**Lab 03: Hacking Lab Report**

Joseph Patrick C. Galvez

American Military University

ISSC262: Red Team and Blue Team Security

Mr. Brian Burnett

7/12/2025

# Lab 03 Report

## Introduction

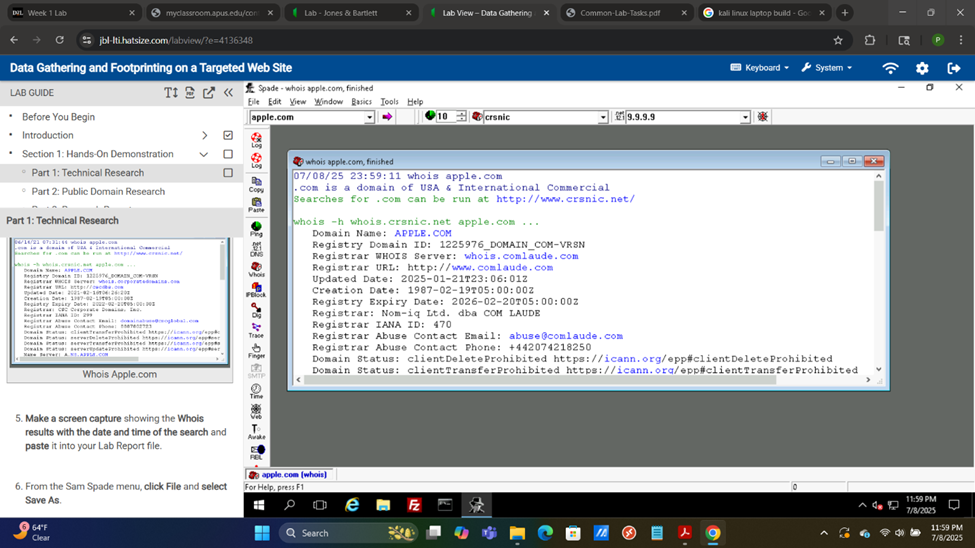
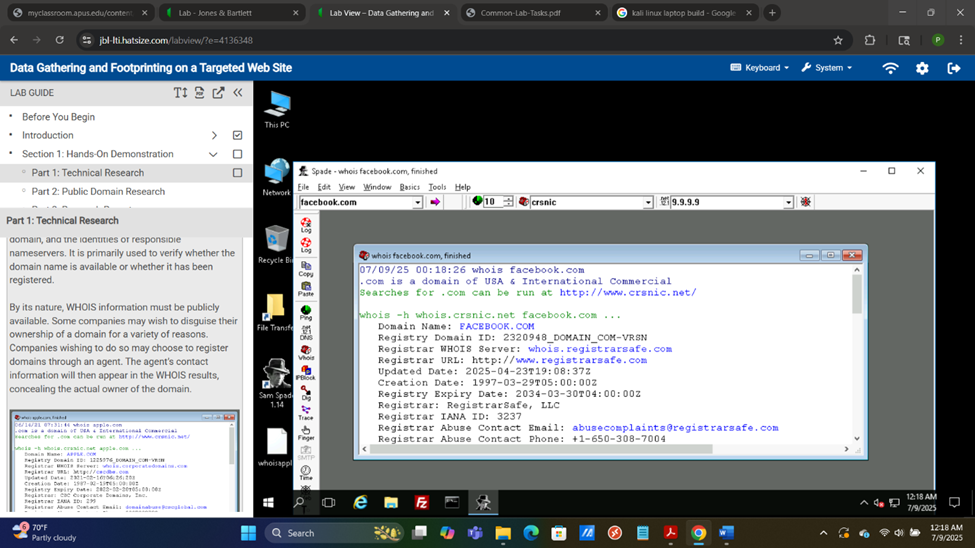
Lab 03 was the first lab exercise and was in week 1. Its contents included how to quickly obtain publicly available information to create a profile on a domain and its company. The information retrieved can be categorized into technical information and further information on the domain and its owner company.

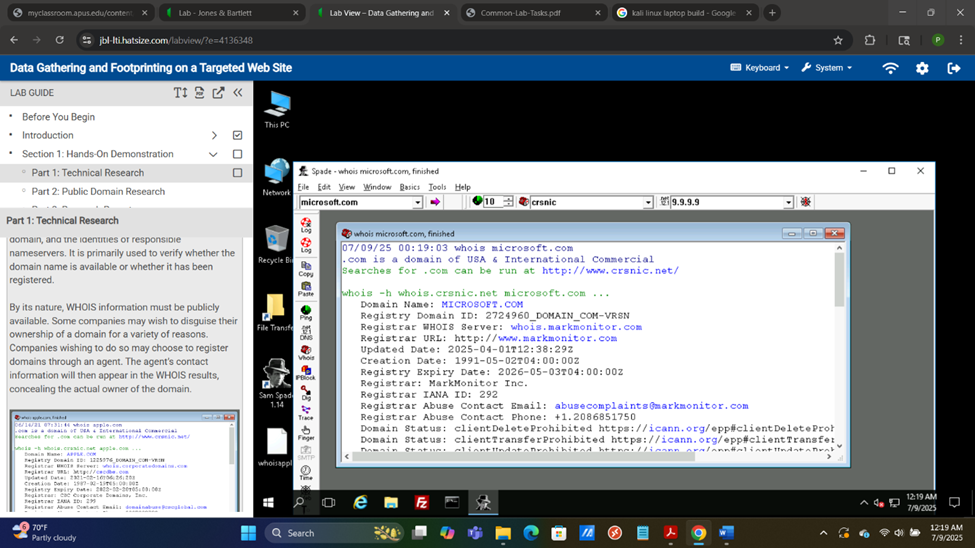
## Methodology

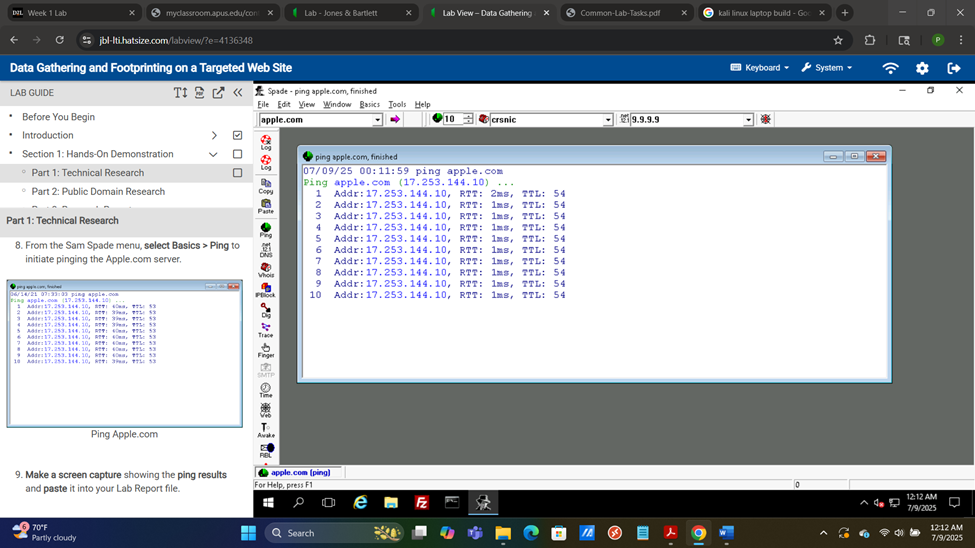
Lab 03 consisted of using tools such as Sam Spade, the windows command prompt, and the Google search engine to obtain publicly available information on the domain of interest. One tool used in Sam Spade were the WHOIS tool which gave information regarding the domain such as when it was created, who owns it, the registrar, and its ip address. Another Tool in Sam Spade that was used was the Ping tools which pinged the publicly registered IP to see if there is a response. The commands used in the Windows Command Prompt were nslookup and tracert. And lastly the Google search engine was used to collect information on the institution tied to the domain.

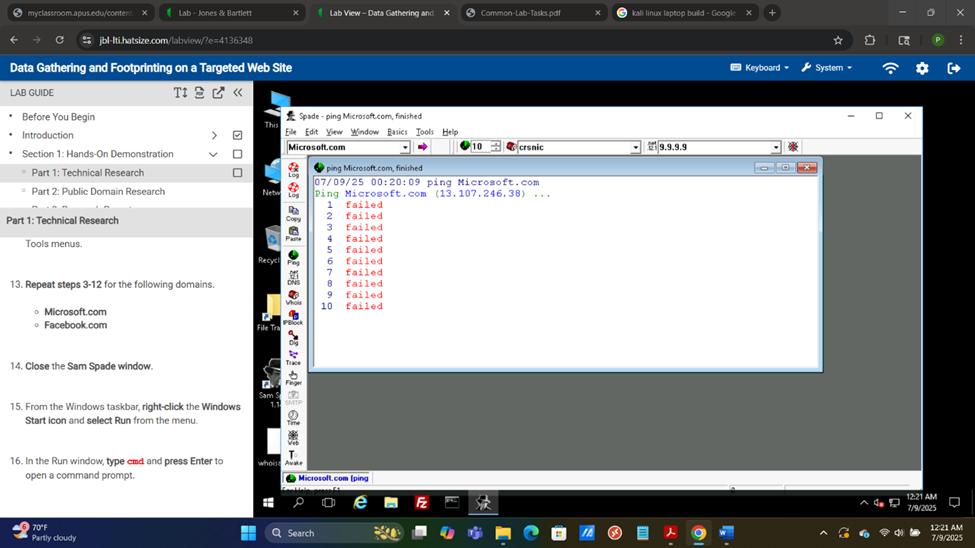
## Technical Research Results

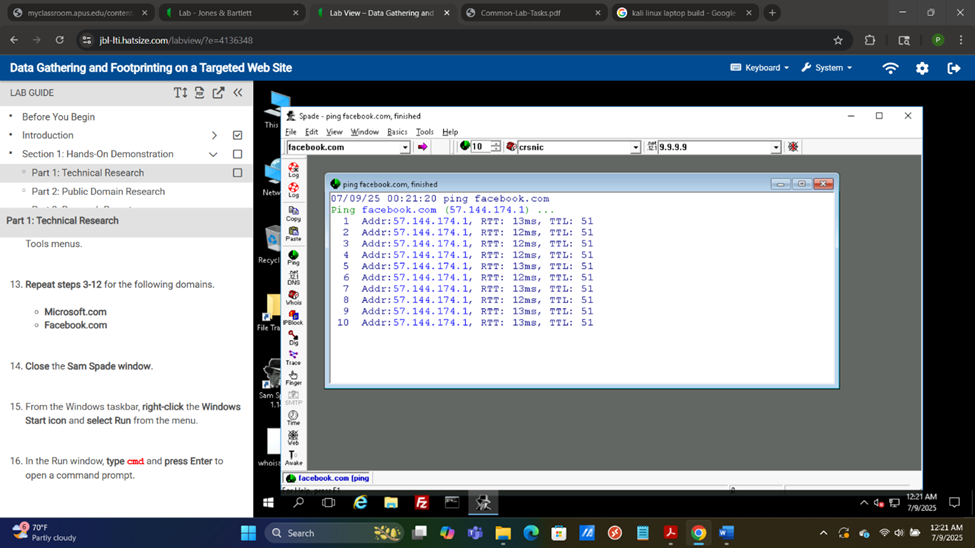
For the technical research portion of the lab the instructions were to use Sam Spade to perform a WHOIS lookup and a PING on the following domains: apple.com, facebook.com, and Microsoft.com. The results of the WHOIS lookup include: domain name, registrar url, last update date, domain creation date, registry expiry date, and the registrar contact information; this process was repeated for all three domains (see Figures 1,2, and 3). Afterwards the PING tool was used for these same three domains, the result was that the domains of apple.com and facebook.com responded; however, the domain of Microsoft.com failed to respond to the ping requests (see Figures 4,5, and 6). The nslookup command on Command Prompt was then used on the three domains, the results were the ipv4 addresses and the ipv6 addresses of the respective domains (see Figure 7). And lastly the tracert command was performed for all three domains, the results are that the tracert request for the Microsoft domain timed out on the 9th request onwards, Facebook took 14 hops from its domain address to my device and apple took 9 hops to go from its domain to my device (see figures 8,9,and 10).

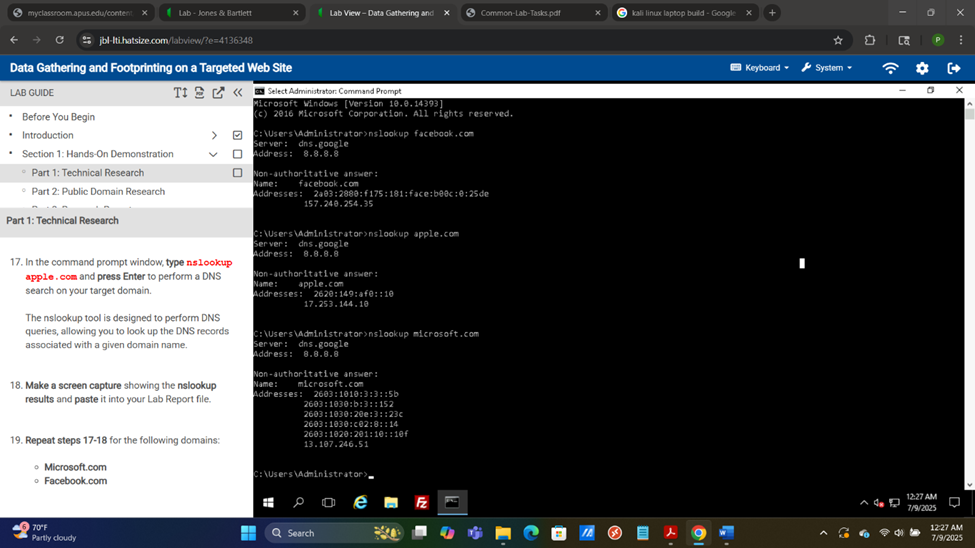
[[1]](#footnote-1)[[2]](#footnote-2)

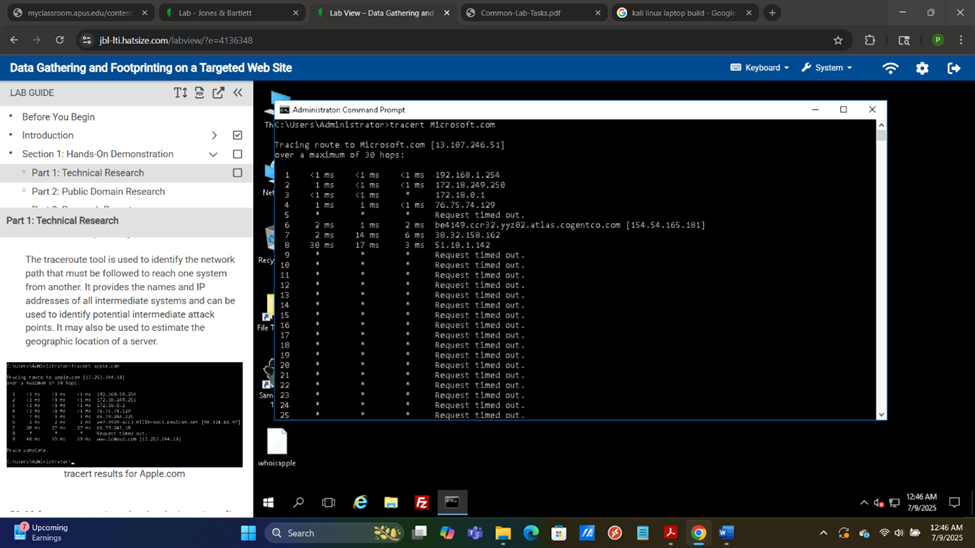
[[3]](#footnote-3)

[[4]](#footnote-4)

[[5]](#footnote-5)

[[6]](#footnote-6)

[[7]](#footnote-7)

[[8]](#footnote-8)

A screenshot of a computer

AI-generated content may be incorrect.[[9]](#footnote-9)A screenshot of a computer

AI-generated content may be incorrect.[[10]](#footnote-10)

## Public Domain Research Results

As part of Lab 03 I was required to perform public domain research, I chose Amazon.com. the domain name for the company is Amazon with a .com extension. The url for the amazon e-commerce store is : <https://www.amazon.com/ap/signin?openid.pape.max_auth_age=900&openid.return_to=https%3A%2F%2Fwww.amazon.com%2Fgp%2Fyourstore%2Fhome%3Fpath%3D%252Fgp%252Fyourstore%252Fhome%26signIn%3D1%26useRedirectOnSuccess%3D1%26action%3Dsign-out%26ref_%3Dnav_AccountFlyout_signout&openid.assoc_handle=usflex&openid.mode=checkid_setup&openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0>

The link to their Facebook page is: <https://www.facebook.com/Amazon/> The address of their corporate headquarters is: 440 Terry Ave N, Seattle, WA 98109. In Amazon’s information page the leadership is identified as: Jeffery P. Beezos, Executive Char; Andy Jassy, President and CEO; Brian T. Olsavsky, Senior VP and CFO; Matt Garman, CEO of Amazon Web Services; Douglas J. Herrington, CEO of Worldwide Amazon Stores (Amazon.com, Inc., n.d.). According to the about page on Amazon 88,000+ employees are employed in the Puget sound region, all other reports are regarding this region and any other sources are not from Amazon (Amazon Staff, 2025). In regard to any business partners that Amazon works with the site only gives a rough estimate that they work with,” thousands of hands-on entrepreneurs “*(Amazon Staff, n.d.)*.

## Findings and Conclusions

The information that can be concluded for each domain are significant in terms of their recon value as well as the added context that can be gleamed from the search engine results. The technical results for each domain are the domain information from WHOIS, whether or not the domain responds to a ping request, its ipv4 and ipvv6 address, and the number of hops away it is from the device which performed the command. I did my public domain search for Amazon.com, from this I found the URL for its ecommerce site, Facebook page, as well as the number of people they employ in a geographical area, lastly they also have thousands of independent small scale partners. With this information I can, for example, see where I can perform man-in-the middle attacks since I know where the traffic goes through, I know where their employees are so I can perform my attacks when they are most active to mask my activity, I know wether or not a domain is reachable from my device, and lastly I could pose as one of their thousands of independent partners so I can do some social engineering.

**References**

Amazon.com, Inc. (n.d.). *Officers and directors*. Investor Relations. Retrieved July 9, 2025, from <https://ir.aboutamazon.com/officers-and-directors/default.aspx>

Amazon Staff. (2025, June 23). *Amazon in the community: Here’s what’s happening in Seattle, Bellevue, and the Puget Sound*. About Amazon. Retrieved July 9, 2025, from <https://www.aboutamazon.com/news/community/amazon-headquarters-seattle-bellevue-puget-sound-news>

Amazon Staff. (n.d.). *Delivery Service Partners*. About Amazon. Retrieved July 9, 2025, from <https://www.aboutamazon.com/impact/empowerment/delivery-partners?utm_source=chatgpt.com>

1. Figure 1 – WHOIS results for Apple.com [↑](#footnote-ref-1)
2. Figure 2 – WHOIS results for Facebook.com [↑](#footnote-ref-2)
3. Figure 3 – WHOIS results for Microsoft.com [↑](#footnote-ref-3)
4. Figure 4 – PING results for Apple.com [↑](#footnote-ref-4)
5. Figure 5 – PING results for Microsoft.com [↑](#footnote-ref-5)
6. Figure 6 – PING results for Facebook.com [↑](#footnote-ref-6)
7. Figure 7 – nslookup results for Apple.com, Microsoft.com, and Facebook.com [↑](#footnote-ref-7)
8. Figure 8 – tracert results for Microsoft.com, failed [↑](#footnote-ref-8)
9. Figure 9 – tracert results for Facebook.com [↑](#footnote-ref-9)
10. Figure 10 – tracert results for apple.com [↑](#footnote-ref-10)