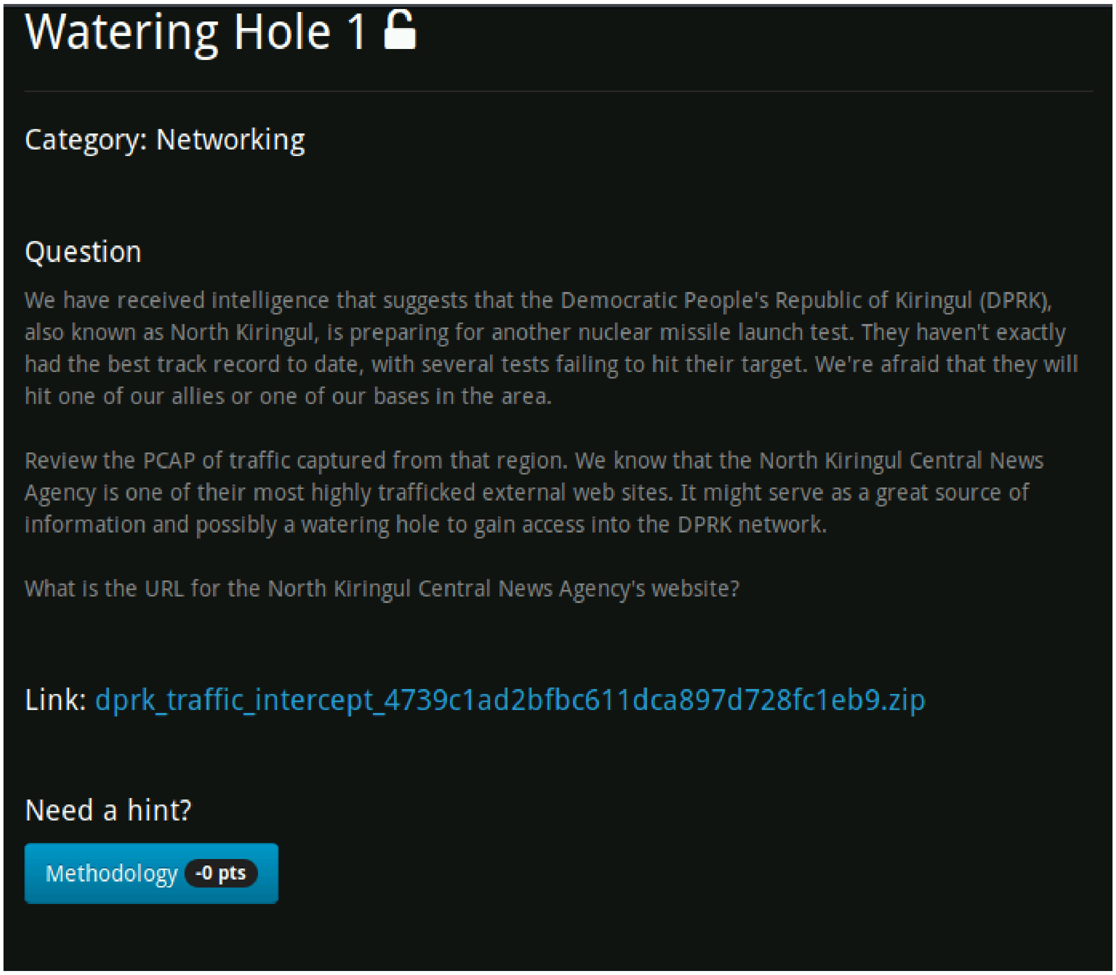


Watering Hole 1

Category: Networking

Question

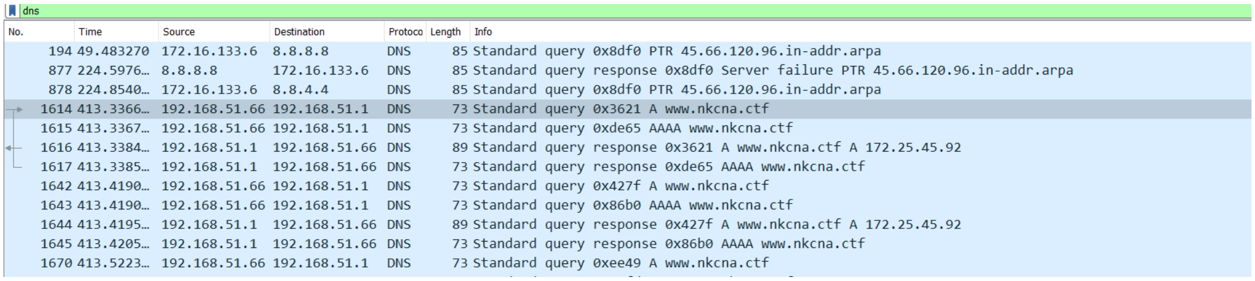
We have received intelligence that suggests that the Democratic People's Republic of Kiringul (DPRK), also known as North Kiringul, is preparing for another nuclear missile launch test. They haven't exactly had the best track record to date, with several tests failing to hit their target. We're afraid that they will hit one of our allies or one of our bases in the area.

Review the PCAP of traffic captured from that region. We know that the North Kiringul Central News Agency is one of their most highly trafficked external web sites. It might serve as a great source of information and possibly a watering hole to gain access into the DPRK network.

What is the URL for the North Kiringul Central News Agency's website?

Link: dprk_traffic_intercept_4739c1ad2bfbc611dca897d728fc1eb9.zip

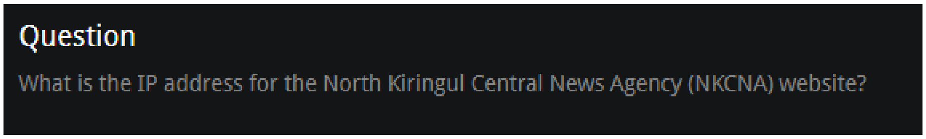
Need a hint?



dns

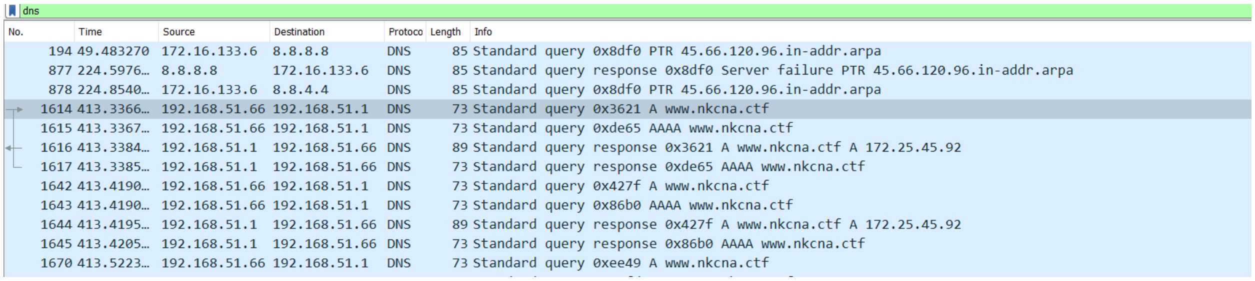
No.	Time	Source	Destination	Protoco	Length	Info
194	49.483270	172.16.133.6	8.8.8.8	DNS	85	Standard query 0x8df0 PTR 45.66.120.96.in-addr.arpa
877	224.5976…	8.8.8.8	172.16.133.6	DNS	85	Standard query response 0x8df0 Server failure PTR 45.66.120.96.in-addr.arpa
878	224.8540…	172.16.133.6	8.8.4.4	DNS	85	Standard query 0x8df0 PTR 45.66.120.96.in-addr.arpa
1614	413.3366…	192.168.51.66	192.168.51.1	DNS	73	Standard query 0x3621 A www.nkcna.ctf
1615	413.3367…	192.168.51.66	192.168.51.1	DNS	73	Standard query 0xde65 AAAA www.nkcna.ctf
1616	413.3384…	192.168.51.1	192.168.51.66	DNS	89	Standard query response 0x3621 A www.nkcna.ctf A 172.25.45.92
1617	413.3385…	192.168.51.1	192.168.51.66	DNS	73	Standard query response 0xde65 AAAA www.nkcna.ctf
1642	413.4190…	192.168.51.66	192.168.51.1	DNS	73	Standard query 0x427f A www.nkcna.ctf
1643	413.4190…	192.168.51.66	192.168.51.1	DNS	73	Standard query 0x86b0 AAAA www.nkcna.ctf
1644	413.4195…	192.168.51.1	192.168.51.66	DNS	89	Standard query response 0x427f A www.nkcna.ctf A 172.25.45.92
1645	413.4205…	192.168.51.1	192.168.51.66	DNS	73	Standard query response 0x86b0 AAAA www.nkcna.ctf
1670	413.5223…	192.168.51.66	192.168.51.1	DNS	73	Standard query 0xee49 A www.nkcna.ctf

Flag: www.nkcna.ctf



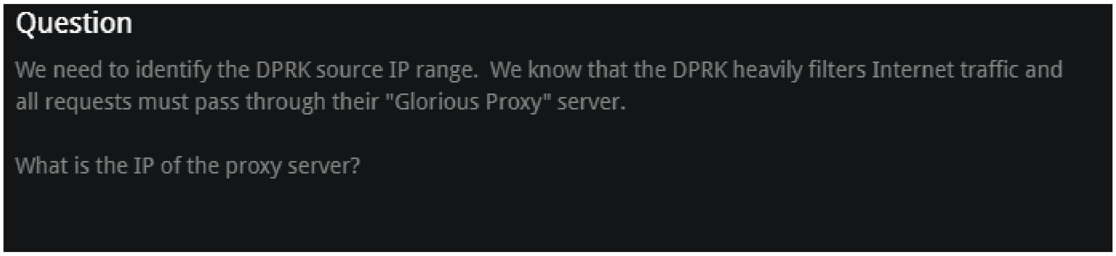
Question

What is the IP address for the North Kiringul Central News Agency (NKCNA) website?



```
dns
No.      Time         Source          Destination    Protoco Length Info
     194 49.483270    172.16.133.6    8.8.8.8        DNS     85 Standard query 0x8df0 PTR 45.66.120.96.in-addr.arpa
     877 224.5976…    8.8.8.8         172.16.133.6   DNS     85 Standard query response 0x8df0 Server failure PTR 45.66.120.96.in-addr.arpa
     878 224.8540…    172.16.133.6    8.8.4.4        DNS     85 Standard query 0x8df0 PTR 45.66.120.96.in-addr.arpa
    1614 413.3366…    192.168.51.66   192.168.51.1   DNS     73 Standard query 0x3621 A www.nkcna.ctf
    1615 413.3367…    192.168.51.66   192.168.51.1   DNS     73 Standard query 0xde65 AAAA www.nkcna.ctf
    1616 413.3384…    192.168.51.1    192.168.51.66  DNS     89 Standard query response 0x3621 A www.nkcna.ctf A 172.25.45.92
    1617 413.3385…    192.168.51.1    192.168.51.66  DNS     73 Standard query response 0xde65 AAAA www.nkcna.ctf
    1642 413.4190…    192.168.51.66   192.168.51.1   DNS     73 Standard query 0x427f A www.nkcna.ctf
    1643 413.4190…    192.168.51.66   192.168.51.1   DNS     73 Standard query 0x86b0 AAAA www.nkcna.ctf
    1644 413.4195…    192.168.51.1    192.168.51.66  DNS     89 Standard query response 0x427f A www.nkcna.ctf A 172.25.45.92
    1645 413.4205…    192.168.51.1    192.168.51.66  DNS     73 Standard query response 0x86b0 AAAA www.nkcna.ctf
    1670 413.5223…    192.168.51.66   192.168.51.1   DNS     73 Standard query 0xee49 A www.nkcna.ctf
```

Flag: 172.25.45.92

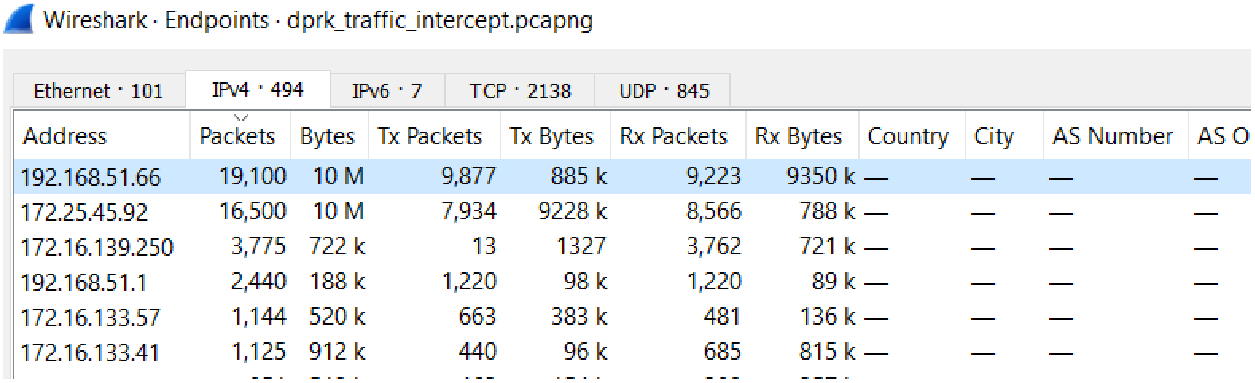


Question

We need to identify the DPRK source IP range. We know that the DPRK heavily filters Internet traffic and all requests must pass through their "Glorious Proxy" server.

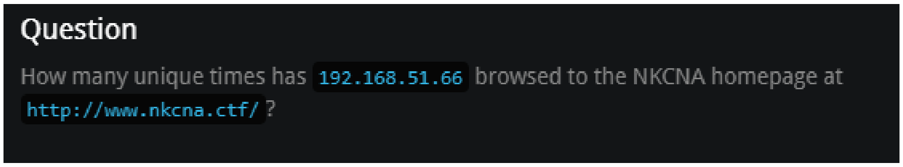
What is the IP of the proxy server?

Look at the top conversations by packet.



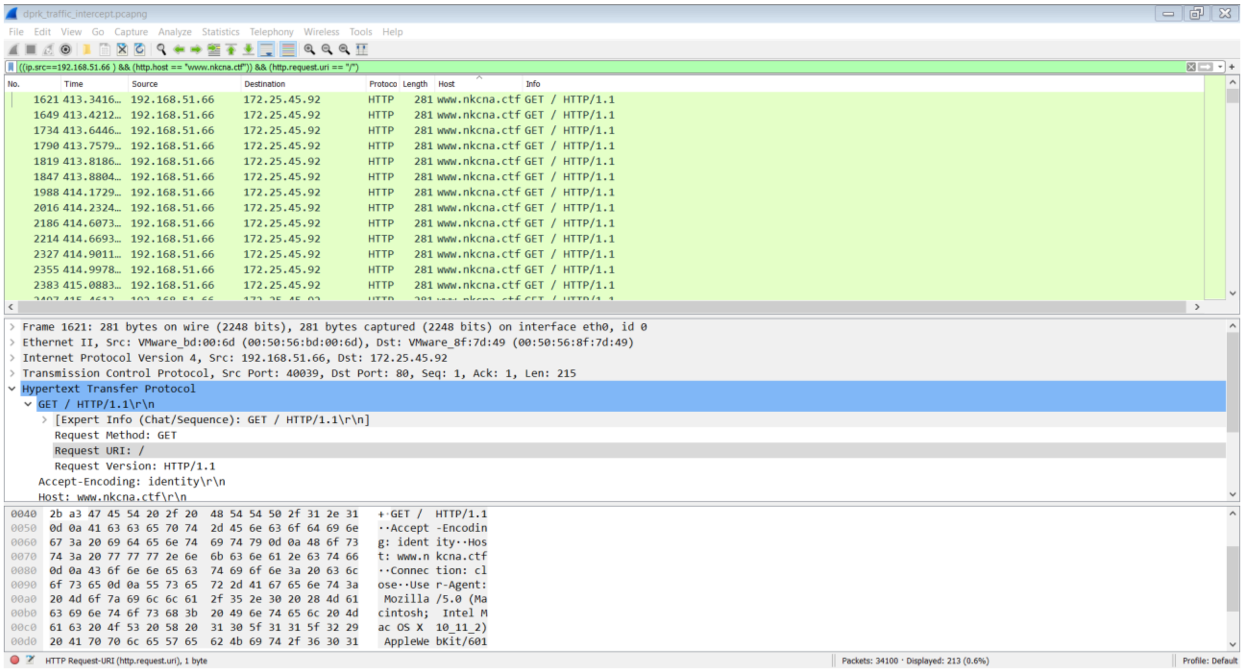
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS O
192.168.51.66	19,100	10 M	9,877	885 k	9,223	9350 k	—	—	—	—
172.25.45.92	16,500	10 M	7,934	9228 k	8,566	788 k	—	—	—	—
172.16.139.250	3,775	722 k	13	1327	3,762	721 k	—	—	—	—
192.168.51.1	2,440	188 k	1,220	98 k	1,220	89 k	—	—	—	—
172.16.133.57	1,144	520 k	663	383 k	481	136 k	—	—	—	—
172.16.133.41	1,125	912 k	440	96 k	685	815 k	—	—	—	—

Flag: 192.168.51.66



Question

How many unique times has `192.168.51.66` browsed to the NKCNA homepage at `http://www.nkcna.ctf/` ?



dprk_traffic_intercept.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
((ip.src==192.168.51.66 ) && (http.host == "www.nkcna.ctf")) && (http.request.uri == "/")
```

```
No.   Time        Source          Destination     Protoco Length Host          Info
1621 413.3416…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
1649 413.4212…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
1734 413.6446…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
1790 413.7579…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
1819 413.8186…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
1847 413.8804…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
1988 414.1729…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
2016 414.2324…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
2186 414.6073…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
2214 414.6693…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
2327 414.9011…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
2355 414.9978…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
2383 415.0883…  192.168.51.66    172.25.45.92     HTTP     281 www.nkcna.ctf GET / HTTP/1.1
```

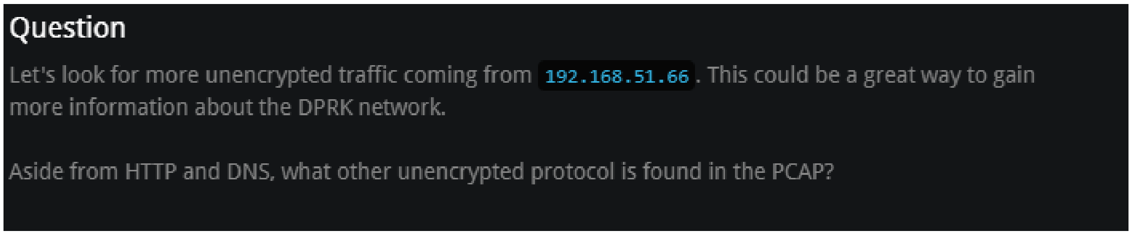
```
> Frame 1621: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_bd:00:6d (00:50:56:bd:00:6d), Dst: VMware_8f:7d:49 (00:50:56:8f:7d:49)
> Internet Protocol Version 4, Src: 192.168.51.66, Dst: 172.25.45.92
> Transmission Control Protocol, Src Port: 40039, Dst Port: 80, Seq: 1, Ack: 1, Len: 215
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Accept-Encoding: identity\r\n
    Host: www.nkcna.ctf\r\n
```

```
0040  2b a3 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   +·GET /  HTTP/1.1
0050  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0060  67 3a 20 69 64 65 6e 74  69 74 79 0d 0a 48 6f 73   g: ident ity··Hos
0070  74 3a 20 77 77 77 2e 6e  6b 63 6e 61 2e 63 74 66   t: www.n kcna.ctf
0080  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 63 6c   ··Connec tion: cl
0090  6f 73 65 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   ose··Use r-Agent:
00a0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 4d 61    Mozilla /5.0 (Ma
00b0  63 69 6e 74 6f 73 68 3b  20 49 6e 74 65 6c 20 4d   cintosh;  Intel M
00c0  61 63 20 4f 53 20 58 20  31 30 5f 31 31 5f 32 29   ac OS X  10_11_2)
00d0  20 41 70 70 6c 65 57 65  62 4b 69 74 2f 36 30 31    AppleWe bKit/601
```

HTTP Request-URI (http.request.uri), 1 byte | Packets: 34100 · Displayed: 213 (0.6%) | Profile: Default

We need the src ip, http.host and the request to homepage only

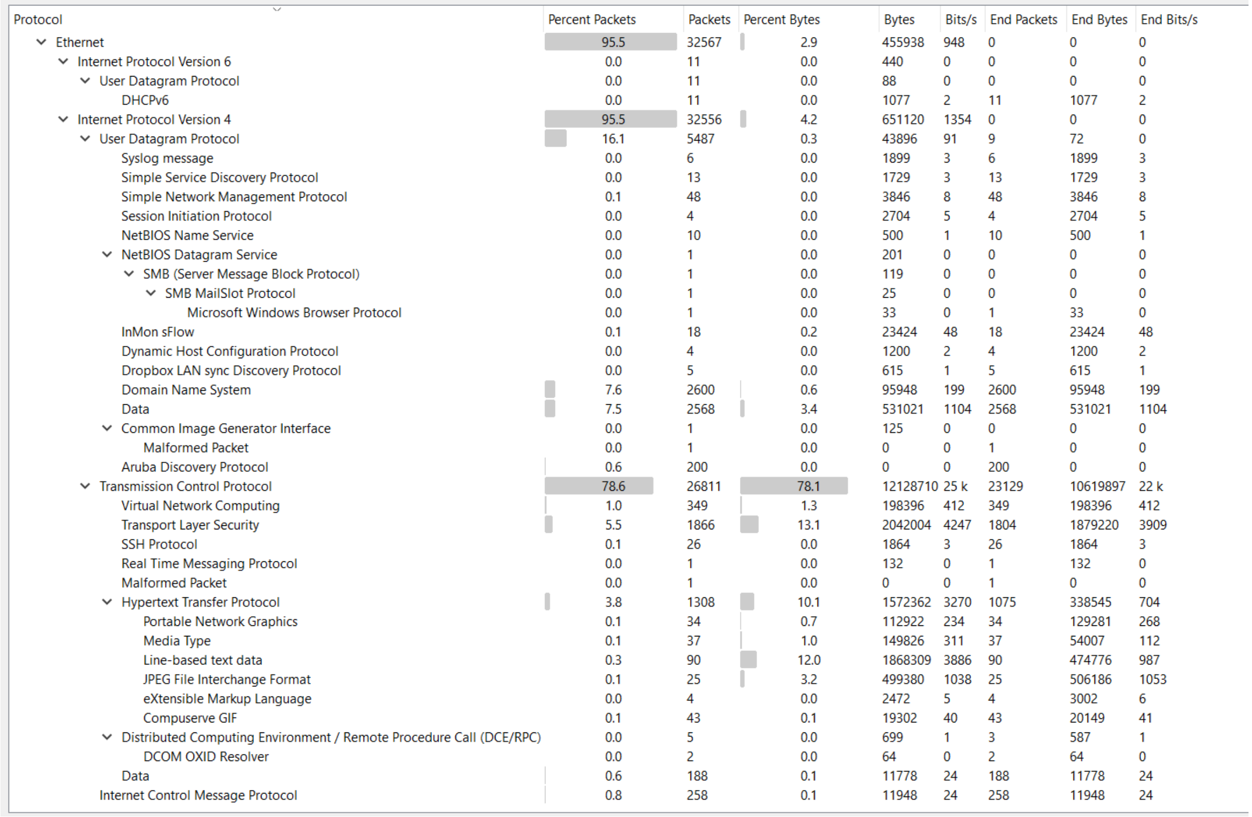
Flag: 213



Question

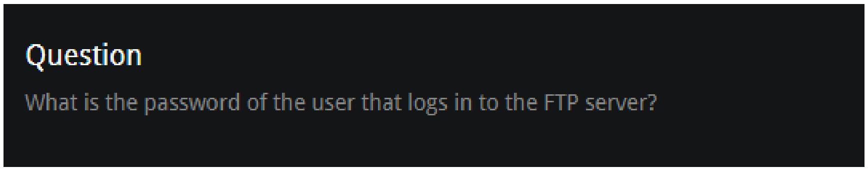
Let's look for more unencrypted traffic coming from `192.168.51.66`. This could be a great way to gain more information about the DPRK network.

Aside from HTTP and DNS, what other unencrypted protocol is found in the PCAP?



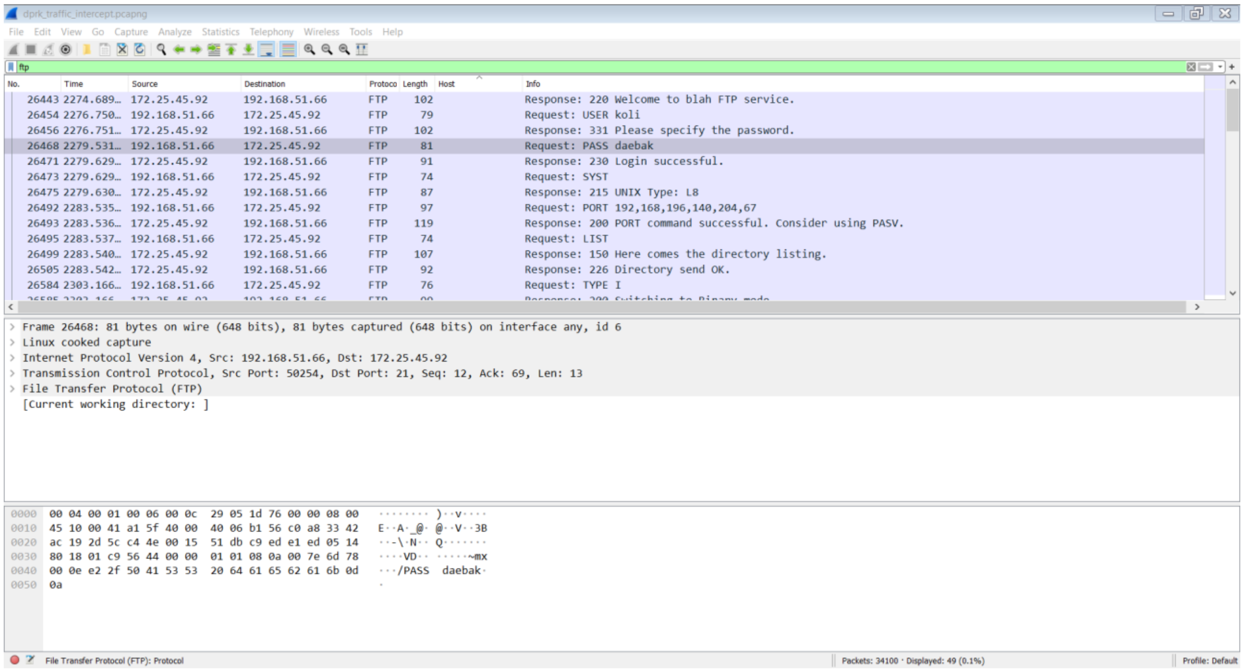
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Ethernet	95.5	32567	2.9	455938	948	0	0	0
Internet Protocol Version 6	0.0	11	0.0	440	0	0	0	0
User Datagram Protocol	0.0	11	0.0	88	0	0	0	0
DHCPv6	0.0	11	0.0	1077	2	11	1077	2
Internet Protocol Version 4	95.5	32556	4.2	651120	1354	0	0	0
User Datagram Protocol	16.1	5487	0.3	43896	91	9	72	0
Syslog message	0.0	6	0.0	1899	3	6	1899	3
Simple Service Discovery Protocol	0.0	13	0.0	1729	3	13	1729	3
Simple Network Management Protocol	0.1	48	0.0	3846	8	48	3846	8
Session Initiation Protocol	0.0	4	0.0	2704	5	4	2704	5
NetBIOS Name Service	0.0	10	0.0	500	1	10	500	1
NetBIOS Datagram Service	0.0	1	0.0	201	0	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	0	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	0	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	0	1	33	0
InMon sFlow	0.1	18	0.2	23424	48	18	23424	48
Dynamic Host Configuration Protocol	0.0	4	0.0	1200	2	4	1200	2
Dropbox LAN sync Discovery Protocol	0.0	5	0.0	615	1	5	615	1
Domain Name System	7.6	2600	0.6	95948	199	2600	95948	199
Data	7.5	2568	3.4	531021	1104	2568	531021	1104
Common Image Generator Interface	0.0	1	0.0	125	0	0	0	0
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Aruba Discovery Protocol	0.6	200	0.0	0	0	200	0	0
Transmission Control Protocol	78.6	26811	78.1	12128710	25 k	23129	10619897	22 k
Virtual Network Computing	1.0	349	1.3	198396	412	349	198396	412
Transport Layer Security	5.5	1866	13.1	2042004	4247	1804	1879220	3909
SSH Protocol	0.1	26	0.0	1864	3	26	1864	3
Real Time Messaging Protocol	0.0	1	0.0	132	0	1	132	0
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Hypertext Transfer Protocol	3.8	1308	10.1	1572362	3270	1075	338545	704
Portable Network Graphics	0.1	34	0.7	112922	234	34	129281	268
Media Type	0.1	37	1.0	149826	311	37	54007	112
Line-based text data	0.3	90	12.0	1868309	3886	90	474776	987
JPEG File Interchange Format	0.1	25	3.2	499380	1038	25	506186	1053
eXtensible Markup Language	0.0	4	0.0	2472	5	4	3002	6
Compuserve GIF	0.1	43	0.1	19302	40	43	20149	41
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.0	5	0.0	699	1	3	587	1
DCOM OXID Resolver	0.0	2	0.0	64	0	2	64	0
Data	0.6	188	0.1	11778	24	188	11778	24
Internet Control Message Protocol	0.8	258	0.1	11948	24	258	11948	24

Flag: ftp



Question

What is the password of the user that logs in to the FTP server?



dprk_traffic_intercept.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp

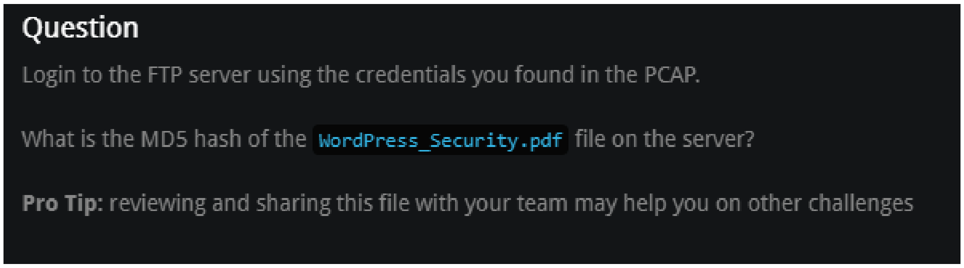
No.	Time	Source	Destination	Protoco	Length	Host	Info
26443	2274.689…	172.25.45.92	192.168.51.66	FTP	102		Response: 220 Welcome to blah FTP service.
26454	2276.750…	192.168.51.66	172.25.45.92	FTP	79		Request: USER koli
26456	2276.751…	172.25.45.92	192.168.51.66	FTP	102		Response: 331 Please specify the password.
26468	2279.531…	192.168.51.66	172.25.45.92	FTP	81		Request: PASS daebak
26471	2279.629…	172.25.45.92	192.168.51.66	FTP	91		Response: 230 Login successful.
26473	2279.629…	192.168.51.66	172.25.45.92	FTP	74		Request: SYST
26475	2279.630…	172.25.45.92	192.168.51.66	FTP	87		Response: 215 UNIX Type: L8
26492	2283.535…	192.168.51.66	172.25.45.92	FTP	97		Request: PORT 192,168,196,140,204,67
26493	2283.536…	172.25.45.92	192.168.51.66	FTP	119		Response: 200 PORT command successful. Consider using PASV.
26495	2283.537…	192.168.51.66	172.25.45.92	FTP	74		Request: LIST
26499	2283.540…	172.25.45.92	192.168.51.66	FTP	107		Response: 150 Here comes the directory listing.
26505	2283.542…	172.25.45.92	192.168.51.66	FTP	92		Response: 226 Directory send OK.
26584	2303.166…	192.168.51.66	172.25.45.92	FTP	76		Request: TYPE I
26585	2303.166…	172.25.45.92	192.168.51.66	FTP	90		Response: 200 Switching to Binary mode.

```
> Frame 26468: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface any, id 6
> Linux cooked capture
> Internet Protocol Version 4, Src: 192.168.51.66, Dst: 172.25.45.92
> Transmission Control Protocol, Src Port: 50254, Dst Port: 21, Seq: 12, Ack: 69, Len: 13
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 04 00 01 00 06 00 0c  29 05 1d 76 00 00 08 00   ········ )··v····
0010  45 10 00 41 a1 5f 40 00  40 06 b1 56 c0 a8 33 42   E··A·_@· @··V··3B
0020  ac 19 2d 5c c4 4e 00 15  51 db c9 ed e1 ed 05 14   ··-\·N·· Q·······
0030  80 18 01 c9 56 44 00 00  01 01 08 0a 00 7e 6d 78   ····VD·· ·····~mx
0040  00 0e e2 2f 50 41 53 53  20 64 61 65 62 61 6b 0d   ···/PASS  daebak·
0050  0a                                                 ·
```

File Transfer Protocol (FTP): Protocol
Packets: 34100 · Displayed: 49 (0.1%)
Profile: Default

Flag: daebak



Question

Login to the FTP server using the credentials you found in the PCAP.

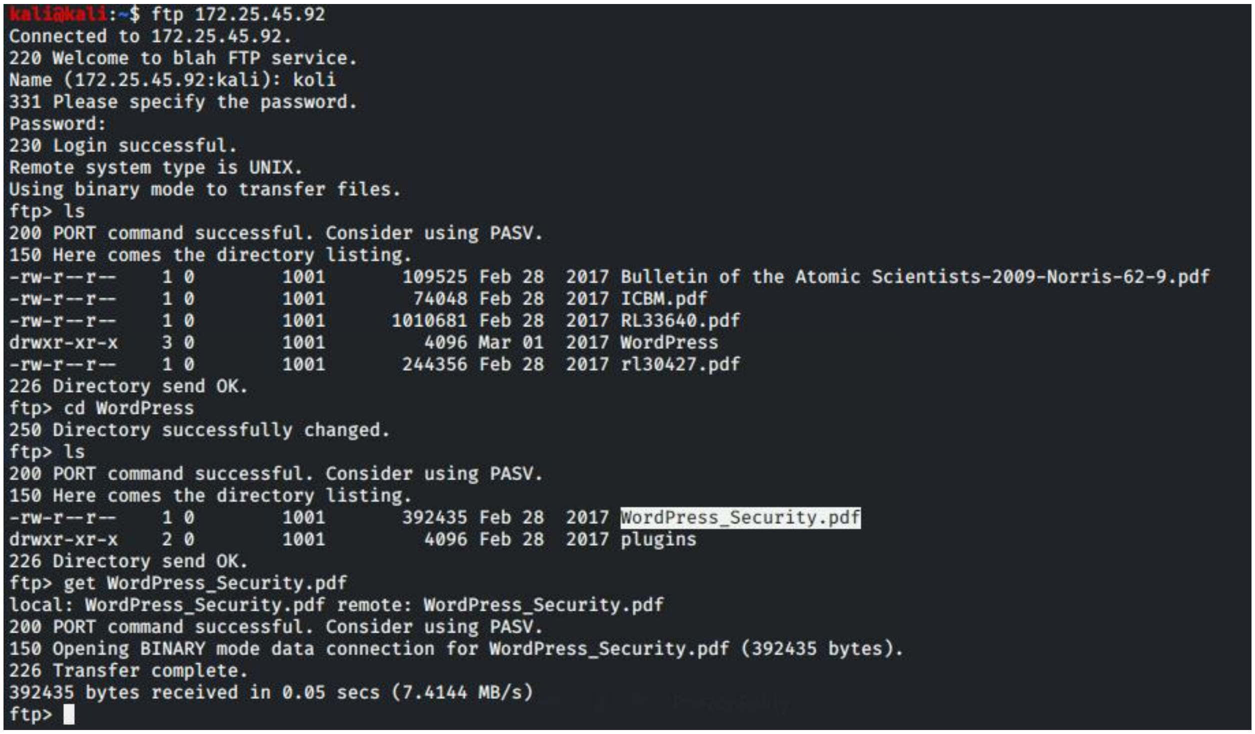
What is the MD5 hash of the `WordPress_Security.pdf` file on the server?

Pro Tip: reviewing and sharing this file with your team may help you on other challenges

Connect to the VPN

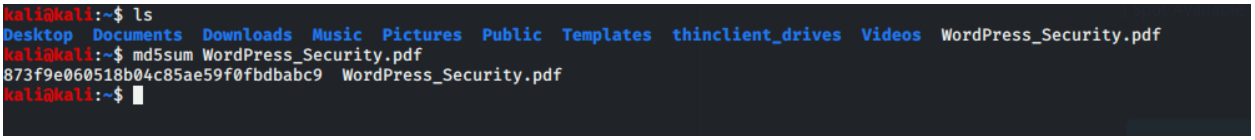
Connect to the FTP server

Download the file.



```
kali@kali:~$ ftp 172.25.45.92
Connected to 172.25.45.92.
220 Welcome to blah FTP service.
Name (172.25.45.92:kali): koli
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        1001       109525 Feb 28  2017 Bulletin of the Atomic Scientists-2009-Norris-62-9.pdf
-rw-r--r--    1 0        1001        74048 Feb 28  2017 ICBM.pdf
-rw-r--r--    1 0        1001      1010681 Feb 28  2017 RL33640.pdf
drwxr-xr-x    3 0        1001         4096 Mar 01  2017 WordPress
-rw-r--r--    1 0        1001       244356 Feb 28  2017 rl30427.pdf
226 Directory send OK.
ftp> cd WordPress
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        1001       392435 Feb 28  2017 WordPress_Security.pdf
drwxr-xr-x    2 0        1001         4096 Feb 28  2017 plugins
226 Directory send OK.
ftp> get WordPress_Security.pdf
local: WordPress_Security.pdf remote: WordPress_Security.pdf
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for WordPress_Security.pdf (392435 bytes).
226 Transfer complete.
392435 bytes received in 0.05 secs (7.4144 MB/s)
ftp> 
```

Md5sum the file



```
kali@kali:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  thinclient_drives  Videos  WordPress_Security.pdf
kali@kali:~$ md5sum WordPress_Security.pdf
873f9e060518b04c85ae59f0fbdbabc9  WordPress_Security.pdf
kali@kali:~$ 
```