Evidence Acquisition and Reports

Cybersecurity

Digital Forensics Day 3

© 2020 Trilogy Education Services, Inc.

Class Objectives

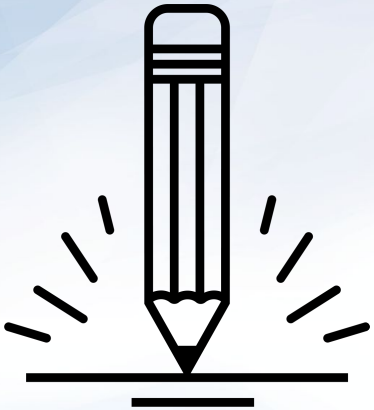
By the end of class, you will be able to:

- Use Autopsy to view and gather evidence from emails.
- Use data exports to analyze email and SMS messages offline.
- Use Autopsy to extract GPS data and identify WiFi locations.
- Prepare a preliminary report of the 2012 National Gallery Case.

As a forensic investigator, it's critical that you understand how to use tools such as Autopsy and know how to **export** data so other team members can perform offline analysis of evidence.

The **.emlx** is a file extension called Mail Message that's used to store email messages.

EMLX files are often referred to as Apple Mail files because they are created with Apple's mail program to store plain text files for a single message.



Activity: Email Export

In this warm-up activity, you will export the email database for offline analysis using examination tools outside of Autopsy.

Suggested Time:
15 Minutes

Tracy’s Email Evidence

Now we'll use offline analysis to uncover details of the National Gallery case.

Email Evidence

We can extract the following evidence from emails:

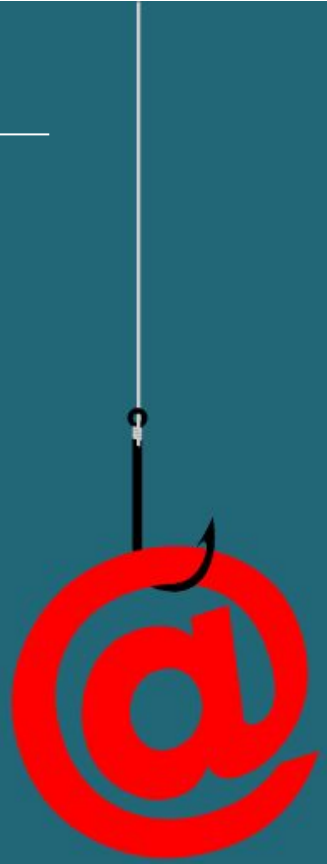
01 Sender’s email address

02 Sender’s IP address

03 Internet Service Provider (ISP)

04 User client (the email app)

05 Location information



Examining Emails in Kali Linux

Displaying email messages in the **INBOX.mbox/Messages** folder is as simple as running the **ls -l** command.

From there, we can review the contents of each EMLX file.

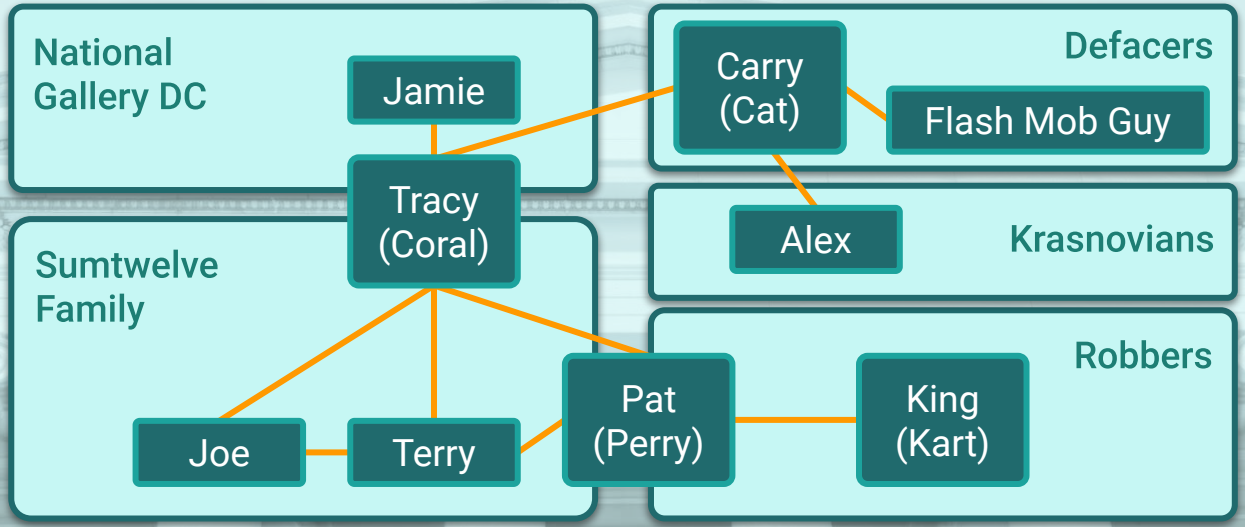

```
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Messages# ls -l
total 7144
-rw-r--r-- 1 root root   24914 May 19 12:19 01FE9965-A923-40CF-A78A-72CE3BD26571.emlx
-rw-r--r-- 1 root root    3758 May 19 12:19 01FE9965-A923-40CF-A78A-72CE3BD26571.emlx-slack
-rw-r--r-- 1 root root 5884773 May 19 12:19 3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
-rw-r--r-- 1 root root    1179 May 19 12:19 3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx-slack
-rw-r--r-- 1 root root 1117462 May 19 12:19 8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
-rw-r--r-- 1 root root     746 May 19 12:19 8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx-slack
-rw-r--r-- 1 root root  121088 May 19 12:19 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
-rw-r--r-- 1 root root    1792 May 19 12:19 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx-slack
-rw-r--r-- 1 root root  136462 May 19 12:19 F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
-rw-r--r-- 1 root root    2802 May 19 12:19 F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx-slack
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Messages#
```

(Source)

Evidence in the Emails

This diagram provides a high-level overview of the threat actors' involvement in the 2012 case.

As you analyze the emails, use this as a roadmap to the Tracy's associates to each incident.

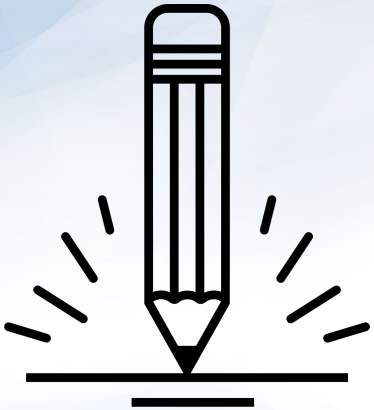


Correspondence Evidence Worksheet

In the next activity, you will use the following worksheet:

Correspondence Evidence Worksheet

- Artifact numbers to help organize records
- Timestamp (time email was sent or received)
- Header information
  - Including names of the individuals involved, their email addresses, and the email subject line.
- Key information
  - Summary of email contents
- Evidence location
  - Source of the data



Activity: Tracy's Email Evidence

In this activity, you will use Autopsy to view Tracy's email correspondence and generate a list of contacts and their email addresses.

Suggested Time:
45 Minutes

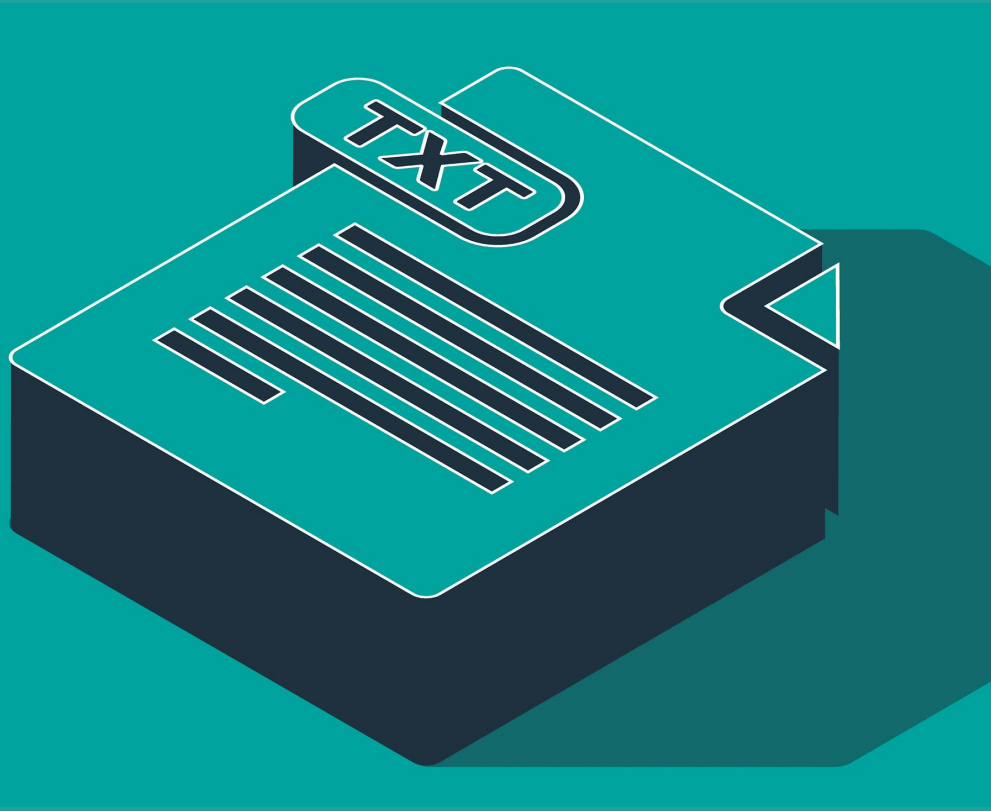
Time’s Up! Let’s Review.


Break

Tracy’s SMS Messages

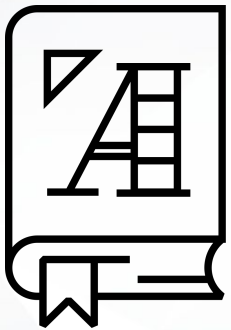
We were able to identify an email attachment called **`needs.txt`** containing a list of tools intended to assist with carrying out the crime.

We'll continue to search for more evidence by examining Tracy's SMS messages.



SMS

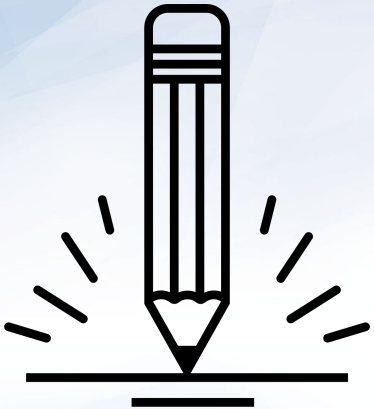

SMS ("short message service") messages are what you know as text messages. They are a person-to-person communication method.
SMS messages can be no more than 918 characters.
SMS messages can and have been used in DoS attacks.



Smishing refers to a social engineering attack performed using SMS messages.

In the following demonstration, we'll walk through different ways of viewing SMS entries.

(Source)



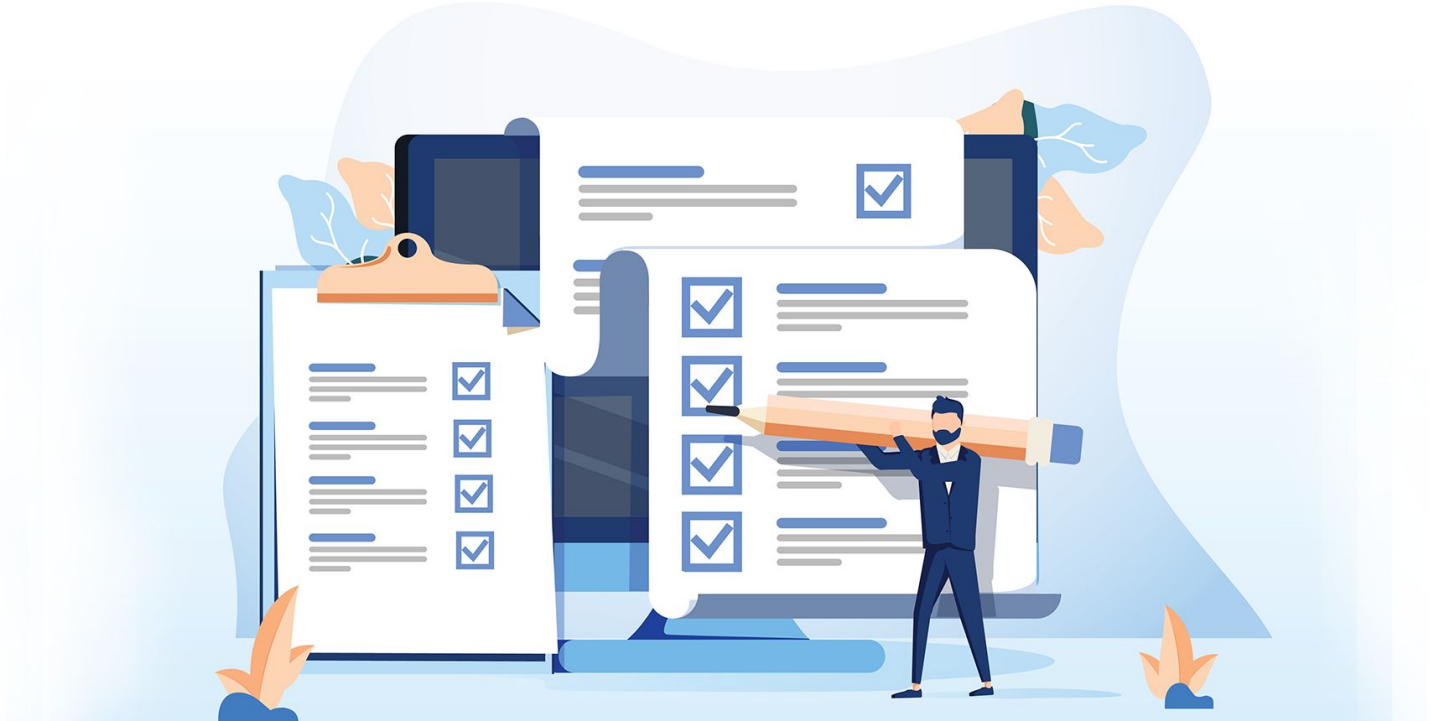
Activity: Tracy's SMS Messages

In this activity, you will work with your group to examine Tracy's SMS messages and gather more information about the case.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

In the final activity, you will conclude your investigation by working in groups to present your findings in a final report.



Unit Recap

We've examined a lot of information and done the following:

01 Performed mobile forensic analysis and compiled details of Tracy's iPhone.

02 Searched through numerous files and directories on the iPhone image.

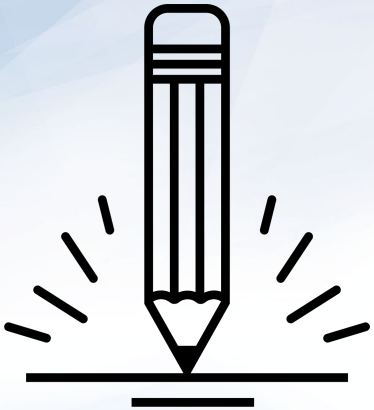
03 Tagged and categorized evidence relevant to the case.

04 Created custom tags.

05 Extracted data for offline analysis using the export function.

06 Examined and documented Tracy's emails.

07 Examined and documented Tracy's SMS messages.



Activity: The Final Report

In this activity, you will start preparing the report of your group's findings. The report will be continued as part of your homework.

Suggested Time:
25 Minutes

Time’s Up! Let’s Review.

You’ll continue your report and work on another bonus assignment for homework.

Digital Forensics Wrap-Up

Digital forensics is a field dedicated to identifying, extracting, preserving, and reporting information obtained from computer and network systems.

Digital forensics relies on the expertise of examiners to analyze and interpret data using trusted forensic examination tools.

Investigative teams may be spread across several time zones, so it's important to follow a standard time zone, as indicated in the case file.

Questions?


The End