Case Study

OWASP AppSec Israel 2016

AppSec Application security Labs

AppSec Labs Ltd.
info@appsec-labs.com
https://appsec-labs.com

Java Hurdling

Obstacles and Techniques in Java Client Penetration-Testing

Tal Melamed
Application Security Expert
Tal@AppSec-Labs.com

Agenda

- Me
- AppSec Labs
- The problems

- Fail #1
- Fail #2
- Fail #3

- 

about:me

- Tech Lead @ AppSec Labs
  Tal@AppSec-Labs.com
- Application Security Expert
- Trainer, builder & breaker
- Follow me @ appsec.it
- https://github.com/nu11p0inter

amdocs
embrace challenge
experience success

Check Point
SOFTWARE TECHNOLOGIES LTD.

RSA
The Security Division of EMC

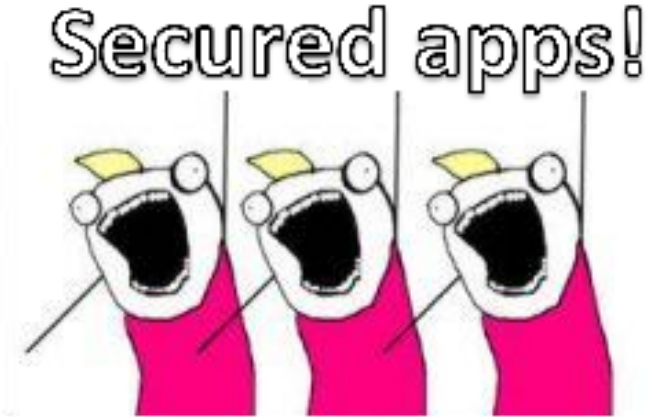
- 

, but when I do:
http://lnkdin.me/cyber

AppSec Labs

AppSec Application security Labs

https://appsec-labs.com/

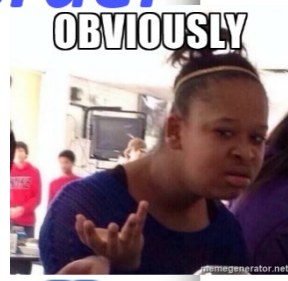


AppSec Labs

Industry vectors:

AppSec Labs provides its high end services to the following industry vectors:

- High Tech software development
- Banking and financing
- National security
- IoT
- Cloud
- Pharmaceuticals
- Commerce
- Travel and transport
- IT Security products
- Biometrics
- Education
- Gaming
- Government
- Telecommunications



We are hiring!

- Experienced PT
- Exp. Code-Review*
- Training skills
- Willing to travel *
- English
- Independent work and self-learning ability

jobs@appsec-labs.com

Disclaimer

- This is a true story. The events depicted in this talk took place in 2016.
- At the request of the survivors, names, characters, places and incidents were changed, and are either products of the author's imagination or are used fictitiously.
- Any resemblance to actual events or locales or persons, living or dead, is entirely coincidental.
- The rest is told exactly as it occurred.
- **Warning**: this presentation might contain memes…

The Problems

- TCP rather than HTTP
- SSL/TLS
- Certificate Pinning
- Runtime manipulation
- Patching the application
- ProKSy – revealed for the first time…

Day 1: I Got This!

- Let's use BURP! - set the HTTP Proxy (option in tool)
- Nothing happens…
- Looking at WireShark
- Port 1XXXX TLS - Not HTTP!

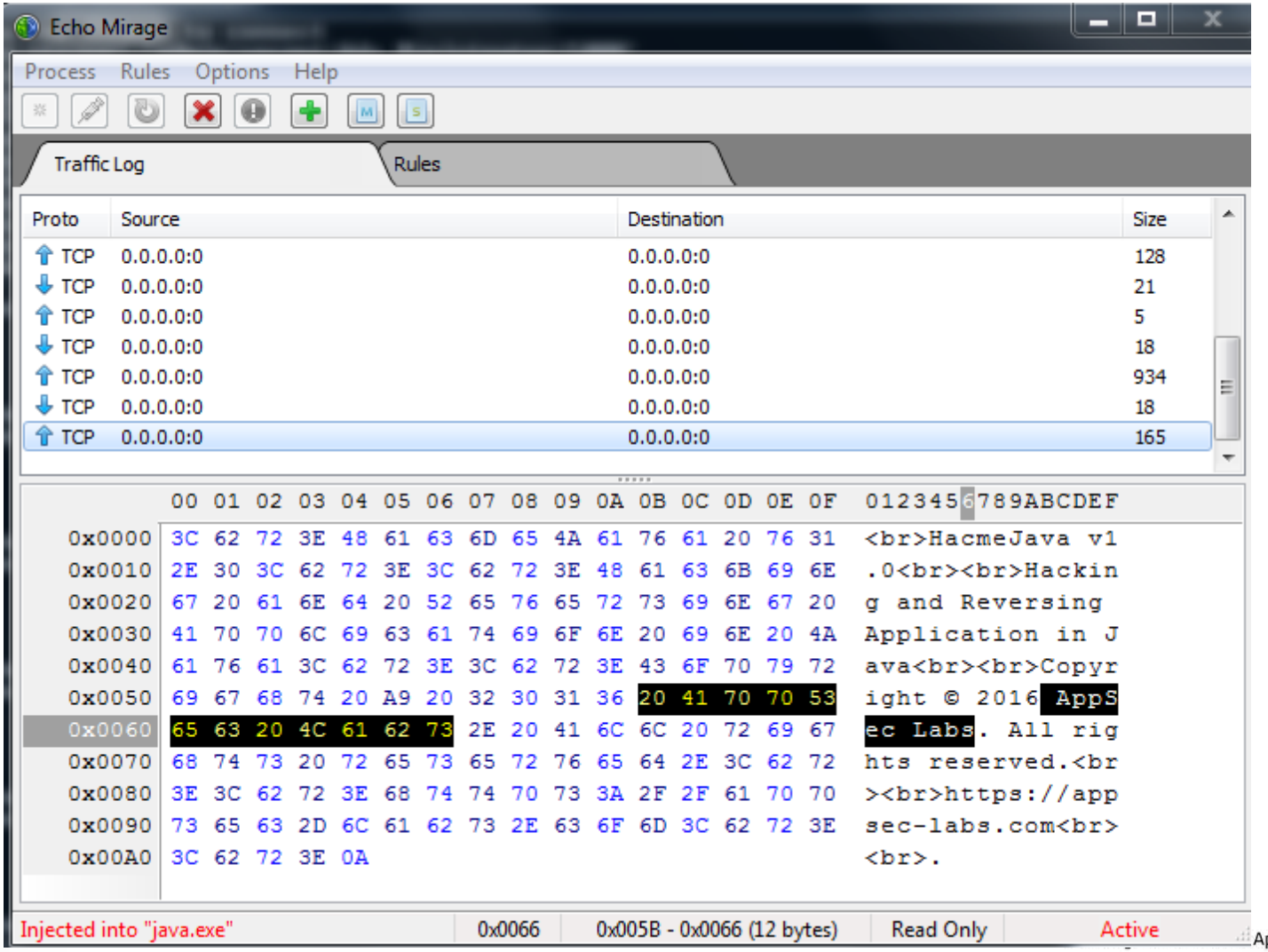
- Sure, let use AppSec Labs' incredible TCP proxy tool (TBC)

Problem #1: No HTTP/S

- We all Burp (nothing to be ashamed about)
- But what if…
  the application is not communicating over HTTP(s)?

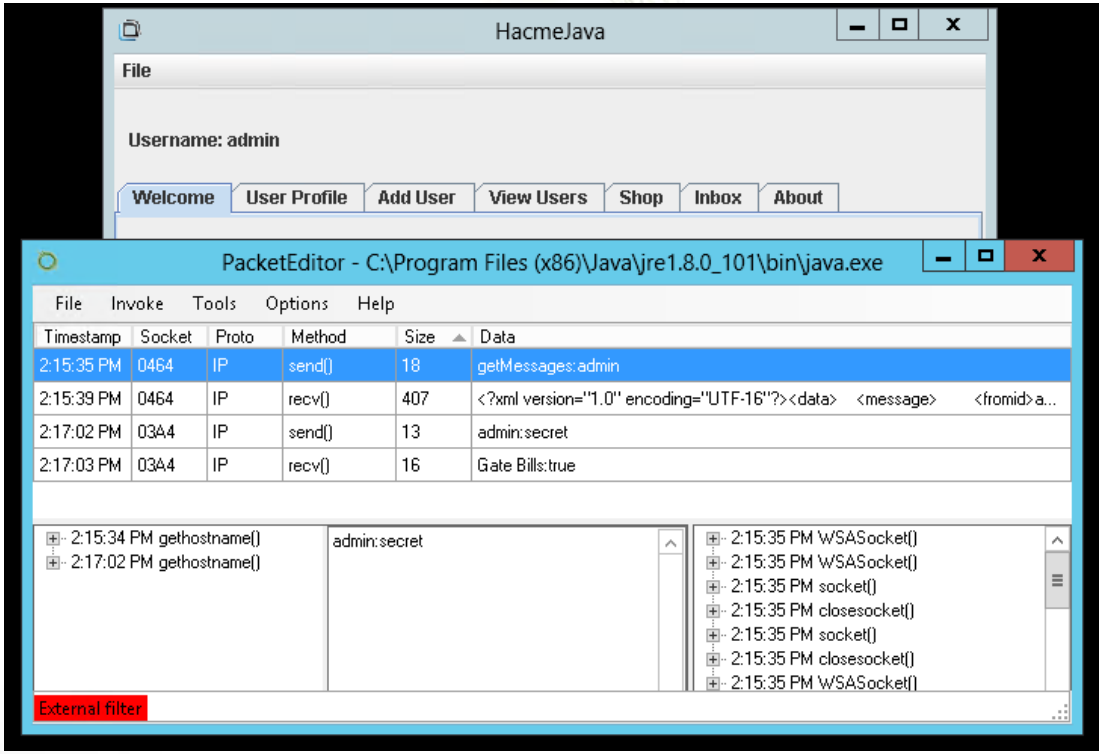
Echo Mirage – by Wildcroft Security

- Link: unknown (good luck with FileHippo)



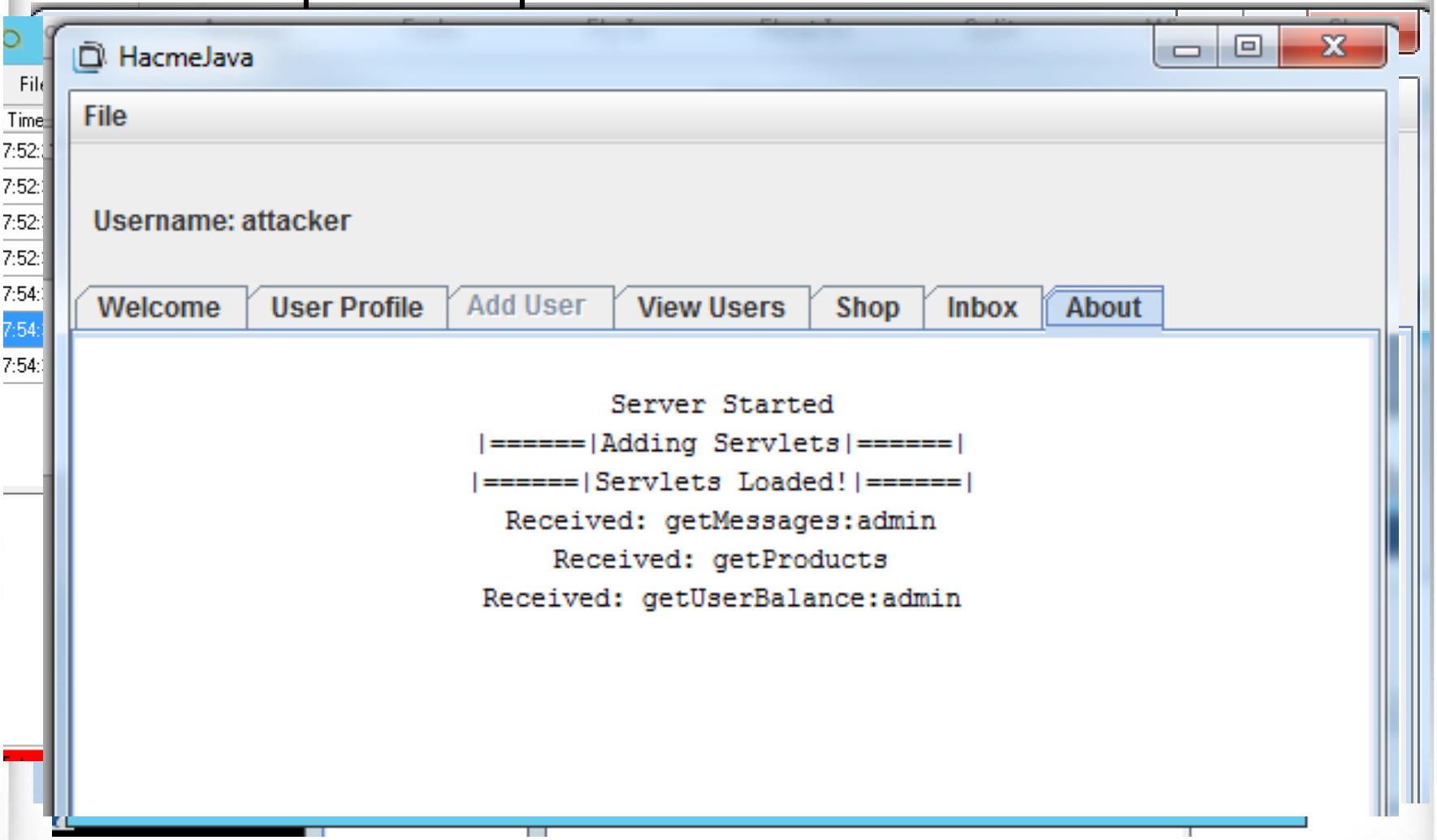
Advanced Packet Editor

- https://appsec-labs.com/advanced-packet-editor/
- https://github.com/appsec-labs/Advanced_Packet_Editor
- Based on:



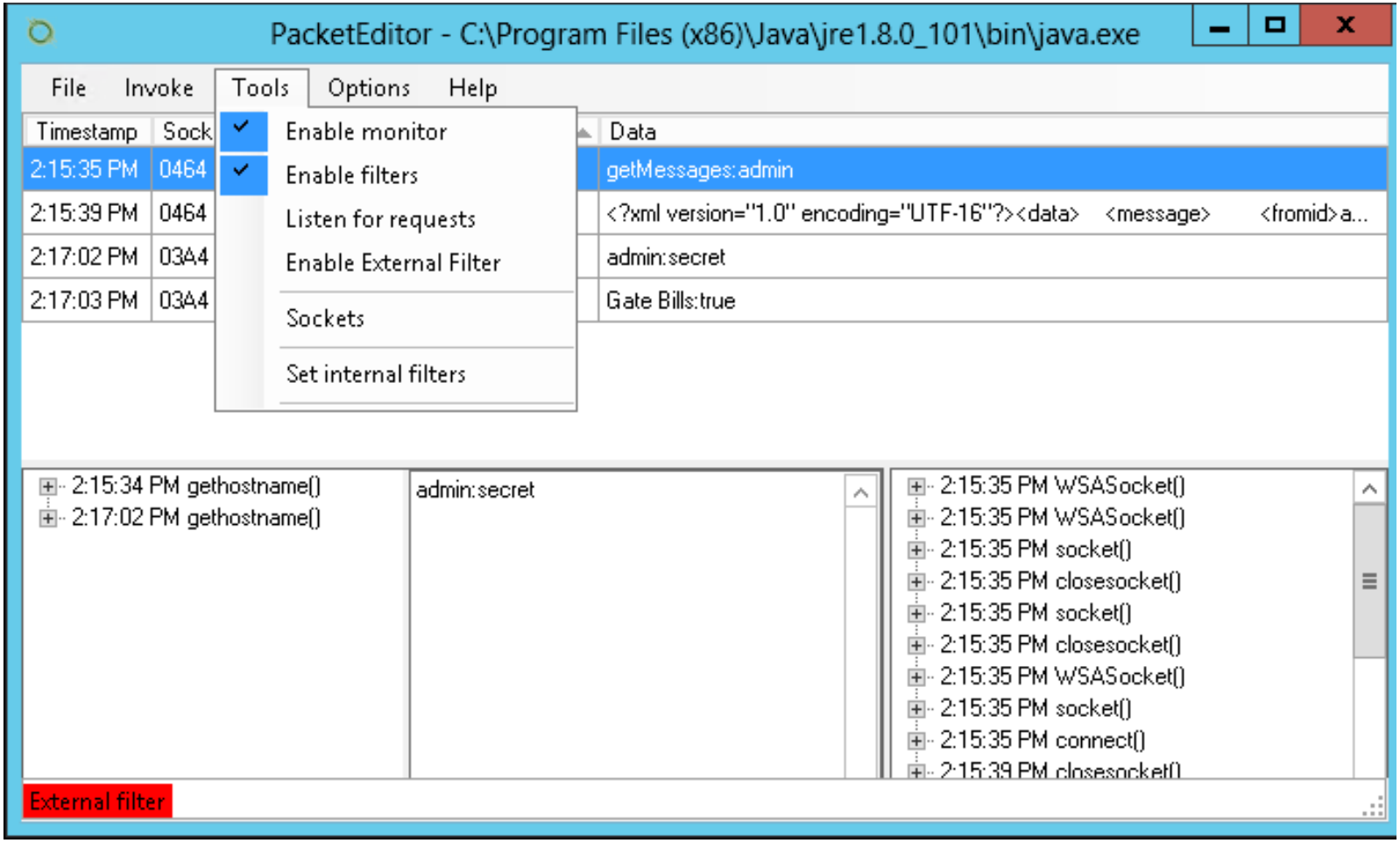
APE

- Intercept & tamper with TCP-based comm



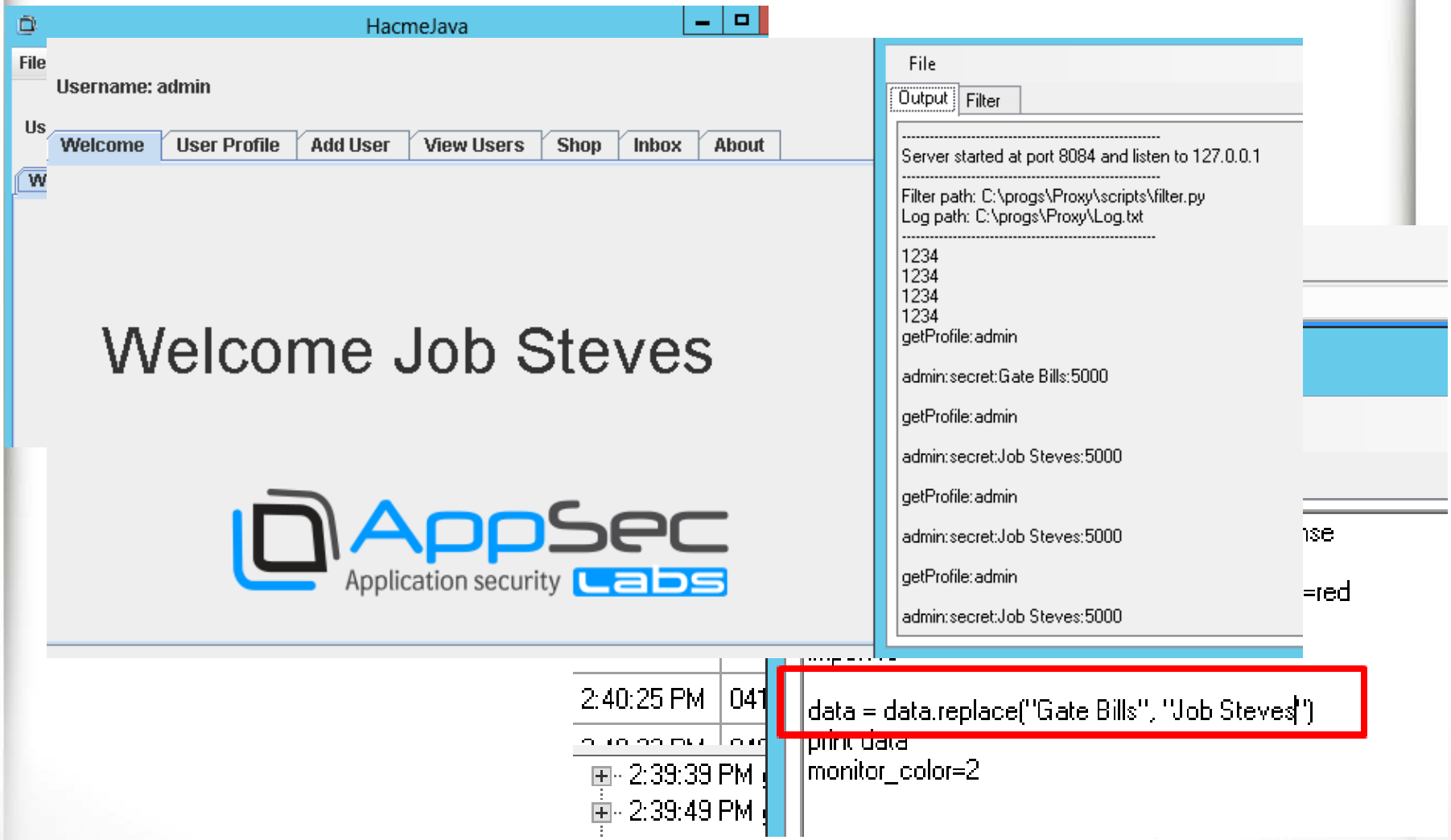
APE

What's new



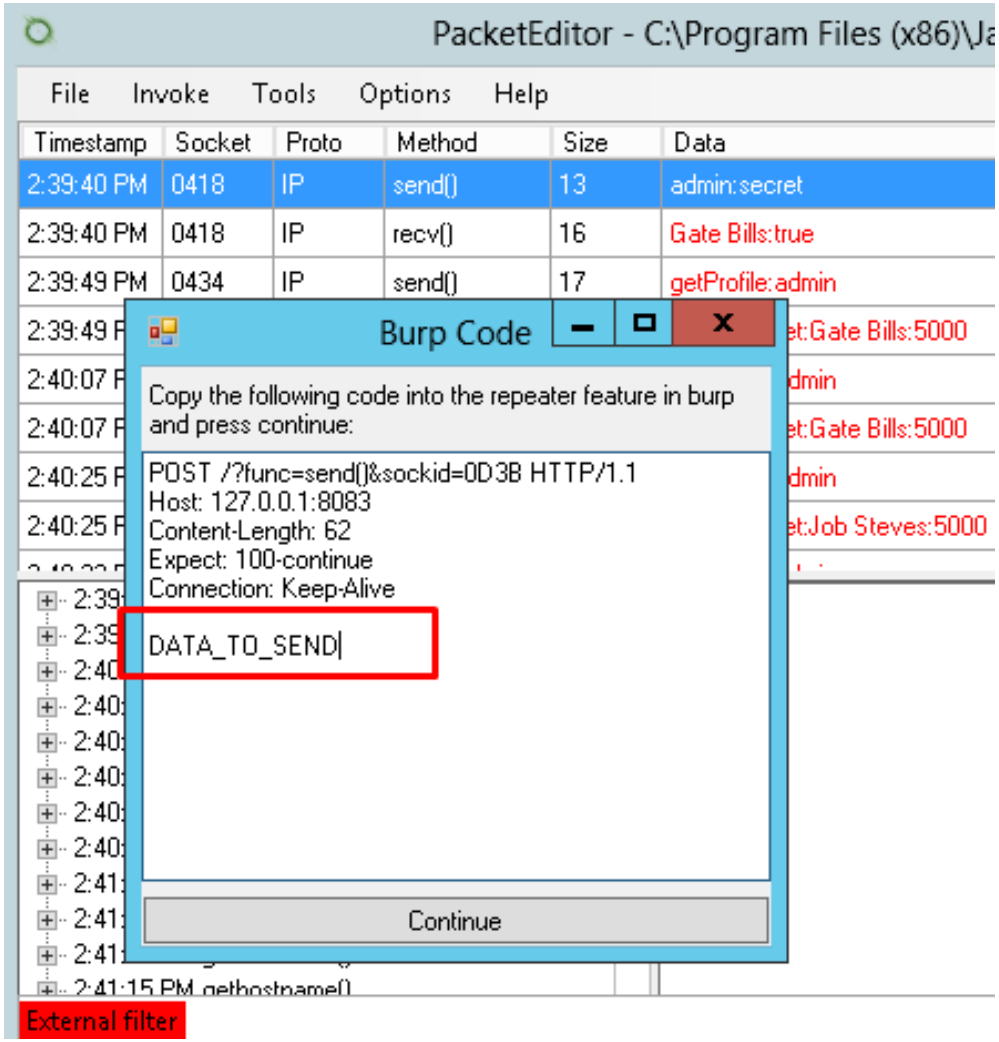
APE

- External Filter – python based



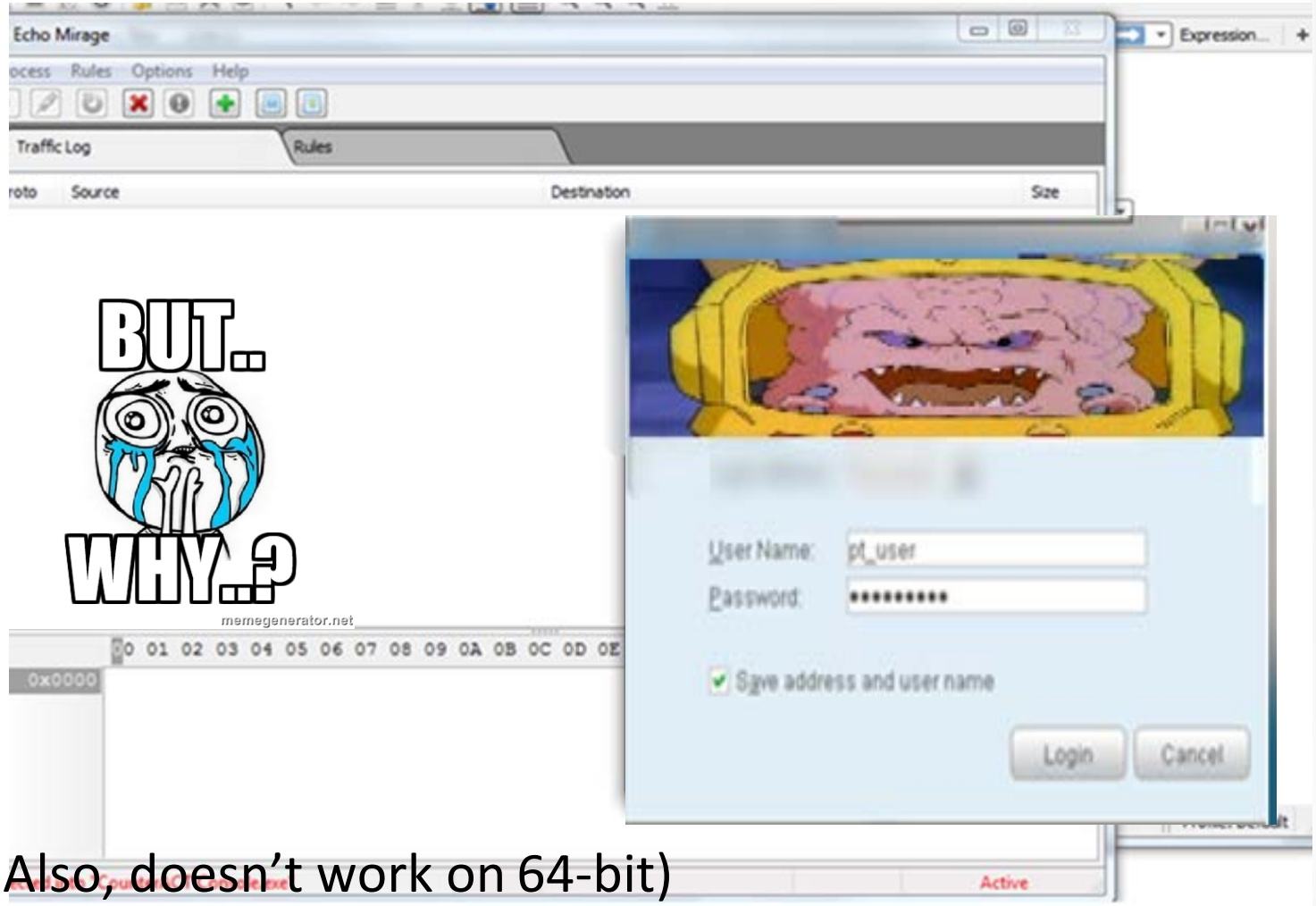
APE – Listen to Requests

- HTTP/S? – Why not integrating with Burp?



What Really Happened?

- Nothing! Probably SSL…



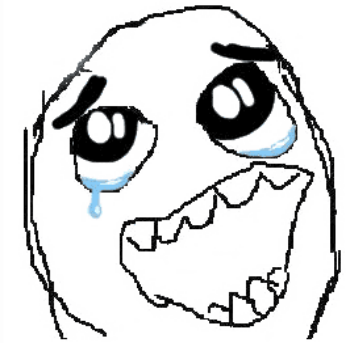
- (Also, doesn't work on 64-bit)

What Else is There?

- Stcppipe
  http://aluigi.altervista.org/mytoolz/stcppipe.zip

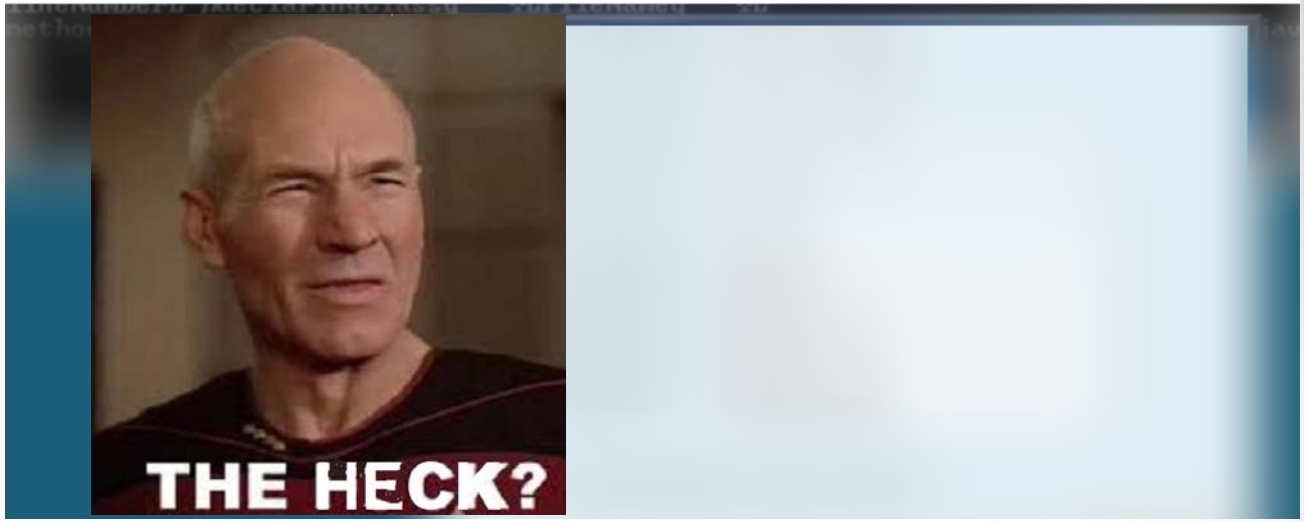
```
Simple TCP proxy/datapipe 0.4.8b
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org


Usage: stcppipe.exe [options] <dest*> <dest_port> <local_port>

Options:
-b HOST   local IP or hostname of the interface to bind, used for security
          10.0.0.105 127.0.0.1
-B IP     as above but works only for the outgoing socket, this means you can
          decide to use a secondary interface for connecting to the host (for
          example using the wi-fi connection instead of the main one)
-d DIR    dump the content of the connections in various tcpdump-like cap files
-D        dump the content of the connections directly here on stdout
-S        enable SSL, both input and output are handled as SSL (good for MITM)
-X M C P options for specifying a custom SSL method M, a certificate file C and
          the needed password P for its private key. by default this tool uses
          method 23 (choices: ssl2, ssl3, tls1, dtls1, 23) and a passwordless
          certificate, use "" for keeping the default fields values
-Y NUM    1 for incoming SSL and destination in plain-text
          2 for incoming plain-text and destination SSL
          3 for incoming and outgoing SSL (default, exactly like -S)
-a IP1,HOST2,...,HOSTn,IPn
          list of IP addresses and hostnames to which allow the access.
          useful for granting access only to a limited amount of trusted IPs
-r H*:P   reverse, this tool will connect to H:P from local_port and then will
          create a connection with dest:dest_port, useful for bypassing NATs.
          local_port equal to 0 for any available. try reconnect in one second
-M        in case of multiple destinations this option allows to connect to all
          the hosts at the same time sending and receiving the data from them
-c NUM    set the maximum number of incoming connections
-q        quiet output, no informations about incoming connections
-p        increase process priority
-x X      stupid XOR function, use X equal to 1 for XORing the data sent through
          local_port with the byte 0xff or 2 for dest_port, interesting for
          doing browsers -> "stcppipe -x 1" ->internet-> "stcppipe -x 2" -> proxy
-s S1 S2  substituite all the occurrences of the S1 string in the connection's
          data with S2. NOTE that this option is experimental since works only
          on the same block of data (so if S1 is half in one packet and half in
          another one it will be NOT modified)
```

A Fraction of Hope…



```
C:\Users\evaluation\Desktop>stcppipe.exe -D -S 192.168.1.30 13000 13000

Simple TCP proxy/datapipe 0.4.8b
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- local port      13000
- remote hosts:   192.168.1.30:13000
- wait connections:
IN  192.168.1.29:1463
OUT 192.168.1.30:13000
```

```
ac ed 00 05 75 72 00 13  5b 4c 6a 61 76 61 2e 6c  |....ur..[Ljava.l|
61 6e 67 2e 4f 62 6a 65  63 74 3b 90 ce 58 9f 10  |ang.Object;..X..|
73 29 6c 02 00 00 78 70  00 00 00 03 73 72 00 47  |s)l...xp....sr.G|
6f 72 67 2e 61 70 61 63  68 65 2e 6d 79 66 61 63  |org.apache.myfac|
65 73 2e 61 70 70 6c 69  63 61 74 69 6f 6e 2e 54  |es.application.T|
72 65 65 53 74 72 75 63  74 75 72 65 4d 61 6e 61  |reeStructureMana|
67 65 72 24 54 72 65 65  53 74 72 75 63 74 43 6f  |ger$TreeStructCo|
6d 70 6f 6e 65 6e 74 46  59 17 d8 9c 4a f6 cf 02  |mponentFY...J...|
```



Side Note: De/Serialization

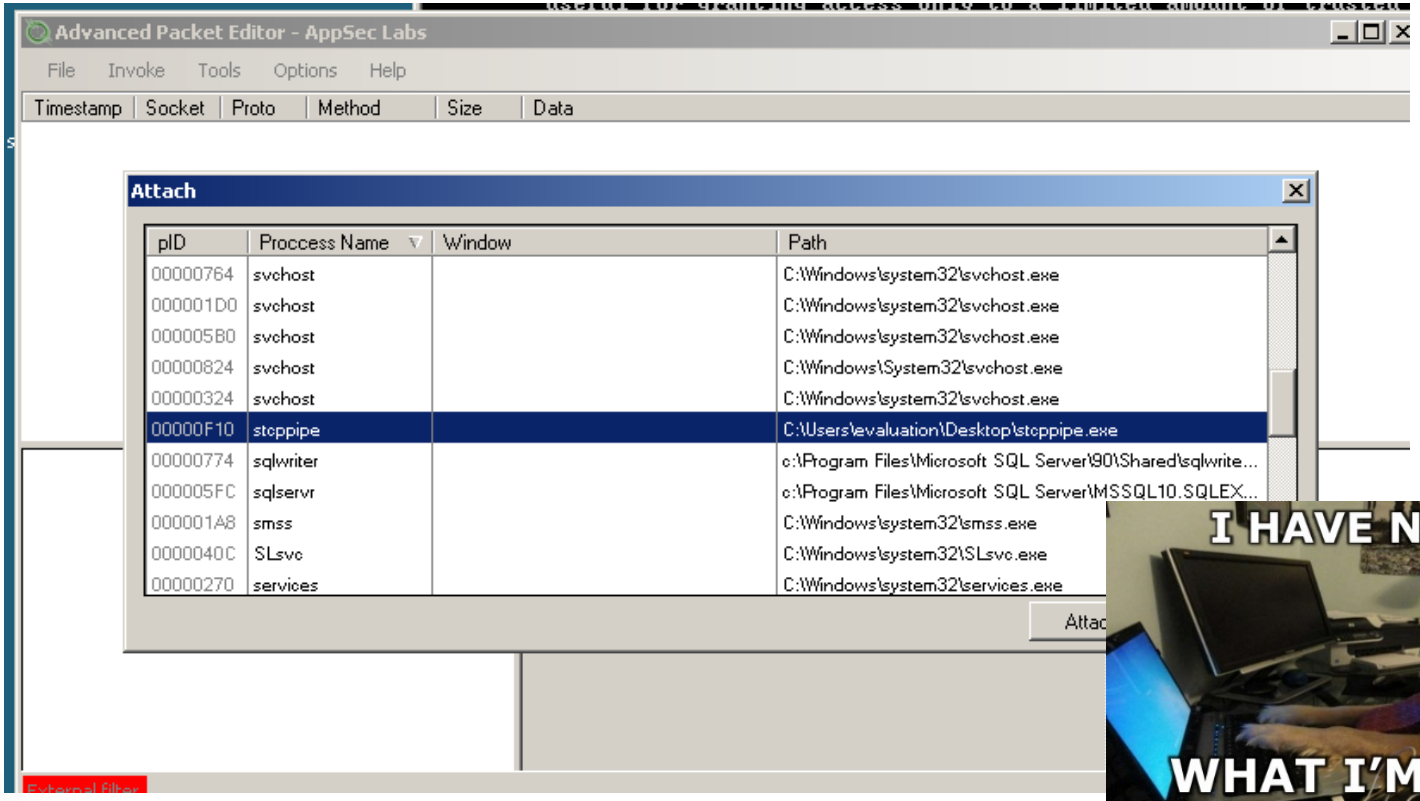
- What is Serialization
  - Converting the state of data to a byte stream so that the byte stream can be reverted back into a copy of the object
- What is the problem?
  - Deserialization of untrusted data
- What does that mean?
  - De-serializing data coming from the client could abuse the application logic, deny service, or execute arbitrary code.
- What to look for?
  - ObjectInput.readObject()
  - Externalizable.readExternal()
  - Serializable.readResolve()
  - ObjectOutputStream.replaceObject()
  - ObjectInputStream.readUnshared()
  - Many more…

All You Need to Know…

- You can find everything here:
  - https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet
  - https://github.com/njfox/Java-Deserialization-Exploit
- PayPal RCE (2016)
  - http://artsploit.blogspot.co.il/2016/01/paypal-rce.html
- Burp Extension
  - https://github.com/NetSPI/JavaSerialKiller
  - https://github.com/federicodotta/BurpJDSer-ng-edited
  - https://appsec-labs.com/belch/
- Scanner
  - https://github.com/federicodotta/Java-Deserialization-Scanner
- Code Analyzer
  - https://github.com/mbechler/serianalyzer

Where Were We?

- I can see the traffic, but how do I tamper with it?
- Tunnel “stripped” traffic onto APE!
- We need to inject APE into stcppipe



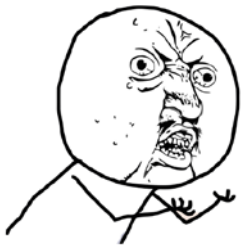
And… Fail #1

- APE got the encrypted data

PacketEditor - C:\Users\evaluation\Desktop\stcppipe.exe

File Invoke Tools Options Help

Timestamp	Socket	Proto	Method	Size	Data
6:39:07 PM	0064		recv()	11	┬└└ Z V└└
6:39:07 PM	0064		recv()	84	WQ¤· O·íjm© «.Îî÷˜ ¤Ih¶Lÿ ♀┬ 3 / 2 ‼ ! ↑ ┬─└ |└| ┘└ └└└ ┐└ ┐┐ÿ
6:39:07 PM	0064		send()	889	┬└└ Q┐ M└└WQ¤8·¡♀‼▯¥Ä`ÈiOE┬é¹ Ä¬ñÅI™→▯ ÷JßUIG¥4yèY4þ_@ sgmí³élf¿ô[|ÿ ┬└└└♪ └◀ └ß...
6:39:07 PM	0064		recv()	5	┬└└ ▯
6:39:07 PM	0064		recv()	134	┼ , ▯*1ſã▯ÕQIã♬½ÄÜMÆØ|ÉO–ªſb◀¼ístmÝa]§[Bv¯ãQv«t{¹«Cx.MWÅ§¯Ä;Ù¶♬▯þ¯üÛ&<Çß%Ûóú℞¼à0Õh?({ſL...
6:39:07 PM	0064		recv()	5	¶└└
6:39:07 PM	0064		recv()	1	
6:39:07 PM	0064		recv()	5	┬└└ 0
6:39:07 PM	0064		recv()	48	øyKW/àÑ£×¡þCOhØÊØ)├Ihcøÿ¡p1ä├aï<^÷fôfD
6:39:07 PM	0064		send()	59	¶└└ ┬└└ 0úRc¦©¨$Ç9Å.◘Ã{ùS·‰bnB/{«┼└ ÚLÔS¤!«ÿB: ½#v
6:39:07 PM	0068	TCP	send()	351	] └└ D ┼ À0 À, À(À$ À¶ À À'' À! £ Ÿ k ¡ 9 8 ^ ‡ À├ À § m : ‰ À2 À. À* À& À...

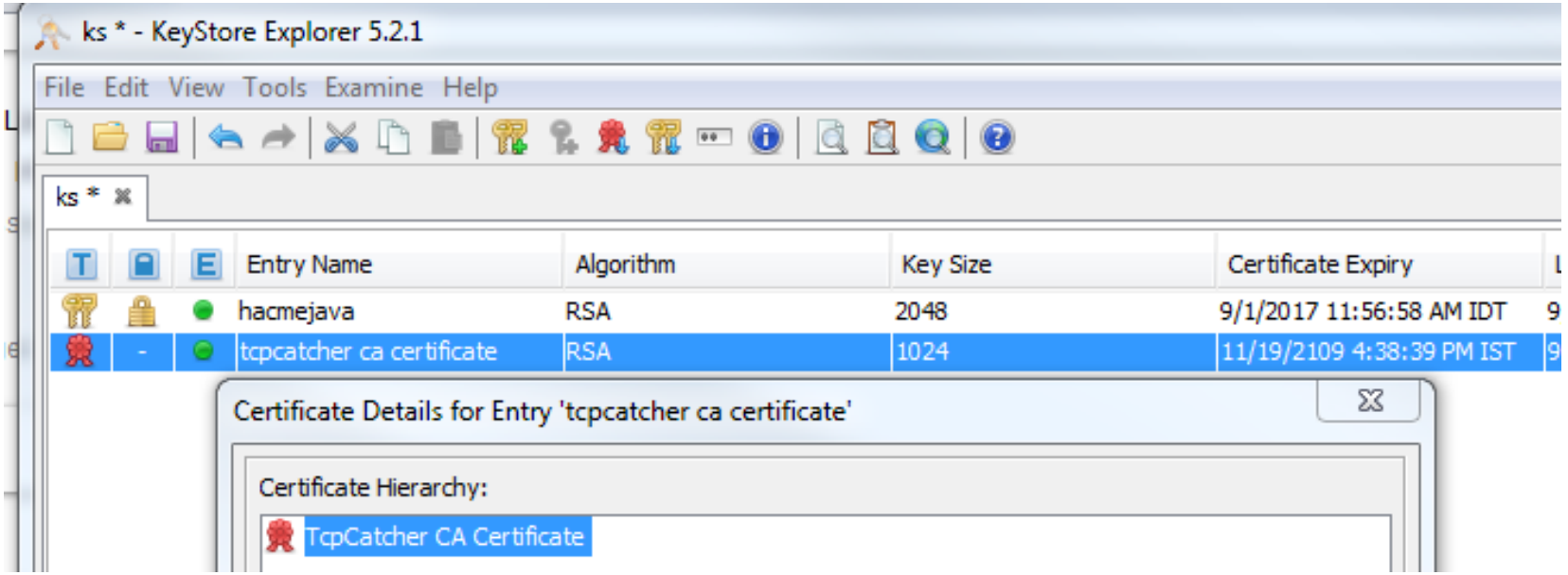


- 6:39:07 PM socket()
- 6:39:07 PM bind()
- 6:39:07 PM connect()
- 6:39:07 PM closesocket()
- 6:39:07 PM closesocket()

External filter

How Do We Intercept TCP Over SSL?

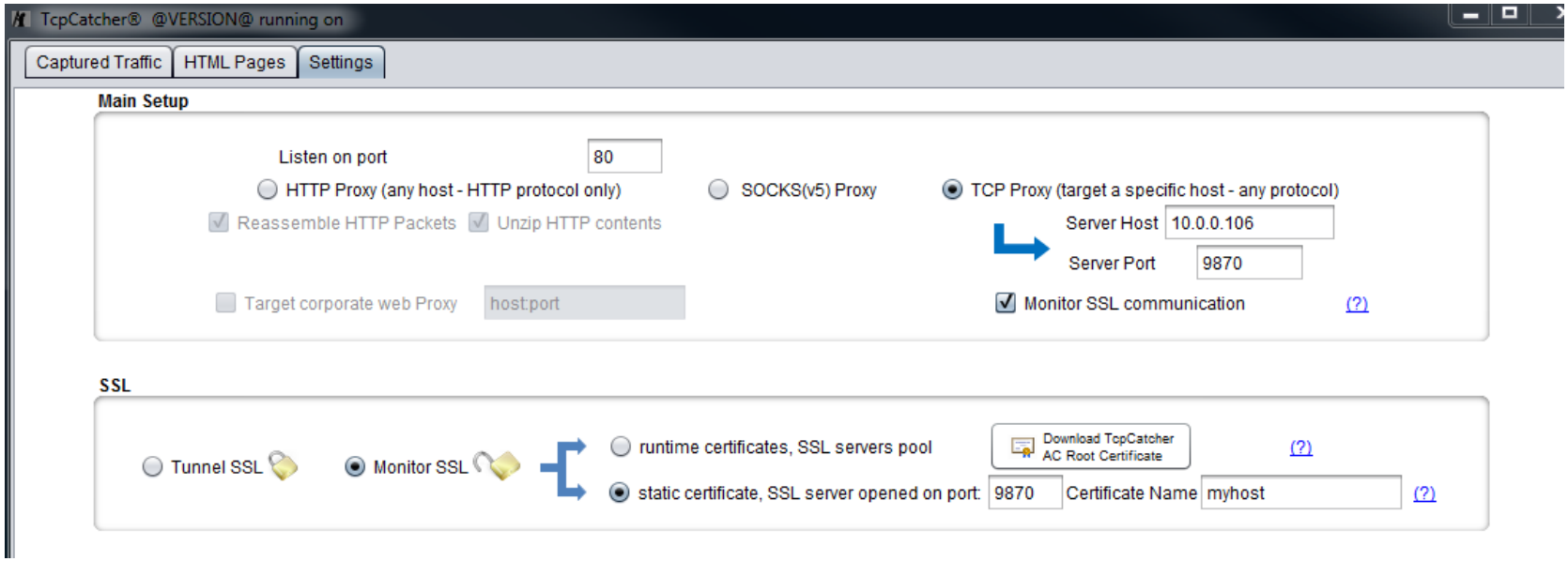
- Download **TcpCatcher**
  http://www.tcpcatcher.org/
- Download TcpCathcer's root certificate
- Install it as a RootCA in the KeyStore



- Download **KeyStore Explorer**
  http://www.keystore-explorer.org/

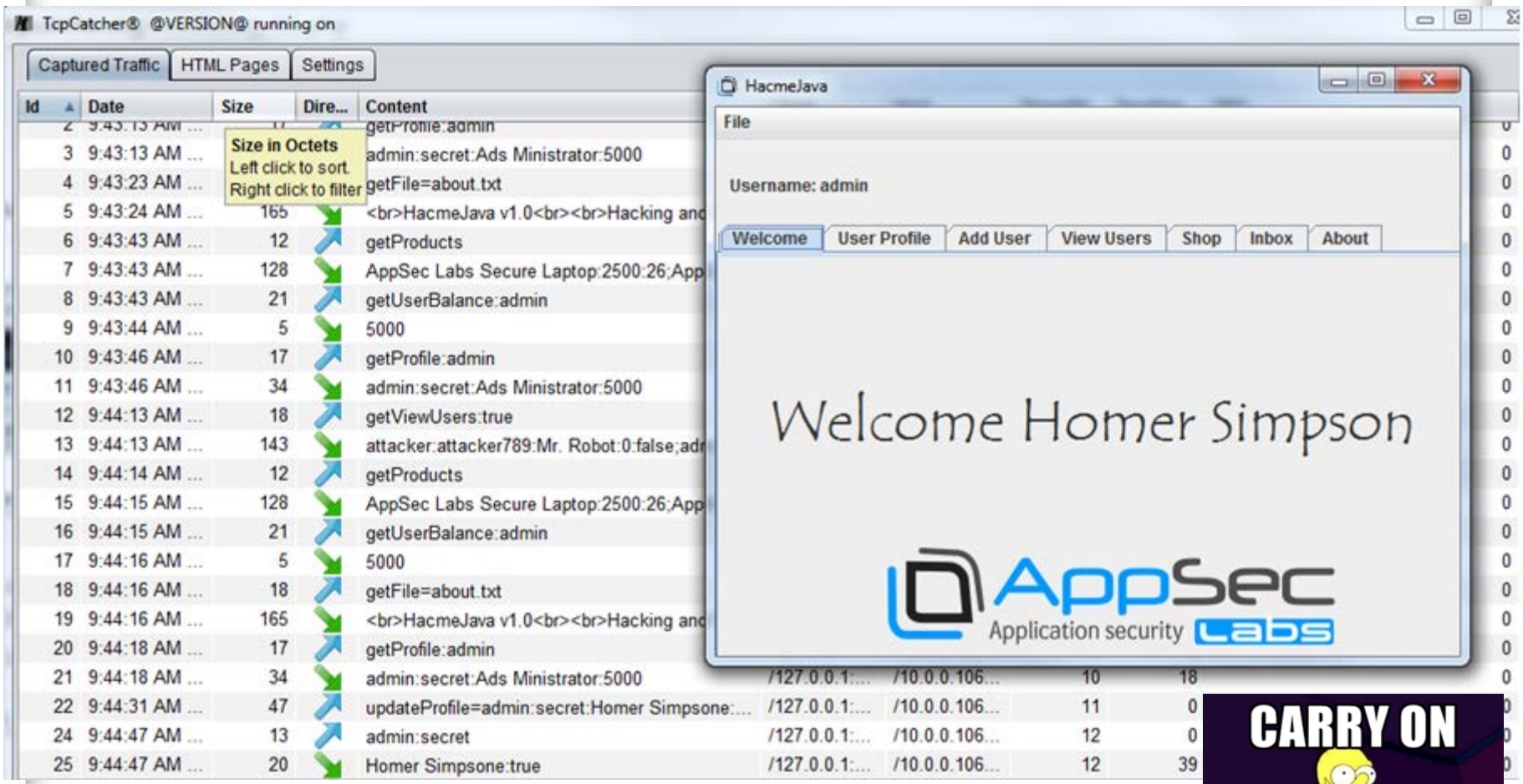
How Do We Intercept TCP Over SSL?

- Configure TcpCatcher to communication with both, the client and the server



- TcpCatcher will now serve as a MitM.

Woohoo!


TcpCatcher® @VERSION@ running on
Captured Traffic
HTML Pages
Settings
Id
Date
Size
Dire...
Content
Size in Octets
Left click to sort.
Right click to filter
3 9:43:13 AM ... admin:secret:Ads Ministrator:5000
4 9:43:23 AM ... getFile=about.txt
5 9:43:24 AM ... 165
HacmeJava v1.0

Hacking and
6 9:43:43 AM ... 12 getProducts
7 9:43:43 AM ... 128 AppSec Labs Secure Laptop:2500:26;App
8 9:43:43 AM ... 21 getUserBalance:admin
9 9:43:44 AM ... 5 5000
10 9:43:46 AM ... 17 getProfile:admin
11 9:43:46 AM ... 34 admin:secret:Ads Ministrator:5000
12 9:44:13 AM ... 18 getViewUsers:true
13 9:44:13 AM ... 143 attacker:attacker789:Mr. Robot:0:false;adr
14 9:44:14 AM ... 12 getProducts
15 9:44:15 AM ... 128 AppSec Labs Secure Laptop:2500:26;App
16 9:44:15 AM ... 21 getUserBalance:admin
17 9:44:16 AM ... 5 5000
18 9:44:16 AM ... 18 getFile=about.txt
19 9:44:16 AM ... 165
HacmeJava v1.0

Hacking and
20 9:44:18 AM ... 17 getProfile:admin
21 9:44:18 AM ... 34 admin:secret:Ads Ministrator:5000 /127.0.0.1:... /10.0.0.106... 10 18
22 9:44:31 AM ... 47 updateProfile=admin:secret:Homer Simpsone:... /127.0.0.1:... /10.0.0.106... 11 0
24 9:44:47 AM ... 13 admin:secret /127.0.0.1:... /10.0.0.106... 12 0
25 9:44:47 AM ... 20 Homer Simpsone:true /127.0.0.1:... /10.0.0.106... 12 39
HacmeJava
File
Username: admin
Welcome
User Profile
Add User
View Users
Shop
Inbox
About
Welcome Homer Simpson
AppSec
Application security
Labs


CARRY ON
IM HERE FOR THE COMMENTS

What Really Happened?

- It didn't work!
- Let's say I got this……


```
C:\Users\keizer\Desktop\OWASP>java -jar HacmeJavaClient_SSL.jar SSL
C=GB, ST=hacme.java, L=hacme.java, O=hacme.java, OU=hacme.java, CN=hacme.java
Please, do not try to MitM me!
```

- Let's decode:

Login.class

```
205         System.setProperty("javax.net.ssl.trustStore", "ks");
206         SSLSocketFactory sslsocketfactory = (SSLSocketFactory)SSLSocketFactory.getDefault();
207         HostnameVerifier hnf = new HostnameVerifier()
            {
              public boolean verify(String arg0, SSLSession arg1)
              {
                try
                {
211               Certificate cert = arg1.getPeerCertificates()[0];
212               X509Certificate x = X509Certificate.getInstance(cert.getEncoded());
213               System.out.println(x.getSubjectDN().getName());
214               String owasp = "OWASP IL";
215               X500Name owner = new X500Name(x.getIssuerDN().getName());
216               if ((owner.getOrganization().compareTo("HacmeJava, Inc.") == 0) &&
217                 (owner.getCommonName().compareTo("hacme.java") == 0) &&
218                 (owner.getLocality().compareTo("localhost") == 0) &&
219                 (owner.getOrganizationalUnit().compareTo("Insecurity") == 0) &&
220                 (owasp.compareTo(owner.getState() + " " + owner.getCountry()) == 0)) {
221                 return true;
                  }
223               return false;
```

Now, That my friends….

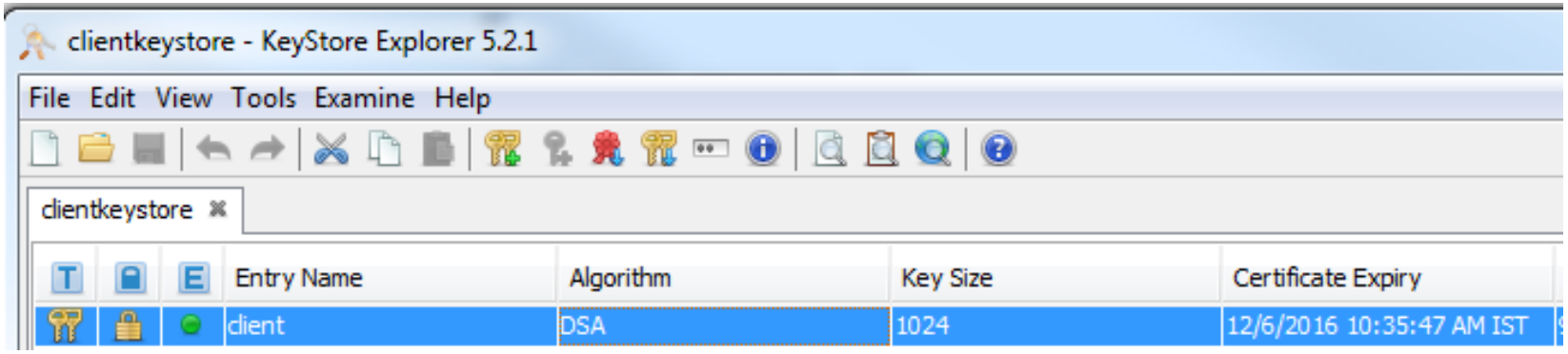
- Is SSL pinning!
- The application validates the info of the received (TcpCatcher's) certificate, against the wanted info, hardcoded in the class.
- Since it's a self-signed certificate – we could just replace it with our own.
- You passphrase is: "OpenSSL"
  - Create you own self-signed certificate
  - Fill in the required info (found in the class)
  - Install the new certificate in the KS.
  - Should do the trick!

Keytool

- keytool -keystore clientkeystore -genkey -alias client

```
C:\Users\keizer\Desktop\OWASP>keytool -keystore clientkeystore -genkey -alias client
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Who me?
What is the name of your organizational unit?
  [Unknown]:  SWAT
What is the name of your organization?
  [Unknown]:  FBI
What is the name of your City or Locality?
  [Unknown]:  USA
What is the name of your State or Province?
  [Unknown]:  N/A
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=Who me?, OU=SWAT, O=FBI, L=USA, ST=N/A, C=US correct?
  [no]:  yes
```

- keytool -keystore clientkeystore -certreq -alias client -keyalg rsa -file client.csr



But, which seems to have happened a lot

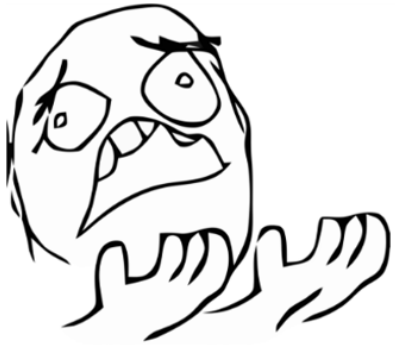
- TcpCatcher does not support using your own certificate
- only on-the-fly ones with a single value.

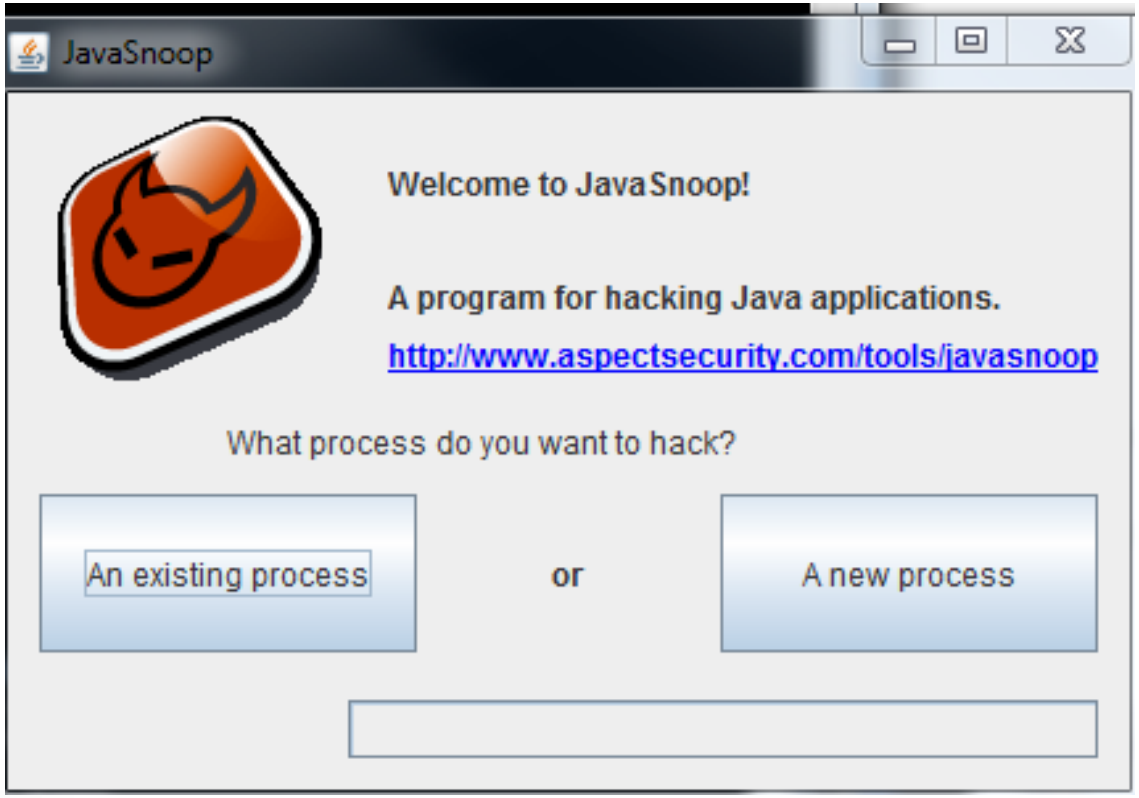
Other Possible Scenarios

- Checking that its “actually” a Root CA.
  - Create a Root CA, using OpenSSL
  - Sign your certificate with the RootCA
  - Import the new Root CA into the default KeyStore (default password: changeme)
- Pinning the Root CA
  - You might need to actually sign your own certificate
- Pinning the intermediate
  - You’ll probably have to patch the code and replace the int. public key with your own.
- Using self-created KeyStore
  - Replace the KeyStore
  - Might require some patching the bypass possible KS validations (e.g. checksum)

What do we do now?

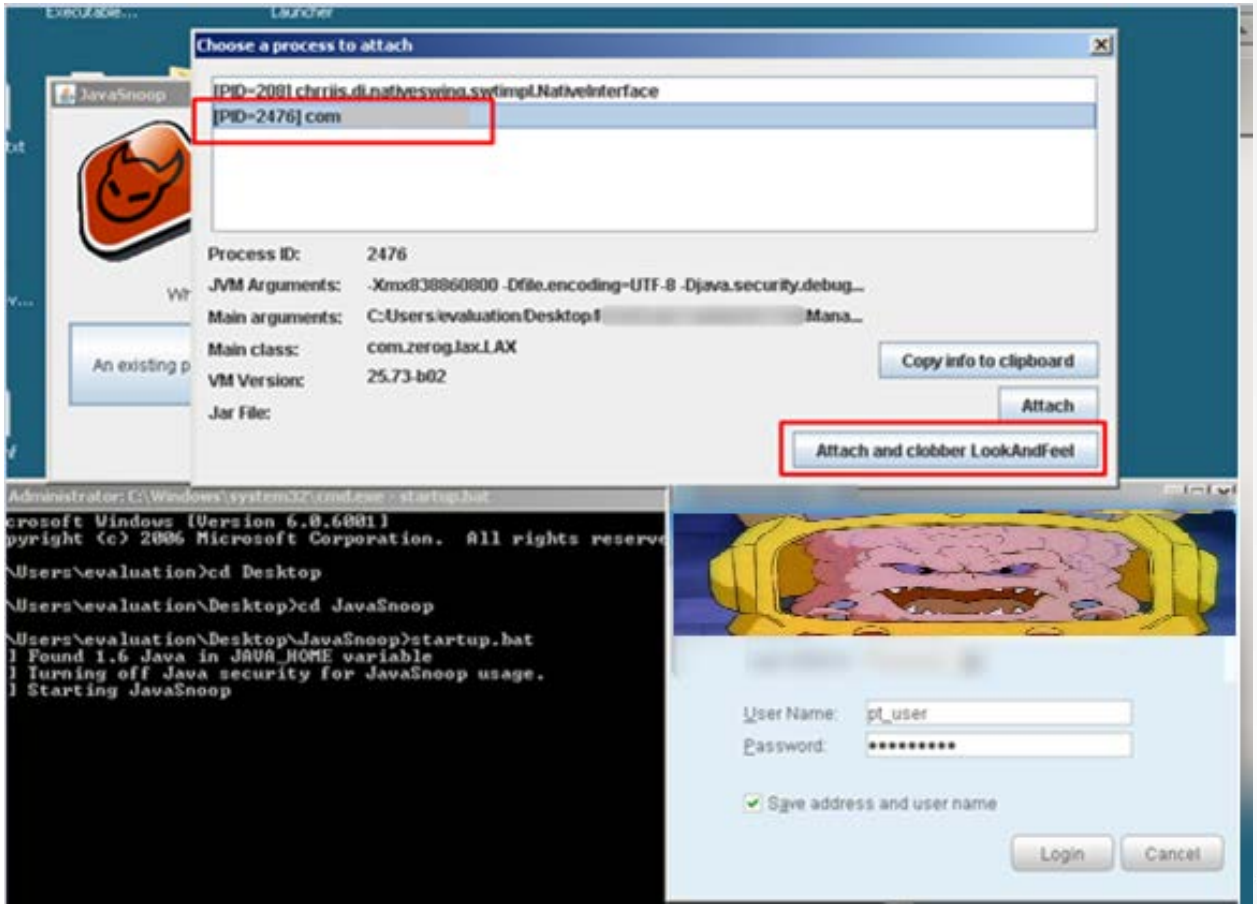
- Let's hook in runtime!
- Goodbye stcppipe.
- Hello… JavaSnoop!





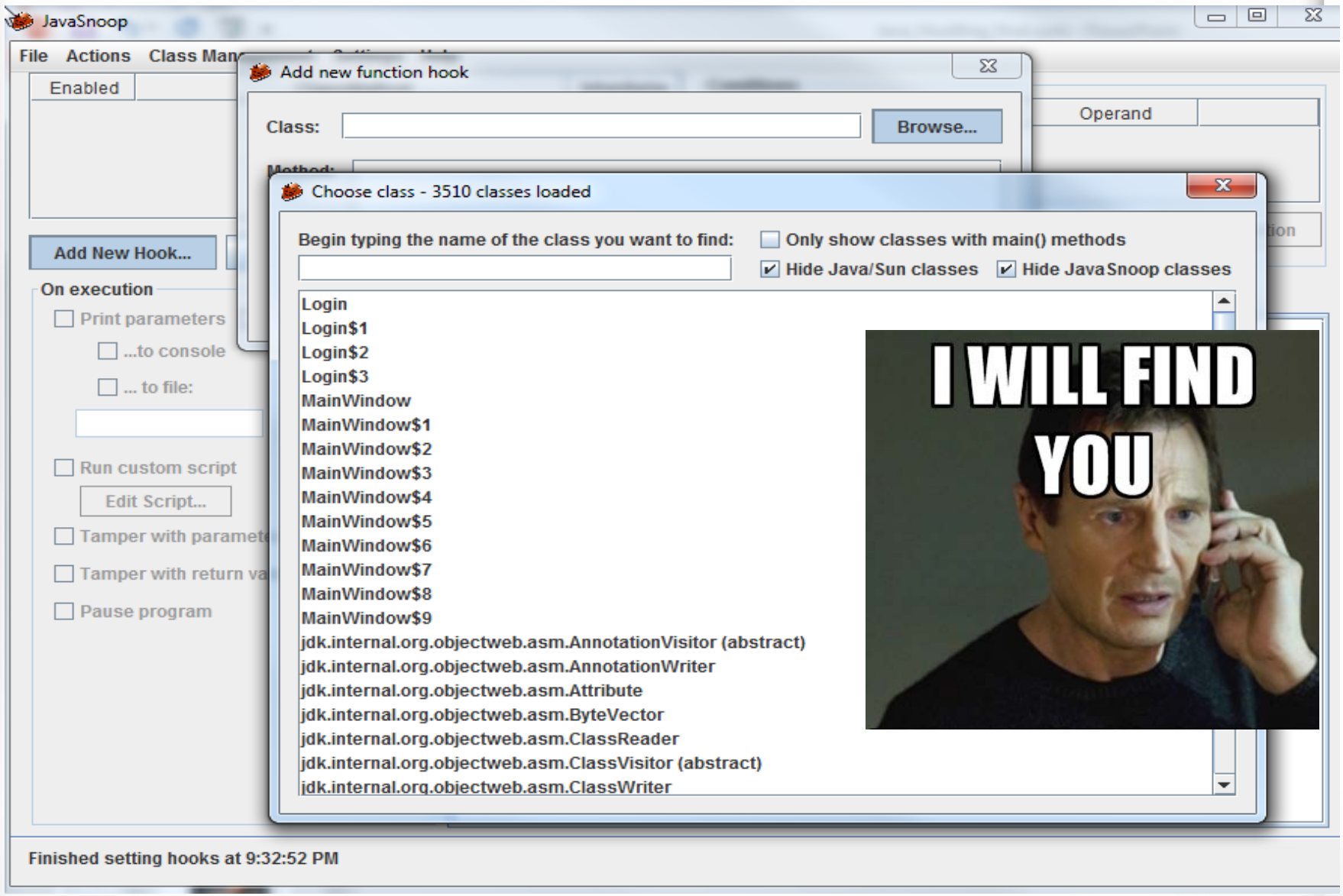
Day 2: JavaSnoop

- Attaches into any app running over JVM
- Hook methods
- Tamper with parameters, print stacks, etc.

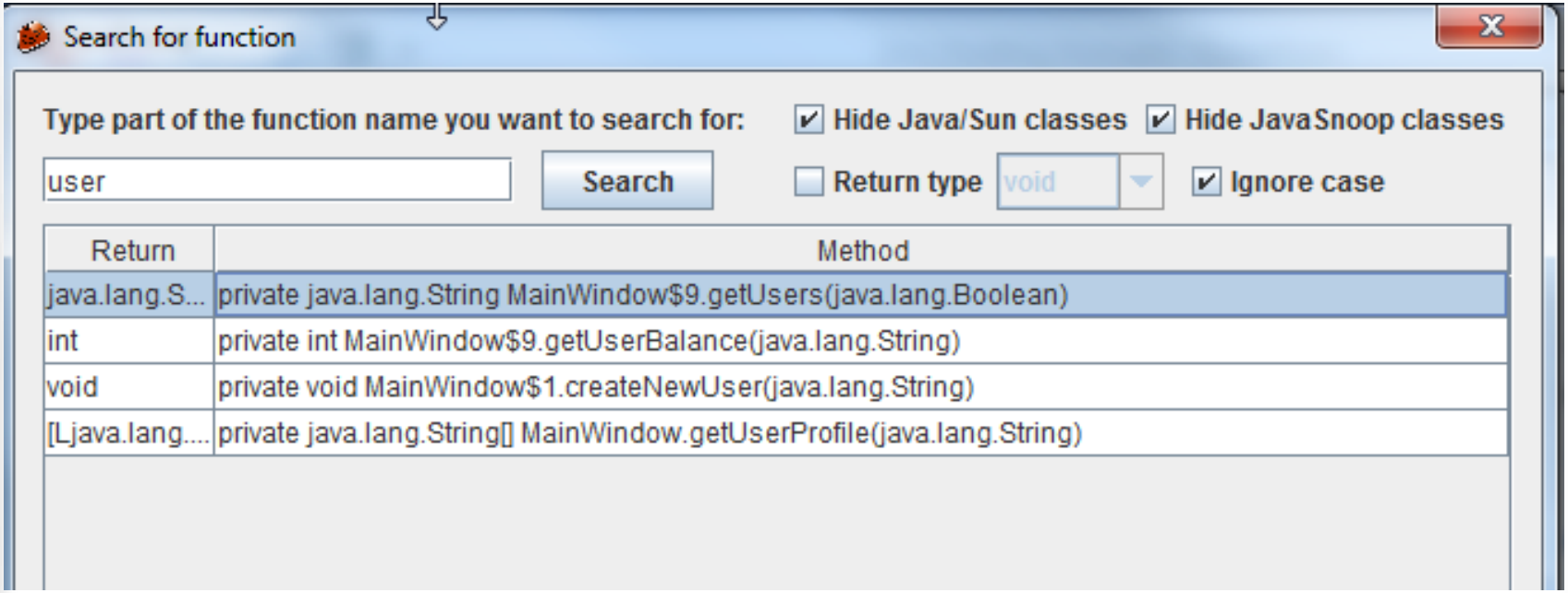


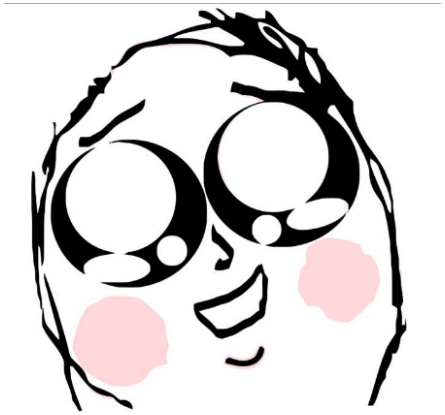
JavaSnoop

What Really Happened?

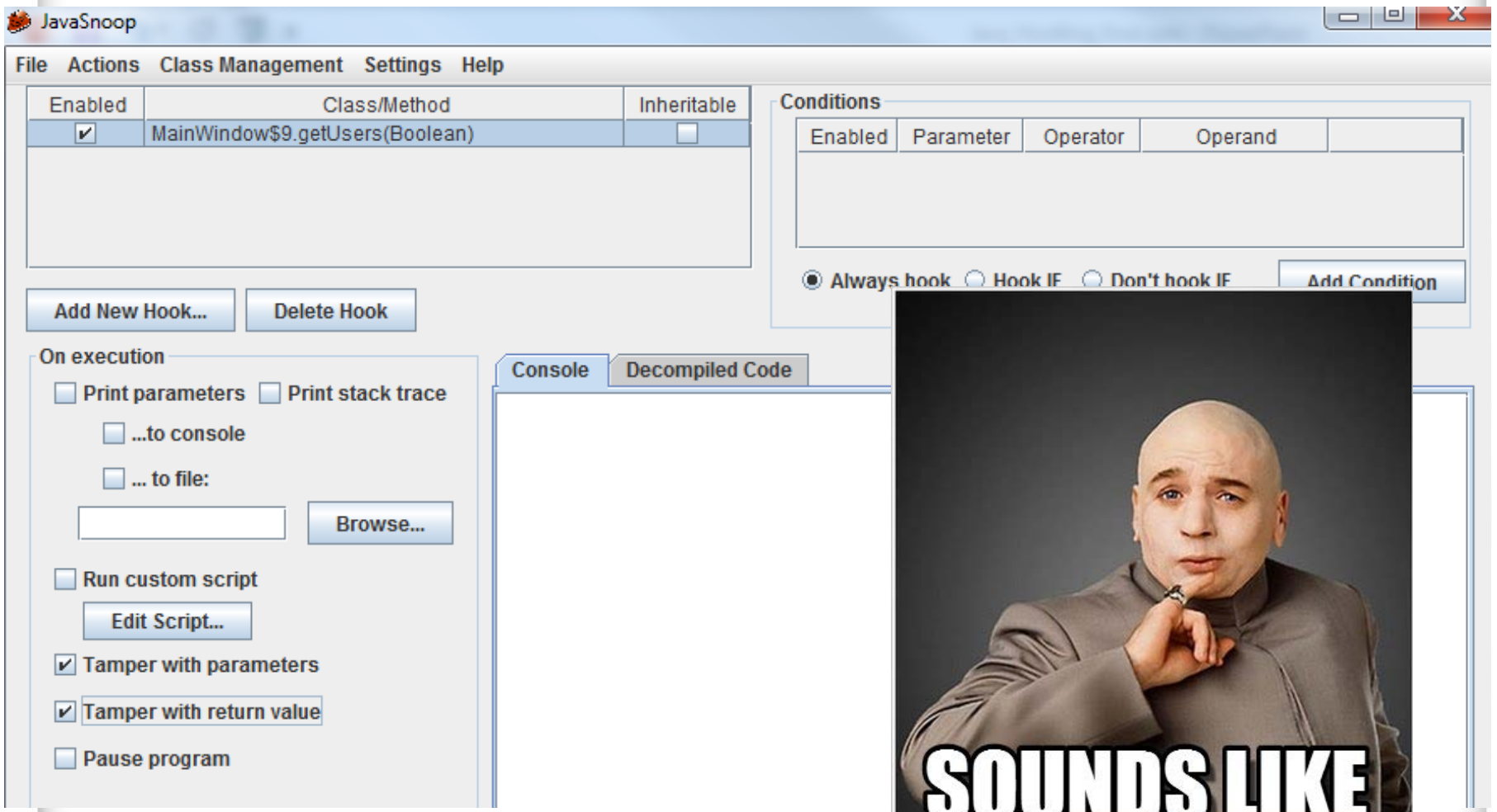


After 5 Hours (on the 2nd day!)





I Shall Call Him…



Fail #2

- Server checked the value… ☹

- What next?
- Let's patch the JAR!

Day 3: Fail #3

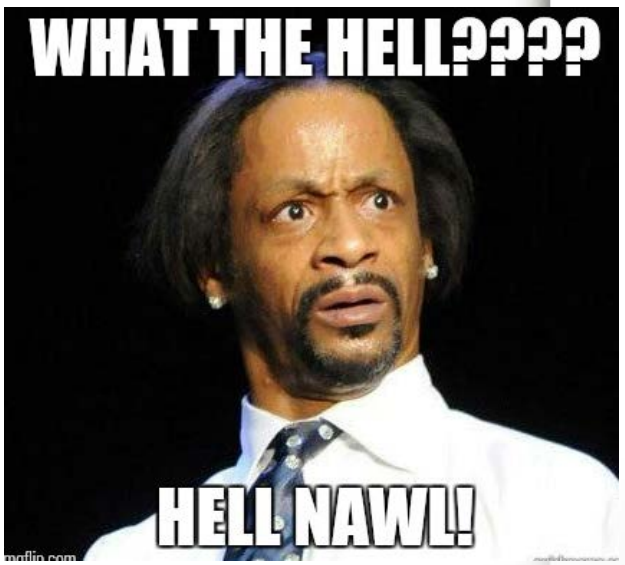
// extract jar
jar -xf myapp.jar

// pack jar
jar –cvf <desired.jar> <files>

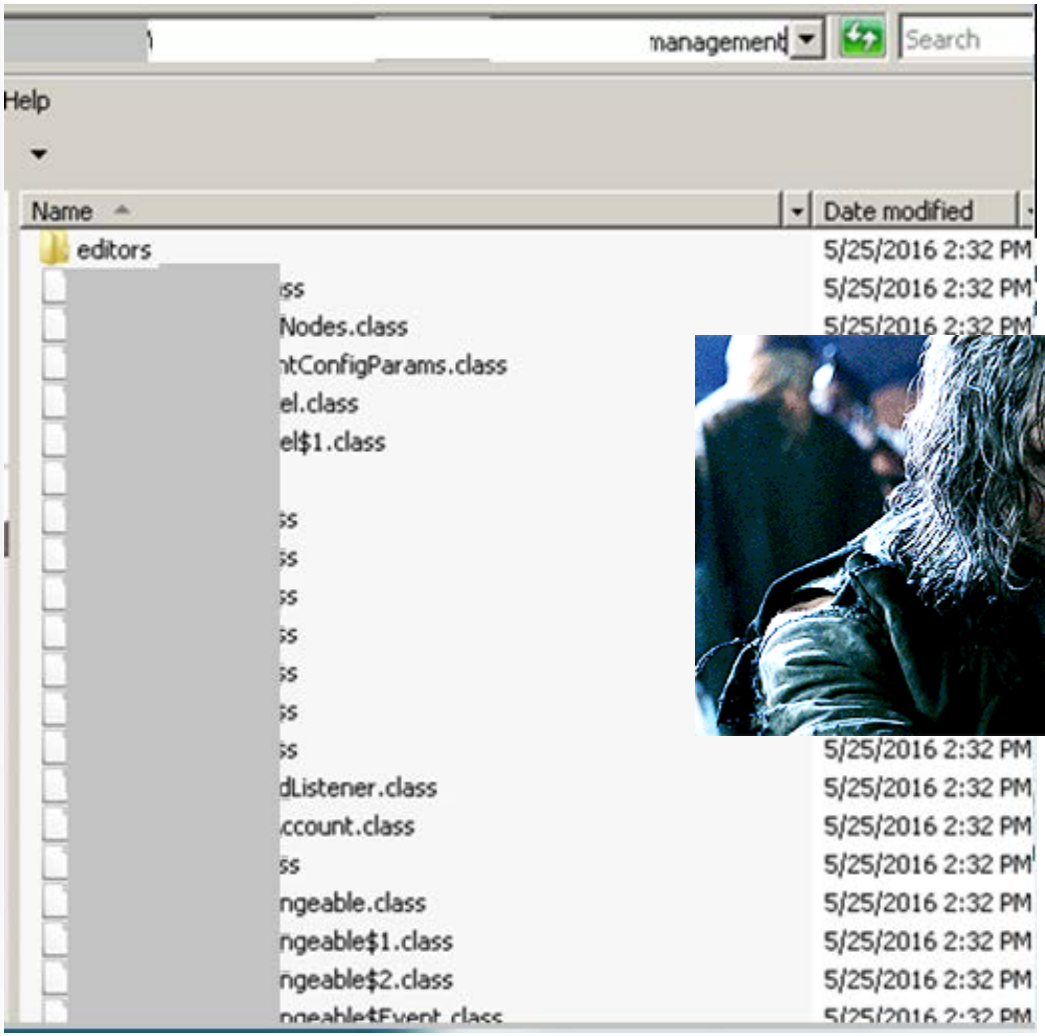
// update jar
jar -uf <file.jar> <my.class>

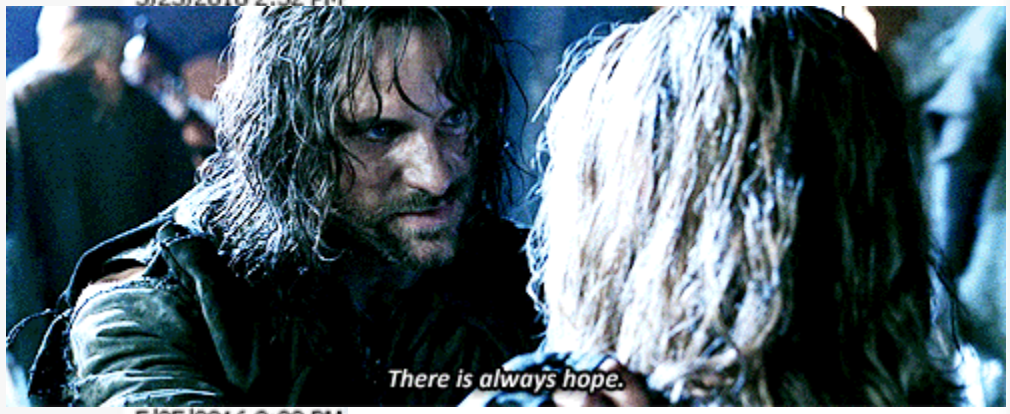
```
 Directory of C:\Users\evaluation\Desktop\temp

06/03/2016  07:57 PM    <DIR>          .
06/03/2016  07:57 PM    <DIR>          ..
11/12/2012  04:05 PM        29,272,452 [redacted].jar
               1 File(s)     29,272,452 bytes
               2 Dir(s)  19,498,246,144 bytes free

C:\Users\evaluation\Desktop\temp>jar -xf [redacted].jar

C:\Users\evaluation\Desktop\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 2808-03AA

 Directory of C:\Users\evaluation\Desktop\temp

06/03/2016  07:57 PM    <DIR>          .
06/03/2016  07:57 PM    <DIR>          ..
06/03/2016  07:57 PM    <DIR>          com
06/03/2016  07:57 PM    <DIR>          [redacted]
06/03/2016  07:57 PM    <DIR>          mseries
06/03/2016  07:57 PM    <DIR>          test
               1 File(s)     29,272,452 bytes
               6 Dir(s)  19,434,831,872 bytes free

C:\Users\evaluation\Desktop\temp>
```

```
C:\Users\evaluation\Desktop\temp>jar -cvf [redacted].jar *

= 782) (out= 448)(deflated 42%)
adding: test/[redacted]/ht/acu/simulation/port/[redacted]EventGenerator.
 = 545) (out= 323)(deflated 40%)
adding: test/[redacted]/ht/acu/simulation/ScriptC[redacted]nsts.class(in = 2799) (
3)(deflated 57%)
adding: test/[redacted]/ht/acu/simulation/Simu[redacted]riptReader$FireMessage.cl
 805) (out= 439)(deflated 45%)
adding: test/[redacted]/ht/acu/simulation/Simu[redacted]criptReader.class(in = 916
 4039)(deflated 55%)

C:\Users\evaluation\Desktop\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 2808-03AA

 Directory of C:\Users\evaluation\Desktop\temp

06/03/2016  08:00 PM    <DIR>          .
06/03/2016  08:00 PM    <DIR>          ..
06/03/2016  07:57 PM    <DIR>          com
06/03/2016  07:57 PM    <DIR>          [redacted]
06/03/2016  08:01 PM        14,405,328 [redacted].jar
06/03/2016  07:57 PM    <DIR>          mseries
06/03/2016  07:57 PM    <DIR>          test
               1 File(s)     14,405,328 bytes
               6 Dir(s)  19,420,426,240 bytes free
```



Let's Modify Classes Directly!

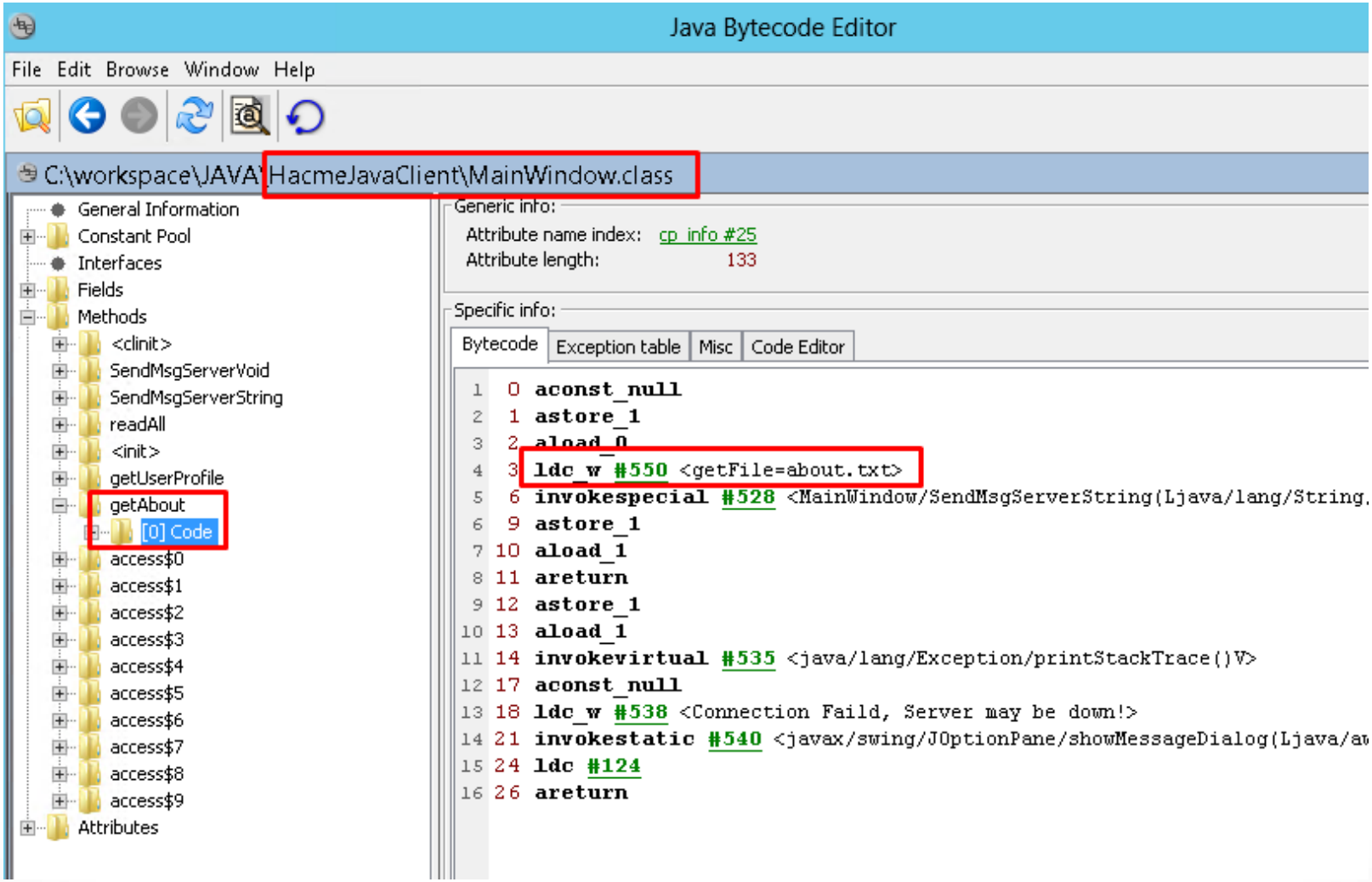




- Now, how do you modify class files??

Introducing - JBE

- Java Bytecode Editor - http://set.ee/jbe/



Java Bytecode

- https://en.wikipedia.org/wiki/Java_bytecode_instruction_listings

Java Bytecode	Human
ifeq / ifne	if *value* is (not) 0, branch to offset
if_icmpeq /if_icmpne	if ints are equal / not equal
iconst_0 / iconst_1	load int=0/ int=1
aload_0	load a reference into a local variable 0
astore_1	store a reference into local variable 1
dcmpg	compare two doubles
areturn	return a reference form a method
fneg	negate a float
ireturn	return an integer from a method
ldc	push a constant from a constant pool to the stack

Java Bytecode Editor

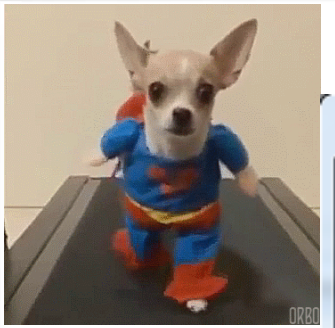
- Demo time…

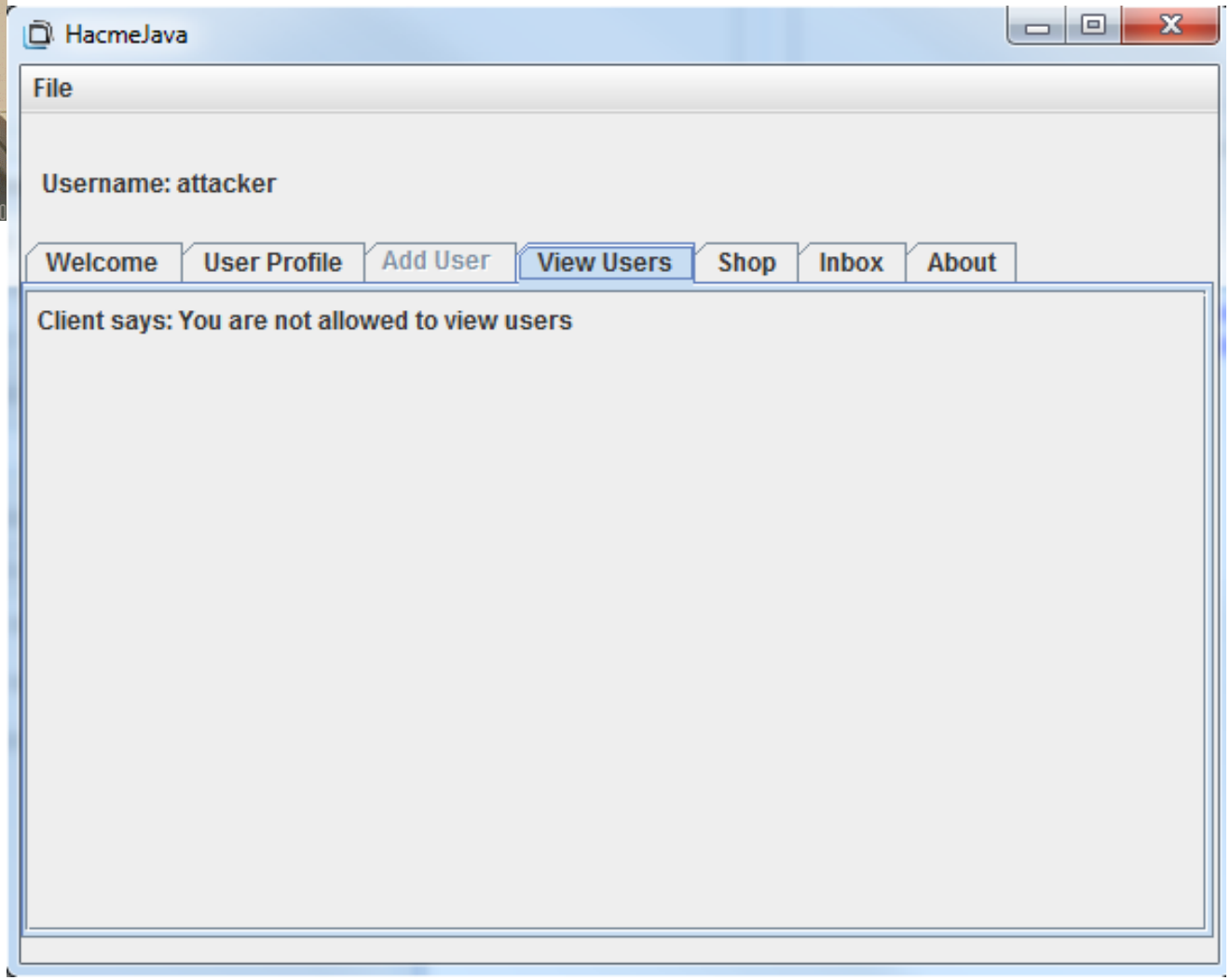
What REALLY Happened?

```
 0 aload_0
 1 ifnull 14 (+13)
 4 aload_0
 5 getstatic #3 <                    /user/management/          User/ADMIN L          /ir
 8 invokevirtual #4 <          /interfaces/util/          InsensitiveString/equals(Ljav
11 ifeq 18 (+7)
14 iconst_0
15 goto 19 (+4)
18 iconst_1
19 ireturn
```

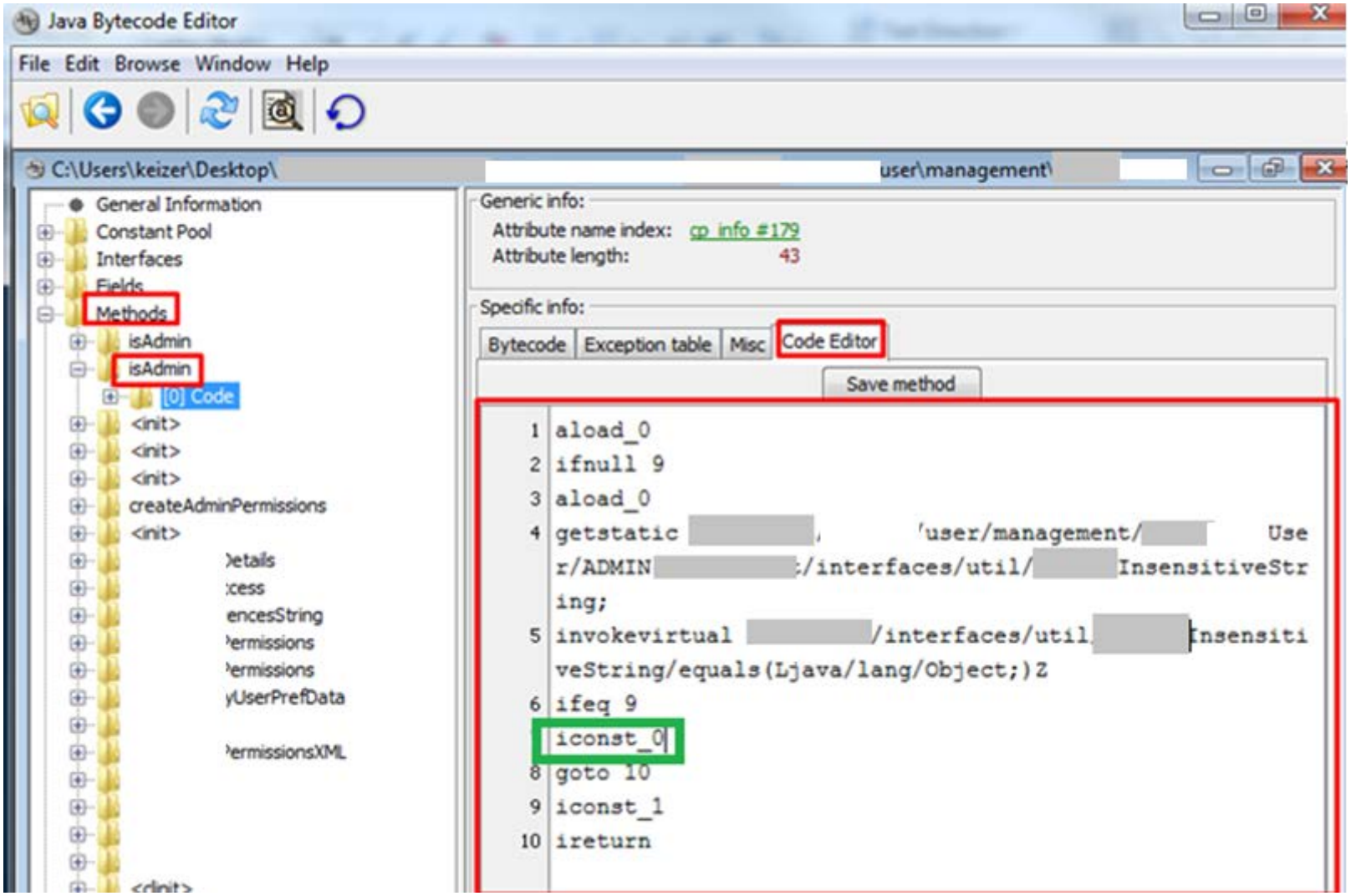
0. Load something…
1. If null → jump to 14 (const_0)
4. Load something…
5. Get static “ADMIN”
8. Invoke equals(x,y)
11. If equals → jump to 18 (const_1)
14. (no jump) const_0
15. Go to → 19 (return)
18. const_1
19. return

Before…





I'll Just....



Let Us Pray!

C:\Users\keizer\Desktop

- General Information
- Constant Pool
- Interfaces
- Fields
- Methods
  - isAdmin
  - isAdmin
    - [0] Code
  - <init>
  - <init>
  - <init>
  - inPermissions
  - Details
  - ccess
  - rencesString
  - Permissions
  - Permissions
  - tyUserPrefData
  - PermissionsXML

\user\managemen User.class

Generic info:

Attribute name index: cp_info #179

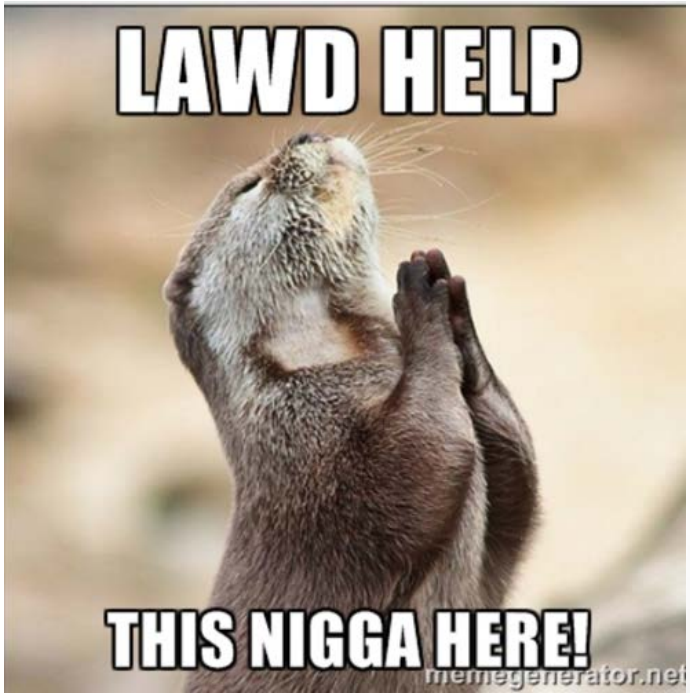
Attribute length: 43

Specific info:

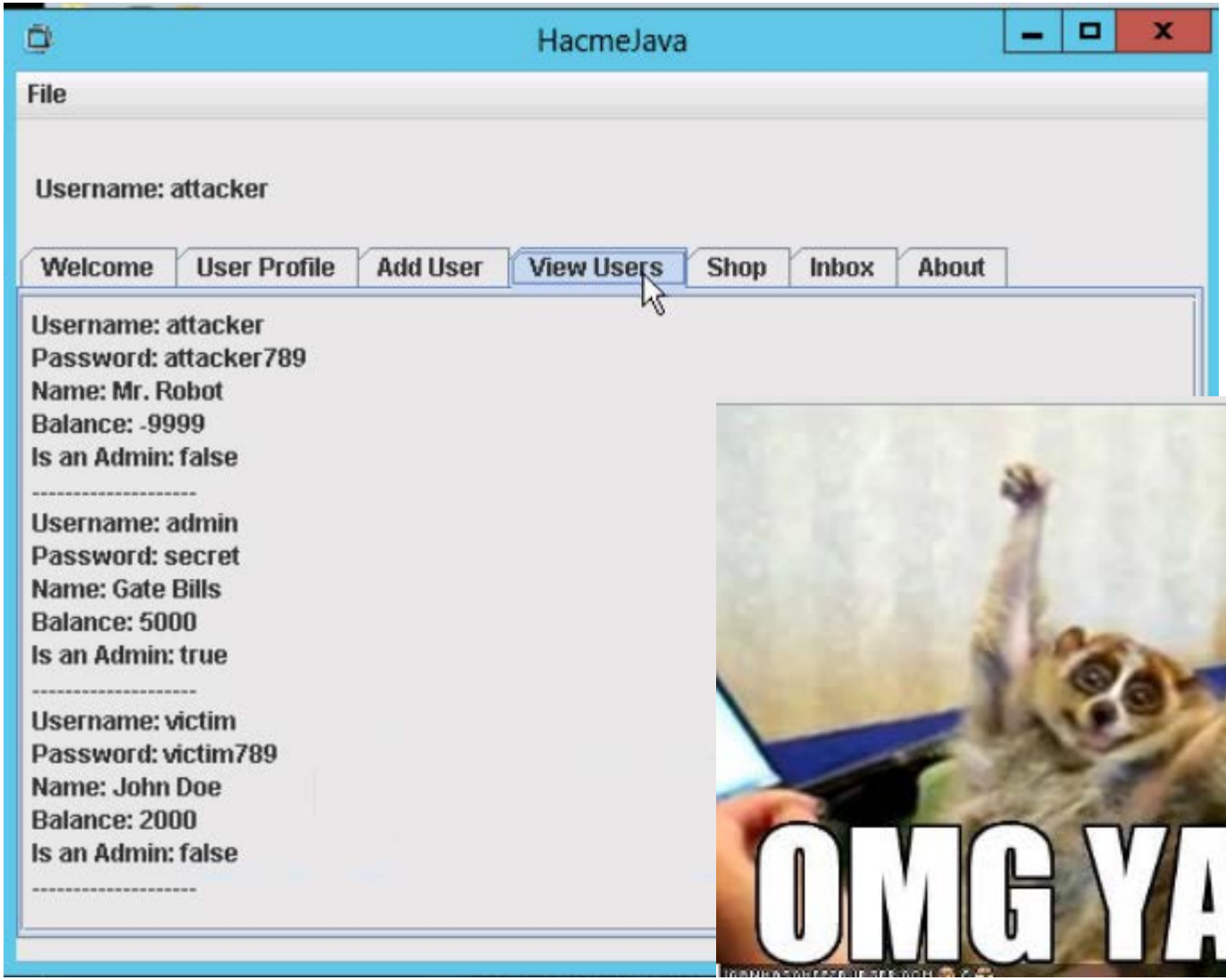
Bytecode | Exception table | Misc | Code Editor

Save method

```
1  aload_0
2  ifnull 9
3  aload_0
4  getstatic                user/management/      soleUser/ADMIN          t/interfaces/util/
5  invokevirtual          /interfaces/util/      InsensitiveString/equals(Ljava/lang/Object;)Z
6  ifeq 9
7  iconst_1
8  goto 10
9  iconst_1
10 ireturn
```

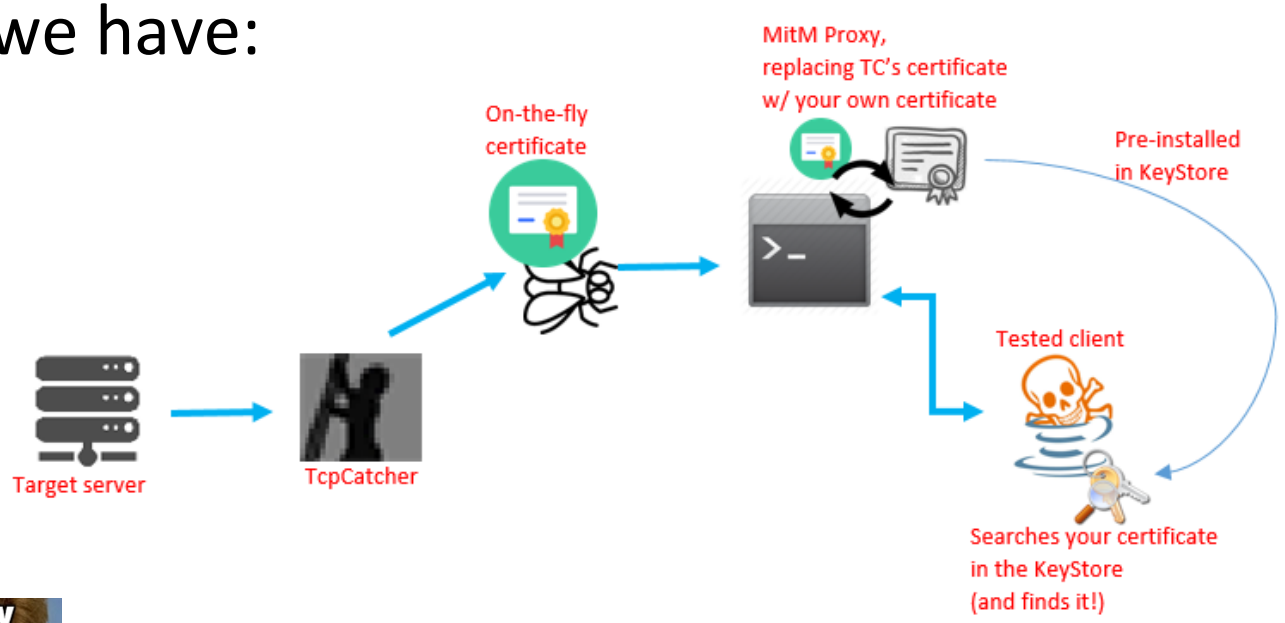


After 2 days and 6 hours



Imagine if…

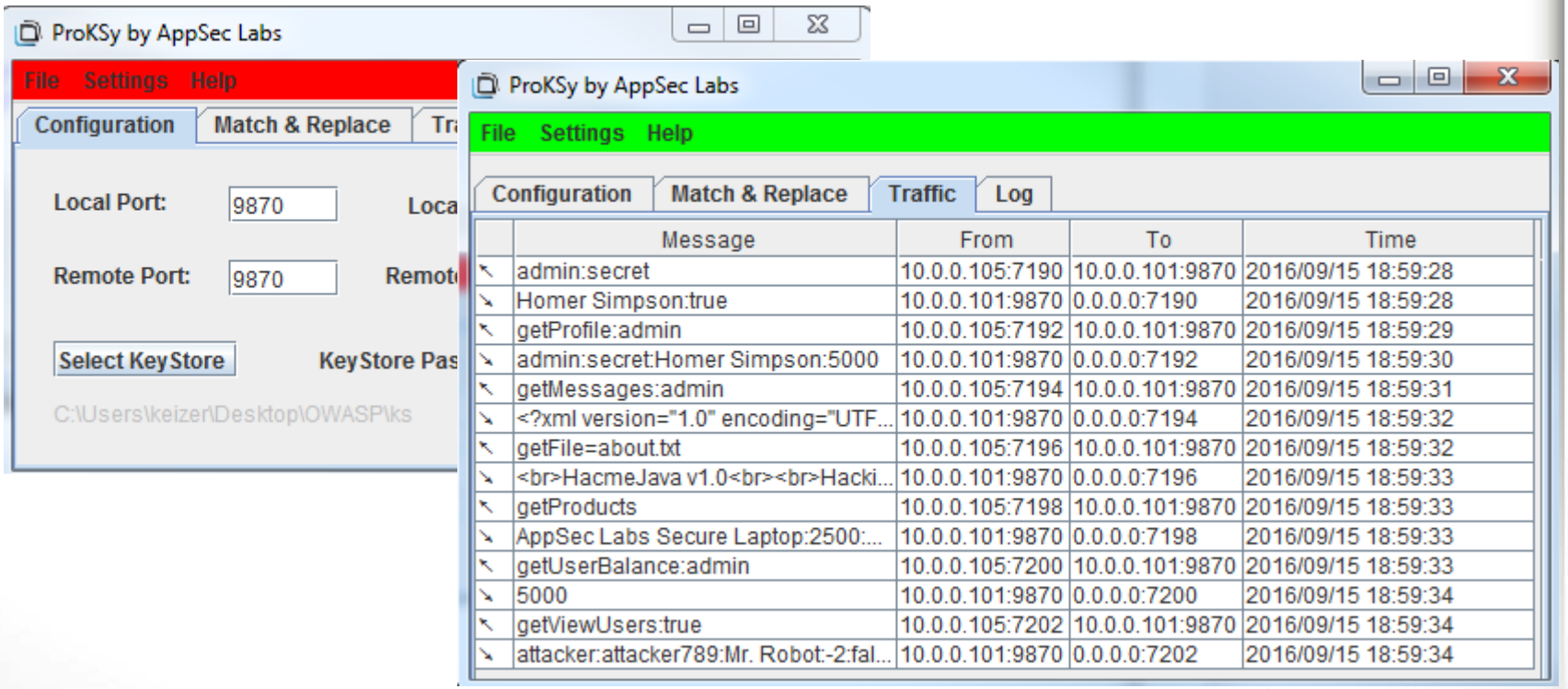
- We needed to create a MitM, to serve as a proxy between the original MitM and the client, replacing its on-the-fly certificate with our own certificate
- So, now we have:



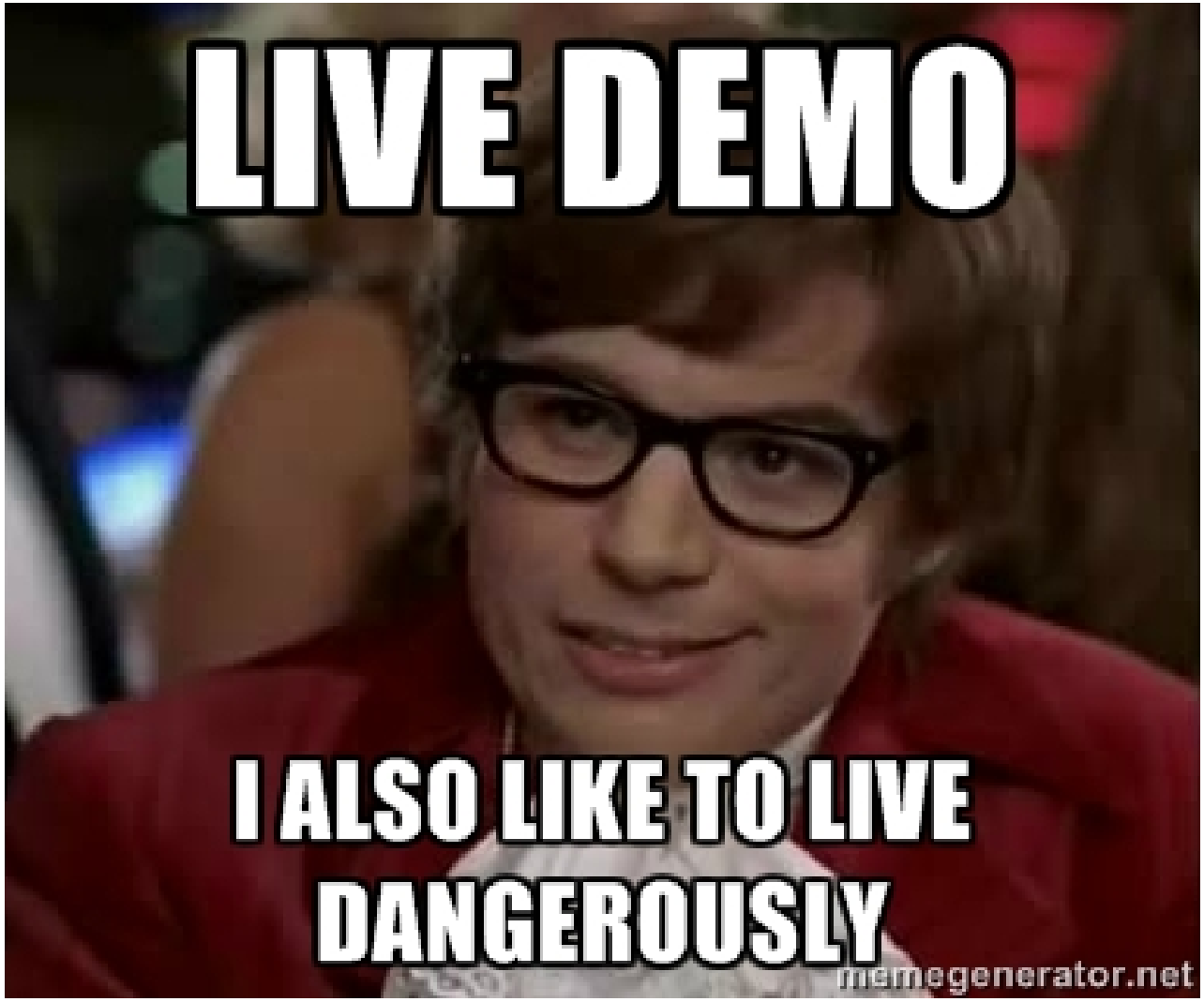
For the first time!

- Introducing…. ProKSy
  - -- What with the “KS”?
  - -- Stands for KeyStore :P

- https://github.com/nu11p0inter/ProKSy



Demo Time!



The Moral of the Story

- What did not work for me, might work for you
- Java – might not (fun) “writable”, but “readable”
- Never give up - there’s no such thing as “unbreakable”
- We love memes
- Download ProKSy!

One slide to d\l them all

- **APE -** TCP (.net) Proxy for Hooking
  https://appsec-labs.com/advanced-packet-editor/
- **ProKSy -** TCP/SSL Proxy for SSL Pinning
  https://github.com/nu11p0inter/ProKSy/
- **JavaSnoop** - Java Runtime Manipulation
  http://www.aspectsecurity.com/tools/javasnoop
- **JBE/reJ** - Java ByteCode Editing
  http://set.ee/jbe/
  https://sourceforge.net/projects/rejava

Thank you! see you @ OWASP IL 2017