A07 – Zeek Logs

**10 points**  
Turn in a Word or PDF document to the D2L Dropbox

# Overview

In this lab, you will use Zeek logs and Security Onion to look at information collected from a traffic capture and derive conclusions about the traffic.

## Security Onion Setup

Using the security onion machine provided in the IA Lab, run through the setup. Security onion has been installed but must be configured.

### Credentials

dsu

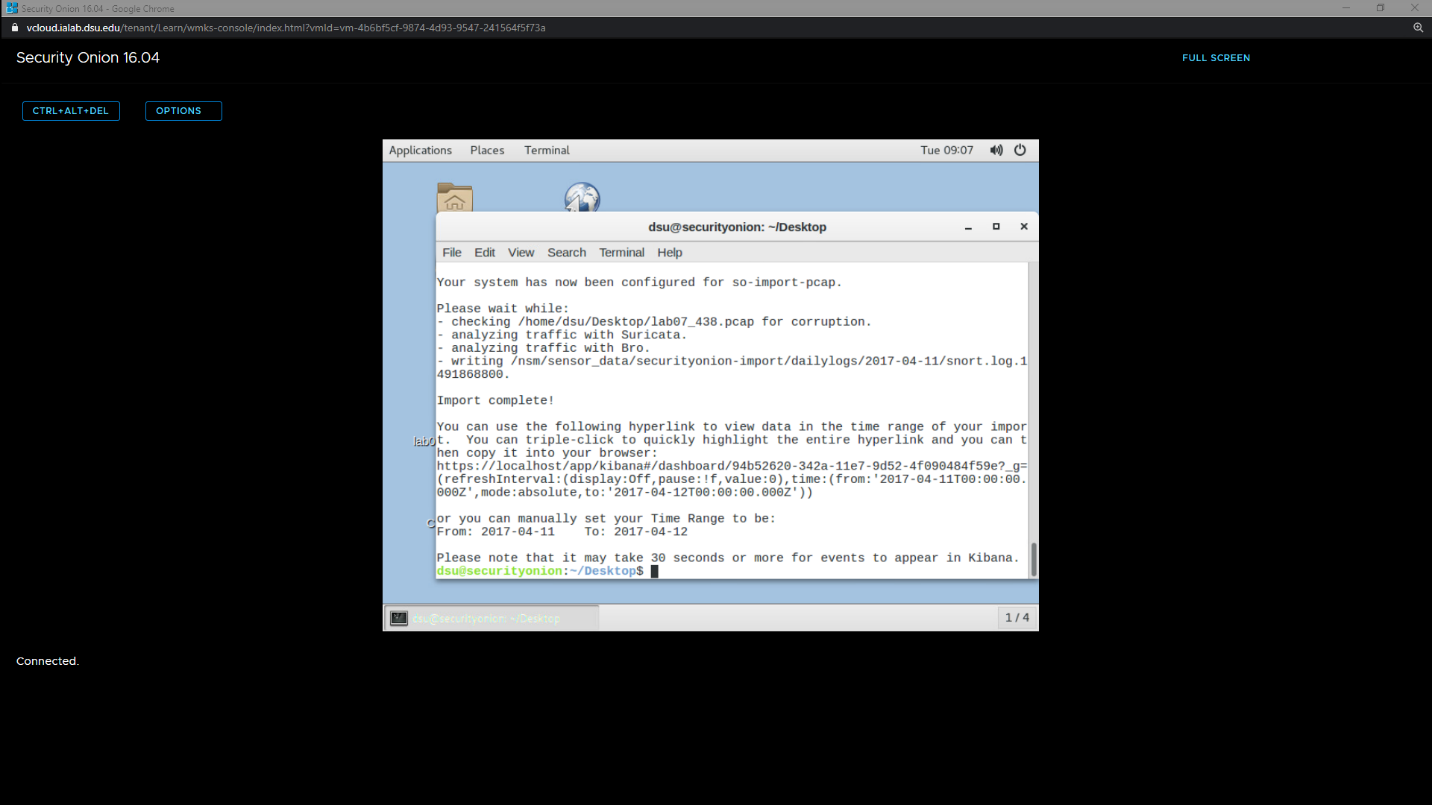
Password1!

### Run the Setup

* 1. Configure the network interfaces
     1. ens192 - Management Interface
        1. Static IP: 192.168.1.5/24
        2. DNS: 8.8.8.8
        3. Domain Name: infs754.local
     2. ens224 - Sniffing Interface
  2. Evaluation Mode
  3. Create a user of your choice

### Load the PCAP

* 1. In a terminal run the following command:
     1. sudo so-import-pcap ~/Desktop/lab07\_438.pcap
     2. **Submit a screenshot of this command successfully completing.**



## Investigation Questions

Use either your newly setup Security Onion VM, or the online server at <https://zeeklab.dakotastate.net/app/kibana> to complete this lab.

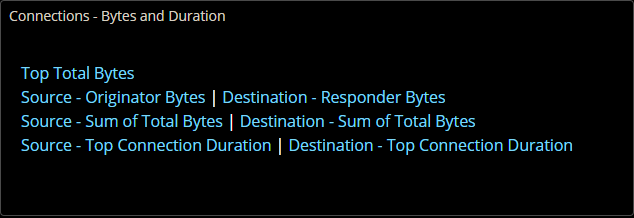
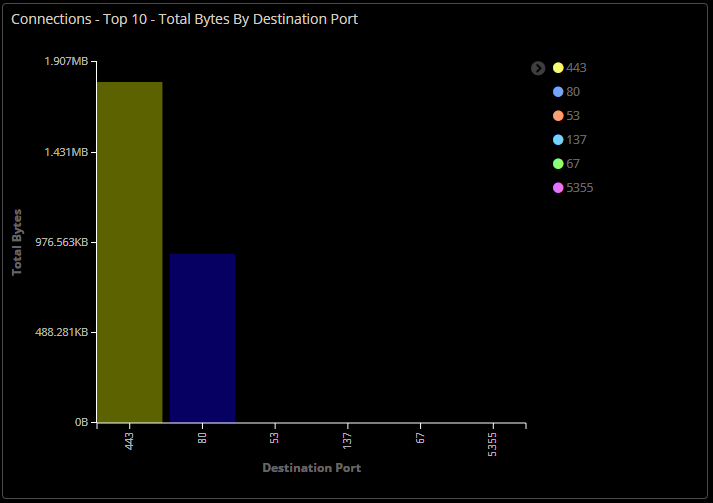
dsu

Password1!

All of the traffic you should be using for this lab occurred on April 10, 2017. Be sure to adjust your time range accordingly.

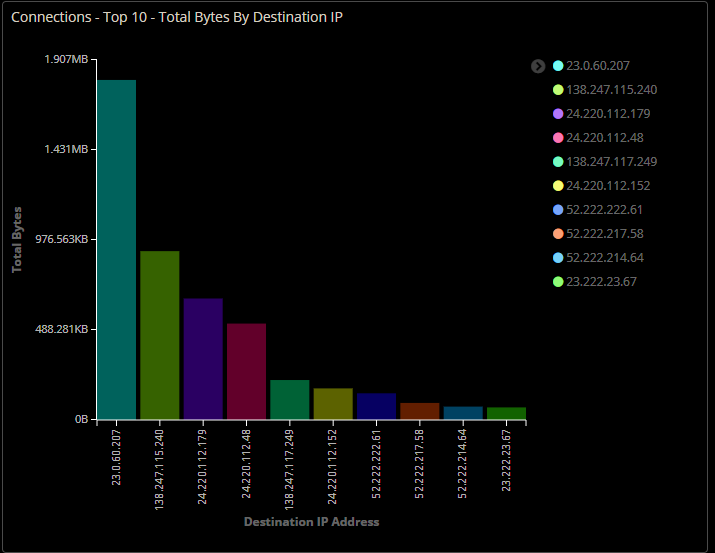
Answer the following questions below with both the answer AND a screenshot showing how you got your results.

1. What are the two most common destination ports for 192.168.19.225, by total bytes transferred?

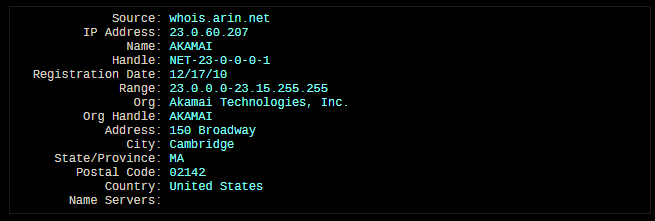
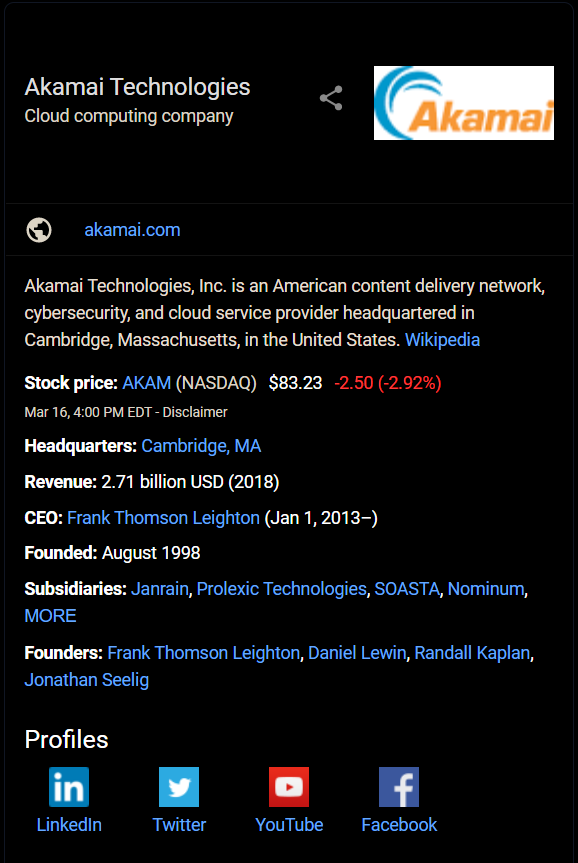
Applied filter: “source\_ip is 192.168.19.225” clicked on “Top total bytes” in ‘bytes and duration’ and found ports 443 and 80  
   


1. What destination IP did 192.168.19.225 talk to most, in terms of bytes?

23.0.60.207

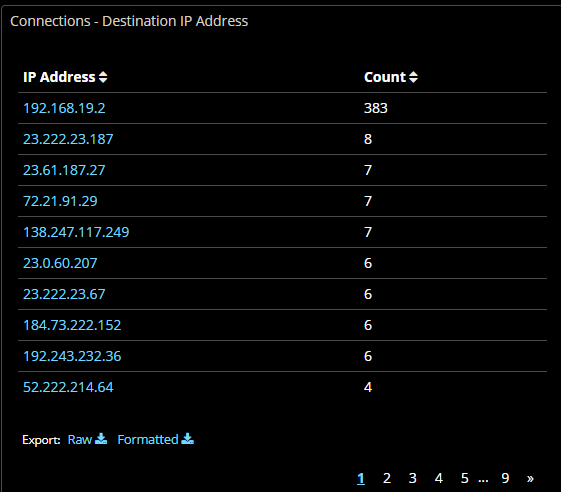


* 1. Can you figure out what this IP is?

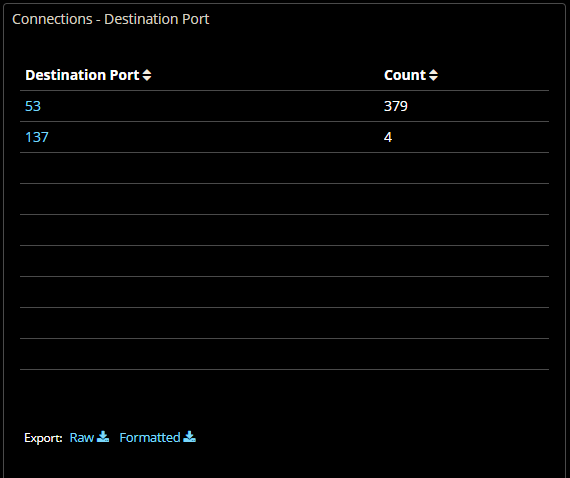
Looks like an Ip that belongs to a company called akamai. When I navigate in browser to the ip over 443 and 80 I get destination unreachable. Akamai is a cloud computing, cybersecurity, and content delivery network which -according to quora- services 15-30% of all web traffic. I would guess that it is an internal webserver, as the traffic is exclusively over port 443 IP and it is not accessible to the general public, or maybe it tunnels a different protocol over port 443. I’m not sure how content delivery works myself, like Netflix and youtube videos. How do those look on a network – are they sent over 443?   
  


1. What destination IP did 192.168.19.225 talk to most, in terms of number of connections?

192.468.19.2 with 383 connections

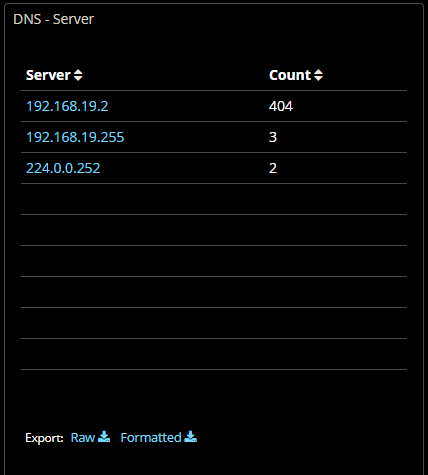


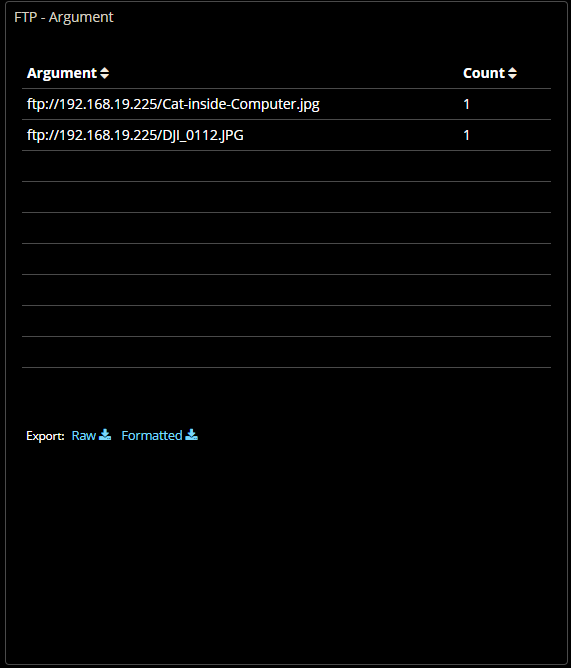
* 1. Can you figure out what this IP is?

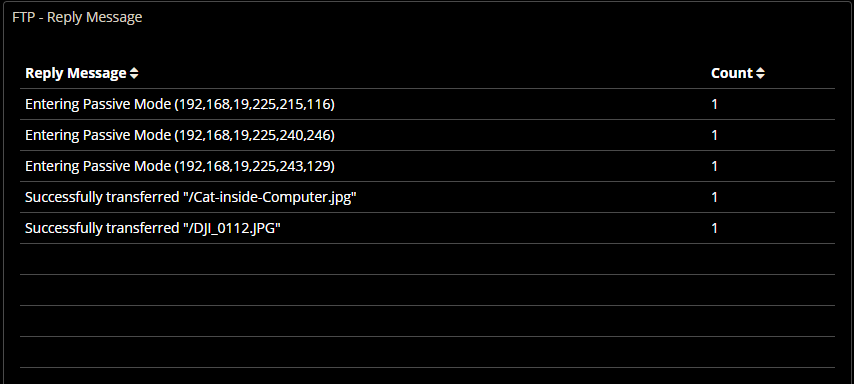
By adding that destination as a filter on top of our current source filter, we can see the traffic going between the two, and it’s probably a dns server.  


1. How many DNS requests did 192.168.19.225 make? What server was it using?

404 requests using 192.168.19.2, there were a few broadcasts to find the server, and a self-assigned address for a bit.

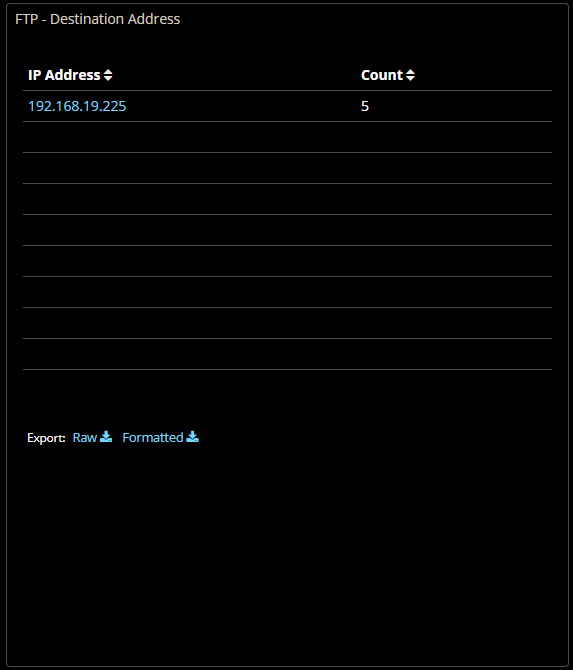


1. What two file names were downloaded from the FTP server?   
   Cat-inside-computer.jpg   
   and   
   DJI\_0112.JPG  
   found under the ftp tab

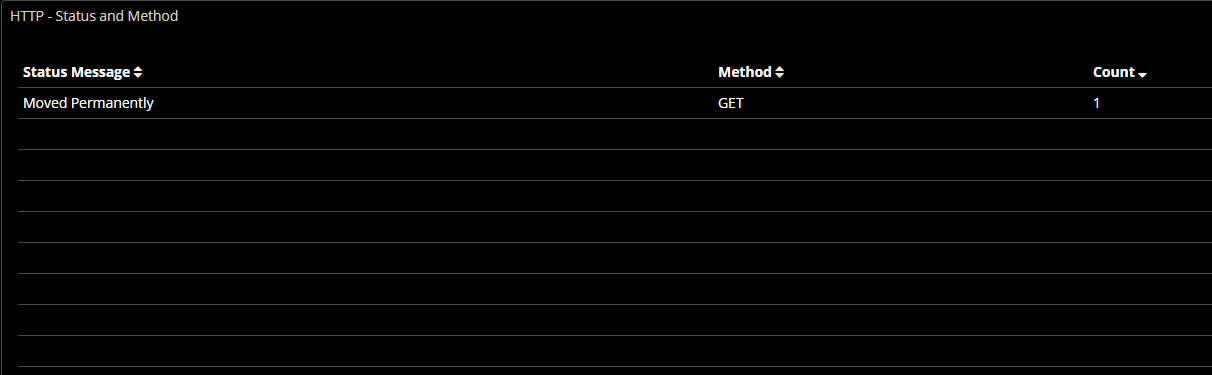
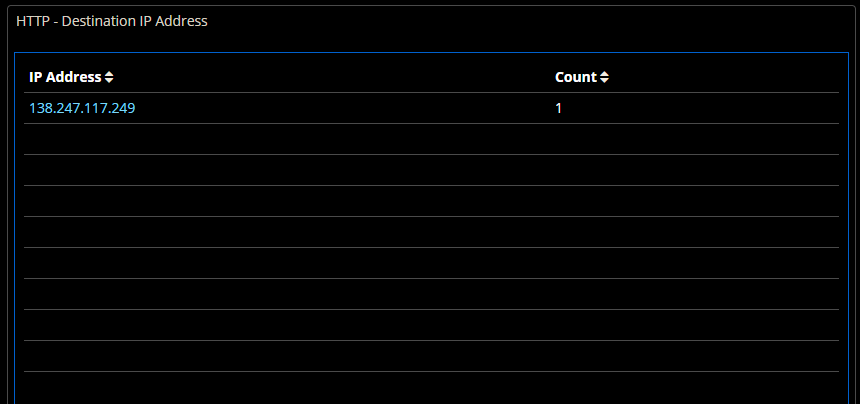


1. What system was browsing to the FTP server? That is, what IP address is the client at?

192.168.19.225 is the only ip that navigated to the ftp server



1. When browsing to a website, 192.168.19.225 got an HTTP 301 Moved Permanently response. Which IP address provided this response?

On the http tab, filtering for “moved permanently” status messages, and then scrolling down to the addresses we find 138.247.117.249  


1. Bro found quite a bit of traffic that it categorized as weird. What were they? Conduct a bit of research – would you say this traffic is weird? Would you say it is malicious?

IP header length is supposed to have a minimum of 5, and the unknown protocol followed it in a matter of seconds. It’s odd, and isolated, but it was only two packets over a matter of seconds, and there is no source/destination information for either packet so there isn’t any information going to or from anyone. It was probably just a malformed packet, or maybe the interface picked up interference / crosstalk. I wouldn’t say yet that it is malicious.

