**Monitorando o tráfego de rede com o ‘top’:** No splunk temos o comando ‘top’ aonde é útil para monitorar o tráfego de rede permitindo a identificação de computadores maliciosos que estão enviando muitas solicitações a um servidor web. Filtrando a busca por um endereço IP é possível observar quais maquinas estão gerando mais requisições identificando atividades suspeitas.

**URI** (**Uniform Resource Identifier):** é qualquer identificador padrão de um recurso — pode ser um link, um e-mail, um livro, um dado. Se ele **identifica de forma única**, é uma URI!

**URL (Uniform Resource Locator):** É **um tipo de URI** que **especifica o endereço completo** para acessar um recurso, incluindo o protocolo (como http://) e o caminho.

**Importância de URLs e URIs na investigação:** Durante a investigação é muito importante usar URLs ou URIs para obter melhores detalhes sobre os sites acessados.

**VirusOT:** É uma ferramenta que após identificarmos um URI malicioso, podemos verifica-los e iniciar uma investigação mais aprofundada sobre a origem do trafego anormal. VirusOT também permite identificar computadores que se comunicaram com o URI suspeito.

**Identificando máquinas infectadas na rede:** Após a execução dos comandos anteriores, conseguimos listar todos os computadores que mais se comunicaram com um IP especifico. Isso pode revelar máquinas infectadas ou scanners de rede, ajudando a identificar padrões de comunicação e potenciais ameaças à segurança da rede.

**HTTP (HyperText Transfer Protocol):** é o **protocolo usado para comunicação entre navegadores e servidores web. É o que permite carregar sites na internet**, enviando e recebendo dados entre seu navegador e o servidor.

**Analisando códigos de resposta HTTP:** Analisar códigos de resposta HTTP é crucial para entender o estado do trafego na rede, um exemplo é o código com status acima de 400 podendo identificar problemas como URLs inexistentes(404). Fornece uma visão clara dos padrões de trafego e possíveis vulnerabilidades.