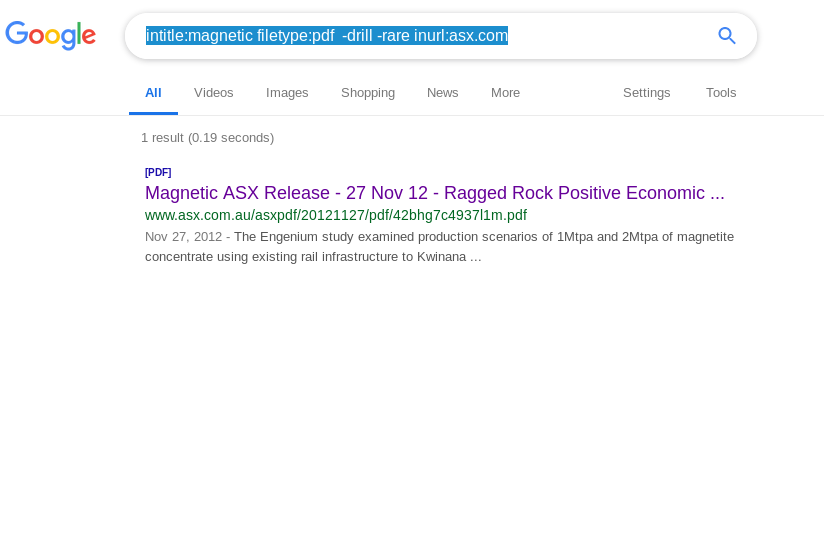
A1691850 2019/03/18

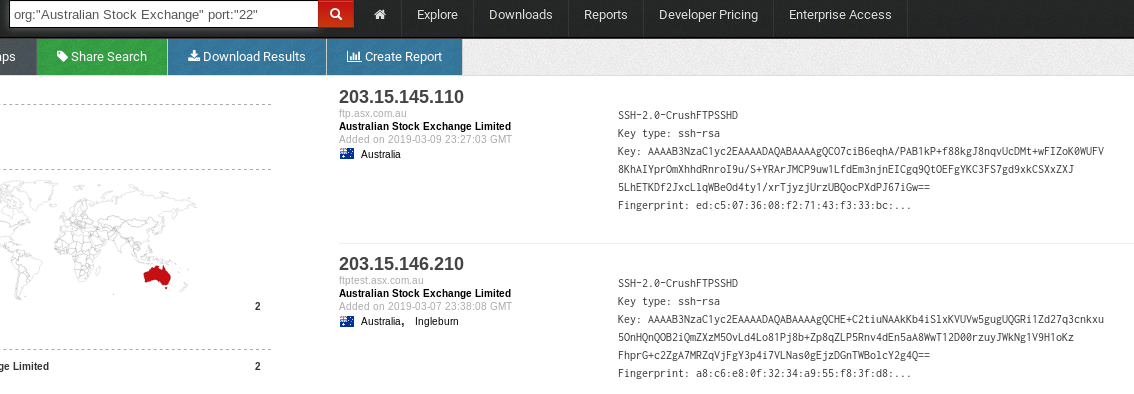
Q1.

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Google Search Syntax | intitle:magnetic filetype:pdf -drill -rare inurl:asx.com |
| SHA256 Hash of the PDF file | 8e5c7b0837e36e3d28b249633e825658180df0d39657d6162049efe5b4b4d34a |
| PDF author according to metadata | rthomson |
| PDF creation software according to metadata | PDFCreator Version 1.4.1 |



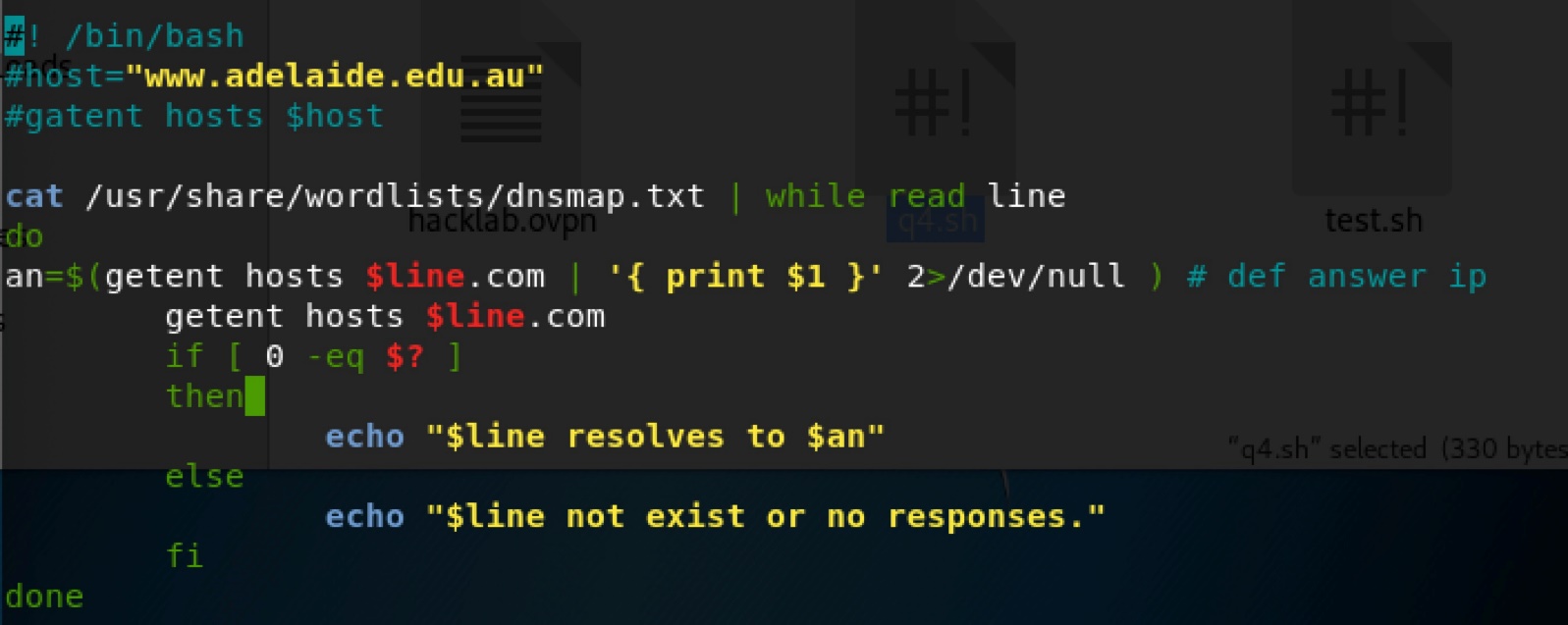
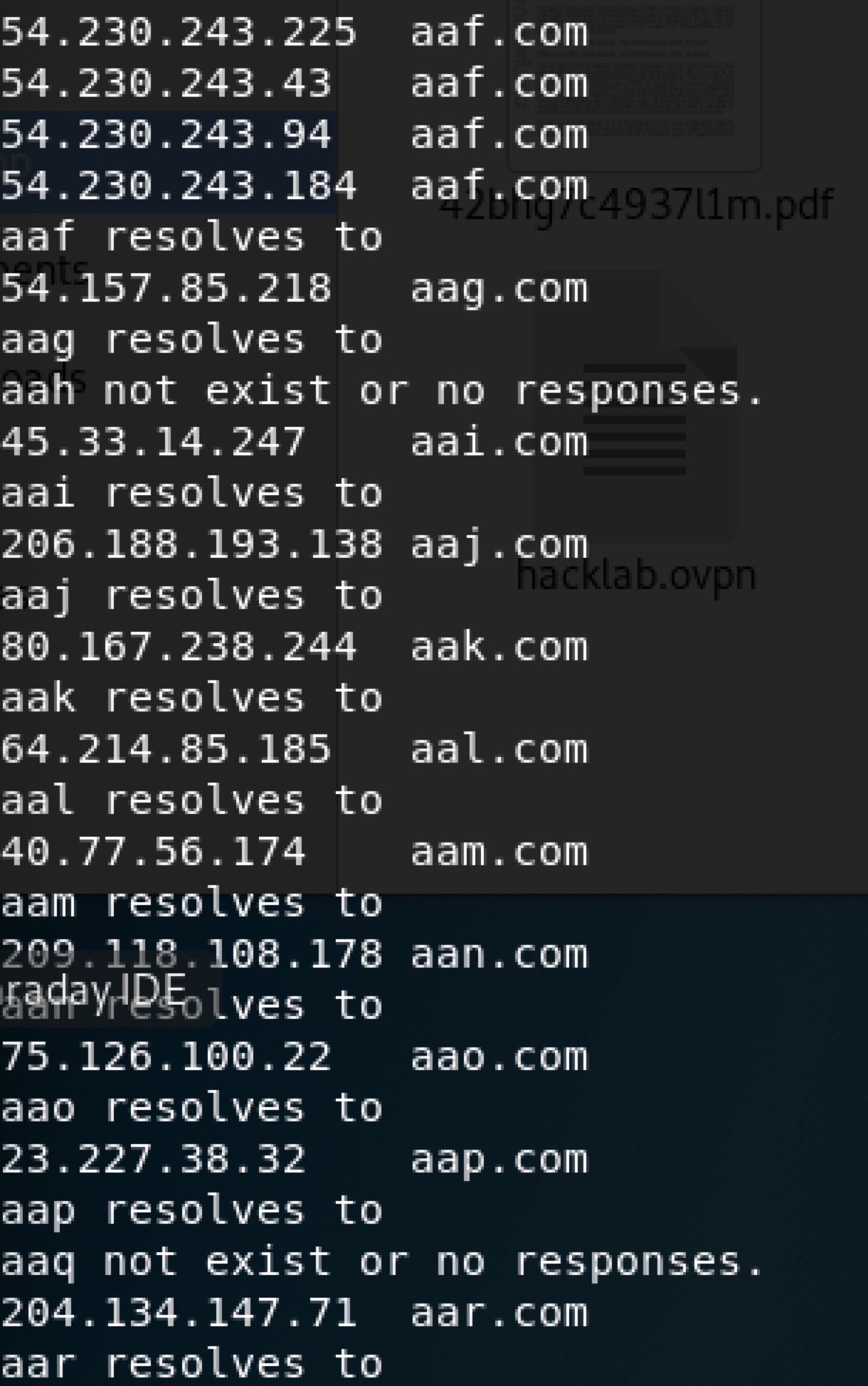
Q2.

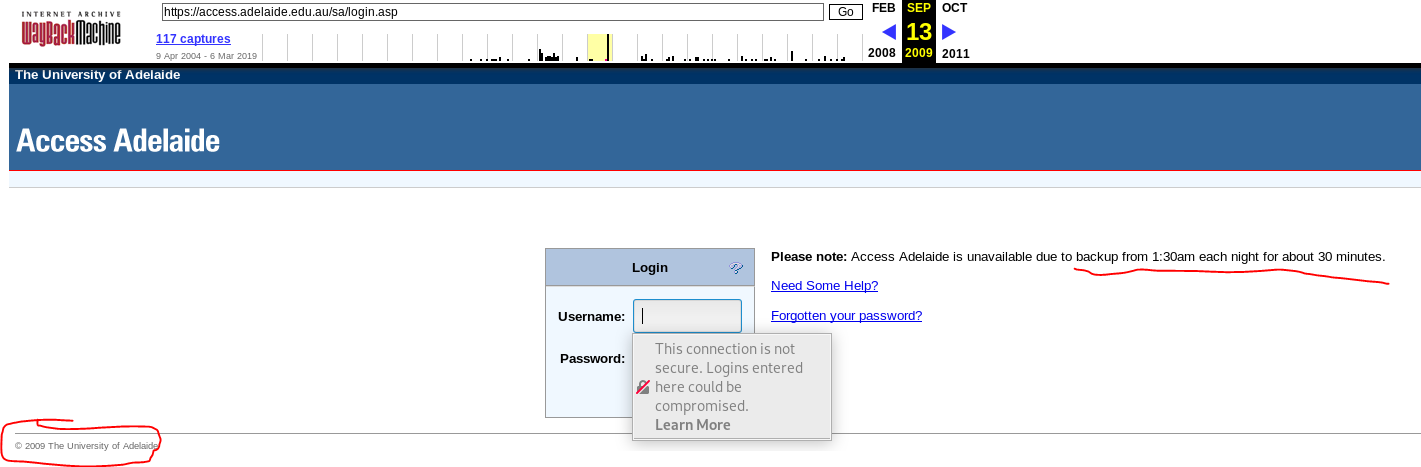
|  |  |
| --- | --- |
| dunstan.org.au resolves to | 129.127.149.1 |
| Other domain names that resolve to the same address | NS.ADELAIDE.EDU.AU |
| Owner of the IP address | University Of Adelaide |
| The IP address range which the IP address belongs | 129.127.149.1-35 |
| The "AS" number of the same IP range | AS1851 |
| Other netblocks registered under the same ASN |  |
|  |

Q3. 

|  |  |
| --- | --- |
| What is the ASN of ASX? | AS18361 |
| There are two IIS7.0 servers running (according to Shodan). What are the IP addresses and the common names (CN)? | Ip: 203.15.147.71  Cn: GeoTrust RSA CA  Ip: 203.15.147.77  Cn: GeoTrust RSA CA |
| There are also two SFTP server running on port 22 according to Shodan. What are the hostnames and the name of the FTP server product? | Hostname: ftptest.asx.com.au  Productname:SSH-2.0-CrushFTPSSHD  Hostname: ftp.asx.com.au  ProductName: SSH-2.0-CrushFTPSSHD |
| Lookup the product in exploit-db.com. Are there known vulnerabilities for that product? | Omniture SiteCatalyst - Multiple Cross-Site Scripting Vulnerabilities |
| Similarly, lookup the product name at https://cve.mitre.org (Links to an external site.)Links to an external site.. What are some of the known vulnerabilities for this product? | Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) processes unspecified commands before TLS is enabled for a session, which allows remote attackers to obtain sensitive information by reading the replies to these commands, aka "FTP Command Injection Vulnerability."  CVE-2010-1899 Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."  CVE-2009-2521 Stack consumption vulnerability in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows remote authenticated users to cause a denial of service (daemon crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot), aka "IIS FTP Service DoS Vulnerability."  CVE-2008-0074 Unspecified vulnerability in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows local users to gain privileges via unknown vectors related to file change notifications in the TPRoot, NNTPFile\Root, or WWWRoot folders. |

Q4.



Q5. 

Q6.

