Rukiya Hassan
10140484
Tutorial 03
Partner: Chintav Shah

How to run and connect program:

On one terminal

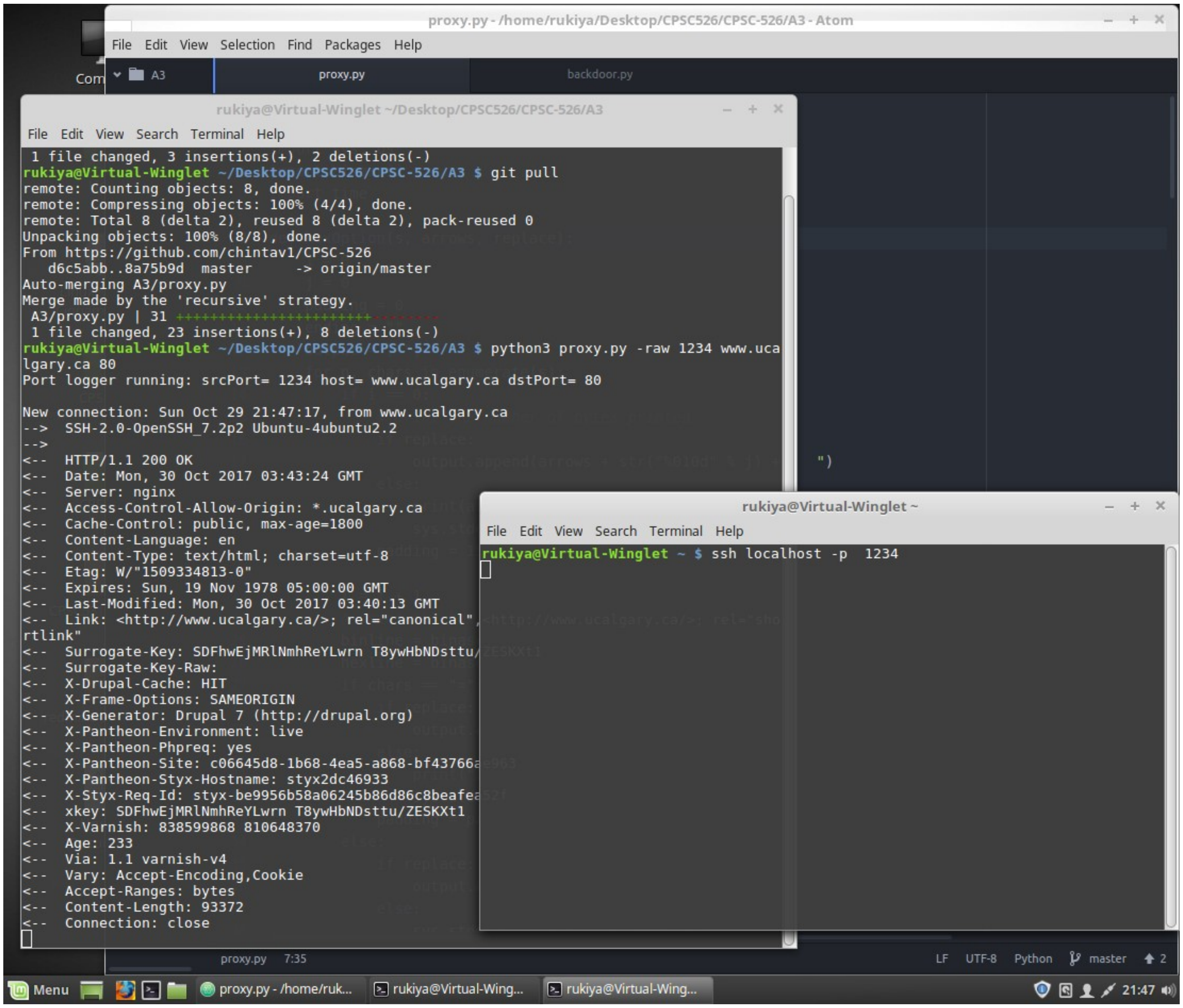
```
python3 proxy.py [logOptions] [replaceOptions] srcPort server dstPort
```

May connect using http, ssh, or nc

Samples in next pages:

Sample outputs:

-raw using ssh

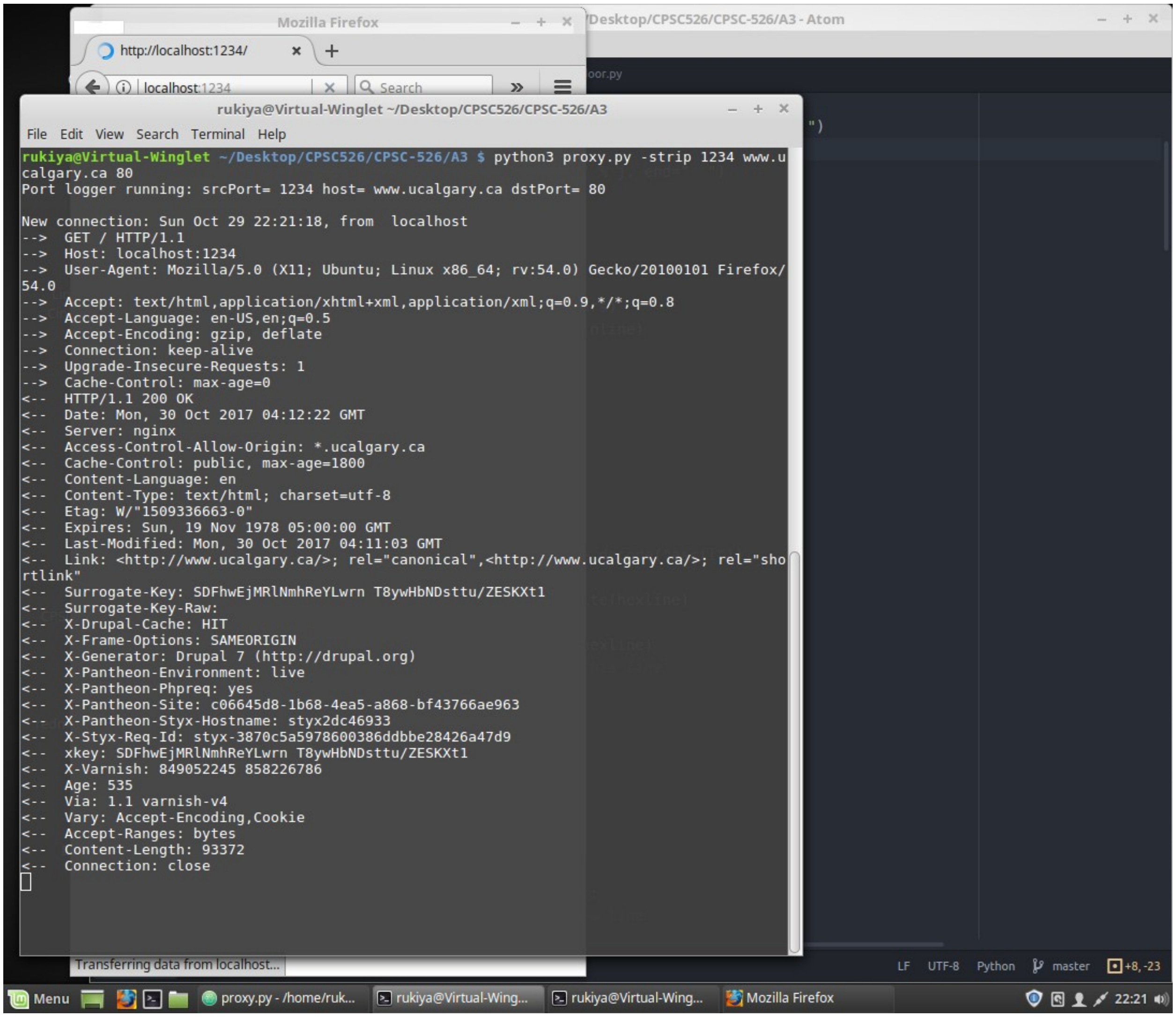


proxy.py - /home/rukiya/Desktop/CPSC526/CPSC-526/A3 - Atom
File Edit View Selection Find Packages Help
A3
proxy.py
backdoor.py
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3
File Edit View Search Terminal Help
rukiya@Virtual-Winglet ~
File Edit View Search Terminal Help
proxy.py 7:35
LF UTF-8 Python master 2
Menu
proxy.py - /home/ruk...
rukiya@Virtual-Wing...
rukiya@Virtual-Wing...
21:47

```
 1 file changed, 3 insertions(+), 2 deletions(-)
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3 $ git pull
remote: Counting objects: 8, done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 8 (delta 2), reused 8 (delta 2), pack-reused 0
Unpacking objects: 100% (8/8), done.
From https://github.com/chintav1/CPSC-526
   d6c5abb..8a75b9d  master     -> origin/master
Auto-merging A3/proxy.py
Merge made by the 'recursive' strategy.
 A3/proxy.py | 31 +++++++++++++++++++++++--------
 1 file changed, 23 insertions(+), 8 deletions(-)
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3 $ python3 proxy.py -raw 1234 www.uca
lgary.ca 80
Port logger running: srcPort= 1234 host= www.ucalgary.ca dstPort= 80

New connection: Sun Oct 29 21:47:17, from www.ucalgary.ca
-->  SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
-->
<--  HTTP/1.1 200 OK
<--  Date: Mon, 30 Oct 2017 03:43:24 GMT
<--  Server: nginx
<--  Access-Control-Allow-Origin: *.ucalgary.ca
<--  Cache-Control: public, max-age=1800
<--  Content-Language: en
<--  Content-Type: text/html; charset=utf-8
<--  Etag: W/"1509334813-0"
<--  Expires: Sun, 19 Nov 1978 05:00:00 GMT
<--  Last-Modified: Mon, 30 Oct 2017 03:40:13 GMT
<--  Link: <http://www.ucalgary.ca/>; rel="canonical",<http://www.ucalgary.ca/>; rel="sho
rtlink"
<--  Surrogate-Key: SDFhwEjMRlNmhReYLwrn T8ywHbNDsttu/ZESKXt1
<--  Surrogate-Key-Raw:
<--  X-Drupal-Cache: HIT
<--  X-Frame-Options: SAMEORIGIN
<--  X-Generator: Drupal 7 (http://drupal.org)
<--  X-Pantheon-Environment: live
<--  X-Pantheon-Phpreq: yes
<--  X-Pantheon-Site: c06645d8-1b68-4ea5-a868-bf43766ae963
<--  X-Pantheon-Styx-Hostname: styx2dc46933
<--  X-Styx-Req-Id: styx-be9956b58a06245b86d86c8beafea52f
<--  xkey: SDFhwEjMRlNmhReYLwrn T8ywHbNDsttu/ZESKXt1
<--  X-Varnish: 838599868 810648370
<--  Age: 233
<--  Via: 1.1 varnish-v4
<--  Vary: Accept-Encoding,Cookie
<--  Accept-Ranges: bytes
<--  Content-Length: 93372
<--  Connection: close
```

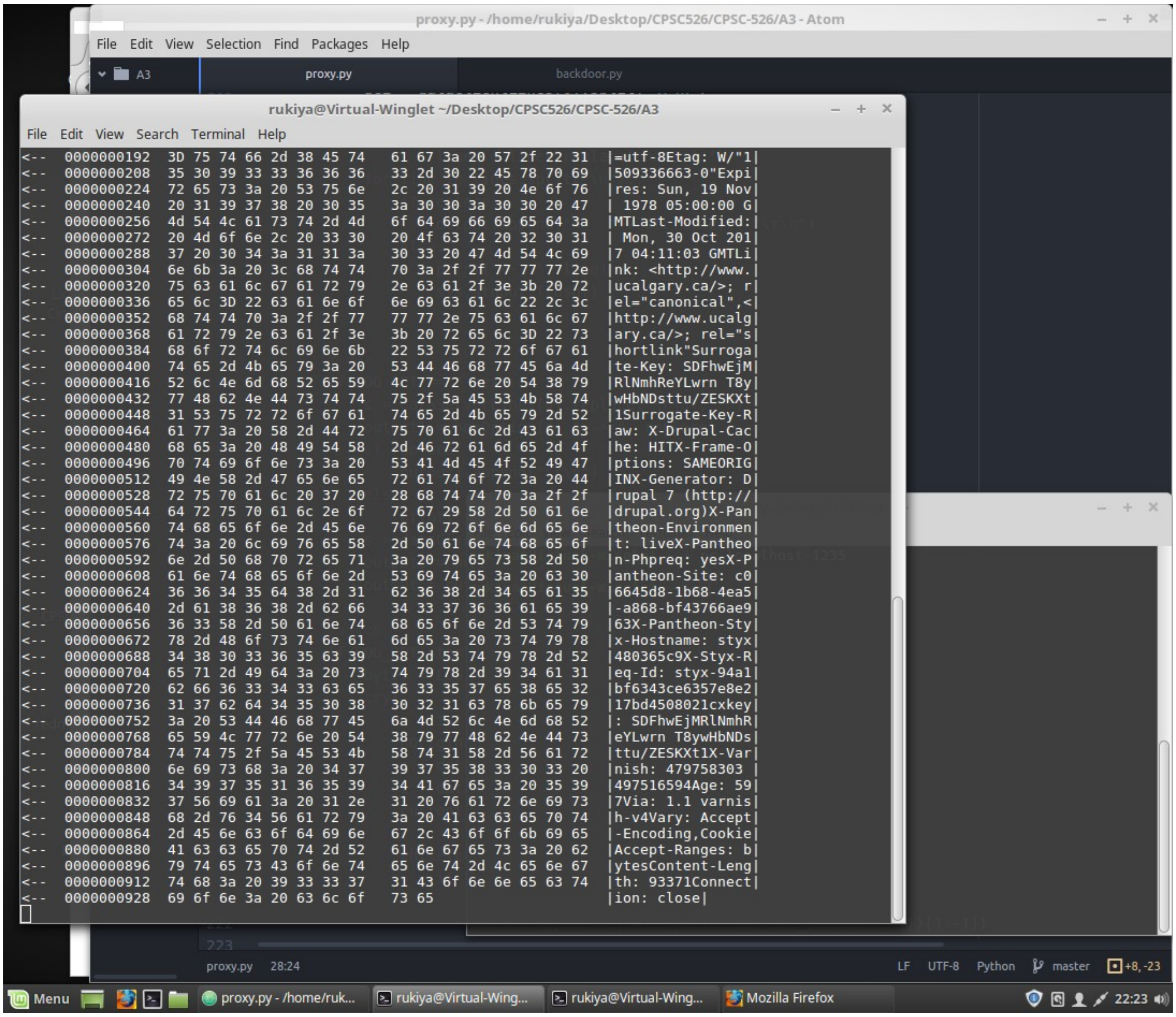
```
rukiya@Virtual-Winglet ~ $ ssh localhost -p  1234
```

-strip using http



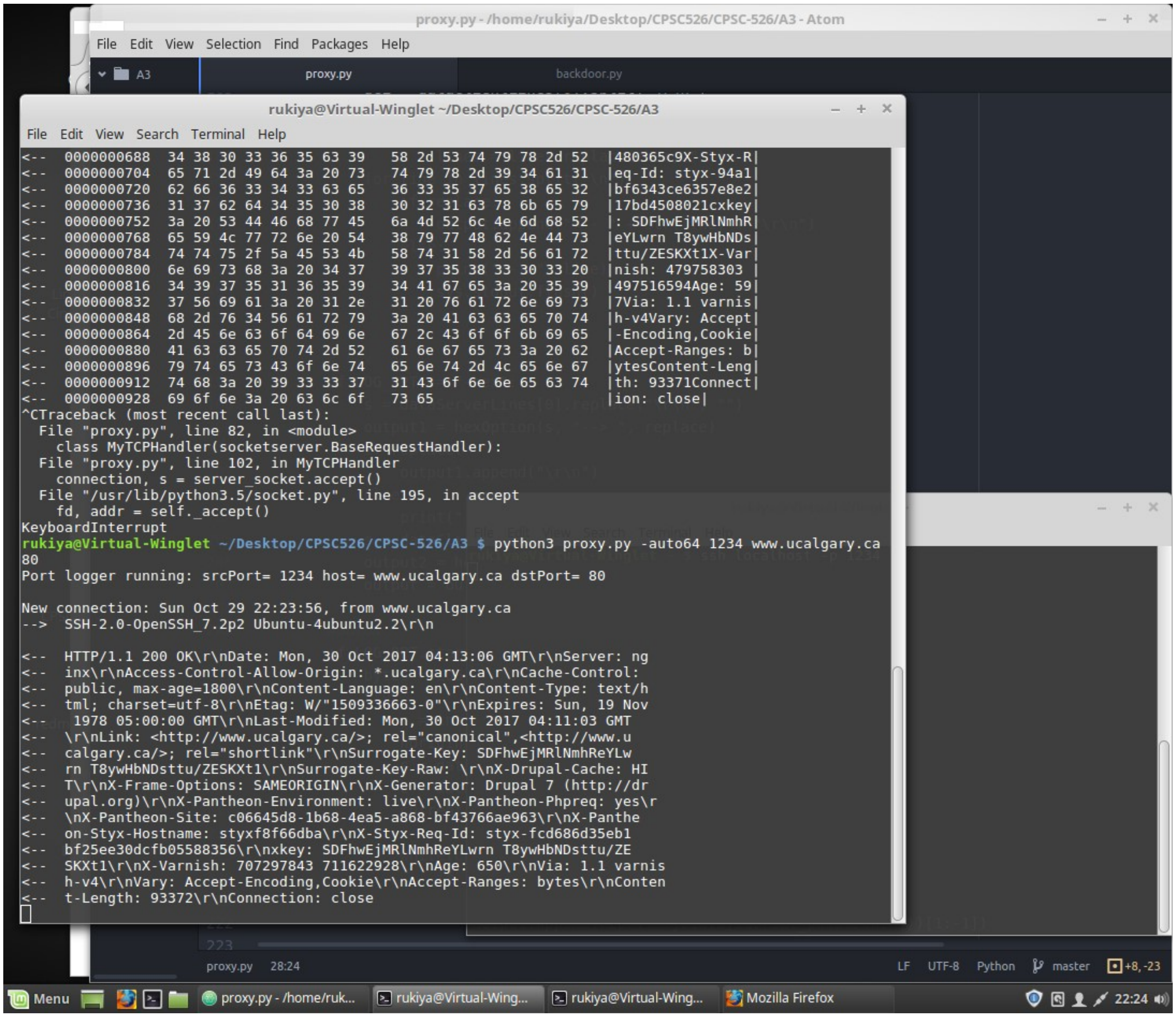
```
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3 $ python3 proxy.py -strip 1234 www.u
calgary.ca 80
Port logger running: srcPort= 1234 host= www.ucalgary.ca dstPort= 80

New connection: Sun Oct 29 22:21:18, from  localhost
-->  GET / HTTP/1.1
-->  Host: localhost:1234
-->  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/
54.0
-->  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
-->  Accept-Language: en-US,en;q=0.5
-->  Accept-Encoding: gzip, deflate
-->  Connection: keep-alive
-->  Upgrade-Insecure-Requests: 1
-->  Cache-Control: max-age=0
<--  HTTP/1.1 200 OK
<--  Date: Mon, 30 Oct 2017 04:12:22 GMT
<--  Server: nginx
<--  Access-Control-Allow-Origin: *.ucalgary.ca
<--  Cache-Control: public, max-age=1800
<--  Content-Language: en
<--  Content-Type: text/html; charset=utf-8
<--  Etag: W/"1509336663-0"
<--  Expires: Sun, 19 Nov 1978 05:00:00 GMT
<--  Last-Modified: Mon, 30 Oct 2017 04:11:03 GMT
<--  Link: <http://www.ucalgary.ca/>; rel="canonical",<http://www.ucalgary.ca/>; rel="sho
rtlink"
<--  Surrogate-Key: SDFhwEjMRlNmhReYLwrn T8ywHbNDsttu/ZESKXt1
<--  Surrogate-Key-Raw:
<--  X-Drupal-Cache: HIT
<--  X-Frame-Options: SAMEORIGIN
<--  X-Generator: Drupal 7 (http://drupal.org)
<--  X-Pantheon-Environment: live
<--  X-Pantheon-Phpreq: yes
<--  X-Pantheon-Site: c06645d8-1b68-4ea5-a868-bf43766ae963
<--  X-Pantheon-Styx-Hostname: styx2dc46933
<--  X-Styx-Req-Id: styx-3870c5a5978600386ddbbe28426a47d9
<--  xkey: SDFhwEjMRlNmhReYLwrn T8ywHbNDsttu/ZESKXt1
<--  X-Varnish: 849052245 858226786
<--  Age: 535
<--  Via: 1.1 varnish-v4
<--  Vary: Accept-Encoding,Cookie
<--  Accept-Ranges: bytes
<--  Content-Length: 93372
<--  Connection: close
```

-hex using nc


proxy.py - /home/rukiya/Desktop/CPSC526/CPSC-526/A3 - Atom
File Edit View Selection Find Packages Help
A3
proxy.py
backdoor.py
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3
File Edit View Search Terminal Help
proxy.py 28:24
LF UTF-8 Python master +8, -23
Menu
proxy.py - /home/ruk...
rukiya@Virtual-Wing...
rukiya@Virtual-Wing...
Mozilla Firefox
22:23

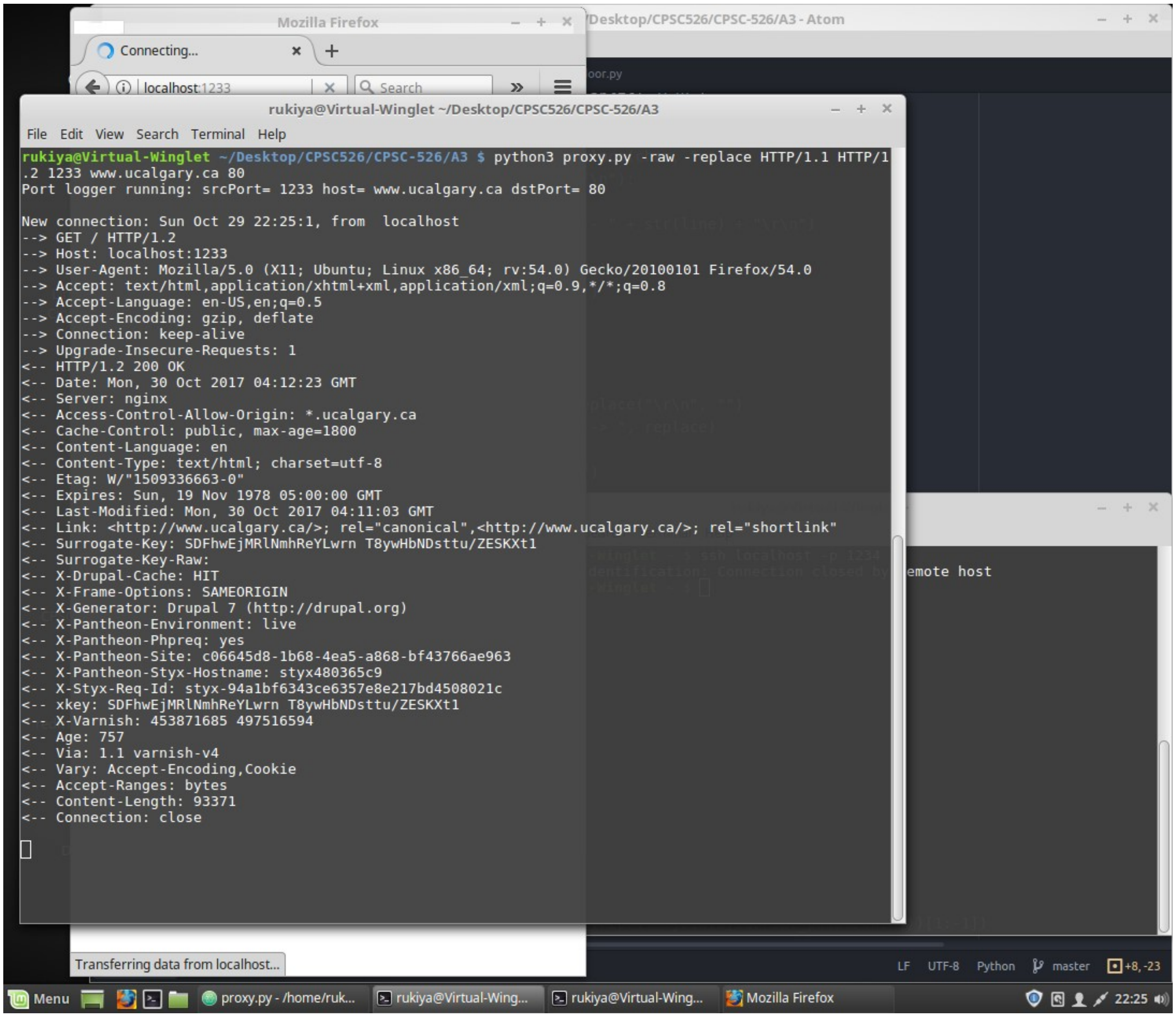
```
<--   0000000192  3D 75 74 66 2d 38 45 74   61 67 3a 20 57 2f 22 31   |=utf-8Etag: W/"1|
<--   0000000208  35 30 39 33 33 36 36 36   33 2d 30 22 45 78 70 69   |509336663-0"Expi|
<--   0000000224  72 65 73 3a 20 53 75 6e   2c 20 31 39 20 4e 6f 76   |res: Sun, 19 Nov|
<--   0000000240  20 31 39 37 38 20 30 35   3a 30 30 3a 30 30 20 47   | 1978 05:00:00 G|
<--   0000000256  4d 54 4c 61 73 74 2d 4d   6f 64 69 66 69 65 64 3a   |MTLast-Modified:|
<--   0000000272  20 4d 6f 6e 2c 20 33 30   20 4f 63 74 20 32 30 31   | Mon, 30 Oct 201|
<--   0000000288  37 20 30 34 3a 31 31 3a   30 33 20 47 4d 54 4c 69   |7 04:11:03 GMTLi|
<--   0000000304  6e 6b 3a 20 3c 68 74 74   70 3a 2f 2f 77 77 77 2e   |nk: <http://www.|
<--   0000000320  75 63 61 6c 67 61 72 79   2e 63 61 2f 3e 3b 20 72   |ucalgary.ca/>; r|
<--   0000000336  65 6c 3D 22 63 61 6e 6f   6e 69 63 61 6c 22 2c 3c   |el="canonical",<|
<--   0000000352  68 74 74 70 3a 2f 2f 77   77 77 2e 75 63 61 6c 67   |http://www.ucalg|
<--   0000000368  61 72 79 2e 63 61 2f 3e   3b 20 72 65 6c 3D 22 73   |ary.ca/>; rel="s|
<--   0000000384  68 6f 72 74 6c 69 6e 6b   22 53 75 72 72 6f 67 61   |hortlink"Surroga|
<--   0000000400  74 65 2d 4b 65 79 3a 20   53 44 46 68 77 45 6a 4d   |te-Key: SDFhwEjM|
<--   0000000416  52 6c 4e 6d 68 52 65 59   4c 77 72 6e 20 54 38 79   |RlNmhReYLwrn T8y|
<--   0000000432  77 48 62 4e 44 73 74 74   75 2f 5a 45 53 4b 58 74   |wHbNDsttu/ZESKXt|
<--   0000000448  31 53 75 72 72 6f 67 61   74 65 2d 4b 65 79 2d 52   |1Surrogate-Key-R|
<--   0000000464  61 77 3a 20 58 2d 44 72   75 70 61 6c 2d 43 61 63   |aw: X-Drupal-Cac|
<--   0000000480  68 65 3a 20 48 49 54 58   2d 46 72 61 6d 65 2d 4f   |he: HITX-Frame-O|
<--   0000000496  70 74 69 6f 6e 73 3a 20   53 41 4d 45 4f 52 49 47   |ptions: SAMEORIG|
<--   0000000512  49 4e 58 2d 47 65 6e 65   72 61 74 6f 72 3a 20 44   |INX-Generator: D|
<--   0000000528  72 75 70 61 6c 20 37 20   28 68 74 74 70 3a 2f 2f   |rupal 7 (http://|
<--   0000000544  64 72 75 70 61 6c 2e 6f   72 67 29 58 2d 50 61 6e   |drupal.org)X-Pan|
<--   0000000560  74 68 65 6f 6e 2d 45 6e   76 69 72 6f 6e 6d 65 6e   |theon-Environmen|
<--   0000000576  74 3a 20 6c 69 76 65 58   2d 50 61 6e 74 68 65 6f   |t: liveX-Pantheo|
<--   0000000592  6e 2d 50 68 70 72 65 71   3a 20 79 65 73 58 2d 50   |n-Phpreq: yesX-P|
<--   0000000608  61 6e 74 68 65 6f 6e 2d   53 69 74 65 3a 20 63 30   |antheon-Site: c0|
<--   0000000624  36 36 34 35 64 38 2d 31   62 36 38 2d 34 65 61 35   |6645d8-1b68-4ea5|
<--   0000000640  2d 61 38 36 38 2d 62 66   34 33 37 36 36 61 65 39   |-a868-bf43766ae9|
<--   0000000656  36 33 58 2d 50 61 6e 74   68 65 6f 6e 2d 53 74 79   |63X-Pantheon-Sty|
<--   0000000672  78 2d 48 6f 73 74 6e 61   6d 65 3a 20 73 74 79 78   |x-Hostname: styx|
<--   0000000688  34 38 30 33 36 35 63 39   58 2d 53 74 79 78 2d 52   |480365c9X-Styx-R|
<--   0000000704  65 71 2d 49 64 3a 20 73   74 79 78 2d 39 34 61 31   |eq-Id: styx-94a1|
<--   0000000720  62 66 36 33 34 33 63 65   36 33 35 37 65 38 65 32   |bf6343ce6357e8e2|
<--   0000000736  31 37 62 64 34 35 30 38   30 32 31 63 78 6b 65 79   |17bd4508021cxkey|
<--   0000000752  3a 20 53 44 46 68 77 45   6a 4d 52 6c 4e 6d 68 52   |: SDFhwEjMRlNmhR|
<--   0000000768  65 59 4c 77 72 6e 20 54   38 79 77 48 62 4e 44 73   |eYLwrn T8ywHbNDs|
<--   0000000784  74 74 75 2f 5a 45 53 4b   58 74 31 58 2d 56 61 72   |ttu/ZESKXt1X-Var|
<--   0000000800  6e 69 73 68 3a 20 34 37   39 37 35 38 33 30 33 20   |nish: 479758303 |
<--   0000000816  34 39 37 35 31 36 35 39   34 41 67 65 3a 20 35 39   |497516594Age: 59|
<--   0000000832  37 56 69 61 3a 20 31 2e   31 20 76 61 72 6e 69 73   |7Via: 1.1 varnis|
<--   0000000848  68 2d 76 34 56 61 72 79   3a 20 41 63 63 65 70 74   |h-v4Vary: Accept|
<--   0000000864  2d 45 6e 63 6f 64 69 6e   67 2c 43 6f 6f 6b 69 65   |-Encoding,Cookie|
<--   0000000880  41 63 63 65 70 74 2d 52   61 6e 67 65 73 3a 20 62   |Accept-Ranges: b|
<--   0000000896  79 74 65 73 43 6f 6e 74   65 6e 74 2d 4c 65 6e 67   |ytesContent-Leng|
<--   0000000912  74 68 3a 20 39 33 33 37   31 43 6f 6e 6e 65 63 74   |th: 93371Connect|
<--   0000000928  69 6f 6e 3a 20 63 6c 6f   73 65                     |ion: close|
```

-autoN (N = 64) using ssh


proxy.py - /home/rukiya/Desktop/CPSC526/CPSC-526/A3 - Atom
File Edit View Selection Find Packages Help
A3
proxy.py
backdoor.py
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3
File Edit View Search Terminal Help
proxy.py 28:24
LF UTF-8 Python master +8, -23
Menu
proxy.py - /home/ruk...
rukiya@Virtual-Wing...
rukiya@Virtual-Wing...
Mozilla Firefox
22:24

```
<--  0000000688  34 38 30 33 36 35 63 39   58 2d 53 74 79 78 2d 52  |480365c9X-Styx-R|
<--  0000000704  65 71 2d 49 64 3a 20 73   74 79 78 2d 39 34 61 31  |eq-Id: styx-94a1|
<--  0000000720  62 66 36 33 34 33 63 65   36 33 35 37 65 38 65 32  |bf6343ce6357e8e2|
<--  0000000736  31 37 62 64 34 35 30 38   30 32 31 63 78 6b 65 79  |17bd4508021cxkey|
<--  0000000752  3a 20 53 44 46 68 77 45   6a 4d 52 6c 4e 6d 68 52  |: SDFhwEjMRlNmhR|
<--  0000000768  65 59 4c 77 72 6e 20 54   38 79 77 48 62 4e 44 73  |eYLwrn T8ywHbNDs|
<--  0000000784  74 74 75 2f 5a 45 53 4b   58 74 31 58 2d 56 61 72  |ttu/ZESKXt1X-Var|
<--  0000000800  6e 69 73 68 3a 20 34 37   39 37 35 38 33 30 33 20  |nish: 479758303 |
<--  0000000816  34 39 37 35 31 36 35 39   34 41 67 65 3a 20 35 39  |497516594Age: 59|
<--  0000000832  37 56 69 61 3a 20 31 2e   31 20 76 61 72 6e 69 73  |7Via: 1.1 varnis|
<--  0000000848  68 2d 76 34 56 61 72 79   3a 20 41 63 63 65 70 74  |h-v4Vary: Accept|
<--  0000000864  2d 45 6e 63 6f 64 69 6e   67 2c 43 6f 6f 6b 69 65  |-Encoding,Cookie|
<--  0000000880  41 63 63 65 70 74 2d 52   61 6e 67 65 73 3a 20 62  |Accept-Ranges: b|
<--  0000000896  79 74 65 73 43 6f 6e 74   65 6e 74 2d 4c 65 6e 67  |ytesContent-Leng|
<--  0000000912  74 68 3a 20 39 33 33 37   31 43 6f 6e 6e 65 63 74  |th: 93371Connect|
<--  0000000928  69 6f 6e 3a 20 63 6c 6f   73 65                    |ion: close|
^CTraceback (most recent call last):
  File "proxy.py", line 82, in <module>
    class MyTCPHandler(socketserver.BaseRequestHandler):
  File "proxy.py", line 102, in MyTCPHandler
    connection, s = server_socket.accept()
  File "/usr/lib/python3.5/socket.py", line 195, in accept
    fd, addr = self._accept()
KeyboardInterrupt
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3 $ python3 proxy.py -auto64 1234 www.ucalgary.ca
80
Port logger running: srcPort= 1234 host= www.ucalgary.ca dstPort= 80

New connection: Sun Oct 29 22:23:56, from www.ucalgary.ca
-->  SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2\r\n

<--  HTTP/1.1 200 OK\r\nDate: Mon, 30 Oct 2017 04:13:06 GMT\r\nServer: ng
<--  inx\r\nAccess-Control-Allow-Origin: *.ucalgary.ca\r\nCache-Control:
<--  public, max-age=1800\r\nContent-Language: en\r\nContent-Type: text/h
<--  tml; charset=utf-8\r\nEtag: W/"1509336663-0"\r\nExpires: Sun, 19 Nov
<--   1978 05:00:00 GMT\r\nLast-Modified: Mon, 30 Oct 2017 04:11:03 GMT
<--  \r\nLink: <http://www.ucalgary.ca/>; rel="canonical",<http://www.u
<--  calgary.ca/>; rel="shortlink"\r\nSurrogate-Key: SDFhwEjMRlNmhReYLw
<--  rn T8ywHbNDsttu/ZESKXt1\r\nSurrogate-Key-Raw: \r\nX-Drupal-Cache: HI
<--  T\r\nX-Frame-Options: SAMEORIGIN\r\nX-Generator: Drupal 7 (http://dr
<--  upal.org)\r\nX-Pantheon-Environment: live\r\nX-Pantheon-Phpreq: yes\r
<--  \nX-Pantheon-Site: c06645d8-1b68-4ea5-a868-bf43766ae963\r\nX-Panthe
<--  on-Styx-Hostname: styxf8f66dba\r\nX-Styx-Req-Id: styx-fcd686d35eb1
<--  bf25ee30dcfb05588356\r\nxkey: SDFhwEjMRlNmhReYLwrn T8ywHbNDsttu/ZE
<--  SKXt1\r\nX-Varnish: 707297843 711622928\r\nAge: 650\r\nVia: 1.1 varnis
<--  h-v4\r\nVary: Accept-Encoding,Cookie\r\nAccept-Ranges: bytes\r\nConten
<--  t-Length: 93372\r\nConnection: close
```

-raw replace HTTP\1.1 HTTP\1.2 using http



```
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3 $ python3 proxy.py -raw -replace HTTP/1.1 HTTP/1
.2 1233 www.ucalgary.ca 80
Port logger running: srcPort= 1233 host= www.ucalgary.ca dstPort= 80

New connection: Sun Oct 29 22:25:1, from  localhost
--> GET / HTTP/1.2
--> Host: localhost:1233
--> User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0
--> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
--> Accept-Language: en-US,en;q=0.5
--> Accept-Encoding: gzip, deflate
--> Connection: keep-alive
--> Upgrade-Insecure-Requests: 1
<-- HTTP/1.2 200 OK
<-- Date: Mon, 30 Oct 2017 04:12:23 GMT
<-- Server: nginx
<-- Access-Control-Allow-Origin: *.ucalgary.ca
<-- Cache-Control: public, max-age=1800
<-- Content-Language: en
<-- Content-Type: text/html; charset=utf-8
<-- Etag: W/"1509336663-0"
<-- Expires: Sun, 19 Nov 1978 05:00:00 GMT
<-- Last-Modified: Mon, 30 Oct 2017 04:11:03 GMT
<-- Link: <http://www.ucalgary.ca/>; rel="canonical",<http://www.ucalgary.ca/>; rel="shortlink"
<-- Surrogate-Key: SDFhwEjMRlNmhReYLwrn T8ywHbNDsttu/ZESKXt1
<-- Surrogate-Key-Raw:
<-- X-Drupal-Cache: HIT
<-- X-Frame-Options: SAMEORIGIN
<-- X-Generator: Drupal 7 (http://drupal.org)
<-- X-Pantheon-Environment: live
<-- X-Pantheon-Phpreq: yes
<-- X-Pantheon-Site: c06645d8-1b68-4ea5-a868-bf43766ae963
<-- X-Pantheon-Styx-Hostname: styx480365c9
<-- X-Styx-Req-Id: styx-94a1bf6343ce6357e8e217bd4508021c
<-- xkey: SDFhwEjMRlNmhReYLwrn T8ywHbNDsttu/ZESKXt1
<-- X-Varnish: 453871685 497516594
<-- Age: 757
<-- Via: 1.1 varnish-v4
<-- Vary: Accept-Encoding,Cookie
<-- Accept-Ranges: bytes
<-- Content-Length: 93371
<-- Connection: close
```

Mozilla Firefox
Connecting...
localhost:1233
Search
/Desktop/CPSC526/CPSC-526/A3 - Atom
rukiya@Virtual-Winglet ~/Desktop/CPSC526/CPSC-526/A3
File Edit View Search Terminal Help
emote host
Transferring data from localhost...
LF UTF-8 Python master +8, -23
Menu
proxy.py - /home/ruk...
rukiya@Virtual-Wing...
rukiya@Virtual-Wing...
Mozilla Firefox
22:25