



INFORME DE CAMUFLAJE (CAMOU121) Y HACKING A BADBLUE

INTEGRANTE

Juan Carlos Palacios Valencia

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDO-CHOCÓ

08/10/2025



INFORME DE CAMUFLAJE (CAMOU121) Y HACKING A BADBLUE

INTEGRANTE

Juan Carlos Palacios Valencia

DOCENTE

Rafael Sandoval

ASIGNATURA

SEGURIDAD Y AUDITORIA

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDO-CHOCÓ

08/10/2025



1. Tabla de contenido

2.	Tabla de imágenes	4
3.	Introducción	6
4.	Objetivo general del Capítulo 1	6
5.	Objetivo general del Capítulo 2	7
6.	Resumen.....	7
7.	CAPITULO 1	8
7.2.	Selección de archivo portador	9
7.3.	Configuración de destino del archivo camuflado en Camouflage.....	10
7.4.	Asignación de contraseña de seguridad en Camouflage	10
7.5.	Límite de archivos que pueden camuflarse en un solo archivo	11
8.	Capítulo 2.....	14
8.1.	Hacking en badblue	14
8.2.	Identificación de servicios y versiones (Nmap)	14
8.3.	Verificación de red.....	15
8.4.	Identificación de servicios activos en equipo con Windows XP	15
8.5.	Verificación del servicio web mediante comando URL	16
8.6.	Buscando exploits para BadBlue 2.7 con SearchSploit.....	17
8.7.	Detalles del exploit para BadBlue 2.72	17
8.8.	Visualización del script exploit y referencias técnicas	18



9. Conclusión	18
---------------------	----

2. Tabla de imágenes

Ilustración 1 Opción de camuflaje de archivos en el menú contextual de Windows.....	8
Ilustración 2 Archivos listos para camuflar	8
Ilustración 3 Selección del archivo portador para el camuflaje	9
Ilustración 4 Archivo portador confirmado.....	9
Ilustración 5 Ruta del archivo camuflado	10
Ilustración 6 Implementar seguridad	10
Ilustración 7 archivo JPEG modificado	11
Ilustración 8 visor de imagen.....	11
Ilustración 9 imagen que vamos a dañar.....	11
Ilustración 10 Archivos para camuflar	12
Ilustración 11 Archivo portador	12
Ilustración 12 Ruta de archivo portador.....	12
Ilustración 13 asignación de contraseña	13
Ilustración 14 imagen portadora	13
Ilustración 15 imagen rota	13
Ilustración 16 interfaz de badblue.....	14
Ilustración 17 Resultado: nmap -sV contra la subred 192.192.0.0/24	14
Ilustración 18 Configuración de red del host objetivo.....	15
Ilustración 19 Resultados del escaneo Nmap del host 192.192.0.8.....	15



Ilustración 20 interfaz de badblue.....	16
Ilustración 21 Confirmación del servidor BadBlue mediante URL.....	16
Ilustración 22 Resultados de búsqueda de exploits para BadBlue 2.7.....	17
Ilustración 23 Exploit-DB (ID 4784).....	17
Ilustración 24 Preparación e inspección del exploit BadBlue 2.7	18



3. Introducción

Capítulo 1 en este se explica cómo utilizar la herramienta Camou121 para camuflar archivos dentro de otro archivo, como una imagen. Se detallan los pasos necesarios: selección de archivos, elección del archivo portador, configuración del destino y asignación de contraseña. Además, se analiza el límite de datos que puede ocultarse sin dañar el archivo portador, mostrando qué ocurre cuando se excede su capacidad. Todo el proceso se acompaña con ilustraciones para facilitar su comprensión.

En el capítulo 2 se describe el proceso práctico de reconocimiento y explotación sobre un servidor BadBlue 2.7 en un entorno de laboratorio. Se abordan la inspección de la interfaz web, la identificación de servicios y versiones mediante Nmap, la verificación de la configuración de red del objetivo y la comprobación del servicio web con curl. Finalmente, se muestran la búsqueda de exploits con SearchSploit y la preparación e inspección del exploit identificado para BadBlue, proporcionando las evidencias y comandos utilizados en cada paso.

4. Objetivo general del Capítulo 1

Describir y demostrar el proceso completo de camuflaje de archivos utilizando la herramienta Camouflage (Camou121), incluyendo la selección de archivos y archivo portador, configuración de destino, protección por contraseña y análisis del límite de datos admitido para evitar la corrupción del archivo portador.



5. Objetivo general del Capítulo 2

Realizar el reconocimiento y la evaluación de vulnerabilidades de un servidor BadBlue 2.7 en un entorno de laboratorio, mediante identificación de servicios y versiones (Nmap), verificación de conectividad y servicio web (ipconfig, curl), búsqueda de exploits con SearchSploit y preparación/inspección del exploit seleccionado.

6. Resumen

El presente informe abarca dos prácticas, en el Capítulo 1, se usó la herramienta Camou121 para el camuflaje de archivos dentro de una imagen, detallando el proceso de selección, configuración del archivo portador, asignación de contraseña y análisis del límite de capacidad que puede soportar sin dañarse.

En el Capítulo 2, se realiza un ejercicio de análisis de seguridad en un servidor BadBlue 2.7, utilizando herramientas como Nmap, ipconfig, curl y SearchSploit. Se identificaron servicios activos, versiones del sistema y vulnerabilidades asociadas, incluyendo un exploit por desbordamiento de búfer. Ambas prácticas permiten comprender técnicas tanto de ocultamiento de información como de detección de vulnerabilidades.

7. CAPITULO 1

7.1. Camuflaje de archivos en camou121

Para realizar el camuflaje de archivos, primero se deben seleccionar los archivos uno a uno y, posteriormente, hacer clic derecho sobre ellos para que aparezca la opción **Camouflage** y le damos clic a esta opción.



Ilustración 1 Opción de camuflaje de archivos en el menú contextual de Windows

Luego de ingresar nos mostrara una vista previa de los archivos seleccionados, para continuar le damos en el botón **Next**.

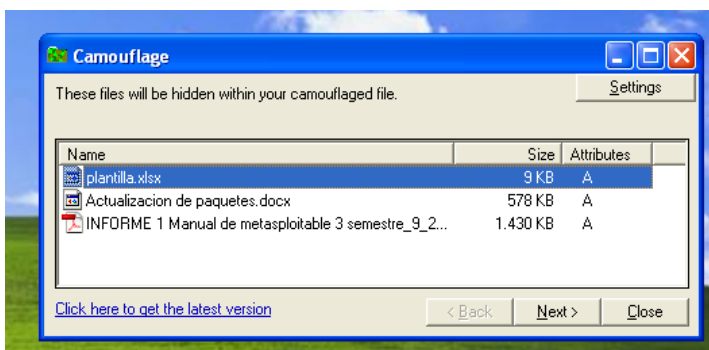


Ilustración 2 Archivos listos para camuflar

7.2. Selección de archivo portador

Para seleccionar el archivo portador, es necesario explorar el equipo y localizar el archivo en el cual se van a camuflar los demás archivos. En este caso seleccionamos una imagen JPEG de 7,85 kb después de seleccionarla le damos al botón abrir.

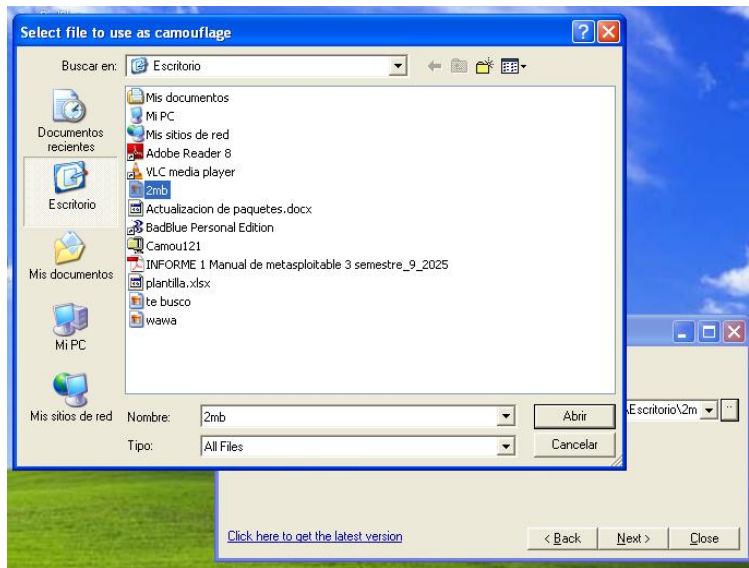


Ilustración 3 Selección del archivo portador para el camuflaje

Aquí ya nos aparece la ruta del archivo seleccionado y para continuar con el siguiente paso le vamos a dar al botón Next.

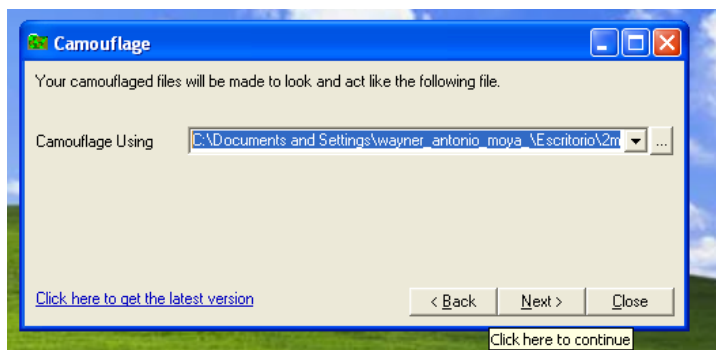


Ilustración 4 Archivo portador confirmado

7.3. Configuración de destino del archivo camuflado en Camouflage

En este paso vamos a modificar la ruta del archivo portador agregándole o quitándole letras, luego de eso le damos Netx.

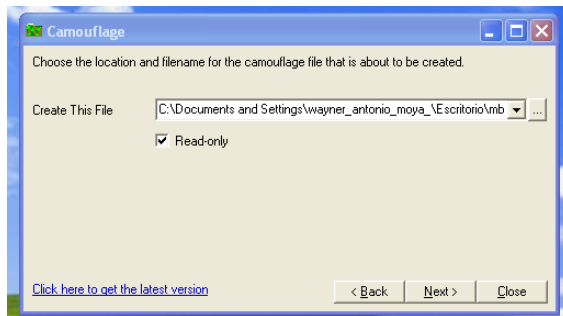


Ilustración 5 Ruta del archivo camuflado

7.4. Asignación de contraseña de seguridad en Camouflage

En este paso vamos a asignarle una contraseña a el archivo portador para proteger nuestros archivos camuflados. Luego de haber ingresado nuestra contraseña le vamos a dar en el botón finish.

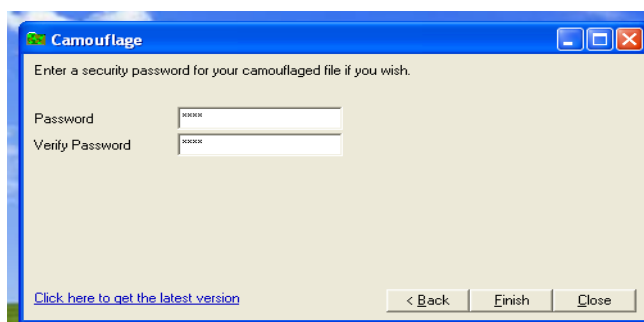


Ilustración 6 Implementar seguridad

Al haber terminado este proceso nos va a quedar una imagen NPEG de mayor tamaño. Al principio nuestra imagen pesaba 7,85 KB ahora pesa 12,5 MB. Esto es debido a los archivos que guardamos dentro de ella.

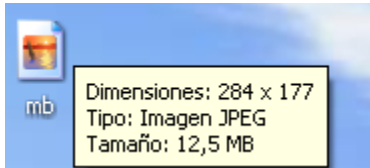


Ilustración 7 archivo JPEG modificado



Ilustración 8 visor de imagen

7.5. Límite de archivos que pueden camuflarse en un solo archivo

No hay un número exacto de archivos, porque el límite depende del tamaño total de los archivos camuflados, no de cuántos archivos sean

Ejemplo: aquí tenemos una imagen NPEG que su tamaño es de 7,85 kb



Ilustración 9 imagen que vamos a dañar

Entonces Camou puede esconder entre un **10 % y 30 %** del tamaño original de la imagen sin corromperla. Es decir que esta imagen puede camuflar entre 0,7 kb y 2,3 kb de forma segura.

Ahora vamos a pasar el límite de datos que soporta la imagen para mirar que pasa. Iniciamos seleccionando los archivos para camuflar.

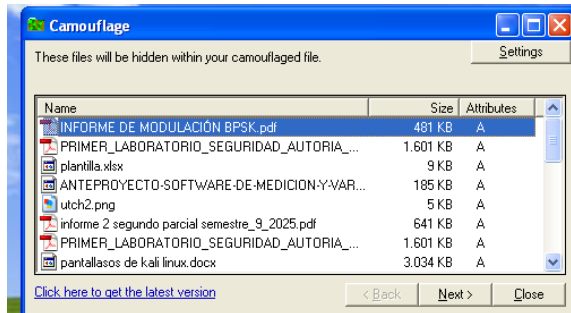


Ilustración 10 Archivos para camuflar

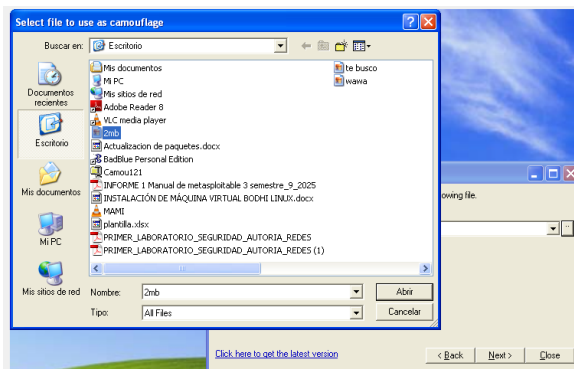


Ilustración 11 Archivo portador

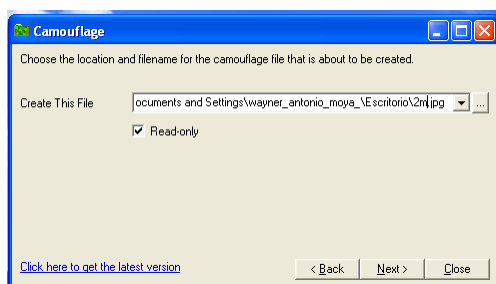


Ilustración 12 Ruta de archivo portador

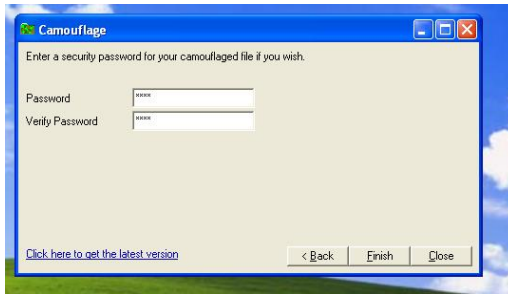


Ilustración 13 asignación de contraseña

Aquí nos arrojo este archivo NPEG con un tamaño de 1,46 GB que al abrirlo podemos ver que está roto debido a la cantidad de datos que se camuflaron dentro de él.



Ilustración 14 imagen portadora

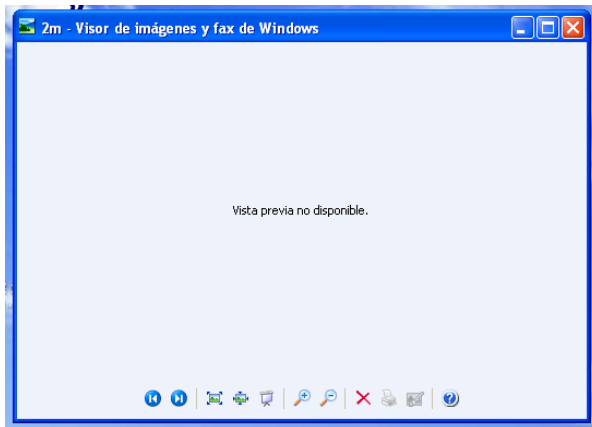


Ilustración 15 imagen rota

8. Capítulo 2

8.1. Hacking en badblue

Ingresamos a la interfaz principal de **BadBlue**, una aplicación de servidor web orientada al compartir archivos en red local o a través de Internet. La interfaz presenta varias pestañas principales las cuales son: search, folders, manage y help.



Ilustración 16 interfaz de badblue

8.2. Identificación de servicios y versiones (Nmap)

Luego pasamos al sistema operativo Kali Linux y ejecutamos al comando **nmap** desde una terminal con privilegios de super usuario, se utilizó la opción **-sV** para hacer un barrido que averigüe qué versiones de servicios están corriendo en la red 192.192.0.0/24.

```
File Actions Edit View Help
(root@kali)-[~]
# nmap -sV 192.192.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-08 20:18 EDT
Nmap scan report for 192.192.0.1
```

Ilustración 17 Resultado: nmap -sV contra la subred 192.192.0.0/24



8.3. Verificación de red

Ahora pasamos a Windows xp y entramos a símbolos del sistema y ejecutamos el comando **ipconfig** para que nos arroje detalladamente la configuración de red del equipo y incluye los siguientes datos: Dirección IP **192.192.0.8**, Mascara de subred **255.255.255.0** y puerta de enlace predeterminada **192.192.0.1**

```
Sufijo de conexión específica DNS :  
Dirección IP. . . . . : 192.192.0.8  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada : 192.192.0.1
```

Ilustración 18 Configuración de red del host objetivo

8.4. Identificación de servicios activos en equipo con Windows XP

En este paso ejecutamos el comando **nmap** y nos muestra que el host 192.192.0.8 esta activo y utiliza el sistema operativo Windows xp y se identificaron 5 puertos **TCP** abierto lo que indica los servicios abiertos en el equipo.

```
Nmap scan report for 192.192.0.8  
Host is up (0.0021s latency).  
Not shown: 995 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         BadBlue httpd 2.7  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds  
3389/tcp  open  ms-wbt-server Microsoft Terminal Services  
MAC Address: 08:00:27:2E:C9:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

Ilustración 19 Resultados del escaneo Nmap del host 192.192.0.8

Aquí ingresamos a la interfaz de badblue mediante la dirección y pe del equipo victima

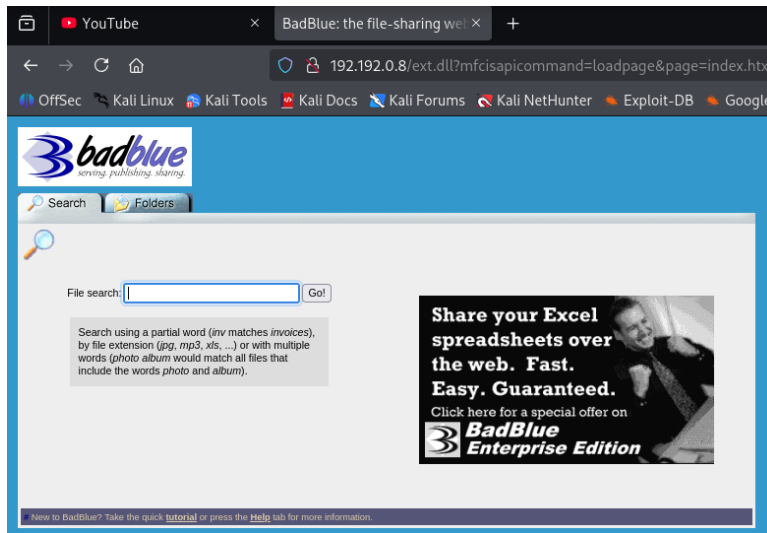


Ilustración 20 interfaz de badblue

8.5. Verificación del servicio web mediante comando URL

El análisis realizado con el comando `curl -I http://192.192.0.8:80/` muestra que el servidor web responde correctamente con el código **HTTP/1.1 200 OK**, indicando que el servicio está activo. Se identifica el servidor **BadBlue versión 2.7**, el cual utiliza el tipo de contenido **text/html** y presenta una última modificación registrada en **agosto de 2003**.

```
(root@kali)-[~]
# curl -I http://192.192.0.8:80/
HTTP/1.1 200 OK
Server: BadBlue/2.7
Content-Type: text/html
Accept-Ranges: bytes
Date: Thu, 09 Oct 2025 01:22:01 GMT
ETag: "3f45655a8f87dbe1:43d"
Last-Modified: Fri, 22 Aug 2003 00:35:38 GMT
Content-Length: 1085
Connection: close
Cache-control: public
```

Ilustración 21 Confirmación del servidor BadBlue mediante URL



8.6. Buscando exploits para BadBlue 2.7 con SearchSploit

En este paso utilizamos el comando **searchsploit badblue 2.7** para buscar vulnerabilidad conocida o asociadas al servidor **badblue versión 2.7** y los resultados nos muestran varias vulnerabilidades entre ellas **remote buffer overflow, Full Path Disclosure y Denial of Service**

```
(kali@kali)-[~]
$ searchsploit badblue 2.7
```

Exploit Title	Path
BadBlue 2.72 - PassThru Remote Buffer Overflow	windows/remote/4784.pl
BadBlue 2.72b - Multiple Vulnerabilities	windows/remote/4715.txt
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)	windows/remote/16806.rb
Working Resources BadBlue 1.2.7 - Denial of Service	windows/dos/20641.txt
Working Resources BadBlue 1.2.7 - Full Path Disclosure	windows/remote/20640.txt

```
Shellcodes: No Results
```

Ilustración 22 Resultados de búsqueda de exploits para BadBlue 2.7

8.7. Detalles del exploit para BadBlue 2.72

El comando **searchsploit -p windows/remote/4784.pl** muestra información detallada sobre un exploit específico para **BadBlue versión 2.72**, relacionado con una vulnerabilidad de **desbordamiento de búfer remoto (PassThru Remote Buffer Overflow)**

```
(kali@kali)-[~]
$ searchsploit -p windows/remote/4784.pl
```

```
Exploit: BadBlue 2.72 - PassThru Remote Buffer Overflow
URL: https://www.exploit-db.com/exploits/4784
Path: /usr/share/exploitdb/exploits/windows/remote/4784.pl
Codes: OSVDB-42416, CVE-2007-6377
Verified: True
File Type: Perl script text executable
Copied EDB-ID #4784's path to the clipboard
```

Ilustración 23 Exploit-DB (ID 4784)

8.8. Visualización del script exploit y referencias técnicas

Se copió el exploit identificado (/usr/share/exploitdb/exploits/windows/remote/4784.pl) al directorio de trabajo y se inspeccionó su contenido (comandos cp, ls, nano/cat).

```
(kali@kali)-[~]
└─$ cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .

(kali@kali)-[~]
└─$ ls
10.0.2.15  10.0.2.5  Desktop  Downloads  kpiHhRzC.jpeg  Music  RcSZmGvL.html  torentino3
10.0.2.3   4784.pl  Diclampoo.txt  DYGeLWAw.jpeg  MpGTwDeF.jpeg  Pictures  sr_j  Videos
10.0.2.4   clase    Documents     eYQqFStL.html  mqBaPjrY.jpeg  Public    Templates  ZoTHGWic.html

(kali@kali)-[~]
└─$ nano 4784.pl
# Exploit for Microsoft Windows XP/SP2/SP3/SP3a/SP3b/SP3c/SP3d/SP3e/SP3f/SP3g/SP3h/SP3i/SP3j/SP3k/SP3l/SP3m/SP3n/SP3o/SP3p/SP3q/SP3r/SP3s/SP3t/SP3u/SP3v/SP3w/SP3x/SP3y/SP3z/SP4/SP4a/SP4b/SP4c/SP4d/SP4e/SP4f/SP4g/SP4h/SP4i/SP4j/SP4k/SP4l/SP4m/SP4n/SP4o/SP4p/SP4q/SP4r/SP4s/SP4t/SP4u/SP4v/SP4w/SP4x/SP4y/SP4z/SP5/SP5a/SP5b/SP5c/SP5d/SP5e/SP5f/SP5g/SP5h/SP5i/SP5j/SP5k/SP5l/SP5m/SP5n/SP5o/SP5p/SP5q/SP5r/SP5s/SP5t/SP5u/SP5v/SP5w/SP5x/SP5y/SP5z/SP6/SP6a/SP6b/SP6c/SP6d/SP6e/SP6f/SP6g/SP6h/SP6i/SP6j/SP6k/SP6l/SP6m/SP6n/SP6o/SP6p/SP6q/SP6r/SP6s/SP6t/SP6u/SP6v/SP6w/SP6x/SP6y/SP6z/SP7/SP7a/SP7b/SP7c/SP7d/SP7e/SP7f/SP7g/SP7h/SP7i/SP7j/SP7k/SP7l/SP7m/SP7n/SP7o/SP7p/SP7q/SP7r/SP7s/SP7t/SP7u/SP7v/SP7w/SP7x/SP7y/SP7z/SP8/SP8a/SP8b/SP8c/SP8d/SP8e/SP8f/SP8g/SP8h/SP8i/SP8j/SP8k/SP8l/SP8m/SP8n/SP8o/SP8p/SP8q/SP8r/SP8s/SP8t/SP8u/SP8v/SP8w/SP8x/SP8y/SP8z/SP9/SP9a/SP9b/SP9c/SP9d/SP9e/SP9f/SP9g/SP9h/SP9i/SP9j/SP9k/SP9l/SP9m/SP9n/SP9o/SP9p/SP9q/SP9r/SP9s/SP9t/SP9u/SP9v/SP9w/SP9x/SP9y/SP9z/SP10/SP10a/SP10b/SP10c/SP10d/SP10e/SP10f/SP10g/SP10h/SP10i/SP10j/SP10k/SP10l/SP10m/SP10n/SP10o/SP10p/SP10q/SP10r/SP10s/SP10t/SP10u/SP10v/SP10w/SP10x/SP10y/SP10z/SP11/SP11a/SP11b/SP11c/SP11d/SP11e/SP11f/SP11g/SP11h/SP11i/SP11j/SP11k/SP11l/SP11m/SP11n/SP11o/SP11p/SP11q/SP11r/SP11s/SP11t/SP11u/SP11v/SP11w/SP11x/SP11y/SP11z/SP12/SP12a/SP12b/SP12c/SP12d/SP12e/SP12f/SP12g/SP12h/SP12i/SP12j/SP12k/SP12l/SP12m/SP12n/SP12o/SP12p/SP12q/SP12r/SP12s/SP12t/SP12u/SP12v/SP12w/SP12x/SP12y/SP12z/SP13/SP13a/SP13b/SP13c/SP13d/SP13e/SP13f/SP13g/SP13h/SP13i/SP13j/SP13k/SP13l/SP13m/SP13n/SP13o/SP13p/SP13q/SP13r/SP13s/SP13t/SP13u/SP13v/SP13w/SP13x/SP13y/SP13z/SP14/SP14a/SP14b/SP14c/SP14d/SP14e/SP14f/SP14g/SP14h/SP14i/SP14j/SP14k/SP14l/SP14m/SP14n/SP14o/SP14p/SP14q/SP14r/SP14s/SP14t/SP14u/SP14v/SP14w/SP14x/SP14y/SP14z/SP15/SP15a/SP15b/SP15c/SP15d/SP15e/SP15f/SP15g/SP15h/SP15i/SP15j/SP15k/SP15l/SP15m/SP15n/SP15o/SP15p/SP15q/SP15r/SP15s/SP15t/SP15u/SP15v/SP15w/SP15x/SP15y/SP15z/SP16/SP16a/SP16b/SP16c/SP16d/SP16e/SP16f/SP16g/SP16h/SP16i/SP16j/SP16k/SP16l/SP16m/SP16n/SP16o/SP16p/SP16q/SP16r/SP16s/SP16t/SP16u/SP16v/SP16w/SP16x/SP16y/SP16z/SP17/SP17a/SP17b/SP17c/SP17d/SP17e/SP17f/SP17g/SP17h/SP17i/SP17j/SP17k/SP17l/SP17m/SP17n/SP17o/SP17p/SP17q/SP17r/SP17s/SP17t/SP17u/SP17v/SP17w/SP17x/SP17y/SP17z/SP18/SP18a/SP18b/SP18c/SP18d/SP18e/SP18f/SP18g/SP18h/SP18i/SP18j/SP18k/SP18l/SP18m/SP18n/SP18o/SP18p/SP18q/SP18r/SP18s/SP18t/SP18u/SP18v/SP18w/SP18x/SP18y/SP18z/SP19/SP19a/SP19b/SP19c/SP19d/SP19e/SP19f/SP19g/SP19h/SP19i/SP19j/SP19k/SP19l/SP19m/SP19n/SP19o/SP19p/SP19q/SP19r/SP19s/SP19t/SP19u/SP19v/SP19w/SP19x/SP19y/SP19z/SP20/SP20a/SP20b/SP20c/SP20d/SP20e/SP20f/SP20g/SP20h/SP20i/SP20j/SP20k/SP20l/SP20m/SP20n/SP20o/SP20p/SP20q/SP20r/SP20s/SP20t/SP20u/SP20v/SP20w/SP20x/SP20y/SP20z/SP21/SP21a/SP21b/SP21c/SP21d/SP21e/SP21f/SP21g/SP21h/SP21i/SP21j/SP21k/SP21l/SP21m/SP21n/SP21o/SP21p/SP21q/SP21r/SP21s/SP21t/SP21u/SP21v/SP21w/SP21x/SP21y/SP21z/SP22/SP22a/SP22b/SP22c/SP22d/SP22e/SP22f/SP22g/SP22h/SP22i/SP22j/SP22k/SP22l/SP22m/SP22n/SP22o/SP22p/SP22q/SP22r/SP22s/SP22t/SP22u/SP22v/SP22w/SP22x/SP22y/SP22z/SP23/SP23a/SP23b/SP23c/SP23d/SP23e/SP23f/SP23g/SP23h/SP23i/SP23j/SP23k/SP23l/SP23m/SP23n/SP23o/SP23p/SP23q/SP23r/SP23s/SP23t/SP23u/SP23v/SP23w/SP23x/SP23y/SP23z/SP24/SP24a/SP24b/SP24c/SP24d/SP24e/SP24f/SP24g/SP24h/SP24i/SP24j/SP24k/SP24l/SP24m/SP24n/SP24o/SP24p/SP24q/SP24r/SP24s/SP24t/SP24u/SP24v/SP24w/SP24x/SP24y/SP24z/SP25/SP25a/SP25b/SP25c/SP25d/SP25e/SP25f/SP25g/SP25h/SP25i/SP25j/SP25k/SP25l/SP25m/SP25n/SP25o/SP25p/SP25q/SP25r/SP25s/SP25t/SP25u/SP25v/SP25w/SP25x/SP25y/SP25z/SP26/SP26a/SP26b/SP26c/SP26d/SP26e/SP26f/SP26g/SP26h/SP26i/SP26j/SP26k/SP26l/SP26m/SP26n/SP26o/SP26p/SP26q/SP26r/SP26s/SP26t/SP26u/SP26v/SP26w/SP26x/SP26y/SP26z/SP27/SP27a/SP27b/SP27c/SP27d/SP27e/SP27f/SP27g/SP27h/SP27i/SP27j/SP27k/SP27l/SP27m/SP27n/SP27o/SP27p/SP27q/SP27r/SP27s/SP27t/SP27u/SP27v/SP27w/SP27x/SP27y/SP27z/SP28/SP28a/SP28b/SP28c/SP28d/SP28e/SP28f/SP28g/SP28h/SP28i/SP28j/SP28k/SP28l/SP28m/SP28n/SP28o/SP28p/SP28q/SP28r/SP28s/SP28t/SP28u/SP28v/SP28w/SP28x/SP28y/SP28z/SP29/SP29a/SP29b/SP29c/SP29d/SP29e/SP29f/SP29g/SP29h/SP29i/SP29j/SP29k/SP29l/SP29m/SP29n/SP29o/SP29p/SP29q/SP29r/SP29s/SP29t/SP29u/SP29v/SP29w/SP29x/SP29y/SP29z/SP30/SP30a/SP30b/SP30c/SP30d/SP30e/SP30f/SP30g/SP30h/SP30i/SP30j/SP30k/SP30l/SP30m/SP30n/SP30o/SP30p/SP30q/SP30r/SP30s/SP30t/SP30u/SP30v/SP30w/SP30x/SP30y/SP30z/SP31/SP31a/SP31b/SP31c/SP31d/SP31e/SP31f/SP31g/SP31h/SP31i/SP31j/SP31k/SP31l/SP31m/SP31n/SP31o/SP31p/SP31q/SP31r/SP31s/SP31t/SP31u/SP31v/SP31w/SP31x/SP31y/SP31z/SP32/SP32a/SP32b/SP32c/SP32d/SP32e/SP32f/SP32g/SP32h/SP32i/SP32j/SP32k/SP32l/SP32m/SP32n/SP32o/SP32p/SP32q/SP32r/SP32s/SP32t/SP32u/SP32v/SP32w/SP32x/SP32y/SP32z/SP33/SP33a/SP33b/SP33c/SP33d/SP33e/SP33f/SP33g/SP33h/SP33i/SP33j/SP33k/SP33l/SP33m/SP33n/SP33o/SP33p/SP33q/SP33r/SP33s/SP33t/SP33u/SP33v/SP33w/SP33x/SP33y/SP33z/SP34/SP34a/SP34b/SP34c/SP34d/SP34e/SP34f/SP34g/SP34h/SP34i/SP34j/SP34k/SP34l/SP34m/SP34n/SP34o/SP34p/SP34q/SP34r/SP34s/SP34t/SP34u/SP34v/SP34w/SP34x/SP34y/SP34z/SP35/SP35a/SP35b/SP35c/SP35d/SP35e/SP35f/SP35g/SP35h/SP35i/SP35j/SP35k/SP35l/SP35m/SP35n/SP35o/SP35p/SP35q/SP35r/SP35s/SP35t/SP35u/SP35v/SP35w/SP35x/SP35y/SP35z/SP36/SP36a/SP36b/SP36c/SP36d/SP36e/SP36f/SP36g/SP36h/SP36i/SP36j/SP36k/SP36l/SP36m/SP36n/SP36o/SP36p/SP36q/SP36r/SP36s/SP36t/SP36u/SP36v/SP36w/SP36x/SP36y/SP36z/SP37/SP37a/SP37b/SP37c/SP37d/SP37e/SP37f/SP37g/SP37h/SP37i/SP37j/SP37k/SP37l/SP37m/SP37n/SP37o/SP37p/SP37q/SP37r/SP37s/SP37t/SP37u/SP37v/SP37w/SP37x/SP37y/SP37z/SP38/SP38a/SP38b/SP38c/SP38d/SP38e/SP38f/SP38g/SP38h/SP38i/SP38j/SP38k/SP38l/SP38m/SP38n/SP38o/SP38p/SP38q/SP38r/SP38s/SP38t/SP38u/SP38v/SP38w/SP38x/SP38y/SP38z/SP39/SP39a/SP39b/SP39c/SP39d/SP39e/SP39f/SP39g/SP39h/SP39i/SP39j/SP39k/SP39l/SP39m/SP39n/SP39o/SP39p/SP39q/SP39r/SP39s/SP39t/SP39u/SP39v/SP39w/SP39x/SP39y/SP39z/SP40/SP40a/SP40b/SP40c/SP40d/SP40e/SP40f/SP40g/SP40h/SP40i/SP40j/SP40k/SP40l/SP40m/SP40n/SP40o/SP40p/SP40q/SP40r/SP40s/SP40t/SP40u/SP40v/SP40w/SP40x/SP40y/SP40z/SP41/SP41a/SP41b/SP41c/SP41d/SP41e/SP41f/SP41g/SP41h/SP41i/SP41j/SP41k/SP41l/SP41m/SP41n/SP41o/SP41p/SP41q/SP41r/SP41s/SP41t/SP41u/SP41v/SP41w/SP41x/SP41y/SP41z/SP42/SP42a/SP42b/SP42c/SP42d/SP42e/SP42f/SP42g/SP42h/SP42i/SP42j/SP42k/SP42l/SP42m/SP42n/SP42o/SP42p/SP42q/SP42r/SP42s/SP42t/SP42u/SP42v/SP42w/SP42x/SP42y/SP42z/SP43/SP43a/SP43b/SP43c/SP43d/SP43e/SP43f/SP43g/SP43h/SP43i/SP43j/SP43k/SP43l/SP43m/SP43n/SP43o/SP43p/SP43q/SP43r/SP43s/SP43t/SP43u/SP43v/SP43w/SP43x/SP43y/SP43z/SP44/SP44a/SP44b/SP44c/SP44d/SP44e/SP44f/SP44g/SP44h/SP44i/SP44j/SP44k/SP44l/SP44m/SP44n/SP44o/SP44p/SP44q/SP44r/SP44s/SP44t/SP44u/SP44v/SP44w/SP44x/SP44y/SP44z/SP45/SP45a/SP45b/SP45c/SP45d/SP45e/SP45f/SP45g/SP45h/SP45i/SP45j/SP45k/SP45l/SP45m/SP45n/SP45o/SP45p/SP45q/SP45r/SP45s/SP45t/SP45u/SP45v/SP45w/SP45x/SP45y/SP45z/SP46/SP46a/SP46b/SP46c/SP46d/SP46e/SP46f/SP46g/SP46h/SP46i/SP46j/SP46k/SP46l/SP46m/SP46n/SP46o/SP46p/SP46q/SP46r/SP46s/SP46t/SP46u/SP46v/SP46w/SP46x/SP46y/SP46z/SP47/SP47a/SP47b/SP47c/SP47d/SP47e/SP47f/SP47g/SP47h/SP47i/SP47j/SP47k/SP47l/SP47m/SP47n/SP47o/SP47p/SP47q/SP47r/SP47s/SP47t/SP47u/SP47v/SP47w/SP47x/SP47y/SP47z/SP48/SP48a/SP48b/SP48c/SP48d/SP48e/SP48f/SP48g/SP48h/SP48i/SP48j/SP48k/SP48l/SP48m/SP48n/SP48o/SP48p/SP48q/SP48r/SP48s/SP48t/SP48u/SP48v/SP48w/SP48x/SP48y/SP48z/SP49/SP49a/SP49b/SP49c/SP49d/SP49e/SP49f/SP49g/SP49h/SP49i/SP49j/SP49k/SP49l/SP49m/SP49n/SP49o/SP49p/SP49q/SP49r/SP49s/SP49t/SP49u/SP49v/SP49w/SP49x/SP49y/SP49z/SP50/SP50a/SP50b/SP50c/SP50d/SP50e/SP50f/SP50g/SP50h/SP50i/SP50j/SP50k/SP50l/SP50m/SP50n/SP50o/SP50p/SP50q/SP50r/SP50s/SP50t/SP50u/SP50v/SP50w/SP50x/SP50y/SP50z/SP51/SP51a/SP51b/SP51c/SP51d/SP51e/SP51f/SP51g/SP51h/SP51i/SP51j/SP51k/SP51l/SP51m/SP51n/SP51o/SP51p/SP51q/SP51r/SP51s/SP51t/SP51u/SP51v/SP51w/SP51x/SP51y/SP51z/SP52/SP52a/SP52b/SP52c/SP52d/SP52e/SP52f/SP52g/SP52h/SP52i/SP52j/SP52k/SP52l/SP52m/SP52n/SP52o/SP52p/SP52q/SP52r/SP52s/SP52t/SP52u/SP52v/SP52w/SP52x/SP52y/SP52z/SP53/SP53a/SP53b/SP53c/SP53d/SP53e/SP53f/SP53g/SP53h/SP53i/SP53j/SP53k/SP53l/SP53m/SP53n/SP53o/SP53p/SP53q/SP53r/SP53s/SP53t/SP53u/SP53v/SP53w/SP53x/SP53y/SP53z/SP54/SP54a/SP54b/SP54c/SP54d/SP54e/SP54f/SP54g/SP54h/SP54i/SP54j/SP54k/SP54l/SP54m/SP54n/SP54o/SP54p/SP54q/SP54r/SP54s/SP54t/SP54u/SP54v/SP54w/SP54x/SP54y/SP54z/SP55/SP55a/SP55b/SP55c/SP55d/SP55e/SP55f/SP55g/SP55h/SP55i/SP55j/SP55k/SP55l/SP55m/SP55n/SP55o/SP55p/SP55q/SP55r/SP55s/SP55t/SP55u/SP55v/SP55w/SP55x/SP55y/SP55z/SP56/SP56a/SP56b/SP56c/SP56d/SP56e/SP56f/SP56g/SP56h/SP56i/SP56j/SP56k/SP56l/SP56m/SP56n/SP56o/SP56p/SP56q/SP56r/SP56s/SP56t/SP56u/SP56v/SP56w/SP56x/SP56y/SP56z/SP57/SP57a/SP57b/SP57c/SP57d/SP57e/SP57f/SP57g/SP57h/SP57i/SP57j/SP57k/SP57l/SP57m/SP57n/SP57o/SP57p/SP57q/SP57r/SP57s/SP57t/SP57u/SP57v/SP57w/SP57x/SP57y/SP57z/SP58/SP58a/SP58b/SP58c/SP58d/SP58e/SP58f/SP58g/SP58h/SP58i/SP58j/SP58k/SP58l/SP58m/SP58n/SP58o/SP58p/SP58q/SP58r/SP58s/SP58t/SP58u/SP58v/SP58w/SP58x/SP58y/SP58z/SP59/SP59a/SP59b/SP59c/SP59d/SP59e/SP59f/SP59g/SP59h/SP59i/SP59j/SP59k/SP59l/SP59m/SP59n/SP59o/SP59p/SP59q/SP59r/SP59s/SP59t/SP59u/SP59v/SP59w/SP59x/SP59y/SP59z/SP60/SP60a/SP60b/SP60c/SP60d/SP60e/SP60f/SP60g/SP60h/SP60i/SP60j/SP60k/SP60l/SP60m/SP60n/SP60o/SP60p/SP60q/SP60r/SP60s/SP60t/SP60u/SP60v/SP60w/SP60x/SP60y/SP60z/SP61/SP61a/SP61b/SP61c/SP61d/SP61e/SP61f/SP61g/SP61h/SP61i/SP61j/SP61k/SP61l/SP61m/SP61n/SP61o/SP61p/SP61q/SP61r/SP61s/SP61t/SP61u/SP61v/SP61w/SP61x/SP61y/SP61z/SP62/SP62a/SP62b/SP62c/SP62d/SP62e/SP62f/SP62g/SP62h/SP62i/SP62j/SP62k/SP62l/SP62m/SP62n/SP62o/SP62p/SP62q/SP62r/SP62s/SP62t/SP62u/SP62v/SP62w/SP62x/SP62y/SP62z/SP63/SP63a/SP63b/SP63c/SP63d/SP63e/SP63f/SP63g/SP63h/SP63i/SP63j/SP63k/SP63l/SP63m/SP63n/SP63o/SP63p/SP63q/SP63r/SP63s/SP63t/SP63u/SP63v/SP63w/SP63x/SP63y/SP63z/SP64/SP64a/SP64b/SP64c/SP64d/SP64e/SP64f/SP64g/SP64h/SP64i/SP64j/SP64k/SP64l/SP64m/SP64n/SP64o/SP64p/SP64q/SP64r/SP64s/SP64t/SP64u/SP64v/SP64w/SP64x/SP64y/SP64z/SP65/SP65a/SP65b/SP65c/SP65d/SP65e/SP65f/SP65g/SP65h/SP65i/SP65j/SP65k/SP65l/SP65m/SP65n/SP65o/SP65p/SP65q/SP65r/SP65s/SP65t/SP65u/SP65v/SP65w/SP65x/SP65y/SP65z/SP66/SP66a/SP66b/SP66c/SP66d/SP66e/SP66f/SP66g/SP66h/SP66i/SP66j/SP66k/SP66l/SP66m/SP66n/SP66o/SP66p/SP66q/SP66r/SP66s/SP66t/SP66u/SP66v/SP66w/SP66x/SP66y/SP66z/SP67/SP67a/SP67b/SP67c/SP67d/SP67e/SP67f/SP67g/SP67h/SP67i/SP67j/SP67k/SP67l/SP67m/SP67n/SP67o/SP67p/SP67q/SP67r/SP67s/SP67t/SP67u/SP67v/SP67w/SP67x/SP67y/SP67z/SP68/SP68a/SP68b/SP68c/SP68d/SP68e/SP68f/SP68g/SP68h/SP68i/SP68j/SP68k/SP68l/SP68m/SP68n/SP68o/SP68p/SP68q/SP68r/SP68s/SP68t/SP68u/SP68v/SP68w/SP68x/SP68y/SP68z/SP69/SP69a/SP69b/SP69c/SP69d/SP69e/SP69f/SP69g/SP69h/SP69i/SP69j/SP69k/SP69l/SP69m/SP69n/SP69o/SP69p/SP69q/SP69r/SP69s/SP69t/SP69u/SP69v/SP69w/SP69x/SP69y/SP69z/SP70/SP70a/SP70b/SP70c/SP70d/SP70e/SP70f/SP70g/SP70h/SP70i/SP70j/SP70k/SP70l/SP70m/SP70n/SP70o/SP70p/SP70q/SP70r/SP70s/SP70t/SP70u/SP70v/SP70w/SP70x/SP70y/SP70z/SP71/SP71a/SP71b/SP71c/SP71d/SP71e/SP71f/SP71g/SP71h/SP71i/SP71j/SP71k/SP71l/SP71m/SP71n/SP71o/SP71p/SP71q/SP71r/SP71s/SP71t/SP71u/SP71v/SP71w/SP71x/SP71y/SP71z/SP72/SP72a/SP72b/SP72c/SP72d/SP72e/SP72f/SP72g/SP72h/SP72i/SP72j/SP72k/SP72l/SP72m/SP72n/SP72o/SP72p/SP72q/SP72r/SP72s/SP72t/SP72u/SP72v/SP72w/SP72x/SP72y/SP72z/SP73/SP73a/SP73b/SP73c/SP73d/SP73e/SP73f/SP73g/SP73h/SP73i/SP73j/SP73k/SP73l/SP73m/SP73n/SP73o/SP73p/SP73q/SP73r/SP73s/SP73t/SP73u/SP73v/SP73w/SP73x/SP73y/SP73z/SP74/SP74a/SP74b/SP74c/SP74d/SP74e/SP74f/SP74g/SP74h/SP74i/SP74j/SP74k/SP74l/SP74m/SP74n/SP74o/SP74p/SP74q/SP74r/SP74s/SP74t/SP74u/SP74v/SP74w/SP74x/SP74y/SP74z/SP75/SP75a/SP75b/SP75c/SP75d/SP75e/SP75f/SP75g/SP75h/SP75i/SP75j/SP75k/SP75l/SP75m/SP75n/SP75o/SP75p/SP75q/SP75r/SP75s/SP75t/SP75u/SP75v/SP75w/SP75x/SP75y/SP75z/SP76/SP76a/SP76b/SP76c/SP76d/SP76e/SP76f/SP76g/SP76h/SP76i/SP76j/SP76k/SP76l/SP76m/SP76n/SP76o/SP76p/SP76q/SP76r/SP76s/SP76t/SP76u/SP76v/SP76w/SP76x/SP76y/SP76z/SP77/SP77a/SP77b/SP77c/SP77d/SP77e/SP77f/SP77g/SP77h/SP77i/SP77j/SP77k/SP77l/SP77m/SP77n/SP77o/SP77p/SP77q/SP77r/SP77s/SP77t/SP77u/SP77v/SP77w/SP77x/SP77y/SP77z/SP78/SP78a/SP78b/SP78c/SP78d/SP78e/SP78f/SP78g/SP78h/SP78i/SP78j/SP78k/SP78l/SP78m/SP78n/SP78o/SP78p/SP78q/SP78r/SP78s/SP78t/SP78u/SP78v/SP78w/SP78x/SP78y/SP78z/SP79/SP79a/SP79b/SP79c/SP79d/SP79e/SP79f/SP79g/SP79h/SP79i/SP79j/SP79k/SP79l/SP79m/SP79n/SP79o/SP79p/SP79q/SP79r/SP79s/SP79t/SP79u/SP79v/SP79w/SP79x/SP79y/SP79z/SP80/SP80a/SP80b/SP80c/SP80d/SP80e/SP80f/SP80g/SP80h/SP80i/SP80j/SP80k/SP80l/SP80m/SP80n/SP80o/SP80p/SP80q/SP80r/SP80s/SP80t/SP80u/SP80v/SP80w/SP80x/SP80y/SP80z/SP81/SP81a/SP81b/SP81c/SP81d/SP81e/SP81f/SP81g/SP81h/SP81i/SP81j/SP81k/SP81l/SP81m/SP81n/SP81o/SP81p/SP81q/SP81r/SP81s/SP81t/SP81u/SP81v/SP81w/SP81x/SP81y/SP81z/SP82/SP82a/SP82b/SP82c/SP82d/SP82e/SP82f/SP82g/SP82h/SP82i/SP82j/SP82k/SP82l/SP82m/SP82n/SP82o/SP82p/SP82q/SP82r/SP82s/SP82t/SP82u/SP82v/SP82w/SP82x/SP82y/SP82z/SP83/SP83a/SP83b/SP83c/SP83d/SP83e/SP83f/SP83g/SP83h/SP83i/SP83j/SP83k/SP83l/SP83m/SP83n/SP83o/SP83p/SP83q/SP83r/SP83s/SP83t/SP83u/SP83v/SP83w/SP83x/SP83y/SP83z/SP84/SP84a/SP84b/SP84c/SP84d/SP84e/SP84f/SP84g/SP84h/SP84i/SP84j/SP84k/SP84l/SP84m/SP84n/SP84o/SP84p/SP84q/SP84r/SP84s/SP84t/SP84u/SP84v/SP84w/SP84x/SP84y/SP84z/SP85/SP85a/SP85b/SP85c/SP85d/SP85e/SP85f/SP85g/SP85h/SP85i/SP85j/SP85k/SP85l/SP85m/SP85n/SP85o/SP85p/SP85q/SP85r/SP85s/SP85t/SP85u/SP85v/SP85w/SP85x/SP85y/SP85z/SP86/SP86a/SP86b/SP86c/SP86d/SP86e/SP86f/SP86g/SP86h/SP86i/SP86j/SP86k/SP86l/SP86m/SP86n/SP86o/SP86p/SP86q/SP86r/SP86s/SP86t/SP86u/SP86v/SP86w/SP86x/SP86y/SP86z/SP87/SP87a/SP87b/SP87c/SP87d/SP87e/SP87f/SP87g/SP87h/SP87i/SP87j/SP87k/SP87l/SP87m/SP87n/SP87o/SP87p/SP87q/SP87r/SP87s/SP87t/SP87u/SP87v/SP87w/SP87x/SP87y/SP87z/SP88/SP88a/SP88b/SP88c/SP88d/SP88e/SP88f/SP88g/SP88h/SP88i/SP88j/SP88k/SP88l/SP88m/SP88n/SP88o/SP88p/SP88q/SP88r/SP88s/SP88t/SP88u/SP88v/SP88w/SP88x/SP88y/SP88z/SP89/SP89a/SP89b/SP89c/SP89d/SP89e/SP89f/SP89g/SP89h/SP89i/SP89j/SP89k/SP89l/SP89m/SP89n/SP89o/SP89p/SP89q/SP89r/SP89s/SP89t/SP89u/SP89v/SP89w/SP89x/SP89y/SP89z/SP90/SP90a/SP90b/SP90c/SP90d/SP90e/SP90f/SP90g/SP90h/SP90i/SP90j/SP90k/SP90l/SP90m/SP90n/SP90o/SP90p/SP90q/SP90r/SP90s/SP90t/SP90u/SP90v/SP90w/SP90x/SP90y/SP90z/SP91/SP91a/SP91b/SP91c/SP91d/SP91e/SP91f/SP91g/SP91h/SP91i/SP91j/SP91k/SP91l/SP91m/SP91n/SP91o/SP91p/SP91q/SP91r/SP91s/SP91t/SP91u/SP91v/SP91w/SP91x/SP91y/SP91z/SP92/SP92a/SP92b/SP92c/SP92d/SP92e/SP92f/SP92g/SP92h/SP92i/SP92j/SP92k/SP92l/SP92m/SP92n/SP92o/SP92p/SP92q/SP92r/SP92s/SP92t/SP92u/SP92v/SP92w/SP92x/SP92y/SP92z/SP93/SP93a/SP93b/SP93c/SP93d/SP93e/SP93f/SP93g/SP93h/SP93i/SP93j/SP93k/SP93l/SP93m/SP93n/SP93o/SP
```

