Forensic Report

Case Number: UofG01Apr2022
Description: Harassing Emails Investigation
Examiner Name: Pritesh Gandhi Date: 6-04-2023

Examination or Validation Tasking:

Saturn University's teacher Ignis Lee, from Mathematics Department had complained about receiving harassing emails. The teacher Ignis Lee suspects that it is one of the students from his Math 199 class. After the complaint was received the IT Department of Saturn University started an investigation into the matter. The teacher Ignis Lee provided the IT Department with the email screenshots and the header of the email. The mail header showed that the mail originated from the IP address 140.187.78.76 which is a lab in the Saturn University. The Lab was shared by five people and had Ethernet connection but no Wi-Fi access. So, the occupants had set up a Wi-Fi router with no password for it. So, the IT Department of Saturn University had placed a network sniffer on the ethernet port. On Monday 28th February, the teacher received another harassing email. Since all the packets were logged, it was found that the suspects had used anonymouse.org, an anonymous email site. The IT Department has authorized the security team to investigate the packet logs to find the suspect.

The following will provide, proof of evidence in the forensic investigation for the suspected:

1. Finding the MAC address of the suspect.
2. Finding the suspects name along with the MAC Address

The examination will follow the systemic objectives as follows:

1. Examining the (.pcap) file which contains the packet logs.
2. Finding out the Harassing Messages.
3. Determining the IP address and MAC address of the suspect.
4. Figuring out which student has sent the messages.

The tools used in the investigation were:

1. Kali Linux OS (Linux kali 6.0.0-kali3-686-pae #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) i686 GNU/Linux)
2. MD5 Checksum (https://emn178.github.io/online-tools/md5_checksum.html)

3. Wireshark (Wireshark Foundation)

The examination criteria for the forensic investigation of packets log file:

1. Describe the evidence found during investigation.
2. Detect activities of suspect to find more information.
3. Find the suspect in question.

Steps Taken:

1. A forensic copy of the (.pcap) files which contain the packets log was created.

   This was done to make sure that the file is not tainted during the investigative process.

2. The MD5 checksum of the File was verified against the chain of custody.

   The result was ***"785b9b7260eb061d4f79c8074432bec8"*** *which is same as the value of the checksum found before the investigation.*

   This takes place to ensure the validity of the file and guarantees a tamper free investigation.

3. The Wireshark application is opened, and the file is provided in the application workspace.

   This step is done to open the packets file and provide a workspace for investigation.

4. The filter option is used to find the keyword "anonymouse".

   The file contains a lot of packets and their information, to ease the process of investigation and find the website the filter is used to only show required packets. The command used in the filter:

   http.host contains "anonymouse"

   The anonymouse.org is a website and thus will have the "http" protocol.
   "HTTP" stands for "Hyper Text Transfer Protocol". The command "http.host" filters the search to only "http" protocol which makes it easier to find. The http packet contains the website name and the request. So that is why we use "contains "anonymouse"" which is the name of the website.

5. The http “post” request packet is selected, and the harassing message is found.

   In Wireshark, if we select a packet, the packet information is displayed in the console. We selected the post request to get the text body of the frame. The information displayed by the console contains Frame information along with ***the frame number, which is 3913****, Ethernet Information, Internet Protocol Version, TCP (Transmission Control Protocol), Hypertext Transfer Protocol and HTML Form URL Encoded.*

   Since HTTP protocols have plain text transmissions, if we open the HTML form URL Encoded dropdown and look at the information, we will find the harassing message and the teacher Ignis Lee’s email ID.

6. The packet is further investigated to find the IP address of anonymouse.com and MAC address of both sender and receiver.

   In the same frame that we opened before we can use the Internet Protocol Version dropdown to find the IP address of source and destination. The source is the Anonymouse.org website and the destination is of teacher Ignis Lee.

   IP Address Source: 192.168.137.218
   IP Address Destination: 193.200.150.82

   In the same frame, if we open the Ethernet dropdown, we find the MAC address of source and destination. Here, the destination MAC address is of the teacher Ignis Lee, but the source MAC is not of anonymouse.org but of the suspect we are trying to find.

   MAC Address Source: 1c:1b:b5:6d:51:0f
   MAC Address Destination: 0a:5b:d6:62:44:d1

   MAC address stands for Media Access Control Address. The MAC address is also known as the hardware ID number. So, it is the ID of the machine used by the suspect.

7. The filter is used to show the MAC address of the suspect along with cookies using that MAC.

   The command we use to filter now:
   eth.addr == 1c:1b:b5:6d:51:0f && frame contains “Cookie”

   The “eth.addr” command is used to find a specific MAC address. We use the command to find the MAC of the suspect found in step 6. The frame contains part finds the cookies which contain data like name, id etc. Both parts are used simultaneously to find only those packets which satisfy both conditions.

8. The list of packets shown by the command is investigated and the name is found.

   All the packets need to be scanned one by one to find any information like name or ID. The name is found in one of the ***packets numbered 2647****.*

9. The filter is used to investigate and collaborate more information like Timestamp and OS.

   The command used:
   eth.addr == 1c:1b:b5:6d:51:0f && http

   The command finds all the packets linked with MAC address of the suspect and the one with "http" protocol.

   The investigation of these packets shows that "Johnson Crossby" was using the ***"kgbook.com" on 28th February 2022 i.e., Monday at 7:24:22 pm GMT.***

   The investigation also shows that "Johnson Crossby" was using ***"anonymouse.com" on 28th February 2022 i.e., Monday at 7:25:04 pm GMT.***

   The investigation of the packets ***after using "anonymouse.com"*** *shows that "Johnson Crossby" was again using the* ***"kgbook.com" on 28th February 2022 i.e., Monday at 7:25:50 pm GMT.***

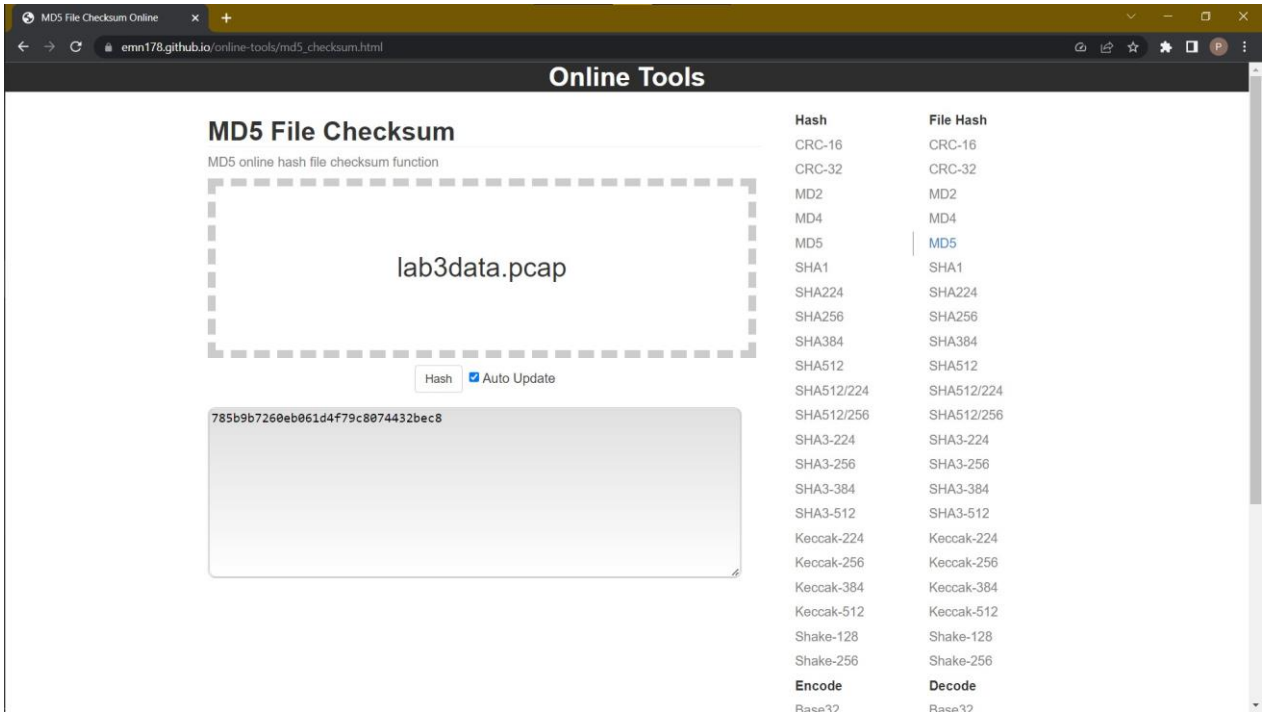
   The Time Difference is only 1 minute.

   The suspect, Johnson Crossby, was using a ***Windows NT system Version 10.0 which is based on a 64-bit architecture.***

10. The evidence is documented and is added to the chain of custody.

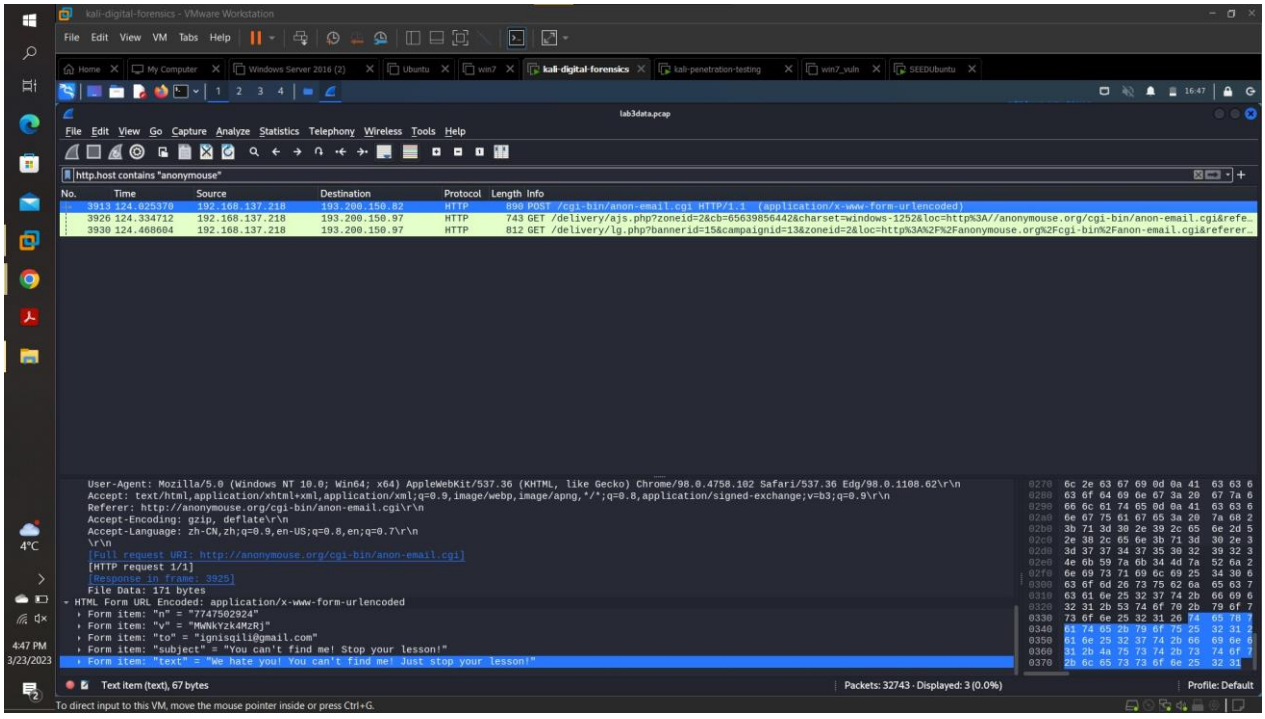
Results:

MD5 Checksum:



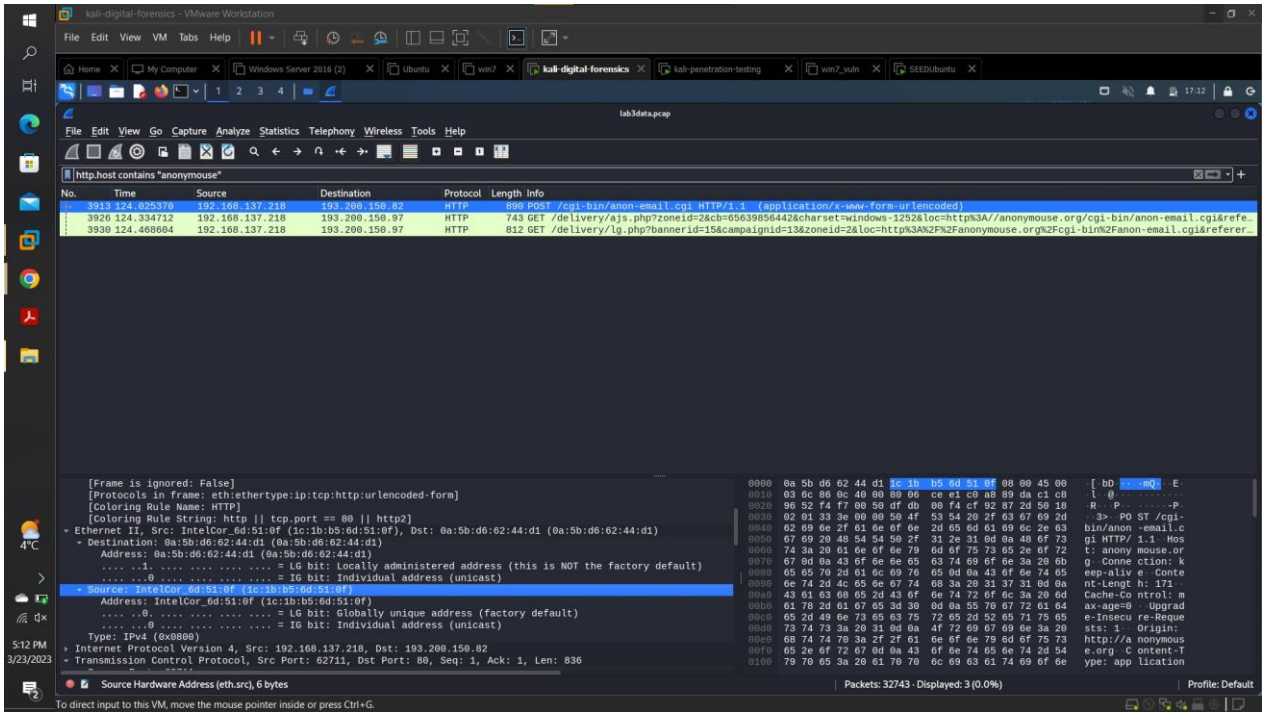
MD5: 785b9b7260eb061d4f79c8074432bec8

Harassing Email:



Frame Number: 3913
Text is Highlighted.

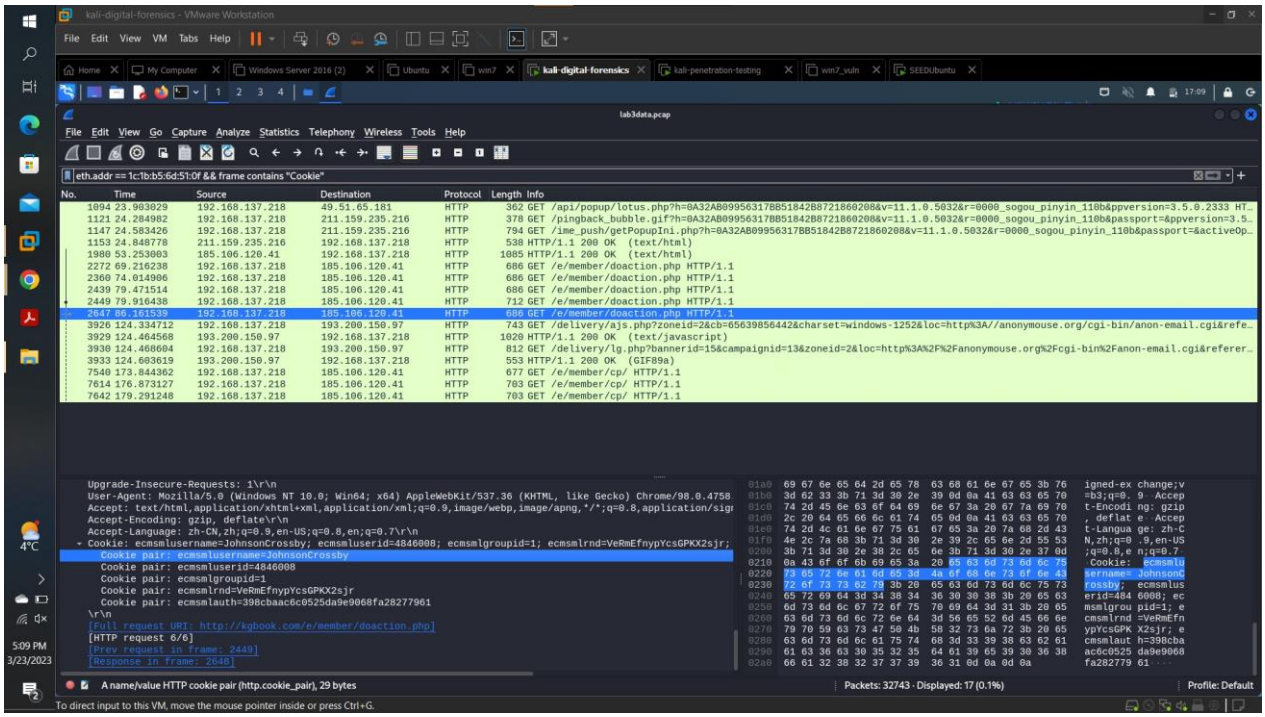
MAC Address:



MAC Address Source: 1c:1b:b5:6d:51:0f

MAC Address Destination: 0a:5b:d6:62:44:d1

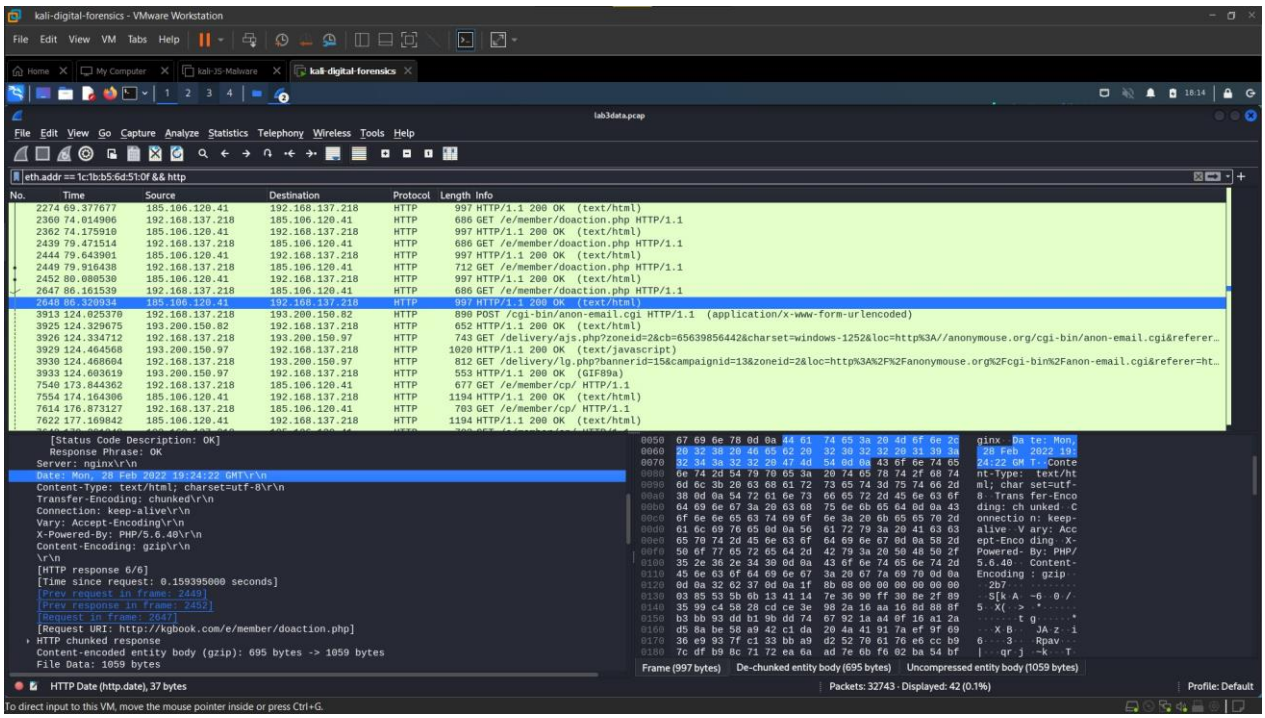
Name:



Frame Number : 2647

Name : Johnson Crossby

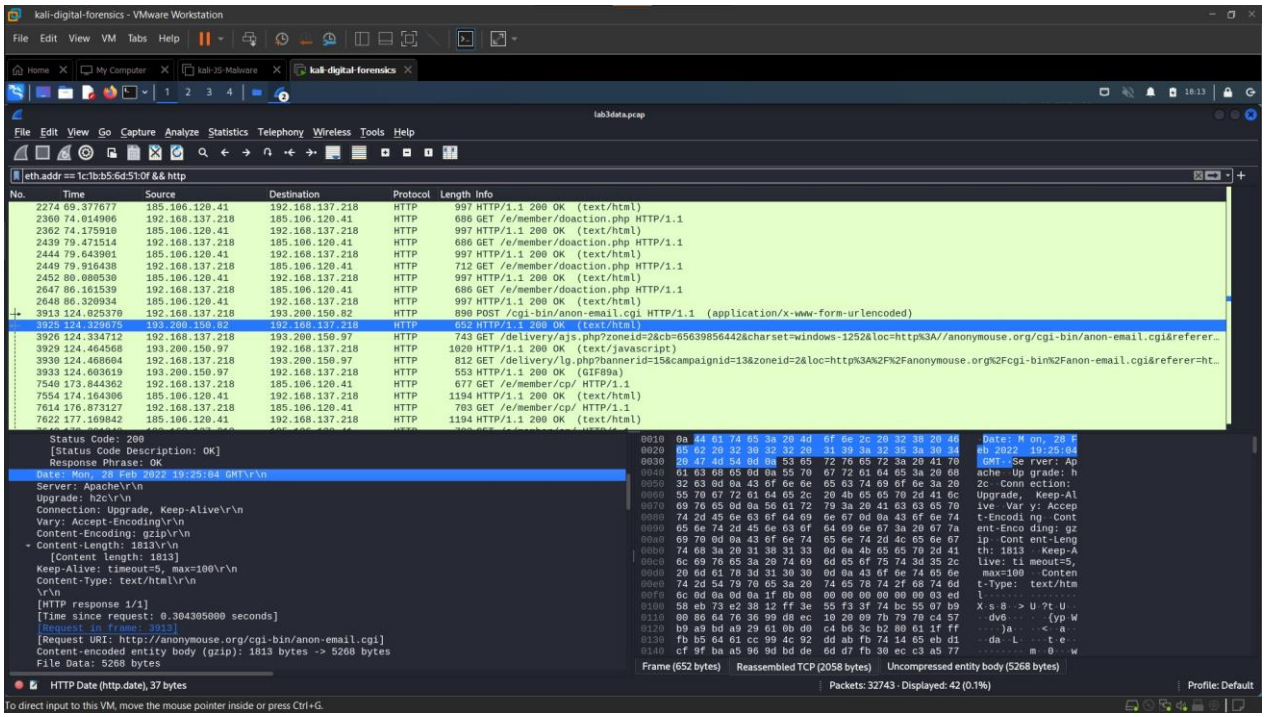
Timestamp Kgbook:



Frame Number : 2648

"kgbook.com" on 28th February 2022 i.e., Monday at 19:24:22 GMT.

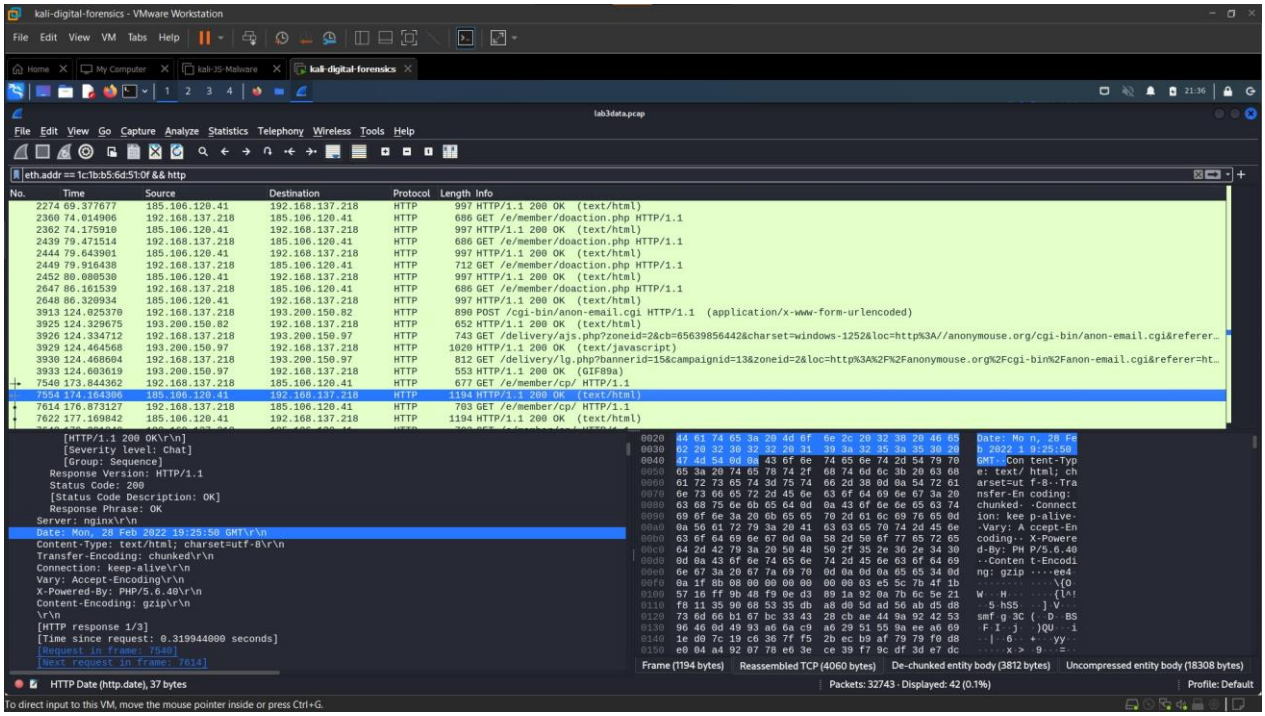
Timestamp Anonymouse:



Frame Number: 3925

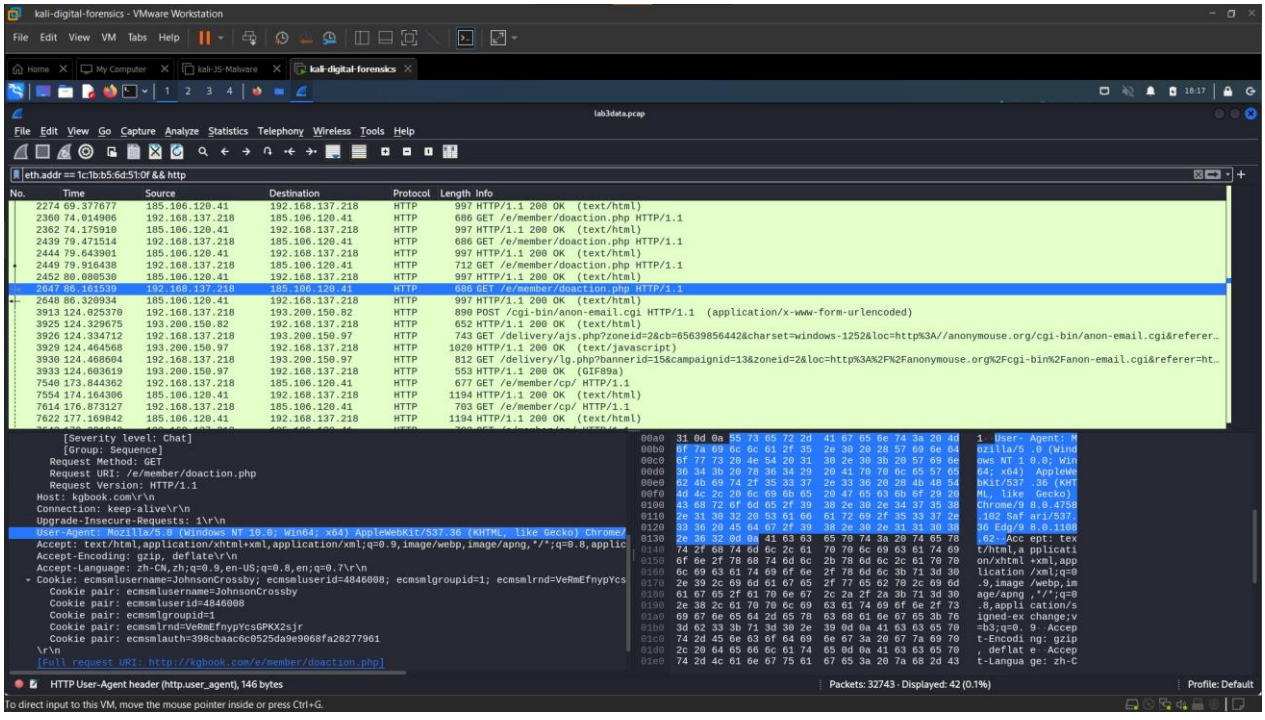
"anonymouse.com" on 28th February 2022 i.e., Monday at 19:25:04 GMT.

Timestamp Kgbook After:



Frame Number : 7554
"kgbook.com" on 28th February 2022 i.e., Monday at 19:25:50 GMT.

OS:



Windows NT system Version 10.0 which is based on a 64-bit architecture.

Forensic Questions and Answers:

1. Which IP accessed the www.anonymouse.com?

   The IP Address that accessed the www.anonymouse.com is 192.168.137.218. The is visible in all Harassing Email Screenshot and Timestamp Screenshot.

2. Does the IP post harassing comments to the website?

   Yes, the IP does post Harassing Comments to the Website in the hopes of harassing their teacher Ignis Lee. The evidence is available in Harassing Email Screenshot.

3. Which HTTP post does contain harassment message?

   The HTTP post is present in *frame 3913* which has post request sent from anonymouse.com. The evidence is present in the result section shown in the Harassment Email Screenshot.

4. Which MAC address is the harassment message sent from?

   The Harassment Message is sent from the MAC Address Source *1c:1b:b5:6d:51:0f* which is the suspect's Hardware ID. As shown in MAC Address Screenshot.

5. Which do you think is more effective in network analysis forensics, IP address or MAC address? Why?

   In network analysis, the IP Address can be static or dynamic means it can change or remain the same whereas the MAC address is static and cannot be changed by the user, so it is more effective in tracking people than IP addresses. But IP addresses clarify the source and destination of traffic. If IP address identifies devices on the network, MAC addresses can identify specific devices on the network. So, in short both IP and MAC are crucial in network analysis.

6. (Not relevant to this scenario) How do servers remember us when we browse websites on a daily basis? For example, we can access Amazon, Twitter, YouTube, etc. without having to repeatedly enter our account name and passwords.

   There are different ways in which a website can remember us when we browse website on daily basis:

   1. **Cookies**: When we visit a website for the first time, the website sends a cookie to our system which contains information about our session and preferences. So, when we visit the website the next time the system sends the cookie back to the website which helps it to identify us.

   2. **Browser Fingerprinting**: In this the website identifies us based on the browser's unique settings and configurations.

3. **Session Token**: They are used for identification like cookies, but they expire after no activity or the user logs out.

7. Who is the suspect?

   The suspect is *Johnson Crossby* as identified in frame number *2647*. The evidence is shown in the Name Screenshot in the results section.

8. When did the suspect use www.anonymouse.com?

   The suspect, Johnson Crossby, used "anonymouse.com" on *28th February 2022 i.e., Monday at 19:25:04 GMT* as shown in Frame Number *3925*. The evidence is shown in the Timestamp Anonymouse screenshot in the result section.

9. In your opinion, were the skills of the abuser low, moderate, or high and why?

   In my opinion the skills of the abuser were low. The suspect was clearly intelligent enough to use "anonymouse.com" to send his harassing emails. But he made a few mistakes, like using the Universities lab to send the emails, not using a secure website, logging in from the same system which left the cookies, etc. So, I would say his skills were low.

10. If the suspect sends a second harassment email using another anonymous email site, instead of "anonymouse.org", can the above analysis process still identify the suspect? Please take the anonymous email site "https://www.guerrillamail.com/" as an example to analysis. (Hint: You can start from the difference between https protocol and http protocol.)

    It is not possible to identify the suspect using the same analysis network if he uses a different anonymous website. We will not be able to identify the harassing messages sent by the suspect or see the MAC address or see the content of the cookies using same analysis method since "HTTPS" is encrypted. But there are other ways in which the suspect could be found. We can still see the source and destination of the packet because IP address is still visible to track.

11. With the rapid update of network protocols, do you think the email forensics method used in this case can continue to be used in the future (e.g. 10 years later)? Why?

    In my opinion, the above analysis method might still be relevant after 10 years. The basic principle of email forensics is capturing network packets, analyzing packets, and tracing email communication flow-likely remain relevant for many years to come. I have always thought computer science was like a never-ending Jenga game. We always develop innovation in technology based on what has been invented. We never question the present system unless some new problem arises. So even if we make many breakthroughs in the network field it doesn't mean we will forget what we already know. There are many factors that affect the forensic method. There might be a need for updated technologies and tools. But just because it's new doesn't mean we forget the old.

Conclusions:

Several evidence supported the fact that Johnson Crossby is the one who sent the harassing emails to his teacher Ignis Lee.

The findings in the current investigation are as follow:

1. When the packet (3913) containing the post request was sent it was tracked to Mr. Johnson Crossby's IP. (MAC Address Screenshot)

2. When the content of the packet (3913) was investigated, it was sent to Mr. Ignis Lee's email and was filled with harassing text.(Harassing Email Screenshot).

3. The MAC address found on the packet (3913) used to access "anonymouse.com" and the one found on packet (2647) used to access "kgbook.com".

4. The Cookies sent by the kgbook.com had Mr. Johnson Crossby's name in it.(Name Screenshot)

5. The time difference between "anonymouse.com" and "kgbook.com" is only 1 minute and after using "anonymouse.com" the suspect went back to use "kgbook.com".(Timestamp Anonymouse and Timestamp Kgbook and Timestamp Kgbook After Screenshot)

6. The OS of the system was Windows NT 10.0 x64 64-bit.(OS Screenshot)

Opinions:

In my opinion, Mr. Johnson Crosby is the culprit behind sending Mr. Ignis Lee the harassing text.

Mr. Johnson Crossby was Mr. Ignis Lee's student in the Math's 199 Class. The .pcap file containing the packets log was cross verified against the MD5 checksum. The hash function would change if a single character was different, so that proves that the log file was correct. The fact that the IP address and the MAC address were found in the packet containing harassment email and later that MAC address pointed to Mr. Johnson Crossby is valid evidence. The Cookie containing Mr. Johnson Crossby's name was associated to the "kgbook" website. According to the packets the time difference between using kgbook.com and using anonymouse.com is only 1 minute. This proves that it was Mr. Johnson Crossby who is the one to send the harassing emails to Mr. Ignis Lee.

There is also a need to further investigate the matter. The following points should be considered:

1. CCTV cameras and witness testimony are required to prove the usage of the computer by Mr. Johnson Crossby at the found time.
2. Further packet capturing and repetition of investigation may make the evidence stronger.

Certification:

I hereby certify that the work presented above was personally performed by me and the opinions and conclusions stated are my own and based upon the work that I performed.

Pritesh Bharat Gandhi

Signature