1.

2.

- Goal:

1.
   -
   -

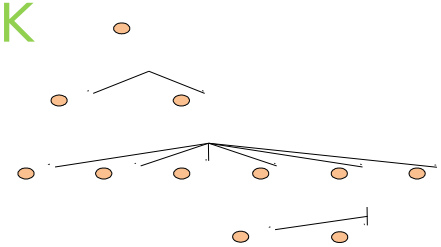
2.

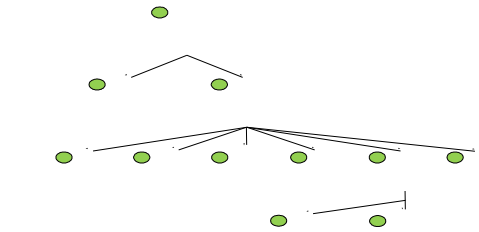
3.

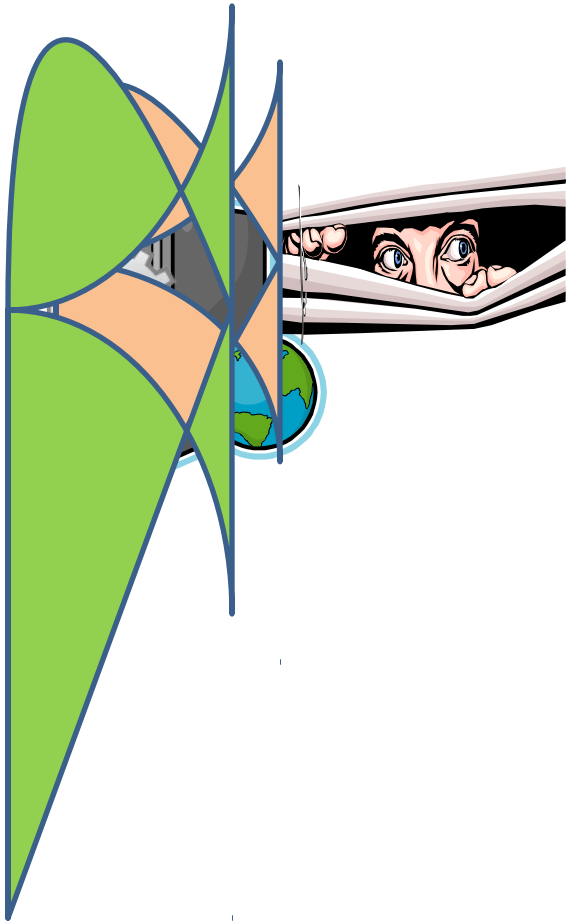
1. Buffer deconstruction, a technique to extract the format of sent messages
   - Ø Earlier work only handles received messages
2. Field semantics inference techniques, for messages sent and received
3. Designing and developing Dispatcher
4. Extending a technique to handle

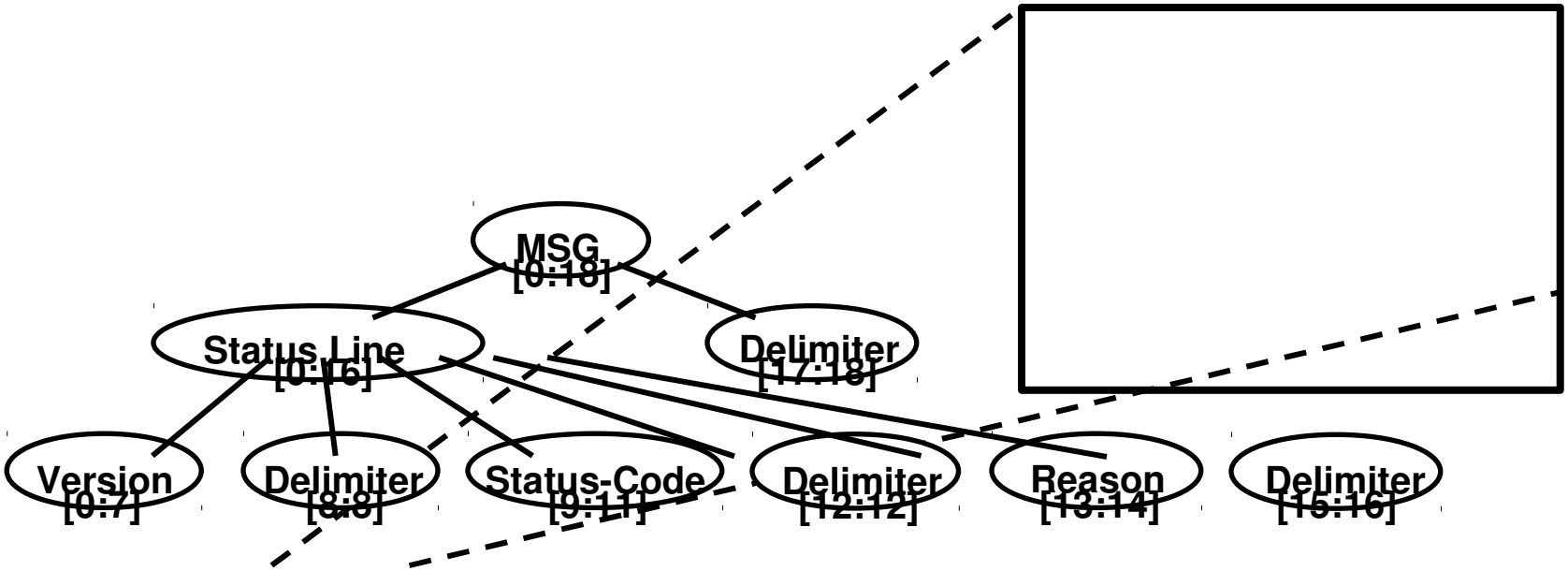
GET /
HTTP/1.1

HTTP/1.1 200
OK



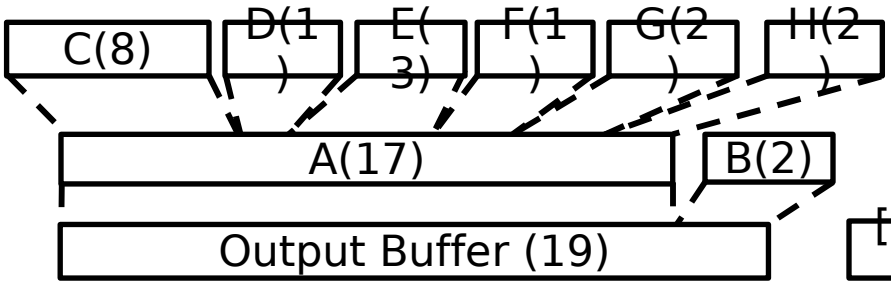


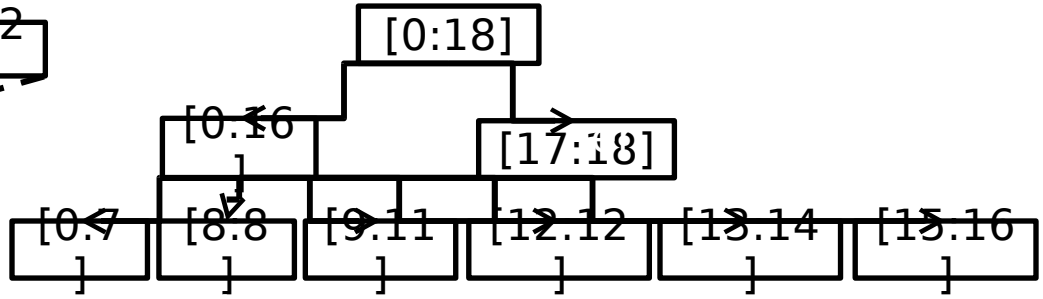



MSG
[0:18]
Status Line
[0:16]
Delimiter
[17:18]
Version
[0:7]
Delimiter
[8:8]
Status-Code
[9:11]
Delimiter
[12:12]
Reason
[13:14]
Delimiter
[15:16]

1.
2.

Buffer Deconstruction


C(8)
D(1
)
E(
3)
F(1
)
G(2
)
H(2
)
A(17)
B(2)
Output Buffer (19)


[0:18]
[0:16
]
[17:18]
[0:7
]
[8:8
]
[9:11
]
[12:12
]
[13:14
]
[15:16
]

-
  -
  -
  -
  -
  -

Attribute	Value
Field Range	[StartOffset : EndOffset]
Field Boundary	Fixed, Length, Delimiter
Field Semantics	IP address, Timestamp, …
Field Keywords	<list of keyworkds in field>

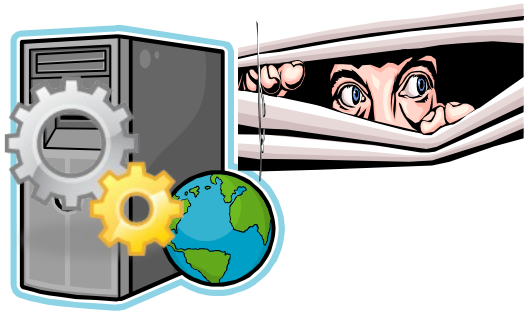
Features the type

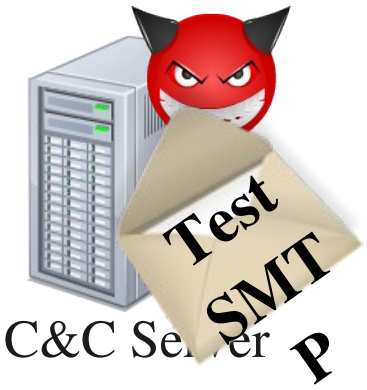
Field names	
Cookies	Keyboard input
Error codes	Keywords
File data	Length
File information	Padding
Filenames	Ports
Hash / Checksum	Registry data
Hostnames	Sleep timers
Host information	Stored data
IP addresses	Timestamps

-
-
  -
-

File path

File length





C&C Server

SMTP Test Server

SMTP Test Server

Template Server