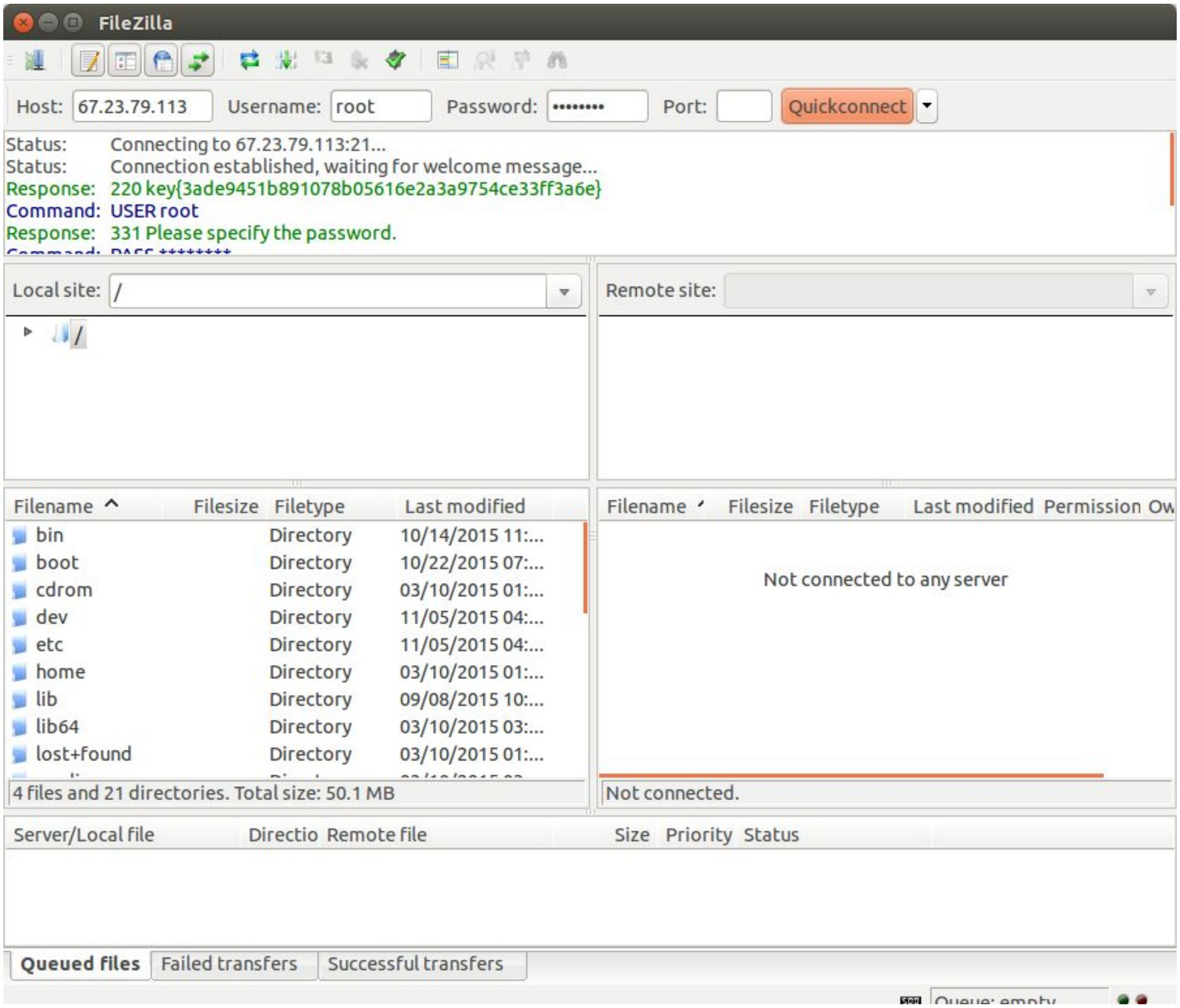
Zachary Sogard
Alex Goldschmidt
Obaid Farooqui
Daniel Kim
Lisa Fan

CTF Team 4 Write-Up

Unnecessary service: Ran “nmap 67.23.79.113”. Noticed that port 21 (FTP) was open. Attempted to connect to the server via filezilla. The response contained a key.



Host: 67.23.79.113 Username: root Password: •••••••• Port:

```
Status:     Connecting to 67.23.79.113:21...
Status:     Connection established, waiting for welcome message...
Response:   220 key{3ade9451b891078b05616e2a3a9754ce33ff3a6e}
Command:    USER root
Response:   331 Please specify the password.
Command:    PASS ********
```

Local site: /

Remote site:

Filename ^	Filesize	Filetype	Last modified
bin		Directory	10/14/2015 11:...
boot		Directory	10/22/2015 07:...
cdrom		Directory	03/10/2015 01:...
dev		Directory	11/05/2015 04:...
etc		Directory	11/05/2015 04:...
home		Directory	03/10/2015 01:...
lib		Directory	09/08/2015 10:...
lib64		Directory	03/10/2015 03:...
lost+found		Directory	03/10/2015 01:...

4 files and 21 directories. Total size: 50.1 MB

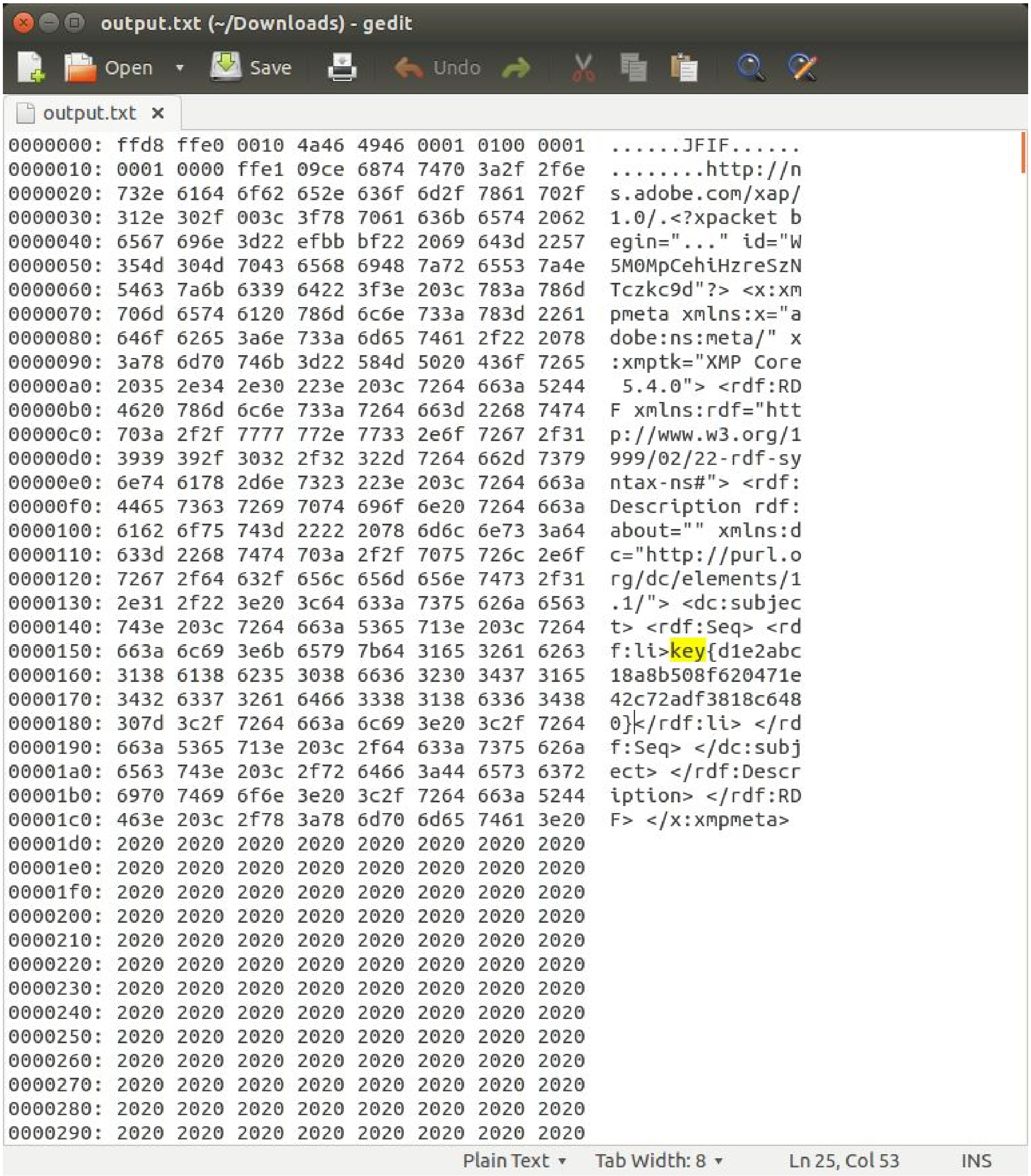
Filename	Filesize	Filetype	Last modified	Permission	Ow

Not connected to any server

Not connected.

Server/Local file	Directio	Remote file	Size	Priority	Status

Searching the binary: Noticed the site was running wordpress and looked at ctf/wp-content/uploads folder. Found 8 jpgs of Uncle Herbert. Downloaded these and searched the binary by running “xxd uncleherbert*.jpg | grep key” on each. Got a match on uncleherbert2.jpg which was a key.

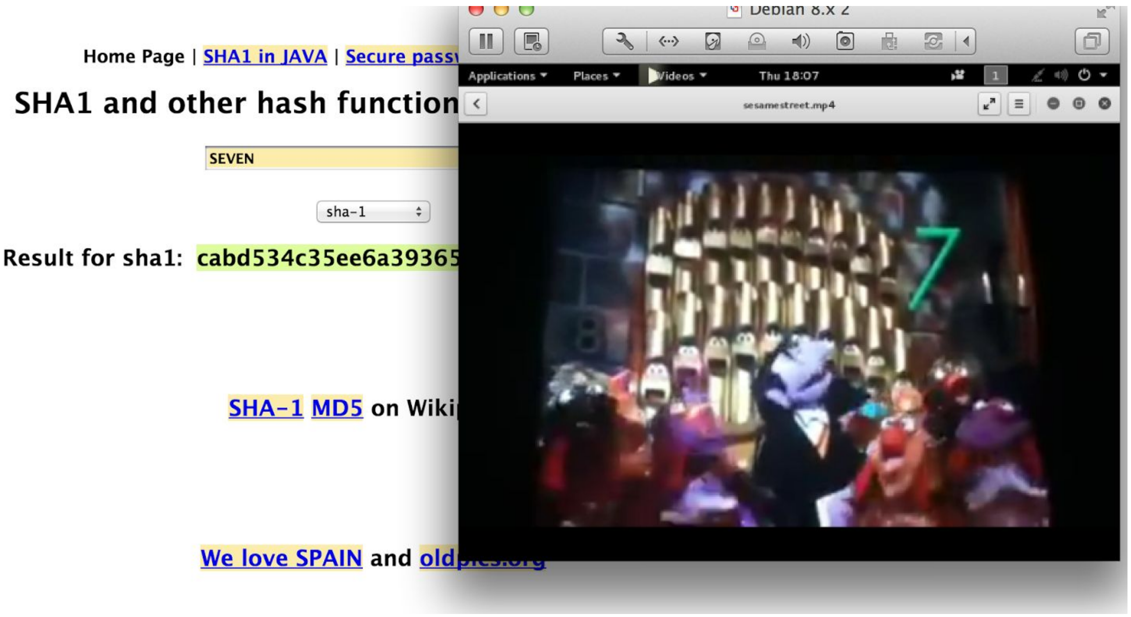


```
0000000: ffd8 ffe0 0010 4a46 4946 0001 0100 0001  ......JFIF......
0000010: 0001 0000 ffe1 09ce 6874 7470 3a2f 2f6e  ........http://n
0000020: 732e 6164 6f62 652e 636f 6d2f 7861 702f  s.adobe.com/xap/
0000030: 312e 302f 003c 3f78 7061 636b 6574 2062  1.0/.<?xpacket b
0000040: 6567 696e 3d22 efbb bf22 2069 643d 2257  egin="..." id="W
0000050: 354d 304d 7043 6568 6948 7a72 6553 7a4e  5M0MpCehiHzreSzN
0000060: 5463 7a6b 6339 6422 3f3e 203c 783a 786d  Tczkc9d"?> <x:xm
0000070: 706d 6574 6120 786d 6c6e 733a 783d 2261  pmeta xmlns:x="a
0000080: 646f 6265 3a6e 733a 6d65 7461 2f22 2078  dobe:ns:meta/" x
0000090: 3a78 6d70 746b 3d22 584d 5020 436f 7265  :xmptk="XMP Core
00000a0: 2035 2e34 2e30 223e 203c 7264 663a 5244   5.4.0"> <rdf:RD
00000b0: 4620 786d 6c6e 733a 7264 663d 2268 7474  F xmlns:rdf="htt
00000c0: 703a 2f2f 7777 772e 7733 2e6f 7267 2f31  p://www.w3.org/1
00000d0: 3939 392f 3032 2f32 322d 7264 662d 7379  999/02/22-rdf-sy
00000e0: 6e74 6178 2d6e 7323 223e 203c 7264 663a  ntax-ns#"> <rdf:
00000f0: 4465 7363 7269 7074 696f 6e20 7264 663a  Description rdf:
0000100: 6162 6f75 743d 2222 2078 6d6c 6e73 3a64  about="" xmlns:d
0000110: 633d 2268 7474 703a 2f2f 7075 726c 2e6f  c="http://purl.o
0000120: 7267 2f64 632f 656c 656d 656e 7473 2f31  rg/dc/elements/1
0000130: 2e31 2f22 3e20 3c64 633a 7375 626a 6563  .1/"> <dc:subjec
0000140: 743e 203c 7264 663a 5365 713e 203c 7264  t> <rdf:Seq> <rd
0000150: 663a 6c69 3e6b 6579 7b64 3165 3261 6263  f:li>key{d1e2abc
0000160: 3138 6138 6235 3038 6636 3230 3437 3165  18a8b508f620471e
0000170: 3432 6337 3261 6466 3338 3138 6336 3438  42c72adf3818c648
0000180: 307d 3c2f 7264 663a 6c69 3e20 3c2f 7264  0}</rdf:li> </rd
0000190: 663a 5365 713e 203c 2f64 633a 7375 626a  f:Seq> </dc:subj
00001a0: 6563 743e 203c 2f72 6466 3a44 6573 6372  ect> </rdf:Descr
00001b0: 6970 7469 6f6e 3e20 3c2f 7264 663a 5244  iption> </rdf:RD
00001c0: 463e 203c 2f78 3a78 6d70 6d65 7461 3e20  F> </x:xmpmeta>
00001d0: 2020 2020 2020 2020 2020 2020 2020 2020
00001e0: 2020 2020 2020 2020 2020 2020 2020 2020
00001f0: 2020 2020 2020 2020 2020 2020 2020 2020
0000200: 2020 2020 2020 2020 2020 2020 2020 2020
0000210: 2020 2020 2020 2020 2020 2020 2020 2020
0000220: 2020 2020 2020 2020 2020 2020 2020 2020
0000230: 2020 2020 2020 2020 2020 2020 2020 2020
0000240: 2020 2020 2020 2020 2020 2020 2020 2020
0000250: 2020 2020 2020 2020 2020 2020 2020 2020
0000260: 2020 2020 2020 2020 2020 2020 2020 2020
0000270: 2020 2020 2020 2020 2020 2020 2020 2020
0000280: 2020 2020 2020 2020 2020 2020 2020 2020
0000290: 2020 2020 2020 2020 2020 2020 2020 2020
```

Video key:

First we looked on http://67.23.79.113/ctf/ and downloaded runme.exe. Next, we ran xxd runme.exe and read through the text, which told us to watch the video and find the SHA-1 of the number from the video spelled in caps.

After a few misguided attempts at looking for the video on the website in /Movies and /sesamestreet, we opened readme.exe in wireshark and exported object as HTTP and then saved the video that was there. Next we watched the video, eventually tried the SHA-1 of SEVEN, and it worked!



Home Page | SHA1 in JAVA | Secure pass

SHA1 and other hash function

SEVEN

sha-1

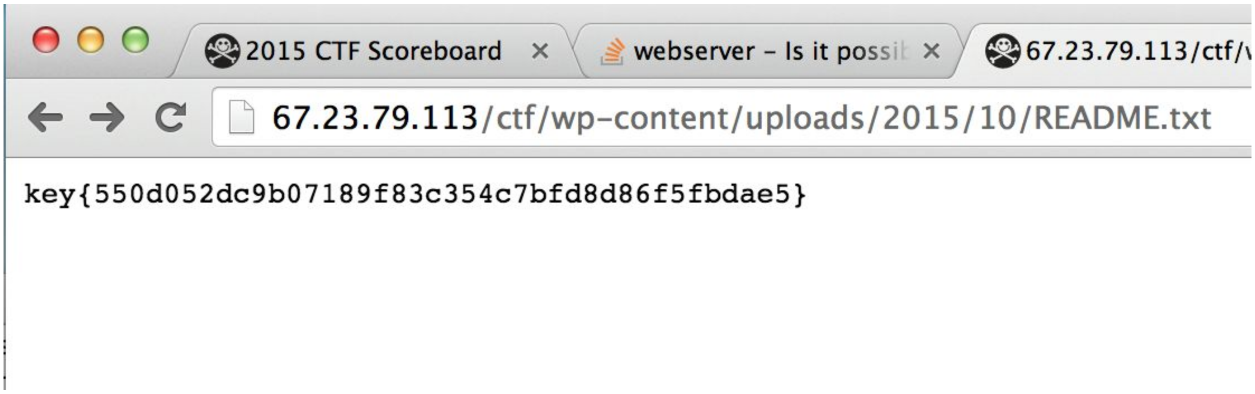
Result for sha1: cabd534c35ee6a39365

SHA-1 MD5 on Wiki

We love SPAIN and oldpics.org

README.txt key:

Noticing that this was a wordpress site, we tried http://67.23.79.113/ctf/wp-content/uploads/ and were happy to see that that we had access to a number of files. Naturally, we opened the README.txt and were elated to find a key there.



```
key{550d052dc9b07189f83c354c7bfd8d86f5fbdae5}
```