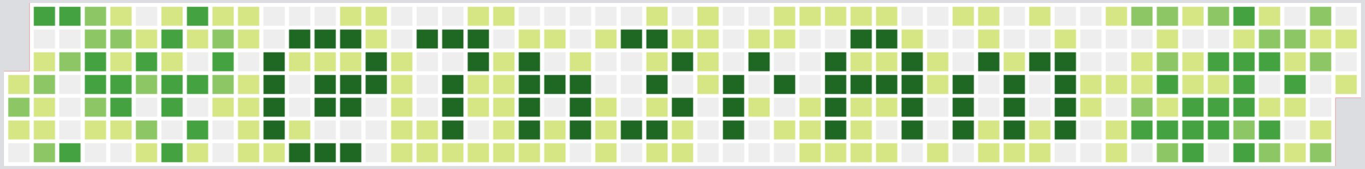
Flowinspect - A Network Inspection Tool

Ankur Tyagi (@7h3rAm)



Outline

- Understanding Incident Response Requirements
- Vision for an Ideal Inspection Tool
- Introducing Flowinspect as a Viable Solution
- Flowinspect: Architecture
- Real-World Usecase Scenarios
- Future Goals

Understanding Incident Response Requirements

- You have been called to investigate an incident
- You analyze evidence and find traces of a malware
- You want to know:
  - Who were the actors?
  - What did they talk about?
  - What secrets did they share?
  - Which other hosts were compromised?

Understanding Incident Response Requirements

- Immediate response requires data
- Data from the exploit, payload delivered, C&C channel, etc.
- Tools like Wireshark, tcpdump, ngrep and flowgrep are helpful

- But they all have a few shortcomings
- Many are flow/stream agnostic and lack inspection features

Understanding Incident Response Requirements

- Tcpdump/Wireshark – Packet sniffing and comprehensive protocol decoding
- Ngrep/Flowgrep – Packet sniffing and regex matching over L4 packets and streams resp.

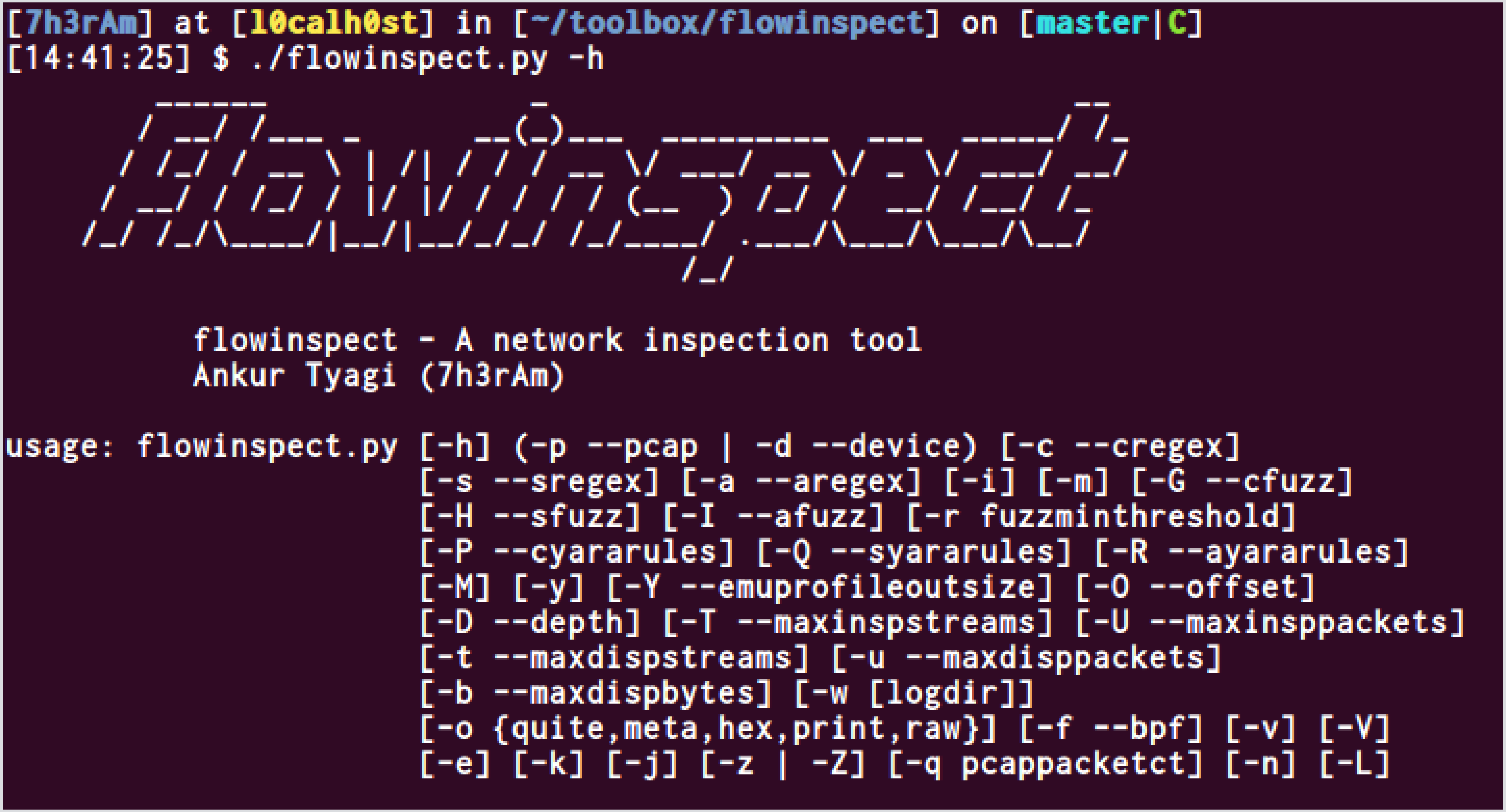
- How about network shellcode detection?
- How about malware identification and extraction from network flows?

- None of above tools address these requirements

Vision for an Ideal Inspection Tool

- **Malware identification via signatures**
- **Shellcode emulation/detection**
- **Extraction of matching flows to files**
- **Match statistics (direction, offset, depth, size, packet #)**
- **Snort like Content Modifiers (offset/depth)**
- **Pcap generation for matching flows**
- **TCP reset for matching flows**

Introducing Flowinspect as a Viable Solution



```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[14:41:25] $ ./flowinspect.py -h
        ______              _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

usage: flowinspect.py [-h] (-p --pcap | -d --device) [-c --cregex]
                      [-s --sregex] [-a --aregex] [-i] [-m] [-G --cfuzz]
                      [-H --sfuzz] [-I --afuzz] [-r fuzzminthreshold]
                      [-P --cyararules] [-Q --syararules] [-R --ayararules]
                      [-M] [-y] [-Y --emuprofileoutsize] [-O --offset]
                      [-D --depth] [-T --maxinspstreams] [-U --maxinsppackets]
                      [-t --maxdispstreams] [-u --maxdisppackets]
                      [-b --maxdispbytes] [-w [logdir]]
                      [-o {quite,meta,hex,print,raw}] [-f --bpf] [-v] [-V]
                      [-e] [-k] [-j] [-z | -Z] [-q pcappacketct] [-n] [-L]
```

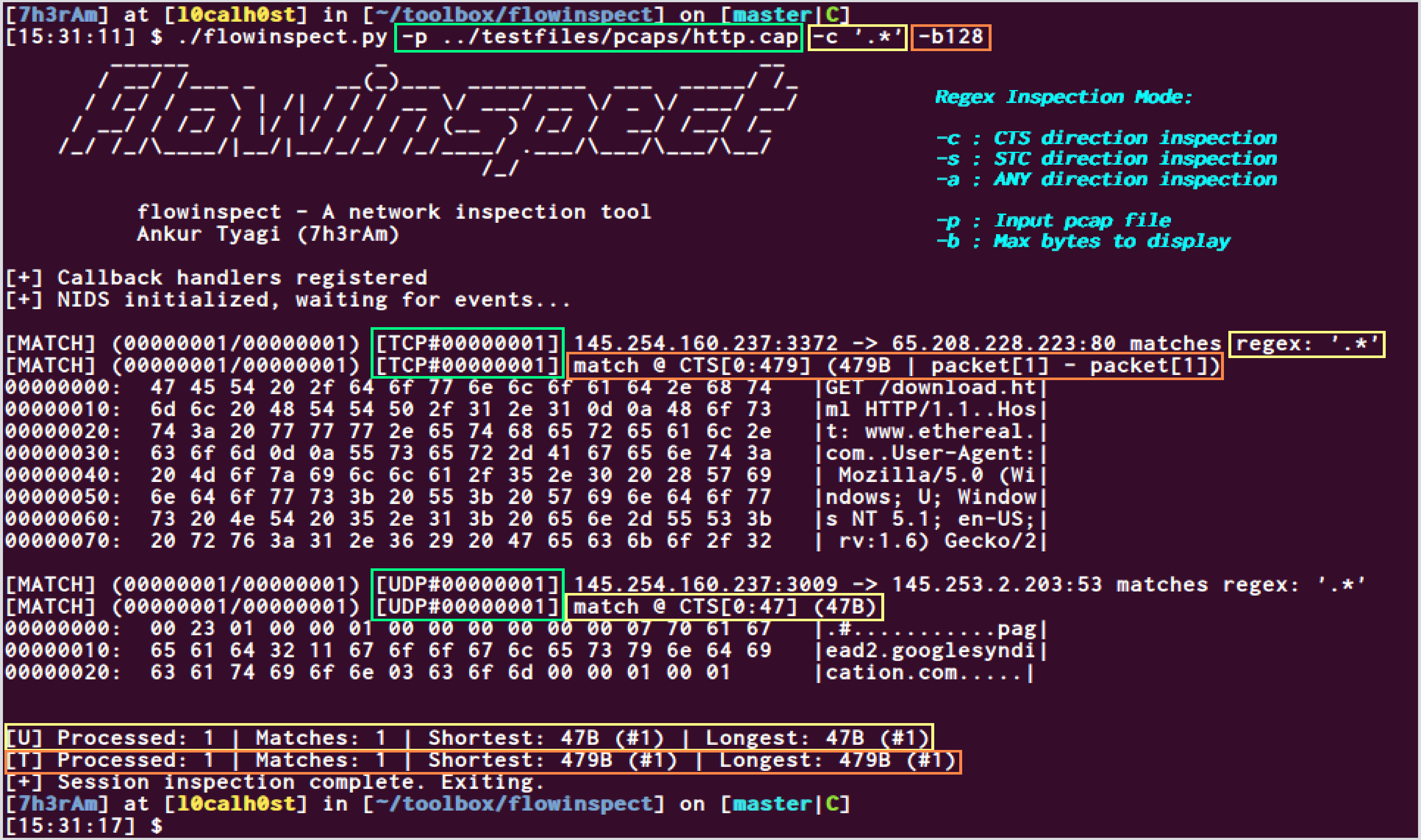
Introducing Flowinspect as a Viable Solution

- IP defragmentation and TCP reassembly - extract data into stream buffers
- Multiple inspection modes – regex, fuzzy string, Yara, shellcode detection
- Inspection happens over layer 4 payload and as such is immune to fragmentation attacks
- Matching flows dumped via (a combination of) output modes for lateral analysis

Flowinspect: Architecture

- Has 3 modules: input, inspection, and output
  - Input: libnids, BPF expressions, offset/depth, max flow/packet inspection counters
  - Inspection: regex, fuzzy, yara, shellcode
  - Output: match statistics, outmodes (meta, print, hex, raw), file writing, pcap generation

Flowinspect: Architecture



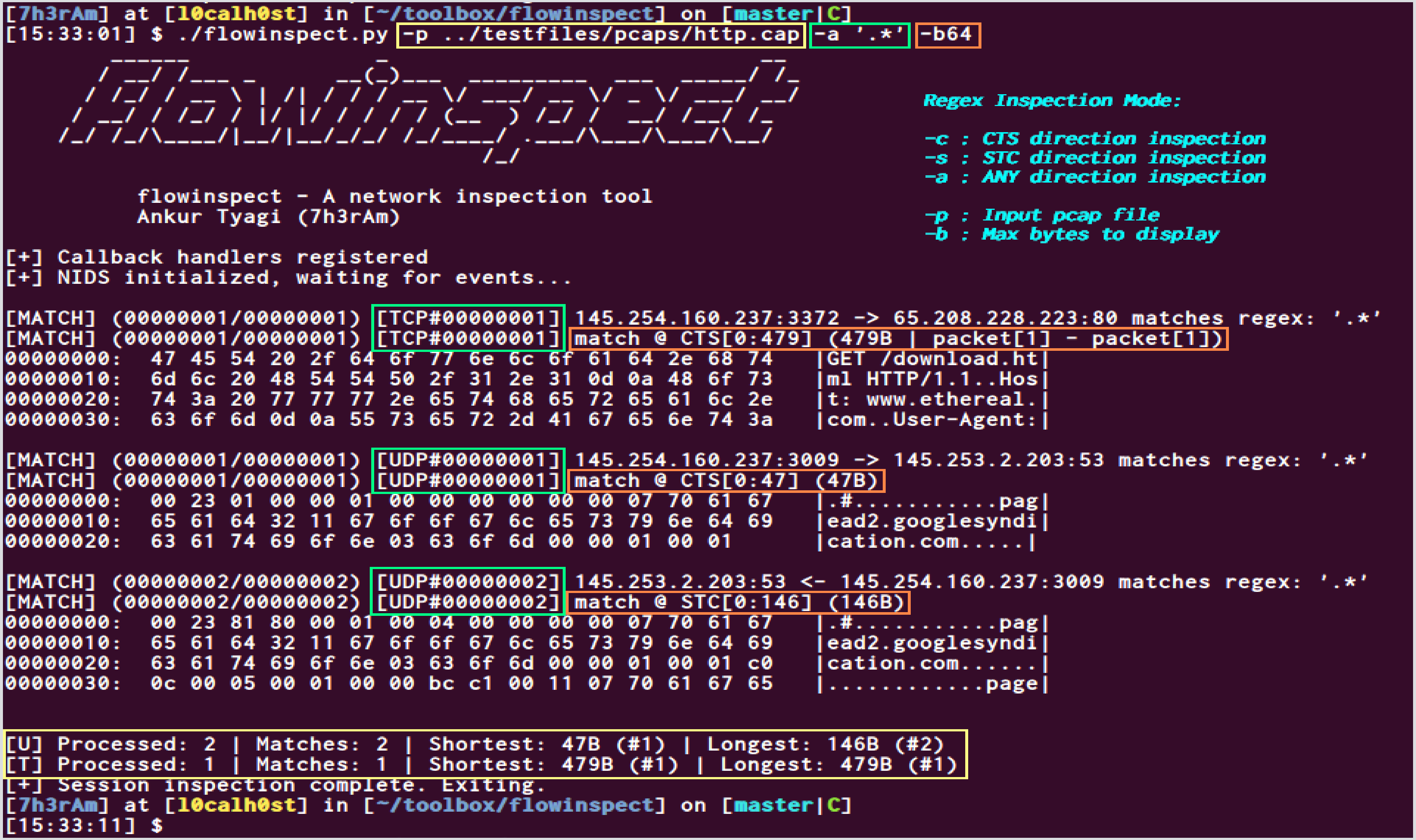
```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:31:11] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -c '.*' -b128
        ______               _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[MATCH] (00000001/00000001) [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80 matches regex: '.*'
[MATCH] (00000001/00000001) [TCP#00000001] match @ CTS[0:479] (479B | packet[1] - packet[1])
00000000:  47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74   |GET /download.ht|
00000010:  6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73   |ml HTTP/1.1..Hos|
00000020:  74 3a 20 77 77 77 2e 65 74 68 65 72 65 61 6c 2e   |t: www.ethereal.|
00000030:  63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a   |com..User-Agent:|
00000040:  20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69   | Mozilla/5.0 (Wi|
00000050:  6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77   |ndows; U; Window|
00000060:  73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b   |s NT 5.1; en-US;|
00000070:  20 72 76 3a 31 2e 36 29 20 47 65 63 6b 6f 2f 32   | rv:1.6) Gecko/2|

[MATCH] (00000001/00000001) [UDP#00000001] 145.254.160.237:3009 -> 145.253.2.203:53 matches regex: '.*'
[MATCH] (00000001/00000001) [UDP#00000001] match @ CTS[0:47] (47B)
00000000:  00 23 01 00 00 01 00 00 00 00 00 00 07 70 61 67   |.#...........pag|
00000010:  65 61 64 32 11 67 6f 6f 67 6c 65 73 79 6e 64 69   |ead2.googlesyndi|
00000020:  63 61 74 69 6f 6e 03 63 6f 6d 00 00 01 00 01      |cation.com.....|


[U] Processed: 1 | Matches: 1 | Shortest: 47B (#1) | Longest: 47B (#1)
[T] Processed: 1 | Matches: 1 | Shortest: 479B (#1) | Longest: 479B (#1)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:31:17] $
```

Regex Inspection Mode:

-c : CTS direction inspection
-s : STC direction inspection
-a : ANY direction inspection

-p : Input pcap file
-b : Max bytes to display

Flowinspect: Architecture



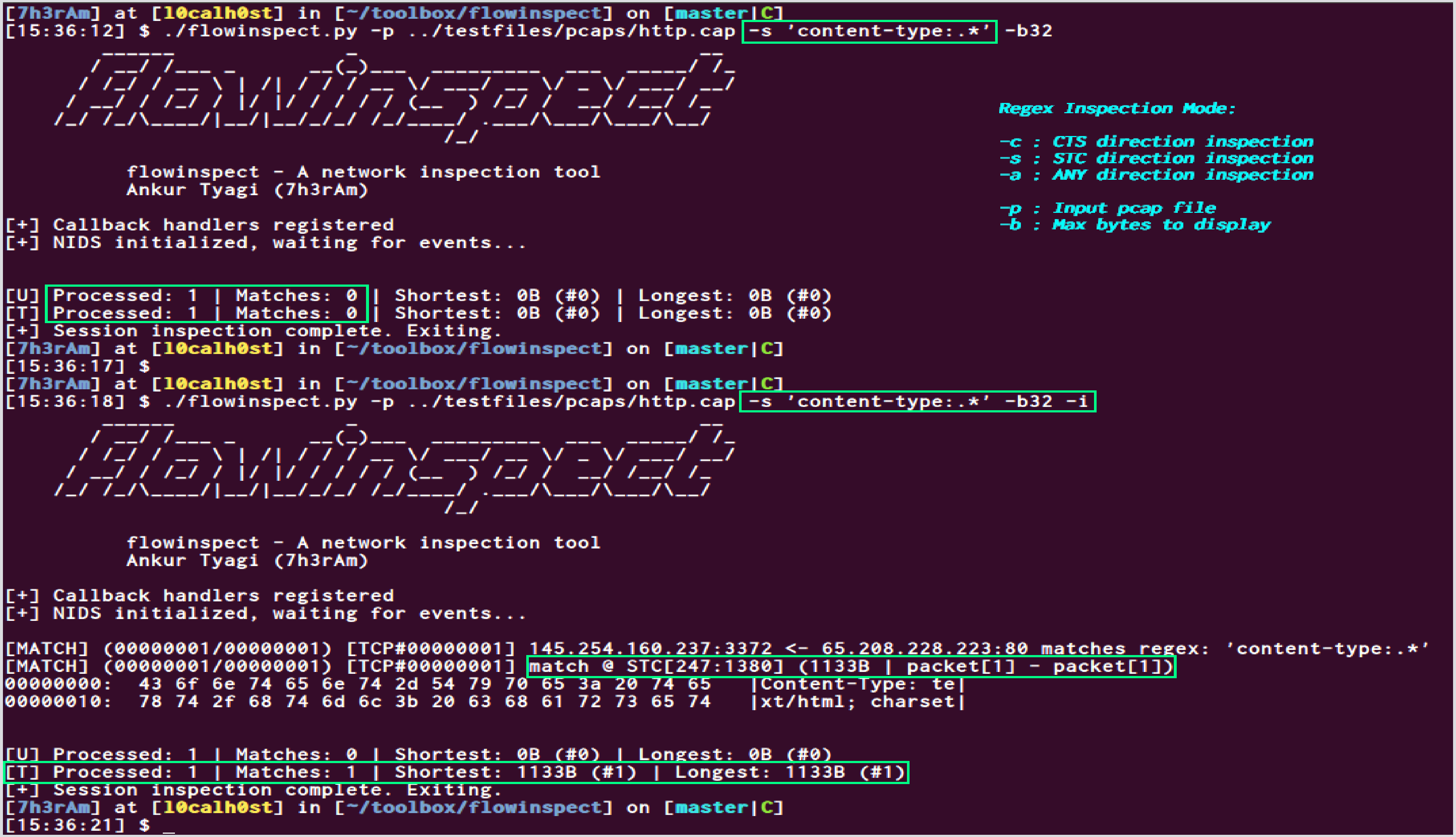
```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:33:01] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -a '.*' -b64
        ______              _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[MATCH] (00000001/00000001) [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80 matches regex: '.*'
[MATCH] (00000001/00000001) [TCP#00000001] match @ CTS[0:479] (479B | packet[1] - packet[1])
00000000:  47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74   |GET /download.ht|
00000010:  6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73   |ml HTTP/1.1..Hos|
00000020:  74 3a 20 77 77 77 2e 65 74 68 65 72 65 61 6c 2e   |t: www.ethereal.|
00000030:  63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a   |com..User-Agent:|

[MATCH] (00000001/00000001) [UDP#00000001] 145.254.160.237:3009 -> 145.253.2.203:53 matches regex: '.*'
[MATCH] (00000001/00000001) [UDP#00000001] match @ CTS[0:47] (47B)
00000000:  00 23 01 00 00 01 00 00 00 00 00 00 07 70 61 67   |.#...........pag|
00000010:  65 61 64 32 11 67 6f 6f 67 6c 65 73 79 6e 64 69   |ead2.googlesyndi|
00000020:  63 61 74 69 6f 6e 03 63 6f 6d 00 00 01 00 01      |cation.com.....|

[MATCH] (00000002/00000002) [UDP#00000002] 145.253.2.203:53 <- 145.254.160.237:3009 matches regex: '.*'
[MATCH] (00000002/00000002) [UDP#00000002] match @ STC[0:146] (146B)
00000000:  00 23 81 80 00 01 00 04 00 00 00 00 07 70 61 67   |.#...........pag|
00000010:  65 61 64 32 11 67 6f 6f 67 6c 65 73 79 6e 64 69   |ead2.googlesyndi|
00000020:  63 61 74 69 6f 6e 03 63 6f 6d 00 00 01 00 01 c0   |cation.com......|
00000030:  0c 00 05 00 01 00 00 bc c1 00 11 07 70 61 67 65   |............page|


[U] Processed: 2 | Matches: 2 | Shortest: 47B (#1) | Longest: 146B (#2)
[T] Processed: 1 | Matches: 1 | Shortest: 479B (#1) | Longest: 479B (#1)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:33:11] $
```

Regex Inspection Mode:

-c : CTS direction inspection
-s : STC direction inspection
-a : ANY direction inspection

-p : Input pcap file
-b : Max bytes to display

Flowinspect: Architecture



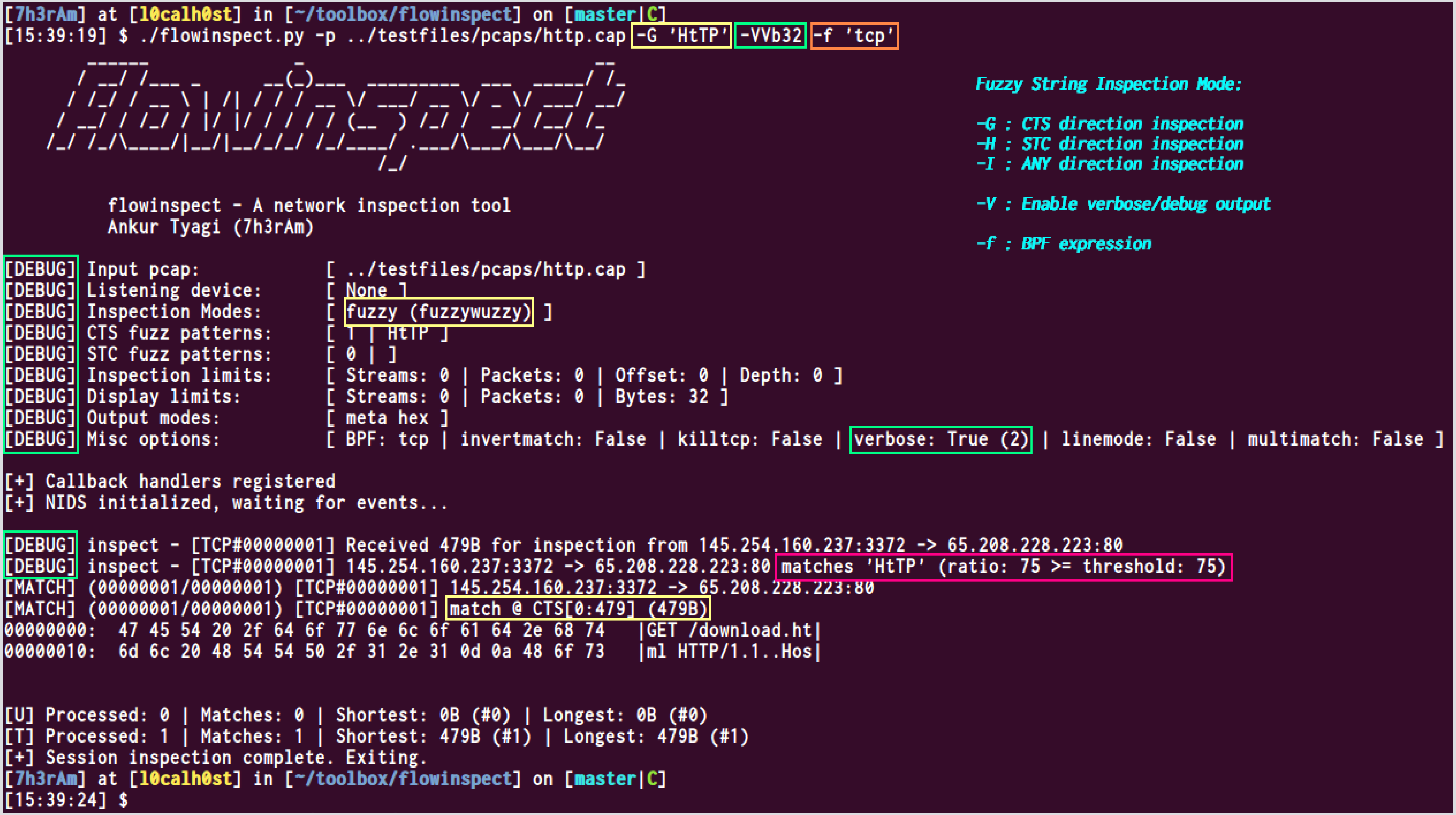
```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:36:12] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -s 'content-type:.*' -b32
        ______                _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...


[U] Processed: 1 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[T] Processed: 1 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:36:17] $
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:36:18] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -s 'content-type:.*' -b32 -i
        ______                _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[MATCH] (00000001/00000001) [TCP#00000001] 145.254.160.237:3372 <- 65.208.228.223:80 matches regex: 'content-type:.*'
[MATCH] (00000001/00000001) [TCP#00000001] match @ STC[247:1380] (1133B | packet[1] - packet[1])
00000000:  43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65   |Content-Type: te|
00000010:  78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74   |xt/html; charset|


[U] Processed: 1 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[T] Processed: 1 | Matches: 1 | Shortest: 1133B (#1) | Longest: 1133B (#1)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:36:21] $ _
```

Regex Inspection Mode:

-c : CTS direction inspection
-s : STC direction inspection
-a : ANY direction inspection

-p : Input pcap file
-b : Max bytes to display

Flowinspect: Architecture



```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:39:19] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -G 'HtTP' -VVb32 -f 'tcp'
        ______              _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

[DEBUG] Input pcap:                    [ ../testfiles/pcaps/http.cap ]
[DEBUG] Listening device:              [ None ]
[DEBUG] Inspection Modes:              [ fuzzy (fuzzywuzzy) ]
[DEBUG] CTS fuzz patterns:             [ 1 | HtTP ]
[DEBUG] STC fuzz patterns:             [ 0 | ]
[DEBUG] Inspection limits:             [ Streams: 0 | Packets: 0 | Offset: 0 | Depth: 0 ]
[DEBUG] Display limits:                [ Streams: 0 | Packets: 0 | Bytes: 32 ]
[DEBUG] Output modes:                  [ meta hex ]
[DEBUG] Misc options:                  [ BPF: tcp | invertmatch: False | killtcp: False | verbose: True (2) | linemode: False | multimatch: False ]

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[DEBUG] inspect - [TCP#00000001] Received 479B for inspection from 145.254.160.237:3372 -> 65.208.228.223:80
[DEBUG] inspect - [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80 matches 'HtTP' (ratio: 75 >= threshold: 75)
[MATCH] (00000001/00000001) [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80
[MATCH] (00000001/00000001) [TCP#00000001] match @ CTS[0:479] (479B)
00000000:  47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74   |GET /download.ht|
00000010:  6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73   |ml HTTP/1.1..Hos|


[U] Processed: 0 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[T] Processed: 1 | Matches: 1 | Shortest: 479B (#1) | Longest: 479B (#1)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:39:24] $
```

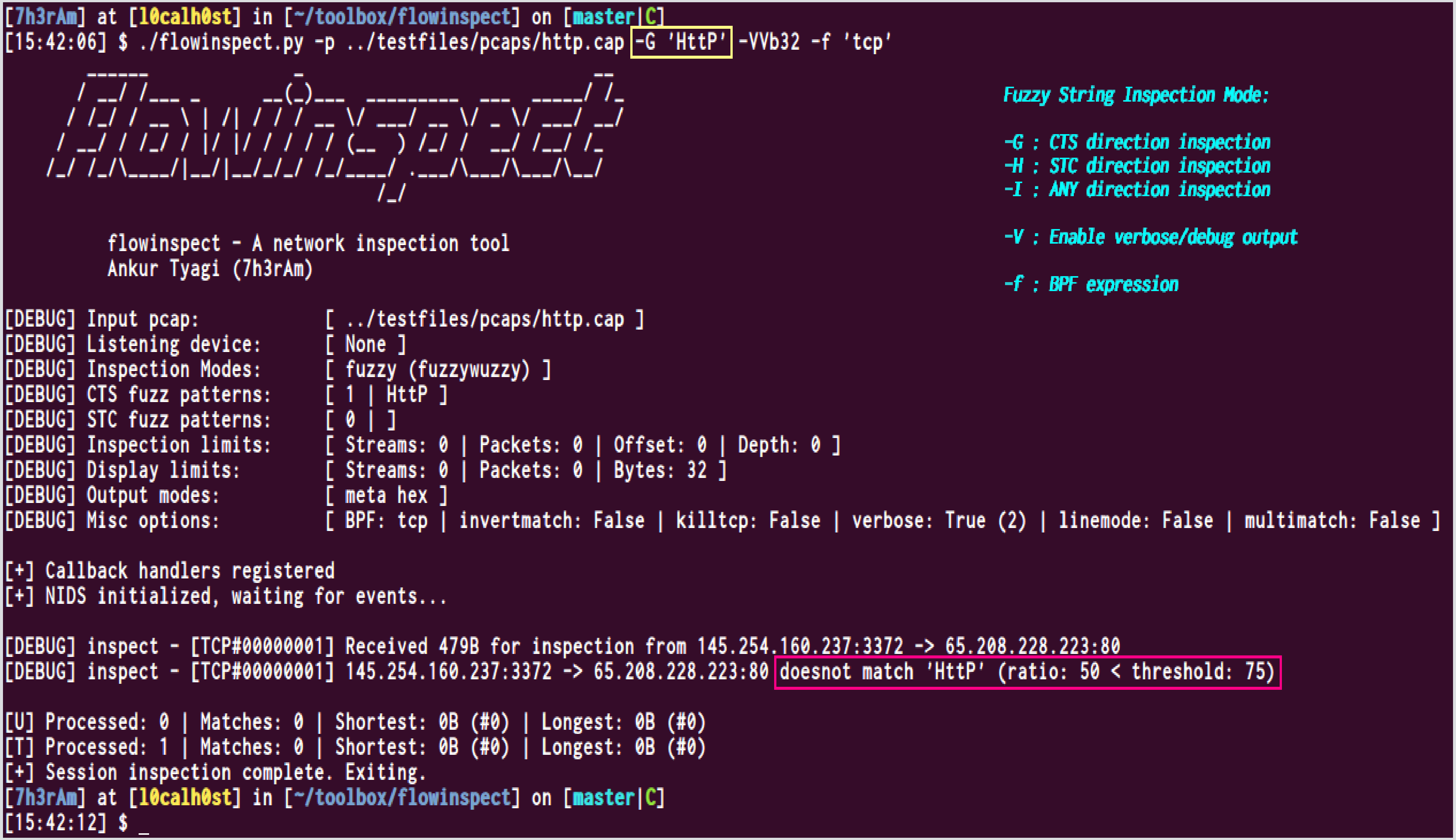
Fuzzy String Inspection Mode:

-G : CTS direction inspection
-H : STC direction inspection
-I : ANY direction inspection

-V : Enable verbose/debug output

-f : BPF expression

Flowinspect: Architecture



```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:42:06] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -G 'HttP' -VVb32 -f 'tcp'
      ______                 _                            __
     / __/ /___ _      __(_)___  _________  ___  _____/ /_
    / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
   / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
  /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                  /_/

        flowinspect - A network inspection tool
        Ankur Tyagi (7h3rAm)

[DEBUG] Input pcap:             [ ../testfiles/pcaps/http.cap ]
[DEBUG] Listening device:       [ None ]
[DEBUG] Inspection Modes:       [ fuzzy (fuzzywuzzy) ]
[DEBUG] CTS fuzz patterns:      [ 1 | HttP ]
[DEBUG] STC fuzz patterns:      [ 0 | ]
[DEBUG] Inspection limits:      [ Streams: 0 | Packets: 0 | Offset: 0 | Depth: 0 ]
[DEBUG] Display limits:         [ Streams: 0 | Packets: 0 | Bytes: 32 ]
[DEBUG] Output modes:           [ meta hex ]
[DEBUG] Misc options:           [ BPF: tcp | invertmatch: False | killtcp: False | verbose: True (2) | linemode: False | multimatch: False ]

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[DEBUG] inspect - [TCP#00000001] Received 479B for inspection from 145.254.160.237:3372 -> 65.208.228.223:80
[DEBUG] inspect - [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80 doesnot match 'HttP' (ratio: 50 < threshold: 75)

[U] Processed: 0 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[T] Processed: 1 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:42:12] $ _
```

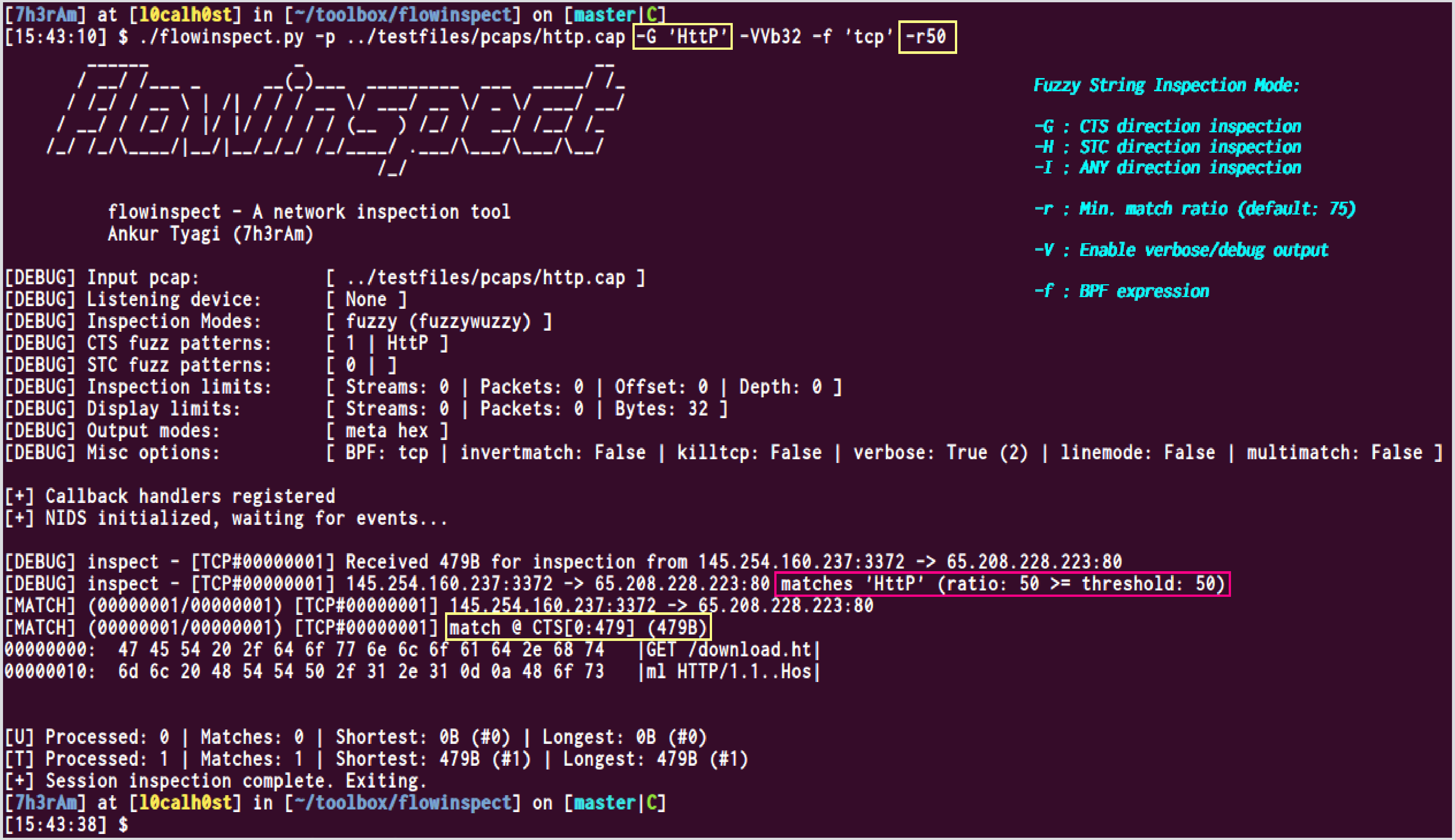
Fuzzy String Inspection Mode:

-G : CTS direction inspection
-H : STC direction inspection
-I : ANY direction inspection

-V : Enable verbose/debug output

-f : BPF expression

Flowinspect: Architecture



```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:43:10] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -G 'HttP' -VVb32 -f 'tcp' -r50
        ______              _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

[DEBUG] Input pcap:            [ ../testfiles/pcaps/http.cap ]
[DEBUG] Listening device:      [ None ]
[DEBUG] Inspection Modes:      [ fuzzy (fuzzywuzzy) ]
[DEBUG] CTS fuzz patterns:     [ 1 | HttP ]
[DEBUG] STC fuzz patterns:     [ 0 | ]
[DEBUG] Inspection limits:     [ Streams: 0 | Packets: 0 | Offset: 0 | Depth: 0 ]
[DEBUG] Display limits:        [ Streams: 0 | Packets: 0 | Bytes: 32 ]
[DEBUG] Output modes:          [ meta hex ]
[DEBUG] Misc options:          [ BPF: tcp | invertmatch: False | killtcp: False | verbose: True (2) | linemode: False | multimatch: False ]

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[DEBUG] inspect - [TCP#00000001] Received 479B for inspection from 145.254.160.237:3372 -> 65.208.228.223:80
[DEBUG] inspect - [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80 matches 'HttP' (ratio: 50 >= threshold: 50)
[MATCH] (00000001/00000001) [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80
[MATCH] (00000001/00000001) [TCP#00000001] match @ CTS[0:479] (479B)
00000000:  47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74   |GET /download.ht|
00000010:  6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73   |ml HTTP/1.1..Hos|


[U] Processed: 0 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[T] Processed: 1 | Matches: 1 | Shortest: 479B (#1) | Longest: 479B (#1)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:43:38] $
```

Fuzzy String Inspection Mode:

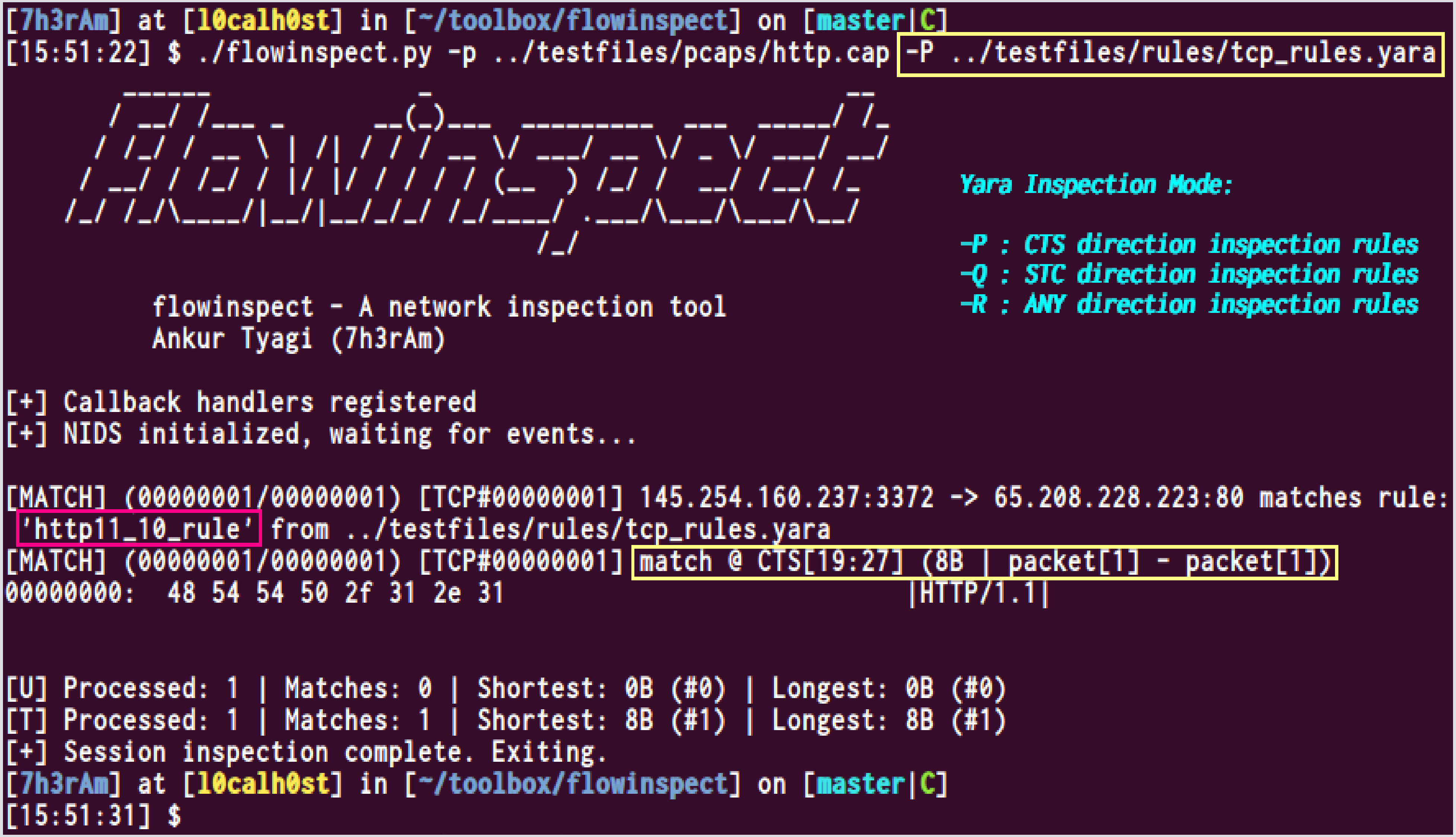
-G : CTS direction inspection
-H : STC direction inspection
-I : ANY direction inspection

-r : Min. match ratio (default: 75)

-V : Enable verbose/debug output

-f : BPF expression

Flowinspect: Architecture

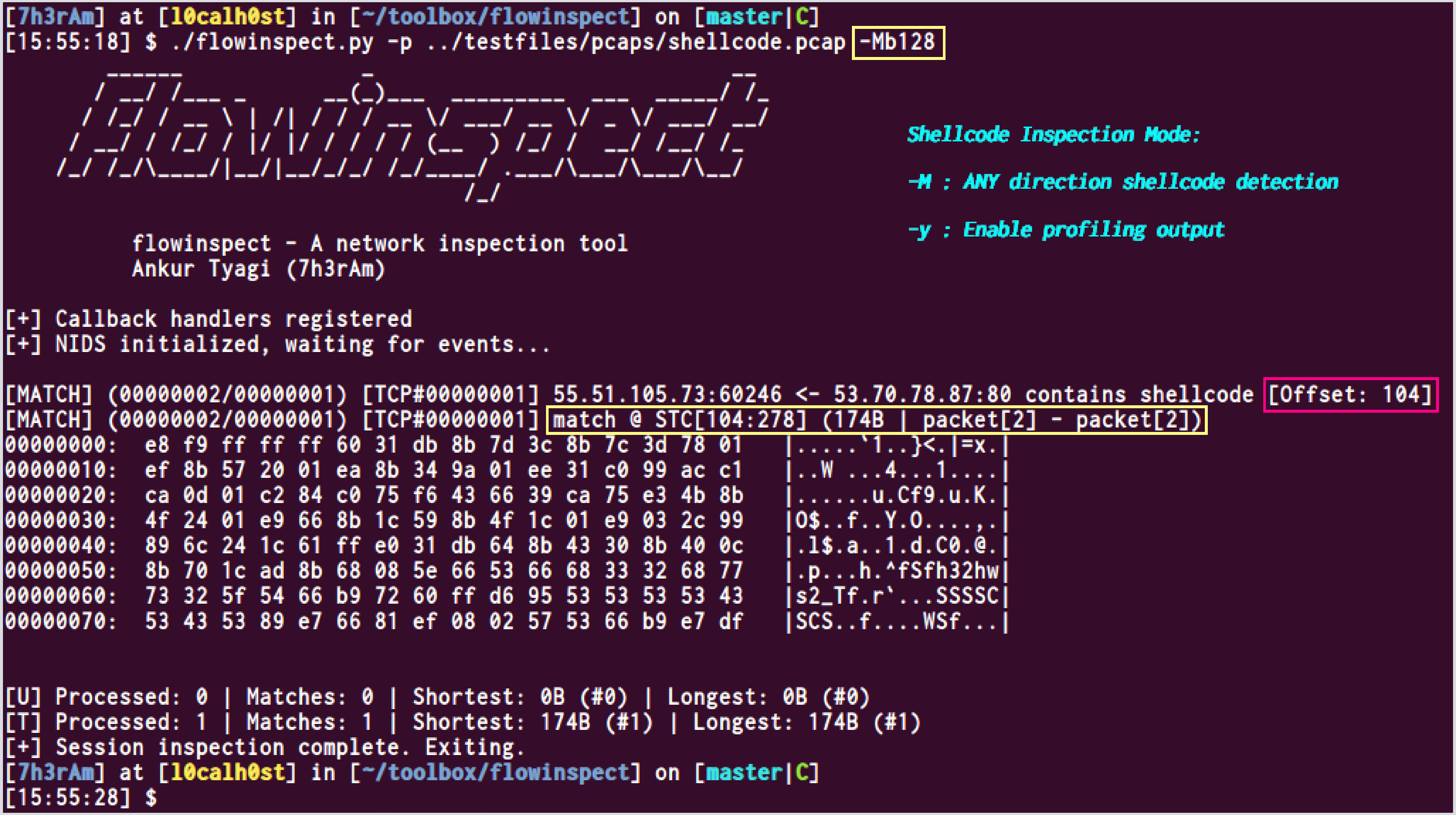


```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:51:22] $ ./flowinspect.py -p ../testfiles/pcaps/http.cap -P ../testfiles/rules/tcp_rules.yara
        ______              _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

         flowinspect - A network inspection tool
         Ankur Tyagi (7h3rAm)

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[MATCH] (00000001/00000001) [TCP#00000001] 145.254.160.237:3372 -> 65.208.228.223:80 matches rule:
 'http11_10_rule' from ../testfiles/rules/tcp_rules.yara
[MATCH] (00000001/00000001) [TCP#00000001] match @ CTS[19:27] (8B | packet[1] - packet[1])
00000000:  48 54 54 50 2f 31 2e 31                          |HTTP/1.1|


[U] Processed: 1 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[T] Processed: 1 | Matches: 1 | Shortest: 8B (#1) | Longest: 8B (#1)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:51:31] $
```

Yara Inspection Mode:

-P : CTS direction inspection rules
-Q : STC direction inspection rules
-R : ANY direction inspection rules

Flowinspect: Architecture



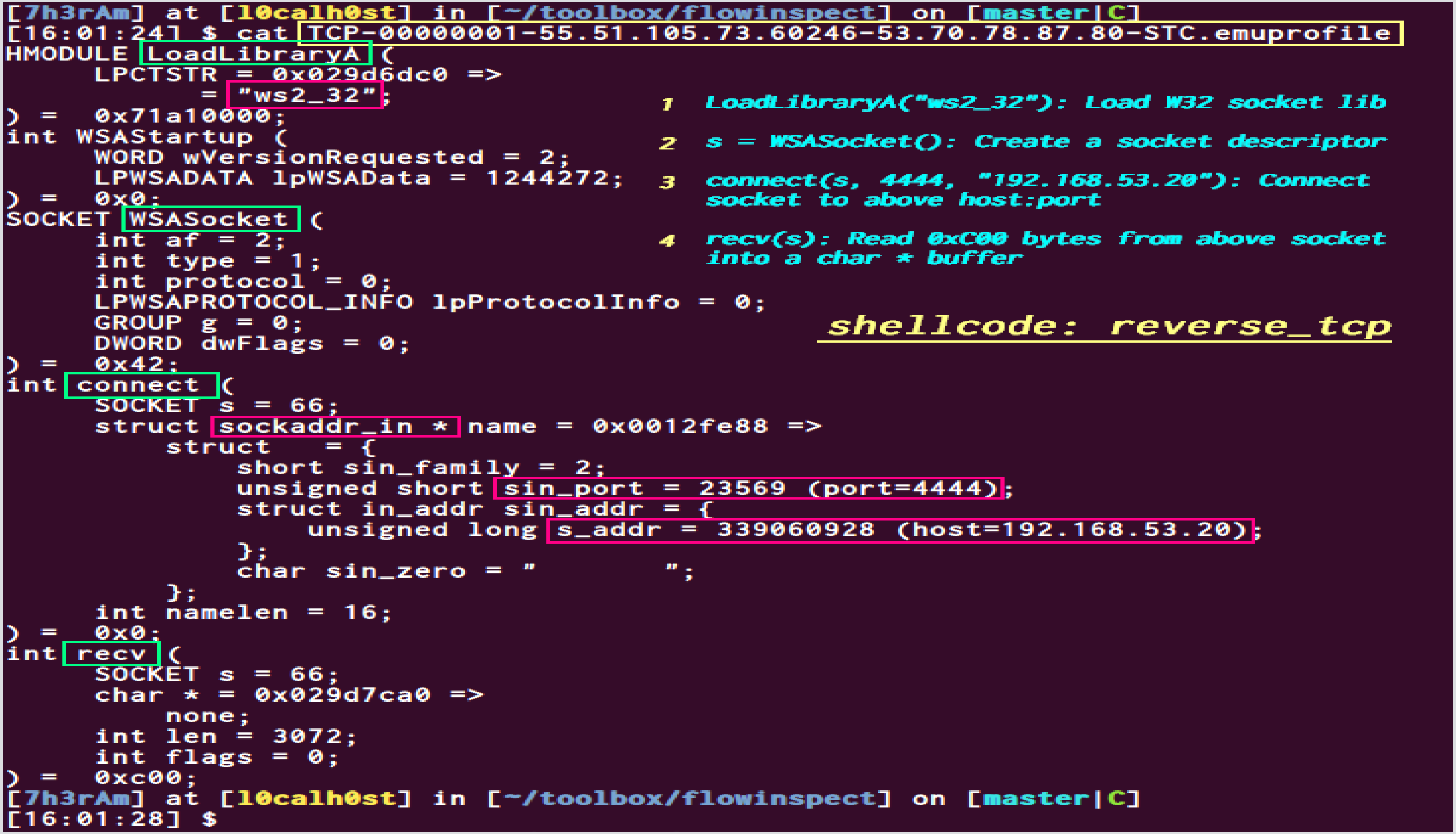
```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:55:18] $ ./flowinspect.py -p ../testfiles/pcaps/shellcode.pcap -Mb128
        ______              _                            __
       / __/ /___ _      __(_)___  _________  ___  _____/ /_
      / /_/ / __ \ | /| / / / __ \/ ___/ __ \/ _ \/ ___/ __/
     / __/ / /_/ / |/ |/ / / / / (__  ) /_/ /  __/ /__/ /_
    /_/ /_/\____/|__/|__/_/_/ /_/____/ .___/\___/\___/\__/
                                    /_/

          flowinspect - A network inspection tool
          Ankur Tyagi (7h3rAm)

[+] Callback handlers registered
[+] NIDS initialized, waiting for events...

[MATCH] (00000002/00000001) [TCP#00000001] 55.51.105.73:60246 <- 53.70.78.87:80 contains shellcode [Offset: 104]
[MATCH] (00000002/00000001) [TCP#00000001] match @ STC[104:278] (174B | packet[2] - packet[2])
00000000:  e8 f9 ff ff ff 60 31 db 8b 7d 3c 8b 7c 3d 78 01   |.....`1..}<.|=x.|
00000010:  ef 8b 57 20 01 ea 8b 34 9a 01 ee 31 c0 99 ac c1   |..W ...4...1....|
00000020:  ca 0d 01 c2 84 c0 75 f6 43 66 39 ca 75 e3 4b 8b   |......u.Cf9.u.K.|
00000030:  4f 24 01 e9 66 8b 1c 59 8b 4f 1c 01 e9 03 2c 99   |O$..f..Y.O....,.|
00000040:  89 6c 24 1c 61 ff e0 31 db 64 8b 43 30 8b 40 0c   |.l$.a..1.d.C0.@.|
00000050:  8b 70 1c ad 8b 68 08 5e 66 53 66 68 33 32 68 77   |.p...h.^fSfh32hw|
00000060:  73 32 5f 54 66 b9 72 60 ff d6 95 53 53 53 53 43   |s2_Tf.r`...SSSSC|
00000070:  53 43 53 89 e7 66 81 ef 08 02 57 53 66 b9 e7 df   |SCS..f....WSf...|


[U] Processed: 0 | Matches: 0 | Shortest: 0B (#0) | Longest: 0B (#0)
[T] Processed: 1 | Matches: 1 | Shortest: 174B (#1) | Longest: 174B (#1)
[+] Session inspection complete. Exiting.
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[15:55:28] $
```

Shellcode Inspection Mode:

-M : ANY direction shellcode detection

-y : Enable profiling output

Flowinspect: Architecture



```
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[16:01:24] $ cat TCP-00000001-55.51.105.73.60246-53.70.78.87.80-STC.emuprofile
HMODULE LoadLibraryA (
     LPCTSTR = 0x029d6dc0 =>
           = "ws2_32";
) =  0x71a10000;
int WSAStartup (
     WORD wVersionRequested = 2;
     LPWSADATA lpWSAData = 1244272;
) =  0x0;
SOCKET WSASocket (
     int af = 2;
     int type = 1;
     int protocol = 0;
     LPWSAPROTOCOL_INFO lpProtocolInfo = 0;
     GROUP g = 0;
     DWORD dwFlags = 0;
) =  0x42;
int connect (
     SOCKET s = 66;
     struct sockaddr_in * name = 0x0012fe88 =>
         struct   = {
             short sin_family = 2;
             unsigned short sin_port = 23569 (port=4444);
             struct in_addr sin_addr = {
                 unsigned long s_addr = 339060928 (host=192.168.53.20);
             };
             char sin_zero = "       ";
         };
     int namelen = 16;
) =  0x0;
int recv (
     SOCKET s = 66;
     char * = 0x029d7ca0 =>
         none;
     int len = 3072;
     int flags = 0;
) =  0xc00;
[7h3rAm] at [l0calh0st] in [~/toolbox/flowinspect] on [master|C]
[16:01:28] $
```

1 LoadLibraryA("ws2_32"): Load W32 socket lib

2 s = WSASocket(): Create a socket descriptor

3 connect(s, 4444, "192.168.53.20"): Connect socket to above host:port

4 recv(s): Read 0xC00 bytes from above socket into a char * buffer

shellcode: reverse_tcp

Real-World Usecase Scenarios/ Demo

Future Goals

- Protocol decoders for HTTP, SMTP, POP3, IMAP, etc.
- File extraction and hash based inspection
- Javascript deobfuscation using SpiderMonkey or/and v8
- File format characterization for Jar/PDF/Flash/MS Office/ELF/PE/...
- Integration with online scanners like VirusTotal, Wepawet, Anubis, Jsunpack, etc.
- New ideas, suggestions, bugfixes are all equally welcome

Credits

- Many thanks to the following projects:
  - The Python Community
  - Libnids and Pynids
  - Fuzzywuzzy
  - Yara
  - Libemu and pyLibemu

- FOSS community in general

Q&A

Thanks for your attention