POLITECHNIKA ŚWIĘTOKRZYSKA

LABORATORIUM CYBERBEZPIECZEŃSTWO

Numer ćwiczenia: 4	**Temat ćwiczenia:** Using File and Data Integrity Checks	Damian Zdyb
Data wykonania: 04.12.2018	**Data oddania do sprawdzenia:** 08.12.2018	**Ocena:**

Part 1: Download the Client Files to Mike’s PC

Step 1: Access the FTP server from Mike’s PC.

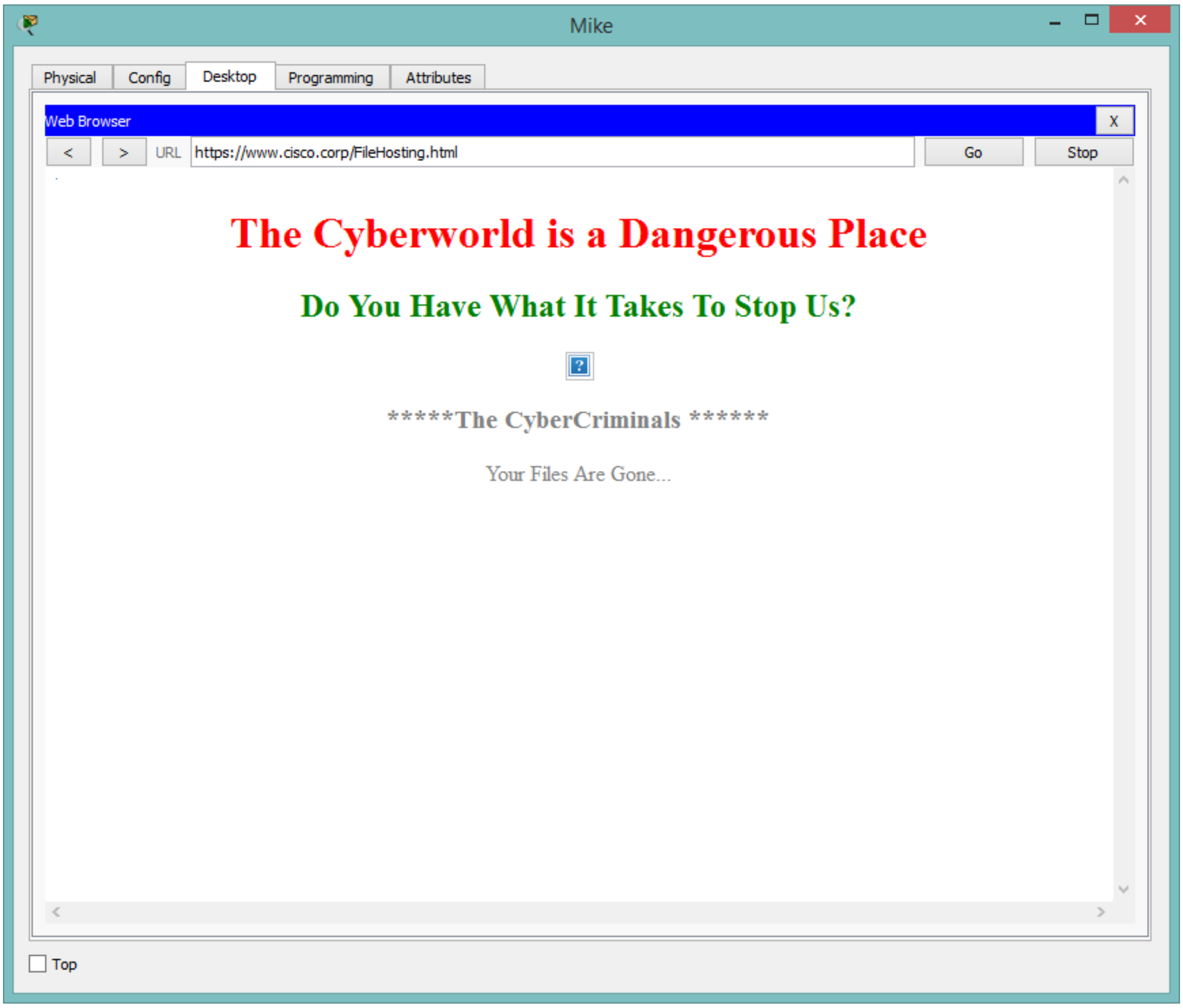
a. Click the **Gotham Healthcare Branch** site and then click the PC **Mike**.

b. Click the **Desktop** tab and then click **Web Browser**.

c. Enter the URL **http://www.cisco.corp** and click **Go**.

d. Click the link to download the most current files.

What protocol was used to access this webpage on the backup file server?



https://www.cisco.corp/FileHosting.html

The Cyberworld is a Dangerous Place

Do You Have What It Takes To Stop Us?

*****The CyberCriminals ******

Your Files Are Gone...

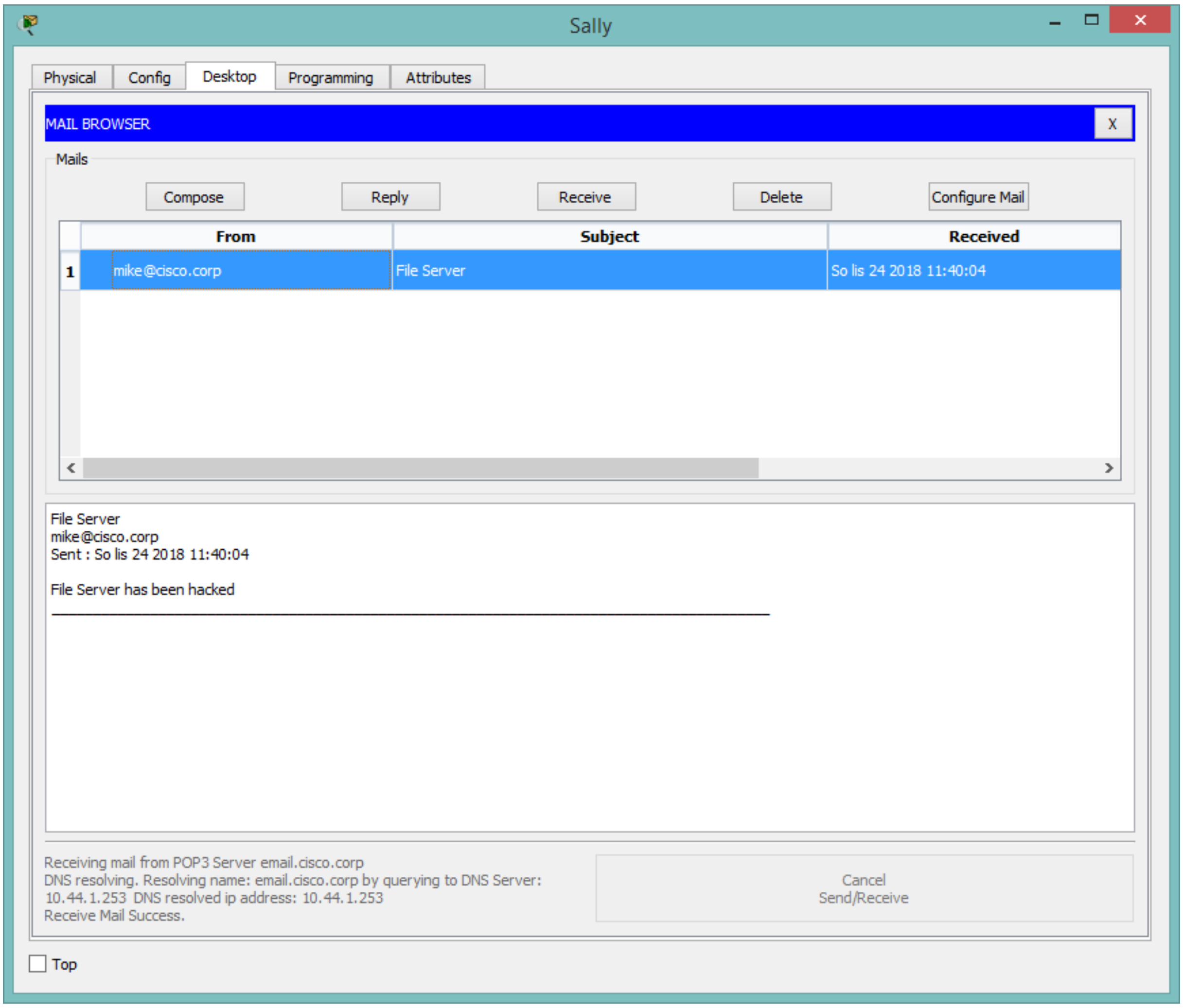
Został tu użyty protokół HTTP dzięki, któremu poprzez strone internetową mamy dostęp do plików kopii zapasowej.

Step 2: The file server has been hacked, notify Sally.

a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

b. Click the **Desktop** tab and then click **Email**.

c. Create an email and send it to Sally@cisco.corp and tell her about the File Server.



	From	Subject	Received
1	mike@cisco.corp	File Server	So lis 24 2018 11:40:04

File Server
mike@cisco.corp
Sent : So lis 24 2018 11:40:04

File Server has been hacked

```
Receiving mail from POP3 Server email.cisco.corp
DNS resolving. Resolving name: email.cisco.corp by querying to DNS Server:
10.44.1.253 DNS resolved ip address: 10.44.1.253
Receive Mail Success.
```

Po wysłaniu maila widzimy, że doszedł on od Mike'a.

Part 2: Download the Client Files from the Backup File Server to Mike’s PC

Step 1: Access the offsite FTP server from Mike’s PC.

a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

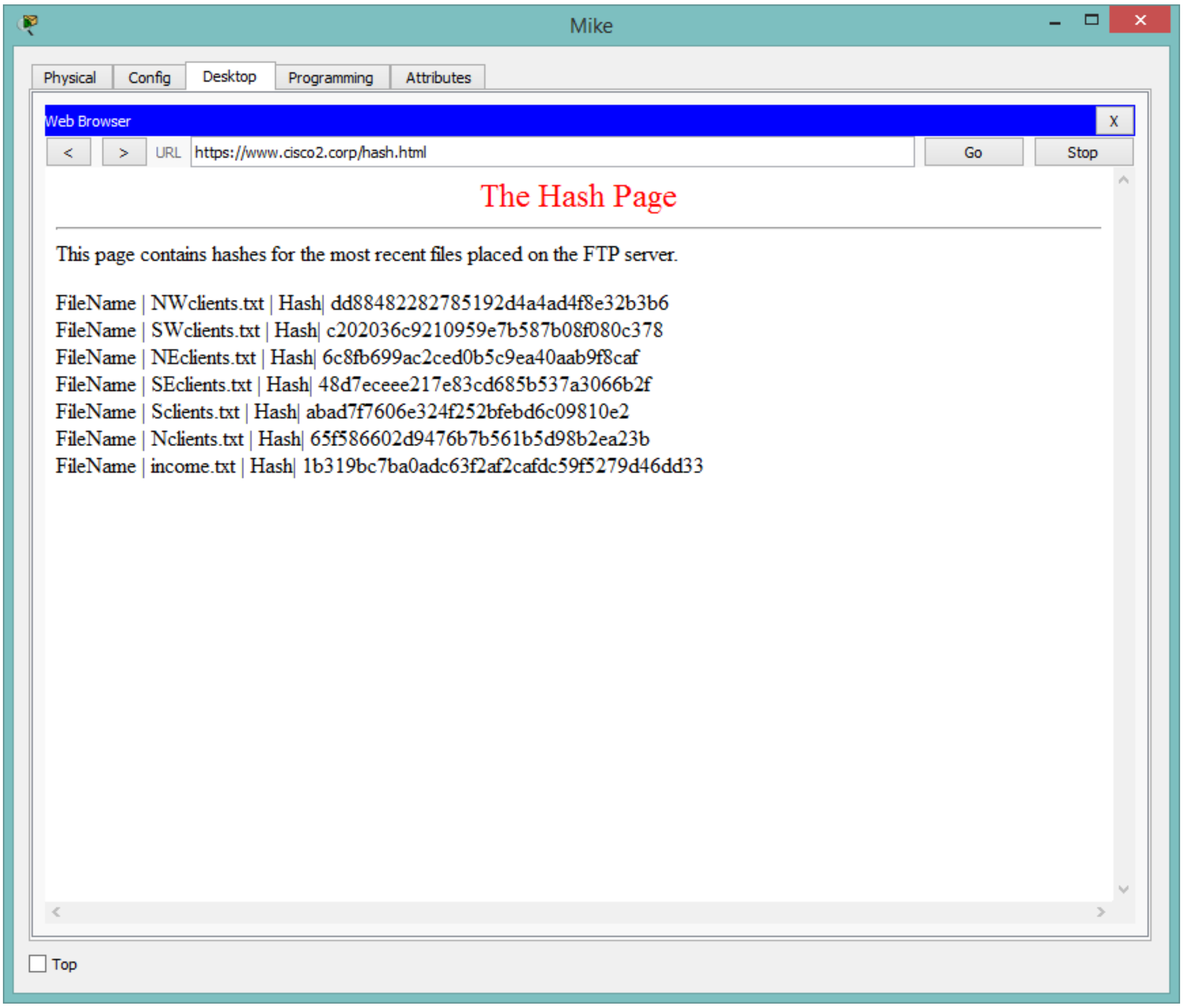
b. Click the **Desktop** tab and then click **Web Browser**.

c. Enter the URL **https://www.cisco2.corp** and click **Go**.

d. Click the link to view the most recent files and their hashes.

What protocol was used to access this webpage on the backup file server?

What are the file names and hashes of the client files on the backup server? (copy and paste them below)



URL: https://www.cisco2.corp/hash.html

The Hash Page

This page contains hashes for the most recent files placed on the FTP server.

```
FileName | NWclients.txt | Hash| dd88482282785192d4a4ad4f8e32b3b6
FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378
FileName | NEclients.txt | Hash| 6c8fb699ac2ced0b5c9ea40aab9f8caf
FileName | SEclients.txt | Hash| 48d7eceee217e83cd685b537a3066b2f
FileName | Sclients.txt | Hash| abad7f7606e324f252bfebd6c09810e2
FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b
FileName | income.txt | Hash| 1b319bc7ba0adc63f2af2cafdc59f5279d46dd33
```

Tutaj również mamy protokół HTTP do plików kopii zapasowej. W tym przypadku pliki są zabezpieczone hashem.

Step 2: Download the client files to Mike’s PC.

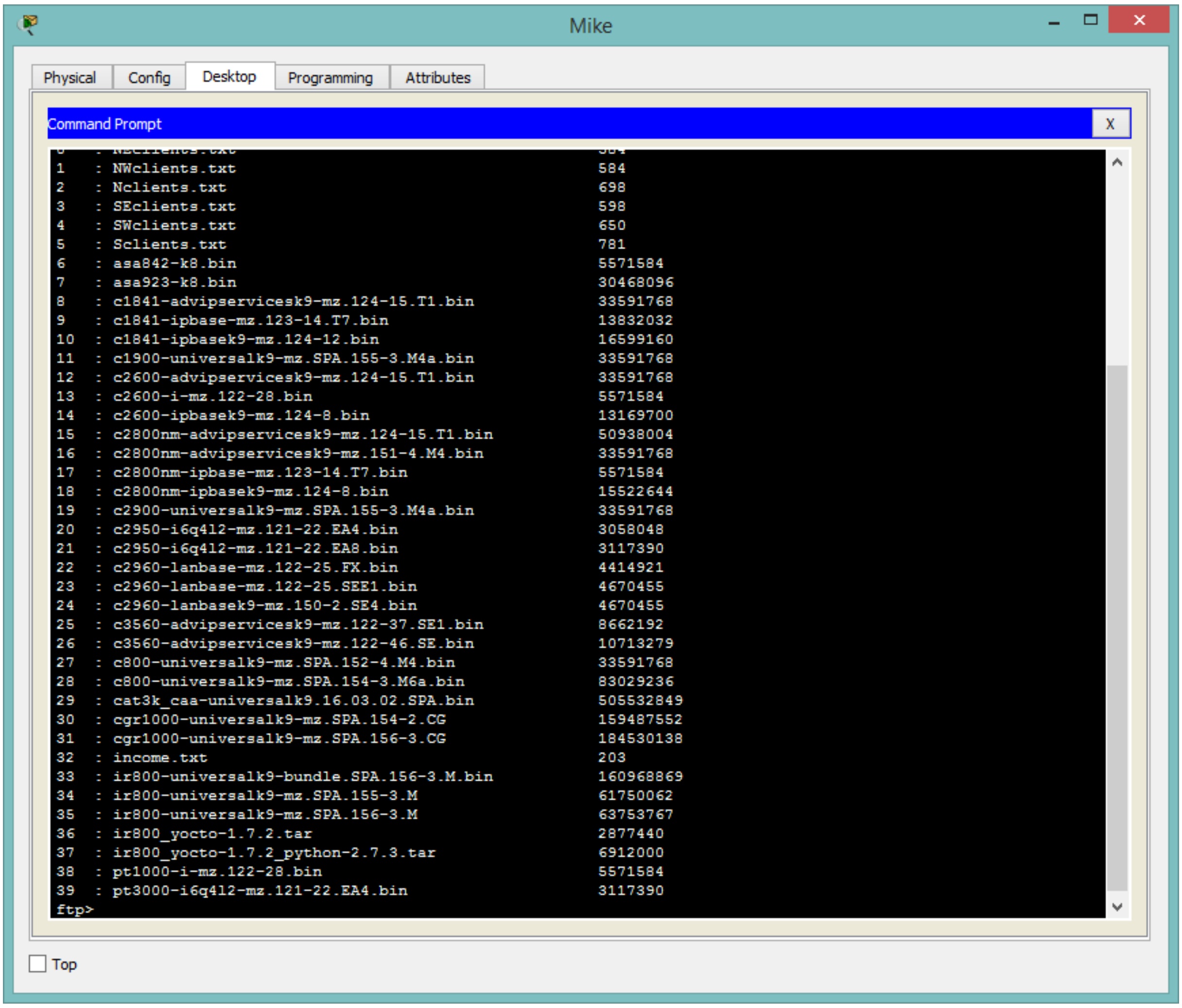
a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

b. Click the **Desktop** tab and then click **Command Prompt**.

c. Connect to the **Backup File** server by entering **ftp www.cisco2.corp** in the command prompt.

d. Enter the username of **mike** and a password of **cisco123**.

e. At the **ftp>** prompt, enter the command **dir** to view the current files stored on the remote FTP server.



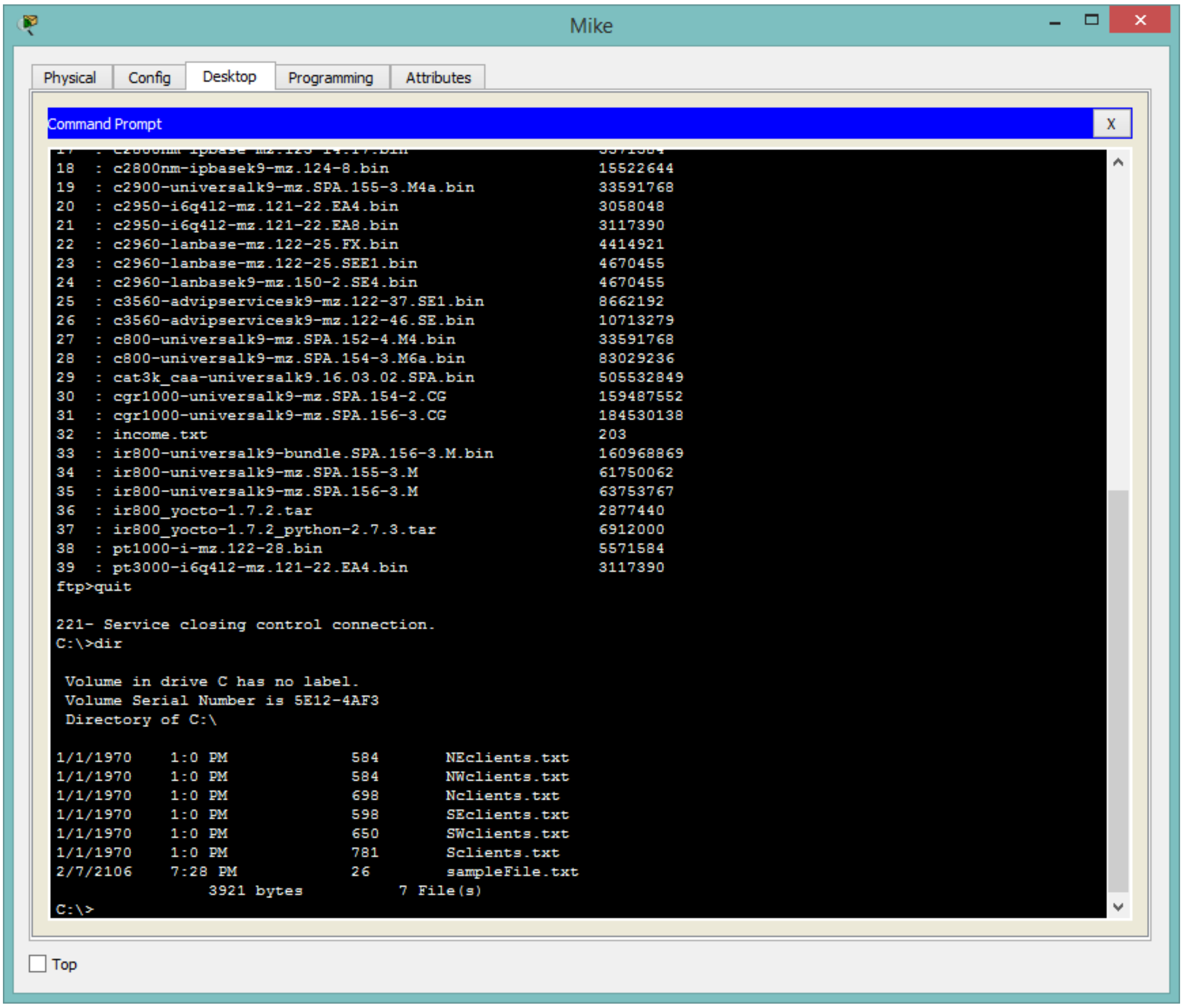
```
0   : NEclients.txt                                    584
1   : NWclients.txt                                    584
2   : Nclients.txt                                     698
3   : SEclients.txt                                    598
4   : SWclients.txt                                    650
5   : Sclients.txt                                     781
6   : asa842-k8.bin                                    5571584
7   : asa923-k8.bin                                    30468096
8   : c1841-advipservicesk9-mz.124-15.T1.bin           33591768
9   : c1841-ipbase-mz.123-14.T7.bin                    13832032
10  : c1841-ipbasek9-mz.124-12.bin                     16599160
11  : c1900-universalk9-mz.SPA.155-3.M4a.bin           33591768
12  : c2600-advipservicesk9-mz.124-15.T1.bin           33591768
13  : c2600-i-mz.122-28.bin                            5571584
14  : c2600-ipbasek9-mz.124-8.bin                      13169700
15  : c2800nm-advipservicesk9-mz.124-15.T1.bin         50938004
16  : c2800nm-advipservicesk9-mz.151-4.M4.bin          33591768
17  : c2800nm-ipbase-mz.123-14.T7.bin                  5571584
18  : c2800nm-ipbasek9-mz.124-8.bin                    15522644
19  : c2900-universalk9-mz.SPA.155-3.M4a.bin           33591768
20  : c2950-i6q4l2-mz.121-22.EA4.bin                   3058048
21  : c2950-i6q4l2-mz.121-22.EA8.bin                   3117390
22  : c2960-lanbase-mz.122-25.FX.bin                   4414921
23  : c2960-lanbase-mz.122-25.SEE1.bin                 4670455
24  : c2960-lanbasek9-mz.150-2.SE4.bin                 4670455
25  : c3560-advipservicesk9-mz.122-37.SE1.bin          8662192
26  : c3560-advipservicesk9-mz.122-46.SE.bin           10713279
27  : c800-universalk9-mz.SPA.152-4.M4.bin             33591768
28  : c800-universalk9-mz.SPA.154-3.M6a.bin            83029236
29  : cat3k_caa-universalk9.16.03.02.SPA.bin           505532849
30  : cgr1000-universalk9-mz.SPA.154-2.CG              159487552
31  : cgr1000-universalk9-mz.SPA.156-3.CG              184530138
32  : income.txt                                       203
33  : ir800-universalk9-bundle.SPA.156-3.M.bin         160968869
34  : ir800-universalk9-mz.SPA.155-3.M                 61750062
35  : ir800-universalk9-mz.SPA.156-3.M                 63753767
36  : ir800_yocto-1.7.2.tar                            2877440
37  : ir800_yocto-1.7.2_python-2.7.3.tar               6912000
38  : pt1000-i-mz.122-28.bin                           5571584
39  : pt3000-i6q4l2-mz.121-22.EA4.bin                  3117390
ftp>
```

f. Download the six client files (NEclients.txt, NWclients.txt, Nclients.txt, SEclients.txt, SWclients.txt, and Sclients.txt) to Mike’s PC by entering the command **get FILENAME.txt**, replace FILENAME with one of the six client filenames.

```
ftp> get NEclients.txt

Reading file NEclients.txt from www.cisco2.corp:
File transfer in progress...

[Transfer complete - 584 bytes]

584 bytes copied in 0.05 secs (11680 bytes/sec)
```

g. After downloading all the files, enter the command **quit** at the **ftp>** prompt.

h. At the **PC>** prompt, enter the command **dir** and verify the client files are now on Mike’s PC.



```
17  : c2800nm-ipbase-mz.123-14.T7.bin                    5571584
18  : c2800nm-ipbasek9-mz.124-8.bin                      15522644
19  : c2900-universalk9-mz.SPA.155-3.M4a.bin             33591768
20  : c2950-i6q4l2-mz.121-22.EA4.bin                     3058048
21  : c2950-i6q4l2-mz.121-22.EA8.bin                     3117390
22  : c2960-lanbase-mz.122-25.FX.bin                     4414921
23  : c2960-lanbase-mz.122-25.SEE1.bin                   4670455
24  : c2960-lanbasek9-mz.150-2.SE4.bin                   4670455
25  : c3560-advipservicesk9-mz.122-37.SE1.bin            8662192
26  : c3560-advipservicesk9-mz.122-46.SE.bin             10713279
27  : c800-universalk9-mz.SPA.152-4.M4.bin               33591768
28  : c800-universalk9-mz.SPA.154-3.M6a.bin              83029236
29  : cat3k_caa-universalk9.16.03.02.SPA.bin             505532849
30  : cgr1000-universalk9-mz.SPA.154-2.CG                159487552
31  : cgr1000-universalk9-mz.SPA.156-3.CG                184530138
32  : income.txt                                         203
33  : ir800-universalk9-bundle.SPA.156-3.M.bin           160968869
34  : ir800-universalk9-mz.SPA.155-3.M                   61750062
35  : ir800-universalk9-mz.SPA.156-3.M                   63753767
36  : ir800_yocto-1.7.2.tar                              2877440
37  : ir800_yocto-1.7.2_python-2.7.3.tar                 6912000
38  : pt1000-i-mz.122-28.bin                             5571584
39  : pt3000-i6q4l2-mz.121-22.EA4.bin                    3117390
ftp>quit

221- Service closing control connection.
C:\>dir

 Volume in drive C has no label.
 Volume Serial Number is 5E12-4AF3
 Directory of C:\

1/1/1970     1:0  PM              584       NEclients.txt
1/1/1970     1:0  PM              584       NWclients.txt
1/1/1970     1:0  PM              698       Nclients.txt
1/1/1970     1:0  PM              598       SEclients.txt
1/1/1970     1:0  PM              650       SWclients.txt
1/1/1970     1:0  PM              781       Sclients.txt
2/7/2106     7:28  PM             26        sampleFile.txt
                3921 bytes             7 File(s)
C:\>
```

Wszystkie pliki zostały pobrane na computer Mike’a

Part 3: Verify the Integrity of the Client Files using Hashing

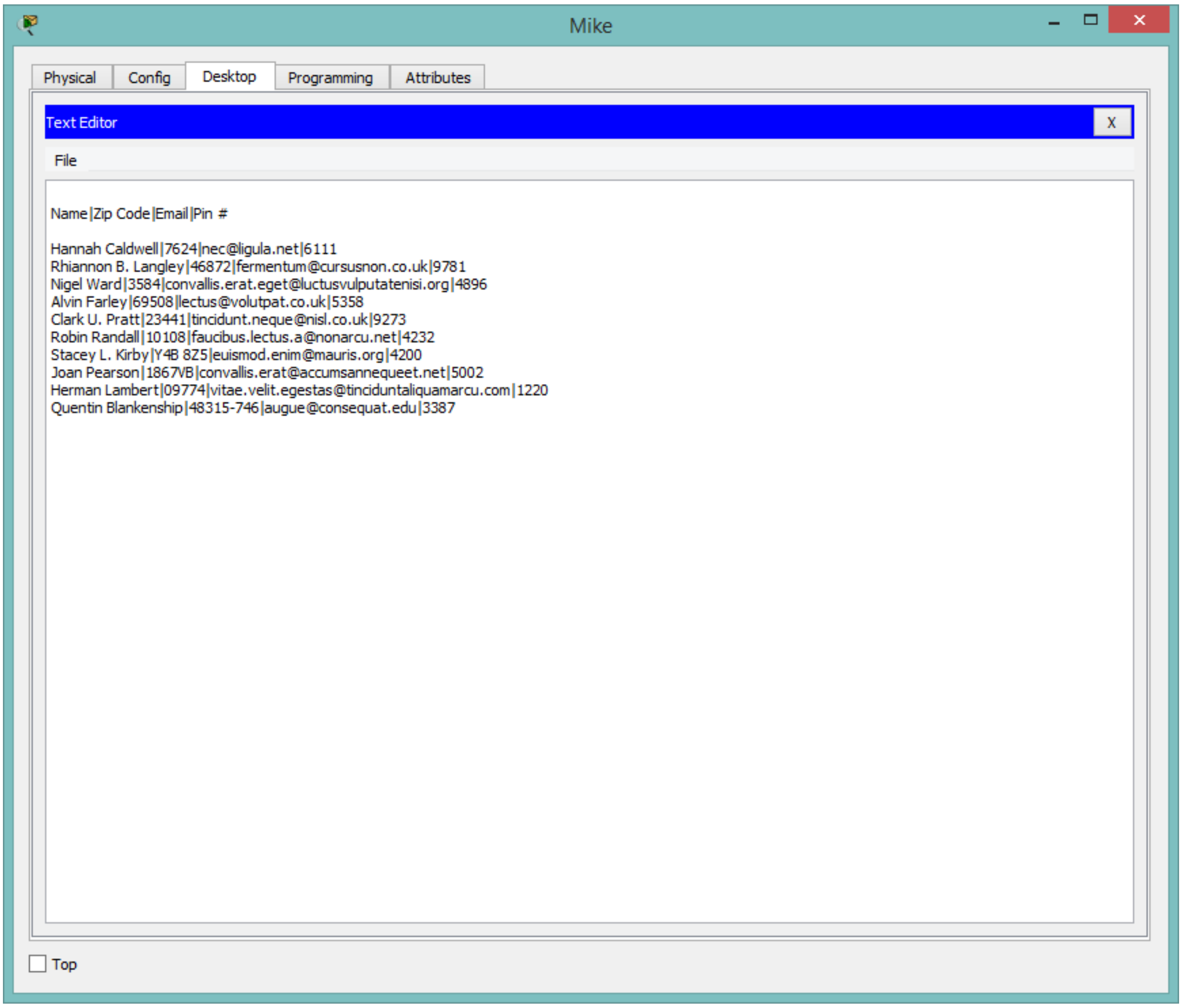
Step 1: Check the hashes on the client files on Mike’s PC.

a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

b. Click the **Desktop** tab and then click **Text Editor**.

c. In the Text Editor window, click **File** > **Open**.

d. Click on the first document **NEclients.txt** and click **OK**.



```
Name|Zip Code|Email|Pin #

Hannah Caldwell|7624|nec@ligula.net|6111
Rhiannon B. Langley|46872|fermentum@cursusnon.co.uk|9781
Nigel Ward|3584|convallis.erat.eget@luctusvulputatenisi.org|4896
Alvin Farley|69508|lectus@volutpat.co.uk|5358
Clark U. Pratt|23441|tincidunt.neque@nisl.co.uk|9273
Robin Randall|10108|faucibus.lectus.a@nonarcu.net|4232
Stacey L. Kirby|Y4B 8Z5|euismod.enim@mauris.org|4200
Joan Pearson|1867VB|convallis.erat@accumsannequeet.net|5002
Herman Lambert|09774|vitae.velit.egestas@tinciduntaliquamarcu.com|1220
Quentin Blankenship|48315-746|augue@consequat.edu|3387
```

e. Copy the entire text document contents.

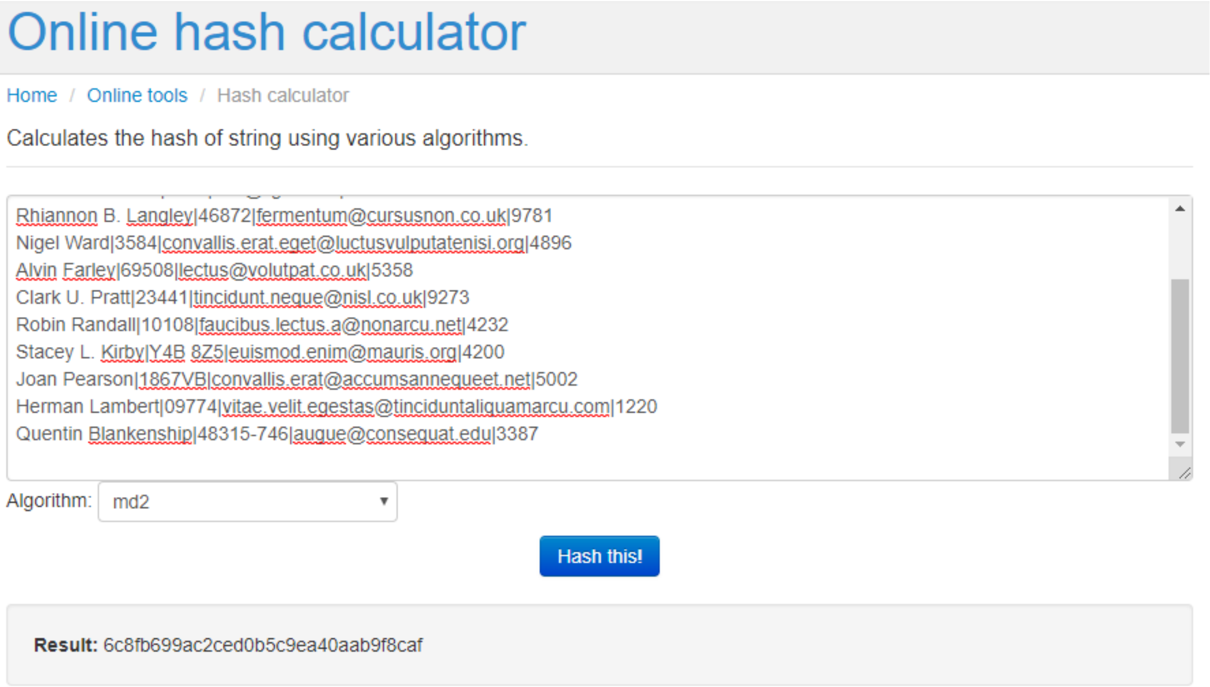
f. Open a web browser on your personal computer and browse to the website https://www.tools4noobs.com/online_tools/hash/

g. Click the whitespace and paste in the text document contents. Make sure the algorithm is set to md2. Click **Hash this!**.

h. To make sure a file has not been tampered with, you will compare the resulting hash with the filename/hash information you found in Part 2 Step 1.

i. Repeat Steps d through h for each client file and compare the generated hash with the original hash shown in Part 2 Step 1.

Which file has been tampered with and has an incorrect hash?



Online hash calculator

Home / Online tools / Hash calculator

Calculates the hash of string using various algorithms.

```
Rhiannon B. Langley|46872|fermentum@cursusnon.co.uk|9781
Nigel Ward|3584|convallis.erat.eget@luctusvulputatenisi.org|4896
Alvin Farley|69508|lectus@volutpat.co.uk|5358
Clark U. Pratt|23441|tincidunt.neque@nisl.co.uk|9273
Robin Randall|10108|faucibus.lectus.a@nonarcu.net|4232
Stacey L. Kirby|Y4B 8Z5|euismod.enim@mauris.org|4200
Joan Pearson|1867VB|convallis.erat@accumsannequeet.net|5002
Herman Lambert|09774|vitae.velit.egestas@tinciduntaliquamarcu.com|1220
Quentin Blankenship|48315-746|augue@consequat.edu|3387
```

Algorithm: md2

Result: 6c8fb699ac2ced0b5c9ea40aab9f8caf

Widzimy, że hash calculator wygenerował na kod.

Step 2: Download the suspected file to Sally’s PC.

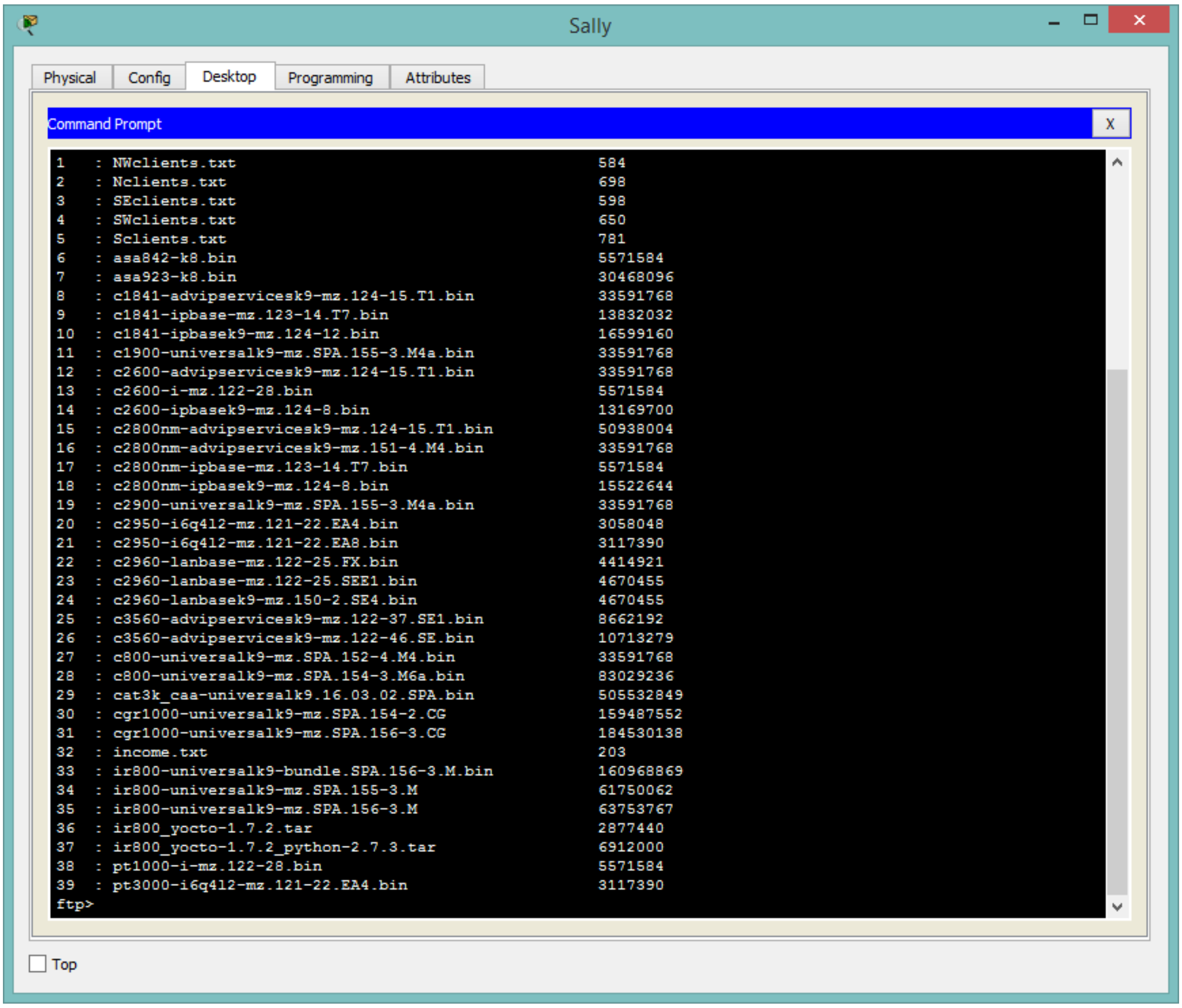
a. Click the **Metropolis Bank HQ** site, and then click the PC **Sally**.

b. Click the **Desktop** tab and then click **Command Prompt**.

c. Connect to the **Backup File** server by entering **ftp www.cisco2.corp** in the command prompt.

d. Enter the username of **sally** and a password of **cisco123**.

e. At the **ftp>** prompt, enter the command **dir** to view the current files stored on the remote FTP server.

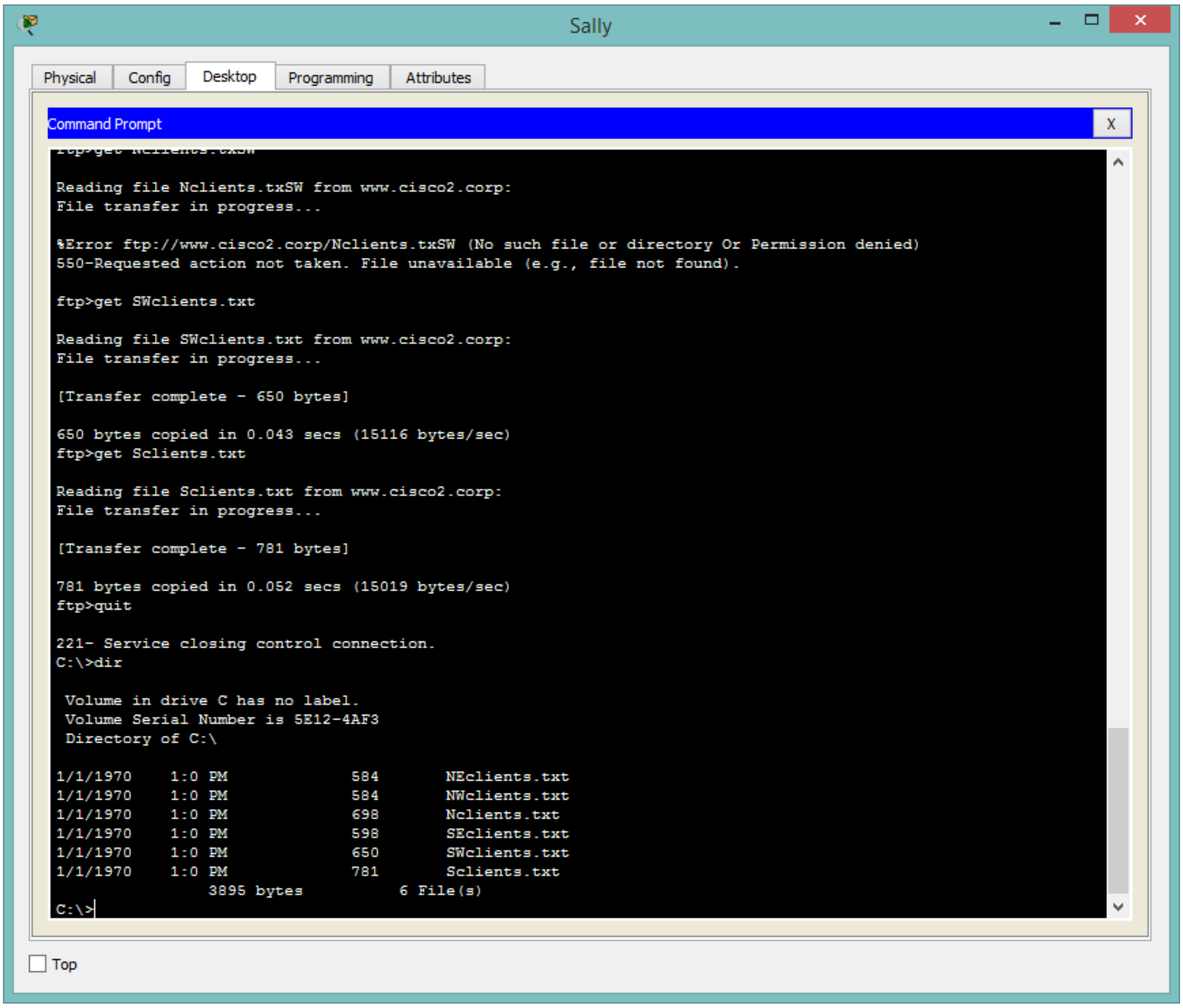


```
1    : NWclients.txt                                  584
2    : Nclients.txt                                   698
3    : SEclients.txt                                  598
4    : SWclients.txt                                  650
5    : Sclients.txt                                   781
6    : asa842-k8.bin                                  5571584
7    : asa923-k8.bin                                  30468096
8    : c1841-advipservicesk9-mz.124-15.T1.bin         33591768
9    : c1841-ipbase-mz.123-14.T7.bin                  13832032
10   : c1841-ipbasek9-mz.124-12.bin                   16599160
11   : c1900-universalk9-mz.SPA.155-3.M4a.bin         33591768
12   : c2600-advipservicesk9-mz.124-15.T1.bin         33591768
13   : c2600-i-mz.122-28.bin                          5571584
14   : c2600-ipbasek9-mz.124-8.bin                    13169700
15   : c2800nm-advipservicesk9-mz.124-15.T1.bin       50938004
16   : c2800nm-advipservicesk9-mz.151-4.M4.bin        33591768
17   : c2800nm-ipbase-mz.123-14.T7.bin                5571584
18   : c2800nm-ipbasek9-mz.124-8.bin                  15522644
19   : c2900-universalk9-mz.SPA.155-3.M4a.bin         33591768
20   : c2950-i6q4l2-mz.121-22.EA4.bin                 3058048
21   : c2950-i6q4l2-mz.121-22.EA8.bin                 3117390
22   : c2960-lanbase-mz.122-25.FX.bin                 4414921
23   : c2960-lanbase-mz.122-25.SEE1.bin               4670455
24   : c2960-lanbasek9-mz.150-2.SE4.bin               4670455
25   : c3560-advipservicesk9-mz.122-37.SE1.bin        8662192
26   : c3560-advipservicesk9-mz.122-46.SE.bin         10713279
27   : c800-universalk9-mz.SPA.152-4.M4.bin           33591768
28   : c800-universalk9-mz.SPA.154-3.M6a.bin          83029236
29   : cat3k_caa-universalk9.16.03.02.SPA.bin         505532849
30   : cgr1000-universalk9-mz.SPA.154-2.CG            159487552
31   : cgr1000-universalk9-mz.SPA.156-3.CG            184530138
32   : income.txt                                     203
33   : ir800-universalk9-bundle.SPA.156-3.M.bin       160968869
34   : ir800-universalk9-mz.SPA.155-3.M               61750062
35   : ir800-universalk9-mz.SPA.156-3.M               63753767
36   : ir800_yocto-1.7.2.tar                          2877440
37   : ir800_yocto-1.7.2_python-2.7.3.tar             6912000
38   : pt1000-i-mz.122-28.bin                         5571584
39   : pt3000-i6q4l2-mz.121-22.EA4.bin                3117390
ftp>
```

f. Download the file that was found to have been tampered with in Part 3 Step 1.

g. At the **ftp>** prompt, enter the command **quit**.

h. At the **PC>** prompt, enter the command **dir** and verify the tampered client file is now on Sally's PC for analysis at a later time.



```
ftp>get Nclients.txSW

Reading file Nclients.txSW from www.cisco2.corp:
File transfer in progress...

%Error ftp://www.cisco2.corp/Nclients.txSW (No such file or directory Or Permission denied)
550-Requested action not taken. File unavailable (e.g., file not found).

ftp>get SWclients.txt

Reading file SWclients.txt from www.cisco2.corp:
File transfer in progress...

[Transfer complete - 650 bytes]

650 bytes copied in 0.043 secs (15116 bytes/sec)
ftp>get Sclients.txt

Reading file Sclients.txt from www.cisco2.corp:
File transfer in progress...

[Transfer complete - 781 bytes]

781 bytes copied in 0.052 secs (15019 bytes/sec)
ftp>quit

221- Service closing control connection.
C:\>dir

 Volume in drive C has no label.
 Volume Serial Number is 5E12-4AF3
 Directory of C:\

1/1/1970    1:0 PM              584       NEclients.txt
1/1/1970    1:0 PM              584       NWclients.txt
1/1/1970    1:0 PM              698       Nclients.txt
1/1/1970    1:0 PM              598       SEclients.txt
1/1/1970    1:0 PM              650       SWclients.txt
1/1/1970    1:0 PM              781       Sclients.txt
                3895 bytes          6 File(s)
C:\>
```

Na komputerze Sally są już wszystkie pliki ściągnięte z serwera FTP.

Part 4: Verify the Integrity of Critical Files using HMAC

Step 1: Compute the HMAC of a critical file.

a. Within the **Metropolis Bank HQ** site, click the PC **Bob**.

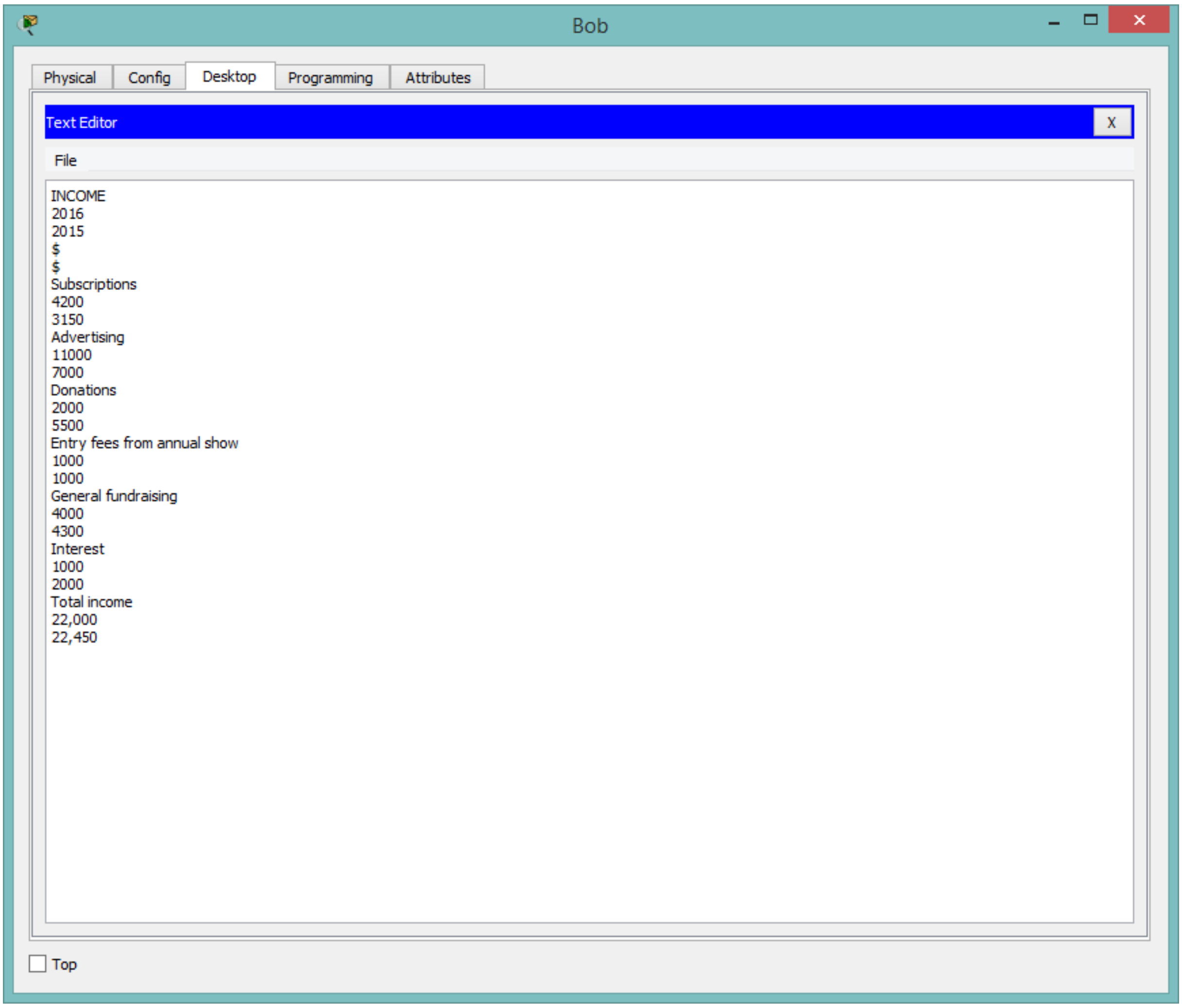
b. Click the **Desktop** tab and then click **Command Prompt**.

c. At the **PC>** prompt, enter the command **dir** and verify the critical file named **income.txt** is on Bob's PC.

d. Within the **Desktop** tab, click **Text Editor**.

e. In the Text Editor window, click **File** > **Open**.

f. Click the document **income.txt** and click **OK**.



```
INCOME
2016
2015
$
$
Subscriptions
4200
3150
Advertising
11000
7000
Donations
2000
5500
Entry fees from annual show
1000
1000
General fundraising
4000
4300
Interest
1000
2000
Total income
22,000
22,450
```

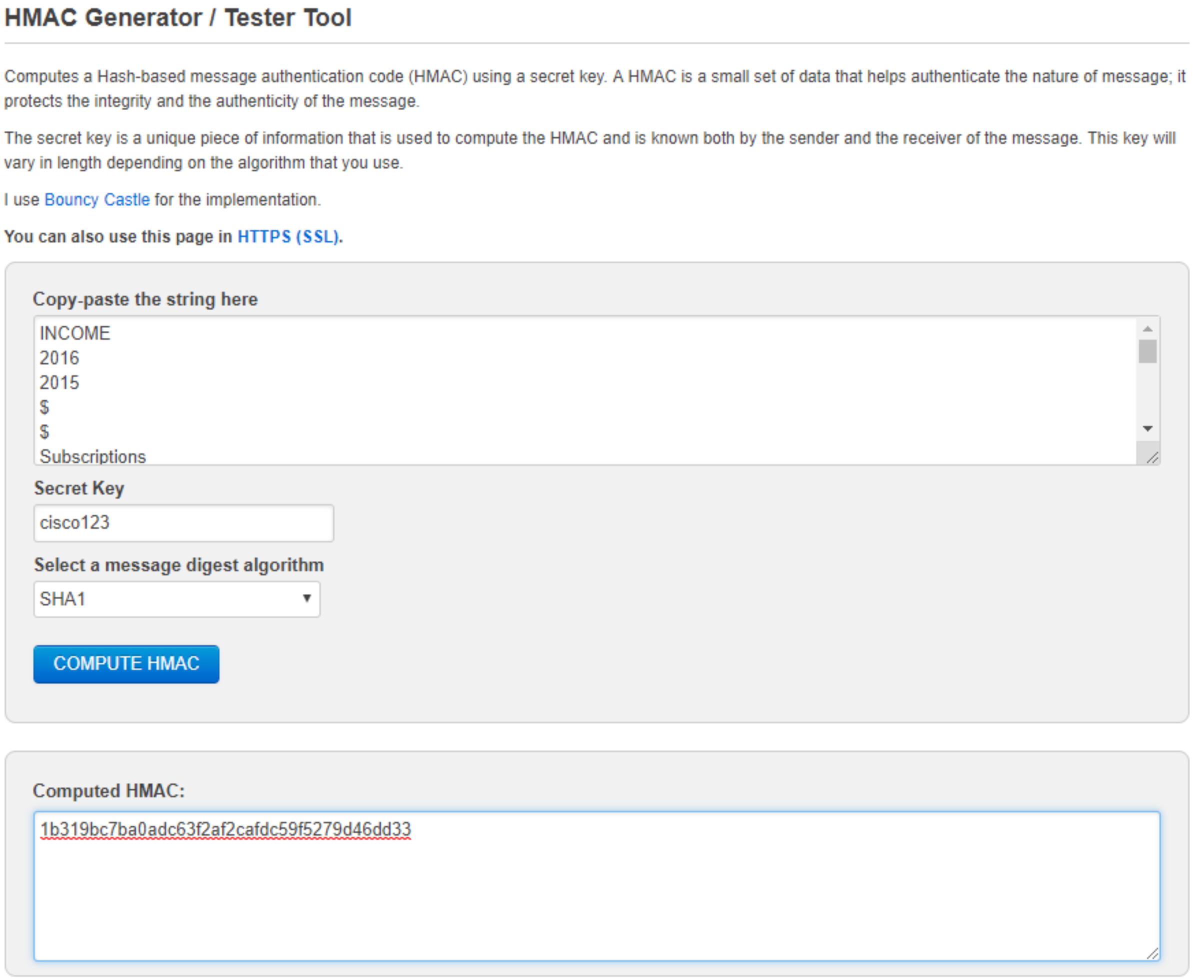
g. Copy the entire text document contents.

h. Open a web browser on your personal computer and browse to the website http://www.freeformatter.com/hmac-generator.html

i. Click the whitespace and paste in the text document contents. Enter the secret key of **cisco123**. Make sure the algorithm is set to **SHA1**. Click **Compute HMAC**.

What is the computed HMAC for the contents of the file?

How is using HMAC more secure than general hashing?



HMAC Generator / Tester Tool

Computes a Hash-based message authentication code (HMAC) using a secret key. A HMAC is a small set of data that helps authenticate the nature of message; it protects the integrity and the authenticity of the message.

The secret key is a unique piece of information that is used to compute the HMAC and is known both by the sender and the receiver of the message. This key will vary in length depending on the algorithm that you use.

I use Bouncy Castle for the implementation.

You can also use this page in HTTPS (SSL).

Copy-paste the string here

```
INCOME
2016
2015
$
$
Subscriptions
```

Secret Key: cisco123

Select a message digest algorithm: SHA1

Computed HMAC:

```
1b319bc7ba0adc63f2af2cafdc59f5279d46dd33
```

Jest to dużo bezpieczniejsze hashowanie ze względu na to iż aby odszyfrować plik trzeba podać hasło, które utworzyliśmy podczas jego hashowania.

Step 2: Verify the computed HMAC.

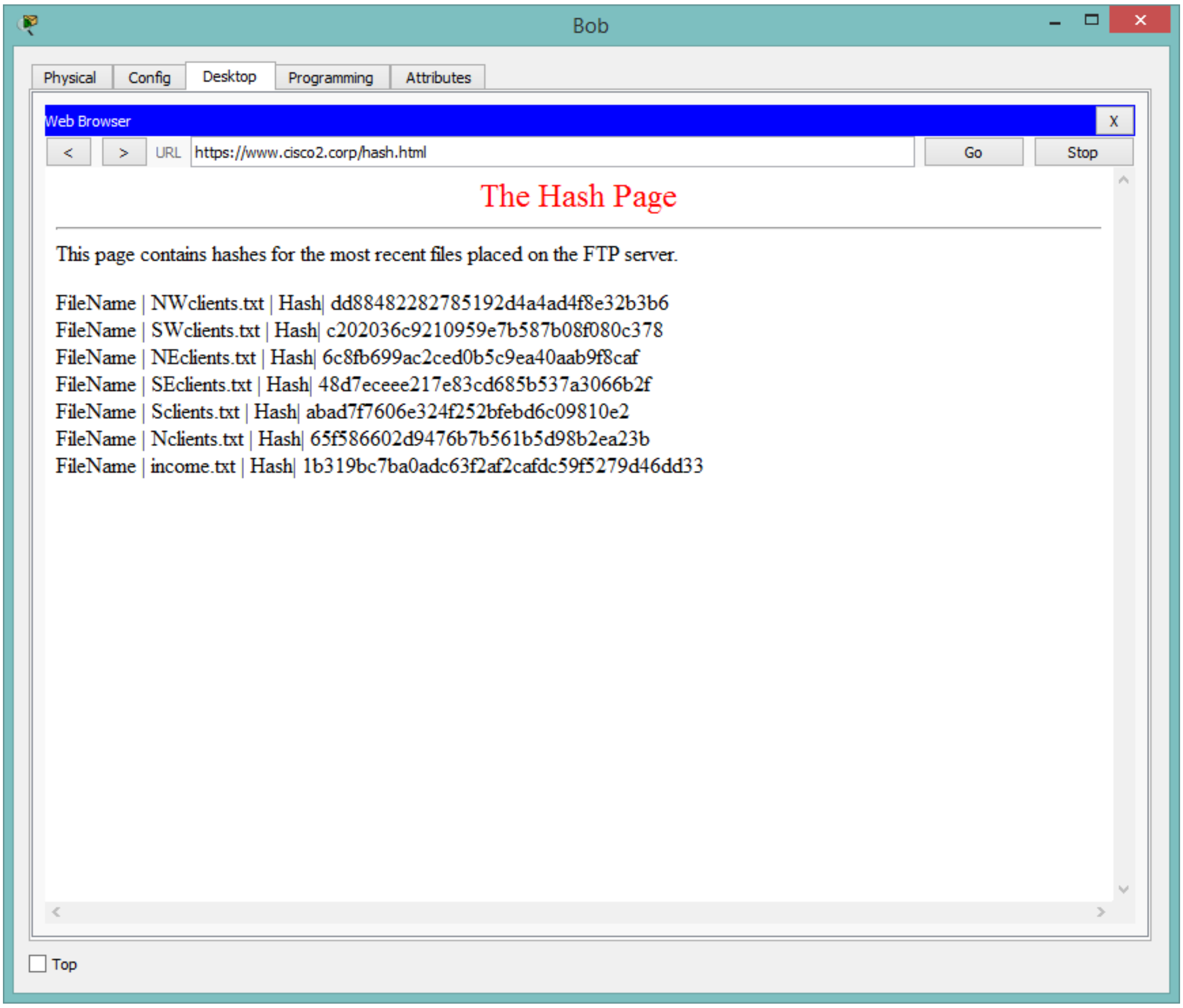
a. Within the **Metropolis Bank HQ** site, click the PC **Bob**.

b. Click the **Desktop** tab and then click **Web Browser**.

c. Enter the URL **https://www.cisco2.corp** and click **Go**.

d. Click on the link to view the most recent files and their hashes.

Does the HMAC hash for the income.txt file match?



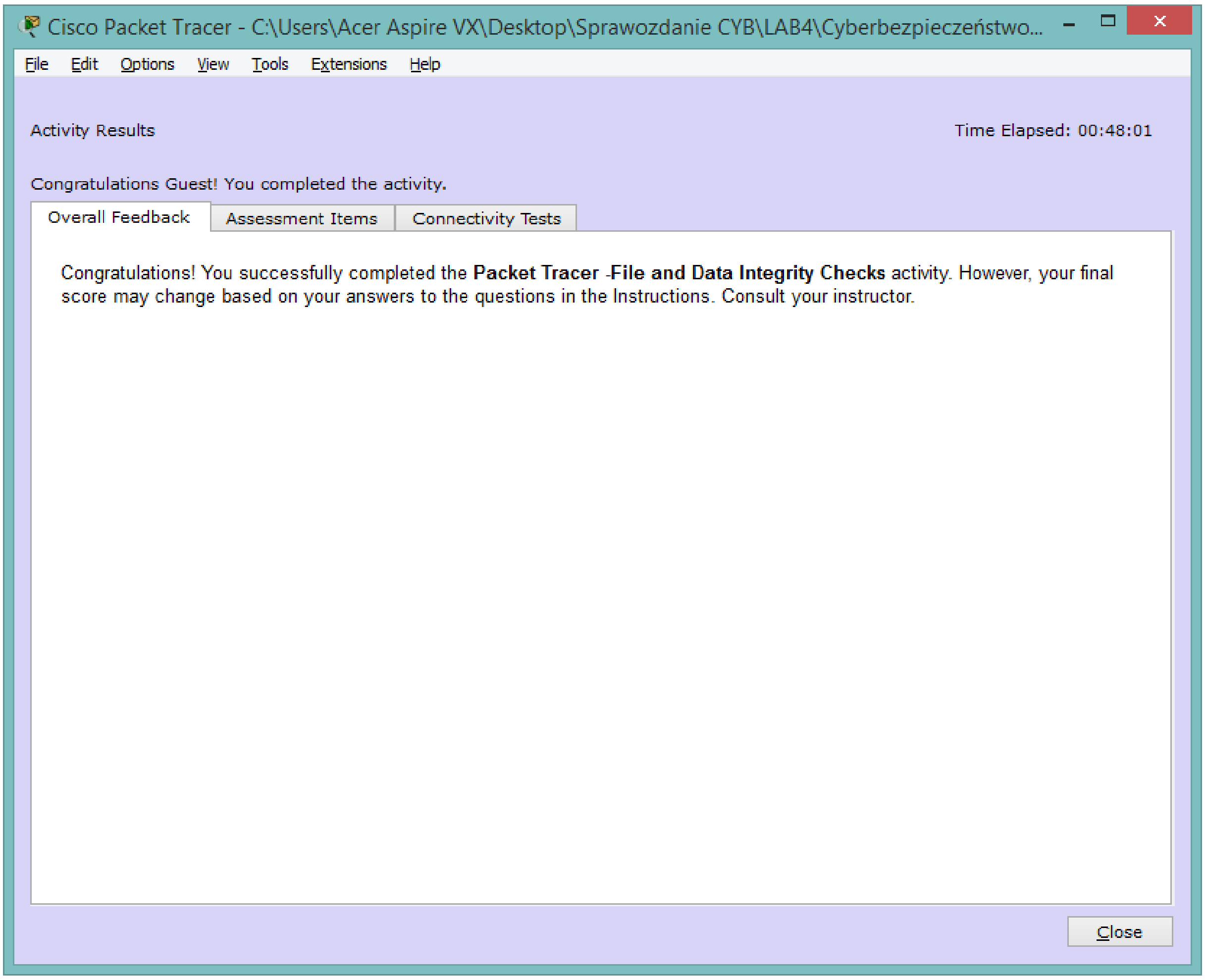
https://www.cisco2.corp/hash.html

The Hash Page

This page contains hashes for the most recent files placed on the FTP server.

```
FileName | NWclients.txt | Hash| dd88482282785192d4a4ad4f8e32b3b6
FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378
FileName | NEclients.txt | Hash| 6c8fb699ac2ced0b5c9ea40aab9f8caf
FileName | SEclients.txt | Hash| 48d7eceee217e83cd685b537a3066b2f
FileName | Sclients.txt | Hash| abad7f7606e324f252bfebd6c09810e2
FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b
FileName | income.txt | Hash| 1b319bc7ba0adc63f2af2cafdc59f5279d46dd33
```

HMAC który utworzyliśmy jest zgodny z tym na stronie.



Cisco Packet Tracer - C:\Users\Acer Aspire VX\Desktop\Sprawozdanie CYB\LAB4\Cyberbezpieczeństwo...
File Edit Options View Tools Extensions Help
Overall Feedback
Assessment Items
Connectivity Tests
Close

Activity Results

Time Elapsed: 00:48:01

Congratulations Guest! You completed the activity.

Congratulations! You successfully completed the **Packet Tracer -File and Data Integrity Checks** activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Wszystkie zadania zostały wykonane poprawnie.