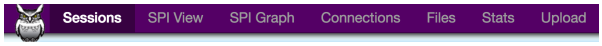
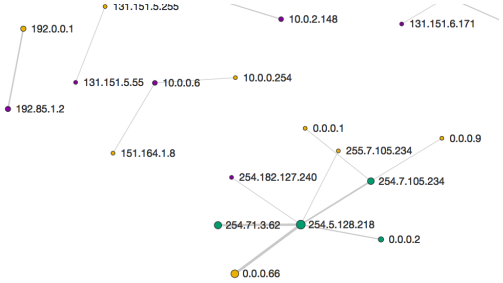
Molochチートシート





メインで利用するタブの解説
(フクロウマーク) –ヘルプ
Sessions – パケットを閲覧、検索が可能
SPI View – L7レイヤーで解析した結果を表示
SPI Graph – L7レイヤーの解析結果をグラフで表示
Connections –ネットワーク全体の通信をノードグラフで表示

検索クエリ表記
・演算子 == != < > <= >= && || ()
・ワイルドカード利用可能 *、? (1文字) 例) http.uri == "www.f*k.com"
・正規表現利用可能/で開始 例) http.uri == /.*www¥.f.*k¥.com.*/.
・リスト表記可能例) protocols == [http, ssh]
・数値比較可能例) bytes <= 10000
・IPは IP表示、部分マッチ、CIDR、ポート指定でサーチ可能 例) ip == 1.2.3/24:80
・存在の確認 例) host.http == EXISTS!

よく使う検索対象フィールド
http.location アクセス先 Scheme+ホスト名+Path
http.uri アクセス先 ホスト名+Path
http.uri.path アクセス先 Path
http.content-type コンテンツタイプ
http.method
http.referer
http.user-agent
http.bodymagic blibfile/magicを利用してcontent-typeを判別
host ホスト名
host.http ホスト名(httpプロトコルのみ)
ip ipアドレス
ip.dst ipアドレス(宛先)
ip.src ipアドレス(送信元)
port ポート番号
protocols プロトコル 認識できる主なプロトコルは http ssh dns email smb tls socks
bytes セッション中の送受信バイト
bytes.dst セッション中の送信バイト(宛先)
bytes.src セッション中の送信バイト(送信元)
tags タグで検索。yaraルールでタグを設定してます。

TIPS
・connections タブはネットワーク全体を可視化。例えば、protocols == smb とフィルタをかけると想定していないsmb通信を見つけることができます。
・yaraルールを設定可能。事前に設定した攻撃検知用ルールは、shellshock: CVE_2014_6271、S2_045 : CVE_2017_5638(struts2)、S2_046 : CVE_2017_5638(strusts2)、SMB_EthernalBlue: MS17_010(smb)です。
検索例) tags == yara:shellshock
競技開始後に売上モニタリング用yaraルールとして P_Success: Buy_Successedを提供予定。ウェブサイトで商品が購入された際のhttp.locationやhttp.methodを用いてトレースできるようにします。
・自分たちで作成したyaraルールの投入はサポートまでお問い合わせください。(マネージドの場合、リクエストに応じてこちらで作成します。)
・検索クエリは検索窓の右の目玉アイコン から Viewを作成することもできます。
・molochは調査用の深掘りツールですが、全てのパケットがキャプチャされるため、監視にも応用できます。その場合は、こまめにF5を押しください。
・SPI Graphで SPI Graph: host.http のように設定し、host単位でのhttpアクセスグラフを表示できます。