microsoft-entra-auth-logs

April 6, 2024

```
[ ]: import pandas as pd
     import matplotlib.pyplot as plt
     import descartes
     import geopandas as gpd
     from shapely.geometry import Point, Polygon
     import folium

     %matplotlib inline
```

```
[ ]: df = pd.read_json(path_or_buf="sign_ins_formatted.json")
     df
```

```
[ ]:                                         id       createdDateTime  \
     0     a24a547c-71e2-47fc-97bb-81d7e4d5aa00  2024-04-06T16:44:27Z
     1     bd5a69d1-0a15-42e0-90da-073377702e00  2024-04-06T16:44:24Z
     2     452d6571-4dba-4ea5-8acf-777ac906b300  2024-04-06T16:44:17Z
     3     c4827fe9-ee3a-4d1e-a320-d166620aa500  2024-04-06T16:40:46Z
     4     d87909c1-c089-4336-be59-fe56ce5ba600  2024-04-06T16:39:31Z
     …                                     …                   …
     5297  f495a8aa-2cf1-449e-afed-2579fc408600  2024-03-07T18:31:20Z
     5298  937f1245-de51-4abb-882c-367019823700  2024-03-07T18:31:03Z
     5299  f495a8aa-2cf1-449e-afed-2579d0358600  2024-03-07T18:30:46Z
     5300  0890237d-aeae-464d-905b-17908bc7b400  2024-03-07T18:28:12Z
     5301  3cb8a923-341a-4d63-8b00-7cc108384f01  2024-03-07T18:09:45Z

                                userDisplayName  \
     0     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
     1                              Tyler Neher
     2                           Tyler M. Neher
     3                           Tyler M. Neher
     4                           Tyler M. Neher
     …                                     …
     5297                        Tyler M. Neher
     5298                        Tyler M. Neher
     5299                        Tyler M. Neher
     5300                        Tyler M. Neher
     5301                        Tyler M. Neher
```

```
                         userPrincipalName  \
0     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
1                      tyler@neherdata.com   
2                      tyler@neherdata.com   
3                      tyler@neherdata.com   
4                      tyler@neherdata.com   
…                                    …   
5297                   tyler@neherdata.com   
5298                   tyler@neherdata.com   
5299                   tyler@neherdata.com   
5300                   tyler@neherdata.com   
5301                   tyler@neherdata.com   

                                    userId  \
0     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
1     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
2     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
3     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
4     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
…                                    …   
5297  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
5298  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
5299  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
5300  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   
5301  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa   

                                     appId               appDisplayName  \
0     c44b4083-3bb0-49c1-b47d-974e53cbdf3c                 Azure Portal   
1     c44b4083-3bb0-49c1-b47d-974e53cbdf3c                 Azure Portal   
2     4813382a-8fa7-425e-ab75-3b753aab3abb  Microsoft Authenticator App   
3     af124e86-4e96-495a-b70a-90f90ab96707             OneDrive iOS App   
4     de8bc8b5-d9f9-48b1-a8ad-b748da725064               Graph Explorer   
…                                    …                           …   
5297  a81d90ac-aa75-4cf8-b14c-58bf348528fe       Microsoft Community v2   
5298  a81d90ac-aa75-4cf8-b14c-58bf348528fe       Microsoft Community v2   
5299  a81d90ac-aa75-4cf8-b14c-58bf348528fe       Microsoft Community v2   
5300  af124e86-4e96-495a-b70a-90f90ab96707             OneDrive iOS App   
5301  27922004-5251-4030-b22d-91ecd9a37ea4               Outlook Mobile   

                                    ipAddress  ipAddressFromResourceProvider  \
0                               69.141.220.21                            NaN   
1                               69.141.220.21                            NaN   
2                               69.141.220.21                            NaN   
3                               69.141.220.21                            NaN   
4                               69.141.220.21                            NaN   
…                                       …                            …   
5297  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN   
```

```
5298  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN
5299  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN
5300  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN
5301                             108.5.169.55                            NaN

                        clientAppUsed  …  \
0                                      …
1                                      …
2     Mobile Apps and Desktop clients  …
3     Mobile Apps and Desktop clients  …
4                             Browser  …
…                               …  …
5297                          Browser  …
5298                          Browser  …
5299                          Browser  …
5300  Mobile Apps and Desktop clients  …
5301  Mobile Apps and Desktop clients  …

     authenticationContextClassReferences  \
0                                      []
1                                      []
2                                      []
3                                      []
4                                      []
…                                   …
5297                                   []
5298                                   []
5299                                   []
5300                                   []
5301                                   []

                        authenticationProcessingDetails  \
0        [{'key': 'Root Key Type', 'value': 'Unknown'}]
1        [{'key': 'Root Key Type', 'value': 'Unknown'}]
2     [{'key': 'Root Key Type', 'value': 'Unknown'},…
3     [{'key': 'Root Key Type', 'value': 'Unknown'},…
4        [{'key': 'Root Key Type', 'value': 'Unknown'}]
…                                                 …
5297     [{'key': 'Root Key Type', 'value': 'Unknown'}]
5298     [{'key': 'Root Key Type', 'value': 'Unknown'}]
5299     [{'key': 'Root Key Type', 'value': 'Unknown'}]
5300  [{'key': 'Root Key Type', 'value': 'Unknown'},…
5301  [{'key': 'Root Key Type', 'value': 'Unknown'},…

     networkLocationDetails  \
0                        []
1                        []
```

```
2                         []
3                         []
4                         []
…                      …
5297                      []
5298                      []
5299                      []
5300                      []
5301                      []

                                   authenticationDetails  \
0                                                     []
1     [{'authenticationStepDateTime': '2024-04-06T16…
2                                                     []
3                                                     []
4                                                     []
…                                                  …
5297  [{'authenticationStepDateTime': '2024-03-07T18…
5298  [{'authenticationStepDateTime': '2024-03-07T18…
5299  [{'authenticationStepDateTime': '2024-03-07T18…
5300                                                  []
5301                                                  []

      authenticationRequirementPolicies  \
0                                   []
1                                   []
2                                   []
3                                   []
4                                   []
…                                …
5297                                []
5298                                []
5299                                []
5300                                []
5301                                []

                                 sessionLifetimePolicies  \
0                                                     []
1                                                     []
2     [{'expirationRequirement': 'rememberMultifacto…
3     [{'expirationRequirement': 'rememberMultifacto…
4     [{'expirationRequirement': 'rememberMultifacto…
…                                                  …
5297  [{'expirationRequirement': 'rememberMultifacto…
5298  [{'expirationRequirement': 'rememberMultifacto…
5299  [{'expirationRequirement': 'rememberMultifacto…
5300  [{'expirationRequirement': 'rememberMultifacto…
```

```
5301  [{'expirationRequirement': 'rememberMultifacto…

                                     privateLinkDetails appliedEventListeners  \
0     {'policyId': '', 'policyName': '', 'resourceId…                    []
1     {'policyId': '', 'policyName': '', 'resourceId…                    []
2     {'policyId': '', 'policyName': '', 'resourceId…                    []
3     {'policyId': '', 'policyName': '', 'resourceId…                    []
4     {'policyId': '', 'policyName': '', 'resourceId…                    []
…                                                   …                   …
5297  {'policyId': '', 'policyName': '', 'resourceId…                    []
5298  {'policyId': '', 'policyName': '', 'resourceId…                    []
5299  {'policyId': '', 'policyName': '', 'resourceId…                    []
5300  {'policyId': '', 'policyName': '', 'resourceId…                    []
5301  {'policyId': '', 'policyName': '', 'resourceId…                    []

               authenticationAppPolicyEvaluationDetails  \
0                                                    []
1     [{'policyName': 'Number Match', 'adminConfigur…
2     [{'policyName': 'App Lock', 'adminConfiguratio…
3     [{'policyName': 'App Lock', 'adminConfiguratio…
4     [{'policyName': 'App Lock', 'adminConfiguratio…
…                                                   …
5297                                                 []
5298                                                 []
5299                                                 []
5300  [{'policyName': 'App Lock', 'adminConfiguratio…
5301  [{'policyName': 'App Lock', 'adminConfiguratio…

                                 managedServiceIdentity
0     {'msiType': 'none', 'associatedResourceId': No…
1     {'msiType': 'none', 'associatedResourceId': No…
2     {'msiType': 'none', 'associatedResourceId': No…
3     {'msiType': 'none', 'associatedResourceId': No…
4     {'msiType': 'none', 'associatedResourceId': No…
…                                                   …
5297  {'msiType': 'none', 'associatedResourceId': No…
5298  {'msiType': 'none', 'associatedResourceId': No…
5299  {'msiType': 'none', 'associatedResourceId': No…
5300  {'msiType': 'none', 'associatedResourceId': No…
5301  {'msiType': 'none', 'associatedResourceId': No…

[5302 rows x 66 columns]
```

[ ]:

```
df.columns.to_list()
```

[ ]:

```
['id',
 'createdDateTime',
  'userDisplayName',
  'userPrincipalName',
  'userId',
  'appId',
  'appDisplayName',
  'ipAddress',
  'ipAddressFromResourceProvider',
  'clientAppUsed',
  'userAgent',
  'correlationId',
  'conditionalAccessStatus',
  'originalRequestId',
  'isInteractive',
  'tokenIssuerName',
  'tokenIssuerType',
  'clientCredentialType',
  'processingTimeInMilliseconds',
  'riskDetail',
  'riskLevelAggregated',
  'riskLevelDuringSignIn',
  'riskState',
  'riskEventTypes_v2',
  'resourceDisplayName',
  'resourceId',
  'resourceTenantId',
  'homeTenantId',
  'homeTenantName',
  'authenticationMethodsUsed',
  'authenticationRequirement',
  'signInIdentifier',
  'signInIdentifierType',
  'servicePrincipalName',
  'signInEventTypes',
  'servicePrincipalId',
  'federatedCredentialId',
  'userType',
  'flaggedForReview',
  'isTenantRestricted',
  'autonomousSystemNumber',
  'crossTenantAccessType',
  'servicePrincipalCredentialKeyId',
  'servicePrincipalCredentialThumbprint',
  'uniqueTokenIdentifier',
  'incomingTokenType',
  'authenticationProtocol',
  'resourceServicePrincipalId',
  'signInTokenProtectionStatus',
 'originalTransferMethod',
 'mfaDetail',
 'authenticationAppDeviceDetails',
 'status',
 'deviceDetail',
 'location',
 'appliedConditionalAccessPolicies',
 'authenticationContextClassReferences',
 'authenticationProcessingDetails',
 'networkLocationDetails',
 'authenticationDetails',
 'authenticationRequirementPolicies',
 'sessionLifetimePolicies',
 'privateLinkDetails',
 'appliedEventListeners',
 'authenticationAppPolicyEvaluationDetails',
 'managedServiceIdentity']
```

[ ]:

```
locations = df["location"]
locations[1]["geoCoordinates"]
```

[ ]:

```
{'altitude': None, 'latitude': 40.35863, 'longitude': -74.13705}
```

[ ]:

```
city = locations.apply(lambda x: x["city"])
state = locations.apply(lambda x: x["state"])
countryOrRegion = locations.apply(lambda x: x["countryOrRegion"])
altitude = locations.apply(lambda x: x["geoCoordinates"]).apply(
    lambda x: x["altitude"])
latitude = locations.apply(lambda x: x["geoCoordinates"]).apply(
    lambda x: x["latitude"])
longitude = locations.apply(lambda x: x["geoCoordinates"]).apply(
    lambda x: x["longitude"]
)

df["city"] = city
df["state"] = state
df["countryOrRegion"] = countryOrRegion
df["altitude"] = altitude
df["latitude"] = latitude
df["longitude"] = longitude


df
```

[ ]:

```
                                         id       createdDateTime  \
0     a24a547c-71e2-47fc-97bb-81d7e4d5aa00  2024-04-06T16:44:27Z
1     bd5a69d1-0a15-42e0-90da-073377702e00  2024-04-06T16:44:24Z
```

```
2     452d6571-4dba-4ea5-8acf-777ac906b300  2024-04-06T16:44:17Z
3     c4827fe9-ee3a-4d1e-a320-d166620aa500  2024-04-06T16:40:46Z
4     d87909c1-c089-4336-be59-fe56ce5ba600  2024-04-06T16:39:31Z
…                                      …                     …
5297  f495a8aa-2cf1-449e-afed-2579fc408600  2024-03-07T18:31:20Z
5298  937f1245-de51-4abb-882c-367019823700  2024-03-07T18:31:03Z
5299  f495a8aa-2cf1-449e-afed-2579d0358600  2024-03-07T18:30:46Z
5300  0890237d-aeae-464d-905b-17908bc7b400  2024-03-07T18:28:12Z
5301  3cb8a923-341a-4d63-8b00-7cc108384f01  2024-03-07T18:09:45Z

                           userDisplayName  \
0     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
1                              Tyler Neher
2                           Tyler M. Neher
3                           Tyler M. Neher
4                           Tyler M. Neher
…                                      …
5297                        Tyler M. Neher
5298                        Tyler M. Neher
5299                        Tyler M. Neher
5300                        Tyler M. Neher
5301                        Tyler M. Neher

                         userPrincipalName  \
0     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
1                      tyler@neherdata.com
2                      tyler@neherdata.com
3                      tyler@neherdata.com
4                      tyler@neherdata.com
…                                      …
5297                   tyler@neherdata.com
5298                   tyler@neherdata.com
5299                   tyler@neherdata.com
5300                   tyler@neherdata.com
5301                   tyler@neherdata.com

                                    userId  \
0     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
1     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
2     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
3     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
4     a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
…                                      …
5297  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
5298  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
5299  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
5300  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa
```

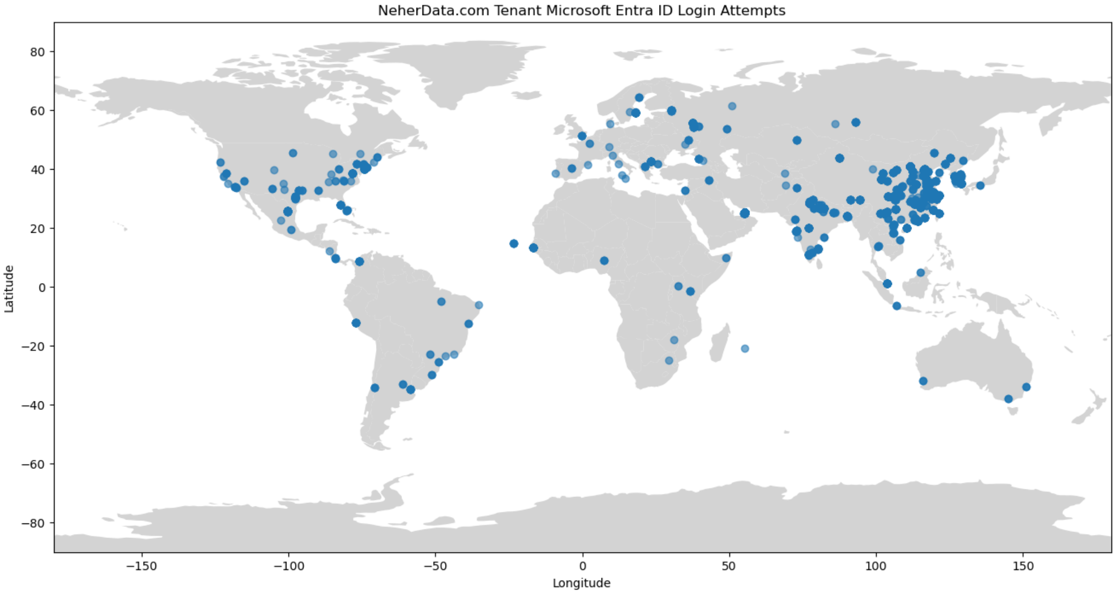
```
5301  a3bc732b-08dc-4ec2-b327-9dcf0c1eeafa

                                     appId                appDisplayName  \
0     c44b4083-3bb0-49c1-b47d-974e53cbdf3c                  Azure Portal
1     c44b4083-3bb0-49c1-b47d-974e53cbdf3c                  Azure Portal
2     4813382a-8fa7-425e-ab75-3b753aab3abb  Microsoft Authenticator App
3     af124e86-4e96-495a-b70a-90f90ab96707              OneDrive iOS App
4     de8bc8b5-d9f9-48b1-a8ad-b748da725064                Graph Explorer
…                                    …                          …
5297  a81d90ac-aa75-4cf8-b14c-58bf348528fe        Microsoft Community v2
5298  a81d90ac-aa75-4cf8-b14c-58bf348528fe        Microsoft Community v2
5299  a81d90ac-aa75-4cf8-b14c-58bf348528fe        Microsoft Community v2
5300  af124e86-4e96-495a-b70a-90f90ab96707              OneDrive iOS App
5301  27922004-5251-4030-b22d-91ecd9a37ea4                Outlook Mobile

                                    ipAddress  ipAddressFromResourceProvider  \
0                               69.141.220.21                            NaN
1                               69.141.220.21                            NaN
2                               69.141.220.21                            NaN
3                               69.141.220.21                            NaN
4                               69.141.220.21                            NaN
…                                        …                            …
5297  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN
5298  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN
5299  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN
5300  2600:1001:b112:cbee:8c5f:2fad:5454:f48e                            NaN
5301                             108.5.169.55                            NaN

                        clientAppUsed  …  \
0                                      …
1                                      …
2     Mobile Apps and Desktop clients  …
3     Mobile Apps and Desktop clients  …
4                             Browser  …
…                               …  …
5297                          Browser  …
5298                          Browser  …
5299                          Browser  …
5300  Mobile Apps and Desktop clients  …
5301  Mobile Apps and Desktop clients  …

                                     privateLinkDetails appliedEventListeners  \
0     {'policyId': '', 'policyName': '', 'resourceId…                    []
1     {'policyId': '', 'policyName': '', 'resourceId…                    []
2     {'policyId': '', 'policyName': '', 'resourceId…                    []
3     {'policyId': '', 'policyName': '', 'resourceId…                    []
4     {'policyId': '', 'policyName': '', 'resourceId…                    []
```

```
…                                                 …                   …
5297  {'policyId': '', 'policyName': '', 'resourceId…                    []
5298  {'policyId': '', 'policyName': '', 'resourceId…                    []
5299  {'policyId': '', 'policyName': '', 'resourceId…                    []
5300  {'policyId': '', 'policyName': '', 'resourceId…                    []
5301  {'policyId': '', 'policyName': '', 'resourceId…                    []

               authenticationAppPolicyEvaluationDetails  \
0                                                    []
1     [{'policyName': 'Number Match', 'adminConfigur…
2     [{'policyName': 'App Lock', 'adminConfiguratio…
3     [{'policyName': 'App Lock', 'adminConfiguratio…
4     [{'policyName': 'App Lock', 'adminConfiguratio…
…                                                 …
5297                                                 []
5298                                                 []
5299                                                 []
5300  [{'policyName': 'App Lock', 'adminConfiguratio…
5301  [{'policyName': 'App Lock', 'adminConfiguratio…

                                 managedServiceIdentity             city  \
0     {'msiType': 'none', 'associatedResourceId': No…
1     {'msiType': 'none', 'associatedResourceId': No…        Lincroft
2     {'msiType': 'none', 'associatedResourceId': No…        Lincroft
3     {'msiType': 'none', 'associatedResourceId': No…        Lincroft
4     {'msiType': 'none', 'associatedResourceId': No…        Lincroft
…                                                 …              …
5297  {'msiType': 'none', 'associatedResourceId': No…        Freehold
5298  {'msiType': 'none', 'associatedResourceId': No…        Freehold
5299  {'msiType': 'none', 'associatedResourceId': No…        Freehold
5300  {'msiType': 'none', 'associatedResourceId': No…        Freehold
5301  {'msiType': 'none', 'associatedResourceId': No…  Hazlet Township

           state countryOrRegion altitude  latitude longitude
0                                    None       NaN       NaN
1     New Jersey              US     None  40.35863 -74.13705
2     New Jersey              US     None  40.35863 -74.13705
3     New Jersey              US     None  40.35863 -74.13705
4     New Jersey              US     None  40.35863 -74.13705
…            …             …      …       …       …
5297  New Jersey              US     None  40.27322 -74.23018
5298  New Jersey              US     None  40.27322 -74.23018
5299  New Jersey              US     None  40.27322 -74.23018
5300  New Jersey              US     None  40.27322 -74.23018
5301  New Jersey              US     None  40.42598 -74.16610

[5302 rows x 72 columns]
```

[ ]:

```
worldmap = gpd.read_file(gpd.datasets.get_path("naturalearth_lowres"))

# Creating axes and plotting world map
fig, ax = plt.subplots(figsize=(16, 10))
worldmap.plot(color="lightgrey", ax=ax)

x = df["longitude"]
y = df["latitude"]
plt.scatter(x, y, alpha=0.6, cmap="autumn")
# plt.colorbar(label='NeherData.com Tenant Microsoft Entra ID Login Attempts')

# Creating axis limits and title
plt.xlim([-180, 180])
plt.ylim([-90, 90])

plt.title("NeherData.com Tenant Microsoft Entra ID Login Attempts")
plt.xlabel("Longitude")
plt.ylabel("Latitude")
plt.show()
```

```
/var/folders/m4/r3wttq2j5hs_1mpf0t1yvhq80000gn/T/ipykernel_76624/2671292473.py:1
: FutureWarning: The geopandas.dataset module is deprecated and will be removed
in GeoPandas 1.0. You can get the original 'naturalearth_lowres' data from
https://www.naturalearthdata.com/downloads/110m-cultural-vectors/.
  worldmap = gpd.read_file(gpd.datasets.get_path("naturalearth_lowres"))
/var/folders/m4/r3wttq2j5hs_1mpf0t1yvhq80000gn/T/ipykernel_76624/2671292473.py:9
: UserWarning: No data for colormapping provided via 'c'. Parameters 'cmap' will
be ignored
  plt.scatter(x, y, alpha=0.6, cmap="autumn")
```



[ ]:
```
# Make an empty map
m = folium.Map(location=[20, 0], tiles="CartoDB Voyager", zoom_start=2)

# Show the map
m
```

[ ]:
```
<folium.folium.Map at 0x1ab143710>
```

[ ]:
```
latlon_df = pd.DataFrame(
    data=df.dropna(subset=["latitude", "longitude"]),
    columns=["latitude", "longitude", "city", "state", "countryOrRegion"],
)
# latlon_df['latitude'] = df['latitude'].notna()


latlon_df
```

[ ]:
```
      latitude  longitude             city       state countryOrRegion
1     40.35863  -74.13705         Lincroft  New Jersey              US
2     40.35863  -74.13705         Lincroft  New Jersey              US
3     40.35863  -74.13705         Lincroft  New Jersey              US
4     40.35863  -74.13705         Lincroft  New Jersey              US
5     40.35863  -74.13705         Lincroft  New Jersey              US
…          …         …               …          …             …
5297  40.27322  -74.23018         Freehold  New Jersey              US
5298  40.27322  -74.23018         Freehold  New Jersey              US
5299  40.27322  -74.23018         Freehold  New Jersey              US
5300  40.27322  -74.23018         Freehold  New Jersey              US
5301  40.42598  -74.16610  Hazlet Township  New Jersey              US

[5295 rows x 5 columns]
```

[ ]:
```
# add marker one by one on the map
for i in range(0, len(latlon_df)):
    folium.Marker(
        location=[latlon_df.iloc[i]["latitude"],
                  latlon_df.iloc[i]["longitude"]],
        popup=latlon_df.iloc[i]["city"],
    ).add_to(m)

# Show the map again
m
```

[ ]:
```
<folium.folium.Map at 0x1ab143710>
```

[ ]:
```
map_html = m._repr_html_()
```