Operations Security (OPSEC)

Part I - Background Reading

(20 pts. Total)

1. When was the term OPSEC first coined? **2.5 pts.**
    a. **During the Vietnam War, around 1966**
2. List the five stages of operations security. **2.5 pts.**
    a. **Identification of Critical Information, Analysis of Threats, Analysis of Vulnerabilities, Assessment of Risks, Application of Countermeasures**
3. What constitutes a risk? **2.5 pts**
    a. **A risk is when you have a matching threat and vulnerability**
4. What is the symbol for OPSEC as stated by your text? **2.5 pts**
    a. **A purple dragon**
5. What does Haas' first law of operations security mean? **2.5 pts.**
    a. **It means that you have to have an understanding of actual and potential threats that any critical data may face.**
6. What is the most important stage of operations security? **2.5 pts.**
    a. **Identification of Critical Information**
7. List five pieces of critical information that you as a private citizen may need to protect? **5 pts.**
    a. **Personal Identifiable Information, Financial Information, Passwords and Login Credentials, Personal Communications, and Home Address and Schedule.**

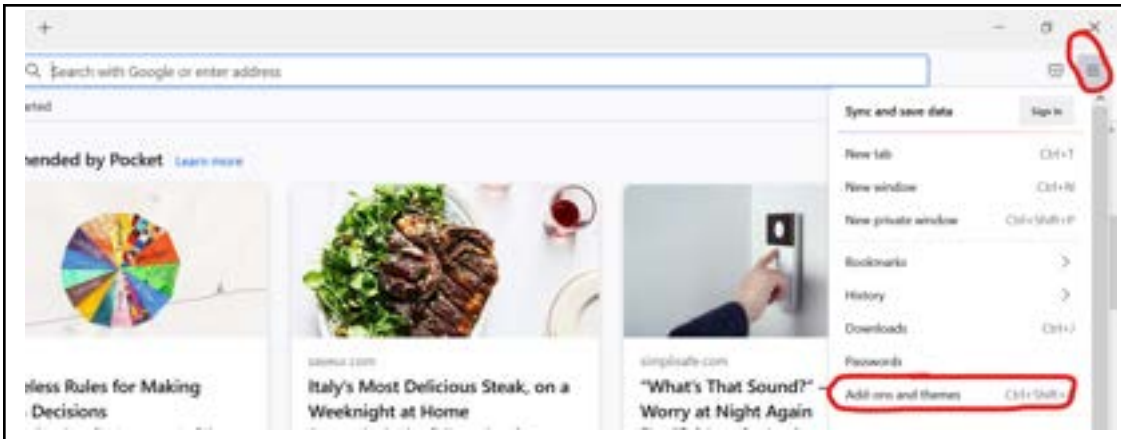
Part II – Protecting Critical Information

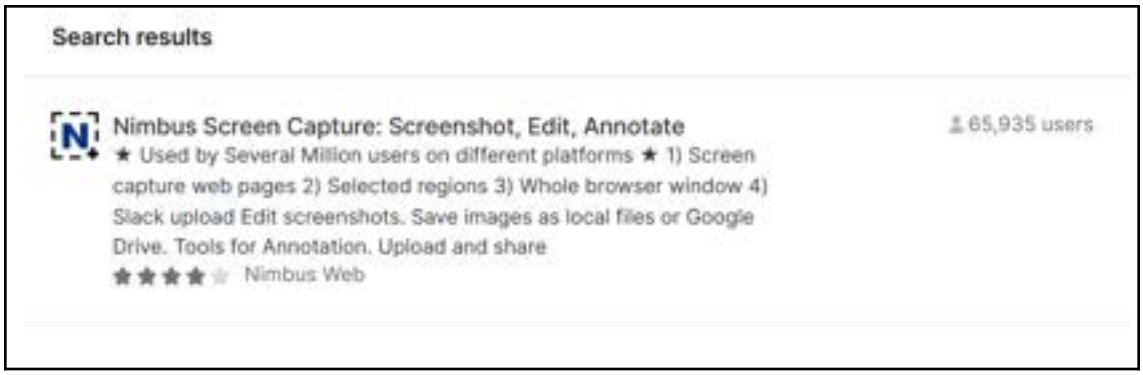
(55 pts. Total)

In this part of the assignment, you will go through a process of protecting the information that is critical to your operation as an investigator. You will learn how to properly document images, and remove as many of your digital footprints as possible. They are equally important. For this assignment, you will be using Firefox to browse the web and using Firefox add-ons to protect your information. It is likely that most of you use Chrome. These apps are available on Chrome as well, and you can use Chrome, but these directions are for Firefox, and Firefox is recommended.

Documenting Information by Using Nimbus

Nimbus is an excellent way of documenting what you do in your web browser. It cannot take screenshots of anything outside of your browser, but for documenting web evidence, it is excellent. Install Nimbus by going to the icon to the right of the address bar, clicking it and going to the “Add-ons and themes” link. Search for Nimbus and add it to Firefox.

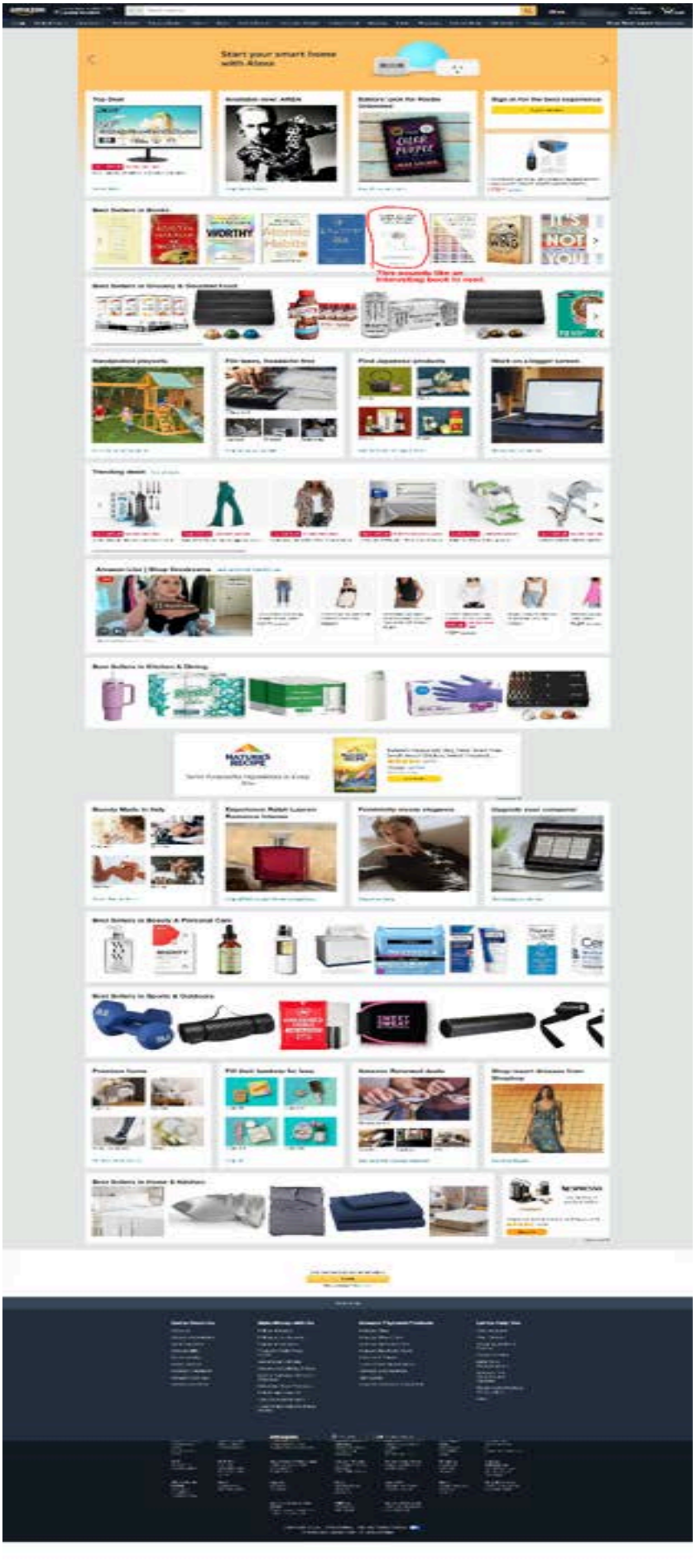




Look for the Nimbus icon, click on it, and look for the “actions after capture” options and toggle to “edit” if it is not there already. Now, whenever you take a screenshot, you will automatically be sent to the edit screen where you can edit the shot. The next few tasks are just for practice with Nimbus.

8. Go to a website of your choosing. **10 pts.**
    a. Take a screenshot using the “visible part of page” (you may have to decrease the size of your web window before taking the screenshot to make sure all the information is recorded)
    b. Resize the picture so that the width is 2200 (keep the “proportional” box checked).
    c. Select two items on the page and write notes beside them. It does not matter what you write. It is just for practice.
    d. Number the notes using the number function.
    e. Save the screenshot and paste it into your assignment (under question 8)

9. Go to Amazon's webpage **10 pts.**
    a. Take a screenshot using "entire page" (you may have to decrease the size of your web window before taking the screenshot to make sure all the information is recorded)
    b. Resize the picture so that the width is 2200 (keep the "proportional" box checked).
    c. Blur the "Hello, Sign-In" section of the page
    d. Circle a product somewhere on the screen using a red pen. Write a note about the product.
    e. Save the screenshot and paste it into your assignment (under question 9)


Start your smart home with Alexa
Time sounds like an interesting book to read.

10. Go to ODU's webpage **10 pts.**
    a. Take a screenshot of any section of the page using "selected area"
    b. Point to something in that section using the "text arrow" option, and write something in the textbox. It doesn't matter what you write.
    c. Save the screenshot and paste it into your assignment (under question 10)

Removing Digital Footprints by Using Firefox Multi-Account Containers

The Multi-Account Containers plug-in allows you to separate browsing sessions without needing to clear your history or using multiple browsers. Whatever you do in one container is not shared with another. This has several applications:

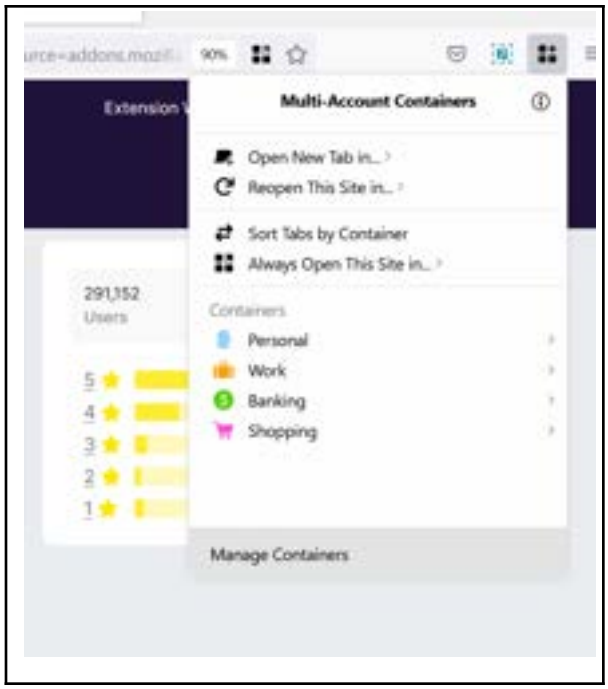
- You can log into several social media accounts at once (using different containers). This means you can browse social media with several different aliases.
- You can avoid being tracked with cookies. When you browse the web, you collect data and carry it with you. If you browse Amazon and then do a Google search, your information will be carried over to Google. You can open a separate

container just for a particular website and keep that website's cookie data separate.

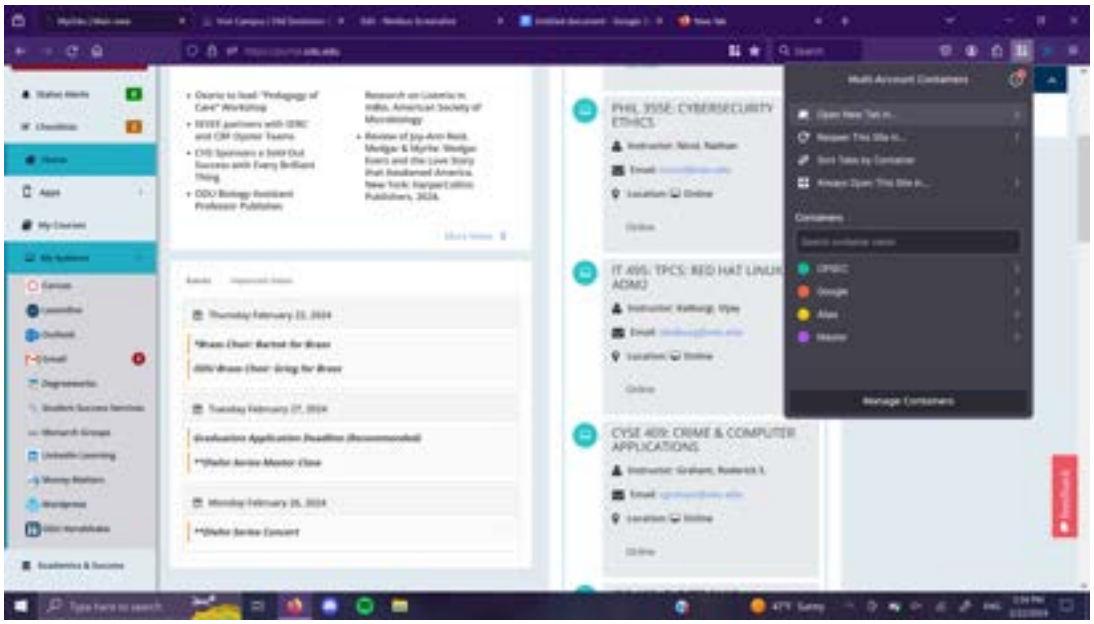
- You can open links in separate containers as a form of "sandboxing" to protect your information. Links often contain scripts (small pieces of code) that can extract data about you. If, however, you use a container, the code can only extract what is in the container.

Install Multi-Account Containers and complete the tasks below (You may be asked to turn on sync. Ignore this.)

Create four separate containers called "OPSEC", "Google", "Alias", and [A container of your choice.] Open the Multi-Account Containers menu and click the "Manage Containers" option. Then you can either delete each container or rename and customize the containers. Your containers before you modify them should look like below.

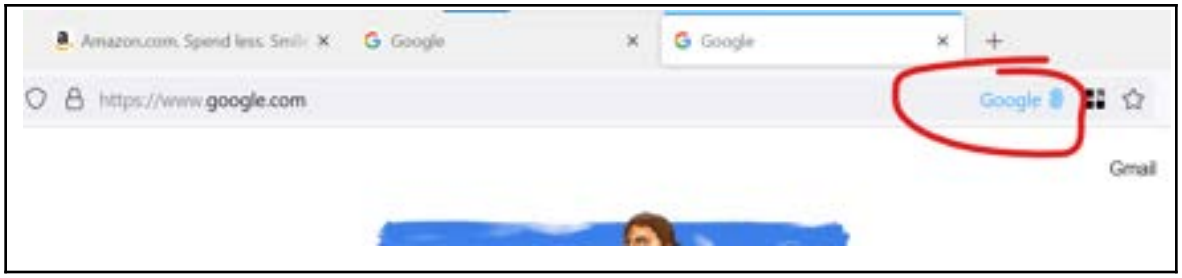


11. Take a screenshot of your four customized containers and paste in your document (Under question 11). **5 pts.** **[Note: Some versions of Nimbus are not allowing students to take a screenshot of the containers. If you like, you can use a different tool to complete this task. I have a windows machine, and I used "Snip and Sketch." If you cannot use another tool, just write me a note saying that you were not able to take this screenshot]**



Assign a specific website to a container so that the website always opens in that container. The most obvious use of this is for Google so that your Google search history is not shared with other websites.

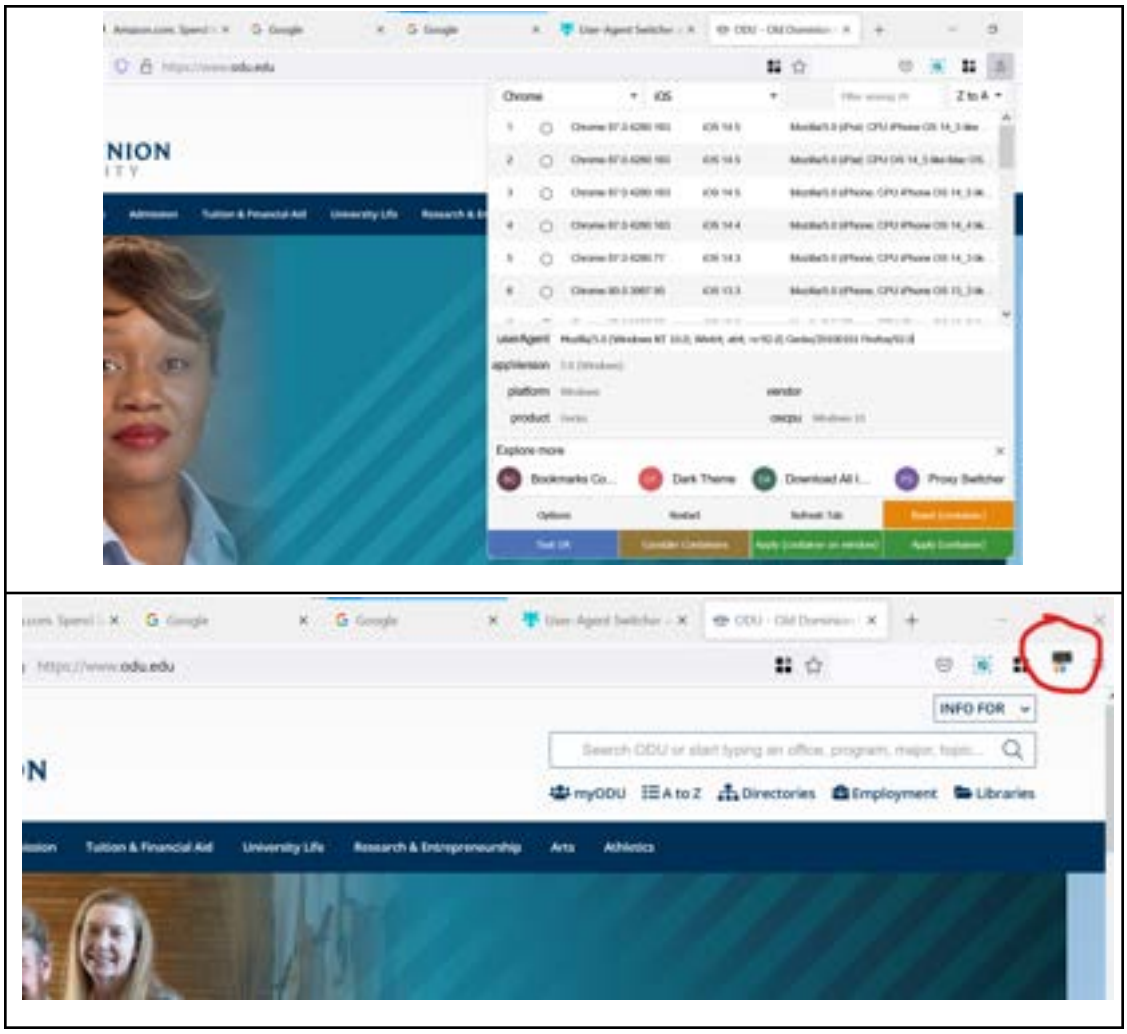
- Go to Google, and then click the container's menu and select “Always open this site in….”
- You will know you have done this correctly when you see the fingerprint the color of your container.



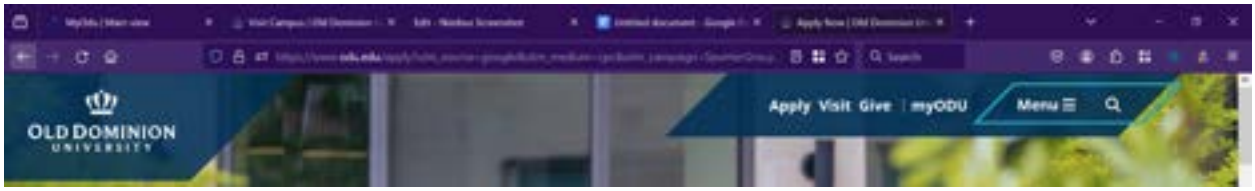
12. Take a screenshot of your Google container (Under Question 12) **5 pts.**

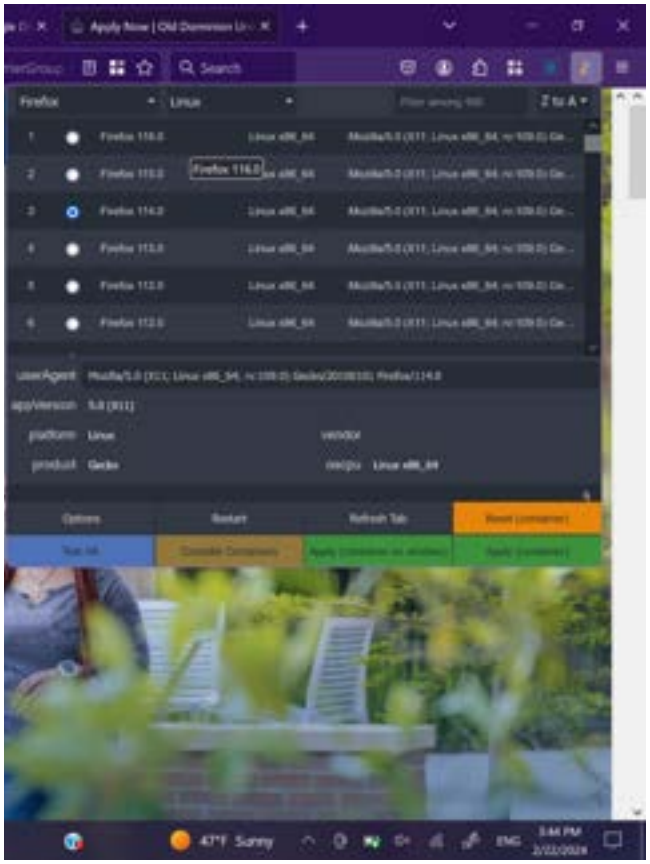
User-Agent Switcher and Manager

User-Agent Switcher allows you to spoof your operating system and browser.



13. Install User-Agent Switcher. Spoof your browsing session with the browser and operating system of your choice and take a screenshot of the spoofed agent (Under Question 13). **5 pts.**



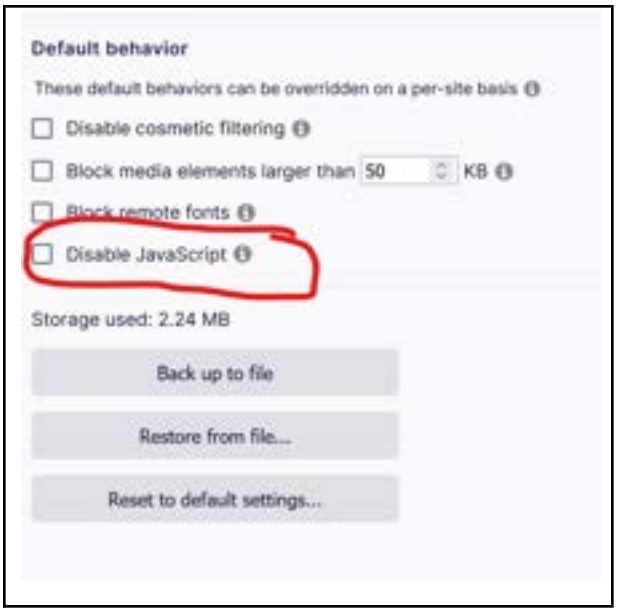


uBlock Origin

uBlock Origin protects you from invasive advertisements, tracking code, and malicious content. It is a wonderful plug-in that can tell you quite a bit about all the malicious or unwanted code – usually trackers and scripts, that run on a website. Trackers are often from advertising agencies. Scripts are pieces of code embedded on a website to perform certain tasks.

Here is what happens when ublock Origin is installed and one navigates to ODU's website. 15 trackers or scripts were blocked.

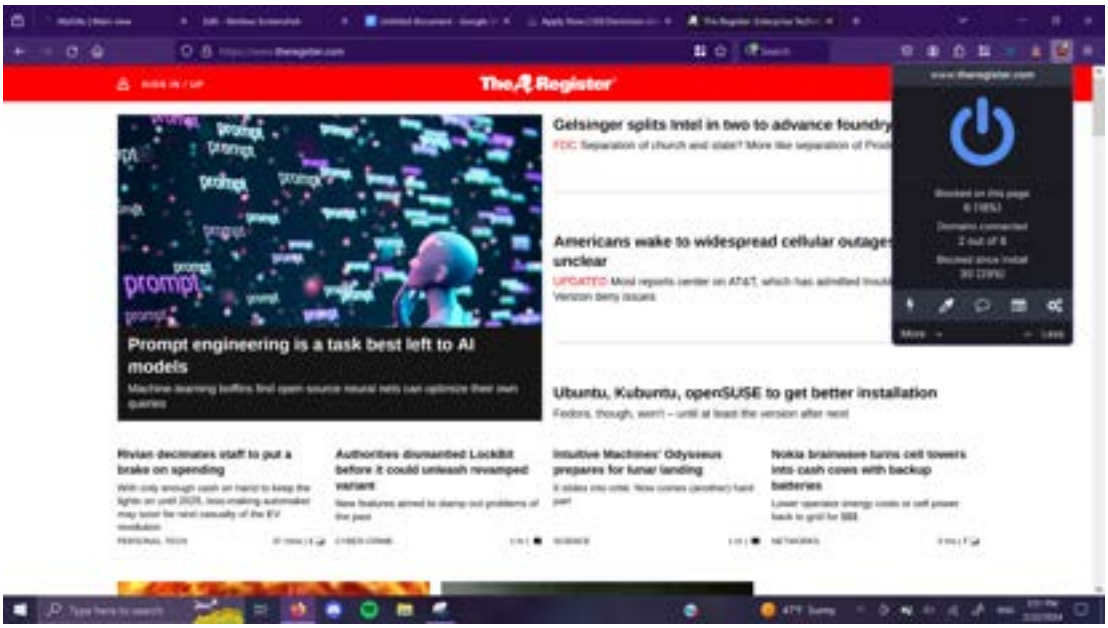
uBlock Origin is an outstanding plug-in with a broad range of functions. However, for this activity, I would like you to go to the settings tab and disable java-script. Java script is a common language that most websites use. However, it is also a common vector for attacks and other malicious software. You may wish to block JavaScript when exploring some sites when doing an investigation.



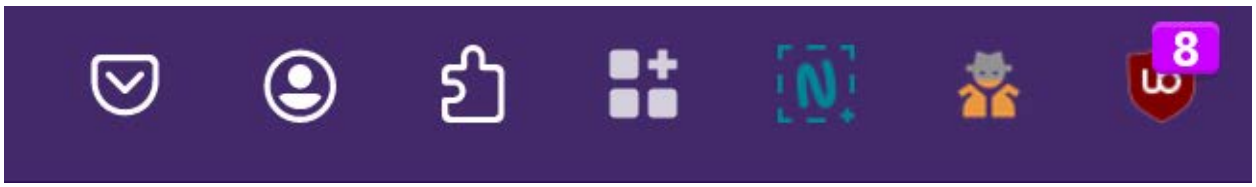
Here is ODU’s entire homepage without JavaScript (captured by Nimbus).


Sep 25
Sep 25
Sep 25
Sep 26
Sep 27
Sep 27
Sep 28
Sep 28
Sep 28

14. Navigate to a site of your choosing and take a screenshot of that site showing how many pieces of code were blocked (Under Question 14). **5 pts.**



15. Disable JavaScript, refresh the site, and take a screenshot of the entire page (Under Question 15). **5 pts.**



SIGN IN / UP

running queries on 'free' dataset

Researcher makes case for default limits after arriving via Python library

DATABASES 22 Feb 2024 | 4

EXCLUSIVE Employees feel frustrated by lack of communication and bosses' inability to tell them which offices are open

PUBLIC SECTOR

EU wants to make undersea internet cables more resilient

Threat to data means submarine infrastructures should get status of 'highest possible national significance'

NETWORKS 22 Feb 2024 | 14

small enough to run on your computer

Your own personal chatbot awaits

BOOTNOTES 22 Feb 2024 | 7

vendor I-Soon is or cyber-attackers for

Trove reveals RATs that campaigns against offsh

SECURITY

Nvidia revenue grows 265 percent with more to come as new GPUs and Ethernet near

Jensen Huang defends colossal GPU purchases made by hyperscalers, claims

Harness the power of security automation

How to ensure policy management keep up with the risks to data integrity presented by the cloud

WEBINAR

Exploiting the lates ConnectWise bug i 'embarrassingly ea

Urgent patching advised against setup wizards

SECURITY

BLOCKS & FILES.

Hammerspace claims fastest file system for AI training

Catching up with H after strategic over

UK demonstrates prowess at hunting the ocean

The successor to Research Unix was Plan 9 from Bell Labs

FOSDEM 2024 A better UNIX than UNIX isn't a UNIX at all

OSES 21 Feb 2024 | 63

Orgs are having a r crisis while crims r

Hacking your way in is s much easier

SECURITY

Hackers mod a Sony PlayStation Portal to run

Modders claim GTA: Liberty City Stories and Tekken 6 are smoothly'

IPO

$37.3M bid significantly down from SPAC flotation valued at $672M

Cops turn LockBit ransomware gang's countdown timers them

Authorities dismantle cybercrime royalty by making mockery of their leak

GlobalFoundries scores $1.5B in Uncle Sam's semiconductor subsidy bonanza

Neuralink patient m mouse maneuvers believed

Part III - Critical Thinking

(25 pts total)

16. Now that you have applied countermeasures to protect your investigation from risk, go back and think about what critical information you may be protecting by applying these measures. Discuss this in two to three paragraphs. (25 pts.)

The sensitive data that makes up the critical information I'm safeguarding with these countermeasures is quite broad and, in the wrong hands, could jeopardize the investigation's success and integrity. First, there is the private information of those connected to the case, such as suspects, victims, and witnesses. To stop possible harassment, intimidation, or manipulation, it is essential to protect their identities, contact information, and any other sensitive data. For this type of data, I would use the multi account containers to provide a safe environment for information and data gathering that won't be impaired by other search sessions. I would also use uBlock as a means to prevent malicious code and unwanted advertisements to pop up while conducting research.

Secondly, there is the private information gleaned from documents, audio files, and digital forensics that was acquired throughout the inquiry. This evidence may include private information about the case, such as chronologies, intentions, or interpersonal relationships. Maintaining the confidentiality of this data guarantees its accuracy and stops any manipulation or disclosure that might damage the investigation's reputation or impair its conclusions. For this type of critical information, again I would use the containers to allow me to have separate research sessions in order to collect evidence as needed without being interrupted by other sessions.

Last but not least, safeguarding operational data is crucial. This includes specifics regarding methods, plans, or ongoing projects related to the investigation. Should this information become public, it might alert suspects, enabling them to avoid apprehension or obliterate evidence, thereby hindering the investigation's advancement. The countermeasures preserve the efficacy and integrity of the investigative process in addition to protecting the individuals concerned by protecting these crucial bits of information. For this type of information, I think that the user-agent switcher would allow for safer browsing and information gathering. Having a spoofing mechanism to not allow websites to track specific user information could be useful.

FIGURE 7.3

Operations security process.