Put together by the WAS Team
Last Updated November 2017

Please note some of the instructions
Included may be reused from https://www.telerik.com/fiddler
This document is meant for internal reference only and not
Meant to be shared externally to Qualys

FIDDLER for Capturing HTTP/S traffic

Contents

Overview of Fiddler

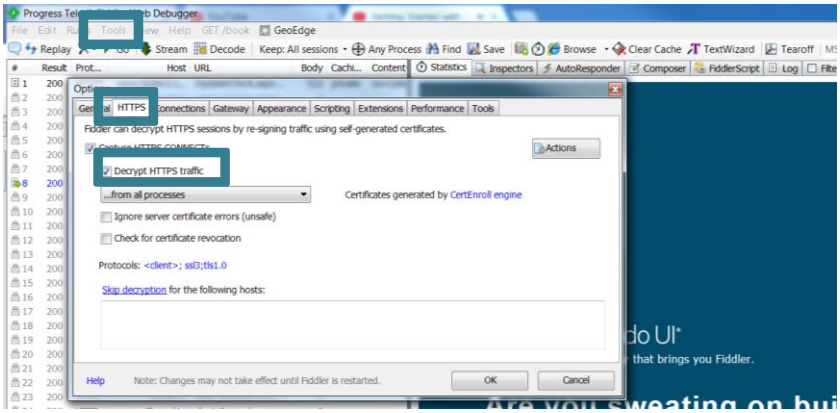
Fiddler is a free tool that can be used to as a proxy to capture web application request just like ZAP and Burp. Below are the instructions of how we would use Fiddler to capture traffic.

Download and Install Fiddler

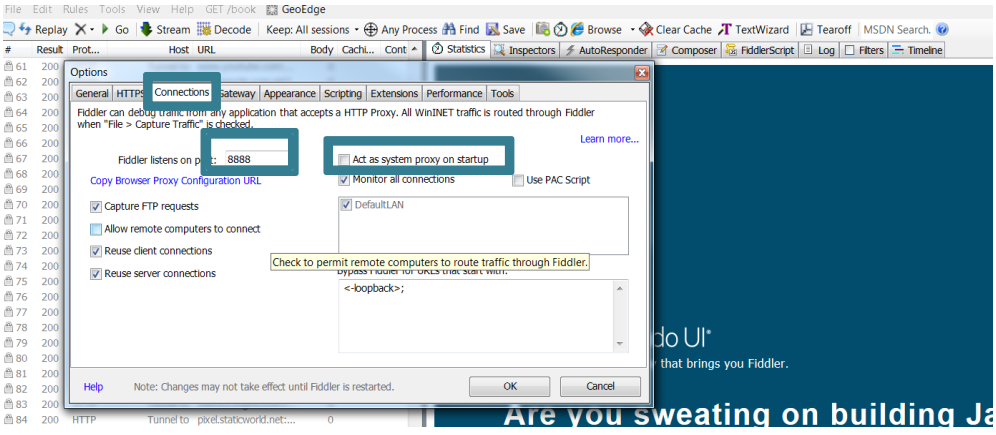
- Free trial of Fiddler is available for download at https://www.telerik.com/download/fiddler
- Installer is available for widely used Windows, Mac OS and Linux operating system

Configure Fiddler to Capture HTTP traffic

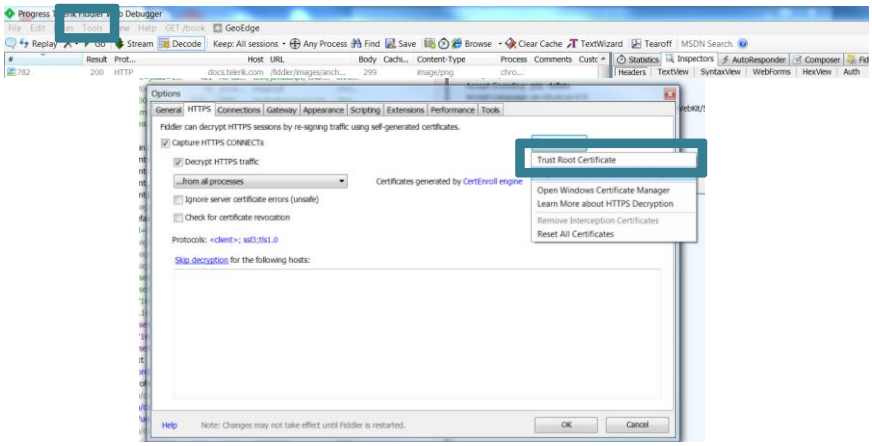
- Fiddler has multiple options to capture traffic current browser session, local machine traffic and Network Traffic
- We are configuring Fiddler to capture only browser specific traffic
- The following settings are important to capture browser specify traffic only
- Enable https:// traffic decryption
    - Open the installed version of Fiddler
    - Click **Tools** > **Options** > **HTTPS** > **Capture HTTPS connect** and **Decrypt HTTPS capture (Select this option)**



- **Proxy port setup**
    - Click **Tools** > **Options** > **Connections** > **{Port Number set on browser}.** Make sure Act as system proxy option was Unchecked under this tab otherwise all machine network traffic will be recorded

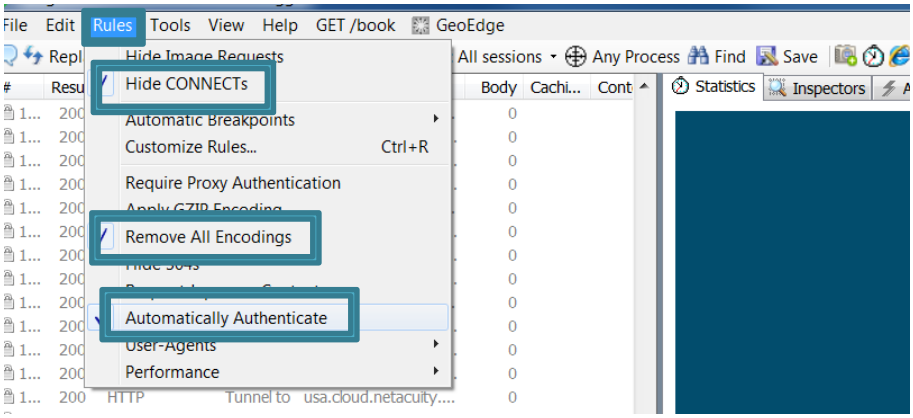


- IMPORTANT – Certificate set up to capture HTTPS traffic
  - Fiddler **--- Tools > Options > HTTPS > Trust Root Certificate (Select)**
    - Please note this may take you through multiple steps to set up this is another way to set up or another option is provided in the 'Configure Browser' section
  - Instructions per Fiddler http://docs.telerik.com/fiddler/Configure-Fiddler/Tasks/FirefoxHTTPS



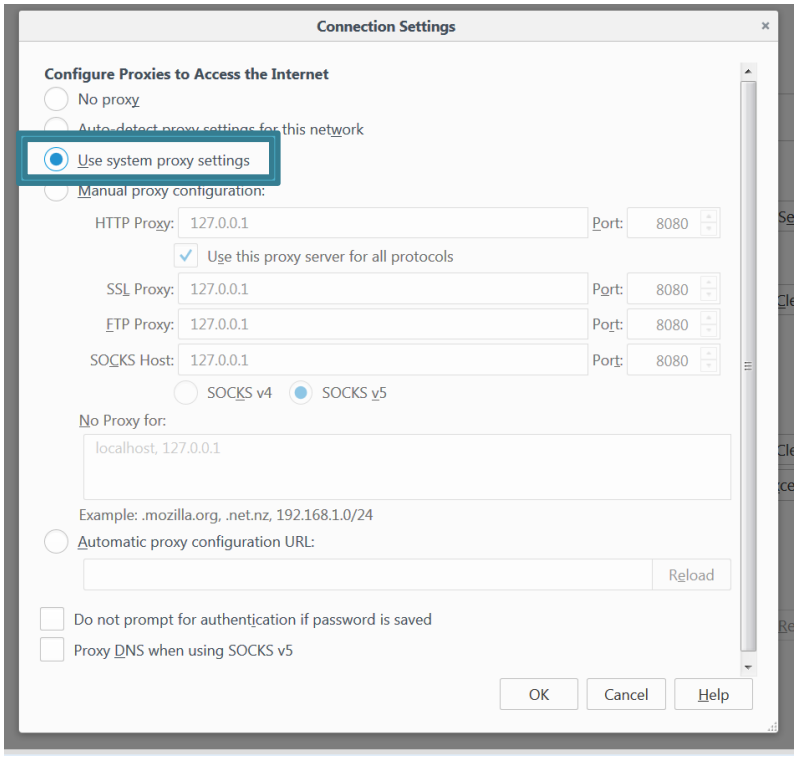
Rule setup on Fiddler

- The rule step is not required for a proxy capture but to filter out captured traffic you can set up different rules
  - Click **Rules** > **Hide Connect**
  - Click **Rules** > **Remove All Encoding**
  - Click **Rules** > **Automatically Authenticate**

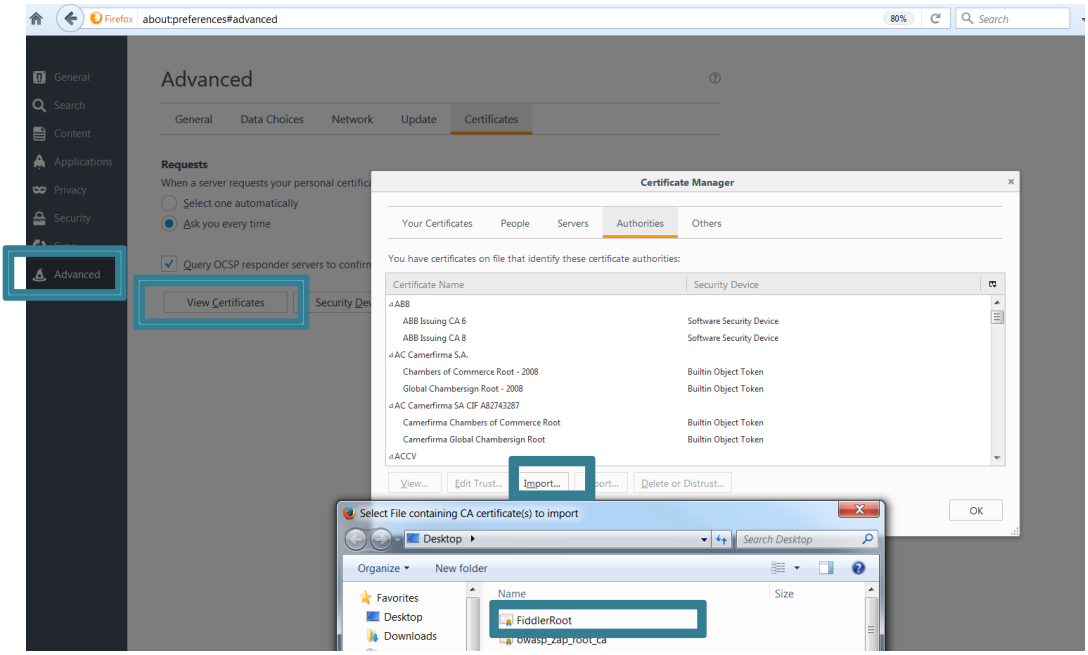


Configure Browser

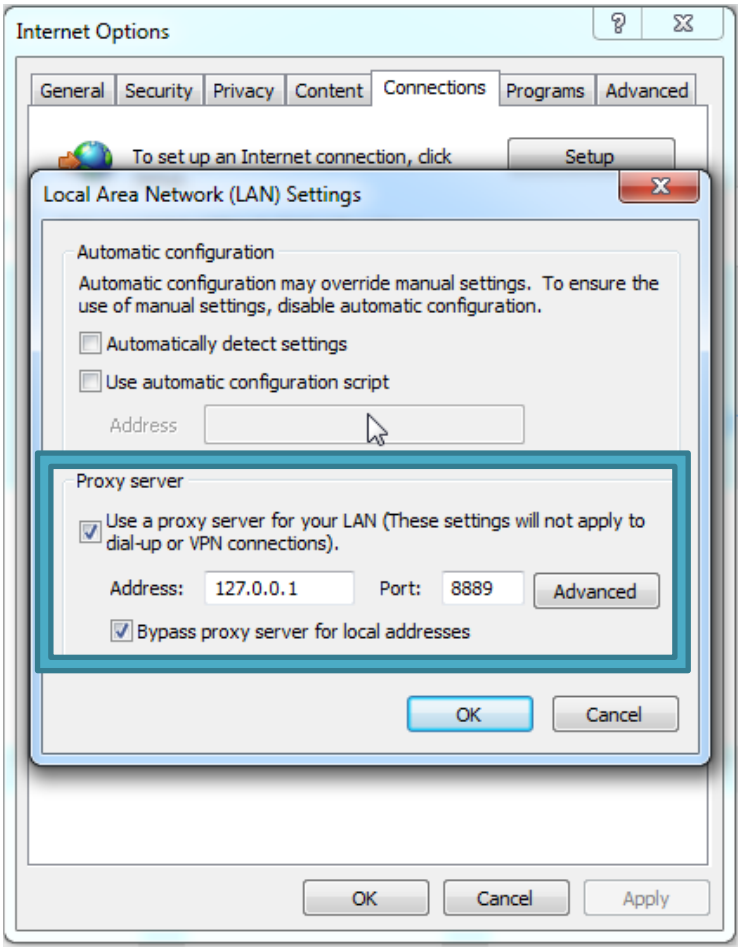
- REQUIRED - Clear browser cookies before starting to capture traffic with Fiddler, this will allow for fresh request and response to be captured by Fiddler, rather than browser cached responses
    - Capture HTTP traffic from **Firefox** browser
    - Open Firefox browser
    - Click **Tools > Options > Advanced > Network > Settings > Use System Proxy Settings**



- In Firefox **Options > Advanced > View Certificates > Import**
    - Select the FiddlerRoot, this certificate was previously downloaded in a previous step while installing Fiddler

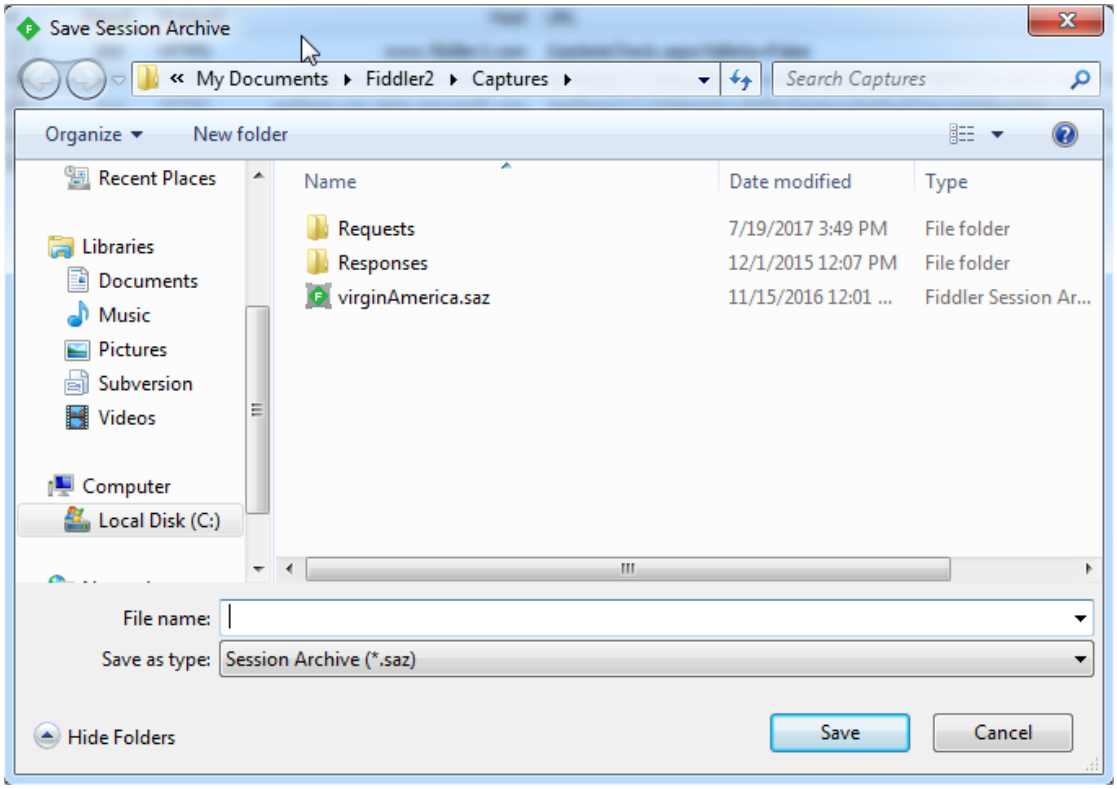


- To capture HTTP traffic from IE:
  - Click **Settings > Options > Internet Options > Connections > LAN Settings > Use Proxy Server for LAN**

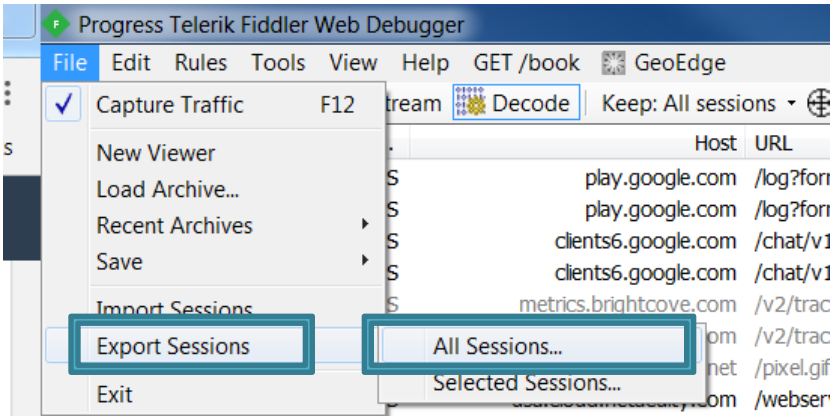

Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
To set up an Internet connection, click
Setup
Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
127.0.0.1
Port:
8889
Advanced
Bypass proxy server for local addresses
OK
Cancel
OK
Cancel
Apply

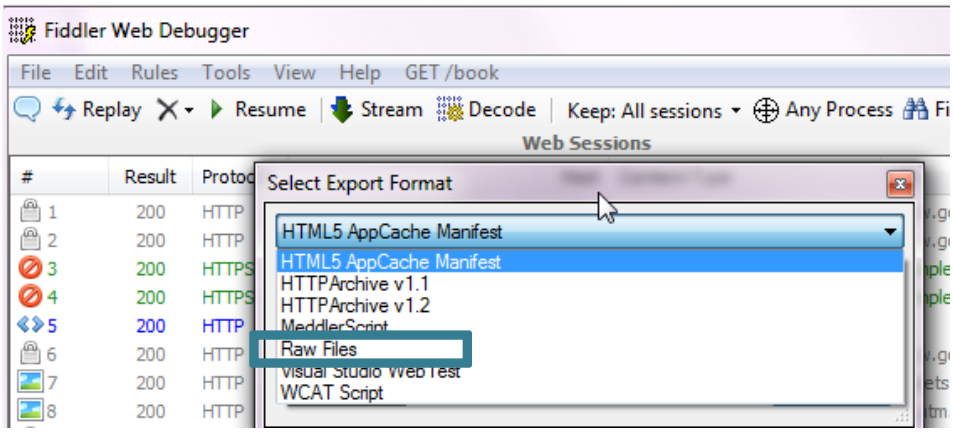
Save and Load Traffic

- Create session archive (.saz) zip
  - Click **File > Save > All Sessions.**
  - Save the traffic to a **.SAZ** file.



- Dump all session request and responses
  - To export traffic to **WCAT Script**, **VS Web Test Script**, **Meddler Script**, **HTML5 AppCache Manifest**, **HTTP Archive Format 1.1**, **HTTP Archive Format 1.2**, or a **Raw File Dump**
  - RECOMMENDED to save session capture in raw file format or .saz session archive





Additional Resources

- Intro to Fiddler video provided by Fiddler https://www.youtube.com/watch?v=gujBKFGwjd4&feature=youtu.be
- Check if the login page was captured
  - Navigate to the location the raw files were saved and travers to the login page
  - For this target the url for login page is at the following http://test.com/bWAPP/login.php
  - The below show the login.php was captured