# 430/530 – Log Inspection Lab

Name: Jacob Boicken

## Email 1

2. Email Service: mailbox.org

   Browser: Firefox

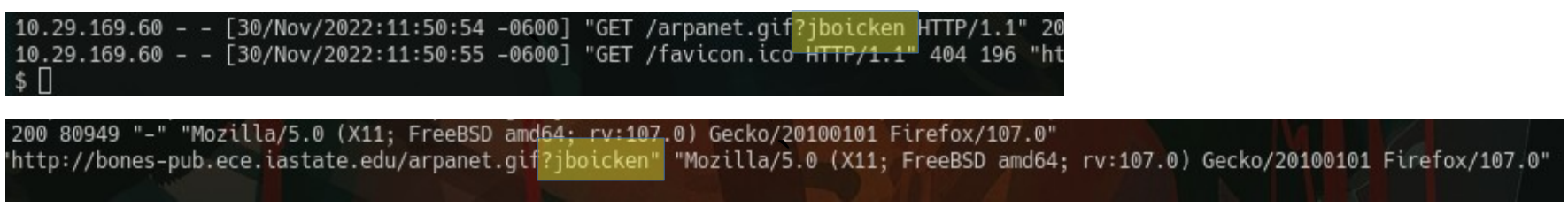
   Device (brand/model): Thinkpad T480, Intel i5

   Operating System: Freebsd

4. Did the log file include a link preview? No

   If so, include a screen capture below.

6. Log file entry screen capture




7. Please type out the entire token (e.g., Windows NT 10.0, Safari/537.36, HTTP 1.1, etc.)

   A. Device information from Platform Token:

   amd64

   B. OS information from Platform Token:

   FreeBSD

   C. Information identifying browser:

   Mozilla/5.0, Gecko/20100101, Firefox/107.0
   (Matches Firefox format)

   D. Information on email service:

   None

   E. Information about IP address:

   10.29.169.60, the IP is a private IP in the 10.0.0.0/8 range. This is the IP of my laptop while I am on campus doing this assignment.

# 430/530 – Log Inspection Lab

## Email 2

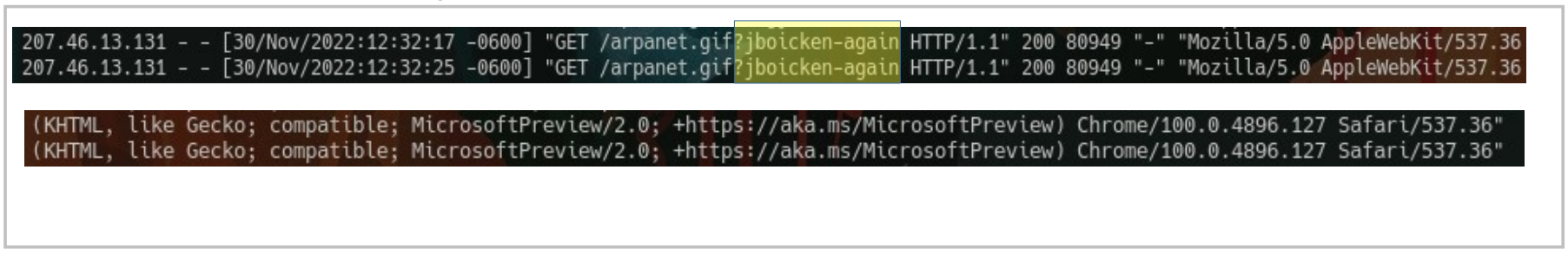
2. Email Service: Gmail

   Browser: Chrome

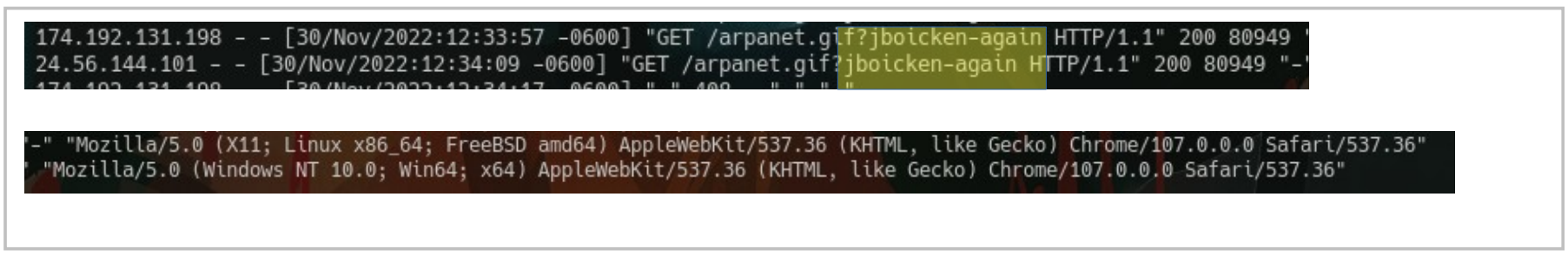
   Device (brand/model): Thinkpad T480 (intel i5)

   Operating System: Freebsd

4. Did the log file include a link preview? Yes
   If so, include a screen capture below.




6. Log file entry screen capture




7. Please type out the entire token (e.g., Windows NT 10.0, Safari/537.36, HTTP 1.1, etc.)
   A. Device information from Platform Token:
   x86_64, amd64

   B. OS information from Platform Token:
   Linux, FreeBSD
   (Seems unsure of it being Linux or Freebsd?)

   C. Information identifying browser:
   Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
   (Matches chrome format)

   D. Information on email service:
   MicrosoftPreview/2.0 – It is showing microsoft preview, however I accessed this using gmail but sent from Outlook. Outlook may preview when send/drafting the message. (This shows that at least one side is using MS.)

   E. Information about IP address:
   207.46.13.131 - from preview, owned by Microsoft
   174.192.131.198 - owned my Verizon (I went onto cellular hotspot to connect to this from non Iastate address)
   24.56.144.101 - This is owned by mid-continent communications

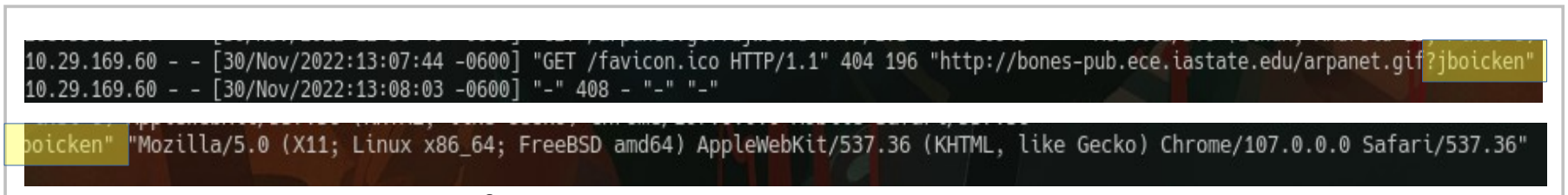
# 430/530 – Log Inspection Lab

## Private Browsing

A. Predictions/expectations for private browsing:

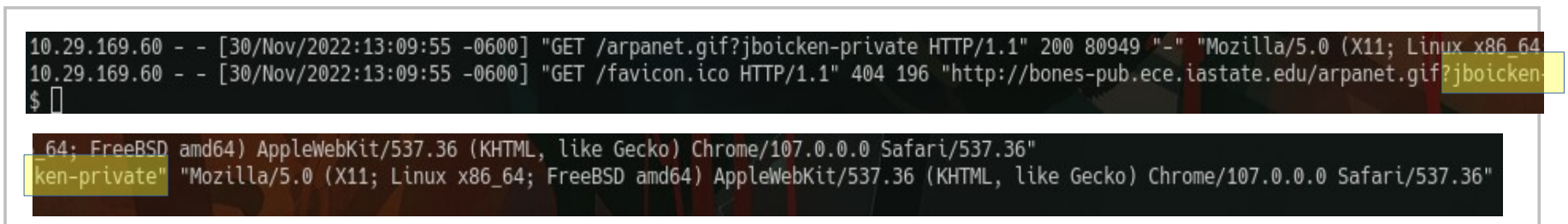
I would expect the private browsing to not change information. I think the browser will just respond with the same UA to the web server. It is still the same browser and will operate the same. As well, I don't think the browser would want to send different information for private browsing as it will the server more information about the client.

Non-private browsing screen capture:




(Didn’t load page but got favicon. Still got the UA.)

Private browsing screen capture:




B. Method of private browsing:

Incognito Mode on Chrome

C. Log file differences:

The UA sent by non-private and private are the exact same. They are just the chrome UA that is sent by the browser as it was sent before. The only difference I see with the log file is the timestamp and the jboicken-private versus jboicken in the URL.

D. Results:

The outcome is what I thought would occur. The UA’s sent were the same regardless of the browser being in incognito mode or not. I think this is because the browser does not want to send a different UA as it could be detected and recorded to know that a user is in incognito Mode. This would go against the purpose of these “privacy enhanced” modes of the browser as they are less commonly used and would make the user easier to identify.

# 430/530 – Log Inspection Lab

## Reflection

A. What I saw within the log file was what I expected to be there. The server is recording the information that is being sent from the browser and the device's IP information seen during the communications between them. Chrome and Firefox on my system seemed to report the same amount of information. However, it seems that my mail services don't preview except my iastate outlook email that I sent the url from. I think that the preview services aren't that bad of an action as they are meant to show the user information on the URLs/links to help prevent them from being phished. But they do show the sender that their email was received without the user clicking the link.

Should the email sender or website owner be required to tell you they are collecting the information from the HTTP request and UA string?
Ultimately my answer is yes. However, a malicous user wouldn't tell you regardless of them being required so it doesn't protect anyone. But a legitimate service being required would tell the user what information they are using and should say what they are doing with that information (minimum). My thought is it is at least a protection for both sides if the user agrees to it. The service can't use the info in an unagreed way.

B. Based on the details in the log file, what are a few ways you think good actors can use this information to their advantage? Be specific.

Good actors could use the info to monitor visitors to the web paged, what types of requests are made, and get some identifying information of the visitors.
Thinking with the requests, if we can identify a malicous actor,then we can follow what requests they are making. I think of setting up a honeypot and viewing how malicous attackers are using the server as a way to learn how attackers are acting on the systems.
As well, I know Doug talked about web application firewalls, it is possible malicous requests are getting through the WAF and being seen by the web server. This helps identify shortcomings in defense strategy and potentially better WAF configuration.
Finally, if we know that a malicous attack went through the web site, like the other two, we can learn from an attacker to see where the web developers created vulnerable code (via which request was made). This helps identify the parts of the code that would need to be patched in the server backend.

C. Based on the details in the log file, what are a few ways you think bad actors can use this information to their advantage? Be specific.

Bad actors would be people who set up a tracking website for purposes like identifying scam/phishing emails that are received. Like with the lab, the url could contiain an query (?) option to identify the visitor and learn which targets are more vulnerable/susceptible to these. For instance, they could do this for both image being auto-loaded in the email client and a link to be clicked to get a little more information on the targets.

Additionally, a malicous web server could use this information to identify the client browser that is visiting. This could the have the server send different malicous javascript/client side code to carry out an attack on the browser.