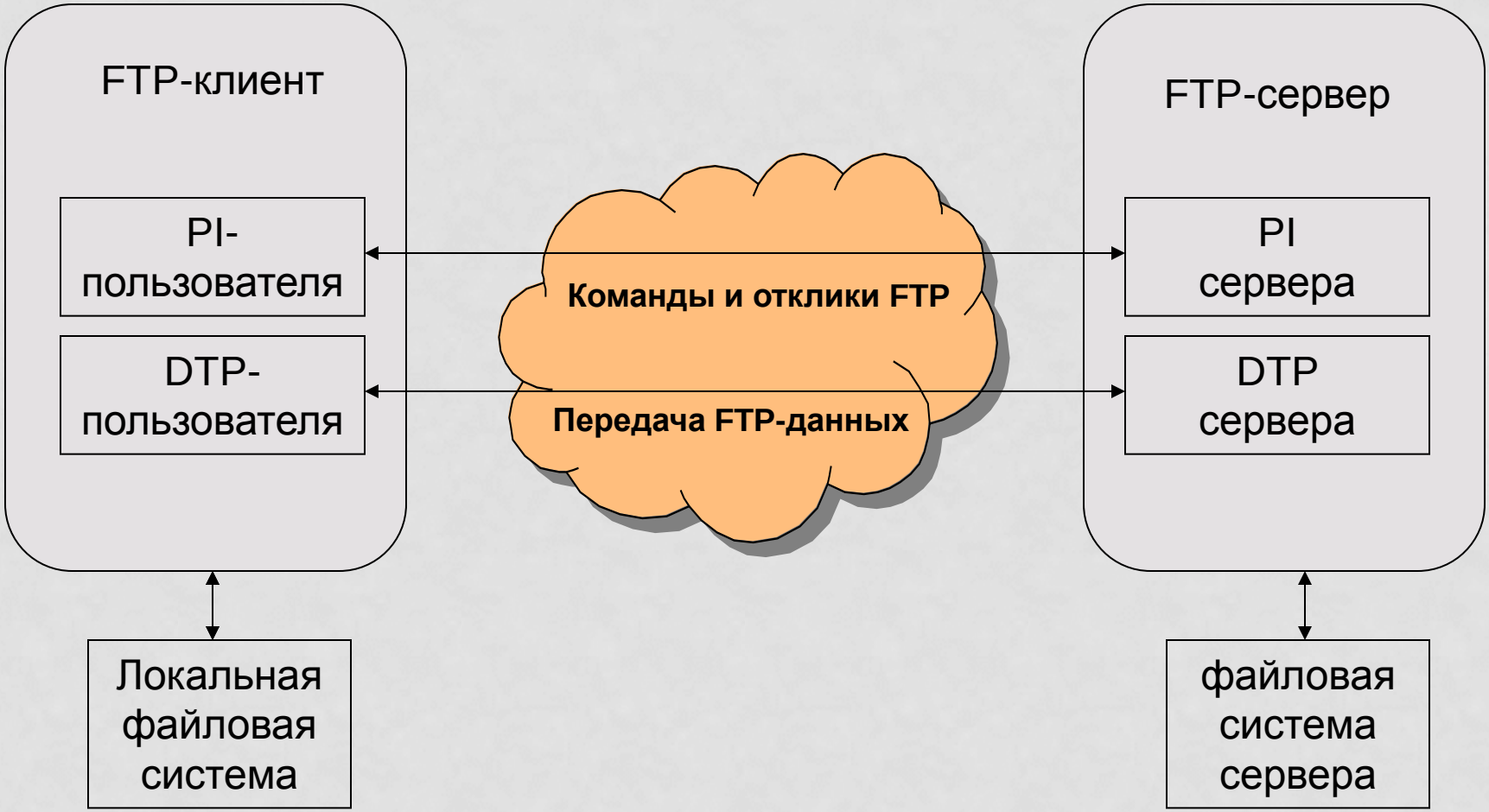
ПРОТОКОЛ FTP

- FTP – один из старейших протоколов прикладного уровня, описан в RFC 959.
- FTP служит основным протоколом для передачи файлов в сети Интернет.
- Протокол обеспечивает общий доступ и передачу файлов между двумя компьютерами, а также применяется для удаленного хранения на других компьютерах.
- Протокол FTP использует возможности протокола TCP транспортного уровня для гарантированности доставки данных.

ТЕРМИНОЛОГИЯ FTP

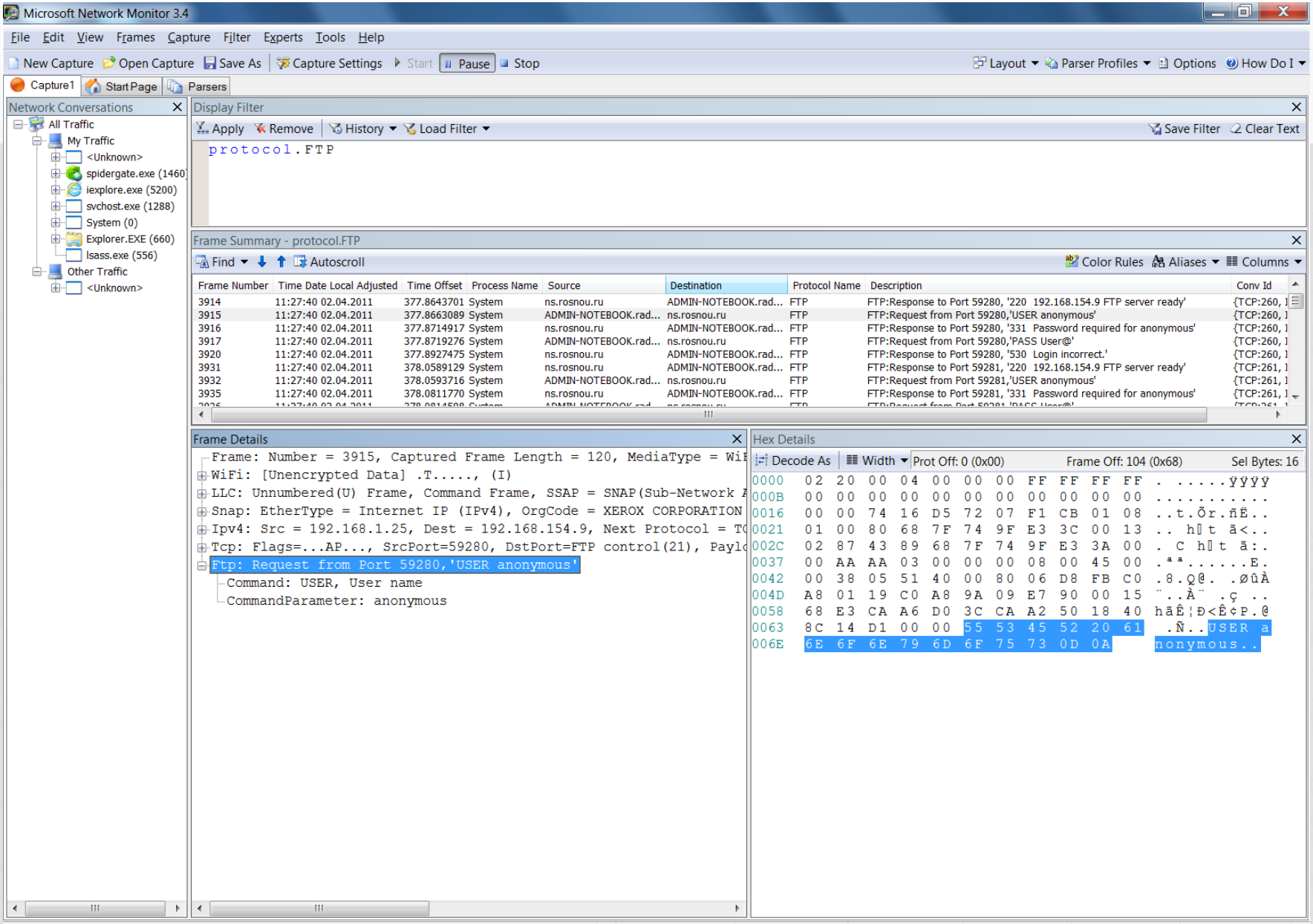
- **Команды FTP –** команды передаются между двумя компьютерами во время сеанса для управления потоком данных
- **Управляющие сообщения** – между клиентом и сервером устанавливается соединение для обмена командами и откликами ftp
- **Отклик** – уведомление, посылаемое сервером через управляющие соединения
- **Соединение для передачи данных** – для передачи данных между компьютерами устанавливается полнодулексное соединение. Это отдельное соединение, отличное от управляющего соединения.
- **Процесс передачи данных (DTP)** – объект, который устанавливает соединение.
- **Интерпретатор протокола (PI)** – на клиентской стороне пользователь инициирует управляющее соединение от клиентского порта к ftp-процессу сервера. На серверной стороне сеанса PI сервера прослушивает соединение PI пользователя и управляет выдачей откликов и DTP сервера.

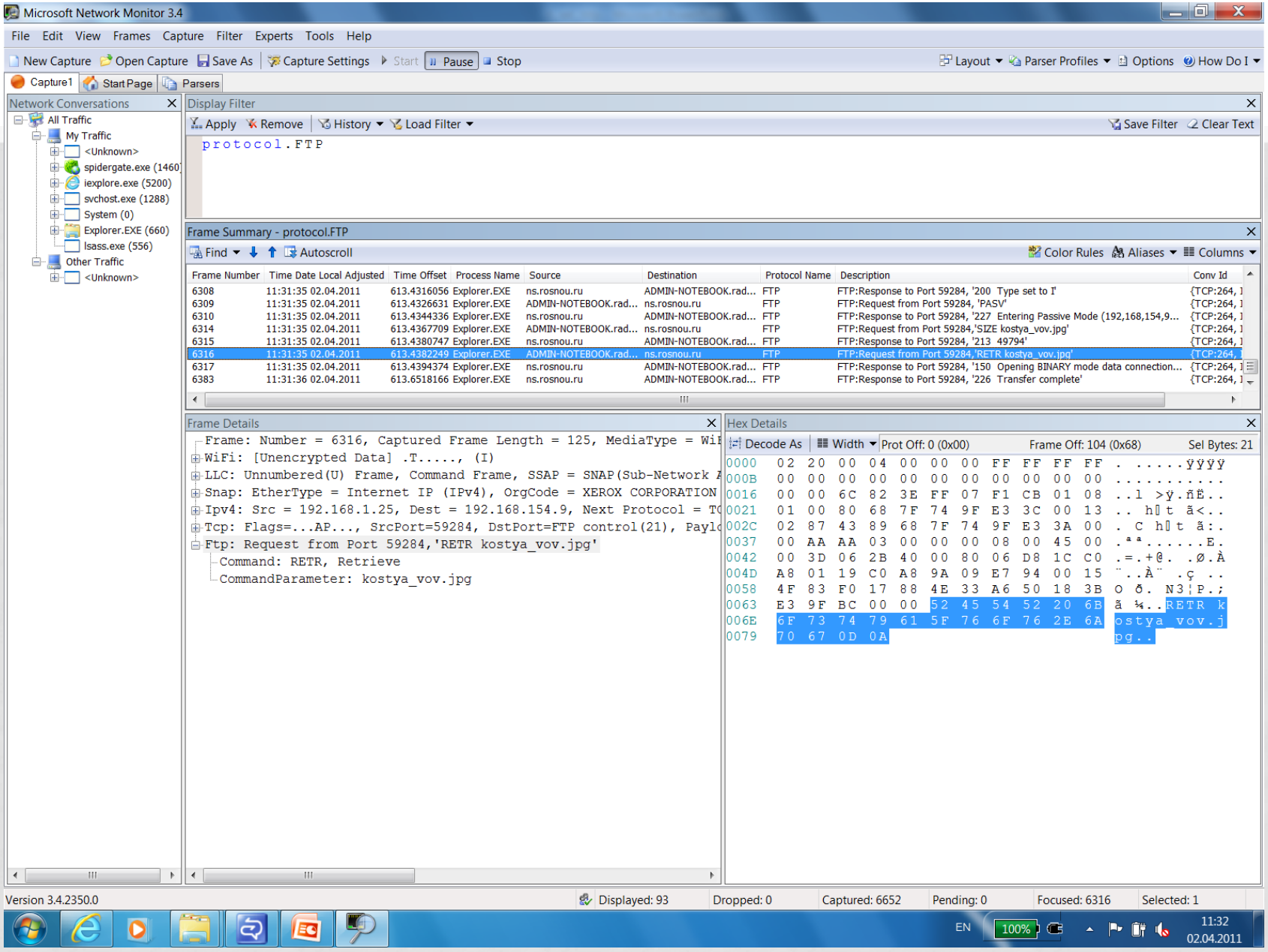
FTP- КОМПОНЕНТЫ



FTP - ДАННЫЕ

- Передача FTP-данных происходит через информационные соединения.
- Управляющие соединения резервируются для приема и передачи ftp-команд управления, а также параметров обмена данными.
- Отправитель и получатель в ftp-сеансе должны согласовать формат передачи данных.
  - Каждый компьютер хранит данные в своих форматах размера логического блока, механизмы должны гарантировать, что данные передаются в согласованном формате.
- Спецификация ftp предусматривает определенные структуры данных и типы представлений, хотя в большинстве случаев используется передача ASCII-данных или данных в двоичном представлении.


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
<Unknown>
spidergate.exe (1460)
iexplore.exe (5200)
svchost.exe (1288)
System (0)
Explorer.EXE (660)
lsass.exe (556)
Other Traffic
<Unknown>
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
protocol.FTP
Frame Summary - protocol.FTP
Find Autoscroll
Color Rules Aliases Columns
Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source | Destination | Protocol Name | Description | Conv Id
3914 | 11:27:40 02.04.2011 | 377.8643701 | System | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59280, '220 192.168.154.9 FTP server ready' | {TCP:260,
3915 | 11:27:40 02.04.2011 | 377.8663089 | System | ADMIN-NOTEBOOK.rad... | ns.rosnou.ru | FTP | FTP:Request from Port 59280,'USER anonymous' | {TCP:260,
3916 | 11:27:40 02.04.2011 | 377.8714917 | System | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59280, '331 Password required for anonymous' | {TCP:260,
3917 | 11:27:40 02.04.2011 | 377.8719276 | System | ADMIN-NOTEBOOK.rad... | ns.rosnou.ru | FTP | FTP:Request from Port 59280,'PASS User@' | {TCP:260,
3920 | 11:27:40 02.04.2011 | 377.8927475 | System | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59280, '530 Login incorrect.' | {TCP:260,
3931 | 11:27:40 02.04.2011 | 378.0589129 | System | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59281, '220 192.168.154.9 FTP server ready' | {TCP:261,
3932 | 11:27:40 02.04.2011 | 378.0593716 | System | ADMIN-NOTEBOOK.rad... | ns.rosnou.ru | FTP | FTP:Request from Port 59281,'USER anonymous' | {TCP:261,
3935 | 11:27:40 02.04.2011 | 378.0811770 | System | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59281, '331 Password required for anonymous' | {TCP:261,
Frame Details
Frame: Number = 3915, Captured Frame Length = 120, MediaType = Wi
WiFi: [Unencrypted Data] .T....., (I)
LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Network
Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION
Ipv4: Src = 192.168.1.25, Dest = 192.168.154.9, Next Protocol = TC
Tcp: Flags=...AP..., SrcPort=59280, DstPort=FTP control(21), Paylc
Ftp: Request from Port 59280,'USER anonymous'
Command: USER, User name
CommandParameter: anonymous
Hex Details
Decode As Width Prot Off: 0 (0x00) Frame Off: 104 (0x68) Sel Bytes: 16
0000 02 20 00 04 00 00 00 FF FF FF FF . .....ÿÿÿÿ
000B 00 00 00 00 00 00 00 00 00 00 00 ....
0016 00 00 74 16 D5 72 07 F1 CB 01 08 ..t.Õr.ñË..
0021 01 00 80 68 7F 74 9F E3 3C 00 13 .. h t ã<..
002C 02 87 43 89 68 7F 74 9F E3 3A 00 . C h t ã:.
0037 00 AA AA 03 00 00 00 08 00 45 00 .ªª.....E.
0042 00 38 05 51 40 00 80 06 D8 FB C0 .8.Q@. .ØûÀ
004D A8 01 19 C0 A8 9A 09 E7 90 00 15 ¨..À¨ .ç ..
0058 68 E3 CA A6 D0 3C CA A2 50 18 40 hãÊ¦Ð<Ê¢P.@
0063 8C 14 D1 00 00 55 53 45 52 20 61 .Ñ..USER a
006E 6E 6F 6E 79 6D 6F 75 73 0D 0A nonymous..
Version 3.4.2350.0
Displayed: 80 Dropped: 0 Captured: 5481 Pending: 0 Focused: 3915 Selected: 1


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
<Unknown>
spidergate.exe (1460)
iexplore.exe (5200)
svchost.exe (1288)
System (0)
Explorer.EXE (660)
lsass.exe (556)
Other Traffic
<Unknown>
Display Filter
Apply Remove History Load Filter Save Filter Clear Text
protocol.FTP
Frame Summary - protocol.FTP
Find Autoscroll Color Rules Aliases Columns
Frame Number | Time Date Local Adjusted | Time Offset | Process Name | Source | Destination | Protocol Name | Description | Conv Id
6308 | 11:31:35 02.04.2011 | 613.4316056 | Explorer.EXE | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59284, '200 Type set to I' | {TCP:264,
6309 | 11:31:35 02.04.2011 | 613.4326631 | Explorer.EXE | ADMIN-NOTEBOOK.rad... | ns.rosnou.ru | FTP | FTP:Request from Port 59284, 'PASV' | {TCP:264,
6310 | 11:31:35 02.04.2011 | 613.4344336 | Explorer.EXE | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59284, '227 Entering Passive Mode (192,168,154,9... | {TCP:264,
6314 | 11:31:35 02.04.2011 | 613.4367709 | Explorer.EXE | ADMIN-NOTEBOOK.rad... | ns.rosnou.ru | FTP | FTP:Request from Port 59284,'SIZE kostya_vov.jpg' | {TCP:264,
6315 | 11:31:35 02.04.2011 | 613.4380747 | Explorer.EXE | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59284, '213 49794' | {TCP:264,
6316 | 11:31:35 02.04.2011 | 613.4382249 | Explorer.EXE | ADMIN-NOTEBOOK.rad... | ns.rosnou.ru | FTP | FTP:Request from Port 59284,'RETR kostya_vov.jpg' | {TCP:264,
6317 | 11:31:35 02.04.2011 | 613.4394374 | Explorer.EXE | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59284, '150 Opening BINARY mode data connection... | {TCP:264,
6383 | 11:31:36 02.04.2011 | 613.6518166 | Explorer.EXE | ns.rosnou.ru | ADMIN-NOTEBOOK.rad... | FTP | FTP:Response to Port 59284, '226 Transfer complete' | {TCP:264,
Frame Details
Frame: Number = 6316, Captured Frame Length = 125, MediaType = Wi
WiFi: [Unencrypted Data] .T....., (I)
LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Network A
Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPORATION
Ipv4: Src = 192.168.1.25, Dest = 192.168.154.9, Next Protocol = TC
Tcp: Flags=...AP..., SrcPort=59284, DstPort=FTP control(21), Paylo
Ftp: Request from Port 59284,'RETR kostya_vov.jpg'
Command: RETR, Retrieve
CommandParameter: kostya_vov.jpg
Hex Details
Decode As Width Prot Off: 0 (0x00) Frame Off: 104 (0x68) Sel Bytes: 21
0000 02 20 00 04 00 00 00 FF FF FF FF . .....ÿÿÿÿ
000B 00 00 00 00 00 00 00 00 00 00 00 ....
0016 00 00 6C 82 3E FF 07 F1 CB 01 08 ..l >ÿ.ñË..
0021 01 00 80 68 7F 74 9F E3 3C 00 13 .. h t ã<..
002C 02 87 43 89 68 7F 74 9F E3 3A 00 . C h t ã:.
0037 00 AA AA 03 00 00 00 08 00 45 00 .ªª.....E.
0042 00 3D 06 2B 40 00 80 06 D8 1C C0 .=.+@. .Ø.À
004D A8 01 19 C0 A8 9A 09 E7 94 00 15 ¨..À¨ .ç ..
0058 4F 83 F0 17 88 4E 33 A6 50 18 3B O ð. N3¦P.;
0063 E3 9F BC 00 00 52 45 54 52 20 6B ã ¼..RETR k
006E 6F 73 74 79 61 5F 76 6F 76 2E 6A ostya_vov.j
0079 70 67 0D 0A pg..
Version 3.4.2350.0
Displayed: 93 Dropped: 0 Captured: 6652 Pending: 0 Focused: 6316 Selected: 1
EN 100% 11:32 02.04.2011

КОМАНДЫ FTP

- FTP-соединение между клиентом и сервером представляется в виде передаваемых последовательностей команд, которые выполняются для клиента, и откликов от сервера, посылаемых в ответ на эти команды.
- PI пользователя выдает команды через управляющее соединение.
- Команды FTP могут передавать данные, идентифицирующие и проверяющие личность пользователя (USER, ACCT, PASS), команды навигации в файловой системе удаленного хоста (CDUP, XCUP, CWD), команды управления передачами файла и самой передачей (PORT, TYPE, MODE, GET, PUT, RETR, STOR).

FTP-ОТКЛИКИ

- Подобно другим службам FTP-серверы выдают коды отклика в ответе команды клиента. Эти расширенные коды отклика передаются в виде трехзначного числа, со значениями первой и второй цифры, указывающими тип отклика:
  - Первая цифра – указывает основной тип ответа;
  - Вторая цифра используется для предоставления конкретных значений ответа;
  - Третья цифра – используется для расширения кода отклика и различается разными реализациями.

КОДЫ ОТКЛИКОВ

- Первая цифра кода отклика:
  - 1## - positive preliminary reply – запрашиваемое действие выполняется;
  - 2## - positive completion replay – запрошенное действие завершено;
  - 3## - positive intermediate replay – запрошенное действие принято и обработка продолжится, когда будет получена дополнительная информация;
  - 4## - transient negative completion replay – произошла временная ошибка, остановившая обработку команды, пользователь должен повторить запрос;
  - 5## - permanent negative completion replay – произошла ошибка, остановившая обработку команды.

КОДЫ FTP-ОТКЛИКОВ

- Вторая цифра кода отклика:
  - #0# - syntax – ошибка синтаксиса команды;
  - #1# - information – ответ на информационный запрос (справка)
  - #2# - connections – относится к управляющим соединениям
  - #3# - authentication and accounting – отклики на регистрацию пользователей или процедуры учета;
  - #4# - unspecified – не определено;
  - #5# - file system – состояние файловой системы.