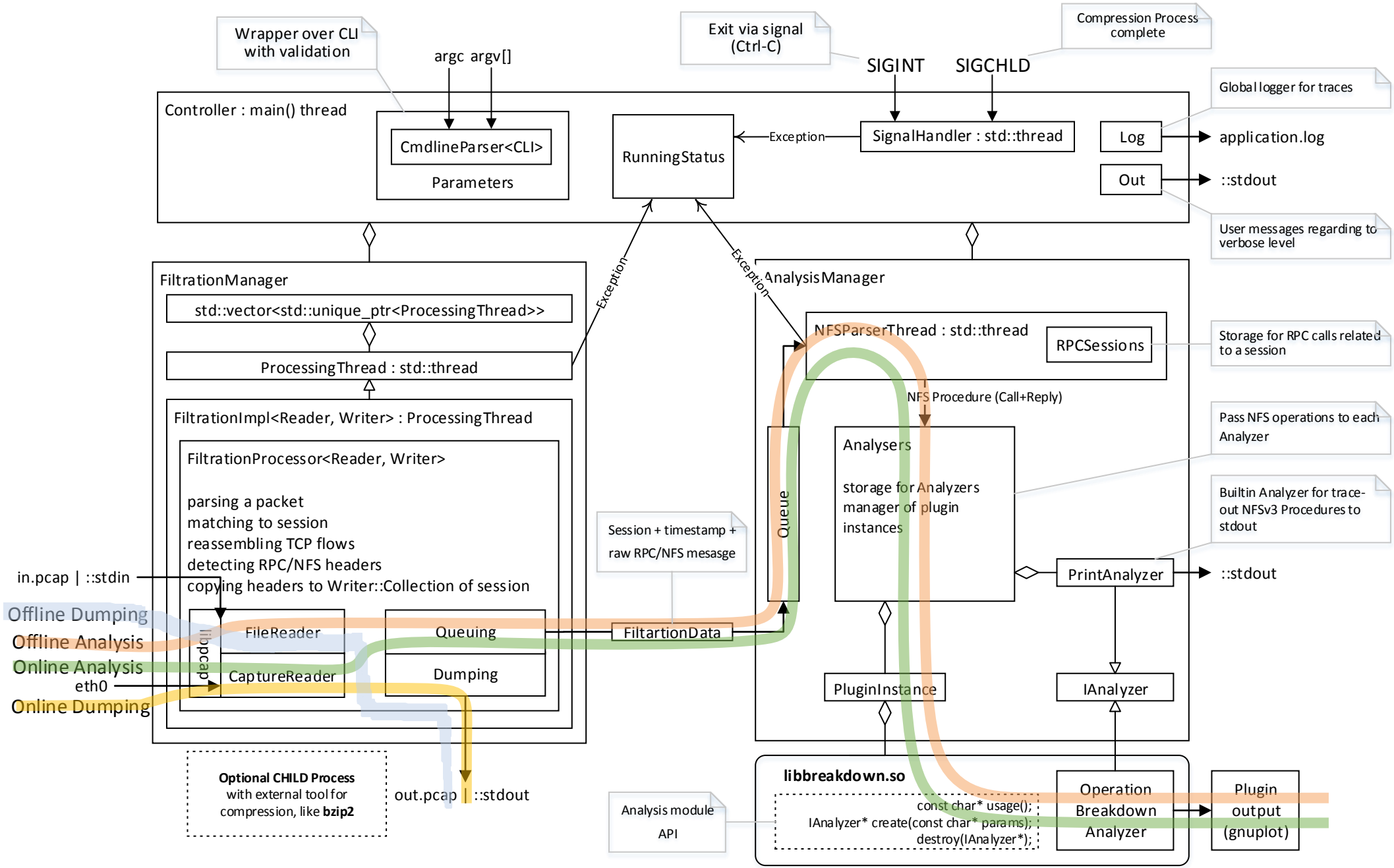
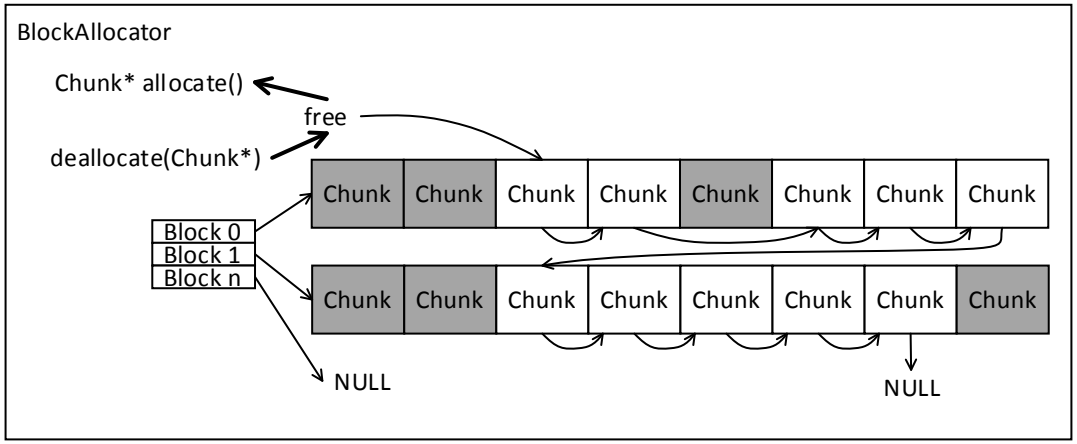
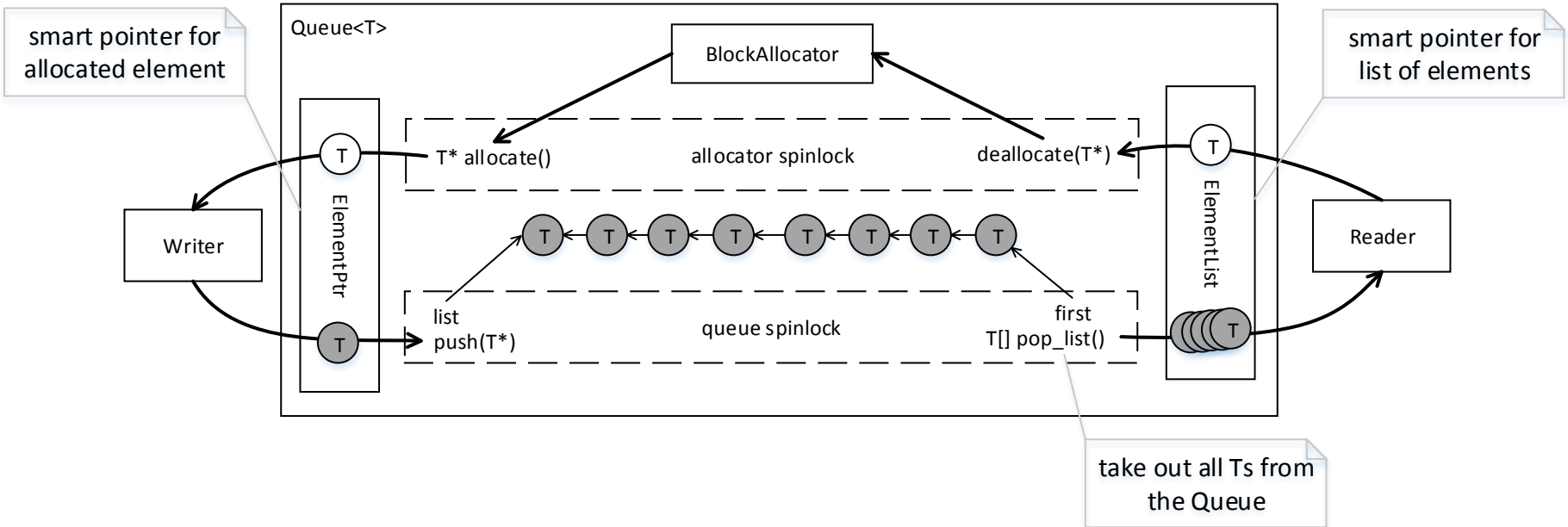
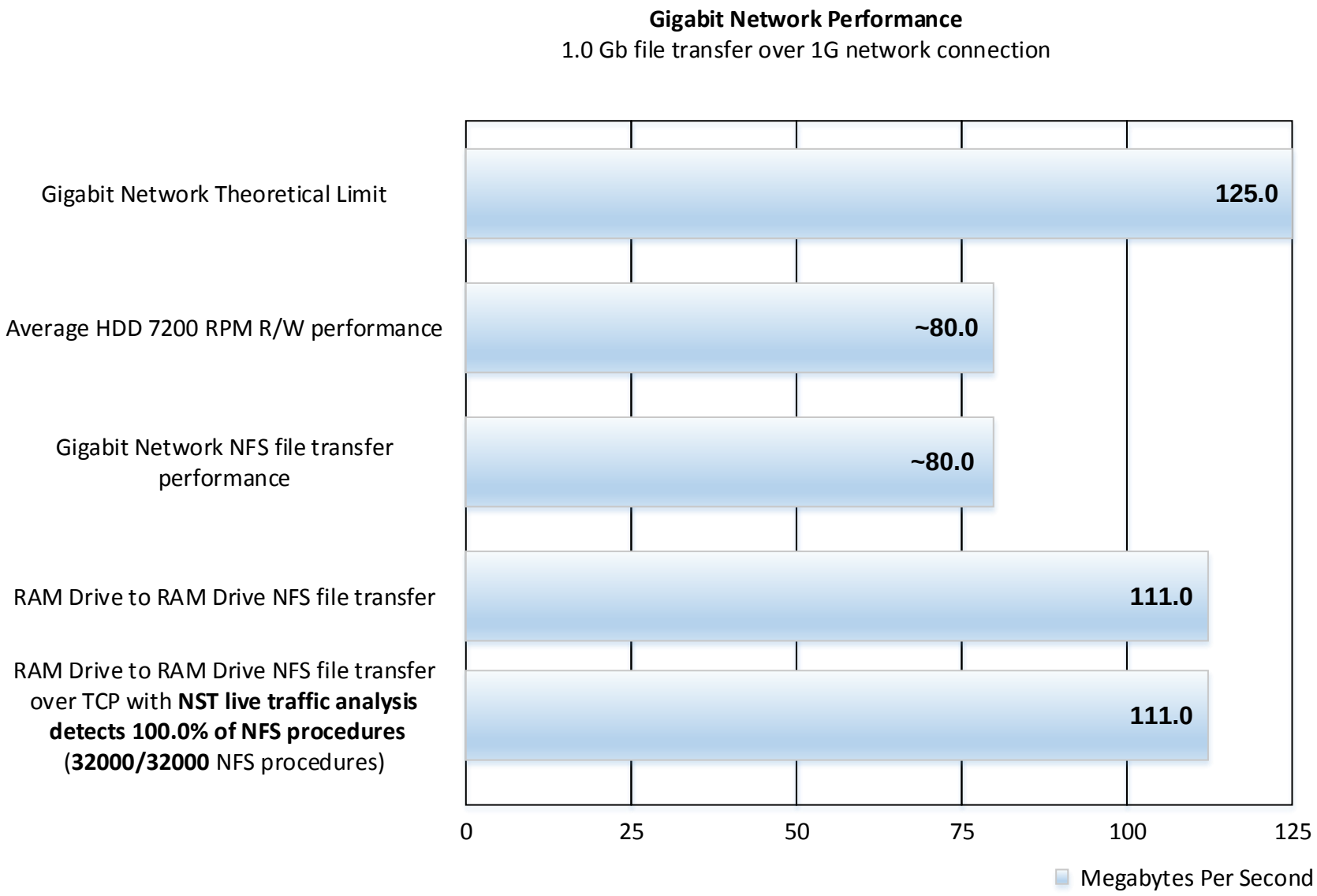

Wrapper over CLI with validation
argc argv[]
Exit via signal (Ctrl-C)
SIGINT
SIGCHLD
Compression Process complete
Global logger for traces
Controller : main() thread
CmdlineParser<CLI>
Parameters
RunningStatus
Exception
SignalHandler : std::thread
Log
application.log
Out
::stdout
User messages regarding to verbose level
Exception
Exception
FiltrationManager
std::vector<std::unique_ptr<ProcessingThread>>
ProcessingThread : std::thread
FiltrationImpl<Reader, Writer> : ProcessingThread
FiltrationProcessor<Reader, Writer>
parsing a packet
matching to session
reassembling TCP flows
detecting RPC/NFS headers
copying headers to Writer::Collection of session
in.pcap | ::stdin
Offline Dumping
Offline Analysis
Online Analysis
eth0
Online Dumping
libpcap
FileReader
CaptureReader
Queuing
Dumping
Optional CHILD Process
with external tool for compression, like bzip2
out.pcap | ::stdout
Session + timestamp + raw RPC/NFS mesasge
FiltartionData
Queue
AnalysisManager
NFSParserThread : std::thread
RPCSessions
Storage for RPC calls related to a session
NFS Procedure (Call+Reply)
Analysers
storage for Analyzers
manager of plugin instances
Pass NFS operations to each Analyzer
Builtin Analyzer for trace-out NFSv3 Procedures to stdout
PrintAnalyzer
::stdout
PluginInstance
IAnalyzer
libbreakdown.so
const char* usage();
IAnalyzer* create(const char* params);
destroy(IAnalyzer*);
Analysis module API
Operation Breakdown Analyzer
Plugin output (gnuplot)


BlockAllocator
Chunk* allocate()
free
deallocate(Chunk*)
Block 0
Block 1
Block n
Chunk
NULL


smart pointer for allocated element
Queue<T>
BlockAllocator
smart pointer for list of elements
T* allocate()
allocator spinlock
deallocate(T*)
Writer
ElementPtr
ElementList
Reader
list push(T*)
queue spinlock
first T[] pop_list()
take out all Ts from the Queue


Gigabit Network Performance
1.0 Gb file transfer over 1G network connection
Gigabit Network Theoretical Limit
125.0
Average HDD 7200 RPM R/W performance
~80.0
Gigabit Network NFS file transfer performance
~80.0
RAM Drive to RAM Drive NFS file transfer
111.0
RAM Drive to RAM Drive NFS file transfer over TCP with NST live traffic analysis detects 100.0% of NFS procedures (32000/32000 NFS procedures)
111.0
0
25
50
75
100
125
Megabytes Per Second