网络安全技术实战

2021

主讲：邵艺豪

目 录

CONTENTS

01

PART 1

流 量 分 析

数据包分析，通常也被称为数据包嗅探或协议分析，指的是捕获和解析网络上在线传输数据的过程，通常是为了能更好地了解在网络上正在发生的事情。

流量分析

CTF 比赛中,流量包的取证分析是另一项重要的考察方向。

通常比赛中会提供一个包含流量数据的 PCAP 文件，有时候也会需要选手们先进行修复或重构传输文件后，再进行分析。

流量数据包这一块作为重点考察方向，复杂的地方在于数据包里充满着大量无关的流量信息，因此如何分类和过滤数据是参赛者需要完成的工作。

主要工具是wireshark，需要熟练掌握使用方法，过滤器语法、追踪流、导出文件。

Wireshark的介绍

Wireshark是目前全球使用最广泛的开源抓包软件，是一个通用化的网络数据嗅探器和协议分析器。如果是网络工程师，可以通过wireshark软件对网络进行故障定位和排错；如果是安全工程师，可以通过wireshark软件对网络黑客渗透攻击进行快速定位并找出攻击源；如果是测试或者软件工程师，可以通过wireshark软件分析底层通信机制等等。

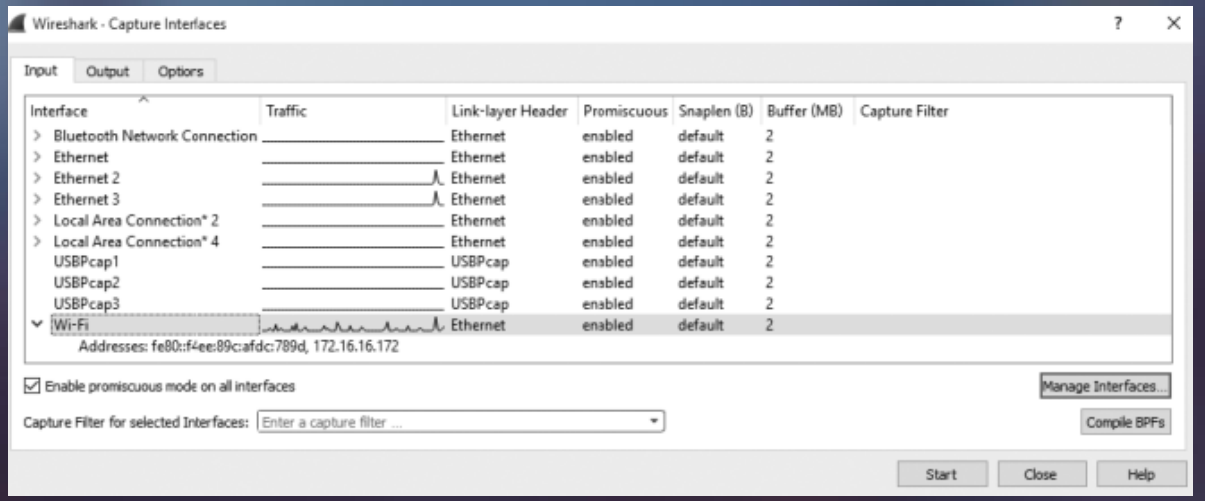
Wireshark的介绍

第一次捕获数据包

（1）打开 Wireshark。

（2）从主下拉菜单中选择 Capture，然后是 Interface。这时你应该可以看到一个对话框，里面列出了你可以用来捕获数据包的各种设备，以及它们的 IP 地址。

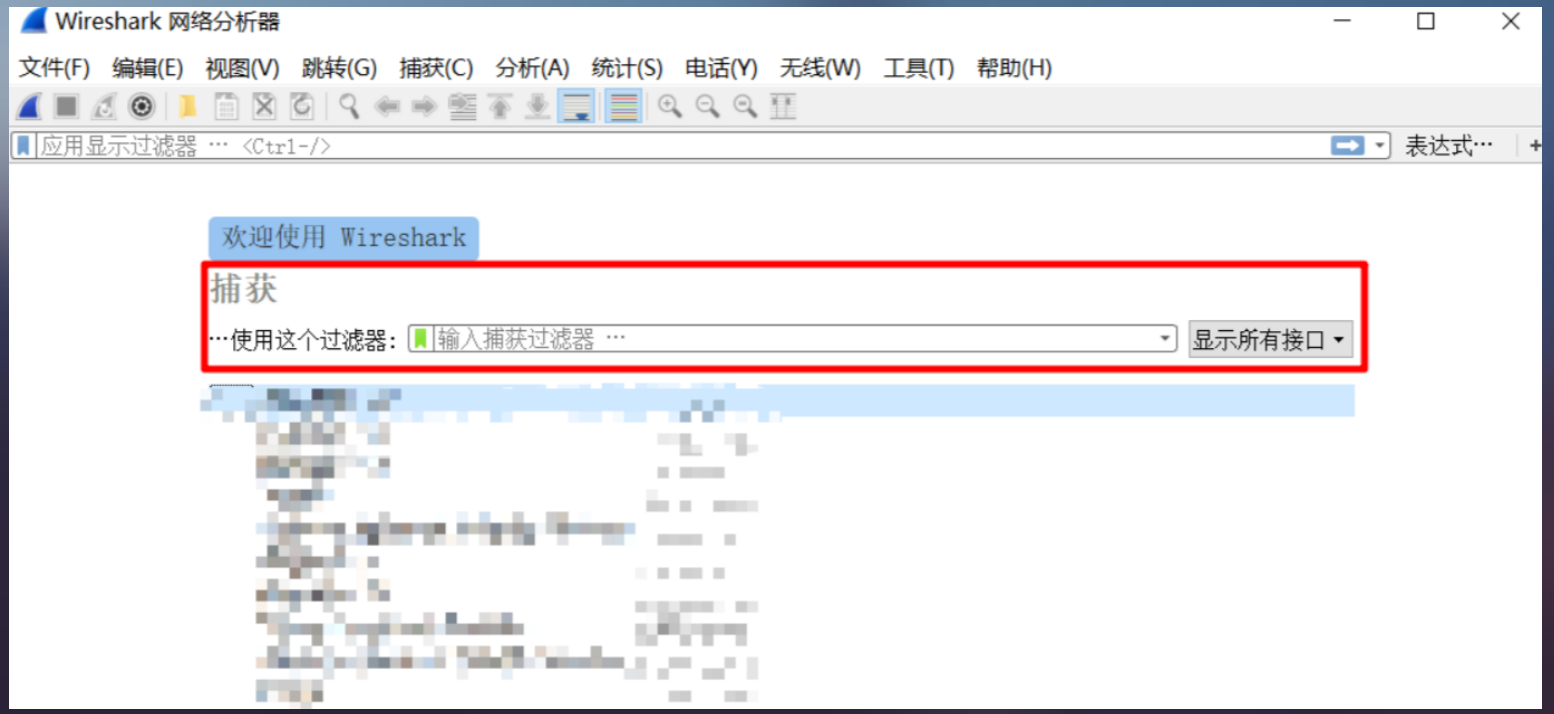
（3）选择你想要使用的设备，如图所示，然后单击 Start，或者直接单击欢迎画面中 Interface List 下的某一个设备。随后数据就会在窗口中呈现出来。



Wireshark

捕捉过滤器

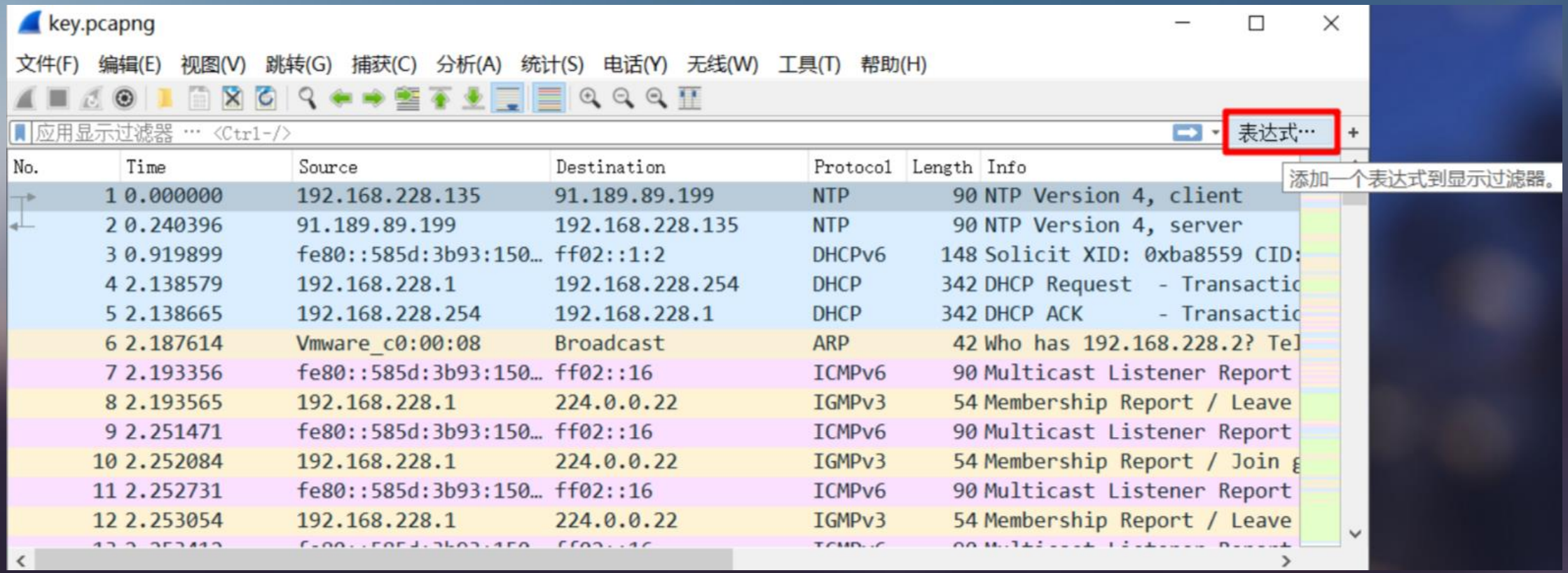
数据经过的第一层过滤器， 它用于控制捕捉数据的数量，以避免产生过大的日志文件，用于决定将什么样的信息记录在捕捉结果中，需要在开始捕捉前设置

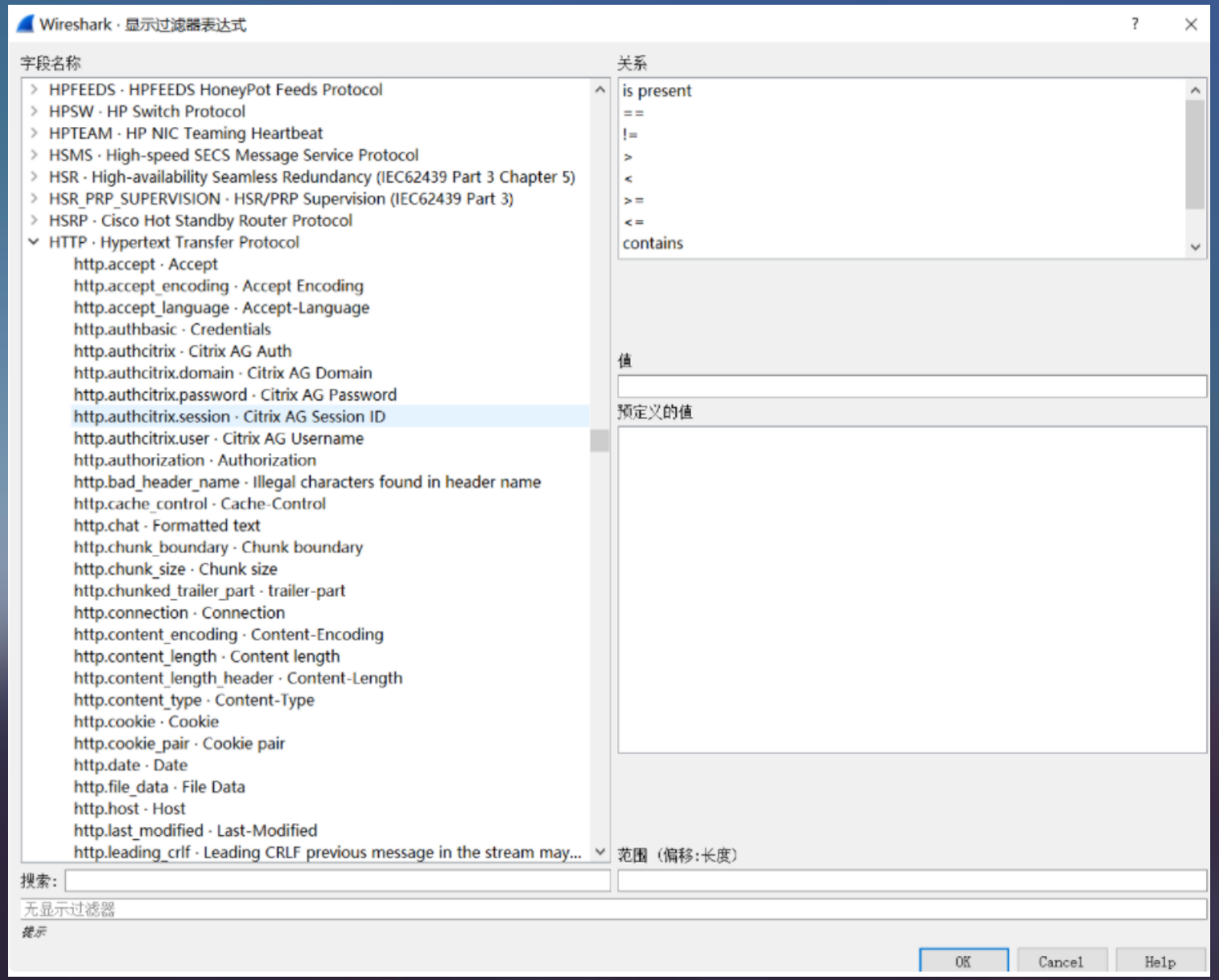


Wireshark

捕捉过滤器

打开一个数据包，点击 表达式 会看到很多字段

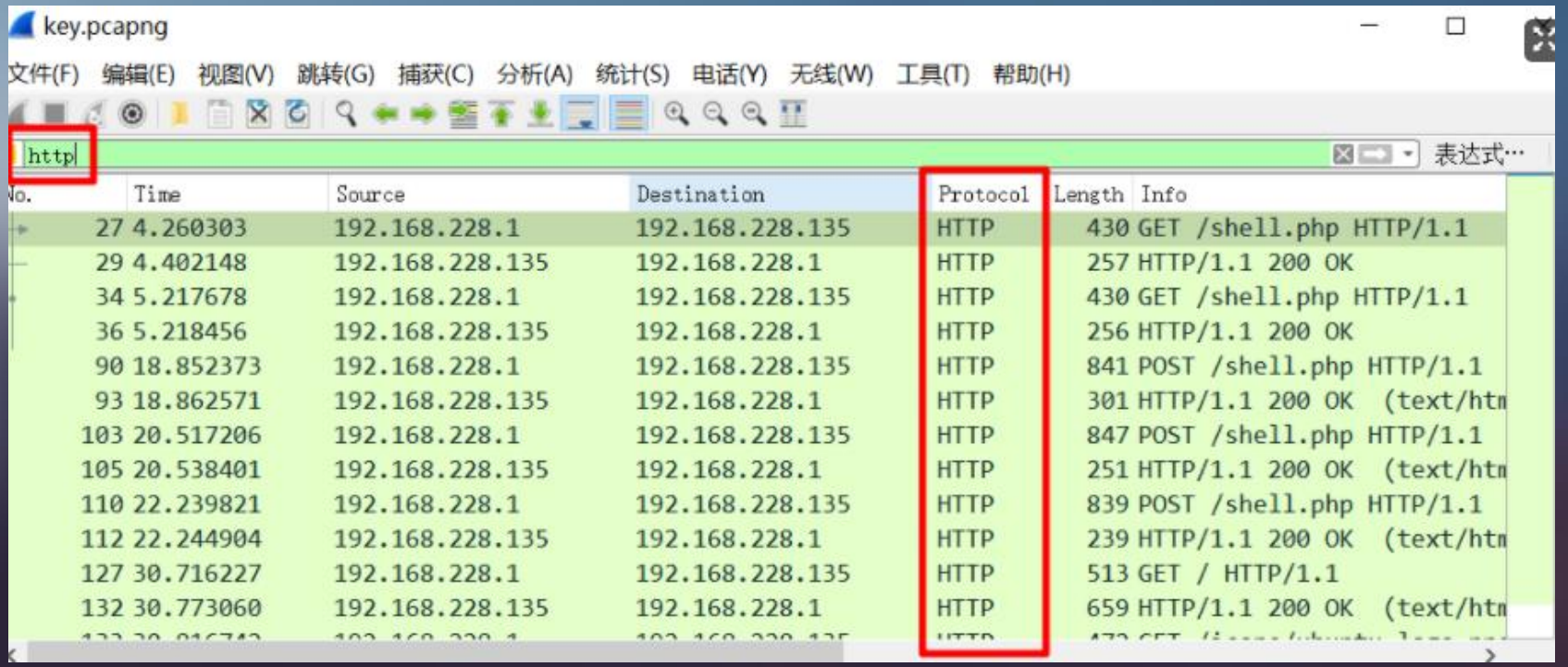



Wireshark · 显示过滤器表达式
字段名称
关系
HPFEEDS · HPFEEDS HoneyPot Feeds Protocol
HPSW · HP Switch Protocol
HPTEAM · HP NIC Teaming Heartbeat
HSMS · High-speed SECS Message Service Protocol
HSR · High-availability Seamless Redundancy (IEC62439 Part 3 Chapter 5)
HSR_PRP_SUPERVISION · HSR/PRP Supervision (IEC62439 Part 3)
HSRP · Cisco Hot Standby Router Protocol
HTTP · Hypertext Transfer Protocol
http.accept · Accept
http.accept_encoding · Accept Encoding
http.accept_language · Accept-Language
http.authbasic · Credentials
http.authcitrix · Citrix AG Auth
http.authcitrix.domain · Citrix AG Domain
http.authcitrix.password · Citrix AG Password
http.authcitrix.session · Citrix AG Session ID
http.authcitrix.user · Citrix AG Username
http.authorization · Authorization
http.bad_header_name · Illegal characters found in header name
http.cache_control · Cache-Control
http.chat · Formatted text
http.chunk_boundary · Chunk boundary
http.chunk_size · Chunk size
http.chunked_trailer_part · trailer-part
http.connection · Connection
http.content_encoding · Content-Encoding
http.content_length · Content length
http.content_length_header · Content-Length
http.content_type · Content-Type
http.cookie · Cookie
http.cookie_pair · Cookie pair
http.date · Date
http.file_data · File Data
http.host · Host
http.last_modified · Last-Modified
http.leading_crlf · Leading CRLF previous message in the stream may...
is present
==
!=
>
<
>=
<=
contains
值
预定义的值
范围（偏移:长度）
搜索:
无显示过滤器
提示
OK
Cancel
Help

Wireshark

捕捉过滤器

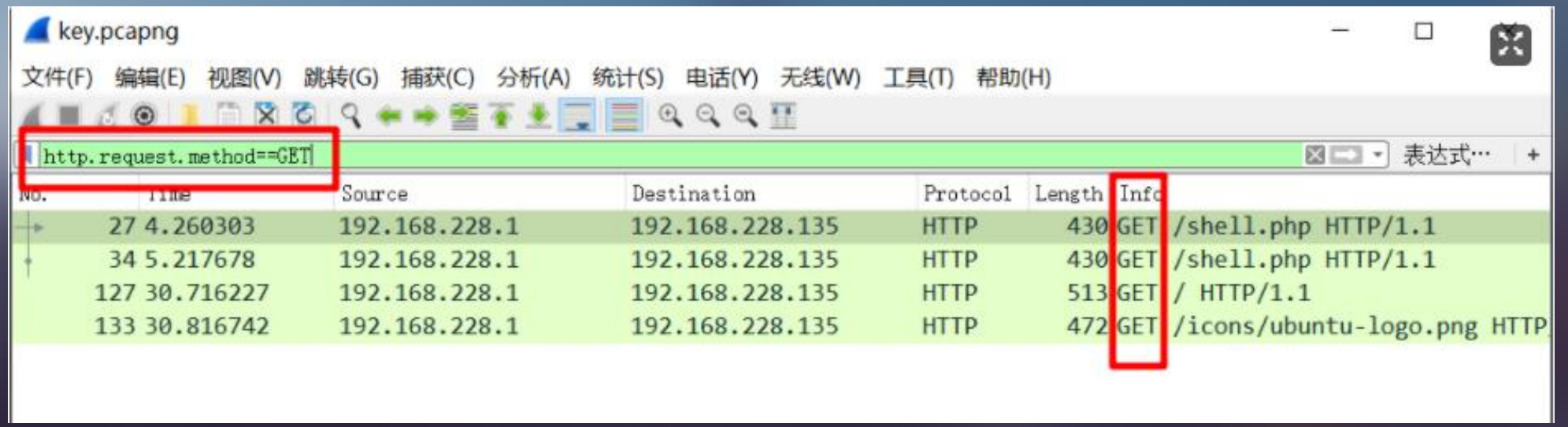
也可以直接输入 http 就会自动过滤



Wireshark

捕捉过滤器

http.request.method==GET



Wireshark

捕捉过滤器

ip.src == 10.230.0.0/16　显示来自10..230网段的封包

tcp.port == 25　显示来源或目的TCP端口号为25的封包

tcp.dstport == 25　显示目的TCP端口号为25的封包

http.request.method == "POST"　显示post请求方式的http封包

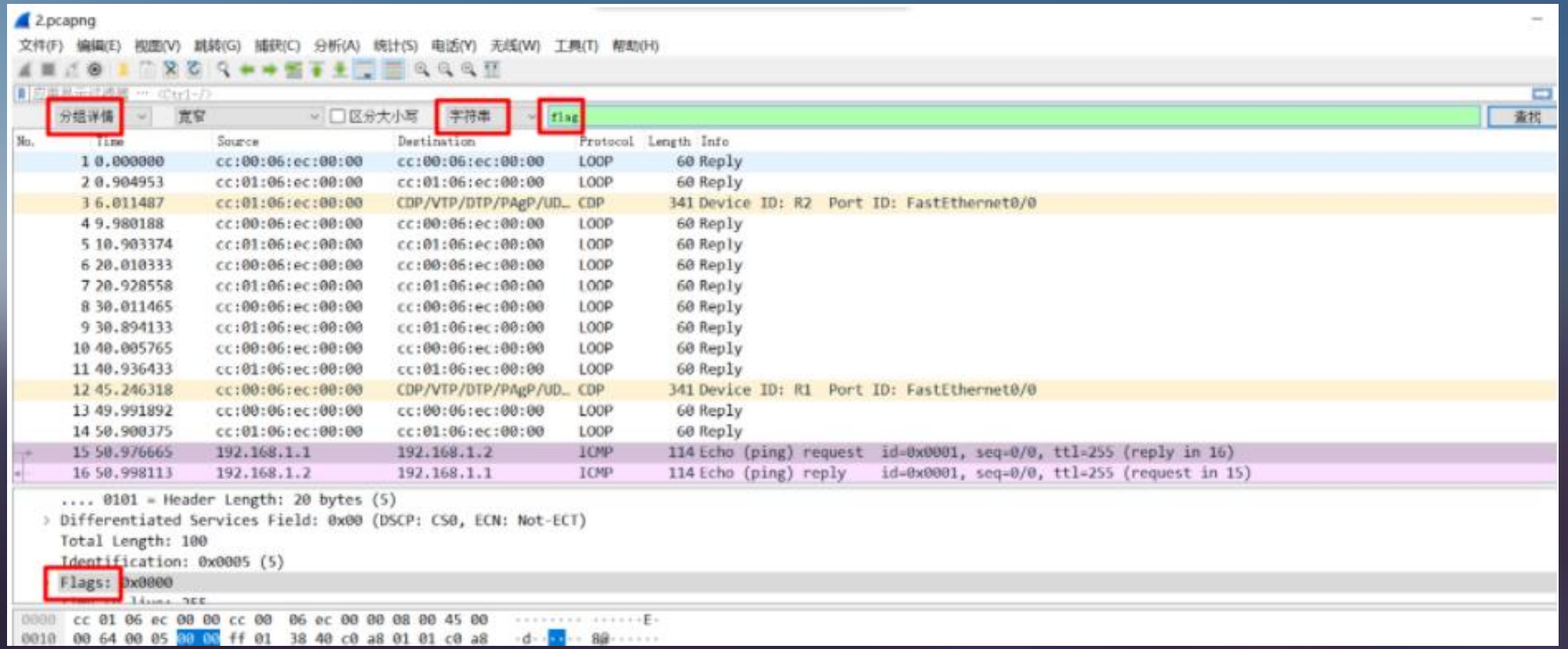
http.host == "example.com"　显示请求域名为example.com的http封包

tcp contains "http"　显示payload中包含"http"字符串封包

http.request.url contains "online"　显示请求的url包含"online"的http封包

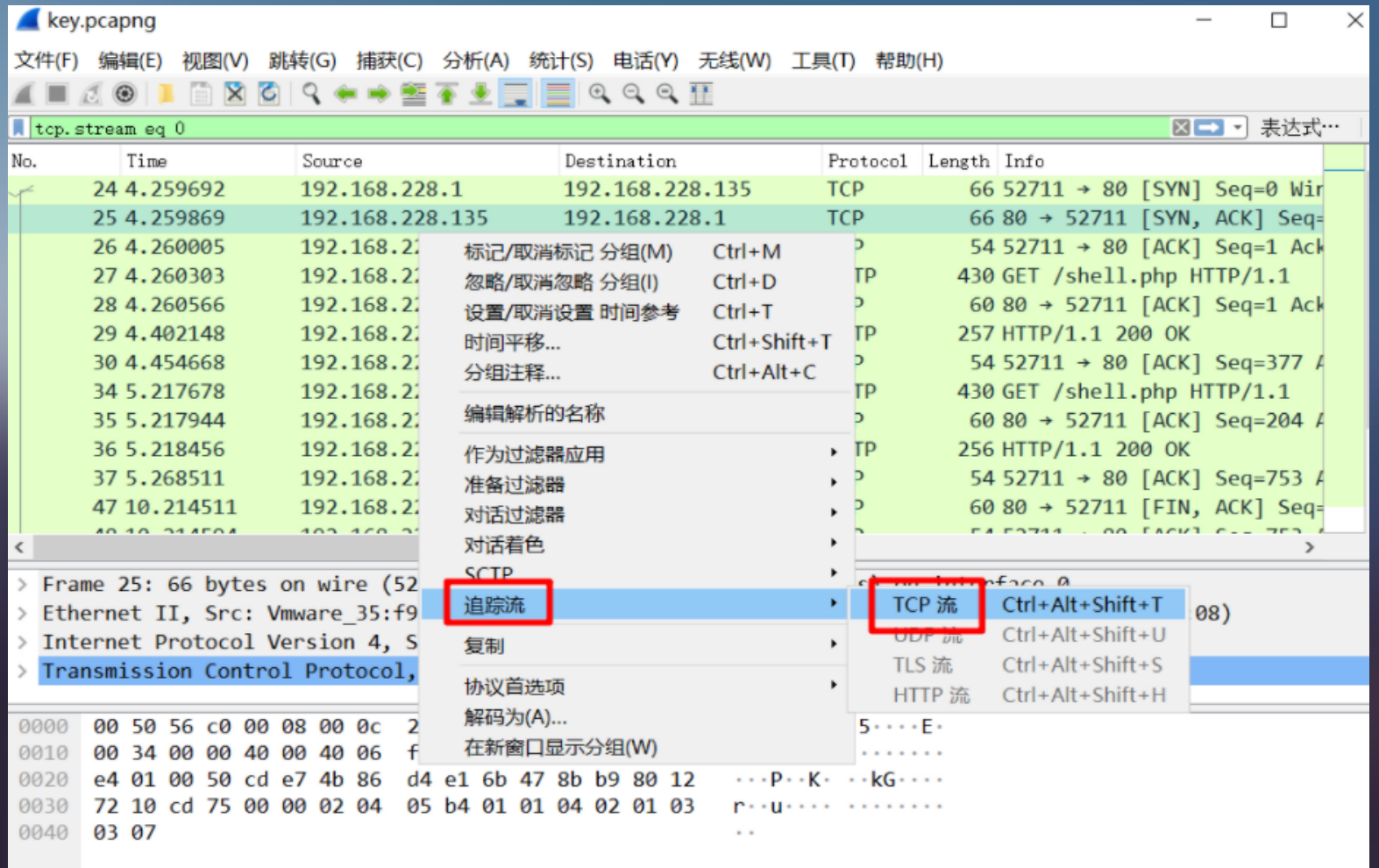
Wireshark

搜索字符串：ctrl+F 选择分组详情、字符串，然后输入想找的查找就可以



Wireshark

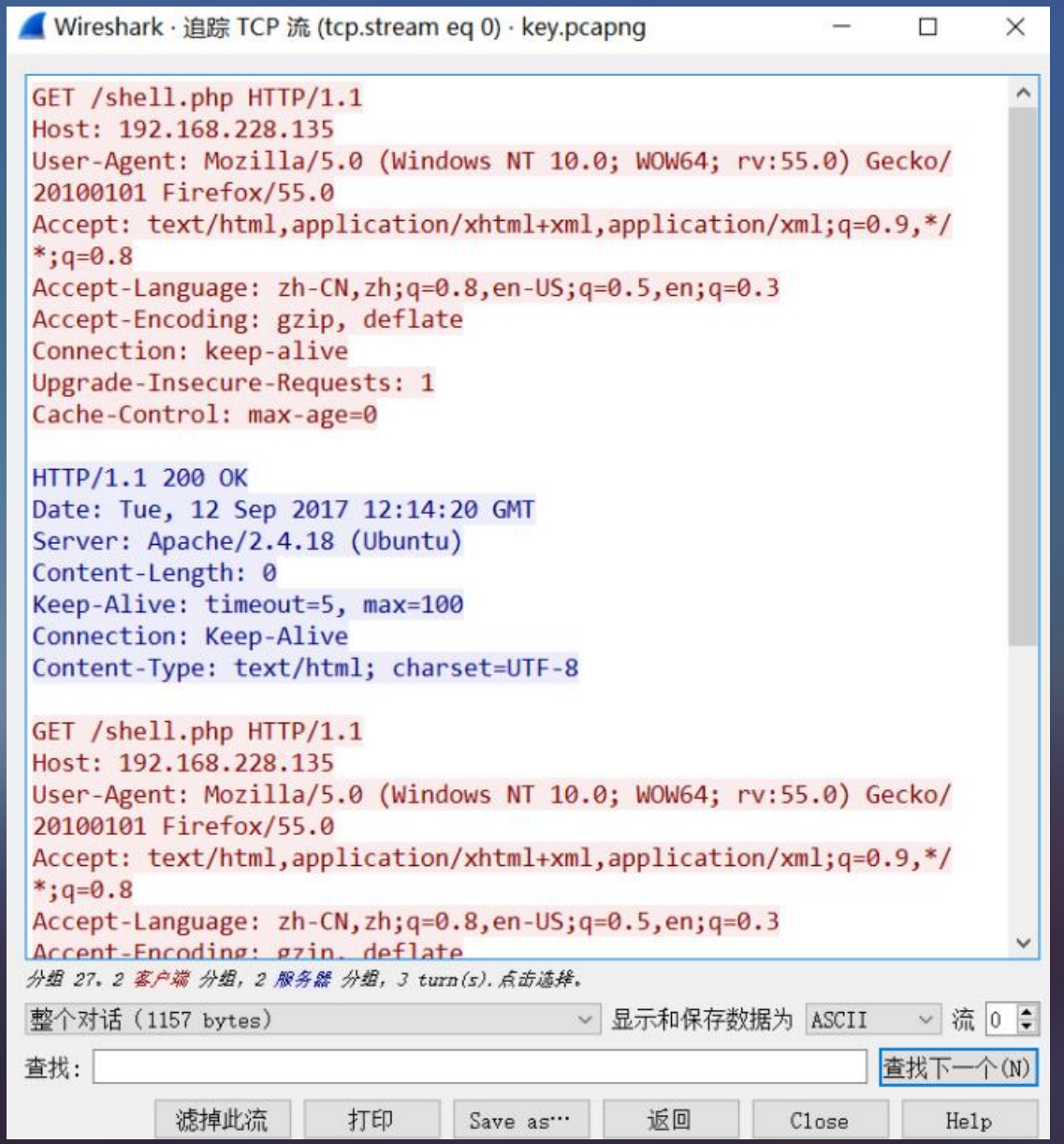
右键 -> 追踪 -> TCP流，可以跟踪TCP会话的过程



Wireshark

右键 -> 追踪 -> TCP流，可以跟踪TCP会话的过程

有时候这里会有一些 zip、png、jpg的信息，如果熟悉文件头的话一眼就能看出来，用下面的save as...就可以保存成出来，然后用 winhex 保存成图片或压缩包



流量分析题型

演示：

练习1：流量分析01

题目地址：http://106.52.138.23:6001/

练习2：流量分析02

题目地址：http://106.52.138.23:6002/

02

PART 2

隐　写　分　析

图像文件有多种复杂的格式，可以用于各种涉及到元数据、信息丢失和信息隐写或修改图片参数等，都是 Misc 中的一个很重要的出题方向。

隐写分析题型

演示：

练习1：隐写分析01

题目地址：http://106.52.138.23:6003/

练习2：隐写分析02

题目地址：http://106.52.138.23:6004/

03

PART 3

字 符 编 码

字符编码

进制

进制也就是进位计数制，在CTF比赛中，常见进制为二进制、八进制、十进制、十六进制。

二进制：代码中全是0和1的数据表示

8进制：用八个阿拉伯数字：0、1、2、3、4、5、6、7；

10进制：用十个阿拉伯数字：0到9；

16进制：以0x开始的数据表示，用0~9和A，B，C，D，E，F这六个字母来分别表示10，11，12，13，14，15。字母不区分大小写。

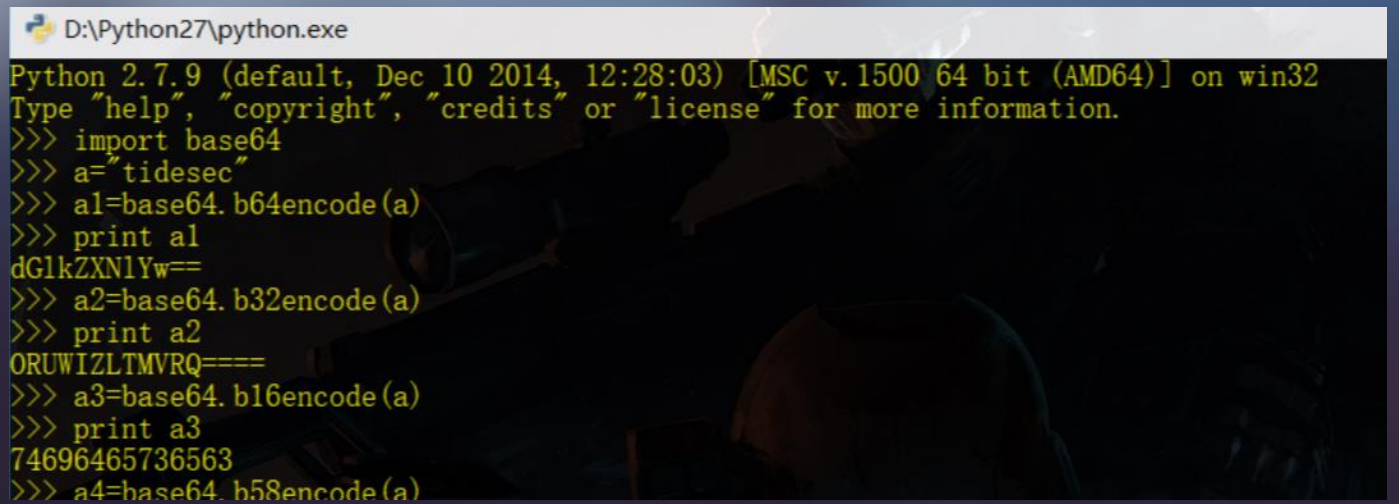
字符编码

BASE家族

BASE64：64个可打印字符，A~Z、a~z、0~9、+、/，64个可打印字符，“=”符号用作后缀填充。

BASE32：32个可打印字符，A~Z、2~7、32个可打印字符，“=”符号用作后缀填充。

BASE16：16个可打印字符，A~F、0-9，16个可打印字符。



字符编码

摩尔斯（Morse）编码

特点

只有 . 和 -

最多 6 位

也可以使用 01 串表示

练习：

例题：-... -.- -.-. - ..-. -- .. ... -.-.

答案格式KEY{xxxxxxxxx}

字符编码

ASCII 编码

特点：我们一般使用的 ascii 编码的时候采用的都是可见字符，而且主要是如下字符

0-9, 49-57

A-Z, 65-90

a-z, 97-122

{ },123/125

练习例题：\u0066\u006c\u0061\u0067\u007b\u0063\u0074\u0066\u005f\u0069\u0073\u005f\u006e\u0069\u0063\u0065\u007d

ASCII 字符代码表 一

高四位 / 低四位		ASCII非打印控制字符										ASCII 打印字符												
		0000					0001					0010		0011		0100		0101		0110		0111		
		0					1					2		3		4		5		6		7		
		+进制	字符	ctrl	代码	字符解释	+进制	字符	ctrl	代码	字符解释	+进制	字符	+进制	字符	+进制	字符	+进制	字符	+进制	字符	+进制	字符	ctrl
0000	0	0	BLANK NULL	^@	NUL	空	16	▶	^P	DLE	数据链路转意	32		48	0	64	@	80	P	96	`	112	p	
0001	1	1	☺	^A	SOH	头标开始	17	◀	^Q	DC1	设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2	☻	^B	STX	正文开始	18	↕	^R	DC2	设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	3	♥	^C	ETX	正文结束	19	‼	^S	DC3	设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	4	♦	^D	EOT	传输结束	20	¶	^T	DC4	设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	♣	^E	ENQ	查询	21	§	^U	NAK	反确认	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	^F	ACK	确认	22	▬	^V	SYN	同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	震铃	23	↨	^W	ETB	传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	8	◘	^H	BS	退格	24	↑	^X	CAN	取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	^I	TAB	水平制表符	25	↓	^Y	EM	媒体结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	换行/新行	26	→	^Z	SUB	替换	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	^K	VT	竖直制表符	27	←	^[	ESC	转意	43	+	59	;	75	K	91	[	107	k	123	{	
1100	C	12	♀	^L	FF	换页/新页	28	∟	^\	FS	文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|	
1101	D	13	♪	^M	CR	回车	29	↔	^]	GS	组分隔符	45	-	61	=	77	M	93	]	109	m	125	}	
1110	E	14	♫	^N	SO	移出	30	▲	^6	RS	记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	F	15	☼	^O	SI	移入	31	▼	^-	US	单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂	^Back space

注：表中的ASCII字符可以用:ALT + "小键盘上的数字键" 输入

字符编码

unicode编码：

国际标准字符，将全球的各种语言的每个字符定义一个唯一的编码。

unicode一般有四种表示形式

&#x [Hex]: The

&# [Decimal]: The

\U [Hex]: \U0054\U0068\U0065

\U+ [Hex]: \U+0054\U+0068\U+0065

URL编码:

特征特点：一个字符ascii码的十六进制，然后在前面加上%

如：%27表示单引号，%20表示空格

URL编码表：https://www.w3school.com.cn/tags/html_ref_urlencode.asp

字符编码题型

演示：

练习1：字符编码01

题目地址：http://106.52.138.23:6005/

练习2：字符编码02

题目地址：http://106.52.138.23:6006/

04

PART 4

文件修复

文件修复

常见图片类型的文件头：

JPEG (jpg)，文件头：FF D8 FF

PNG (png)，文件头：89 50 4E 47

GIF (gif)，文件头：47 49 46 38

Windows Bitmap (bmp)，文件头：42 4D

常见压缩包文件头：

ZIP Archive (zip)，文件头：50 4B 03 04

rar文件: 52 61 72 21

7z文件头：37 7A BC AF 27 1C

可使用十六进制编辑器 winHex、010Ediitor等工具进行练习查看

文件修复题型

演示：

练习1：文件修复01

题目地址：http://106.52.138.23:6007/

练习2：文件修复02

题目地址：http://106.52.138.23:6008/

感谢您的观赏！

主讲：邵艺豪　981484617@qq.com