# Introduction

Protobuf is a binary data representation developed by Google. It is a way of encoding objects into their smallest representation. The encoding of these objects is done by way of a contract. This contract is called a “Proto” file. The proto file contains details about the messages and fields in the messages. This information is stripped from the objects when they are encoded. When the objects are decoded, the information is added back.

When debugging an application that uses the Protobuf data representation, it may be difficult to examine and modify traffic as the traffic is in a binary Protobuf format. To address this, Security Innovation extended the Fiddler Web Debugging tool to allow for encoding, decoding, and modifying Protobuf byte streams between the client and the server. This document describes the design of the ProtoMiddler Fiddler plugin, as well as the installation and usage.

# Description

Fiddler has the concept of an Inspector plugin. These plugins are invoked when examining a sessions. Further, if a breakpoint is set (either on request or response), an Inspector plugin allows for the modification of traffic before the operation is completed.

With this in mind, Security Innovation developed the ProtoMiddler Inspector plugin. This plugin uses the Protobuf.NET tool; specifically protoc.exe. This has three modes which are used by ProtoMiddler. \*

* The first mode is the blind “raw” decoding of Protobuf packets without the aid of a proto.
* The second mode is the smart decoding of Protobuf packets. This requires the proto file as well as the name of the message type being decoded.
* The third mode is the encoding of text into a protobuf byte stream.

Given these three modes, the ProtoMiddler Inspector initially uses the raw decoding mode to decode session data and display it in the Fiddler UI. The user can select a proto file and message type (parsed from the proto file selected), and then re-decode the binary stream using the smart decoding.

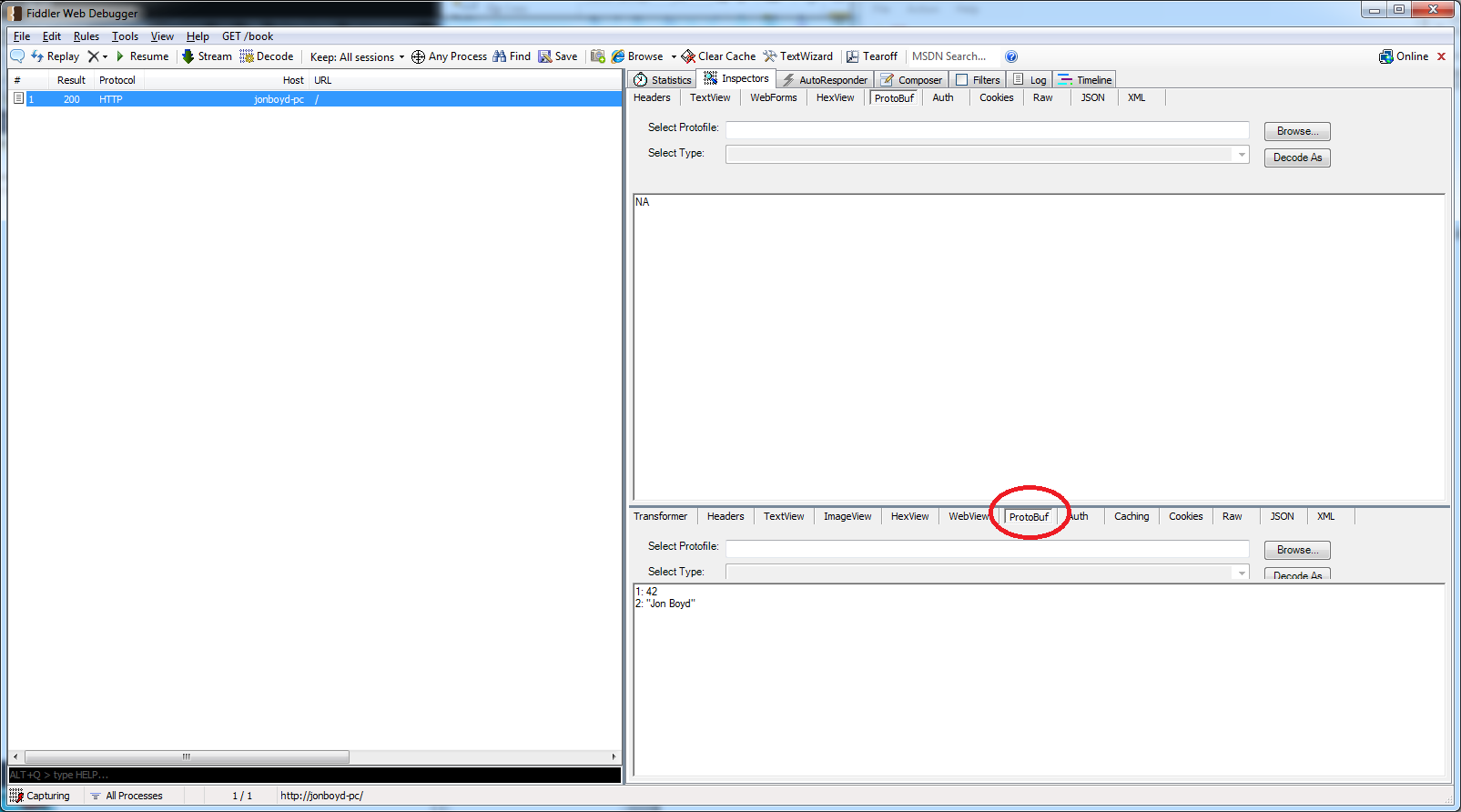
If the user has set a breakpoint on the session (eg break before sending this request to the server), the user can modify the decoded protobuf. This will then be encoded into a protobuf byte stream and forwarded.

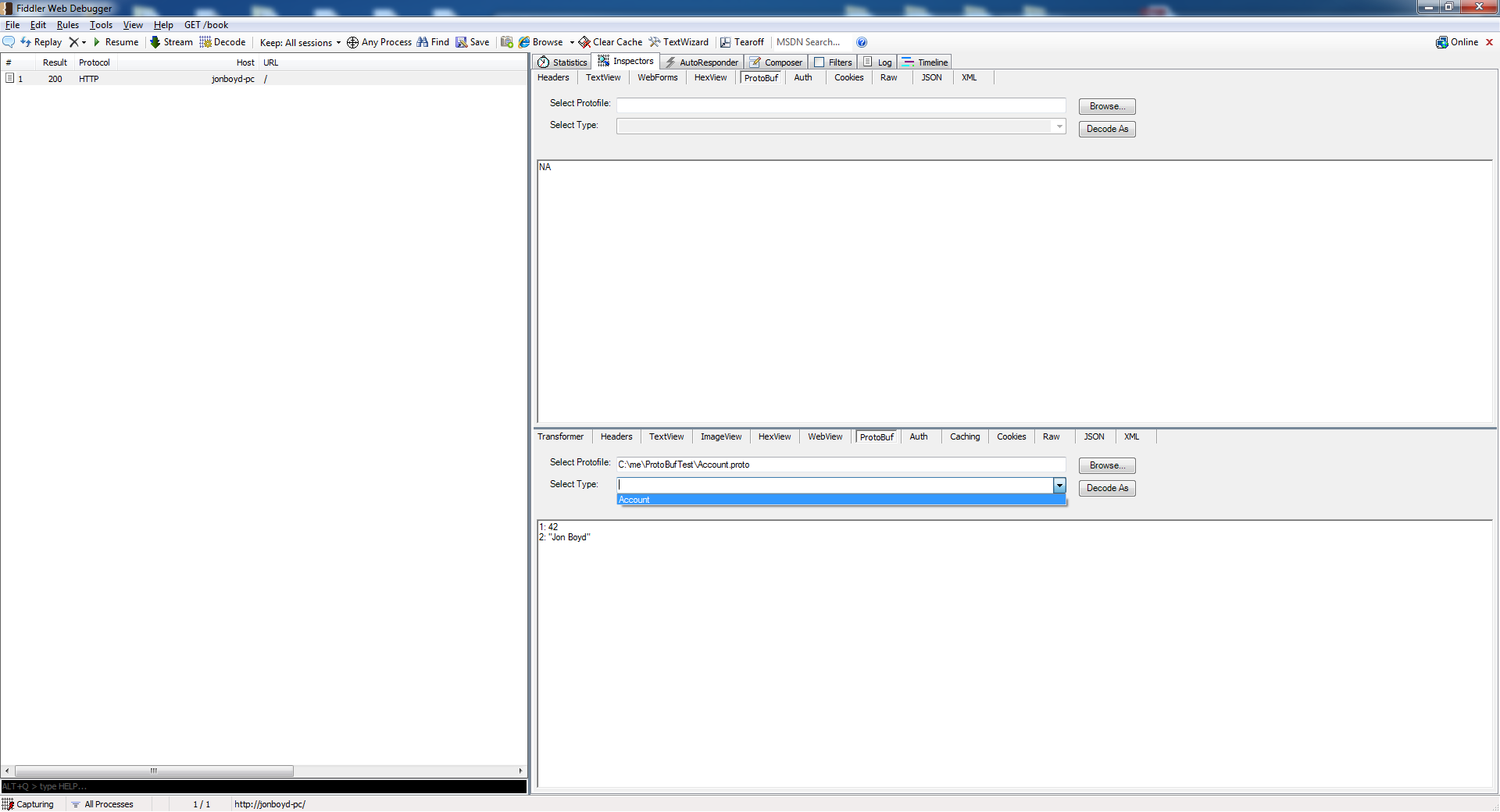
# Installing ProtoMiddler

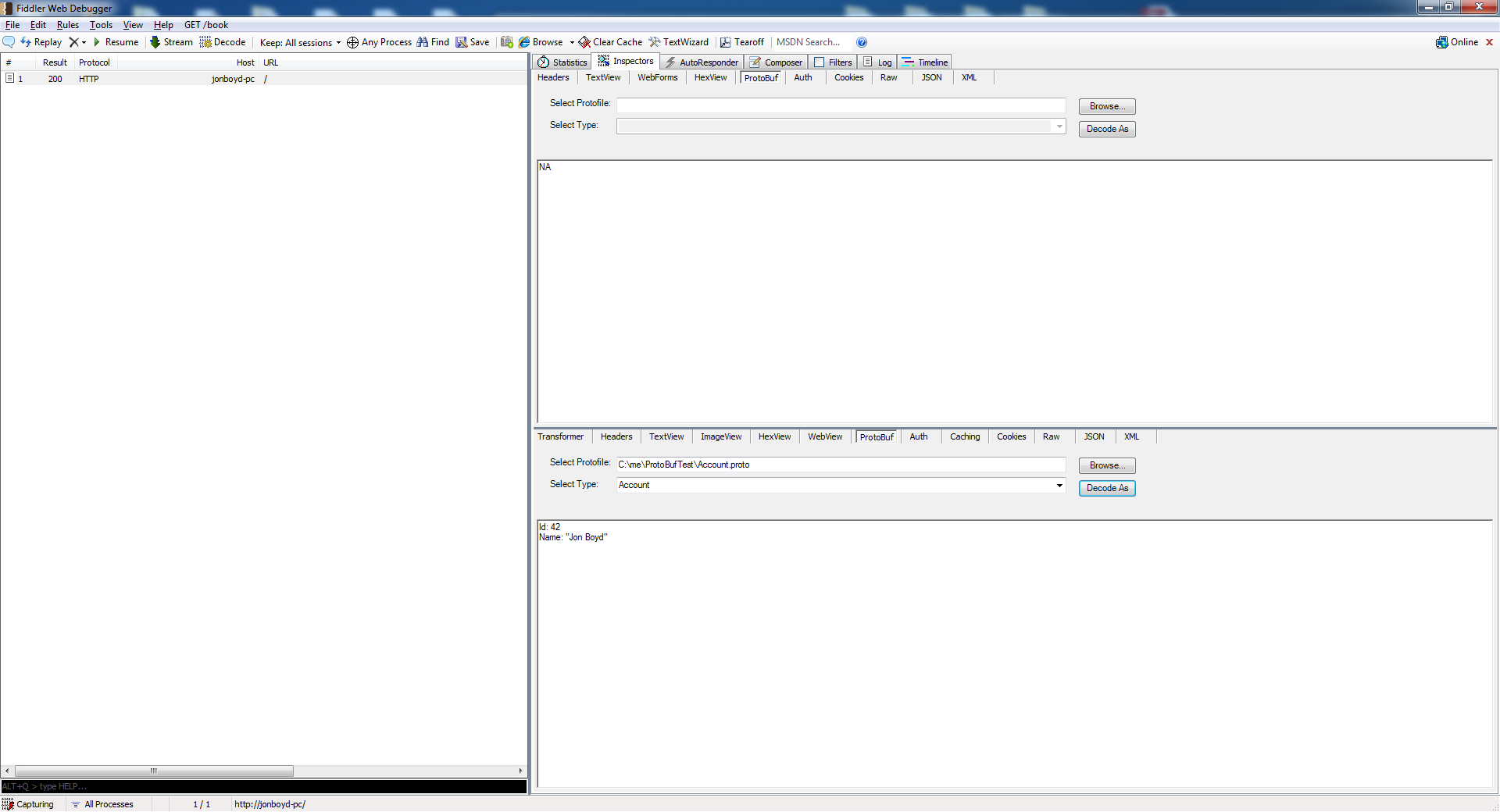
Protomiddler requires Fiddler2 be installed. It also requires Protobuf.NET be installed to: C:\Program Files (x86)\protobuf-net\protobuf-net-VS9. Specifically, the protoc.exe must be available at: C:\Program Files (x86)\protobuf-net\protobuf-net-VS9. Finally, the ProtoMiddler.dll must be installed to: C:\Users\<User>\Documents\Fiddler2\Inspectors\ProtoMiddler.dll

# Usage

The following demonstrates using the protobuf plugin via Fiddler2:







# References

1. Google Protobuf - <http://code.google.com/p/protobuf/>
2. Fiddler2 Inspector - <http://fiddler2.com/documentation/Extend-Fiddler/CustomInspector>