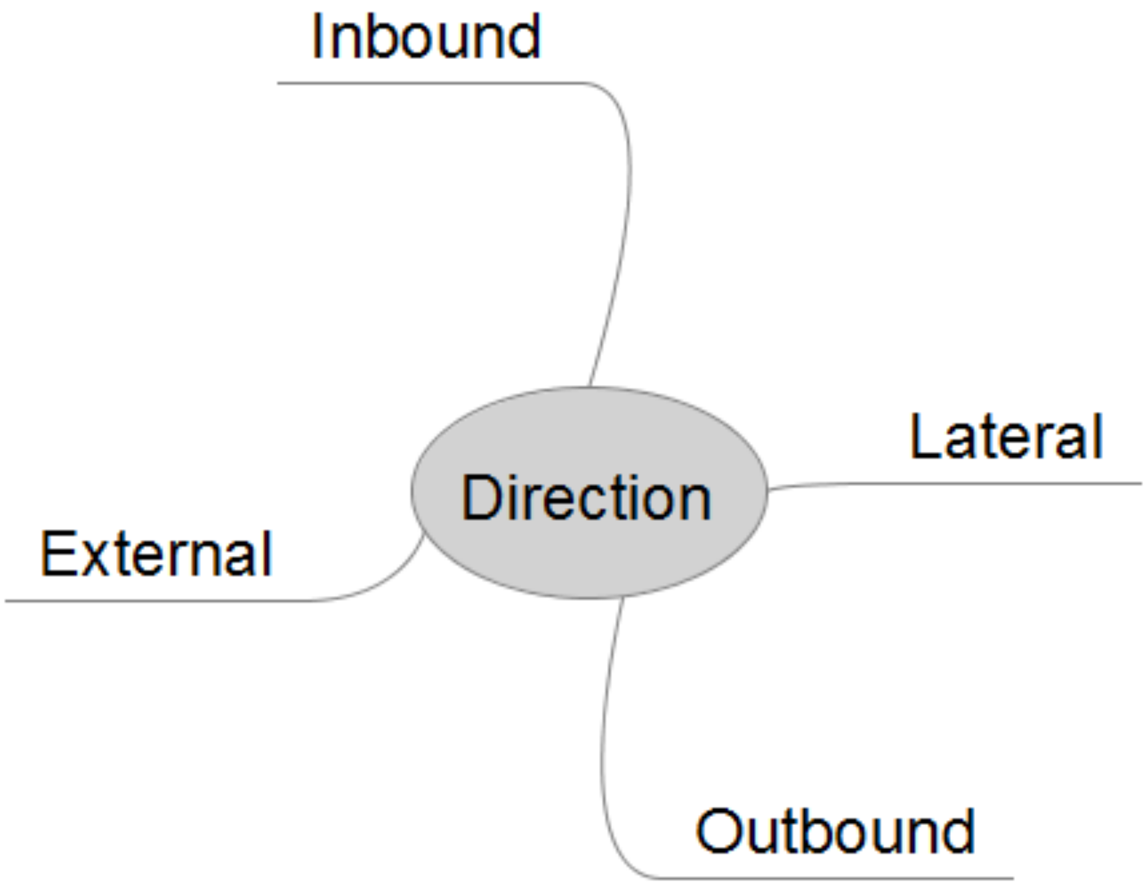
NetWitness Packets Hunting Cheat Sheets

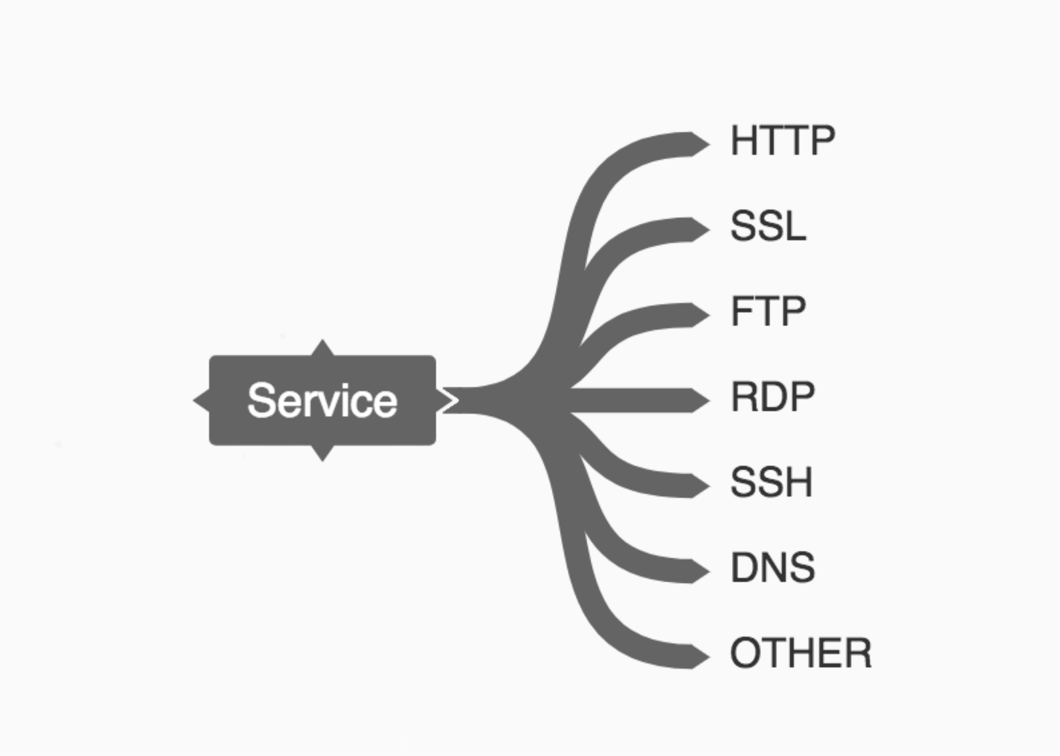
DIRECTIONALITY

- **North / South**
  - Inbound
    - External to DMZ
    - External to Internal
  - Outbound
    - Internal to external
    - Proxy to external
- **East / West**
  - Lateral
    - Internal to DMZ
    - DMZ to Internal
- **External to External**
    - Likely an unknown ‘owned’ network is in
    - Subnet reuse?

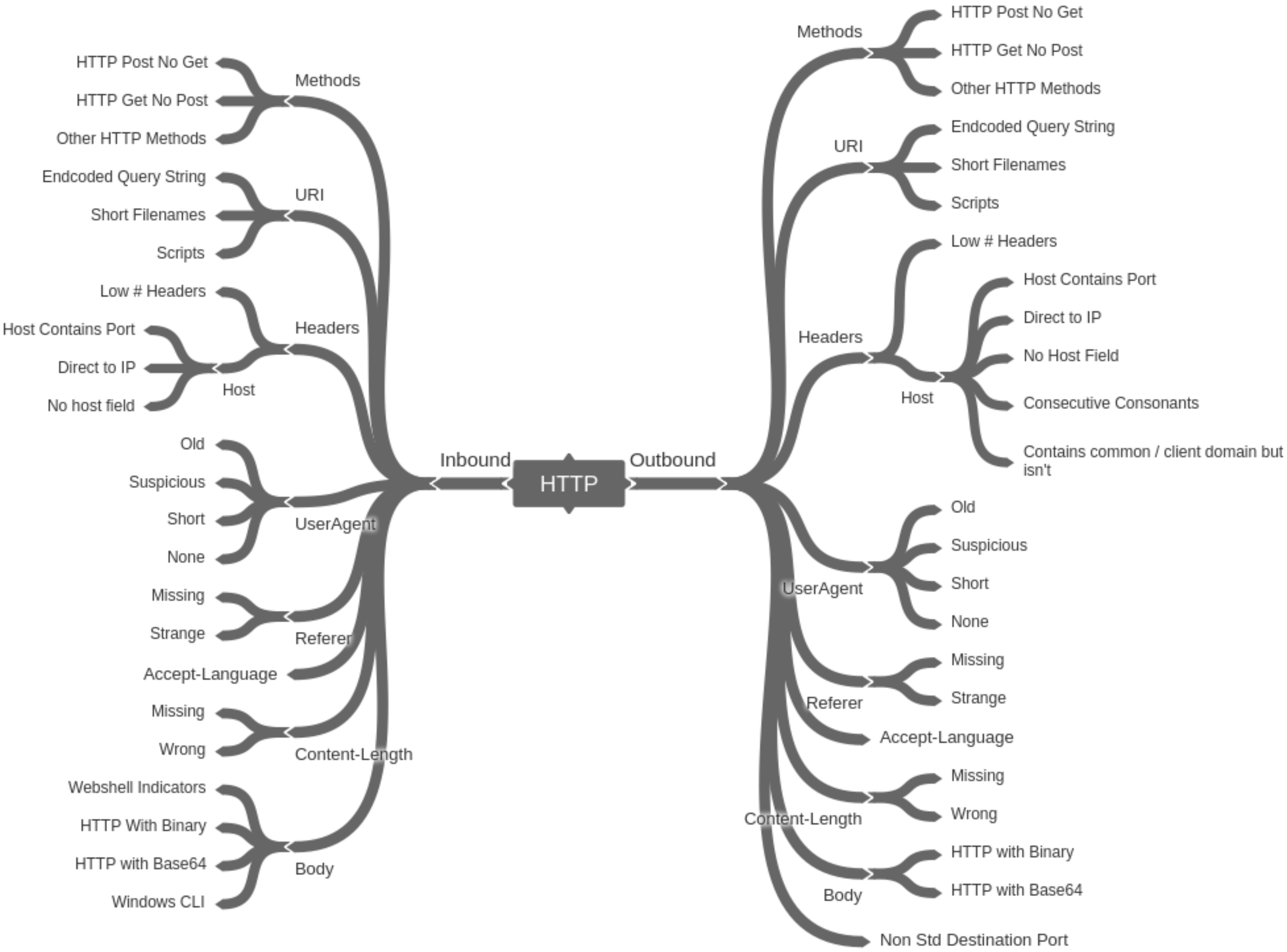


SERVICE

- Requires an analyst to have a plan
  - Focus on One Service at a time
- What are you looking for?
  - Changes depending on directionality / Service
- How does this protocol send and receive data to and from the Internet?
- What aspects of the protocol indicate behavior and how do human requests differ from machine generated requests?
- What legitimate looking requests shouldn't be there?
- Define "normal" traffic and remove it from your view
- Customize meta groups & Column Groups for specific views on each protocol

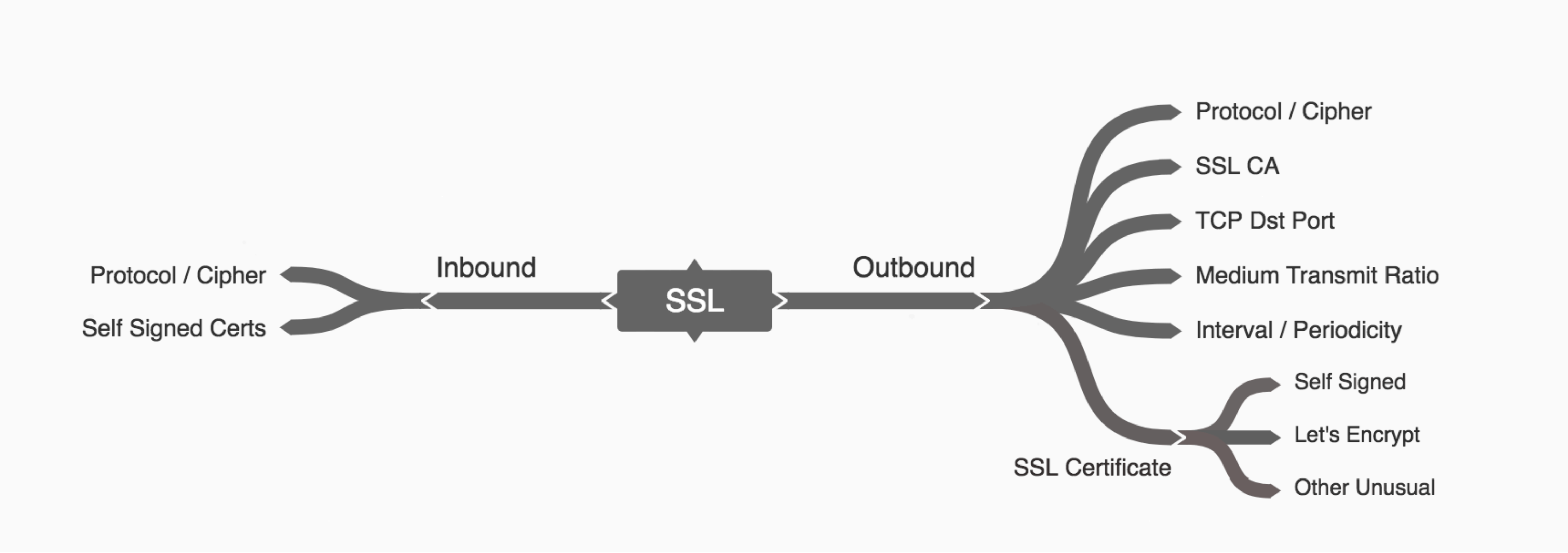


HTTP

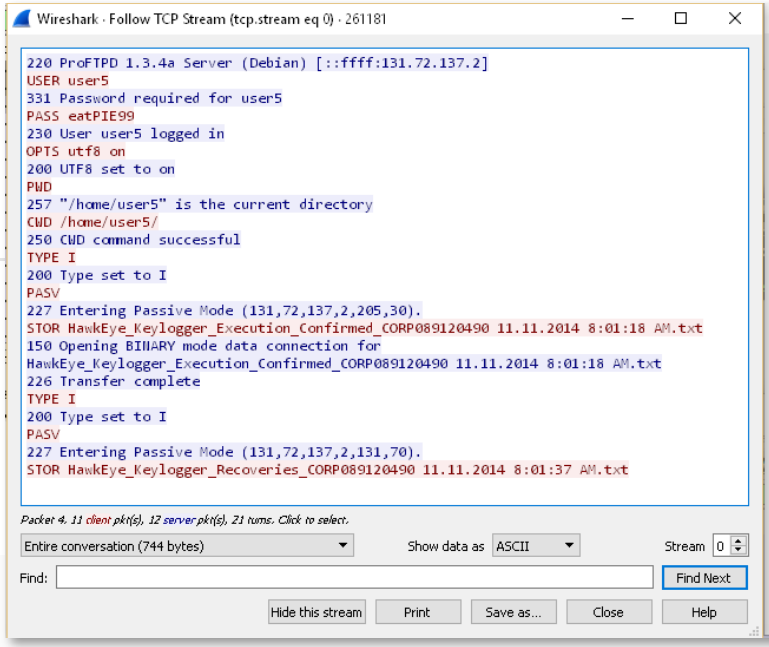


- HTTP
  - Inbound
    - Methods
      - HTTP Post No Get
      - HTTP Get No Post
      - Other HTTP Methods
    - URI
      - Endcoded Query String
      - Short Filenames
      - Scripts
    - Headers
      - Low # Headers
      - Host
        - Host Contains Port
        - Direct to IP
        - No host field
    - UserAgent
      - Old
      - Suspicious
      - Short
      - None
    - Referer
      - Missing
      - Strange
    - Accept-Language
    - Content-Length
      - Missing
      - Wrong
    - Body
      - Webshell Indicators
      - HTTP With Binary
      - HTTP with Base64
      - Windows CLI
  - Outbound
    - Methods
      - HTTP Post No Get
      - HTTP Get No Post
      - Other HTTP Methods
    - URI
      - Endcoded Query String
      - Short Filenames
      - Scripts
    - Headers
      - Low # Headers
      - Host
        - Host Contains Port
        - Direct to IP
        - No Host Field
        - Consecutive Consonants
        - Contains common / client domain but isn't
    - UserAgent
      - Old
      - Suspicious
      - Short
      - None
    - Referer
      - Missing
      - Strange
    - Accept-Language
    - Content-Length
      - Missing
      - Wrong
    - Body
      - HTTP with Binary
      - HTTP with Base64
    - Non Std Destination Port

SSL


Protocol / Cipher
Self Signed Certs
Inbound
SSL
Outbound
Protocol / Cipher
SSL CA
TCP Dst Port
Medium Transmit Ratio
Interval / Periodicity
SSL Certificate
Self Signed
Let's Encrypt
Other Unusual

FTP

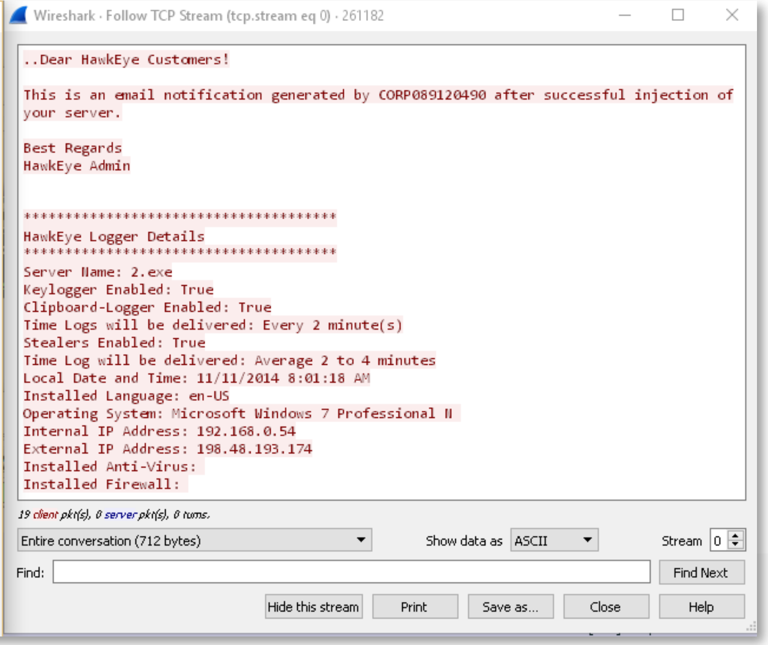


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 261181

```
220 ProFTPD 1.3.4a Server (Debian) [::ffff:131.72.137.2]
USER user5
331 Password required for user5
PASS eatPIE99
230 User user5 logged in
OPTS utf8 on
200 UTF8 set to on
PWD
257 "/home/user5" is the current directory
CWD /home/user5/
250 CWD command successful
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (131,72,137,2,205,30).
STOR HawkEye_Keylogger_Execution_Confirmed_CORP089120490 11.11.2014 8:01:18 AM.txt
150 Opening BINARY mode data connection for
HawkEye_Keylogger_Execution_Confirmed_CORP089120490 11.11.2014 8:01:18 AM.txt
226 Transfer complete
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (131,72,137,2,131,70).
STOR HawkEye_Keylogger_Recoveries_CORP089120490 11.11.2014 8:01:37 AM.txt
```

Packet 4. 11 client pkt(s), 12 server pkt(s), 21 turns. Click to select.

Entire conversation (744 bytes) | Show data as: ASCII | Stream: 0

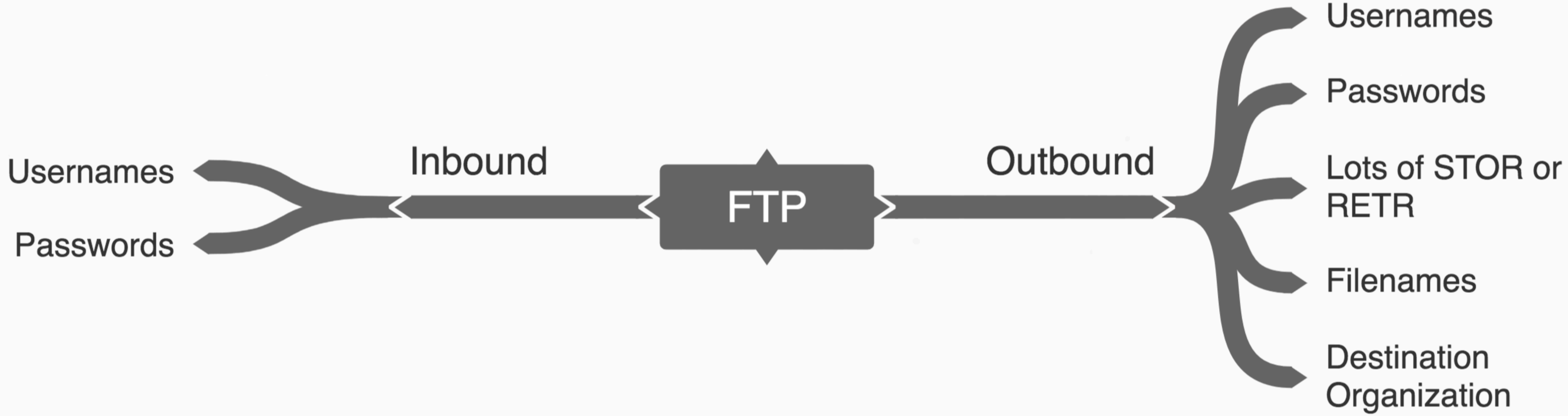


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 261182

```
..Dear HawkEye Customers!

This is an email notification generated by CORP089120490 after successful injection of
your server.

Best Regards
HawkEye Admin


**************************************
HawkEye Logger Details
**************************************
Server Name: 2.exe
Keylogger Enabled: True
Clipboard-Logger Enabled: True
Time Logs will be delivered: Every 2 minute(s)
Stealers Enabled: True
Time Log will be delivered: Average 2 to 4 minutes
Local Date and Time: 11/11/2014 8:01:18 AM
Installed Language: en-US
Operating System: Microsoft Windows 7 Professional N
Internal IP Address: 192.168.0.54
External IP Address: 198.48.193.174
Installed Anti-Virus:
Installed Firewall:
```

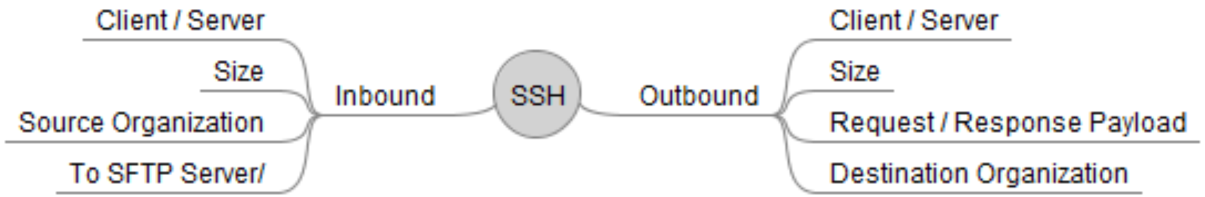
19 client pkt(s), 0 server pkt(s), 0 turns.

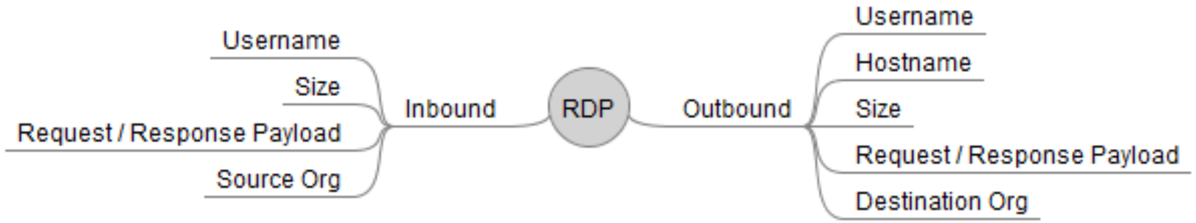
Entire conversation (712 bytes) | Show data as: ASCII | Stream: 0



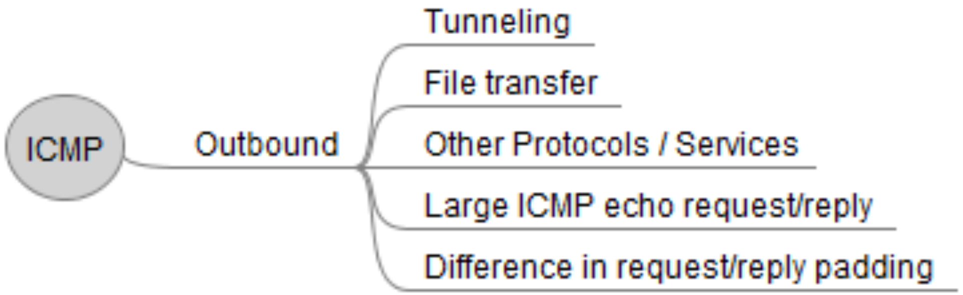
RDP and SSH

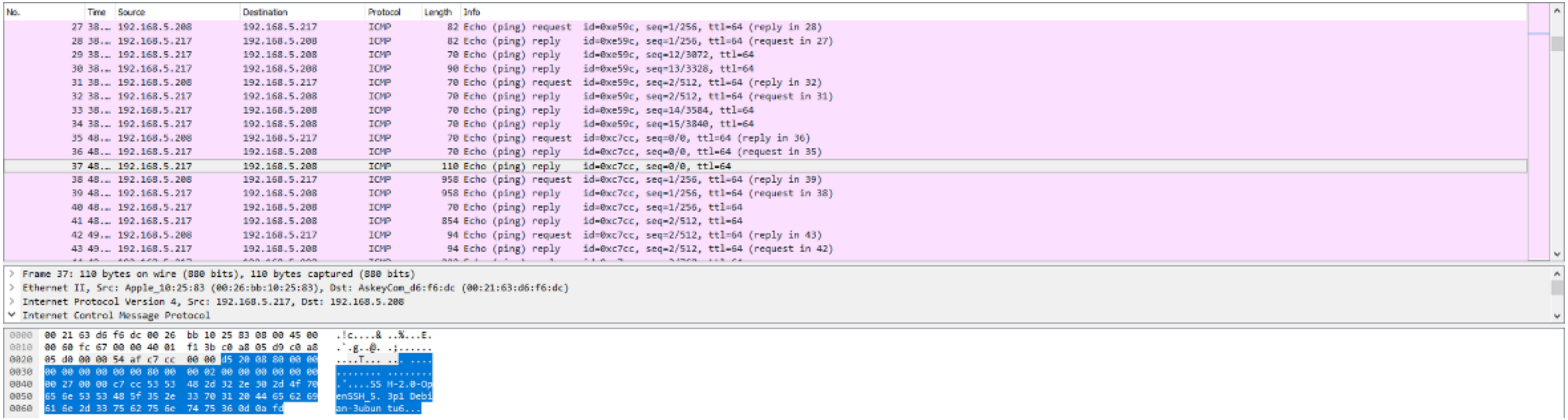
- Both encrypted by default , RDP encryption available starting with 5.2+ in Win 2K3
- SSH declares client , server and encryption algorithm + HMAC in clear text
- RDP may show username and hostname
- Use similar tactics as SSL with SSH, although SSH port forwarding from can be one off access
- Pivot into odd, lone SSH sessions and find host that made them, investigate from there
- Use session size and request/response payload to find large transmitters/receivers and pivot to those hosts, source and destination
- Find the organizations DMZ’s [inbound web traffic should lead you to the network] and look for SSH/RDP from those machines to the internal network





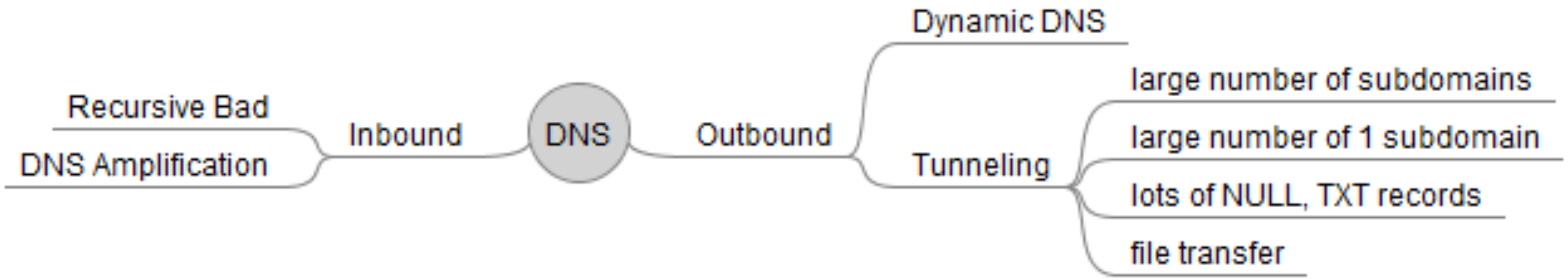
ICMP

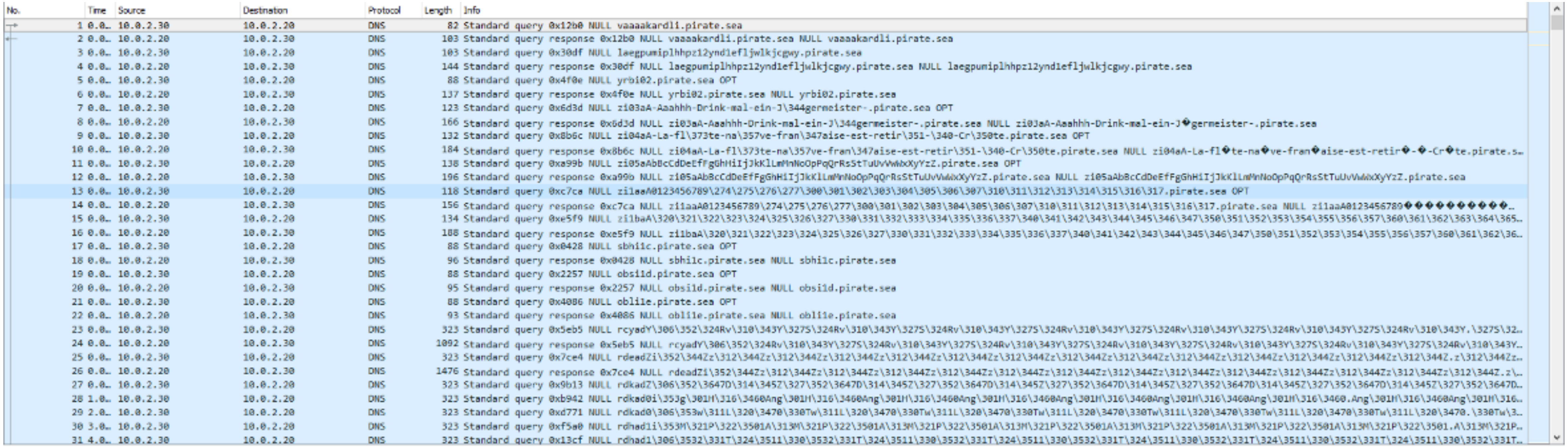

ICMP
Outbound
Tunneling
File transfer
Other Protocols / Services
Large ICMP echo request/reply
Difference in request/reply padding



```
No.   Time   Source          Destination     Protocol  Length Info
   27 38...  192.168.5.208   192.168.5.217   ICMP        82 Echo (ping) request  id=0xe59c, seq=1/256, ttl=64 (reply in 28)
   28 38...  192.168.5.217   192.168.5.208   ICMP        82 Echo (ping) reply    id=0xe59c, seq=1/256, ttl=64 (request in 27)
   29 38...  192.168.5.217   192.168.5.208   ICMP        70 Echo (ping) reply    id=0xe59c, seq=12/3072, ttl=64
   30 38...  192.168.5.217   192.168.5.208   ICMP        90 Echo (ping) reply    id=0xe59c, seq=13/3328, ttl=64
   31 38...  192.168.5.208   192.168.5.217   ICMP        70 Echo (ping) request  id=0xe59c, seq=2/512, ttl=64 (reply in 32)
   32 38...  192.168.5.217   192.168.5.208   ICMP        70 Echo (ping) reply    id=0xe59c, seq=2/512, ttl=64 (request in 31)
   33 38...  192.168.5.217   192.168.5.208   ICMP        70 Echo (ping) reply    id=0xe59c, seq=14/3584, ttl=64
   34 38...  192.168.5.217   192.168.5.208   ICMP        70 Echo (ping) reply    id=0xe59c, seq=15/3840, ttl=64
   35 48...  192.168.5.208   192.168.5.217   ICMP        70 Echo (ping) request  id=0xc7cc, seq=0/0, ttl=64 (reply in 36)
   36 48...  192.168.5.217   192.168.5.208   ICMP        70 Echo (ping) reply    id=0xc7cc, seq=0/0, ttl=64 (request in 35)
   37 48...  192.168.5.217   192.168.5.208   ICMP       110 Echo (ping) reply    id=0xc7cc, seq=0/0, ttl=64
   38 48...  192.168.5.208   192.168.5.217   ICMP       958 Echo (ping) request  id=0xc7cc, seq=1/256, ttl=64 (reply in 39)
   39 48...  192.168.5.217   192.168.5.208   ICMP       958 Echo (ping) reply    id=0xc7cc, seq=1/256, ttl=64 (request in 38)
   40 48...  192.168.5.217   192.168.5.208   ICMP        70 Echo (ping) reply    id=0xc7cc, seq=1/256, ttl=64
   41 48...  192.168.5.217   192.168.5.208   ICMP       854 Echo (ping) reply    id=0xc7cc, seq=2/512, ttl=64
   42 49...  192.168.5.208   192.168.5.217   ICMP        94 Echo (ping) request  id=0xc7cc, seq=2/512, ttl=64 (reply in 43)
   43 49...  192.168.5.217   192.168.5.208   ICMP        94 Echo (ping) reply    id=0xc7cc, seq=2/512, ttl=64 (request in 42)

> Frame 37: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Ethernet II, Src: Apple_10:25:83 (00:26:bb:10:25:83), Dst: AskeyCom_d6:f6:dc (00:21:63:d6:f6:dc)
> Internet Protocol Version 4, Src: 192.168.5.217, Dst: 192.168.5.208
v Internet Control Message Protocol

0000  00 21 63 d6 f6 dc 00 26  bb 10 25 83 08 00 45 00   .!c....& ..%...E.
0010  00 60 fc 67 00 00 40 01  f1 3b c0 a8 05 d9 c0 a8   .`.g..@. .;......
0020  05 d0 00 00 54 af c7 cc  00 00 d5 20 08 80 00 00   ....T... .. ....
0030  00 00 00 00 00 00 80 00  00 02 00 00 00 00 00 00   ........ ........
0040  00 27 00 00 c7 cc 53 53  48 2d 32 2e 30 2d 4f 70   .'....SS H-2.0-Op
0050  65 6e 53 53 48 5f 35 2e  33 70 31 20 44 65 62 69   enSSH_5. 3p1 Debi
0060  61 6e 2d 33 75 62 75 6e  74 75 36 0d 0a fd         an-3ubun tu6...
```

DNS



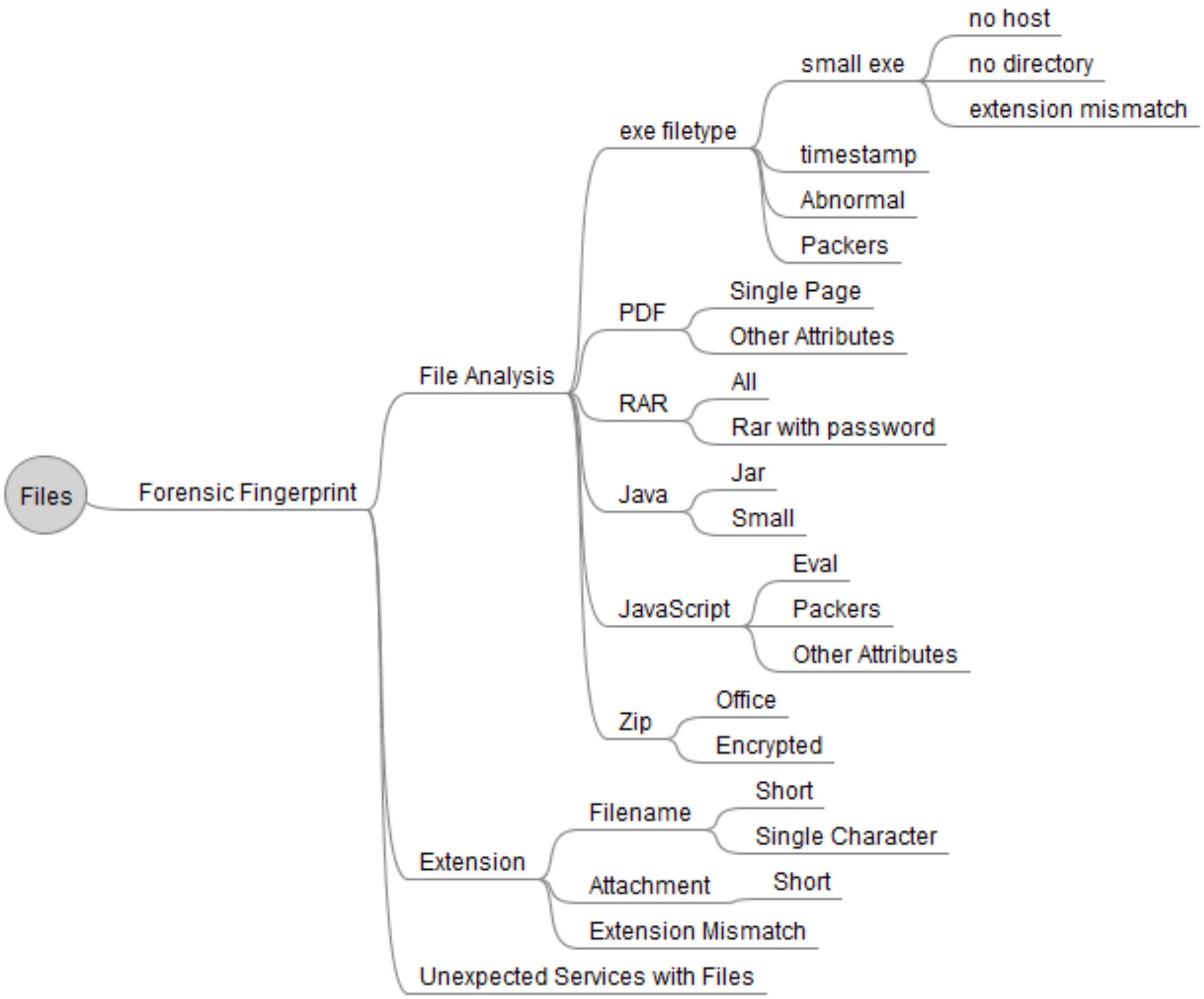


```
No.    Time  Source     Destination  Protocol  Length  Info
   1 0.0… 10.0.2.30  10.0.2.20  DNS    82 Standard query 0x12b0 NULL vaaaakardli.pirate.sea
   2 0.0… 10.0.2.20  10.0.2.30  DNS   103 Standard query response 0x12b0 NULL vaaaakardli.pirate.sea NULL vaaaakardli.pirate.sea
   3 0.0… 10.0.2.30  10.0.2.20  DNS   103 Standard query 0x30df NULL laegpumiplhhpz12ynd1efljwlkjcgwy.pirate.sea
   4 0.0… 10.0.2.20  10.0.2.30  DNS   144 Standard query response 0x30df NULL laegpumiplhhpz12ynd1efljwlkjcgwy.pirate.sea NULL laegpumiplhhpz12ynd1efljwlkjcgwy.pirate.sea
   5 0.0… 10.0.2.30  10.0.2.20  DNS    88 Standard query 0x4f0e NULL yrbi02.pirate.sea OPT
   6 0.0… 10.0.2.20  10.0.2.30  DNS   137 Standard query response 0x4f0e NULL yrbi02.pirate.sea NULL yrbi02.pirate.sea
   7 0.0… 10.0.2.30  10.0.2.20  DNS   123 Standard query 0x6d3d NULL zi03aA-Aaahhh-Drink-mal-ein-J\344germeister-.pirate.sea OPT
   8 0.0… 10.0.2.20  10.0.2.30  DNS   166 Standard query response 0x6d3d NULL zi03aA-Aaahhh-Drink-mal-ein-J\344germeister-.pirate.sea NULL zi03aA-Aaahhh-Drink-mal-ein-J�germeister-.pirate.sea
   9 0.0… 10.0.2.30  10.0.2.20  DNS   132 Standard query 0x8b6c NULL zi04aA-La-fl\373te-na\357ve-fran\347aise-est-retir\351-\340-Cr\350te.pirate.sea OPT
  10 0.0… 10.0.2.20  10.0.2.30  DNS   184 Standard query response 0x8b6c NULL zi04aA-La-fl\373te-na\357ve-fran\347aise-est-retir\351-\340-Cr\350te.pirate.sea NULL zi04aA-La-fl�te-na�ve-fran�aise-est-retir�-�-Cr�te.pirate.s…
  11 0.0… 10.0.2.30  10.0.2.20  DNS   138 Standard query 0xa99b NULL zi05aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ.pirate.sea OPT
  12 0.0… 10.0.2.20  10.0.2.30  DNS   196 Standard query response 0xa99b NULL zi05aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ.pirate.sea NULL zi05aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ.pirate.sea
  13 0.0… 10.0.2.30  10.0.2.20  DNS   118 Standard query 0xc7ca NULL zi1aaA0123456789\274\275\276\277\300\301\302\303\304\305\306\307\310\311\312\313\314\315\316\317.pirate.sea OPT
  14 0.0… 10.0.2.20  10.0.2.30  DNS   156 Standard query response 0xc7ca NULL zi1aaA0123456789\274\275\276\277\300\301\302\303\304\305\306\307\310\311\312\313\314\315\316\317.pirate.sea NULL zi1aaA0123456789����������…
  15 0.0… 10.0.2.30  10.0.2.20  DNS   134 Standard query 0xe5f9 NULL zi1baA\320\321\322\323\324\325\326\327\330\331\332\333\334\335\336\337\340\341\342\343\344\345\346\347\350\351\352\353\354\355\356\357\360\361\362\363\364\365…
  16 0.0… 10.0.2.20  10.0.2.30  DNS   188 Standard query response 0xe5f9 NULL zi1baA\320\321\322\323\324\325\326\327\330\331\332\333\334\335\336\337\340\341\342\343\344\345\346\347\350\351\352\353\354\355\356\357\360\361\362\36…
  17 0.0… 10.0.2.30  10.0.2.20  DNS    88 Standard query 0x0428 NULL sbhi1c.pirate.sea OPT
  18 0.0… 10.0.2.20  10.0.2.30  DNS    96 Standard query response 0x0428 NULL sbhi1c.pirate.sea NULL sbhi1c.pirate.sea
  19 0.0… 10.0.2.30  10.0.2.20  DNS    88 Standard query 0x2257 NULL obsi1d.pirate.sea OPT
  20 0.0… 10.0.2.20  10.0.2.30  DNS    95 Standard query response 0x2257 NULL obsi1d.pirate.sea NULL obsi1d.pirate.sea
  21 0.0… 10.0.2.30  10.0.2.20  DNS    88 Standard query 0x4086 NULL obli1e.pirate.sea OPT
  22 0.0… 10.0.2.20  10.0.2.30  DNS    93 Standard query response 0x4086 NULL obli1e.pirate.sea NULL obli1e.pirate.sea
  23 0.0… 10.0.2.30  10.0.2.20  DNS   323 Standard query 0x5eb5 NULL rcyadY\306\352\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y.\327S\32…
  24 0.0… 10.0.2.20  10.0.2.30  DNS  1092 Standard query response 0x5eb5 NULL rcyadY\306\352\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y\327S\324Rv\310\343Y…
  25 0.0… 10.0.2.30  10.0.2.20  DNS   323 Standard query 0x7ce4 NULL rdeadZi\352\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Z.z\312\344Zz…
  26 0.0… 10.0.2.20  10.0.2.30  DNS  1476 Standard query response 0x7ce4 NULL rdeadZi\352\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Zz\312\344Z.z\…
  27 0.0… 10.0.2.30  10.0.2.20  DNS   323 Standard query 0x9b13 NULL rdkadZ\306\352\3647D\314\345Z\327\352\3647D\314\345Z\327\352\3647D\314\345Z\327\352\3647D\314\345Z\327\352\3647D\314\345Z\327\352\3647D\314\345Z\327\352\3647D…
  28 1.0… 10.0.2.30  10.0.2.20  DNS   323 Standard query 0xb942 NULL rdkad0i\353g\301M\316\3460Ang\301M\316\3460Ang\301M\316\3460Ang\301M\316\3460Ang\301M\316\3460Ang\301M\316\3460Ang\301M\316\3460.Ang\301M\316\3460Ang\301M\316…
  29 2.0… 10.0.2.30  10.0.2.20  DNS   323 Standard query 0xd771 NULL rdkad0\306\353w\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470\330Tw\311L\320\3470.\330Tw\3…
  30 3.0… 10.0.2.30  10.0.2.20  DNS   323 Standard query 0xf5a0 NULL rdhad1i\353M\321P\322\3501A\313M\321P\322\3501A\313M\321P\322\3501A\313M\321P\322\3501A\313M\321P\322\3501A\313M\321P\322\3501A\313M\321P\322\3501.A\313M\321P…
  31 4.0… 10.0.2.30  10.0.2.20  DNS   323 Standard query 0x13cf NULL rdhad1\306\3532\331T\324\3511\330\3532\331T\324\3511\330\3532\331T\324\3511\330\3532\331T\324\3511\330\3532\331T\324\3511\330\3532\331T\324\3511\330\3532\331T…
```

DNS

FIles

- Analysis.file
- Filetype
  - (Forensic Fingerprint)
- Extension
- Filename
- Attachment
- Combine with Service



Service Type Other

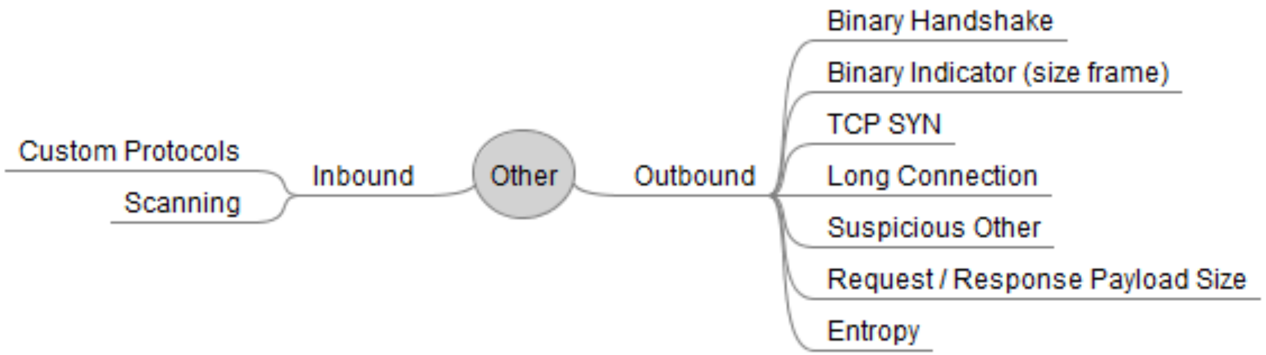
Binary_Streams.lua

- Reads first 256 bytes of request and response streams
- If the combined 512 bytes has more than 310 non-ASCII printable bytes, it fires in Binary_Handshake
- Pair with first_carve_!dns and Other traffic, look for beaconing, counts, SYN beaconing followed by successful connections

Binary_Indicators.lua

- Reads the first 8 bytes of a request stream and compares the value of each byte to the payload frame size for that packet.
- Reads the first 16 bytes of a request stream and compares each word to the payload frame size and then does the same but reads the word in Little Endian
- If either of these conditions match it fires Binary_Indicator

long connection	A session with a lifetime > 30 seconds
suspicious other	A TCP session with a service type of OTHER, payload > 0 and the TCP_SYN flag was seen



Custom Protocols
Scanning
Inbound
Other
Outbound
Binary Handshake
Binary Indicator (size frame)
TCP SYN
Long Connection
Suspicious Other
Request / Response Payload Size
Entropy