Debugging the JVM

Fredrik Öhrström
Principal Member of Technical Staff
ORACLE JRockit+Hotspot

Debugging the JVM

Fredrik Öhrström
Principal Member of Technical Staff
ORACLE JRockit+Hotspot

Worked on JRockit for seven years, and OpenJDK for two years.

I started my JVM career debugging JVM crashes and other obscure JVM problems.

Now working in the Java language team. Though I am currently sidetracked to rewrite the build system for OpenJDK (including making javac multi-core).

The statistical law of large numbers

Because there are so many running JVMs out there...

The statistical law of large numbers

Because there are so many running JVMs out there...

We will get the core dump, even if the crash required the phase of the moon to correlate with the timezone data of Burkina Faso, whilst the OS was task switching between a Java thread and a Tetris game.

I have enough war stories for a week

- Customer app threw so many exceptions that...
- Customer xslt transform sorted the output in the wrong order...
- Customer got the wrong results when using floating point...
- Customer triggered a very slow memory leak in the JVM...
- and many more...
- However I will talk about a particular crash....

What do we get when the JVM crashes?

What do we get when the JVM crashes?

- A dump text (a few KiB of text)
- A core dump (several GiB)

```
[JRockit] ERROR: The JVM has crashed. Writing crash information to
/home/fredrik/perforce/main/jvm/jrockit.4626.dump.

===== BEGIN DUMP =============================================================
JRockit dump produced after 0 days, 00:00:04 on Mon May 21 09:18:46 2012

Error Message: Illegal memory access. [54]
Signal info  : si_signo=11, si_code=1 si_addr=(nil)
Version      : Oracle JRockit(R)
DEBUG-R28.2.0-fredrik_noview-0-1.6.0_29-20120521-0918-linux-ia32
CPU          : Intel  (HT) SSE SSE2 SSE3 SSSE3
Number CPUs  : 2
Tot Phys Mem : 1041997824 (993 MB)
OS version   : wheezy/sid
Linux version 3.0.0-15-generic (buildd@zirconium) (gcc version 4.6.1
(Ubuntu/Linaro 4.6.1-9ubuntu3) ) #26-Ubuntu SMP Fri Jan 20 15:59:53
UTC 2012 (i686)
Thread System: Linux NPTL
LibC release : 2.13-stable
Java locking : Lazy unlocking enabled (class banning) (transfer
banning)
State        : JVM is running
Command Line : .....
StackOverFlow: 0 StackOverFlowErrors have occured
OutOfMemory  : 0 OutOfMemoryErrors have occured
C Heap       : Good; no memory allocations have failed
```

```
GC Strategy  : Mode: throughput, with strategy: genparpar (basic strategy: genparpar)
GC Status    : OC is not running. Last finished OC was OC#0.
             : YC is currently running. This is YC#1.
YC Promotion : This YC has been able to promote all found objects so far
YC History   : Started 1 YCs since last OC.
Heap         : 0x882b6000 - 0x8c2b6000  (Size: 64 MB)
Compaction   : (no compaction area)
Allocation   : TLA-min: 2048, TLA-preferred: 65536 TLA-waste limit: 2048
NurseryList  : 0x882b6000 - 0x8a2b6000
KeepArea     : 0x89ab5fe8 - 0x8a2b6000
KA Markers   : [ 0x892b5ff0,  0x89ab5fe8 , 0x8a2b6000 ]
Forbidden A  : (none)
Previous KA  : (none)
Previous FA  : (none)
CompRefs     : References are 32-bit.
```

```
Registers (from ThreadContext: 0x39ae7c:
   eax = 00000000    ecx = 000020f8    edx = 00000002    ebx = 00127ff4
   esp = 0039b170    ebp = 0039b198    esi = 00000000    edi = 003d0f00
    es = 0000007b     cs = 00000073     ss = 0000007b     ds = 0000007b
    fs = 00000000     gs = 00000033    eip = 00848767 eflags = 00210202

Loaded modules:
(* denotes the module where the exception occured)
08048000-0804c11b /home/fredrik/perforce/main/jvm/build/linux_ia32/debug/work/ext/launcher/jrockit
00c6a000-00c6a416 /home/fredrik/perforce/main/jvm/build/linux_ia32/debug/work/ext/launcher/jrockit
00d69000-00d6b15b /lib/i386-linux-gnu/libdl.so.2
00110000-00126b87 /lib/i386-linux-gnu/libpthread.so.0
0012b000-002a0e8f /lib/i386-linux-gnu/libc.so.6
0050a000-00527ae7 /lib/ld-linux.so.2
00562000-008d7fd7 */home/fredrik/perforce/main/jvm/build/linux_ia32/debug/libjvm.so
00e57000-00e7a3bb /home/fredrik/perforce/main/jvm/build/linux_ia32/debug/libjrosal.so
00326000-003322b7 /home/fredrik/perforce/main/jvm/build/linux_ia32/debug/libjrutil.so
002a7000-002cef4f /lib/i386-linux-gnu/libm.so.6
00f84000-00f8acbb /lib/i386-linux-gnu/librt.so.1
00bf9000-00c00013 /lib/i386-linux-gnu/libnss_compat.so.2
00c3c000-00c50fcf /lib/i386-linux-gnu/libnsl.so.1
00f00000-00f0968f /lib/i386-linux-gnu/libnss_nis.so.2
002d1000-002dbe37 /lib/i386-linux-gnu/libnss_files.so.2
003b1000-003be82b /home/fredrik/perforce/main/jvm/build/linux_ia32/debug/libjfr.so
002de000-002e89bb /localhome/buildtools/jdk-6u29-fcs-bin-b11-linux-i586-03_oct_2011/jre/lib/i386/libverify
00d07000-00d29f07 /localhome/buildtools/jdk-6u29-fcs-bin-b11-linux-i586-03_oct_2011/jre/lib/i386/libjava.s
002ea000-002efe50 /localhome/buildtools/jdk-6u29-fcs-bin-b11-linux-i586-03_oct_2011/jre/lib/i386/native_th
00a73000-00a816e4 /home/localhome/buildtools/jdk-6u29-fcs-bin-b11-linux-i586-03_oct_2011/jre/lib/i386/libz
```

```
Stack:
(* marks the word pointed to by the stack pointer)
0039b170: 093991a8* 0039b1c4  0039b198  008459b7  0039b1c4  0178ce80
0039b188: 0039b198  00847a7d  00000000  00000000  0039b298  00848945
0039b1a0: 09541cc0  0039b1c4  00000000  00e6fce5  093b6ea8  093b6ea8
0039b1b8: 0039b1c8  093991a8  00000002  007e2fcd  007e2b0b  007e2a1f

Code:
(* marks the word pointed to by the instruction pointer)
00848734: a1e82404  c7fff9f8  00042444  8b000000  0489e445  f8b5e824
0084874c: c481fff9  00000124  55c35d5b  ec83e589  fc45c728  00000000
00848764: c7fc458b* 00002a00  08458b00  8d0c508b  4489ec45  14890424
0084877c: f841e824  0eebfff9  8d104d8b  458bec55  fc33e808  458dffff


NOTE: Dump Helper crashed and was aborted

Scan Dump Helper:
Processing roots from a workchunk at 0x39b1c4.
This is a Thread Roots workchunk.
"Main Thread" id=1 idx=0x4 tid=4641The current state is: Initialized

No objRef registered in the workchunk.

Last optimized methods:
No methods optimized.
```

```
Thread:
"(GC Worker Thread 2)" id=? idx=0x14 tid=4645 lastJavaFrame=0xfffffffc
Stack 0: start=0x378000, end=0x39c000, guards=0x37d000 (ok),
forbidden=0x37b000

Thread Stack Trace:
    at ycProcessWorkChunk+16(ycgc.c:218)@0x848767
    at ycWorkerProcessRoots+162(ycgc.c:371)@0x848945
    at mmGCWorkerThread+223(gcthreads.c:828)@0x697428
    at thread_stub+353(lifecycle.c:808)@0x72b370
    at start_thread+208()@0x116d31
    at __clone+93()@0x1fd0ce
    -- Java stack --
```

Start debugging the core dump.
Eventually, you can read hex as if it was english.

Start debugging the core dump.
Eventually, you can read hex as if it was english.

Some time passes....

Start debugging the core dump.
Eventually, you can read hex as if it was english.

Some time passes....

Some more time passes....

Start debugging the core dump.
Eventually, you can read hex as if it was english.

Some time passes....

Some more time passes....

Oookay, it seems like the object that we tried to examine during the gc, points to a clazz that no longer exists!

Start debugging the core dump.
Eventually, you can read hex as if it was english.

Some time passes....

Some more time passes....

Oookay, it seems like the object that we tried to examine during the gc, points to a clazz that no longer exists!

I.e. we have an instance of a class, but not the class meta data! It cannot be found anywhere in the JVM!

```
Object header:     Vtable&co:     Clazz:
ClassBlock ptr --> Clazz ptr -->  All the meta
Flags
```

```
Object header:     Vtable&co:     Not a Clazz at all:
ClassBlock ptr --> Clazz ptr -->  Was one here?
Flags
```

```
       Young space                 Old space
------------------------------------------------------------
|                     |                                    |
------------------------------------------------------------
```

```
       Young space                        Old space
-----------------------------------------------------------
|obj             clazz|                                    |
-----------------------------------------------------------
```

```
       Young space                 Old space
-----------------------------------------------------------
|obj             xxxxx|                                   |
-----------------------------------------------------------
```

I.e. There have been a young gc between the allocation of the clazz and the allocation of its object instance.

I.e. There have been a young gc between the allocation of the clazz and the allocation of its object instance.

For some reason the clazz was not kept alive. Immediate suspect: code generation and livemaps!

What is a livemap?

What is a livemap?

On safepoint, where the gc can force your program to stop executing. The meta-data for your code, tells the gc which registers (esi,eax, etc) contains pointers to objects.

```
Registers (from ThreadContext: 0x39ae7c:
eax = 00000000  ecx = 000020f8  edx = 00000002  ebx = 00127ff4
esp = 0039b170  ebp = 0039b198  esi = af853040  edi = 003d0f00
 es = 0000007b   cs = 00000073   ss = 0000007b   ds = 0000007b
 fs = 00000000   gs = 00000033  eip = 00848767 eflags = 00210202
```

Lets have a look at the allocation code for this test program:

```
public class Test4
{
    public static class Bar {
        public Bar(int k) { x = k; }
        int x;
    }
    public static void main(String... args) {
        for (;;) test(42);
    }
    public static Bar test(int k) {
        return new Bar(k);
    }
}
```

Slow case, out of tla.

```
public Object allocObject() {
  pd_addr classID = IClass.getID(this);


  Object o = allocObject(classID);

  if (jvmtiVMObjectAllocs) {
    jvmtiVMObjectAlloc(o);
  }
  if (IClass.hasFinalizer(classID)) {
    registerFinalizer(o);
  }
  return o;
}
```

Problematic safe point is here.

```
public Object allocObject() {
  pd_addr classID = IClass.getID(this);
  // Problematic safepoint the register esi (this)
  // that points to this clazz is not live.
  Object o = allocObject(classID);

  if (jvmtiVMObjectAllocs) {
    jvmtiVMObjectAlloc(o);
  }
  if (IClass.hasFinalizer(classID)) {
    registerFinalizer(o);
  }
  return o;
}
```

Start debugging the livemaps and code generation to find out why this is not live.

Start debugging the livemaps and code generation to find out why this is not live.

Some time passes....

Start debugging the livemaps and code generation to find out why this is not live.

Some time passes....

Some more time passes....

Start debugging the livemaps and code generation to find out why this is not live.

Some time passes....

Some more time passes....

More than a week later, customer is quite annoyed....

Start debugging the livemaps and code generation to find out why this is not live.

Some time passes....

Some more time passes....

More than a week later, customer is quite annoyed....

Ouch, it is supposed to do that!

Woot? Can the “this” pointer be garbage collected before the instance method has ended?

Woot? Can the “this” pointer be garbage collected before the instance method has ended?

Yes, it can, because the method is no longer using it.

Woot? Can the “this” pointer be garbage collected before the instance method has ended?

Yes, it can, because the method is no longer using it.

Normally, this is not a problem, nor is it detectable. Except that finalizers can be run before the method has finished. (Surprise!)

Woot? Can the “this” pointer be garbage collected before the instance method has ended?

Yes, it can, because the method is no longer using it.

Normally, this is not a problem, nor is it detectable. Except that finalizers can be run before the method has finished. (Surprise!)

But in this case we are implementing the JVM using Java and there is nothing to tell the JVM that this particular pointer does escape, as a side effect of creating the object instance! (Through the vtable.)

```
public Object allocObject() {
  pd_addr classID = IClass.getID(this);
  Object o = allocObject(classID);

  // dummy usages to rescue that the code
  // generator doesn't keep clazz alive.
  // dummy objects are statics!
  if (this == dummyObject1) {
      dummyObject2 = this;
  }

  if (jvmtiVMObjectAllocs) {
    jvmtiVMObjectAlloc(o);
  }
  if (IClass.hasFinalizer(classID)) {
    registerFinalizer(o);
  }
  return o;
}
```

Summary

If an object is garbage collected in the forest?
Will it make a sound?

Summary

If an object is garbage collected in the forest?
Will it make a sound?

Only if anyone is listening.

Thank you!

fredrik.ohrstrom@oracle.com

copenhagen goto; conference

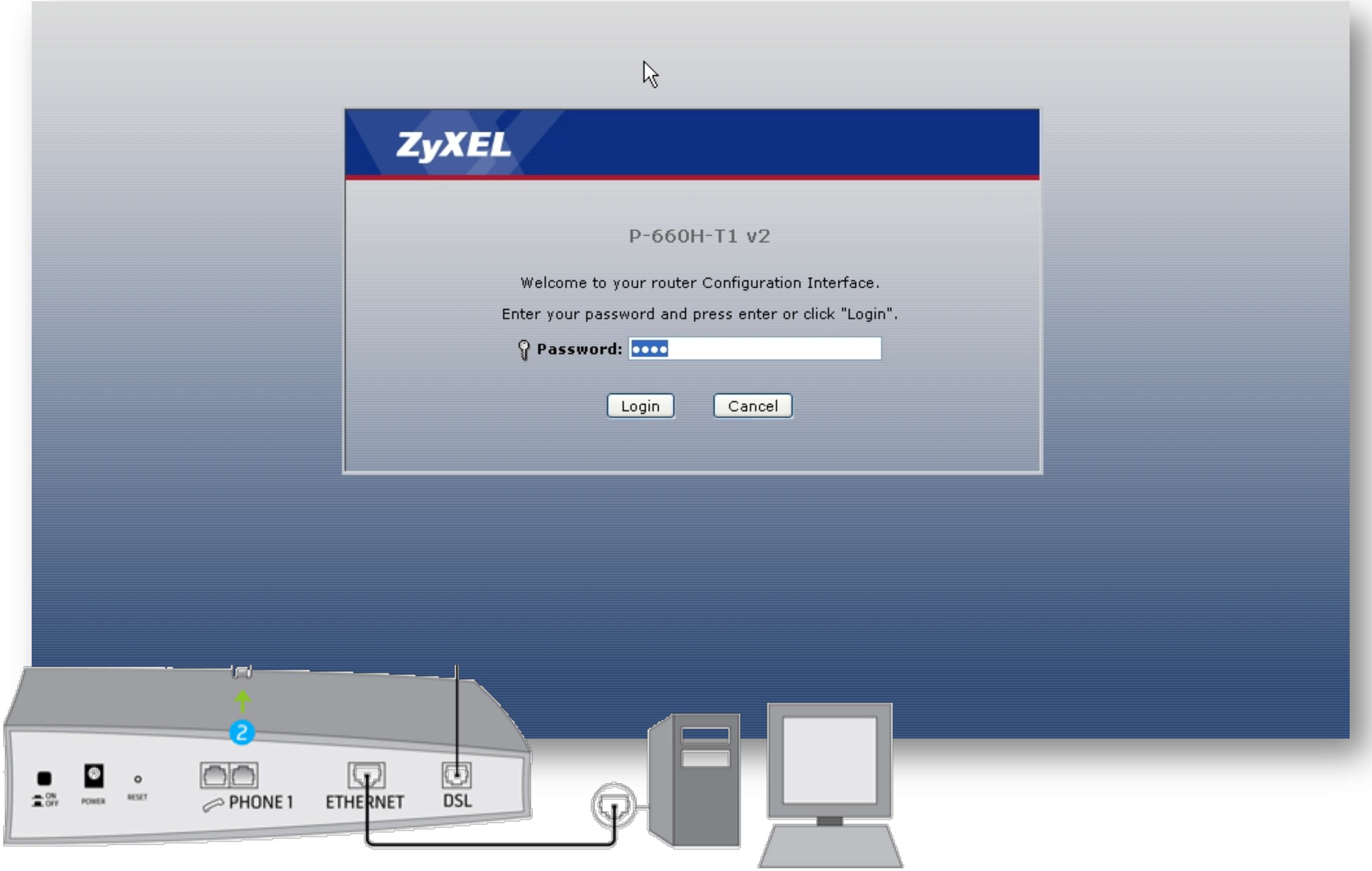
HACKING MY ROUTER

Anders Skovsgaard
Hackavoid

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

gotocon.com

The Router



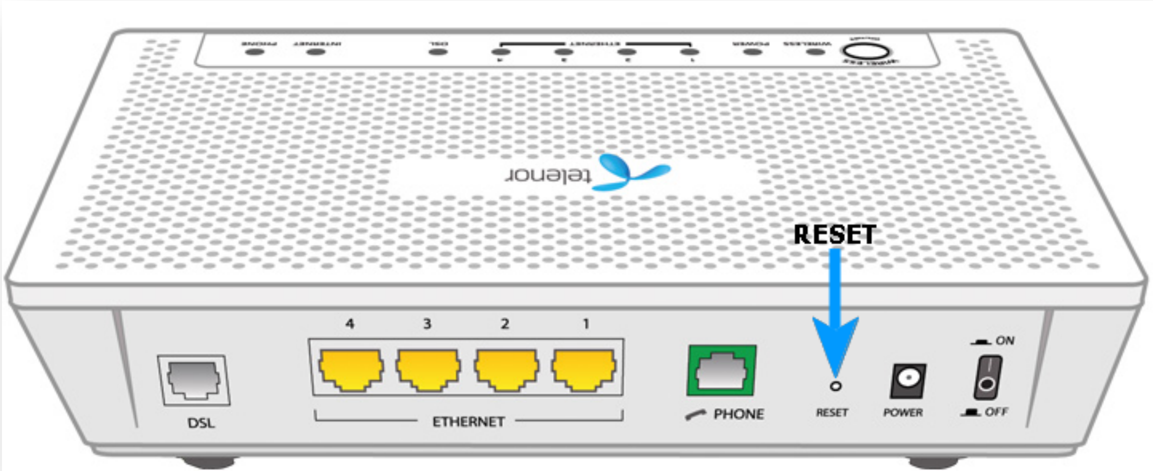
P-660H-T1 v2

Welcome to your router Configuration Interface.

Enter your password and press enter or click "Login".

Password: ••••

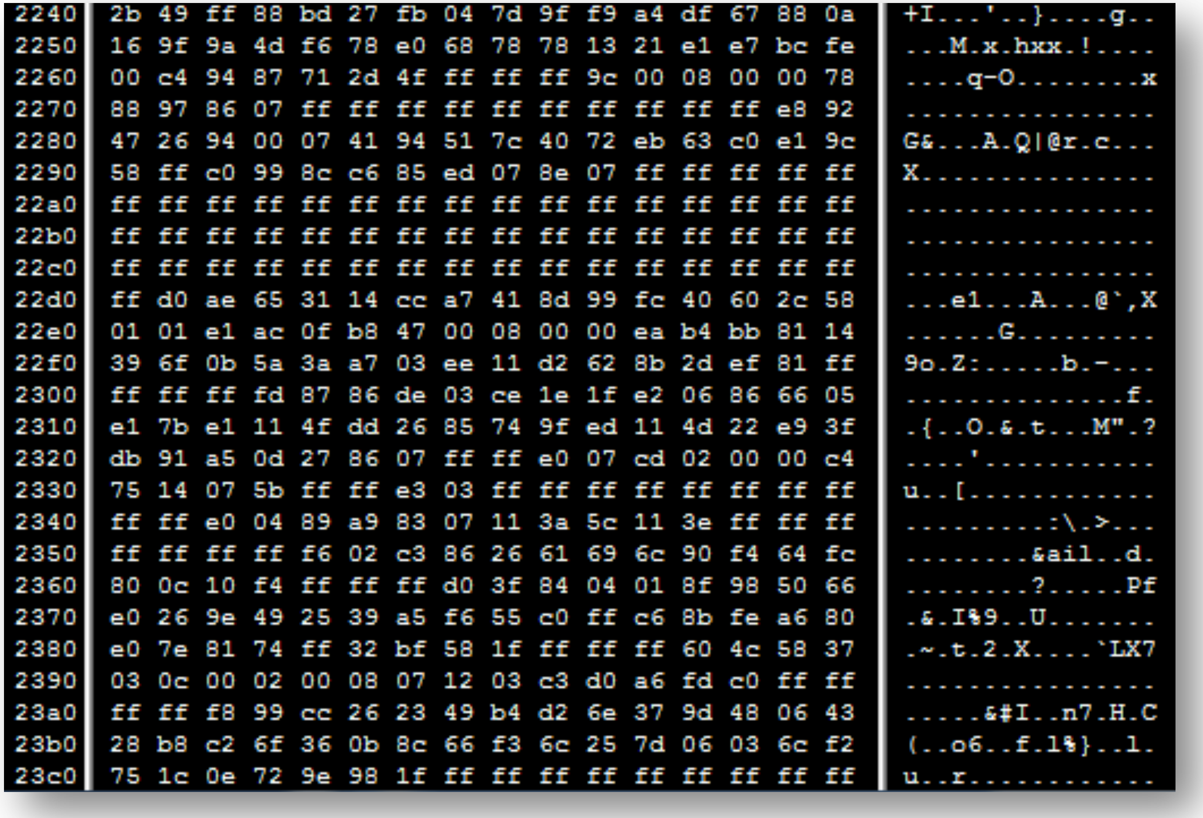
The Router



The Config File

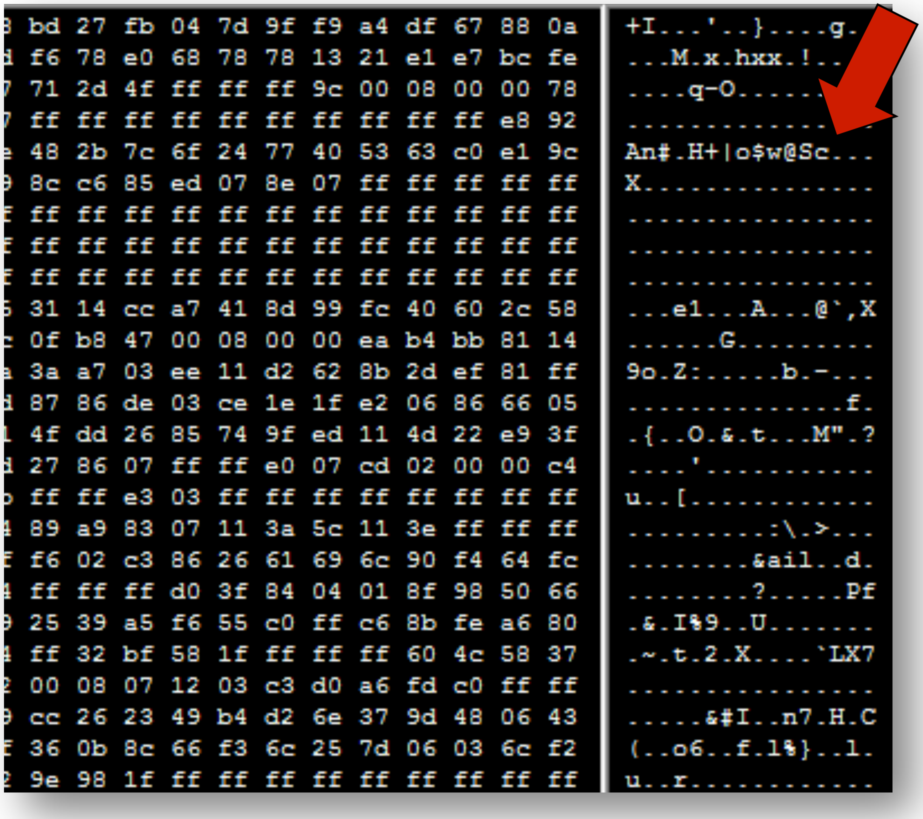
`http://10.0.0.1:2033/rom-0`

and public (WAN) `http://212.242.220.16/rom-0`



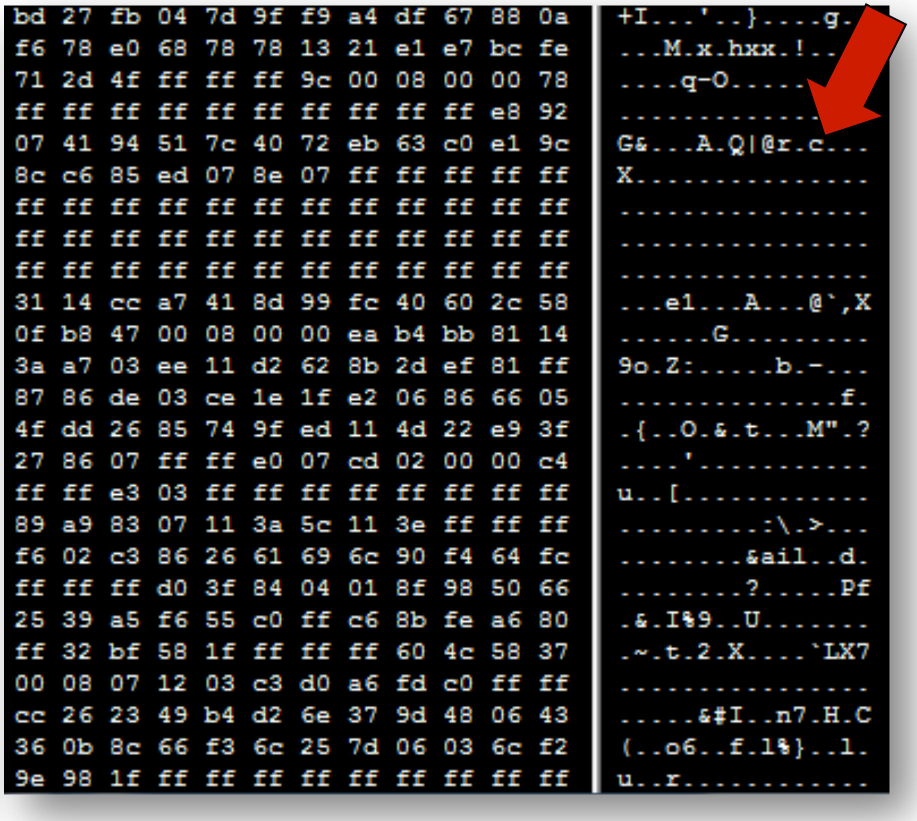
```
2240  2b 49 ff 88 bd 27 fb 04 7d 9f f9 a4 df 67 88 0a  +I...'..}....g..
2250  16 9f 9a 4d f6 78 e0 68 78 78 13 21 e1 e7 bc fe  ...M.x.hxx.!....
2260  00 c4 94 87 71 2d 4f ff ff ff 9c 00 08 00 00 78  ....q-O........x
2270  88 97 86 07 ff ff ff ff ff ff ff ff ff ff e8 92  ................
2280  47 26 94 00 07 41 94 51 7c 40 72 eb 63 c0 e1 9c  G&...A.Q|@r.c...
2290  58 ff c0 99 8c c6 85 ed 07 8e 07 ff ff ff ff ff  X...............
22a0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ................
22b0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ................
22c0  ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  ................
22d0  ff d0 ae 65 31 14 cc a7 41 8d 99 fc 40 60 2c 58  ...e1...A...@`,X
22e0  01 01 e1 ac 0f b8 47 00 08 00 00 ea b4 bb 81 14  ......G.........
22f0  39 6f 0b 5a 3a a7 03 ee 11 d2 62 8b 2d ef 81 ff  9o.Z:.....b.-...
2300  ff ff ff fd 87 86 de 03 ce 1e 1f e2 06 86 66 05  ..............f.
2310  e1 7b e1 11 4f dd 26 85 74 9f ed 11 4d 22 e9 3f  .{..O.&.t...M".?
2320  db 91 a5 0d 27 86 07 ff ff e0 07 cd 02 00 00 c4  ....'...........
2330  75 14 07 5b ff ff e3 03 ff ff ff ff ff ff ff ff  u..[............
2340  ff ff e0 04 89 a9 83 07 11 3a 5c 11 3e ff ff ff  .........:\.>...
2350  ff ff ff ff f6 02 c3 86 26 61 69 6c 90 f4 64 fc  ........&ail..d.
2360  80 0c 10 f4 ff ff ff d0 3f 84 04 01 8f 98 50 66  ........?.....Pf
2370  e0 26 9e 49 25 39 a5 f6 55 c0 ff c6 8b fe a6 80  .&.I%9..U.......
2380  e0 7e 81 74 ff 32 bf 58 1f ff ff ff 60 4c 58 37  .~.t.2.X....`LX7
2390  03 0c 00 02 00 08 07 12 03 c3 d0 a6 fd c0 ff ff  ................
23a0  ff ff f8 99 cc 26 23 49 b4 d2 6e 37 9d 48 06 43  .....&#I..n7.H.C
23b0  28 b8 c2 6f 36 0b 8c 66 f3 6c 25 7d 06 03 6c f2  (..o6..f.l%}..l.
23c0  75 1c 0e 72 9e 98 1f ff ff ff ff ff ff ff ff ff  u..r............
```

The Diff



```
3 bd 27 fb 04 7d 9f f9 a4 df 67 88 0a   +I...'..}....g.
d f6 78 e0 68 78 78 13 21 e1 e7 bc fe   ...M.x.hxx.!..
7 71 2d 4f ff ff ff 9c 00 08 00 00 78   ....q-O.......
7 ff ff ff ff ff ff ff ff ff ff e8 92   ...............
e 48 2b 7c 6f 24 77 40 53 63 c0 e1 9c   An#.H+|o$w@Sc...
9 8c c6 85 ed 07 8e 07 ff ff ff ff ff   X...............
f ff ff ff ff ff ff ff ff ff ff ff ff   ................
f ff ff ff ff ff ff ff ff ff ff ff ff   ................
f ff ff ff ff ff ff ff ff ff ff ff ff   ................
5 31 14 cc a7 41 8d 99 fc 40 60 2c 58   ...e1...A...@`,X
c 0f b8 47 00 08 00 00 ea b4 bb 81 14   ......G.........
a 3a a7 03 ee 11 d2 62 8b 2d ef 81 ff   9o.Z:.....b.-...
d 87 86 de 03 ce 1e 1f e2 06 86 66 05   ...............f.
1 4f dd 26 85 74 9f ed 11 4d 22 e9 3f   .{..O.&.t...M".?
d 27 86 07 ff ff e0 07 cd 02 00 00 c4   ....'...........
b ff ff e3 03 ff ff ff ff ff ff ff ff   u..[............
4 89 a9 83 07 11 3a 5c 11 3e ff ff ff   ..........:\.>...
f f6 02 c3 86 26 61 69 6c 90 f4 64 fc   .........&ail..d.
4 ff ff ff d0 3f 84 04 01 8f 98 50 66   .........?.....Pf
9 25 39 a5 f6 55 c0 ff c6 8b fe a6 80   .&.I%9..U.......
4 ff 32 bf 58 1f ff ff ff 60 4c 58 37   .~.t.2.X....`LX7
2 00 08 07 12 03 c3 d0 a6 fd c0 ff ff   ................
9 cc 26 23 49 b4 d2 6e 37 9d 48 06 43   .....&#I..n7.H.C
f 36 0b 8c 66 f3 6c 25 7d 06 03 6c f2   (..o6..f.1%}..l.
2 9e 98 1f ff ff ff ff ff ff ff ff ff   u..r............
```

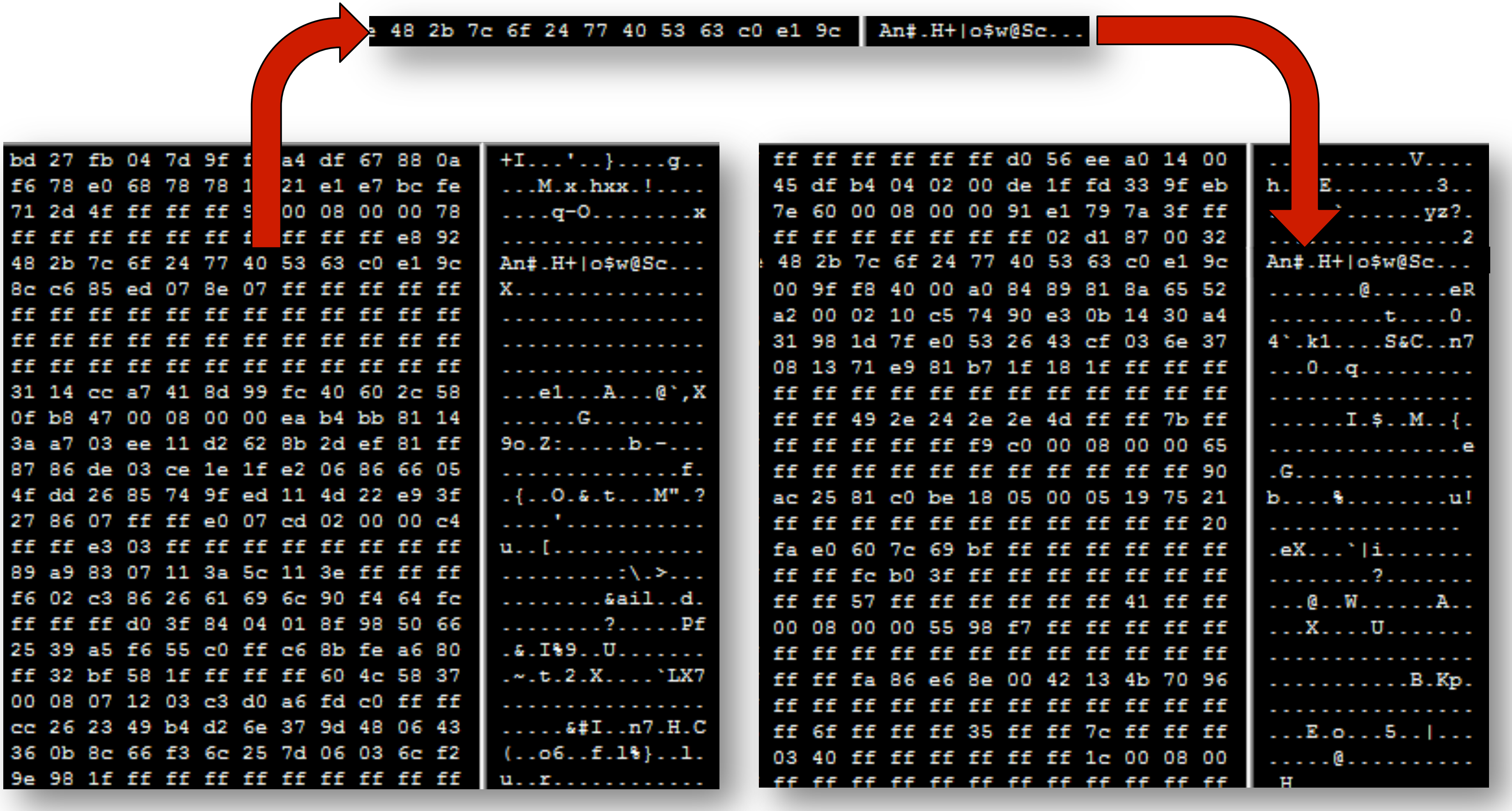
Fabricated Config File #1
Password: 1234



```
bd 27 fb 04 7d 9f f9 a4 df 67 88 0a   +I...'..}....g.
f6 78 e0 68 78 78 13 21 e1 e7 bc fe   ...M.x.hxx.!..
71 2d 4f ff ff ff 9c 00 08 00 00 78   ....q-O.......
ff ff ff ff ff ff ff ff ff ff e8 92   ...............
07 41 94 51 7c 40 72 eb 63 c0 e1 9c   G&...A.Q|@r.c...
8c c6 85 ed 07 8e 07 ff ff ff ff ff   X...............
ff ff ff ff ff ff ff ff ff ff ff ff   ................
ff ff ff ff ff ff ff ff ff ff ff ff   ................
ff ff ff ff ff ff ff ff ff ff ff ff   ................
31 14 cc a7 41 8d 99 fc 40 60 2c 58   ...e1...A...@`,X
0f b8 47 00 08 00 00 ea b4 bb 81 14   ......G.........
3a a7 03 ee 11 d2 62 8b 2d ef 81 ff   9o.Z:.....b.-...
87 86 de 03 ce 1e 1f e2 06 86 66 05   ...............f.
4f dd 26 85 74 9f ed 11 4d 22 e9 3f   .{..O.&.t...M".?
27 86 07 ff ff e0 07 cd 02 00 00 c4   ....'...........
ff ff e3 03 ff ff ff ff ff ff ff ff   u..[............
89 a9 83 07 11 3a 5c 11 3e ff ff ff   ..........:\.>...
f6 02 c3 86 26 61 69 6c 90 f4 64 fc   .........&ail..d.
ff ff ff d0 3f 84 04 01 8f 98 50 66   .........?.....Pf
25 39 a5 f6 55 c0 ff c6 8b fe a6 80   .&.I%9..U.......
ff 32 bf 58 1f ff ff ff 60 4c 58 37   .~.t.2.X....`LX7
00 08 07 12 03 c3 d0 a6 fd c0 ff ff   ................
cc 26 23 49 b4 d2 6e 37 9d 48 06 43   .....&#I..n7.H.C
36 0b 8c 66 f3 6c 25 7d 06 03 6c f2   (..o6..f.1%}..l.
9e 98 1f ff ff ff ff ff ff ff ff ff   u..r............
```

Fabricated Config File #2
Password: 4321

The Replace



```
48 2b 7c 6f 24 77 40 53 63 c0 e1 9c   An#.H+|o$w@Sc...
```

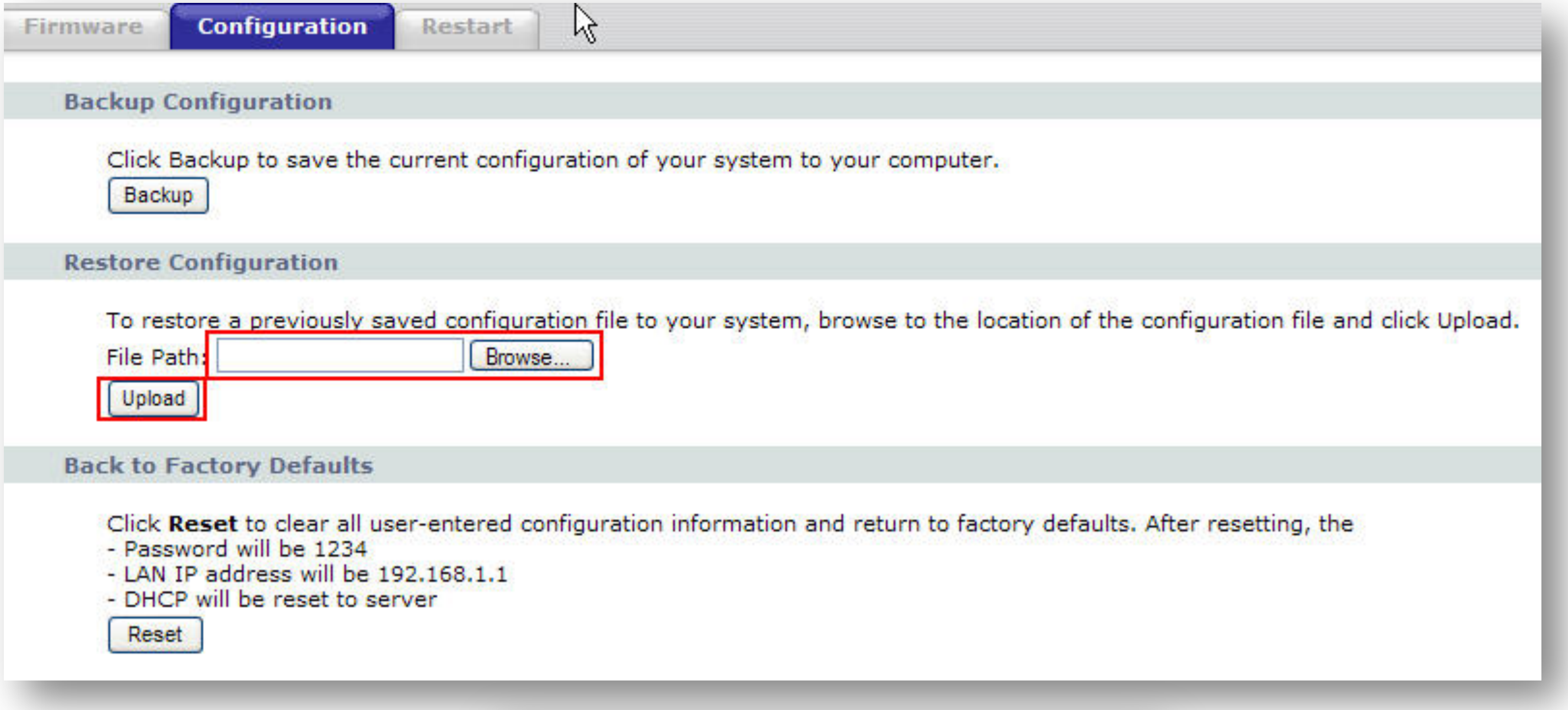
```
bd 27 fb 04 7d 9f f  a4 df 67 88 0a   +I...'..}....g..
f6 78 e0 68 78 78 1  21 e1 e7 bc fe   ...M.x.hxx.!....
71 2d 4f ff ff ff 9  00 08 00 00 78   ....q-O........x
ff ff ff ff ff ff f  ff ff ff e8 92   ................
48 2b 7c 6f 24 77 40 53 63 c0 e1 9c   An#.H+|o$w@Sc...
8c c6 85 ed 07 8e 07 ff ff ff ff ff   X...............
ff ff ff ff ff ff ff ff ff ff ff ff   ................
ff ff ff ff ff ff ff ff ff ff ff ff   ................
ff ff ff ff ff ff ff ff ff ff ff ff   ................
31 14 cc a7 41 8d 99 fc 40 60 2c 58   ...e1...A...@`,X
0f b8 47 00 08 00 00 ea b4 bb 81 14   ......G.........
3a a7 03 ee 11 d2 62 8b 2d ef 81 ff   9o.Z:.....b.-...
87 86 de 03 ce 1e 1f e2 06 86 66 05   ..............f.
4f dd 26 85 74 9f ed 11 4d 22 e9 3f   .{..O.&.t...M".?
27 86 07 ff ff e0 07 cd 02 00 00 c4   ....'...........
ff ff e3 03 ff ff ff ff ff ff ff ff   u..[............
89 a9 83 07 11 3a 5c 11 3e ff ff ff   ..........:\.>...
f6 02 c3 86 26 61 69 6c 90 f4 64 fc   .........&ail..d.
ff ff ff d0 3f 84 04 01 8f 98 50 66   .........?.....Pf
25 39 a5 f6 55 c0 ff c6 8b fe a6 80   .&.I%9..U.......
ff 32 bf 58 1f ff ff ff 60 4c 58 37   .~.t.2.X....`LX7
00 08 07 12 03 c3 d0 a6 fd c0 ff ff   ................
cc 26 23 49 b4 d2 6e 37 9d 48 06 43   .....&#I..n7.H.C
36 0b 8c 66 f3 6c 25 7d 06 03 6c f2   (..o6..f.l%}..l.
9e 98 1f ff ff ff ff ff ff ff ff ff   u..r............
```

```
ff ff ff ff ff ff d0 56 ee a0 14 00   ..........V....
45 df b4 04 02 00 de 1f fd 33 9f eb   h. E.........3..
7e 60 00 08 00 00 91 e1 79 7a 3f ff   . `......yz?.
ff ff ff ff ff ff ff 02 d1 87 00 32   ...............2
48 2b 7c 6f 24 77 40 53 63 c0 e1 9c   An#.H+|o$w@Sc...
00 9f f8 40 00 a0 84 89 81 8a 65 52   ........@.......eR
a2 00 02 10 c5 74 90 e3 0b 14 30 a4   ..........t....0.
31 98 1d 7f e0 53 26 43 cf 03 6e 37   4`.k1....S&C..n7
08 13 71 e9 81 b7 1f 18 1f ff ff ff   ...0..q.........
ff ff ff ff ff ff ff ff ff ff ff ff   ................
ff ff 49 2e 24 2e 2e 4d ff ff 7b ff   ......I.$..M..{.
ff ff ff ff ff f9 c0 00 08 00 00 65   ...............e
ff ff ff ff ff ff ff ff ff ff ff 90   .G..............
ac 25 81 c0 be 18 05 00 05 19 75 21   b....%.........u!
ff ff ff ff ff ff ff ff ff ff ff 20   ................
fa e0 60 7c 69 bf ff ff ff ff ff ff   .eX...`|i.......
ff ff fc b0 3f ff ff ff ff ff ff ff   .........?.......
ff ff 57 ff ff ff ff ff ff 41 ff ff   ...@..W.......A..
00 08 00 00 55 98 f7 ff ff ff ff ff   ...X....U.......
ff ff ff ff ff ff ff ff ff ff ff ff   ................
ff ff fa 86 e6 8e 00 42 13 4b 70 96   .............B.Kp.
ff ff ff ff ff ff ff ff ff ff ff ff   ................
ff 6f ff ff ff 35 ff ff 7c ff ff ff   ...E.o...5..|...
03 40 ff ff ff ff ff ff 1c 00 08 00   .....@..........
ff ff ff ff ff ff ff ff ff ff ff ff    H
```

Fabricated Config File
Password: 1234

Real Config File
Password: ?

The New Config File



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

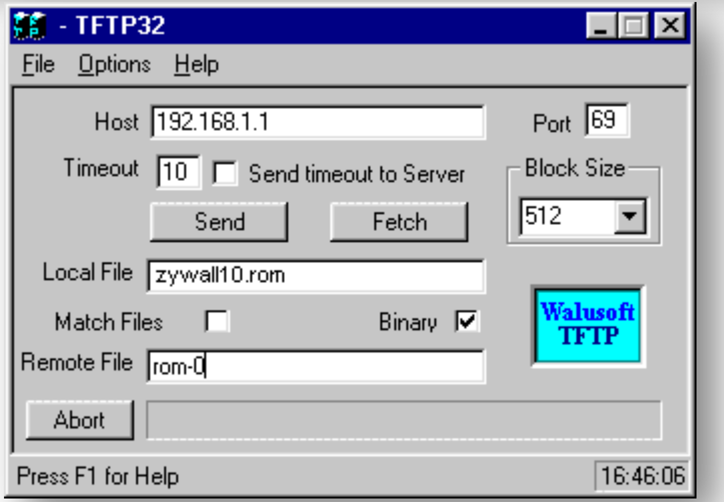
Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:

Back to Factory Defaults

Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server



Host 192.168.1.1

Port 69

Timeout 10 □ Send timeout to Server

Block Size 512

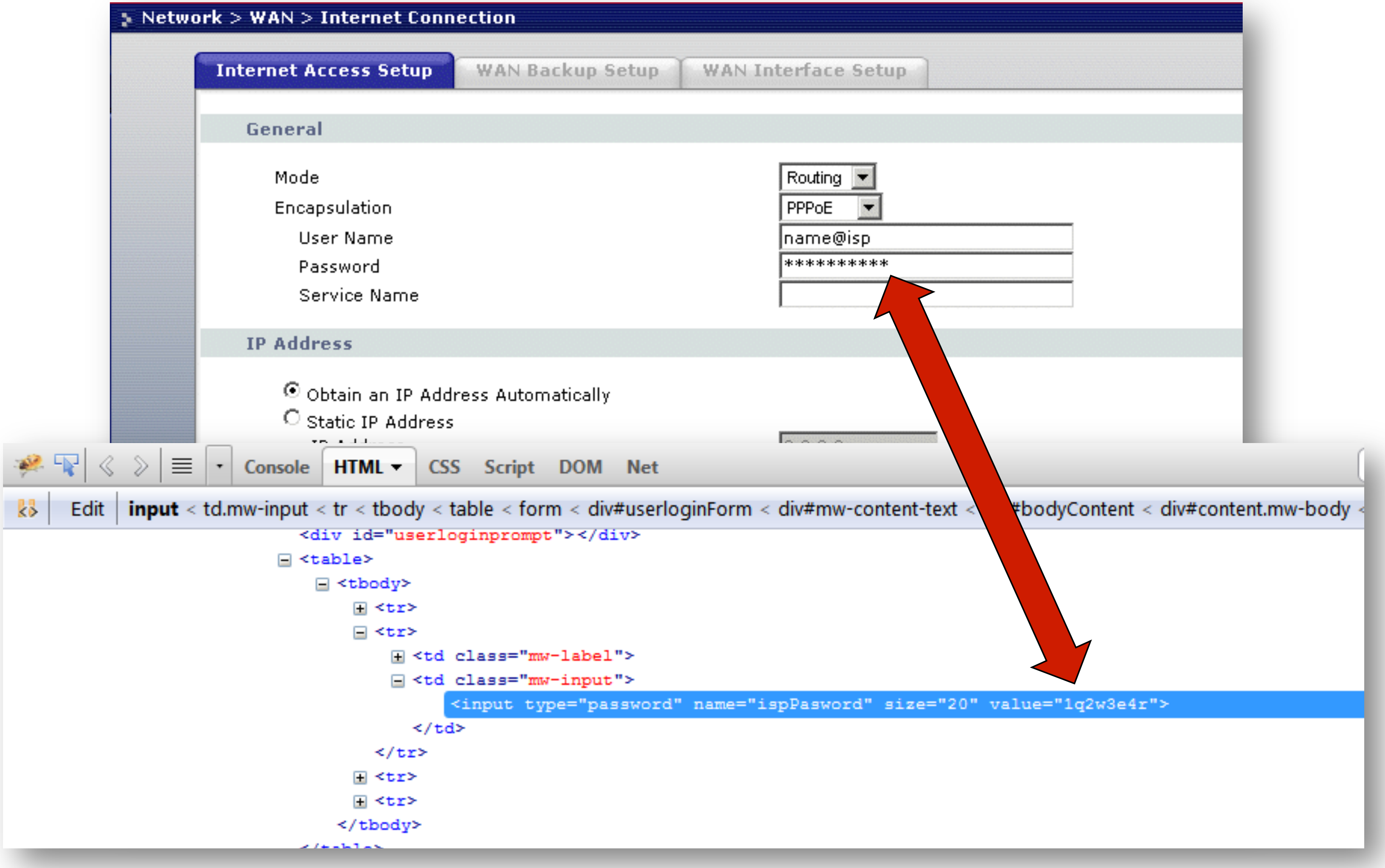
Local File zywall10.rom

Match Files □ Binary ☑

Remote File rom-0

Press F1 for Help 16:46:06

Router and Connection Password



General

Mode: Routing

Encapsulation: PPPoE

User Name: name@isp

Password: **********

Service Name:

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

input < td.mw-input < tr < tbody < table < form < div#userloginForm < div#mw-content-text < #bodyContent < div#content.mw-body

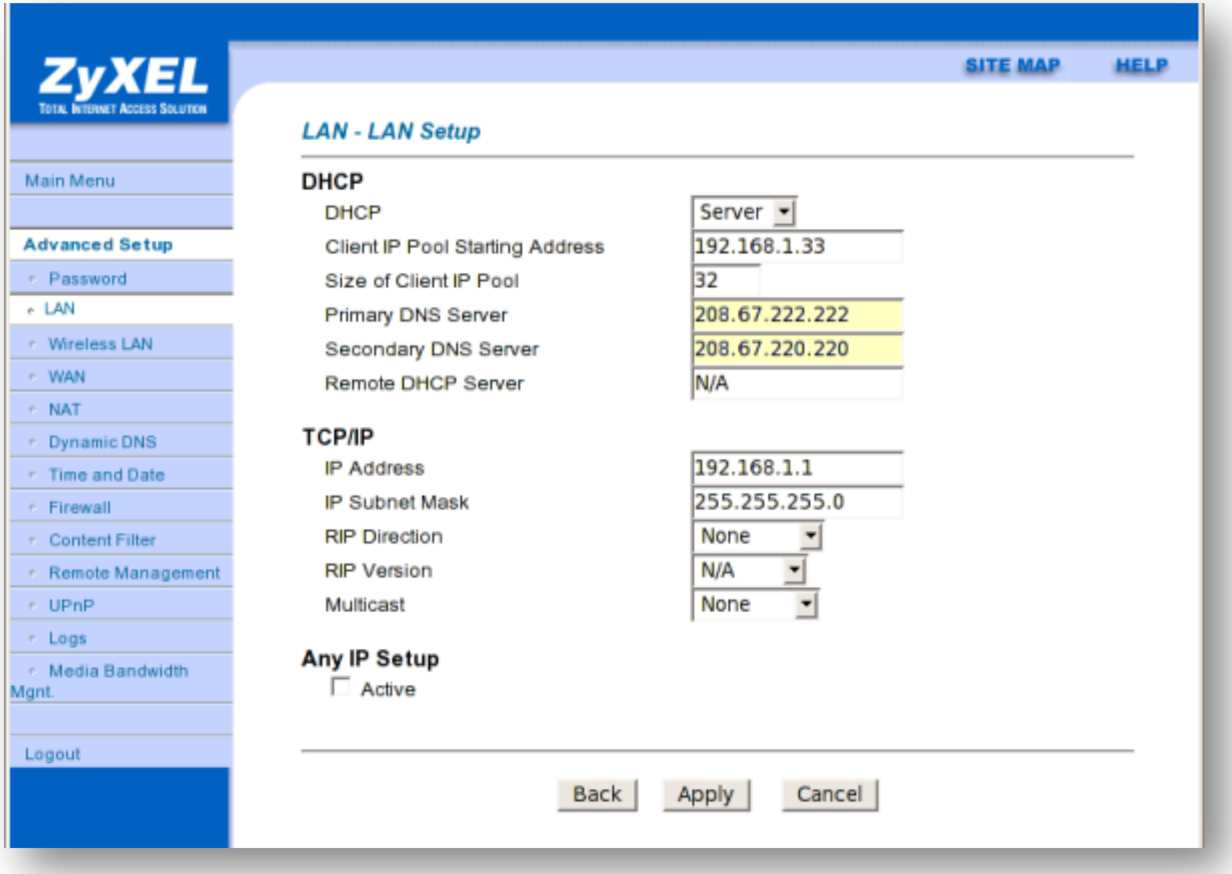
```
<div id="userloginprompt"></div>
⊟ <table>
  ⊟ <tbody>
    ⊞ <tr>
    ⊟ <tr>
      ⊞ <td class="mw-label">
      ⊟ <td class="mw-input">
          <input type="password" name="ispPasword" size="20" value="1q2w3e4r">
        </td>
      </tr>
    ⊞ <tr>
    ⊞ <tr>
    </tbody>
```

Attacks

- Make fun
  - Reset the router.
  - Change passwords.
  - Change NAT settings.

- More severe
  - Upload buggy firmware.
  - Upgrade his connection.
  - Change DNS settings.

DNS Attack



LAN - LAN Setup

DHCP

DHCP	Server
Client IP Pool Starting Address	192.168.1.33
Size of Client IP Pool	32
Primary DNS Server	208.67.222.222
Secondary DNS Server	208.67.220.220
Remote DHCP Server	N/A

TCP/IP

IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
RIP Direction	None
RIP Version	N/A
Multicast	None

Any IP Setup

□ Active

DNS Attack

- ISP Name Server returns:

```
www.google.com. CNAME www.l.google.com.
www.l.google.com. A 173.194.69.99
www.l.google.com. A 173.194.69.104
www.l.google.com. A 173.194.69.106
www.l.google.com. A 173.194.69.147
www.l.google.com. A 173.194.69.105
www.l.google.com. A 173.194.69.103
www.l.google.com. A 173.194.69.99
www.l.google.com. A 173.194.69.104
```

DNS Attack

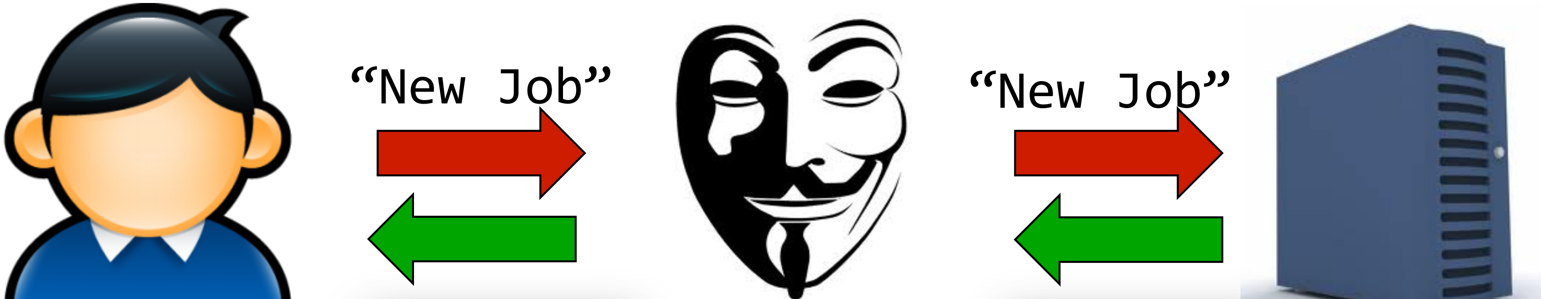
- New DNS settings:

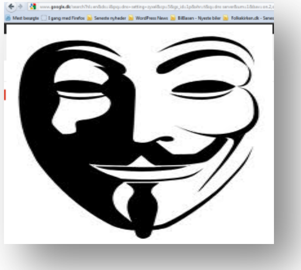
  Primary DNS Server: `212.242.220.16` (attacker IP)

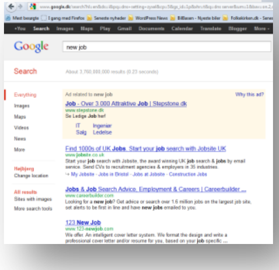
- Returns:

```
www.google.com. A 212.242.220.16
```

DNS Attack







new job

About 3,760,000,000 results (0.23 seconds)

Ad related to new job Why this ad?

Job - Over 3.000 Attraktive **Job** | Stepstone.dk
www.stepstone.dk
Se Ledige **Job** her!
IT Ingeniør
Salg Ledelse

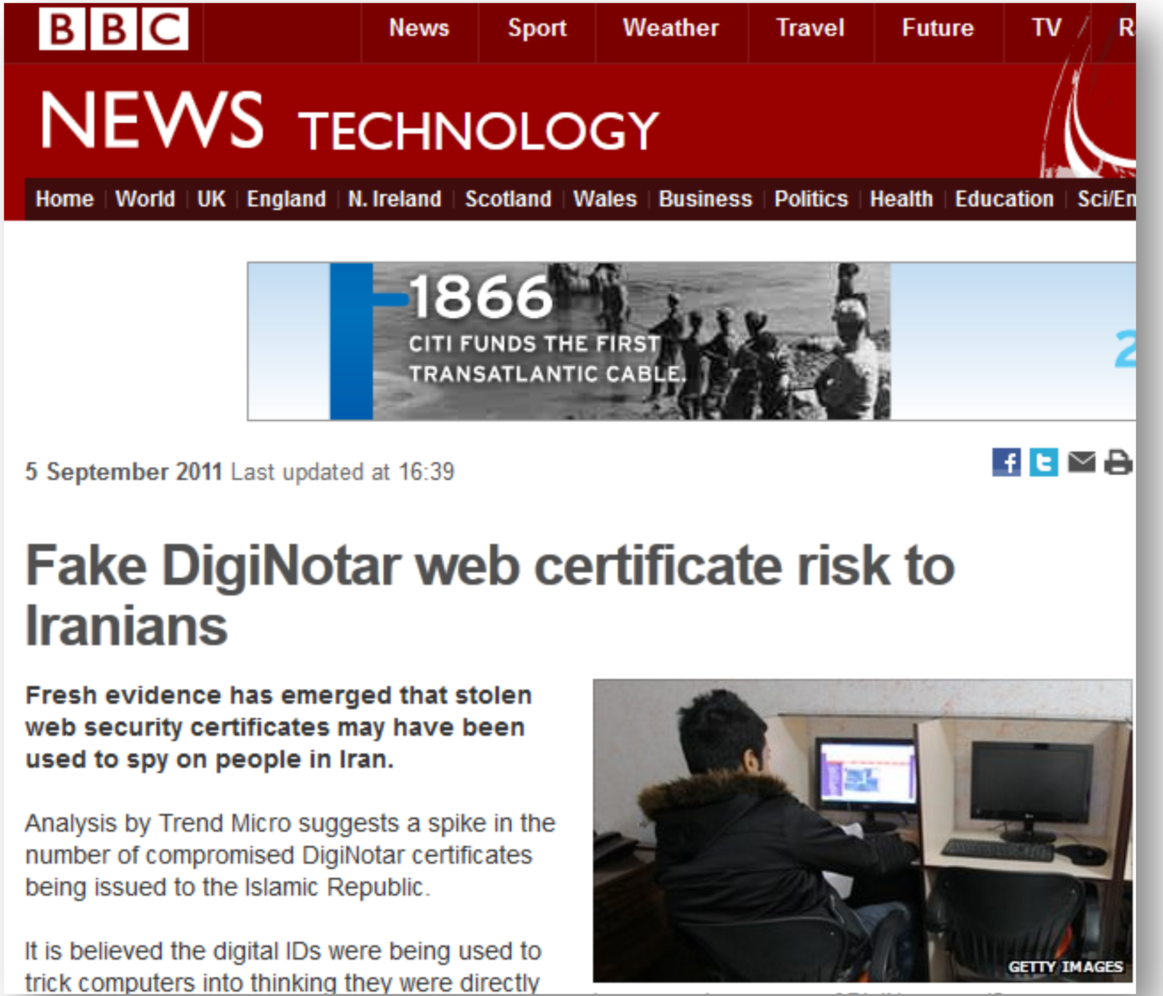
Find 1000s of UK **Jobs**. Start your **job** search with Jobsite UK
www.jobsite.co.uk
Start your **job** search with Jobsite, the award winning UK **job** search & **jobs** by email service. Send CVs to recruitment agencies & employers in 35 industries.
My Jobsite - Jobs in Bristol - Jobs at Jobsite - Construction Jobs

Jobs & **Job** Search Advice, Employment & Careers | Careerbuilder ...
www.careerbuilder.com
Looking for a **new job**? Get advice or search over 1.6 million jobs on the largest job site, set alerts to be first in line and have **new jobs** emailed to you.

123 **New Job**
www.123-newjob.com
We offer. An intelligent cover letter system. We format the design and write a professional cover letter and/or resume for you, based on your **job** specific ...

DNS Attack

- Attacks on `https://` not possible.
- Unless:



5 September 2011 Last updated at 16:39

Fake DigiNotar web certificate risk to Iranians

Fresh evidence has emerged that stolen web security certificates may have been used to spy on people in Iran.

Analysis by Trend Micro suggests a spike in the number of compromised DigiNotar certificates being issued to the Islamic Republic.

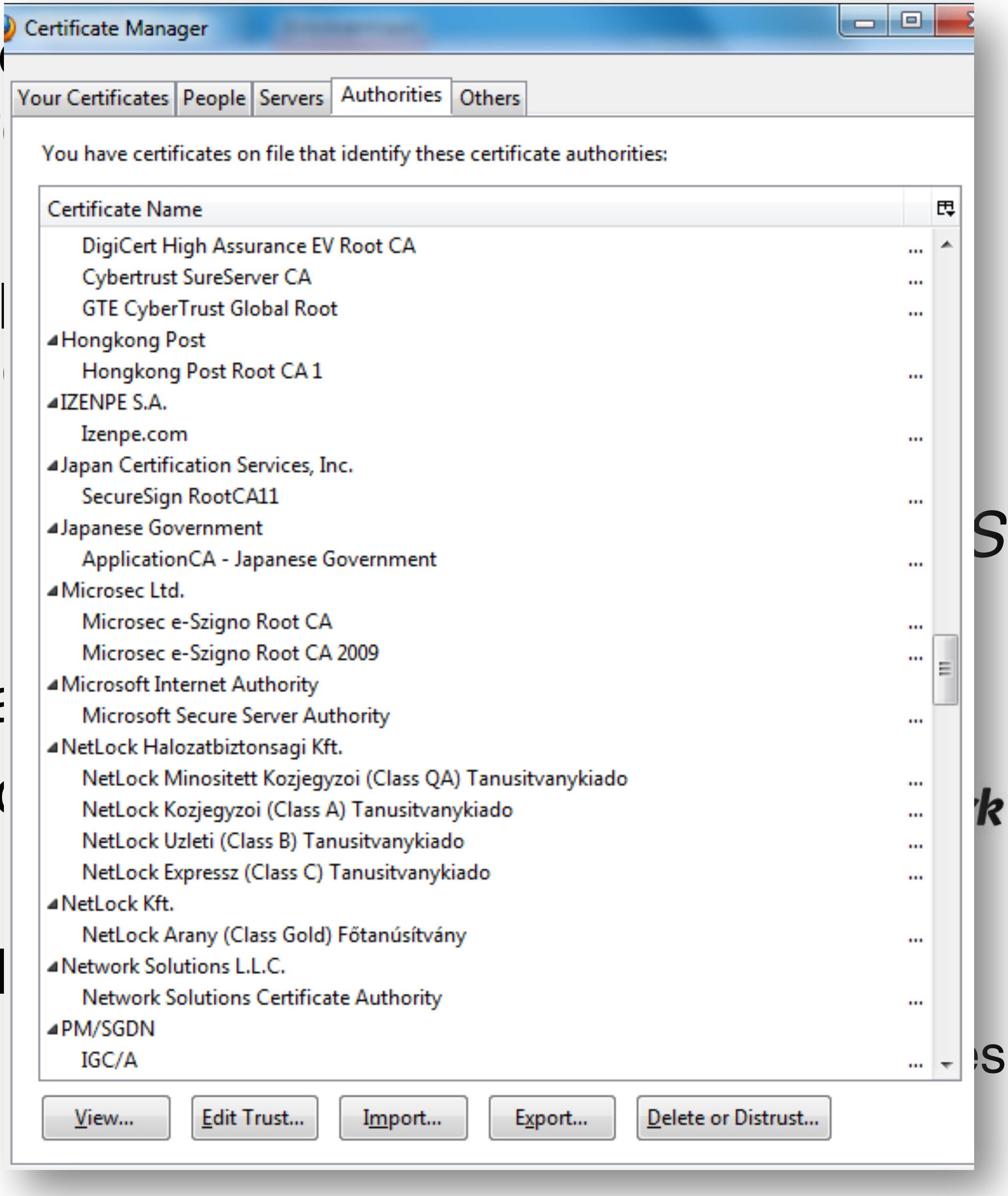
It is believed the digital IDs were being used to trick computers into thinking they were directly

DNS Risks

- G
  7
- O
  3
- M *ScrubIT*.

+ Fa
+ N ***k***

- D
  s (CA).



You have certificates on file that identify these certificate authorities:

Certificate Name

DigiCert High Assurance EV Root CA ...
Cybertrust SureServer CA ...
GTE CyberTrust Global Root ...
◢Hongkong Post
Hongkong Post Root CA 1 ...
◢IZENPE S.A.
Izenpe.com ...
◢Japan Certification Services, Inc.
SecureSign RootCA11 ...
◢Japanese Government
ApplicationCA - Japanese Government ...
◢Microsec Ltd.
Microsec e-Szigno Root CA ...
Microsec e-Szigno Root CA 2009 ...
◢Microsoft Internet Authority
Microsoft Secure Server Authority ...
◢NetLock Halozatbiztonsagi Kft.
NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado ...
NetLock Kozjegyzoi (Class A) Tanusitvanykiado ...
NetLock Uzleti (Class B) Tanusitvanykiado ...
NetLock Expressz (Class C) Tanusitvanykiado ...
◢NetLock Kft.
NetLock Arany (Class Gold) Főtanúsítvány ...
◢Network Solutions L.L.C.
Network Solutions Certificate Authority ...
◢PM/SGDN
IGC/A ...

The Router Fix

- ZyXEL fixed the problem in 2008.

- The solution:

  Default setting: Public (WAN) access is disabled.

- What could be done?

  - Secure the Config File – require login.

  - Encrypt the complete Config File – not only the password.

Questions?

Anders Skovsgaard

anders@hackavoid.dk

www.hackavoid.dk

War Stories

Tracking down an IE7 performance problem

The Problem

- Application load time in Internet Explorer 7 suddenly and dramatically increased

My job?

- To track down the revision that caused it

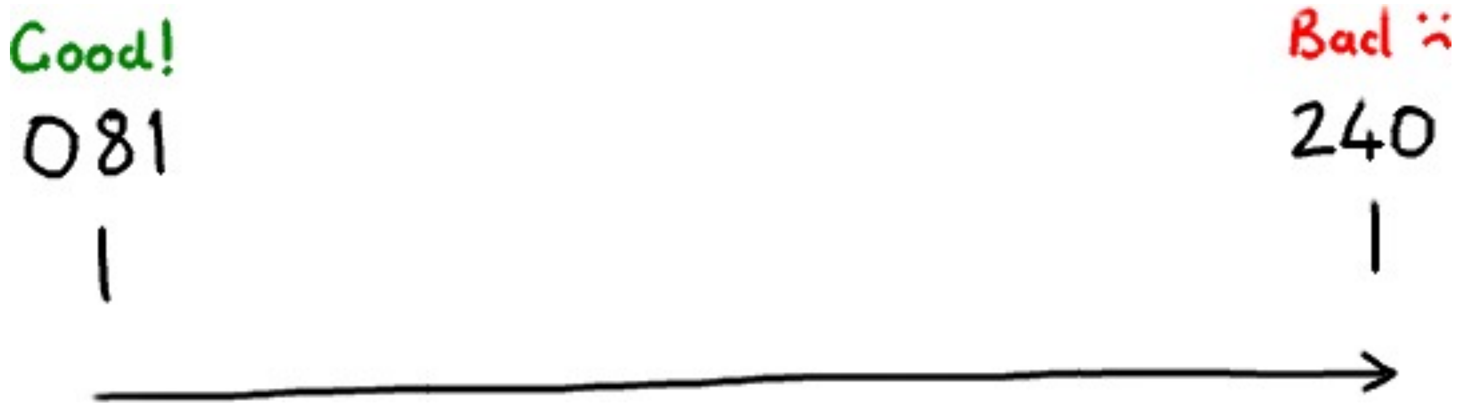
Simple?

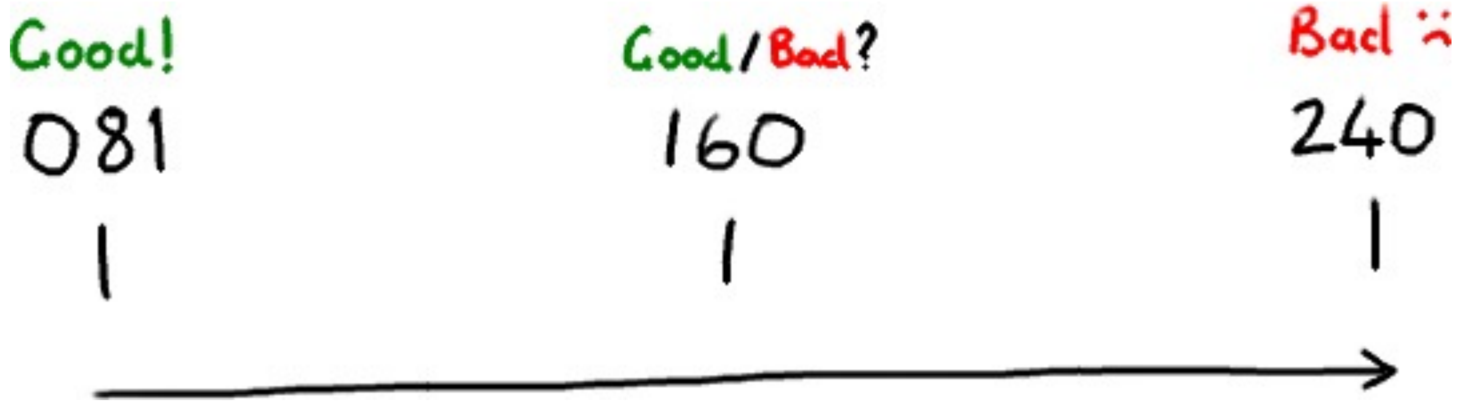
Not really...

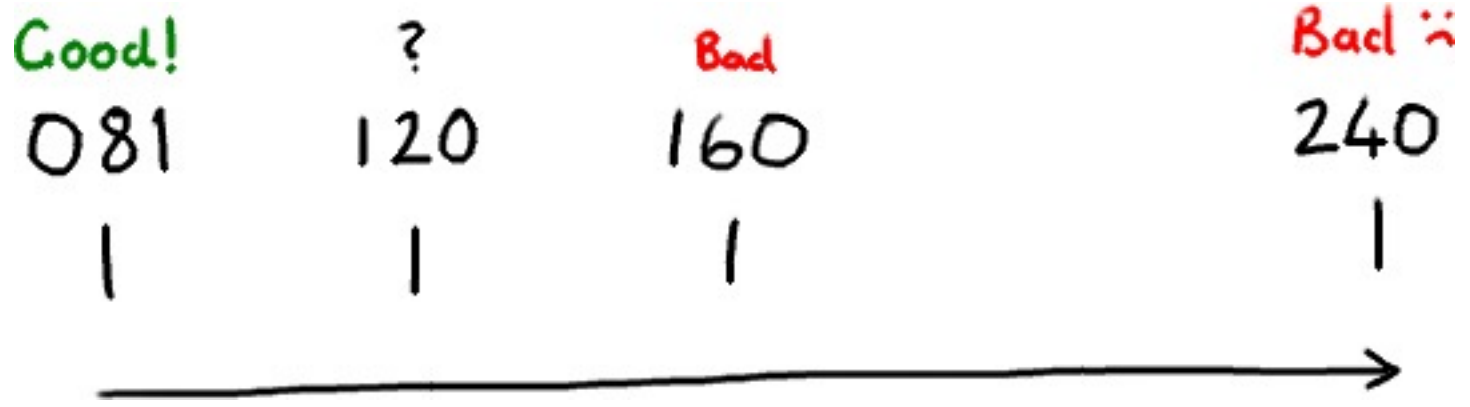
- Automated tests hadn’t been running for several days
- The performance environment didn’t have a simple way to redeploy previous versions
- ...it’s Internet Explorer

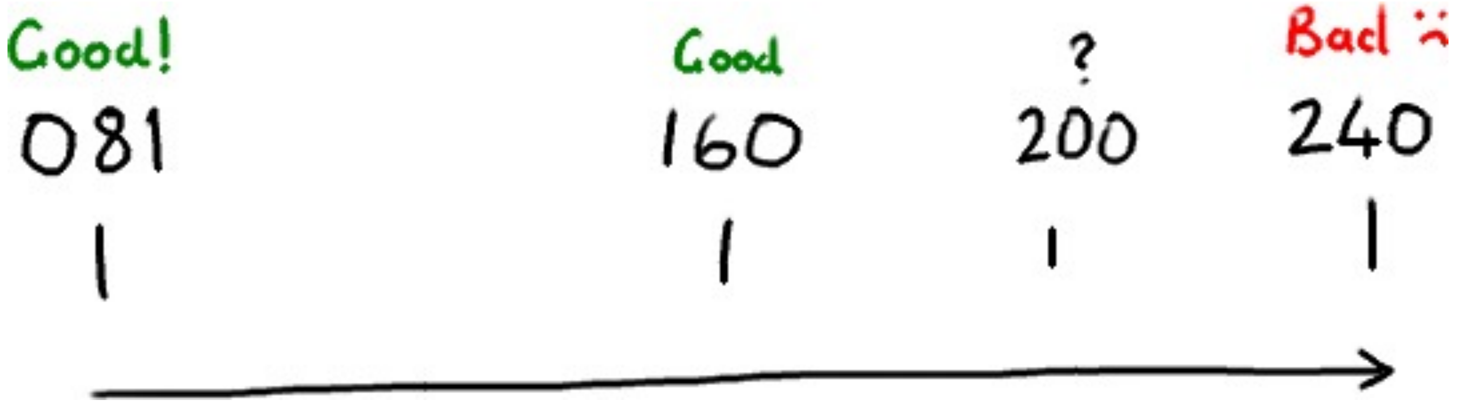
1. Eyeball the Revisions

2. Binary Search


Good!
081
Bad ☹
240


Good!
081
Good/Bad?
160
Bad :(
240


Good!
081
?
120
Bad
160
Bad ☹
240


Good!
081
Good
160
?
200
Bad ☹
240

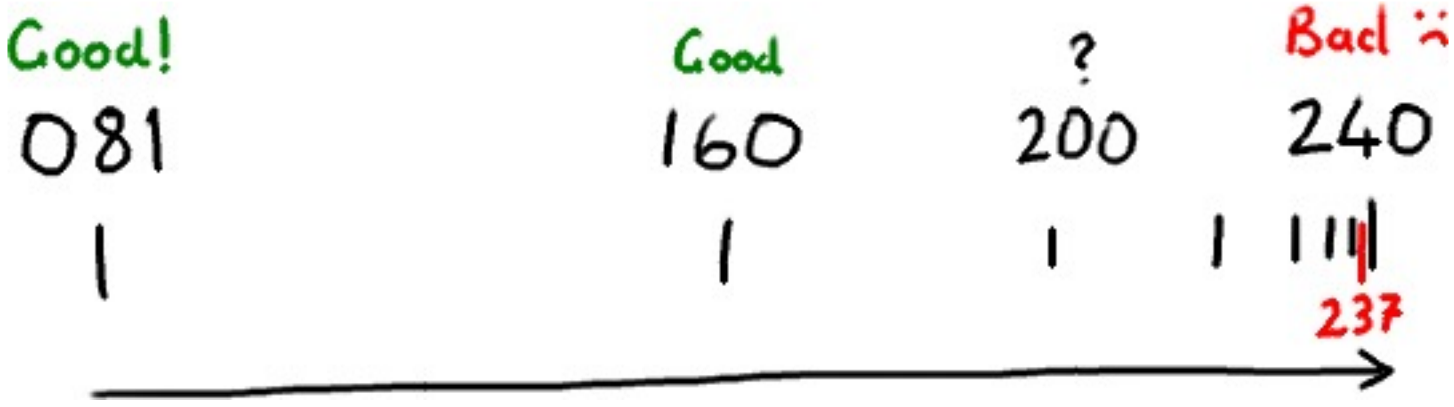
But first...

...can we start now?

Are we there yet?

I’m dying here

Binary search worst case?


Good!
081
Good
160
?
200
Bad :(
240
237

In Conclusion

- It’s a good thing we had perf tests
- Repeatable, reliable tests are handy
- Ask everyone in the team individually if they broke it
- Sometimes, it’s just not worth the time