Due to the large volume of network traffic that is collected, we need a tool to help us parse through the traffic. Bro enables us to simply pull out the data we need from the entire network trace so it is not necessary for us to look through all the traffic.

**Event driven language:**
- Any requests and responses sent/received by a computer
- Specifically designed for analyzing network traffic

1. Run the application and collect network data packets (using Wireshark).

**How to find the signature?**

- Create a script that identifies each application in a network trace
- Script looks for our signature in a given input file and would write to a notice log if found

**What do we do with the signatures?**

- Create skeleton Bro script provided to us to use our signature
- Run the application with our Bro scripts and were able to identify particular application usage from each trace

**Testing**

- Generated real results by testing a large volume of traffic. Our grad student mentor tested our signatures against 48 hours of network traffic from the Computer Science and Engineering Building.

**Final Design and Results**

With our signatures and scripts, we are able to run the scripts on network traffic to collect data on usage of certain applications.

**HOW THE SCRIPT WORKS**

- Scans each packet (when triggered by the HTTP request event)
- Continuously checks to see if signature is found in packet
- If so, packet is pulled out and the corresponding information is printed to the notice log
- If not, continue scanning the packets

After the script is completed running, we check to see if a notice log has been created. This leaves us with two cases:

- **No notice log:**
  - No instances of the application in the trace
- **Notice log exists:**
  - Application was found in trace

The results showed us how many machines during a 48 hour period in the CSE building used the following applications:

<table>
<thead>
<tr>
<th>Application</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pandora</td>
<td>10</td>
</tr>
<tr>
<td>Vimeo</td>
<td>20</td>
</tr>
<tr>
<td>Netflix</td>
<td>4</td>
</tr>
<tr>
<td>Viber</td>
<td>2</td>
</tr>
<tr>
<td>Aim</td>
<td>0</td>
</tr>
<tr>
<td>Twitch</td>
<td>7</td>
</tr>
</tbody>
</table>

**Conclusion/Future Work**

Over the course of this project, we have found and verified signatures for a variety of applications including music, video, and chat services. This allows us to take anonymous traffic and quickly identify application usage. As far as future implications, this work provides a way to discover correlations between online activity and machine compromises. As a result, it will be easier to define “risky behavior” for computer users, and we will have a better understanding of computer security in general.

The future work for this project will be to continue developing more signatures in order to have more data to analyze. With more data, there are more possible correlations. We may start looking at mobile applications and finding signatures for them. The ultimate goal for our project: to run our signatures on real-world traffic so that we can gather data to analyze and create these correlations about user behavior.

**Acknowledgements**

- Thanks to Louis Dekoven for mentoring us and always helping us when we had questions
- Thanks to Shelby Thomas for offering their time and expertise
- Thanks to the Early Research Scholar Program and Christine Alvarado for giving us this opportunity
- This material is based upon work supported by the National Science Foundation under Grant No. CCF-1320328