Lesson Plan  
BitTorrent Detection Challenge

short line

# Summary

1. Preparation
2. Goal
3. Lab
4. Answer

# Preparation

* Kali VM
* Download
  + Starter Code.py: <https://drive.google.com/file/d/1yGe4OxdIu-HSWRNEU9O6-dg6qhlFhyn0/view?usp=sharing>
  + BitTorrent\_multiple.pcap: <https://drive.google.com/file/d/1lLuB0kqEEB5Pxi5Zt1fRl130UQsbwpIO/view?usp=sharing>
  + BitTorrent\_mixed.pcap: <https://drive.google.com/file/d/1Fl_rNEiK3FlS7fch_Itv5j7huicFWOiN/view?usp=sharing>
  + BitTorrent\_single.pcap: <https://drive.google.com/file/d/1CEBvlnavrWUna-ROteuKBaGe5A-1Z0IB/view?usp=sharing>

# Goal

* Be able to analyze a specific protocol and find a pattern.
* Wireshark automatically categorizes protocols for us and it even knows when BitTorrent handshakes happen.
  + This is not magic. Packets do not come in saying I am protocol ‘BitTorrent’. They all come in bits. Think about how wireshark knows when BitTorrent traffic comes in, and create that algorithm in python.

# 

# Lab

## Bittorrent Detection

* + You are a new hire network analyst / Security Engineer of a big company. On your first day, you are monitoring company network traffic and you find someone using BitTorrent! Looking back into network logs, this wasn't the first time using BitTorrent in the company! To make things worse, its multiple employees downloading stuff through BitTorrent!
  + Your mission is to be that awesome new employee who will create an algorithm to DETECT any employees in company network using BitTorrent
  + Starter Code is given.

# !!SPOILER ALERT!!

# ====================Answer=====================

Detection.py: <https://drive.google.com/file/d/1YWc3-RteTy272pnsSOnALv-DzMIpYZB9/view?usp=sharing>