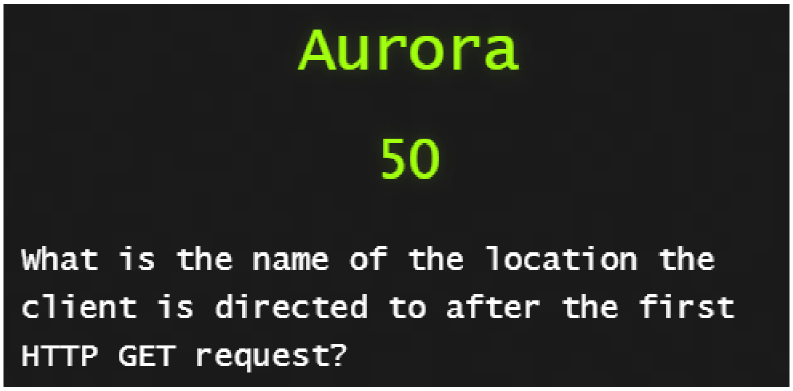
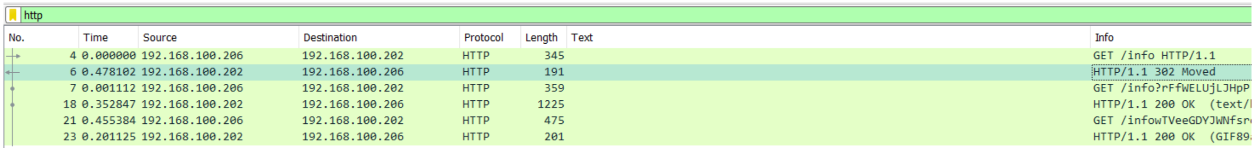


Aurora

50

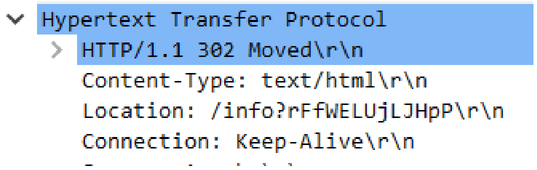
What is the name of the location the client is directed to after the first HTTP GET request?

Filter: http



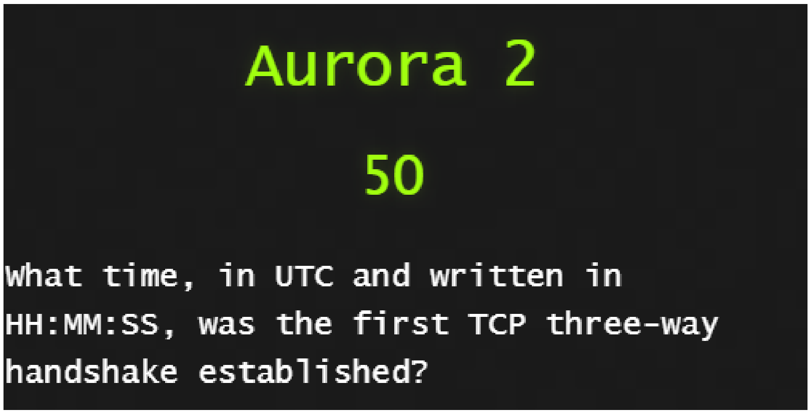
http

No.	Time	Source	Destination	Protocol	Length	Text	Info
4	0.000000	192.168.100.206	192.168.100.202	HTTP	345		GET /info HTTP/1.1
6	0.478102	192.168.100.202	192.168.100.206	HTTP	191		HTTP/1.1 302 Moved
7	0.001112	192.168.100.206	192.168.100.202	HTTP	359		GET /info?rFfWELUjLJHpP
18	0.352847	192.168.100.202	192.168.100.206	HTTP	1225		HTTP/1.1 200 OK (text/
21	0.455384	192.168.100.206	192.168.100.202	HTTP	475		GET /infowTVeeGDYJWNfsr
23	0.201125	192.168.100.202	192.168.100.206	HTTP	201		HTTP/1.1 200 OK (GIF89



```
Hypertext Transfer Protocol
  HTTP/1.1 302 Moved\r\n
  Content-Type: text/html\r\n
  Location: /info?rFfWELUjLJHpP\r\n
  Connection: Keep-Alive\r\n
```

Flag: /info?rFfWELUjLJHpP

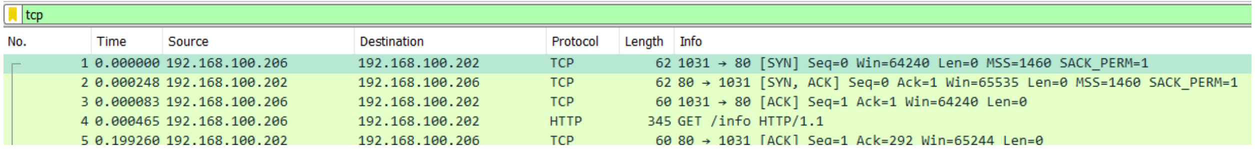


Aurora 2

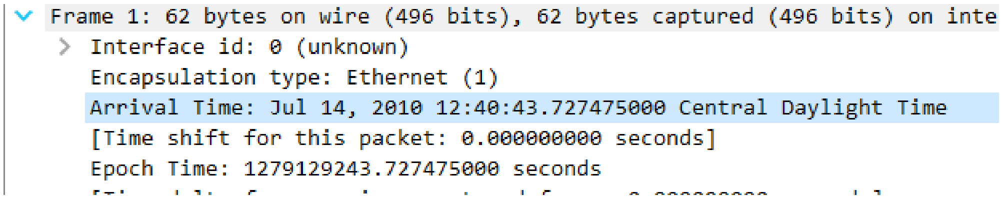
50

What time, in UTC and written in HH:MM:SS, was the first TCP three-way handshake established?

Filter: tcp



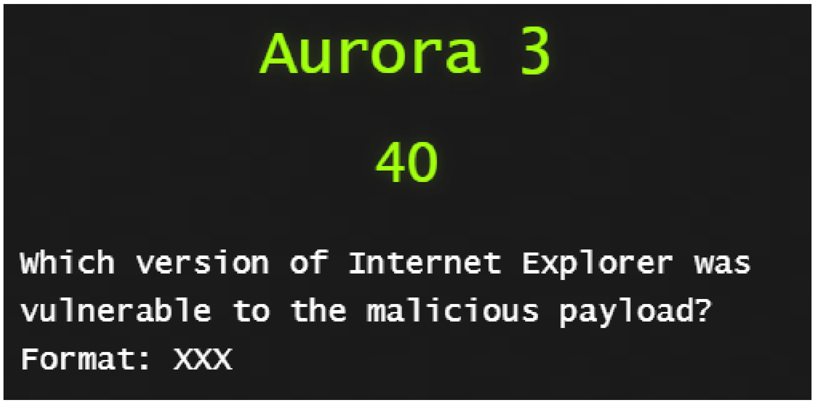
```
tcp
No.  Time     Source           Destination      Protocol  Length Info
   1 0.000000 192.168.100.206  192.168.100.202  TCP           62 1031 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
   2 0.000248 192.168.100.202  192.168.100.206  TCP           62 80 → 1031 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
   3 0.000083 192.168.100.206  192.168.100.202  TCP           60 1031 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   4 0.000465 192.168.100.206  192.168.100.202  HTTP         345 GET /info HTTP/1.1
   5 0.199260 192.168.100.202  192.168.100.206  TCP           60 80 → 1031 [ACK] Seq=1 Ack=292 Win=65244 Len=0
```



```
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on inte
   Interface id: 0 (unknown)
   Encapsulation type: Ethernet (1)
   Arrival Time: Jul 14, 2010 12:40:43.727475000 Central Daylight Time
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1279129243.727475000 seconds
   [Time delta from previous captured frame: 0.000000000 seconds]
```

Time: 7/14/2010 12:40:43 CST -> 17:40:43 UTC

Flag: 17:40:43



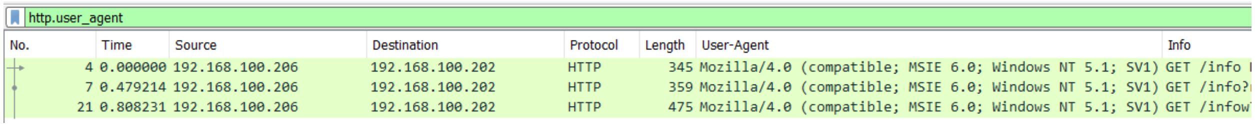
Aurora 3

40

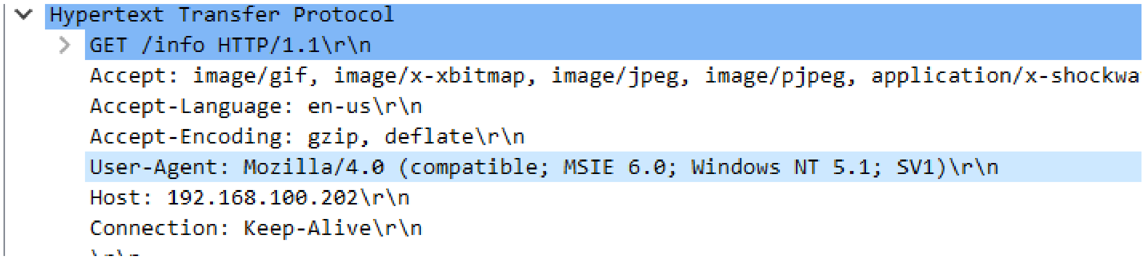
Which version of Internet Explorer was vulnerable to the malicious payload?
Format: XXX

Filter: http.user_agent

You can add a column to view all the user agent strings

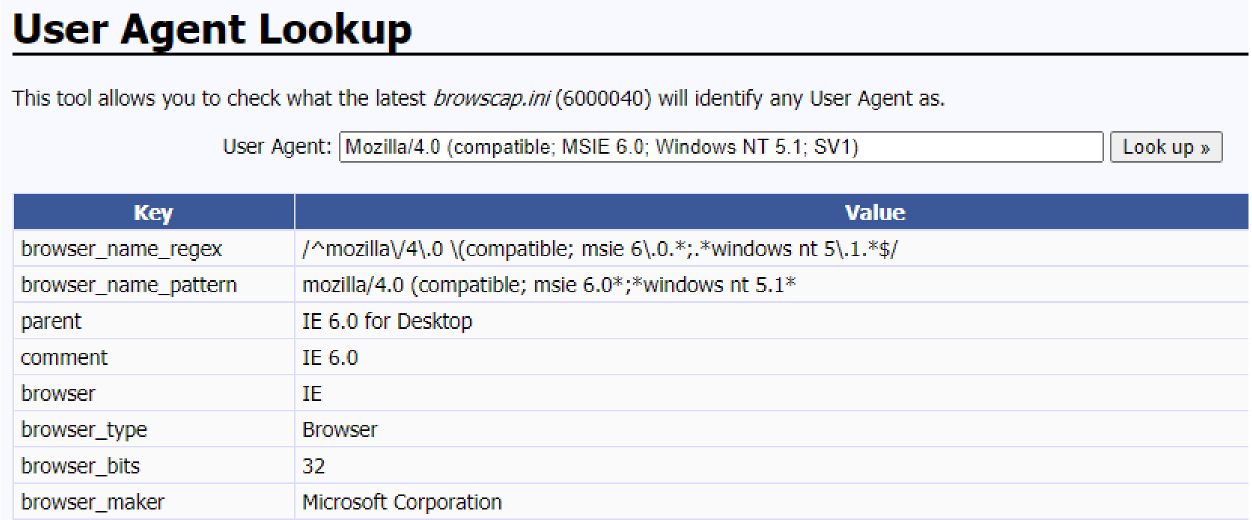


```
http.user_agent
No.   Time      Source           Destination      Protocol  Length User-Agent                                            Info
   4 0.000000 192.168.100.206 192.168.100.202 HTTP        345 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) GET /info 
   7 0.479214 192.168.100.206 192.168.100.202 HTTP        359 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) GET /info?
  21 0.808231 192.168.100.206 192.168.100.202 HTTP        475 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) GET /infow
```



```
Hypertext Transfer Protocol
  > GET /info HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwa
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
    Host: 192.168.100.202\r\n
    Connection: Keep-Alive\r\n
```

Take that string and look up the agent string online: http://www.browscap.org/ua-lookup



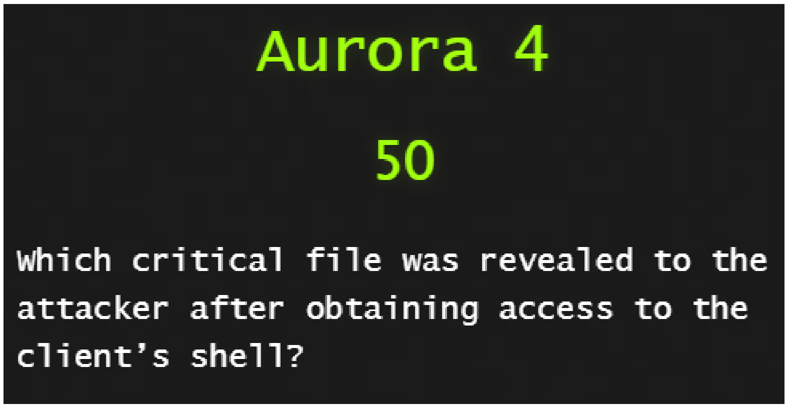
User Agent Lookup

This tool allows you to check what the latest *browscap.ini* (6000040) will identify any User Agent as.

User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Look up »

Key	Value
browser_name_regex	/^mozilla\/4\.0 \(compatible; msie 6\.0.*;.*windows nt 5\.1.*$/
browser_name_pattern	mozilla/4.0 (compatible; msie 6.0*;*windows nt 5.1*
parent	IE 6.0 for Desktop
comment	IE 6.0
browser	IE
browser_type	Browser
browser_bits	32
browser_maker	Microsoft Corporation

Flag: IE6



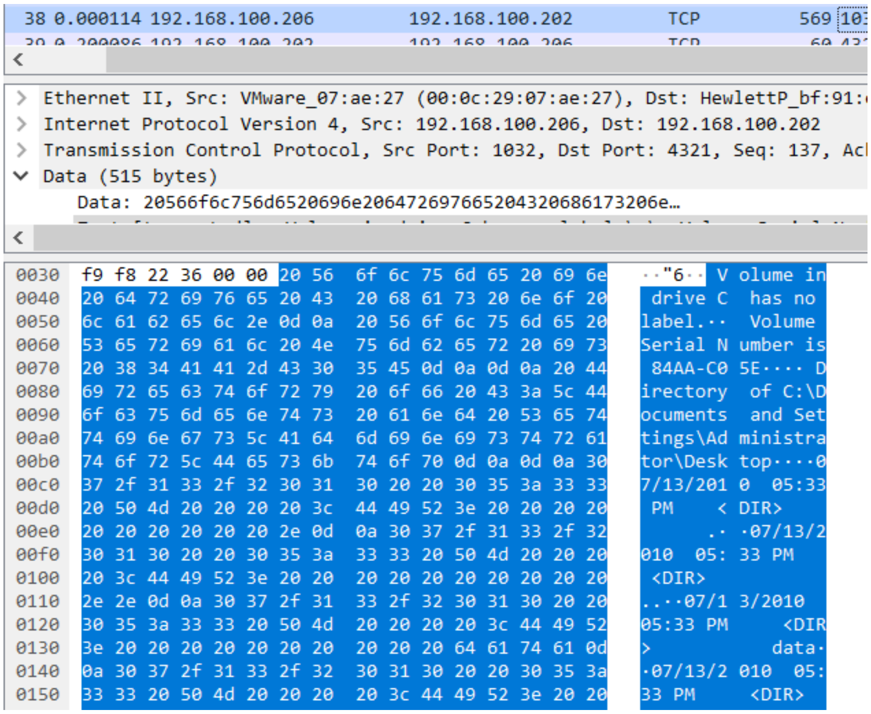
Aurora 4

50

Which critical file was revealed to the attacker after obtaining access to the client’s shell?

Filter: none

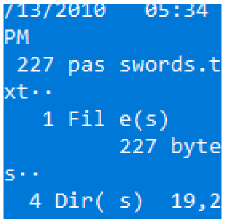
Looking at the tcp connection (this is the shellcode communication), we see that they are looking in the dir for the Administrator’s Desktop.



```
38 0.000114 192.168.100.206          192.168.100.202          TCP          569 10
```

```
> Ethernet II, Src: VMware_07:ae:27 (00:0c:29:07:ae:27), Dst: HewlettP_bf:91:
> Internet Protocol Version 4, Src: 192.168.100.206, Dst: 192.168.100.202
> Transmission Control Protocol, Src Port: 1032, Dst Port: 4321, Seq: 137, Ac
v Data (515 bytes)
     Data: 20566f6c756d6520696e206472697665204320686173206e…
```

```
0030  f9 f8 22 36 00 00 20 56  6f 6c 75 6d 65 20 69 6e   ··"6·· V olume in
0040  20 64 72 69 76 65 20 43  20 68 61 73 20 6e 6f 20    drive C  has no
0050  6c 61 62 65 6c 2e 0d 0a  20 56 6f 6c 75 6d 65 20   label.··  Volume
0060  53 65 72 69 61 6c 20 4e  75 6d 62 65 72 20 69 73   Serial N umber is
0070  20 38 34 41 41 2d 43 30  35 45 0d 0a 0d 0a 20 44    84AA-C0 5E···· D
0080  69 72 65 63 74 6f 72 79  20 6f 66 20 43 3a 5c 44   irectory  of C:\D
0090  6f 63 75 6d 65 6e 74 73  20 61 6e 64 20 53 65 74   ocuments  and Set
00a0  74 69 6e 67 73 5c 41 64  6d 69 6e 69 73 74 72 61   tings\Ad ministra
00b0  74 6f 72 5c 44 65 73 6b  74 6f 70 0d 0a 0d 0a 30   tor\Desk top····0
00c0  37 2f 31 33 2f 32 30 31  30 20 20 30 35 3a 33 33   7/13/201 0  05:33
00d0  20 50 4d 20 20 20 20 3c  44 49 52 3e 20 20 20 20    PM    < DIR>
00e0  20 20 20 20 20 20 2e 0d  0a 30 37 2f 31 33 2f 32         .· ·07/13/2
00f0  30 31 30 20 20 30 35 3a  33 33 20 50 4d 20 20 20   010  05: 33 PM
0100  20 3c 44 49 52 3e 20 20  20 20 20 20 20 20 20 20    <DIR>
0110  2e 2e 0d 0a 30 37 2f 31  33 2f 32 30 31 30 20 20   ..··07/1 3/2010
0120  30 35 3a 33 33 20 50 4d  20 20 20 20 3c 44 49 52   05:33 PM     <DIR
0130  3e 20 20 20 20 20 20 20  20 20 20 64 61 74 61 0d   >           data·
0140  0a 30 37 2f 31 33 2f 32  30 31 30 20 20 30 35 3a   ·07/13/2 010  05:
0150  33 33 20 50 4d 20 20 20  20 3c 44 49 52 3e 20 20   33 PM    <DIR>
```



```
/13/2010   05:34
PM
 227 pas swords.t
xt··
   1 Fil e(s)
         227 byte
s··
  4 Dir( s)   19,2
```

One file they look at is passwords.txt

Flag: passwords.txt