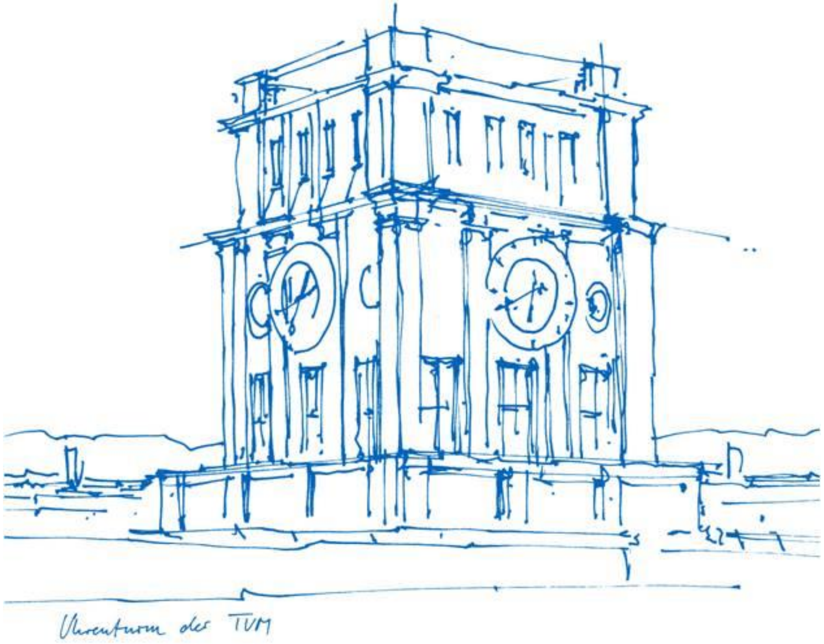
Protocol Analysis

Fabian Sauter, Kilian Traub, Atakan Yenel

Group 5

Technische Universität München

Garching, 10.08.2018

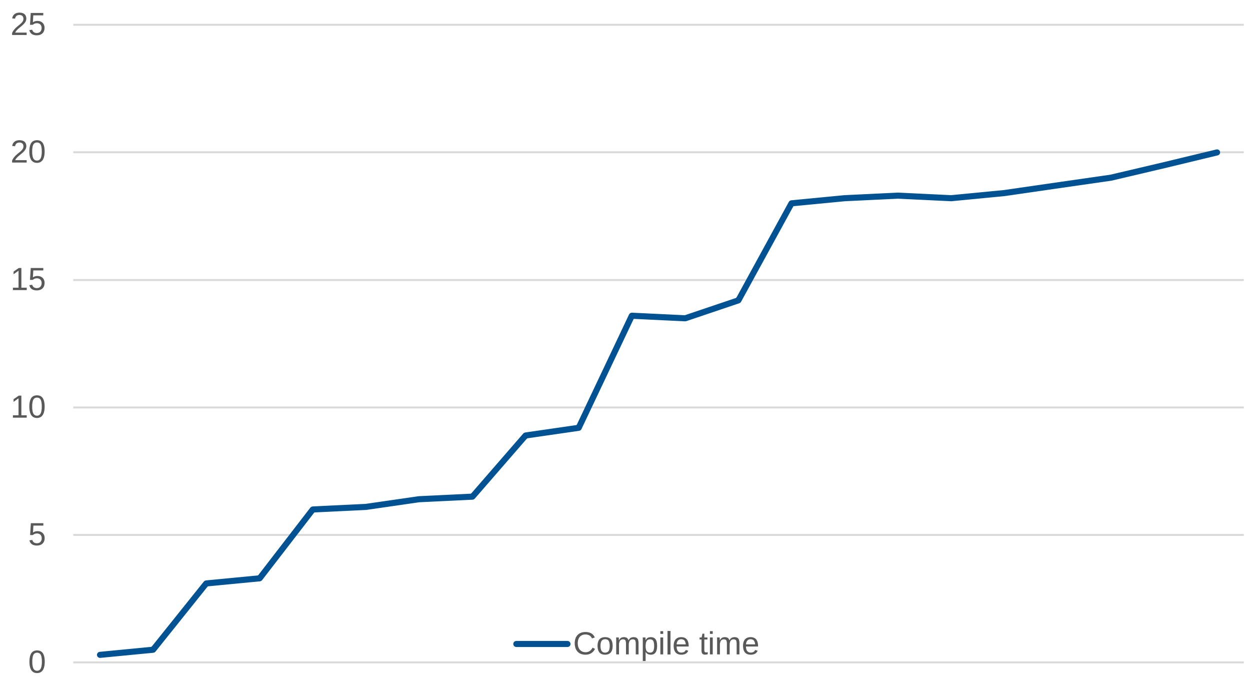


General

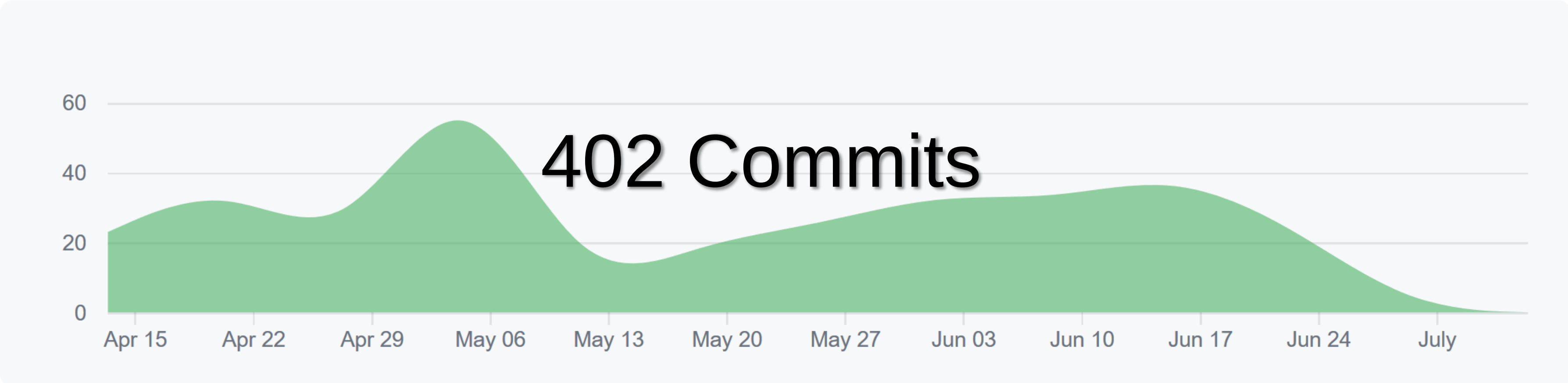
- C++17
- Compiler: g++/clang
- OS: Unix like, (Windows possible)

General

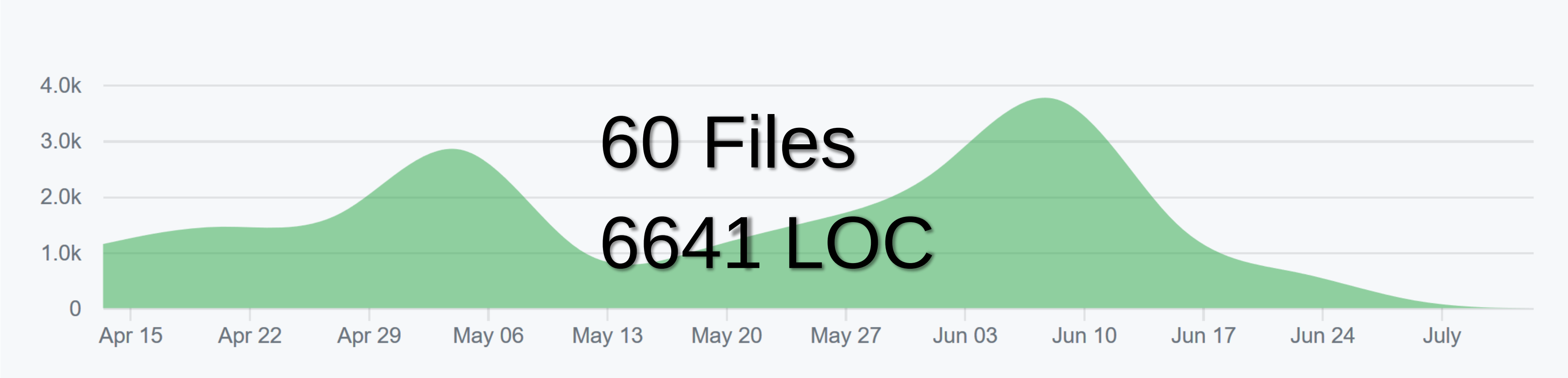
Compile time ~20 seconds



General



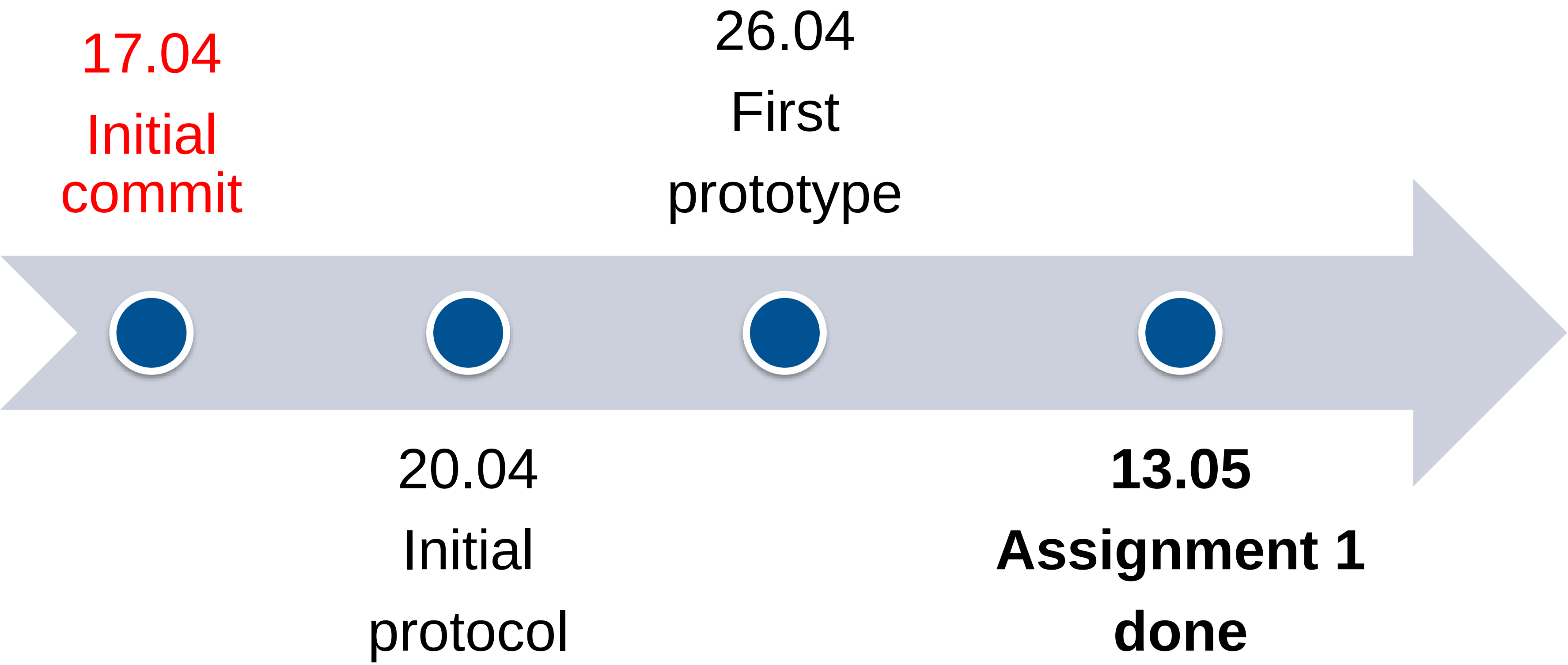
402 Commits



60 Files

6641 LOC

The process



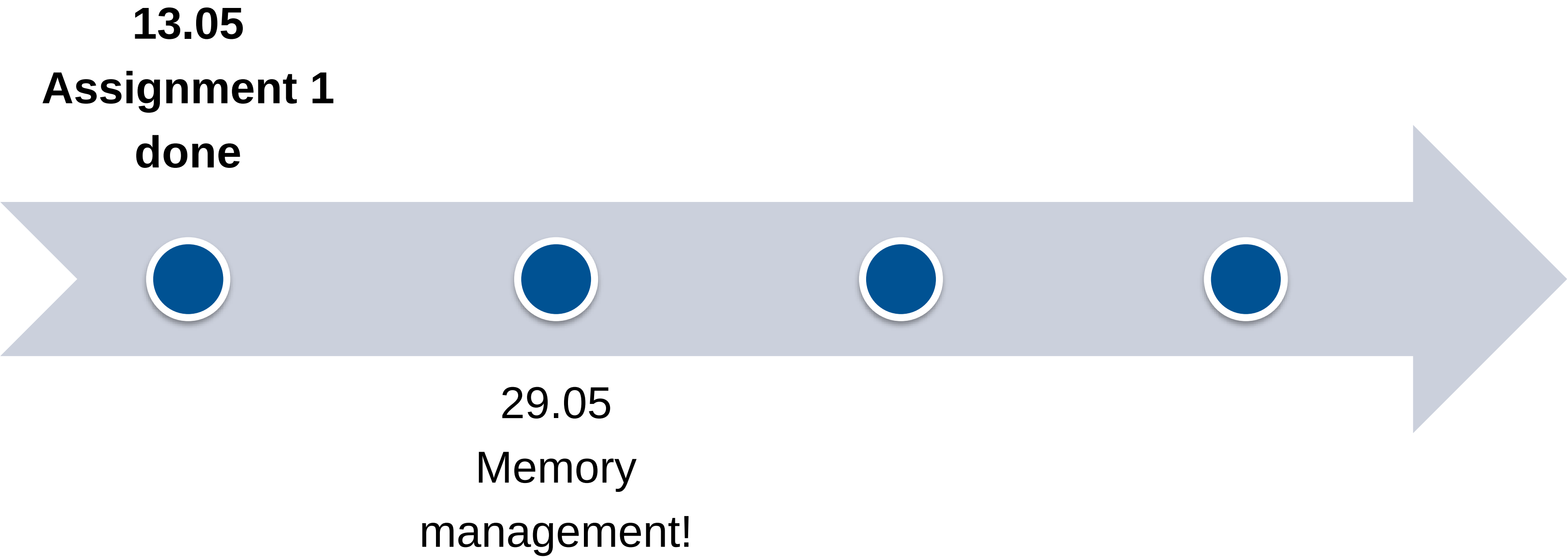
17.04 Initial commit

20.04 Initial protocol

26.04 First prototype

13.05 Assignment 1 done

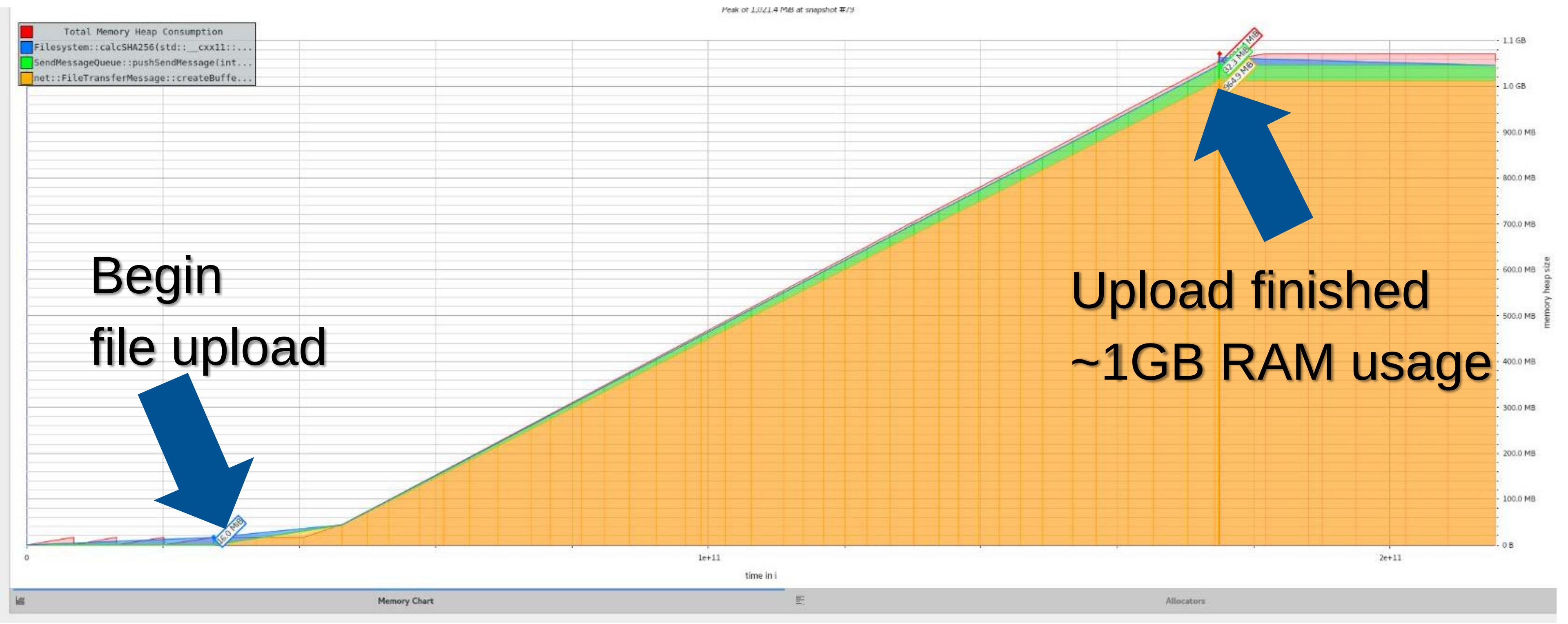
The process



13.05
Assignment 1
done

29.05
Memory
management!

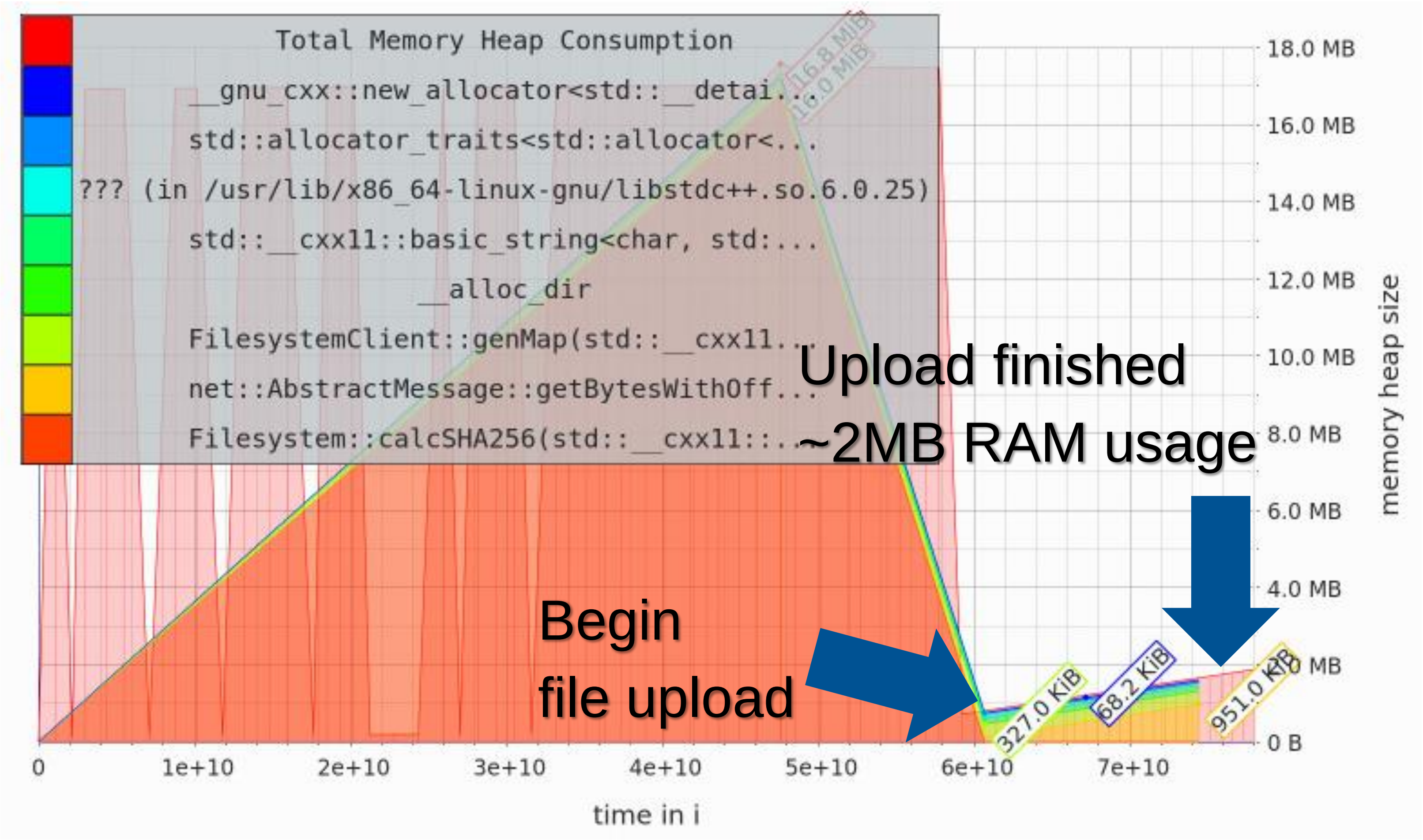
Memory management



Begin file upload

Upload finished ~1GB RAM usage

Memory management



Upload finished
~2MB RAM usage

Begin
file upload

The process

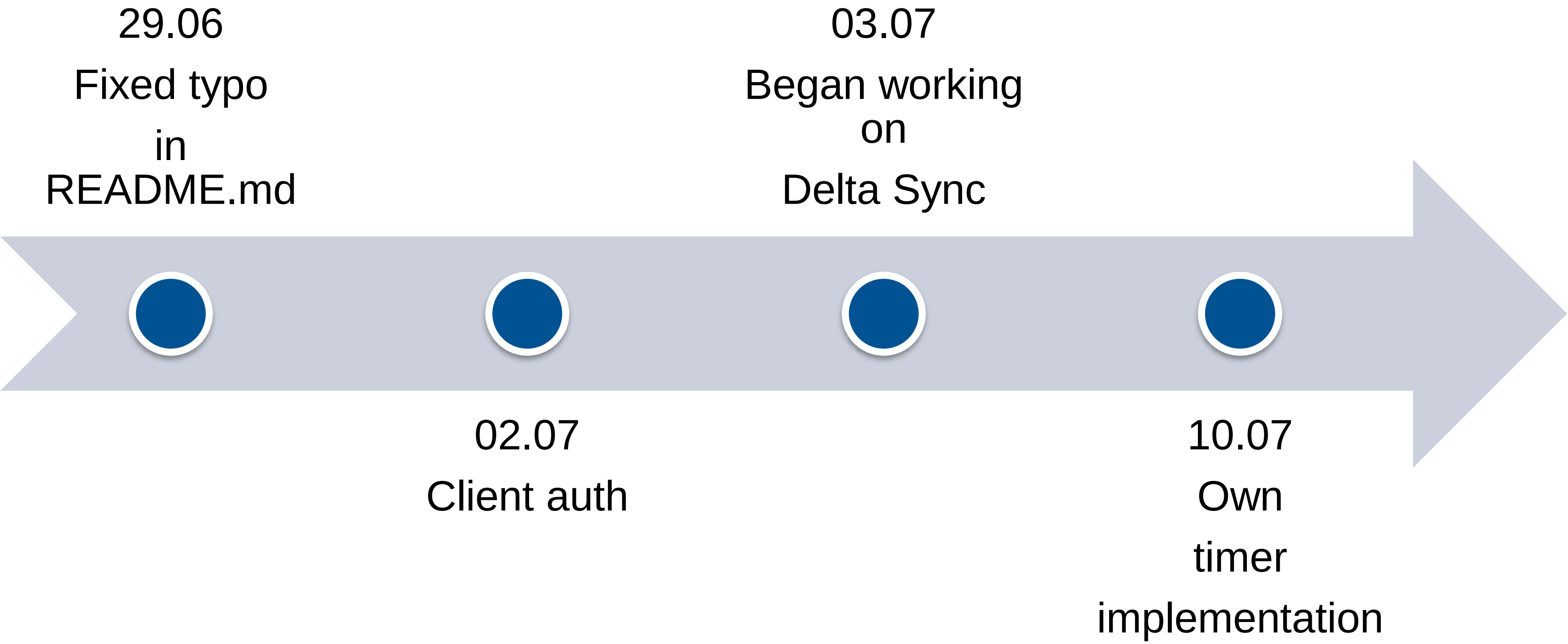
13.05
Assignment 1 done

29.05
Memory management!

05.06
Encryption support

09.06
“Congestion control”

The process



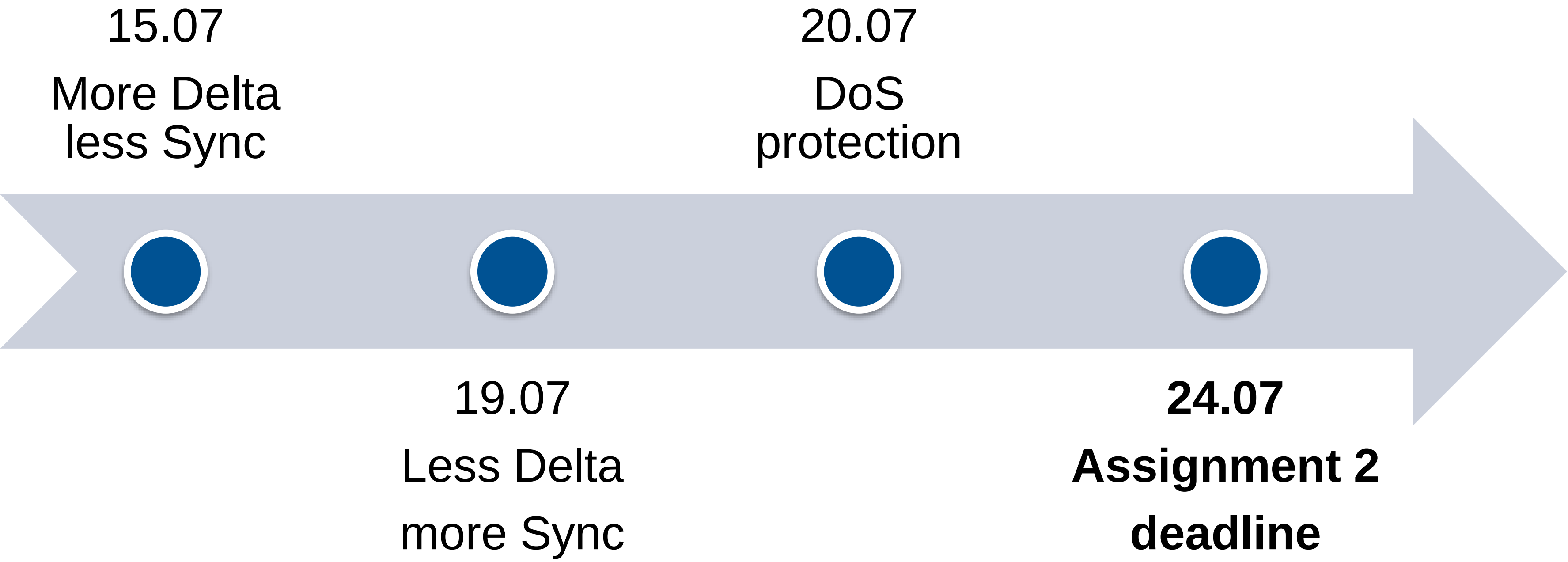
29.06
Fixed typo
in
README.md

02.07
Client auth

03.07
Began working
on
Delta Sync

10.07
Own
timer
implementation

The process



15.07
More Delta
less Sync

19.07
Less Delta
more Sync

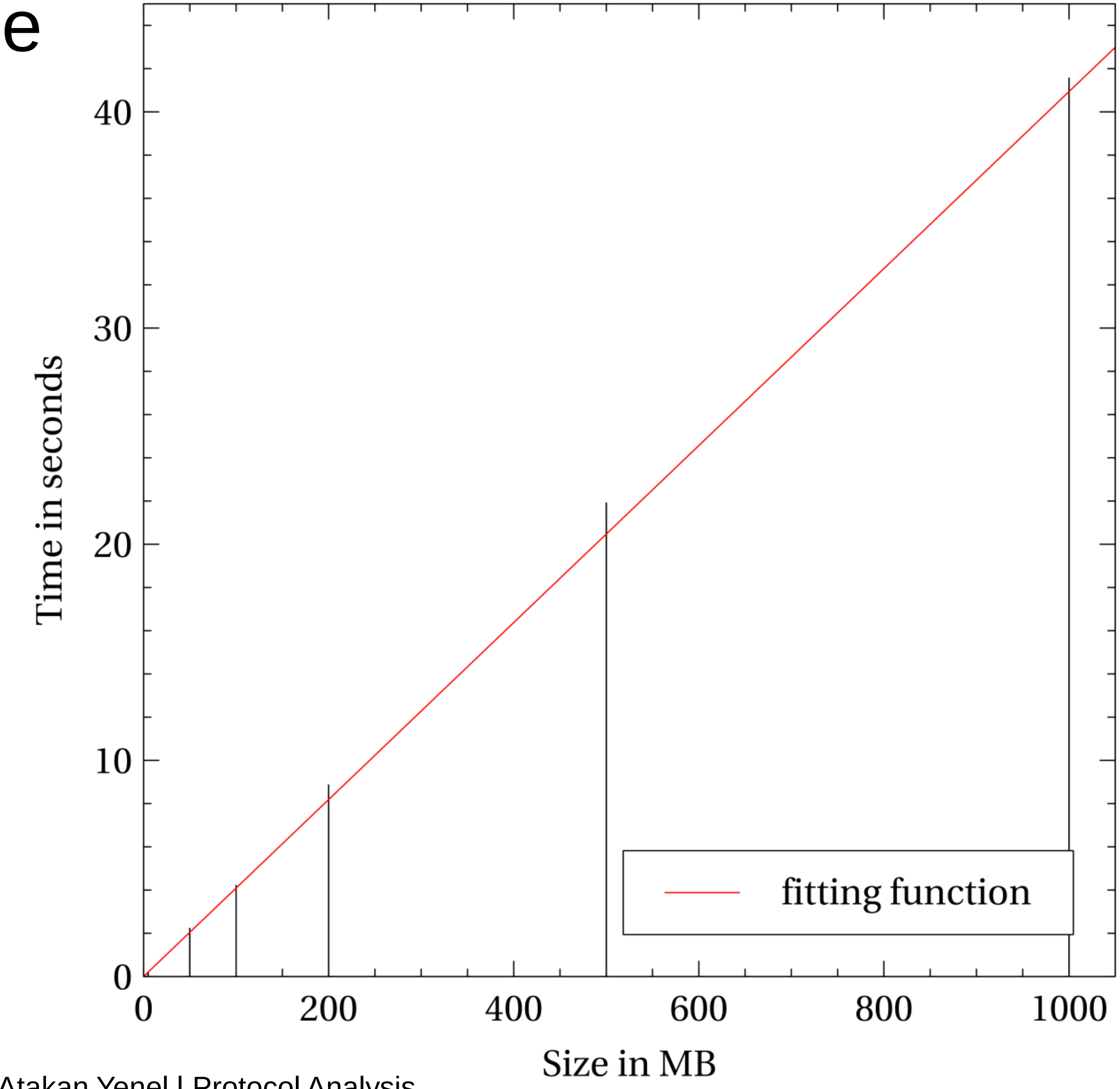
20.07
DoS
protection

24.07
Assignment 2
deadline

Performance

1Gb – 40s

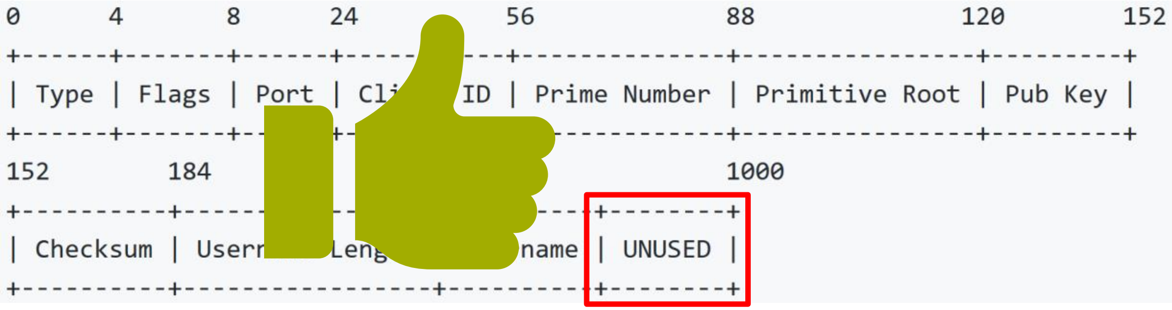
→26.64MB/s



Security

User authentication

DoS protection



```
0      4       8      24          56              88               120        152
+------+-------+------+-----      ---+--------------+----------------+---------+
| Type | Flags | Port | Cli       ID | Prime Number | Primitive Root | Pub Key |
+------+-------+--          +-      ----------------+----------------+---------+
152        184                                    1000
+----------+-----          -                 ---+--------+
| Checksum | Usern          Leng           name | UNUSED |
+----------+----------------+--------------------+--------+
```

Multi-way handshake

Encryption

Security

Man-in-the-Middle attacks

What we learned

- If you use *new* or *malloc:*
  - ➢ Use smart pointers
  - ➢ If not *delete* your shit
- If it says „experimental“ it actually means experimental
- Wait till C++20 for the filesystem module
- Doing your own crypto suckz, use libraries
- Certificate checks are no snake oil
- C++ is awesome♡