Java: HTTP Listener and XML Parsing

## Use Java and any available resources to accomplish the following tasks.

## Deliverables:

* Java Classes used to accomplish the following (tarred or zipped)
* Optional: Plaintext logs/output from local testing

## Note:

* All of these can be accomplished locally; i.e. have your ‘listener’ and ‘client’ on your local machine. There is no need to setup VM’s.

## Part 1:

1. Create an HTTP Listener that will receive HTTP POST messages.
2. When XML is submitted in the body of the request, parse the XML and respond with the appropriate information (See Part 2)

## Part 2:

See the attached XML on the following page to complete the following. You should send this in the HTTP body to the listener’s URL using a simple POST client (e.g. [Postman](https://www.getpostman.com/)).

1. Retrieve the value of the ‘title’ element, along with the ‘version’, and ‘id’ attributes from the root element. Provide an HTTP response with this information, along with a status code 200.

I.e. if your service were running, a request that contained the sample STIX provided, sent via Postman, would return a 200 status along with:

{“title”: “Example watchlist that contains IP information.”, “version”: “1.0.1”, “id”: “example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d”}

We chose JSON output for this example, but the information can be returned in any fashion.

## Optional/Bonus:

1. Use HTTPS
2. Do something interesting or useful with the XML

<stix:STIX\_Package

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:stix="http://stix.mitre.org/stix-1"

xmlns:indicator="http://stix.mitre.org/Indicator-2"

xmlns:cybox="http://cybox.mitre.org/cybox-2"

xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"

xmlns:cyboxVocabs="http://cybox.mitre.org/default\_vocabularies-2"

xmlns:stixVocabs="http://stix.mitre.org/default\_vocabularies-1"

xmlns:example="http://example.com/"

xsi:schemaLocation="

http://stix.mitre.org/stix-1 ../stix\_core.xsd

http://stix.mitre.org/Indicator-2 ../indicator.xsd

http://cybox.mitre.org/default\_vocabularies-2 ../cybox/cybox\_default\_vocabularies.xsd

http://stix.mitre.org/default\_vocabularies-1 ../stix\_default\_vocabularies.xsd

http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address\_Object.xsd"

id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"

version="1.0.1"

>

<stix:STIX\_Header>

<stix:Title>Example watchlist that contains IP information.</stix:Title>

<stix:Package\_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package\_Intent>

</stix:STIX\_Header>

<stix:Indicators>

<stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d">

<indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>

<indicator:Description>Sample IP Address Indicator for this watchlist. This contains one indicator with a set of three IP addresses in the watchlist.</indicator:Description>

<indicator:Observable id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">

<cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">

<cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">

<AddressObject:Address\_Value condition="Equals" apply\_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Address\_Value>

</cybox:Properties>

</cybox:Object>

</indicator:Observable>

</stix:Indicator>

</stix:Indicators>

</stix:STIX\_Package>