Assignment 3
CPSC 526 Fall 2017
October 29, 2017

Mason Lieu
ID: 10110089
Tutorial 04
mlieu@ucalgary.ca

Shane Sims
ID: 00300601
Tutorial 04
shane.sims@ucalgary.ca

Contents

1 How to monitor HTTP

Terminal 1: Run the proxy server

```
python3 simpleProxyServer.py [log options] <source port> <web server URL> <destination port>
```

Web browser: Connect to the server

```
localhost:<source port>
```

2   How to monitor SSH

Terminal 1: Run the proxy server

```
python3 simpleProxyServer.py [log options] <source port> localhost 22
```

Terminal 2: Connect to the server through SSH

```
ssh localhost -p 22
```

3   How to monitor NetCat-to-NetCat

Terminal 1: Run NetCat to listen for incoming connections

```
nc -l <destination port>
```

Terminal 2: Run the proxy server

```
python3 simpleProxyServer.py [log options] <source port> localhost <destination port>
```

Terminal 3: Run NetCat

```
nc localhost <source port>
```

4   How to monitor backdoor server from Assignment 2

Terminal 1: Run backdoor server

```
python3 backdoor_server.py <destination port>
```

Terminal 2: Run the proxy server

```
python3 simpleProxyServer.py [log options] <source port> localhost <destination port>
```

Terminal 3: Run NetCat
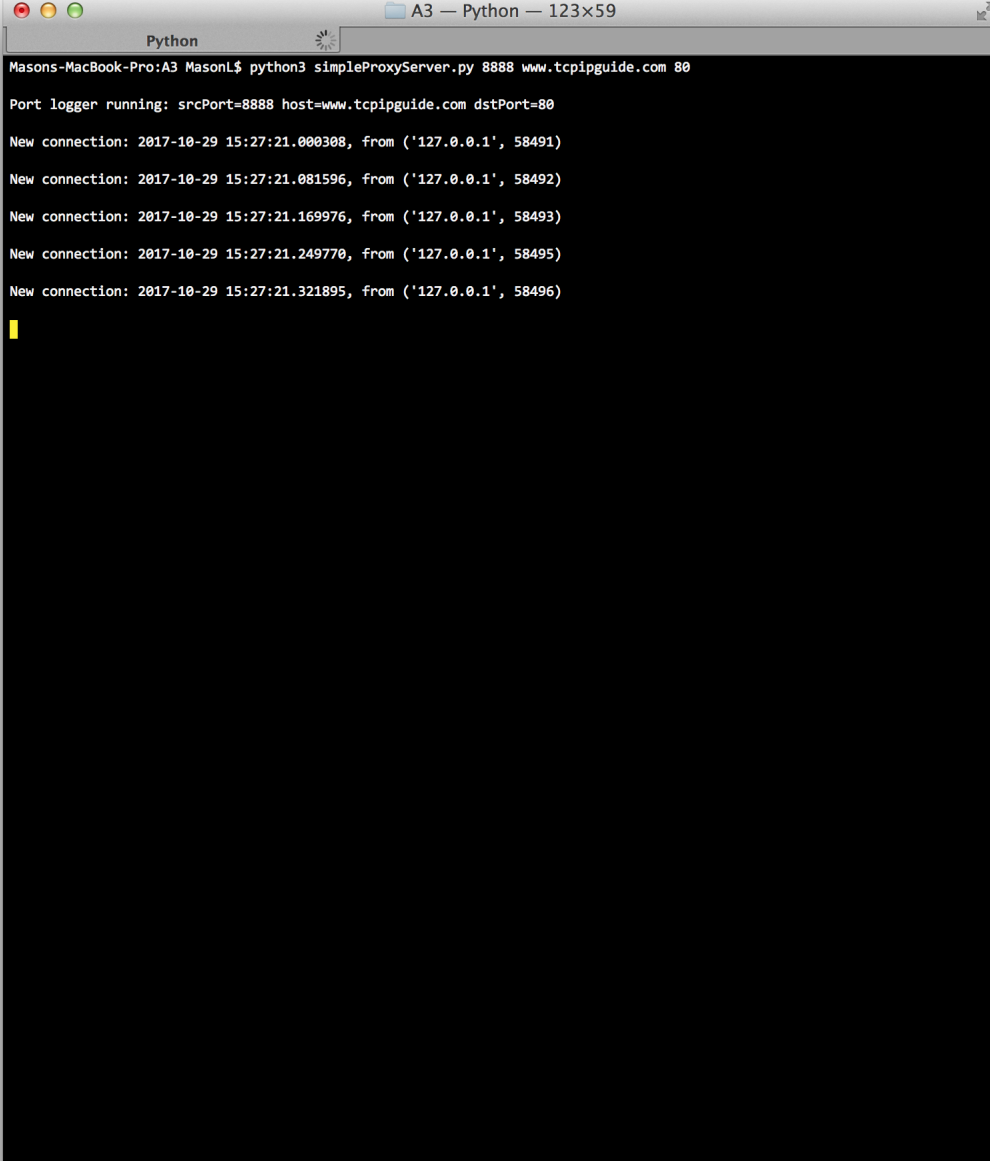
```
nc localhost <source port>
```

5   Supported logging formats

This program supports the following logging formats

1. -raw

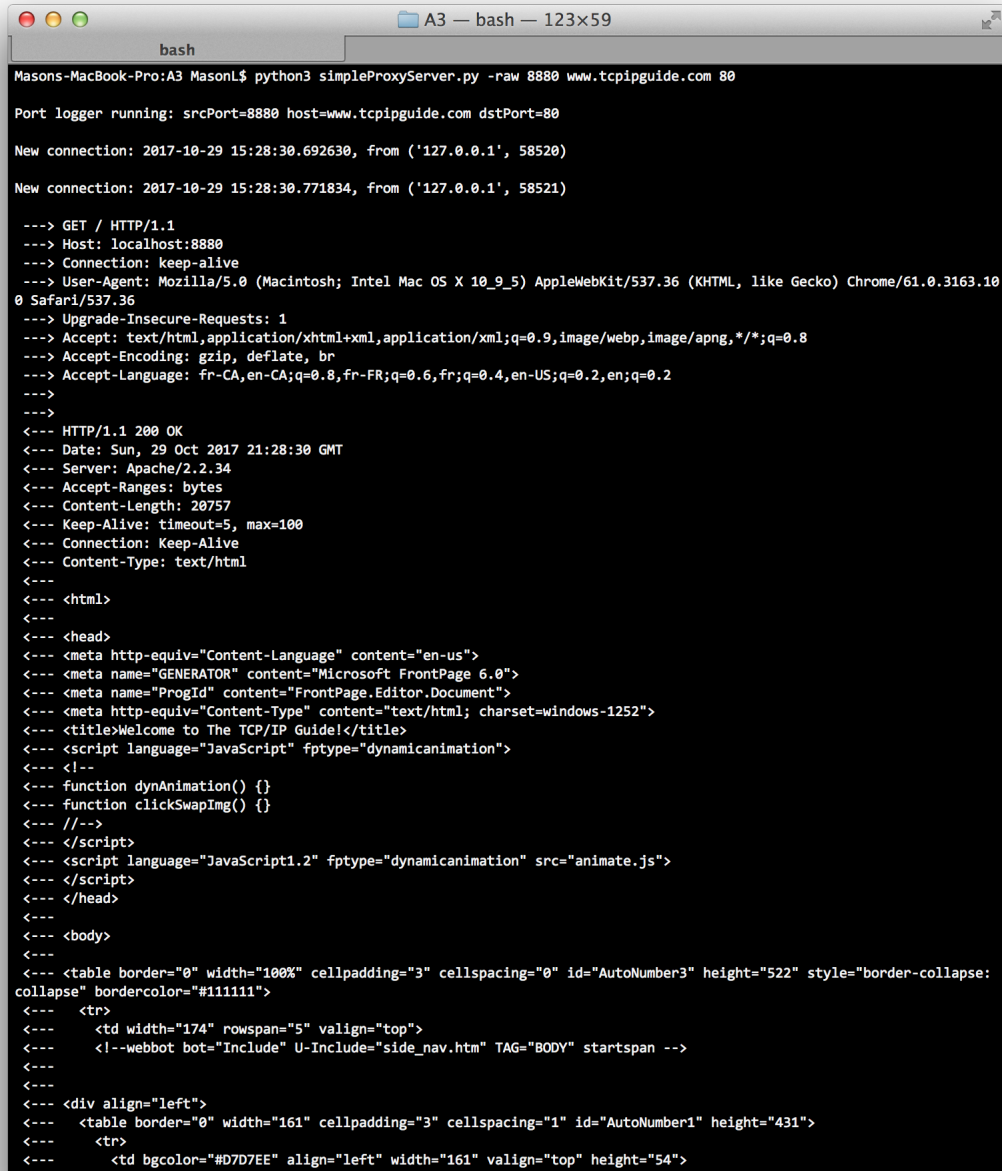2. -strip

3. -hex

4. -autoN

5. -replace

6 Sample output

6.1 Output - no logging

Figure 1: No logging options selected

6.2   Output - raw

```
●●●                        📁 A3 — bash — 123×59
         bash
Masons-MacBook-Pro:A3 MasonL$ python3 simpleProxyServer.py -raw 8880 www.tcpipguide.com 80

Port logger running: srcPort=8880 host=www.tcpipguide.com dstPort=80

New connection: 2017-10-29 15:28:30.692630, from ('127.0.0.1', 58520)

New connection: 2017-10-29 15:28:30.771834, from ('127.0.0.1', 58521)

 ---> GET / HTTP/1.1
 ---> Host: localhost:8880
 ---> Connection: keep-alive
 ---> User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.10
0 Safari/537.36
 ---> Upgrade-Insecure-Requests: 1
 ---> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
 ---> Accept-Encoding: gzip, deflate, br
 ---> Accept-Language: fr-CA,en-CA;q=0.8,fr-FR;q=0.6,fr;q=0.4,en-US;q=0.2,en;q=0.2
 --->
 --->
<--- HTTP/1.1 200 OK
<--- Date: Sun, 29 Oct 2017 21:28:30 GMT
<--- Server: Apache/2.2.34
<--- Accept-Ranges: bytes
<--- Content-Length: 20757
<--- Keep-Alive: timeout=5, max=100
<--- Connection: Keep-Alive
<--- Content-Type: text/html
<---
<--- <html>
<---
<--- <head>
<--- <meta http-equiv="Content-Language" content="en-us">
<--- <meta name="GENERATOR" content="Microsoft FrontPage 6.0">
<--- <meta name="ProgId" content="FrontPage.Editor.Document">
<--- <meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<--- <title>Welcome to The TCP/IP Guide!</title>
<--- <script language="JavaScript" fptype="dynamicanimation">
<--- <!--
<--- function dynAnimation() {}
<--- function clickSwapImg() {}
<--- //-->
<--- </script>
<--- <script language="JavaScript1.2" fptype="dynamicanimation" src="animate.js">
<--- </script>
<--- </head>
<---
<--- <body>
<---
<--- <table border="0" width="100%" cellpadding="3" cellspacing="0" id="AutoNumber3" height="522" style="border-collapse:
collapse" bordercolor="#111111">
<---   <tr>
<---     <td width="174" rowspan="5" valign="top">
<---       <!--webbot bot="Include" U-Include="side_nav.htm" TAG="BODY" startspan -->
<---
<---
<--- <div align="left">
<---   <table border="0" width="161" cellpadding="3" cellspacing="1" id="AutoNumber1" height="431">
<---     <tr>
<---       <td bgcolor="#D7D7EE" align="left" width="161" valign="top" height="54">
```
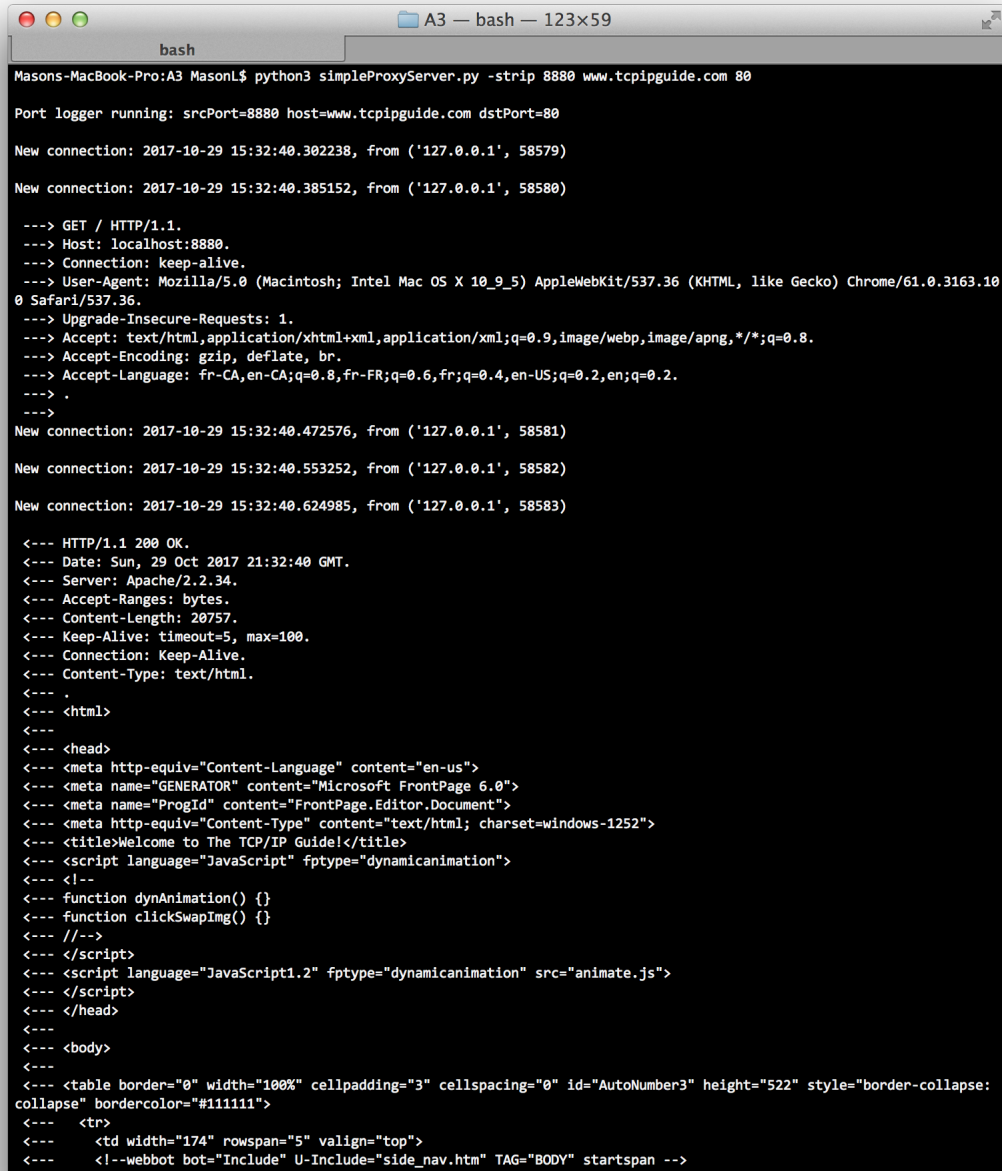
Figure 2: Initialization of proxy server with raw formatting

Figure 3: Sample output in the middle of execution

6.3 Output - strip

```
● ● ●                        📁 A3 — bash — 123×59
              bash
Masons-MacBook-Pro:A3 MasonL$ python3 simpleProxyServer.py -strip 8880 www.tcpipguide.com 80

Port logger running: srcPort=8880 host=www.tcpipguide.com dstPort=80

New connection: 2017-10-29 15:32:40.302238, from ('127.0.0.1', 58579)

New connection: 2017-10-29 15:32:40.385152, from ('127.0.0.1', 58580)

 ---> GET / HTTP/1.1.
 ---> Host: localhost:8880.
 ---> Connection: keep-alive.
 ---> User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.10
0 Safari/537.36.
 ---> Upgrade-Insecure-Requests: 1.
 ---> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8.
 ---> Accept-Encoding: gzip, deflate, br.
 ---> Accept-Language: fr-CA,en-CA;q=0.8,fr-FR;q=0.6,fr;q=0.4,en-US;q=0.2,en;q=0.2.
 ---> .
 --->
New connection: 2017-10-29 15:32:40.472576, from ('127.0.0.1', 58581)

New connection: 2017-10-29 15:32:40.553252, from ('127.0.0.1', 58582)

New connection: 2017-10-29 15:32:40.624985, from ('127.0.0.1', 58583)

 <--- HTTP/1.1 200 OK.
 <--- Date: Sun, 29 Oct 2017 21:32:40 GMT.
 <--- Server: Apache/2.2.34.
 <--- Accept-Ranges: bytes.
 <--- Content-Length: 20757.
 <--- Keep-Alive: timeout=5, max=100.
 <--- Connection: Keep-Alive.
 <--- Content-Type: text/html.
 <--- .
 <--- <html>
 <---
 <--- <head>
 <--- <meta http-equiv="Content-Language" content="en-us">
 <--- <meta name="GENERATOR" content="Microsoft FrontPage 6.0">
 <--- <meta name="ProgId" content="FrontPage.Editor.Document">
 <--- <meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
 <--- <title>Welcome to The TCP/IP Guide!</title>
 <--- <script language="JavaScript" fptype="dynamicanimation">
 <--- <!--
 <--- function dynAnimation() {}
 <--- function clickSwapImg() {}
 <--- //-->
 <--- </script>
 <--- <script language="JavaScript1.2" fptype="dynamicanimation" src="animate.js">
 <--- </script>
 <--- </head>
 <---
 <--- <body>
 <---
 <--- <table border="0" width="100%" cellpadding="3" cellspacing="0" id="AutoNumber3" height="522" style="border-collapse:
collapse" bordercolor="#111111">
 <---   <tr>
 <---     <td width="174" rowspan="5" valign="top">
 <---       <!--webbot bot="Include" U-Include="side_nav.htm" TAG="BODY" startspan -->
```

Figure 4: Initialization of proxy server with strip formatting

```
<--- </p>
<--- <!--webbot bot="Include" i-checksum="38707" endspan --></td>
<---    </tr>
<--- </table>
<---
<--- </body>
<---
<--- </html>
---> GET /images/features/btn_featuresdown.gif HTTP/1.1.
---> Host: localhost:8888.
---> Connection: keep-alive.
---> User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.10
0 Safari/537.36.
---> Accept: image/webp,image/apng,image/*,*/*;q=0.8.
---> Referer: http://localhost:8888/news.htm.
---> Accept-Encoding: gzip, deflate, br.
---> Accept-Language: fr-CA,en-CA;q=0.8,fr-FR;q=0.6,fr;q=0.4,en-US;q=0.2,en;q=0.2.
---> .
--->
<--- HTTP/1.1 200 OK.
<--- Date: Sun, 29 Oct 2017 21:33:55 GMT.
<--- Server: Apache/2.2.34.
<--- Last-Modified: Fri, 19 Dec 2003 20:20:46 GMT.
<--- ETag: "34b-3cedb133c2380".
<--- Accept-Ranges: bytes.
<--- Content-Length: 843.
<--- Keep-Alive: timeout=5, max=93.
<--- Connection: Keep-Alive.
<--- Content-Type: image/gif.
<--- .
<---
<--- GIF89a................................................................................................
................w....|t.og{aZlSM\E@M73=)&.................................!.......,..........@.A......r.l:..
.tJ......X.z....Y``...x.n....dSQ...~.............. ....................
<--- .. ..........
<--- ...................!t..............
<--- ...............!..............3.3+.+)......./-D...KD.Y.DX....3..,(....8w..5D.C..X...P.b.
<--- ..Q*p......g|T.".K....+....../^(.aBA....*X1..F.O7..aB...GSth....,.....
<--- .[...Q....N.F..4mP..d..J..X.}k=U ....".`a.d..P.:,|.1..0......fY.#...+Ba.&......,..K...!.R.B?...SwdY,d.U.....L_.H...o
X.a./.b.Q..xc..xV..E...]z9..+.....<,....n..}........{.E..@....h...&....6....F(!..Hp..#|.A..t.h.. .(..$.h..(....'V...%.....d
`..8....<....@.)..D....'.P..L6...PF)..TVi..Xf.%.%....`.)..d.i..h....l....A..;
---> GET /features.htm HTTP/1.1.
---> Host: localhost:8888.
---> Connection: keep-alive.
---> Upgrade-Insecure-Requests: 1.
---> User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.10
0 Safari/537.36.
---> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8.
---> Referer: http://localhost:8888/news.htm.
---> Accept-Encoding: gzip, deflate, br.
---> Accept-Language: fr-CA,en-CA;q=0.8,fr-FR;q=0.6,fr;q=0.4,en-US;q=0.2,en;q=0.2.
---> .
--->
<--- HTTP/1.1 200 OK.
<--- Date: Sun, 29 Oct 2017 21:34:00 GMT.
<--- Server: Apache/2.2.34.
<--- Accept-Ranges: bytes.
<--- Content-Length: 16046.
<--- Keep-Alive: timeout=5, max=92.
```

Figure 5: Sample output in the middle of execution

6.4 Output - hex

Figure 6: Initialization of proxy server with hex formatting

6.5 Output - autoN
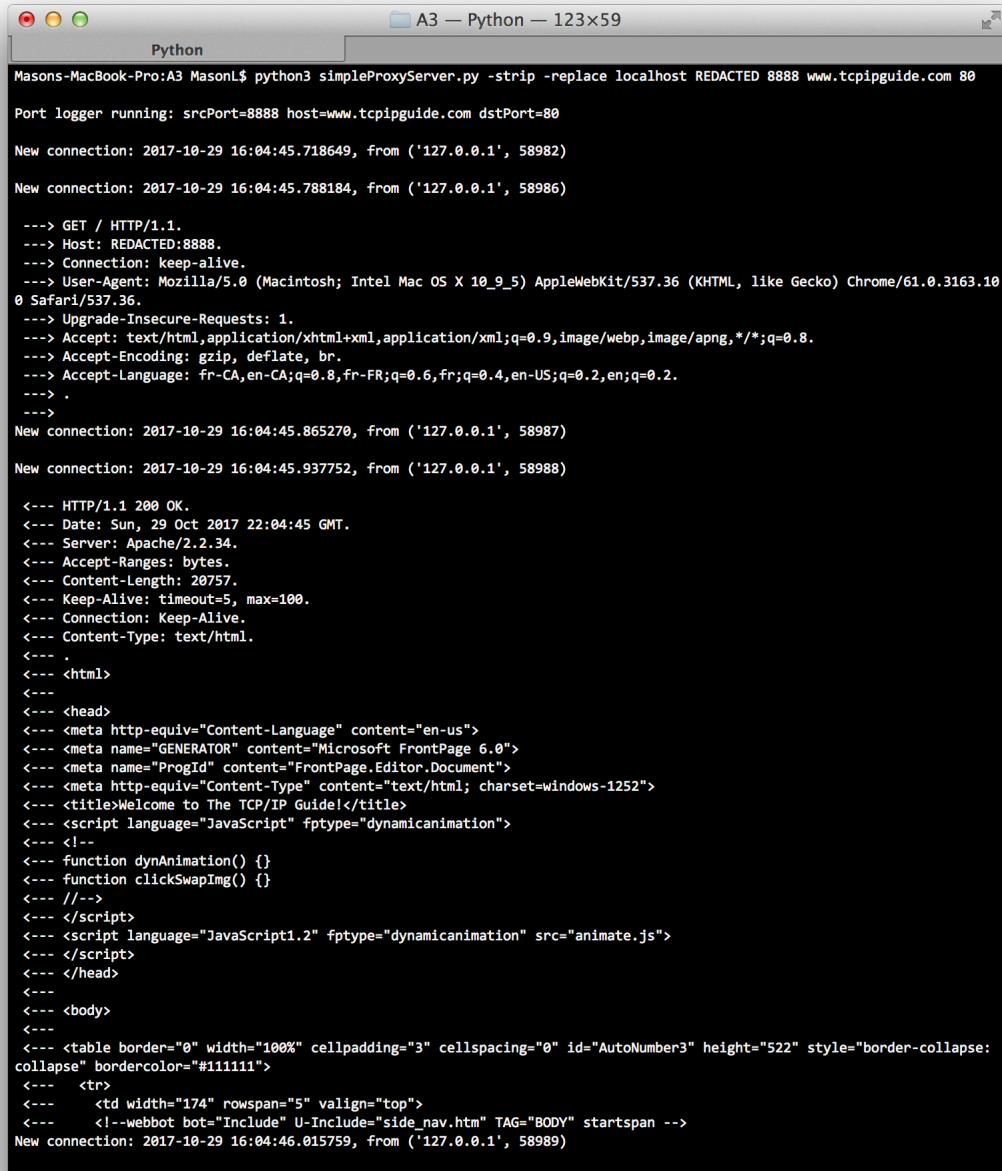

```
● ● ●                          A3 — bash — 123×59
           bash
Masons-MacBook-Pro:A3 MasonL$ python3 simpleProxyServer.py -autoN 30 8888 www.tcpipguide.com 80

Port logger running: srcPort=8888 host=www.tcpipguide.com dstPort=80

New connection: 2017-10-29 15:39:15.871428, from ('127.0.0.1', 58646)

New connection: 2017-10-29 15:39:15.953720, from ('127.0.0.1', 58647)

  ---> GET / HTTP/1.1\r\nHost: localhos
  ---> t:8888\r\nConnection: keep-alive
  ---> \r\nUser-Agent: Mozilla/5.0 (Mac
  ---> intosh; Intel Mac OS X 10_9_5)
  --->  AppleWebKit/537.36 (KHTML, li
  ---> ke Gecko) Chrome/61.0.3163.100
  --->  Safari/537.36\r\nUpgrade-Insecu
  ---> re-Requests: 1\r\nAccept: text/h
  ---> tml,application/xhtml+xml,appl
  ---> ication/xml;q=0.9,image/webp,i
  ---> mage/apng,*/*;q=0.8\r\nAccept-En
  ---> coding: gzip, deflate, br\r\nAcc
  ---> ept-Language: fr-CA,en-CA;q=0.
  ---> 8,fr-FR;q=0.6,fr;q=0.4,en-US;q
  ---> =0.2,en;q=0.2\r\n\r\n
New connection: 2017-10-29 15:39:16.041709, from ('127.0.0.1', 58648)

New connection: 2017-10-29 15:39:16.123697, from ('127.0.0.1', 58650)

New connection: 2017-10-29 15:39:16.201673, from ('127.0.0.1', 58651)

  <--- HTTP/1.1 200 OK\r\nDate: Sun, 29
  <---  Oct 2017 21:39:15 GMT\r\nServer
  <--- : Apache/2.2.34\r\nAccept-Ranges
  <--- : bytes\r\nContent-Length: 20757
  <--- \r\nKeep-Alive: timeout=5, max=1
  <--- 00\r\nConnection: Keep-Alive\r\nCo
  <--- ntent-Type: text/html\r\n\r\n<html
  <--- >\n\n<head>\n<meta http-equiv="Co
  <--- ntent-Language" content="en-us
  <--- ">\n<meta name="GENERATOR" cont
  <--- ent="Microsoft FrontPage 6.0">
  <--- \n<meta name="ProgId" content="
  <--- FrontPage.Editor.Document">\n<m
  <--- eta http-equiv="Content-Type"
  <--- content="text/html; charset=wi
  <--- ndows-1252">\n<title>Welcome to
  <---  The TCP/IP Guide!</title>\n<sc
  <--- ript language="JavaScript" fpt
  <--- ype="dynamicanimation">\n<!--\nf
  <--- unction dynAnimation() {}\nfunc
  <--- tion clickSwapImg() {}\n//-->\n<
  <--- /script>\n<script language="Jav
  <--- aScript1.2" fptype="dynamicani
  <--- mation" src="animate.js">\n</sc
  <--- ript>\n</head>\n\n<body>\n\n<table
  <--- border="0" width="100%" cellpa
  <--- dding="3" cellspacing="0" id="
  <--- AutoNumber3" height="522" styl
  <--- e="border-collapse: collapse"
  <--- bordercolor="#111111">\n  <tr>\n
```

Figure 7: Initialization of proxy server with autoN formatting where n = 30

6.6   Output - replace

Figure 8: Initialization of proxy server with replace formatting. All instances of 'localhost' replaced with '**REDACTED**'

6.7 Output - netcat-to-netcat communication
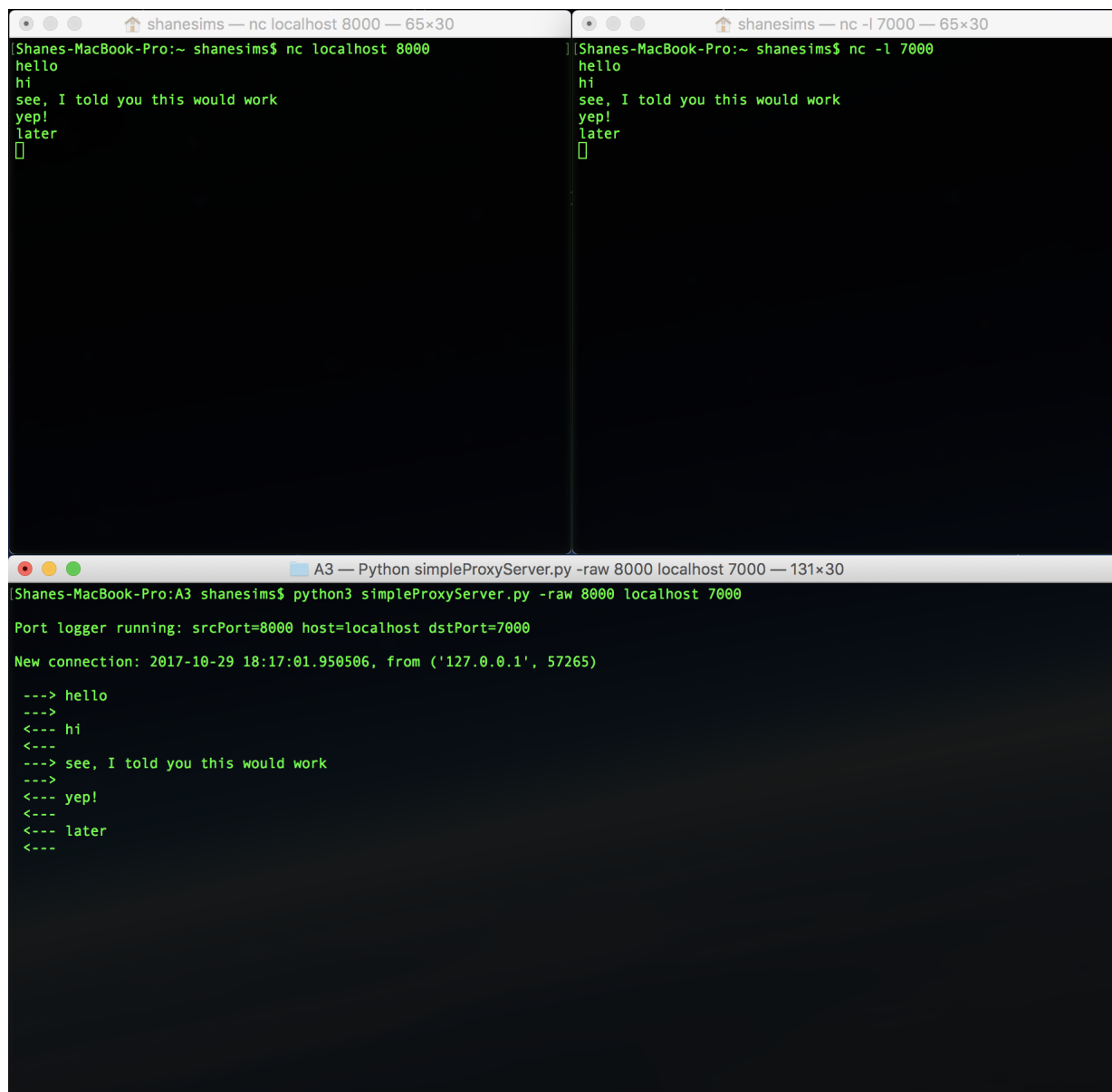

Figure 9: Initialization of proxy (bottom), netcat server (top-right), and netcat client (top-left)

Figure 10: Sample output in the middle of execution