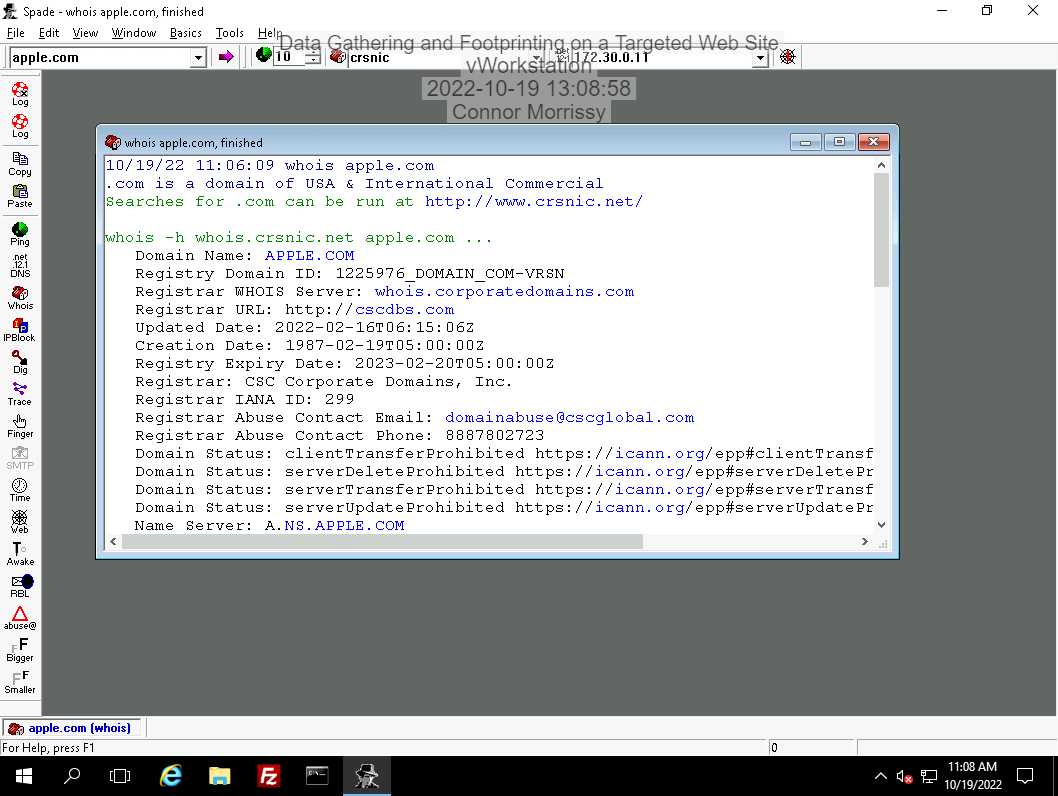
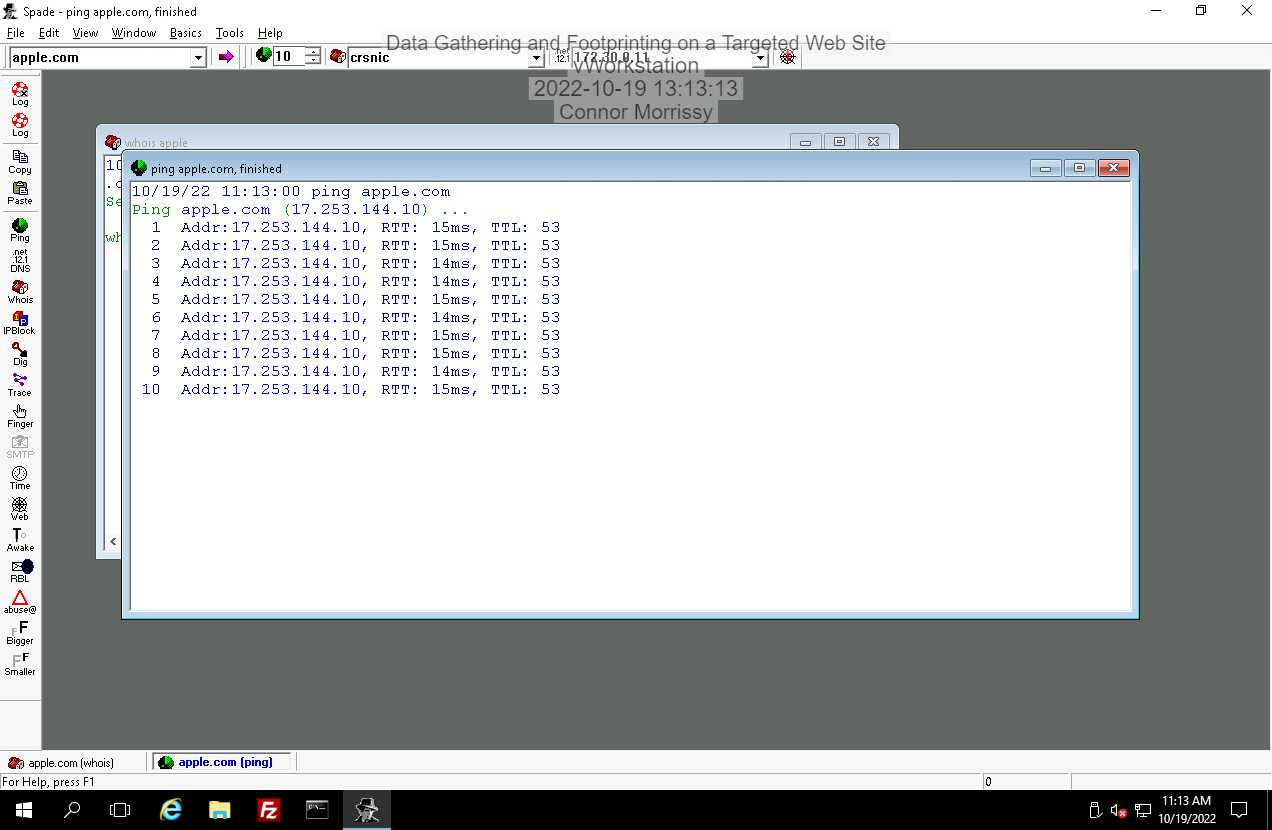
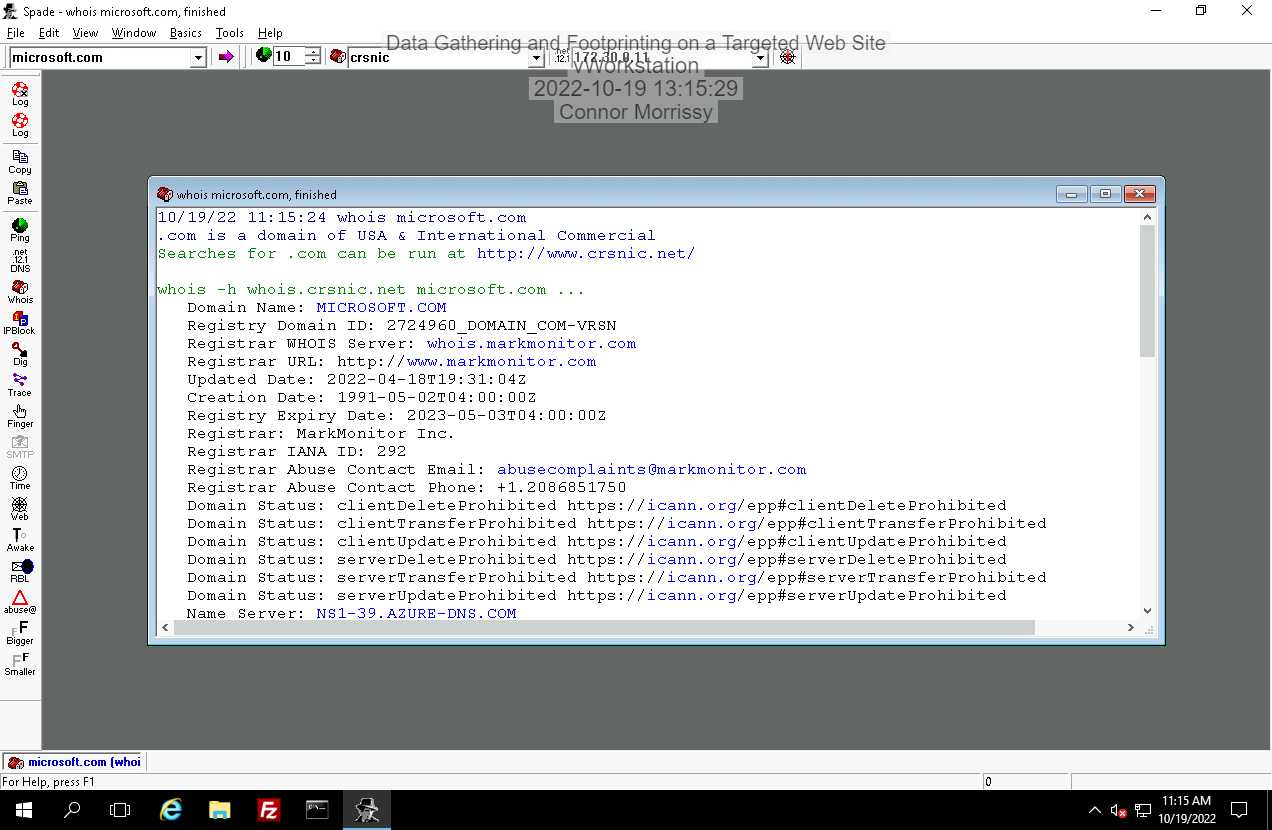
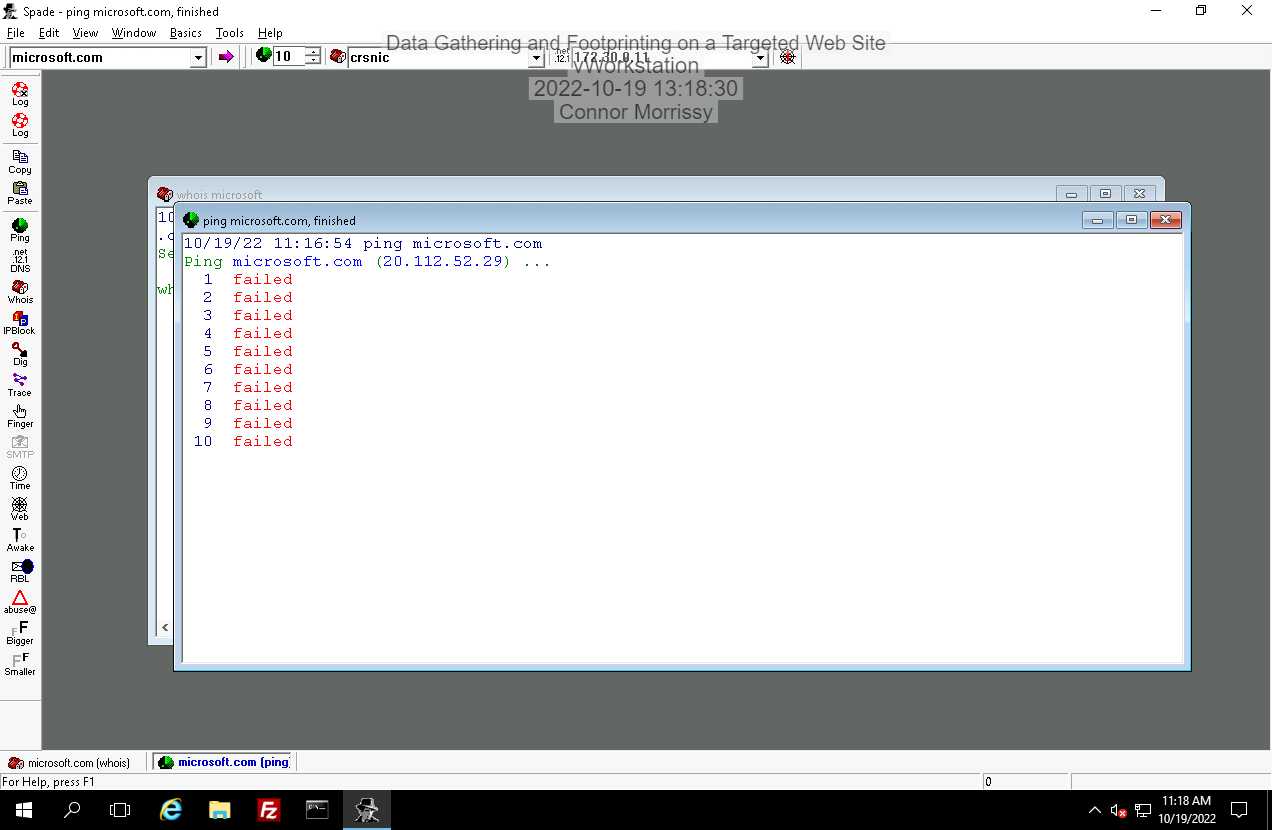
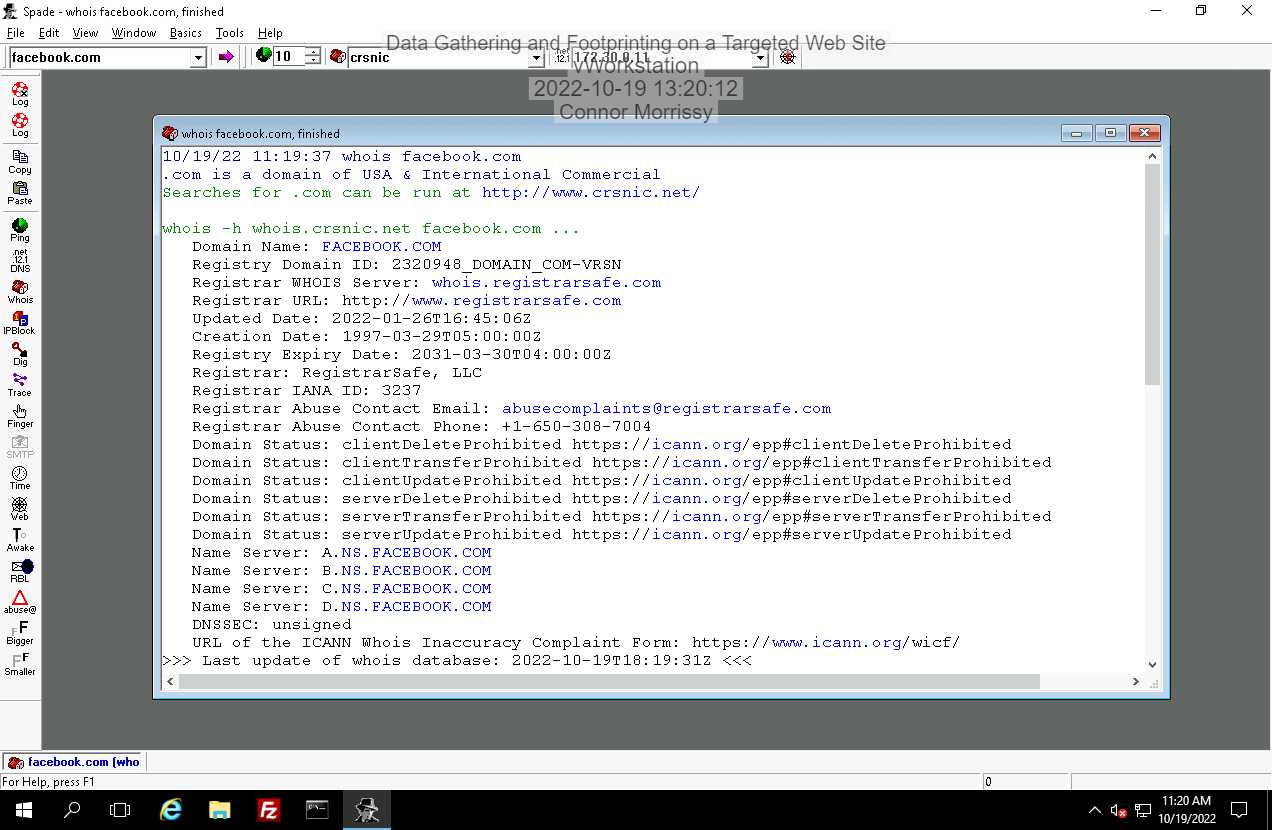
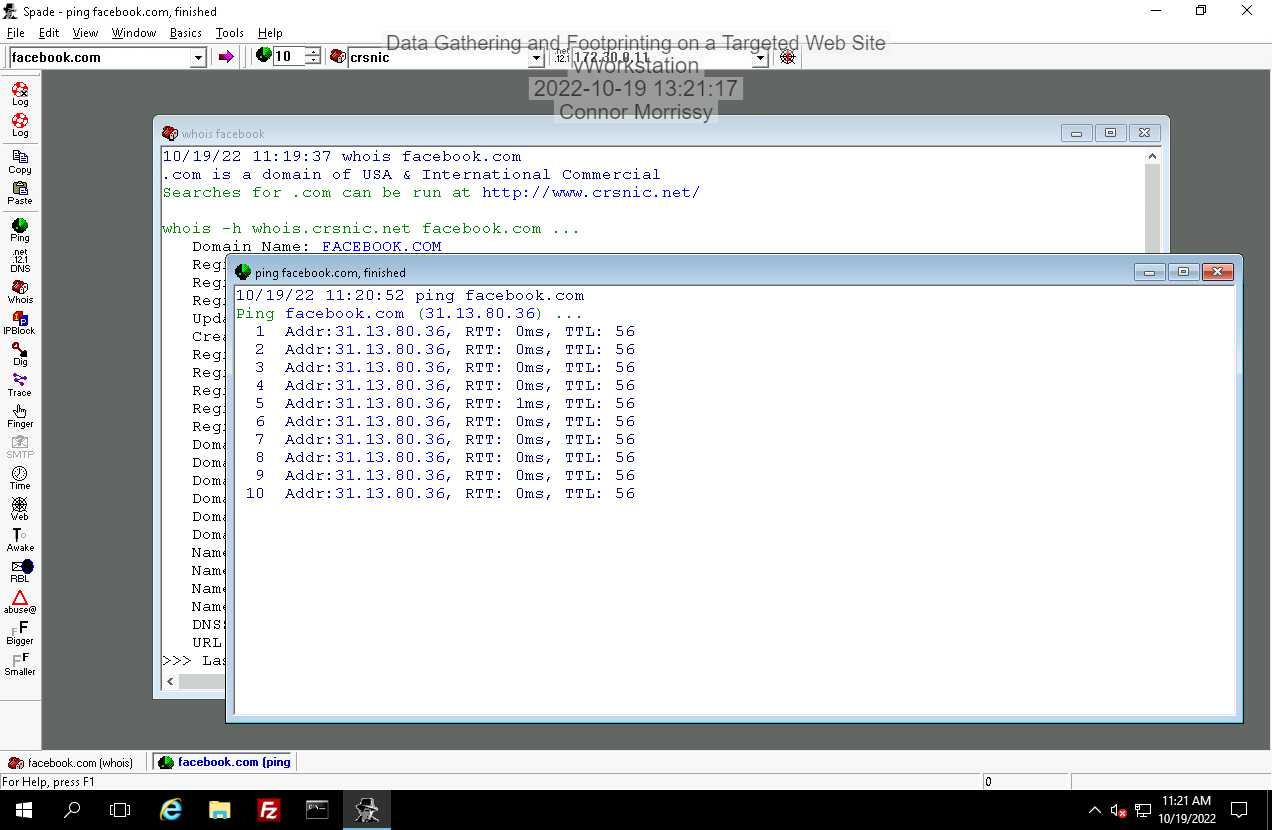
**Section 1 – Part 1**

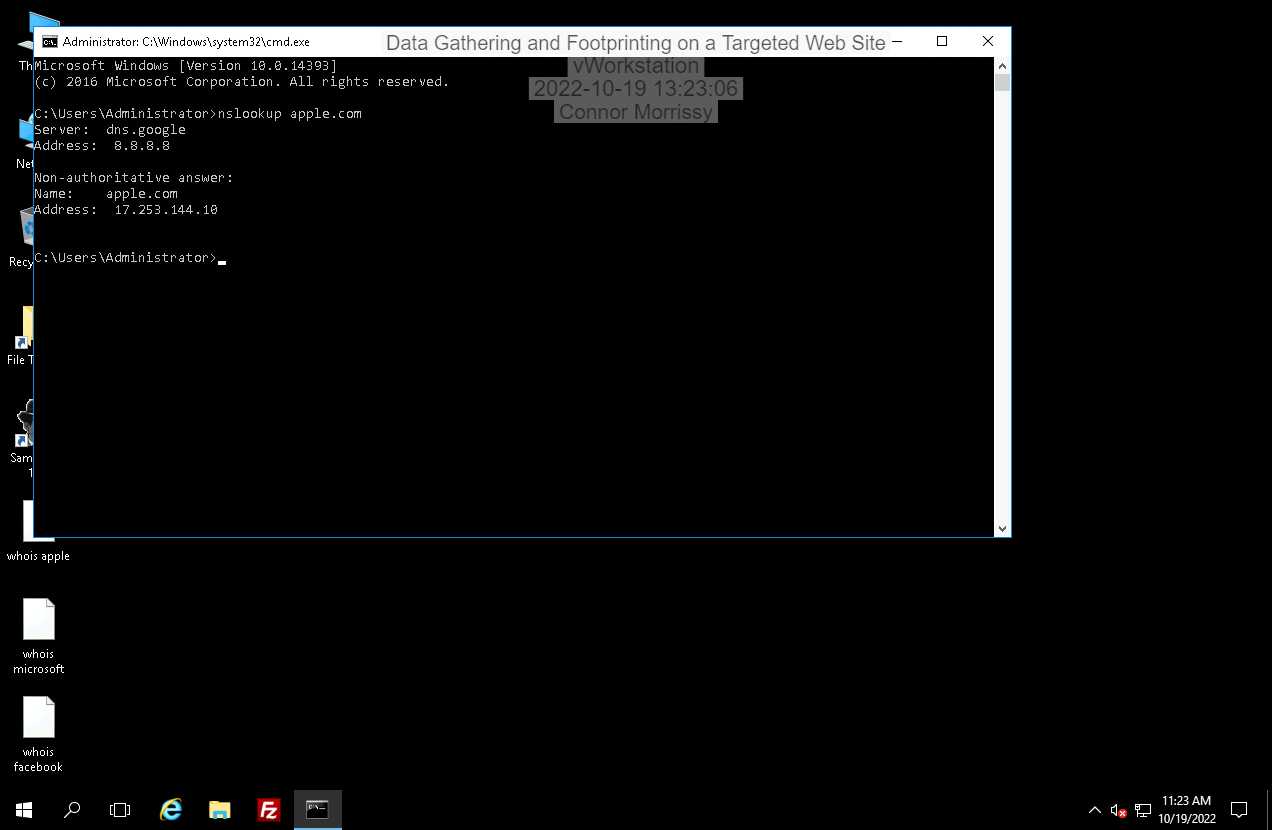


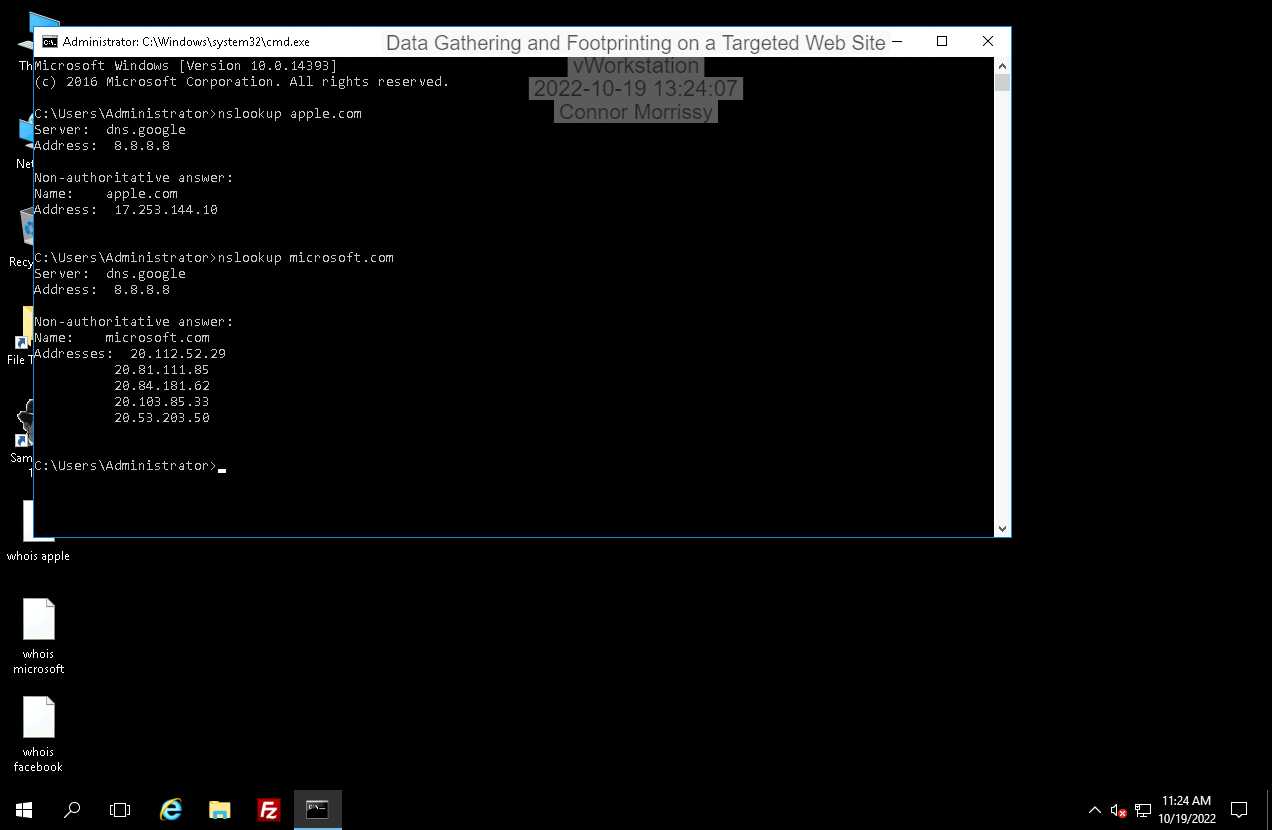


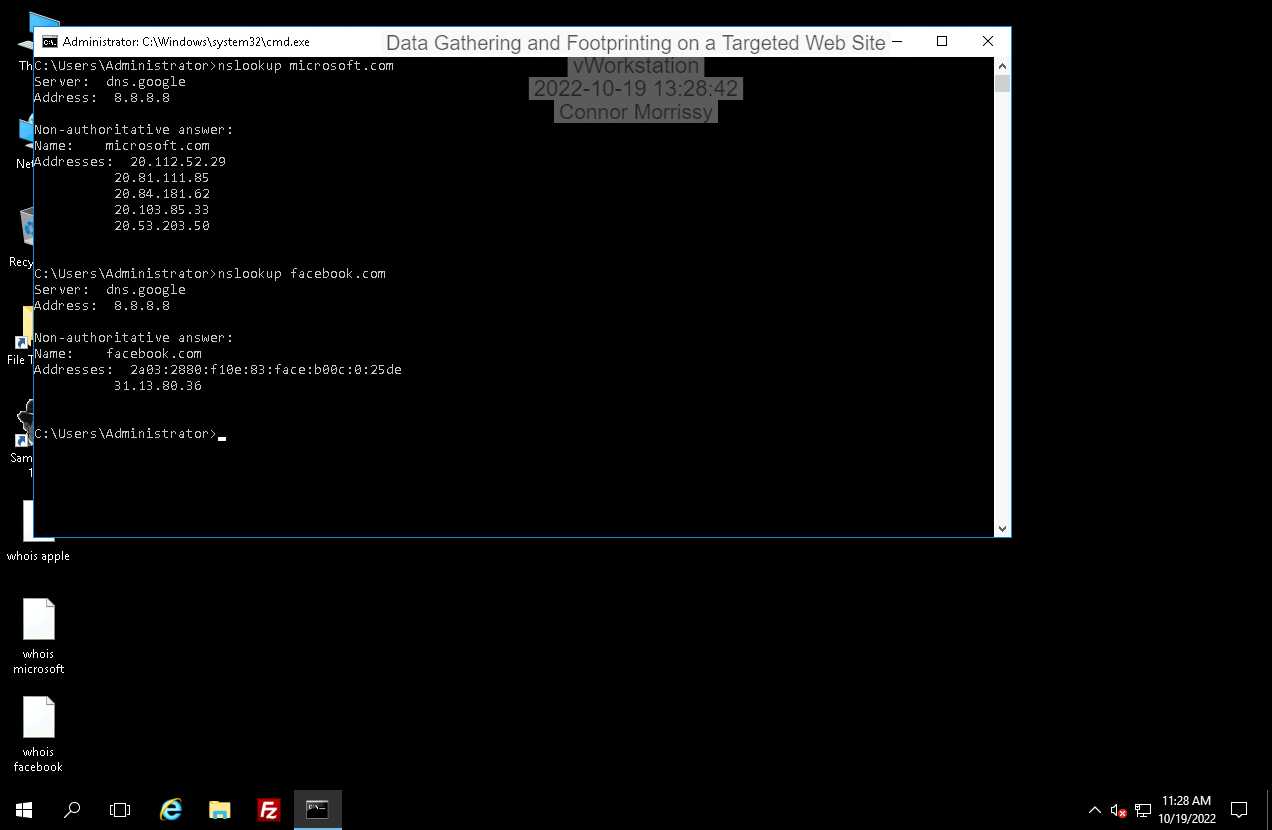
  


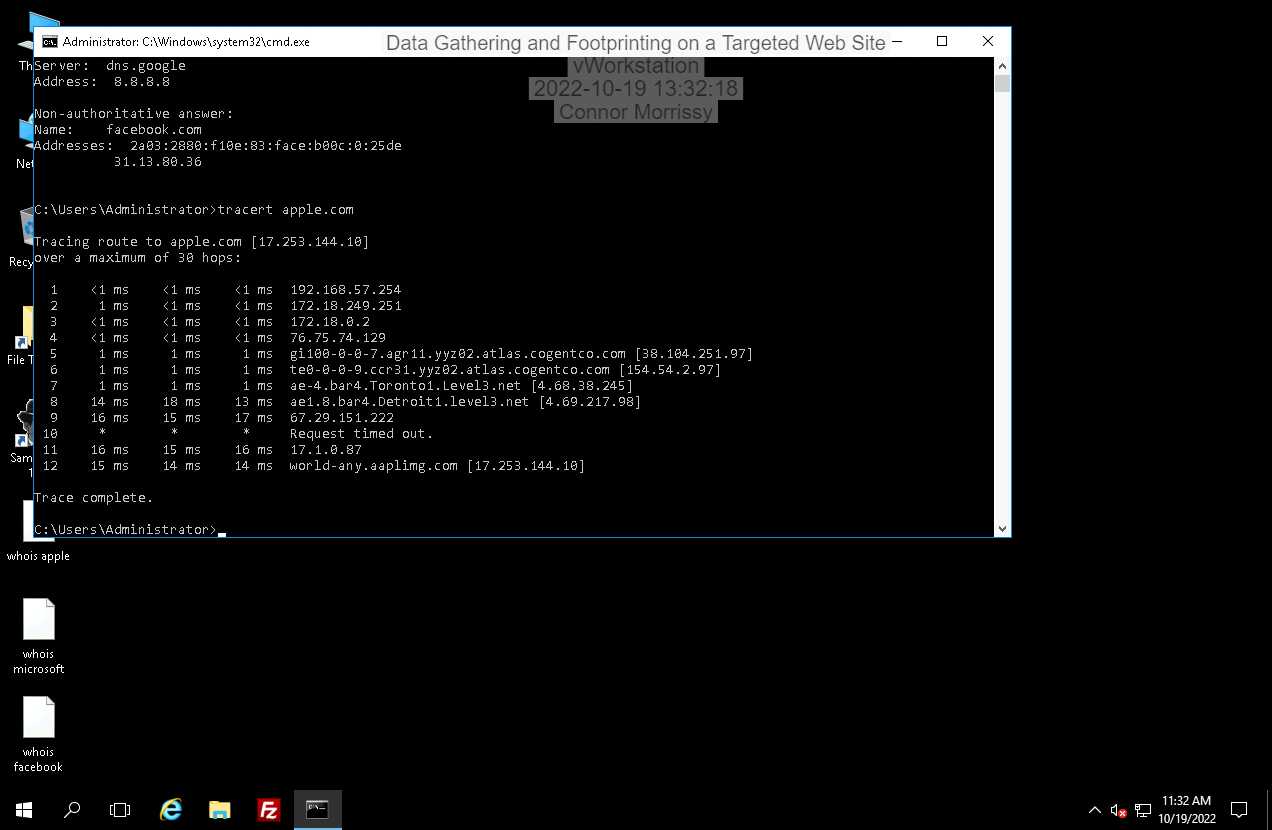


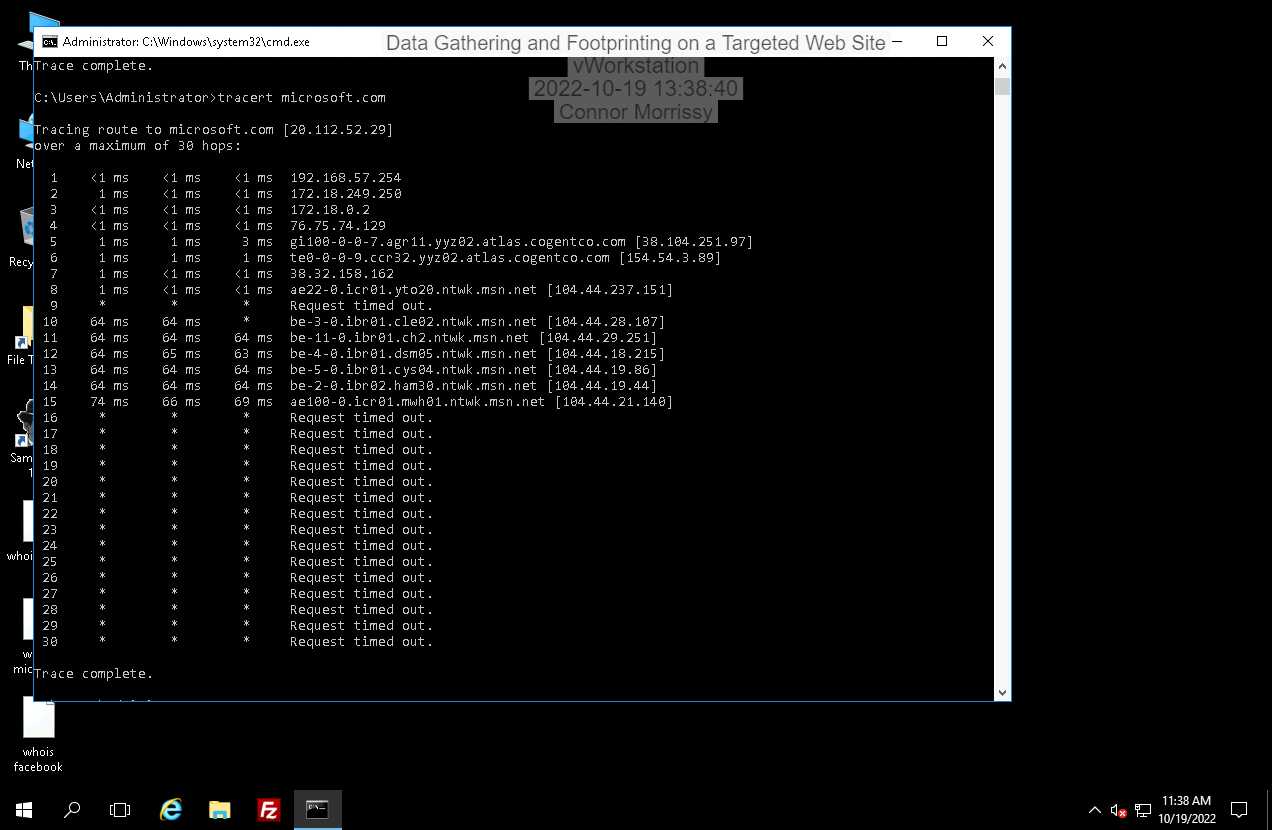


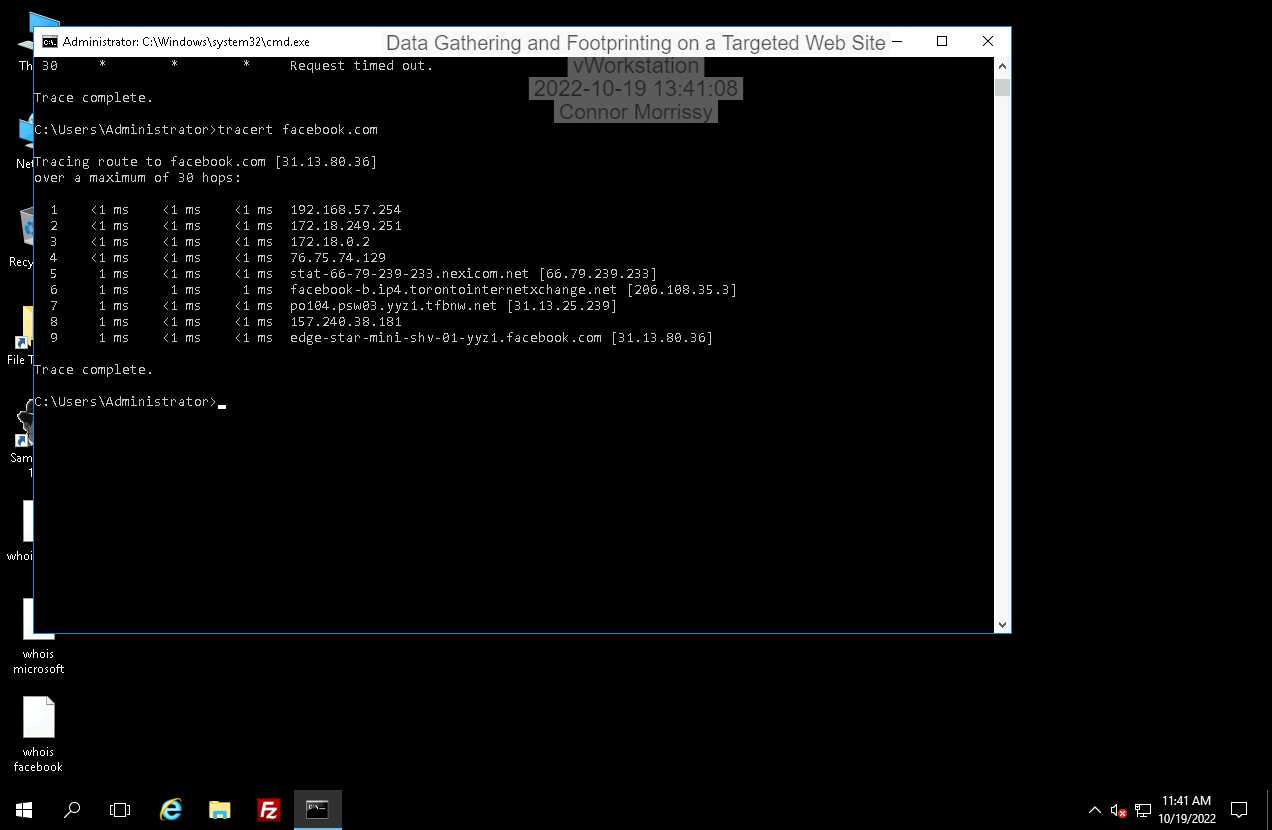












**Section 1 – Part 2**

 Name of the target organization: Amazon.com, Inc.

 Domain name and extension (*domain.ext*) for the target organization (for example, amazon.com): amazon.com

 URLs for the e-commerce website and any social networking sites:   
amazon.com is an e-commerce website, and aboutamazon.com for their information and background

 Physical address of the main headquarters location used by the target company; use Google Maps to locate the building. – Seattle, Washington

 Names of officers (for example, CEO, president, and CIO) at the organization:

Executive Chair – Jeffery Bezos  
 President and Chief Executive Officer – Andy Jassy

Senior Vice President and Chief Financial Officer – Brian Olsavsky

 Number of employees at each major physical location:

85000+ at Seattle, Washington HQ

35000+ at Arlington, Virginia Office

5000+ at Nashville, Tennessee Office

 Business partners or clients of the organization:  
They have a Business Partner Network program, which tells me they probably have a ton of business partners. They also have a ton of clients, including the public.

**Section 1 – Part 3**

**Executive Summary:** The goal of this lab was to scan four different company domains and acquire information that is publicly available in order to find weaknesses or gain knowledge about the domain. The program Sam Spade was used in collaboration with command-line tools to scan information about the domain. Additional public domain research was done using the internet. This information is useful for a hacker to find weaknesses and plan an attack.

**Methodology** The Sam Spade program was used to run WHOIS and PING commands to perform domain reconnaissance of popular websites apple.com, microsoft.com, and facebook.com. The nslookup command was used to look up their DNS records.The tracert command was used to see the path to the business’s domain server and to find potential intermediate attack points. Then, public domain research was performed via an internet search engine to find more public information about a company that you couldn’t find with command-line utilities.

**Technical Research Results**: The Sam Spade WHOIS results gave information about each domain such as the name of the domain owner, the contact for the entity responsible for the domain, and the relevant nameservers that are responsible for the domain.

**Public Domain Research Results:** An internet search engine (google.com) was used to find public information about the company such as the domain name, the headquarters location, the officers and important people in the company, and the number of employees the company has in different locations.

**Findings and Conclusions:**

**Apple.com:  
 Domain name:** apple.com **Registrar WHOIS server:** whois.corporatedomains.com **Registrar contact email:** domainabuse@cscglobal.com **Contact phone:** 888-780-2723 **Name server:** a.ns.apple.com

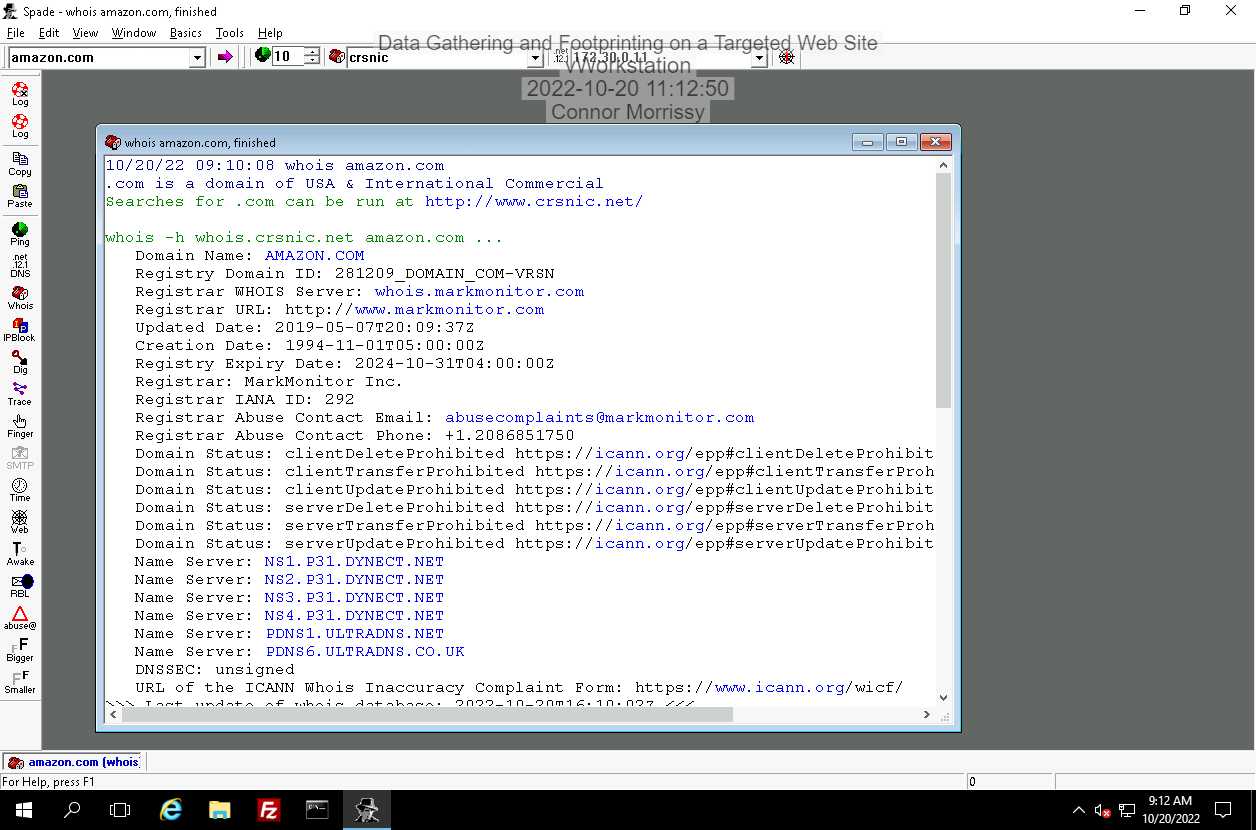
**Microsoft.com:  
 Domain name:** microsoft.com **Registrar WHOIS server:** whois.markmonitor.com **Registrar contact email:** abusecomplaints@markmonitor.com **Contact phone:** 208-685-1750 **Name server:** ns1-39.azure-dns.com

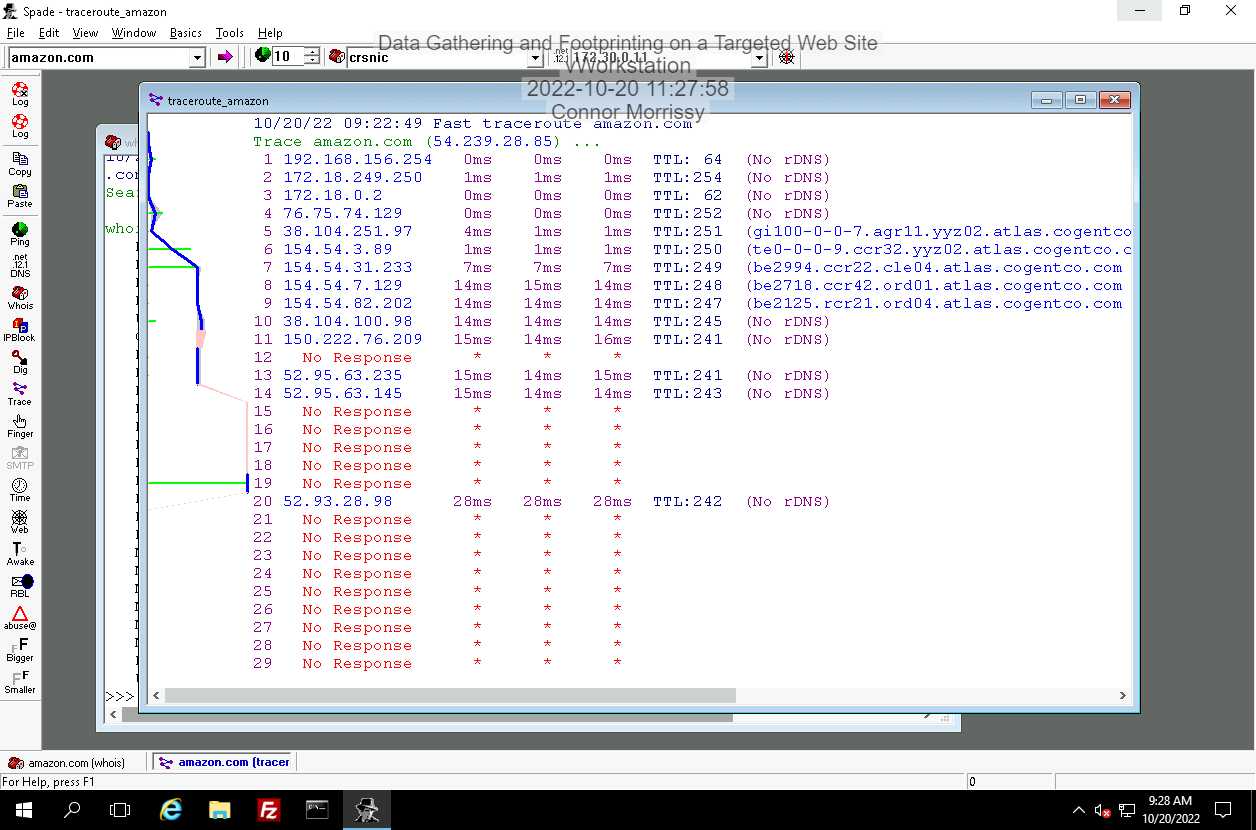
**Facebook.com:  
 Domain name:** facebook.com **Registrar WHOIS server:** whois.registrarsafe.com **Registrar contact email:** abusecomplaints@registrarsafe.com **Contact phone:** 650-308-7004 **Name server:** a.ns.facebook.com

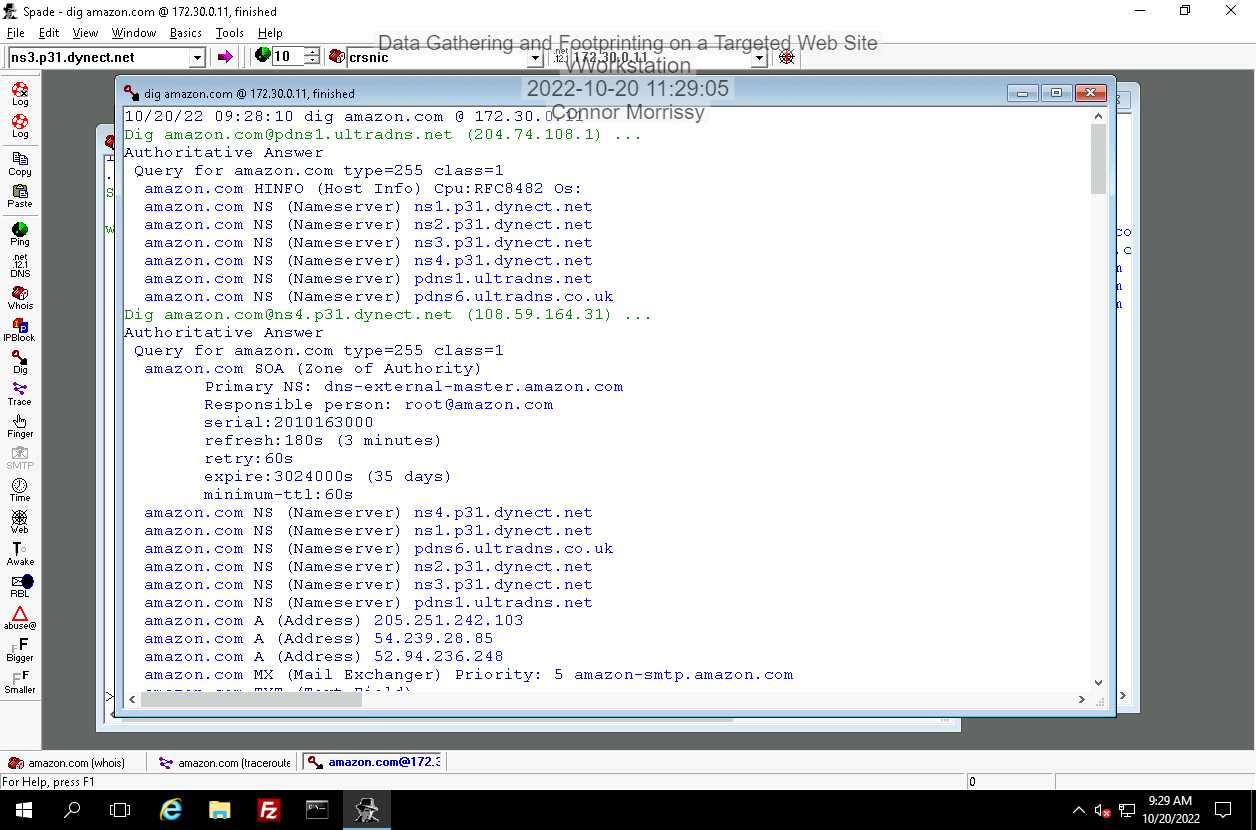
**Avenues of Further Research:**

If I was planning a hacking attempt on this company, I would want to know more about the network and what kind of security they have on the network and their operating systems. I would also check other sites they host on the domain to look for potential weaknesses.

**Section 1 – Part 1:**

****





**Section 2 – Part 2:**

The lab states to SKIP Part 2 of this section if we have completed Section 1, which I have.

**Section 2 – Part 3:**

The lab states to use the previous research report as a draft and add on to it for the amazon.com domain:

**Executive Summary:** The goal of this lab was to scan four different company domains and acquire information that is publicly available in order to find weaknesses or gain knowledge about the domain. The program Sam Spade was used in collaboration with command-line tools to scan information about the domain. Additional public domain research was done using the internet. This information is useful for a hacker to find weaknesses and plan an attack. I then made the same scans for another company, amazon.com.

**Methodology** The Sam Spade program was used to run WHOIS and PING commands to perform domain reconnaissance of popular websites apple.com, microsoft.com, and facebook.com. The nslookup command was used to look up their DNS records.The tracert command was used to see the path to the business’s domain server and to find potential intermediate attack points. Then, public domain research was performed via an internet search engine to find more public information about a company that you couldn’t find with command-line utilities. To find out more about amazon.com, a WHOIS, TRACERT, and DIG command was executed on Sam Spade.

**Technical Research Results**: The Sam Spade WHOIS results gave information about each domain such as the name of the domain owner, the contact for the entity responsible for the domain, and the relevant nameservers that are responsible for the domain.

**Public Domain Research Results:** An internet search engine (google.com) was used to find public information about the company such as the domain name, the headquarters location, the officers and important people in the company, and the number of employees the company has in different locations.

**Findings and Conclusions:**

**Apple.com:  
 Domain name:** apple.com **Registrar WHOIS server:** whois.corporatedomains.com **Registrar contact email:** domainabuse@cscglobal.com **Contact phone:** 888-780-2723 **Name server:** a.ns.apple.com

**Microsoft.com:  
 Domain name:** microsoft.com **Registrar WHOIS server:** whois.markmonitor.com **Registrar contact email:** abusecomplaints@markmonitor.com **Contact phone:** 208-685-1750 **Name server:** ns1-39.azure-dns.com

**Facebook.com:  
 Domain name:** facebook.com **Registrar WHOIS server:** whois.registrarsafe.com **Registrar contact email:** abusecomplaints@registrarsafe.com **Contact phone:** 650-308-7004 **Name server:** a.ns.facebook.com

**Amazon.com**:  
 **Domain name:** amazon.com **Registrar WHOIS server:** whois.markmonitor.com **Registrar contact email:** abusecomplaints@markmonitor.com **Contact phone:** 208-685-1750 **Name server:** ns1.p31.dynect.net

**Jblearning.com: (added for Section 3 – Part 3)  
 Domain name:** jblearning.com **Registrar WHOIS server:** whois.namecheap.com **Registrar contact email:** abuse@namecheap.com **Contact phone:** 661-310-2107 **Name server:** cass.ns.cloudfare.com

**Avenues of Further Research:**

If I was planning a hacking attempt on this company, I would want to know more about the network and what kind of security they have on the network and their operating systems. I would also check other sites they host on the domain to look for potential weaknesses.

**Section 3 – Part 1:**

Information found from https://www.garykessler.net/library/is\_tools\_sam\_spade.html:

* *Ping* sends a series of packets to the indicated host to determine if that system is reachable via the network and provides an estimate of the round trip packet time.
* *Traceroute* traces the route that packets take from the user's system to the specified target host address, listing all intermediate routers and showing a graph of the hop-by-hop delay times. Fast and slow traceroute differ only in the number of attempts made to learn the route.
* *Nslookup* and *Decode URL* display the IP address and name of a specified host. This can help an investigator learn about the owner of a system from the domain name or obtain an IP address with which to further investigate the geographic location of a system.
* *Whois* provides ownership and contact information for the specified host's domain. This tool is increasingly convenient as the number of domain name registrars grows. When Network Solutions was the sole registrar for .com, for example, their whois database was the only one you needed to search. With about 100 accredited registrars today, you have to do a search just to find out which registrar to lookup. Sam Spade's whois function does this for you.
* *IP Block* indicates the owner of the IP address block to which the specified host belongs. By identifying the owner of an address block, you can start to narrow down where a host is geographically located and/or learn about the host's upstream Internet service provider (ISP).
* *DIG (Domain Internet Groper)*, like nslookup, looks up DNS information. Sam Spade's DIG function returns all DNS records associated with a specified host or domain, including the start of authority (SOA), mail exchange (MX) and name server (NS) records. This information allows the user to determine where to send e-mail to a host's domain and how to access the manager of the domain's name space.
* *Zone Transfer* is used to request that a DNS server send all of the information that it has about a given domain. Properly configured DNS servers will not comply with this request as a security precaution, but it will work surprisingly often. This is a great way to test your own name servers.
* *Finger* obtains host/user information from a system running the finger daemon (TCP port 79). Finger is generally (or should be) disabled at a host because it can give an attacker a lot ofinformation about users and/or the host itself, but it isn't always turned off.

**Section 3 – Part 2:**

The traceroute command can give a relative, general idea of how far a target IP address is. The whois command, however, gives detailed public information about who owns the domain, who to contact, and also locations for the ISP or relevant parties who own/manage the domain.

**Section 3 – Part 3:**

Domain information about jblearning.com was added to the Research Report located in Section 2 – Part 3 of this lab file.