Man in th Middle

Team 5

B073040047 Chih-Hsuan Yang[1]
M093040096 Tian-Lang Li
M093040094 Wen-Tao Wang

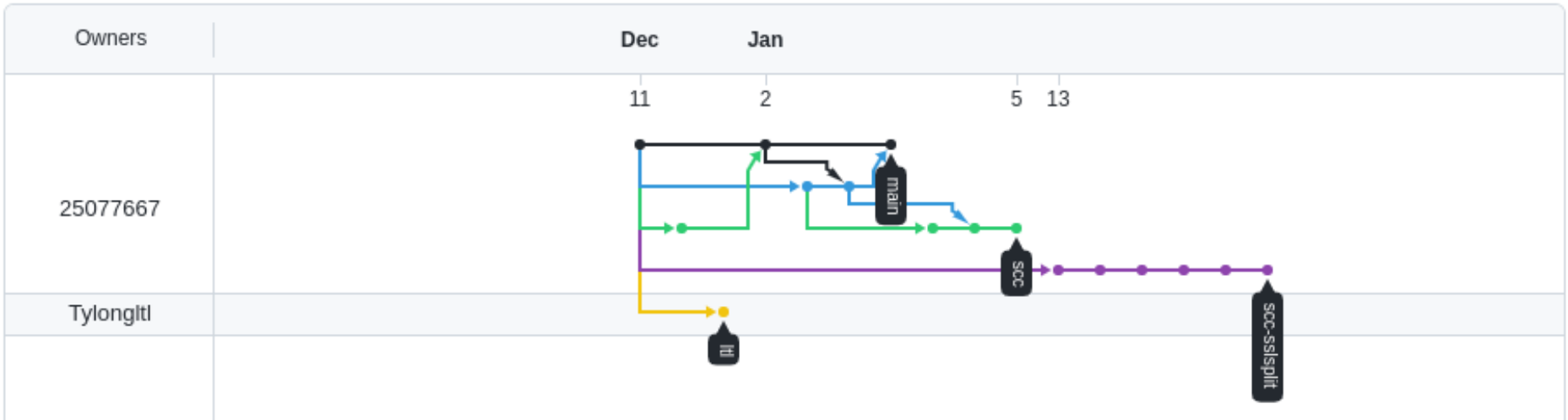
January 14, 2022

Open Source

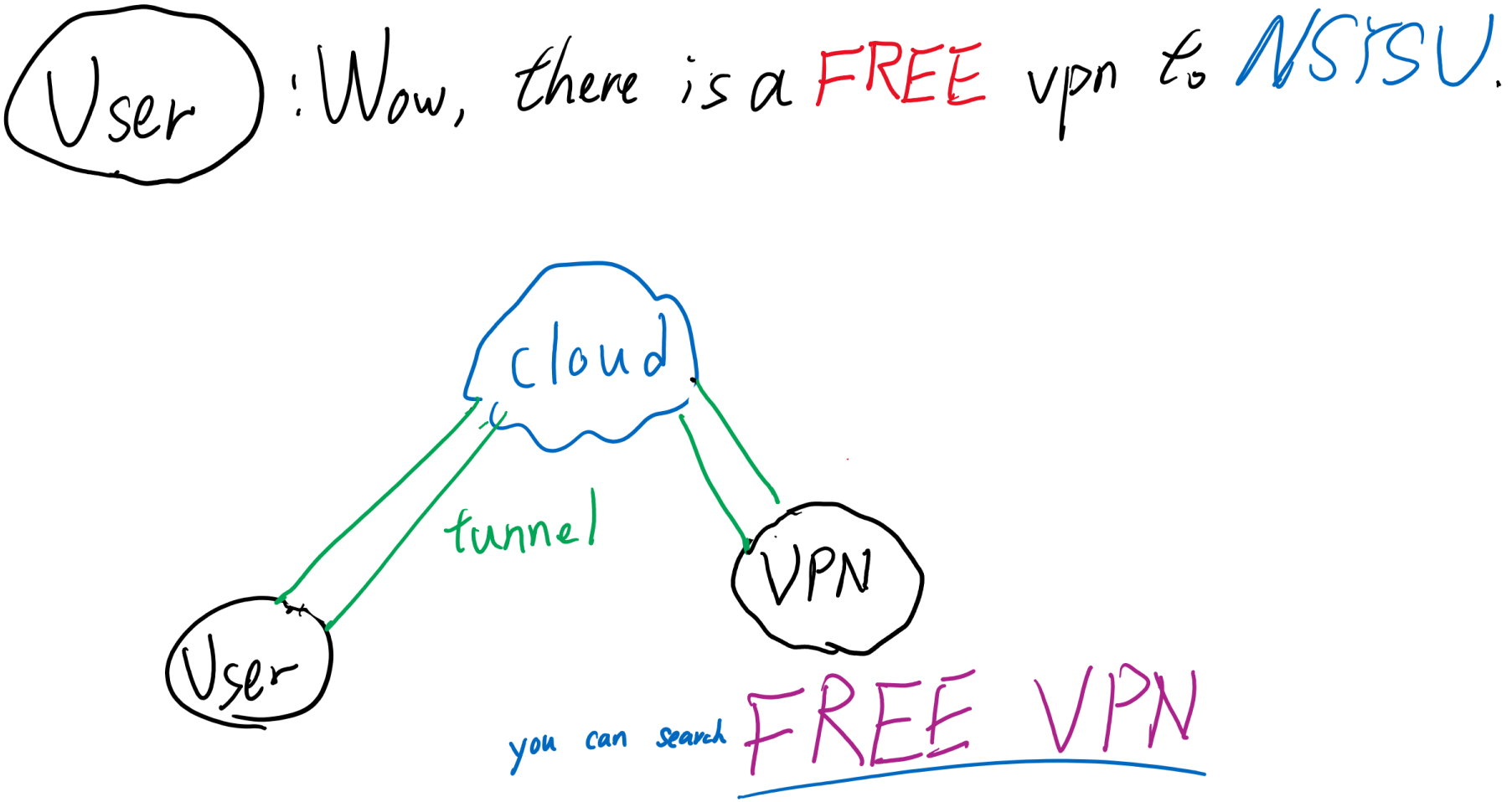
GitHub repository

Network graph

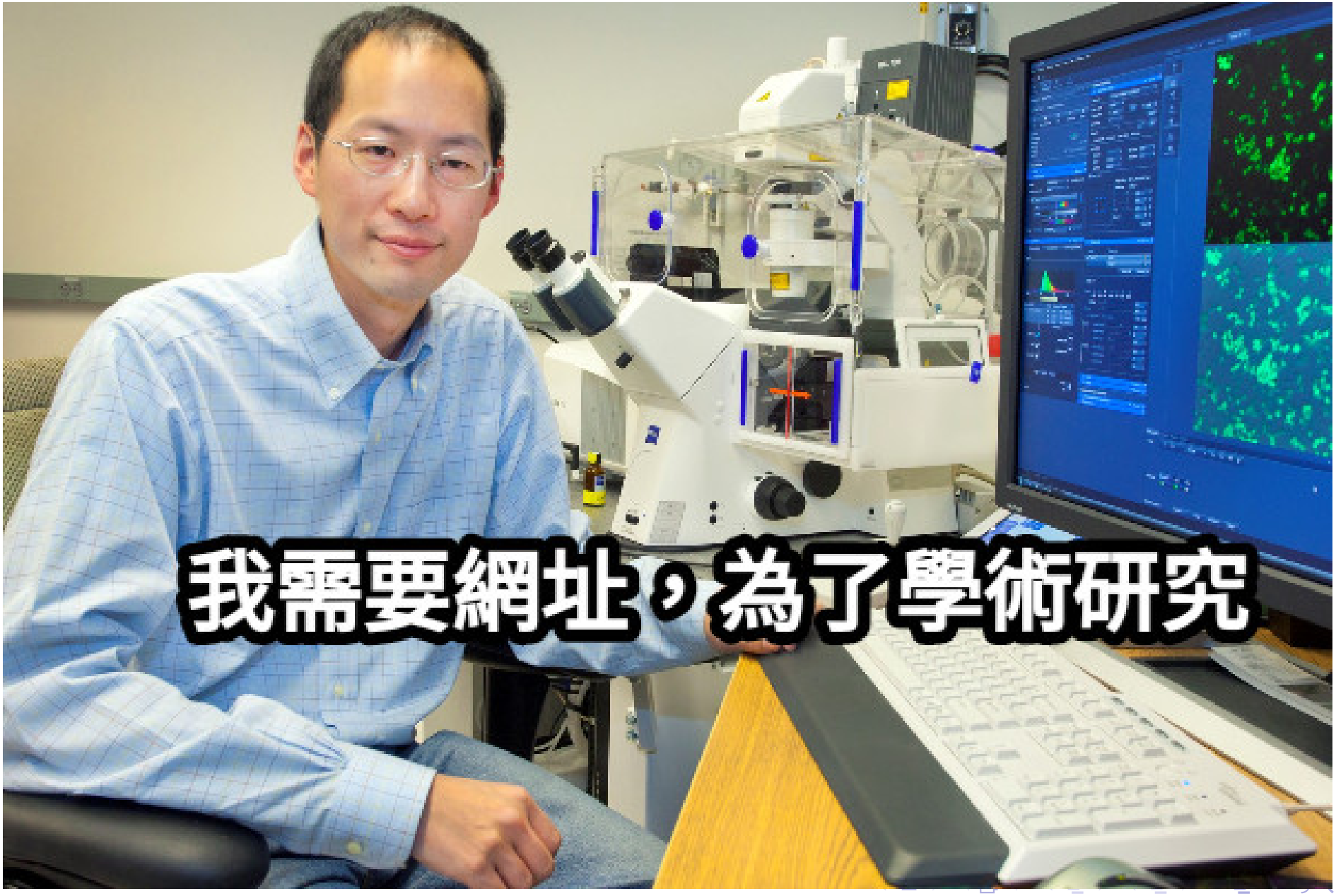
Timeline of the most recent commits to this repository and its network ordered by most recently pushed to.



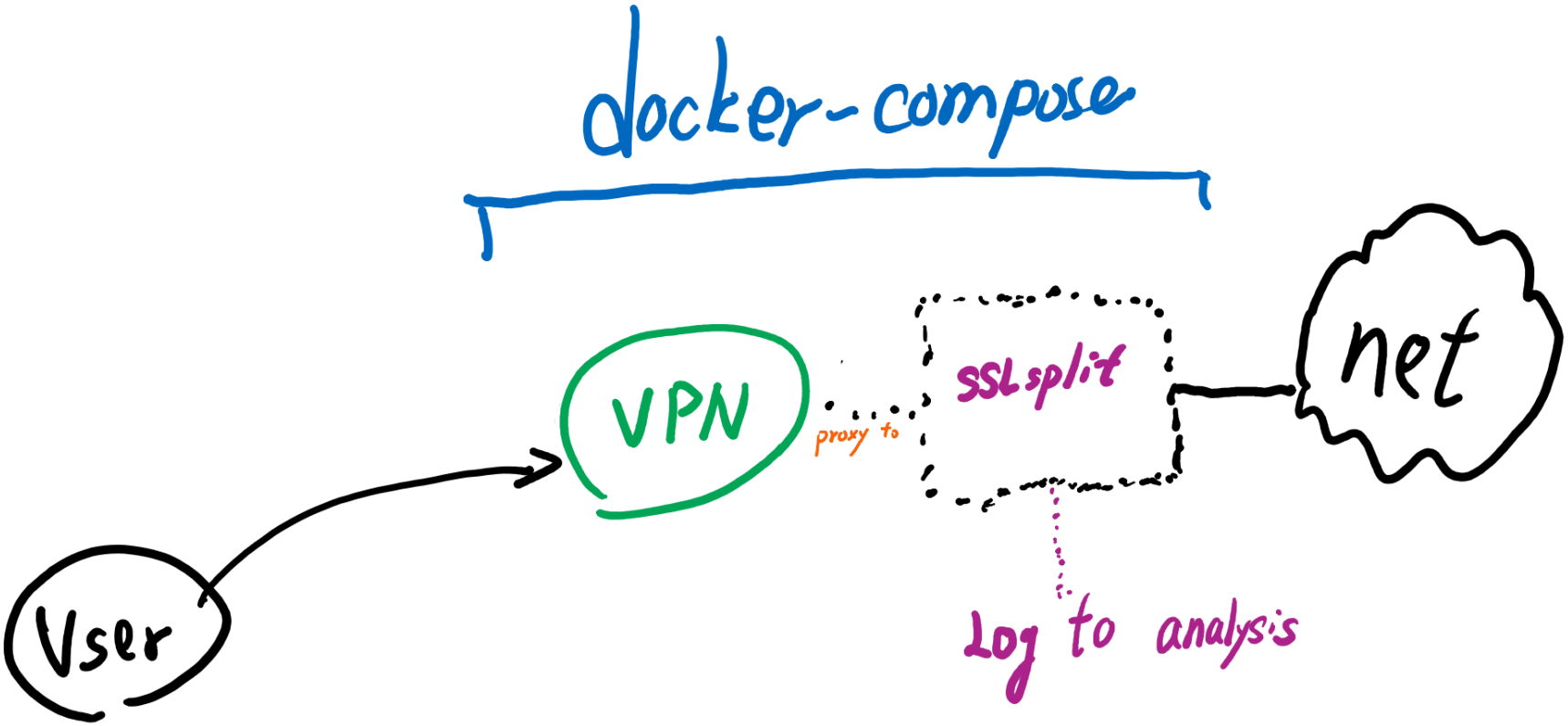
Scenario


User
: Wow, there is a FREE vpn to NSYSU.
cloud
tunnel
VPN
User
you can search FREE VPN

Scenario



Architecture



Video Records

Vulnerabilities

```
48      var pwdmask = "**********************************";
49      /* NSYSU@Cs begin @p@@K@X@[@K@覜(@]@@@@@@@@@s@K@X, @@@ي|@€@@}) */
50      // var md5key  = MD5(node.password.value);
51      // var cypkey  = md5key.substr(0,4) + node.login_key.value.substr(0,4);
52      var cypkey = node.login_key.value.substr(0,8);
53      /* NSYSU@Cs begin end */
54      node.encrypt_pwd.value = stringToBase64(des(cypkey, node.password.value, 1));
55      node.password.value    = pwdmask.substr(0,node.password.value.length);
56
57      return true;
```

```
<form method="post" action="/login.php" id="loginForm" name="loginForm" onsubmit="return formSubmit();" autocomplete="off">
  <input type="hidden" name="reurl" value>
  <input type="hidden" name="login_key" value="3041aad0ed4a952bf8e4501c1291188">
  <input type="hidden" name="encrypt_pwd" value>
  <div id="loginBlockContainer">…</div> == $0
</form>
```

Extra - CTF

- login_key: 3041aad0ed4a952bf8e4501c1291188
- encrypt_pwd: SQNsTh2hn82RYnDMkn/7u3blVO+u62p4

Hint

$F = base_{64}^{-1}$
$G = DES^{-1}(3041aad0ed4a952bf8e4501c1291188)$
Flag: $G \circ F(encrypt\_pwd)$

Future

DNS pollution

Hack you in silence

Solution: Certificate pinning