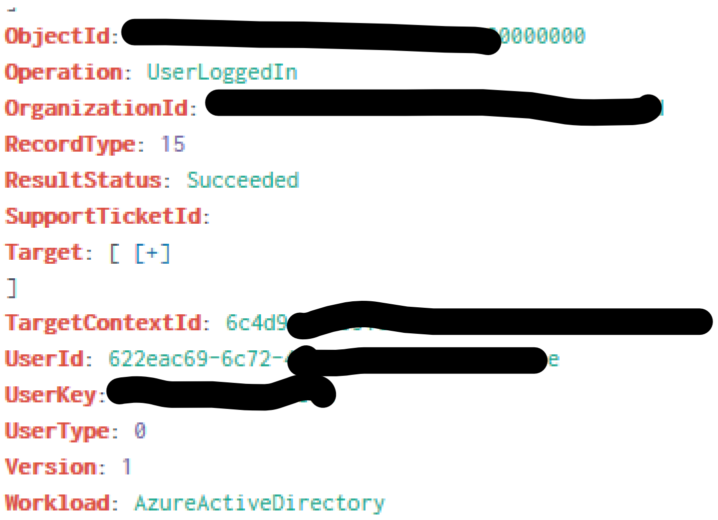
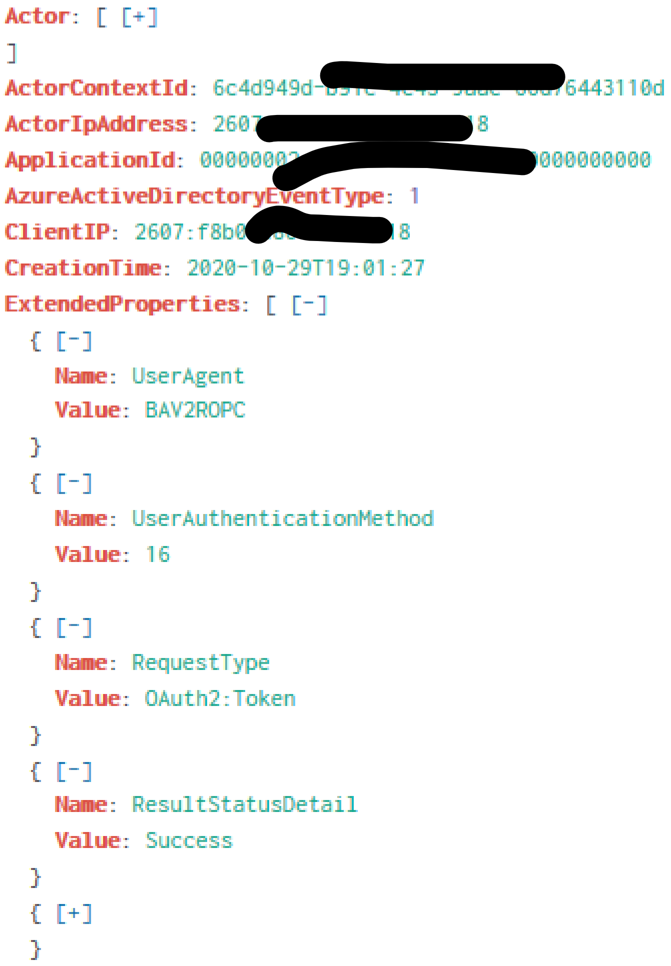
Digging Up the Bones:
O365 Authentication Types via Splunk Log Examples

Workload: Azure AD

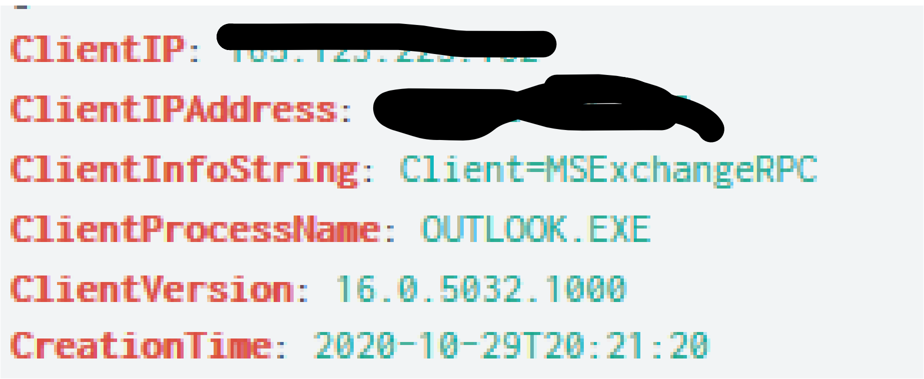


```
ObjectId: [redacted]0000000
Operation: UserLoggedIn
OrganizationId: [redacted]
RecordType: 15
ResultStatus: Succeeded
SupportTicketId:
Target: [ [+]
]
TargetContextId: 6c4d9[redacted]
UserId: 622eac69-6c72-[redacted]e
UserKey: [redacted]
UserType: 0
Version: 1
Workload: AzureActiveDirectory
```

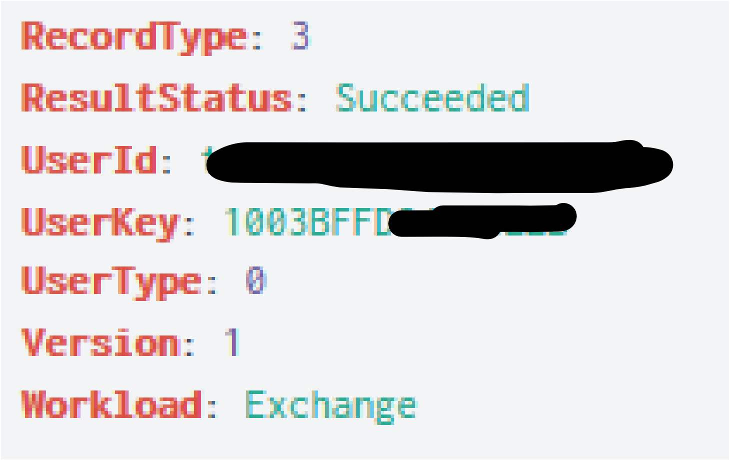


```
Actor: [ [+]
]
ActorContextId: 6c4d949d-[redacted]6443110d
ActorIpAddress: 2607[redacted]8
ApplicationId: 0000000[redacted]000000000
AzureActiveDirectoryEventType: 1
ClientIP: 2607:f8b0[redacted]18
CreationTime: 2020-10-29T19:01:27
ExtendedProperties: [ [-]
  { [-]
    Name: UserAgent
    Value: BAV2ROPC
  }
  { [-]
    Name: UserAuthenticationMethod
    Value: 16
  }
  { [-]
    Name: RequestType
    Value: OAuth2:Token
  }
  { [-]
    Name: ResultStatusDetail
    Value: Success
  }
  { [+]
  }
```

Workload: Exchange

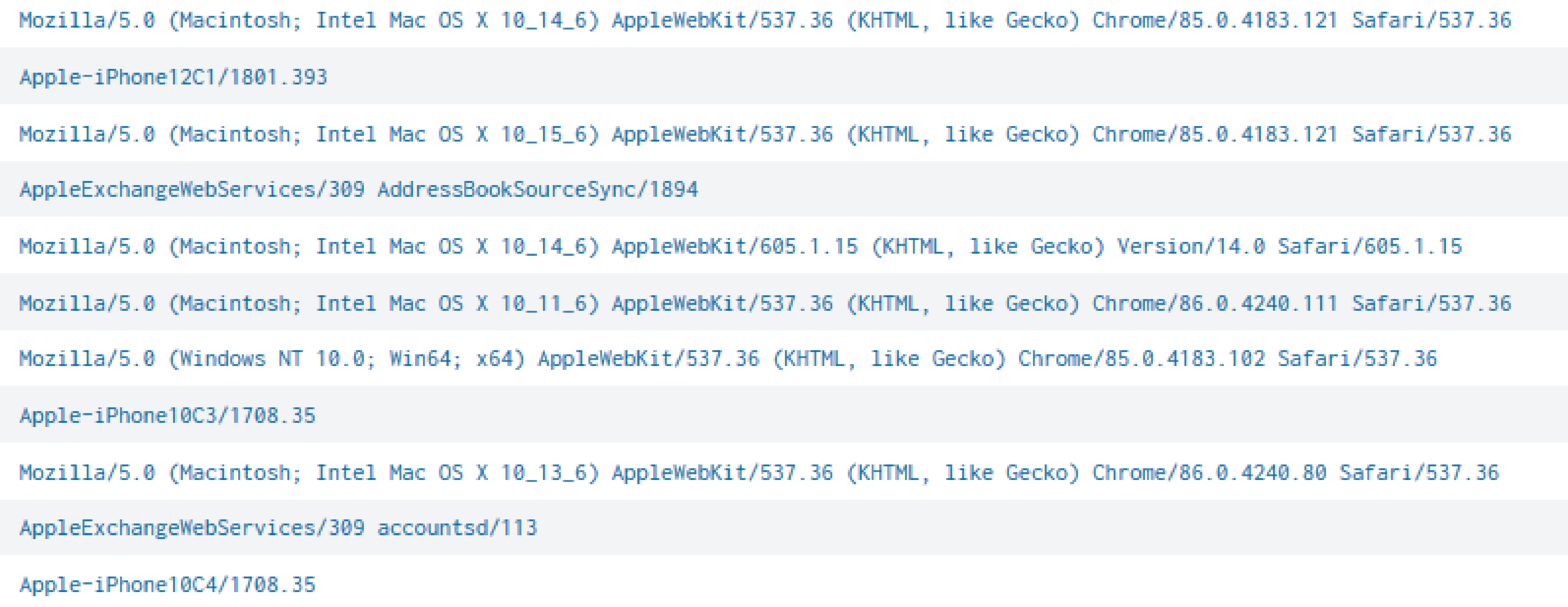


```
ClientIP: [redacted]
ClientIPAddress: [redacted]
ClientInfoString: Client=MSExchangeRPC
ClientProcessName: OUTLOOK.EXE
ClientVersion: 16.0.5032.1000
CreationTime: 2020-10-29T20:21:20
```



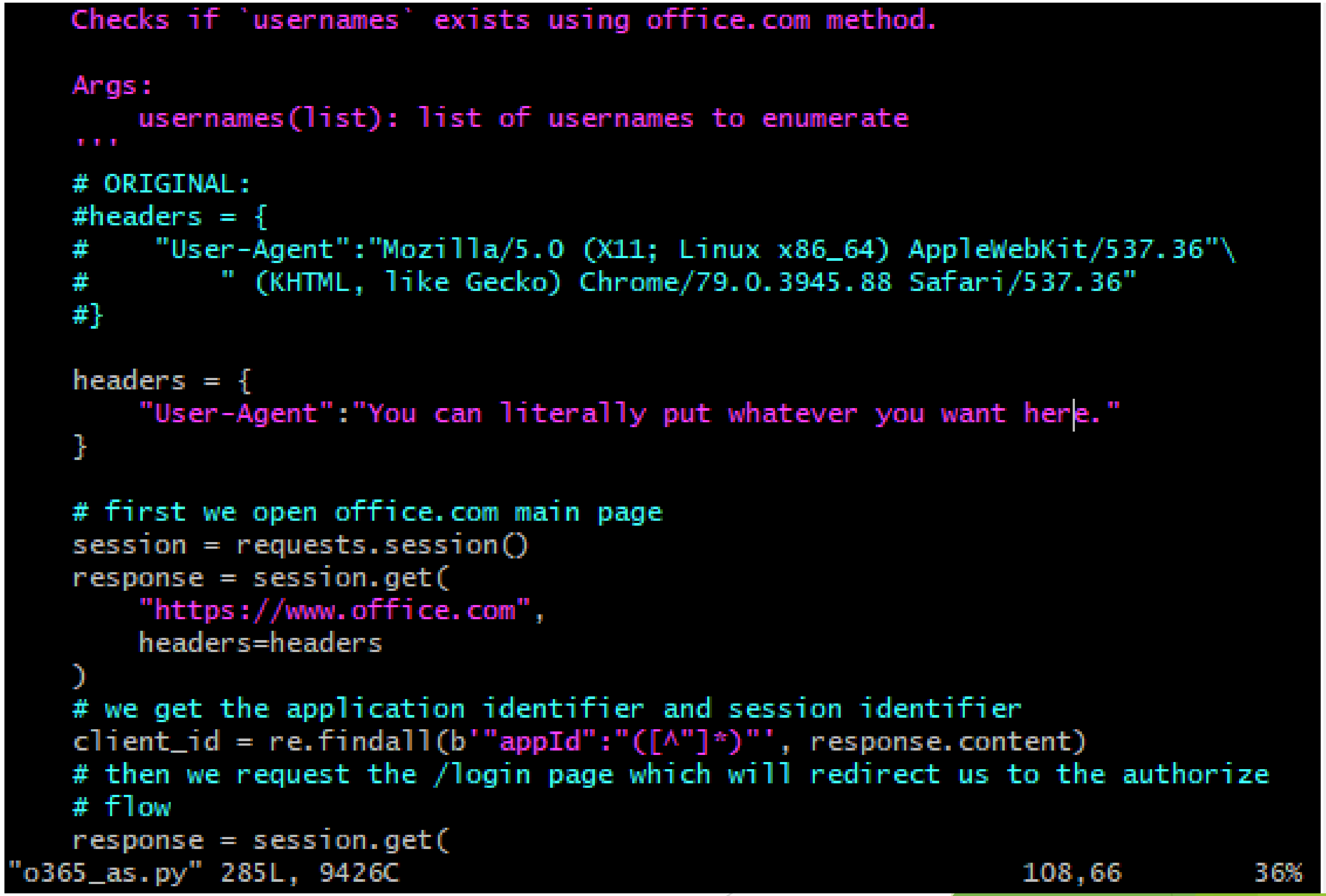
```
RecordType: 3
ResultStatus: Succeeded
UserId: [redacted]
UserKey: 1003BFFD[redacted]
UserType: 0
Version: 1
Workload: Exchange
```

UserAgent / ClientInfoString



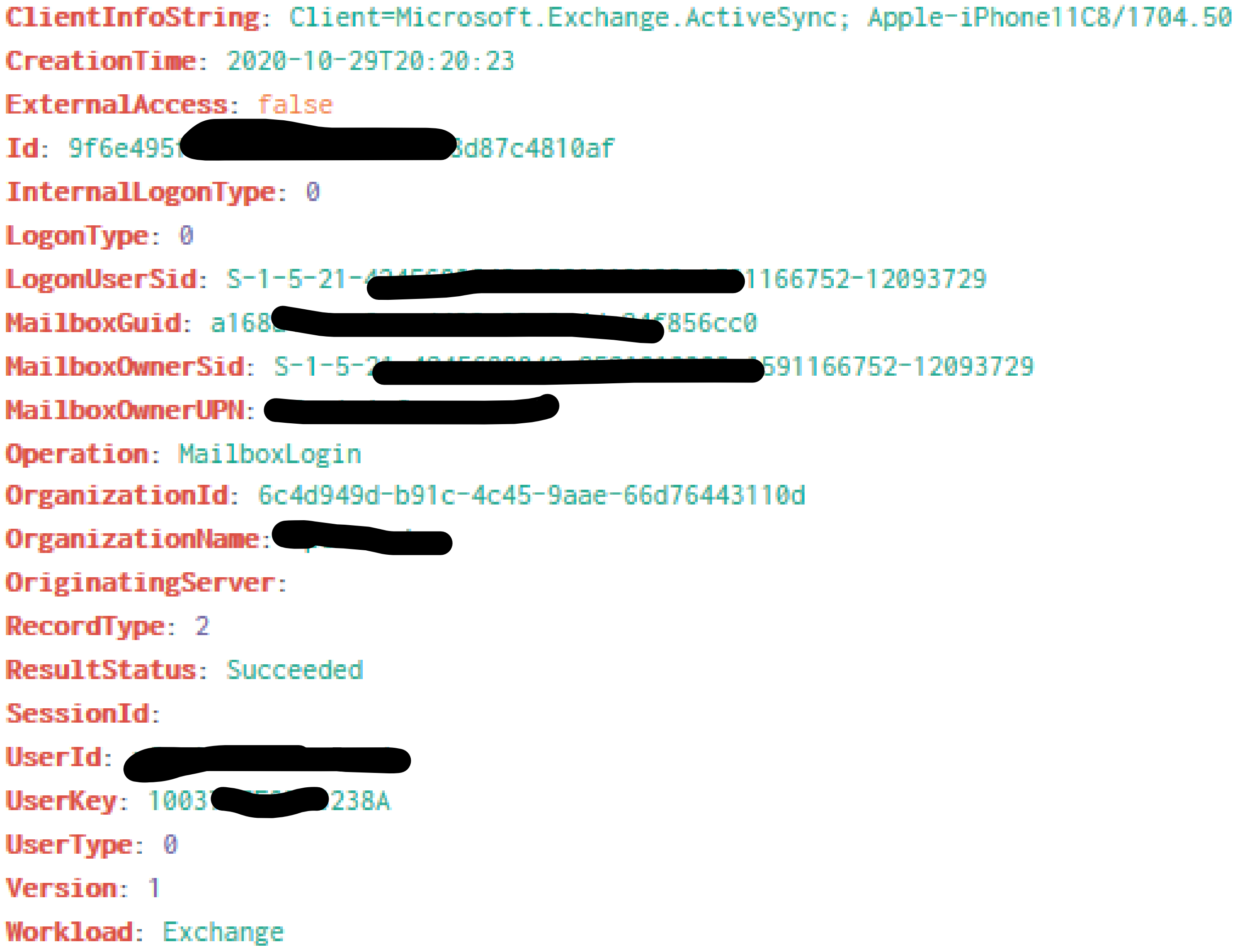
```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36
Apple-iPhone12C1/1801.393
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36
AppleExchangeWebServices/309 AddressBookSourceSync/1894
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36
Apple-iPhone10C3/1708.35
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.80 Safari/537.36
AppleExchangeWebServices/309 accountsd/113
Apple-iPhone10C4/1708.35
```

User Agent is not 100% accurate…



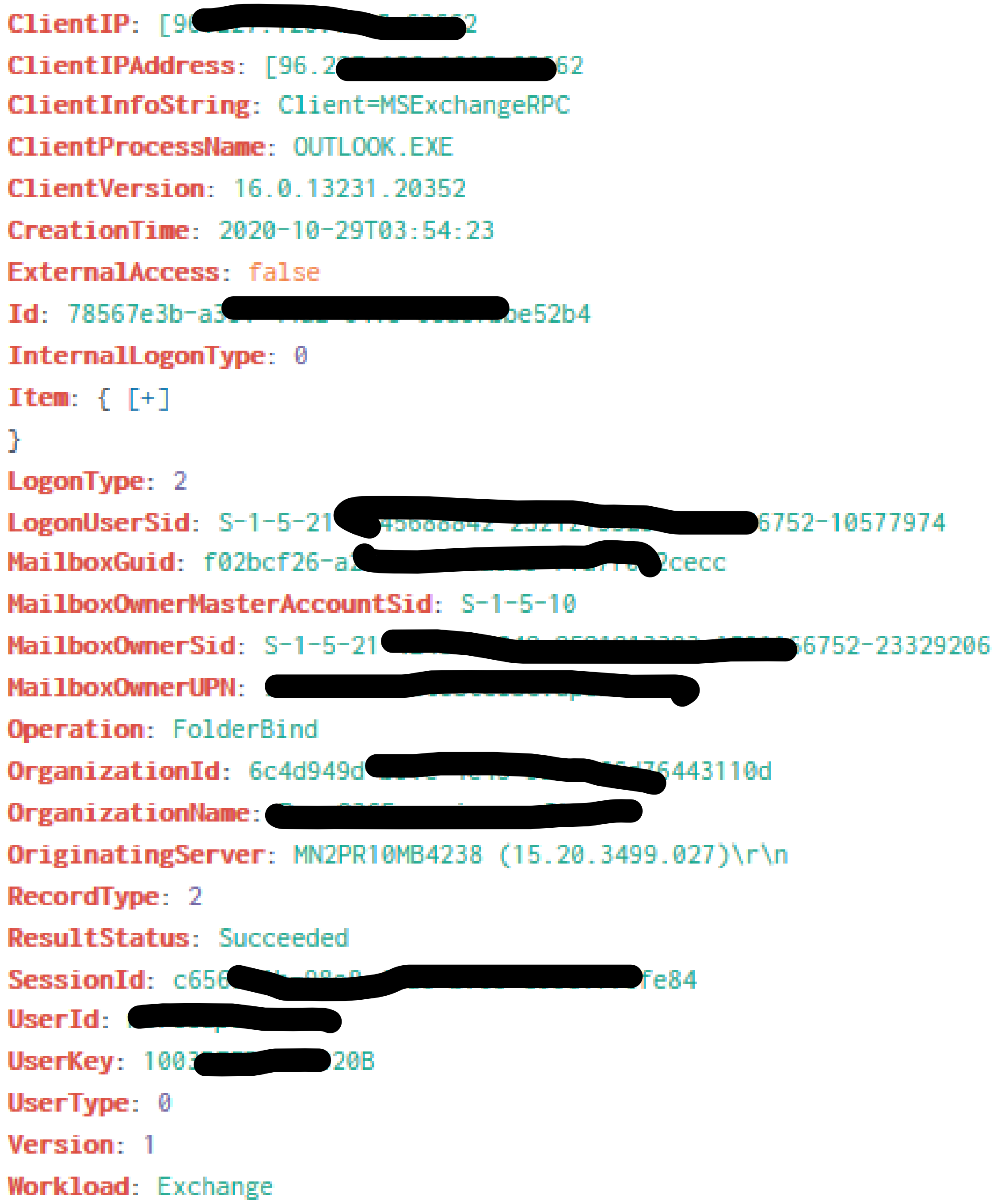
```
    Checks if `usernames` exists using office.com method.

    Args:
        usernames(list): list of usernames to enumerate
    '''
    # ORIGINAL:
    #headers = {
    #    "User-Agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36"\
    #        " (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36"
    #}

    headers = {
        "User-Agent":"You can literally put whatever you want here."
    }

    # first we open office.com main page
    session = requests.session()
    response = session.get(
        "https://www.office.com",
        headers=headers
    )
    # we get the application identifier and session identifier
    client_id = re.findall(b'"appId":"([^"]*)"', response.content)
    # then we request the /login page which will redirect us to the authorize
    # flow
    response = session.get(
"o365_as.py" 285L, 9426C                                      108,66        36%
```

ActiveSync w/ Basic Auth



```
ClientInfoString: Client=Microsoft.Exchange.ActiveSync; Apple-iPhone11C8/1704.50
CreationTime: 2020-10-29T20:20:23
ExternalAccess: false
Id: 9f6e495[redacted]d87c4810af
InternalLogonType: 0
LogonType: 0
LogonUserSid: S-1-5-21-[redacted]1166752-12093729
MailboxGuid: a168[redacted]f856cc0
MailboxOwnerSid: S-1-5-2[redacted]591166752-12093729
MailboxOwnerUPN: [redacted]
Operation: MailboxLogin
OrganizationId: 6c4d949d-b91c-4c45-9aae-66d76443110d
OrganizationName: [redacted]
OriginatingServer:
RecordType: 2
ResultStatus: Succeeded
SessionId:
UserId: [redacted]
UserKey: 1003[redacted]238A
UserType: 0
Version: 1
Workload: Exchange
```

Delegation



```
ClientIP: [9[redacted]2
ClientIPAddress: [96.2[redacted]62
ClientInfoString: Client=MSExchangeRPC
ClientProcessName: OUTLOOK.EXE
ClientVersion: 16.0.13231.20352
CreationTime: 2020-10-29T03:54:23
ExternalAccess: false
Id: 78567e3b-a3[redacted]be52b4
InternalLogonType: 0
Item: { [+]
}
LogonType: 2
LogonUserSid: S-1-5-21[redacted]6752-10577974
MailboxGuid: f02bcf26-a[redacted]cecc
MailboxOwnerMasterAccountSid: S-1-5-10
MailboxOwnerSid: S-1-5-21[redacted]6752-23329206
MailboxOwnerUPN: [redacted]
Operation: FolderBind
OrganizationId: 6c4d949d[redacted]6443110d
OrganizationName: [redacted]
OriginatingServer: MN2PR10MB4238 (15.20.3499.027)\r\n
RecordType: 2
ResultStatus: Succeeded
SessionId: c656[redacted]fe84
UserId: [redacted]
UserKey: 1003[redacted]20B
UserType: 0
Version: 1
Workload: Exchange
```

Legacy vs. Modern Auth

- Legacy is repeated authentications
- Modern auth starts with initial auth, but refresh tokens are used
  - These may not be in the logs
- 2-Step may look confusing:
  - Portal shows result as auth, “Interrupted” for security challenge, then “Success”