Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и кибербезопасности

Высшая школа компьютерных технологий и информационных систем

**Отчет по лабораторной работе №8**

**по курсу «Технологии компьютерный сетей»**

«Wireshark: SSL»

**Работу выполнил студент группы №5130901/10203:**

Алексеев Лев Сергеевич

Подпись:

**Работу принял преподаватель:**

Богач Наталья Владимировна

Подпись:

Санкт-Петербург

2024

**Wireshark: SSL**

В этой лабораторной работе мы исследуем уровень защищенных сокетов (протокол SSL), уделив особое внимание SSL-записям, передаваемым по TCP-соединению. Для этого мы проанализируем трассировку SSL-записей, которыми обмениваются ваш компьютер и сервер Интернет-магазина. Мы рассмотрим различные типы записей SSL, а также поля в SSL-сообщениях.

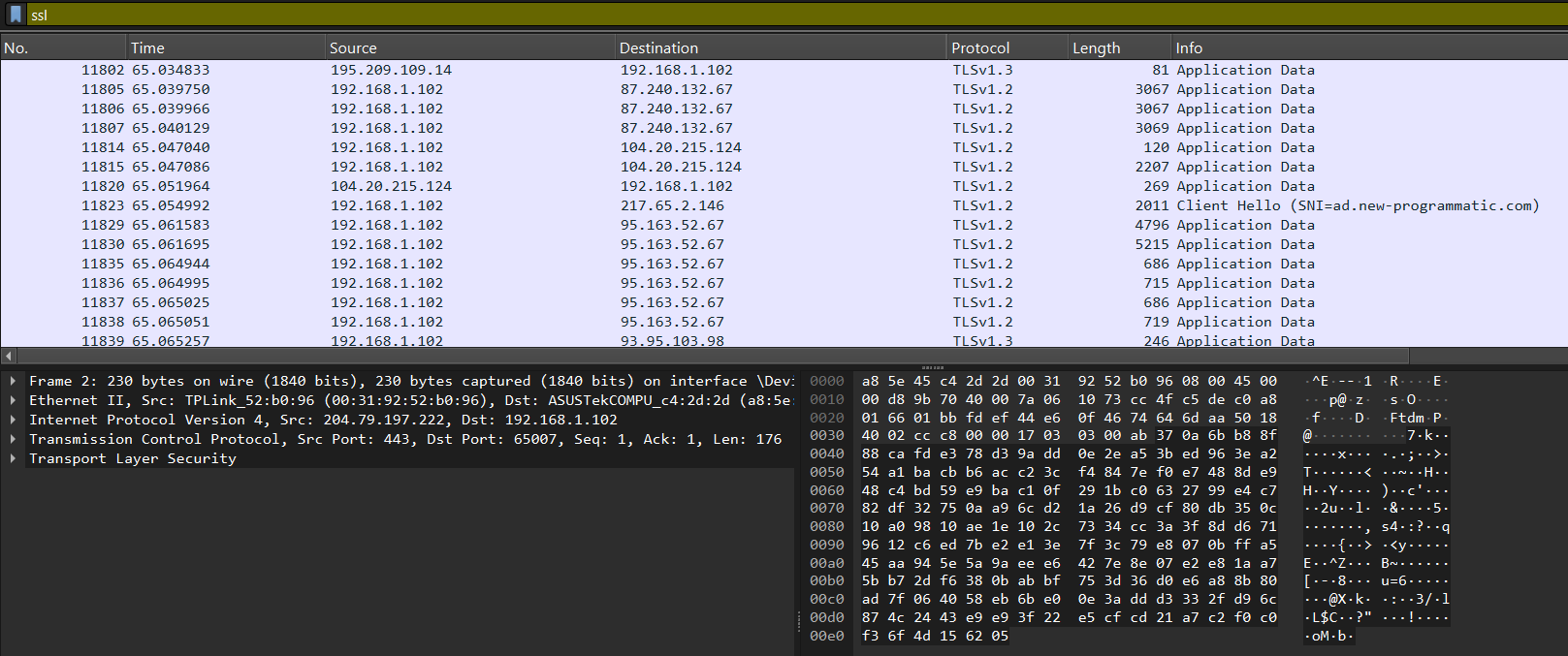
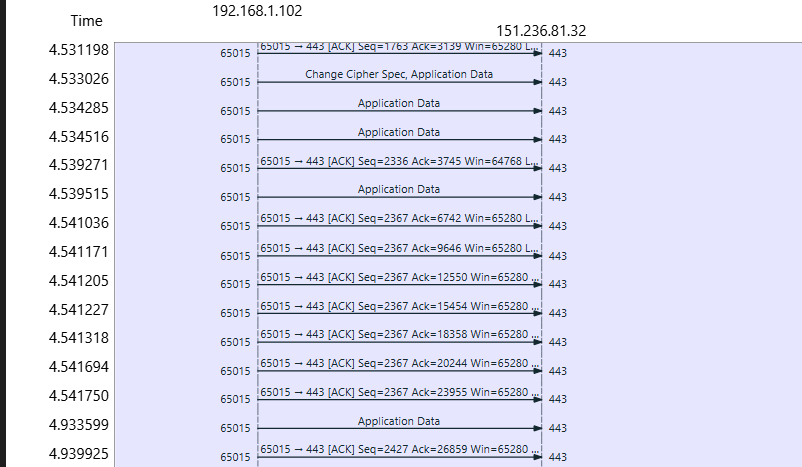


Рис. 1. Перехваченная трасса SSL.

1. Для каждого из первых 8 Ethernet-кадров укажите его источник (клиент или сервер), определите количество SSL-записей, включаемых в кадр, а также перечислите типы SSL-записей, находящихся в этом кадре. Начертите временную диаграмму, отражающую связь между клиентом и сервером, каждой SSL-записи должна соответствовать одна стрелка.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ кадра в Wireshark** | **№ кадра** | **Исходный адрес** | **Конечный адрес** | **Количество SSL-записей** | **Список SSL-записе** |
| 1240 | 1 | 192.168.1.102 | 151.236.81.32 | 1 | Клиентское приветствие (Hello) |
| 1244 | 2 | 151.236.81.32 | 192.168.1.102 | 1 | Серверное приветствие (Hello) |
| 1245 | 3 | 151.236.81.32 | 192.168.1.102 | 1 | Данные приложений |
| 1246 | 4 | 151.236.81.32 | 192.168.1.102 | 2 | Данные приложений |
| 1249 | 5 | 192.168.1.102 | 151.236.81.32 | 2 | Изменение параметров шифра, данные приложений |
| 1250 | 6 | 192.168.1.102 | 151.236.81.32 | 1 | Данные приложений |
| 1251 | 7 | 192.168.1.102 | 151.236.81.32 | 1 | Данные приложений |
| 1252 | 8 | 130.193.52.39 | 192.168.1.102 | 1 | Данные приложений |



1. Все SSL-записи начинаются с одних и тех же трех полей (значения в которых могут отличаться). Одно из этих полей – content type (тип содержимого) – имеет длину 1 байт. Перечислите все три поля и их длины.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ кадра** | **Тип записи SSL** | **Тип содержимого** | **Версия** | **Длина** |
| 1 | Клиентское приветствие | Рукопожатие (22) | SSL 3.0 (0x0300) | 76 |
| 2 | Серверное приветствие | Рукопожатие (22) | SSL 3.0 (0x0300) | 74 |
| 3 | Сертификат, Серверное приветствие завершено | Рукопожатие (22)  Рукопожатие (22) | SSL 3.0 (0x0300)  SSL 3.0 (0x0300) | 2691  4 |
| 4 | Клиентская запись об обмене ключами, Изменение параметров шифра, Сообщение о зашифрованном рукопожатии | Рукопожатие (22)  Изменение параметров шифра (20)  Рукопожатие (22) | SSL 3.0 (0x0300)  SSL 3.0 (0x0300)  SSL 3.0 (0x0300) | 132  1  56 |
| 5 | Изменение параметров шифра, Сообщение о зашифрованном рукопожатии | Изменение параметров шифра (20)  Рукопожатие (22) | SSL 3.0 (0x0300)  SSL 3.0 (0x0300) | 1  56 |
| 6 | Данные приложений | Данные приложений (23) | SSL 3.0 (0x0300) | 747 |
| 7 | Данные приложений | Данные приложений (23) | SSL 3.0 (0x0300) | 213 |
| 8 | Данные приложений | Данные приложений (23) | SSL 3.0 (0x0300) | 8208 |

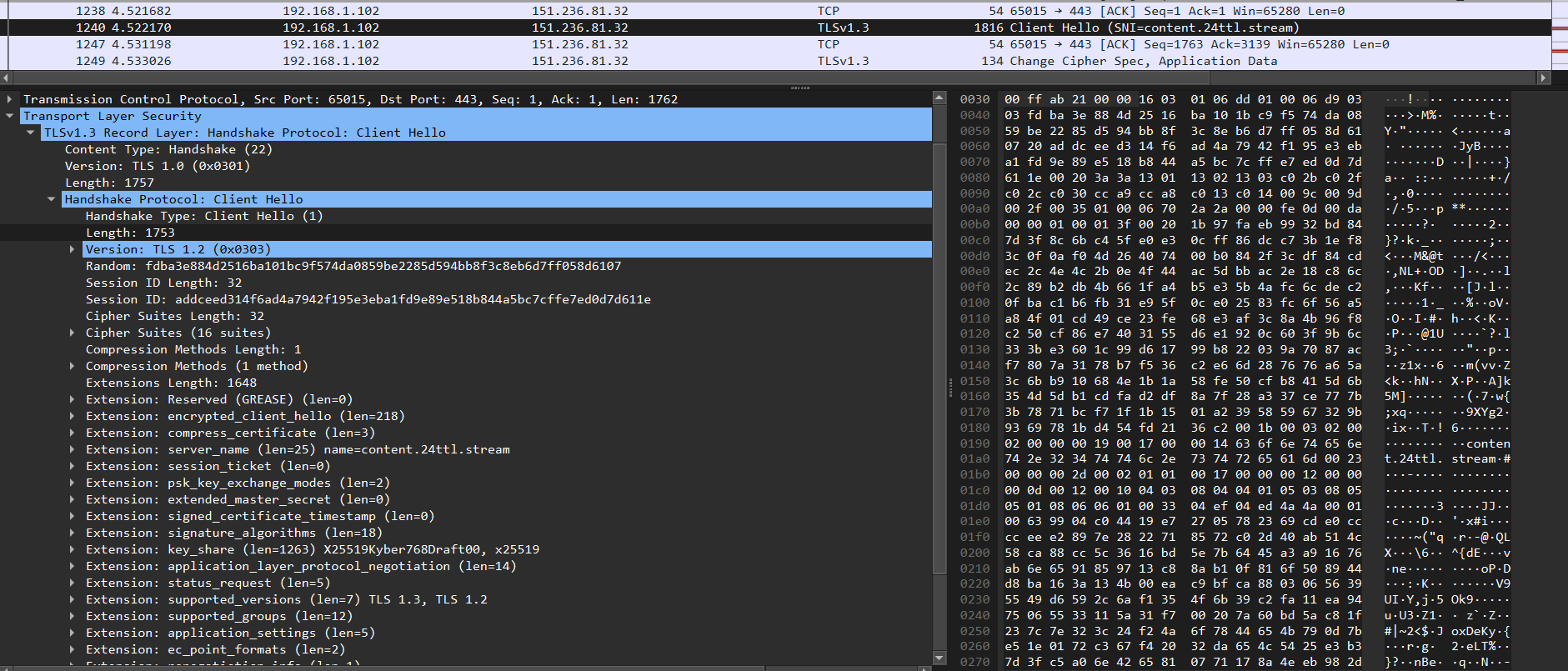


Рис. 2. Расширенная запись с клиентским приветствием.

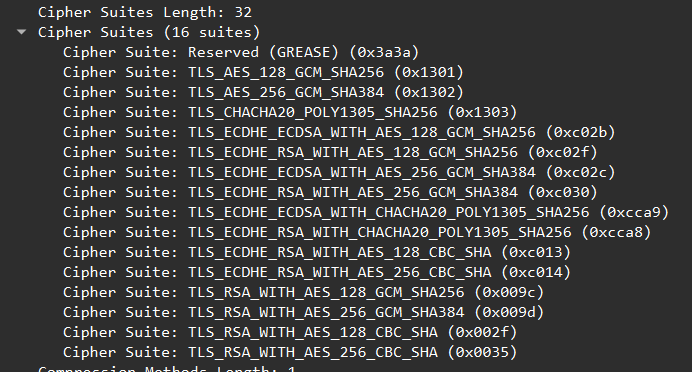
1. Раскройте запись ClientHello. (Если в вашей трассе присутствует несколько записей ClientHello, раскройте кадр с первой такой записью.) Какое значение типа содержимого в нем записано?

Значение типа содержимого – Рукопожатие (22), так как именно таков тип сообщения

1. Есть ли в записи ClientHello одноразовый номер (также называемый «вызов» (challenge))? При наличии вызова – каково его значение в шестнадцатеричном представлении?

Да, в записи с клиентским сообщением содержится вызов, его значение в шестнадцатеричном представлении равно 0x66df784c048cd60435dc448989469909.

1. Объявляются ли в записи ClientHello те крипто-наборы, которые в ней поддерживаются? Если они поддерживаются, то назовите следующие данные по первому из перечисленных наборов: алгоритм шифрования открытым ключом, алгоритм шифрования симметричными ключами, хеш-алгоритм?

Да, запись с клиентским приветствием объявляет поддерживаемый ею криптографический набор, как показано ниже:  


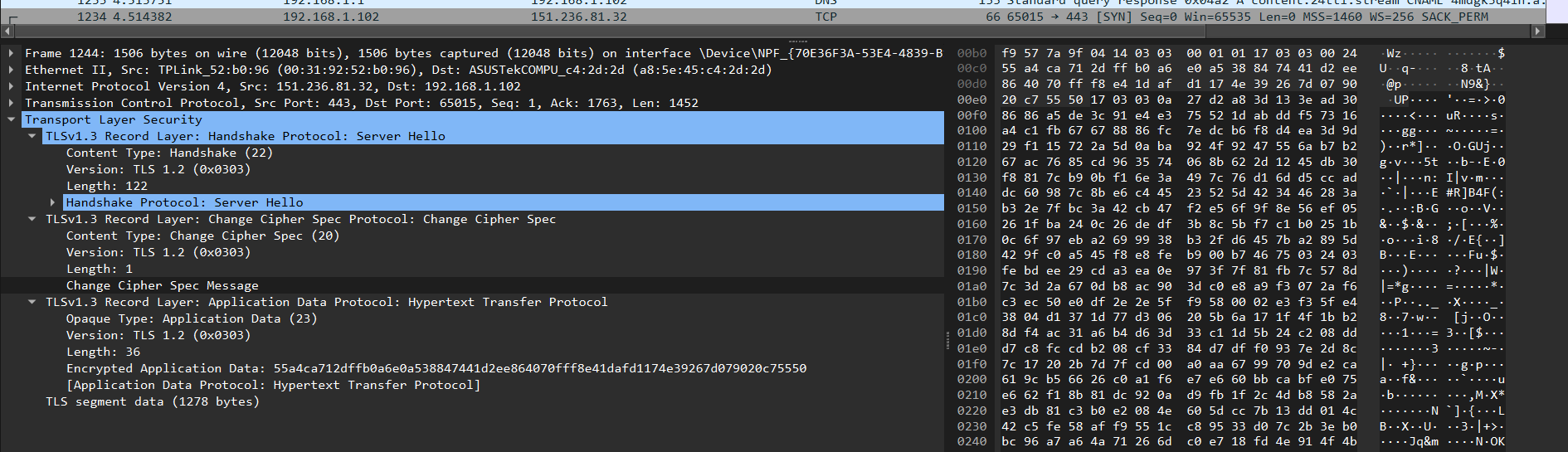


Рис. 3. Расширенная запись с серверным приветствием.

1. Найдите SSL-запись ServerHello. Указан ли в этой записи выбранный шифровальный набор? Какие алгоритмы находятся в этом наборе?

Да, в записи указывается криптографический набор. Здесь выбран набор TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004). Иными словами, здесь применяются алгоритмы RSA (шифрование с открытым ключом), 128-разрядный алгоритм RC4 (строится на основе генератора псевдослучайных битов) и MD5 (алгоритм хеширования).

1. Есть ли в этой записи одноразовый номер? Если так – какова его длина? Каково назначение клиентских и серверных одноразовых номеров в протоколе SSL?

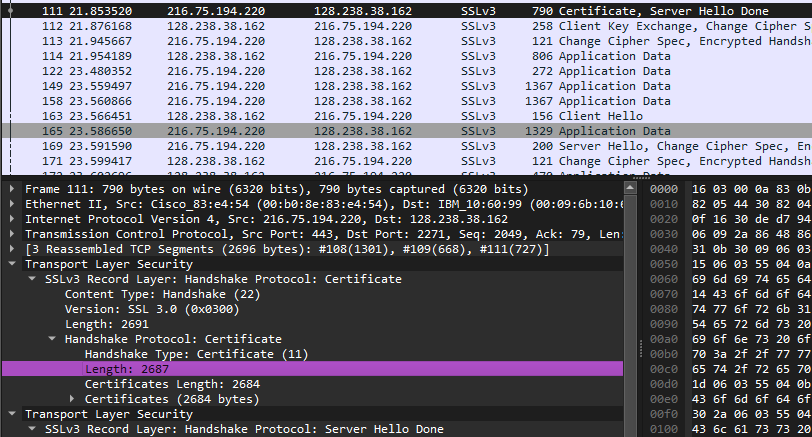
Да, в этой записи содержится одноразовый номер, также называемый Random.bytes, его длина составляет 28 байт (как показано выше). Назначение клиентских и серверных одноразовых номеров при работе по SSL – не позволить злоумышленнику повторно воспроизвести или переупорядочить записи.

1. Есть ли в этой записи сеансовый ID? Каково назначение сеансового ID?

Да, в этой записи содержится сеансовый идентификатор (ID), его длина составляет 32 байт. Идентификатор нужен для возобновления сеанса; такие операции возобновления позволяют существенно снизить количество длительных серверных рукопожатий, применяемых для создания новых сеансовых идентификаторов. В записи о клиентском приветствии ненулевой сеансовый идентификатор означает, что клиент должен возобновить установленный ранее сеанс. Нулевой сеансовый идентификатор означает, что клиенту требуется установить с сервером новый сеанс.

1. Есть ли в этой записи сертификат, либо сертификат включается в отдельную запись. Умещается ли сертификат в одном Ethernet-кадре?

Нет, в этой записи сертификата нет, он находится в следующей записи. Длина сертификата составляет 2684 байта – то есть, он не входит в один кадр Ethernet.



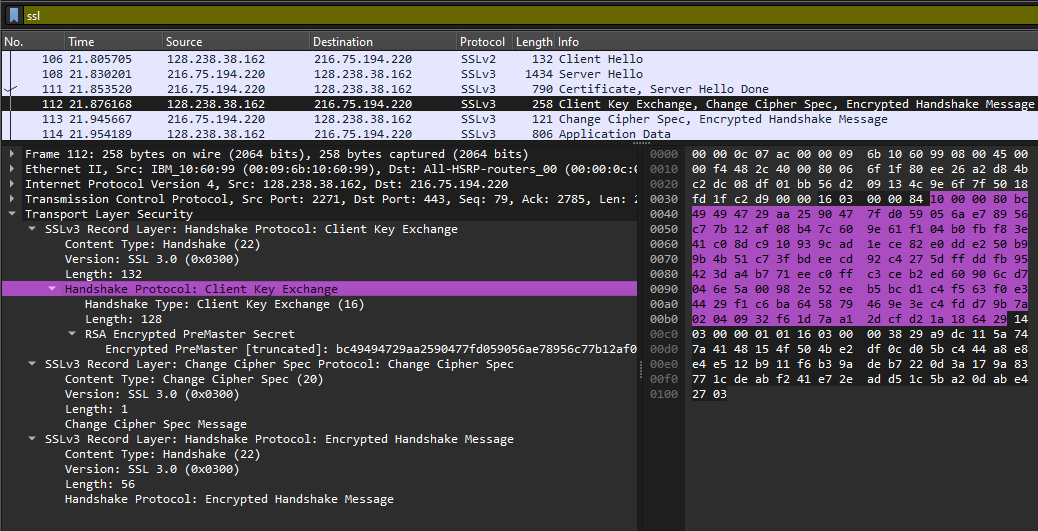


Рис. 4. Записи об обмене ключами, изменении параметров шифра и о сообщении о зашифрованном рукопожати

1. Найдите клиентскую запись об обмене ключами. Содержится ли в этой записи предварительный главный секретный ключ? Для чего он используется? Шифруется ли секретный ключ? Если да – то как? Какова длина зашифрованного секретного ключа?

Да, в этой записи содержится предварительный главный секретный ключ (рис. 4). Этот зашифрованный предварительный главный секретный ключ дешифруется на стороне сервера и используется для формирования главного секретного ключа. Далее главный секретный ключ применяется для создания «блока ключей», который затем разрезается на клиентский MAC-ключ, серверный MAC-ключ, клиентский ключ шифрования, серверный ключ шифрования, клиентский вектор инициализации и серверный вектор инициализации. Секретный ключ расшифровывается с применением серверного открытого ключа. Длина зашифрованного секретного ключа составляет 130 байт.

1. Каково назначение записи об изменении параметров шифра? Сколько байт занимает эта запись в исследуемой вами трассе?

Назначение записи об изменении параметров шифра – указать изменение в алгоритмах шифрования и аутентификации, а также обновить криптографический набор, который будет использоваться при данном соединении. В моей трассе длина этой записи составляет всего 1 байт.

1. Что именно шифруется в зашифрованной записи рукопожатия? Как?

В этой записи с сообщением о зашифрованном рукопожатии указан отправитель, а также зашифрован отправитель всех предыдущих сообщений о рукопожатии, исключая данное. Эта информация объединяется путем сцепления (конкатенации) и хешируется при помощи двух алгоритмов хеширования, MD5 и SHA. Содержимое данной записи получено путем конкатенации этих двух хеш-значений. Сообщение о зашифрованном рукопожатии удостоверяет, что операции обмена ключами и аутентификации прошли успешно.

1. Отсылает ли и сервер клиенту запись об изменении параметров шифра и зашифрованную запись рукопожатия? Чем эти записи у сервера отличаются от аналогичных записей, отсылаемых клиентом?

Да, сервер также отсылает свои записи об изменении параметров шифра и о зашифрованном рукопожатии. Вся разница заключается в том, какой узел является отправителем этой информации – в данном случае это сервер, в предыдущем же сообщении отправителем был клиент.

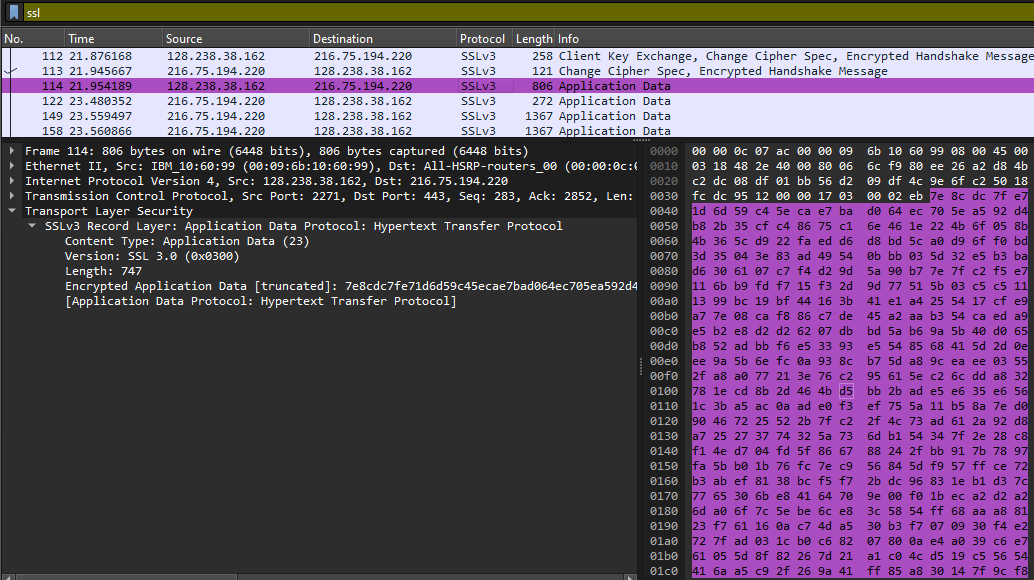
****

Рис. 5. Расширенная запись о данных приложений

1. Как зашифровываются данные приложений? Присутствует ли в записях с данными приложений код MAC? Различает ли Wireshark зашифрованные данные приложений и MAC?

Данные приложений зашифровываются при помощи алгоритмов, входящих в выбранный криптографический набор; в моем случае это алгоритмы RSA (шифрование с открытым ключом), 128-разрядный алгоритм RC4 (строится на основе генератора псевдослучайных битов) и MD5 (алгоритм хеширования). Да, в записях с данными приложений содержатся коды MAC, но Wireshark не делает различий между зашифрованными данными приложений и MAC.