**Field name standards** (always follow):

1. Only use lower case characters (“first\_name” instead of “FirstName”)
2. Avoid special characters except underscores (“first\_name” instead of “first name”)
3. Use underscores to separate words in a field name (“destination\_port” instead of “destinationport”)
4. Due to individuals abbreviating differently, do not use appreviations (“source\_port” instead of “src\_port”)
5. Always use singular forms not plural (“message” instead of “messages”)
6. Use proper spelling of words
7. IP address fields must end with “\_ip” (this is for dynamic mapping)
8. All IP addresses will receive GeoIP lookups for geo and ASN, which will be added to a corresponding “\*\_geo” field (i.e. “source\_ip” will derive “source\_geo”)
9. All IP addresses must be added to the ips array
10. All user fields must be added to the users array (field data from fields such as “user”, “source\_user”, “destination\_user” should be added to users array)

**Field name guidelines** (try to follow):

1. Use present tense unless field describes historical information (Example: end of connection recording “bytes\_received”)
2. Always use singular forms not plural (“message” instead of “messages”)
   1. Exception: When describing something that is past tense and the expectation is for multiple values (“bytes\_received” instead of “byte\_received”)
3. Whenever possible rename fields to match consistent names so long as renaming the field does not cause the event to lose context (Example: “unauthorized\_user” may be able to be renamed to “user” if the only event that contains the field “unauthorized\_user” has another field that provides the context of a failed login)
4. Whenever possible, rename field names with the same purpose to one field name (“SrcIP”, “SourceIP”, “src\_ip”, should be consolidated to “source\_ip”)

**Common field name replacement standards**

Previous Field Name New Name

IPAddress, IP, ip\_addr ip

SourceIP, src\_ip, local\_ip source\_ip

DestinationIP,dst\_ip, remip destination\_ip

Username, User user

SourcePort, src\_port, locport source\_port

DestinationPort, dst\_port, remport destination\_port