Deloitte.

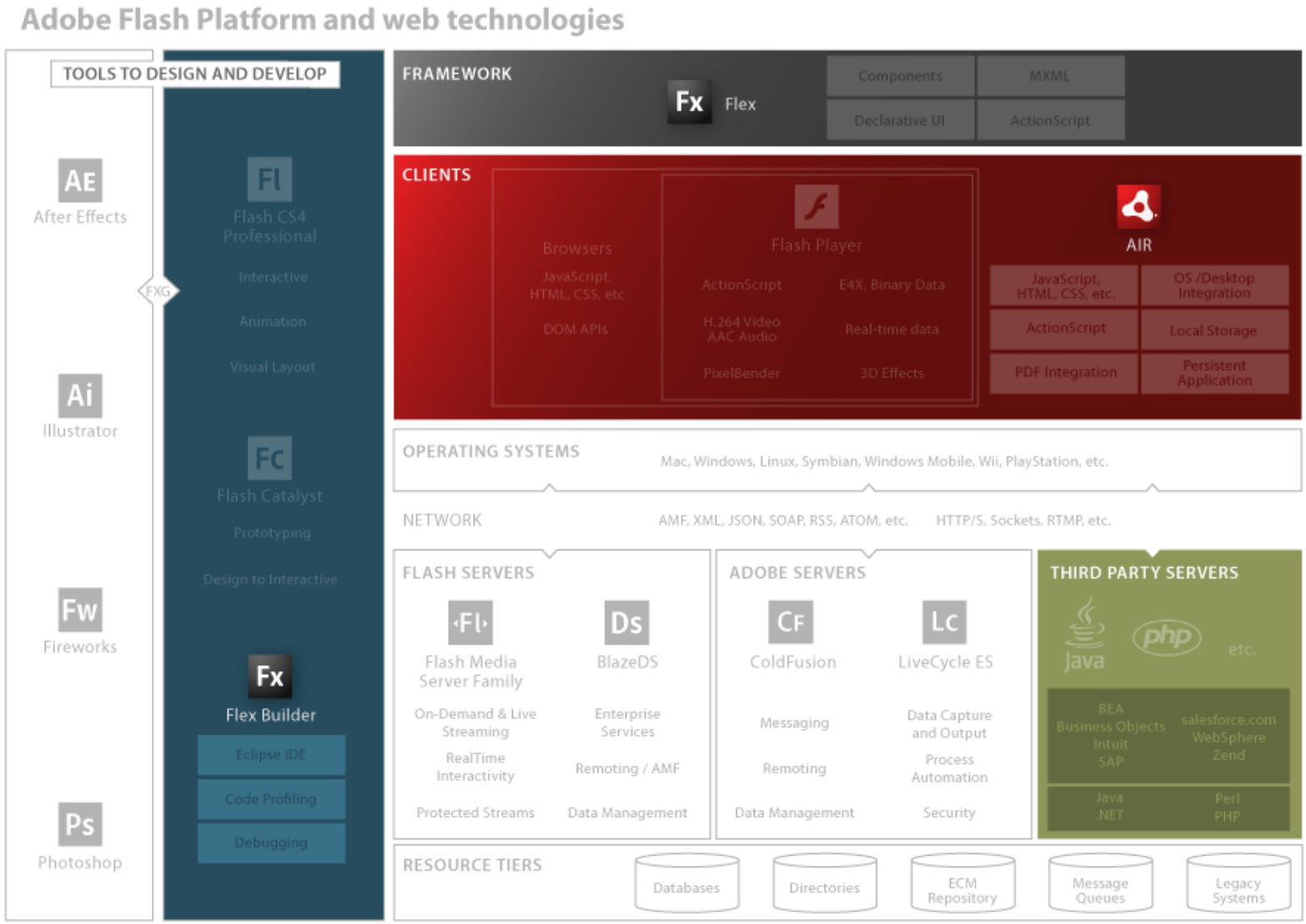
Testing Flash Applications using WebScarab

Martin Clausen <mclausen@deloitte.dk>

Introduction

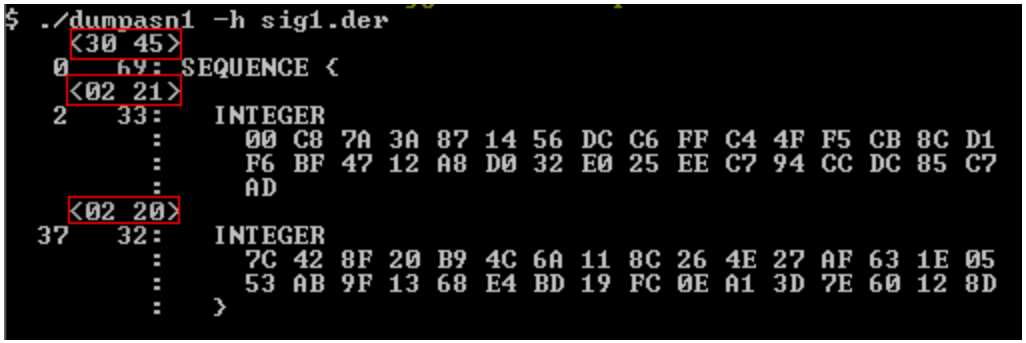
- Flash
  - Used to create animations, ads, and various Web components, to integrate video into web pages and, more recently, to develop RIA
  - Includes scripting languages - ActionScript 1, 2 & 3
- Flash Player
  - Runs Flash content (SWF file format)
- Flex
  - Framework for developing RIAs that run in Flash Player
  - Design GUI in MXML (XML document) for components, and ActionScript for programming
- Flash application can interact with a web page using JavaScript and vice versa

Adobe Flash Platform



ActionScript Message Format (AMF)

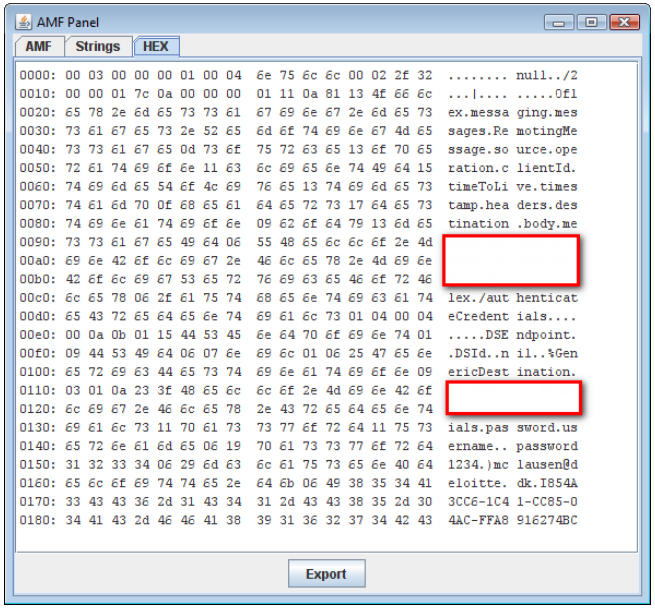
- Mostly used to exchange data between Flash application and server side component
- Asynchronous RPC mechanism, where objects are serialized and deserialized to and from AMF
- AMF is a binary format
  - Like ASN.1 where data is encoded in TLVs
- Two versions: 0 & 3
- Specifications now open



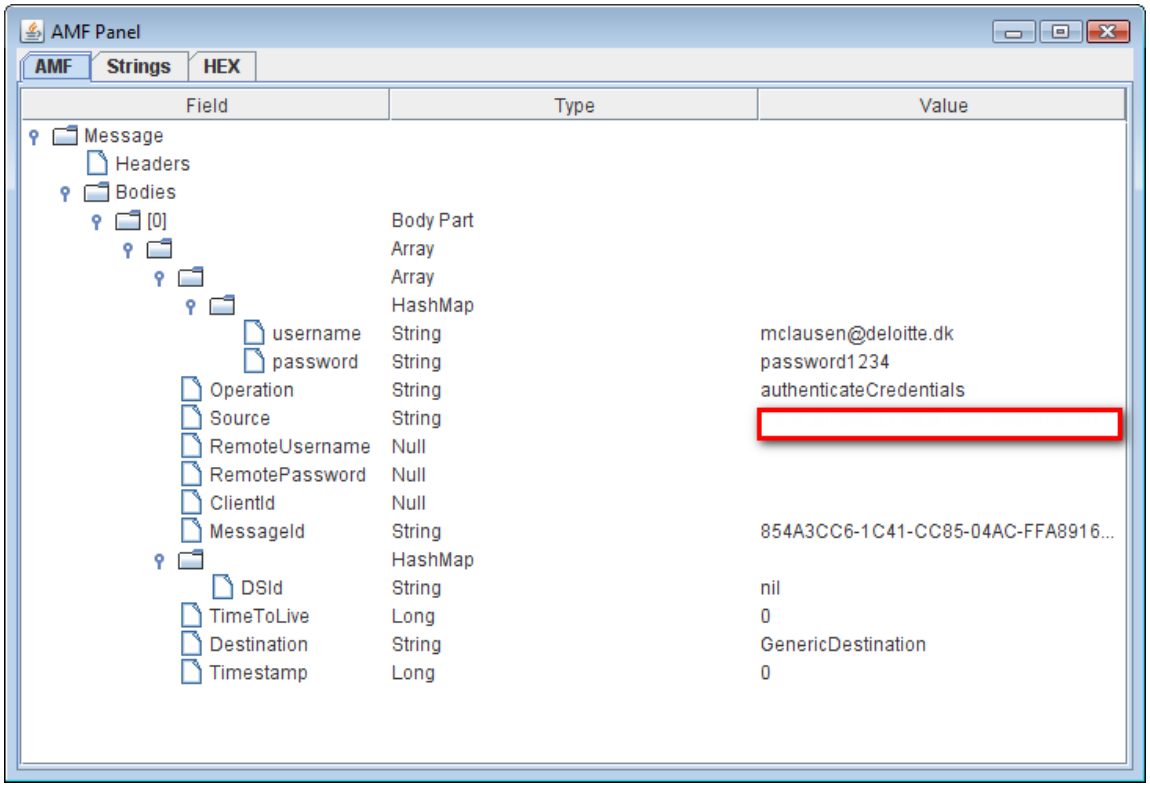
Remoting envelope

- Preamble containing version: 0 or 3
- Header(s)
  - Name
  - Data: serialized AMF object
- Message(s)
  - Target URI
  - Response URI
  - Data: serialized AMF object

Remoting example



Raw request



Decoded request

Text

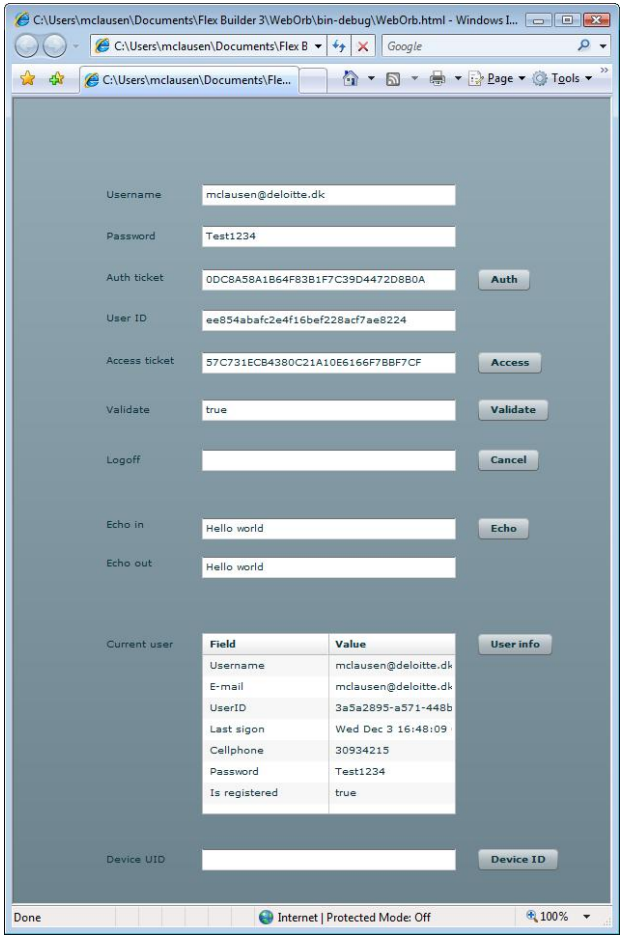
```
1  □□□□□□□□□null□□□/2□□□x
2  □□□□□□
3  □□□flex.messaging.messages.RemotingMessage□source□operation□headers□destination     body□messageId□clientId□timeToLive□timestamp□U                                    □/authenticateCredentials
4  □□□□DSEndpoint□DSId□□nil□□%GenericDestination□□
5  #1                 Credentials□username□password□)mclausen@deloitte.dk□□Test1234□IBDE40CA9-EA66-0978-423F-F95FB14B5AB3□□□□□
```

Techniques

Some support:

- WebScarab
- Charles
- ServiceCapture
- (Burp suite)
- (WireShark)
- No write support!

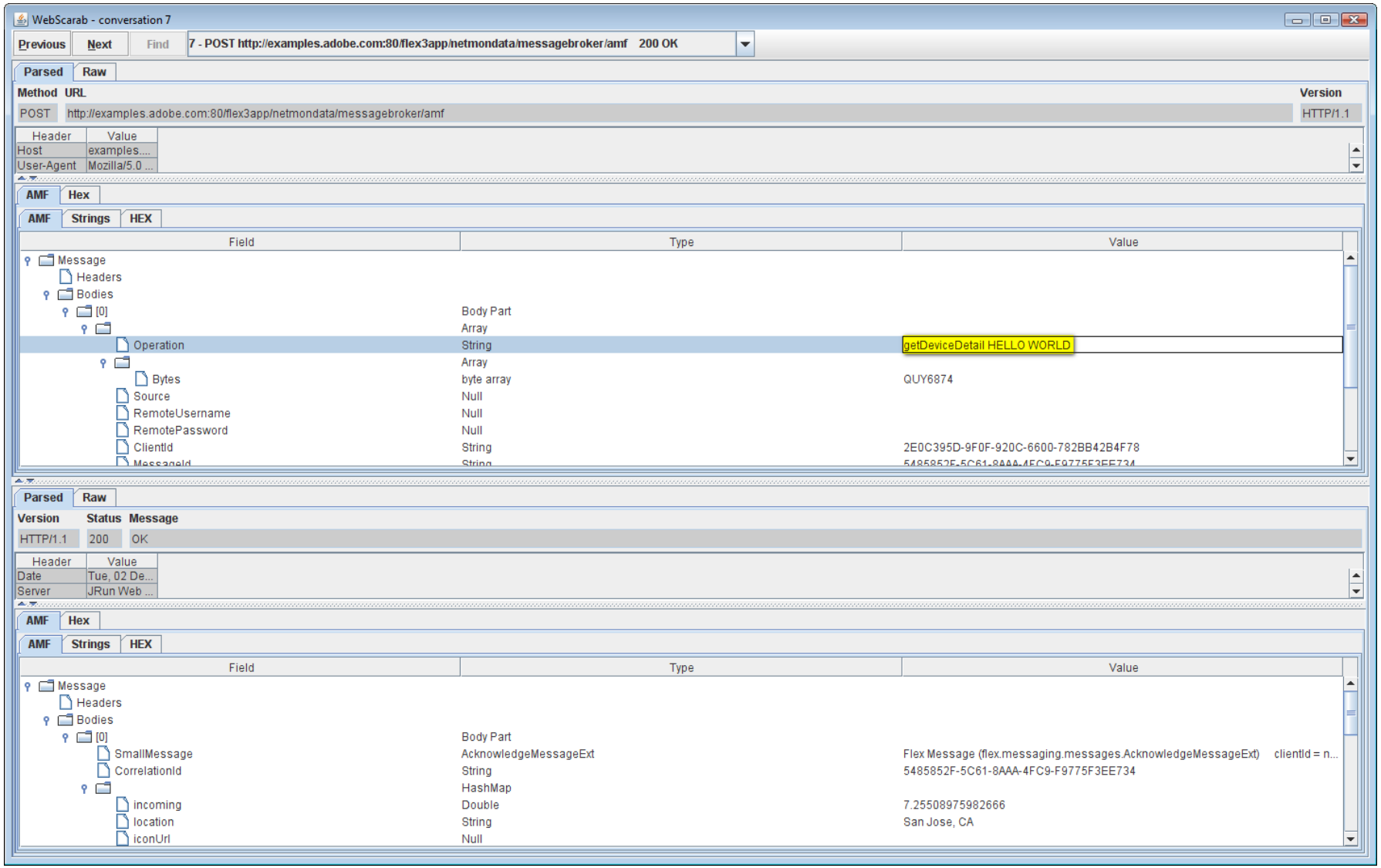
Write ”custom” Flex application:



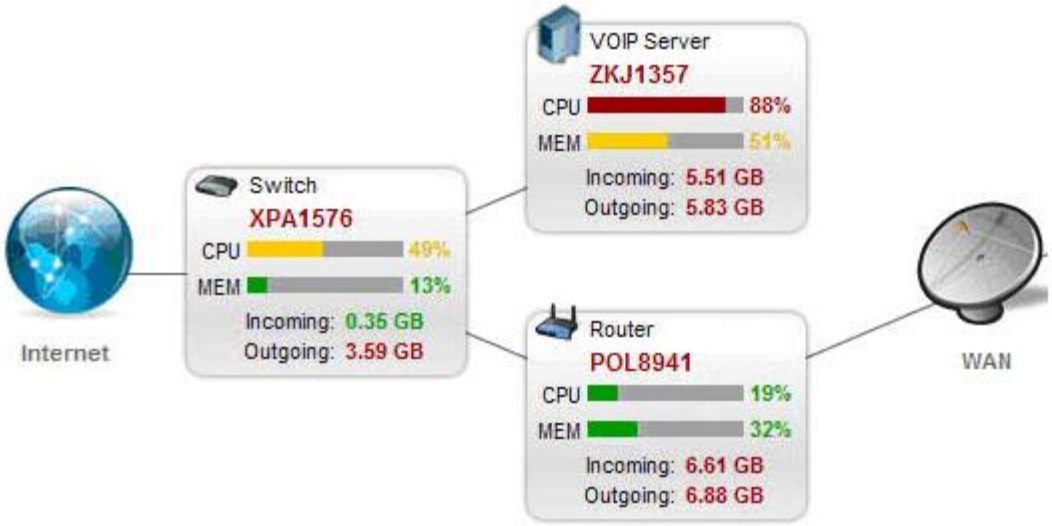
WebScarab AMF extension

- WebScarab supports a plugin “infrastructure”
- Our plugin:
  - Replaces the existing (reads AMF 0)
  - Supports AMF 0 & 3
  - Supports read / write
  - Still in development

WebScarab AMF extension – ctd.



Demo



More information

- Testing Flash Applications (Stefano Di Paola / OWASP): http://www.wisec.it/en/Docs/flash_App_testing_Owasp07.pdf
- Adobe Flash Player 9 Security: http://www.adobe.com/devnet/flashplayer/articles/flash_player_9_security.pdf
- AMF 0 Specification: http://download.macromedia.com/pub/labs/amf/amf0_spec_121207.pdf
- AMF 3 Specification: http://download.macromedia.com/pub/labs/amf/amf3_spec_121207.pdf
- OWASP / WebScarab: http://www.owasp.org
- Open Source Flash: http://osflash.org