



CONTENTS



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。



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 - Capture Interfaces								?	×
Input Output Options									
Interface Tr > Bluetooth Network Connection > Ethernet 2 > Ethernet 2 > Ethernet 3 > Local Area Connection* 4 USBPcap1 USBPcap2 USBPcap3 VUSPCAP3 VUSPCAP	۲۹۴۴ic ۸ ۸ ۲۵۶۰ ۲۶9d, 172.16.16.172	Link-layer Header Ethernet Ethernet Ethernet Ethernet Ethernet USBPcap USBPcap USBPcap Ethernet	Promiscuous enabled enabled enabled enabled enabled enabled enabled enabled enabled	Snaplen (B) default default default default default default default default default	Buffer (MB) 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Capture Filter			
Enable promiscuous mode on all interfac Capture Filter for selected Interfaces:	ces iter a capture filter				Manage I	interfaces ompile BPF			
						Start	Close	Help	

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



捕捉过滤器

打开一个数据包, 点击 表达式 会看到很多字段

📕 key	pcapng				-		×	
文件(F)	编辑(E) 视图(V) 跳	转(G) 捕获(C) 分析(A) 统计	+(S) 电话(Y) 无线(W)	工具(T) 帮助	(H)			
	2 🛛 📕 🖉	۹ 🗰 🗃 著 💆 📃 📃	0,0,0,1			_	_	
■ 应用:	显示过滤器 … <ctrl-></ctrl->					表达式	tt +	
No.	Time	Source	Destination	Protoco1	Length Info		法加一个	表达式到显示过滤器
	10.000000	192.168.228.135	91.189.89.199	NTP	90 NTP Version 4, clie	nt ⁽		
<u></u>	2 0.240396	91.189.89.199	192.168.228.135	NTP	90 NTP Version 4, serv	rer		
	3 0.919899	fe80::585d:3b93:150	ff02::1:2	DHCPv6	148 Solicit XID: 0xba85	59 CII):	
	4 2.138579	192.168.228.1	192.168.228.254	DHCP	342 DHCP Request - Tra	nsacti	ic	
	5 2.138665	192.168.228.254	192.168.228.1	DHCP	342 DHCP ACK - Tra	nsacti	ic	
	6 2.187614	Vmware_c0:00:08	Broadcast	ARP	42 Who has 192.168.228	.2? Te	2]	
	7 2.193356	fe80::585d:3b93:150	ff02::16	ICMPv6	90 Multicast Listener	Report	t	
	8 2.193565	192.168.228.1	224.0.0.22	IGMPv3	54 Membership Report /	Leave	2	
	9 2.251471	fe80::585d:3b93:150	ff02::16	ICMPv6	90 Multicast Listener	Report	t	
	10 2.252084	192.168.228.1	224.0.0.22	IGMPv3	54 Membership Report /	Join	٤	
	11 2.252731	fe80::585d:3b93:150	ff02::16	ICMPv6	90 Multicast Listener	Report	t	
	12 2.253054	192.168.228.1	224.0.0.22	IGMPv3	54 Membership Report /	Leave	2	
<	11 2 252412	C-00F0FJ.3L03.4F0	£5001C	TCMDC	00 M.112	D	, *	

🚄 Wireshark · 显示过滤器表达式

-段名称	关系
> HPFEEDS · HPFEEDS HoneyPot Feeds Protocol	is present ^
> 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	contains 🗸
http.accept · Accept	
http.accept_encoding · Accept Encoding	
http.accept_language · Accept-Language	
http.authbasic · Credentials	
http.authcitrix · Citrix AG Auth	植
http.authcitrix.domain · Citrix AG Domain	
http.authcitrix.password · Citrix AG Password	
http.authcitrix.session · Citrix AG Session ID	预定义时值
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.date · Date	
http:nie_data · File Data	
http://doi.org/10.1001	
http://ast_modified + Last-Modified	
http://eduling_chi + Leading CKLr previous message in the stream may *	」 紀国(偏移:大度)
·[索:	
无显示过滤器	
ŧ <i>r</i>	
	OK Cancel Help

?

 \times

捕捉过滤器

也可以直接输入 http 就会自动过滤

🚄 key	y.pcapng				- 🗆 🕅									
文件(F)编辑(E)视图(V) 3	姚转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	L具(T) 帮助((H)									
(H	3 🗙 🗂 📕 🕥 为	9 + + = = + 1												
http	http													
lo.	Time	Source	Destination	Protocol	Length Info									
	27 4.260303	192.168.228.1	192.168.228.135	HTTP	430 GET /shell.php HTTP/1.1									
-	29 4.402148	192.168.228.135	192.168.228.1	HTTP	257 HTTP/1.1 200 OK									
+	34 5.217678	192.168.228.1	192.168.228.135	HTTP	430 GET /shell.php HTTP/1.1									
	36 5.218456	192.168.228.135	192.168.228.1	HTTP	256 HTTP/1.1 200 OK									
10	90 18.852373	192.168.228.1	192.168.228.135	HTTP	841 POST /shell.php HTTP/1.1									
	93 18.862571	192.168.228.135	192.168.228.1	HTTP	301 HTTP/1.1 200 OK (text/htm									
	103 20.517206	192.168.228.1	192.168.228.135	HTTP	847 POST /shell.php HTTP/1.1									
	105 20.538401	192.168.228.135	192.168.228.1	HTTP	251 HTTP/1.1 200 OK (text/htm									
	110 22.239821	192.168.228.1	192.168.228.135	HTTP	839 POST /shell.php HTTP/1.1									
	112 22.244904	192.168.228.135	192.168.228.1	HTTP	239 HTTP/1.1 200 OK (text/htm									
	127 30.716227	192.168.228.1	192.168.228.135	HTTP	513 GET / HTTP/1.1									
	132 30.773060	192.168.228.135	192.168.228.1	HTTP	659 HTTP/1.1 200 OK (text/htm									
	177 70 01 747	100 100 000 1	100 100 000 105	UTTO	ATT OFT 12 Inhuman Toma have									

捕捉过滤器

http.request.method==GET

▲ I 文件	key.pcapng (F) 编辑(E) 视图(V) 跳	.转(G) 捕获(C) 分析(A)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助	(H)			X
11	3 X 🗂 🛛 🕥 为	9 + + 2 7 1	📜 🔍 🔍 🔍 🔢					
ht	tp.request.method==GET						表达式·	• +
NO.	ilme	Source	Destination	Protocol	Length Info			
	27 4.260303	192.168.228.1	192.168.228.135	HTTP	430 GET	/shell.php HTTP/	1.1	
+	34 5.217678	192.168.228.1	192.168.228.135	HTTP	430 GET	/shell.php HTTP/	1.1	
	127 30.716227	192.168.228.1	192.168.228.135	HTTP	513 GET	/ HTTP/1.1		
	133 30.816742	192.168.228.1	192.168.228.135	HTTP	472 GET	/icons/ubuntu-lo	go.png	HTTP

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

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

Z 2	2.pcapng			_		57.0
文件	\$(F) 编辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A) 1	统计(5) 电话(Y) 无线(W) 工	與(T) 帮助	(H)	
4	I 1 0 1 1 X	8 9 * * E T 1	<u> </u>			
112	THE REPORT OF COM	1-D				
	分組详備 ~ プ	19 · · · · · · · · · · · · · · · · · · ·	大小写 字符串 ~ 11	ie i		重找
No.	Time	Source	Destination	Protocol	Length Info	
	10.000000	cc:00:05:ec:00:00	cc:00:05:ec:00:00	LOOP	60 Reply	
	2 0.904953	cc:01:06:ec:00:00	cc:01:06:ec:00:00	LOOP	60 Reply	
	3 6.011487	cc:01:05:ec:00:00	CDP/VTP/DTP/PAgP/UD.	. CDP	341 Device ID: R2 Port ID: FastEthernet0/0	
	4 9.980188	cc:00:05:ec:00:00	cc:00:05:ec:00:00	LOOP	60 Reply	
	5 10.903374	cc:01:06:ec:00:00	cc:01:06:ec:00:00	LOOP	60 Reply	
	6 20.010333	cc:00:06:ec:00:00	cc:00:06:ec:00:00	LOOP	60 Reply	
	7 20.928558	cc:01:06:ec:00:00	cc:01:06:ec:00:00	LOOP	60 Reply	
	8 30.011465	cc:00:06:ec:00:00	cc:00:06:ec:00:00	LOOP	60 Reply	
	9 30.894133	cc:01:06:ec:00:00	cc:01:06:ec:00:00	LOOP	60 Reply	
	10 40.005765	cc:00:06:ec:00:00	cc:00:06:ec:00:00	LOOP	60 Reply	
	11 40.936433	cc:01:06:ec:00:00	cc:01:06:ec:00:00	LOOP	60 Reply	
	12 45.246318	cc:00:06:ec:00:00	CDP/VTP/DTP/PAgP/UD.	. COP	341 Device ID: R1 Port ID: FastEthernet0/0	
	13 49.991892	cc:00:06:ec:00:00	cc:00:06:ec:00:00	LOOP	60 Reply	
	14 50.900375	cc:01:06:ec:00:00	cc:01:06:ec:00:00	LOOP	60 Reply	
-19-	15 50.976665	192.168.1.1	192.168.1.2	1CMP	114 Echo (ping) request id=0x0001, seq=0/0, ttl=255 (reply in 16)	
4	16 50,998113	192,168,1.2	192.168.1.1	ICMP	114 Echo (ping) reply id=0x0001, seq=0/0, ttl=255 (request in 15)	
000	0101 = Hea Differentiated Total Length: 1 Identification Flags: Dx0000 Duest	ader Length: 20 bytes (Services Field: 0x00 (100 : 0x0005 (5) ncc 0 00 cc 00 06 ec 00 0	5) DSCP: CS0, ECN: Not-EC	т)	•E •	
00	18 00 64 00 05	0 00 ff 01 38 40 c0 a	8 01 01 c0 a8 -d- 💀		111	

右键 -> 追踪 -> TCP流,可以跟踪TCP会话的过程

4	🕻 key.pcapng						-		\times		
3	マ件(F) 编辑(E) 视图(V)	跳转(G) 捕获(C) 分标	沂(A) 统计(S) 电话(Y) 🗄	无线(W) 工具	Į(T) 帮助	(H)					
1	(🔳 🖉 🛞 📕 🗋 🗙 🕻	🗿 🤇 🗢 🏓 🖀 🚡	🖢 📃 📃 Q, Q, Q, I	Ì							
I.	tcp.stream eq 0						×	表达式	···		
N	o. Time	Source	Destination		Protocol	Length Info					
Ч	< 24 4.259692	192.168.228.1	192.168.228	.135	тср	66 52711 → 80 [5	SYN] Se	q=0 Wir			
	25 4.259869	192.168.228.13	192.168.228	.1	тср	66 80 → 52711 [5	SYN, AC	K] Seq=			
П	26 4.260005	192.168.2	际记/取消标记 分组(M)	Ctrl+M	P	54 52711 → 80 [4	ACK] Se	q=1 Ack			
Н	27 4.260303	192.168.2	忽略/取消忽略 分组(I)	Ctrl+D	TP	430 GET /shell.ph	пр НТТР	/1.1			
Н	28 4.260566	192.168.22	设置/取消设置 时间参考	Ctrl+T	P	60 80 → 52711 [<i>l</i>	ACK] Se	q=1 Ack			
Н	29 4.402148	192.168.2	时间平移	Ctrl+Shift+T	r <mark>TP</mark>	257 HTTP/1.1 200	OK				
Н	30 4.454668	192.168.2	分组注释	Ctrl+Alt+C	P	54 52711 → 80 [4	ACK] Se	q=377 /			
	34 5.217678	192.168.2	白キ目も刀もご かわくて ギケ		- TP	430 GET /shell.ph	пр НТТР	/1.1			
	35 5.217944	192.168.2	海 特耳斯的TEV-石小V		P	60 80 → 52711 [4	ACK] Se	q=204 A			
	36 5.218456	192.168.2	作为过滤器应用		• TP	256 HTTP/1.1 200	OK				
	37 5.268511	192.168.22 y	隹备过滤器		• P	54 52711 → 80 [4	ACK] Se	q=753 A			
	47 10.214511	192.168.2	对话过滤器		• ?	60 80 → 52711 [F	IN, AC	K] Seq=			
<	40 10 214504	102 100 21	对话着色		•						
>	Frame 25: 66 bytes	on wire (52 🗗	SCTP		·	http://www.faco.co					
5	Ethernet II. Src:	Vmware 35:f9	自踪流		• TC	2P流 Ctrl+Alt+Shift+T	08)				
>	Internet Protocol	Version 4, S	同制		, -0	Ctrl+Alt+Shift+L	J				
>	Transmission Contr	ol Protocol.	Sec.193		TL	S 流 Ctrl+Alt+Shift+S	;				
			办议首选项		' HT	TP 流 Ctrl+Alt+Shift+H	1				
6	000 00 50 56 c0 00	08 00 0c 2 🇯	解码为(A)		5	E					
6	0010 00 34 00 00 40	00 40 06 f 1	在新窗口显示分组(W)								
6	020 e4 01 00 50 cd	e7 4b 86 d4 e1	6b 47 8b b9 80 12	•••P••K•	· · · kG · ·						
6	030 72 10 cd 75 00	00 02 04 05 b4	01 01 04 02 01 03	r··u····							
6	040 03 07										

Wireshark	GET Hos Use
右键 -> 追踪 -> TCP流,可以	201 Acc *;q
跟踪TCP会话的过程	Acco Acco Con Upg Cac
	HTT Dat Ser Con Kee
有时候这里会有一些 zip、png、	Con Con
jpg的信息,如果熟悉文件头的话一	GET Hos Use
眼就能看出来,用下面的save as	201 Acc *;q
就可以保存成出来,然后用 winhex	Acco 分组。
保存成图片或压缩包	<u>整</u> 个 查找:

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · key.pcapng	-		×
ET /shell.php HTTP/1.1			^
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)	; rv:55.0) G	iecko/	
<pre>accept: text/html,application/xhtml+xml,applicat ig=0.8</pre>	tion/xml;q=0	1.9,*/	
<pre>cccept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;c cccept-Encoding: gzip, deflate connection: keep-alive pgrade-Insecure-Requests: 1 ache-Control: max-age=0</pre>	1=0.3		
TTP/1.1 200 OK Date: Tue, 12 Sep 2017 12:14:20 GMT Derver: Apache/2.4.18 (Ubuntu) Content-Length: 0 Deep-Alive: timeout=5, max=100 Deprection: Keen-Alive			
ontent-Type: text/html; charset=UTF-8			
ET /shell.php HTTP/1.1 lost: 192.168.228.135 lser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; 0100101 Firefox/55.0 accept: text/html,application/xhtml+xml,applicat	; rv:55.0) G tion/xml;q=0	iecko/).9,*/	
;q=0.8 accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;a accent-Encoding: gzin. deflate 组 27.2 客户端 分组,2 服务器 分组,3 turn(s).点击选择.	-0. 3		~
隆个对话(1157 bytes) - 显示和保存	字数据为 ASCII	~ 流	0 🗘
找:		查找下一个	`(N)
滤掉此流 打印 Save as… 返回	Close	Help	5



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/

0 2 PART 2



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。



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/

PART 3









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。

D:\Python27\python.exe

Python 2.7.9 (default, Dec 10 2014	4, 12:28:03)	[MSC v. 1500	64 bit (AMD6	4)] on win32
Type "help", "copyright", "credit:	s" or "licen	se" for more	information.	
>>> import base64				
>>> a="tidesec"				
>>> a1=base64. b64encode (a)				
>>> print al				
dG1kZXN1Yw==				
>>> a2=base64. b32encode (a)				
>>> print a2				
ORUWIZLTMVRQ====				
>>> a3=base64. b16encode (a)				
>>> print a3				
74696465736563				
>>> a4=base64. b58encode(a)				

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{xxxxxxxx}

国际摩尔斯电码

1. 一点的长度是一个单位. 2. 一划是三个单位. 3. 在一个字母中点划之间的间隔是一点. 4. 两个字母之间的间隔是三点(一划). 5. 两个单词之间的间隔是七点.

F

Р О

R



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\u007 b\u0063\u0074\u0066\u005f\u0069\u0073\u00 5f\u006e\u0069\u0063\u0065\u007d

	四位					ASCI14##	「印控制	訓字符									ASCI	I 打日]字符					
1.		1112-1361		00	00			0001			0010		00	11	01	00	01	01	01	10		0111		
<i>\</i> م¢.m.	4			C)			Lineire Lineire		1	and the second of	2		3		1		5		- I - E		BEH	7	
高四	$\pi /$	十进制	字符	ctrl	代码	字符解释	十進制	字符	ctrl	代码	字符解释	十進制	字符	十进制	字符	十進制	字符	十進制	字符	十進制	字符	十進制	字符	ctrl
0000	0	0	BLANK	^@	NUL	空	16		ŶΡ	DLE	数据链路转意	32		48	0	64	0	80	P	96		112	р	
0001	1	1	\odot	^ A	SOH	头标开始	17	•	^Q	DC1	设备控制 1	33	1	49	1	65	A	81	Q	97	а	113	q	
0010	2	2	•	^B	STX	正文开始	18	1	^R	DC2	设备控制 2	34	U.	50	2	66	В	82	R	98	b	114	r	
0011	3	3	۷	^c	ETX	正文结束	19	!!	^s	DC3	设备控制 3	35	#	51	3	67	С	83	S	99	С	115	s	
0100	4	4	٠	^ D	EOT	传输结束	20	1	ŶΤ	DC4	设备控制 4	36	\$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	4	^ E	ENQ	查询	21	¢	^ U	NAK	反确认	37	%	53	5	69	E	85	U	101	е	117	u	
0110	6	6	٨	^ 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	1	^ W	ETB	传输块结束	39	1	55	7	71	G	87	w	103	g	119	W	
1000	8	8	۵	^ H	BS	退格	24	1	^x	CAN	取消	40	(56	8	72	Н	88	X	104	h	120	х	
1001	9	9	0	^Ι	TAB	水平制表符	25	Ţ	^γ	EM	媒体结束	41)	57	9	73	1	89	Y	105	i	121	у	
1010	A	10	O	^J	LF	换行/新行	26	\rightarrow	^ Z	SUB	替换	42	*	58	•	74	J	90	Ζ	106	j	122	z	
1011	В	11	đ	^ K	VT	竖直制表符	27	←	1 ^	ESC	转意	43	+	59	÷	75	K	91	[107	k	123	{	
1100	с	12	Q	^L	FF	换页/新页	28	L	^\	FS	文件分隔符	44	,	60	<	76	L	92	1	108	1	124	Î	
1101	D	13		^ M	CR	回车	29	↔	^]	GS	组分隔符	45	÷	61	=	77	M	93	1	109	m	125	}	
1110	E	14	1	^N	SO	移出	30		^6	RS	记录分隔符	46		62	>	78	N	94	^	110	n	126	~	
1111	F	15	a	^0	SI	移入	31	¥	^_	US	单元分隔符	47	1	63	?	79	0	95		111	0	127	Δ	[°] Back space

ASCII 字符代码表 一



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/





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



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/



