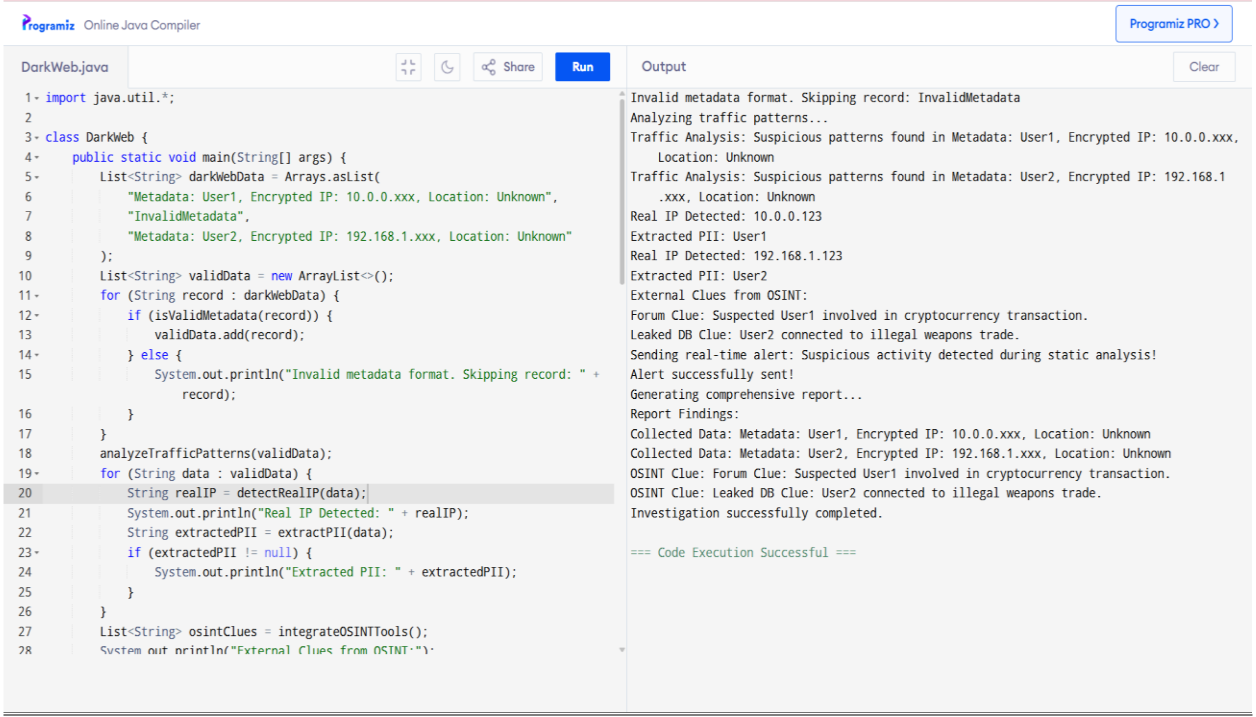
code

```
import java.util.*;

class DarkWeb {
    public static void main(String[] args) {
        List<String> darkWebData = Arrays.asList(
            "Metadata: User1, Encrypted IP: 10.0.0.xxx, Location: Unknown",
            "InvalidMetadata",
            "Metadata: User2, Encrypted IP: 192.168.1.xxx, Location: Unknown"
        );
        List<String> validData = new ArrayList<>();
        for (String record : darkWebData) {
            if (isValidMetadata(record)) {
                validData.add(record);
            } else {
                System.out.println("Invalid metadata format. Skipping record: " + record);
            }
        }
        analyzeTrafficPatterns(validData);
        for (String data : validData) {
            String realIP = detectRealIP(data);
            System.out.println("Real IP Detected: " + realIP);
            String extractedPII = extractPII(data);
            if (extractedPII != null) {
                System.out.println("Extracted PII: " + extractedPII);
            }
        }
        List<String> osintClues = integrateOSINTTools();
        System.out.println("External Clues from OSINT:");
        osintClues.forEach(System.out::println);
        sendRealTimeAlerts("Suspicious activity detected during static analysis!");
        generateComprehensiveReport(validData, osintClues);


        System.out.println("Investigation successfully completed.");
    }
    private static boolean isValidMetadata(String data) {
        return data.startsWith("Metadata: ") && data.contains("Encrypted IP: ") &&
data.contains("Location:");
    }
    private static void analyzeTrafficPatterns(List<String> data) {
        System.out.println("Analyzing traffic patterns...");
        for (String record : data) {
            System.out.println("Traffic Analysis: Suspicious patterns found in " + record);
        }
    }
    private static String detectRealIP(String data) {
        try {
            String ipSegment = data.split("Encrypted IP: ")[1].split(",")[0];
            return ipSegment.replace("xxx", "123"); // Simulate reconstruction of a real IP
        } catch (Exception e) {
            System.out.println("Error detecting real IP: Invalid data format");
            return "Unknown";
        }
    }
    private static String extractPII(String data) {
        try {
            return data.split("Metadata: ")[1].split(",")[0];
        } catch (ArrayIndexOutOfBoundsException e) {
            System.out.println("Error extracting PII: Invalid data format");
            return null;
        }
    }
    private static List<String> integrateOSINTTools() {
        return Arrays.asList(
            "Forum Clue: Suspected User1 involved in cryptocurrency transaction.",
            "Leaked DB Clue: User2 connected to illegal weapons trade."
        );
    }
    private static void sendRealTimeAlerts(String alertMessage) {
        System.out.println("Sending real-time alert: " + alertMessage);
        System.out.println("Alert successfully sent!");
    }
    private static void generateComprehensiveReport(List<String> collectedData,
List<String> osintData) {
        System.out.println("Generating comprehensive report...");
        System.out.println("Report Findings:");
        collectedData.forEach(data -> System.out.println("Collected Data: " + data));
        osintData.forEach(clue -> System.out.println("OSINT Clue: " + clue));
    }
}
```

Output:



```java
import java.util.*;

class DarkWeb {
    public static void main(String[] args) {
        List<String> darkWebData = Arrays.asList(
            "Metadata: User1, Encrypted IP: 10.0.0.xxx, Location: Unknown",
            "InvalidMetadata",
            "Metadata: User2, Encrypted IP: 192.168.1.xxx, Location: Unknown"
        );
        List<String> validData = new ArrayList<>();
        for (String record : darkWebData) {
            if (isValidMetadata(record)) {
                validData.add(record);
            } else {
                System.out.println("Invalid metadata format. Skipping record: " +
                    record);
            }
        }
        analyzeTrafficPatterns(validData);
        for (String data : validData) {
            String realIP = detectRealIP(data);
            System.out.println("Real IP Detected: " + realIP);
            String extractedPII = extractPII(data);
            if (extractedPII != null) {
                System.out.println("Extracted PII: " + extractedPII);
            }
        }
        List<String> osintClues = integrateOSINTTools();
        System.out.println("External Clues from OSINT:");
```

```
Invalid metadata format. Skipping record: InvalidMetadata
Analyzing traffic patterns...
Traffic Analysis: Suspicious patterns found in Metadata: User1, Encrypted IP: 10.0.0.xxx,
    Location: Unknown
Traffic Analysis: Suspicious patterns found in Metadata: User2, Encrypted IP: 192.168.1
    .xxx, Location: Unknown
Real IP Detected: 10.0.0.123
Extracted PII: User1
Real IP Detected: 192.168.1.123
Extracted PII: User2
External Clues from OSINT:
Forum Clue: Suspected User1 involved in cryptocurrency transaction.
Leaked DB Clue: User2 connected to illegal weapons trade.
Sending real-time alert: Suspicious activity detected during static analysis!
Alert successfully sent!
Generating comprehensive report...
Report Findings:
Collected Data: Metadata: User1, Encrypted IP: 10.0.0.xxx, Location: Unknown
Collected Data: Metadata: User2, Encrypted IP: 192.168.1.xxx, Location: Unknown
OSINT Clue: Forum Clue: Suspected User1 involved in cryptocurrency transaction.
OSINT Clue: Leaked DB Clue: User2 connected to illegal weapons trade.
Investigation successfully completed.

=== Code Execution Successful ===
```