Anonymous network

«Hidden Lake»

Kovalenko Gennady Alexandrovich

«**Hidden Lake**» (HL) is a decentralized anonymous F2F (Friend-to-Friend) network with queue-theoretic provability (QB-problem)

F2F

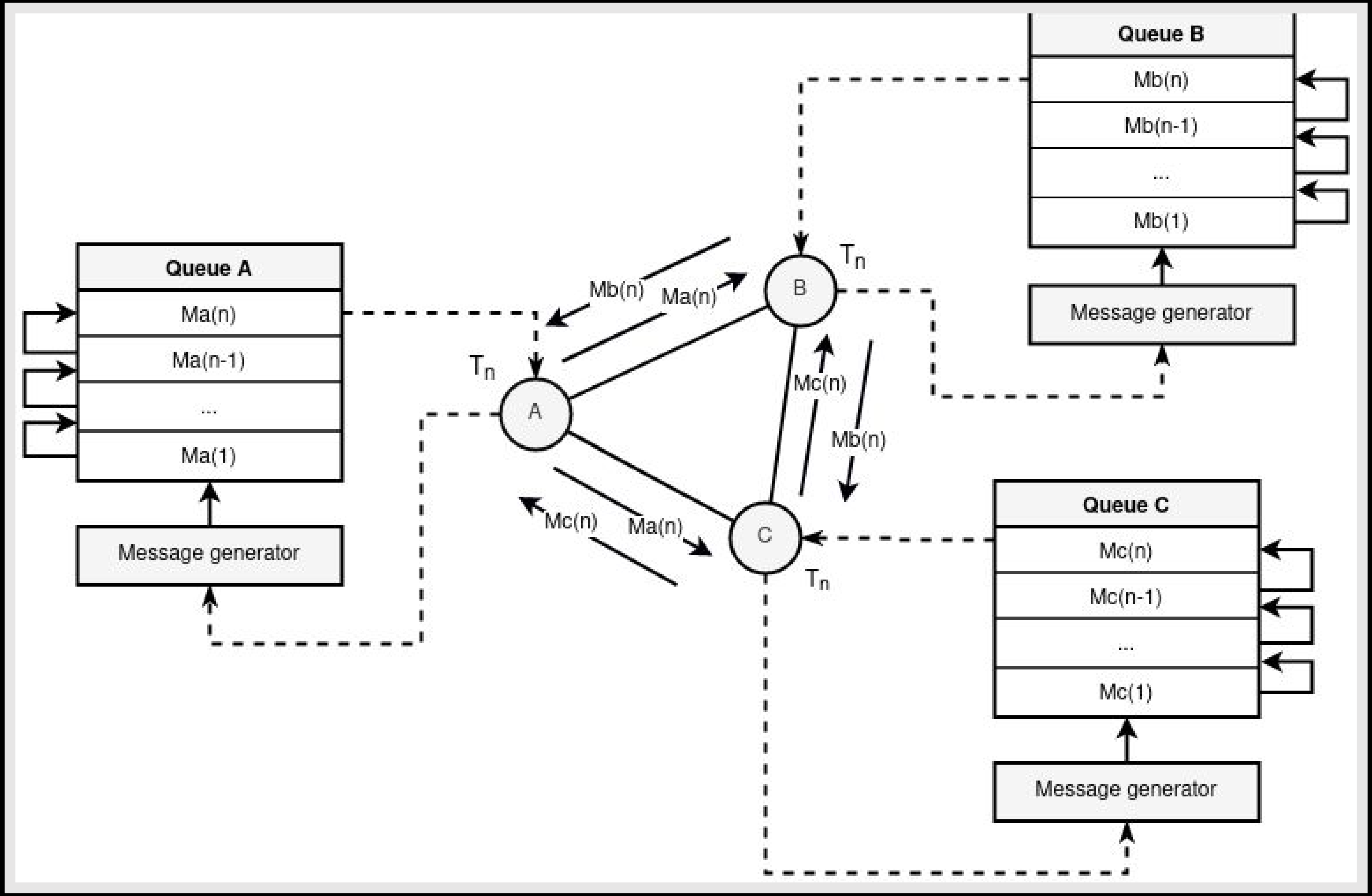
"Hidden Lake" is**Friend-to-Friend**network. This property defines a specific type of connection of participants in the system by manually setting the list of friends

Queue-based task (QB task)

in simple words

1. Each message is encrypted with the recipient's key.,
2. The message is sent during the period $= \mathbf{T}$ to all network participants,
3. Period $\mathbf{T}$ one participant is independent of periods $\mathbf{T_1, T_2, \ldots, T_n}$ other participants,
4. Iffor the period $\mathbf{T}$ messagesdoes not exist, then a false message is sent to the network without a recipient,
5. Each participant tries to decrypt the message received from the network.

Queue-based task (QB task)



Queue-based task (QB task)

formal language

System:

$QB\text{-}net = \Sigma^{n}_{i=1}(T = \{t_i\}, K = \{k_i\}, C = \{(c \in \{E_{kj}(m), E_r(v)\}) \leftarrow {}^{ti}Qi\})$

States:

1. $Q \leftarrow (c= E_{ki}(m))$, where $k_i \in K$, $c \in C$,

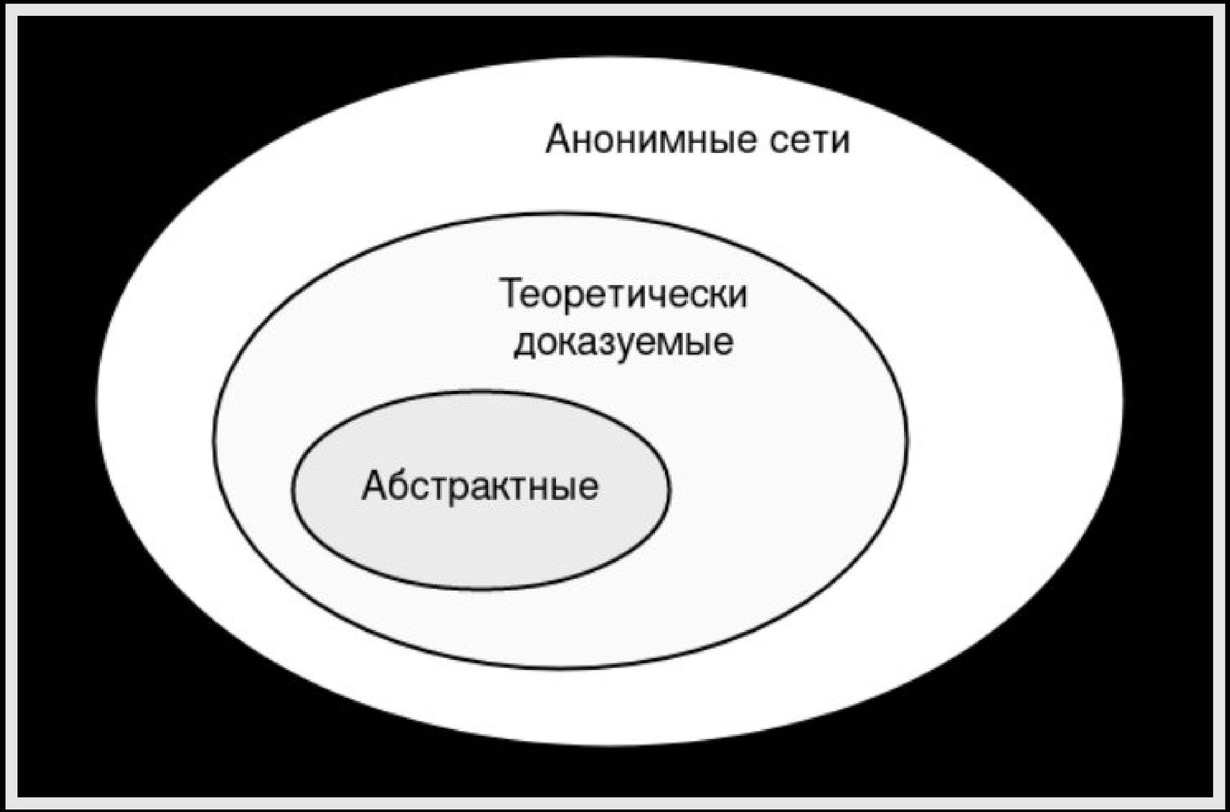
2. $(c= E_{ki}(m)) \leftarrow {}^{t}Q$ if $Q \neq Ø$, where $t \in T, k_i \in K$, $c \in C$,

3. $(c= E_r(v)) \leftarrow {}^{t}Q$ if $Q= Ø$, where $t \in T, r \notin K$, $c \in C$,

4. $m' = D_k^{-1}(c)$, wherec$\in C$

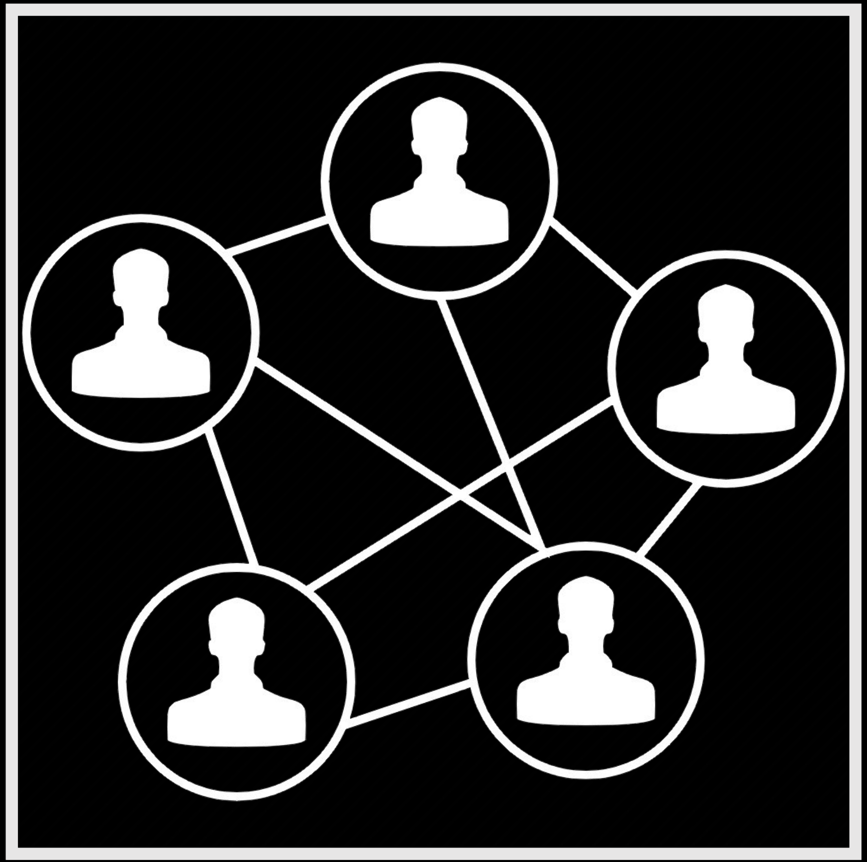
Comparison with other anonymization tasks

	QB	E.I.	DC	Onion	Proxy
Theoretical provability	+	+	+	-	-
Cumulative effect of anonymity	-	+	-	-	-
Information polymorphism	-	+	+	+	-
Probabilistic Routing	-	+	-	+/-	+/-
Frequency of message generation	+/-	-	+	-	-
Independence of anonymity from connections	+	-	-	-	-
Easy to scale	-	-	-	+	+
Simplicity of software implementation	+	-	-	+	+
Stage of anonymity	5^	6	1^	4 or 6	3
Representative network	Hidden Lake		Herbivore	Tor	Crowds



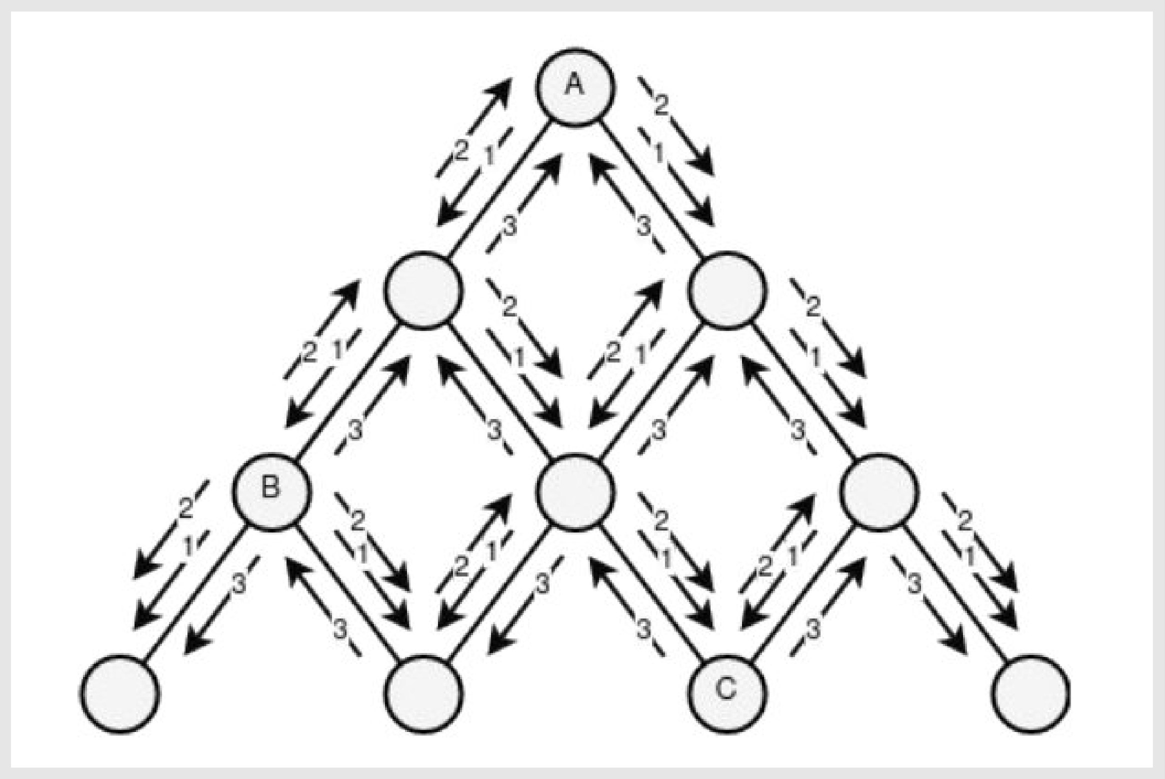
"Hidden Lake" refers to**abstract**anonymous networks that do not care about criteria such as:

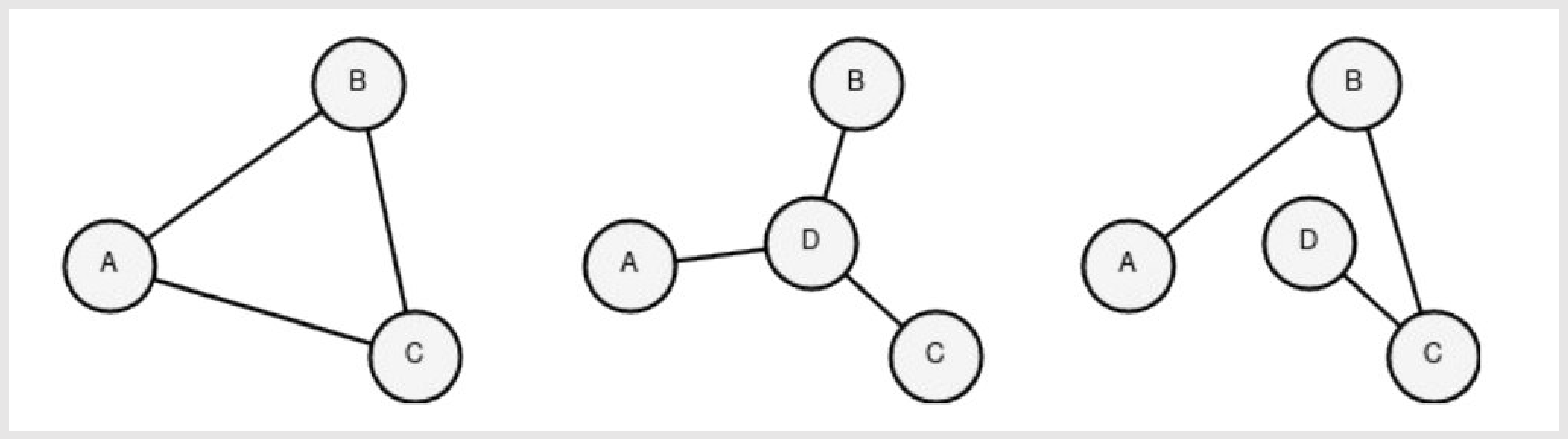
1. level of centralization
2. number of nodes
3. arrangement of nodes
4. communication between nodes



Due to its abstract nature, the Hidden Lake network is capable ofto form**secret communication channels**with anonymizing properties even within centralized services

The main disadvantage of the network is**llinear load**on a system dependent on the number of participants



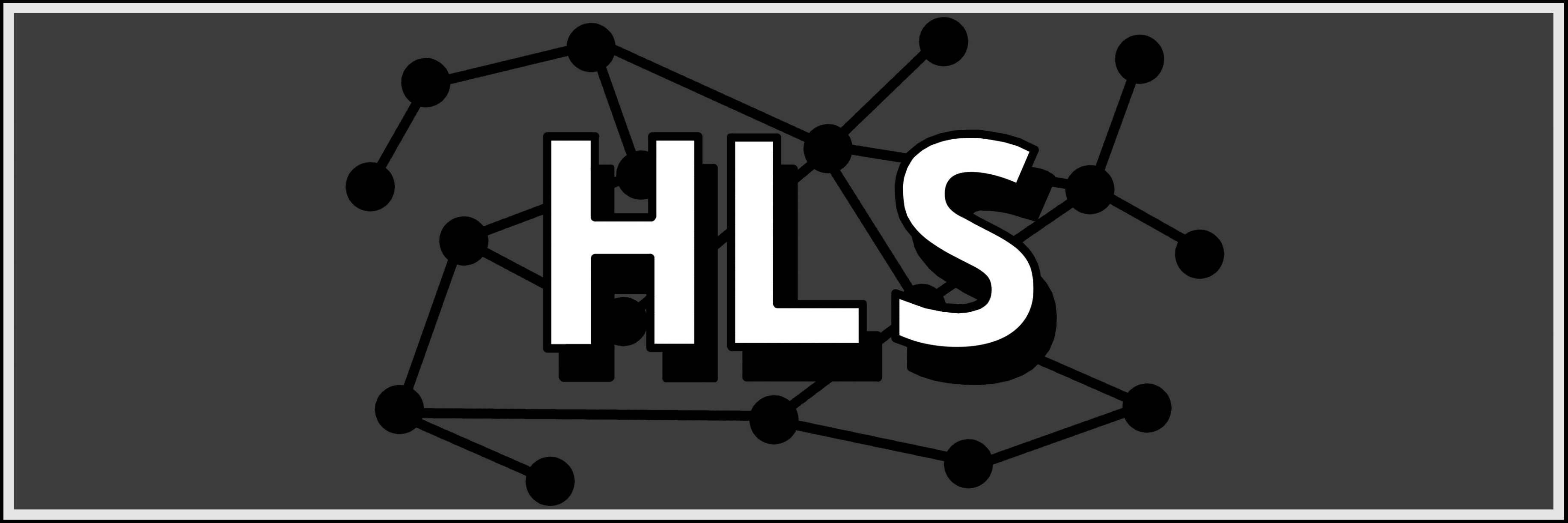


A partial solution to the linear load problem was the creation ofisolated from each other **"small lakes"**(networks)through application**network key**

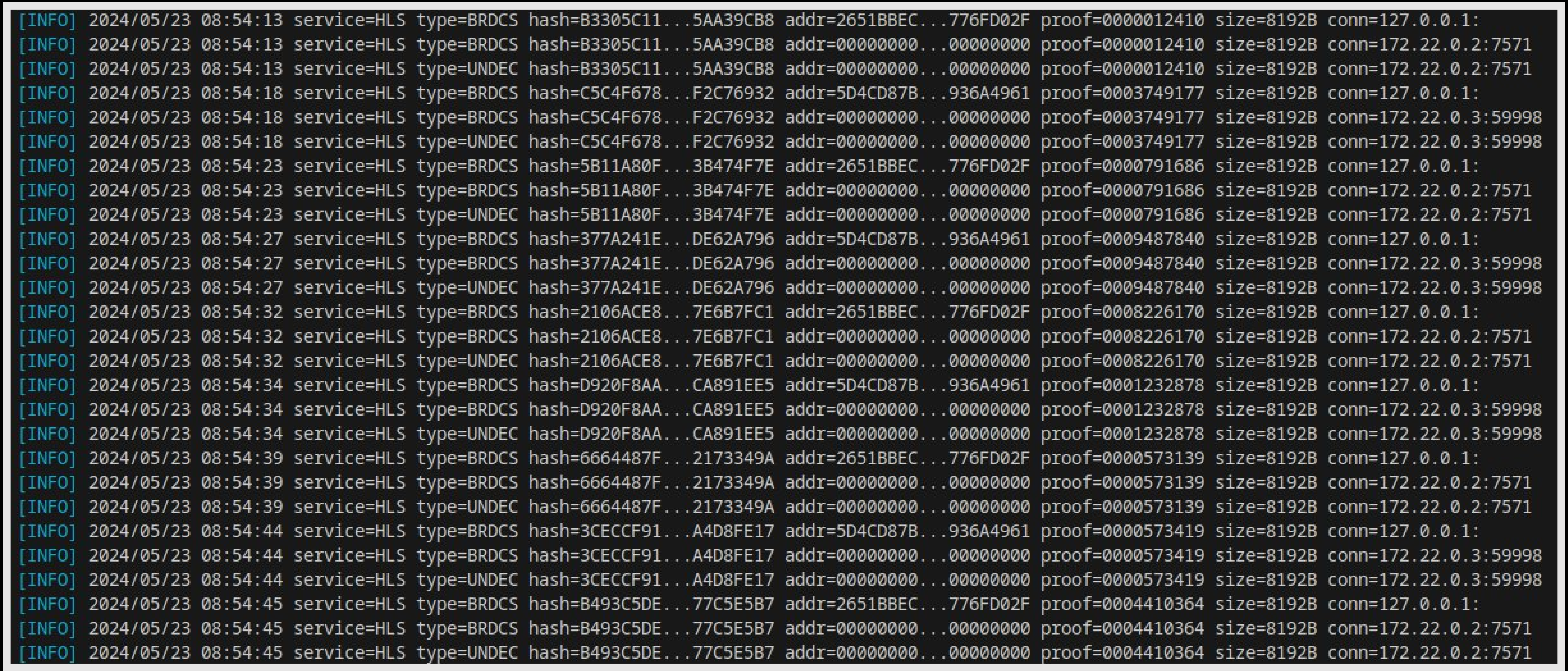
Development Philosophy networks«Hidden Lake» is based on**microservice**architecture

- At the moment there is7 services, where one**basic**service - HLS, three**applied**services - HLM, HLF, HLR, three**auxiliary**service - HLT, HLE, HLL
- There may also be specific services in the Hidden Lake network description -**adapters**, referred to as HLA. They perform the role of "implanting" anonymized traffic into a foreign system

HLS (Hidden Lake Service) —**core**anonymous network. Represents**API**for sending/receiving messages over anonymizing traffic



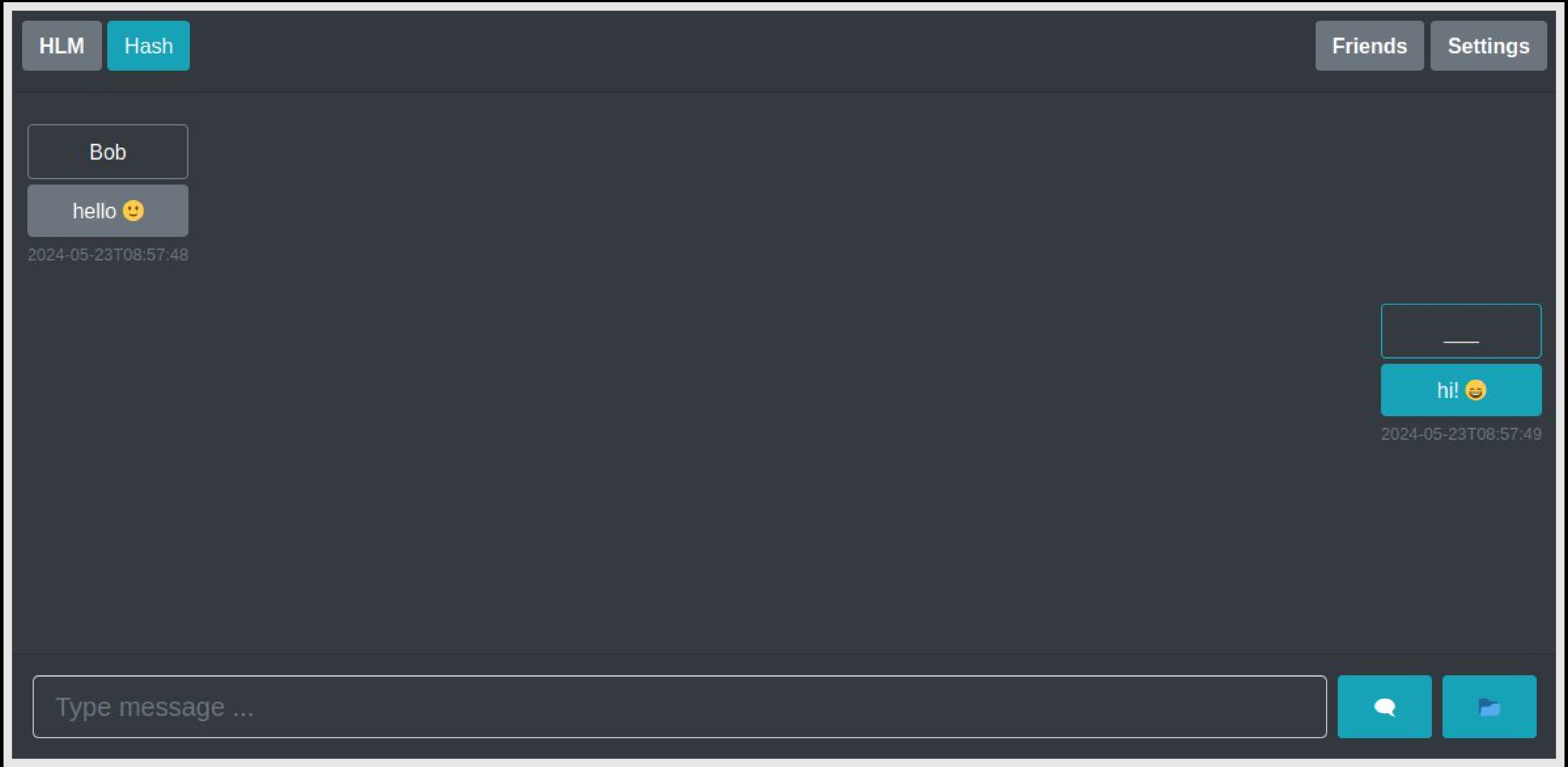
Generating Anonymized Traffic in HLS Application



```
[INFO] 2024/05/23 08:54:13 service=HLS type=BRDCS hash=B3305C11...5AA39CB8 addr=2651BBEC...776FD02F proof=0000012410 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:13 service=HLS type=BRDCS hash=B3305C11...5AA39CB8 addr=00000000...00000000 proof=0000012410 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:13 service=HLS type=UNDEC hash=B3305C11...5AA39CB8 addr=00000000...00000000 proof=0000012410 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:18 service=HLS type=BRDCS hash=C5C4F678...F2C76932 addr=5D4CD87B...936A4961 proof=0003749177 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:18 service=HLS type=BRDCS hash=C5C4F678...F2C76932 addr=00000000...00000000 proof=0003749177 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:18 service=HLS type=UNDEC hash=C5C4F678...F2C76932 addr=00000000...00000000 proof=0003749177 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:23 service=HLS type=BRDCS hash=5B11A80F...3B474F7E addr=2651BBEC...776FD02F proof=0000791686 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:23 service=HLS type=BRDCS hash=5B11A80F...3B474F7E addr=00000000...00000000 proof=0000791686 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:23 service=HLS type=UNDEC hash=5B11A80F...3B474F7E addr=00000000...00000000 proof=0000791686 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:27 service=HLS type=BRDCS hash=377A241E...DE62A796 addr=5D4CD87B...936A4961 proof=0009487840 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:27 service=HLS type=BRDCS hash=377A241E...DE62A796 addr=00000000...00000000 proof=0009487840 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:27 service=HLS type=UNDEC hash=377A241E...DE62A796 addr=00000000...00000000 proof=0009487840 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:32 service=HLS type=BRDCS hash=2106ACE8...7E6B7FC1 addr=2651BBEC...776FD02F proof=0008226170 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:32 service=HLS type=BRDCS hash=2106ACE8...7E6B7FC1 addr=00000000...00000000 proof=0008226170 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:32 service=HLS type=UNDEC hash=2106ACE8...7E6B7FC1 addr=00000000...00000000 proof=0008226170 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:34 service=HLS type=BRDCS hash=D920F8AA...CA891EE5 addr=5D4CD87B...936A4961 proof=0001232878 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:34 service=HLS type=BRDCS hash=D920F8AA...CA891EE5 addr=00000000...00000000 proof=0001232878 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:34 service=HLS type=UNDEC hash=D920F8AA...CA891EE5 addr=00000000...00000000 proof=0001232878 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:39 service=HLS type=BRDCS hash=6664487F...2173349A addr=2651BBEC...776FD02F proof=0000573139 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:39 service=HLS type=BRDCS hash=6664487F...2173349A addr=00000000...00000000 proof=0000573139 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:39 service=HLS type=UNDEC hash=6664487F...2173349A addr=00000000...00000000 proof=0000573139 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:44 service=HLS type=BRDCS hash=3CECCF91...A4D8FE17 addr=5D4CD87B...936A4961 proof=0000573419 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:44 service=HLS type=BRDCS hash=3CECCF91...A4D8FE17 addr=00000000...00000000 proof=0000573419 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:44 service=HLS type=UNDEC hash=3CECCF91...A4D8FE17 addr=00000000...00000000 proof=0000573419 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:45 service=HLS type=BRDCS hash=B493C5DE...77C5E5B7 addr=2651BBEC...776FD02F proof=0004410364 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:45 service=HLS type=BRDCS hash=B493C5DE...77C5E5B7 addr=00000000...00000000 proof=0004410364 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:45 service=HLS type=UNDEC hash=B493C5DE...77C5E5B7 addr=00000000...00000000 proof=0004410364 size=8192B conn=172.22.0.2:7571
```

HLM (Hidden Lake Messenger)
-anonymous**messenger**, calling
HLS functions

Chat interface in HLM application



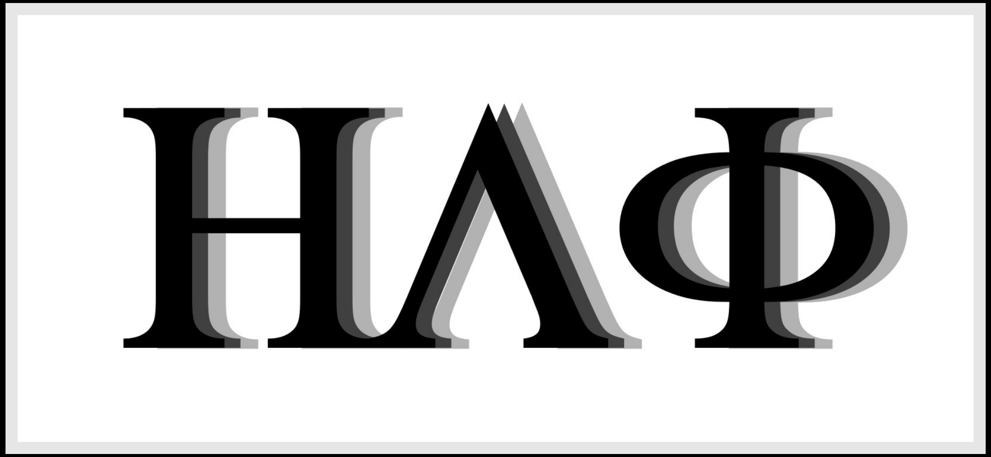
Bob

hello 🙂

2024-05-23T08:57:48

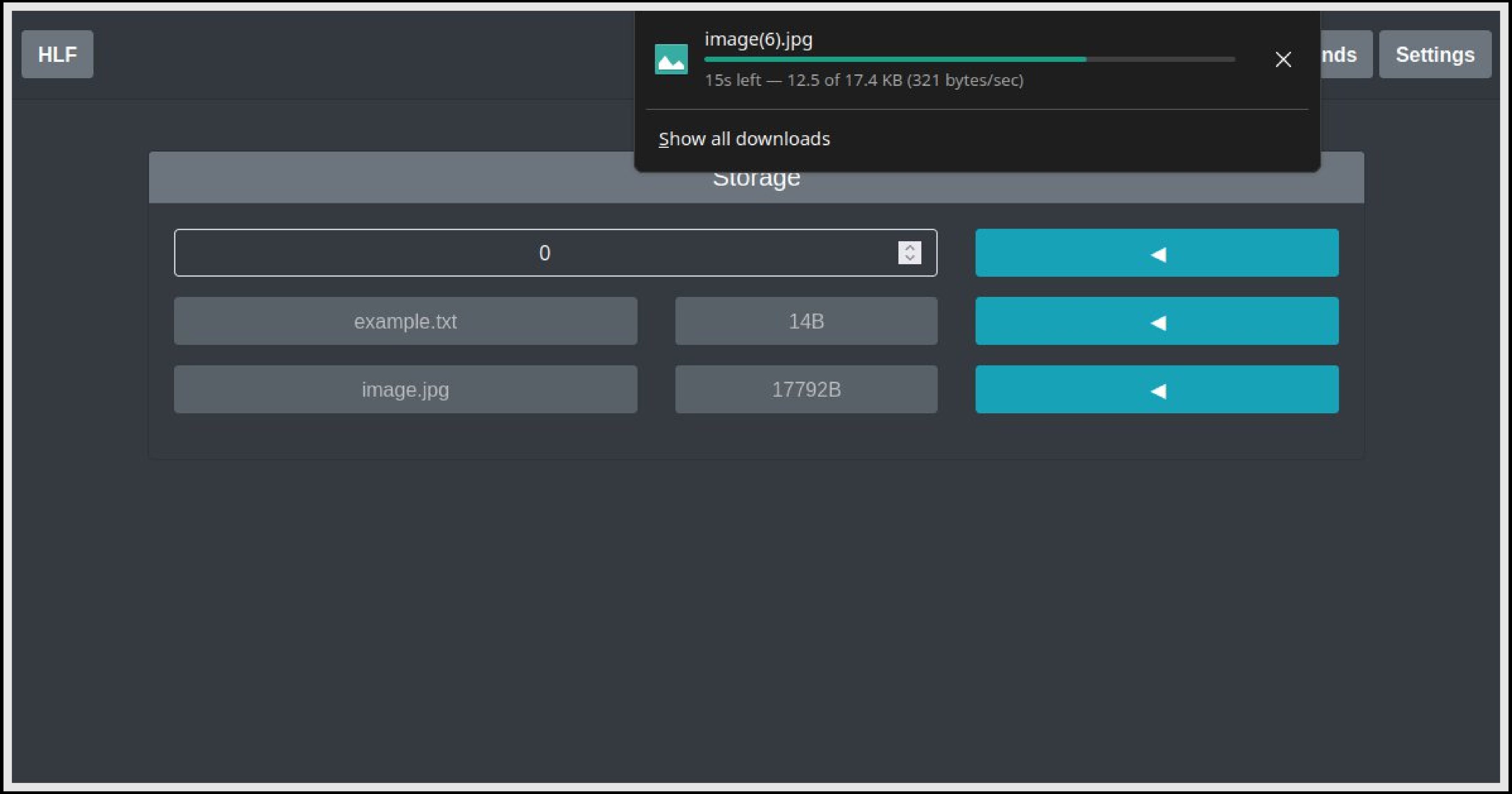
hi! 😄

2024-05-23T08:57:49



HLF (Hidden Lake Filesharer) - anonymous**file sharing**, calling HLS functions

Downloading a file in HLF application



image(6).jpg

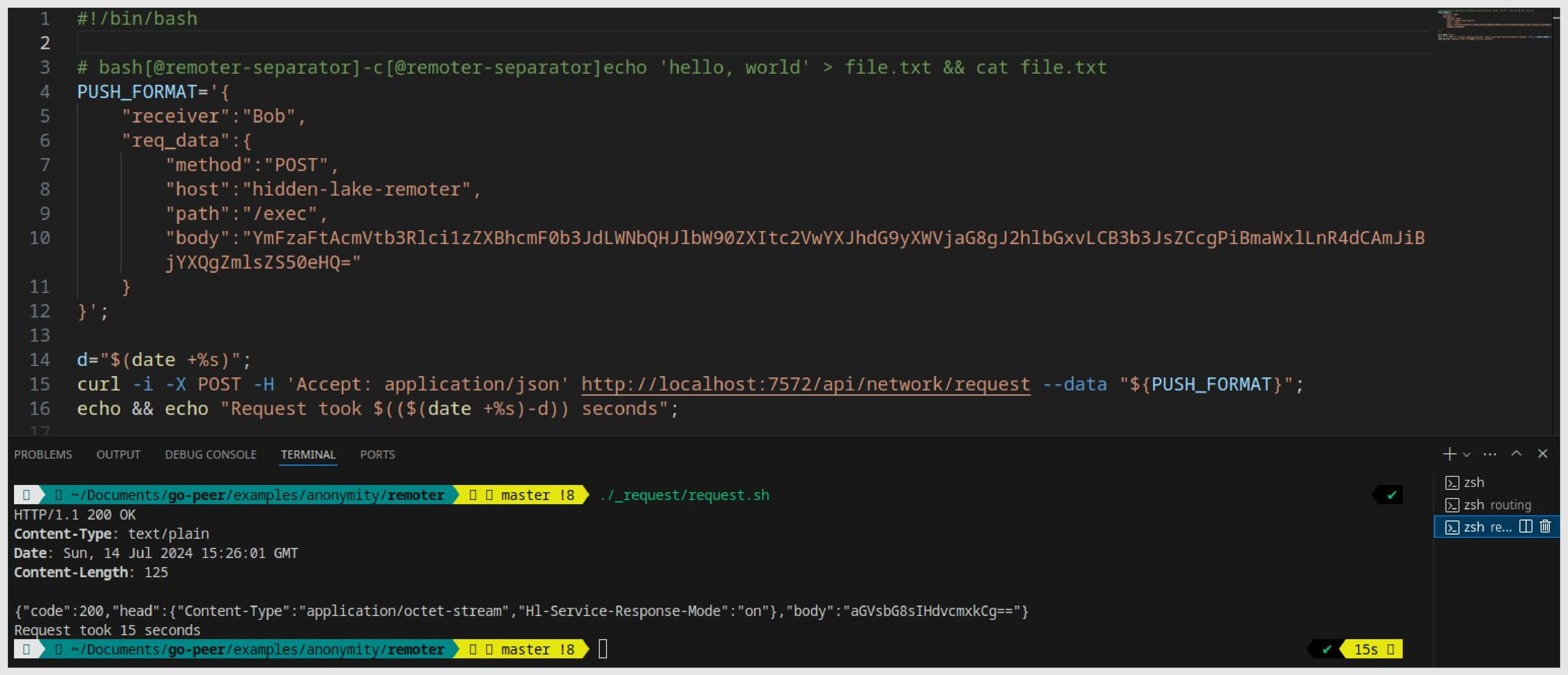
15s left — 12.5 of 17.4 KB (321 bytes/sec)

0		◀
example.txt	14B	◀
image.jpg	17792B	◀

HLR (Hidden Lake Remoter) — anonymous**remote access**, calling HLS functions

HLR

Executing a Remote Command Using HLR



```bash
#!/bin/bash

# bash[@remoter-separator]-c[@remoter-separator]echo 'hello, world' > file.txt && cat file.txt
PUSH_FORMAT='{
    "receiver":"Bob",
    "req_data":{
        "method":"POST",
        "host":"hidden-lake-remoter",
        "path":"/exec",
        "body":"YmFzaFtAcmVtb3Rlci1zZXBhcmF0b3JdLWNbQHJlbW90ZXItc2VwYXJhdG9yXWVjaG8gJ2hlbGxvLCB3b3JsZCcgPiBmaWxlLnR4dCAmJiBjYXQgZmlsZS50eHQ="
    }
}';

d="$(date +%s)";
curl -i -X POST -H 'Accept: application/json' http://localhost:7572/api/network/request --data "${PUSH_FORMAT}";
echo && echo "Request took $(($(date +%s)-d)) seconds";
```

```
~/Documents/go-peer/examples/anonymity/remoter   master !8  ./_request/request.sh
HTTP/1.1 200 OK
Content-Type: text/plain
Date: Sun, 14 Jul 2024 15:26:01 GMT
Content-Length: 125

{"code":200,"head":{"Content-Type":"application/octet-stream","Hl-Service-Response-Mode":"on"},"body":"aGVsbG8sIHdvcmxkCg=="}
Request took 15 seconds
~/Documents/go-peer/examples/anonymity/remoter   master !8                    ✓ 15s
```

HLT

HLT (Hidden Lake Traffic) — **distributor**traffic in an anonymous network. Can act as a relay and storage of traffic

HLE (Hidden Lake Encryptor) - service**encryption**Anddecryptionmessages format**go-peer**

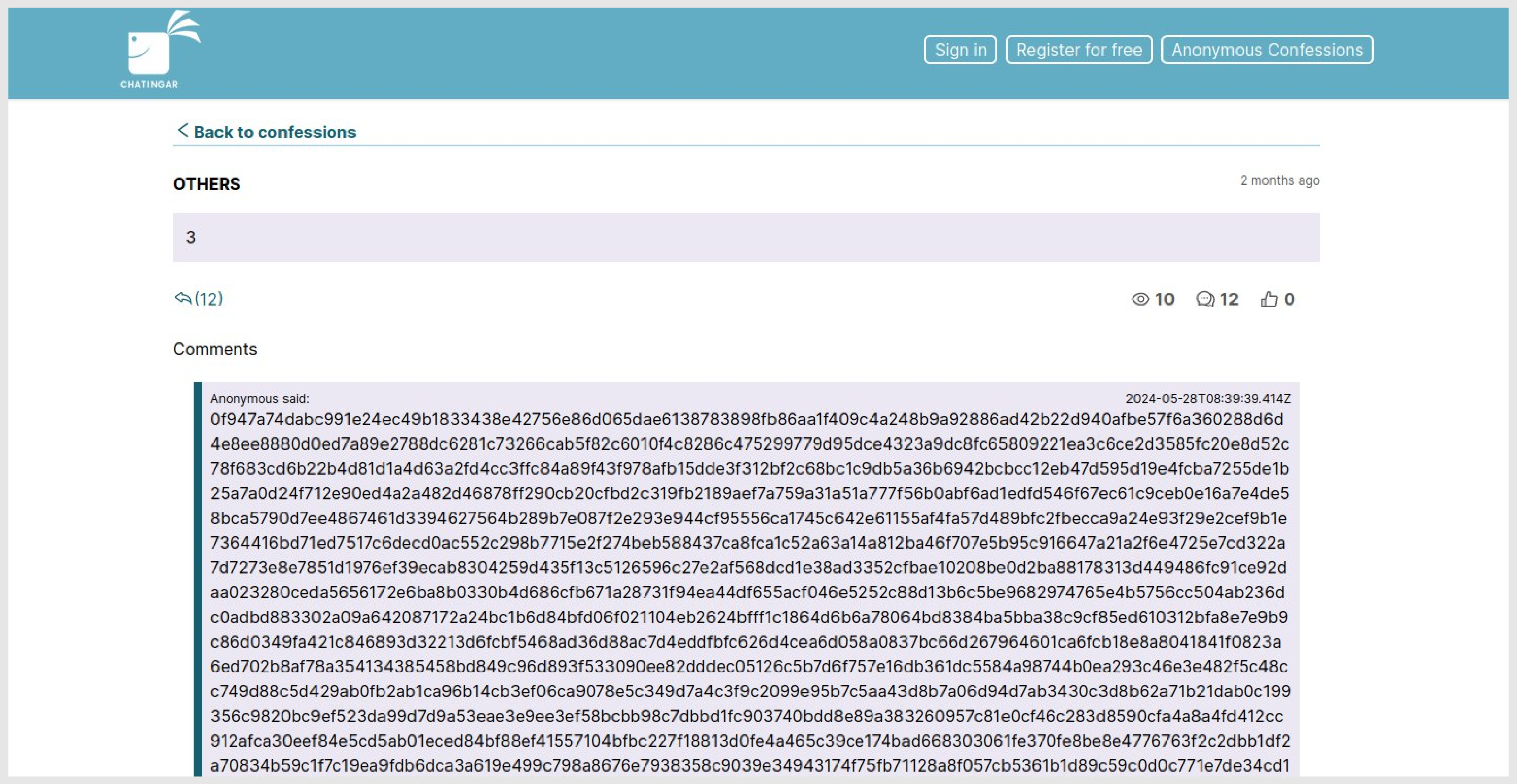
HLE

HLL (Hidden Lake Loader) — **downloader**and manual traffic distributor between several HLT services

HLA (Hidden Lake Adapters) - **adapters**to create anonymous communications in foreign systems, including centralized ones

HLA

Using the centralized service "chatingar"



< Back to confessions

OTHERS

2 months ago

3

(12)

10 12 0

Comments

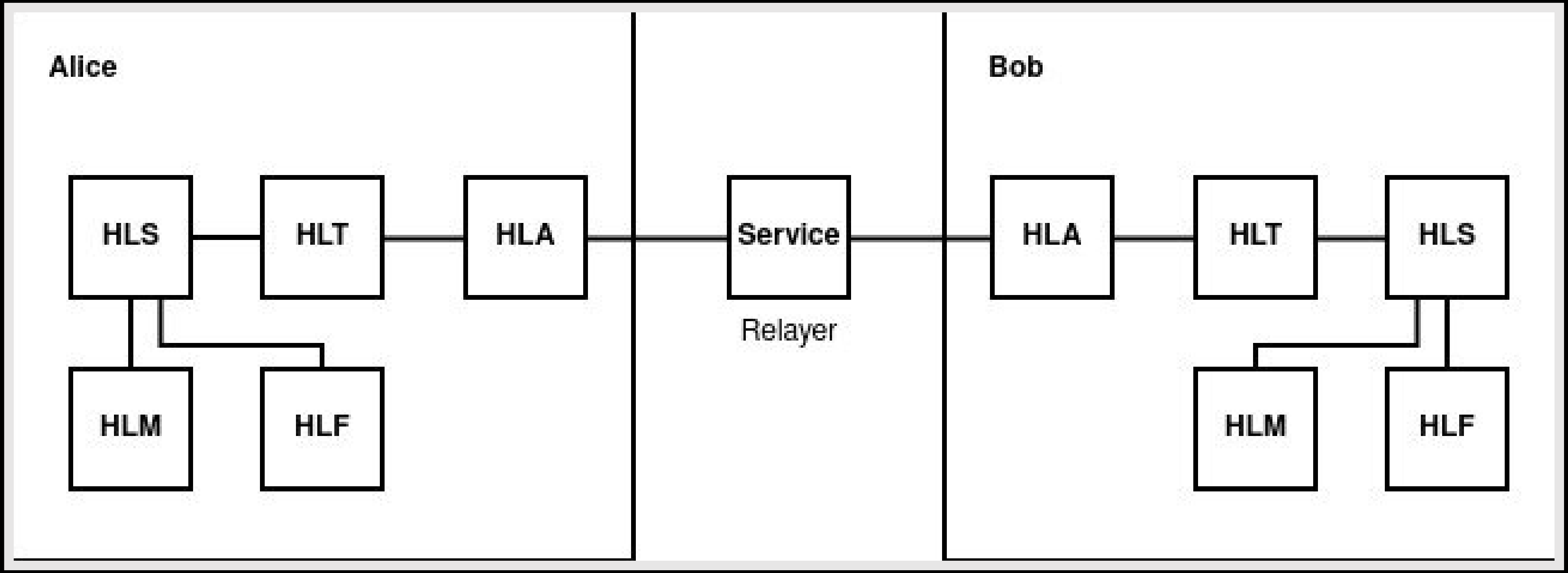
Anonymous said:

2024-05-28T08:39:39.414Z

```
0f947a74dabc991e24ec49b1833438e42756e86d065dae6138783898fb86aa1f409c4a248b9a92886ad42b22d940afbe57f6a360288d6d
4e8ee8880d0ed7a89e2788dc6281c73266cab5f82c6010f4c8286c475299779d95dce4323a9dc8fc65809221ea3c6ce2d3585fc20e8d52c
78f683cd6b22b4d81d1a4d63a2fd4cc3ffc84a89f43f978afb15dde3f312bf2c68bc1c9db5a36b6942bcbcc12eb47d595d19e4fcba7255de1b
25a7a0d24f712e90ed4a2a482d46878ff290cb20cfbd2c319fb2189aef7a759a31a51a777f56b0abf6ad1edfd546f67ec61c9ceb0e16a7e4de5
8bca5790d7ee4867461d3394627564b289b7e087f2e293e944cf95556ca1745c642e61155af4fa57d489bfc2fbecca9a24e93f29e2cef9b1e
7364416bd71ed7517c6decd0ac552c298b7715e2f274beb588437ca8fca1c52a63a14a812ba46f707e5b95c916647a21a2f6e4725e7cd322a
7d7273e8e7851d1976ef39ecab8304259d435f13c5126596c27e2af568dcd1e38ad3352cfbae10208be0d2ba88178313d449486fc91ce92d
aa023280ceda5656172e6ba8b0330b4d686cfb671a28731f94ea44df655acf046e5252c88d13b6c5be9682974765e4b5756cc504ab236d
c0adbd883302a09a642087172a24bc1b6d84bfd06f021104eb2624bfff1c1864d6b6a78064bd8384ba5bba38c9cf85ed610312bfa8e7e9b9
c86d0349fa421c846893d32213d6fcbf5468ad36d88ac7d4eddfbfc626d4cea6d058a0837bc66d267964601ca6fcb18e8a8041841f0823a
6ed702b8af78a354134385458bd849c96d893f533090ee82dddec05126c5b7d6f757e16db361dc5584a98744b0ea293c46e3e482f5c48c
c749d88c5d429ab0fb2ab1ca96b14cb3ef06ca9078e5c349d7a4c3f9c2099e95b7c5aa43d8b7a06d94d7ab3430c3d8b62a71b21dab0c199
356c9820bc9ef523da99d7d9a53eae3e9ee3ef58bcbb98c7dbbd1fc903740bdd8e89a383260957c81e0cf46c283d8590cfa4a8a4fd412cc
912afca30eef84e5cd5ab01eced84bf88ef41557104bfbc227f18813d0fe4a465c39ce174bad668303061fe370fe8be8e4776763f2c2dbb1df2
a70834b59c1f7c19ea9fdb6dca3a619e499c798a8676e7938358c9039e34943174f75fb71128a8f057cb5361b1d89c59c0d0c771e7de34cd1
```

Formaldescription of the composition of services

$$Hidden\ Lake = \Sigma^{n}_{i=1} APP_{i} \times HLS \times (HLT \times \Sigma^{m}_{j=1} HLA_{j})^{t}$$



Comparison with other anonymous networks

	Hidden Lake	Herbivore	I2P	Tor	Mixminion	Crowds
Decentralized architecture	+	+	+	-	-	+
Service API implementation	+	-	+	+	-	-
Delay in data transmission	+	+	-	-	+	-
Closed network architecture	+	-	+	+/-	-	-
Hiding the fact of data generation	+	-	-	-	-	-
Hiding the recipient from the sender	+/-	-	+	+/-	-	-
Hiding the sender from the recipient	+/-	+	+	+	+	+
Anonymization task	QB	DC	Onion	Onion	Onion	Proxy

Possible Uses of the Hidden Lake Anonymous Network

1. Protecting local/corporate networks from eavesdropping
2. Protecting military communications nodes from eavesdropping
3. Strengthening the security of already existing/formed systems
4. Using an existing platform to create your own applications

Links

- Hidden Lake

https://github.com/number571/hidden-lake

- Documentation

https://github.com/number571/hidden-lake/tree/master/docs