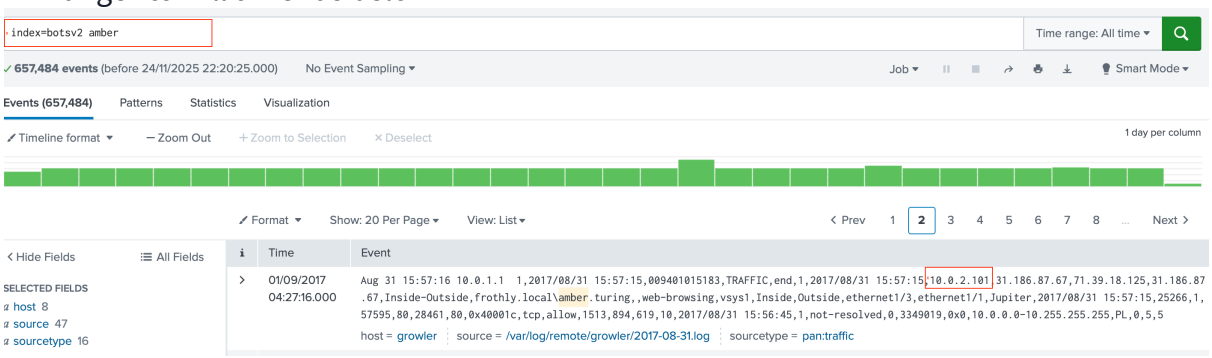
LAB 8 INSTRUCTION – SIEM

1. Read and extract some information from the scenario: view the highlighted keywords

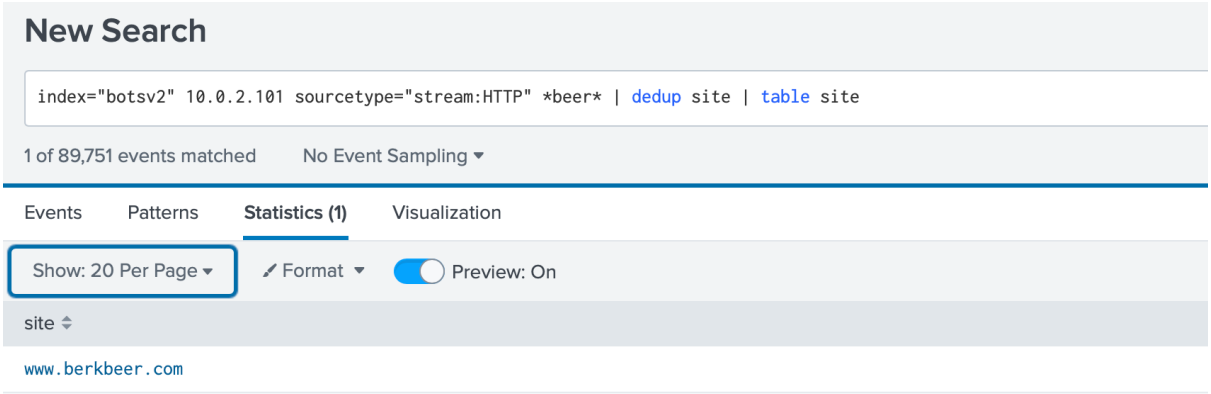
"Scenario: In this exercise, you assume the persona of Alice Bluebird, the analyst who successfully assisted Wayne Enterprises and was recommended to Grace Hoppy at Frothly (*a **beer** company*) to assist them with their recent issues. The focus is on **Amber** Turing and her communication with a competitor."

2. Read: https://help.splunk.com/en/splunk-enterprise/get-started/get-data-in/9.4/configure-indexed-field-extraction/about-default-fields-host-source-sourcetype-and-more
3. Additional material to understand Splunk SPL syntax: https://www.splunk.com/en_us/pdfs/ebooks/exploring-splunk.pdf

4. **Example of finding the answer for the list of questions100 series questions example:**
   Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the **website** domain that she visited?
   a. Find Amber's IP address: Search "index=botsv2 amber" and configure the "Time range" to "All time" as below



   Answer: Amber's IP address: 10.0.2.101
   b. Search for http protocol and src_ip=10.0.2.101 and "beer" ("beer" is the relevant industry), then present the results in a table without duplication
   Protocol: http -> Keyword: sourcetype="stream:http"
   Use keyword "dedup" to avoid duplication
   Use keyword "table" to present the results in table format



5. Correct answers:

Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?

www.berkbeer.com — ✓ Correct Answer

Amber found the executive contact information and sent him an email. What image file displayed the executive's contact information? Answer example: /path/image.ext

/images/ceoberk.png — ✓ Correct Answer

What is the CEO's name? Provide the first and last name.

Martin Berk — ✓ Correct Answer

What is the CEO's email address?

mberk@berkbeer.com — ✓ Correct Answer

After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?

hbernhard@berkbeer.com — ✓ Correct Answer

What is the name of the file attachment that Amber sent to a contact at the competitor?

Saccharomyces_cerevisiae_patent.docx — ✓ Correct Answer

What is Amber's personal email address?

ambersthebest@yeastiebeastie.com — ✓ Correct Answer

What version of TOR Browser did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.

7.0.4 ✓ Correct Answer

What is the public IPv4 address of the server running www.brewertalk.com?

52.42.208.228 ✓ Correct Answer

Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.

45.77.65.211 ✓ Correct Answer

The IP address from Q#2 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URI. Answer example: /phpinfo.php

/member.php ✓ Correct Answer

What SQL function is being abused on the URI path from the previous question?

updatexml ✓ Correct Answer

What was the value of the cookie that Kevin's browser transmitted to the malicious URL as part of an XSS attack? Answer guidance: All digits. Not the cookie name or symbols like an equal sign.

1502408189 ✓ Correct Answer

What brewertalk.com username was maliciously created by a spear phishing attack?

klagerfield ✓ Correct Answer