Visual Threat Hunting

By Ryan Nolette

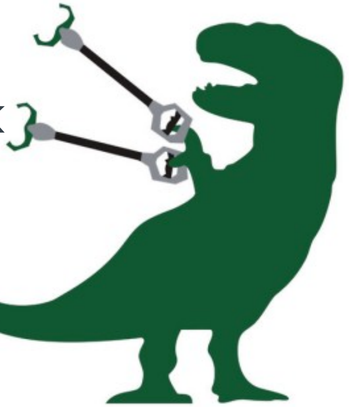
Security Technologist

What am I trying to accomplish?

- Perform a Threat Hunt
  - Find internal hosts beaconing out
- Explain what I found to my management
- Justify my time to Hunt

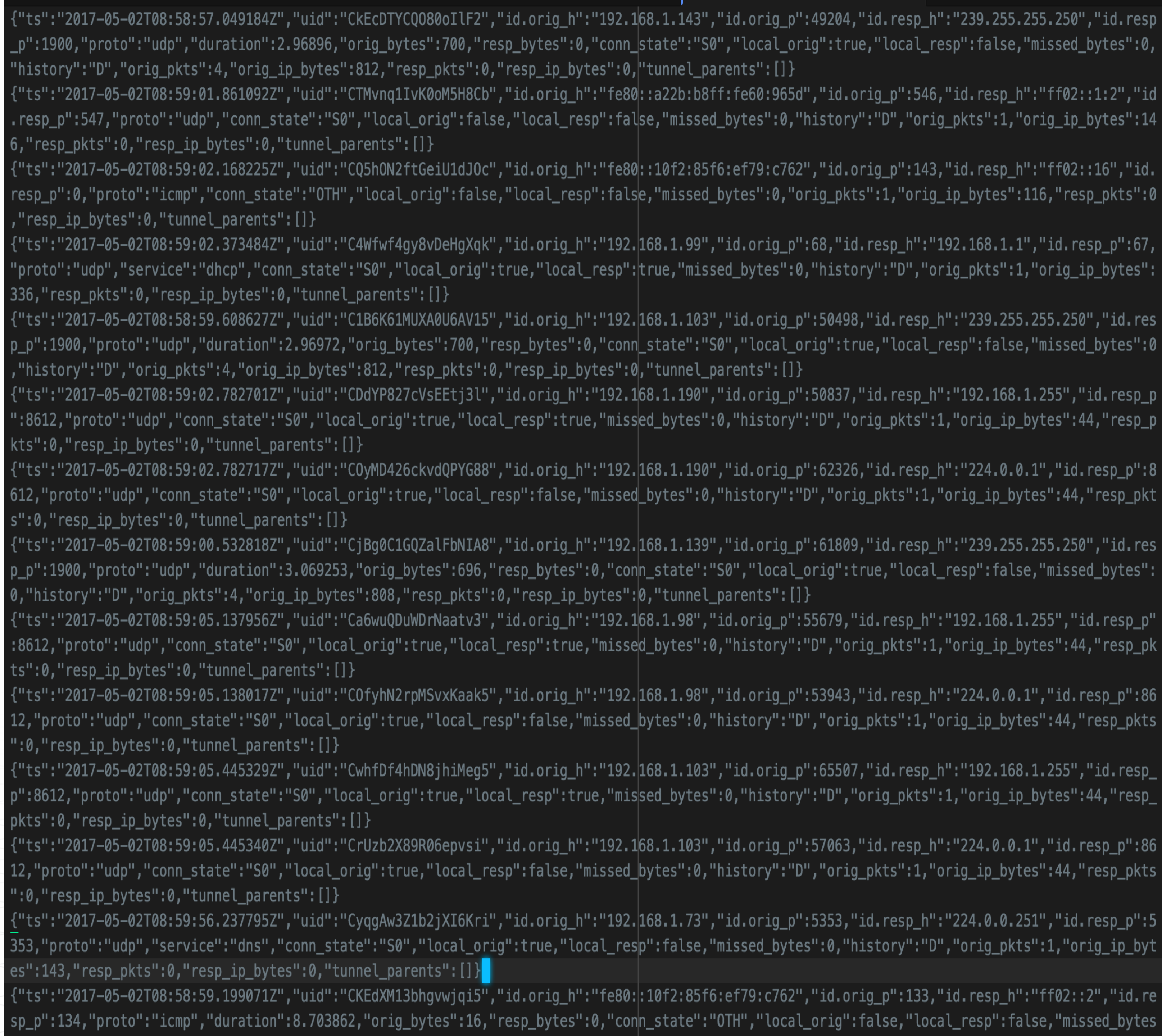
Tools used in this talk

- Bro sensor - https://www.bro.org/
  - Configured to output logs to json
- Graphviz - http://www.graphviz.org/
  - To create visuals of the data bro is producing
- Python - https://www.python.org/
  - To convert bro data to graphviz formatting
  - https://github.com/sonofagl1tch/visualization/tree/master/VisualThreatHunting
- Centos 7 minimal server to run bro
  - Because the GUI makes you weak



Log Crawling

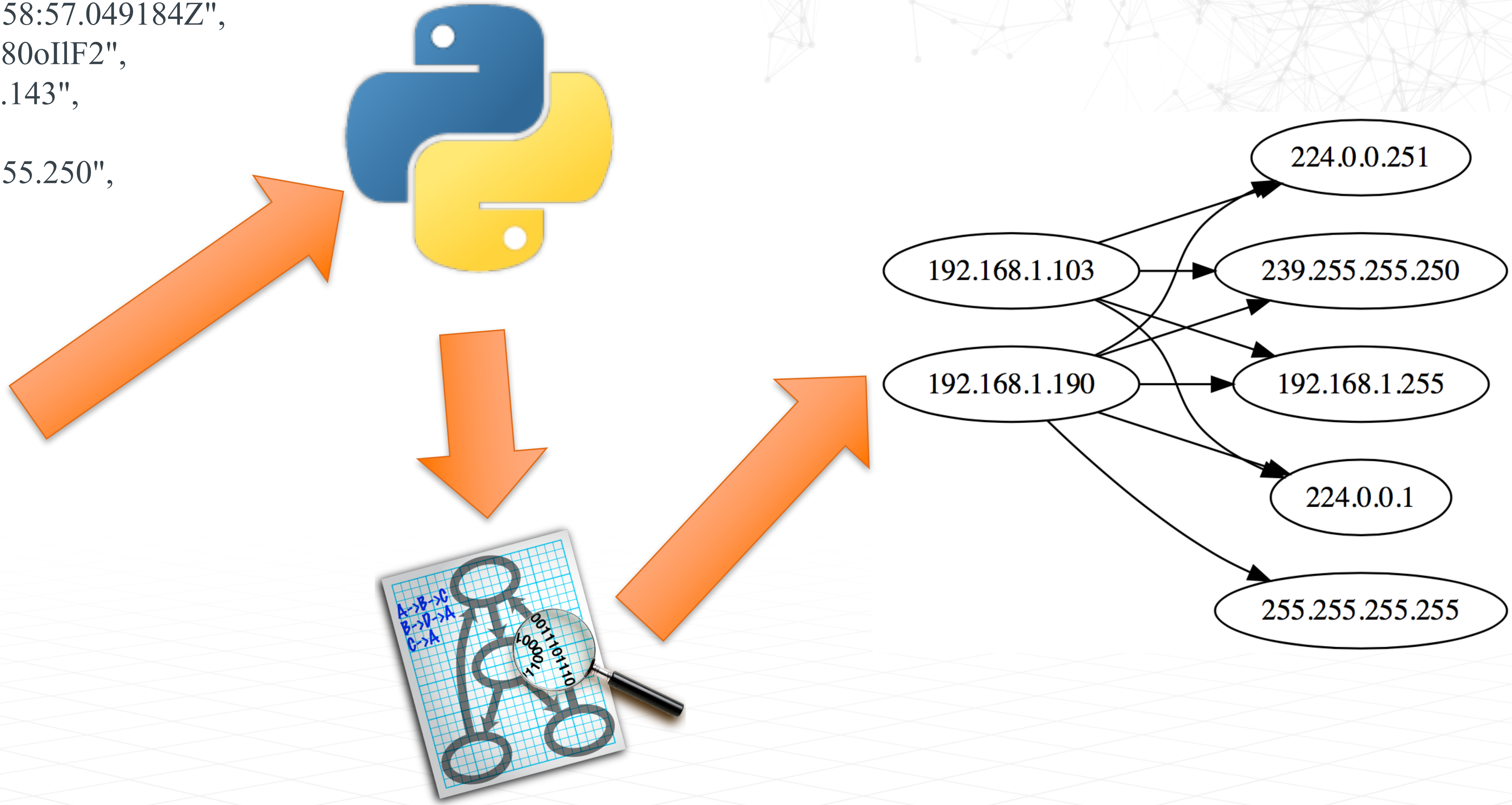
- What systems if any are beaconing out?
- Where did it beacon out?
- How do I know it was beaconing and not legitimate traffic?



```
{"ts":"2017-05-02T08:58:57.049184Z","uid":"CkEcDTYCQ080oIlF2","id.orig_h":"192.168.1.143","id.orig_p":49204,"id.resp_h":"239.255.255.250","id.resp
_p":1900,"proto":"udp","duration":2.96896,"orig_bytes":700,"resp_bytes":0,"conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,
"history":"D","orig_pkts":4,"orig_ip_bytes":812,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:01.861092Z","uid":"CTMvnq1IvK0oM5H8Cb","id.orig_h":"fe80::a22b:b8ff:fe60:965d","id.orig_p":546,"id.resp_h":"ff02::1:2","id
.resp_p":547,"proto":"udp","conn_state":"S0","local_orig":false,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":14
6,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.168225Z","uid":"CQ5hON2ftGeiU1dJOc","id.orig_h":"fe80::10f2:85f6:ef79:c762","id.orig_p":143,"id.resp_h":"ff02::16","id.
resp_p":0,"proto":"icmp","conn_state":"OTH","local_orig":false,"local_resp":false,"missed_bytes":0,"orig_pkts":1,"orig_ip_bytes":116,"resp_pkts":0
,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.373484Z","uid":"C4Wfwf4gy8vDeHgXqk","id.orig_h":"192.168.1.99","id.orig_p":68,"id.resp_h":"192.168.1.1","id.resp_p":67,
"proto":"udp","service":"dhcp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":
336,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:58:59.608627Z","uid":"C1B6K61MUXA0U6AV15","id.orig_h":"192.168.1.103","id.orig_p":50498,"id.resp_h":"239.255.255.250","id.res
p_p":1900,"proto":"udp","duration":2.96972,"orig_bytes":700,"resp_bytes":0,"conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0
,"history":"D","orig_pkts":4,"orig_ip_bytes":812,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.782701Z","uid":"CDdYP827cVsEEtj3l","id.orig_h":"192.168.1.190","id.orig_p":50837,"id.resp_h":"192.168.1.255","id.resp_p
":8612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_p
kts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.782717Z","uid":"COyMD426ckvdQPYG88","id.orig_h":"192.168.1.190","id.orig_p":62326,"id.resp_h":"224.0.0.1","id.resp_p":8
612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pkt
s":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:00.532818Z","uid":"CjBg0C1GQZalFbNIA8","id.orig_h":"192.168.1.139","id.orig_p":61809,"id.resp_h":"239.255.255.250","id.res
p_p":1900,"proto":"udp","duration":3.069253,"orig_bytes":696,"resp_bytes":0,"conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":
0,"history":"D","orig_pkts":4,"orig_ip_bytes":808,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.137956Z","uid":"Ca6wuQDuWDrNaatv3","id.orig_h":"192.168.1.98","id.orig_p":55679,"id.resp_h":"192.168.1.255","id.resp_p"
:8612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pk
ts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.138017Z","uid":"COfyhN2rpMSvxKaak5","id.orig_h":"192.168.1.98","id.orig_p":53943,"id.resp_h":"224.0.0.1","id.resp_p":86
12,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pkts
":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.445329Z","uid":"CwhfDf4hDN8jhiMeg5","id.orig_h":"192.168.1.103","id.orig_p":65507,"id.resp_h":"192.168.1.255","id.resp_
p":8612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_
pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.445340Z","uid":"CrUzb2X89R06epvsi","id.orig_h":"192.168.1.103","id.orig_p":57063,"id.resp_h":"224.0.0.1","id.resp_p":86
12,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pkts
":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:56.237795Z","uid":"CyqgAw3Z1b2jXI6Kri","id.orig_h":"192.168.1.73","id.orig_p":5353,"id.resp_h":"224.0.0.251","id.resp_p":5
353,"proto":"udp","service":"dns","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_byt
es":143,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:58:59.199071Z","uid":"CKEdXM13bhgvwjqi5","id.orig_h":"fe80::10f2:85f6:ef79:c762","id.orig_p":133,"id.resp_h":"ff02::2","id.re
sp_p":134,"proto":"icmp","duration":8.703862,"orig_bytes":16,"resp_bytes":0,"conn_state":"OTH","local_orig":false,"local_resp":false,"missed_bytes
```

Process: High Level

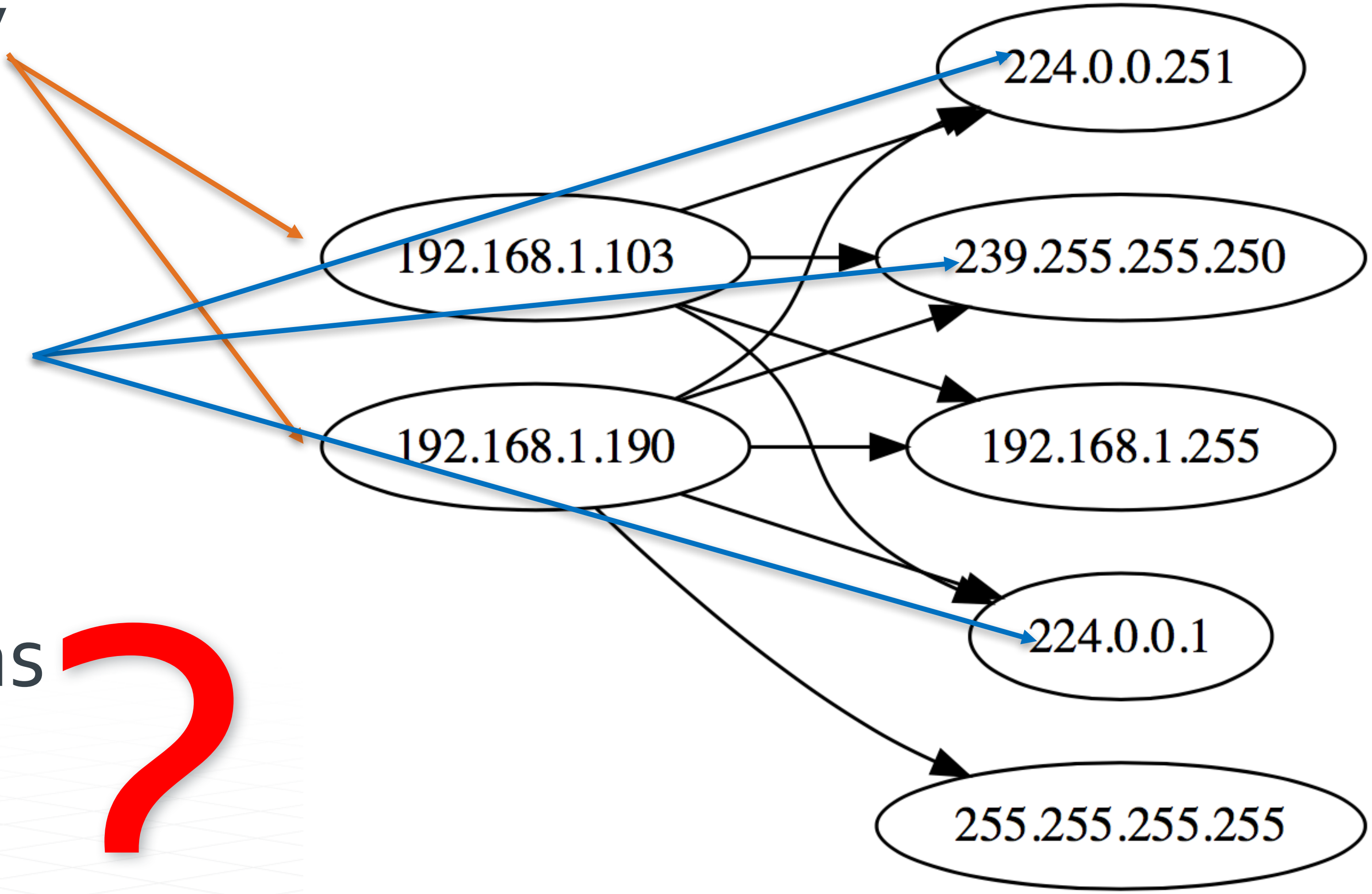
{"ts":"2017-05-02T08:58:57.049184Z",
"uid":"CkEcDTYCQO80oIlF2",
"id.orig_h":"192.168.1.143",
"id.orig_p":49204,
"id.resp_h":"239.255.255.250",
"id.resp_p":1900,
"proto":"udp",
"duration":2.96896,
"orig_bytes":700,
"resp_bytes":0,
"conn_state":"S0",
"local_orig":true,
"local_resp":false,
"missed_bytes":0,
"history":"D",
"orig_pkts":4,
"orig_ip_bytes":812,
"resp_pkts":0,
"resp_ip_bytes":0,
"tunnel_parents":[]}



relationships

- What systems if any are beaconing out?
- Where did it beacon out?
- How do I know it was beaconing and not legitimate traffic?

?



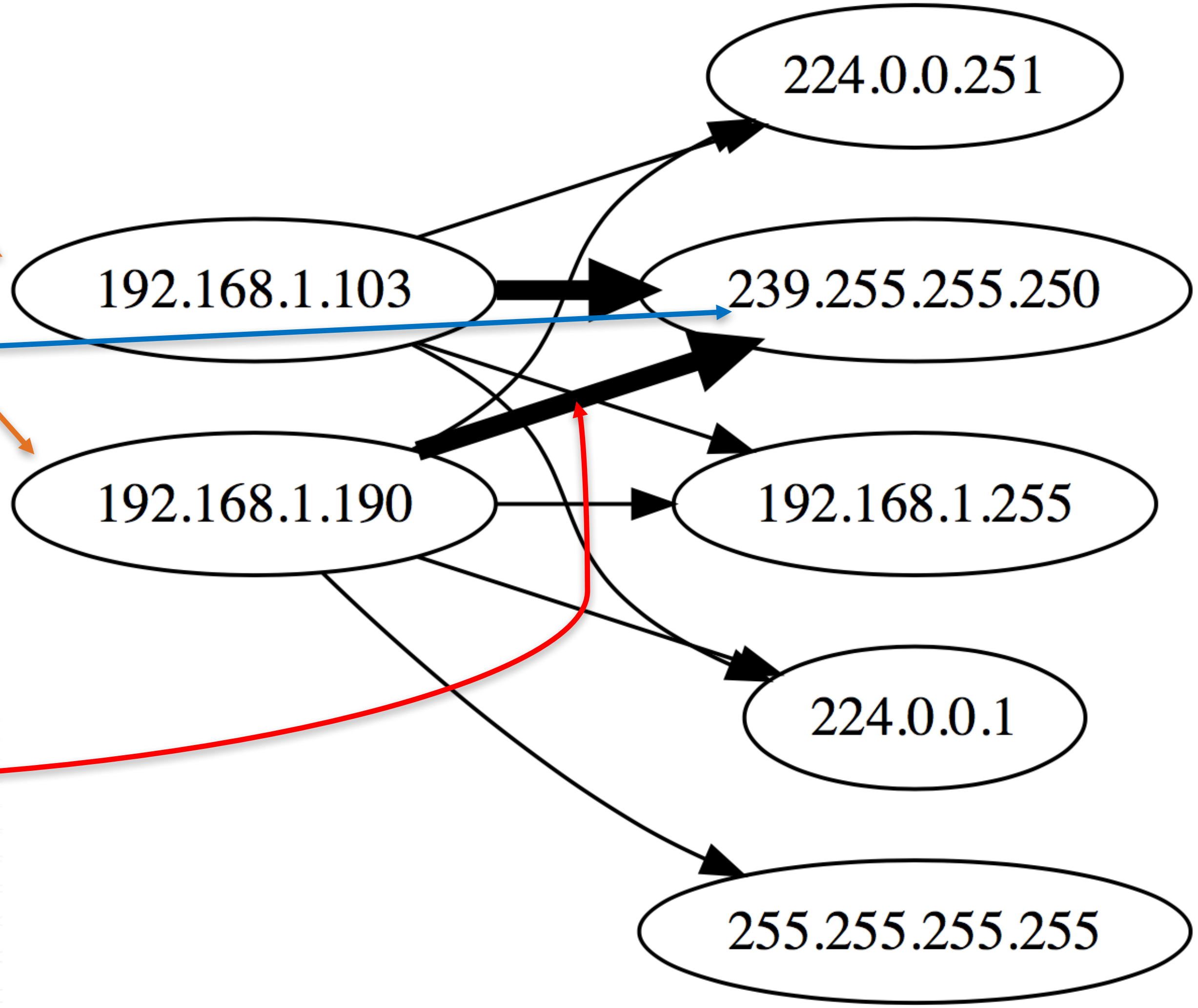
Explain what I found to my management

sqrrl

- What systems if any are beaconing out?

- Where did it beacon out?

- How do I know it was beaconing and not legitimate traffic?



Justify my time to Hunt

Log Crawling

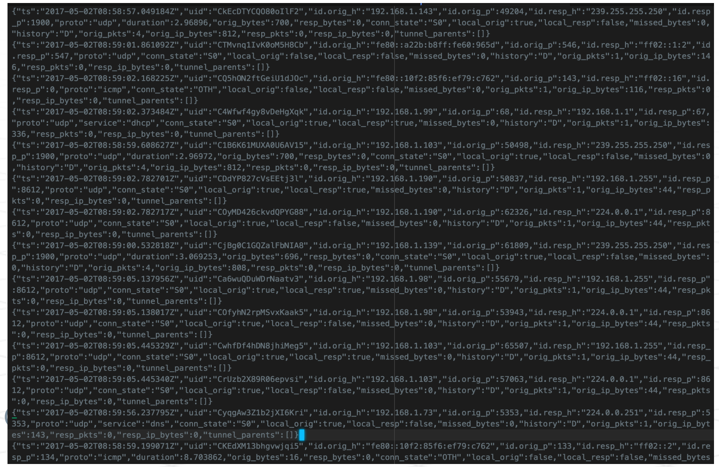
- Cost of hunt
- 8 hours
- $50/hr
- $400/day

Explain what I found to my management

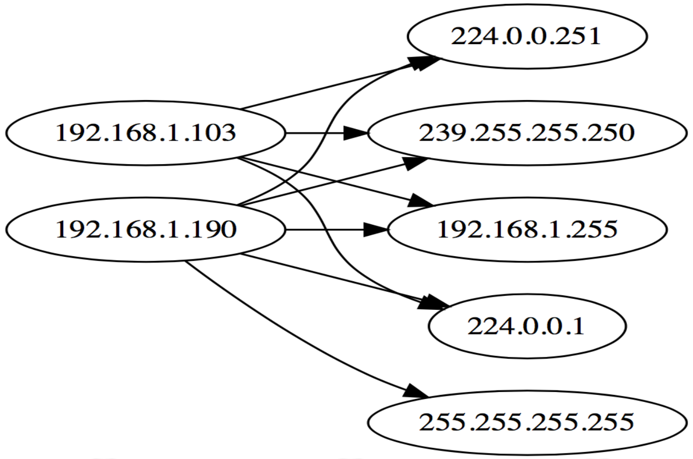
- Cost of hunt
- 4 hours
- $50/hr
- $200/day

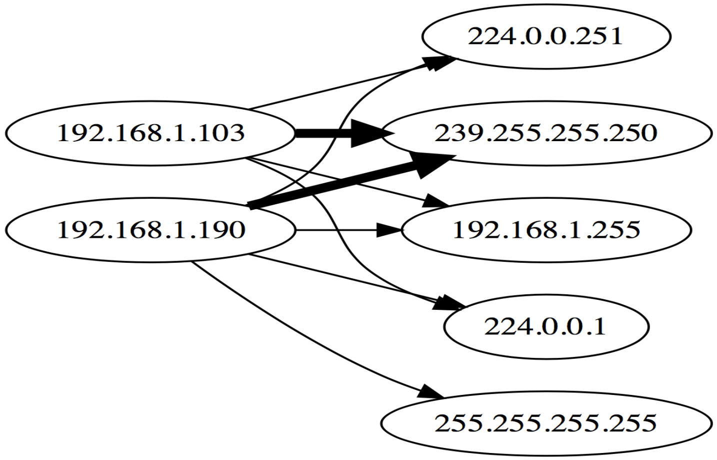
Actionable Hunting

- Cost of hunt
- 2 hours
- $50/hr
- $100/day



```
{"ts":"2017-05-02T08:58:57.049184Z","uid":"CkEcDTYCQ080oIlF2","id.orig_h":"192.168.1.143","id.orig_p":49204,"id.resp_h":"239.255.255.250","id.resp
_p":1900,"proto":"udp","duration":2.96896,"orig_bytes":700,"resp_bytes":0,"conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,
"history":"D","orig_pkts":4,"orig_ip_bytes":812,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:01.861092Z","uid":"CTMvnq1IvK0oM5H8Cb","id.orig_h":"fe80::a22b:b8ff:fe60:965d","id.orig_p":546,"id.resp_h":"ff02::1:2","id
.resp_p":547,"proto":"udp","conn_state":"S0","local_orig":false,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":14
6,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.168225Z","uid":"CQ5hON2ftGeiU1dJOc","id.orig_h":"fe80::10f2:85f6:ef79:c762","id.orig_p":143,"id.resp_h":"ff02::16","id.
resp_p":0,"proto":"icmp","conn_state":"OTH","local_orig":false,"local_resp":false,"missed_bytes":0,"orig_pkts":1,"orig_ip_bytes":116,"resp_pkts":0
,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.373484Z","uid":"C4Wfwf4gy8vDeHgXqk","id.orig_h":"192.168.1.99","id.orig_p":68,"id.resp_h":"192.168.1.1","id.resp_p":67,
"proto":"udp","service":"dhcp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":
336,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:58:59.608627Z","uid":"C1B6K61MUXA0U6AV15","id.orig_h":"192.168.1.103","id.orig_p":50498,"id.resp_h":"239.255.255.250","id.res
p_p":1900,"proto":"udp","duration":2.96972,"orig_bytes":700,"resp_bytes":0,"conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0
,"history":"D","orig_pkts":4,"orig_ip_bytes":812,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.782701Z","uid":"CDdYP827cVsEEtj3l","id.orig_h":"192.168.1.190","id.orig_p":50837,"id.resp_h":"192.168.1.255","id.resp_p
":8612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_p
kts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:02.782717Z","uid":"COyMD426ckvdQPYG88","id.orig_h":"192.168.1.190","id.orig_p":62326,"id.resp_h":"224.0.0.1","id.resp_p":8
612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pkt
s":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:00.532818Z","uid":"CjBg0C1GQZalFbNIA8","id.orig_h":"192.168.1.139","id.orig_p":61809,"id.resp_h":"239.255.255.250","id.res
p_p":1900,"proto":"udp","duration":3.069253,"orig_bytes":696,"resp_bytes":0,"conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":
0,"history":"D","orig_pkts":4,"orig_ip_bytes":808,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.137956Z","uid":"Ca6wuQDuWDrNaatv3","id.orig_h":"192.168.1.98","id.orig_p":55679,"id.resp_h":"192.168.1.255","id.resp_p"
:8612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pk
ts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.138017Z","uid":"COfyhN2rpMSvxKaak5","id.orig_h":"192.168.1.98","id.orig_p":53943,"id.resp_h":"224.0.0.1","id.resp_p":86
12,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pkts
":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.445329Z","uid":"CwhfDf4hDN8jhiMeg5","id.orig_h":"192.168.1.103","id.orig_p":65507,"id.resp_h":"192.168.1.255","id.resp_
p":8612,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_
pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:05.445340Z","uid":"CrUzb2X89R06epvsi","id.orig_h":"192.168.1.103","id.orig_p":57063,"id.resp_h":"224.0.0.1","id.resp_p":86
12,"proto":"udp","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_bytes":44,"resp_pkts
":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:59:56.237795Z","uid":"CyqgAw3Z1b2jXI6Kri","id.orig_h":"192.168.1.73","id.orig_p":5353,"id.resp_h":"224.0.0.251","id.resp_p":5
353,"proto":"udp","service":"dns","conn_state":"S0","local_orig":true,"local_resp":false,"missed_bytes":0,"history":"D","orig_pkts":1,"orig_ip_byt
es":143,"resp_pkts":0,"resp_ip_bytes":0,"tunnel_parents":[]}
{"ts":"2017-05-02T08:58:59.199071Z","uid":"CKEdXM13bhgvwjqi5","id.orig_h":"fe80::10f2:85f6:ef79:c762","id.orig_p":133,"id.resp_h":"ff02::2","id.re
sp_p":134,"proto":"icmp","duration":8.703862,"orig_bytes":16,"resp_bytes":0,"conn_state":"OTH","local_orig":false,"local_resp":false,"missed_bytes
```





Questions?

"I use Sqrrl to find those dark places in my environment, poke it with a stick, and see what crawls out."
-Ryan Nolette