

David Thomsen
SYS-255

Deliverable 1:

On wks02 as a domain user using powershell, provide screenshots similar to the one below that shows:

whoami (1 Point)

```
C:\Users\david.thomsen-adm>whoami
david\david.thomsen-adm
```

ipconfig /all (2 Points)

```
C:\Users\david.thomsen-adm>ipconfig /all

Windows IP Configuration

Host Name . . . . . : wks02-david
Primary Dns Suffix . . . . . : david.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : david.local
                                   home.arpa

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : david.local
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-50-56-B3-08-7F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f429:a0c7:a686:a289%10(Preferred)
    IPv4 Address. . . . . : 10.0.5.100(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Monday, October 4, 2021 12:31:49 PM
    Lease Expires . . . . . : Tuesday, October 5, 2021 12:31:49 AM
    Default Gateway . . . . . : fe80::250:56ff:feb3:41a6%10
                                   10.0.5.2
    DHCP Server . . . . . : 10.0.5.4
    DHCPv6 IAID . . . . . : 100683862
    DHCPv6 Client DUID. . . . . : 00-01-00-01-28-ED-1E-AA-00-50-56-B3-08-7F
    DNS Servers . . . . . : 10.0.5.6
    NetBIOS over Tcpip. . . . . : Enabled
    Connection-specific DNS Suffix Search List :
                                   home.arpa
```

tracert -h 3 champlain.edu (1 Point)

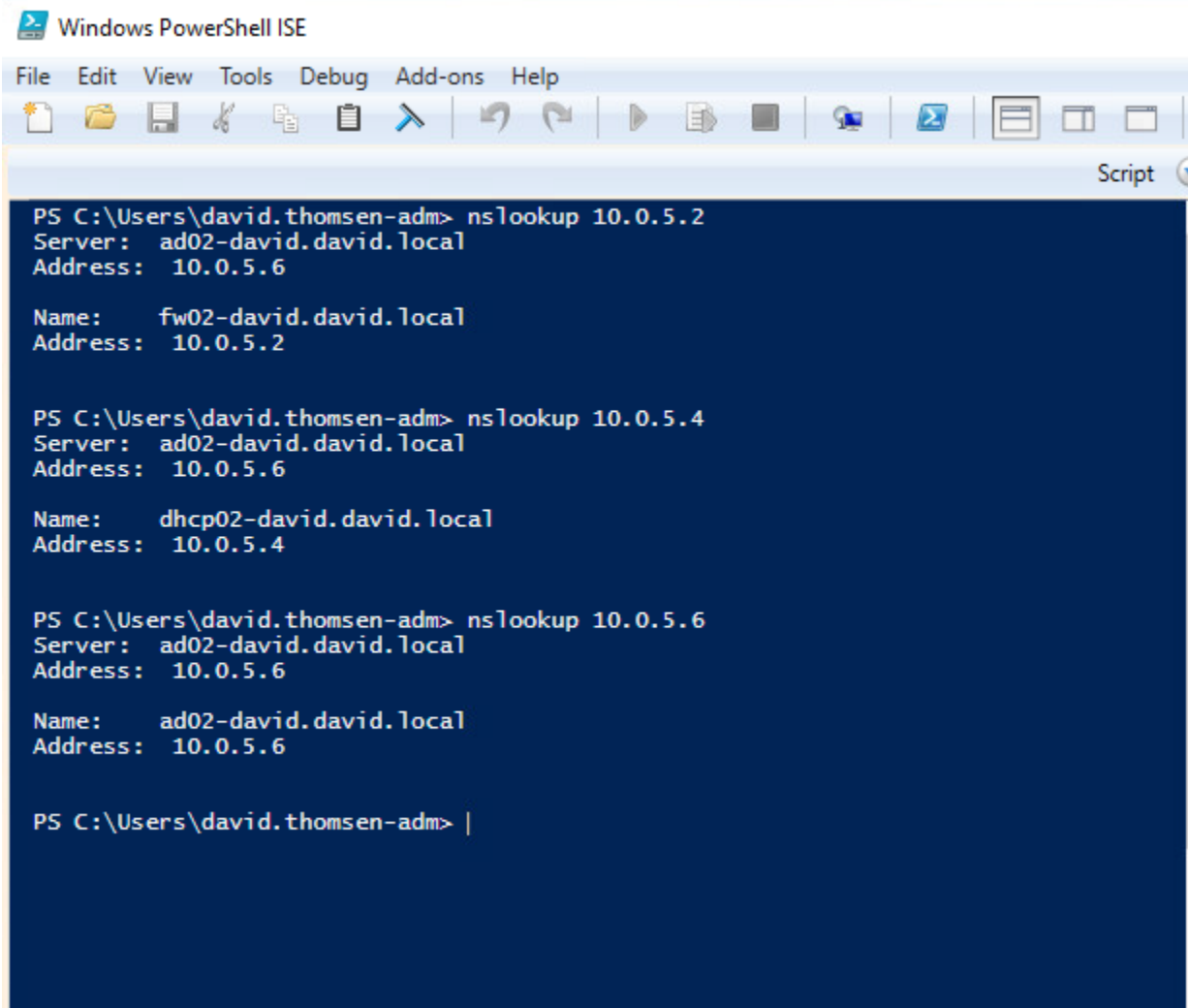
```
C:\Users\david.thomsen-adm>tracert -h 3 champlain.edu

Tracing route to champlain.edu [208.115.107.132]
over a maximum of 3 hops:

  1    <1 ms    <1 ms    <1 ms  fw02-david.david.local [10.0.5.2]
  2     1 ms    <1 ms    <1 ms  10.0.17.2
  3     2 ms     1 ms     1 ms  192.168.4.252

Trace complete.
```

Deliverable 2: Provide a screenshot that shows a nslookup/PTR lookup of the following IP addresses from WKS02 (4 points): 10.0.5.2, 10.0.5.4, 10.0.5.6. Looking for appropriately named A records. Server should not be "unknown".



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
[Icons]
Script

PS C:\Users\david.thomsen-adm> nslookup 10.0.5.2
Server:  ad02-david.david.local
Address: 10.0.5.6

Name:     fw02-david.david.local
Address:  10.0.5.2

PS C:\Users\david.thomsen-adm> nslookup 10.0.5.4
Server:  ad02-david.david.local
Address: 10.0.5.6

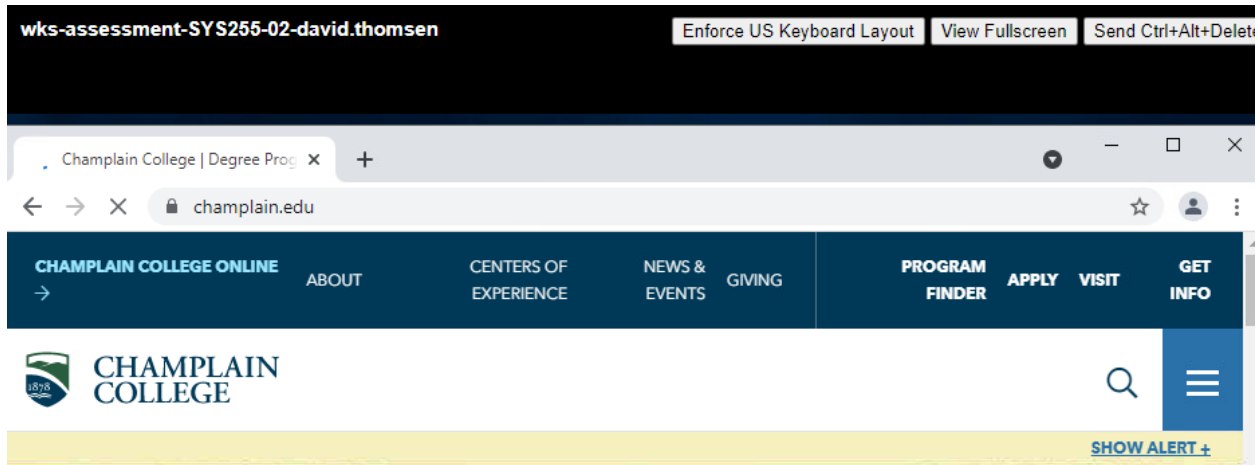
Name:     dhcp02-david.david.local
Address:  10.0.5.4

PS C:\Users\david.thomsen-adm> nslookup 10.0.5.6
Server:  ad02-david.david.local
Address: 10.0.5.6

Name:     ad02-david.david.local
Address:  10.0.5.6

PS C:\Users\david.thomsen-adm> |
```

Deliverable 3: Provide a screenshot showing a browsing session between wks02 and champlain.edu,& make sure to grab the wks02 banner for your screenshot.(2 Points)



Deliverable 4: On AD02, as the named domain admin, provide the output of the following commands:

Get-ADComputer

```
PS C:\Users\Administrator> Get-ADComputer -filter "*"

DistinguishedName : CN=AD02-DAVID,OU=Domain Controllers,DC=david,DC=local
DNSHostName       : ad02-david.david.local
Enabled           : True
Name              : AD02-DAVID
ObjectClass       : computer
ObjectGUID        : b4081993-c481-434f-b6f7-a1d50cb16a81
SamAccountName    : AD02-DAVID$
SID               : S-1-5-21-4270978361-3958365237-99608879-1000
UserPrincipalName :

DistinguishedName : CN=WKS02-DAVID,CN=Computers,DC=david,DC=local
DNSHostName       : wks02-david.david.local
Enabled           : True
Name              : WKS02-DAVID
ObjectClass       : computer
ObjectGUID        : c64982b2-f85c-4afc-8af6-338f54aa072d
SamAccountName    : WKS02-DAVID$
SID               : S-1-5-21-4270978361-3958365237-99608879-1105
UserPrincipalName :
```

Get-ADGroup -Identity "Domain Users" -Property member

Get-ADGroup -Identity "Domain Admins" -Property member

```
PS C:\Users\Administrator> Get-ADGroup -Identity "Domain Users" -Property member
```

```
DistinguishedName : CN=Domain Users,CN=Users,DC=david,DC=local
GroupCategory      : Security
GroupScope         : Global
Name               : Domain Users
ObjectClass        : group
ObjectGUID         : 54c10798-4b6d-48be-a303-2b0a574a10e4
SamAccountName     : Domain Users
SID                : S-1-5-21-4270978361-3958365237-99608879-513
```

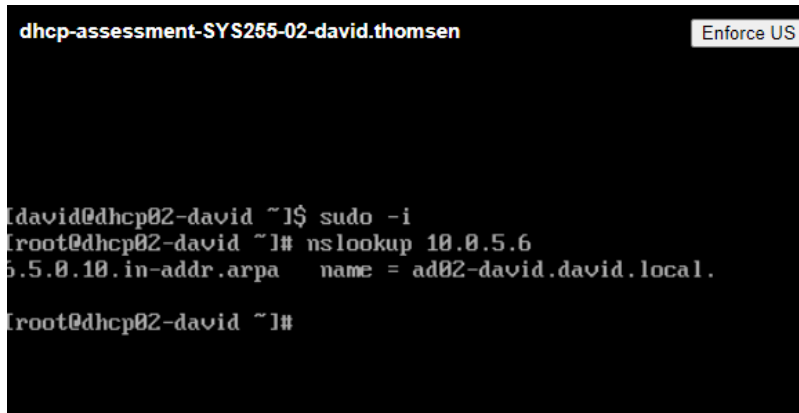
```
PS C:\Users\Administrator> Get-ADGroup -Identity "Domain Admins" -Property member
```

```
DistinguishedName : CN=Domain Admins,CN=Users,DC=david,DC=local
GroupCategory      : Security
GroupScope         : Global
member             : {CN=david thomsen-adm,CN=Users,DC=david,DC=local, CN=Administrator,CN=Users,DC=david,DC=local}
Name               : Domain Admins
ObjectClass        : group
ObjectGUID         : 6ef5cf18-7546-4ab7-91e3-2d40b1e02195
SamAccountName     : Domain Admins
SID                : S-1-5-21-4270978361-3958365237-99608879-512
```

Deliverable 5: On DHCP02, provide a screenshot (with vSphere dhcp02 banner) showing the following:

login as a named user and sudo -i to root (2 points)

nslookup 10.0.5.6 (1 point)

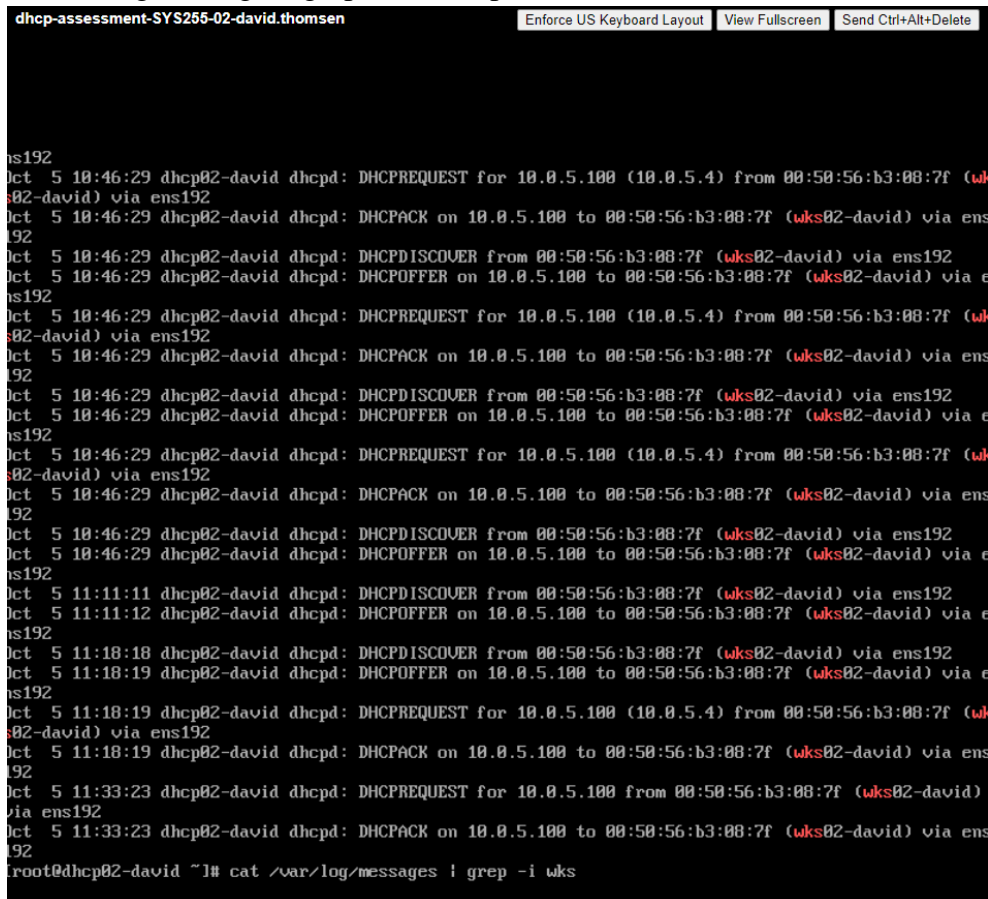


```
dhcp-assessment-SYS255-02-david.thomsen Enforce US Keyboard Layout

[david@dhcp02-david ~]$ sudo -i
[root@dhcp02-david ~]# nslookup 10.0.5.6
5.5.0.10.in-addr.arpa    name = ad02-david.david.local.

[root@dhcp02-david ~]#
```

cat /var/log/messages | grep -i wks (2 points)

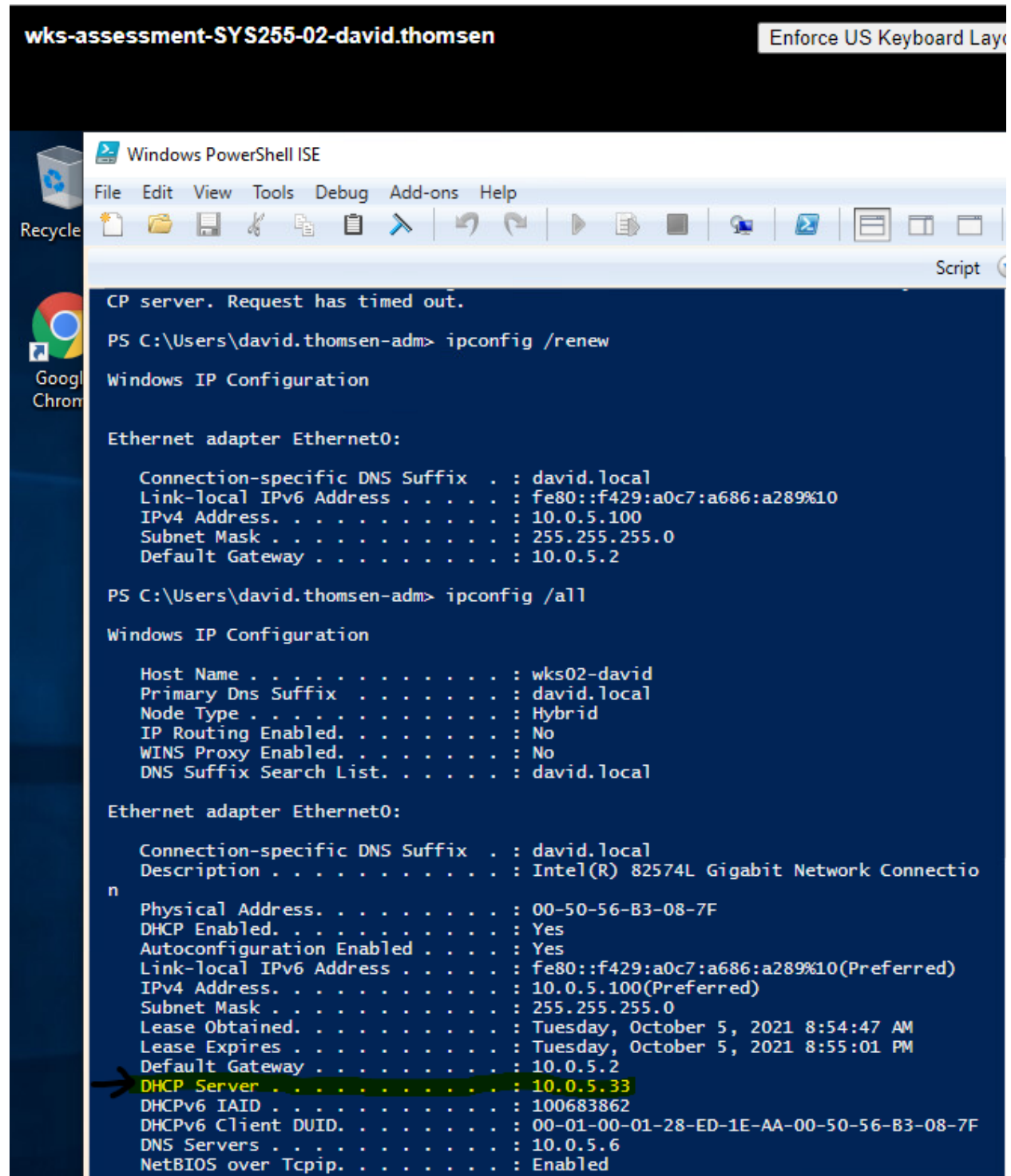


```
dhcp-assessment-SYS255-02-david.thomsen Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

ns192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPREQUEST for 10.0.5.100 (10.0.5.4) from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPACK on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPDISCOVER from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPOFFER on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPREQUEST for 10.0.5.100 (10.0.5.4) from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPACK on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPDISCOVER from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPOFFER on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPREQUEST for 10.0.5.100 (10.0.5.4) from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPACK on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPDISCOVER from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 10:46:29 dhcp02-david dhcpd: DHCPOFFER on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:11:11 dhcp02-david dhcpd: DHCPDISCOVER from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:11:12 dhcp02-david dhcpd: DHCPOFFER on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:18:18 dhcp02-david dhcpd: DHCPDISCOVER from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:18:19 dhcp02-david dhcpd: DHCPOFFER on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:18:19 dhcp02-david dhcpd: DHCPREQUEST for 10.0.5.100 (10.0.5.4) from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:18:19 dhcp02-david dhcpd: DHCPACK on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:33:23 dhcp02-david dhcpd: DHCPREQUEST for 10.0.5.100 from 00:50:56:b3:08:7f (wks02-david) via ens192
Oct 5 11:33:23 dhcp02-david dhcpd: DHCPACK on 10.0.5.100 to 00:50:56:b3:08:7f (wks02-david) via ens192
[root@dhcp02-david ~]# cat /var/log/messages | grep -i wks
```

Deliverable 6: Re-configure DHCP02 to have the IP address of: 10.0.5.33. Make sure you update the A and PTR records for DHCP02 IP in DNS. On WKS02, release and renew your ip address
ipconfig /release || ipconfig /renew

Provide a screenshot that shows ipconfig /all



The screenshot shows a Windows PowerShell ISE window with the following content:

```
wks-assessment-SYS255-02-david.thomsen Enforce US Keyboard Layo
```

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Recycle

Google Chrome

Script

```
CP server. Request has timed out.
PS C:\Users\david.thomsen-adm> ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : david.local
    Link-local IPv6 Address . . . . . : fe80::f429:a0c7:a686:a289%10
    IPv4 Address. . . . . : 10.0.5.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.5.2

PS C:\Users\david.thomsen-adm> ipconfig /all

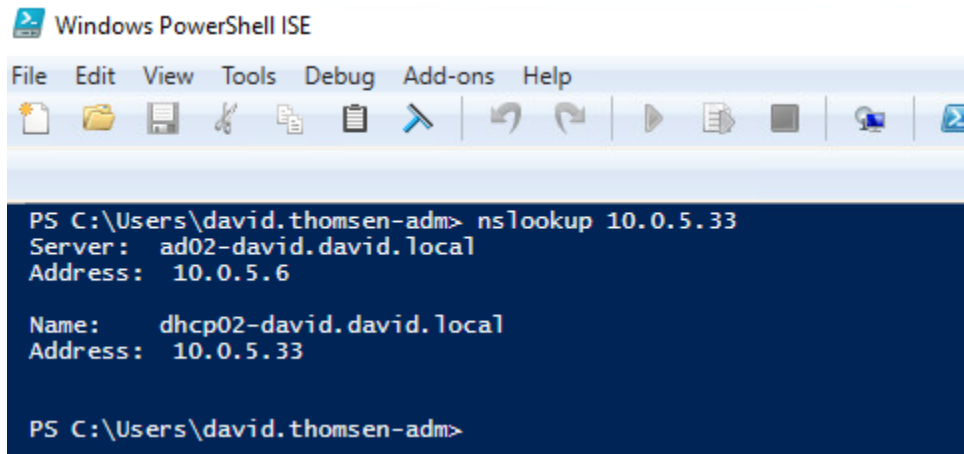
Windows IP Configuration

    Host Name . . . . . : wks02-david
    Primary Dns Suffix . . . . . : david.local
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : david.local

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : david.local
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-50-56-B3-08-7F
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f429:a0c7:a686:a289%10(Preferred)
    IPv4 Address. . . . . : 10.0.5.100(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Tuesday, October 5, 2021 8:54:47 AM
    Lease Expires . . . . . : Tuesday, October 5, 2021 8:55:01 PM
    Default Gateway . . . . . : 10.0.5.2
    DHCP Server . . . . . : 10.0.5.33
    DHCPv6 IAID . . . . . : 100683862
    DHCPv6 Client DUID. . . . . : 00-01-00-01-28-ED-1E-AA-00-50-56-B3-08-7F
    DNS Servers . . . . . : 10.0.5.6
    NetBIOS over Tcpip. . . . . : Enabled
```

Deliverable 7: On WKS02, run an nslookup 10.0.5.33. Looking for indications that you adjusted the PTR and A records for dhcp02.



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\Users\david.thomsen-adm> nslookup 10.0.5.33
Server: ad02-david.david.local
Address: 10.0.5.6

Name: dhcp02-david.david.local
Address: 10.0.5.33

PS C:\Users\david.thomsen-adm>
```