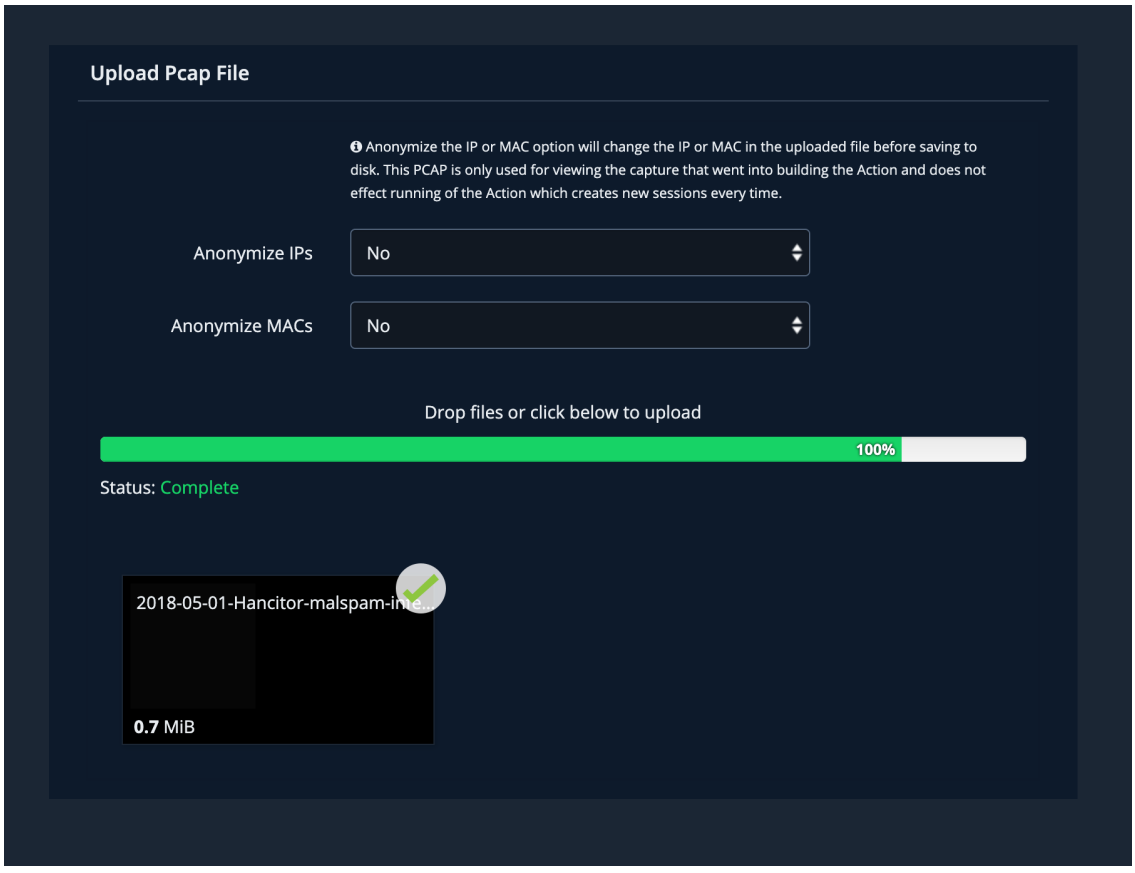
ADDING ACTIONS FROM PACKET CAPTURE

NOTE: All PCAP files should be supported. If you have issues with a PCAP file, submit a support ticket.

1. Go to **Library > Actions**.
2. Select **Add Action > From PCAP**. The Upload PCAP File page comes up.
3. Before uploading your PCAP file, determine if the IP and MAC addresses should be anonymized. You may choose to do this if you don't want to use your network information in an Action.
   a. If you want to anonymize IP addresses in the PCAP file, select **Yes**.
   b. If you want to anonymize MACs in the PCAP file, select **Yes**.
4. Add a PCAP (.pcap) file. The platform will automatically advance to the next page after the upload completes.

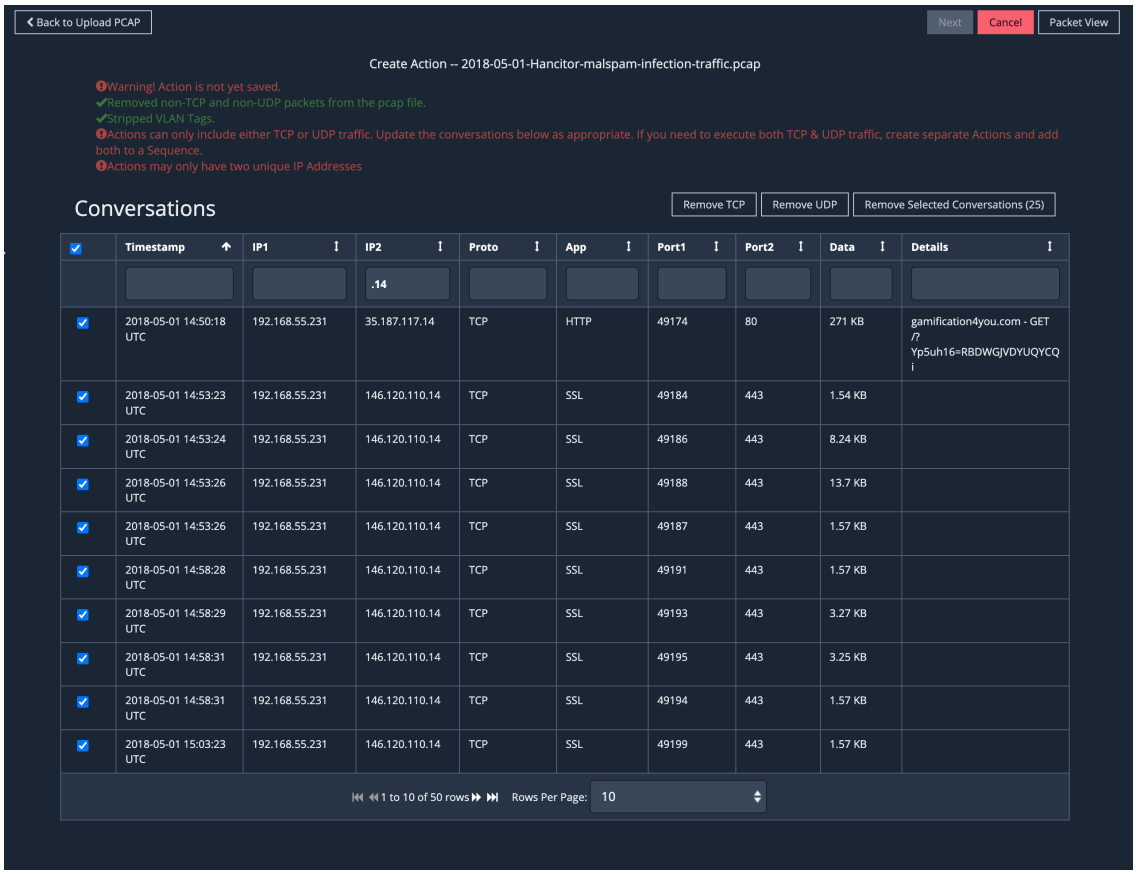
   NOTE: A progress bar that includes an estimated time remaining is displayed to show how the PCAP import is progressing.



Uploading a PCAP file

5. The **Add PCAP Action Step 2** page appears.
   The platform analyzes the PCAP and identifies conversations. It automatically displays feedback regarding issues with the PCAP that must be resolved.

- Actions can only contain TCP or UDP traffic, not both. Actions can only have 2 unique IP Addresses.
- If you use **Back to Upload PCAP** or exit this screen without using one of the buttons, your PCAP will stay in the system.



PCAP upload feedback

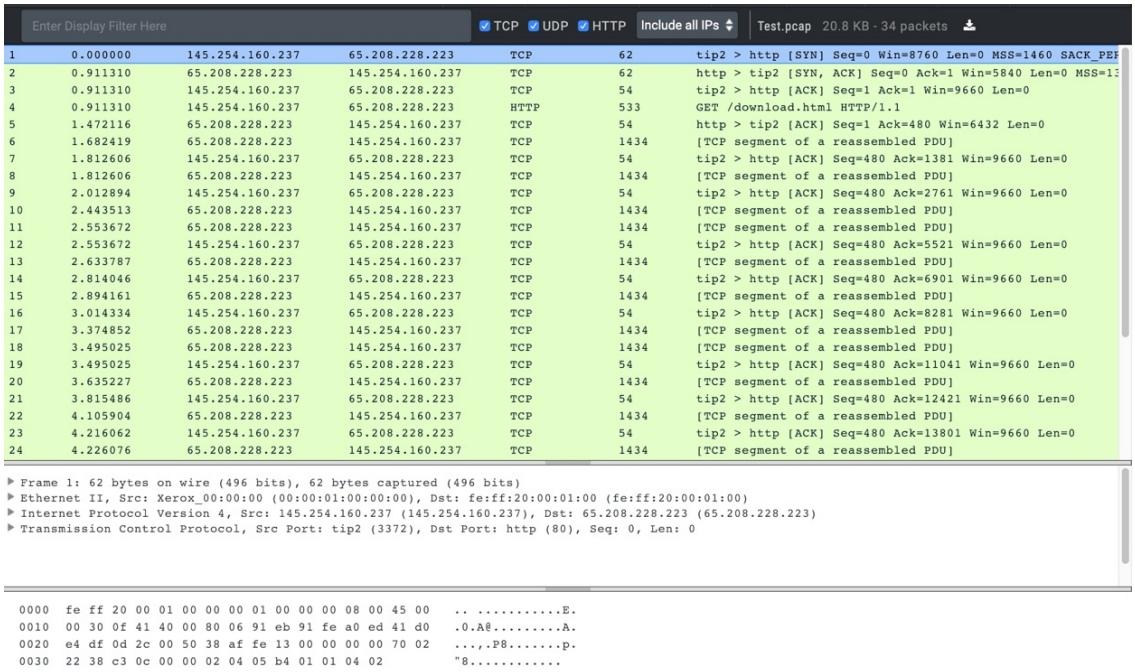
6. Remove Conversations as necessary.
   a. (Optional) Select one or more conversations and click **Remove Conversations**.

      NOTE: This button only appears when conversations are selected.

      TIP: You can select conversations across pages. This includes selecting a conversation on one page, using the page arrows to advanced to another page, and then Shift +clicking on a conversation to select all conversations in between.

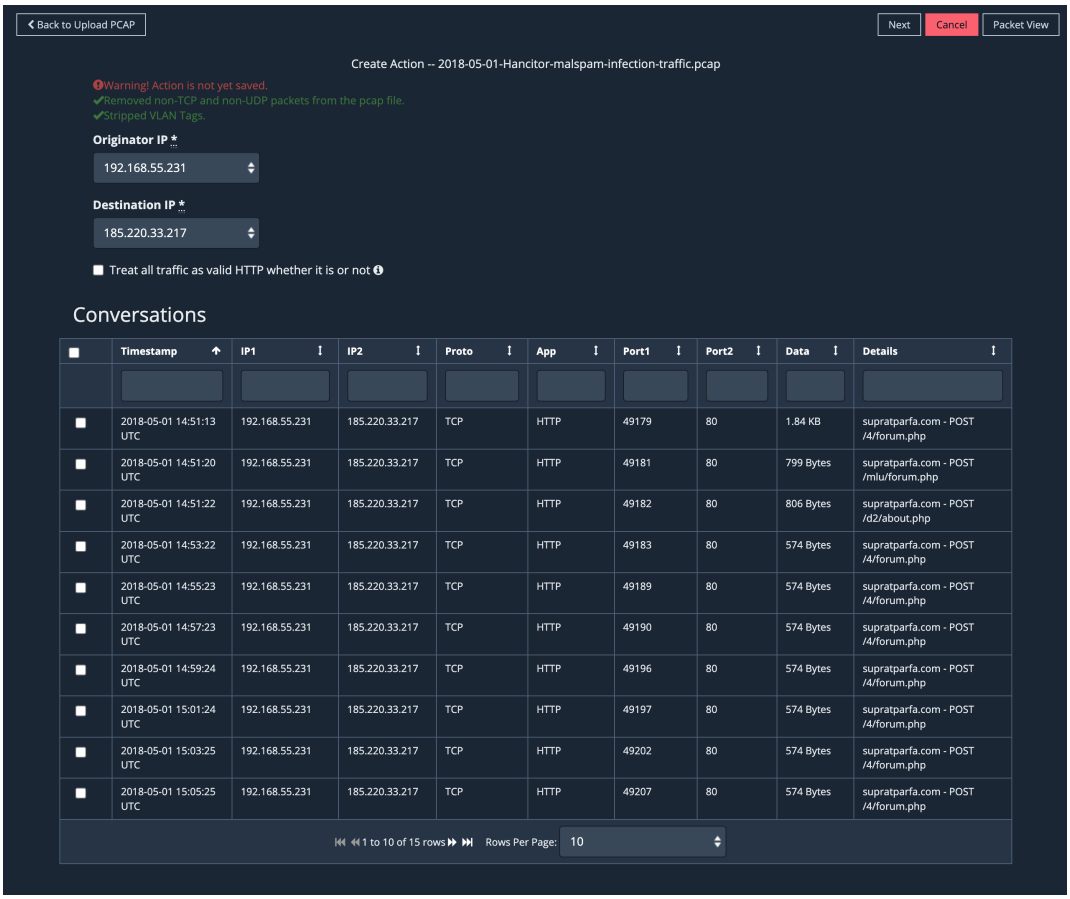
   b. (Optional) Select **Remove TCP** or **Remove UDP** to remove all conversations of that type.
7. (Optional) Click **Packet View** to view remaining packets.

NOTE: When viewing PCAP (Packet View) in MA-SV, you will see rows of gray alternately, not the color scheme available in MSV.



Adding Actions from packet

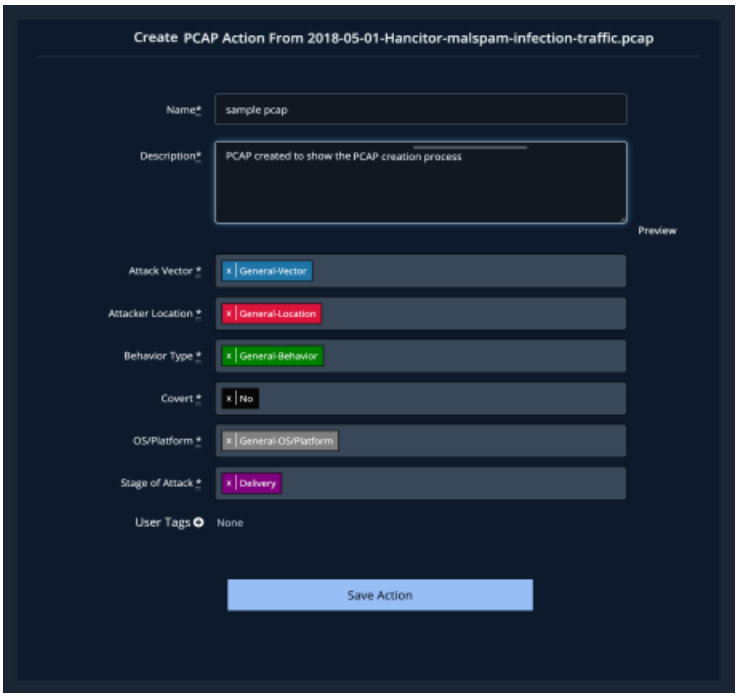
8. When all errors have been resolved, you will see the Originator IP and the Treat all traffic as valid HTTP whether it is or not fields. Make your desired selections and click **Next**.
    a. Originator IP: Choose which of the two IP Addresses the traffic should come from
    b. Treat all traffic as valid HTTP whether it is or not: This is only used when you know the HTTP traffic is intentionally not in a valid format. If you use this option, there is a high chance the traffic will be blocked by a proxy.



Errors resolved in PCAP upload

9. Complete the applicable Dimensions presented and click **Save Action**.
   The Action Library displays. A confirmation message that your Action was created successfully is shown and the Action is selected and displayed in the Action preview.

> **NOTE:** If you click Cancel during the creation process, the Action will not be created.



Complete Dimension selections

HTTP Headers for Hex Actions

The Validation Platform includes a global setting, **Hex Actions - Update Host in HTTP Header** . This allows you to configure the platform so the host is always or never replaced when running Actions. However, to demonstrate specific behavior, such as demonstrating Header Spoofing techniques or leveraging web services as C2s, you may need the Action to run the opposite of the global setting. To support this, there is a **Update Host in HTTP Header** runtime parameter. This defaults to the global setting but can be modified. We recommend you add a note in the Action's description if the Action requires a specific setting for that parameter.