МОНИТОРИНГ СКРЫТОЙ СЕТЕВОЙ АКТИВНОСТИ

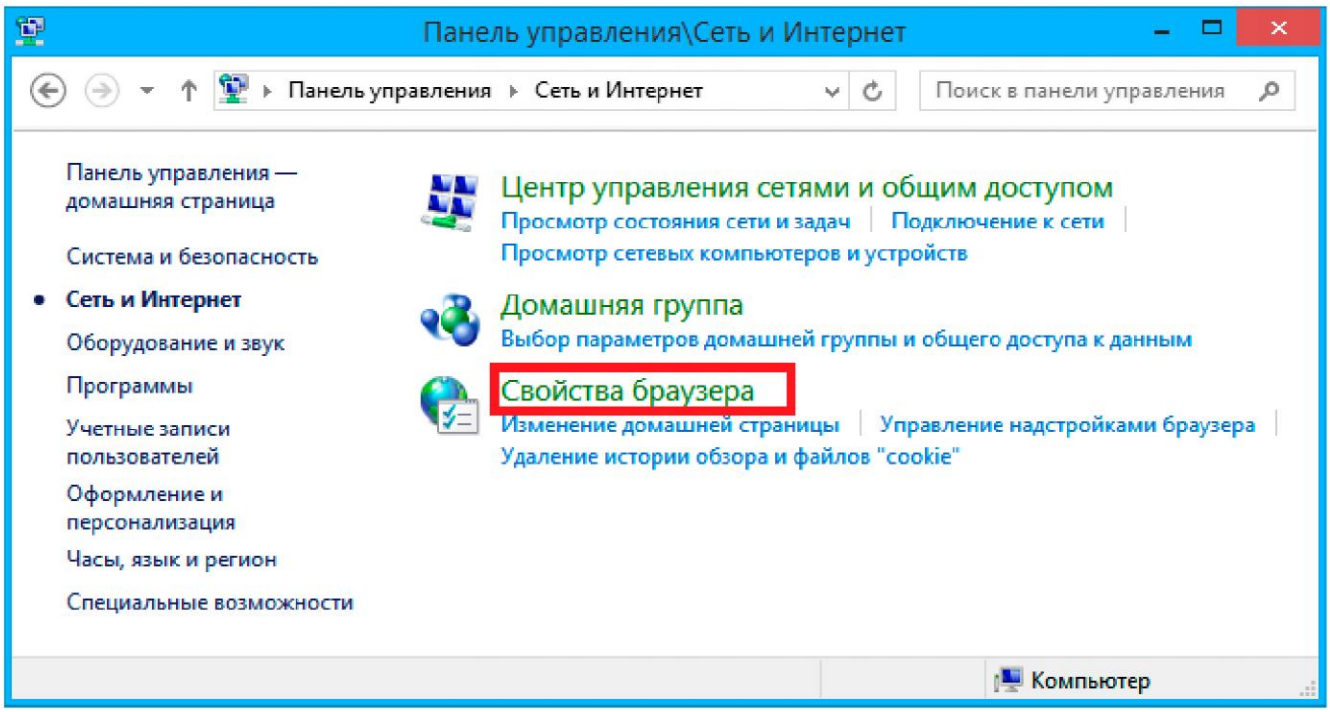
В период с 2012 г. в политике компании Microsoft – разработчика и поставщика наиболее распространённой операционной системы для настольных компьютеров и рабочих станций (под управлением ОС Windows работает 84,31% всех ПК, данные StatCounter на 1 июля 2017 г.) – в отношении конечных пользователей произошли серьёзные изменения: компоненты операционных системы начали проявлять нежелательную сетевую активность, выражающуюся в приёме и передаче значительных объёмов информации на сервера компании Microsoft и её партнёров, в том числе и в незашифрованной форме. В тоже время из состава операционных систем были исключены встроенные средства по отслеживанию и контролю такой активности. Более того, скрытую сетевую активность – «слив» личной информации – имеют и многие сторонние приложения.

Для предотвращения утечки личной информации – пар логин-пароль для сайтов, данных реальных фамилии и имени пользователя, данных кредитных карт в платёжных системах и так далее, вплоть до файлов пользователя – необходима установка и настройка сетевых экранов (другие названия «брандмауэр» и «файрволл»). В составе операционных систем Microsoft, начиная с Windows XP SP 2 (2004 г.), присутствует встроенный брандмауэр. Однако, являясь продуктом заинтересованной стороны, данное средство не препятствует передаче личной информации пользователя другими компонентами операционной системы Windows. Данный факт подкрепляется исследованиями поведения брандмауэра Windows многих компаний сферы ИТ-безопасности. Для обычного пользователя из этого вытекает настоятельная рекомендация установки сетевого экрана стороннего разработчика, например, входящего в состав пакетов Kaspersky Internet Security, ESET Endpoint Security или других. Предназначение сетевого экрана – блокирование (в соответствии с заданными правилами) нежелательного сетевого трафика как входящего, так и исходящего с компьютера пользователя. Процедура полностью автоматизирована и не требует вмешательства пользователя.

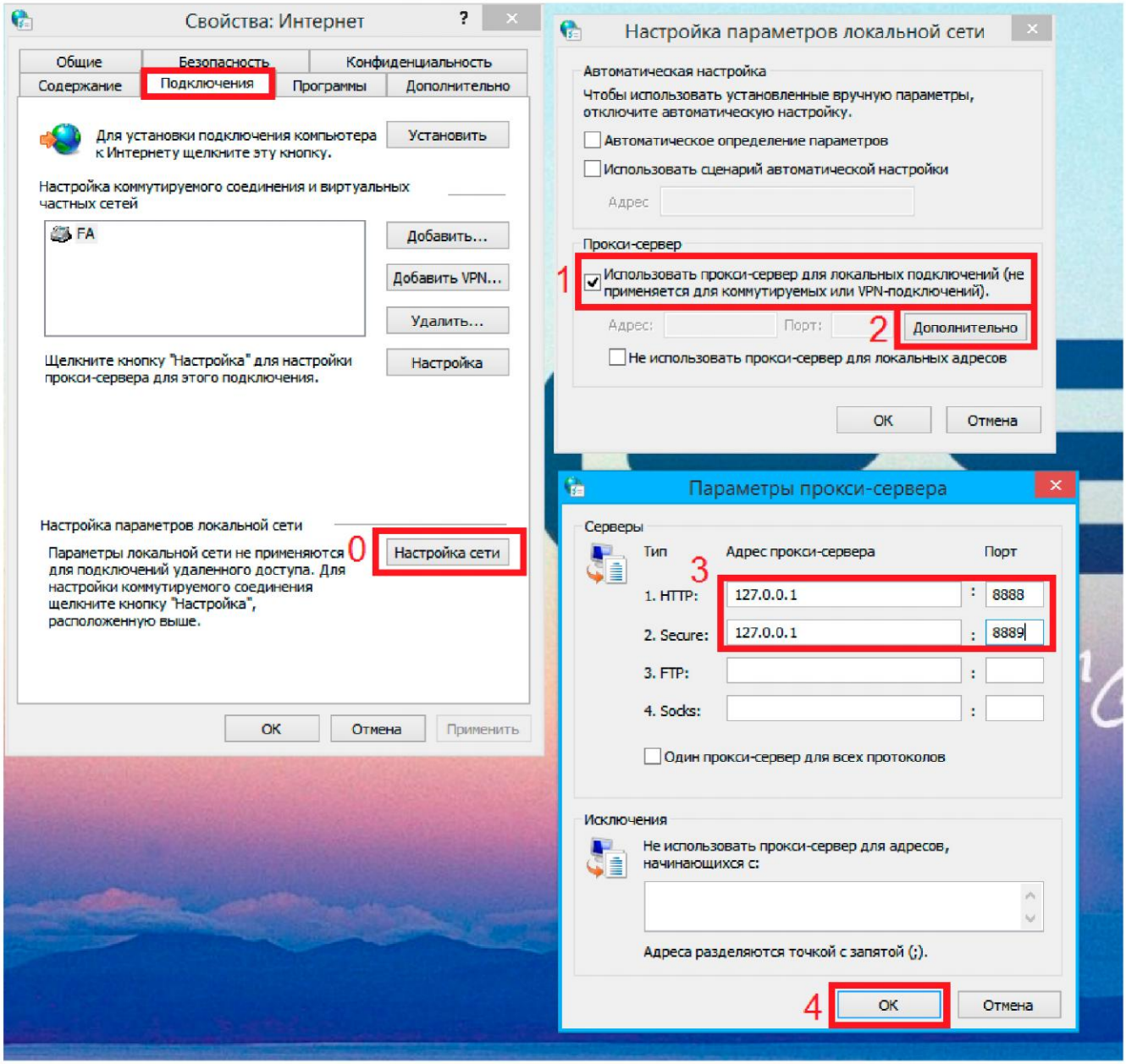
Для отслеживания (мониторинга) всей сетевой активности необходимо использование других программных средств – мониторов WEB-пакетов. Наиболее широко зарекомендовавшим себя программным продуктом для автоматизированного сетевого администрирования является Wireshark, разработки Wireshark Foundation, а наиболее эффективное его использование сопряжено с установкой и функционированием данного продукта на сетевом маршрутизаторе, что не актуально для домашнего использования.

Для индивидуального использования одним из средств мониторинга скрытой сетевой активности является программный продукт Charles WEB Debugging Proxy. Суть работы программы – настройка перенаправления всей информации принимаемой и отправляемой компьютером в интернет на локальный хост (адрес 127.0.0.1, порт 8888), перехват пакетов информации и отображение детальных сведений о каждом из них.

Рассмотрим процесс настройки и работы Charles WEB Debugging Proxy. После установки программы, необходимо настроить подключение к сети в операционной системе. Для этого необходимо открыть «Панель управления», перейти в раздел «Сеть и интернет» и щёлкнуть по ссылке «Свойства браузера».

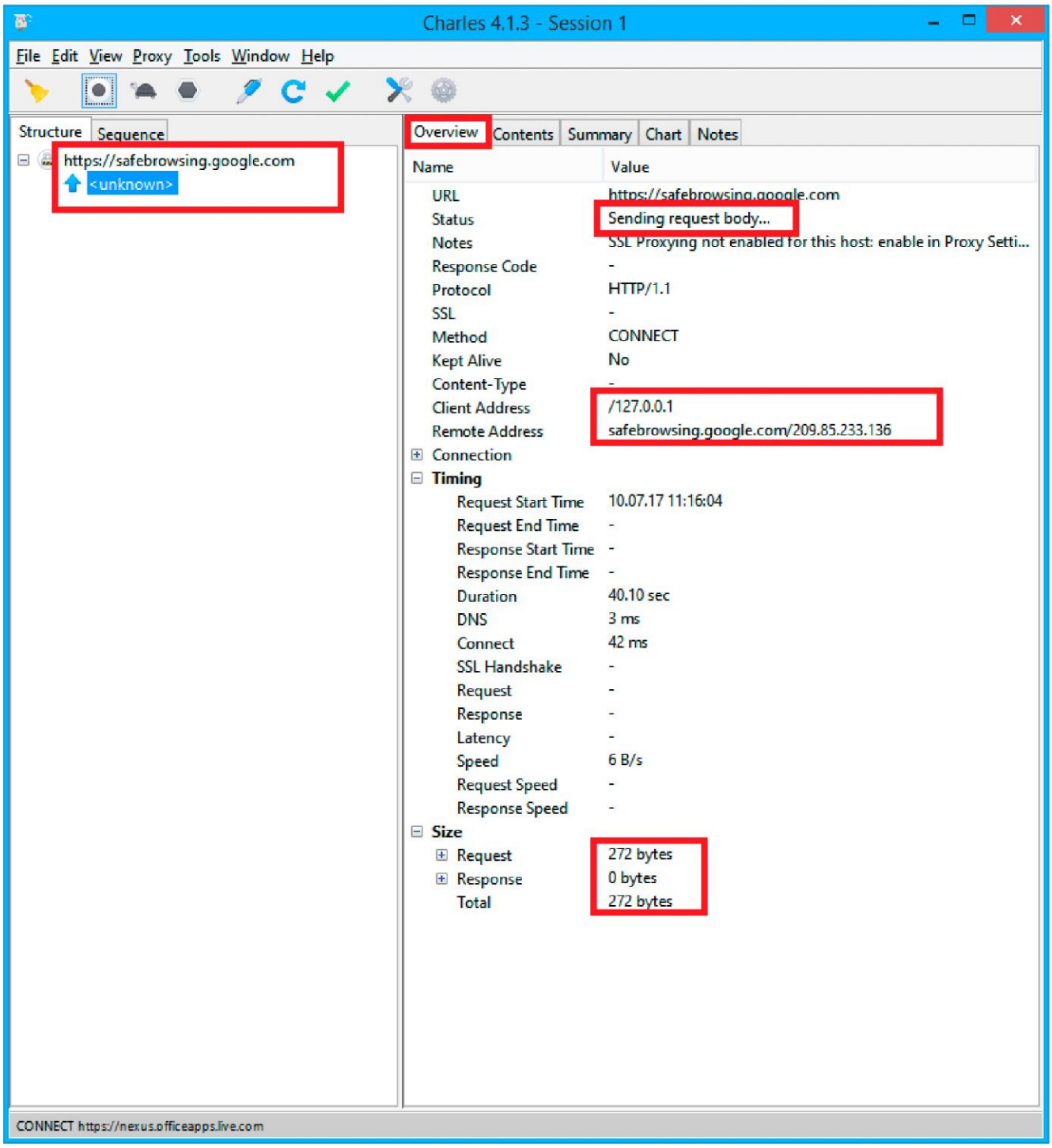


В появившемся окне перейти на вкладку «Подключения» и нажать на кнопку «Настройка сети». Дальнейшая процедура заключается в настройке локального прокси-сервера – той промежуточной точки, в которой Charles WEB Debugging Proxy будет перехватывать пакеты данных и отображать их для анализа. Настройки необходимо установить, как показано на рисунке ниже.



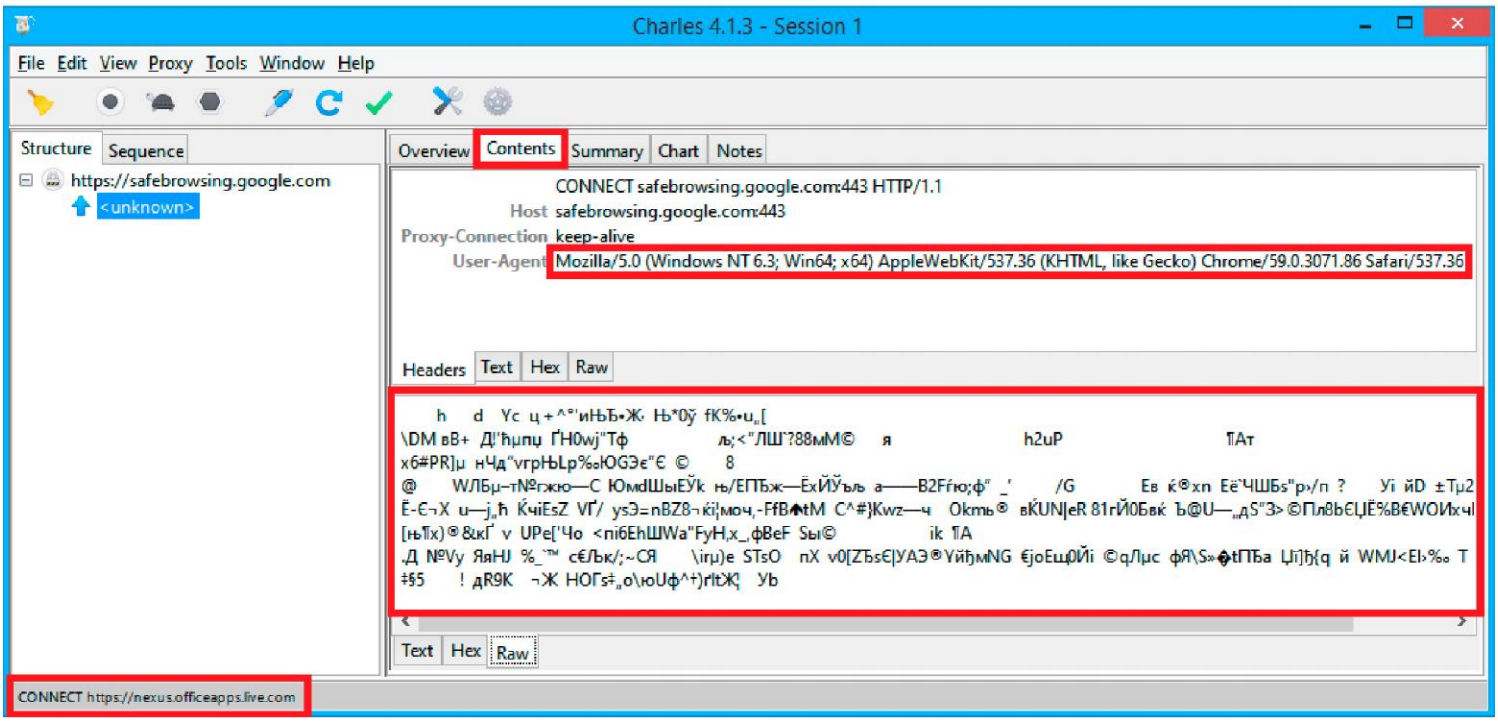
Следует обратить внимание, что на шаге 3, в окне «Параметры прокси-сервера», под Secure подразумевается протокол зашифрованной передачи HTTPS. Данный факт неочевиден, но необходим для дальнейшего понимания функционирования системы.

По завершении настройки запустим программу Charles WEB Debugging Proxy. Стандартный вид окна программы представлен ниже.



Так, на рисунке выделены наиболее значимые для анализа области: на вкладке «Overview» (Обобщённая информация) мы видим, что с адреса клиента (Client Address), т.е. компьютера на котором запущена программа (локального адреса 127.0.0.1) был отправлен запрос на удаленный адрес (Remote Address), т.е. адрес одного из серверов Google (safebrowsing.google.com/209.85.233.136). Общий размер запроса (Total size) составил 272 байта.

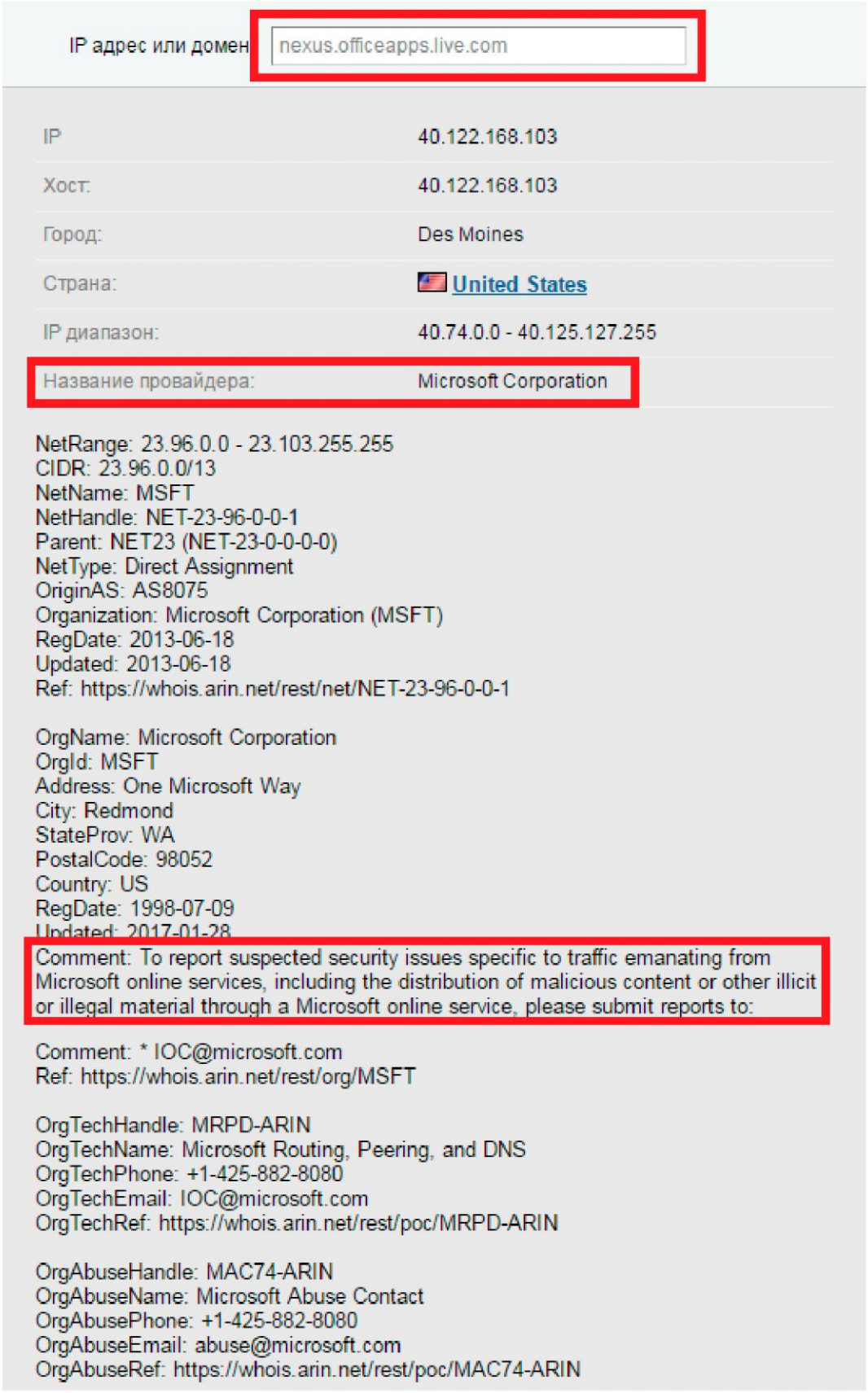
Для того, чтобы просмотреть содержимое отправленного пакета данных перейдём на вкладку «Содержимое» (Contents).



Анализ содержимого окна позволяет сказать, что запрос был выполнен программой Chrome версии 59.0.3071.86 (User-Agent). Содержимое запроса не поддаётся осмысленному прочтению человеком: содержимое было зашифровано, т.к. запрос был выполнен по протоколу HTTPS. В таком случае корректное прочтение содержимого возможно лишь сторонами обмена, создавшими и владеющими закрытым ключом шифрования и исключает перехват и использование информации злоумышленниками. В нашем случае закрытым ключом обладают лишь участники обмены: браузер Google Chrome, запущенный на компьютере пользователя, и сервер компании Google, находящийся по адресу 209.85.233.136. В случае обмена траффиком по незашифрованному протоколу HTTP, в окне с содержимым пакета будут отображаться данные, пригодные для извлечения информации, в том числе с злонамеренными целями.

При детальном анализе, также видно в строке состояния программы (левый нижний угол), что в текущий момент есть попытка в фоновом режиме (скрыто) установить соединение с сервером по адресу https://nexus.officeapps.live.com.

Определим принадлежность субсервера nexus.officeapps на сервере live.com посредством онлайн сервиса 2ip.ru. Для этого перейдём по адресу https://2ip.ru/whois/ и введём https://nexus.officeapps.live.com в поле для проведения анализа.



Анализ полученной информации указывает на то, что сервер находится по адресу 40.122.168.103 и принадлежит Корпорации Microsoft. Содержимое поля «Комментарий» для этого IP-адреса, содержит следующую информацию: «По вопросам предполагаемого нарушения безопасности трафика, исходящего от онлайн-сервисов Microsoft, в том числе распространение вредоносного контента или других незаконных или нелегальных материалов через службу Microsoft в Интернете, пожалуйста, представьте отчеты…». Это указывает на служебное предназначение адреса https://nexus.officeapps.live.com для обмена технической информацией онлайн-сервисов Корпорации Microsoft с программным обеспечением, установленным на компьютере пользователя, из чего становится понятным, что запрос на адрес https://nexus.officeapps.live.com пытался установить один из продуктов компании Microsoft, предположительно пакет Microsoft Office, что не представляет особой опасности. Понятно, что анализ на примере данного сетевого адреса служит лишь для демонстрации алгоритма и при иных результатах следует говорить о необходимости принятия мер.

Таким образом, в случаях вынужденного использования вызывающих сомнения программ, низкой отзывчивости компьютера при работе в сети интернет, его неполного излечения после заражения вирусами-троянами, либо вирусами-майнерами, ввиду недостаточной антивирусной и иной защиты компьютера, и в других случаях, проведение подобного анализа сетевой активности поможет выявить факт обмена нежелательным траффиком и предпринять меры по пресечению такой сетевой активности.