2017第三届美亚杯全国电子数据取证大赛个人赛write up

原创

奇乃正 于 2022-01-02 17:22:59 发布 258 收藏 1

分类专栏： 取证 网络安全 电子数据取证 文章标签： 网络安全 安全

本文链接：https://blog.csdn.net/weixin_42744595/article/details/122277621


取证 同时被 3 个专栏收录

5 篇文章 2 订阅

订阅专栏


网络安全

5 篇文章 1 订阅

订阅专栏


电子数据取证

6 篇文章 3 订阅

订阅专栏

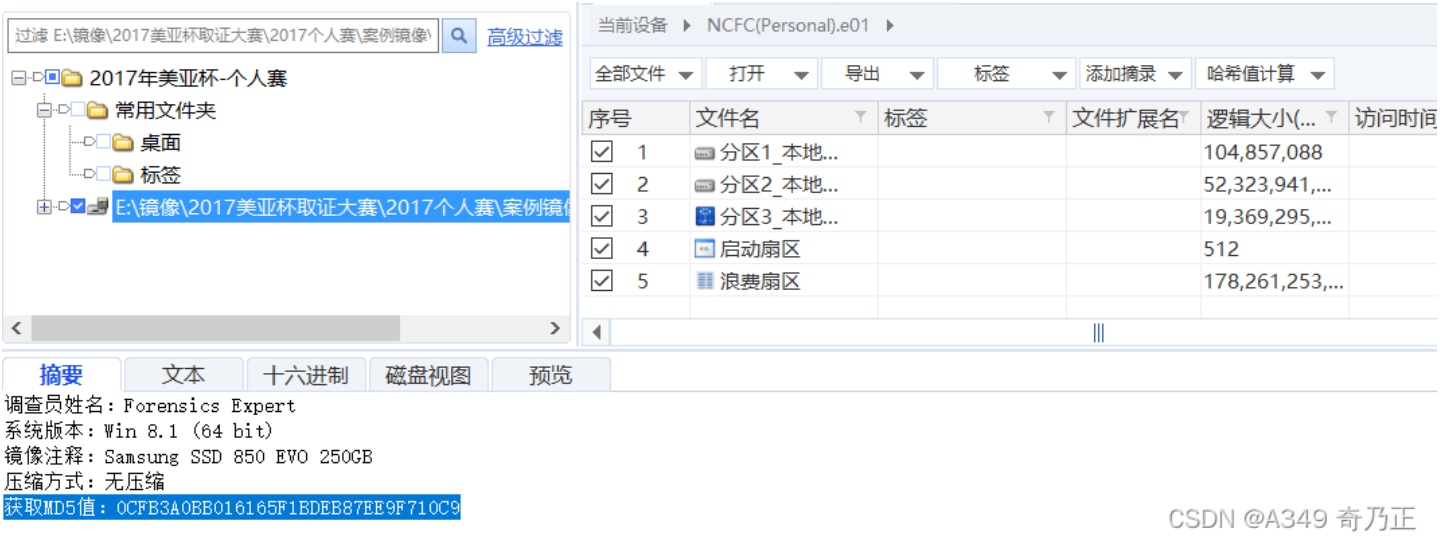
2017年美亚杯全国电子数据取证大赛

本人TEL15543132658 同wechat，欢迎多多交流，wp有不足欢迎大家补充多多探讨！

Questions

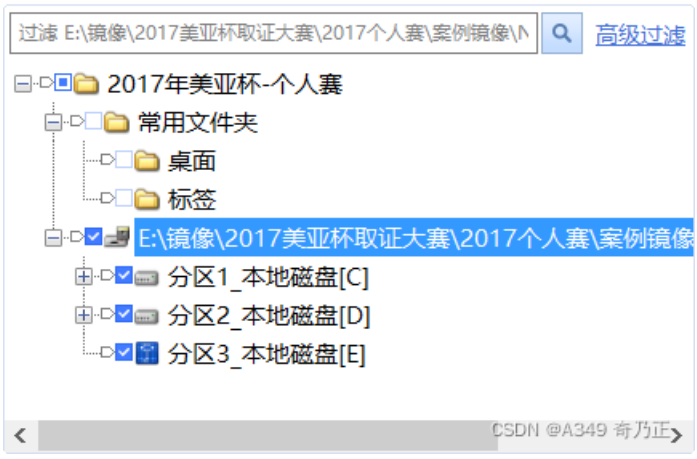
	1	Gary的笔记本电脑已成功取证并制作成镜像 (Forensic Image)，下列哪个是其MD5哈希值。
√	A.	0CFB3A0BB016165F1BDEB87EE9F710C9
	B.	5F1BDEB87EE9F710C90CFB3A0BB01616
	C.	A0BB016160CFB3A0BB0161661670CFB3
	D.	16160CFB3A0BB016166A0BB016166167
	E.	FB3A0BB016165 B016166 A0DF7FJE2EJ0

解析：使用取证大师进行分析



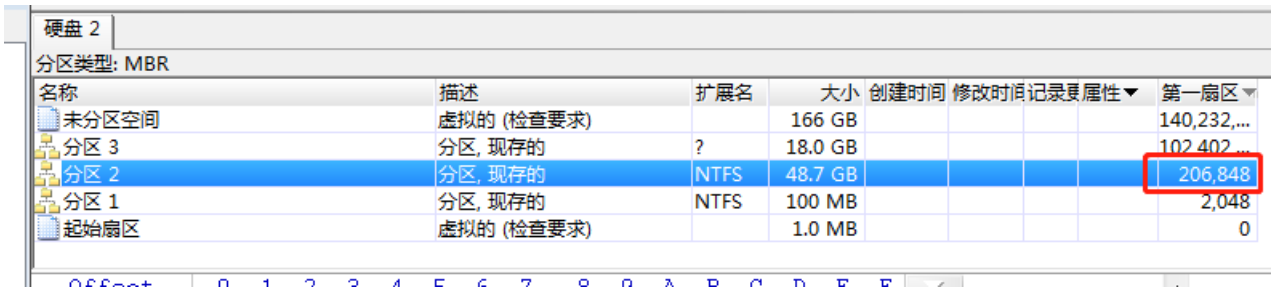
	2	根据此镜像 (Forensic Image)，里面有多少个硬盘分区？
	A.	1
	B.	2
√	C.	3
	D.	4
	E.	5

解析：使用取证大师进行分析



	3	你能找到硬盘操作系统分区内的开始逻辑区块地址（LBA）？
	A.	0
	B.	512
	C.	2,048
√	D.	206848
	E.	102,402,047

解析：HEX 32800=DEC 206848

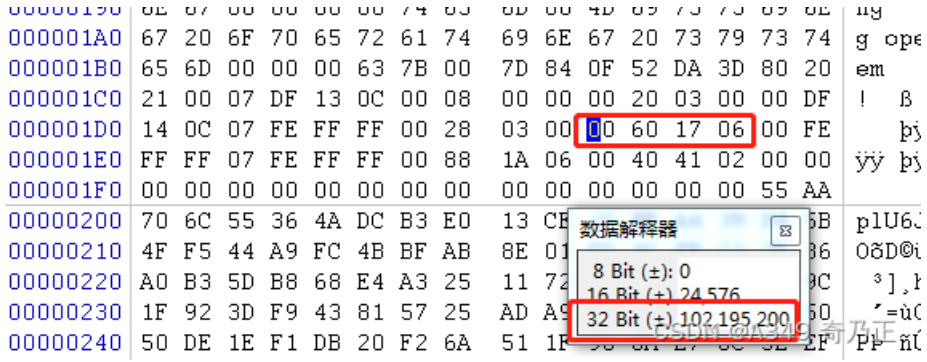


	4	你能找到硬盘操作系统分区的大小吗 (字节byte)?
	A.	48.7
	B.	102,195,200
	C.	140,232,703
	D.	19,369,295,872
√	E.	52,323,942,400

解析：winhex直接查看

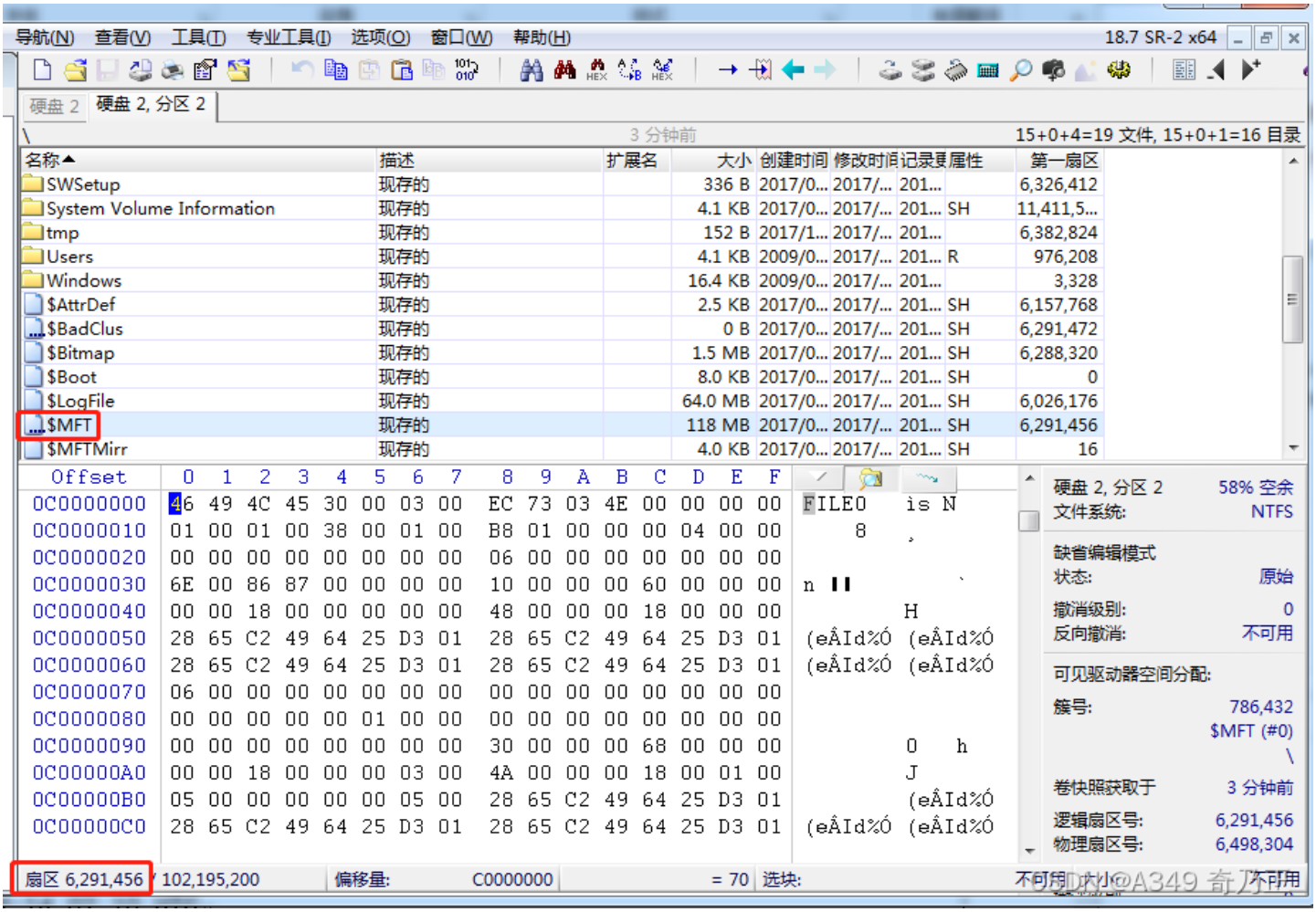
用扇区数乘以512个字节即可得出

102195200*512=?



	5	在包含操作系统的分区内，$MFT的物理起始偏移位置是什么？
	A.	3328
	B.	4170040
	C.	6026176
√	D.	6291456
	E.	16949352

解析：winhex直接查看



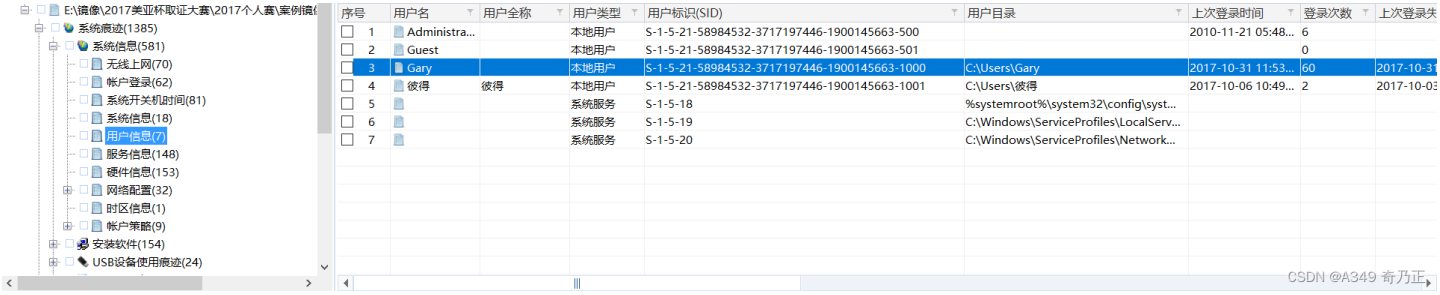
	6	请找出系统文件“SOFTWARE"，请问操作系统的安装日期是？（答案格式 一“世界协调时间"：YYYY-MM-DD HH:MM UTC）
	A.	2017-09-14 02:10 UTC
√	B.	2017-09-14 02:11 UTC
	C.	2017-09-14 02:12 UTC
	D.	2017-09-14 02:13 UTC
	E.	2017-09-14 02:14 UTC

解析：使用取证大师进行分析

	7	用户“Gary"的SID是什么？

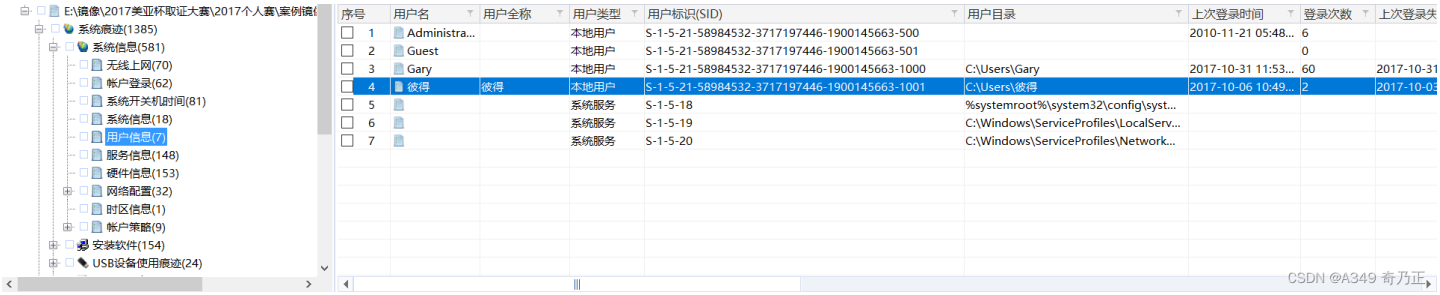
	7	用户“Gary " 的SID是什么？
√	A.	1000
	B.	1001
	C.	1002
	D.	1005
	E.	1007

解析：使用取证大师进行分析



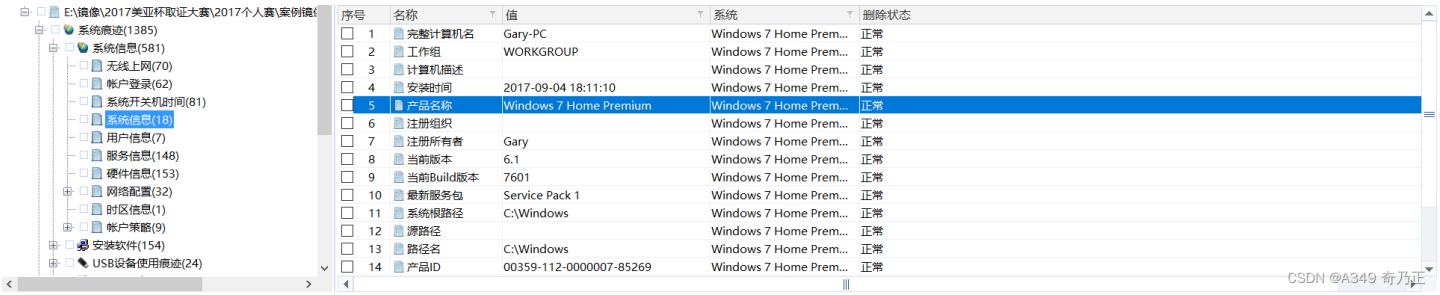
	8	用户“彼得 " 的SID是什么？
	A.	1000
√	B.	1001
	C.	1002
	D.	1005
	E.	1007

解析：使用取证大师进行分析



	9	硬盘的操作系统是什么？
√	A.	Windows 7
	B.	Windows 8
	C.	Windows 10
	D.	Linux Red Hat 7.1
	E.	MAC OS X

解析：使用取证大师进行分析



	10	哪个是Windows的默认浏览器？
√	A.	Microsoft Internet Explorer
	B.	Google Chrome
	C.	Mozilla Firefox
	D.	Opera
	E.	QQ 浏览器

解析：

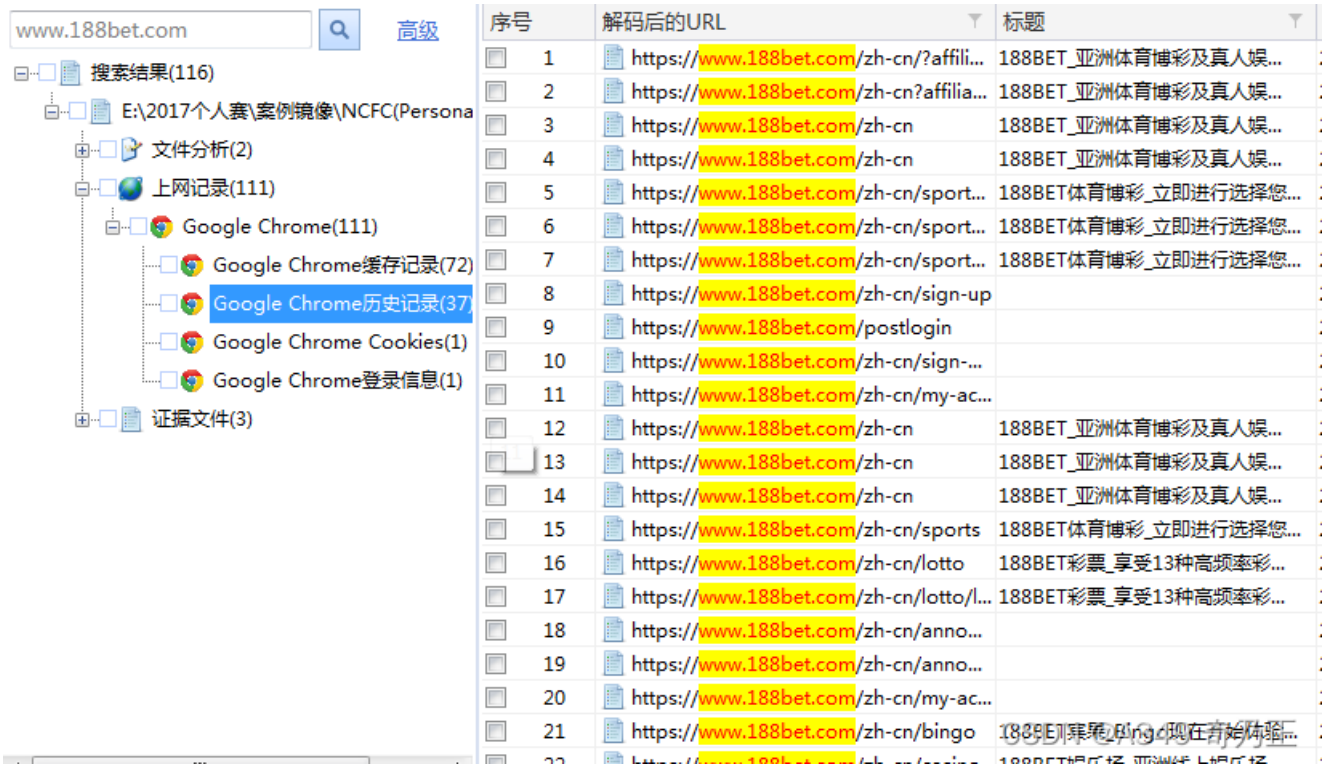
方法一：在仿真中，桌面新建txt文件，将后缀改为.html可见图标更改为相应的默认浏览器图标。

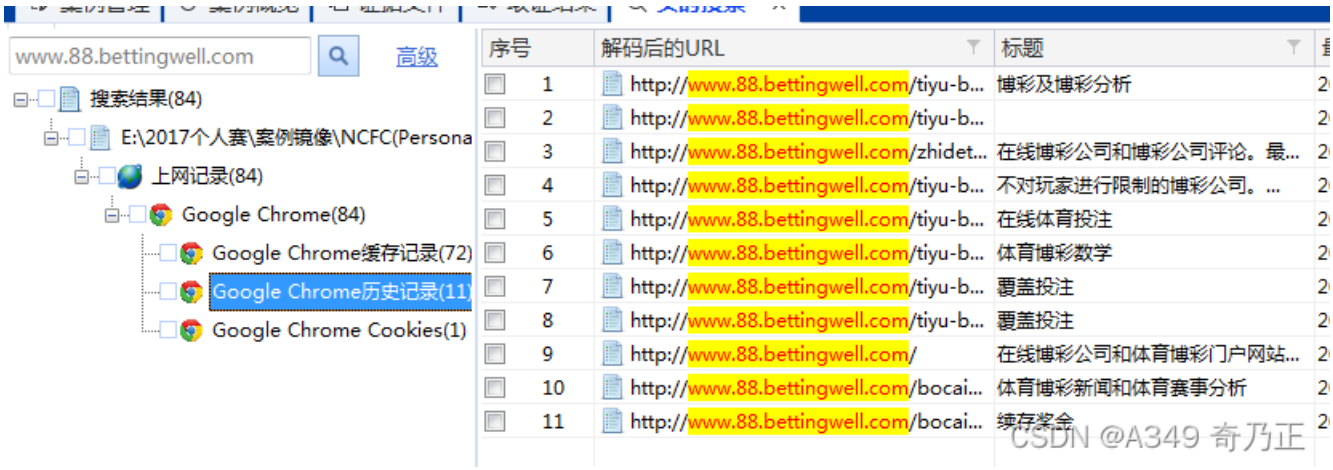
方法二：打开各个浏览器查看设置里，是否标注默认浏览器

	11	用户“Gary”曾经浏览过一些非法博彩网站，下列哪项URL符合？
	a.	www1.10086.com

	11	用户“Gary"曾经浏览过一些非法博彩网站，下列哪项URL符合？
	b.	www.188bet.com
	c.	www.hv5858.com
	d.	www.12377.cn
	e.	www.88.bettingwell.com
	f.	www.aaakk.org
	A.	只有(a) & (b)
	B.	(a), (b), (d) & (f)
	C.	(b), ©, (d) & (f)
√	D.	(b), ©, (e) & (f)
	E.	以上皆是

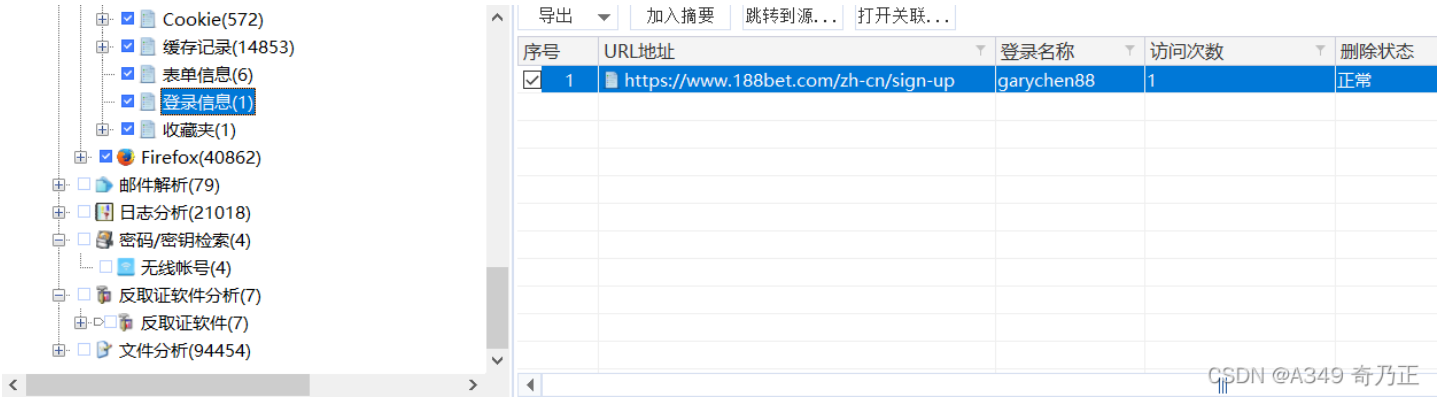
解题：搜索网址关键词





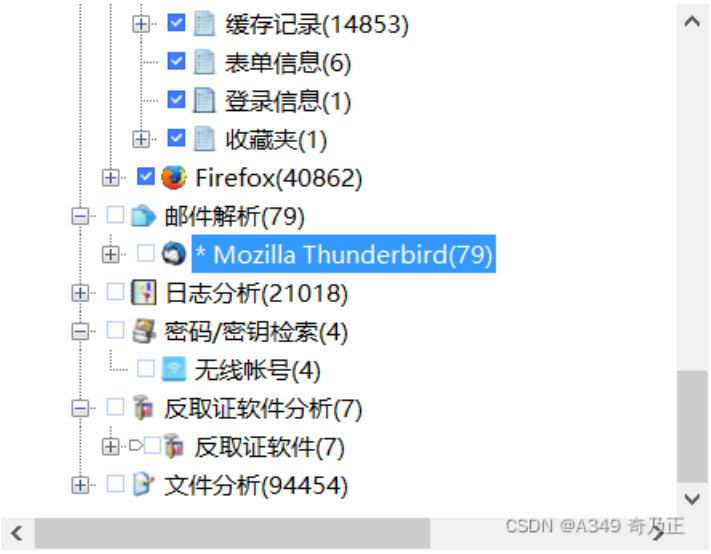
	12	用户Gary曾经登入上述非法博彩网站，下列哪个是其登入名称？
	A.	ggchey68
	B.	gany-cher88
	C.	galy_chen88
	D.	garychen1688
√	E.	garychen88

解析：在取证大师中打开浏览器解析-Google Chrome-登陆信息可见。



	13	在所有用户中，用于电子邮件发送/接收的程序名称是什么？
	A.	新浪邮箱
	B.	网易163
	C.	阿里邮箱
	D.	Foxmail
√	E.	Mozilla Mail – ThunderBird

解析：在取证大师中打开邮件解析直接可见。



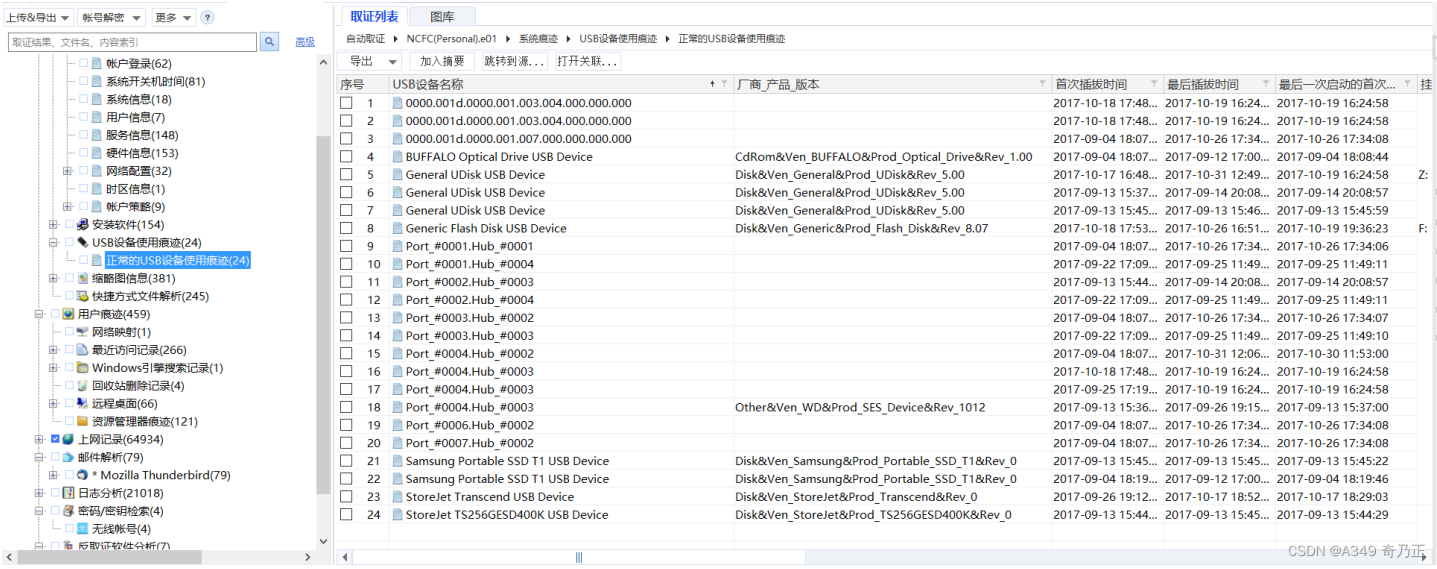
	14	在该Windows系统中，曾经连接数个USB移动储存装置 (U盘)，下列那个不是该系统连接过的USB移动储存装置？
	A.	WD My Passport 0827 USB Device

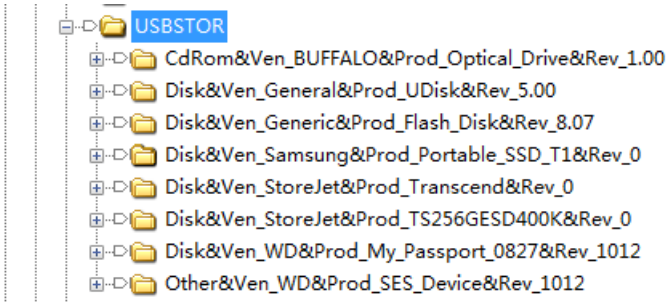
	14	**在该Windows系统中，曾经连接数个USB移动储存装置 (U盘)，下列那个不是该系统连接过的USB移动储存装置？**

	B.	StoreJet Transcend USB Device
	C.	Samsung Portable SSD USB Device
	D.	StoreJet TS256GESD400K USB Device
	E.	General UDisk USB Device

解析：在取证大师中打开USB使用痕迹查找。

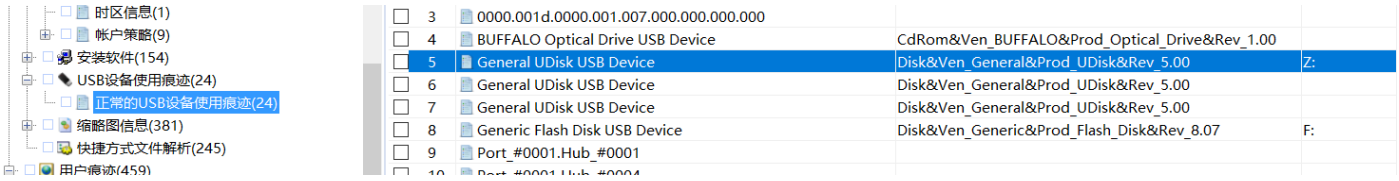
再在注册表里仔细查找发现这五个设备好像都有，这道题我感觉没有正确答案





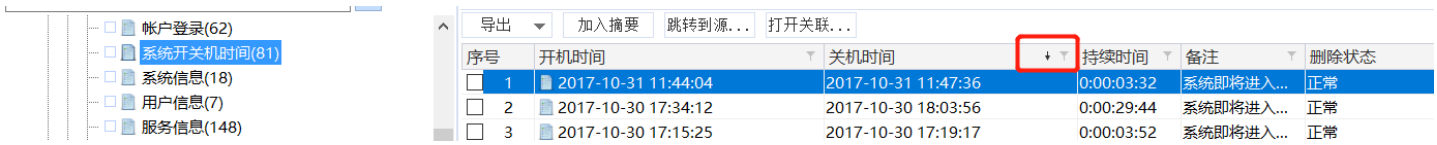
	15	**在该Windows系统中，下列哪个USB移动储存装置 (U盘)曾被指派为'Z'磁盘分区代号(Drive Letter)？**
	A.	WD My Passport 0827 USB Device
	B.	StoreJet Transcend USB Device
	C.	Samsung Portable SSD USB Device
	D.	StoreJet TS256GESD400K USB Device
√	E.	General UDisk USB Device

解析：同上题



	16	该Windows系统中，下列哪个是最后的关机时间？
	A.	2017-10-31 4:52:54 UTC
	B.	2017-10-31 4:53:54 UTC
	C.	2017-10-31 4:54:54 UTC
	D.	2017-10-31 4:55:54 UTC
	E.	2017-10-31 4:56:54 UTC

关机时间：2017-10-31 11:47:36

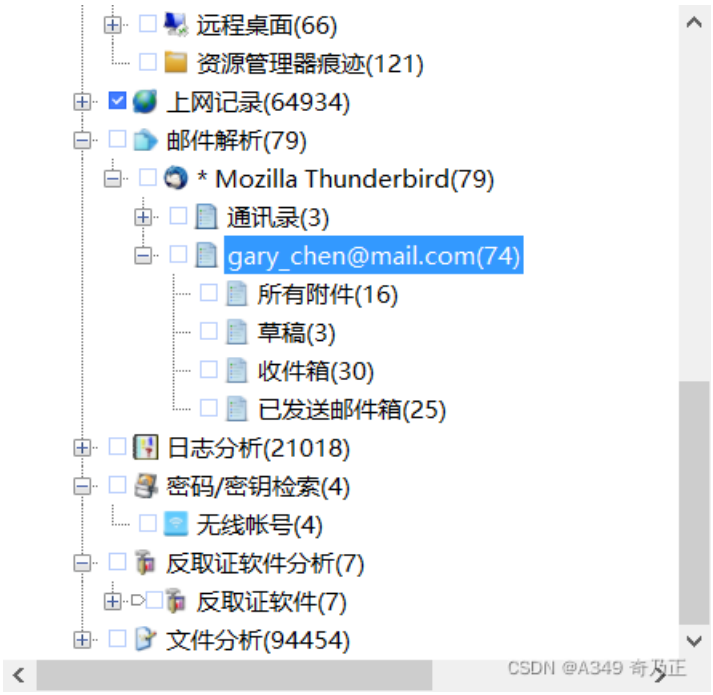


	17	该Windows系统中，下列哪个是电脑名称？
	A.	GARYPC
√	B.	GARY-PC
	C.	GARY_PC
	D.	GARY
	E.	GARY-NB

解析：在取证大师中系统信息项直接可见。

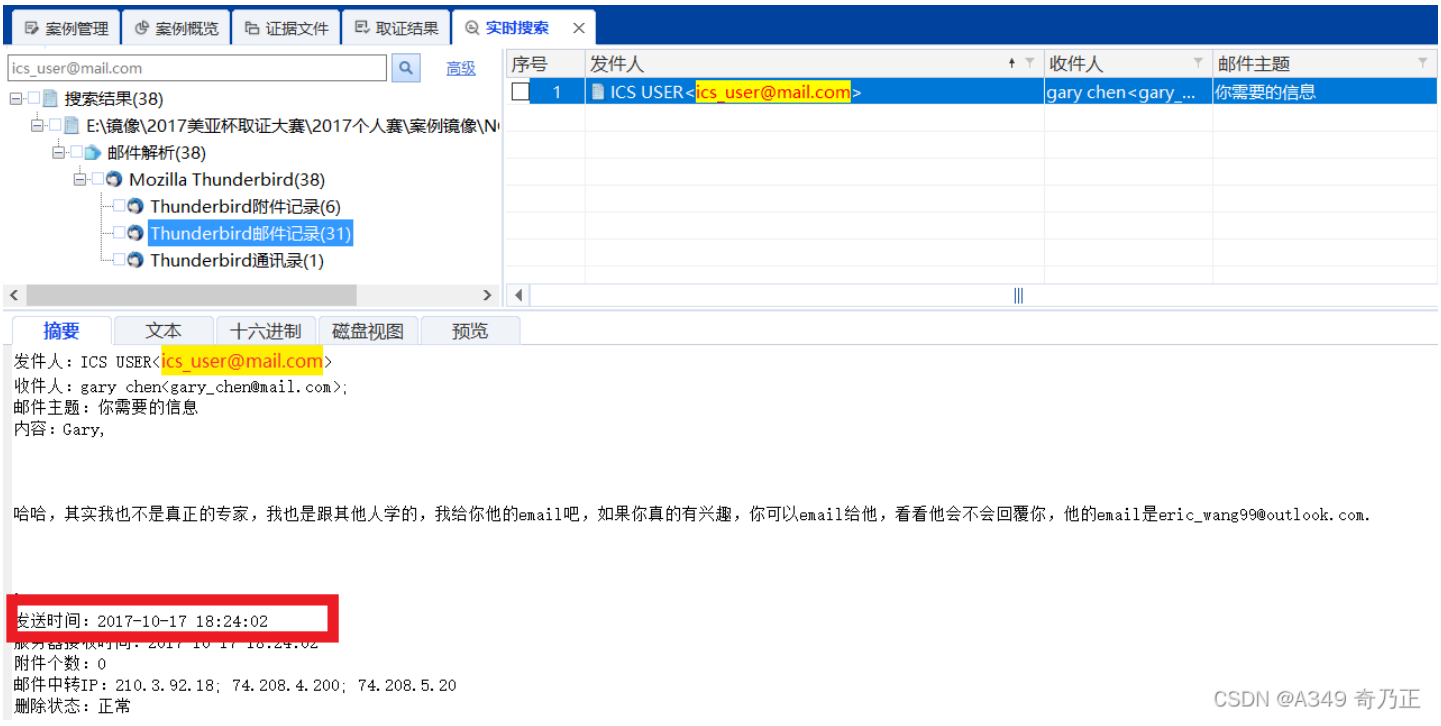
	18	在该Windows系统中，下列哪个是用户Gary日常使用的邮箱帐号？
	A.	ics_user@mail.com
	B.	ics_user@gmail.com
	C.	gary@mail.com
√	D.	gary_chen@mail.com
	E.	gary_chen@gmail.com

解析：在取证大师中打开邮件解析直接可见。



	19	**在该Windows系统中，用户Gary曾经收过一封来自邮箱帐号 ics_user@mail.com 的邮件，内容提及有关制作钓鱼网站及邮件帐号eric_wang99@outlook.com，下列哪个是此封邮件的发送日期和时间？**
	A.	2017-09-25 17:07:15
	B.	2017-10-17 14:35:45
√	C.	2017-10-17 18:24:02
	D.	2017-10-26 19:17:08
	E.	2017-10-26 19:24:57

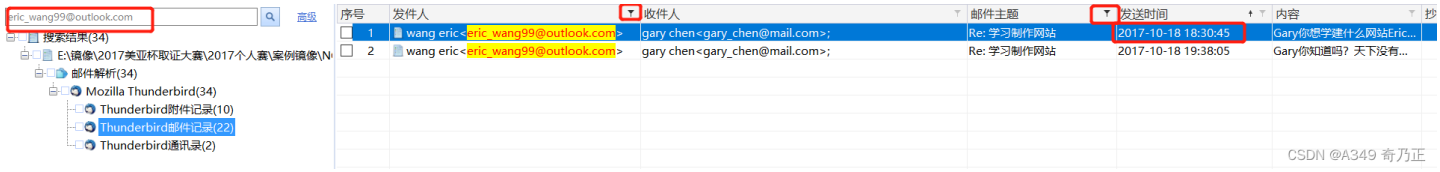
解析：在取证大师以“ics_user@mail.com”为关键词实时搜索，在邮件解析-邮件记录项中



	20	**在该Windows系统中，用户Gary还曾经收过两封来自邮箱帐号 eric_wang99@outlook.com的邮件，标题为“学习制作网站”，下列哪个是第一封邮件的发送日期和时间？**

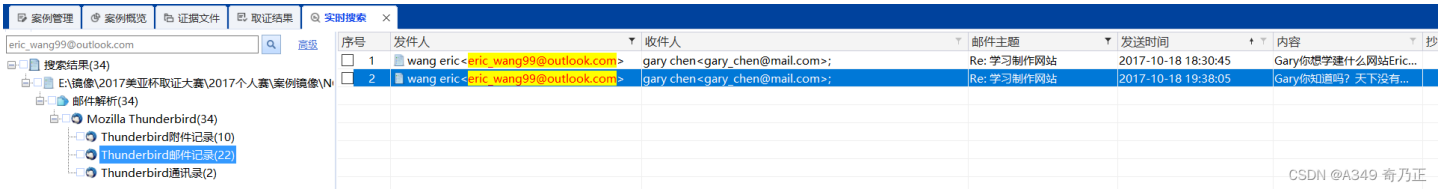
	20	在该Windows系统中，用户Gary还曾经收过两封来自邮箱帐号 eric_wang99@outlook.com的邮件，标题为“学习制作网站”，下列哪个是第一封邮件的发送日期和时间？
	A.	2017-09-25 17:07:15
	B.	2017-10-17 14:35:45
	C.	2017-10-17 18:24:02
√	D.	2017-10-18 18:30:45
	E.	2017-10-18 19:38:05

解析：在取证大师以“eric_wang99@outlook.com”为关键词实时搜索，在邮件解析-邮件记录项中查看，针对收件人和邮件主题进行过滤，按发送时间排序，得出答案。



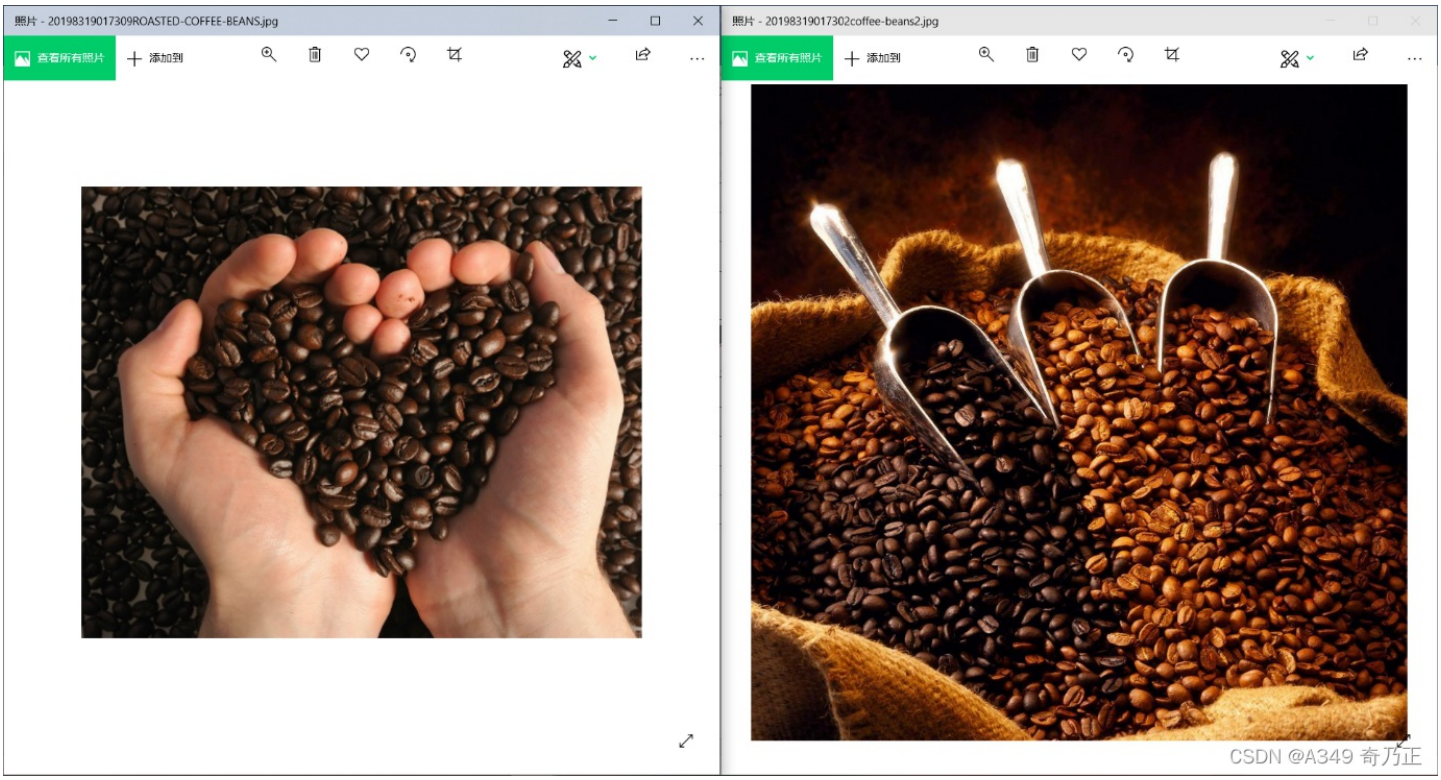
	21	在该Windows系统中，用户Gary还曾经收过两封来自邮箱帐号 eric_wang99@outlook.com邮件，标题为“学习制作网站”，下列哪个是第二封电邮的发送日期和时间？
	A.	2017-09-25 17:07:15
	B.	2017-10-17 14:35:45
	C.	2017-10-17 18:24:02
	D.	2017-10-18 18:30:45
√	E.	2017-10-18 19:38:05

解析：方法同上题。

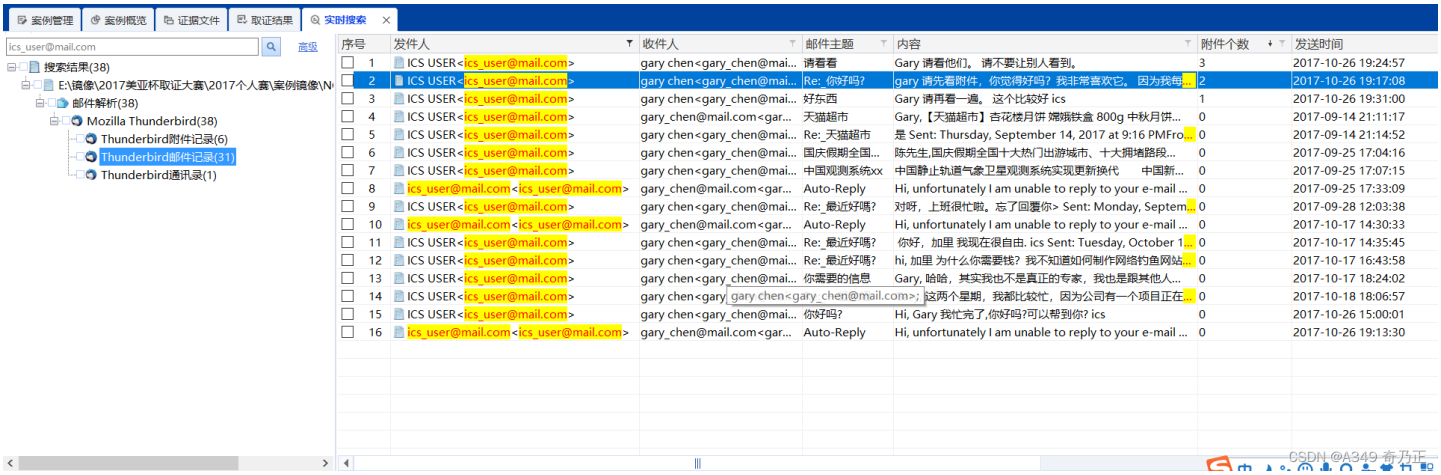


	22	用户Gary还曾经收过一封来自邮箱帐号 ics_user@mail.com 的邮件，附加了两张与咖啡豆有关的相片，下列哪个是此封邮件的发送日期和时间？
	A.	2017-09-25 17:07:15
	B.	2017-10-17 14:35:45
	C.	2017-10-17 18:24:02
√	D.	2017-10-26 19:17:08
	E.	2017-10-26 19:24:57

解析：在取证大师中以“ics_user@mail.com”为关键词实时搜索，在邮件解析-邮件记录项中对发件人和附件个数进行过滤，可得答案



序号	附件名	附件路径	附件大小(字节)
1	coffee-beans2.jpg	C:\Program Files\取证大师\FMP\Case\...	200609
2	ROASTED-COFFE...	C:\Program Files\取证大师\FMP\Case\...	96375



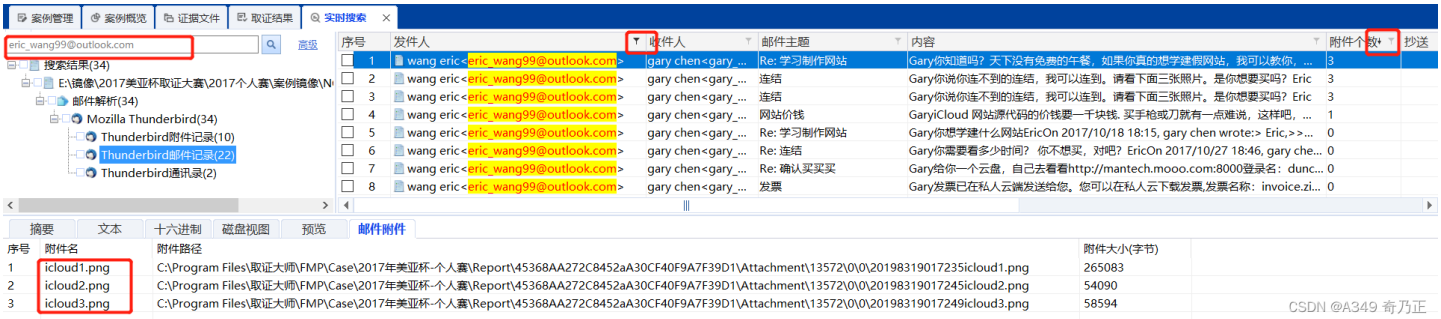
	23	下列那项是與上述咖啡豆有關相片的MD5哈希值/哈希值(Hash value)?
	A.	449cebf0eb96499df047fe0bff8e1627
√	B.	17f9c6bcca44d128f7ed6769a6920278
	C.	4bc48ce355acd4732f33a79e29728e96
	D.	4bc48ce355acd4732f33a79e29728e96

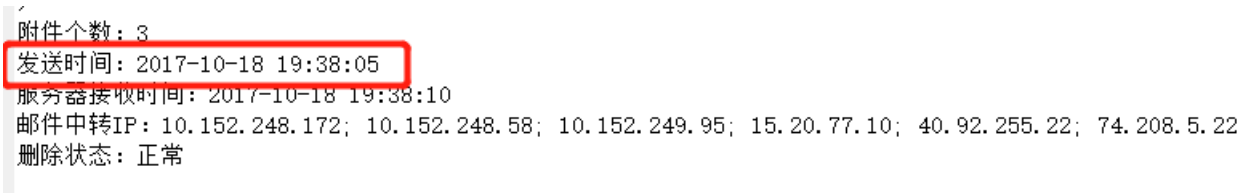
	23	下列那项是與上述咖啡豆有關相片的MD5哈希值/哈希值(Hash value)?
	E.	e3e545c80a7273b7b0d7c73dacdd7227

答案：取证大师直接计算MD5

	24	在该Windows系统中，用户Gary还曾经收到一封来自邮箱帐号 eric_wang99@outlook.com 的邮件，附加有三张与Apple iCloud相关的相片，下列哪个为该封邮件的发送日期和时间？
	A.	2017-09-25 17:07:15
	B.	2017-10-17 14:35:45
	C.	2017-10-17 18:24:02
	D.	2017-10-18 18:30:45
√	E.	2017-10-18 19:38:05

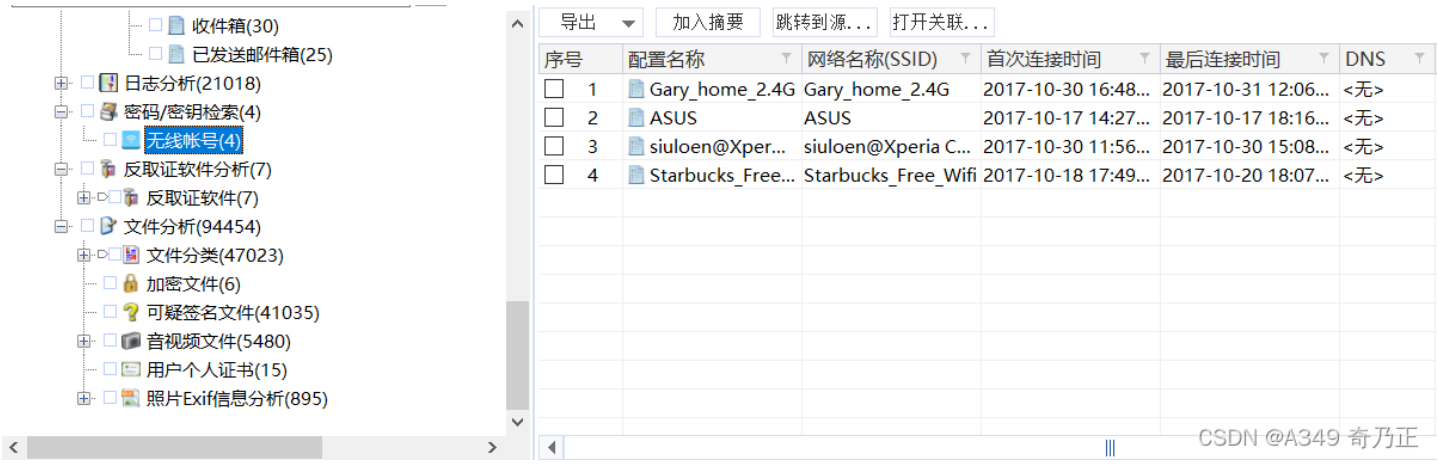
解析：在取证大师以“ics_user@mail.com”为关键词实时搜索，在邮件解析-邮件记录项中





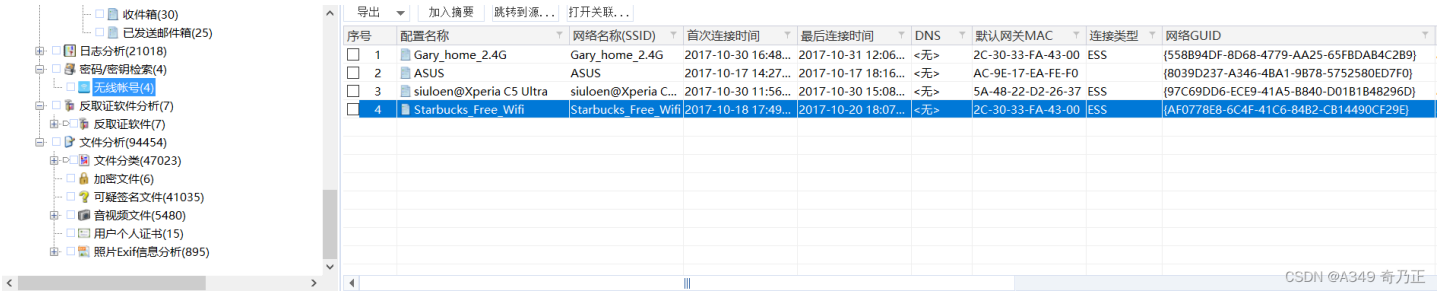
	25	Gary经常使用笔记本电脑浏览互联网，他的笔记本电脑上曾经连接过多少WIFI热点？
	A.	1
	B.	2
	C.	3
√	D.	4
	E.	5

解析：在取证大师-密码秘钥检索-无线账号中可见



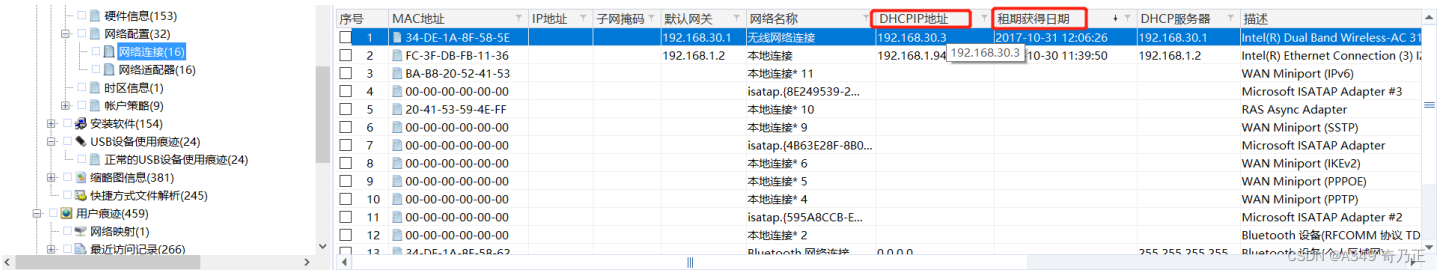
	26	上述电脑曾经连接过星巴克WIFI热点，下列哪项是其全局唯一识别元（Globally Unique Identifier, GUID）？
	A.	{8039D237-A346-4BA1-9B78-5752580ED7F0}
	B.	{39489FA0-DE35-4989-8730-E2E2ED15E85A}
	C.	{558B94DF-8D68-4779-AA25-65FBDAB4C2B9}
	D.	{4EFCDA7E-CE51-4EC2-8980-8629647C9968}
√	E.	{AF0778E8-6C4F-41C6-84B2-CB14490CF29E}

解析：同上题图，找到星巴克WIFI热点：Starbucks-Free-WiFi，可见后边的网络GUID。



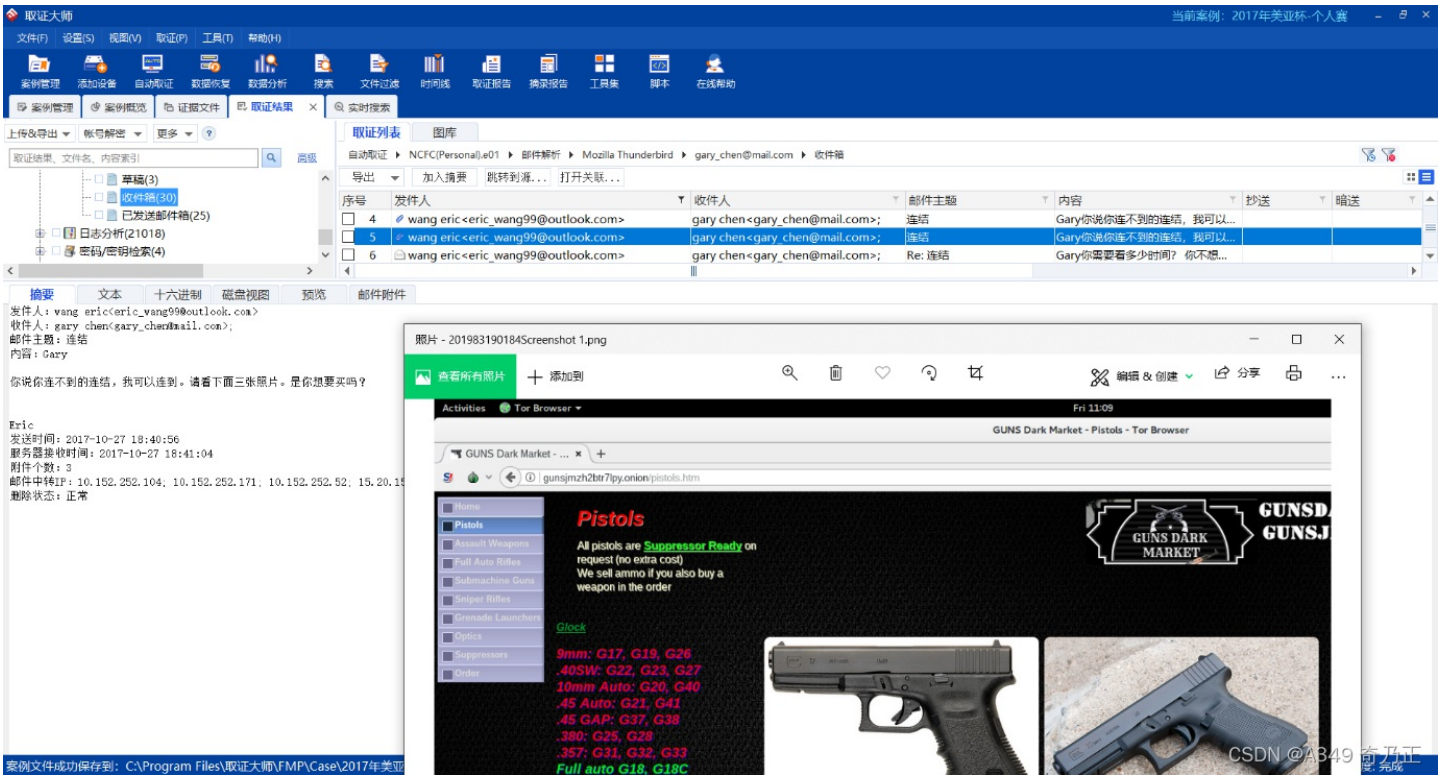
	27	有关Gary的笔记本电脑，下列哪项是其最后分派得到的IP地址？
	A.	192.168.0.1
	B.	192.168.10.4
	C.	192.168.20.6
√	D.	192.168.30.3
	E.	192.168.40.5

解析：在取证大师-网络配置-网络连接中，对租期获得时间进行排序，找到其DHCPIP地址。



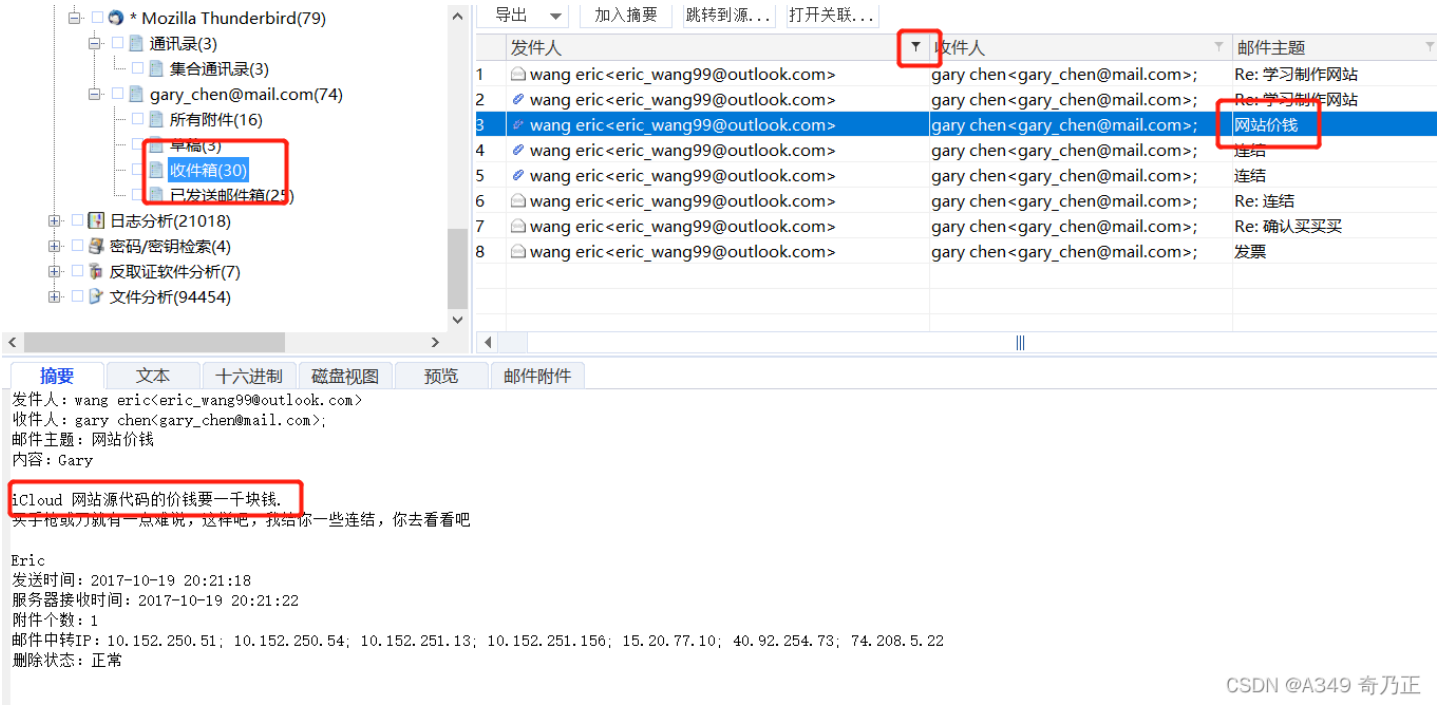
	28	Eric曾发邮件给Gary，内容是关于如何在暗网(Dark Web)中浏览枪械的信息，以下哪个URL是由Eric提供的？
	A.	http://hhnovpxmqrw5xaqg.onion
√	B.	http://gunsjmzh2btr7lpy.onion
	C.	http://gunsdtk58tolcrre.onion
	D.	http://armoryohajjhou6m.onion
	E.	http://armory45jijdf7d.onion

解析：由题意可知，Eric为发件人，在邮件解析-收件箱中对发件人进行过滤后，查看图片。



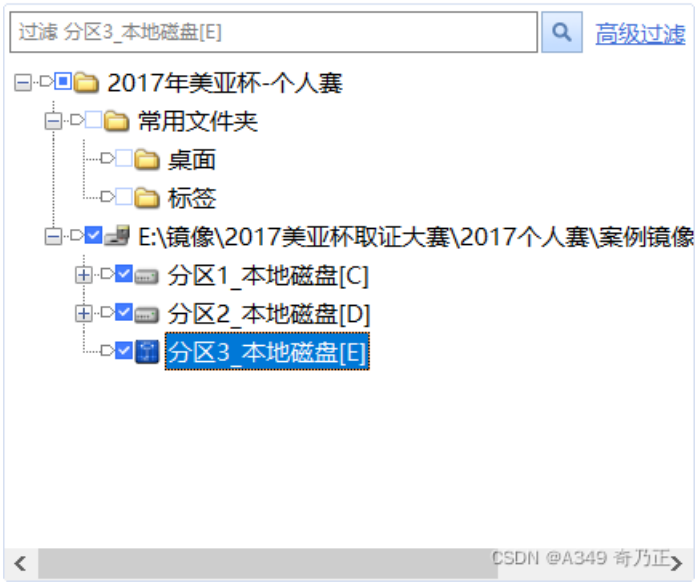
	29	Eric 售卖iCloud 网站给Gary 的价钱是多少？
	A.	$500
	B.	$800
√	C.	$1000
	D.	$1400
	E.	$1500

解析：取证大师-Mozilla thunderbird-收件箱，对发件人进行过滤，看到其中一封邮件主题为“网站价钱”，与题目相关，在摘要中发现符合题意的部分。



	30	Gary经常将非法文件存储到该笔记本电脑的加密分区中，下列哪一个为该加密软件？
	A.	TrueCrypt
√	B.	VeraCrypt
	C.	Bitlocker
	D.	LUKS
	E.	PGP WDE

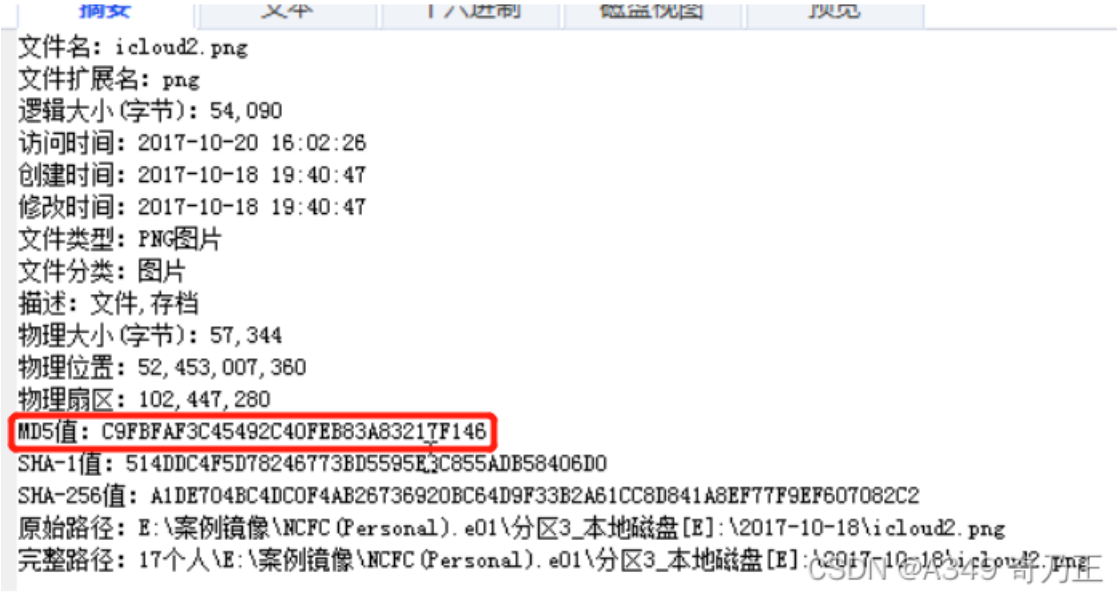
解析：



	31	在加密磁区内有三张与Apple iCloud有关的相片，下列哪个为其中一张相片的MD5哈希值(Hash Value)?
√	A.	c9fbfaf3c45492c40feb83a83217f146
	B.	14903a7bd9d709b653f9afe8e3e51cdd
	C.	7cb0f29812317db645edbcd6cf46e1ba

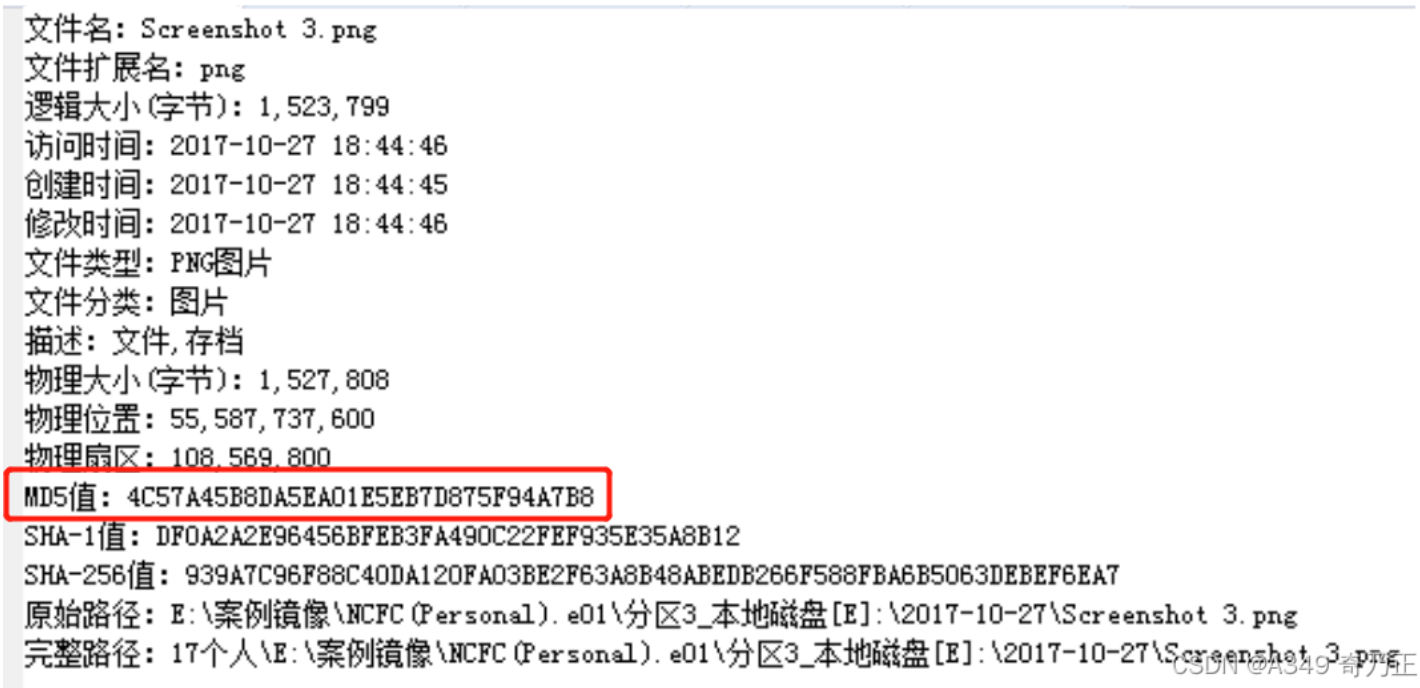
	31	在加密磁区内有三张与Apple iCloud有关的相片，下列哪个为其中一张相片的MD5哈希值(Hash Value)?
	D.	5503d096bdf832460c8f51da62fbbb5d
	E.	9918465b62171ba2c0a95595db629bf3

解析：解开加密磁盘分区，找到Apple iCloud有关的相片，计算MD5值



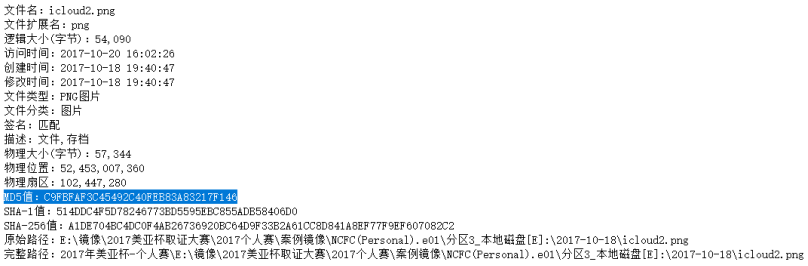
	32	在加密磁区内有三张与暗网(Dark Web)有关的相片，下列哪个为其中一张相片的MD5哈希值(Hash Value)?
	A.	2836d35fb45c591211d5b6865c4a82f5
	B.	d2b14799050b6c4ad6b07cd1227b91a5
	C.	9110c96baa70c00acd8fbdfe2dc7c397
	D.	703899985d881e2d103eb4fd1306be2e
√	E.	4c57a45b8da5ea01e5eb7d875f94a7b8

解析：找到相应图片，计算MD5即可



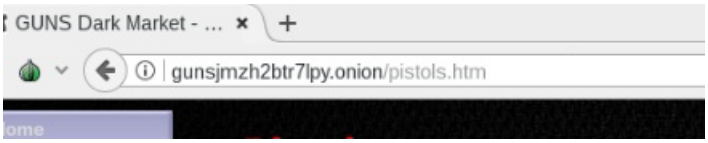
	33	Gary的计算机系统时区是什么？？
√	A.	中国标准时间
	B.	日本标准时间
	C.	泰国标准时间
	D.	新加坡标准时间
	E.	伦敦标准时间

解析：取证大师直接查看



	34	在上述加密磁区内，存有一个名为”2017-10-27”的文件夹，内有三张枪械的图片，该三张图片是来自哪个网站？
	A.	http://gunsdtk58tolcrre.onion
√	B.	http://gunsjmzh2btr7lpy.onion
	C.	thegunstorelasvegas.com
	D.	cabelas.com
	E.	hyattgunstore.com

解析：找到相应图片，找到网址即可



	35	Gary的笔记本电脑曾经下载过多少张有关恐怖组织的图片？
	A.	1
	B.	2
	C.	3
	D.	4
	E.	5

解析：你说几张就几张。。。恐怖组织图片到底怎么算

	36	根据Gary与Eric邮件的内容，Eric曾经提供Gary一个私有云盘，下列哪项是该邮件提供的资料？
	A.	动物图

	36	根据Gary与Eric邮件的内容，Eric曾经提供Gary一个私有云盘，下列哪项是该邮件提供的资料？
√	B.	枪的结构图
	C.	博彩图
	D.	博彩文件
	E.	恐怖主义图

解析：查找相关邮件

	37	下列哪项是上述私有云盘的网址？
	A.	http://mantech.mooo.cn
√	B.	http://mantech.mooo.com
	C.	http://mooo.com
	D.	http://mantech.com
	E.	http://23.54.45.113

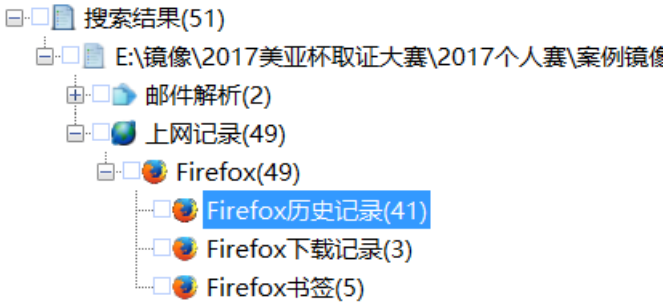
解析：查找相关邮件

	38	下列哪项是上述私有云盘网址的连接端口？
	A.	TCP 80
	B.	TCP 8080
	C.	UDP 80
√	D.	TCP 8000
	E.	TCP 443

解析：查找相关邮件，同上题图

	39	下列哪项是Gary第一次浏览该私有云盘网址时，所使用的浏览器？
	A.	Microsoft Explorer
	B.	Google Chrome
√	C.	Mozilla Firefox
	D.	Opera
	E.	QQ 浏览器

解析：以云盘地址为关键词进行搜索，发现答案

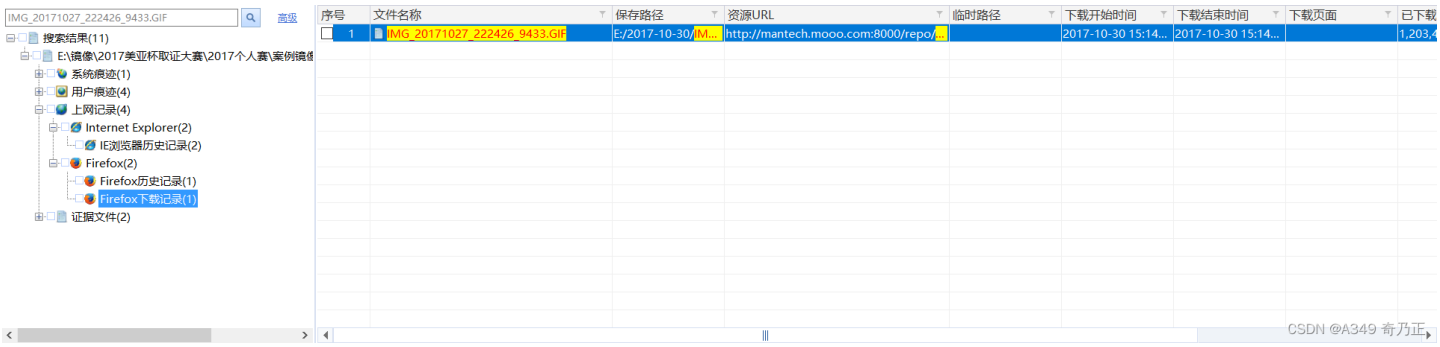


	40	下列哪项是Gary第一次浏览该私有云盘网址的日期和时间？
	A.	2017-10-29 12:42:09
	B.	2017-10-30 12:42:09
	C.	2017-10-31 12:42:09
	D.	2017-10-30 10:42:09
	E.	2017-10-30 11:42:09

2017-10-30 12:42:11

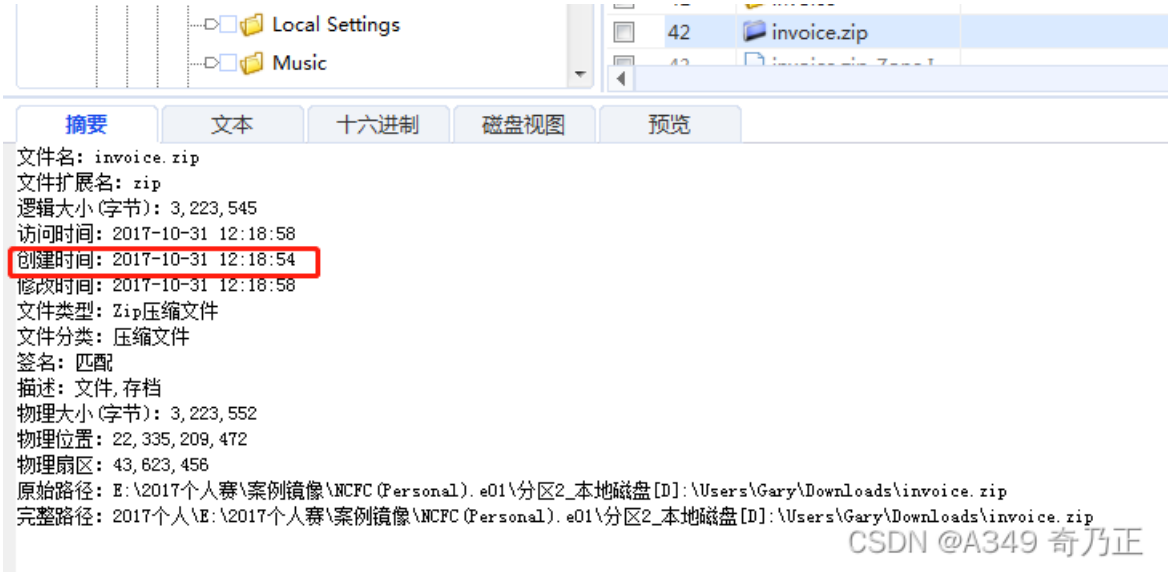
	41	在上述加密磁区内，存有一个名为”2017-10-30”的文件夹，里面有三张与枪械结构有关的图片，该三张图片是从哪个方法/软件下载？
	A.	邮件
√	B.	Firefox
	C.	Chrome
	D.	USB thumb drive
	E.	ftp

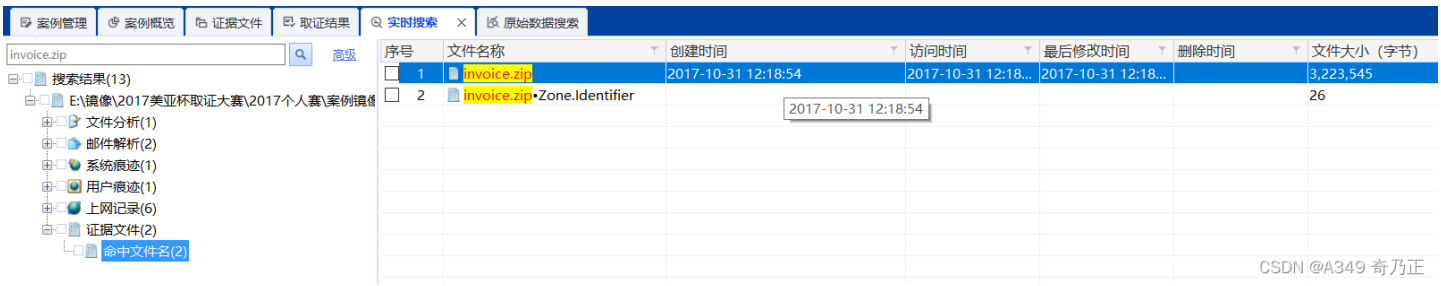
解析：找到文件夹，查看图片名称，以图片名称进行搜索



	42	Gary的笔记本电脑，曾经下载过一个感染了电脑病毒的文件，名为invoice.zip。该病毒程序文件是什么时候下载？
	A.	2017-10-31 12:26:20
	B.	2017-10-31 12:50:34
	C.	2017-10-31 12:29:55
	D.	2017-10-31 10:52:10
√	E.	2017-10-31 12:18:54

解析：以文件名“invoice.zip”为关键词进行搜索，在搜索结果中-证据文件
-命中文件名中可找到答案。



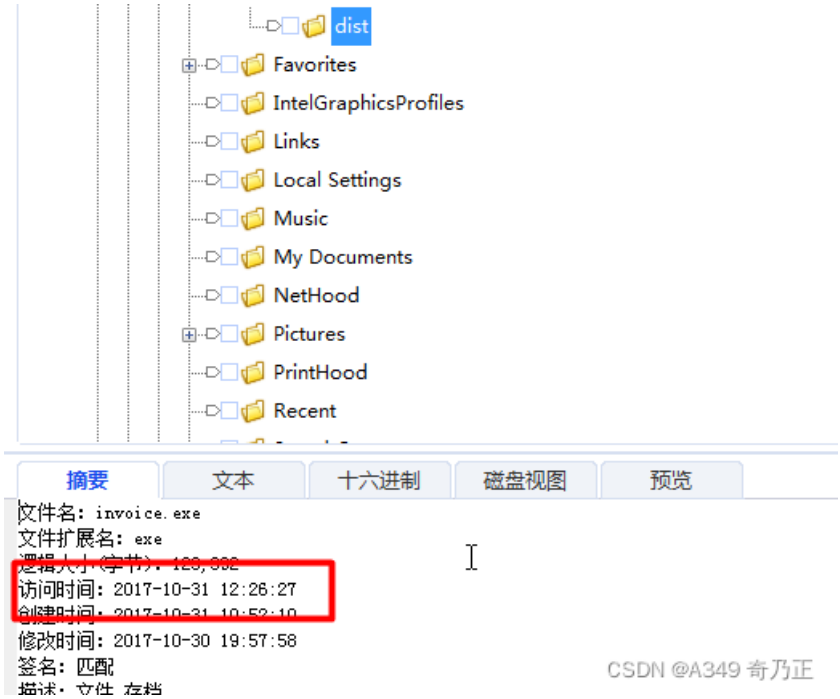


	43	Gary的笔记本电脑，还存有一个感染了电脑病毒的程序文件，名为\User\Gary\Downloads\invoice\dist\invoice.exe。该文件的最后存取日期/时间(Last Accessed Data/Time) 是什么？
√	A.	2017-10-31 12:26:27
	B.	2017-10-31 12:50:34
	C.	2017-10-31 12:29:55

	43	Gary的笔记本电脑，还存有一个感染了电脑病毒的程序文件，名为\User\Gary\Downloads\invoice\dist\invoice.exe。该文件的最后存取日期/时间(Last Accessed Data/Time) 是什么？

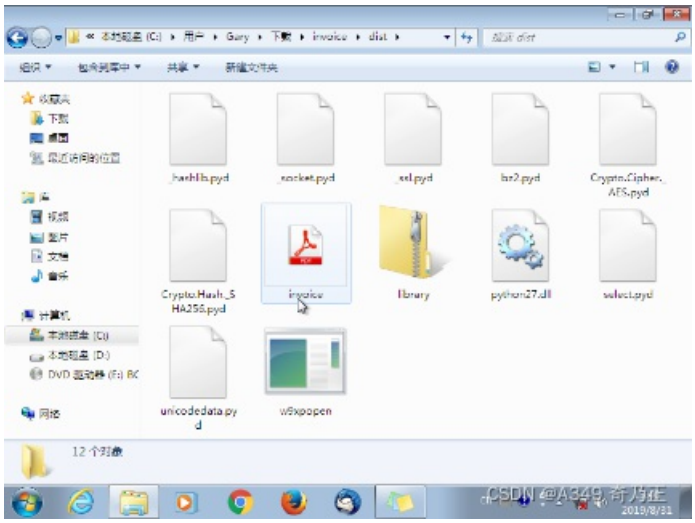
	D.	2017-10-31 10:52:10
	E.	2017-10-31 12:18:54

解析：通过路径找到文件，可找到答案



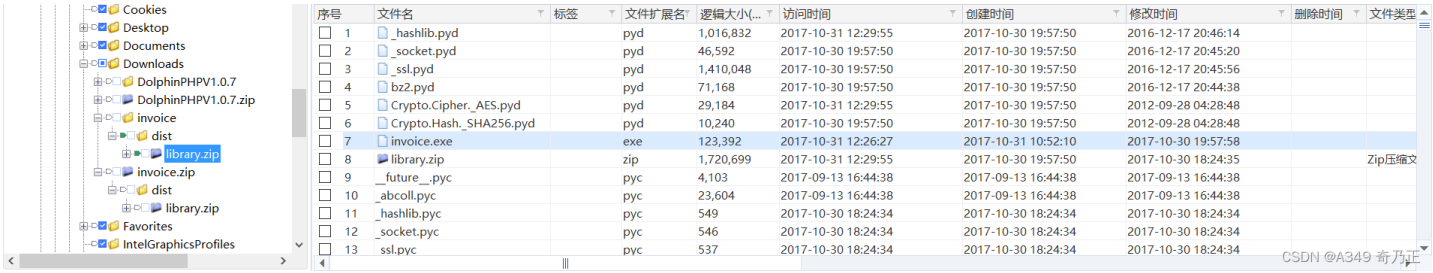
	44	上述invoice.exe文件伪装成什么格式的软件？
√	A.	pdf
	B.	jpg
	C.	psd
	D.	Docx
	E.	Doc

解析：在仿真系统中，可看到这个文件的图标为PDF图标



	45	上述的\User\Gary\Downloads\invoice\dist\invoice.exe文件，最后执行日期/时间(Last Accessed Data/Time) 是什么？
√	A.	2017-10-31 12:26:27
	B.	2017-10-31 12:50:34
	C.	2017-10-31 12:29:55
	D.	2017-10-31 10:52:10
	E.	2017-10-31 12:18:54

解析：找到文件，查看访问时间

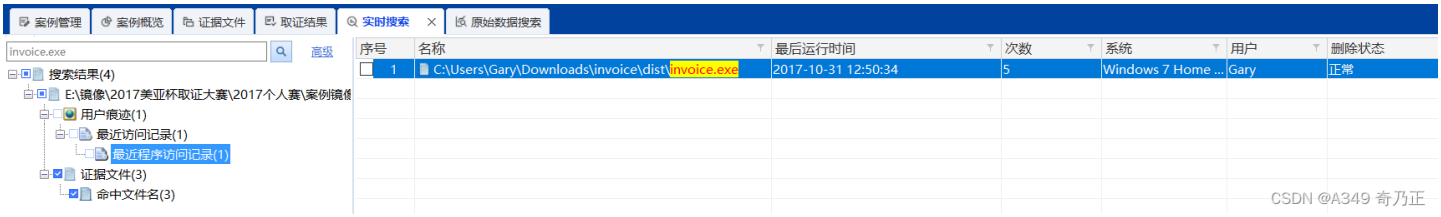


	46	事实上，Gary的笔记本电脑被电脑病毒感染了，部份文件被加密，当中包括下列哪种文件类型？
	a.	exe
	b.	gif
	c.	jpg
	d.	psd
	e.	Docx
	f.	Doc
	A.	只有(a) & (b)
	B.	(a), (b), (d) & (f)
	C.	(b), ©, (d) & (f)
√	D.	(b), ©, (e) & (f)
	E.	以上皆是

本题没找到有说服力的证据

	47	上述\User\Gary\Downloads\invoice\dist\invEoice.exe文件共执行多少？
	A.	1
	B.	2
	C.	3
	D.	4
	E.	5

解析：搜索文件，找到最近访问记录即可



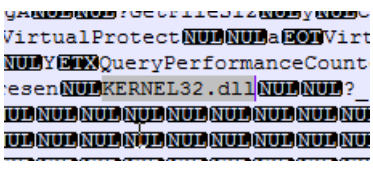
	48	上述\User\Gary\Downloads\invoice\dist\invoice.exe文件是由什么程序编写？
	A.	LISP
	B.	C++
	C.	Visual Basic
√	D.	Python
	E.	Java

解析：有py配置脚本

	49	上述\User\Gary\Downloads\invoice\dist\invoice.exe文件，执行时会呼叫下列哪个动态连结函式库(Dynamic Linked Library)
√	A.	KERNEL32.DLL ruanjian
	B.	USER32.DLL
	C.	SHELL32.DLL baogongtou
	D.	NTDLL.DLL neihe
	E.	SYSTEM32.DLL

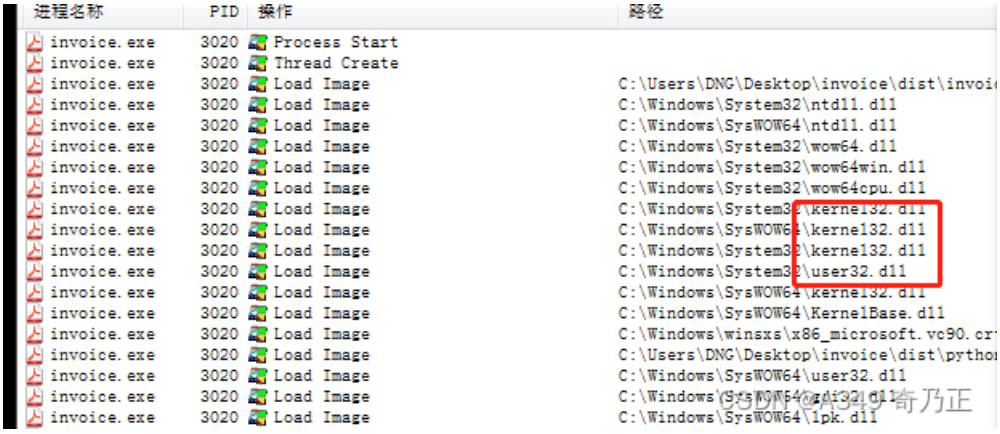
解析：

方法一：直接用文本方式打开搜索关键字dll（这是一个应试为了快才做的方法）



方法二：把这个可执行文件拖进一个空的win7虚拟机中，使用process monitor进行分析

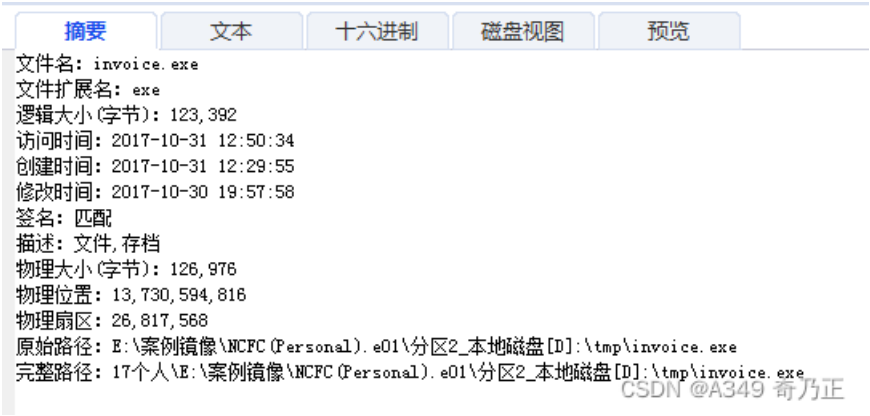
结果发现，这到底是答案似乎应该是多选，而不是单选，我个人觉得我的方法没问题。



	进程名称	PID	操作	路径
	invoice.exe	3020	Process Start	
	invoice.exe	3020	Thread Create	
	invoice.exe	3020	Load Image	C:\Users\DNG\Desktop\invoice\dist\invoi
	invoice.exe	3020	Load Image	C:\Windows\System32\ntdll.dll
	invoice.exe	3020	Load Image	C:\Windows\SysWOW64\ntdll.dll
	invoice.exe	3020	Load Image	C:\Windows\System32\wow64.dll
	invoice.exe	3020	Load Image	C:\Windows\System32\wow64win.dll
	invoice.exe	3020	Load Image	C:\Windows\System32\wow64cpu.dll
	invoice.exe	3020	Load Image	C:\Windows\System32\kernel32.dll
	invoice.exe	3020	Load Image	C:\Windows\SysWOW64\kernel32.dll
	invoice.exe	3020	Load Image	C:\Windows\System32\kernel32.dll
	invoice.exe	3020	Load Image	C:\Windows\System32\user32.dll
	invoice.exe	3020	Load Image	C:\Windows\SysWOW64\kernel32.dll
	invoice.exe	3020	Load Image	C:\Windows\SysWOW64\KernelBase.dll
	invoice.exe	3020	Load Image	C:\Windows\winsxs\x86_microsoft.vc90.cr
	invoice.exe	3020	Load Image	C:\Users\DNG\Desktop\invoice\dist\pytho
	invoice.exe	3020	Load Image	C:\Windows\SysWOW64\user32.dll
	invoice.exe	3020	Load Image	C:\Windows\SysWOW64\gdi32.dll
	invoice.exe	3020	Load Image	C:\Windows\SysWOW64\1pk.dll

	50	Gary的笔记本电脑，还存有另一感染了电脑病毒的程序文件，名为\tmp\invoice.exe。该文件的最后存取日期/时间(Last Accessed Data/Time) 是什么？
	A.	2017-10-31 12:26:27
√	B.	2017-10-31 12:50:34
	C.	2017-10-31 12:29:55
	D.	2017-10-31 10:52:10
	E.	2017-10-31 12:18:54

解析：

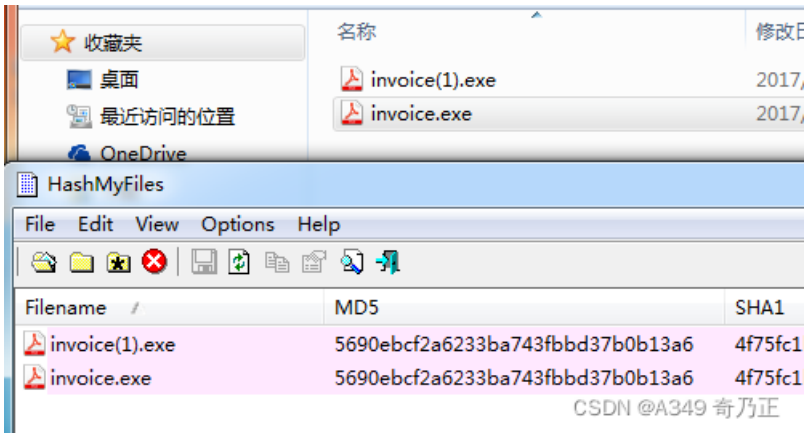


摘要 | 文本 | 十六进制 | 磁盘视图 | 预览

文件名：invoice.exe
文件扩展名：exe
逻辑大小(字节)：123,392
访问时间：2017-10-31 12:50:34
创建时间：2017-10-31 12:29:55
修改时间：2017-10-30 19:57:58
签名：匹配
描述：文件,存档
物理大小(字节)：126,976
物理位置：13,730,594,816
物理扇区：26,817,568
原始路径：E:\案例镜像\NCFC(Personal).e01\分区2_本地磁盘[D]:\tmp\invoice.exe
完整路径：17个人\E:\案例镜像\NCFC(Personal).e01\分区2_本地磁盘[D]:\tmp\invoice.exe

	51	上述两个文件\User\Gary\Downloads\invoice\dist\invoice.exe和 \tmp\invoice.exe是什么关系？
	A.	前者是后者的复本
√	B.	后者是前者的复本
	C.	两者MD5不相同
	D.	两者元数据(Metadata)相同
	E.	两者无关系

解析：使用process monitor，发现这个文件一运行，就复制一个和自己一模一样的文件。

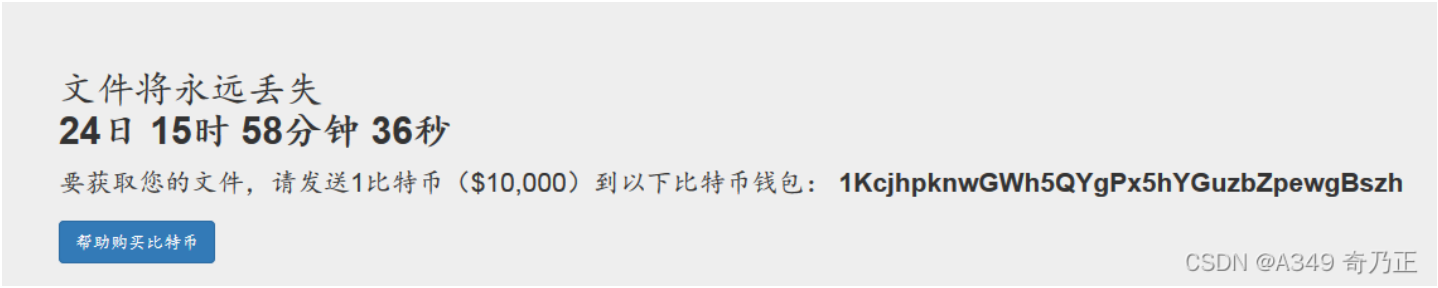


	52	根据勒索讯息的显示，勒索网址是什么？
	A.	http://223.17.250.208:6000/C&C/
	B.	http://223.17.250.208/C&C/
√	C.	http://223.17.250.208:6060/C&C/
	D.	http://223.17.250.208:80/C&C/
	E.	http://223.17.250.208:8080/C&C/

解析：

	53	根据勒索讯息的显示，勒索金额是多少钱？
	A.	$1,000
√	B.	$10,000
	C.	$20,000
	D.	$50,000
	E.	$100,000

解析：



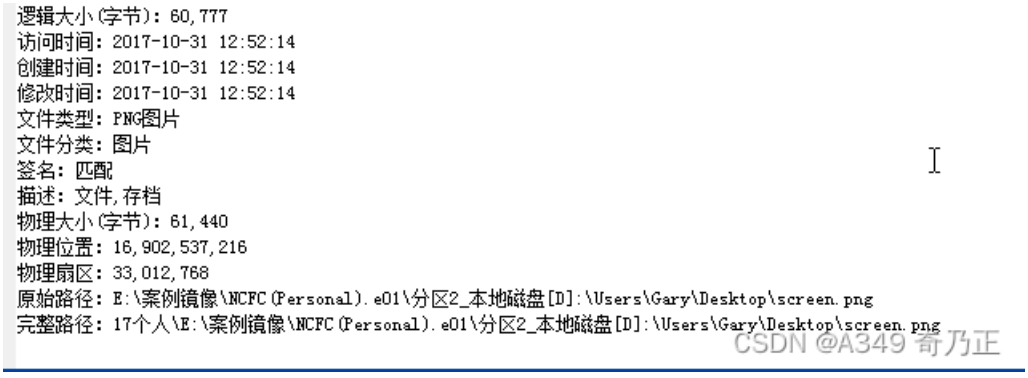
	54	根据勒索讯息的显示，下列哪个是与勒索案件有关的比特币钱包？
	A.	1KcjhpkowGWh5QYgPx5hYGuzbZpewgBszh
√	B.	1KcjhpknwGWh5QYgPx5hYGuzbZpewgBszh
	C.	1KcjhpknwGWh5QYgPx5hYGuzbZpewgBzzh
	D.	1KcjhpknwGWh5QYgPx6hYGuzbZpewgBszh
	E.	1KcjhpknwGWh6QYgPx5hYGuzbZpewgBszh

解析：

1KcjhpknwGWh5QYgPx5hYGuzbZpewgBszh

	55	执法机关曾在现场对Gary的电脑进行电子法证检验，期间曾撷取与勒索软件相关的屏幕影像，并储存为png格式。下列哪项是其储存位置？
	A.	\Users\彼得\Downloads\
	B.	\Users\彼得\Desktop\
	C.	\Users\Gary\Downloads\
√	D.	\Users\Gary\Desktop\
	E.	\Users\Gary\Documents

解析：



Keys point 分高下

	经法证工具分析后发现Gary的笔记本电脑有三个分区硬盘，所有敏感文件均储存在一个加密磁区，而其加密匙放在下列哪个位置？	
	A.	\Windows\

	经法证工具分析后发现Gary的笔记本电脑有三个分区硬盘，所有敏感文件均储存在一个加密磁区，而其加密匙放在下列哪个位置？	
	B.	\Users\
	C.	\Users\Gary\Desktop
	D.	\Users\Gary\Documents
√	E.	\

解析：

这个文件在C盘根目录下，文件名是mk

ws\ |
	B.	\Users\
	C.	\Users\Gary\Desktop
	D.	\Users\Gary\Documents
√	E.	\

解析：

这个文件在C盘根目录下，文件名是mk