Writing IDS Signatures for Suricata and Snort

Jack Mott and Jason Williams

Who are we?

Jack Mott

- Security Research Analyst
  - Emerging Threats now part of Proofpoint
- Malware analysis
  - Ransomware and exploit kits are my favorite
- IDS Signature development
  - ETPRO/OPEN Rulesets
- ClamAV Signature Development
- OISF Core Training Team Member

Jae Williams

- Security Research Analyst
  - Emerging Threats now part of Proofpoint
- Malware analysis
  - Oddball targeted/exploit/vuln stuff
- IDS Signature development
  - ETPRO/OPEN Rulesets
- Phishing
- OISF Core Training Team Member

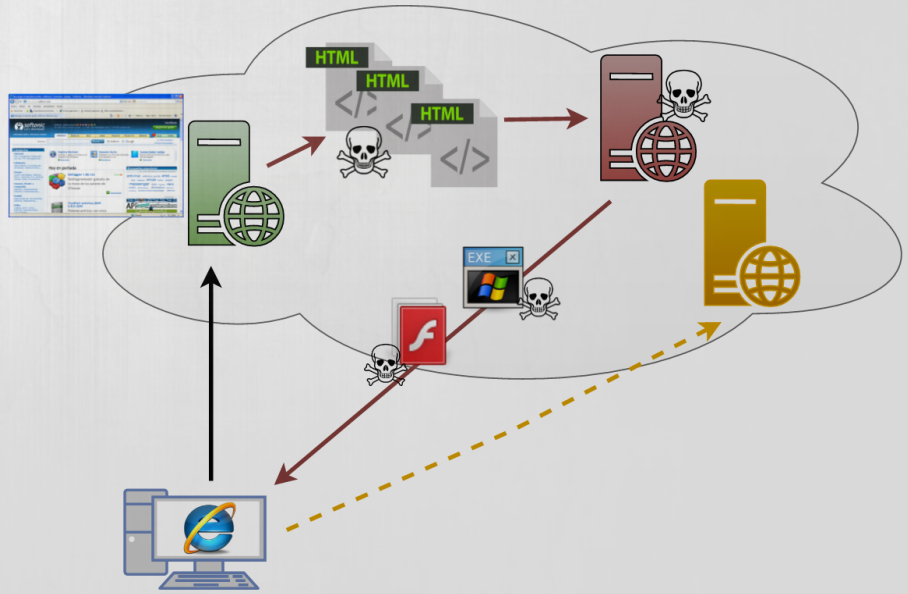
What is the point of this?

- Introduction to IDS rule language
- Be comfortable interpreting IDS rules
- Feel empowered to write IDS rules
- Be knowledgeable on detecting threats on the network

Network Analysis Basics

Network Traffic Analysis

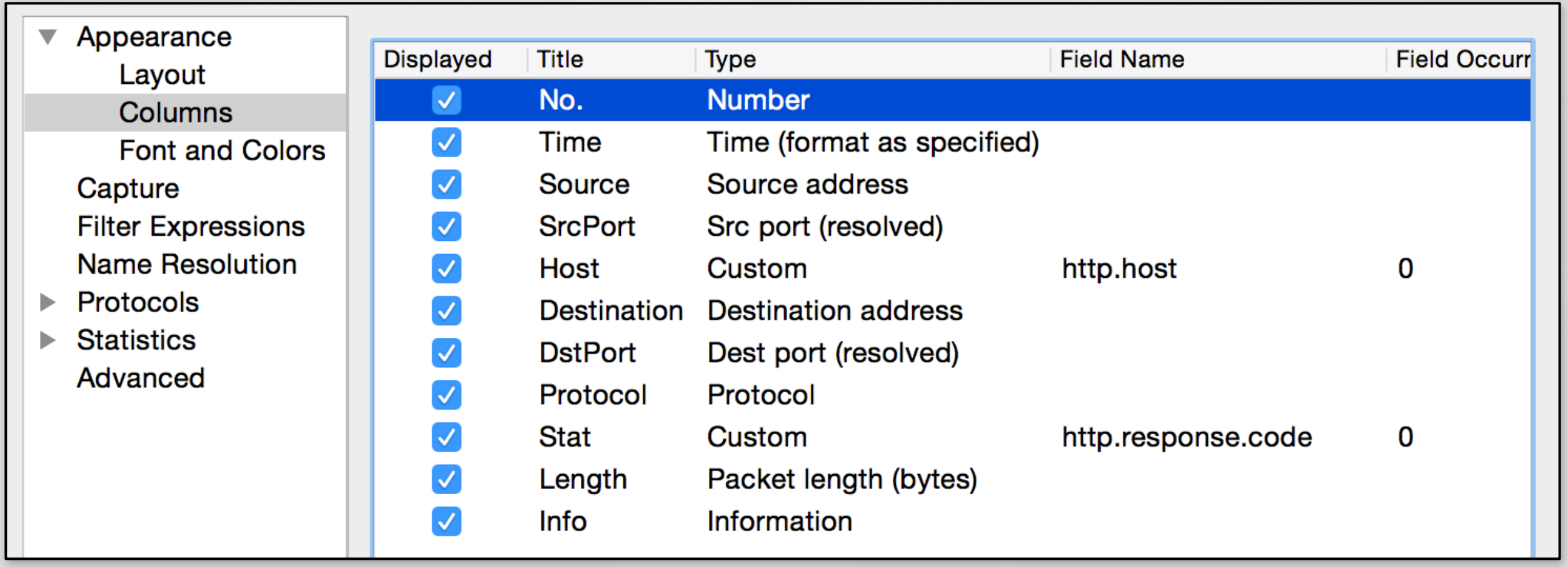
- A basic understanding of TCP/IP
- Not enough time to dig into low-level stuff here
- We can talk about some tools
- Basic network traffic analysis techniques



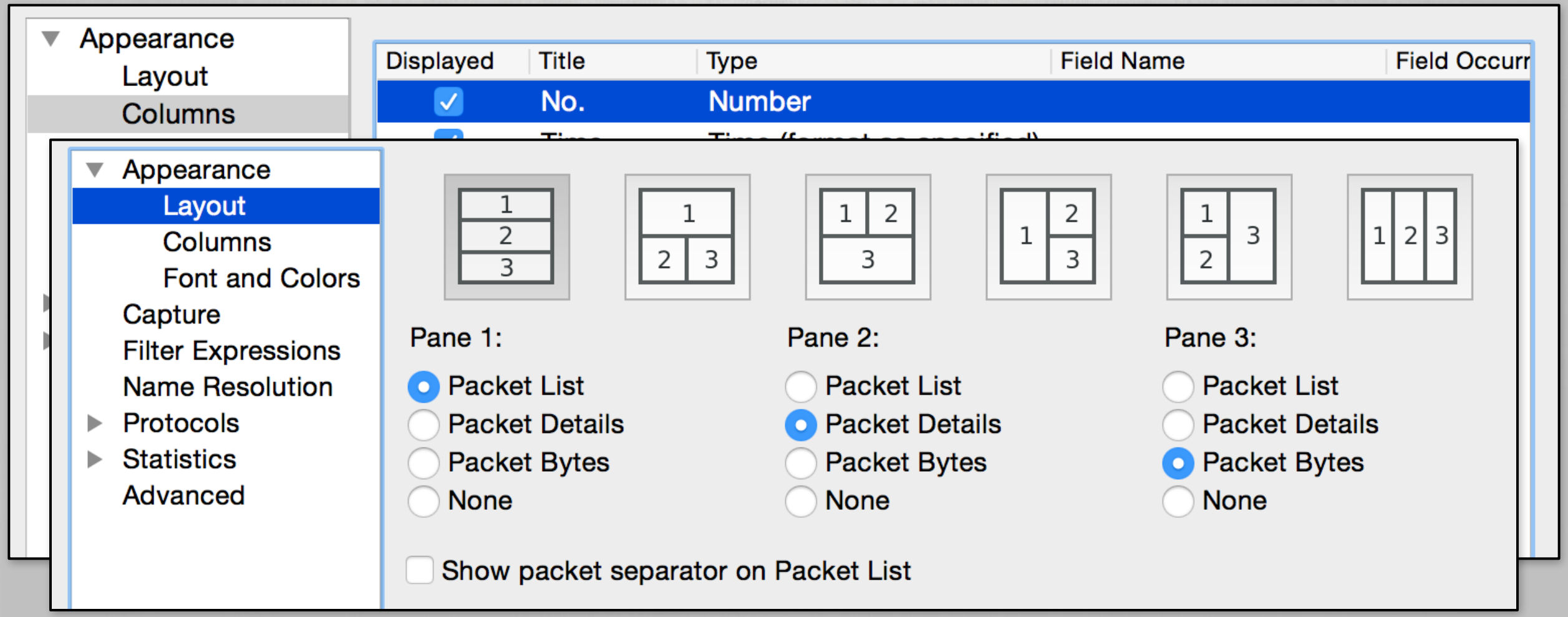
Wireshark

- The best tool out there for graphical packet analysis
- Views & Column Layout
- Wireshark -> Preferences
- Arrange and edit columns for viewing packet data
  - Ability to add custom fields by clicking “+” and entering a filter (e.g http.response.code)
  - Arrange packet data layout for ease of analysis under “Layout” and chose a configuration

Wireshark - Appearance

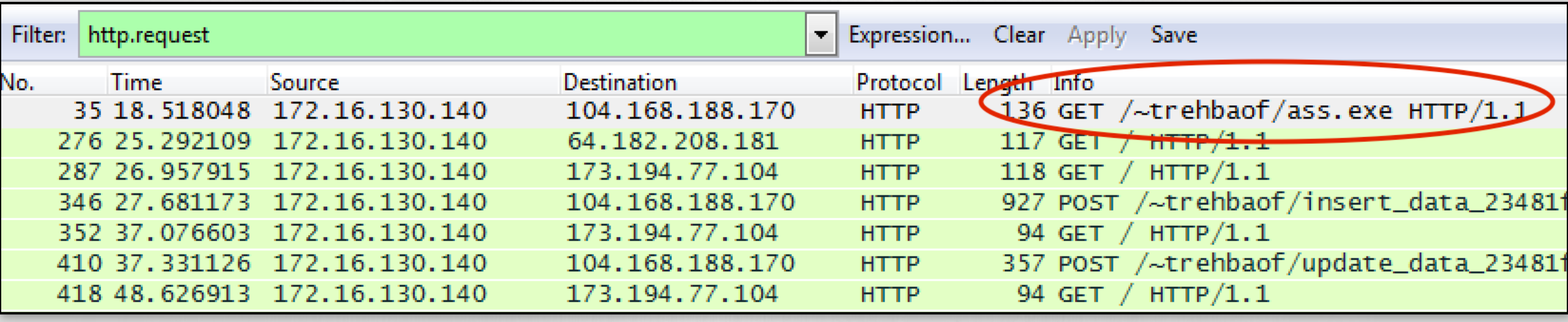


Wireshark - Appearance - Layout

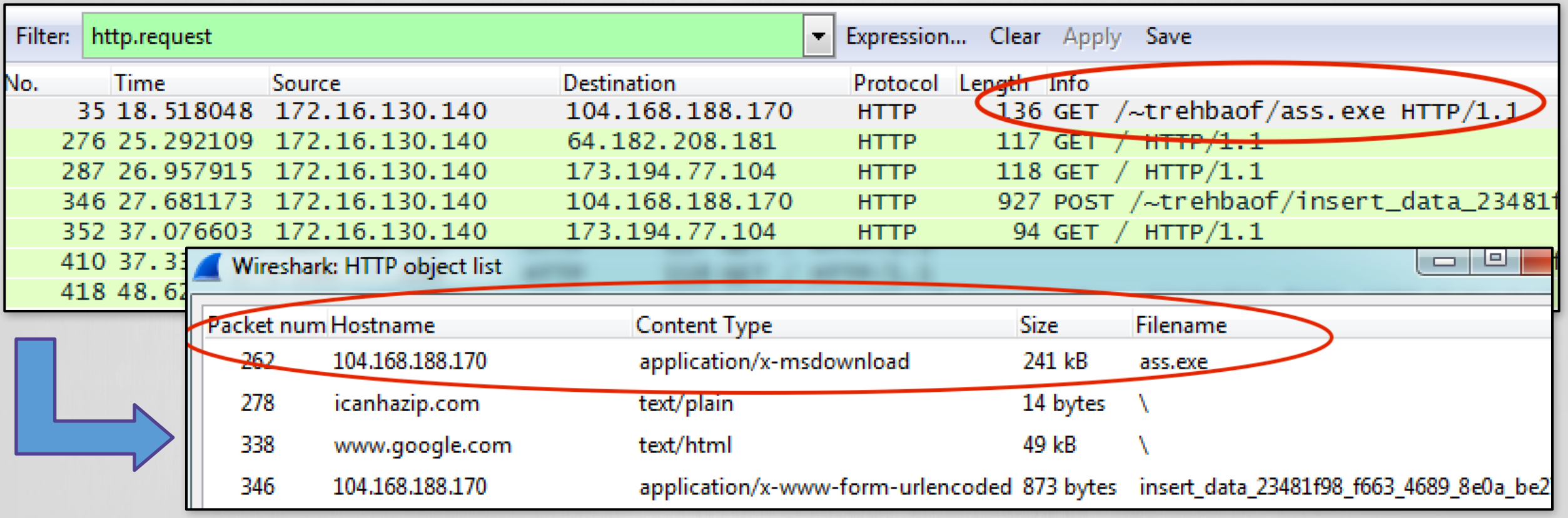


Wireshark - File Extraction (1)

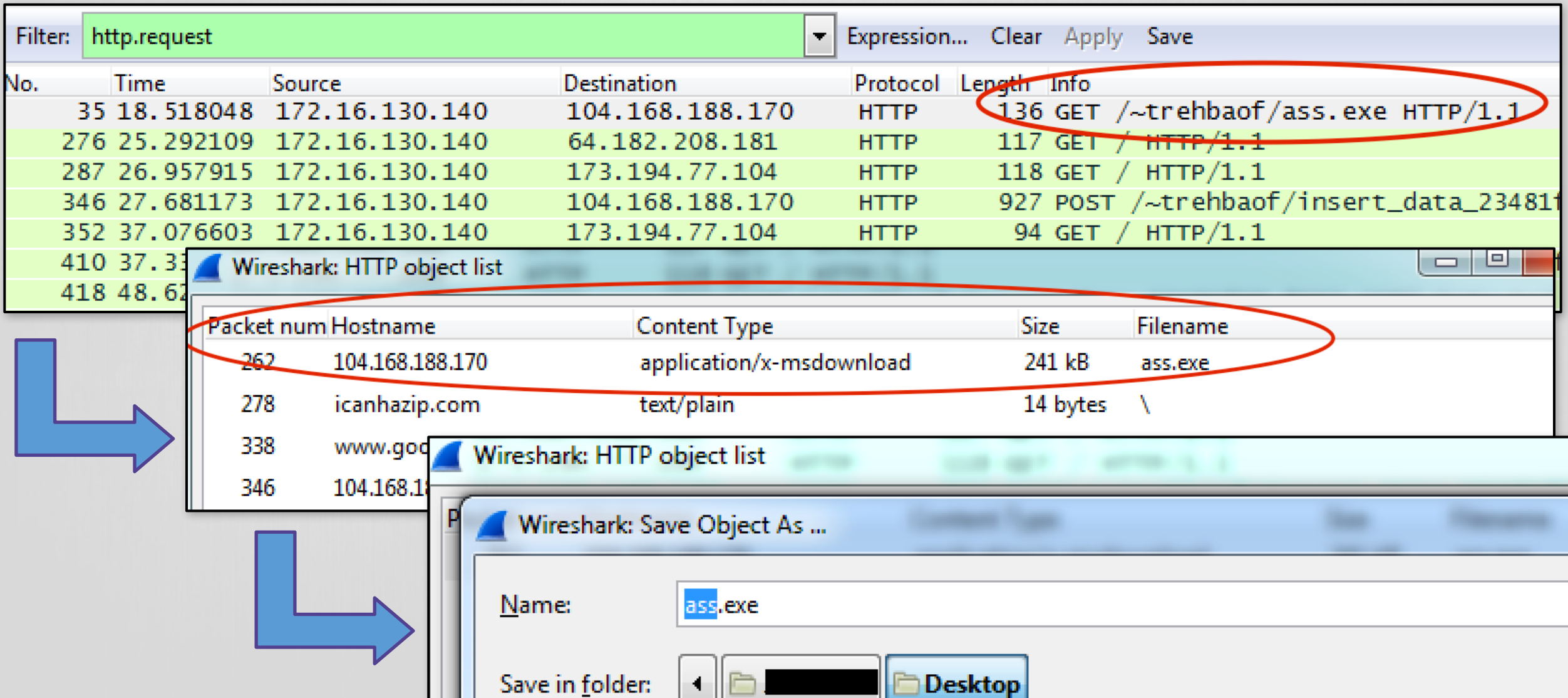
Built in ability to parse PCAP for known HTTP, SMB/2, DICOM and TFTP objects (File -> Export Objects)



Wireshark - File Extraction (2)

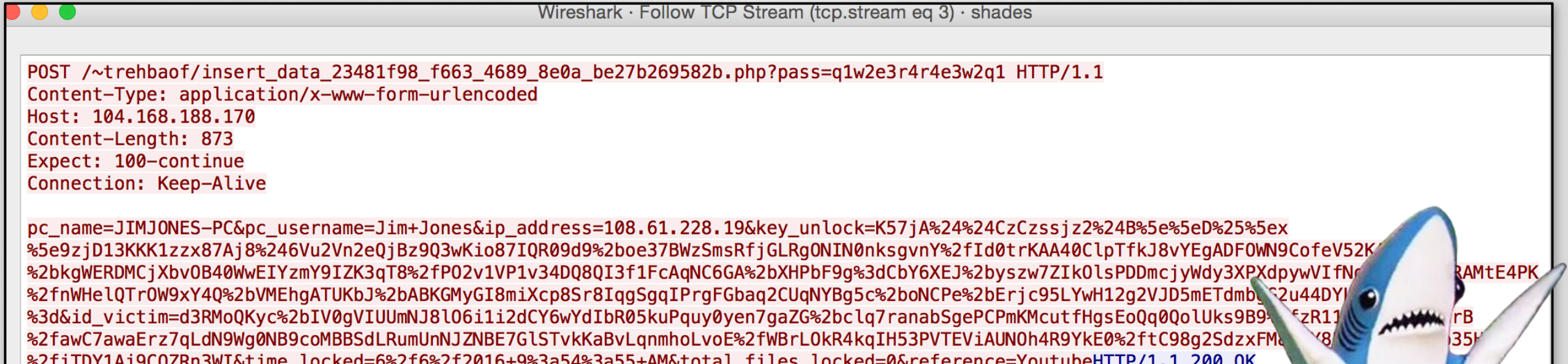


Wireshark - File Extraction (3)



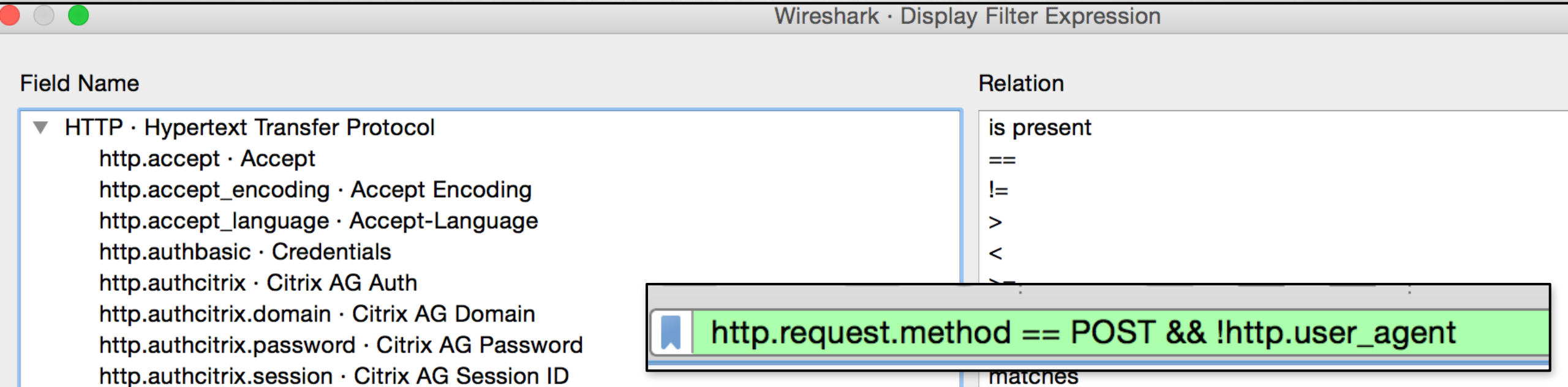
Wireshark - Following Streams

- Ability to assemble TCP/HTTP streams to view session data
- Default view is ASCII, can change to Hex (useful) and other encodings
- Right click packet of interest -> Follow -> TCP (HTTP) Stream



Wireshark - Filters

- Filters are entered in the top bar and are limited to specific search parameters
- Can use qualifiers like &&, !=, ==, ||, <=, =>



Network Analysis

- Use tools to your advantage - NSM!
- Proactive detection is hard, but can be fruitful
- Use your day-one knowledge of pattern recognition to your advantage!
- Look at small datasets and refine as you increase the size
- Baseline, baseline, baseline (do your best…)

Why IDS/IPS?

- Still an extremely valuable tool in your arsenal
- Applicable when discussing defense in depth
- Not perfect
- Provide context
- What can full PCAP provide?

IDS Rule Theory

- Generally, we want agile but effective rules
  - Don’t be like generic AV names and hash-based detections
- Specific enough to capture desired traffic without False Negatives
- Loose enough to capture variants without False Positives
- Balance!
- Won’t always work this way ☹️

IDS Landscape

- **Suricata** (https://suricata-ids.org/)
  - Open-source, community driven
  - Multi-threaded for fast performance
  - Robust protocol identification (can parse HTTP on off-ports, etc)
  - More than just IDS - NSM! Lua! File Extraction!

- **Snort** (https://snort.org/)
  - Most influential IDS developed
  - Open-source
  - Developed/maintained by Sourcefire, now part of Cisco/Talos

- http://suricata.readthedocs.io/en/latest/rules/differences-from-snort.html

A word about (the common) rulesets

Emerging Threats

- ET OPEN
  - https://rules.emergingthreats.net/open/
- ETPRO
  - Paid

Talos (Cisco/VRT/Snort)

- Community
  - https://snort.org/downloads/#rule-downloads
- Snort Subscriber Ruleset
  - Paid

What is an IDS rule?

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=sdJoFsAv3jSNMEYxHTTP/1.1 200 OK
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 186
Connection: close
Content-Type: text/html

MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
<!-- End Of Analytics Code -->
```

What is an IDS rule?

Suricata
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"DetoxCrypto Ransomware CnC Activity"; flow:established,to_server; content:"POST"; http_method; content:"/generate.php"; http_uri; content:"DetoxCrypto"; fast_pattern; http_user_agent; content:"publickey="; depth:10; http_client_body; content:!"Referer|3a|"; http_header; pcre:"/\.php$/U"; reference:md5,e273508a2f2ed45c20a2412f7d62eceb; classtype:trojan-activity; sid:1000000001; rev:1;)

Snort
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ETPRO TROJAN DetoxCrypto Ransomware CnC Activity"; flow:established,to_server; content:"POST"; http_method; content:"/generate.php"; http_uri; content:"User-Agent|3a 20|DetoxCrypto"; fast_pattern:3,20; http_header; content:"publickey="; depth:10; http_client_body; content:!"Referer|3a|"; http_header; pcre:"/\.php$/U"; reference:md5,e273508a2f2ed45c20a2412f7d62eceb; sid:10000000001; rev:1;)

Rule Foundations

IDS Rule Basic Format

action protocol from_ip port -> to_ip port

(msg:”something"; content:"something";

content:"something else"; sid:10000000; rev:1;)

IDS Rule Basic Format

```
action protocol from_ip port -> to_ip port

(msg:”something"; content:"something";

content:"something else"; sid:10000000; rev:1;)
```

IDS Rule Basic Format

```
action protocol from_ip port -> to_ip port
(msg:”something"; content:"something";
content:"something else"; sid:10000000; rev:1;)
```

IDS Rule Basic Format

action protocol from_ip port -> to_ip port

(msg:”something"; content:"something";

content:"something else"; sid:10000000; rev:1;)

Rule Action

- Tells the IDS engine what to do when traffic matches this rule
- alert
  - Generate alert, and log matching packets, but let the traffic through
- log
  - Log traffic– no alert
- pass
  - Ignore the packet, allow it through
- drop
  - If IPS mode, sensor should drop the offending packet
- reject
  - IDS will send TCP reset packet

Rule Action

- Tells the IDS engine what to do when traffic matches this rule
- alert
  - Generate alert, and log matching packets, but let the traffic through

```
action protocol from_ip port -> to_ip port (msg:"something";

content:"something"; content:"something else"; sid:10000000; rev:1;)
```

  - If IPS mode, sensor should drop the offending packet
- reject
  - IDS will send TCP reset packet

Rule Protocol

- Suricata and Snort have the ability to detect specific protocols declared by the rule writer
- tcp
- udp
- icmp
- ip
- http (Suricata only)
- tls (Suricata only)

Rule Protocol

- Suricata and Snort have the ability to detect specific protocols declared by the rule writer

```
action protocol from_ip port -> to_ip port (msg:"something";

content:"something"; content:"something else"; sid:10000000; rev:1;)
```

- ip
- http (Suricata only)
- tls (Suricata only)

Rule Hosts Variables

- This is how you declare who is sending traffic to who
- Configurable via suricata.yaml and snort.conf
  - Contains defaults, but double check them
- $HOME_NET
  - Refers to internal networks, specified in the conf/yaml
- $EXTERNAL_NET
  - Not $HOME_NET, or what you choose in conf/yaml
- $HTTP_SERVERS, $SMTP_SERVERS, etc...
- Single IP

Rule Hosts Variables

- This is how you declare who is sending traffic to who

```
action protocol from_ip port -> to_ip port (msg:"something";

content:"something"; content:"something else"; sid:10000000; rev:1;)
```

  - $EXTERNAL_NET
    - Not $HOME_NET, or what you choose in conf/yaml
  - $HTTP_SERVERS, $SMTP_SERVERS, etc...
  - Single IP

Rule Direction

- Simply stated by an arrow: ->
- This tells the engine what direction traffic is flowing between hosts
- Traffic from internal host -> outbound
  - $HOME_NET any -> $EXTERNAL_NET any
- Traffic from external host -> inbound
  - $EXTERNAL_NET -> $HOME_NET any
- Can be bidirectional by using: <>
  - $EXTERNAL_NET any <> $HOME_NET any

Rule Direction

- Simply stated by an arrow: ->

```
action protocol from_ip port -> to_ip port (msg:"something";

content:"something"; content:"something else"; sid:10000000; rev:1;)
```

- Traffic from external host -> inbound
  - $EXTERNAL_NET -> $HOME_NET any
- Can be bidirectional by using: <>
  - $EXTERNAL_NET any <> $HOME_NET any

Rule Ports

- Used in tandem with the src/dst host variables
- Declares the port in which traffic for this rule will be evaluated
  - alert tcp $HOME_NET any -> $EXTERNAL_NET 9003
- Like the Hosts variables, ports may have variables as well
  - $HTTP_PORTS, $SMTP_PORTS, $FTP_PORTS, etc...
  - Configurable in conf/yaml
- Ports may be negated by placing a ! In front of it
  - $EXTERNAL_NET !80

Rule Ports (cont...)

- Ports may be expressed in various ways
  - Single port
    - 80
  - Multiple ports
    - [80,8080,443,9000]
  - Port ranges
    - [8000:9000]
  - Combination
    - $HOME_NET [1024:] -> $EXTERNAL_NET [80,800,6667:6669,!200]
    - What does this say?

Rule Ports (cont...)

- Ports may be expressed in various ways
  - Single port

```
action protocol from_ip port -> to_ip port (msg:"something";

content:"something"; content:"something else"; sid:10000000; rev:1;)
```

    - [8000:9000]
  - Combination
    - $HOME_NET [1024:] -> $EXTERNAL_NET [80,800,6667:6669,!200]
    - What does this say?

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1464 WS=4
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MS
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=1 Ack=1 Win=65900 Len=0
192.168.4.151	49689	free.diendancacanh.net	137.74.223.62	80	HTTP		336	GET /radio/sometime-estate-sleepy-10006700 HTTP/1.
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [ACK] Seq=1 Ack=337 Win=30336 Len=0
137.74.223.62	80		192.168.4.151	49689	TCP		1318	[TCP segment of a reassembled PDU]
137.74.223.62	80		192.168.4.151	49689	TCP		1209	[TCP segment of a reassembled PDU]
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=337 Ack=1319 Win=65900 Len=0
137.74.223.62	80		192.168.4.151	49689	HTTP	200	5	HTTP/1.1 200 OK (text/html)

alert ___ $_____ _____ -> $_____ _____

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1464 WS=4
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MS
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=1 Ack=1 Win=65900 Len=0
192.168.4.151	49689	free.diendancacanh.net	137.74.223.62	80	HTTP		336	GET /radio/sometime-estate-sleepy-10006700 HTTP/1.
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [ACK] Seq=1 Ack=337 Win=30336 Len=0
137.74.223.62	80		192.168.4.151	49689	TCP		1318	[TCP segment of a reassembled PDU]
137.74.223.62	80		192.168.4.151	49689	TCP		1209	[TCP segment of a reassembled PDU]
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=337 Ack=1319 Win=65900 Len=0
137.74.223.62	80		192.168.4.151	49689	HTTP	200	5	HTTP/1.1 200 OK (text/html)

Suricata

alert http $HOME_NET any -> $EXTERNAL_NET any

Snort

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		8	1052→27132 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=8
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [ACK] Seq=1 Ack=9 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [RST, ACK] Seq=9 Ack=1 Win=0 Len=0

alert ___ $_____ _____ -> $_____ _____

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		8	1052→27132 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=8
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [ACK] Seq=1 Ack=9 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [RST, ACK] Seq=9 Ack=1 Win=0 Len=0

alert tcp $HOME_NET any -> $EXTERNAL_NET any

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.25.10	1032		143.215.130.30	53	DNS			Standard query 0x9491 A ErnestRodgerRamsey.com
143.215.130.30	53		10.0.25.10	1032	DNS			Standard query response 0x9491 A ErnestRodgerRamsey.com A

alert ___ $_____ _____ -> $_____ _____

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.25.10	1032		143.215.130.30	53	DNS			Standard query 0x9491 A ErnestRodgerRamsey.com
143.215.130.30	53		10.0.25.10	1032	DNS			Standard query response 0x9491 A ErnestRodgerRamsey.com A

alert udp $HOME_NET any -> any 53

Rule Message

- msg:”DetoxCrypto Ransomware CnC Activity”;
  - Not the flavor
- Arbitrary text that appears when the rule fires and is logged/alert
- Consistency is key
- Consider adding:
  - Malware architecture: Win32/64, MSIL, ELF, OSX, etc
  - Malware family/name: njRAT, Locky, CryptXXX, Zeus
  - Malware action: Checkin, Activity, Key Exchange, Heartbeat, Exfil

Rule Message - Exercise

- msg:”Zeus Variant Checkin”;
- msg:”IP [illegible]kup”;
- msg:”Unknown Exploit Kit Plugin Check”;
- msg:”CnC [illegible]tivity”;

Flow

- Declare the originator and responder in the conversation
- Most rules we will write, we want to have the engine looking at “established” tcp sessions
- flow:<established>,<to_server|to_client>;
  - can also use from_server, from_client
- alert tcp $HOME_NET any -> $EXTERNAL_NET any
  - flow:established,to_server;
- If protocol is UDP, can use direction
  - flow:from_server;

Dsize

- Allows rule writer to match using the size of the packet payload (not http)
- Based on TCP segment length, NOT total packet length
  - Wireshark filter: tcp.len
- dsize:<number>;
- Can be represented as single number, range, greater than, or less than
  - dsize:312;
  - dsize:<300;
  - dsize:>300;
  - dsize:300<>400;

Rule Content

- The most basic building block for pattern matching
- Matching unique content in packets for detection
- Careful on what you choose
- **Must use hex for certain characters**
  - ; “ :
- content:”some thing”;
- content:”some|20|thing”;
- content:”User-Agent|3a 20|”;
- content:”s|00|o|00|m|00|e|00|t|00|h|00|i|00|n|00|g”;

Rule Content (cont...)

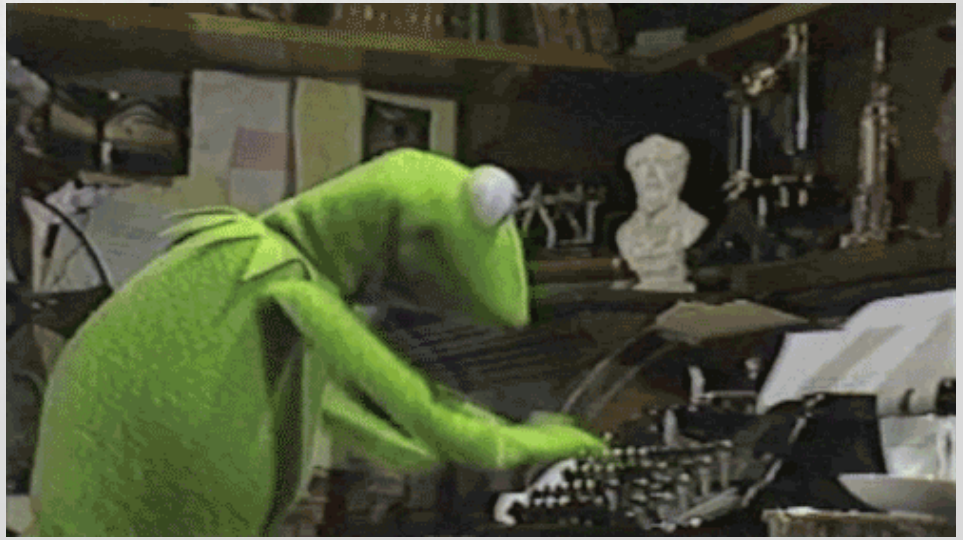
```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=sdJoFsAv3jSNMEYxHTTP/1.1 200 OK
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 186
Connection: close
Content-Type: text/html

MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
<!-- End Of Analytics Code -->
```

Rule Content (cont...)

- content:”POST”;
- content:”/generate.php”;
- content:”User-Agent|3a 20|DetoxCrypto”;
  - Same as “User-Agent: DetoxCrypto”
- content:”publickey=“;

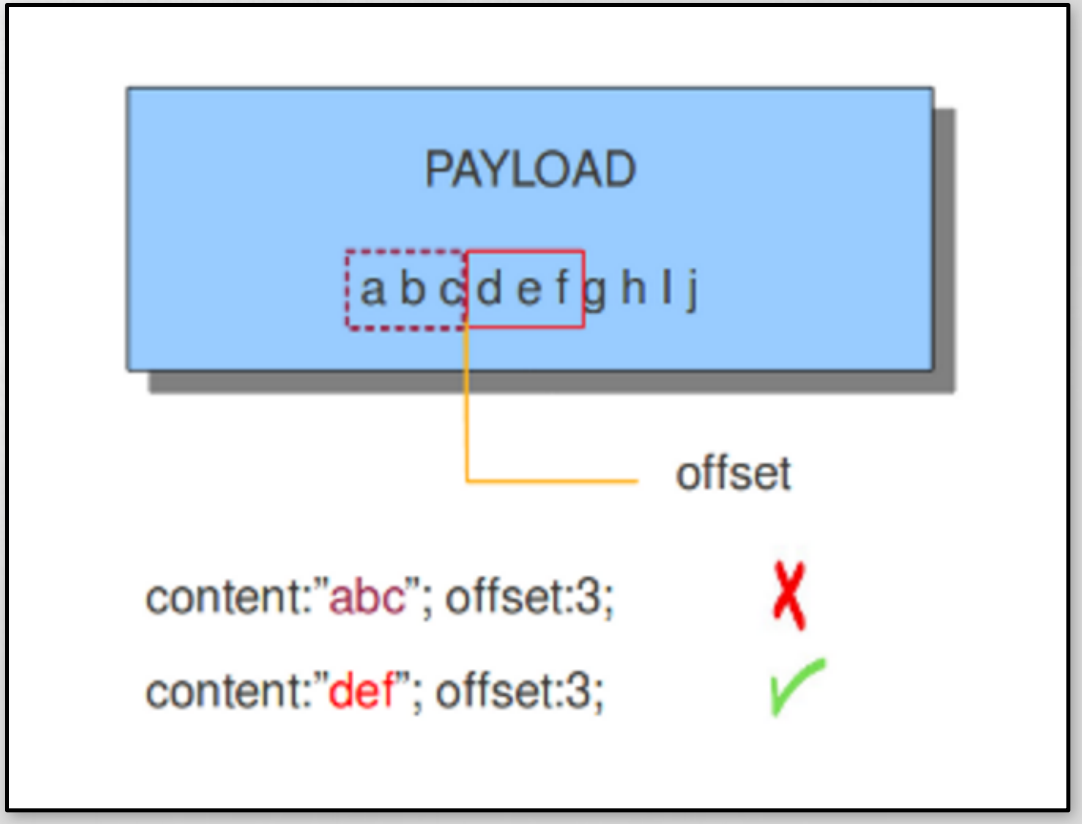
Rule Options

- Now that we have some content to match on, we can also add modifiers to assist in detection
- These can help the engine in finding exactly where content should be found
- Efficiency
- Accuracy



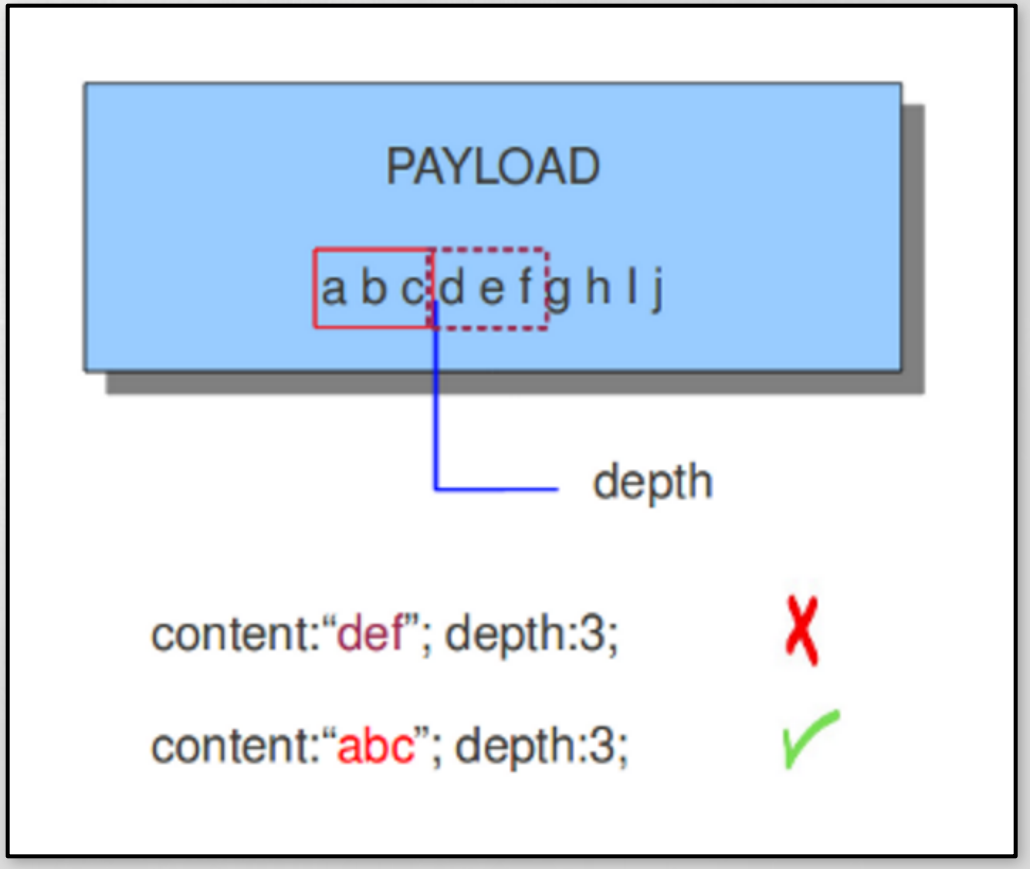
Offset

- Tells the engine to “go this far into the packet and start matching”
- content:”blah”; offset:5;
- Used in conjunction with “depth”



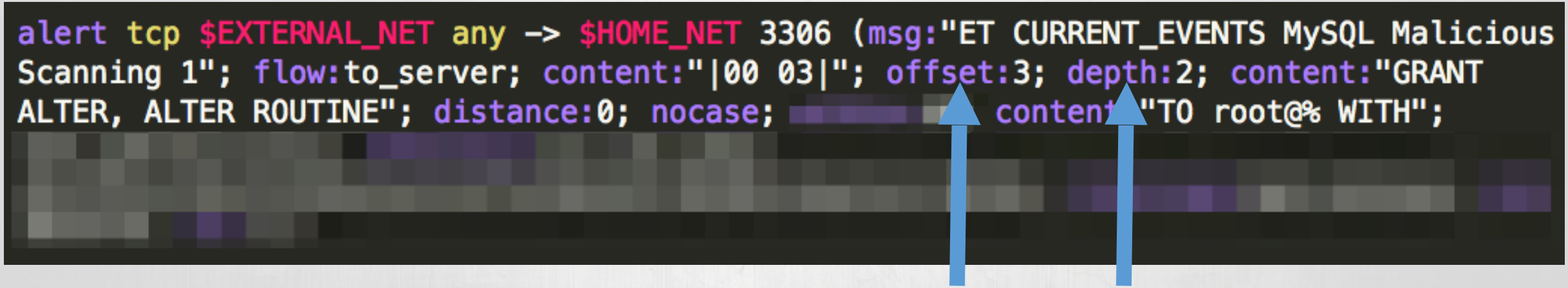
Depth

- Tells the engine how “deep” into the packet the content should be found
- content:”blah”; depth:4;
- Assumes offset:0; if not given



Offset + Depth

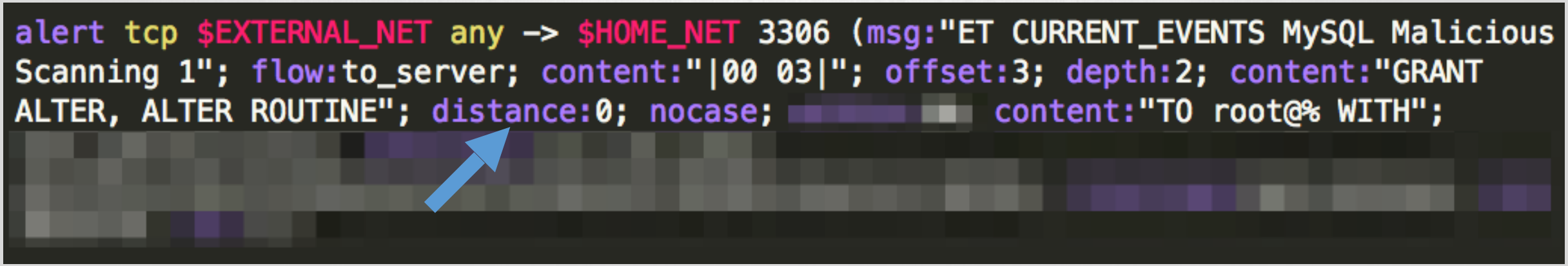
- Always together forever and ever ☺️



- Content of hex |00 03| will be found 3 bytes in, 2 bytes deep

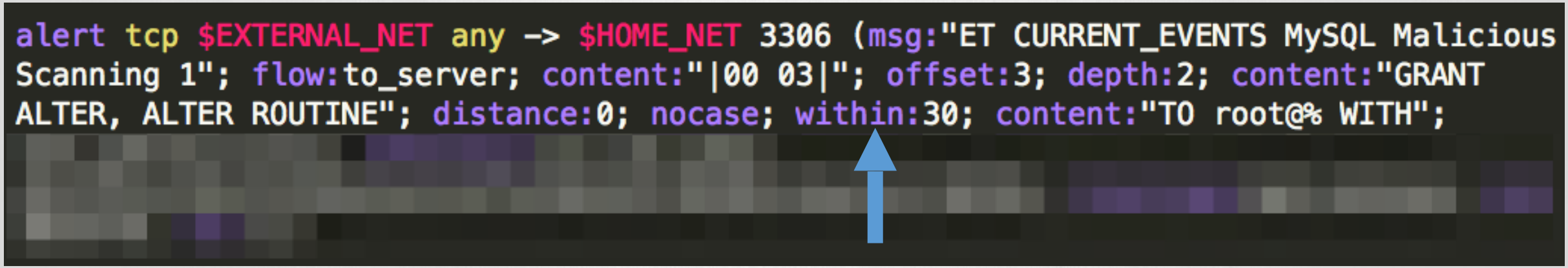
Distance

- Tells engine to look for your content n bytes relative to the previous match
- content:”something”; content:”something else”; distance:5;
- distance:0; can be used to tell the engine a content comes after another
  - content:”x”; content:”y”; distance:0; means “y” must come **after** “x”



Within

- Tells the engine how many bytes within this content will be found
- Allows us to dictate the amount of packet data being analyzed



- Content match is 26 characters
- 30 bytes within the previous match, this string must exist
- goes with “Distance”

Negation

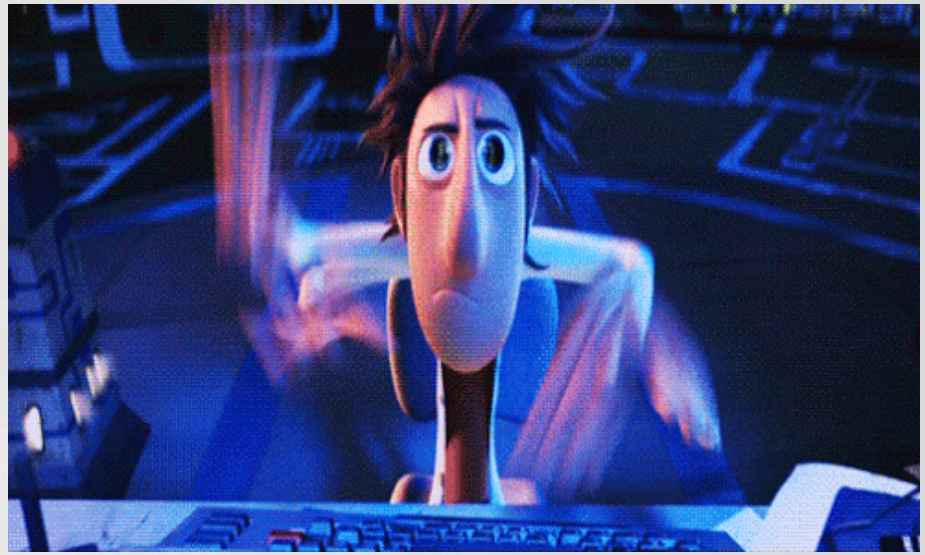
- We can negate content just as easy as we match content
- Rule will not fire if negated content is present
- Simply place a ! before the content
- content:!”Referer|3a 20|”;

- Negate “normal“ content that doesn’t appear in traffic
  - Careful! Can cause False Negatives

Checking in

- content:”foo”; offset:4; depth:3; content:”bar”; distance:20; within:3;
- content:”something”; depth:9; content:”some|20|more”; distance:0
- alert udp $HOME_NET any -> $EXTERNAL_NET 53
- alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:”Something Evil”; flow:established,to_server; dsize:45;
- content:”User-Agent|3a 20|Internet”; content:!”Accept|3a|”;

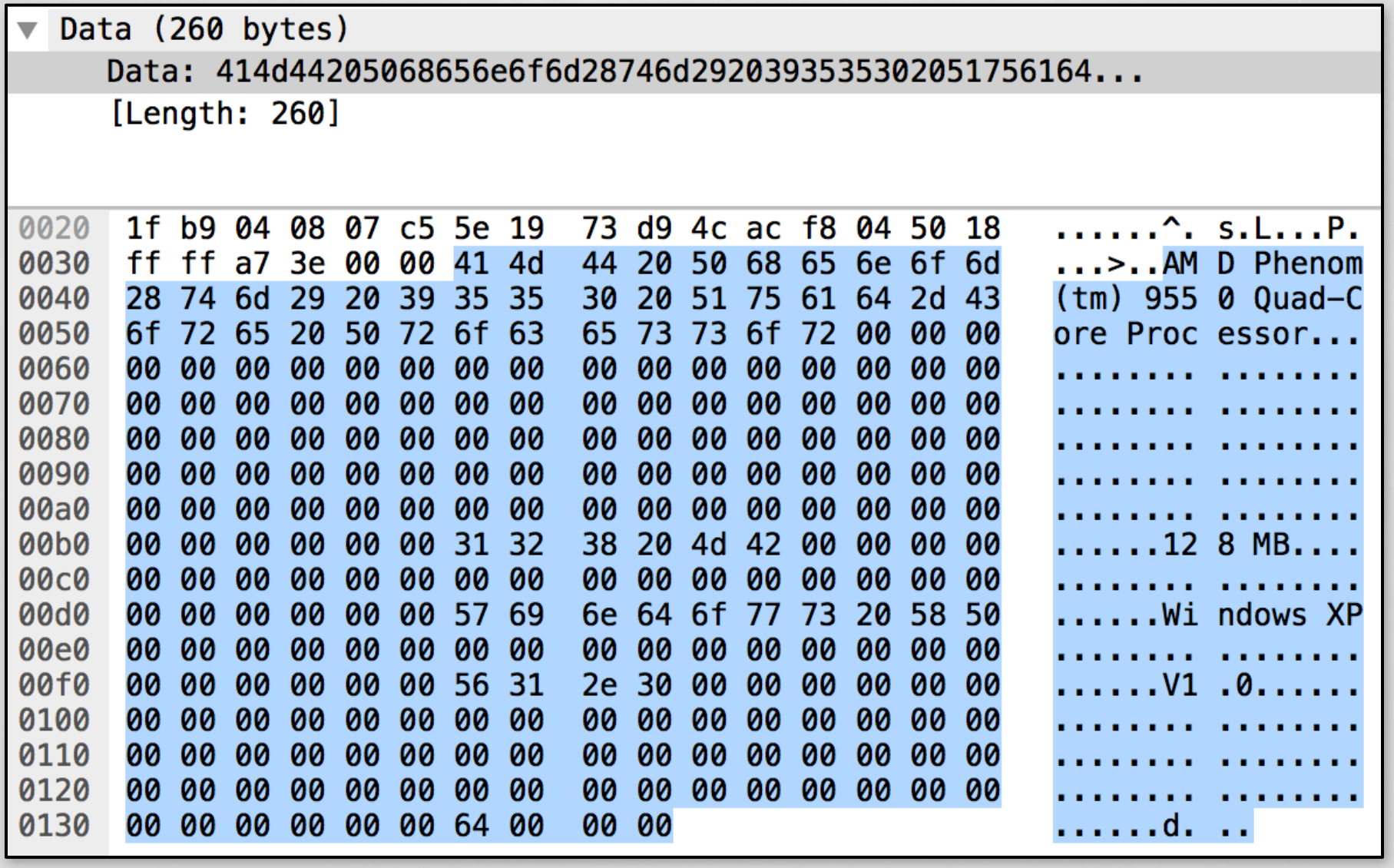
Rule Meta



- SID
  - Signature ID
  - sid:10000000
- Reference
  - Attach reference to our rule to help provide context
  - reference:md5, e273508a2f2ed45c20a2412f7d62eceb;
  - reference:url,malwarefor.me/2015-12-27-sundown-ek-sending-neutrino;
  - reference:cve,2016-3254;
- Revision
  - Tells us what version of the rule we are on
  - rev:9;

Basic Group Exercise

dsize:___; content:"_____"; content:"_____";
distance:0; content:"_____"; distance:0;



dsize:260; content:"MB|00 00|"; content:"Windows|20|"; distance:0; content:"V1.0|00 00|"; distance:0;

```
▼ Data (260 bytes)
    Data: 414d44205068656e6f6d28746d2920393535302051756164...
    [Length: 260]

0020  1f b9 04 08 07 c5 5e 19  73 d9 4c ac f8 04 50 18   ......^. s.L...P.
0030  ff ff a7 3e 00 00 41 4d  44 20 50 68 65 6e 6f 6d   ...>..AM D Phenom
0040  28 74 6d 29 20 39 35 35  30 20 51 75 61 64 2d 43   (tm) 955 0 Quad-C
0050  6f 72 65 20 50 72 6f 63  65 73 73 6f 72 00 00 00   ore Proc essor...
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 31 32  38 20 4d 42 00 00 00 00   ......12 8 MB....
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 57 69  6e 64 6f 77 73 20 58 50   ......Wi ndows XP
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 56 31  2e 30 00 00 00 00 00 00   ......V1 .0......
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0130  00 00 00 00 00 00 64 00  00 00                     ......d. ..
```

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"njRAT/Syrian Malware Variant CnC Checkin "; flow:_____; content:"_____"; offset:_; depth:_; content:"_____"; distance:0; content:"_____"; distance:0; classtype:trojan-activity; sid:100; rev:1;)

```
0030  f4 23 93 43 00 00 21 30  2f 6a 7c 6e 5c 53 79 72   .#.C..!0 /j|n\Syr
0040  69 61 6e 20 4d 61 6c 77  61 72 65 2f 6a 7c 6e 5c   ian Malw are/j|n\
0050  74 65 6d 75 63 6f 2f 6a  7c 6e 5c 6d 65 2f 6a 7c   temuco/j |n\me/j|
0060  6e 5c 55 53 41 2f 6a 7c  6e 5c 57 69 6e 20 58 50   n\USA/j| n\Win XP
0070  20 50 72 6f 66 65 73 73  69 6f 6e 61 6c 53 50 32    Profess ionalSP2
0080  20 78 38 36 2f 6a 7c 6e  5c 4e 6f 2f 6a 7c 6e 5c    x86/j|n \No/j|n\
0090  30 2e 31 2f 6a 7c 6e 5c  2f 6a 7c 6e 5c 61 62 6f   0.1/j|n\ /j|n\abo
00a0  75 74 3a 62 6c 61 6e 6b  20 2d 20 4d 69 63 72 6f   ut:blank  - Micro
00b0  73 6f 66 74 20 49 6e 74  65 72 6e 65 74 20 45 78   soft Int ernet Ex
00c0  70 6c 6f 72 65 72 2f 6a  7c 6e 5c 5b 65 6e 64 6f   plorer/j |n\[endo
00d0  66 5d                                             f]
```

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"njRAT/Syrian Malware Variant CnC Checkin "; flow:established,to_server; content:"|2f|j|7c|n|5c|"; offset:2; depth:5; content:"Syrian Malware"; distance:0; content:"[endof]"; distance:0; classtype:trojan-activity; sid:100; rev:1;)

```
0030  f4 23 93 43 00 00 21 30  2f 6a 7c 6e 5c 53 79 72   .#.C..!0 /j|n\Syr
0040  69 61 6e 20 4d 61 6c 77  61 72 65 2f 6a 7c 6e 5c   ian Malw are/j|n\
0050  74 65 6d 75 63 6f 2f 6a  7c 6e 5c 6d 65 2f 6a 7c   temuco/j |n\me/j|
0060  6e 5c 55 53 41 2f 6a 7c  6e 5c 57 69 6e 20 58 50   n\USA/j| n\Win XP
0070  20 50 72 6f 66 65 73 73  69 6f 6e 61 6c 53 50 32    Profess ionalSP2
0080  20 78 38 36 2f 6a 7c 6e  5c 4e 6f 2f 6a 7c 6e 5c    x86/j|n \No/j|n\
0090  30 2e 31 2f 6a 7c 6e 5c  2f 6a 7c 6e 5c 61 62 6f   0.1/j|n\ /j|n\abo
00a0  75 74 3a 62 6c 61 6e 6b  20 2d 20 4d 69 63 72 6f   ut:blank  - Micro
00b0  73 6f 66 74 20 49 6e 74  65 72 6e 65 74 20 45 78   soft Int ernet Ex
00c0  70 6c 6f 72 65 72 2f 6a  7c 6e 5c 5b 65 6e 64 6f   plorer/j |n\[endo
00d0  66 5d                                             f]
```

Basic Rule Writing Lab

Exercise 1: **DDoSClient.pcap** in the **workbook.pdf** on the vm desktop

If you are confident in your rule writing abilities, begin on page 7.

If you would like some assistance start on page 8.

We will write the rule live in **15 minutes**.

Additional Rule Writing Features

fast_pattern

- Keyword placed after a content which **must** be matched before the rule is evaluated
- content:”something|20|unique”; fast_pattern;
- Should be used in every rule on most valuable content chosen by rule author
  - VERY efficient
- fast_pattern; by default is 20 bytes
  - If matching content:”User-Agent|3a 20|Mozilla/5.0 (Evilness)”; fast_pattern;
  - fast_pattern will be “User-Agent|3a 20|Mozilla/”

fast_pattern (cont...)

- If a content is longer than 20 bytes... fast_pattern “chop”
- fast_pattern:x,y;
- Allows us to choose the 20 bytes of the content we want to use for our fast_pattern
- content:”User-Agent|3a 20|Mozilla/5.0 (Evilness)”; fast_pattern:14,20;
  - fast_pattern becomes “ozilla/5.0 (Evilness)”
- content:"User-Agent|3a 20|DetoxCrypto"; fast_pattern:3,20;
  - fast_pattern becomes “r-Agent|3a 20|DetoxCrypto”

HTTP Buffers

- Suricata and Snort have the ability to parse HTTP and place packet contents into buffers to easily match.
- Much faster than searching raw packet
- We can use these to our advantage in conjunction with the other keywords and modifiers!
  - content:”User-Agent|3a 20|DetoxCrypt”; http_header; fast_pattern:3,20;

- Suricata HTTP Buffers: http://suricata.readthedocs.io/en/latest/rules/http-keywords.html
- Snort HTTP Buffers: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node32.html

HTTP Buffer (cont...)

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=sdJoFsAv3jSNMEYxHTT
Date: Sat, 13 Aug 2016 04:45:
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 186
Connection: close
Content-Type: text/html

MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
```

content:”POST”; http_method;

content:”/generate.php”; http_uri;

content:”User-Agent|3a 20|DetoxCrypto”; http_header;

content:”publickey=“; http_client_body;

http_method

- The http_method; keyword can be used for a content involving the method in which the HTTP Request was made
  - content:”GET”; http_method;
  - content:”POST”; http_method;
  - content:”HEAD”; http_method;

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive
```

http_uri

- Used for capturing any content present in the URI string of a request
- content:”/generate.php”; http_uri;
- urilen keyword
  - urilen:<number>;
  - Used like dsize, but for the length of the URI

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive
```

http_header

- This is used for any field present in the Header section
- content:”User-Agent|3a|”; http_header;
- content:!”Referer|3a|”; http_header;
- Cookie is not able to be used with this buffer
  - It has its own buffer —> http_cookie

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=sdJoFsAv3jSNMEYxHTTP/1.1 200 OK
```

http_client_body

- Used for an HTTP request's payload
- Commonly observed with POST requests
- content:"publickey="; http_client_body;

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=sdJoFsAv3jSNMEYxHTTP/1.1 200 OK
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
```

http_user_agent

- Suricata only! Fast! Use it!
- Will parse the field between User-Agent|3a 20| and |0d 0a|
- **Suricata**
  - content:"DetoxCrypto"; fast_pattern; **http_user_agent;**
- **Snort**
  - content:"User-Agent|3a 20|DetoxCrypto"; fast_pattern:3,20; **http_header;**

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
```

file_data

- Keyword used to declare content that is in the Response Body
- Used once in a rule; applies to content used after
- file_data;

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=sdJoEsAv3jSNMEYxHTTP/1.1 200 OK
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 186
Connection: close
Content-Type: text/html

MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
<!-- End Of Analytics Code -->
```

HTTP Response Headers

HTTP Response Body

Additional Rule Writing Features Group Exercise

content:”/g76gyui?”; _____; depth:_; content:”User-Agent|3a 20|Mozilla/4.0 (compatible|3b 20|MSIE 6.0|3b 20|Windows NT 5.0)|0d 0a|”; _____; content:”Connection|3a 20|Keep-Alive|0d 0a|”; _____;

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.szm.com
Connection: Keep-Alive
```

content:”/g76gyui?”; http_uri; depth:9; content:”User-Agent|3a 20|Mozilla/4.0 (compatible|3b 20|MSIE 6.0|3b 20|Windows NT 5.0)|0d 0a|”; http_header; content:”Connection|3a 20|Keep-Alive|0d 0a|”; http_header;

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.szm.com
Connection: Keep-Alive
```

content:”Content-Length|3a 20|2”; _____;
content:”Content-Type|3a 20|text/html”;
_____; _____; content:”<iframe src=|
22|”; depth:__; content:”width=|22|”; distance:_;
content:”height=|22|”; distance:_;
content:”_____”; fast_pattern;

```
HTTP/1.1 200 OK
Date: Fri, 02 Sep 2016 07:36:36 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/5.3.3
Content-Length: 278
Connection: close
Content-Type: text/html; charset=UTF-8

<iframe src="http://v42pdxqt.top/?x3qJc7iaLxjHCYE=l3SKfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-
ofSih17OIFxzsqAycFUKCqrF4Qu4Fah2h1QWScEZrmYRPFgVIove8hQLfyhSWkpGBrBSOaAhA_pSRF-
U_2AygzLJFdcomwRWA6mcCmL5PQFFd" width="468" height="60" style="position:absolute;left:-10000px;"></
iframe>
```

content:”Content-Length|3a 20|2”; http_header; content:”Content-Type|3a 20|text/html”; http_header; file_data; content:”<iframe src=|22|”; depth:13; content:”width=|22|”; distance:0; content:”height=|22|”; distance:0; content:”absolute|3b|left|3a|-1”; fast_pattern;

```
HTTP/1.1 200 OK
Date: Fri, 02 Sep 2016 07:36:36 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/5.3.3
Content-Length: 278
Connection: close
Content-Type: text/html; charset=UTF-8

<iframe src="http://v42pdxqt.top/?x3qJc7iaLxjHCYE=l3SKfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-ofSih17OIFxzsqAycFUKCqrF4Qu4Fah2h1QWScEZrmYRPFgVIove8hQLfyhSWkpGBrBSOaAhA_pSRF-U_2AygzLJFdcomwRWA6mcCmL5PQFFd" width="468" height="60" style="position:absolute;left:-10000px;"></iframe>
```

HTTP Rule Writing Lab

Exercise 2: **Ursnif.pcap** in the **workbook.pdf** on the vm desktop

If you are confident in your rule writing abilities, begin on page 10.

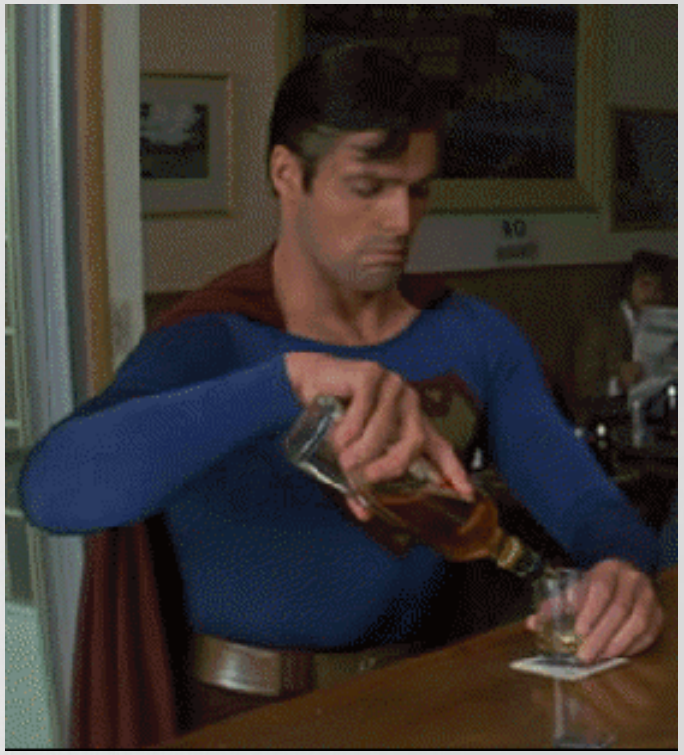
If you would like some assistance start on page 11.

We will write the rule live in **15 minutes**.

PCRE

welcome to hell

PCRE



- Pearl Compatible Regular Expression
- Similar to other regex vernacular (JavaScript, etc)
- Called using “pcre” followed by the regular expression
- PCRE must be wrapped in leading and trailing forward slashes
- pcre:”/something/flags”;

PCRE (cont...)

- pcre:”/\/[A-Za-z0-9]{6}\.php$/U”;
- Looks for 6 chars in the range followed by .php and nothing after
- Must wrap the PCRE with forward slashes (“/”)
- Flags go after the last forward slash
- Anchors go after and before wrapped slashes
- Need to escape certain characters with a backslash if used literally
  - \/
  - \$
  - \?

PCRE - Special Chars

- ^
  - Leading anchor (start matching here)
  - pcre:"/^foo/P";
- $
  - Trailing anchor (nothing after)
  - pcre:"/foo$/P";
- []
  - Character set– wrap characters in brackets
  - pcre:"/[A-Za-z0-9]/U";
- ()
  - Capturing group
  - pcre:”([A-Z0-9]{8})+/”;
- {}
  - Certain number, or range of something you match
  - pcre:"/[A-Za-z0-9]{5,10}/U";
  - Matches between 5 and 10 of alphanumeric
- \s
  - Matches a space
  - Good for Javascript and HTML
- \r
  - Matches Carrage return
  - Same is |0d|
- \n
  - Matches new-line
  - Same as |0a|
- .
  - Matches anything
- ?
  - Matches 1 or 0
- *
  - Matches 0 or more
- +
  - 1 or more
  - pcre:"/[A-Za-z0-9]+/U";
- ?:
  - Non-capture group
  - ALWAYS use this...
  - pcre:”/(?:this|that)/”;

PCRE - Flags

- Used to represent the various buffers available in the engine

- To be used just like content + buffer

- U - http_uri;
- H - http_header;
- P - http_client_body;
- i - Makes PCRE case-insensitive
- R - Makes PCRE relative (distance:0;) to last match
- m - Multi-line matching

PCRE Group Exercise

Exercise - PCRE

- What could a PCRE look like for this traffic...? We know the command (URI) is between 2 and 5 characters long

```
GET /PWD HTTP/1.1
Host: cdn.fastaccesshosting.xyz
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Tue, 08 Mar 2016 19:55:28 GMT
Content-Type: application/octet-stream
Content-Length: 283702
Last-Modified: Sun, 31 May 2015 17:47:42 GMT
Connection: keep-alive
Accept-Ranges: bytes
```

Exercise - PCRE

- What could a PCRE look like for this traffic...?
- **pcre:"/^\/[A-Z]{2,5}$/U";**

```
GET /PWD HTTP/1.1
Host: cdn.fastaccesshosting.xyz
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Tue, 08 Mar 2016 19:55:28 GMT
Content-Type: application/octet-stream
Content-Length: 283702
Last-Modified: Sun, 31 May 2015 17:47:42 GMT
Connection: keep-alive
Accept-Ranges: bytes
```

Exercise - PCRE

- Write a PCRE for this HTTP URI string, assuming the variables will change per infection

```
GET /ping.php?hostname=AMBROSE&username=peggysue&domain=AMBROSE HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/
7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Host: 52.65.108.15
Connection: Keep-Alive
```

Exercise - PCRE

- Write a PCRE for this HTTP URI string, assuming the variables will change per infection
- **pcre:"/^\/ping\.php\?hostname=[^\r\n]+&username=[^\r\n]+&domain=[^\r\n]+$/Ui";**

```
GET /ping.php?hostname=AMBROSE&username=peggysue&domain=AMBROSE HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/
7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Host: 52.65.108.15
Connection: Keep-Alive
```

Exercise - PCRE

- Write a PCRE for the http_header order

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.szm.com
Connection: Keep-Alive
```

Exercise - PCRE

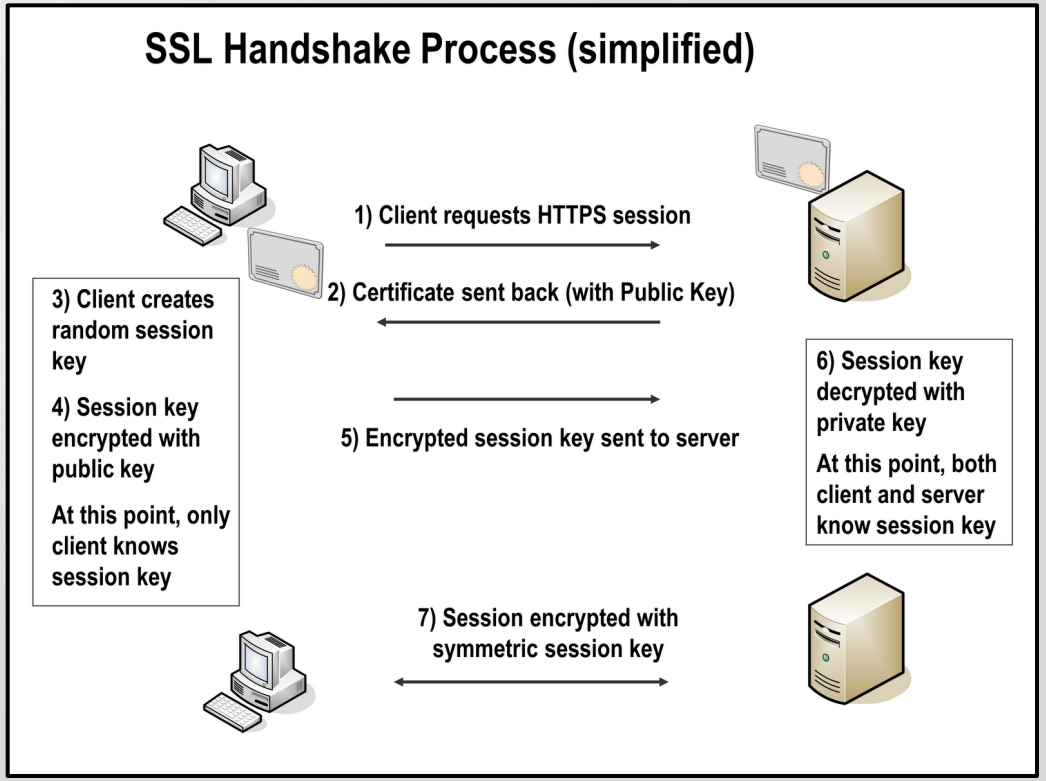
- Write a PCRE for the http_header order
- **pcre:"/^Accept\x3a\x20[^\r\n]+\r\nAccept-Language\x3a\x20en-us\r\nUser-Agent\x3a\x20[^\r\n]+\r\nAccept-Encoding[^\r\n]+\r\nHost\x3a\x20[^\r\n]+\r\nConnection[^\r\n]+\r\n\r\n$/Hmi";**

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.szm.com
Connection: Keep-Alive
```

SSL / TLS

SSL / TLS

- A blind spot for most IDS/IPS
- Cannot see into the traffic, just that its happening
  - Unless MITM, which is cool too!
- Let's Encrypt!
- Wait!
- We can do something with SSL/TLS



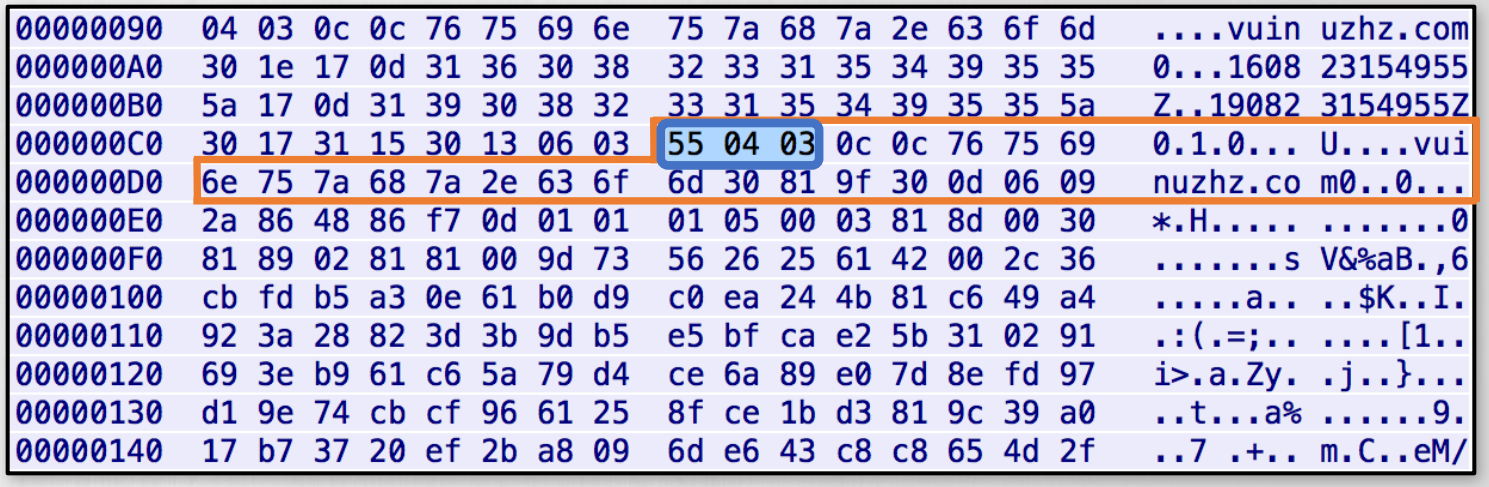
SSL / TLS Basics

No.	Time	Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
67	2016-09-06 13:38:19.229795	192.168.78.20	49181		91.219.31.12	443	TLSv1		117	Client Hello
69	2016-09-06 13:38:19.833871	91.219.31.12	443		192.168.78.20	49181	TLSv1		741	Server Hello, Certificate,
70	2016-09-06 13:38:19.901833	192.168.78.20	49181		91.219.31.12	443	TLSv1		198	Client Key Exchange, Change
71	2016-09-06 13:38:20.336401	91.219.31.12	443		192.168.78.20	49181	TLSv1		59	Change Cipher Spec, Encrypt

```
▼ TLSv1 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 641
  ▼ Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 637
      Certificates Length: 634
    ▼ Certificates (634 bytes)
        Certificate Length: 631
      ▼ Certificate: 30820273308201dca00302010202045da0decc300d06092a... (id-at-commonName=vuinuzhz.com)
        ▼ signedCertificate
            version: v3 (2)
            serialNumber: 1570823884
          ▶ signature (sha256WithRSAEncryption)
          ▶ issuer: rdnSequence (0)
          ▶ validity
          ▼ subject: rdnSequence (0)
            ▼ rdnSequence: 1 item (id-at-commonName=vuinuzhz.com)
              ▼ RDNSequence item: 1 item (id-at-commonName=vuinuzhz.com)
                ▼ RelativeDistinguishedName item (id-at-commonName=vuinuzhz.com)
```

SSL / TLS - What to sig on

- Serial Number
  - content:"|09 00 97 ae 20 7e 61 5f 58 15|";
- Common Name (CN)
  - content:"|55 04 03|";
- Organization (O)
  - content:"|55 04 0a|";
- Organizational Unit (OU)
  - content:"|55 04 0b|";
- Country (C)
  - content:"|55 04 06|";
- State (S)
  - content:"|55 04 08|";
- Locality (L)
  - content:"|55 04 07|";



Writing Signatures for SSL / TLS

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN ABUSE.CH SSL Fingerprint
Blacklist Malicious SSL Certificate Detected (H1N1 CnC)"; flow:established,from_server;
content:"|09 00 cc e5 16 49 2c 1e 96 57|"; content:"|55 04 0a|"; distance:0; content:
"|13|Default Company Ltd"; distance:1; within:20; reference:url,sslbl.abuse.ch; classtype:
trojan-activity; sid:2022959; rev:2;)
```

- Protocol: tls (Suricata) or tcp (Snort)
- Ports: any/any (Suricata) or 443/any (Snort)
- Content: Serial number
- Content: Organization
  - \x13 is the length of the field in Decimal
  - 13 hex = 19 decimal

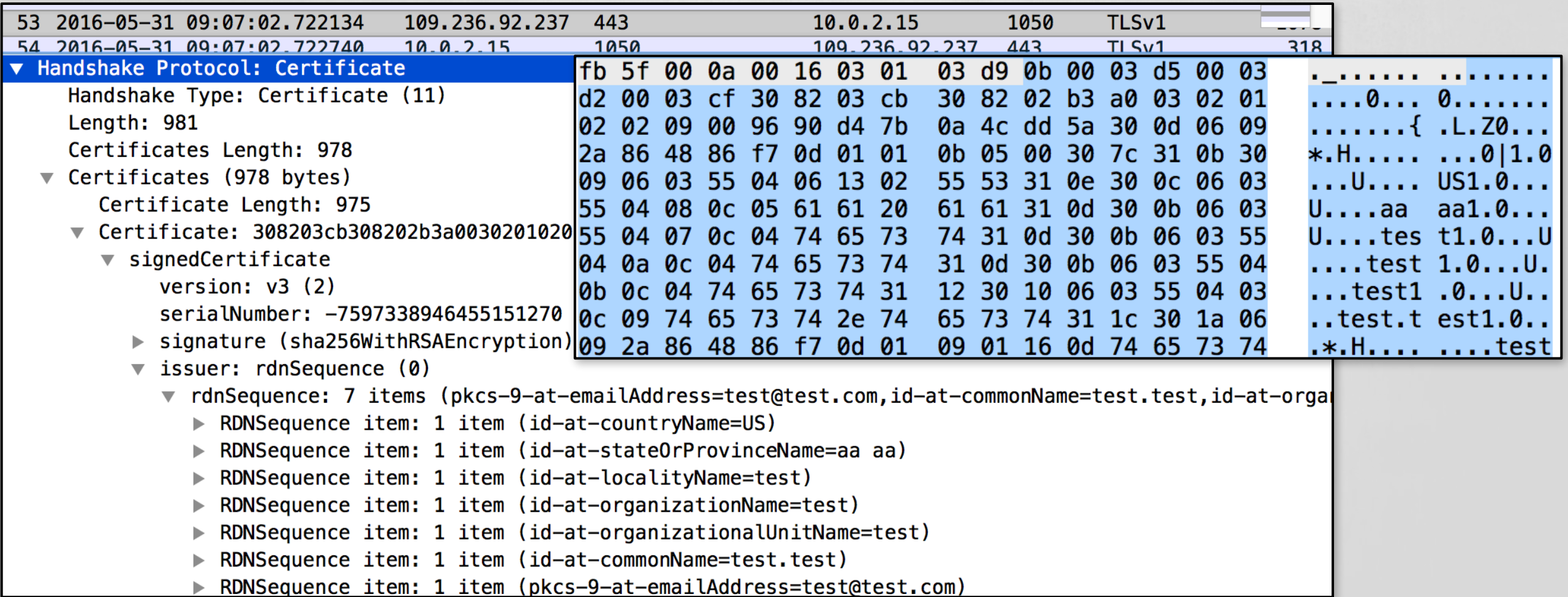
Writing Signatures for SSL / TLS

```
alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ETPRO TROJAN Malicious SSL Certificate Observed (Vawtrak)
"; flow:established,from_server; content:"|55 04 03|"; content:"|0c|vuinuzhz.com"; distance:1; within:13;
classtype:trojan-activity; sid:100000034; rev:1;)
```

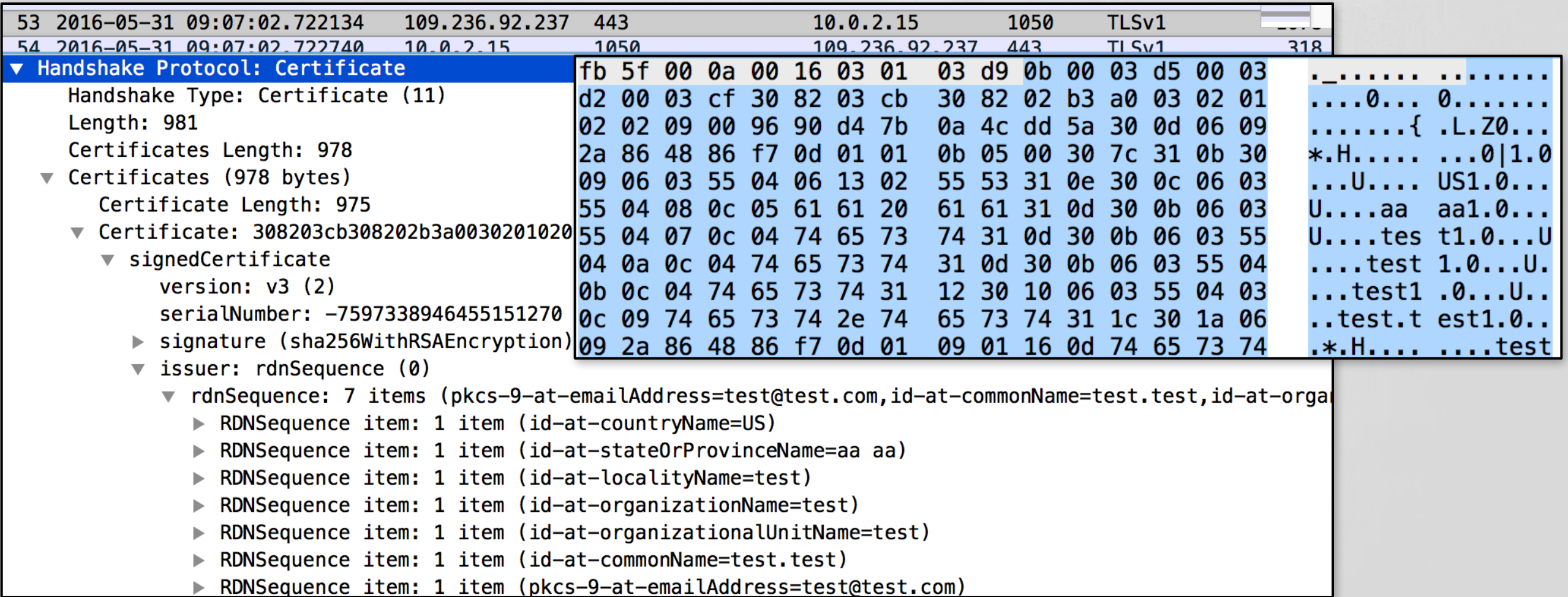
- Protocol: tls (Suricata) or tcp (Snort)
- Ports: any/any (Suricata) or 443/any (Snort)
- Content: Common Name (CN)
  - \x0c is the length of the domain name
  - \x0c hex = 12 in decimal

SSL / TLS Group Exercise

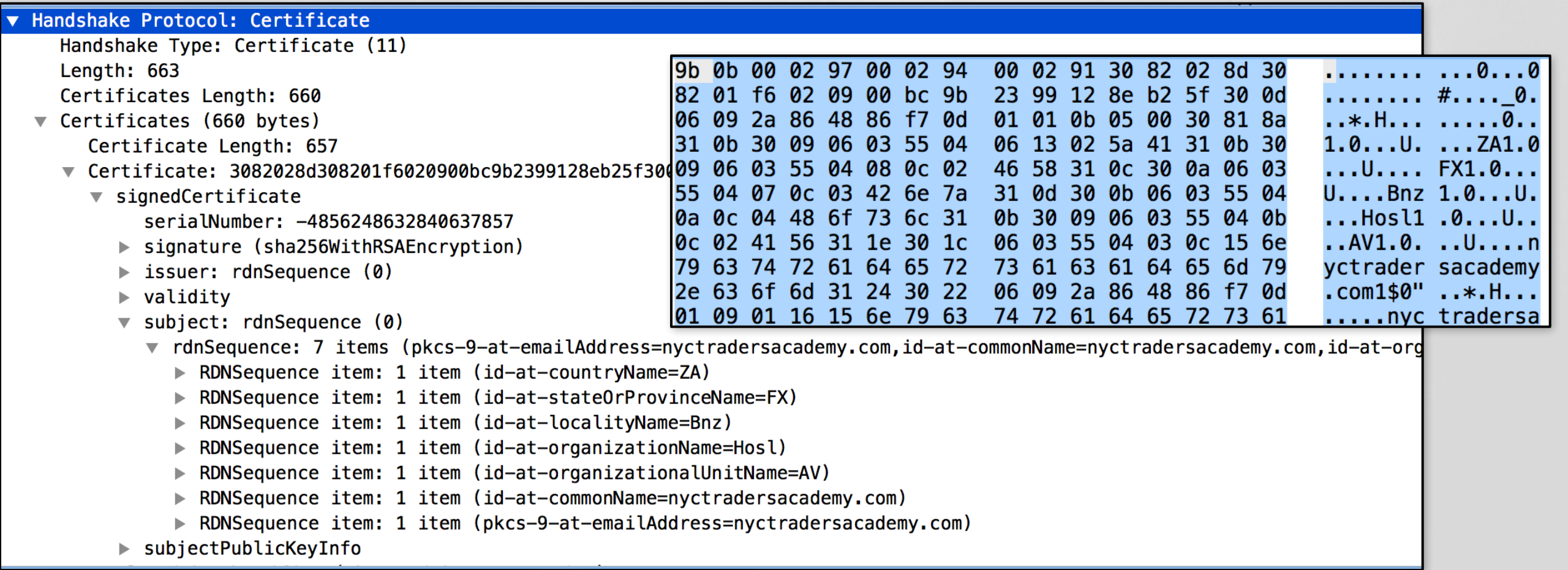
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Malicious SSL Cert Inbound"; flow:_____; content:"_____"; fast_pattern; content:"_____"; content:"_____"; distance:0; content:"_____"; distance:___; within:___;



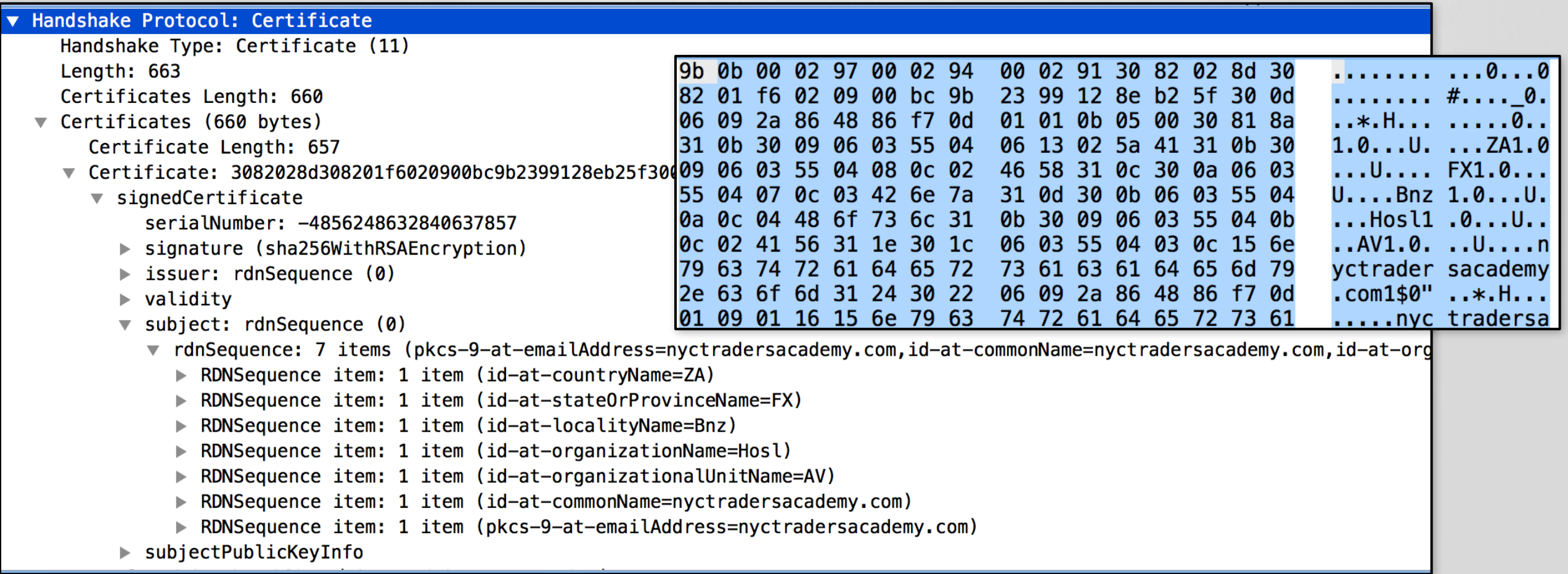
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Malicious SSL Cert Inbound"; flow:established,from_server; content:"|00 96 90 d4 7b 0a 4c dd 5a|"; fast_pattern; content:"|55 04 0a|"; distance:0; content:"|04|test"; distance:1; within:5;



alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Malicious SSL Cert Inbound"; flow:_____; content:"____"; content:"_____"; distance:___; within:___;



alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Malicious SSL Cert Inbound"; flow:established,from_server; content:"|55 04 03|"; content:"|15|nyctradersacademy.com"; distance:1; within:22;



SSL Rule Writing Lab

Exercise 3: **Zeus.pcap** in the **workbook.pdf** on the vm desktop

If you are confident in your rule writing abilities, begin on page 13.

If you would like some assistance start on page 14.

We will write the rule live in **10 minutes**.

Writing Signatures for SSL/TLS

- ssl_sigs.py
  - https://github.com/malwareforme/ssl_sigs

- Example:
  - $ python ssl_sigs.py -d something.bad.com -m "TROJAN Observed Malicious SSL Cert (Ursnif Injects)" -s 100000000

- alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"TROJAN Observed Malicious SSL Cert (Ursnif Injects)"; flow:established:from_server; content"|55 04 03|"; content:"|11|something.bad.com"; distance:1; within:18; classtype:trojan-activity; sid:100000000; rev:1;)

APPLICATION LABS

Phishing: Ex. 4 - Adobe.pcap
Ransomware: Ex. 5 - Cerber.pcap
Malicious Document: Ex. 6 - Maldoc.pcap
Exploit Kit: Ex. 7 - Neutrino.pcap
Targeted Attack: Ex. 8 - Patchwork.pcap

BSIDES LAS VEGAS

Wrapping Up

- Network analysis!
- The more you look into your network, the more likely you will be to know what “normal” and “abnormal” look like.
- Use multiple rule options together for maximum detection/efficiency
- Continue working…
  - ET OPEN Ruleset - Free to download and play with (learn from)
  - Snort Community Ruleset - Free to download and play with (learn from)
  - Security Onion – Free Ubuntu distro with Network Analysis tools
  - malware-traffic-analysis.net– PCAPs and malware samples galore
  - broadanalysis.net- PCAPs and malware samples galore

Resources

- Suricata Manual
  - http://suricata.readthedocs.io/en/latest/index.html
- Snort Manual
  - http://manual-snort-org.s3-website-us-east-1.amazonaws.com/
- Emerging Threats Open Mailing List
  - https://lists.emergingthreats.net/mailman/listinfo/emerging-sigs
- OISF Mailing List
  - https://lists.openinfosecfoundation.org/mailman/listinfo/oisf-users
- Snort Community Mailing List
  - https://lists.snort.org/mailman/listinfo/snort-sigs

Continued Education

- **OISF -** https://suricata-ids.org/training/
  - Suricata User Training (2 Day)
    - Suricon - Nov 15-17 2017, Prague, CZ - https://suricon.net/
  - Suricata Sigdev (2 Day)
    - ~~Derbycon 2017~~ (Sold Out)
    - Suricon
  - Suricata Developer Training
    - Sept 11 2017, Cork, Ireland
  - Private trainings available
- **SANS 503 -** https://www.sans.org/course/intrusion-detection-in-depth

Contact

Jack Mott

@malwareforme

Security Research Analyst

jmott@emergingthreats.net

Jae Williams

@switchingtoguns

Security Research Analyst

jae@emergingthreats.net